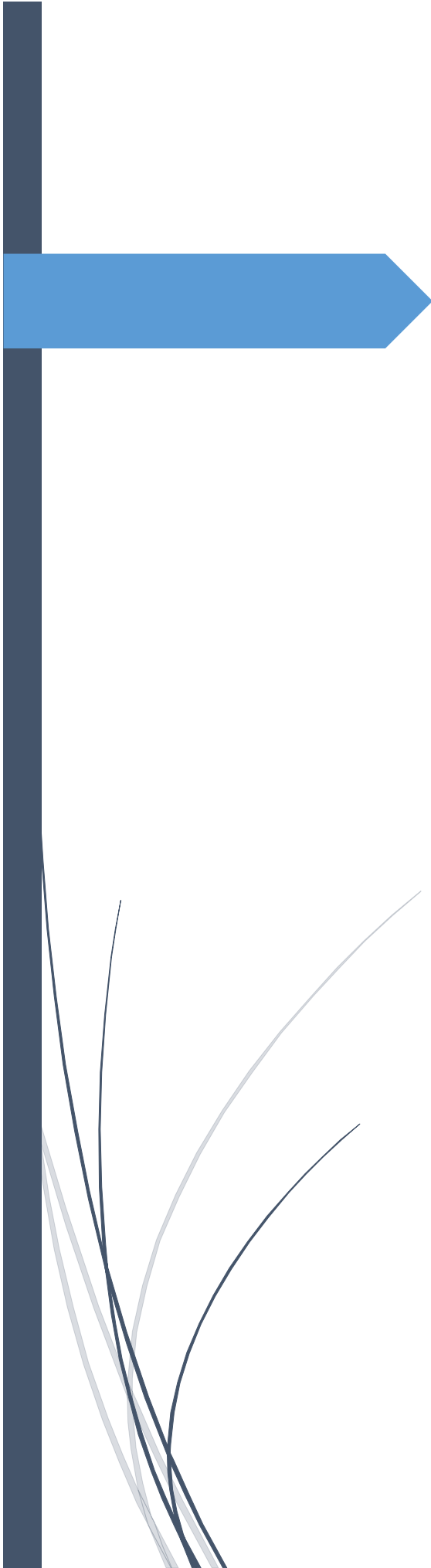




METASPLOIT 4.11

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Оглавление

Приступая к работе.	14
Что такое Metasploit?	14
Metasploit Framework	14
Metasploit Pro и прочие коммерческие издания	14
Совместимость Metasploit	15
Компоненты Metasploit Pro	15
Основные понятия и термины	16
Рабочий процесс Metasploit Pro	18
Получение доступа к Metasploit Pro	19
Поддерживаемые браузеры	19
Изучение страницы проектов	20
Основная панель инструментов\Global Toolbar	21
Мастера быстрого запуска\Quick Start Wizards	21
Новости продукта\Product News.....	22
Создание проекта.....	23
Получение целевых данных	24
Сканирование целей.....	24
Импорт данных.....	25
Просмотр и управление данными хоста	25
Запуск сканирования уязвимостей	26
Поиск и использование уязвимостей простым способом.....	28
Эксплуатация известных уязвимостей	28
Автоматическое использование эксплойтов	28
Ручное использование эксплойтов.....	29
Конфигурирование общих настроек модуля эксплойта	30
Пост-эксплуатация и сбор полезных данных.....	30
Создание отчета	31
Создание и управление проектами.....	31
Создание проекта.....	32
Удаление проекта.	33
Установка диапазона сети.	34
Ограничение работы проекта до сетевого диапазона	36
Изменение владельца проекта.....	38

Управление доступом пользователей.....	39
Командная работа.....	40
Добавление пользователей в проект.....	41
Удаление пользователей из проекта.....	42
Переназначение проекта пользователю.....	43
Комментарии к хостам.....	44
Добавление комментариев к хостам.....	44
Обновление комментария к хосту.....	45
Управление учетными записями.....	46
Типы учётных записей.....	46
Создание учётной записи пользователя.....	47
Требования к учётным записям.....	48
Смена пароля учётной записи.....	48
Удаление аккаунта пользователя.....	50
Поисковое сканирование.....	51
Как работает поисковое сканирование.....	52
Сканирование пинга.....	52
Сканирование портов.....	52
Определение операционных систем и их версий.....	52
Импорт данных.....	52
Порты, включенные в поисковое сканирование.....	53
Параметры поискового сканирования.....	53
Указание адресов IPv6.....	55
Импорт файла с адресами IPv6.....	55
Запуск поискового сканирования.....	56
Просмотр результатов сканирования.....	57
Данные, полученные при поисковом сканировании.....	58
Расшифровка статусов хоста.....	58
Сканирование на уязвимости с помощью Nexpose.....	58
Терминология Nexpose.....	59
Скачивание и установка Nexpose.....	59
Добавление консоли Nexpose.....	59
Запуск сканирования Nexpose.....	61
Импорт данных Nexpose.....	62
Импорт Nexpose Simple XML или XML-файл экспорта.....	62
Импортирование существующих в Nexpose групп хостов.....	63

Импорт данных.....	63
Импортирование данных из сканеров уязвимостей	63
Поддерживаемые отчеты сканирования	64
Импортирование данных Nexpose	65
Импорт Nexpose Simple XML или XML-файл экспорта	65
Импортирование существующих в Nexpose сайтов	65
Проверка уязвимостей	66
Подтверждение уязвимостей Помощником проверки уязвимостей	66
Последовательность работы с Помощником проверки уязвимостей	67
Перед использованием Помощника	67
Добавление консоли Nexpose.....	67
Настройка и запуск Помощника проверки уязвимостей.....	68
Отправка результатов в Nexpose	81
Правила проверки.....	81
Исключенные уязвимости	82
Доступ к странице исключений.....	82
Доступ к странице исключений из списка уязвимостей	83
Получение доступа к странице исключений с отдельной страницы уязвимости	84
Разбираемся в статусах.....	84
Статусы в списке уязвимостей	84
Статусы на странице уязвимости	85
Разбираемся с кодами результатов	85
Отметка Not Exploitable	85
Отправка подтвержденных уязвимостей.....	86
Отправка подтвержденных уязвимостей при помощи Помощника проверки уязвимостей	86
Отправка подтвержденных уязвимостей со страницы списка уязвимостей.....	87
Отправка одной подтвержденной уязвимости	88
Создание и отправка исключений	88
Отправка исключений при помощи Помощника проверки уязвимостей	89
Отправка исключений в Nexpose со страницы списка уязвимостей	92
Отправка исключений в Nexpose со страницы уязвимости.....	95
Обновление исключений в Nexpose.....	96
Отслеживание статистики в реальном времени и событий во время проверки уязвимостей.....	97
Доступ к окну результатов.....	97
Вкладка статистики	97
Просмотр списка импортированных хостов из окна Findings («Результаты»).....	98

Просмотр списка импортированных уязвимостей из окна Findings («Результаты»).....	99
Просмотр списка совпадений в окне Findings («Результаты»).....	101
Просмотр списка проверенных уязвимостей из окна Findings («Результаты»).....	101
Просмотр списка исключений уязвимостей из окна Findings («Результаты»).....	102
Вкладка Tasks Log («Журнал задач»)	102
Управление исключениями для Nexpose.....	103
Страница Exceptions («Исключения»).....	103
Доступ к странице Exceptions («Исключения»).....	104
Создание и поддержка исключений Nexpose	105
Просмотр исключений уязвимостей в Nexpose.....	108
Использование эксплойтов	109
Автоматизированные эксплойты.....	110
Запуск автоматизированных эксплойтов.....	110
Настройка параметров автоматического использования эксплойтов	111
Эксплойты, работающие в ручном режиме.....	111
Поиск эксплойтов	112
Настройка службы следающего агента Listener	112
Учётные данные	113
Понимание терминологии учётных данных	113
Приватный тип (Private Type)	114
Невоспроизводимый хэш (Nonreplayable Hash).....	114
Хэш NTLM (NTLM Hash)	114
Область (Realm)	114
Неполный открытый тип (Incomplete Public)	114
Неполный приватный тип (Incomplete Private).....	114
Логин (Login)	114
Источник (Origin)	114
Подтверждённые учётные данные (Validated Credential)	115
Получение учётных данных.....	115
Источники учётных данных	116
Управление учётными данными	116
Добавление учётных данных	116
Ввод пароля вручную.....	116
Добавление приватного ключа SSH вручную	119
Добавление хэша NTLM вручную	121
Добавление неповторяющегося хэша вручную	123

Импорт и экспорт учётных данных	125
Импорт учётных данных, экспортируемых из других проектов	126
Импорт созданного вручную файла учётных данных	128
Импорт файла PWDump	130
Экспорт всех учётных данных	132
Экспорт выбранных учётных данных	134
Экспорт файла PWDump	135
Создание файла учётных данных CSV для импорта	136
Клонирование и редактирование учётных данных	137
Удаление учётных данных	137
Повторное использование учётных данных	138
Процесс работы с повторным использованием учётных данных	139
Целевые задачи повторного использования учётных данных	139
Настройка и запуск повторного использования учётных данных	139
Поиск учетных данных	146
Создание поискового запроса	146
Операторы поиска	147
Синтаксис поиска учетных данных	147
Поиск открытых данных (по имени пользователя)	147
Поиск скрытых (непубличных) данных	147
Поиск данных скрытого типа	147
Поиск по типу области идентификации	148
Поиск по имени области	148
Поиск учетных данных по определенному тегу	148
Фильтрация по Метаданным учетных записей	148
Брутфорс-атаки	149
Доступ к Bruteforce Workflow	149
Определение хостов для атаки грубой силой	150
Исключение хостов из атаки грубой силы	151
Выбор служб для брутфорса	152
Создание списка паролей для брутфорса	153
Использование всех учетных данных в проекте для атаки «грубой силы»	154
Ввод учетных данных вручную для атаки «грубой силы»	154
Импорт списка паролей для атаки грубой силы	155
Использование заводских настроек для атаки «грубой силы»	156
Использование пустых паролей при хакерских атаках методом перебора («грубой силы»)	159

Использование имени пользователя в качестве пароля.....	160
Настройка выполняемых действий на случай взломов программой Bruteforce	161
Настройка периода выполнения для атаки с помощью Bruteforce	162
Применение правил мутации для атак с помощью программы Bruteforce	163
Применение leetspeak-замен	163
Присоединение спецсимволов в начало (!#*)	164
Присоединение спецсимволов в конец (!#*)	164
Присоединение одноразрядного числа в начало	164
Присоединение одноразрядного числа в конец.....	164
Присоединение чисел в начало	164
Присоединение чисел в конец.....	164
Присоединение текущего года в начало	165
Присоединение текущего года в конец	165
Запуск брутфорс-атаки.....	165
Трактовка результатов брутфорса	166
Вкладка статистики	166
Просмотр таблицы попыток логина	167
Просмотр таблицы скомпрометированных целей	167
Просмотр таблицы успешных логинов.....	168
Вкладка журнала регистрации задач	168
Заданные пользователем мутации элемента учетных данных	170
John the Ripper	170
Скачивание и установка John the Ripper	170
Установка John the Ripper в Linux.....	171
Установка John the Ripper в Windows	171
Использование John the Ripper в Linux.....	171
Использование John the Ripper в Windows	172
Заданные пользователем правила мутации	172
Требования к заданному пользователем набору правил	172
Получение доступа к файлу конфигурации John the Ripper	173
Основные синтаксические правила John the Ripper	174
Создание заданных пользователем правил мутации.....	175
Присоединение в конец пароля цифр	175
Присоединение в начало пароля цифр.....	176
Присоединение в конец пароля спецсимволов.....	176
Присоединение в начало пароля спецсимволов	176

Смена регистра пароля на нижний и присоединение к нему цифр и спецсимволов	176
Генерация подвергнувшегося мутации списка слов.....	177
Импорт списков слов из John the Ripper в проект	177
Credentials Domino MetaModule	178
Получение доступа к Credentials Domino MetaModule	179
Выбор первоначального хоста для Credentials Domino MetaModule	180
Определение области применения Credentials Domino MetaModule	181
Присвоение статуса "Особо важный хост" в Credentials Domino MetaModule	182
Настройка параметров нагрузки для Credentials Domino MetaModule	185
Установка условий прерывания для Credentials Domino MetaModule.....	186
Включение сгенерированного отчета Credentials Domino MetaModule	187
Запуск Credentials Domino MetaModule	188
Понимание результатов Credentials Domino MetaModule	189
Статистика	190
Просмотр и Визуализация атак.....	191
Просмотр уникальных зарегистрированных учетных данных	191
Просмотр взломанных хостов.....	192
Журнал задач.....	194
Метамодуль проверки единых учетных данных.....	194
Риски блокировки	195
Запуск Метамодуля проверки единых учетных данных	195
Метамодуль проверки SSH-ключей.....	199
Запуск Метамодуля проверки SSH-ключей	200
Метамодуль взлома известных учетных данных.....	204
Запуск Метамодуля взлома известных учетных данных.....	205
Метамодуль тестирования сегментации и брандмауэра.....	208
Egress Scan Target	208
Состояния портов	208
Настройка сервера тестирования выхода (egress)	209
Запуск Метамодуля сегментации и тестирования брандмауэра	210
Экспорт данных	213
Каталог экспортированных данных.....	214
Просмотр экспортированных данных, сгенерированных с помощью Metasploit Pro 4.8 и более ранних версий	214
Журналы экспортированных данных	214
Просмотр журнала экспорта	214

Очистка журнала экспорта	214
Сигналы центра оповещений для экспорта	215
Методы экспорта	215
Экспорт в XML	216
Создание XML файла с данными проекта	216
ZIP-архив рабочего пространства	218
Создание ZIP-архива проекта	218
Скрипты повтора	219
Экспортирование скриптов повтора	219
Запуск скрипта повтора при помощи Pro Console или MSFConsole	220
PWDDumps	220
Экспортирование в файл PWDump	220
Просмотр экспортированных данных	221
Социальная инженерия	221
Методики социальной инженерии	222
Фишинг	222
Эксплойты для использования на компьютере пользователя	223
Файлы с прикрепленным эксплойтом	223
Подписанные Java-апплеты	223
Портативные файлы	224
Терминология в социальной инженерии	224
Кампания/Campaign	224
Отслеживание кликов/Click Tracking	224
Шаблон электронного письма/e-mail template	224
Файл-приложение/executable	224
Файл с прикрепленным эксплойтом/File Format Exploit	224
Цель/Human Target	224
Фишинговая атака	224
Портативный файл	225
Файл ресурса/Resource File	225
Список целей/Target List	225
Отслеживание GIF/Tracking GIF	225
Отслеживание ссылки/Tracking Link	225
Строка отслеживания/Tracking String	225
Посещение/Visit	225
Веб шаблон/Web Template	225

Управление кампаниями.....	225
Ограничения кампаний	226
Панель кампании	226
Блок задач кампании	226
Виджет кампании.....	227
Модальные окна	227
Активные ссылки	227
Состояние кампании	228
Создание кампании	228
Редактирование названия кампании	229
Запуск и работка кампании	229
Очистка данных кампании	229
Просмотр результатов кампании	230
Добавление компонента кампании	230
Удаление компонентов кампании.....	231
Остановка кампании	232
Отправка электронного письма с уведомлением о начале кампании	232
Загрузка инфицированного файла	232
Удаление кампании	233
Экспорт собранных во время кампании данных в файл CSV	233
Экспорт разосланных электронных писем кампании в файл CSV	233
Экспорт списка целей, открывших электронное письмо, в файл CSV	233
Экспорт списка целей, кликнувших на ссылку, в файл CSV	234
Экспорт целей, заполнивших веб форму, в файл CSV.....	234
Наилучшие стратегии для атак при помощи социальной инженерии.....	234
Социальная инженерия вместе с Metasploit Pro.....	236
Фишинг	237
Фишинг. Совет №1. Клонировать, клонировать и клонировать.....	238
Фишинг. Совет №2. Используйте реалистичный домен.....	238
Фишинг. Совет №3. Бейте по малым аудиториям	239
Фишинг. Совет №4. Используйте SMTP серверы для рассылок.....	239
Фишинг. Совет №5. Собирайте ценную информацию.....	239
Фишинг. Совет №6. Обязательно имитируйте стиль и текст ссылки при наведении курсора	240
USB-приманка	240
USB-приманка. Совет №1. Аккуратно планируйте атаку	241
USB-приманка. Совет №2. Называйте файлы интересно	241

Инфицированные вложения	241
Инфицированные вложения. Совет №1. Создавайте убедительные письма	242
Инфицированные вложения. Совет №2. Почаще применяйте файлы с вложенными эксплойтами	242
Инфицированные вложения. Совет №3. Архивируйте вложенные файлы	243
Отчеты	243
Сигналы Центра Оповещений при работе с отчетами	243
Создание стандартного отчета	244
Создание отчета в нескольких форматах	246
Создание отчетов Мета-модулей	247
Создание пользовательского отчета	247
Скачивание отчета	249
Просмотр отчета	250
Отправка отчета по почте	251
Настройка почтового сервера	251
Клонирование настроек отчета	251
Удаление отчетов	252
Изменение стандартных отчетов	253
Исключение секций данных в отчете	253
Исключение и включение хостов	254
Создание списков включенных хостов	254
Создание списков исключенных хостов	254
Удаление личных данных из отчета	255
Удаление графиков из отчетов	255
Включение HTML-кода веб страниц в отчеты по социальной инженерии	256
Изменение названий отчетов	256
Добавление пользовательского лого к отчету	257
Загрузка пользовательского логотипа	258
Добавление пользовательского лого к стандартному отчету	260
Работа с пользовательскими шаблонами	260
Jasper Reports и iReport Designer	260
Скачивание Jasper iReport	261
Требования для создания шаблонов	261
Настройка баз данных Metasploit и iReport Designer	262
Пользовательская директория ресурсов	266
Загрузка шаблонов	266

Скачивание пользовательского шаблона для отчетов	268
Удаление пользовательского шаблона для отчетов	269
Скачивание примера шаблона	270
Отчеты по аудиту	271
Основные результаты	273
Детализированные результаты	274
Опции для отчета по аудиту	274
Отчет по личным данным	274
Дополнительная информация	275
Детали личных данных	275
Детали логинов	275
Детали хостов	276
Детали модулей	276
Источники служб	276
Источники сеанса	276
Дополнительные данные	276
Опции отчетов по личным данным	276
Отчет по соответствию нормам FISMA	277
Общая сводка	278
Детализация результатов	278
Контроль доступа. FISMA AC-7	278
Бдительность и тренинги. FISMA AT-2	278
Менеджмент конфигураций. FISMA CM-7	278
Идентификация и аутентификация. FISMA - IA-2	279
Идентификация и аутентификация. FISMA - IA-5	279
Идентификация и аутентификация. FISMA - IA-7	279
Оценка риска. FISMA RA-5	279
Целостность систем и информации. FISMA SI-2	280
Целостность систем и информации. FISMA SI-10	280
Отчет по соответствию нормам PCI	280
Общая сводка	281
Сводка по соответствию требованиям	281
Сводка по состоянию хостов	282
Детализация результатов	282
Требования PCI. 2.2.1	282
Требования PCI. 2.3	282

Требования PCI. 6.1	282
Требования PCI. 8.2	283
Требования PCI. 8.4	283
Требования PCI. 8.5.8	283
Требования PCI. 8.5.10	283
Требования PCI. 8.5.11	284
Отчет мета-модуля Credentials Domino	284
Общая сводка	285
Сводка по проекту	285
Сводка по запускам	285
Сводка по результатам	285
Графики данных	285
Успешно атакованные хосты повышенной значимости	286
Неуспешно атакованные хосты повышенной значимости	287
Все успешно атакованные хосты	287
Все неуспешно атакованные хосты	287
Дополнительные сведения	287
Опции отчета по работе Мета-модуля Credentials Domino	287
Отчёт вторжения по узанным учётным данным	288
Сводка по проекту	288
Сводка по результатам	288
Графики с данными о сервисах и хостах, к которым был получен доступ	288
Детализированные данные о сервисах и хостах, к которым был получен доступ	288
Дополнительные сведения	289
Опции отчета	289
Отчет по работе мета-модуля Single Password Testing.....	289
Сводка по проекту	289
Сводка по результатам	289
Графики с данными о сервисах и хостах, к которым был получен доступ	290
Детализированные данные о сервисах и хостах, к которым был получен доступ	290
Дополнительные сведения	290
Опции отчета по работе мета-модуля Single Password Testing	290
Отчет по работе мета-модуля SSH Key Testing.....	291
Сводка по проекту	291
Сводка по результатам	291
Графики с данными о сервисах и хостах, к которым был получен доступ	291

Детализированные данные о сервисах и хостах, к которым был получен доступ	291
Дополнительные сведения	292
Опции отчета по работе мета-модуля SSH Key Testing	292
Отчет по прохождению хэшей	292
Сводка по проекту	293
Сводка по результатам	293
Графики с данными о сервисах и хостах, к которым был получен доступ	293
Детализированные данные о сервисах и хостах, к которым был получен доступ	293
Дополнительные сведения	293
Опции отчета по работе мета-модуля Pass the Hash	293

Приступая к работе.

Для начала, если вы еще не установили Metasploit, то обязательно ознакомьтесь с этими инструкциями, если вы коммерческий пользователь. Если же у вас уже установлен Metasploit, поздравляем! Это самое подходящее место для начала работы.

Что такое Metasploit?

Metasploit - это платформа тестирования проникновений, которая позволяет находить, использовать и подтверждать уязвимости. Платформа включает в себя Metasploit Framework и ее коммерческие версии: Metasploit Pro, Express, Community и Nexpose Ultimate.

Metasploit Framework

Metasploit Framework - это основа, на которой разработаны коммерческие продукты. [Это открытый источник](#), который предоставляет инфраструктуру, контент и инструменты для выполнения тестов на уязвимости и обширную проверку безопасности. Благодаря сообществу разработчиков открытого исходного кода и собственной тяжелой работе группы разработчиков контента Rapid7, добавление новых модулей происходит на регулярной основе. Это означает, что вам будет доступна последняя уязвимость сразу по мере её публикации.

В интернете вы можете найти немало ресурсов, которые помогут вам узнать, как пользоваться Metasploit Framework. Но мы настоятельно рекомендуем вам обратить внимание на [Metasploit Framework Wiki](#), которая поддерживается и наполняется сотрудниками Rapid7, и обеспечит вам самую новую информацию. Также, вы можете изучить левую боковую панель, чтобы просмотреть документацию, доступную на этом сайте: просто нажмите на раздел **Metasploit Framework** или воспользуйтесь поиском для ответа на интересующий вас вопрос. Если же вы не можете найти то, что вам нужно, [свяжитесь с нами](#), и мы добавим эту информацию в журнал документации.

Metasploit Pro и прочие коммерческие издания

Коммерческие выпуски Metasploit, которые включают в себя Pro, Express, Community и Nexpose Ultimate, доступны пользователям, которые предпочитают использовать веб-интерфейс для пентеста (имитации реальных атак для тестирования систем безопасности). Помимо вышеупомянутого веб-интерфейса, некоторые коммерческие выпуски включают в себя функции, которые недоступны в Metasploit Framework. Основное количество дополнительных функций нацелены на автоматизацию и оптимизацию общих задач пентеста, таких как определение уязвимостей, социальная инженерия, создание специфичных вредоносных файлов и атак с использованием брутфорсинга.

!!! Все функции, указанные в данном руководстве, доступны в издании Metasploit Pro. Некоторые из них могут быть недоступны в других изданиях.

Если вы предпочитаете использовать командную строку, но все же хотите получить доступ к коммерческим функциям, это не повод для беспокойства. Metasploit Pro включает в себя свою уникальную консоль, которая почти всем схожа с `msfconsole`, за исключением того, что она дает вам доступ к большей части функций Metasploit Pro через текстовый набор команд.

Совместимость Metasploit

Rapid7 занимается распространением коммерческих изданий Metasploit как приложений (исполняемых файлов) для Linux и Windows.

Вы можете загрузить и запустить исполняемый файл для установки Metasploit Pro на вашем личном локальном компьютере или же через удаленный доступ, например, на веб-сервере. Независимо от того, куда вы установите Metasploit Pro, вы в любом случае сможете получить доступ к интерфейсу пользователя с помощью браузера. Metasploit Pro использует безопасное соединение, чтобы подключиться к серверу, на котором он запущен.

Если вы установите Metasploit Pro на сервере, пользователи смогут использовать веб-браузер для получения доступа к пользовательскому интерфейсу из любого места. Им потребуется адрес и порт сервера, который использует Metasploit Pro. По умолчанию, служба Metasploit использует порт 3790. Вы можете изменить порт, который Metasploit использует во время процесса установки. Например, если Metasploit Pro запущен на сервере с адресом 192.168.184.142 и портом 3790, пользователи могут использовать <https://192.168.184.142:3790> для запуска интерфейса.

Если Metasploit Pro работает на вашем локальном компьютере, вы можете использовать `localhost` (так называемый, «локальный хост», по смыслу — этот компьютер) и порт 3790 для доступа к Metasploit Pro. К примеру, введите <https://localhost:3790> в поле URL-адреса браузера, чтобы загрузить пользовательский интерфейс.

!!! Вам будет необходим лицензионный ключ для активации продукта. Если у вас его нет, пожалуйста свяжитесь с отделом продаж Rapid7 по адресу sales@rapid7.com.

Компоненты Metasploit Pro

Metasploit Pro состоит из нескольких компонентов, работающих в совокупности, чтобы предоставить вам полноценный инструмент для тестирования уязвимостей. В состав Metasploit Pro входят следующие компоненты:

1) Metasploit Framework

Собственно, платформа для тестирования и разработки приложений с открытым исходным кодом, которая предоставляет вам доступ к каждому модулю, который нужен Metasploit Pro для выполнения поставленной задачи. Metasploit Framework содержит базу уязвимостей, которая предоставляет вам последний набор кодов уязвимостей для различных приложений, операционных систем и платформ. Вы можете использовать возможности Metasploit Framework для создания дополнительных инструментов, обеспечивающих вашу безопасность либо написать собственный эксплойт (компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему) для новых уязвимостей. Команда Metasploit постоянно выпускает еженедельные обновления, содержащие новые модули и раз в две

недели - обновления, которые содержат исправления и улучшения для известных вопросов по Metasploit Pro.

2) Модули

Модуль представляет собой отдельную часть кода либо отдельную программу, которые расширяют функциональность Metasploit Framework. Модули автоматизируют функции, предоставляемые Metasploit Framework, и позволяют вам выполнять задачи с помощью Metasploit Pro.

Модуль может быть эксплойтным, вспомогательным, с дополнительной нагрузкой, без нагрузки (NOP) или пост-эксплуатационным. Тип модуля определяет его назначение. Например, любой модуль, который открывает какую-либо программную оболочку на цели атаки, является эксплойтным.

3) Службы

Metasploit Pro использует PostgreSQL, Ruby on Rails и Pro Service. PostgreSQL запускает базу данных, которой Metasploit Pro пользуется для хранения проектных данных. Ruby on Rails запускает сам веб-интерфейс Metasploit Pro. Службы Pro Service или Metasploit Service оформляют Rails, Metasploit Framework и Metasploit RPC-сервер.

4) Веб-интерфейс.

Это компонент, с помощью которого вы взаимодействуете с Metasploit Pro. Для его запуска, откройте браузер и пройдите по адресу <https://localhost:3790>.

Основные понятия и термины

Чтобы помочь вам ознакомиться с Metasploit Pro, мы предоставим следующие основные понятия и термины, которые вы должны освоить.

1) Проект

Вся работа в Metasploit Pro происходит внутри проекта. Проект представляет собой емкость для данных, которые вы используете и получаете во время проведения теста на проникновение.

2) Рабочее пространство

Рабочее пространство - это то же самое, что и проект, за исключением того, что оно используется только при обращении к Metasploit Framework.

3) Задача

Всё, что вы делаете в Metasploit, является задачами. Это любое действие, производимое в Metasploit, к примеру запуск эксплойта либо сканирования.

4) Модуль

Большинство задач, которые вы выполняете в Metasploit, требуют использования модулей, которые являются автономным элементом кода, расширяющими функциональные возможности Metasploit Framework. Модуль может быть эксплуатационным (эксплойтным), вспомогательным либо пост-эксплуатационным. Тип модуля определяет его назначение. Например, любой модуль, который

открывает какую-либо программную оболочку на назначенной цели, является эксплойтным. Широко известным модулем данного типа является модуль MS08-067.

5) Эксплуатационный модуль

Данный модуль выполняет последовательность команд для вычисления определенной уязвимости, обнаруженной в системе или приложении. Эксплуатационный модуль использует уязвимость для обеспечения доступа к целевой системе. Такие модули включают переполнение буфера, внедрение кода и эксплойты веб-приложений.

6) Вспомогательный модуль

Вспомогательный модуль не выполняет файловую нагрузку и выполняет произвольные действия, которые не могут быть отнесены к использованию эксплойтов. Примерами вспомогательных модулей являются сканеры, фаззеры (Фаззинг - техника тестирования программного обеспечения, часто автоматическая или полуавтоматическая, заключающая в передаче приложению на вход неправильных, неожиданных или случайных данных), и атаки, приводящие к отказу в обслуживании.

7) Пост-эксплуатационные модули

Такой модуль позволяет собирать дополнительную информацию или получать дальнейший доступ к целевой системе, подверженной влиянию эксплуатационного модуля. Примеры пост-эксплуатационных модулей включают в себя хеш-дампы и счётчики служб и приложений.

8) Нагрузка

Payload/нагрузка (данные или сообщения, передаваемые по сети - например, данные, включённые в ячейку АТМ или пакет) - это код оболочки, который запускается после успешного взлома эксплойтом системы. Она позволяет вам указать, как именно вы хотите подключиться к оболочке, и что именно вы хотите сделать с целевой системой после того, как вы возьмете над ней контроль. Нагрузка может открыть Meterpreter или оболочку командной строки. Meterpreter – это расширенный вариант нагрузки, который позволяет вам писать DLL-файлы для динамического создания новых функций по мере появления необходимости.

9) Нагрузка, привязанная к оболочке

Такой тип нагрузки прикрепляет следащего агента к взломанной системе и ожидает подключения атакующей системы к агенту.

10) База данных

В базе данных хранятся данные хостов, системные логи (журналы), собранные данные и отчёты.

11) Поисковое сканирование

Поисковое сканирование (discovery scan) - это тип сканирования Metasploit, которое объединяет Nmap и несколько модулей Metasploit для перечисления и идентификации целей.

12) Эксплойт

Эксплойт - это программа, которая использует определенную уязвимость и предоставляет атакующему доступ к целевой системе. Эксплойт обычно несет в себе нагрузку и доставляет ее к цели. Например, одним из наиболее распространенных эксплойтов является windows/smb/MS08-067_netscan, целью которого является уязвимость служб Windows Server, позволяющая выполнять код через удалённый доступ.

13) Следящий агент

Агент ожидает входящего соединения либо от эксплуатируемой цели, либо от атакующей машины и управляет соединением при его получении.

14) Meterpreter

Meterpreter - это расширенная многофункциональная нагрузка, которая предоставляет вам интерактивную оболочку. Из этой оболочки, вы можете загружать файлы, получать хэши паролей для учетных записей пользователей, и внедряться в другие сети. Процесс meterpreter работает в памяти, поэтому он не может быть обнаружен большинством защитных систем.

15) Модули

Это заранее собранная группа кода Metasploit Framework, которая выполняет отдельную задачу, например, запуск сканирования или выполнение эксплойта.

16) Нагрузка

Это код, который запускается после того, как эксплойт будет успешно выполнен в целевой системе. Она может представлять собой реверсивную нагрузку оболочки или же нагрузку, привязанную непосредственно к оболочке. Основное различие между этими типами нагрузки - это направление соединения после проведения эксплойта

17) Проект

Проект – это контейнер для целей, задач, отчетов и данных, которые являются частью теста на проникновение. Проект содержит рабочее пространство, которое вы используете для создания самого теста и настройки задач. Каждый тест запускается в проекте.

18) Реверсивная нагрузка

Реверсивная нагрузка связывает цель с атакующей машиной через командную строку.

19) Код оболочки

Это набор инструкций, который эксплойт использует как нагрузку.

20) Оболочка

Оболочка – это консольный интерфейс, который даёт вам доступ к удалённой цели.

21) Задача

Задача – это действие, которое может выполнить Metasploit Pro. Примерами задач являются выполнение сканирования, запуск брутфорса, эксплуатация уязвимой цели или создание отчета.

22) Уязвимость

Уязвимость - это трещина в безопасности, которая позволяет атакующему взломать цель. Взломанная система может привести к эскалации привилегий, отказу в обслуживании, несанкционированному доступу к данным, краже паролей и переполнению буфера.

Рабочий процесс Metasploit Pro

Общий процесс тестирования на проникновение можно разбить на несколько этапов или фаз. В

зависимости от метода, которому вы следуете, может производиться от четырёх до семи фаз теста. Названия этих фаз могут различаться, но обычно они включают в себя разведку, сканирование, внедрение эксплойта, пост-эксплуатацию, сохранение доступа к системе, отчетности и очистки.

Рабочий процесс Metasploit Pro может быть настроен на основе различных этапов тестирования. Основными шагами, которые рабочий процесс Metasploit Pro включает в себя, являются:

- 1. Создание проекта** - создайте проект для хранения данных, собранных из целевых систем.
- 2. Сбор информации** - используйте поисковое сканирование, сканирование Nexpose или импорт инструментария, чтобы обеспечить Metasploit Pro списком целей, запущенных служб и открытых портов, которые связаны с этими целями.
- 3. Использование эксплойта** – используйте автоматические либо ручные эксплойты для запуска атаки на целевые машины. Также, вы можете запустить брутфорс, чтобы повысить привилегии учетной записи и получить доступ к системе, на которой запущен эксплойт.
- 4. Выполнение пост-эксплуатации** - используйте модули пост-эксплуатации или интерактивные сеансы для получения большего количества информации со взломанных целей. Metasploit Pro предоставляет вам несколько инструментов, которые вы можете использовать для взаимодействия с открытыми сеансами на целевой машине. Например, вы можете просмотреть общедоступный файл системы на взломанной машине для получения информации о внутренних приложениях. Эту информацию можно использовать для выгрузки еще большей информации о целевых системах.
- 5. Очистка открытых сеансов** - используйте параметр «Очистить», чтобы закрыть любые открытые сеансы на взломанной цели и удалить любые следы данных, которые использовались во время теста. Этот шаг восстанавливает изначальные настройки в целевой системе.
- 6. Генерация отчетов** - используйте механизм создания отчетов для получения журнала, в котором описываются результаты теста на вторжение. Metasploit Pro предоставляет несколько типов отчетов, которые позволяют вам указать тип информации, которую содержит отчет.

Получение доступа к Metasploit Pro

Чтобы получить доступ к веб-интерфейсу Metasploit Pro, откройте браузер и перейдите по ссылке <https://localhost:3790>, в случае, если Metasploit Pro работает на вашей локальной машине. Если Metasploit Pro запущен на удаленной машине, вам необходимо заменить «localhost» на IP-адрес удаленного компьютера.

Чтобы войти в веб-интерфейс, вам понадобятся логин и пароль от учетной записи, созданной вами при активации лицензионного ключа Metasploit Pro. Если же вы не можете вспомнить пароль, его необходимо сбросить.

Поддерживаемые браузеры

Если в интерфейсе пользователя не все элементы отображаются корректно, удостоверьтесь, что вы используете один из поддерживаемых браузеров. Они перечислены ниже.

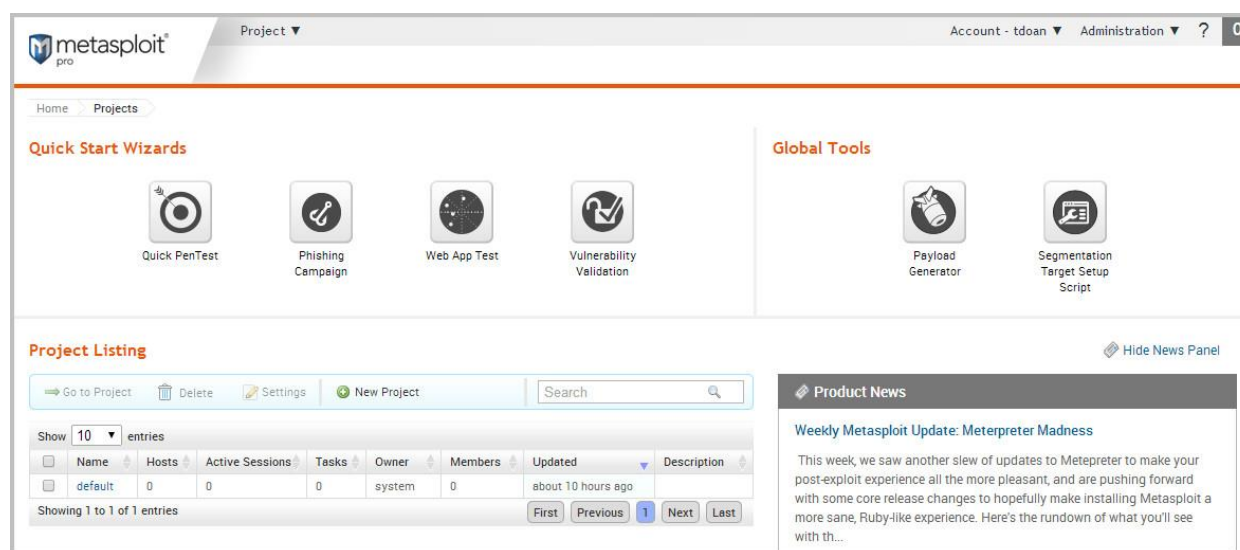
- Google Chrome 10
- Mozilla Firefox 18+
- Internet Explorer 10+

- Iceweasel 18+

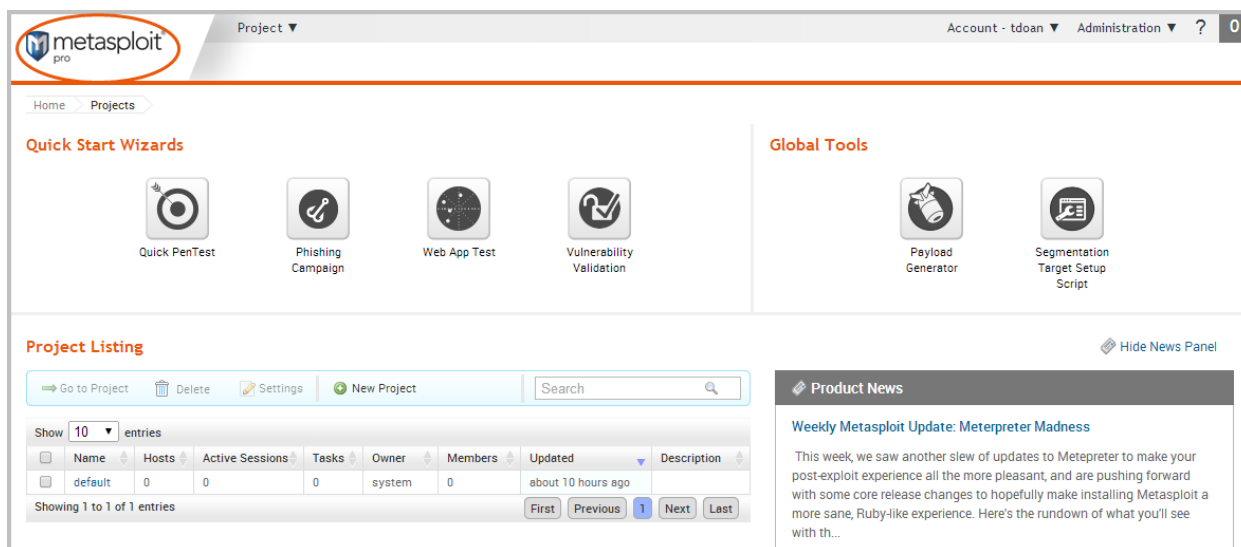
Изучение страницы проектов

Теперь, когда вы знакомы с основами Metasploit, давайте более детально рассмотрим Metasploit Pro.

После входа в Metasploit Pro первое, что вы увидите, будет страница «Проекты». Она перечисляет все проекты, которые в настоящее время хранятся в вашей программе Metasploit Pro, и предоставляет вам доступ к мастеру быстрого запуска, основным инструментам и новостям о продукте.

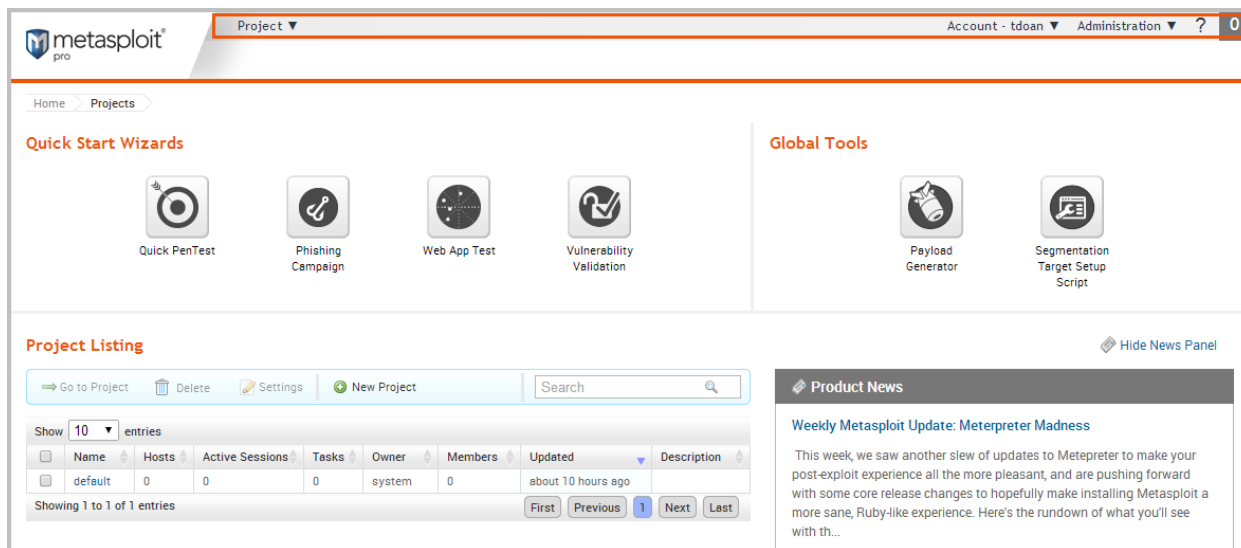


Независимо от того, где вы находитесь в приложении, вы можете перейти в меню Project > Show All Projects с основной панели инструментов, либо щелкнув логотип Metasploit Pro для доступа к странице «Проекты», как показано ниже:



Основная панель инструментов\Global Toolbar

Эта панель инструментов расположена в верхней части веб-интерфейса. Она доступна с любой страницы Metasploit Pro. Вы можете использовать основную панель инструментов для доступа к меню проектов, настройкам своей учетной записи и меню администрирования.



Мастера быстрого запуска\Quick Start Wizards

Каждый мастер быстрого запуска предоставляет вам управляемый интерфейс, который проведёт вас по шагам задачи тестирования, таким как сканирование и внедрение эксплойта в целевую систему, построение компаний соц. инженерии, сканирование и заражение веб-приложений и выявление уязвимостей.

Вы можете щелкнуть по любому из значков мастеров быстрого запуска, чтобы запустить его интерфейс.

metasploit^{pro}

Project ▼ Account - tdoan Administration ▼ ? 0

Home Projects

Quick Start Wizards

Quick PenTest Phishing Campaign Web App Test Vulnerability Validation

Global Tools

Payload Generator Segmentation Target Setup Script

Project Listing

Go to Project Delete Settings New Project Search

Show 10 entries

Name	Hosts	Active Sessions	Tasks	Owner	Members	Updated	Description
default	0	0	0	system	0	about 10 hours ago	

Showing 1 to 1 of 1 entries First Previous 1 Next Last

Product News

Weekly Metasploit Update: Meterpreter Madness

This week, we saw another slew of updates to Meterpreter to make your post-exploit experience all the more pleasant, and are pushing forward with some core release changes to hopefully make installing Metasploit a more sane, Ruby-like experience. Here's the rundown of what you'll see with th...

Новости продукта\Product News

Раздел «Новости продукта» покажет вам наиболее свежие статьи Rapid7. Если вы хотите быть в курсе новейших модулей и новостей безопасности от Rapid7 и сообщества, панель Product News – то, что вам нужно для проверки свежего контента.

metasploit^{pro}

Project ▼ Account - tdoan Administration ▼ ? 0

Home Projects

Quick Start Wizards

Quick PenTest Phishing Campaign Web App Test Vulnerability Validation

Global Tools

Payload Generator Segmentation Target Setup Script

Project Listing

Go to Project Delete Settings New Project Search

Show 10 entries

Name	Hosts	Active Sessions	Tasks	Owner	Members	Updated	Description
default	0	0	0	system	0	about 10 hours ago	

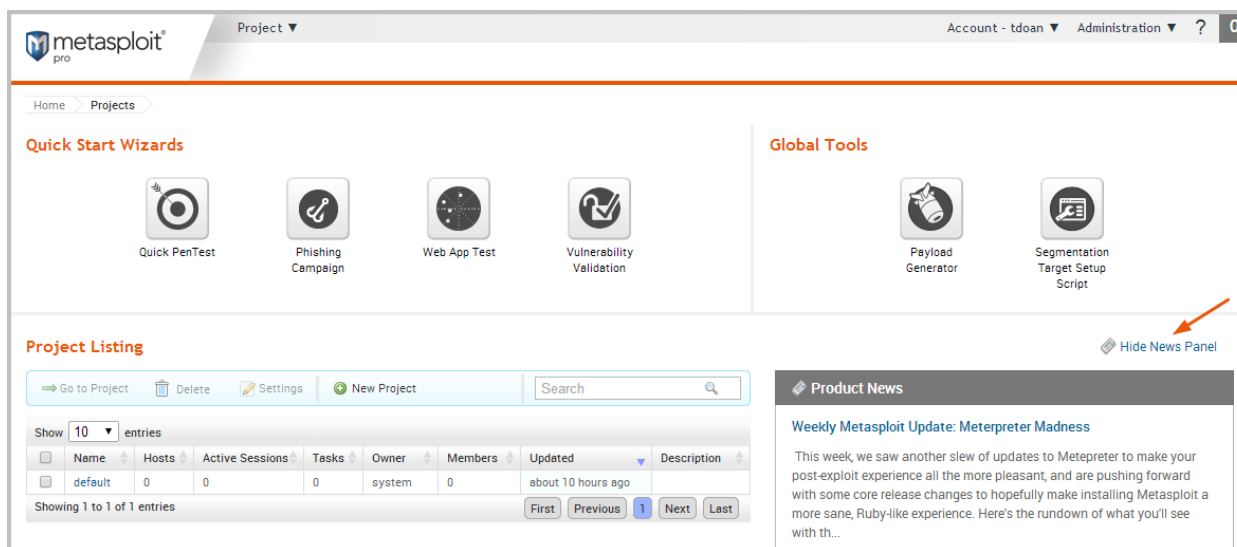
Showing 1 to 1 of 1 entries First Previous 1 Next Last

Product News

Weekly Metasploit Update: Meterpreter Madness

This week, we saw another slew of updates to Meterpreter to make your post-exploit experience all the more pleasant, and are pushing forward with some core release changes to hopefully make installing Metasploit a more sane, Ruby-like experience. Here's the rundown of what you'll see with th...

Если же по какой-либо причине вы не хотите видеть данную панель, вы можете скрыть её со страницы проектов.



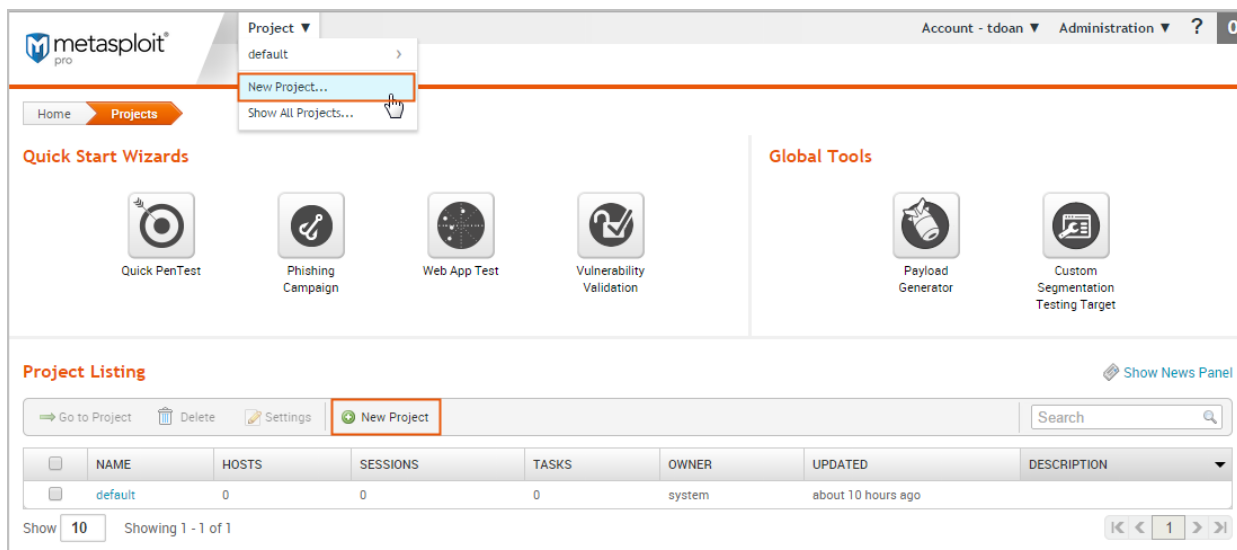
Создание проекта

Теперь, когда вы знакомы со страницей «Проекты», давайте приступим к созданию проекта.

Проект содержит в себе рабочее пространство, хранит данные и позволяет вам разделить действия на логические группы. Часто будет происходить так, что у вас будут разные требования к различным подсетям в организации. Следовательно, достаточно эффективным решением будет иметь несколько проектов для осуществления этих требований.

Например, вы можете создать отдельный проект для отдела кадров и еще один проект для ИТ-отдела. Ваши требования к этим отделам могут значительно различаться, будет логично разделить эти цели на несколько проектов. В конце работы вы можете создать отдельные отчеты для каждого отдела, чтобы провести сравнительный анализ и предоставить ваши данные организации.

В создание проекта нет ничего сложного. Вы можете нажать кнопку «Новый проект (**New Project**)» на странице «Проекты» или перейти по пути **Project > New Project** с основной панели инструментов.



Когда появится страница «Новые проекты/New Projects», вам будет нужно указать имя проекта. Если вы хотите кастомизировать проект, вы также можете добавить здесь описание, указать сетевой диапазон проекта и назначить уровни доступа для пользователей.

Получение целевых данных

Следующее, что вы сможете сделать, это добавить данные в свой проект. Есть несколько способов сделать это:

- Запустить поисковое сканирование
- Импортируйте данные, которые у вас уже есть

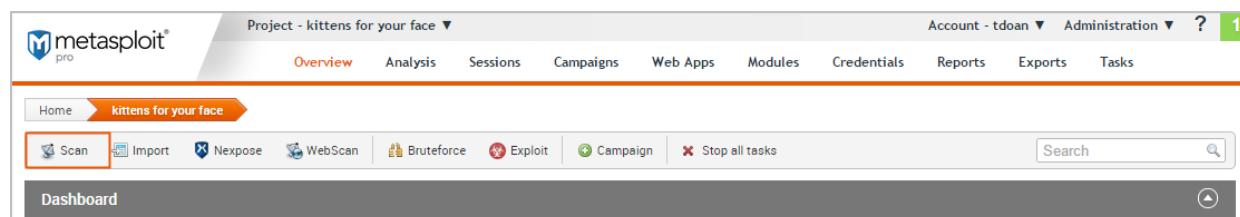
Сканирование целей

Сканирование - это процесс идентификации хостов и перечисление открытых портов для того, чтобы увидеть службы, которые работают в сети. Сканирование позволяет вам идентифицировать активные системы со службами, с которыми вы можете взаимодействовать, чтобы вы могли создать эффективный план атаки. Metasploit имеет собственный встроенный сканер, который использует Nmap для сканирования базового TCP-порта и сбора дополнительной информации о целевых узлах.

По умолчанию, процедура поискового сканирования включает в себя сканирование UDP, которая чаще всего отправляет UDP-зонды в известные UDP-порты, такие как NETBIOS, DHCP, DNS и SNMP. Сканирование проверяет приблизительно 250 портов, которые обычно открыты внешним службам и чаще всего проверяются во время теста на вторжение.

Во время поискового сканирования Metasploit Pro автоматически сохраняет данные хоста в проекте. Вы можете просмотреть эти данные для лучшего понимания структуры сети и определения наилучшего способа атаковать каждую цель. Часто, структура сети дает представление о типах приложений и устройств, которые установлены в целевой системе. Чем больше информации вы можете получить о цели, тем проще вам будет настроить тест точно для неё.

Запуск поискового сканирования также прост. Зайдя в проект, нажмите кнопку «Сканировать (Scan)».



Когда появится новое поле поискового сканирования, введите хосты, которые вы хотите отсканировать в поле целевых адресов (**Targeted Addresses**). Вы можете ввести один IP-адрес, диапазон IP (введённый с дефисами), или стандартную запись CIDR. При вводе каждый элемент пишется с новой строки.

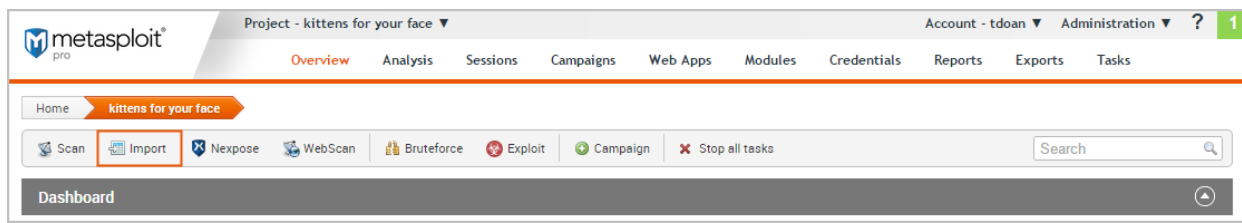
Вы можете запустить сканирование для целевого диапазона; но, если вы хотите точно настроить сканирование, вы можете изменить расширенные параметры. Например, вы можете указать хосты, которые будут исключены из сканирования, и установить скорость сканирования из меню дополнительных опций. Дополнительную информацию о сканировании см. в разделе «[Поисковое сканирование](#)».

Импорт данных

Если вы используете сканер уязвимостей, вы можете импортировать отчет об уязвимостях в проект Metasploit для подтверждения. Импортированные данные также включают метаданные хоста, которые вы можете анализировать на предмет определения дополнительных путей атаки. Metasploit поддерживает несколько сторонних сканеров уязвимостей, в том числе Nessus, Qualys и Core Impact. Полный список поддерживаемых типов импорта см. в разделе «[Импорт данных](#)»

Вы также можете экспортировать и импортировать данные между проектами Metasploit. Это позволяет вам делиться результатами между своими проектами и с другими членами команды.

Чтобы импортировать данные в проект, нажмите кнопку «Import», расположенную на панели «Быстрые задачи (Quick Tasks bar)». Когда появится страница импорта данных, выберите параметр «Import from Nexpose» или «Import from File». В зависимости от опции, которую вы выберете, форма отобразит параметры, которые необходимо настроить для импорта файла.

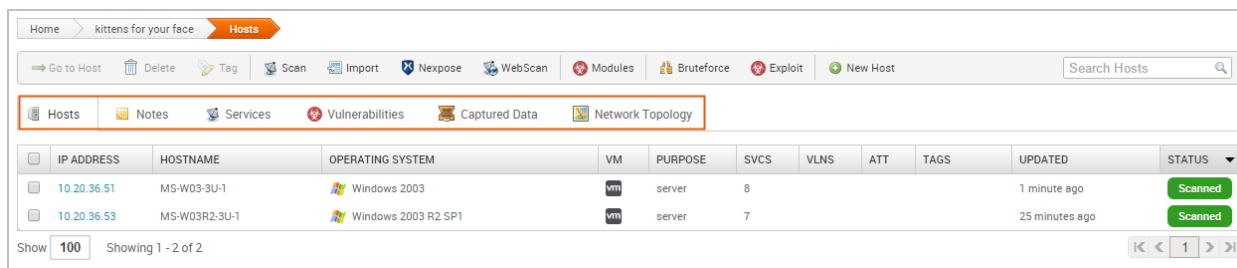


Например, если вы решите импортировать данные из Nexpose, вам нужно будет выбрать консоль, которую вы хотите использовать для того, чтобы запустить сканирование или импортировать сайт. Если же вы решите импортировать файл, вам нужно будет выбрать его расположение.

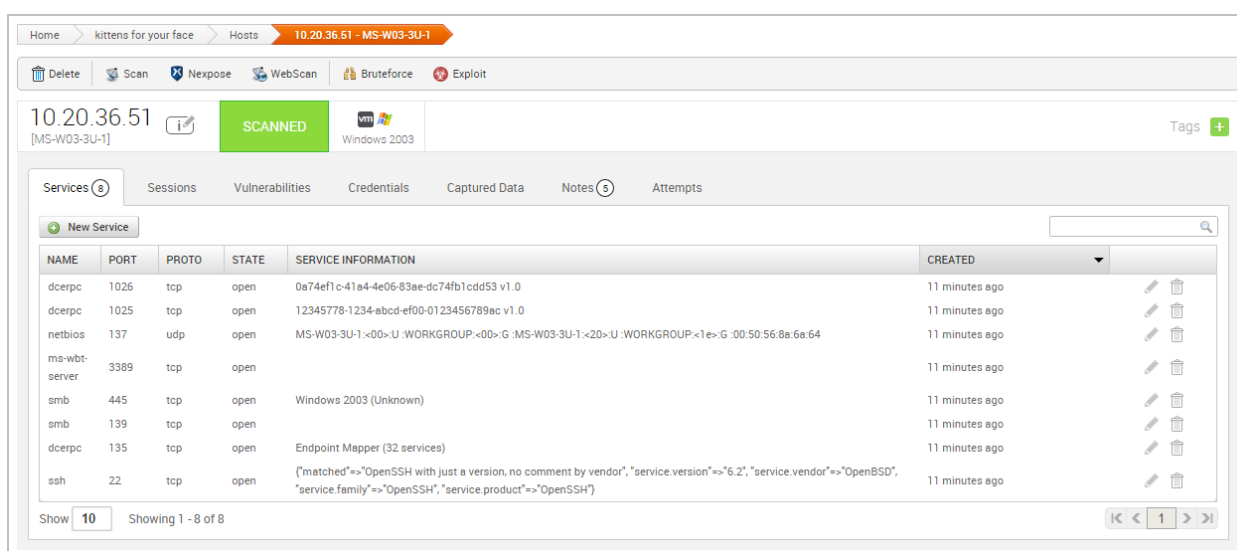
Просмотр и управление данными хоста

Вы можете просматривать эти данные на уровне проекта или на уровне хоста. На уровне проекта Metasploit предоставляет вам полноценный просмотр всех хостов, которые были добавлены в проект. Чтобы получить доступ к виду с уровня проекта, выберите **Analysis > Hosts**. Вначале отобразится список хостов, в котором отображаются идентификаторы и перечисляются порты и службы для каждого хоста. Вы также можете просмотреть все заметки, службы, уязвимости, и

данные, полученные для проекта. Чтобы получить доступ к этой информации, щелкните нужные вкладки в окне просмотра уровня проекта.



Чтобы просмотреть подробные данные для конкретного хоста, вы можете кликнуть на IP-адрес хоста, чтобы получить доступ к просмотру вида одного хоста. Это хороший способ изучить уязвимости и учетные данные определенного хоста.

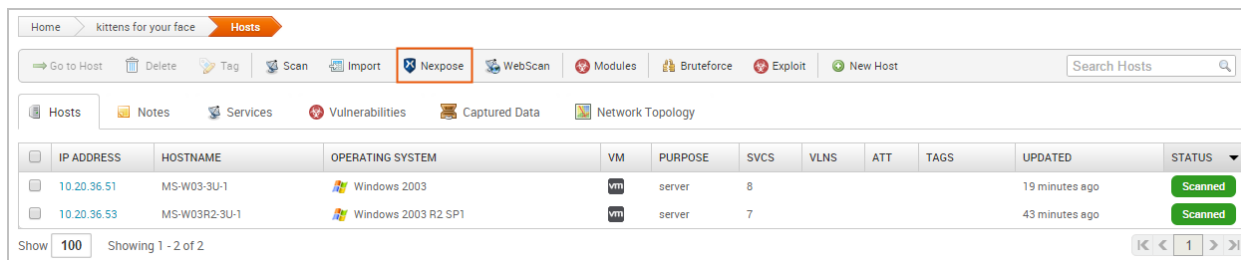


Запуск сканирования уязвимостей

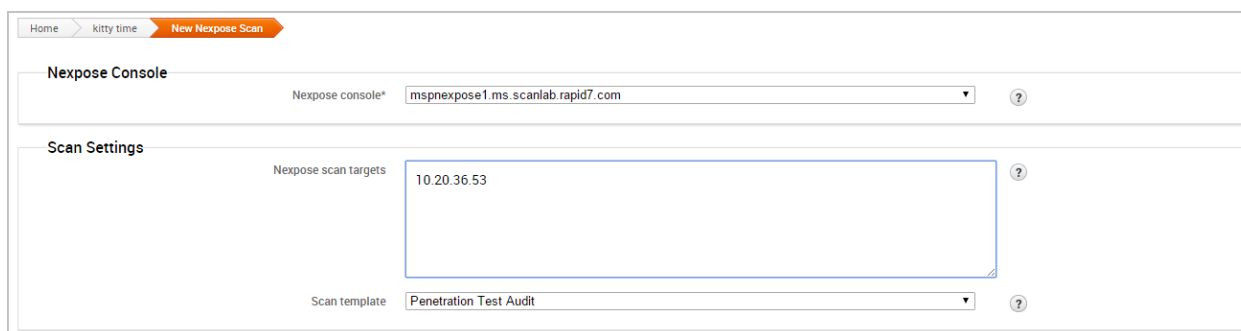
После того, как вы добавите данные цели в проект, вы можете запустить сканирование на уязвимости, чтобы выявить недостатки безопасности, которые могут быть использованы для взлома. Сканеры уязвимостей используют базы данных уязвимостей и проверяют целевые машины на известные уязвимости и ошибки конфигурации. Эта информация может помочь вам предугадать потенциальные типы и направления атак, а также план атаки, которые позволят вам подвергнуть риску нужные цели во время внедрения эксплойта.

Интеграция с Nexpose позволяет запускать сканирование уязвимостей непосредственно из веб-интерфейса Metasploit. Сканирование Nexpose определяет активные службы, открытые порты и приложения, которые запускаются на каждом узле и делает попытки выявить уязвимости, которые могут действовать на основе атрибутов известных служб и приложений. Nexpose сохраняет и показывает результаты в отчете о сканировании, который вы можете импортировать в Metasploit для проверки.

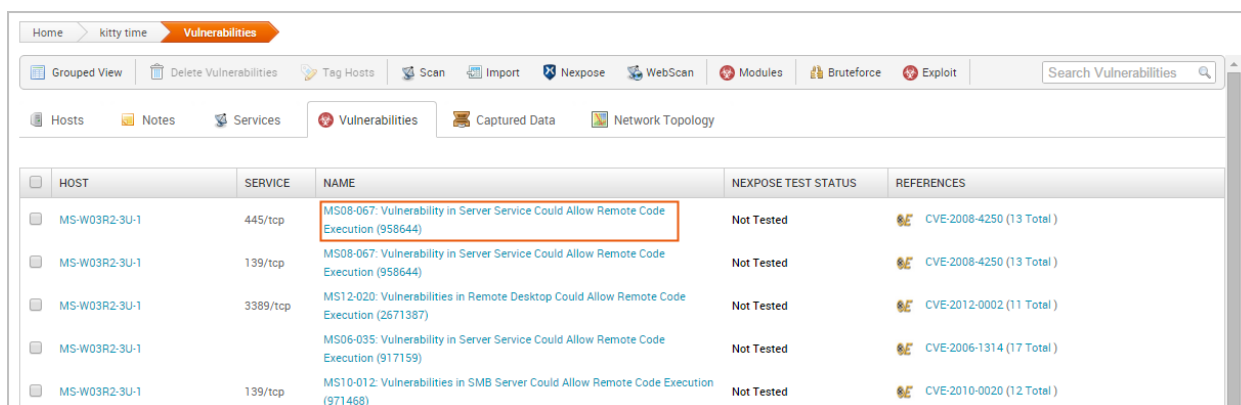
Чтобы запустить данное сканирование, нажмите кнопку «**Nexpose**», расположенную на панели «Быстрые задачи (Quick Tasks Bar)».



Когда появится вкладка конфигурации Nexpose, вам будет необходимо настроить и выбрать консоль, которую вы будете использовать для выполнения сканирования. Так же, как и в поисковом сканировании, вам нужно будет указать хосты для сканирования. Вам также нужно будет выбрать один из доступных шаблонов сканирования, который определяет уровень глубины проверки, используемый Nexpose. Дополнительные сведения о шаблонах сканирования см. в [руководстве пользователя Nexpose](#).



Чтобы просмотреть все потенциальные уязвимости, найденные с помощью Nexpose, перейдите в меню **Analysis > Vulnerabilities**. Вы можете увидеть модули, которые могут быть использованы для вторжения через уязвимость, просто щёлкнув по её названию.



Эта информация станет нам полезной на следующем этапе пентеста – внедрении эксплойта.

!!! Сканы уязвимостей - это полезные инструменты, которые помогут вам быстро найти потенциальные щели в системе безопасности цели. Однако существуют случаи, когда вам нужно избежать обнаружения и минимизировать заметные действия. В этих случаях будет разумно запустить вспомогательные модули, такие как FTP, SMB и VNC, чтобы вручную выявлять потенциальные уязвимости, которые могут быть использованы для доступа в систему. Ручной анализ уязвимости значительно более трудоемкий и требует от вас кропотливого изучения, критического мышления и глубоких знаний, но данный способ может помочь вам создать точный и эффективный план атаки.

Поиск и использование уязвимостей простым способом

Самый простой способ сканирования и проверки на уязвимости - это мастер проверки уязвимостей (Vulnerability Validation Wizard), который автоматизирует процесс проверки для пользователей версий Nexpose и Metasploit Pro. Данный мастер предоставляет вам интерфейс, который проведет вас через каждый шаг процесса проверки - от импорта данных Nexpose до автоматического использования уязвимостей для последующей отправки результатов проверки обратно в Nexpose. Для получения дополнительной информации о проверке уязвимости, см. раздел «[Проверка уязвимости](#)».

Если у вас нет доступа к Nexpose и/или Metasploit Pro, процесс проверки требует ручного анализа уязвимостей. Ручная проверка требует немного больше работы, но обеспечивает гораздо больший контроль над целевыми уязвимостями.

Эксплуатация известных уязвимостей

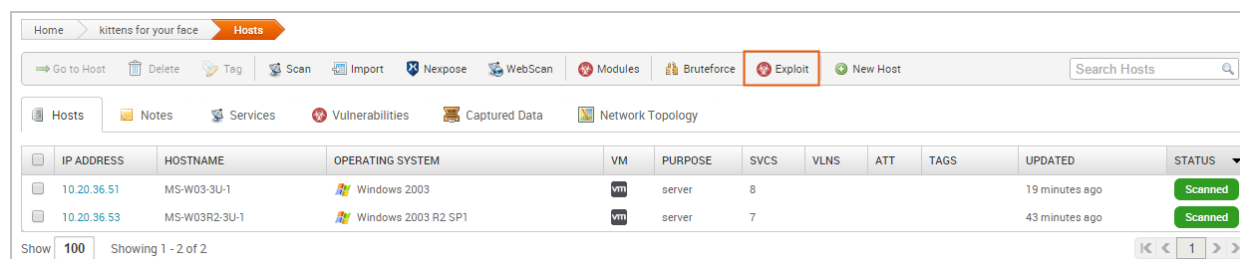
После того, как вы собрали необходимую информацию о своих целях и определили потенциальные уязвимости, вы можете перейти на этап внедрения эксплойтов. Эксплуатация - это просто процесс запуска эксплойтов против обнаруженных уязвимостей. Успешные попытки эксплойта обеспечивают вам доступ к целевым системам, и далее вы можете выкрасть хэши паролей и скачивать файлы конфигурации. Они также позволяют идентифицировать и подтвердить риск существования уязвимости.

Metasploit предлагает несколько различных методов, которые вы можете использовать для использования эксплойтов.

Автоматическое использование эксплойтов

Metasploit в этом случае автоматически перекрестно ссылается на открытые службы, ссылки на уязвимости и данные идентификации, чтобы найти подходящие эксплойты. Все эти эксплойты добавляются в формируемый план атаки, который содержит все эксплойты, доступные к запуску. Простейшая цель автоматического использования эксплойтов - как можно быстрее открыть сеанс, используя данные, которые Metasploit уже имеет для целевых хостов.

Чтобы запустить его, нажмите кнопку «**Exploit**», расположенную на панели «Быстрые задачи (Quick Tasks Bar)».



Как минимум, вы должны будете предоставить узлы, которые вы хотите взломать, и установить минимальный уровень надежности для каждого эксплойта. Минимальный уровень надежности устанавливается, чтобы гарантировать безопасность запускаемых эксплойтов. Чем выше уровень надежности, тем меньше вероятность того, что используемые эксплойты приведут к прекращению работы служб или негативно повлияют на цель.

Также, вы можете использовать расширенные настройки, чтобы указать варианты нагрузки и настройки выбора эксплойта.

Ручное использование эксплойтов

Ручное использование обеспечивает более целенаправленный и методичный подход к использованию уязвимостей. Это позволяет запускать отдельные эксплойты по одному за раз. Этот метод особенно полезен, если имеется конкретная уязвимость, которую вы хотите использовать. Например, если вы знаете, что целевой SMB-сервер на системе Windows XP не имеет патча MS08-067, вы можете попробовать запустить соответствующий модуль конкретно против него.

Для поиска модулей выберите **Modules > Search** и введите имя модуля, который вы хотите запустить. Наилучший способ найти точно соответствующий модуль – поиск по ссылке на уязвимость. Например, если вы хотите найти ms08-067, вы можете либо искать «ms08-067», либо выполнить поиск по пути к модулю: `exploit/Windows/SMB/ms08_067_netapi`.

Один из самых простых способов найти эксплойт под уязвимость - это непосредственно на странице просмотра уязвимости. Чтобы просмотреть все уязвимости в проекте, выберите **Analysis > Vulnerabilities**. Вы можете щелкнуть по названию уязвимости, чтобы просмотреть связанные модули, которые могут использоваться для её использования.

HOST	SERVICE	NAME	NEXPOSE TEST STATUS	REFERENCES
MS-W03R2-3U-1	445/tcp	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Not Tested	CVE-2008-4250 (13 Total)
MS-W03R2-3U-1	139/tcp	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Not Tested	CVE-2008-4250 (13 Total)
MS-W03R2-3U-1	3389/tcp	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)	Not Tested	CVE-2012-0002 (11 Total)
MS-W03R2-3U-1		MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159)	Not Tested	CVE-2006-1314 (17 Total)
MS-W03R2-3U-1	139/tcp	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)	Not Tested	CVE-2010-0020 (12 Total)

Режим просмотра одной уязвимости показывает список эксплойтов, которые могут быть запущены для атаки хоста. Вы можете нажать кнопку «**Exploit**», чтобы открыть страницу конфигурации модуля.

MODULE TYPE	PLATFORM	MODULE	RANKING	REFERENCES	ACTION
Exploit	Windows	MS08-067 Microsoft Server Service Relative Path Stack Corruption	★★★★☆	CVE-2008-4250 (4 Total)	Exploit

Конфигурирование общих настроек модуля эксплойта

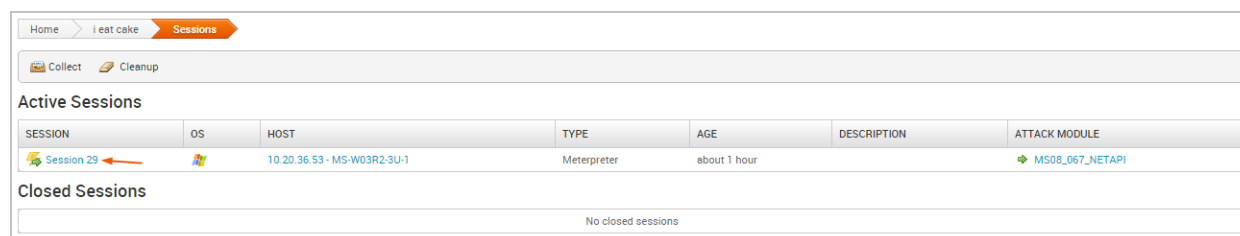
Каждый модуль имеет собственный набор параметров, которые могут быть настроены под ваши нужды. Вот несколько опций, которые обычно используются для настройки модулей:

- **Тип нагрузки:** указывает тип нагрузки, которую эксплойт будет доставлять цели. Можно выбрать один из следующих типов:
 - Команда: нагрузка в виде выполнения команды, которая позволяет вам выполнять команды на удалённой системе.
 - Meterpreter: расширенный тип нагрузки, который предоставляет вам командную строку, позволяющую вам добавлять команды и устанавливать расширения прямо в ходе работы с ней.
- **Тип соединения:** определяет, как вы хотите, чтоб Metasploit подключался к цели. Есть выбор между следующими вариантами подключения:
 - Автоматическое: автоматически использует связанное с оболочкой соединение в случае обнаружения NAT; в противном случае, использует реверсивное соединение.
 - Связанное: будет полезно, если цель защищена NAT либо файрволом.
 - Реверсивное: это соединение стоит использовать, если ваша система не способна инициировать подключение к целевым системам.
- **LHOST:** указывает адрес локального узла.
- **LPORT:** указывает порты, которые вы желаете использовать для реверсивного соединения.
- **RHOST:** указывает IP-адрес цели.
- **RPORT:** указывает удалённый порт, который вы хотите атаковать.
- **Настройки цели:** уточняет операционную систему цели и её версию.
- **Тайм-аут эксплойта:** указывает, длину тайм-аута для модуля (в минутах).

Пост-эксплуатация и сбор полезных данных

Любой эксплойт, который успешно использует уязвимость, даёт результат в виде открытого сеанса. Вы можете использовать его для извлечения информации из системы цели. Реальная ценность атаки зависит от данных, которые вы можете получить от цели, к примеру, хэши паролей, системные файлы и скриншоты, а также то, как вы можете использовать эти данные для последующего доступа к дополнительным системам.

Чтобы просмотреть список открытых сессий, выберите вкладку «Сеансы (**Sessions**)». Нажмите на идентификатор сеанса, чтобы просмотреть пост-эксплуатационные задачи, которые могут быть запущены против хоста.



Чтобы получить данные из взломанной системы, нажмите кнопку «**Collect**».

Home > i eat cake > Sessions

Collect Cleanup

Active Sessions

SESSION	OS	HOST	TYPE	AGE	DESCRIPTION	ATTACK MODULE
Session 29	Windows	10.20.36.53 - MS-W03R2-3U-1	Meterpreter	about 1 hour		MS08_067_NETAPI

Closed Sessions

No closed sessions

Список всех открытых сеансов показывает вам типы полезных данных, которые могут быть получены.

Home > kitty time > Sessions > Collect System Data

Active Sessions

ACTIVE SESSIONS	SESSION TYPE
Session 28 - 10.20.36.53	meterpreter

Evidence to collect

Universal

- ☒ System information
- ☒ System passwords

***Nix Shell**

- ☒ SSH Keys

Windows Meterpreter

- ☒ Screenshots
- ☒ Installed Applications
- ☒ Drives
- ☒ Logged on Users
- ☒ Primary Domain
- ☐ Collect other files

Filename pattern:

Maximum File Count:

Maximum File Size: (kilobytes)

Создание отчета

В конце пентеста вам нужно будет создать отчёт, содержащий результаты ваших действий. Metasploit предоставляет ряд отчетов, которые можно использовать для компоновки результатов тестирования и объединения данных в удобный формат, которым можно делиться. Каждый отчет распределяет ваши результаты в соответствующие разделы, показывает диаграммы и графики для статистических данных, и суммирует основные итоги. Для получения дополнительной информации ознакомьтесь с разделом о «Отчёты».

Создание и управление проектами

Проект содержит в себе рабочее пространство, которое используется для выполнения различных стадий теста на вторжение и хранит данные, которые вы получаете, атакуя цели. Вы создаете проект

для настройки задач и запуска тестов. Вы можете создавать такое число проектов, которое вам понадобится, и легко переключаться между проектами в процессе выполнения задач.

У каждого проекта есть владелец. Владелец может выбирать пользователей, которые могут иметь доступ к редактированию, просмотру, и запуску задач в проекте. Тем не менее, пользователи с уровнем доступа администратора могут просматривать и редактировать любой проект независимо от того, предоставляет ли им доступ владелец проекта.

Вы можете создавать проекты для разделения взаимодействия на логические группы. Часто будет происходить так, что у вас будут разные требования к различным подсетям в организации. Следовательно, достаточно эффективным решением будет иметь несколько проектов для осуществления этих требований.

Например, вы можете создать отдельный проект для отдела кадров и еще один проект для ИТ-отдела. Ваши требования к этим отделам могут значительно различаться, будет логично разделить эти цели на несколько проектов. В конце работы вы можете создать отдельные отчеты для каждого отдела, чтобы провести сравнительный анализ и предоставить ваши данные организации.

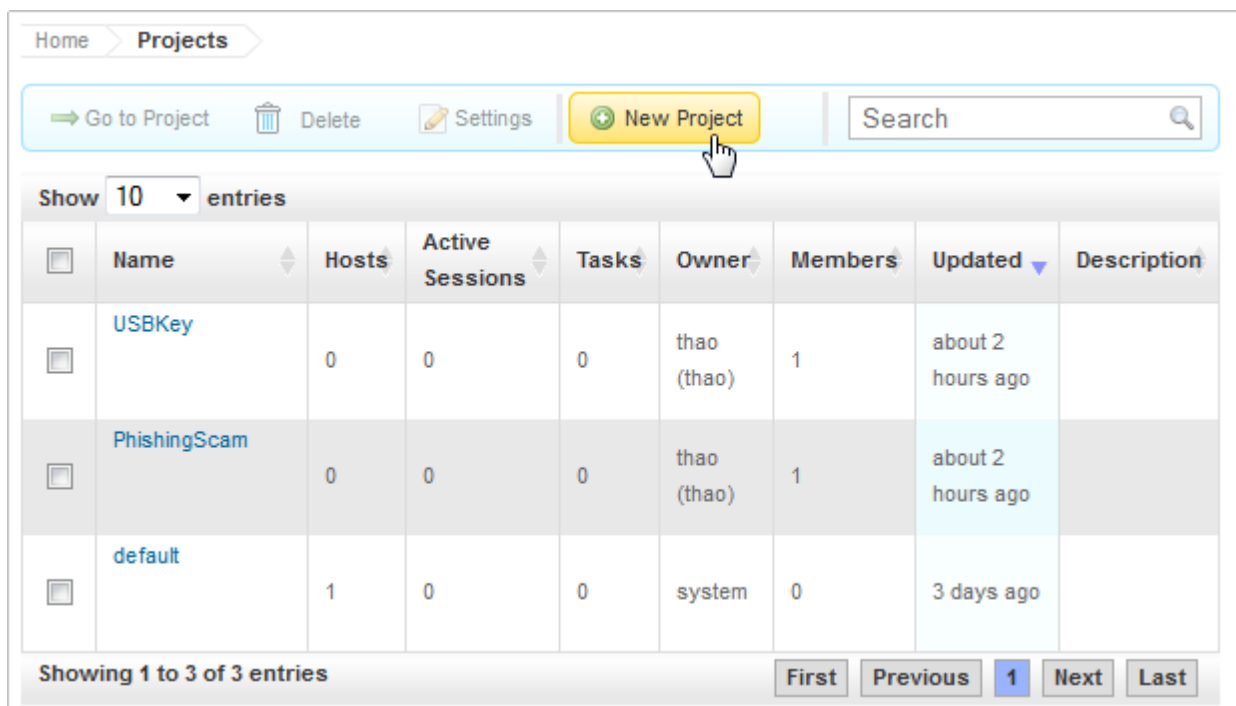
Создание проекта

Проект - это рабочее пространство, которое вы используете для создания теста на вторжение. Каждый проект логически объединяет вместе хосты, которые вы хотите атаковать, и тип информации, которую вы хотите получить в итоге. У каждого проекта имеется следующая информация:

1. Название: присваивает уникальный идентификатор проекту.
2. Описание: раскрывает цели и масштабы проекта.
3. Диапазон сети: определяет сетевой диапазон по умолчанию для проекта. Когда вы создаете проект, Metasploit Pro автоматически заполняет целевой диапазон диапазоном сети, который вы определяете для проекта. Metasploit Pro не будет принуждать проект использовать сетевой диапазон, если вы не включите параметр ограничения диапазона сети.
4. Ограничение диапазона сети: параметр, который ограничивает проект определенным диапазоном. Включите эту опцию, если вы хотите убедиться, что тест не нацелен на устройства, выходящие за рамки сего диапазона. Если эта опция будет включена, Metasploit Pro не будет запускать задачи против цели, адрес которой не попадает в пределы диапазона сети.

Чтобы создать проект:

1. На странице проектов, нажмите кнопку «Новый проект (**New Project**)».



- Когда откроется окно нового проекта, найдите область настроек (**Project Settings**), и введите название проекта, его описание и сетевой диапазон:

Project Settings

Project name*

Description

Network range

☐ Restrict to network range

* denotes required field

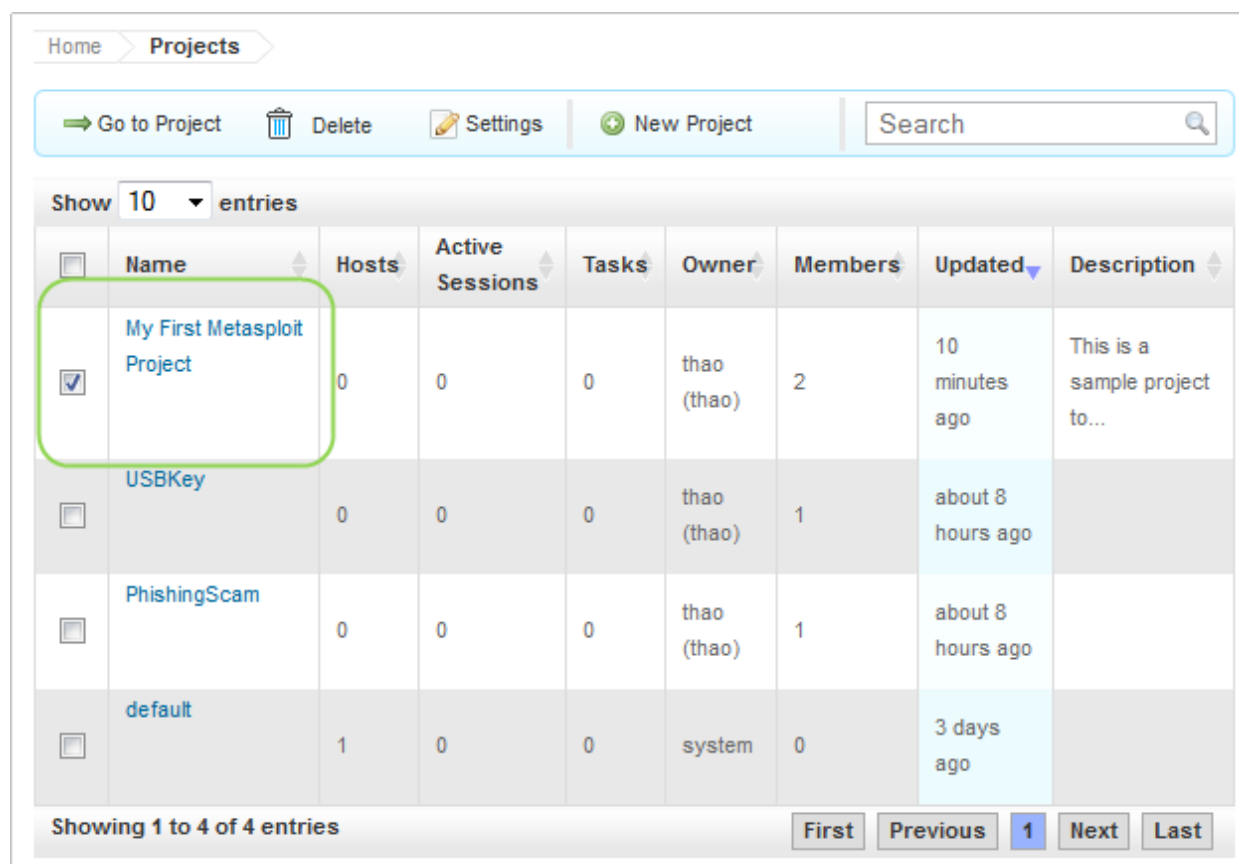
- Выберите опцию ограничения сетевого диапазона (**Restrict to network range**), если вы хотите установить границы диапазона для проекта.
- В области установки доступа (**User Access**), укажите следующую информацию:
 - Project owner** – человек, который является владельцем проекта.
 - Project members** – пользователи, которые могут получать доступ к задачам в проекте, редактировать и запускать их.
- Завершите создание проекта.

Удаление проекта.

Когда вы удаляете проект, вы удаляете все данные, которые содержит проект, включая отчеты, данные хоста, выгруженную информацию, данные уязвимости и теги хоста. После удаления проекта вы не сможете снова просмотреть или получить доступ к нему.

В случае, если вы хотите удалить проект, но сохранить его данные, есть возможность экспортировать данные проекта. Когда вы экспортируете данные проекта, система предоставит вам XML или ZIP-файл с содержимым проекта. Вы всегда можете импортировать этот файл, чтобы загрузить данные проекта в Metasploit Pro.

1. Перейдите в **Project > Show all Projects** из главного меню.
2. Когда откроется страница проектов, выберите те, которые вы хотите удалить.



3. Нажмите удалить (**Delete**).
4. Когда появится окно подтверждения, кликните «**OK**» для удаления проекта.

Установка диапазона сети.

При создании проекта, вы можете установить вариативный сетевой диапазон, который задает масштаб работы проекта. Диапазон сети определяет адреса, которые Metasploit Pro использует для автоматического заполнения целевых адресов поискового сканирования и сканирования Nexpose. Он также определяет границы сети, в которых Metasploit Pro будет выполнять проект.

Вам не нужно устанавливать сетевой диапазон в случае, если вы не хотите использовать чёткие границы. Если же вы решите обеспечить соблюдение границ сетевого диапазона в проекте, Metasploit Pro использует сетевой диапазон, который вы определяете для проекта.

1. В открытом проекте, выберите **Project > Show all Projects** из главного меню.
2. Выберите проект, для которого вы хотите установить сетевой диапазон.

Home > **Projects**

[Go to Project](#)
[Delete](#)
[Settings](#)
[New Project](#)

Show 10 entries

☐	Name	Hosts	Active Sessions	Tasks	Owner	Members	Updated	Description
☒	My First Metasploit Project	0	0	0	john	1	about 21 hours ago	This is a sample project to...
☐	USBKey	0	0	0	thao (thao)	1	1 day ago	
☐	PhishingScam	0	0	0	thao (thao)	1	1 day ago	
☐	default	1	0	0	system	0	4 days ago	

Showing 1 to 4 of 4 entries

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

3. Нажмите на кнопку настроек (**Settings**).

Home > **Projects**

[Go to Project](#)
[Delete](#)
[Settings](#)
[New Project](#)

Show 10 entries

☐	Name	Hosts	Active Sessions	Tasks	Owner	Members	Updated	Description
☒	My First Metasploit Project	0	0	0	thao (thao)	2	10 minutes ago	This is a sample project to...
☐	USBKey	0	0	0	thao (thao)	1	about 8 hours ago	
☐	PhishingScam	0	0	0	thao (thao)	1	about 8 hours ago	
☐	default	1	0	0	system	0	3 days ago	

Showing 1 to 4 of 4 entries

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

4. В поле сетевого диапазона (**Network range**), введите сетевой диапазон, которым вы хотите ограничить проект. Вы можете ввести один IP-адрес, диапазон IP-адресов, написанный через дефис, или стандартную запись CIDR. Если будет указана запись CIDR, вы можете использовать звездочку как случайное число. Например, 192.168.1.* будет значить диапазон 192.168.1.1-255.

Project Settings * denotes required field

Project name*

Description

Network range

☒ Restrict to network range

5. Нажмите клавишу обновления проекта (**Update Project**)

Ограничение работы проекта до сетевого диапазона

Вы можете жёстко ограничить сетевой диапазон, чтобы обеспечить соблюдение его границ проектом. Когда вы ставите подобное ограничение, вы не можете запускать какие-либо задачи, если целевые адреса этих задач не попадают в определённый вами диапазон сети.

Например, если у вас есть клиент, который хочет, чтобы вы тестировали определенный сетевой диапазон, вы можете настроить проект так, чтобы убедиться, что вы случайно не повлияете на какие-либо устройства, которые находятся за пределами указанного диапазона.

1. Перейдите в **Project > Show all Projects** из главного меню.
2. Выберите проект и нажмите на кнопку настройки (**Settings**).

Home > **Projects**

[Go to Project](#)
[Delete](#)
[Settings](#)
[New Project](#)

Show **10** entries

☐	Name	Hosts	Active Sessions	Tasks	Owner	Members	Updated	Description
☒	My First Metasploit Project	0	0	0	thao (thao)	2	10 minutes ago	This is a sample project to...
☐	USBKey	0	0	0	thao (thao)	1	about 8 hours ago	
☐	PhishingScam	0	0	0	thao (thao)	1	about 8 hours ago	
☐	default	1	0	0	system	0	3 days ago	

Showing 1 to 4 of 4 entries

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

3. В поле сетевого диапазона (**Network range**), введите сетевой диапазон, которым вы хотите ограничить проект. Вы можете ввести один IP-адрес, диапазон IP-адресов, написанный через дефис, или стандартную запись CIDR. Если будет указана запись CIDR, вы можете использовать звездочку как случайное число. Например, 192.168.1.* будет значить диапазон 192.168.1.1-255.

Project Settings * denotes required field

Project name*

Description

Network range

☒ Restrict to network range

4. Поставьте галочку в поле «**Restrict to Network Range**».

Project Settings * denotes required field

Project name*

Description

Network range

☒ Restrict to network range

5. Нажмите клавишу обновления проекта (**Update Project**)

Изменение владельца проекта

По умолчанию владельцем проекта является человек, который первоначально создаёт и настраивает проект. Вы можете изменить владельца проекта для передачи права собственности и передачи проектов членам команды.

Владелец проекта предоставляет вам и вашим членам команды возможность легко идентифицировать проекты как собственные. Например, если вы хотите увидеть проекты, которые были назначены вам, вы можете включить сортировку списка проектов по владельцу. Все ваши проекты будут сгруппированы вместе.

1. Перейдите в **Project > Show all Projects** из главного меню.

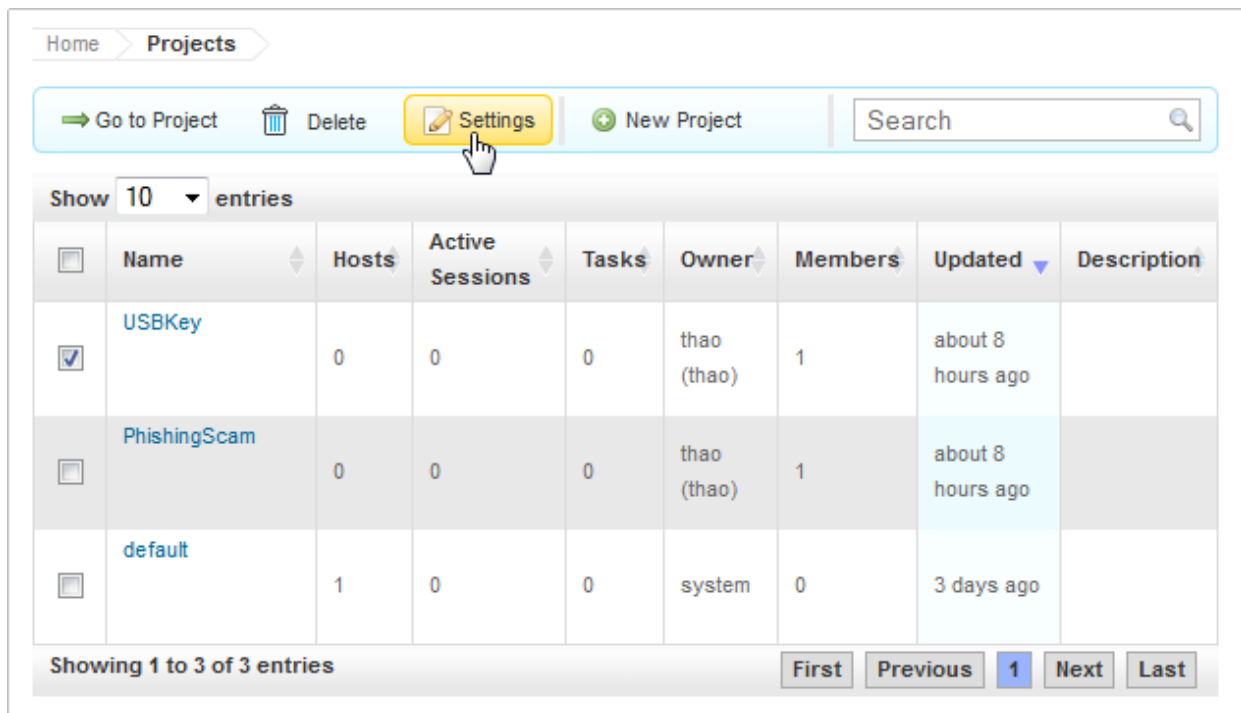
User Access

Project owner

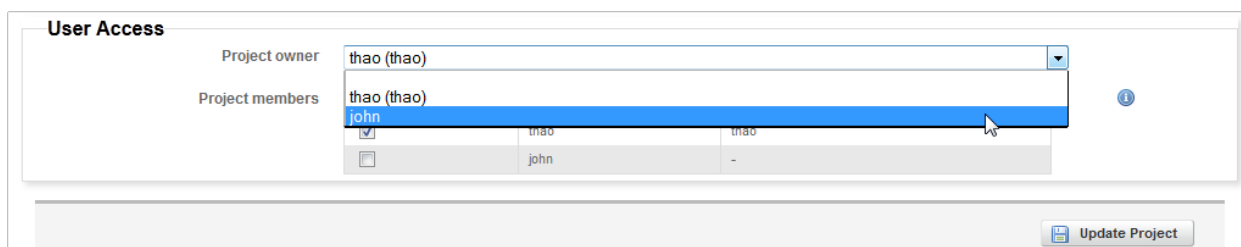
Project members

☒	thao	thao
☐	john	-

2. Когда откроется страница проектов, выберите тот, которому вы хотите назначить владельца.
3. Нажмите кнопку настроек (**Settings**).



4. Когда откроется окно настроек, найдите область настройки доступа пользователей (User Access).
5. Нажмите на выпадающее меню владельцев проекта (**Project owner**) и выберите человека, которого вы хотите назначить.



6. Нажмите клавишу обновления проекта (**Update Project**).

Управление доступом пользователей

Как владелец проекта, вы можете ограничить число членов команды, которые могут просматривать и редактировать ваш проект. Например, если у вас есть данные, которые вы хотите сохранить только у себя, вы можете отключить права доступа для других членов команды.

!!! Члены команды с правами доступа администратора могут просматривать и редактировать все проекты, независимо от настроек прав доступа.

Чтобы управлять доступом пользователя, который он имеет к проекту:

1. Перейдите в **Project > Show all Projects** из главного меню.
2. Когда откроется страница проектов, выберите тот, который вы хотите изменить.
3. Нажмите кнопку настроек (**Settings**).

Home Projects

Go to Project Delete Settings New Project Search

Show 10 entries

☐	Name	Hosts	Active Sessions	Tasks	Owner	Members	Updated	Description
☒	My First Metasploit Project	0	0	0	thao (thao)	2	10 minutes ago	This is a sample project to...
☐	USBKey	0	0	0	thao (thao)	1	about 8 hours ago	
☐	PhishingScam	0	0	0	thao (thao)	1	about 8 hours ago	
☐	default	1	0	0	system	0	3 days ago	

Showing 1 to 4 of 4 entries

First Previous 1 Next Last

4. Когда откроется окно настроек, найдите область настройки доступа пользователей (User Access).
5. Выставьте галочки около участников проекта, которые смогут просматривать и изменять проект или уберите их около участников, которые не смогут модифицировать проект.

User Access

Project owner: thao (thao)

Project members:

☒	User	Full Name
☒	thao	thao
☒	john	-

Create Project

6. Нажмите клавишу обновления проекта (**Update Project**).

Командная работа

Поддержка многопользовательской работы предоставляет вам возможность сотрудничать или взаимодействовать с другими членами команды в рамках проведения теста на вторжение. Вы и ваша команда можете войти в один и тот же экземпляр Metasploit Pro, чтобы выполнять задачи, просматривать данные и делиться проектами. Вы можете получить доступ к Metasploit Pro через веб-интерфейс Metasploit Web UI, который может работать на локальной машине либо через сеть.

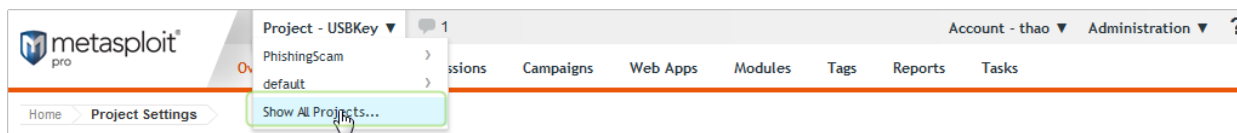
Некоторые функции, которые можно реализовать для улучшения совместной работы - это границы сети, теги хостов, и комментарии к хостам. Эти функции помогают создавать отдельные рабочие

задания для каждого члена команды и сгруппировать их действия в логические группы. Например, вы можете присвоить определенные хосты конкретному члену команды для их тестирования.

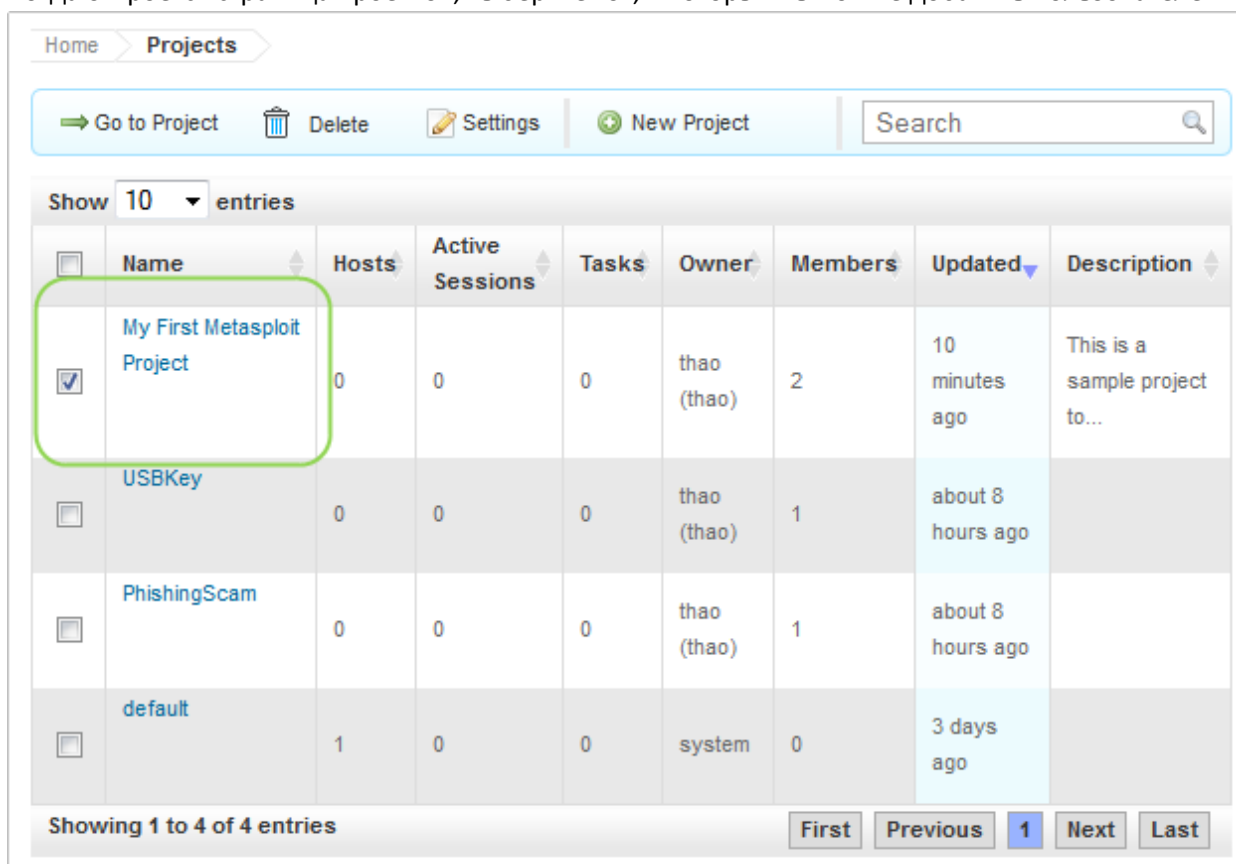
Добавление пользователей в проект.

Вы можете дать членам команды доступ к проекту, чтобы они могли просматривать, редактировать и запускать задачи.

1. Перейдите в **Project > Show all Projects** из главного меню.



2. Когда откроется страница проектов, выберите тот, в который вы хотите добавить пользователей.



3. Найдите настройки доступа пользователей (**User Access**). Этот список показывает всех пользователей Metasploit Pro.
4. Нажмите кнопку настроек (**Settings**).
5. Выберите пользователей, которым вы хотите дать доступ к проекту.

User Access

Project owner: thao (thao)

Project members:

	User	Full Name
☒	thao	thao
☒	john	-

[Update Project](#)

- Нажмите клавишу обновления проекта (**Update Project**).

Удаление пользователей из проекта.

Вы можете удалить членов команды из проекта, чтобы они не могли просматривать, редактировать и запускать задачи. Когда вы удаляете пользователя из проекта, вы отключаете им доступ к проекту.

- В открытом проекте, выберите **Project > Show all Projects** из главного меню.

Home > **Projects**

[Go to Project](#)
[Delete](#)
[Settings](#)
[New Project](#)

Show 10 entries

	Name	Hosts	Active Sessions	Tasks	Owner	Members	Updated	Description
☒	My First Metasploit Project	0	0	0	thao (thao)	2	10 minutes ago	This is a sample project to...
☐	USBKey	0	0	0	thao (thao)	1	about 8 hours ago	
☐	PhishingScam	0	0	0	thao (thao)	1	about 8 hours ago	
☐	default	1	0	0	system	0	3 days ago	

Showing 1 to 4 of 4 entries

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

- Найдите настройки доступа пользователей (**User Access**). Этот список показывает всех пользователей Metasploit Pro.
- Снимите галочки около пользователей, которым вы хотите отключить доступ к проекту.

User Access

Project owner: john

Project members:

	User	Full Name
☒	thao	thao
☐	john	-

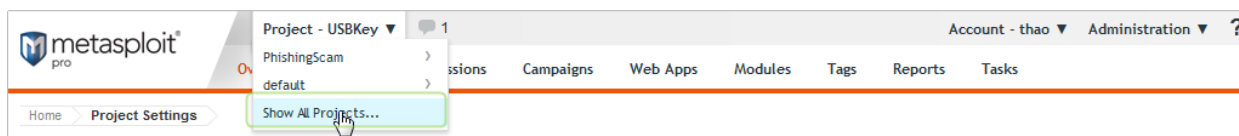
[Update Project](#)

- Нажмите клавишу обновления проекта (**Update Project**).

Переназначение проекта пользователю

Владелец проекта - это лицо, которое создает проект и берет на себя ответственность за данные и проводимые тесты на вторжение. Вы можете использовать роль владельца проекта для делегирования проектов или рабочих заданий членам вашей команды.

- Перейдите в **Project > Show all Projects** из главного меню.



- Выберите проект, который вы хотите переназначить пользователю.

Home > **Projects**

[Go to Project](#)
[Delete](#)
[Settings](#)
[New Project](#)

Show 10 entries

☐	Name	Hosts	Active Sessions	Tasks	Owner	Members	Updated	Description
☒	My First Metasploit Project	0	0	0	thao (thao)	2	10 minutes ago	This is a sample project to...
☐	USBKey	0	0	0	thao (thao)	1	about 8 hours ago	
☐	PhishingScam	0	0	0	thao (thao)	1	about 8 hours ago	
☐	default	1	0	0	system	0	3 days ago	

Showing 1 to 4 of 4 entries

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

- Нажмите кнопку настроек (**Settings**).

- Найдите настройки доступа пользователей (User Access). Этот список показывает всех пользователей Metasploit Pro.
- Из выпадающего меню назначения владельцев проекта (**Project Owner**) выберите будущего владельца проекта.

- Нажмите клавишу обновления проекта (**Update Project**).

Комментарии к хостам

Вы можете добавить комментарий к хосту для обмена информацией о нём. Например, если вы обнаружите уязвимость на хосте, и вы хотите поделиться этой информацией с другими пользователями проекта, вы можете добавить комментарий к этому узлу. Когда вы просматриваете детали хоста, вы можете видеть комментарии, которые добавили другие пользователи.

Добавление комментариев к хостам

- Из открытого проекта, перейдите в меню **Analysis > Hosts**
- Кликните по идентификатору хоста, к которому вы хотите добавить комментарий.
- Когда откроется окно информации о хосте, нажмите кнопку добавления комментария (**Update Comment**).

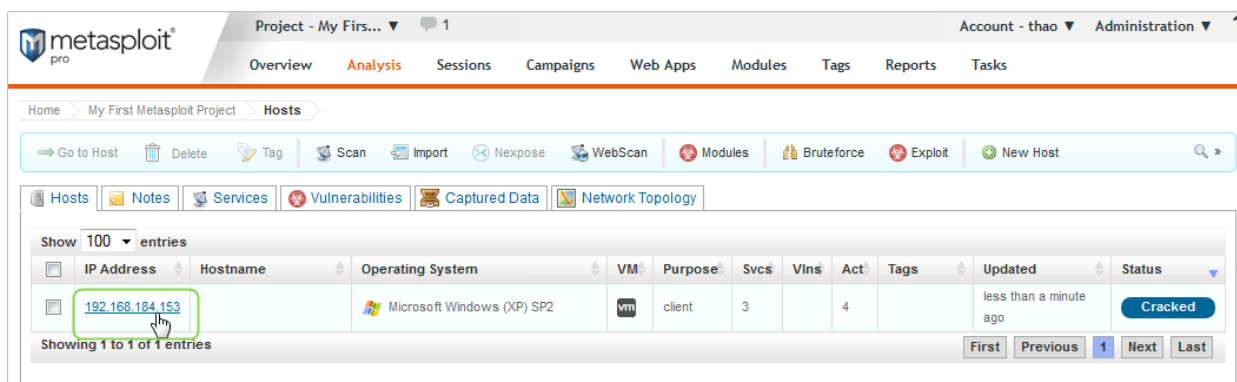
- Введите информацию, которую вы хотите добавить к хосту в поле «Комментарии (**Comments**)». Например, если вы знаете, что хост не подвержен влиянию эксплойтов, вы можете добавить эту

информацию в качестве комментария. Когда другие члены команды увидят это примечание, они узнают, что им не следует пытаться взламывать хост.

5. Нажмите на кнопку сохранения комментария (**Save comments**).

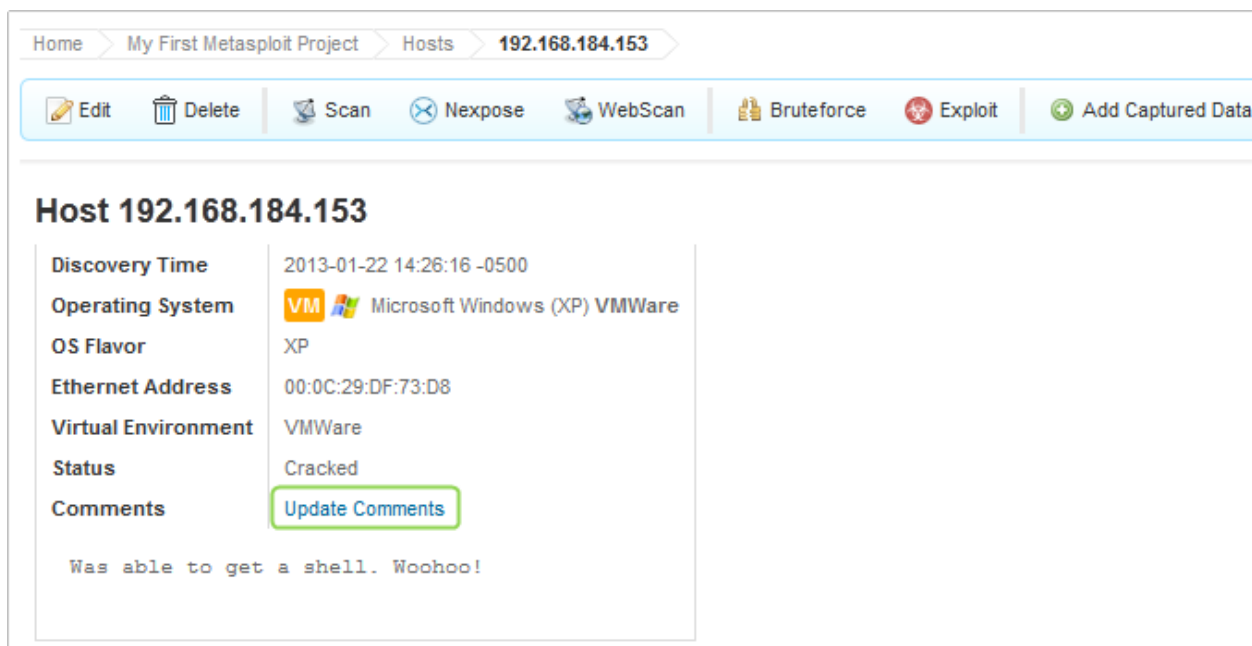
Обновление комментария к хосту

1. Из открытого проекта, перейдите в меню **Analysis > Hosts**
2. Кликните по идентификатору хоста, к которому вы хотите добавить комментарий.

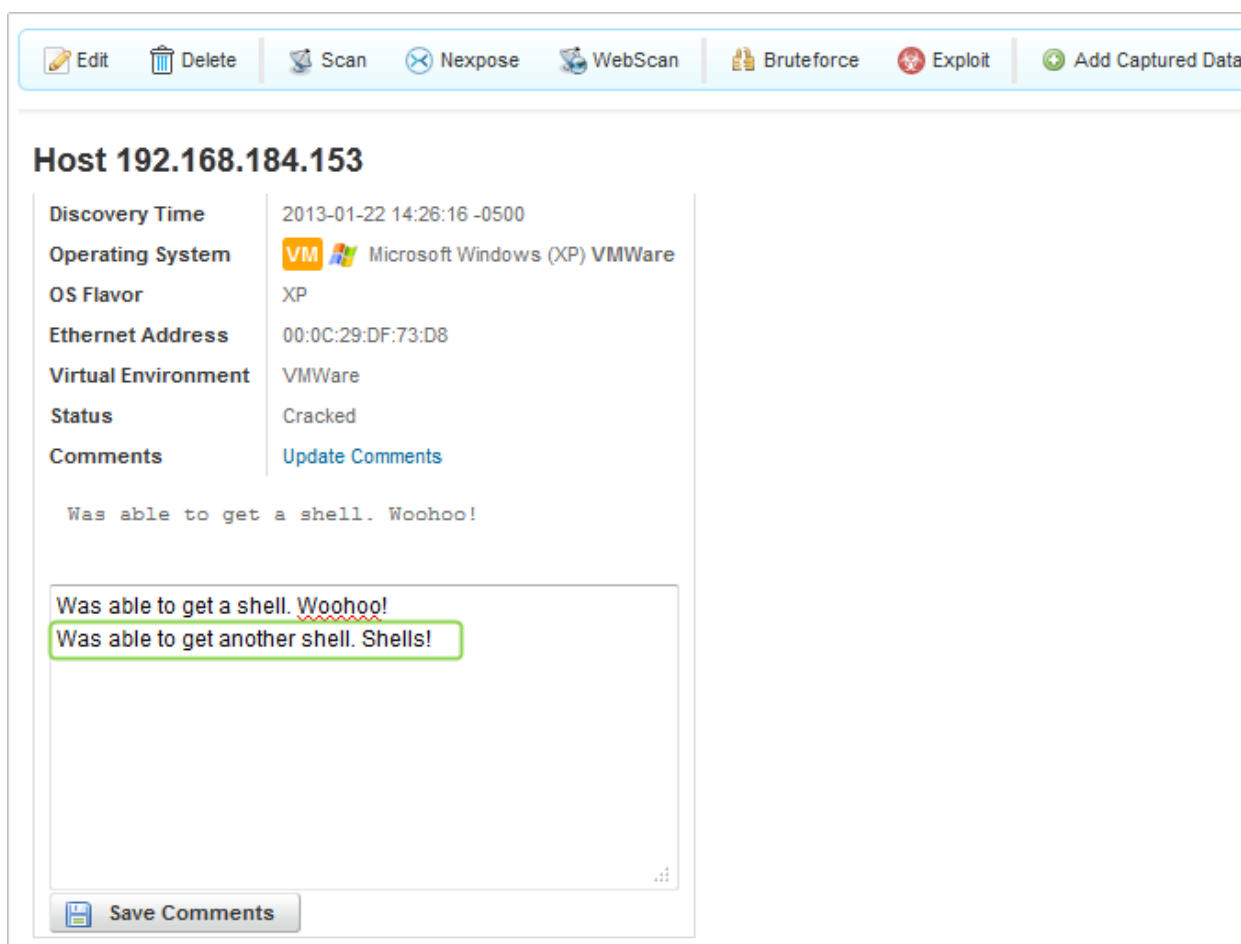


3. Когда откроется окно информации о хосте, нажмите кнопку добавления комментария (**Update Comment**).

32



4. Измените информацию в поле «Комментарии (Comments)».



5. Нажмите на кнопку сохранения комментария (Save comments).

Управление учетными записями

Учетная запись пользователя даёт вам и вашим членам команды доступ к Metasploit Pro. Вы используете учётную запись пользователя чтобы заходить в Metasploit Pro и создавать идентификаторы для других членов команды.

Учетная запись пользователя состоит из логина, полного имени пользователя, пароля и роли. Используйте следующую информацию для настройки учетной записи пользователя:

- *Логин* – имя пользователя, которое система использует для уникальной идентификации.
- *Полное имя* – имя и фамилия пользователя, владеющего учётной записью.
- *Пароль* – ряд из восьми знаков, который позволяет использовать аккаунт.
- *Роль* – уровень доступа, который имеет пользователь в Metasploit Pro и других проектах. Это может быть администратор либо стандартный пользователь.

Типы учётных записей

Учетная запись пользователя может быть либо записью администратора, либо записью стандартного пользователя. Тип учетной записи определяет уровень привилегий, которые должны

быть у пользователя для выполнения определенных задач. Например, администраторы имеют неограниченный доступ к системе, и могут выполнять обновления системы, управлять учетными записями и настраивать параметры системы. С другой стороны, учетные записи, не являющиеся администраторами, имеют доступ к Metasploit Pro, но могут выполнять только ограниченный набор задач.

Учетная запись администратора

У учетной записи администратора есть неограниченный доступ ко всем функциям Metasploit Pro. Будучи администратором, вы можете удалять и добавлять учетные записи пользователей, обновлять Metasploit Pro и иметь доступ ко всем проектам.

Стандартная учетная запись

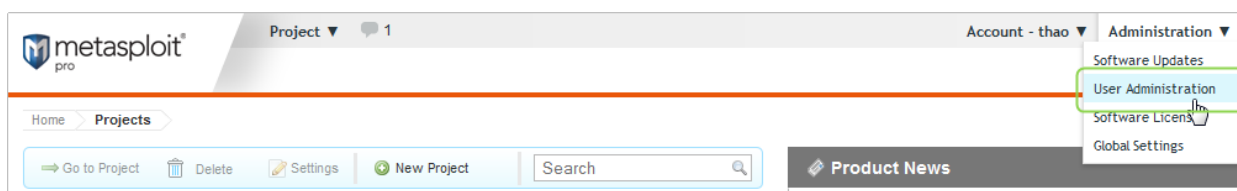
Стандартная учетная запись дает пользователям доступ к Metasploit Pro, но не предоставляет им неограниченный контроль над проектами и системными настройками. Эта учетная запись ограничивает доступ пользователя проектами, к которым они имеют доступ и проектами, принадлежащими им.

Пользователь со стандартной учетной записью может выполнять следующие задачи:

- Создавать другие учетные записи и управлять ими.
- Изменять основные настройки Metasploit Pro.
- Обновлять Metasploit Pro.
- Обновлять лицензионный ключ.
- Просматривать проекты, к которым у него имеется доступ.

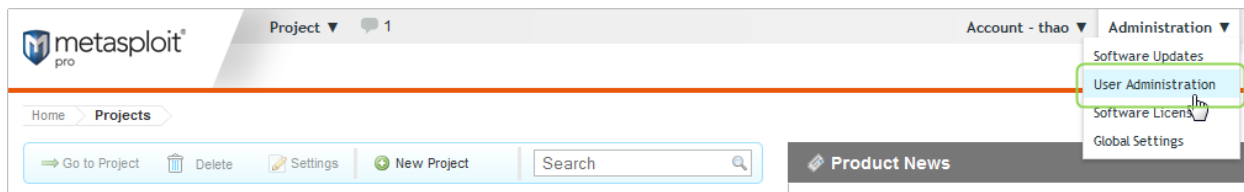
Создание учетной записи пользователя

1. Перейдите в меню **Administrator > User Accounts** из главного меню.

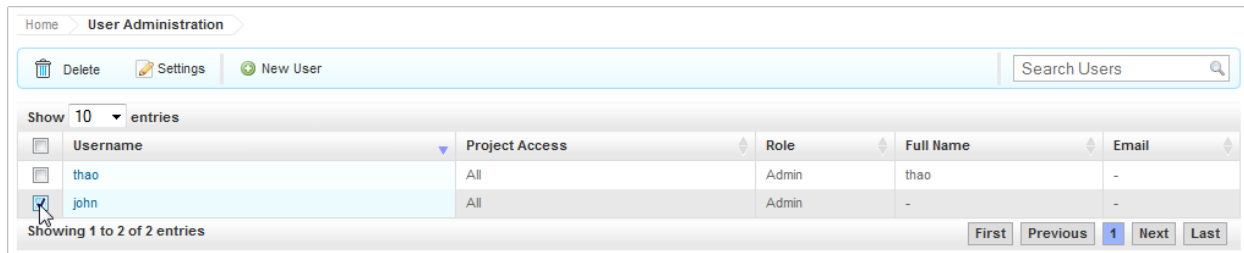


2. Когда откроется окно администрирования пользователей, нажмите кнопку добавления нового пользователя (**New User**).
3. Когда откроется окно добавления нового пользователя, введите следующую информацию для создания нового пользователя:

- **Имя пользователя (User name)** - введите идентификатор пользователя для учетной записи.
- **Полное имя (Full name)** - введите имя пользователя и фамилию.



2. Выберите учётную запись, которую вы хотите изменить.



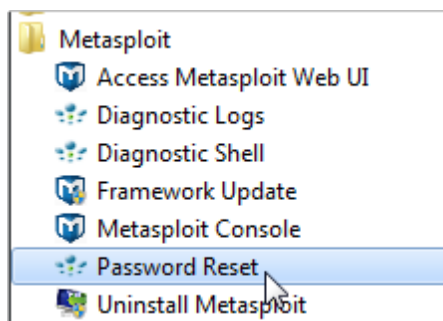
3. Нажмите кнопку настроек (**Settings**).
4. Найдите поле смены пароля (**Change Password**).
5. В поле нового пароля (**New Password**) введите пароль к учётной записи. Пароль должен содержать не менее восьми символов и состоять из букв, цифр и, по крайней мере, одного специального символа.

6. Повторно введите пароль в поле подтверждения (**Password Confirmation**).
7. Нажмите кнопку смены пароля (**Change Password**).

Если вы забыли пароль или хотите его сбросить, следуйте инструкциям для вашей операционной системы.

Windows

8. Из меню «Пуск», перейдите в **All Programs > Metasploit > Password Reset**.
9. Когда появится окно сброса пароля, подождите загрузки окружения.

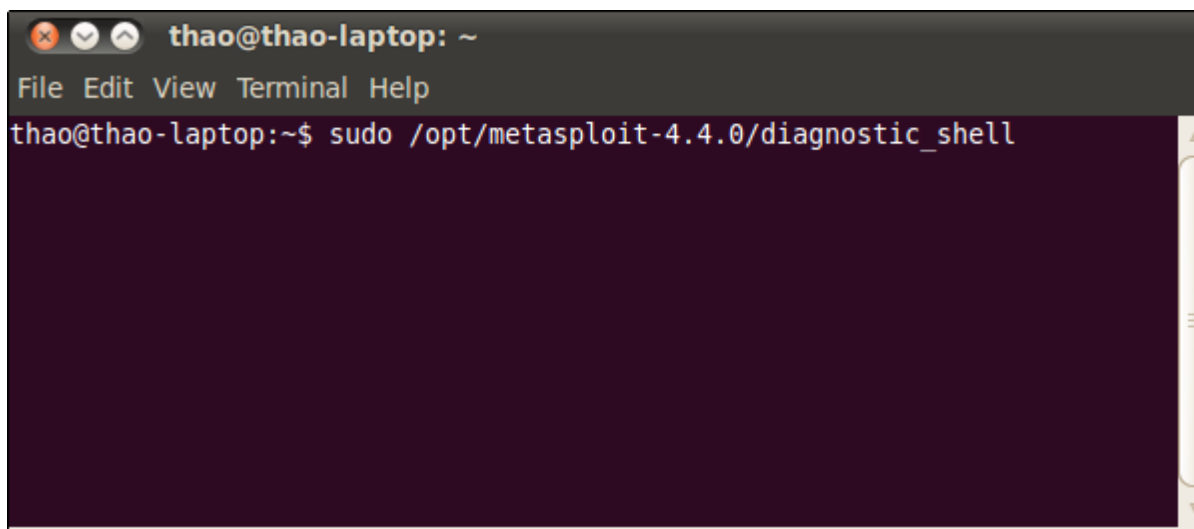


10. Когда диалоговое окно запросит у вас подтверждение продолжения, кликните «YES». Система сбросит пароль на случайное значение.
11. Скопируйте пароль и используйте его для следующего входа в Metasploit Pro. Вы сможете изменить пароль после входа в систему.

12. Выйдите из окна сброса пароля.

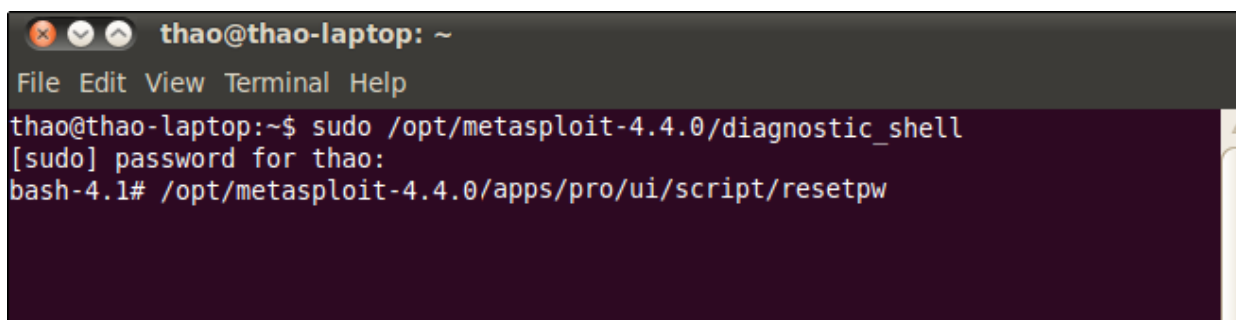
Linux

1. Откройте терминал и выполните следующую команду:
`sudo </path/to/metasploit>/diagnostic_shell`.



```
thao@thao-laptop: ~
File Edit View Terminal Help
thao@thao-laptop:~$ sudo /opt/metasploit-4.4.0/diagnostic_shell
```

2. Если понадобится, введите ваш пароль для выполнения команды `sudo`.
3. Когда система сделает запрос `bash#`, введите
`</path/to/metasploit>/apps/pro/ui/script/resetpw`
чтобы запустить скрипт сброса пароля.



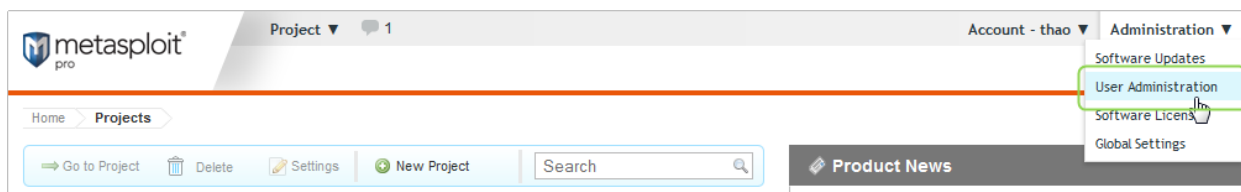
```
thao@thao-laptop: ~
File Edit View Terminal Help
thao@thao-laptop:~$ sudo /opt/metasploit-4.4.0/diagnostic_shell
[sudo] password for thao:
bash-4.1# /opt/metasploit-4.4.0/apps/pro/ui/script/resetpw
```

4. Скопируйте пароль и используйте его для следующего входа в Metasploit Pro.
Вы сможете изменить пароль после входа в систему.
5. Выйдите из терминала.

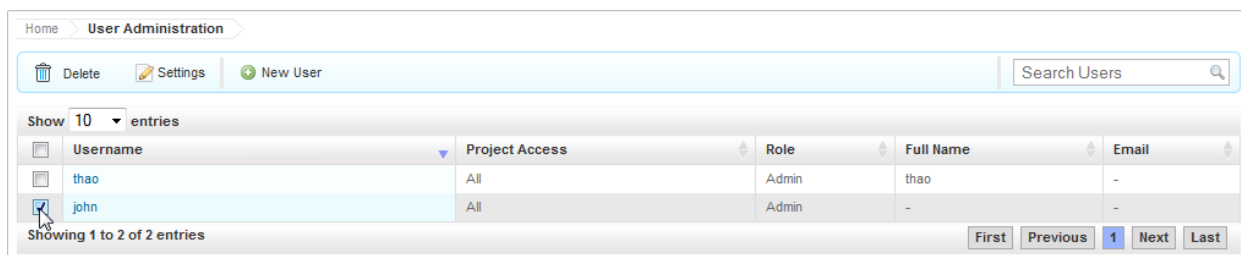
Удаление аккаунта пользователя

Если у вас учетная запись администратора, вы можете удалять учетные записи пользователей, которые вам больше не нужны. Когда вы удалите учетную запись пользователя, система переназначит проекты, принадлежащие учетной записи. Любые проекты, у которых нет владельца, будут иметь в качестве владельца проекта систему.

1. Перейдите в меню **Administrator > User Accounts** из главного меню.

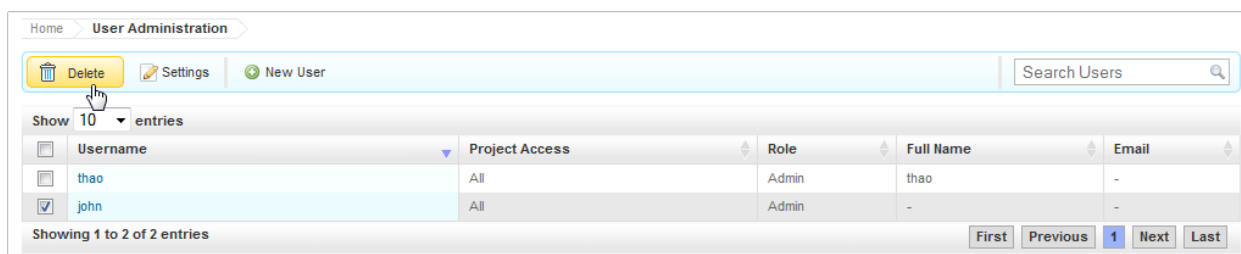


2. Выберите учётную запись, которую вы хотите удалить.



3. Нажмите «Удалить (Delete)».

39



4. Нажмите «ОК», чтобы подтвердить удаление аккаунта.

Поисковое сканирование

Одним из первых шагов в тестировании на вторжение является разведка. Разведка - это процесс сбора информации для лучшего понимания целевой сети. Она позволяет вам создать список целевых IP-адресов и разработать план атаки. После того, как вы получите список IP-адресов, вы можете запустить поисковое сканирование, чтобы узнать больше об этих хостах. Поисковое сканирование определяет операционные системы, работающие в сети, сопоставляет их с IP-адресами и перечисляет открытые порты и службы для этих систем.

Поисковое сканирование - это внутренний сканер Metasploit. Он использует Nmap для сканирования базового TCP-порта и запускает дополнительные модули сканирования для сбора дополнительной информации о целевых хостах. По умолчанию поисковое сканирование включает в себя проверку UDP, которая отправляет UDP-зонды на наиболее известные порты UDP, такие как NETBIOS, DHCP, DNS и SNMP. Поисковое сканирование проверяет приблизительно 250 портов, которые обычно открыты внешним службам и чаще всего проверяются во время теста на вторжение.

Во время поискового сканирования Metasploit Pro автоматически сохраняет данные хоста в проекте. Вы можете просмотреть эти данные для лучшего понимания структуры сети и определения наилучшего способа атаковать каждую цель. Часто, структура сети дает представление о типах

приложений и устройств, которые установлены в целевой системе. Чем больше информации вы можете получить о цели, тем проще вам будет настроить тест точно для неё.

Как работает поисковое сканирование

Данное сканирование может быть разделено на четыре отдельные фазы:

- Сканирование пинга
- Сканирование портов
- Определение ОС и их версий
- Импорт данных

Сканирование пинга

Первая фаза поискового сканирования, сканирование пинга, определяет, находятся ли хосты в сети. Поисковое сканирование устанавливает параметр `-PI`, который приказывает Nmap выполнить стандартный обмен пингами ICMP. Один запрос ICMP-эха отправляется к цели. Если получен отзыв ICMP-эха, хост считается находящимся в сети. Если хост онлайн, поисковое сканирование включает его в список сканирования портов.

Сканирование портов

Во время второй фазы сканирования портов Metasploit Pro запускает Nmap для определения портов, которые являются открытыми и служб, доступных в этих портах. Nmap отправляет зонды различным портам и классифицирует ответы для определения текущего состояния порта. Сканирование охватывает широкий спектр широко распространенных портов, такие как HTTP, telnet, SSH и FTP.

Поисковое сканирование использует настройки Nmap по умолчанию, но у вас есть возможность добавить дополнительные параметры Nmap для настройки сканирования. Например, поисковое сканирование запускает сканирование TCP SYN по умолчанию. Если вы хотите запустить сканирование подключения TCP вместо сканирования TCP SYN, вы можете указать параметр `-sT`. Любые варианты, которые вы указываете, будут превалировать над стандартными параметрами Nmap, которые используются поисковым сканированием.

Определение операционных систем и их версий

После того, как поисковое сканирование определит открытые порты, начинается третья фаза. Nmap отправляет множество зондов к этим портам и обнаруживает номера версий служб и операционную систему, базируясь на откликах системы на запросы. Операционная система и номер версии дают ценную информацию об атакуемой системе и может помочь вам определить возможную уязвимость и предупредить ложные срабатывания.

Импорт данных

Наконец, после того, как Nmap собирает все данные и создает отчет, Metasploit Pro импортирует собранные данные в проект. Metasploit Pro использует полученную информацию для отправки дополнительных модулей, нацеленных на обнаруженные службы, которые исследуют цель для получения дополнительных данных. Например, если сканирование обнаружит цель с помощью зондов telnet, целевая система может ответить запросом аутентификации. Это может значить, что служба допускает удаленный доступ к системе, поэтому на данном этапе вы можете запустить брутфорс, чтобы взломать учётные данные.

Порты, включенные в поисковое сканирование

В целом, поисковое сканирование включает в себя более чем 250 портов, которые содержат следующие группы:

- Стандартные и хорошо известные порты, такие как 20, 21, 22, 23, 25, 53, 80 и 443.
- Альтернативные служебные порты, такие как 8080 и 8442, которые являются дополнительными портами, которые используются HTTP и веб-службами.
- Порты, которые указаны по умолчанию в модулях.

Если вы не можете найти порт, который хотите сканировать, вы можете вручную добавить его в поисковое сканирование. Например, если вы знаете, что ваша компания запускает веб-серверы с открытым портом 9998, вам необходимо вручную добавить этот порт в список сканирования. Это гарантирует, что сканирование будет включать в себя каждый порт, который потенциально открыт.

Если вы хотите просканировать абсолютно все порты, вы можете указать «1-65535» в качестве диапазона портов. Имейте в виду, что поисковое сканирование, включающее в себя все порты, может занять несколько часов.

Если есть порт, который вы не хотите сканировать, вы можете его исключить. Поисковое сканирование будет пропускать любые порты в списке исключений. Например, если ваша компания использует приложение, которое выполняется на порту 1234, и вы не хотите влиять на производительность приложения, вы можете добавить порт в список исключений.

Параметры поискового сканирования

Вы можете настроить следующие параметры для поискового сканирования:

Параметр	Описание
Адреса целей	Определяет отдельные хосты или диапазон сети, которые вы хотите сканировать
Выполнить первичное сканирование портов	Выполняет сканирование портов до того, как поисковое сканирование выполнит проверку версии службы
Пользовательские аргументы Nmap	Отправляет флаги и команды в исполняемый файл Nmap. Поисковое сканирование не поддерживает следующие параметры Nmap: -o, -i, -resume, -script, -datadir и -stylesheet.
Дополнительные TCP порты	Добавляет дополнительные TCP-порты в процесс сканирования портов. По умолчанию сканирование портов охватывает небольшой, но широкий спектр портов. Используйте этот параметр, если вы хотите добавить больше портов для сканирования.
Исключённые TCP порты	Исключает определенные TCP-порты из сканирования. По умолчанию сканирование портов охватывает определенный диапазон портов. Используйте эту опцию, чтобы исключить порт, который вы не хотите сканировать.
Пользовательский диапазон TCP портов	Устанавливает ваш диапазон портов TCP для сканирования, а не указанный по умолчанию. Если вы задаете собственный диапазон портов TCP, сканирование обнаружения игнорирует все остальные порты, и использует диапазон, который вы указали.

Пользовательский источник TCP диапазона	Указывает порт источника TCP, используемый сканированием, вместо стандартного порта. Используйте этот параметр для проверки правил брандмауэра.
Быстрое обнаружение: только стандартные TCP порты	Выполняет сканирование только на наиболее распространенных портах TCP, что уменьшает количество сканируемых портов.
Скорость сканирования портов	Управляет параметром времени сканирования Nmap. Выберите один из следующих шаблонов: Insane (5) – значительно ускоряет сканирование. Предполагается, что вы находитесь в быстродействующей сети и жертвует точностью ради скорости. Задержка сканирования составляет менее 5 мс. Aggressive (4) - ускоряет сканирование. Предполагается, что вы находитесь в быстродействующей и надежной сети. Задержка сканирования составляет менее 10 мс. Normal (3) - скорость сканирования по умолчанию. Не влияет на сканирование. Polite (2) - использует меньшую пропускную способность и меньшие ресурсы цели для замедления сканирования. Sneaky (1) - скорость, используемая для избежания IDS. Paranoid (0) - скорость, используемая для избежания IDS.
Тайм-аут сканирования портов	Определяет время, которое Nmap тратит на каждый хост. Значение по умолчанию – 5 минут.
Обнаружение UDP служб	Настраивает поисковое сканирование для нахождения всех служб, которые находятся в сети. Metasploit использует пользовательские модули вместо Nmap для выполнения поиска служб UDP.
Сканирование общих строк SNMP	Запускает фоновую задачу, которая сканирует устройства, реагирующие на общие строки.
Сканирование N.323 видеоточек выхода	Сканирование на нахождение устройств N.323
Перечислять пользователей с протоколом Finger	Запрашивает имена пользователей и совершает попытки брутфорсинга списка пользователей, если сканирование обнаруживает протокол Finger.
Определять неизвестные службы	Настраивает поисковое сканирование для обнаружения всех неизвестных служб и приложений в сети.
Единичное сканирование: скан каждого хоста в индивидуальном порядке	Выполняет сканирование хостов в индивидуальном порядке. Поисковое сканирование сначала сканирует хост полностью и сохраняет информацию в базе данных, и лишь потом переходит к следующему узлу.
Прогон: показать только информацию о сканировании	Если этот параметр включен, то он подготавливает сканирование и отображает все параметры, которые поисковое сканирование будет использовать в журнале задач. Однако этот параметр не запускает сканирование.
Веб-сканирование: автоматический запуск сканера Pro Web	Автоматически запускает веб-сканирование, веб-аудит и веб-эксплойт наряду с поисковым сканированием. Обычно рекомендуется не включать этот параметр, если вы не сканируете очень узкий набор хостов. Если вы используете поисковое сканирование для большого количества хостов, веб-сканер запускается отдельно от поискового сканирования.
Имя пользователя SMB	Определяет имя пользователя SMB, которое используется поисковым сканированием для попытки входа в SMB службы.

Пароль SMB	Определяет пароль пользователя SMB, которое используется поисковым сканированием для попытки входа в SMB службы.
Домен SMB	Определяет имя SMB сервера и общедоступное имя.

Указание адресов IPv6

Metasploit Pro не определяет адреса IPv6 в автоматическом режиме во время поискового сканирования. Для хостов с IPv6 адресом, вы должны знать IP-адреса этого типа, которые используются целевыми устройствами, и указать эти адреса в Metasploit Pro. Чтобы определить отдельные адреса IPv6, вы можете использовать SNMP, Nmap или же thc-alive6, который является частью инструментария thc-ipv6.

После того, как вы узнали IPv6 адреса целевых устройств, вы можете либо импортировать текстовый файл, содержащий адреса хоста в проект, либо добавить их вручную.

Импорт файла с адресами IPv6

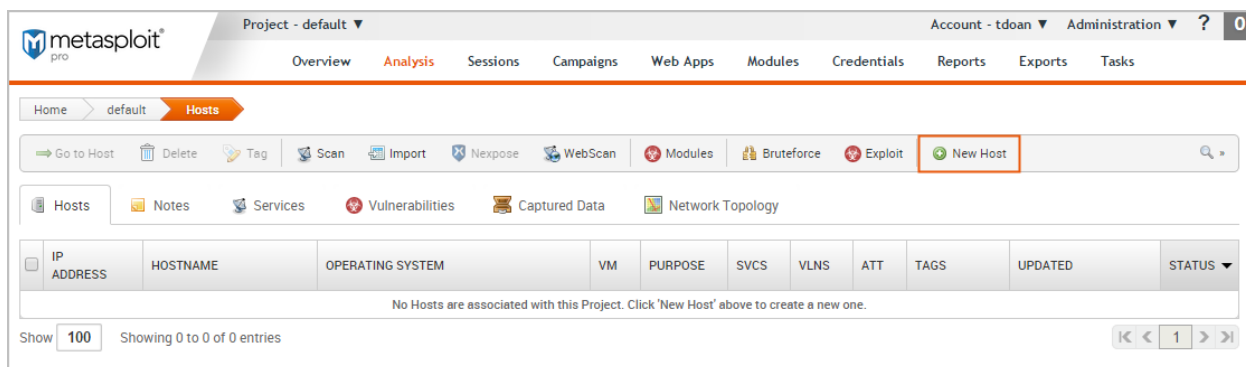
Чтобы импортировать файл, перейдите в **Analysis > Hosts**. Когда откроется страница хостов, нажмите кнопку «Импорт (**Import**)». Затем, когда откроется страница импорта данных, укажите местоположение файла с адресами хоста и импортируйте его. Это должен быть текстовый файл, в котором каждый IPv6-адрес записан в новой строке, как показано ниже:

```
FE80:0000:0000:0000:0202:B3FF:FE1E:8329
```

```
FE80:0000:0000:0000:0202:B3FF:FE1E:8328
```

Добавление хоста с IPv6 адресом в ручном режиме

Чтобы добавить хост вручную, перейдите в **Analysis > Hosts**. Когда откроется страница хостов, нажмите кнопку добавления нового хоста (**New Host**).



Когда откроется окно добавления нового хоста, введите следующую информацию:

- **Имя (Name):** Название хоста.
- **IP-адрес (IP address):** IPv6 адрес хоста

Остальные поля, такие как адрес Ethernet и информация про ОС, необязательны.

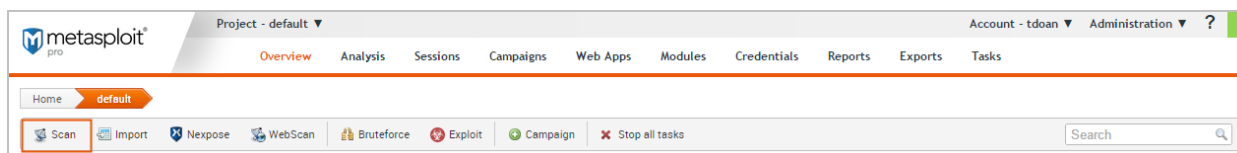
Запуск поискового сканирования

Поисковое сканирование запускает Nmap наряду с несколькими специализированными модулями для идентификации «живых» систем в сети и нахождения открытых портов и служб. Как минимум, вам нужно указать адреса систем, которые вы желаете просканировать. Также, есть дополнительные параметры, которые вы можете установить для точной настройки различных фаз сканирования. Например, вы можете обойти фазу сканирования портов и перейти сразу на определение версий, или вы можете сканировать каждый хост отдельно, чтобы ускорить импорт хостов в проект. Кроме того, дополнительные настройки позволяют вам выбирать порты, целевые службы, скорость сканирования и его режим.

Так как поисковое сканирование использует в основном Nmap, вы можете указать дополнительные параметры Nmap для настройки сканирования. Например, если вы хотите изменить технику сканирования, вы можете указать Nmap аргумент командной строки для использования того метода, который вы хотите, и сканирование будет опираться на эти настройки вместо стандартных. Для получения дополнительной информации о параметрах Nmap посетите страницу с [документацией по Nmap](#).

Чтобы запустить поисковое сканирование:

1. Из запущенного проекта, нажмите вкладку «Обзор (**Overview**)»
Возьмите на заметку: так же вы можете найти кнопку «Сканирование (**Scan**)» на странице анализа (Analysis).
2. Когда откроется окно обзора, нажмите на кнопку «Сканирование (**Scan**)».



3. Когда откроется окно нового поискового сканирования (New Discovery Scan), введите целевые адреса в поле «**Target addresses**».

Вы можете ввести один IP-адрес, диапазон адресов или запись CIDR. Если имеется несколько адресов или диапазонов, вводите каждую запись в новой строке.

- На этом этапе вы можете запустить сканирование. Однако, если вы хотите более тонко настроить сканирование, вы можете нажать кнопку «Дополнительные параметры (**Show Advanced Options**)», чтобы увидеть дополнительные параметры, которые вы можете установить для поискового сканирования. Например, вы можете указать IP-адреса, которые вы хотите включить либо исключить из сканирования.

Дополнительные сведения о доступных вариантах сканирования см. в разделе «параметры поискового сканирования».

- Когда вы будете готовы приступить к сканированию, нажмите кнопку «Запустить сканирование (**Launch Scan**)».

После запуска поискового сканирования, вы можете видеть журнал задач, показывающий статус прогресса и статус сканирования. Если сканирование завершается без ошибок, появится статус «завершен (complete)».

Просмотр результатов сканирования

Наиболее удобный способ просмотра данных, полученных при сканировании – это переход со страницы хостов. Для просмотра этой страницы перейдите по **Hosts > Analysis**. Каждый хост будет иметь один из следующих статусов: отсканирован, взломан, с оболочкой либо выгружен (scanned, cracked, shelled, или looted). Простой способ определить последние отсканированные хосты – это включить их сортировку по дате и статусу.

IP ADDRESS	HOSTNAME	OPERATING SYSTEM	VM	PURPOSE	SVCS	VLNS	ATT	TAGS	UPDATED	STATUS
10.20.36.1		Linux (Ubuntu) 2.6.X		server	1				15 minutes ago	Scanned
10.20.36.51	MS-W03-3U-1	Windows XP (XP)	vm	client	7				14 minutes ago	Scanned
10.20.36.52	MS-W03-6U-1	Windows 2003 (2003)	vm	server	8				14 minutes ago	Scanned
10.20.36.53	MS-W03R2-3U-1	Windows 2003 (2003 R2) SP1	vm	server	7				14 minutes ago	Scanned
10.20.36.54	MS-W03R2-6U-1	Windows PocketPC/CE (2003 R2) SP1	vm	device	7				14 minutes ago	Scanned
10.20.36.55	MS-W03S2-3U-1	Windows 2003 (2003 R2) SP2	vm	server	6				14 minutes ago	Scanned
10.20.36.56	MS-W082-3U-1	Windows 2008 (2008 Enterprise without Hyper-V) SP2	vm	server	12				14 minutes ago	Scanned

Данные, полученные при поисковом сканировании

Нетрудно обратить внимание, что для каждого просканированного или импортированного хоста отображается следующая информация, в случае её доступности:

- IP-адрес
- Имя хоста
- Операционная система
- Активные службы
- Время последнего обновления хоста
- Статус хоста

Расшифровка статусов хоста

Статус хоста описывает вам последнее событие, которое произошло с хостом. Существует иерархический порядок статусов хоста.

- Scanned - указывает на то, что были произведены поисковое сканирование, сканирование Nexpose или импорт.
- Shelled – указывает на то, что на хосте был открыт сеанс.
- Looted - указывает, что с хоста были получены данные.
- Cracked

Сканирование на уязвимости с помощью Nexpose

Сканирование и анализ уязвимостей - это процесс, который обнаруживает и оценивает существующие уязвимости в сетевой инфраструктуре. Уязвимость является характеристикой актива, который злоумышленник может использовать, чтобы получить несанкционированный доступ к конфиденциальным данным, ввести вредоносный код или произвести атаку отказа в обслуживании (denial of service). Чтобы предотвратить нарушения безопасности, очень важно выявлять и устранять недочёты в системе безопасности и уязвимости, из-за которых система может быть подвержена атаке.

Вы можете использовать Nexpose для проверки сети на наличие уязвимостей. Nexpose отмечает активные службы, открытые порты и запущенные приложения на каждом компьютере, и пытается найти уязвимости, которые могут существовать на основе атрибутов обнаруженных служб и приложений. Nexpose предоставляет результаты сканирования в виде отчета, который поможет вам

определить приоритеты уязвимостей на основе фактора риска и вывести наиболее эффективные решения для реализации решений по защите от них.

Nexpose интегрируется в Metasploit Pro как инструмент, оценивающий и проверяющий уязвимости, помогающий устранять ложные срабатывания, подтверждать уязвимости и находить решения по исправлению оных. Есть несколько способов для использования Metasploit Pro с Nexpose. Metasploit Pro обеспечивает путь, позволяющий вам добавить консоль Nexpose для запуска сканирования уязвимостей непосредственно из веб-интерфейса и далее автоматически импортировать результаты сканирования в проект. Вы также можете запускать сканирование прямо из Nexpose и импортировать отчеты сканирования в Metasploit Pro для анализа и подтверждения уязвимости. Вам необходимо лишь выбрать метод, больше всего вас устраивающий.

Терминология Nexpose

Некоторые термины в Nexpose отличаются от используемых в Metasploit. Вот те из них, которые вы должны запомнить:

- **Asset:** узел (хост) в сети.
- **Site:** Логическая группа хостов с выделенным механизмом сканирования. Она может работать в течение длительного периода времени и предоставлять вам историю и данные и аналогична проекту в Metasploit.
- **Scan Template:** Шаблон, определяющий уровень проверки, который Nexpose использует для сканирования уязвимостей. Дополнительные сведения о шаблонах сканирования см. в [руководстве пользователя Nexpose](#).

Скачивание и установка Nexpose

Вы можете загрузить общее издание Nexpose с [сайта Rapid7](#). Для получения дополнительной информации о том, как установить и настроить Nexpose, изучите это [руководство по установке](#).

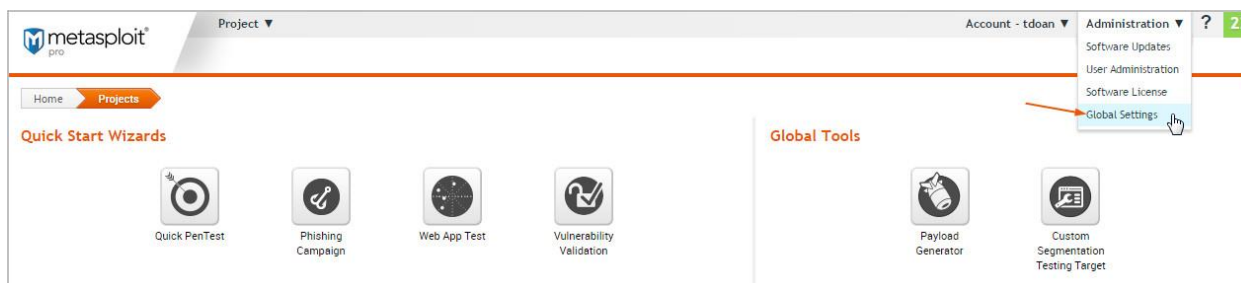
Если вы заинтересованы в приобретении Nexpose Enterprise, свяжитесь с [отделом продаж Rapid7](#).

Добавление консоли Nexpose

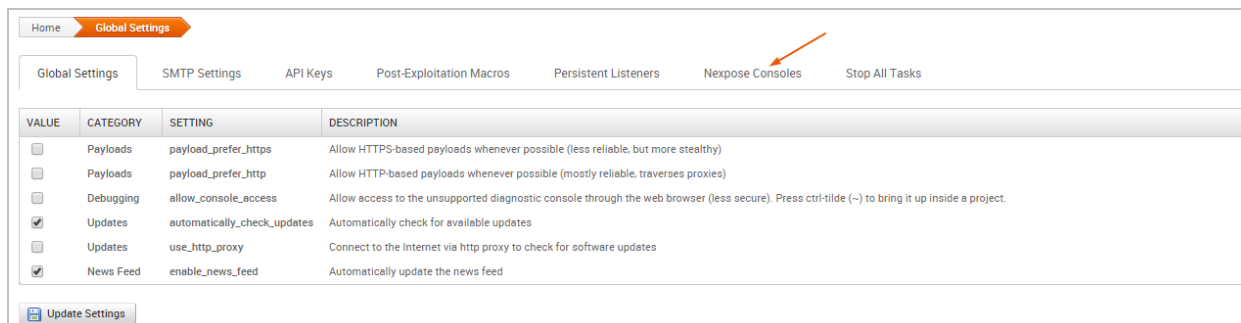
Прежде чем вы сможете запустить сканирование Nexpose из Metasploit Pro, вам необходимо добавить консоль Nexpose. Нужно будет знать адрес и порт, на которых запущен Nexpose, также вам понадобятся учетные данные для входа в консоль Nexpose.

Чтобы добавить консоль Nexpose

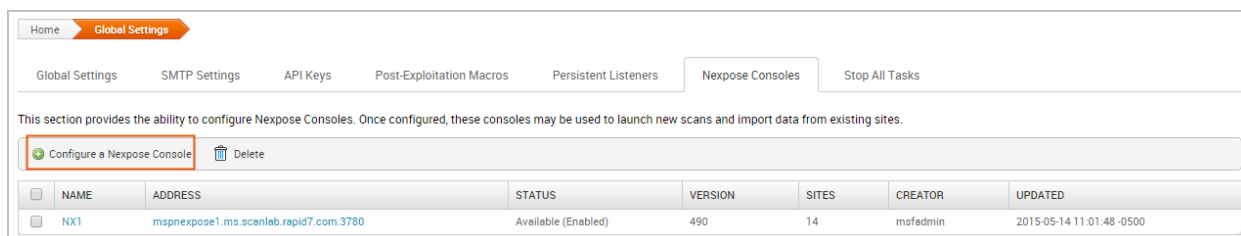
1. Перейдите по **Administration > Global Settings** из главного меню.



2. Щелкните по вкладке консолей Nexpose.



3. Нажмите на кнопку конфигурации консоли (**Configure a Nexpose Console**).



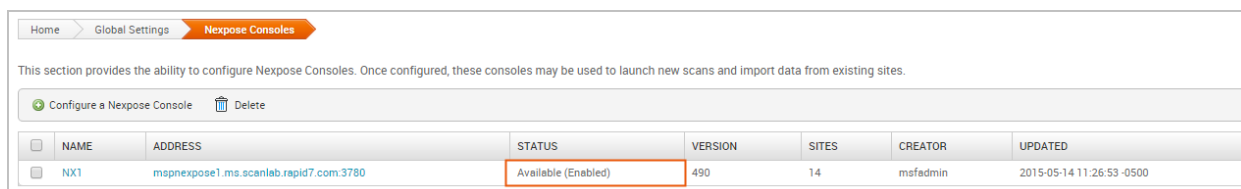
4. Когда откроется страница конфигурации консоли, введите следующие данные:

- Адрес консоли (Console Address): адрес сервера или IP для установки Nexpose.
- Порт консоли (Console Port): порт, на котором работает служба Nexpose. По умолчанию – 3780.
- Имя пользователя консоли (Console Username): имя пользователя, используемое для входа в консоль.
- Пароль консоли (Console Password): пароль, который используется для аутентификации в аккаунте.

5. Выберите параметр «**Enabled**» для инициализации и активации консоли.

6. Сохраните настройки.

Таблица Nexpose Consoles обновляется с консолью вместе. Если Metasploit Pro может успешно подключиться и аутентифицироваться в консоли Nexpose, появится статус «Available (Enabled)», как показано ниже:



В противном случае, если есть проблема с конфигурацией консоли, будет отображён статус «Error». Могут возникнуть следующие ошибки:

- «Error: Nexpose host is unreachable» означает, что Metasploit Pro не может получить доступ к консоли. Необходимо убедиться, что вы ввели правильный адрес и порт.
- «Error: Authentication required for API access», значит, что предоставленные вами учетные данные не верны. Необходимо убедиться, что вы ввели правильные учетные данные.

Запуск сканирования Nexpose

Чтобы иметь возможность определять приоритетность рисков безопасности, вы должны знать, какие устройства работают в среде и понять, как они уязвимы для атак. Вы можете запустить сканирование Nexpose, чтобы определить службы и приложения, работающие на хосте, и выявить потенциальные уязвимости, существующие на основе собранных данных. Чтобы узнать, как работает Nexpose, ознакомьтесь с [руководством пользователя Nexpose](#).

Все данные сканирования, полученные от Nexpose, хранятся в проекте Metasploit и могут быть просмотрены на странице анализа. Информация, собранная с каждого хоста, включает в себя IP-адрес, имя хоста, ОС, запущенные службы и возможные уязвимости. Metasploit Pro сопоставляет каждую уязвимость с соответствующим модулем, если она присутствует в базе данных модуля. Эти модули можно просмотреть на вкладке «Modules» в режиме просмотра отдельного хоста.

Чтобы настроить сканирование Nexpose:

1. Из открытого проекта, нажмите на вкладку «Overview» или «Analysis».
2. Нажмите на кнопку «Import», расположенную на панели быстрых задач.
3. Когда откроется страница импорта, нажмите на выпадающее меню «Choose a Nexpose console» и выберите консоль для запуска сканирования.

Список показывает консоли Nexpose, которые вы добавили в Metasploit Pro. Если таковых нет, вначале [добавьте консоль Nexpose](#).

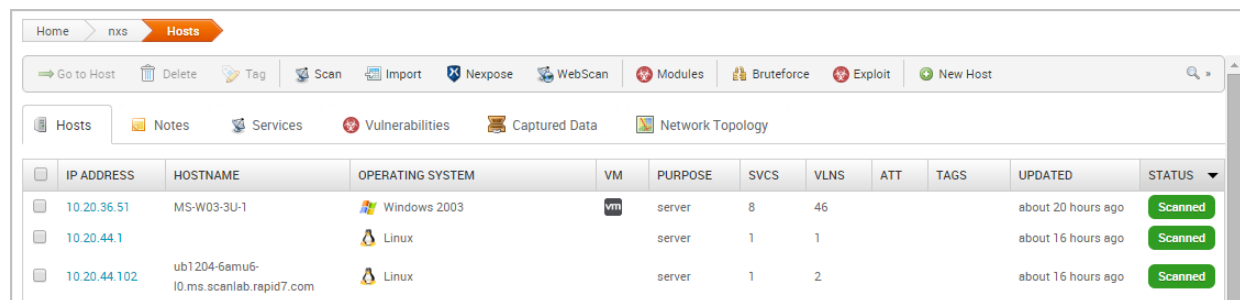
4. Введите адреса для сканирования в поле «**Scan targets**».
- Вы можете указать IP-адрес, IP-диапазон или запись CIDR. Каждый элемент должен быть записан на новой строке.

Вы можете использовать стандартную адресацию IPv6 для определения отдельных адресов IPv6. Например, используйте fe80::202:b3ff:fe1e:8329 для одиночных адресов и 2001:db8::/32 для записей CIDR. Для привязки локального адреса, необходимо добавить идентификатор интерфейса к адресу. К примеру, введите fe80::1% eth0 для привязки локального адреса.

Вы можете сканировать только то количество хостов, на которое у вас есть лицензия Nexpose. Если вы вводите больше хостов, чем позволяет ваша лицензия, произойдет сбой сканирования. Например, если у вас лицензия Community, максимальное количество доступных хостов - 32. Если же вы укажете более 32 хостов, произойдет сбой сканирования.

5. Нажмите на выпадающее меню «**Scan template**» и выберите шаблон. Для получения более подробной информации о шаблонах, изучите [руководство пользователя Nexpose](#).
6. Если вы не хотите, чтобы сканирование перезаписывало данные для существующих хостов, примените параметр «Don't change existing hosts».
7. Нажмите на кнопку «**Import data**», чтобы начать сканирование.

После завершения сканирования, перейдите на **Analysis > Hosts**, чтобы просмотреть результаты сканирования.



IP ADDRESS	HOSTNAME	OPERATING SYSTEM	VM	PURPOSE	SVCS	VLNS	ATT	TAGS	UPDATED	STATUS
10.20.36.51	MS-W03-3U-1	Windows 2003	vm	server	8	46			about 20 hours ago	Scanned
10.20.44.1		Linux		server	1	1			about 16 hours ago	Scanned
10.20.44.102	ub1204-6amu6- l0.ms.scanlab.rapid7.com	Linux		server	1	2			about 16 hours ago	Scanned

После запуска сканирования Nexpose из Metasploit Pro на консоли Nexpose временно создается группа хостов (Site). Синтаксис её именования - `METASPLOIT-<PROJECT NAME>-<ID>`. В Nexpose, перейдите на **Assets > Sites** для просмотра списка групп и поиска по названию проекта.



Name	Assets	Vulnerabilities	Risk	Type	Scan Status	Scan	Edit	Delete
Metasploit-nxs-1431623161	1	16	10,380	Static	Scan finished on Thu May 14 2015			
Metasploit-asasdasdf-20150507T154603	5	41	21,521	Static	Scan finished on Thu May 07 2015			

Импорт данных Nexpose

Если вы предпочитаете запускать сканирование непосредственно из консоли Nexpose, вы можете импортировать результаты сканирования и подтвердить их с помощью Metasploit Pro. Когда вы импортируете данные из Nexpose, Metasploit Pro автоматически индексирует данные уязвимости из Nexpose, используя идентификаторы служб и уязвимостей, чтобы сопоставить каждую уязвимость с подходящим эксплойтом. Подготовленные эксплойты помогают вам легко атаковать уязвимости и быстро отличать реальные риски от ложноположительных. Вы можете импортировать группу напрямую из консоли Nexpose или просто импортировать Nexpose Simple XML или XML-файл экспорта.

Импорт Nexpose Simple XML или XML-файл экспорта

1. В проекте кликните вкладку «**Overview**» или «**Analysis**».
2. Кликните кнопку «**Import**» в панели «Quick Tasks».
3. Когда появится страница «Импорт данных/Import Data», выберите «Импортировать из файла/Import from file».
4. Кликните на «**Choose file**», чтобы открыть окно загрузки файлов.
5. Когда откроется окно загрузки файлов, найдите расположение файла, который вы хотите импортировать. Выберите его и нажмите кнопку «Открыть/Open».

Metasploit Pro поддерживает следующие типы экспортированных файлов Nexpose: XML Export, XML Export 2.0 и Nexpose Simple XML Export.

6. Настройте дополнительные параметры (Необязательно):
 - **Исключенные адреса.** Введите хосты, которые вы хотите исключить из импорта. Вы можете ввести адрес одного хоста, интервал адресов (через дефис) или запись CIDR. Каждая новая запись должна быть отделена новой строкой.

- **Не менять существующие хосты.** Выберите эту опцию, если вы не хотите перезаписывать данные хостов, уже добавленных в проект.
 - **Автоматически отмечать.** Введите любые отметки, которые вы хотите применить к импортированным хостам. Вы можете выбрать опцию «Автоматически отмечать ОС/**Automatically tag by OS**». В этом случае все добавленные хосты будут отмечены как «os_windows», «os_linux» или «os_unknown» в зависимости от установленной на хосте операционной системы.
7. Кликните кнопку «**Импортировать Данные**».

Появится журнал задач, в котором будет отображено состояние импорта. Когда процесс будет завершен, журнал задач отображает статус «Completed». Чтобы просмотреть импортированные данные, выберите **Analysis > Hosts**, чтобы перейти на страницу хостов.

Импортирование существующих в Nexpose групп хостов

1. Откройте проект, в который нужно импортировать данные.
2. Во вкладке задач кликните кнопку «**Import**». Появится страница импорта.
3. Выберите опцию «Импортировать из Nexpose/**Import from Nexpose**».
4. Кликните «Выбрать консоль Nexpose/**Choose a Nexpose Console**» для вызова ниспадающего меню и выберите нужную вам консоль, из которой нужно импортировать данные.
5. Выберите опцию «Импортировать существующие данные/**Import existing data**».
6. Выберите группу или группы, которые вы хотите импортировать в таблице сайтов.
7. Выберите опцию «Не изменять существующие хосты/**Do not change existing hosts**», если вы не хотите, чтобы уже импортированные хосты были модифицированы.
8. Кликните кнопку «**Import Data**», чтобы начать процесс импорта.

Появится журнал задач, в котором будет отображено состояние импорта. Когда процесс будет завершен, журнал задач отображает статус «Completed». Чтобы просмотреть импортированные данные, выберите **Analysis > Hosts**, чтобы перейти на страницу хостов.

Импорт данных

Вы можете импортировать данные, чтобы загрузить результаты сканирования или добавить данные из других проектов Metasploit. Функция импорта будет полезной, если в наличии есть уязвимости, нуждающиеся в проверке, или данные, которые нужно использовать в нескольких проектах.

Импортирование данных из сканеров уязвимостей

Metasploit позволяет вам импортировать отчеты сканирования широко используемых сканеров уязвимости (Nessus, Core Impact и Qualys). Когда вы импортируете отчет сканирования, данные хостов (например, перечень операционных систем, сервисов и обнаруженных уязвимостей) также импортируются в проект.

Чтобы импортировать отчеты сканирования других сканеров уязвимостей:

1. В проекте кликните вкладку «Обзор/**Overview**».
2. Найдите и кликните кнопку «**Import**».
3. Когда появится страница «**Import Data**».
4. Кликните кнопку «Выбрать файл», выберите «**Import**» в появившейся радиальной кнопке.
5. Когда откроется окно загрузки файлов, найдите расположение файла, который вы хотите импортировать. Выберите его и нажмите кнопку «Открыть/**Open**».
6. Настройте дополнительные параметры (Необязательно):
 - **Исключенные адреса.** Введите хосты, которые вы хотите исключить из импорта. Вы можете ввести адрес одного хоста, интервал адресов (через дефис) или запись CIDR. Каждая новая запись должна быть отделена новой строкой.
 - **Не менять существующие хосты.** Выберите эту опцию, если вы не хотите перезаписывать данные хостов, уже добавленных в проект.
 - **Автоматически отмечать.** Введите любые отметки, которые вы хотите применить к импортированным хостам. Вы можете выбрать опцию «Автоматически отмечать ОС/**Automatically tag by OS**». В этом случае все добавленные хосты будут отмечены как «os_windows», «os_linux» или «os_unknown» в зависимости от установленной на хосте операционной системы.
7. Кликните кнопку «**Import data**», чтобы начать процесс импорта.
 Появится журнал задач, в котором будет отображено состояние импорта. Когда процесс будет завершен, журнал задач отображает статус «Completed». Чтобы просмотреть импортированные данные, выберите **Analysis > Hosts**, чтобы перейти на страницу хостов.

Поддерживаемые отчеты сканирования

Metasploit поддерживает большинство сканеров уязвимостей на рынке, включая собственную разработку Rapid7 — Nexpose, а также другие инструменты типа Qualys и Core Impact. Поддерживаются следующие отчеты сканирования:

- Foundstone Network Inventory XML
- Microsoft MBSA SecScan XML
- nCircle IP360 XMLv3 and ASPL
- NetSparker XML
- Nessus NBE
- Nessus XML v1 and v2
- Qualys Asset XML
- Qualys Scan XML
- Burp Session XML
- Acunetix XML
- AppScan XML
- Nmap XML
- Retina XML
- Amap Log
- Critical Watch VM XML
- IP Address List
- Libpcap Network Capture
- Spiceworks Inventory Summary CSV
- Core Impact XML

! Metasploit Pro не поддерживает импорт сервисов и информацию о портах от Qualys. Если вы импортируете файл ресурсов Qualys, то нужно будет провести дополнительное сканирование для обнаружения сервисов и портов, активных на импортированных хостах.

Импорт данных Nexpose

Если вы предпочитаете проводить сканирования напрямую из консоли Nexpose, вы можете импортировать результаты сканирования и проверить их при помощи Metasploit Pro. Когда вы импортируете данные из Nexpose, Metasploit Pro автоматически индексирует все уязвимости из Nexpose с учетом сервисов и привязки к каждой уязвимости подходящего для тестирования эксплойта. Отмеченные эксплойты помогут быстро начать атаковать уязвимости и оперативно определит, представляет ли уязвимость опасность или носит ложноположительный характер.

Импорт Nexpose Simple XML или XML-файл экспорта

1. В проекте кликните вкладку «**Overview**» или «**Analysis**».
2. Кликните кнопку «**Import**» в панели «Quick Tasks».
3. Когда появится страница «Импорт данных/Import Data», выберите «Импортировать из файла/**Import from file**».
4. Кликните на «**Choose file**», чтобы открыть окно загрузки файлов.
5. Когда откроется окно загрузки файлов, найдите расположение файла, который вы хотите импортировать. Выберите его и нажмите кнопку «Открыть/**Open**».

Metasploit Pro поддерживает следующие типы экспортированных файлов Nexpose: XML Export, XML Export 2.0 и Nexpose Simple XML Export.

6. Настройте дополнительные параметры (Необязательно):
 - **Исключенные адреса.** Введите хосты, которые вы хотите исключить из импорта. Вы можете ввести адрес одного хоста, интервал адресов (через дефис) или запись CIDR. Каждая новая запись должна быть отделена новой строкой.
 - **Не менять существующие хосты.** Выберите эту опцию, если вы не хотите перезаписывать данные хостов, уже добавленных в проект.
 - **Автоматически отмечать.** Введите любые отметки, которые вы хотите применить к импортированным хостам. Вы можете выбрать опцию «Автоматически отмечать ОС/Automatically tag by OS». В этом случае все добавленные хосты будут отмечены как «os_windows», «os_linux» или «os_unknown» в зависимости от установленной на хосте операционной системы.
 7. Кликните кнопку «**Импортировать Данные**».
- Появится журнал задач, в котором будет отображено состояние импорта. Когда процесс будет завершен, журнал задач отображает статус «Completed». Чтобы просмотреть импортированные данные, выберите **Analysis > Hosts**, чтобы перейти на страницу хостов.

Импорт существующих в Nexpose сайтов

1. Откройте проект, в который нужно импортировать данные.
2. Во вкладке задач кликните кнопку «**Import**». Появится страница импорта.

3. Выберите опцию «Импортировать из Nexpose/**Import from Nexpose**».
4. Кликните «Выбрать консоль Nexpose/**Choose a Nexpose Console**» для вызова ниспадающего меню и выберите нужную вам консоль, из которой нужно импортировать данные.
5. Выберите опцию «Импортировать существующие данные/**Import existing data**».
6. Выберите сайт или сайты, которые вы хотите импортировать в таблице сайтов.
7. Выберите опцию «Не изменять существующие хосты/**Do not change existing hosts**», если вы не хотите, чтобы уже импортированные хосты были модифицированы.
8. Кликните кнопку «**Import Data**», чтобы начать процесс импорта.

Появится журнал задач, в котором будет отображено состояние импорта. Когда процесс будет завершен, журнал задач отображает статус «Completed». Чтобы просмотреть импортированные данные, выберите **Analysis > Hosts**, чтобы перейти на страницу хостов.

Проверка уязвимостей

После сканирования целей и идентификации потенциальных уязвимостей следующим шагом становится определение того, какой риск они представляют. Чтобы подтвердить уязвимость, у вас есть несколько вариантов:

- **Помощник проверки уязвимостей/The Vulnerability Validation Wizard.** Помощник оснащен удобным интерфейсом «все в одном», который проведет вас через все этапы импортирования и создания атак на уязвимости, обнаруженные Nexpose. Это позволяет вам быстро определить насколько серьезно их могут атаковать подобранные эксплойты и передать эту информацию обратно в Nexpose. Эта функция очень полезна, если вы используете Nexpose для поиска и управления уязвимостями.
- **Ручное подтверждение.** Этот метод заставит вас немного поработать. У вас будет больше контроля над целевыми уязвимостями. Обычно этот способ используется для тех случаев, когда вы хотите сами подтвердить уязвимость или же проверяете уязвимости, найденные сторонними сканерами уязвимостей (Qualys или Nessus).

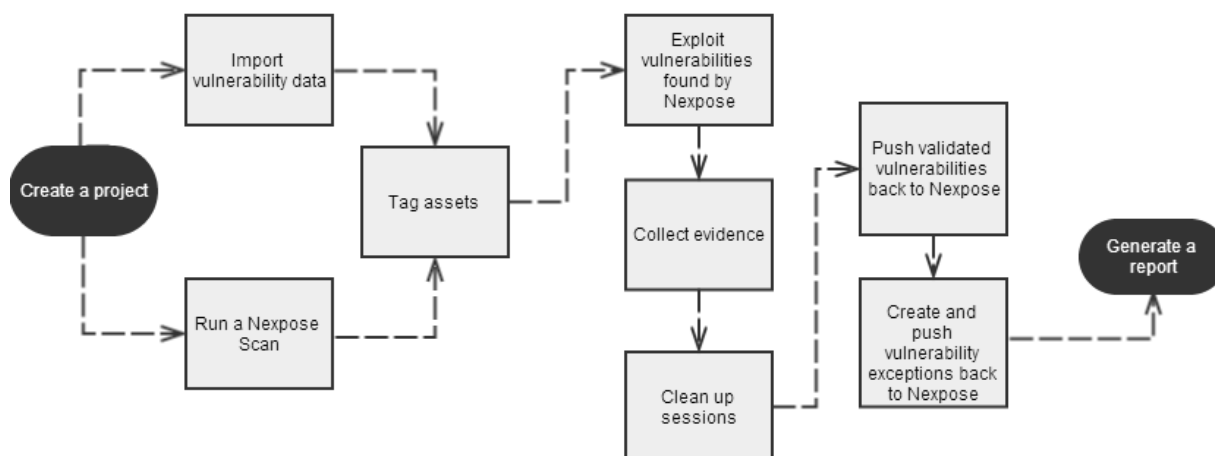
Когда производится ручное подтверждение, нужно провести стандартный тест на проникновение, как в любой другой ситуации. Тест включает в себя создание проекта и добавление данных уязвимости посредством сканирования или импорта. Затем нужно попытаться атаковать уязвимость, чтобы определить, насколько они опасны. Если уязвимости были обнаружены при помощи Nexpose, вы сможете отправить результаты обратно.

Подтверждение уязвимостей Помощником проверки уязвимостей

Помощник проверки уязвимостей упрощает и максимально ускоряет процесс проверки уязвимостей для пользователей Nexpose. Помощник обеспечивает пользователя удобным интерфейсом и ведет вас от одного шага к другому, от импортирования данных Nexpose до автоматической проверки на устойчивость к подобранным эксплойтам и отправки данных обратно. Вы можете также создать отчет с детализированными результатами тестирования и создать исключения для уязвимостей, которые не были успешно атакованы.

Последовательность работы с Помощником проверки уязвимостей

Чтобы понять, как настроить помощника, прочитайте последовательность его работы:



Перед использованием Помощника

До начала использования Помощника убедитесь в том, что у вас настроен доступ к вашей версии Nexpose. Вы можете проверять уязвимости, если у вас установлена версии Nexpose Enterprise или Nexpose Consultant 5.7.16 или выше. Пожалуйста, проверьте тип вашей консоли Nexpose перед началом работы с помощником.

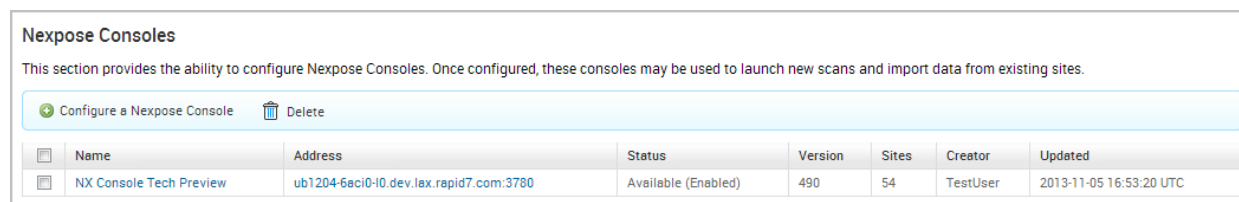
У вас должен быть хотя бы один сайт работающий под Nexpose. О том, как настроить сайт, читайте в [руководстве по установке и началу работы с Nexpose](#).

Добавление консоли Nexpose

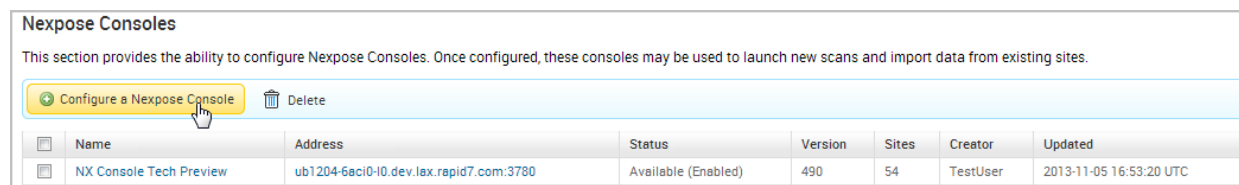
Вы можете добавить консоль Nexpose в глобальных настройках или же при запуске помощника проверки уязвимостей. Если вы хотите добавить консоль в глобальных настройках, следуйте инструкции ниже.

Чтобы добавить консоль Nexpose:

1. Выберите **Administrator > Global Settings** в меню администратора.
2. Найдите раздел «Консоли Nexpose».



3. Кликните на кнопку «Сконфигурировать консоль Nexpose/Configure a Nexpose Console».



4. После появления следующей страницы, введите следующую информацию:

- **Адрес консоли** – IP-адрес сервера, на котором работает Nexpose. Вы можете также ввести точное имя сервера.
- **Порт консоли** – порт, обеспечивающий работу сервиса консоли. По умолчанию – 3780.
- **Имя пользователя консоли** – имя пользователя Nexpose.
- **Пароль для консоли** – пароль пользователя Nexpose, используемый для аутентификации.

Configure a Nexpose Console

Console Name

Console Address

Console Port

Console Username

Console Password

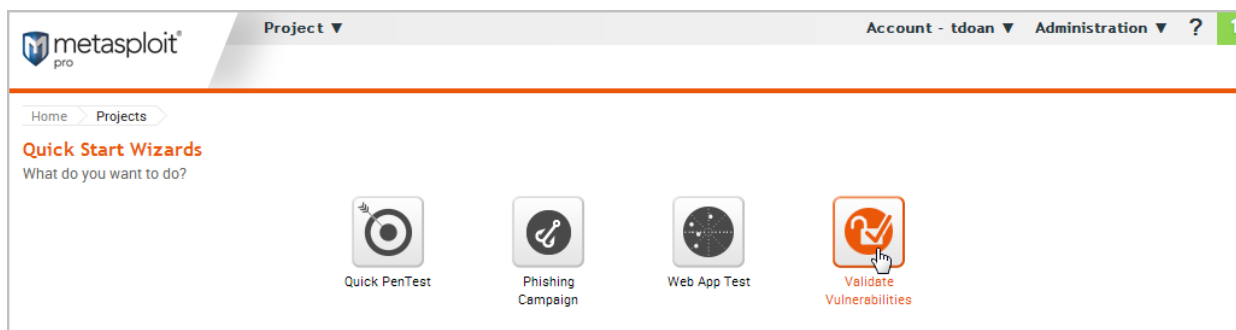
Enabled
☒

 Save

5. Сохраните консоль Nexpose.

Настройка и запуск Помощника проверки уязвимостей

1. На странице Проектов кликните на виджет проверки уязвимостей под разделом «Quick Start Wizards». Откроется окно помощника и отобразит страницу «**Create Project**».



2. В поле «**Название проекта**» введите имя проекта. Название может содержать любые комбинации цифр и букв алфавита, специальные символы и пробелы. Вы также можете заполнить необязательное поле с описанием для проекта, где обычно описывается общий план тестирования и его задачи.

Vulnerability Validation

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose.

Create Project

Pull from Nexpose

Tag

Exploit

☒ Generate Report

Project Name*

demo

Description

Imports assets from demo site and exploits vulnerabilities.

Advanced ▾

Vulnerability Validation

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose.

Create Project

Pull from Nexpose

Tag

Exploit

☒ Generate Report

Project Name*

demo

Description

Imports assets from demo site and exploits vulnerabilities.

Advanced ▾

3. Кликните на вкладку «Pull from Nexpose». Появится страница консолей Nexpose.

Vulnerability Validation

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose.

Create Project

Pull from Nexpose

Tag

Exploit

☒ Generate Report

Nexpose Console

Choose a Nexpose Console... ▾

[+ Configure a Nexpose Console](#)

☒ Import existing Nexpose vulnerability data
 ☐ Start a Nexpose scan to get data

Select or configure a Nexpose Console.

Cancel

Start

Vulnerability Validation

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose.

Create Project

Nexpose Console Choose a Nexpose Console... + Configure a Nexpose Console

Pull from Nexpose

Tag

Exploit

☒ Generate Report

☒ Import existing Nexpose vulnerability data

☐ Start a Nexpose scan to get data

Select or configure a Nexpose Console.

Cancel Start

4. Кликните на ниспадающее меню **Nexpose console** и выберите консоль, из которой хотите получить данные. Если нет доступных консолей, вы можете кликнуть на активную ссылку «**Configure an Nexpose Console**» для ее добавления.

Vulnerability Validation

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose.

Create Project

Nexpose Console 10.6.201.160 [+ Configure a Nexpose Console](#)

Pull from Nexpose

Tag

Exploit

☒ Generate Report

☐ Import existing Nexpose vulnerability data
☒ Start a Nexpose scan to get data

Scan targets*

Excluded Addresses*

Scan template* Denial of service ?

Cancel Start

5. После выбора консоли вы можете выбрать, следует ли запускать сканирование Nexpose или же импортировать уже существующие данные. В зависимости от выбранного варианта, помощник покажет вам соответствующую страницу конфигурации.
6. Опция «**Start a Nexpose Scan to get data**».
7. Введите адреса хостов или отмеченные ресурсы, которые вы хотите просканировать, в поле «Цели сканирования/**Scan targets**». Вы можете ввести один IP-адрес или же список адресов через запятую. Интервал IP-адресов можно оформить при помощи дефиса. Можно использовать стандартные записи CIDR.

Vulnerability Validation ✕

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose.

Create Project

Pull from Nexpose

Tag

Exploit

☒ Generate Report

Nexpose Console 10.6.201.160 + Configure a Nexpose Console

☐ Import existing Nexpose vulnerability data

☒ Start a Nexpose scan to get data

Scan targets* 10.6.201.148

Excluded Addresses*

Scan template* Penetration test ?

Cancel Start

8. Кликните на «Шаблон сканирования/**Scan template**» для вызова ниспадающего меню и выберите необходимый вам шаблон.

Внимание: шаблон сканирования — это предустановленный набор настроек сканирования. Есть несколько вариантов по умолчанию, из которых вы можете выбрать любой. Для получения дополнительной информации о шаблонах сканирования читайте [пользовательский мануал для Nexpose](#).

9. Кликните вкладку «**Tag**».

Внимание: если вы не хотите использовать отметки, перейдите к шагу №13.

10. Выберите «Автоматически отмечать ОС/**Automatically tag by OS**», если вы хотите отметить каждый хост наименованием его операционной системы.

Внимание: если эта опция включена, хосты будут отмечены как `os_linux` или `os_windows`.

Vulnerability Validation ✕

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose.

Create Project

Pull from Nexpose

Tag

Exploit

☒ Generate Report

☒ Automatically Tag by OS ?

☐ Use Custom Tag ?

11. Выберите «Использовать пользовательские настройки для создания отметок/**Use custom tag**», если вы хотите отметить каждый хост каким-то определенным образом. Когда включена эта опция, помощник по проверке уязвимостей/Vulnerability Validation Wizard отобразит поля и опции, которые вы можете использовать для создания пользовательских отметок.

Vulnerability Validation ✕

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose.

Create Project

Pull from Nexpose

Tag

Exploit

☒ Generate Report

☒ Automatically Tag by OS ?

☒ Use Custom Tag ?

Name*

Description

☐ Include in report summary?

☐ Include in report details?

☐ Critical Finding?

12. После того, как вы настроили порядок создания отметок, кликните на вкладку эксплойтов. Появится страница «Auto-Exploitation».

Vulnerability Validation

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose.

Create Project
Pull from Nexpose
Tag
Exploit
☒ Generate Report

Minimum Reliability
Great
?

Dry Run
☐ Only show exploit information, but do not run

Evidence
☐ Collect evidence

Sessions
☒ Clean up sessions when done

Excluded Addresses

Payload Type
Meterpreter
?

Connection Type
Auto
?

Listener Ports
1024-65535

Listener Host

Auto Launch Macro
?

Concurrent Exploits
5

Timeout in Minutes
5
?

Transport Evasion
None
?

Application Evasion
None
?

Included Ports
1-65535

Excluded Ports

Cancel
Start

13. Кликните «**Minimum Reliability**» для вызова ниспадающего меню и выберите ранжирование модулей, которое вы хотите использовать. Выберите либо Great, либо Excellent.
14. Кликните на вкладку «**Generate Report**», если вы хотите включить автоматически создаваемые отчеты в тестирование уязвимостей. Если вы не хотите включать в него отчет, снимите соответствующую галочку и пропустите последние шаги.

Vulnerability Validation

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose.

Create Project

Pull from Nexpose

Tag

Exploit

☒ Generate Report

Report is **enabled**

☒ PDF ☐ Word ☐ RTF ☐ HTML

Report name Type

Sections

☒ Project Summary ☒ Vulnerabilities and Exploits ☒ Include charts and graphs

☒ Executive Summary

☒ Compromised Summary ☒ Compromised Hosts

Excluded Addresses

☐ Email Report ?

Email addresses...

Cancel

Start

15. Введите название отчета в поле «Название отчета/**Report name**», если вы хотите использовать определенное имя. В другом случае, помощник будет использовать автоматически сгенерированные названия отчетов.

Vulnerability Validation

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose.

Create Project

Pull from Nexpose

Tag

Exploit

☒ Generate Report

Report is **enabled**

☒ PDF ☐ Word ☐ RTF ☐ HTML

Report name Type

Sections

☒ Project Summary ☒ Vulnerabilities and Exploits ☒ Include charts and graphs

☒ Executive Summary

☒ Compromised Summary

☒ Compromised Hosts

Excluded Addresses

☐ Email Report ?

Email addresses...

Cancel

Start

16. Выберите в каком формате будут созданы отчеты (PDF, RTF или HTML). Предпочтительный формат по умолчанию – PDF.

Vulnerability Validation

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose.

Create Project
Pull from Nexpose
Tag
Exploit
☒ Generate Report

Report is **enabled**

Report name Type

☒ PDF
☐ Word
☐ RTF
☐ HTML

☒ Project Summary
☒ Executive Summary
☒ Compromised Summary
☒ Compromised Hosts

☒ Vulnerabilities and Exploits
☒ Include charts and graphs

Excluded Addresses

☐ Email Report

Email addresses...

Cancel
Start

- Кликните на «**Type**» для вызова ниспадающего меню и выберите тип отчета, который нужно создать. Вы можете выбрать отчет по аудиту или отчет по успешно атакованным и уязвимым хостам.
- В разделе «Секции/Sections» снимите галочки с тех секций, которые вы не хотите включать в отчет. Пропустите этот шаг, если вы хотите включить в отчет все типы данных.

Vulnerability Validation

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose.

Create Project

Pull from Nexpose

Tag

Exploit

☒ Generate Report

Report is **enabled**

Report name Type

Sections

☒ Project Summary
 ☒ Vulnerabilities and Exploits

☒ Executive Summary
 ☒ Compromised Summary
 ☒ Compromised Hosts

Options

☒ Include charts and graphs

Excluded Addresses

☐ Email Report ?

Email addresses...

Cancel

Start

19. Введите хосты или ресурсы, информацию о которых вы не хотите включать в отчет, в поле «Исключенные адреса/**Excluded Addresses**». Вы можете ввести 1 IP-адрес, список IP-адресов через запятую или интервал адресов, оформленный через дефис, а также стандартные записи CIDR.

Vulnerability Validation

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose.

Create Project
Pull from Nexpose
Tag
Exploit
☒ Generate Report

Report is **enabled**

Report name: VulnerabilityValidation_138426 Type: Compromised and Vulnerable Hosts

☒ PDF
☐ Word
☐ RTF
☐ HTML

Sections

☒ Project Summary
☒ Executive Summary
☒ Compromised Summary
☒ Compromised Hosts

☒ Vulnerabilities and Exploits

Options

☒ Include charts and graphs

Excluded Addresses

☐ Email Report

Email addresses...

Cancel
Start

20. Выберите «Отправить отчет по почте/**Email Report**», если вы хотите отправить отчет по электронной почте. Если эта опция включена, нужно добавить адреса получателей. Если их несколько, то адреса следует разделить запятой.

Внимание: Если вы хотите отправить отчет по почте, то нужно настроить локальный почтовый сервис или сервис для использования вместе с Metasploit Pro. Чтобы задать настройки почтового сервера, выберите **Administration > Global Settings > SMTP Settings**.

21. Кликните на кнопку **«Запуск»**. Появится окно результатов, где будет показана статистика тестирования.

Отправка результатов в Nexpose

После проведения проверки уязвимостей вы будете готовы отправить данные в Nexpose. Процесс передачи результатов проверки уязвимостей в Nexpose называется «Толканием/Pushing». Когда вы «пушите» результаты в Nexpose, Metasploit Pro отмечает подтвержденные уязвимости как успешно атакованные и добавляет все неуспешно атакованные уязвимости в страницы «Исключения/Vulnerability Exceptions» и «Policy Override». Это значительно упрощает отслеживание и выставление приоритетов для уязвимостей, которые были протестированы.

Есть несколько способов отправки данных в Nexpose:

- С помощью помощника проверки уязвимостей. Если вы пользуетесь помощником, у вас будет возможность «протолкнуть» уязвимости и исключения напрямую из страницы результатов.
- С помощью «толчка вручную». Если вы хотите самостоятельно отправить данные в Nexpose, вы сможете отправить уязвимости и исключения со стартовой страницы уязвимостей или же отдельных страниц уязвимостей.

Правила проверки

Есть два типа результатов, которые можно отправлять в Nexpose: подтвержденные уязвимости и исключения.

Подтвержденные уязвимости

Подтвержденные уязвимости/Validated Vulnerabilities – это уязвимости, которые Metasploit Pro сумел успешно атаковать для открытия сессии на целевом хосте. Подтвержденная уязвимость будет отмечена соответствующей иконкой на странице со списком уязвимостей для конкретного ресурса так, как это показано на изображении.

Title	CVSS	Risk	Published On	Severity	Instances	Exceptions
MS11-050: Cumulative Security Update for Internet Explorer (2530548)	9.3	697	Thu Jun 16 2011	Critical	1	Exclude
MS12-063: Cumulative Security Update for Internet Explorer (2744842)	9.3	562	Tue Sep 18 2012	Critical	1	Exclude
MS13-069: Cumulative Security Update for Internet Explorer (2870699)	9.3	300	Tue Sep 10 2013	Critical	1	Exclude
MS13-059: Cumulative Security Update for Internet Explorer (2862772)	9.3	311	Tue Aug 13 2013	Critical	1	Exclude
MS13-055: Cumulative Security Update for Internet Explorer (2846071)	9.3	327	Tue Jul 09 2013	Critical	1	Exclude

Это просто дает вам знать, что уязвимость была протестирована и успешно атакована при помощи Metasploit Pro.

Исключенные уязвимости

Исключения – это уязвимости, найденные Nexpose, которые Metasploit Pro не сумел успешно атаковать. Такие уязвимости получают статус «Not Exploited», означающий, что Metasploit Pro не смог открыть сессию на целевом хосте из-за компенсации контроля и обратного портирования. В целом, исключенные уязвимости представляют собой уязвимости с низким риском поражения или вообще используются специально для нейтрализации более серьезных угроз. Исключения полезны потому, что они позволяют вам исключить определенные уязвимости из отчета, чтобы манипулировать оценкой риска.

Вот несколько причин, по которым вы можете захотеть создать список исключений:

- Уязвимость используется для компенсации контроля или для уменьшения дополнительных рисков.
- Уязвимость существует по причине допущения ее использования или определенного функционала (например, анонимный доступ к FTP ресурсам).
- Уязвимость связана с приемлемыми рисками и может потребовать больше ресурсов для интеграции оптимального решения. Такие уязвимости обычно представляют наименьший риск.
- Уязвимость носит ложноположительный характер.

[Доступ к странице исключений](#)

Передача исключений в Nexpose осуществляется на странице исключений. Как уже было замечено, есть несколько разделов в приложении, где вы можете создавать и «толкать» исключения: страница

результатов помощника проверки уязвимостей, страница со списком уязвимостей и страницы отдельно взятых уязвимостей.

! Чтобы получить доступ к странице исключений со страницы уязвимостей или страницы отдельных уязвимостей, вам нужно настроить консоль Nexpose таким образом, чтобы у Metasploit был к ней доступ. Если Metasploit Pro не обнаружит консоль Nexpose, он не отобразит опции для Push'a.

Доступ к странице исключений из списка уязвимостей

Чтобы получить доступ к странице исключений из списка, выберите **Analysis > Vulnerabilities**. Когда появится список уязвимостей, вы увидите кнопку «**Push Exploited Vulnerabilities**» и «**Create Exceptions**». Кликните на «**Create Exception**», чтобы открыть страницу исключений.

The screenshot shows the 'Vulnerabilities' tab in the Nexpose interface. It displays a table with columns: HOST, SERVICE, NAME, NEXPOSE TEST STATUS, and REFERENCES. The table lists various vulnerabilities, including MS08-067, CVE-2008-4250, and others. The 'NEXPOSE TEST STATUS' column shows 'Exploited', 'Not Tested', and 'Exploited'.

HOST	SERVICE	NAME	NEXPOSE TEST STATUS	REFERENCES
MS-WXP2-3U-1		MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (4 Total)
metasploitable.localdomain		Tomcat Application Manager Tomcat Tomcat Password Vulnerability	Not Tested	CVE-2009-3843 (4 Total)
webtarget1.ms.scanlab.rapid7.com		Tomcat Application Manager Tomcat Tomcat Password Vulnerability	Not Tested	CVE-2009-3843 (4 Total)
metasploitable.localdomain		HTTP TRACE Method Enabled	Not Exploited	CVE-2005-3398 (2 Total)
MS-WXP2-3U-1		MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)	Not Tested	CVE-2012-0002 (2 Total)
metasploitable.localdomain		'rsh' Remote Shell Service Enabled	Not Tested	CVE-1999-0651
webtarget1.ms.scanlab.rapid7.com		HTTP TRACE Method Enabled	Not Tested	CVE-2005-3398 (2 Total)
metasploitable.localdomain		Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368)	Not Tested	CVE-2011-3368
webtarget1.ms.scanlab.rapid7.com		TLS/SSL Server Supports SSL version 3	Not Tested	CVE-2014-3566
MS-WXP2-3U-1		MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Not Tested	CVE-2008-4114 (3 Total)
MS-WXP2-3U-1		MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Not Tested	CVE-2010-2550 (2 Total)

Страница исключений показана на изображении ниже. На этой странице вы сможете установить даты истечения и причины для каждой исключенной уязвимости в проекте. Вы также можете обойти необходимость проверять их в Nexpose, подтверждая их автоматически.

The screenshot shows the 'Create Nexpose Exceptions' page. It includes a section for 'Vulnerability Exceptions' with a table of exceptions. The table has columns for Host, Reason, Comment, Expire, and Result Code. The 'Reason' column shows 'False Positive' for all entries.

Host	Reason	Comment	Expire	Result Code
10.20.36.75	False Positive			no-access
10.20.36.75	False Positive			payload-failed
10.20.36.74	False Positive			no-target
10.20.36.74	False Positive			no-access
10.20.36.72	False Positive			no-access
10.20.36.51	False Positive			no-target
10.20.36.51	False Positive			no-access

Получение доступа к странице исключений с отдельной страницы уязвимости

Выберите **Analysis > Vulnerabilities**. Когда появится список уязвимостей, кликните на название уязвимости, чтобы открыть ее страницу. На этой странице вы можете настроить причину исключения и дату его истечения.

HOST	SERVICE	NAME	NEXPOSE TEST STATUS	REFERENCES
MS-WXP2-3U-1		MS09-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (4 Total)
metasploitable.localdomain		Tomcat Application Manager Tomcat Tomcat Password Vulnerability	Not Tested	CVE-2009-3843 (4 Total)
webtarget1.ms.scanlab.rapid7.com		Tomcat Application Manager Tomcat Tomcat Password Vulnerability	Not Tested	CVE-2009-3843 (4 Total)
metasploitable.localdomain		HTTP TRACE Method Enabled	Not Exploited	CVE-2005-3398 (2 Total)
MS-WXP2-3U-1		MS12-028: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)	Not Tested	CVE-2012-0002 (2 Total)
metasploitable.localdomain		'rsh' Remote Shell Service Enabled	Not Tested	CVE-1999-0651
webtarget1.ms.scanlab.rapid7.com		HTTP TRACE Method Enabled	Not Tested	CVE-2005-3398 (2 Total)
metasploitable.localdomain		Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368)	Not Tested	CVE-2011-3368
webtarget1.ms.scanlab.rapid7.com		TLS/SSL Server Supports SSL version 3	Not Tested	CVE-2014-3566
MS-WXP2-3U-1		MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Not Tested	CVE-2008-4114 (3 Total)
MS-WXP2-3U-1		MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Not Tested	CVE-2010-2550 (2 Total)

! Помните, вы можете создавать исключений только для уязвимостей со статусом «Not Exploited».

Разбираемся в статусах

Все уязвимости, импортированные в Nexpose, имеют статус. Он помогает вам легко идентифицировать были ли уязвимости протестированы и найти результаты теста. Статус зависит от типа уязвимости, а также от того, где вы просматриваете уязвимость, в списке или на отдельной странице.

Статусы в списке уязвимостей

В списке статусы показывают, были уязвимости протестированы или нет. Эти статусы можно увидеть в столбце **«Nexpose Test Status»**.

- Не протестирован/Not Tested – соответствующий эксплойт с рейтингом «Great» или выше не был найден для этой уязвимости, и Помощник проверки уязвимостей не смог провести авто-проверку Auto-exploitation. Вы можете запустить вручную модули с низким рейтингом или вспомогательные модули для проведения специального теста.

Чтобы найти подходящие по параметрам модули проверки для отдельно взятых уязвимостей, зайдите на страницу уязвимости и просмотрите информацию во вкладке **«Related Modules»**.

- Попытка эксплойта совершена/Exploit Attempted – соответствующий эксплойт с рейтингом «Great» или выше был найден для этой уязвимости, но попытка его использования была неудачной. Уязвимость с этим статусом вернет результат **«Failed»** после запуска модуля.

Для любой уязвимости, для которой была осуществлена попытка использования эксплойта, вы можете выбрать специальную метку **«Not Exploitable»**. Эта уязвимость не будет отправлена в Nexpose как исключение.

- Успешно атакована/Exploited – соответствующий эксплойт с рейтингом «Great» или выше был найден для данной уязвимости. Эксплойт был использован успешно. Была открыта сессия на целевом хосте.

Статусы на странице уязвимости

Эти статусы показывают результат запуска модуля.

- Неудача/Failed – модуль не смог открыть сессию на целевом хосте.
- Успешно атакована/Exploited – модуль успешно открыл сессию на целевом хосте.
- Не поддается атакам/Not Exploitable – модуль не смог открыть сессию, и вы вручную установили данный статус для уязвимости.
- Нет статуса/No Status Available – уязвимость не была протестирована из-за отсутствия подходящих эксплойтов.

Разбираемся с кодами результатов

Код результата – это примечание, описывающее причину неудачного использования эксплойта. Если вы видите статус «**Failed**», вы можете навести на статус курсор, чтобы увидеть код для определения проблемы. Следующие коды могут быть отображены:

- Нет кода/None – Metasploit не смог определить результат запуска модуля.
- Неизвестно/Unknown – Metasploit не смог определить результат запуска модуля.
- Недоступен/Unreachable – Metasploit не смог связаться с сетевым сервисом.
- Плохая конфигурация/Bad-config – настройки эксплойта были заданы неверно.
- Разъединение/Disconnected – связь с сетевым сервисом была разорвана во время работы модуля.
- Не найден/Not found – Metasploit не смог найти приложение или сервис.
- Неожиданный ответ/Unexpected-reply – Metasploit не получил ожидаемого ответа от приложения.
- Таймаут/Timeout-expired – время ожидания было превышено.
- Прервано пользователем/User-interrupt – пользователь сам остановил выполнение задач модуля.
- Нет доступа/No-access – Metasploit не смог получить доступ к приложению.
- Нет цели/No-target – настройки модуля не соответствовали цели.
- Неуязвима/Not-vulnerable – приложение не было уязвимым.
- Доставка не состоялась/Payload-failed – Metasploit доставил данные, но не смог открыть сессию.

Отметка Not Exploitable

Вы можете вручную отметить отметкой «**Not Exploitable**» любую уязвимость, у которой есть статус «**Exploit Attempted**» или «**Not Tested**». Статус «**Not Exploitable**» означает, что уязвимость не представляет реального риска и может считаться исключением.

Чтобы отметить неуязвимость как «**Not Exploitable**», выберите соответствующую опцию на странице уязвимости, как показано на изображении.

! Вы можете назначить отметку «Not Exploitable» только тем уязвимостям, которые имеют Nexpose статус «Exploit attempted» или «Not Tested».

Отправка подтвержденных уязвимостей

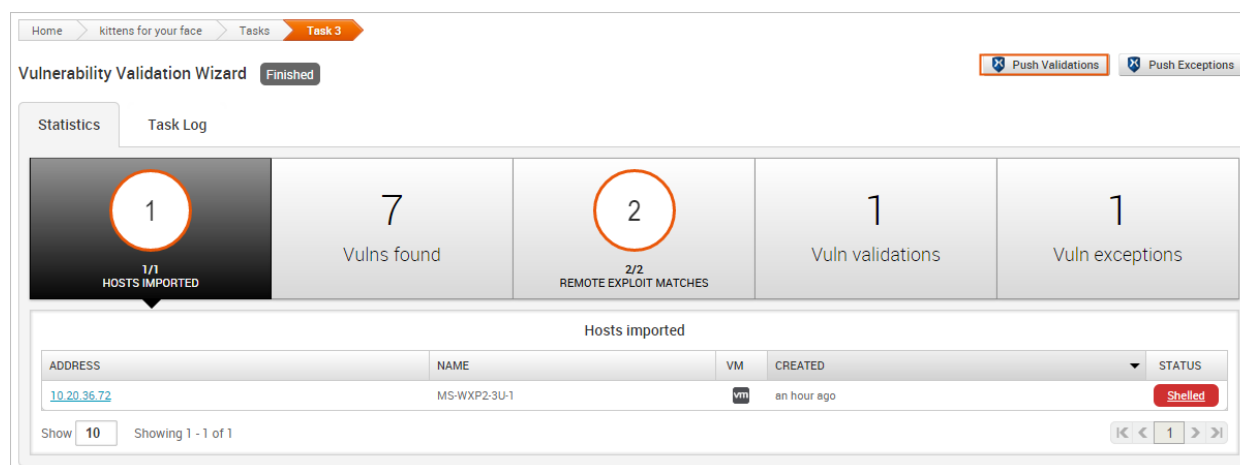
Вы можете отправить все подтвержденные уязвимости в Nexpose при помощи одной кнопки. Когда вы подготовите все подтвержденные уязвимости для отправки, есть несколько способов отправить их:

- Со страницы результатов Помощника проверки уязвимостей.
- Со страницы списка уязвимостей.
- Со страницы уязвимости.

! Чтобы отправить проверки в Nexpose, у вас должна быть активная консоль Nexpose, к которой имеет доступ ваша копия Metasploit Pro. Если консоль не будет обнаружена, возможность отправки будет отключена.

Отправка подтвержденных уязвимостей при помощи Помощника проверки уязвимостей

Когда помощник закончит работу, вы сможете отправить все подтвержденные уязвимости в Nexpose. Процесс отправки в Nexpose потребует от вас нажатия кнопки «**Push Validations**» в окне результатов. Она будет активна лишь в том случае, когда у вас есть уязвимости, подходящие для отправки. На изображении показана активная кнопка «**Push Validations**».



Когда вы отправляете подтвержденные уязвимости в Nexpose, любая успешно атакованная уязвимость будет отмечена как подтвержденная в консоли Nexpose, как показано на изображении.

Vulnerability Listing								
View details about discovered vulnerabilities. To use one of the exception controls on a vulnerability, select a row. To use the control with all displayed vulnerabilities, select the top row and use Select Visible. Cancel all selections using Clear All.								
Exposures: ☒ Susceptible to malware attacks ☑ Metasploit-exploitable ☑ Validated with Metasploit ☐ Exploit published ☑ Validated with published exploit								
Exclude Recall Resubmit		Total Vulnerabilities Selected: 0 of 137						
	Title		CVSS	Risk	Published On	Severity	Instances	Exceptions
☐	MS11-050: Cumulative Security Update for Internet Explorer (2530548)	☒	9.3	697	Thu Jun 16 2011	Critical	1	Exclude
☐	MS12-063: Cumulative Security Update for Internet Explorer (2744842)	☒	9.3	562	Tue Sep 18 2012	Critical	1	Exclude
☐	MS13-069: Cumulative Security Update for Internet Explorer (2870699)	☒	9.3	300	Tue Sep 10 2013	Critical	1	Exclude
☐	MS13-059: Cumulative Security Update for Internet Explorer (2862772)	☑	9.3	311	Tue Aug 13 2013	Critical	1	Exclude
☐	MS13-055: Cumulative Security Update for Internet Explorer (2846071)	☑	9.3	327	Tue Jul 09 2013	Critical	1	Exclude

Отправка подтвержденных уязвимостей со страницы списка уязвимостей

1. В проекте выберите **Analysis > Vulnerabilities**. Появится список уязвимостей.
2. Найдите кнопку «**Push Exploited Vulnerabilities**». Кнопка будет доступна, если есть подтвержденные уязвимости, требующие отправки в Nexpose.

Home > kittens for life! > Vulnerabilities					
Grouped View Delete Vulnerabilities Tag Hosts Scan Import Nexpose WebScan Modules Bruteforce Exploit Search Vulnerabilities					
Hosts Notes Services <input checked="" type="button" value="Vulnerabilities"/> Captured Data Network Topology					
<input checked="" type="button" value="Push Exploited Vulnerabilities"/> Create Exception					
	HOST	SERVICE	NAME	NEXPOSE TEST STATUS	REFERENCES
☐	MS-WXP2-3U-1		MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (4 Total)
☐	metasploitable.localdomain		Tomcat Application Manager Tomcat Tomcat Password Vulnerability	Not Tested	CVE-2009-3843 (4 Total)
☐	webtarget1.ms.scanlab.rapid7.com		Tomcat Application Manager Tomcat Tomcat Password Vulnerability	Not Tested	CVE-2009-3843 (4 Total)
☐	metasploitable.localdomain		HTTP TRACE Method Enabled	Not Exploited	CVE-2005-3398 (2 Total)
☐	MS-WXP2-3U-1		MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)	Not Tested	CVE-2012-0002 (2 Total)
☐	metasploitable.localdomain		'rsb' Remote Shell Service Enabled	Not Tested	CVE-1999-0651
☐	webtarget1.ms.scanlab.rapid7.com		HTTP TRACE Method Enabled	Not Tested	CVE-2005-3398 (2 Total)
☐	metasploitable.localdomain		Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368)	Not Tested	CVE-2011-3368
☐	webtarget1.ms.scanlab.rapid7.com		TLS/SSL Server Supports SSL version 3	Not Tested	CVE-2014-3566
☐	MS-WXP2-3U-1		MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Not Tested	CVE-2008-4114 (3 Total)
☐	MS-WXP2-3U-1		MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Not Tested	CVE-2010-2550 (2 Total)

- 3.
4. Кликните кнопку «**Push Exploited Vulnerabilities**». Появится Журнал задач/Task Log и покажет, когда отправка будет завершена.

Home

kittens for your face

Tasks

Task 4

Bruteforce...

Exploit...

Nexpose Push Exceptions and Validations

Completed

Started: 2015-02-23 15:09:04
-0600
Duration: less than 5 seconds

```
[*] [2015.02.23-13:09:05] Pushing Nexpose Validations
[*] [2015.02.23-13:09:05] Successfully pushed validations to Nexpose.
```

После отправки подтвержденных уязвимостей в Nexpose любая уязвимость, успешно атакованная эксплойтом, будет отмечена в консоли Nexpose, как показано на изображении.

Vulnerability Listing

View details about discovered vulnerabilities. To use one of the exception controls on a vulnerability, select a row. To use the control with all displayed vulnerabilities, select the top row and use Select Visible. Cancel all selections using Clear All.

Exposures: Susceptible to malware attacks Metasploit-exploitable Validated with Metasploit Exploit published Validated with published exploit

Exclude Recall Resubmit

Total Vulnerabilities Selected: 0 of 137

☐	Title		CVSS	Risk	Published On	Severity	Instances	Exceptions
☐	MS11-050: Cumulative Security Update for Internet Explorer (2530548)		9.3	697	Thu Jun 16 2011	Critical	1	Exclude
☐	MS12-063: Cumulative Security Update for Internet Explorer (2744842)		9.3	562	Tue Sep 18 2012	Critical	1	Exclude
☐	MS13-069: Cumulative Security Update for Internet Explorer (2870699)		9.3	300	Tue Sep 10 2013	Critical	1	Exclude
☐	MS13-059: Cumulative Security Update for Internet Explorer (2862772)		9.3	311	Tue Aug 13 2013	Critical	1	Exclude
☐	MS13-055: Cumulative Security Update for Internet Explorer (2846071)		9.3	327	Tue Jul 09 2013	Critical	1	Exclude

Отправка одной подтвержденной уязвимости

1. В проекте выберите **Analysis > Vulnerabilities**. Появится список уязвимостей.
2. Найдите уязвимость, которую нужно отправить в Nexpose и кликните на название для перехода на ее страницу. Подтвержденные уязвимости отмечены статусом **«Exploited»**.

Home > test-4 > Hosts > 10.20.36.53 - ms-w03r2-3u-1.ms.scanlab.rapid7.com

MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)

NAME: MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644) HOST: 10.20.36.53 REFERENCES: CVE-2008-4250 MS08-067 OSVDB-49243 rapid7

Overview Related Modules Related Hosts

Comments

Attempts History

ACTION	DESCRIPTION	STATUS	USER	TIME
Exploit	Run Module MS08-067 Microsoft Server Service Relative Path Stack Corruption	Exploited	tdoan	2015-03-06 21:03:40

Show 20 Showing 1 - 1 of 1

Mark as Not Exploitable **Push to Nexpose**

3. Нажмите кнопку **«Push to Nexpose»**.
4. При появлении окна подтверждения, кликните **«YES»**, чтобы отправить подтверждения в Nexpose.

Если Metasploit не сможет связаться с консолью Nexpose, появится сообщение об ошибке и оповестит о проблемах с консолью. Вы можете кликнуть **«YES»** еще раз для повторной попытки отправки. Если ошибки продолжают появляться, закройте модальное окно и продиагностируйте соединение с консолью.

Создание и отправка исключений

Когда вы готовы создать и отправить исключения, это можно сделать из разных разделов программы:

- Со страницы результатов Помощника проверки уязвимостей.
- Со страницы списка уязвимостей.
- Со страницы уязвимости.

! Чтобы отправить проверки в Nexpose, у вас должна быть активная консоль Nexpose, к которой имеет доступ ваша копия Metasploit Pro. Если консоль не будет обнаружена, возможность отправки будет отключена.

Как было уже замечено, исключения – это уязвимости, найденные консолью Nexpose, но не атакованные успешно программой Metasploit Pro. Когда вы создаете исключения, нужно выставить дату истечения, определяющую, когда исключение более не будет работать, а также сопроводить его причиной, почему исключение вообще существует.

Вы должны привязать к исключению одну из следующих причин:

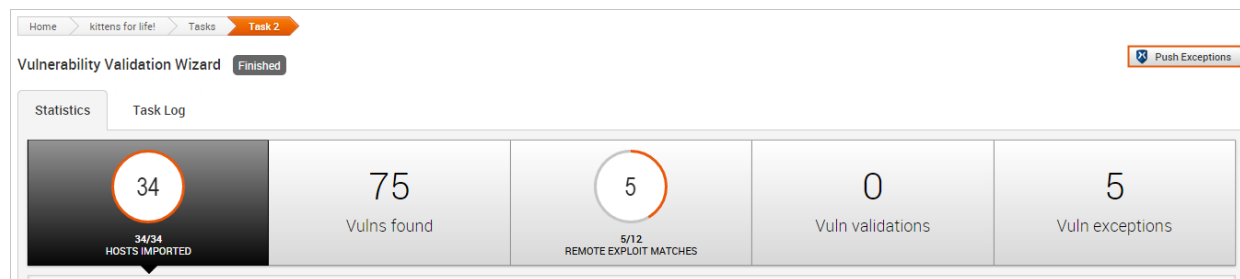
- Ложноположительная уязвимость/False Positive – указанная уязвимость не существует.
- Компенсация контроля - уязвимость является компенсирующей или специально внедрена для выполнения требований безопасности.
- Допустимое использование/Acceptable use – используйте эту причину, если уязвимость используется в работе организации.
- Допустимый риск/Acceptable risk – уязвимость представляет низкий уровень риска. Такие уязвимости представляют минимальную угрозу безопасности и требуют слишком много ресурсов для поиска решения.
- Другое/Other – уязвимость перенесена в исключения по другой причине. Если вы выбираете эту причину, введите объяснение в поле «Комментарий/Comment».

Отправка исключений при помощи Помощника проверки уязвимостей

Помощник проверки уязвимостей делает отправку исключений в Nexpose чрезвычайно простой. Когда помощник закончит работу, вы сможете отправить все исключения в Nexpose нажатием кнопки «**Push Exceptions**» в окне результатов, которая появится, если Metasploit Pro не сможет атаковать одну из уязвимостей. Чтобы открыть страницу «Создание исключений Nexpose/Create Nexpose Exceptions», нажмите кнопку «**Push Exceptions**». На этой странице вы сможете создать и отправить все исключения.

Чтобы отправить исключения при помощи Помощника проверки уязвимостей:

1. Кликните кнопку «**Push Exceptions**» в окне результатов. Появится страница «Create Nexpose Exceptions».



2. Выберите хосты, для которых вы хотите создать исключения. Используйте опцию «Использовать все хосты/Select All Hosts», если вы хотите создать исключения для всех хостов, для которых была найдена уязвимость, которую нельзя использовать.

Create Nexpose Exceptions

EXCEPTION SETTINGS ☒ Automatically Approve

Vulnerability Exceptions

☐ Select All Hosts ☒ Never Expire ☐ All Expire

MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)

☐ All Hosts with this Vulnerability ☒ Individual Hosts with this Vulnerability

☒	10.20.36.75	Reason: False Positive	Comment:	Expire:	Result Code: no-access
☒	10.20.36.75	Reason: False Positive	Comment:	Expire:	Result Code: payload-failed
☐	10.20.36.74	Reason: False Positive	Comment:	Expire:	Result Code: no-target
☒	10.20.36.74	Reason: False Positive	Comment:	Expire:	Result Code: no-access
☐	10.20.36.72	Reason: False Positive	Comment:	Expire:	Result Code: no-access
☐	10.20.36.51	Reason: False Positive	Comment:	Expire:	Result Code: no-target
☐	10.20.36.51	Reason: False Positive	Comment:	Expire:	Result Code: no-access

3. Для каждой уязвимости кликните «Причина/**Reason**» для вызова ниспадающего меню и выберите причину исключения, которую вы хотите задать для нее. Вы также можете добавить дополнительные сведения в поле для комментария.

Create Nexpose Exceptions

EXCEPTION SETTINGS ☒ Automatically Approve

Vulnerability Exceptions

☐ Select All Hosts ☒ Never Expire ☐ All Expire

MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)

☐ All Hosts with this Vulnerability ☒ Individual Hosts with this Vulnerability

☒	10.20.36.75	Reason: Acceptable Use	Comment:	Expire:	Result Code: no-access
☒	10.20.36.75	Reason: False Positive	Comment:	Expire:	Result Code: payload-failed
☐	10.20.36.74	Reason: Compensating Control	Comment:	Expire:	Result Code: no-target
☒	10.20.36.74	Reason: Acceptable Risk	Comment:	Expire:	Result Code: no-access
☐	10.20.36.72	Reason: Acceptable Use	Comment:	Expire:	Result Code: no-access
☐	10.20.36.51	Reason: Other	Comment:	Expire:	Result Code: no-target
☐	10.20.36.51	Reason: False Positive	Comment:	Expire:	Result Code: no-access

4. Выберите опцию «**All Expire**», если вы хотите задать дату истечения для всех исключений. Если вы не хотите задавать дату истечения исключения, оставьте опцию «Никогда не истекает/**Never expire**» и перейдите к шагу 6.

Чтобы установить единую дату истечения для всех исключений, выберите опцию «**All Expire**». Появится календарь. Найдите и выберите дату, которую хотите использовать.

Create Nexpose Exceptions

EXCEPTION SETTINGS ☒ Automatically Approve

Vulnerability Exceptions

☐ Select All Hosts

MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)

☐ All Hosts with this Vulnerability ☒ Individual Hosts with this Vulnerability

Host	Reason	Comment	Expire	Result Code
☒ 10.20.36.75	Acceptable Use			
☒ 10.20.36.75	Other			
☐ 10.20.36.74	False Positive			Result Code: no-target
☒ 10.20.36.74	False Positive			Result Code: no-access
☐ 10.20.36.72	False Positive			Result Code: no-access
☐ 10.20.36.51	False Positive			Result Code: no-target
☐ 10.20.36.51	False Positive			Result Code: no-access

Calendar: February 2015

Never Expire ☒ All Expire

Если вы хотите применить уникальную дату истечения для каждого отдельно взятого хоста, пропустите этот шаг и перейдите к шагу 5.

- Чтобы задать уникальную дату истечения для каждого хоста, кликните поле «**Expire**» рядом с исключением для вызова календаря. Найдите дату истечения, которую хотите использовать, и выберите ее.

Create Nexpose Exceptions

EXCEPTION SETTINGS ☒ Automatically Approve

Vulnerability Exceptions

☐ Select All Hosts

MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)

☐ All Hosts with this Vulnerability ☒ Individual Hosts with this Vulnerability

Host	Reason	Comment	Expire	Result Code
☒ 10.20.36.75	Acceptable Use			Result Code: no-access
☒ 10.20.36.75	Other			Result Code: payload-failed
☐ 10.20.36.74	False Positive			Result Code: no-target
☒ 10.20.36.74	False Positive			Result Code: no-access
☐ 10.20.36.72	False Positive			Result Code: no-access
☐ 10.20.36.51	False Positive			Result Code: no-target
☐ 10.20.36.51	False Positive			Result Code: no-access

Calendar: February 2015

Never Expire ☐ All Expire ☒

- Подтвердите запросы на создание исключений от Metasploit Pro. Если включена опция «Автоматическое подтверждение/**Automatically Approve**», Nexpose будет автоматически принимать все запросы на создание исключений, импортированные из Metasploit Pro. В ином случае, исключения должны будут проверены и подтверждены вручную в консоли Nexpose.

Create Nexpose Exceptions

EXCEPTION SETTINGS ☒ Automatically Approve

Vulnerability Exceptions

☐ Select All Hosts ☐ Never Expire ☒ All Expire 02/28/2015

MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)

☒ All Hosts with this Vulnerability ☐ Individual Hosts with this Vulnerability

Reason: **False Positive** Comment:

Host	Reason	Comment	Expire	Result Code
☒ 10.20.36.75	Reason: Acceptable Use	Comment:	Expire: 02/28/2015	Result Code: no-access
☒ 10.20.36.75	Reason: Other	Comment:	Expire: 02/28/2015	Result Code: payload-failed
☐ 10.20.36.74	Reason: False Positive	Comment:	Expire: 02/28/2015	Result Code: no-target
☒ 10.20.36.74	Reason: False Positive	Comment:	Expire: 02/28/2015	Result Code: no-access
☐ 10.20.36.72	Reason: False Positive	Comment:	Expire: 02/28/2015	Result Code: no-access
☐ 10.20.36.51	Reason: False Positive	Comment:	Expire: 02/28/2015	Result Code: no-target
☐ 10.20.36.51	Reason: False Positive	Comment:	Expire: 02/28/2015	Result Code: no-access

- Когда вы будете готовы отправить исключения, кликните кнопку «**Push Exceptions**».

Если отправка будет успешной, вместо этой кнопки появится статусное сообщение «Отправка прошла успешно/Push Succeeded».

Отправка исключений в Nexpose со страницы списка уязвимостей

Вы можете совершать отправки из списка уязвимостей, если вам нужно отправить все или несколько исключений одновременно.

Чтобы отправить исключения со страницы списка уязвимостей:

- В проекте выберите **Analysis > Vulnerabilities**. Появится список уязвимостей.
- Кликните «Создать исключения/**Create Exceptions**» для вызова ниспадающего меню и выберите опцию «**All not exploited**». Появится страница создания исключений для Nexpose.

Home > kittens for life! > **Vulnerabilities**

Grouped View Delete Vulnerabilities Tag Hosts Scan Import Nexpose WebScan Modules Bruteforce Exploit Search Vulnerabilities

Hosts Notes Services **Vulnerabilities** Captured Data Network Topology

HOST	SERVICE	NAME	NEXPOSE TEST STATUS	REFERENCES
☐ MS-WXP2-3U-1		MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (4 Total)
☐ metasploitable.localdomain		Tomcat Application Manager Tomcat Tomcat Password Vulnerability	Not Tested	CVE-2009-3843 (4 Total)
☐ webtarget1.ms.scanlab.rapid7.com		Tomcat Application Manager Tomcat Tomcat Password Vulnerability	Not Tested	CVE-2009-3843 (4 Total)
☐ metasploitable.localdomain		HTTP TRACE Method Enabled	Not Exploited	CVE-2005-3398 (2 Total)
☐ MS-WXP2-3U-1		MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)	Not Tested	CVE-2012-0002 (2 Total)
☐ metasploitable.localdomain		'rsb' Remote Shell Service Enabled	Not Tested	CVE-1999-0651
☐ webtarget1.ms.scanlab.rapid7.com		HTTP TRACE Method Enabled	Not Tested	CVE-2005-3398 (2 Total)
☐ metasploitable.localdomain		Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368)	Not Tested	CVE-2011-3368
☐ webtarget1.ms.scanlab.rapid7.com		TLS/SSL Server Supports SSL version 3	Not Tested	CVE-2014-3566
☐ MS-WXP2-3U-1		MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	Not Tested	CVE-2008-4114 (3 Total)
☐ MS-WXP2-3U-1		MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	Not Tested	CVE-2010-2550 (2 Total)

Show 100 Showing 1 - 11 of 11

- Выберите хосты, для которых вы хотите создать исключения. Используйте опцию «Использовать все хосты/**Select All Hosts**», если вы хотите создать исключения для всех хостов, на которых были обнаружены уязвимости, которые нельзя использовать.

Create Nexpose Exceptions

EXCEPTION SETTINGS ☒ Automatically Approve [Push Exceptions](#)

Vulnerability Exceptions

☒ Select All Hosts ☒ Never Expire ☐ All Expire

MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)

☒ All Hosts with this Vulnerability ☐ Individual Hosts with this Vulnerability

Reason: **False Positive** Comment:

IP	Reason	Comment	Expire	Result Code
☒ 10.20.36.75	Reason: Acceptable Use	Comment:	Expire:	Result Code: no-access
☒ 10.20.36.75	Reason: Other	Comment:	Expire:	Result Code: payload-failed
☒ 10.20.36.74	Reason: False Positive	Comment:	Expire:	Result Code: no-target
☒ 10.20.36.74	Reason: False Positive	Comment:	Expire:	Result Code: no-access
☒ 10.20.36.72	Reason: False Positive	Comment:	Expire:	Result Code: no-access
☒ 10.20.36.51	Reason: False Positive	Comment:	Expire:	Result Code: no-target
☒ 10.20.36.51	Reason: False Positive	Comment:	Expire:	Result Code: no-access

- Для каждой уязвимости кликните «**Reason**» для вызова ниспадающего меню и выберите причину для исключения. Вы можете добавить дополнительные сведения в поле для комментария.
- Выберите опцию «**All Expire**», если вы хотите задать дату истечения для всех исключений. Если вы не хотите задавать дату истечения исключения, оставьте опцию «Никогда не истекает/**Never expire**» и перейдите к шагу 7.

Чтобы установить единую дату истечения для всех исключений, выберите опцию «All Expire». Появится календарь. Найдите и выберите дату, которую хотите использовать.

Create Nexpose Exceptions

EXCEPTION SETTINGS ☒ Automatically Approve [Push Exceptions](#)

Vulnerability Exceptions

☐ Select All Hosts ☐ Never Expire ☒ All Expire

MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)

☐ All Hosts with this Vulnerability ☒ Individual Hosts with this Vulnerability

Reason: **Acceptable Use** Comment: Expire:

☒ 10.20.36.75 Reason: **Other** Comment: Expire:

☐ 10.20.36.74 Reason: **False Positive** Comment: Expire:

☒ 10.20.36.74 Reason: **False Positive** Comment: Expire:

☐ 10.20.36.72 Reason: **False Positive** Comment: Expire:

☐ 10.20.36.51 Reason: **False Positive** Comment: Expire:

☐ 10.20.36.51 Reason: **False Positive** Comment: Expire:

February 2015

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

Если вы хотите применить уникальную дату истечения для каждого отдельно взятого хоста, пропустите этот шаг и перейдите к следующему шагу.

- Чтобы задать уникальную дату истечения для каждого хоста, кликните поле «**Expire**» рядом с исключением для вызова календаря. Найдите дату истечения, которую хотите использовать, и выберите ее.

Create Nexpose Exceptions

EXCEPTION SETTINGS ☒ Automatically Approve [Push Exceptions](#)

Vulnerability Exceptions

☐ Select All Hosts ☐ Never Expire ☒ All Expire

MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)

☒ All Hosts with this Vulnerability ☐ Individual Hosts with this Vulnerability

Host	Reason	Comment	Expire	Result Code
☒ 10.20.36.75	Acceptable Use			no-access
☒ 10.20.36.75	Other			payload-failed
☐ 10.20.36.74	False Positive			no-target
☒ 10.20.36.74	False Positive			no-access
☐ 10.20.36.72	False Positive			no-access
☐ 10.20.36.51	False Positive			no-target
☐ 10.20.36.51	False Positive			no-access

7. Подтвердите запросы на создание исключений от Metasploit Pro. Если включена опция «Автоматическое подтверждение/**Automatically Approve**», Nexpose будет автоматически принимать все запросы на создание исключений, импортированные из Metasploit Pro. В ином случае, исключения должны будут проверены и подтверждены вручную в консоли Nexpose.

Create Nexpose Exceptions

EXCEPTION SETTINGS ☒ Automatically Approve [Push Exceptions](#)

Vulnerability Exceptions

☐ Select All Hosts ☐ Never Expire ☒ All Expire

MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)

☒ All Hosts with this Vulnerability ☐ Individual Hosts with this Vulnerability

Reason: **False Positive** Comment:

Host	Reason	Comment	Expire	Result Code
☒ 10.20.36.75	Acceptable Use		02/28/2015	no-access
☒ 10.20.36.75	Other		02/28/2015	payload-failed
☐ 10.20.36.74	False Positive		02/28/2015	no-target
☒ 10.20.36.74	False Positive		02/28/2015	no-access
☐ 10.20.36.72	False Positive		02/28/2015	no-access
☐ 10.20.36.51	False Positive		02/28/2015	no-target
☐ 10.20.36.51	False Positive		02/28/2015	no-access

8. Когда вы будете готовы отправить исключения, кликните кнопку «**Push Exceptions**».

Появится Журнал задач, где будет отображен статус отправки. Если отправка будет успешной, вместо этой кнопки появится статусное сообщение «Отправка прошла успешно/**Push Succeeded**».

Home > kittens for your face > Tasks > **Task 3** Bruteforce... Exploit...

Nexpose Push Exceptions and Validations ✔ Completed

Started: 2015-02-24 10:43:42
-0600
Duration: less than 5 seconds

```
[*] [2015.02.24-08:43:42] Pushing Nexpose Exceptions
[*] [2015.02.24-08:43:44] Successfully pushed exceptions to Nexpose.
```

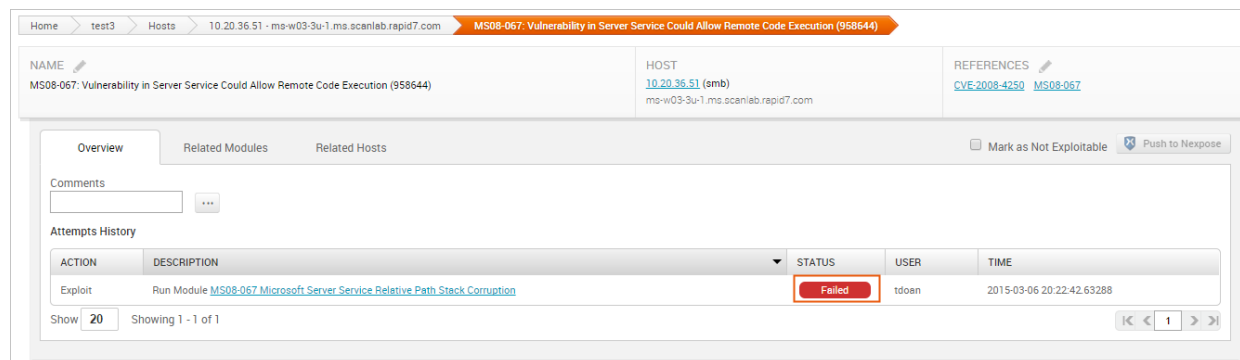
Если Metasploit не сможет связаться с консолью Nexpose, появится сообщение об ошибке и оповестит о проблемах с консолью. Вы можете кликнуть «**YES**» еще раз для повторной попытки отправки. Если ошибки продолжают появляться, закройте модальное окно и продиагностируйте соединение с консолью.

Отправка исключений в Nexpose со страницы уязвимости

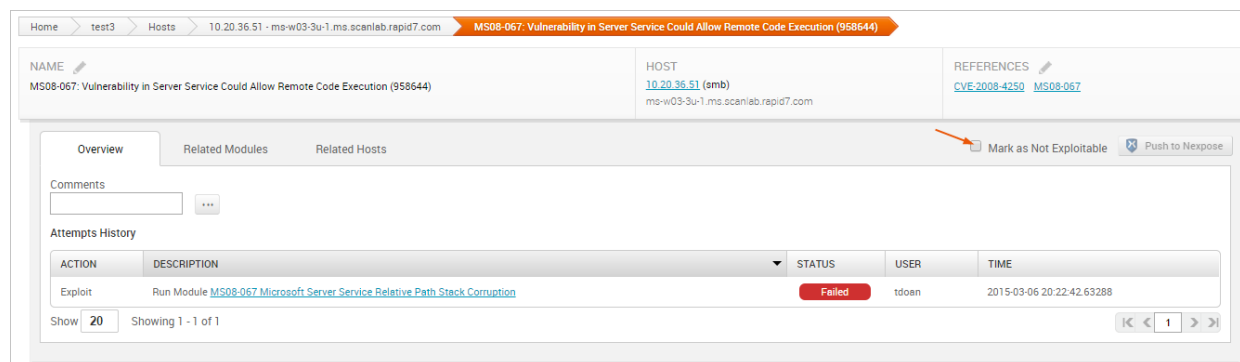
Вы можете отправить одну уязвимость, если нужно отправить какое-то определенное исключение обратно в Nexpose.

1. В проекте выберите **Analysis > Vulnerabilities**. Появится список уязвимостей.
2. Найдите уязвимость, которую нужно отправить в Nexpose и кликните на название для перехода на ее страницу. Подтвержденные уязвимости отмечены статусом «Exploited».

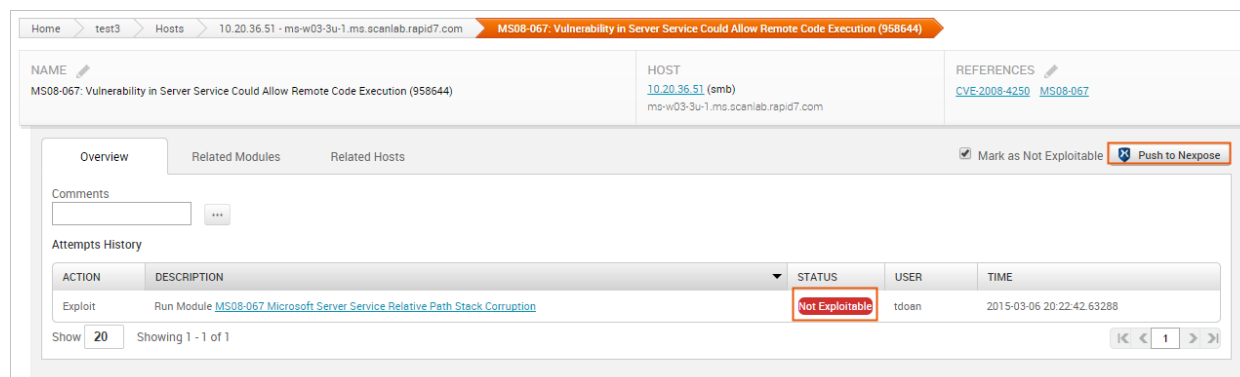
Когда появится страница уязвимости, на ней должен быть статус «Неудачно/Failed» или вообще никакого статуса, если уязвимость не было протестирована.



3. Выберите опцию «Отметить как Not Exploitable/Mark as Not Exploitable».



После выбора этой опции статус модуля будет заменен на «**Not Exploitable**» и кнопка «**Push**» станет активной.

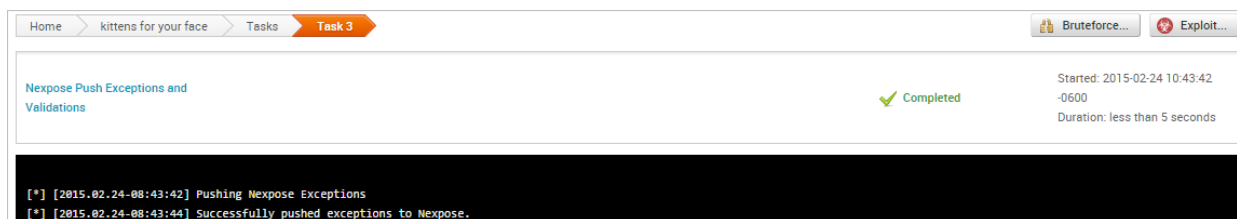


4. Кликните кнопку «**Push to Nexpose**». Появится окно «Push to Nexpose».

Кликните «**Reason**» для вызова ниспадающего меню и выберите [причину исключения уязвимости](#).

6. Кликните поле «**Expiration date**» рядом с исключением для вызова календаря. Найдите дату истечения, которую хотите использовать, и выберите ее. Если вы не хотите указывать какую-то определенную дату, оставьте поле пустым.
7. Подтвердите запросы на создание исключений от Metasploit Pro. Если включена опция «Автоматическое подтверждение/**Automatically Approve**», Nexpose будет автоматически принимать все запросы на создание исключений, импортированные из Metasploit Pro. В ином случае, исключения должны будут проверены и подтверждены вручную в консоли Nexpose.
8. При появлении окна подтверждения, кликните «**YES**», чтобы отправить подтверждения в Nexpose.

Появится Журнал задач, где будет отображен статус отправки. Если отправка будет успешной, вместо этой кнопки появится статусное сообщение «Отправка прошла успешно/Successfully pushed exceptions to Nexpose».



Если Metasploit не сможет связаться с консолью Nexpose, появится сообщение об ошибке и оповестит о проблемах с консолью. Вы можете кликнуть «**YES**» еще раз для повторной попытки отправки. Если ошибки продолжают появляться, закройте модальное окно и продиагностируйте соединение с консолью.

Обновление исключений в Nexpose

Когда-нибудь вам может понадобиться изменить исключения и подтвержденные уязвимости после того, как они уже были отправлены из Metasploit Pro в Nexpose. Для обновления списка подтверждений и исключений необходимо войти в консоль Nexpose и вручную изменить необходимые данные. На данный момент способа обновить информацию из интерфейса Metasploit Pro нет. Для получения дополнительной информации по управлению исключениями читайте [руководство пользователя для Nexpose](#).

Отслеживание статистики в реальном времени и событий во время проверки уязвимостей

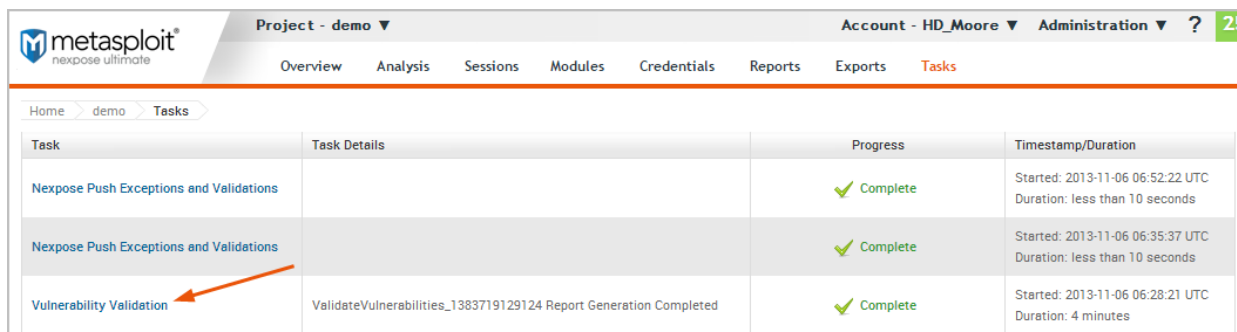
В окне результатов отображается статистика в реальном времени для тестов и журнал задач. Вы можете кликнуть на вкладку в верхней части окошка для переключения между статистикой в реальном времени и журналом задач. Вы также можете автоматически отправлять подтвержденные уязвимости и открыть страницу настройки исключений.

Доступ к окну результатов

Окно результатов появляется в момент начала работы Помощника проверки уязвимостей. Если вы потеряете окно во время навигации, вы всегда сможете вернуться на страницу задач и вновь открыть его.

Чтобы открыть окно результатов:

1. В проекте выберите **Tasks > Show Tasks** во вкладке управления проектом. Появится страница задач.
2. Найдите задачу по проверке уязвимостей.

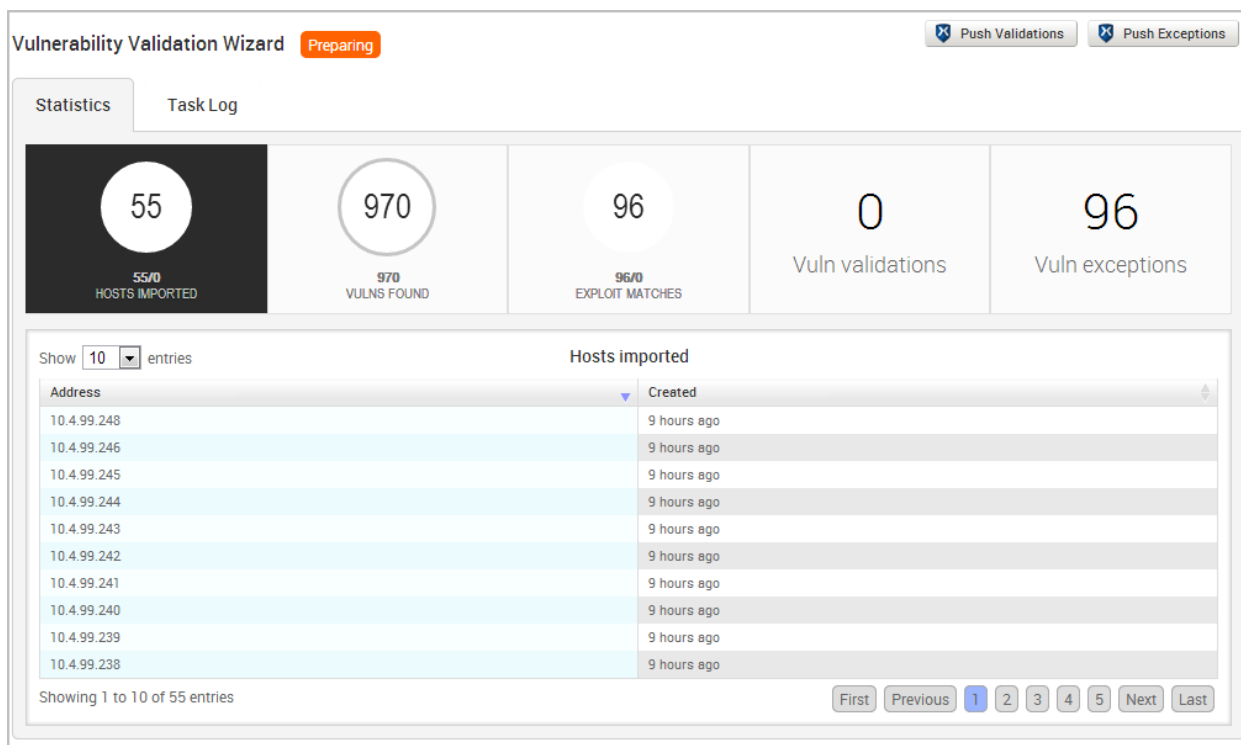


Task	Task Details	Progress	Timestamp/Duration
Nexpose Push Exceptions and Validations		✓ Complete	Started: 2013-11-06 06:52:22 UTC Duration: less than 10 seconds
Nexpose Push Exceptions and Validations		✓ Complete	Started: 2013-11-06 06:35:37 UTC Duration: less than 10 seconds
Vulnerability Validation	ValidateVulnerabilities_1383719129124 Report Generation Completed	✓ Complete	Started: 2013-11-06 06:28:21 UTC Duration: 4 minutes

3. Кликните на название задачи. Появится окно результатов.

Вкладка статистики

В этой вкладке отображаются общие данные касательно хостов, уязвимостей и эксплойтов. Значения отображаются в окне статистики вместе с оранжевым индикатором прогресса. Индикатор делает полный оборот вокруг окошка статистики и отображается, когда есть какая-то активность, относящаяся к какому-то определенному типу данных.



Во вкладке статистики вы можете отслеживать следующие типы данных:

- Общее количество отсканированных и импортированных хостов.
- Общее количество уникальных обнаруженных идентифицированных уязвимостью.
- Общее количество модулей эксплойтов, подходящих для тестирования уязвимостей в Nexpose.
- Общее количество уязвимостей, успешно атакованных Metasploit Pro.
- Общее количество уязвимостей, неуспешно атакованных Metasploit Pro.

Просмотр списка импортированных хостов из окна Findings («Результаты»)

1. Откройте окно Findings.
2. Перейдите на вкладку **Hosts Imported** («Импортировано хостов»). Появится список хостов и отобразятся IP-адреса для каждого хоста, который был импортирован с группы Nexpose.

Vulnerability Validation Wizard Preparing Push Validations Push Exceptions

Statistics Task Log

55
55/0
HOSTS IMPORTED

970
970
VULNS FOUND

96
96/0
EXPLOIT MATCHES

0
Vuln validations

96
Vuln exceptions

Show 10 entries

Hosts imported

Address	Created
10.4.99.248	9 hours ago
10.4.99.246	9 hours ago
10.4.99.245	9 hours ago
10.4.99.244	9 hours ago
10.4.99.243	9 hours ago
10.4.99.242	9 hours ago
10.4.99.241	9 hours ago
10.4.99.240	9 hours ago
10.4.99.239	9 hours ago
10.4.99.238	9 hours ago

Showing 1 to 10 of 55 entries

First Previous 1 2 3 4 5 Next Last

3. Используйте кнопки навигации для просмотра большего количества хостов, или щёлкните раскрывающееся меню **Show Entries** («Показать записи»), чтобы увеличить количество отображаемых хостов.

Vulnerability Validation Wizard Preparing Push Validations Push Exceptions

Statistics Task Log

55
55/0
HOSTS IMPORTED

970
970
VULNS FOUND

96
96/0
EXPLOIT MATCHES

0
Vuln validations

96
Vuln exceptions

Show 10 entries

Hosts imported

Address	Created
10.4.99.248	9 hours ago
10.4.99.246	9 hours ago
10.4.99.245	9 hours ago
10.4.99.244	9 hours ago
10.4.99.243	9 hours ago
10.4.99.242	9 hours ago
10.4.99.241	9 hours ago
10.4.99.240	9 hours ago
10.4.99.239	9 hours ago
10.4.99.238	9 hours ago

Showing 1 to 10 of 55 entries

First Previous 1 2 3 4 5 Next Last

Просмотр списка импортированных уязвимостей из окна Findings («Результаты»)

1. Откройте окно Findings.
2. Перейдите на вкладку **Vulns Found**. Появится список импортированных уязвимостей.

Vulnerability Validation Wizard Preparing Push Validations Push Exceptions

Statistics Task Log

55 55/0 HOSTS IMPORTED	970 970 VULNS FOUND	96 96/0 EXPLOIT MATCHES	0 Vuln validations	96 Vuln exceptions
------------------------------	---------------------------	-------------------------------	-----------------------	-----------------------

Show 10 entries Vulns found

Vulnerability	Created
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago

Showing 1 to 10 of 865 entries

First Previous 1 2 3 4 5 Next Last

3. Используйте кнопки навигационной страницы для просмотра большего количества хостов, или нажмите раскрывающееся меню **Show Entries** («Показать записи»), чтобы развернуть список обнаруженных уязвимостей.

Vulnerability Validation Wizard Preparing Push Validations Push Exceptions

Statistics Task Log

55 55/0 HOSTS IMPORTED	970 970 VULNS FOUND	96 96/0 EXPLOIT MATCHES	0 Vuln validations	96 Vuln exceptions
------------------------------	---------------------------	-------------------------------	-----------------------	-----------------------

Show 10 entries Vulns found

Vulnerability	Created
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago
windows-hotfix-ms13-080	9 hours ago

Showing 1 to 10 of 865 entries

First Previous 1 2 3 4 5 Next Last

Просмотр списка совпадений в окне Findings («Результаты»)

1. Откройте окно Findings.
2. Перейдите на вкладку Exploit Matches. Появится список импортированных уязвимостей.

Home demo Tasks Task 27

Vulnerability Validation Wizard **Preparing** [Push Validations](#) [Push Exceptions](#)

Statistics Task Log

55 HOSTS IMPORTED 970 VULNS FOUND 96 EXPLOIT MATCHES 0 Vuln validations 96 Vuln exceptions

Show 10 entries

Id	Name	Metasploit module
252	MS11-006: Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185)	exploit/windows/fileformat/ms11_006_createsizeddibsection
251	MS11-006: Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185)	exploit/windows/fileformat/ms11_006_createsizeddibsection

3. Используйте навигационные кнопки для просмотра большего количества хостов, или нажмите раскрывающееся меню **Show Entries** («Показать записи»), чтобы развернуть список отображаемых модулей эксплойтов.

Просмотр списка проверенных уязвимостей из окна Findings («Результаты»)

1. Откройте окно Findings.
2. Перейдите на вкладку **Vulns validations**. Появится список импортированных уязвимостей.

Home demo Tasks Task 27

Vulnerability Validation Wizard **Preparing** [Push Validations](#) [Push Exceptions](#)

Statistics Task Log

55 HOSTS IMPORTED 970 VULNS FOUND 96 EXPLOIT MATCHES 0 Vuln validations 96 Vuln exceptions

Show 10 entries

Id	Name	Metasploit module	State
No data has been recorded.			

Showing 0 to 0 of 0 entries

First Previous Next Last

Вы можете посмотреть наименование уязвимости, модуль эксплойтов, который был задействован против этой уязвимости, и результат эксплойта. Для подтвержденной уязвимости статус будет «exploited».

- Используйте навигационные кнопки для просмотра большего количества хостов, или нажмите раскрывающееся меню **Show Entries** («Показать записи»), чтобы увеличить количество отображаемых на экране проверок.

Просмотр списка исключений уязвимостей из окна Findings («Результаты»)

- Откройте окно Findings.
- Перейдите на вкладку **Vulns exceptions**. Появится список исключений уязвимостей.

Id	Name	Metasploit module	State
158	USN-758-1: udev vulnerabilities	exploit/linux/local/udev_netlink	failed
159	MS11-006: Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185)	exploit/windows/fileformat/ms11_006_createsizeddibsection	failed

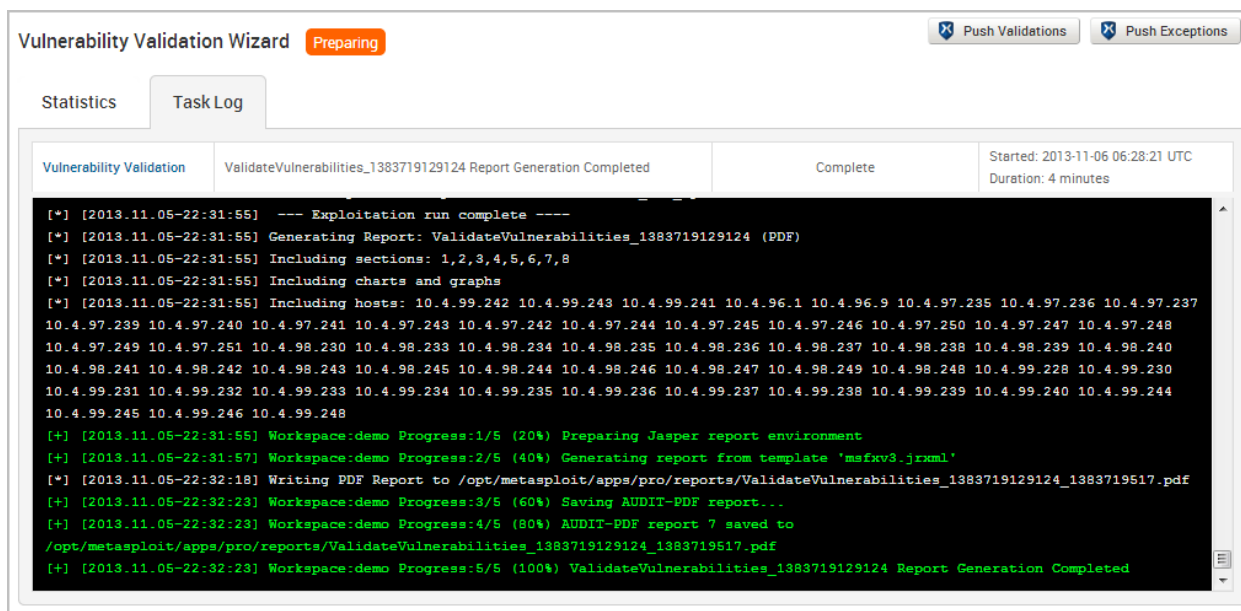
Вы можете посмотреть имя уязвимости, модуль эксплойтов, который был задействован против этой уязвимости, и результат эксплойта. Для исключений уязвимости статус будет «failed».

- Используйте навигационные кнопки для просмотра большего количества хостов, или нажмите раскрывающееся меню **Show Entries** («Показать записи»), чтобы увеличить количество отображаемых на экране исключений.

Вкладка Tasks Log («Журнал задач»)

Вкладка Tasks Log («Журнал задач») отображает подробный журнал активности для мастера проверки уязвимостей. Каждая задача, которую выполняет Metasploit Pro, задокументирована в журнале задач. Например, вы можете просматривать определения активов и уязвимостей по мере их импорта в проект, или просматривать модули эксплойтов по мере их запуска. Если вы решили выполнить пробный запуск задачи автоматической эксплуатации, можно перейти в журнал задач, чтобы посмотреть предлагаемый план атаки.

Кроме того, журнал задач отображает текущее состояние теста, время начала теста и время, в течение которого тест был запущен.



Управление исключениями для Nexpose

Исключение определяет причину, по которой существует уязвимость. Как правило, исключения применяются к уязвимостям, которые являются низкорисковыми или используются специально для уменьшения более серьёзных угроз. Исключения для уязвимостей помогают исключить определённые уязвимости из отчёта, чтобы вы могли управлять своими оценками риска.

Вы можете применять исключения к уязвимостям, которые Metasploit Pro не смог использовать. Эти уязвимости имеют статус Not Exploitable, что указывает на то, что Metasploit Pro не смог получить сеанс на целевом хосте из-за некоего компенсирующего управления или обратного портирования.

Как правило, исключения могут быть определены для уязвимостей по следующим причинам:

- Они используются в качестве компенсирующих средств контроля или для уменьшения излишних рисков.
- Они представляют собой допустимый случай либо целенаправленное действие – такое, как анонимный доступ к FTP.
- Они представляют собой приемлемый риск, и могут потребовать больше ресурсов, чем вы готовы задействовать для их устранения. Как правило это минимальный риск.
- Это ложные срабатывания.

Страница Exceptions («Исключения»)

Вы создаёте и вводите Nexpose-исключения на странице Exceptions («Исключения»). Страница Exceptions доступна из окна Findings («Результаты») или на странице Vulnerabilities («Уязвимости»).

На странице Exceptions вы можете определить параметры исключения для группы хостов с определённой уязвимостью, или определить их отдельно для каждого хоста.

Create Nexpose Exceptions

EXCEPTION SETTINGS Nexpose Console **nx** ☒ Automatically Approve **Push Exceptions**

Vulnerability Exceptions

☐ Select All Hosts ☒ Never Expire ☐ All Expire

Tomcat Application Manager Tomcat Tomcat Password Vulnerability Result Code: Bad-config

☐ All Hosts with this Vulnerability ☒ Individual Hosts with this Vulnerability

Host	Reason	Comment	Expire
☐ 10.6.201.148	False Positive		
☐ 10.6.201.148	False Positive		

На странице Exceptions вы можете выполнять следующие задачи:

- Просматривать все уязвимости, которые Metasploit Pro не смог использовать.
- Назначать причину исключения для каждой уязвимости.
- Назначать даты истечения срока действия для исключений уязвимостей.
- Добавлять комментарии к исключениям уязвимостей.
- Автоматически утверждать запросы об исключениях для уязвимостей.
- Удалять исключения в Nexpose.

Доступ к странице Exceptions («Исключения»)

1. В рамках проекта выберите **Analysis > Vulnerabilities** на панели Project Tab. Появится страница Vulnerabilities («Уязвимости»).
2. Нажмите раскрывающееся меню **Create Exception** («Создать исключение») и выберите **All Not Exploited**. Появится страница Exceptions («Исключения»).

Примечание. Параметр **All Not Exploited** выбирает все уязвимости со статусом «Not Exploited», и отображает их на странице Exceptions. Если вы хотите создавать исключения только для нескольких конкретных уязвимостей, вы можете вручную выбрать их из списка Vulnerabilities и выбрать опцию All Selected.

Home > test-manual > Vulnerabilities

Grouped View Delete Vulnerabilities Tag Hosts Scan Import Nexpose WebScan Modules Bruteforce Exploit

Hosts Notes Services Vulnerabilities Captured Data Network Topology

Push Exploited Vulnerabilities Create Exception

Show 100 entries

Host	Service	Name	Status	References
metasploitable	80/tcp	PHP Vulnerability: CVE-2012-1823	Exploited	CVE-2012-1823 (6 Total)
metasploitable	139/tcp	Samba MS-RPC Shell Command Injection Vulnerability	Exploited	CVE-2007-2447 (5 Total)
metasploitable	8180/tcp	Tomcat Application Manager Tomcat Tomcat Password Vulnerability	Not Exploited	CVE-2009-3843 (4 Total)
metasploitable	80/tcp	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368)	Not Exploitable	CVE-2011-3368
metasploitable	8180/tcp	Apache Tomcat: Important: Remote Denial Of Service and Information Disclosure Vulnerability (CVE-2010-2227)	Not Exploitable	CVE-2010-2227 (2 Total)
metasploitable	8180/tcp	Apache Tomcat: Low: Information disclosure (CVE-2009-0580)	Not Exploitable	CVE-2009-0580 (2 Total)
metasploitable	8180/tcp	Apache Tomcat: Low: Insecure default password (CVE-2009-3548)	Not Exploited	CVE-2009-3548 (2 Total)

Create Exception dropdown: All Not Exploited, All Selected

Создание и поддержка исключений Nexpose

1. В рамках проекта выберите **Analysis > Vulnerabilities** на панели Project Tab. Появится страница Vulnerabilities («Уязвимости»).
2. Нажмите раскрывающееся меню **Create Exception** («Создать исключение») и выберите **All Not Exploited**. Появится страница Exceptions («Исключения»).

Примечание. Кнопка **Create Exceptions** («Создать исключения») доступна в окне **Findings** («Результаты»), когда имеются уязвимости, которые могут быть отнесены к исключениям; в противном случае она будет недоступна.

Home > test-manual > Vulnerabilities

Grouped View Delete Vulnerabilities Tag Hosts Scan Import Nexpose WebScan Modules Bruteforce Exploit

Hosts Notes Services Vulnerabilities Captured Data Network Topology

Push Exploited Vulnerabilities Create Exception

Show 100 entries

Host	Service	Name	Status	References
metasploitable	80/tcp	PHP Vulnerability: CVE-2012-1823	Exploited	CVE-2012-1823 (6 Total)
metasploitable	139/tcp	Samba MS-RPC Shell Command Injection Vulnerability	Exploited	CVE-2007-2447 (5 Total)
metasploitable	8180/tcp	Tomcat Application Manager Tomcat Tomcat Password Vulnerability	Not Exploited	CVE-2009-3843 (4 Total)
metasploitable	80/tcp	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368)	Not Exploitable	CVE-2011-3368
metasploitable	8180/tcp	Apache Tomcat: Important: Remote Denial Of Service and Information Disclosure Vulnerability (CVE-2010-2227)	Not Exploitable	CVE-2010-2227 (2 Total)
metasploitable	8180/tcp	Apache Tomcat: Low: Information disclosure (CVE-2009-0580)	Not Exploitable	CVE-2009-0580 (2 Total)
metasploitable	8180/tcp	Apache Tomcat: Low: Insecure default password (CVE-2009-3548)	Not Exploited	CVE-2009-3548 (2 Total)

Create Exception dropdown: All Not Exploited, All Selected

3. Нажмите раскрывающийся список **Nexpose Console** и выберите консоль, для которой вы хотите сделать исключения.

Home > dsf > New Nexpose Exception Push

Create Nexpose Exceptions

EXCEPTION SETTINGS Nexpose Console nx ☒ Automatically Approve Push Exceptions

Vulnerability Exceptions

Select All Hosts

Never Expire All Expire

4. Для каждой уязвимости щёлкните раскрывающееся меню **Reason** («Причина») и выберите причину исключения уязвимости, которую вы хотите назначить. Вы также можете предоставить дополнительную информацию об исключении в поле **Comment** («Комментарий»). Дополнительные сведения о причинах исключения смотрите в разделе «[Причины исключения уязвимостей](#)»

Примечание. Если вы хотите определить параметры массового исключения для всех узлов в группе уязвимостей, выберите опцию **All Hosts with this Vulnerability** («Все хосты с этой уязвимостью»). Поля Reason и Comment становятся доступными под именем этой уязвимости. Выбранная вами причина исключения относится ко всем хостам в этой группе уязвимостей.

The screenshot shows the 'Vulnerability Exceptions' section. At the top, there's a 'Select All Hosts' checkbox and two radio buttons: 'Never Expire' (selected) and 'All Expire'. Below this, the vulnerability is identified as 'Tomcat Application Manager Tomcat Tomcat Password Vulnerability' with a 'Result Code: Bad-config'. There are two radio buttons for selection: 'All Hosts with this Vulnerability' and 'Individual Hosts with this Vulnerability' (selected). A table lists four entries for IP addresses 10.6.201.168 and 10.6.201.172. The 'Reason' dropdown for the first entry is open, showing a list of reasons. The 'Comment' and 'Expire' fields are empty for all entries.

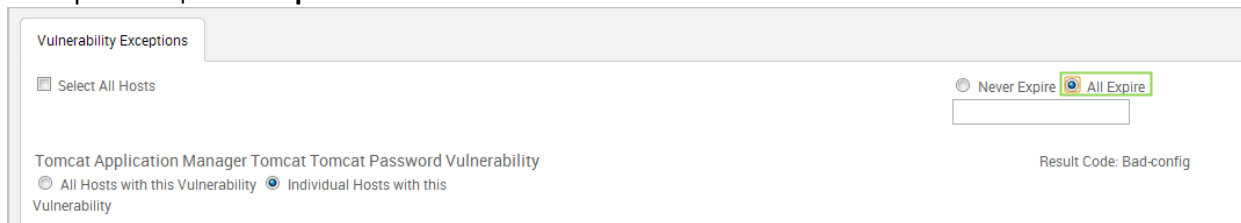
5. Выберите опцию **All Expire**, если вы хотите установить дату истечения срока действия для исключений уязвимостей. Если вы не хотите устанавливать дату истечения срока действия для каких-либо исключений уязвимостей, сохраните опцию **Never Expire** по умолчанию и перейдите к шагу 6.

This screenshot is similar to the previous one, but the 'All Expire' radio button is now selected, and the 'Never Expire' button is unselected. The rest of the interface remains the same.

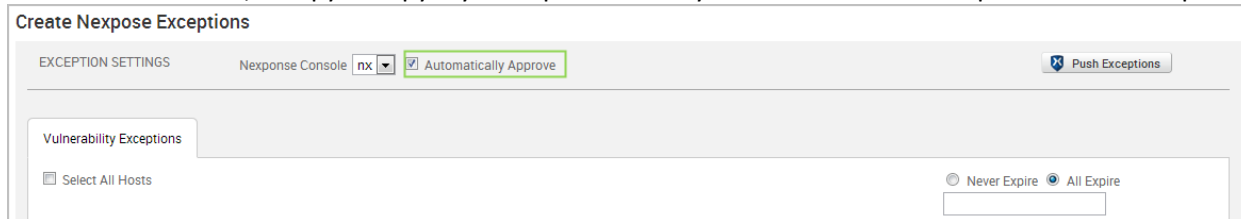
6. Чтобы установить ту же дату истечения срока действия для всех исключений уязвимостей, выберите опцию **All Expire**. Появится календарь. Найдите и выберите дату, которую хотите использовать. Если вы хотите установить индивидуальную дату истечения срока действия для каждого хоста, пропустите этот шаг и перейдите к следующему.

This screenshot shows the 'Vulnerability Exceptions' interface with a calendar overlay. The 'All Expire' radio button is selected. The calendar is for November 2013, showing days from Sunday to Saturday. The 'Expire' field for the first entry is now populated with a date from the calendar. The 'Reason' dropdown for the first entry is still open.

7. Чтобы установить индивидуальную дату истечения срока действия для каждого хоста:

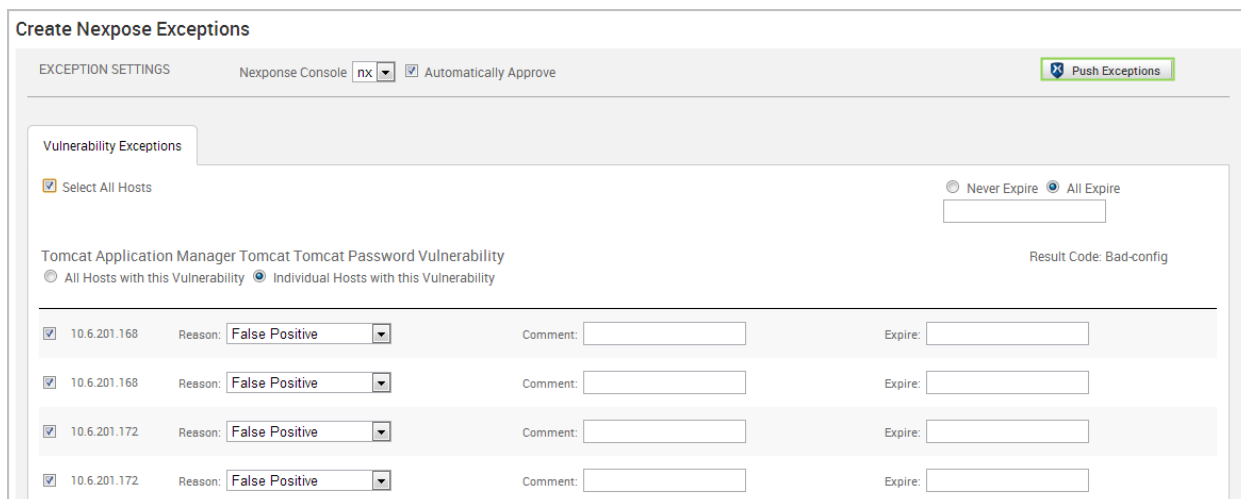
a. Выберите опцию **All Expire**.

b. Нажмите на поле **Expire** рядом с каждым хостом, чтобы отобразить календарь.


- c. Найдите дату истечения срока действия, которую вы хотите использовать, и выберите её.
8. Отмените выбор параметра **Automatically Approve** («Автоматическое одобрение»), если вы не хотите одобрять какие-либо из запросов об исключениях для уязвимостей от Metasploit Pro. Вместо этого санкционируйте вручную запросы на получение исключений через консоль Nexpose.



9. Выберите хосты, для которых вы хотите использовать исключения. Установите флажок **Select All Hosts** («Выбрать все хосты»), если вы хотите добавить исключения для всех хостов.

10. Когда вы уже готовы выбрать исключения, нажмите кнопку **Push Exceptions** («Добавить исключения»).



Причины исключений уязвимости

Доступны следующие причины исключения уязвимости:

- **False positive** («Ложная тревога») - используйте эту исключаящую причину для уязвимости, которая в действительности не существует.
- **Compensating control** («Компенсация контроля») - используйте эту исключаящую причину, чтобы указать, что уязвимость является компенсационным контролем или обходным решением по требованиям безопасности.
- **Acceptable use** («Допустимое использование») - используйте эту исключаящую причину для любой уязвимости, которая используется как часть организационной практики.
- **Acceptable risk** («Допустимый риск») - используйте эту исключаящую причину для любой уязвимости, которая считается низкорисковой. Эти уязвимости, как правило, представляют собой минимальный риск для безопасности и, вероятно, будут потреблять больше ресурсов, чем они того заслуживают.
- **Other** («Другое») - используйте эту исключаящую причину, если причина не соответствует ни одной из вышеперечисленных. Вы можете указать причину в поле **Comment** («Комментарий»).

Коды результатов модуля

Код результата определяет причину неудачи эксплойта. Вы можете просмотреть код результата для уязвимости на странице **Vulnerability Exceptions** («Исключения уязвимостей»).

Доступны следующие коды результатов:

None - указывает, что Metasploit Pro не смог определить, успешно ли работает модуль, или его запустить не удалось.

- **Unknown** - указывает, что Metasploit Pro не смог определить, успешно ли работает модуль, или его запустить не удалось.
- **Unreachable** - указывает, что Metasploit Pro не смог получить доступ к сетевому сервису.
- **Bad-config** - указывает, что параметры эксплойта настроены неправильно.
- **Disconnected** - указывает, что сетевая служба отключена во время работы модуля.
- **Not-found** - указывает, что Metasploit Pro не смог найти приложение или услугу.
- **Unexpected-reply** - указывает, что Metasploit Pro не получил ожидаемого ответа от приложения.
- **Timeout-expired** - указывает, что произошёл тайм-аут.
- **User-interrupt** - указывает, что пользователь остановил запуск модуля.
- **No-access** - указывает, что Metasploit Pro не может получить доступ к приложению.
- **No-target** - указывает, что конфигурация модуля несовместима с целью.
- **Not-vulnerable** - указывает, что приложение не имеет уязвимости.
- **Payload-failed** - указывает, что Metasploit Pro предоставил полезную нагрузку, но не смог открыть сеанс.

Просмотр исключений уязвимостей в Nexpose

После того, как вы внесёте исключения, можно перейти к Vulnerability Exception Listing, списку исключений для уязвимостей (**Administration > Exceptions and Overrides > Manage**) в Nexpose

Console для просмотра запросов об исключениях, которые были одобрены или ожидают рассмотрения. Vulnerability Exception Listing показывает исключения, которые активны для всех сайтов. Дополнительные сведения об управлении исключениями уязвимостей смотрите в инструкции пользователя [Nexpose User's Guide](#).

Vulnerability Exception Listing						
 Review  Delete						
 Vulnerability	Exception Scope	Reason	Reported By	Review Status	Expires On	
 Apache Tomcat Low: Insecure default password (CVE-2009-3548)	Specific instance on asset METASPLOITABLE:8180	False Positive	msfadmin	 Under review	N/A	
 Apache Tomcat Low: Insecure default password (CVE-2009-3548)	All instances on asset METASPLOITABLE	Acceptable Risk	msfadmin	 Approved by msfadmin	Wed Nov 13 2013	
 Apache Tomcat Low: Insecure default password (CVE-2009-3548)	All instances on asset METASPLOITABLE	Acceptable Risk	msfadmin	 Approved by msfadmin	Wed Nov 13 2013	
 Tomcat Application Manager Tomcat Tomcat Password Vulnerability	All instances on asset METASPLOITABLE	Acceptable Risk	msfadmin	 Approved by msfadmin	Wed Nov 13 2013	
 Apache Tomcat Low: Insecure default password (CVE-2009-3548)	All instances on asset METASPLOITABLE	Compensating Control	msfadmin	 Approved by msfadmin	Wed Nov 13 2013	
 Tomcat Application Manager Tomcat Tomcat Password Vulnerability	All instances on asset METASPLOITABLE	Acceptable Risk	msfadmin	 Approved by msfadmin	Wed Nov 13 2013	
 Tomcat Application Manager Tomcat Tomcat Password Vulnerability	All instances on asset METASPLOITABLE	Compensating Control	msfadmin	 Approved by msfadmin	Wed Nov 13 2013	
 Apache Tomcat Low: Insecure default password (CVE-2009-3548)	All instances on asset METASPLOITABLE	Compensating Control	msfadmin	 Approved by msfadmin	Wed Nov 13 2013	
 Tomcat Application Manager Tomcat Tomcat Password Vulnerability	All instances on asset METASPLOITABLE	Compensating Control	msfadmin	 Approved by msfadmin	Wed Nov 13 2013	

Использование эксплойтов

Эксплойт выполняет последовательность команд, которые нацелены на определённую уязвимость, обнаруженную в системе или приложении, чтобы предоставить злоумышленнику доступ к системе. Эксплойты включают переполнение буфера, внедрение кода и эксплойты веб-приложений.

Metasploit Pro предлагает автоматизированные эксплойты и эксплойты, работающие в ручном режиме. Тип используемого вами эксплойта зависит от уровня гранулярного управления, который вы хотите использовать для эксплойтов.

Когда вы запускаете автоматизированный эксплойт, Metasploit Pro строит план атаки на основе имеющейся по целевой системе информации о её службе, операционной системе и уязвимости. Автоматизированные эксплойты перекрестно ссылаются на открытые порты, импортированные уязвимости и данные аутентификации с помощью модулей эксплойтов. План определяет модули эксплойтов, которые Metasploit Pro будет использовать для атаки на целевые системы.

Автоматизированный эксплойт использует обратные соединения или связующие данные для следающего агента, и не злоупотребляет обычными аутентифицированными механизмами управления.

Чтобы запустить автоматизированный эксплойт, вы должны указать хосты, которые хотите использовать, и минимальную надёжность, которую должен использовать Metasploit Pro. Минимальная настройка надёжности указывает на потенциальное воздействие, которое эксплойты оказывают на целевую систему. Если вы используете высокий рейтинг - например, excellent или great - Metasploit Pro применит эксплойты, которые вряд ли смогут привести к сбою службы или системы. Эксплойты, обычно имеющие высокий рейтинг надёжности, включают в себя эксплойты SQL-инъекций, эксплойты веб-приложений и эксплойты выполнения команд. Эксплойты, которые повреждают память, скорее всего не будут иметь высокого рейтинга надёжности.

Вы также можете указать тип нагрузки, который вы хотите использовать. По умолчанию автоматизированные эксплойты используют Meterpreter, но вместо этого вы можете применить командную оболочку.

Автоматизированные эксплойты

Когда вы запускаете автоматизированный эксплойт, Metasploit Pro строит план атаки на основе имеющейся по целевой системе информации о её службе, операционной системе и уязвимости. Автоматизированные эксплойты перекрестно ссылаются на открытые порты, импортированные уязвимости и данные отпечатка пальца с помощью модулей эксплойтов. План определяет модули эксплойтов, которые Metasploit Pro будет использовать для атаки на целевые системы.

Автоматизированный эксплойт использует обратные соединения или связующие данные для следящего агента, и не злоупотребляет обычными аутентифицированными механизмами управления.

Чтобы запустить автоматизированный эксплойт, вы должны указать хосты, которые хотите использовать, и минимальную надёжность, которую должен использовать Metasploit Pro. Минимальная настройка надёжности указывает на потенциальное воздействие, которое эксплойты оказывают на целевую систему. Если вы используете высокий рейтинг - например, excellent или great - Metasploit Pro применит эксплойты, которые вряд ли смогут привести к сбою службы или системы. Эксплойты, обычно имеющие высокий рейтинг надёжности, включают в себя эксплойты SQL-инъекций, эксплойты веб-приложений и эксплойты выполнения команд. Эксплойты, которые повреждают память, скорее всего не будут иметь высокого рейтинга надёжности.

Вы также можете указать тип нагрузки, который вы хотите использовать. По умолчанию автоматизированные эксплойты используют Meterpreter, но вместо этого вы можете применить командную оболочку.

Запуск автоматизированных эксплойтов

1. В рамках проекта перейдите на вкладку **Analysis** («Анализ»).
2. Когда появится окно Hosts, выберите хосты, которые вы хотите использовать, и нажмите кнопку **Exploit**.
3. Когда появится окно New Automated Exploitation Attempt («Новая автоматическая попытка использования»), убедитесь, что в поле целевого адреса указаны адреса, которые вы хотите использовать.
4. Выберите минимальную надёжность для эксплойта.
5. Определите хосты, которые вы хотите исключить из эксплойта.
6. Обозначьте параметры нагрузки. Это определит тип нагрузки, используемой эксплойтом, тип соединения, создаваемого полезной нагрузкой, и порты агента, которые использует эксплойт.
7. Обозначьте параметры выбора эксплойтов. Это определит порты, которые эксплойт включает и исключает из атаки.
8. Обозначьте дополнительные параметры. Они позволят определить количество эксплойтов, которые вы можете запускать одновременно, время ожидания для каждого эксплойта и опции скрытия.
9. Запустите эксплойт.

Настройка параметров автоматического использования эксплойтов

- Dry Run: распечатывает расшифровку эксплойтов в плане атаки без их запуска.
- Collect Evidence: собирает данные - скриншоты, системные файлы, пароли и настройки конфигурации из открытых сеансов.
- Clean Up Sessions: закрывает все сеансы после выполнения всех задач.
- Payload Type: указывает тип нагрузки, которую эксплойт будет оказывать на цель. Выберите один из следующих типов нагрузки:
- **Command**: нагрузка, которая позволяет выполнять команды на удалённой машине.
- **Meterpreter**: продвинутая нагрузка, которая предоставляет вам командную строку, позволяющую вам отправлять команды и добавлять расширения в процессе работы.
- Connection Type: определяет, как Metasploit будет подключаться к цели. Выберите один из следующих типов соединений:
 - **Auto**: автоматически использует соединение привязки при обнаружении NAT; в противном случае используется реверсивное соединение.
 - **Bind**: использует связывание, которое полезно, когда целевые объекты находятся под защитой брандмауэра или за NAT-шлюзом.
 - **Reverse**: использует реверсивное соединение, которое полезно, если ваша система не может инициировать подключения к целевым объектам.
- Listener Ports: определяет порты, которые вам нужно использовать для обратных соединений.
- Listener Host: определяет IP-адрес на который придут ответы агента.
- Auto Launch Macro: задаёт макрос, который вам нужно запустить во время пост-эксплуатации.
- Concurrent Exploits: указывает нужное количество попыток запуска эксплойта одновременно.
- Timeout in Minutes: определяет количество минут, ожидаемых эксплойтом до следующей попытки.
- Transport Evasion: выберите один из следующих уровней избегания трафика:
 - **Low**: вносит задержки между TCP-пакетами.
 - **Medium**: отправляет небольшие TCP-пакеты.
 - **High**: Отправляет небольшие TCP-пакеты и вносит задержки между ними.
- Application Evasion: Настраивает параметры уклонения от конкретных приложений для эксплойтов, связанных с DCERPC, SMB и HTTP. Чем выше уровень, тем больше применяются методы уклонения.
- Included Ports: Определяет конкретные порты, которые вам нужно атаковать эксплойтом.
- Excluded Ports: Определяет конкретные порты, которые вам нужно исключить из эксплойт-атаки.

Эксплойты, работающие в ручном режиме

Эксплойт, работающий в ручном режиме - это модуль, который вы можете выбирать и запускать индивидуально. Вы применяете этот вид эксплойта, когда нужно атаковать некую известную уязвимость.

Вы выбираете модуль эксплойта на основе имеющейся информации о хосте. Например, если вы знаете, что на хосте выполняется Windows Service Pack 1, вы можете запустить эксплойт, нацеленный на уязвимости Windows Service Pack 1. Или, если вы знаете, что целевая система имеет определённую уязвимость, которую вы хотите протестировать, вы можете запустить эксплойт, который нацелен на эту конкретную уязвимость.

Ручное управление обеспечивает детальный контроль над модулем и опциями уклонения, которые использует эксплойт. В то время как автоматизированные эксплойты позволяют одновременно запускать несколько эксплойтов, ручные эксплойты позволяют запускать только один эксплойт.

Параметры и инструкции, которые вы выполняете для ручных эксплойтов, зависят от эксплойта, который вы выбрали для запуска. Поэтому в качестве руководства для ручного запуска эксплойтов используйте следующие инструкции.

Поиск эксплойтов

Модуль поисковой системы ищет в базе данных модуль по ключевым словам, и затем возвращает список результатов, соответствующих запросу. Используйте поисковую систему модуля, чтобы найти модуль, который вам нужно запустить против целевой системы.

1. В рамках проекта перейдите на вкладку Modules («Модули»).
2. В поле Search Modules («Поисковые модули») введите выражение ключевого слова для поиска конкретного эксплойта.
3. Используйте теги ключевых слов для определения выражения ключевого слова.
4. Нажмите Enter («Ввод»), чтобы выполнить поиск.

Запуск автоматизированных эксплойтов

1. В рамках проекта перейдите на вкладку Analysis («Анализ»).
2. Когда появится окно Hosts, выберите хосты, которые вы хотите использовать.
3. Нажмите **Exploit**.
4. Когда появится окно New Automated Exploitation Attempt («Новая автоматическая попытка использования эксплойтов»), убедитесь, что в поле целевого адреса содержатся адреса, которые вы хотите атаковать.
5. Выберите минимальную надёжность для эксплойта.
6. Нажмите **Show Advanced Options** («Показать дополнительные параметры»).
7. Определите целевые хосты, которые вы хотите включить или исключить из эксплойта.
8. Обозначьте параметры нагрузки. Это определит тип полезной нагрузки, используемой эксплойтом, тип соединения, создаваемого нагрузкой, и порты агента, которые использует эксплойт.
9. Обозначьте параметры выбора эксплойтов. Это определит порты, которые эксплойт включает и исключает из атаки.
10. Обозначьте дополнительные параметры. Они позволят определить количество эксплойтов, которые вы можете запускать одновременно, время ожидания для каждого эксплойта и опции скрытия.
11. Запустите эксплойт.

Настройка службы слеящего агента Listener

1. В главном меню выберите **Administration > Global Settings**.
2. Нажмите кнопку **New Listener**, расположенную под кнопкой Persistent Listeners.
3. Когда появится окно Create a Listener, выберите соответствующий проект для агента.

4. Определите тип нагрузки агента.
5. Введите IP-адрес агента.
6. Введите порт агента.
7. Выберите макрос постобработки для развёртывания после того, как агента подключится к целевой системе. Включите агента.
8. Сохраните агента.

Учётные данные

В наши дни всё больше организаций становятся уязвимыми перед внешними угрозами из-за использования «слабых» паролей и небезопасных систем управления паролями. Учётные данные дают вход в различные аккаунты и системы, что потенциально может открыть путь к дополнительным «мишеням» в сети и привести к утечке оттуда конфиденциальной информации. Поэтому, в рамках теста на проникновение, важно обнаружить и предоставить учётные данные, что заставит организации усиливать защиту и больше применять «сложные» пароли - для предотвращения таких уязвимостей, как повторное использование паролей и «слабые» пароли.

В рамках вашего аудита учётных данных вам нужно идентифицировать «слабые» пароли, наиболее часто используемые пароли и высокосложные пароли. Также потребуется повторно использовать актуальные учётные данные, чтобы можно было определить влияние похищенных учётных данных в сети. Это поможет организации понять уровень её безопасности на данный момент, определить, как она может усилить систему использования паролей и обеспечить соблюдение требований к паролям, отвечающих самым передовым методам в данной сфере.

Чтобы вы могли разобраться, как получать, хранить и использовать учётные данные в Metasploit Pro, в следующем разделе будет представлен обзор ключевых понятий и терминов, которые необходимо знать для работы с учётными данными.

Понимание терминологии учётных данных

Как правило, под учётными данными понимаются имя пользователя и пароль. В Metasploit Pro имя пользователя является открытым, а пароль – приватным; поэтому учётные данные могут быть приватными, открытыми, или составлять учётную пару (credential pair).

Подведём итог по ключевым терминам учётных данных:

- Публичным является имя пользователя, используемое для входа в систему.
- Приватным, по сути, является пароль, используемый для аутентификации в системе. Обычно это пароль незашифрованного текста, ключ SSH, хэш NTLM или невоспроизводимый хэш. Поскольку приватными могут быть ключ SSH или хэш, термин «пароль» недостаточно широк, чтобы включать эти приватные типы.
- Учётной парой (credential pair) является комбинация открытых и приватных данных, которая может быть использована для аутентификации в системе.

В дополнение к ключевым терминам, вот некоторые дополнительные, с которыми вам следует ознакомиться:

Приватный тип (Private Type)

Приватный тип ссылается на то, является ли приватным пароль незашифрованного текста, ключ SSH, хэш NTLM или невозпроизводимый хэш.

Невозпроизводимый хэш (Nonreplayable Hash)

Невозпроизводимый хэш - это хэш, который нельзя воспроизвести для аутентификации в сервисах. Например, любой хэш, который был получен из `/etc/passwd` или `/etc/shadow`, - это невозпроизводимый хэш.

Хэш NTLM (NTLM Hash)

Хэш NTLM - это хэш, который можно воспроизвести для аутентификации на SMB.

Область (Realm)

Термин «область» относится к функциональной группировке схем баз данных, к которой принадлежит учётная запись. Типом области может быть директория активного домена (Active Domain Directory), база данных Postgres, база данных DB2 или системный идентификатор Oracle (SID). Открытые, приватные типы данных, учётные пары (credential pairs) могут иметь область, но это не обязательно.

Неполный открытый тип (Incomplete Public)

Неполный открытый тип ссылается на открытые данные, которые не имеют приватной составляющей. Он может иметь область, но это не обязательно.

Неполный приватный тип (Incomplete Private)

Неполный приватный тип ссылается на приватные данные, которые не имеют открытой составляющей. Он может иметь область, но это не обязательно.

Логин (Login)

Термин «логин» относится к имени пользователя и приватной информации, которые связаны с конкретным сервисом. Логин указывает, что вы теоретически можете аутентифицироваться в сервисе, используя учётную пару (credential pair). Metasploit Pro создаёт логины, когда собирает данные с атакуемой цели, и в случае успеха захватывает её. Во время эксплуатации, если хост успешно взломан, Metasploit Pro попытается создать логины на основе типа учётных данных, которые были добыты. Например, если хэши NTLM были получены, то для каждого хэша будет добавлен логин для SMB.

К примеру, учётная пара (credential pair), такая как `admin/admin`, которая может быть использована для аутентификации в сервисе, как Telnet, является логином.

Источник (Origin)

Термин «источник» относится к тому, как учётные данные были получены или добавлены в проект - например, через брутфорс, ручной ввод или импортированный список учётных данных. Источник может быть ручным, импортированным, сеансовым, служебным, или взломанным паролем.

Подтверждённые учётные данные (Validated Credential)

Термин «Подтверждённые учётные данные» относится к учётным данным, которые успешно аутентифицированы в системе-цели.

Чтобы получить учётные данные, вы должны выгрузить их у уязвимой цели. Выгруженные учётные данные можно использовать для попыток дополнительного входа в систему других служб и хостов. Metasploit Pro хранит все выгруженные, импортированные и добавленные вручную учётные данные в проекте.

Получение учётных данных

Существует несколько способов получения учётных данных. Основные методы включают использование уязвимости и сброс учётных данных из уязвимой цели, брутфорсинг целей, используя «слабые» и общие учётные данные по умолчанию, и поиск общедоступных ресурсов для выгрузки учётных данных. Используемый вами метод зависит от уровня доступа к цели, который у вас есть.

Metasploit Pro позволяет использовать множество методов атаки для получения учётных данных - таких как использование уязвимостей. Например, если вы можете обнаружить систему Windows, уязвимую для MS08-067, то можно использовать эту цель и войти в систему для сбора информации у нее. Благодаря доступу к системе вы можете извлекать данные - такие как хэши паролей, пароли незашифрованного текста и токены домена.

Многие информационные системы настроены на использование паролей в качестве первой, а иногда и единственной линии защиты. И часто используются легко отгадываемые или даже пустые пароли. Это означает, что, если у вас есть имя пользователя, вы можете попытаться угадать пароль для входа в цель. Например, учётную запись домена Windows, использующую слабый или пустой пароль, можно легко угадать с помощью Bruteforce.

Кроме того, многие системы сконфигурированы с настройками учётной записи по умолчанию. Эти учётные записи обычно используют один и тот же пароль для нескольких экземпляров, что означает: если вы знаете настройки по умолчанию для одной учётной записи, вы можете использовать эти учётные данные для «прощупывания» также и других целей по всей сети. В этом случае можно вручную добавить общие учётные данные по умолчанию и использовать функцию быстрой проверки (Quick Validation) для данных учётных записей. Если какие-либо учётные данные успешно аутентифицируются для цели, вы можете запустить повторное использование учётных данных (Credential Reuse) для поиска дополнительных целей, для которых эти учётные данные действительны.

Итак, обобщим методы, которые можно использовать для получения учётных данных с помощью Metasploit:

- Вы можете найти уязвимости и использовать их для получения доступа к цели. После того, как у вас есть доступ к цели, вы можете сбросить учётные данные и другую конфиденциальную информацию из атакуемой цели.
- Вы можете запустить Bruteforce, чтобы угадать часто используемые, «слабые» и используемые по умолчанию учётные данные в таких службах как AFP, DB2, FTP, HTTP, HTTPS, MSSQL, MySQL, POP3, PostgreSQL, SMB, SNMP, SSH, Telnet, VNC и WinRM.
- Вы можете вручную добавлять или импортировать учётные данные в проект и запускать Quick Validation или Credential Reuse, чтобы найти цели, которые могут быть аутентифицированы. Этот метод полезен, когда у вас есть набор часто используемых или известных учётных данных, которые вы хотите применить для какой-либо группы целей.

Источники учётных данных

Каждый учётный файл, добавленный в проект, имеет происхождение, которое относится к источнику учётных данных. Учётные данные всегда будут иметь один из следующих источников:

- Мануальное происхождение - указывает, что вы вручную добавили учётные данные в проект с помощью кнопки Add («Добавить») на странице Manage Credentials («Управление учётными данными»).
- Импортированное происхождение - указывает, что вы импортировали учётные данные, загрузив файл CSV или PWDump в проект.
- Служебное происхождение - указывает, что учётные данные были получены с помощью службы Bruteforce.
- Сессионное происхождение - указывает, что учётные данные были собраны во время сессии на обнаруженной цели.
- Происхождение через взлом пароля - указывает, что Metasploit Pro смогла взломать хэш во время сбора данных, и расшифровать пароль незашифрованного текста.

Управление учётными данными

Во время проверки учётных данных вы будете собирать конфиденциальные данные у своих целей и управлять ими со страницы управления учётными данными (Manage Credentials). Там отображаются все учётные данные, доступные в конкретном проекте, и предоставляется доступ к функциям, которые позволяют добавлять, удалять и экспортировать учётные данные. В следующих разделах вы узнаете, как управлять учётными данными в рамках проекта.

Добавление учётных данных

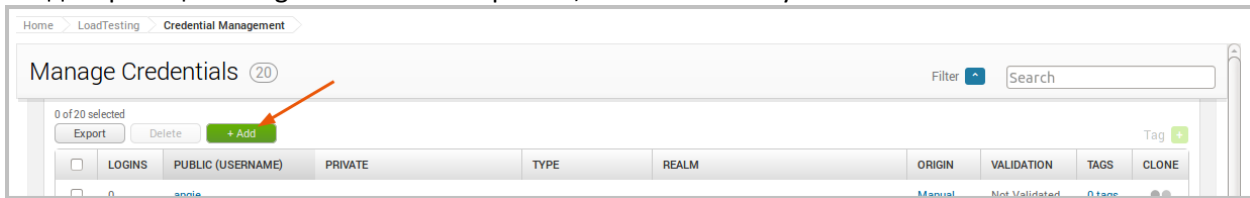
Чтобы добавить учётные данные в проект, вы можете вводить вручную отдельно каждый учётный файл, либо импортировать файл PWDump или CSV. В следующих разделах показано, как вручную добавить пароль незашифрованного текста, ключ SSH, хэш NTLM и невоспроизводимый хэш.

Ввод пароля вручную

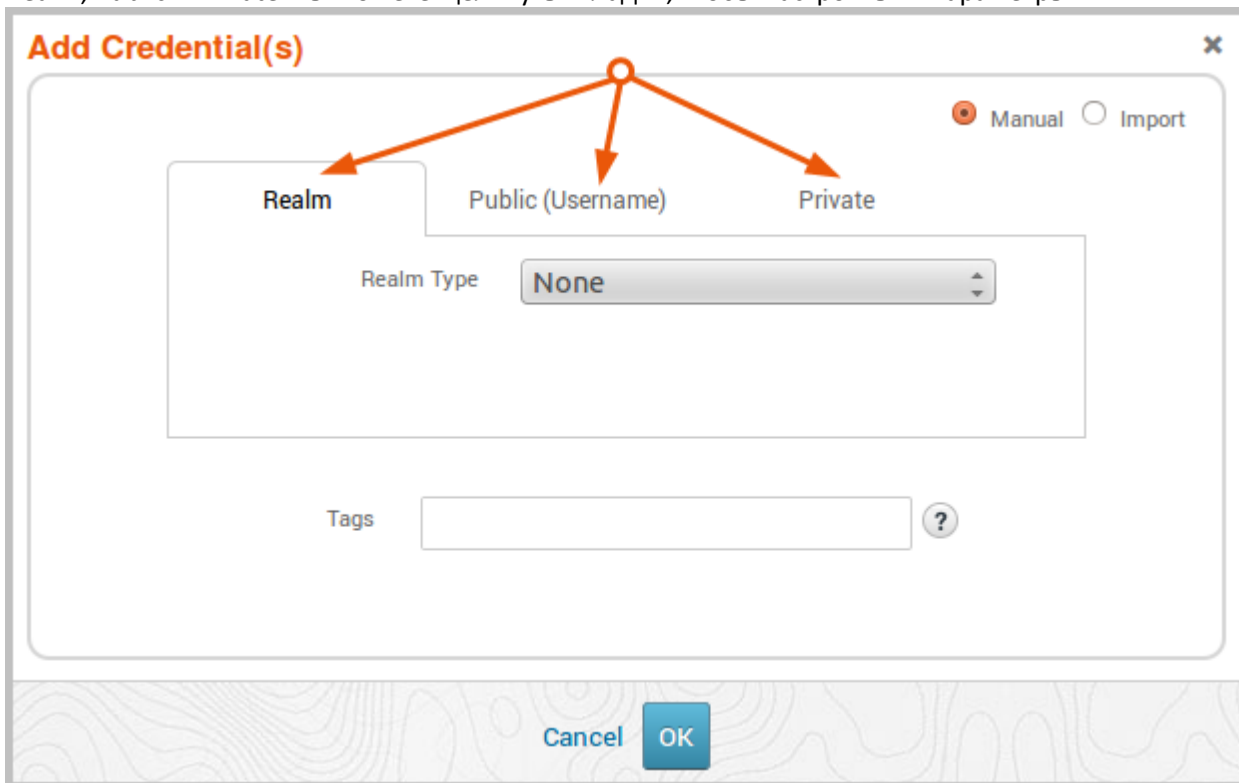
Вы можете вручную добавить пароль, когда у вас есть один пароль незашифрованного текста, который нужно добавить в проект – например, обычный по умолчанию, как admin/admin. Если у вас есть несколько учётных данных, которые вы хотите добавить, вы должны создать для них файл CSV

и импортировать их в проект. Импорт учётных данных в этом конкретном случае будет намного более эффективным.

1. В рамках проекта перейдите в **Credentials > Manage** для доступа к области Manage Credentials.
2. Когда страница Manage Credentials откроется, нажмите кнопку **Add**.



Появится окно **Add Credentials**, и отобразятся вкладки для трёх разных частей учётных данных: Realm, Public и Private. Вы можете щёлкнуть вкладки, чтобы настроить их параметры.



3. Нажмите вкладку **Private (Passwords)**.
4. Нажмите выпадающее меню **Credential Type** и выберите **Plaintext Password**.

Add Credential(s) [X]

Manual ☒ Import ☐

Realm Public (Username) Private

Private type Plaintext Password

Password admin

Tags [] ?

Cancel OK

5. Введите пароль в поле **Password**.
6. Нажмите вкладку **Public (Username)** и введите имя пользователя. Если вы его не введёте, имя пользователя будет *BLANK*. (Необязательно)

Add Credential(s) [X]

Manual ☒ Import ☐

Realm Public (Username) Private

Public (Username) admin

Tags [] ?

Cancel OK

7. Нажмите вкладку **Realm** и выберите один из следующих типов областей: None, Active Directory Domain, Postgres DB, DB2 или Oracle SID. (Необязательно). Если вы не знаете область, можно использовать значение по умолчанию «None».

8. Если вы выбрали тип области, введите его имя в поле **Realm Name**. (Необязательно)
9. Введите теги для учётной пары (credential pair). (Необязательно)

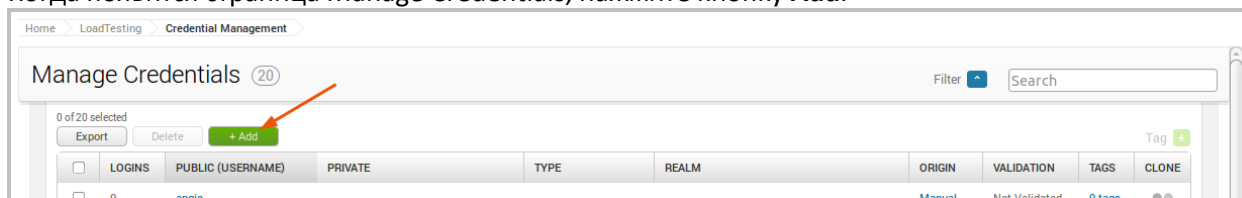
Чтобы ввести тег, начните печатать его имя в поле **Tag**. Пока вы печатаете, Metasploit Pro автоматически подсказывает теги, которые могут быть похожи на те, которые вы ищете. Если такого тега не существует, Metasploit Pro создаст его.

10. Нажмите **OK**.

Пароль добавлен в проект и становится доступен для просмотра на странице Manage Credentials.

Добавление приватного ключа SSH вручную

1. В рамках проекта перейдите в **Credentials > Manage** для доступа к области Manage Credentials.
2. Когда появится страница Manage Credentials, нажмите кнопку **Add**.



Появится окно **Add Credentials**, и отобразятся вкладки для трёх разных частей учётных данных: Realm, Public и Private. Вы можете щёлкнуть вкладки, чтобы настроить их параметры.

Add Credential(s)

Manual ☒ Import ☐

Realm Public (Username) Private

Realm Type **None**

Tags

Cancel OK

3. Нажмите вкладку **Private (Passwords)**.
4. Нажмите выпадающее меню **Credential Type** и выберите **SSH Key**.

Add Credential(s)

Manual ☒ Import ☐

Realm Public (Username) Private

Private type **SSH Key**

SSH Key

```

-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAM1zHfbSBercDZmY
onRwrosFmRRgdfgfdgr/vYouaoziM8
Uv1xx7
wnl f38Y6x8P7nShD1W8.IPvIWKHRd
-----END RSA PRIVATE KEY-----

```

Tags

Cancel OK

5. Скопируйте содержимое приватного SSH-ключа и вставьте его в поле **SSH Key**. Ключ должен начинаться с -----BEGIN RSA PRIVATE KEY----- и заканчиваться на -----END RSA PRIVATE KEY-----.
6. Введите теги для SSH-ключа. (Необязательно)
Чтобы ввести тег, начните печатать его имя в поле **Tag**. Пока вы печатаете, Metasploit Pro автоматически подсказывает теги, которые могут быть похожи на те, которые вы ищете. Если такого тега не существует, Metasploit Pro создаст его.

- Нажмите вкладку **Public (Username)** и введите имя пользователя. Все SSH-ключи должны иметь имя пользователя.

Add Credential(s)

Manual ☒ Import ☐

Realm Public (Username) Private

Public (Username)

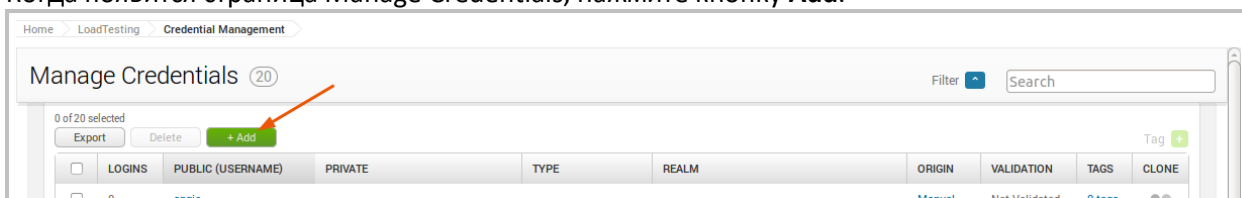
Tags ?

Cancel OK

- Нажмите **OK**.
Ключ SSH добавлен в проект и доступен для просмотра на странице Manage Credentials.

Добавление хэша NTLM вручную

- В рамках проекта перейдите в **Credentials > Manage** для доступа к области Manage Credentials.
- Когда появится страница Manage Credentials, нажмите кнопку **Add**.



Появится окно **Add Credentials**, и отобразятся вкладки для трёх разных частей учётных данных: Realm, Public и Private. Вы можете щёлкнуть вкладки, чтобы настроить их параметры.

Add Credential(s)

Manual ☒ Import ☐

Realm Public (Username) Private

Realm Type: None

Tags:

Cancel OK

3. Нажмите вкладку **Private (Passwords)**.
4. Нажмите выпадающее меню **Credential Type** и выберите **NTLM Hash**.

Add Credential(s)

Manual ☒ Import ☐

Realm Public (Username) Private

Private type: NTLM Hash

NTLM Hash: aad3b435b51404eeaad3b435b5140ee:daf8f5e499bb9da2a3ff8f2a399040be

Tags:

Cancel OK

5. Скопируйте хэш и вставьте его в поле **NTLM Hash**.
 Действительный хэш NTLM использует следующий формат: <LAN Manager hex digest>:<NT LAN Manager hex digest>, где каждый шестнадцатеричный дайджест - это 32 строчных шестнадцатеричных символа. Например, для хэша NTLM допустимым вводом для является следующий:
aad3b435b51404eeaad3b435b5140ee:daf8f5e499bb9da2a3ff8f2a399040be.

- Нажмите вкладку **Public (Username)** и введите имя пользователя. Если вы его не введёте, имя пользователя будет ***BLANK***. (Необязательно)

Add Credential(s)

Manual ☒ Import ☐

Realm Public (Username) Private

Public (Username)

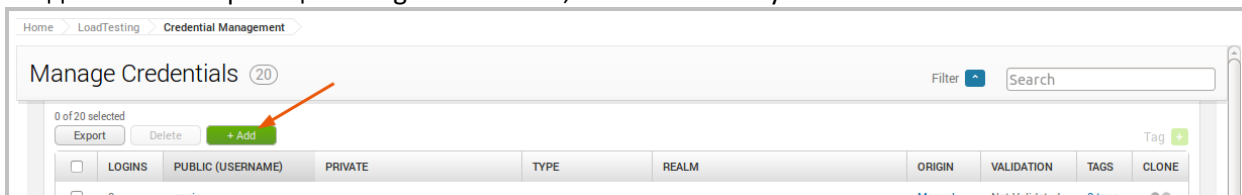
Tags ?

Cancel OK

- Нажмите вкладку **Realm** и выберите один из следующих типов областей: None, Domain Name, Postgres DB, DB2 или Oracle SID. (Необязательно)
- Если вы указали тип области и знаете его имя, введите его в поле **Realm Name**.
- Введите теги для хэша NTLM. (Необязательно)
Чтобы ввести тег, начните печатать его имя в поле **Tag**. Пока вы печатаете, Metasploit Pro автоматически подсказывает теги, которые могут быть похожи на те, которые вы ищете. Если такого тега не существует, Metasploit Pro создаст его.
- Нажмите **OK**.
Хэш NTLM добавлен в проект и доступен для просмотра на странице Manage Credentials.

Добавление неповторяющегося хэша вручную

- В рамках проекта перейдите в **Credentials > Manage** для доступа к области Manage Credentials.
- Когда появится страница Manage Credentials, нажмите кнопку **Add**.



Появится окно **Add Credentials**, и отобразятся вкладки для трёх разных частей учётных данных: Realm, Public и Private. Вы можете щёлкнуть вкладки, чтобы настроить их параметры.

Add Credential(s)

Manual ☒ Import ☐

Realm Public (Username) Private

Realm Type **None**

Tags

Cancel OK

3. Нажмите вкладку **Private (Passwords)**.
4. Нажмите выпадающее меню **Credential Type** и выберите **Hash**.

Add Credential(s)

Manual ☒ Import ☐

Realm Public (Username) Private

Private type **Hash**

Hash 40bdee771d42eb80d47a7d34ed7fc0a318927197

Tags

Cancel OK

5. Скопируйте хэш и вставьте его в поле **Hash**.
6. Нажмите вкладку **Public (Username)** и введите имя пользователя.

Если вы его не введёте, имя пользователя будет *BLANK*. (Необязательно)

7. Нажмите вкладку **Realm** и выберите один из следующих типов областей: None, Domain Name, Postgres DB, DB2, or Oracle SID. (Необязательно)
8. Если вы указали тип области, введите его имя в поле **Realm Name**.
9. Введите теги для хэша. (Необязательно)

Чтобы ввести тег, начните печатать его имя в поле **Tag**. Пока вы печатаете, Metasploit Pro автоматически подсказывает теги, которые могут быть похожи на те, которые вы ищете. Если такого тега не существует, Metasploit Pro создаст его.

10. Нажмите **OK**.

Ключ SSH добавлен в проект и доступен для просмотра на странице Manage Credentials.

Импорт и экспорт учётных данных

Вы можете импортировать и экспортировать учётные данные, чтобы легко делиться ими между проектами или с другими членами организации. Очень важно, чтобы эта конфиденциальная информация была разделена ответственно, поскольку она может содержать учётные данные нешифрованного текста и чрезвычайно конфиденциальные данные.

Учётные данные можно импортировать парой способов. Вы можете импортировать их как часть рабочего пространства ZIP, в котором автоматически будут указаны все учётные данные, содержащиеся в экспорте, а также любые другие данные, которые были частью проекта. Файлы ZIP рабочей области можно импортировать со страниц Hosts или Overview. Если вы хотите импортировать только учётные данные, вам нужно будет сделать это на странице Manage Credentials. Вы можете импортировать учётные данные, которые были экспортированы из проекта, или импортировать список учётных данных, который вы создали вручную.

Когда вы экспортируете учётные данные из проекта, Metasploit Pro создаёт файл манифеста, который содержит учётные данные, и сжимает его в ZIP-файл. Файл манифеста представляет собой файл CSV, в котором перечислены все учётные данные в проекте, и включает следующую

информацию для всех учётных данных: имя пользователя, частный тип, тип области, имя домена, адрес хоста, служебный порт, служба и служебный протокол. Если проект содержит SSH-ключи, они будут включены в экспортированный файл. Каждый ключ SSH будет сопоставлен с соответствующим именем пользователя в файле манифеста.

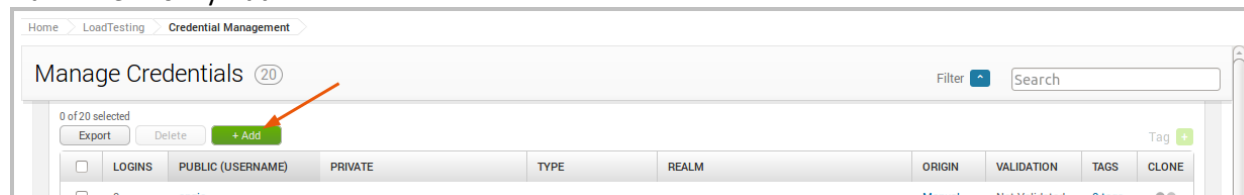
Чтобы помочь вам понять, как можно делиться учётными данными, следующие разделы расскажут, как их импортировать и экспортировать.

Импорт учётных данных, экспортируемых из других проектов

Когда вы экспортируете учётные данные из проекта, Metasploit Pro создаёт файл манифеста, который представляет собой файл CSV, который содержит все учётные данные проекта, и сжимает его в ZIP-файл. Если вы хотите импортировать учётные данные, которые были экспортированы из другого проекта, вы должны импортировать ZIP-файл рабочей области. Это гарантирует, что файл содержит требуемую строку заголовка, которая нужна Metasploit Pro для того, чтобы правильно импортировать учётные и любые другие дополнительные данные - такие как ключи SSH, связанные с файлом манифеста. Вы не можете просто импортировать файл manifest.csv; при попытке импортировать файл манифеста, созданный Metasploit Pro, импорт завершится неудачно.

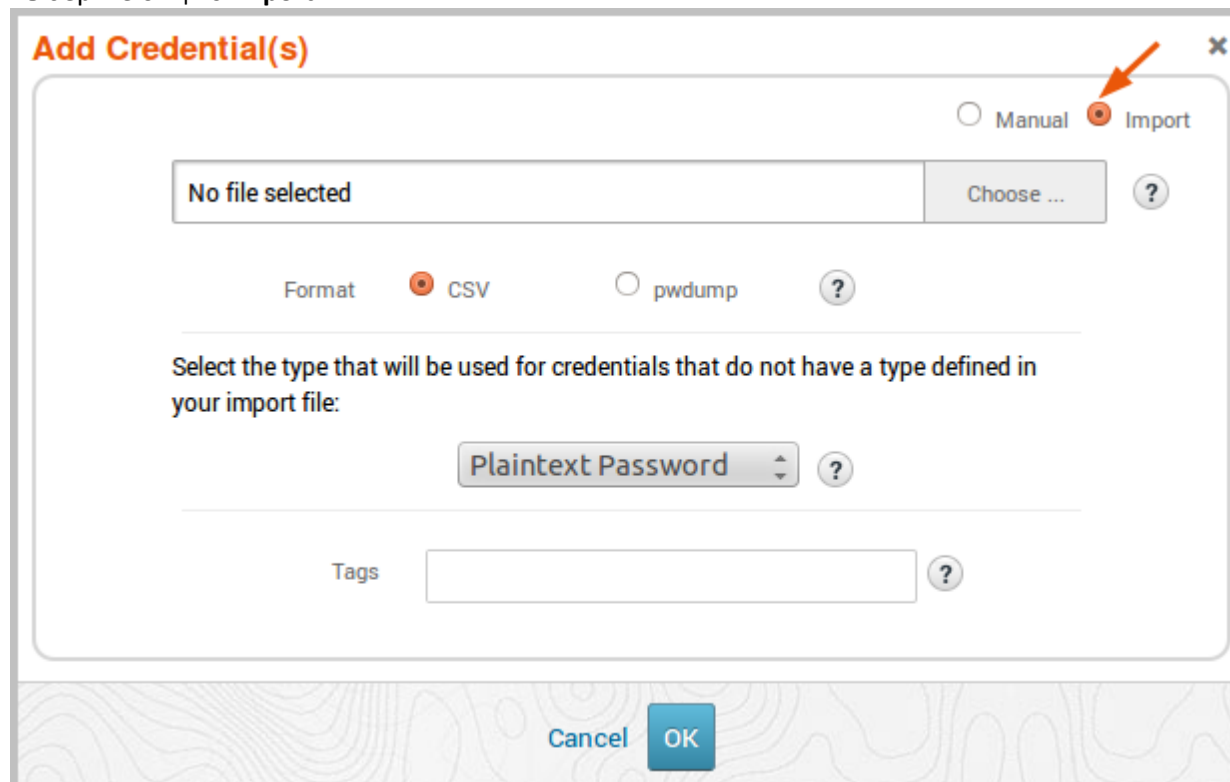
Чтобы импортировать экспортированные учётные данные:

1. В рамках проекта перейдите в **Credentials > Manage** для доступа к области Manage Credentials.
2. Нажмите кнопку **Add**.

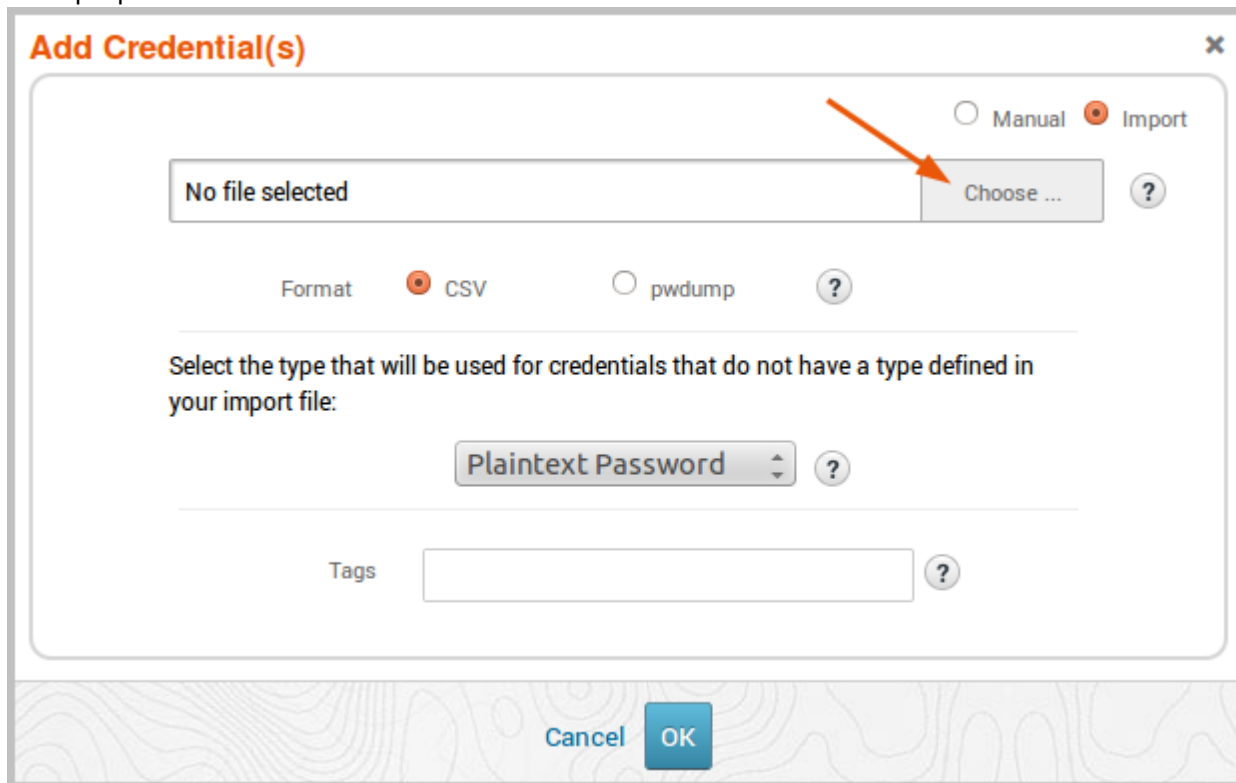


Появится окно **Add Credentials**.

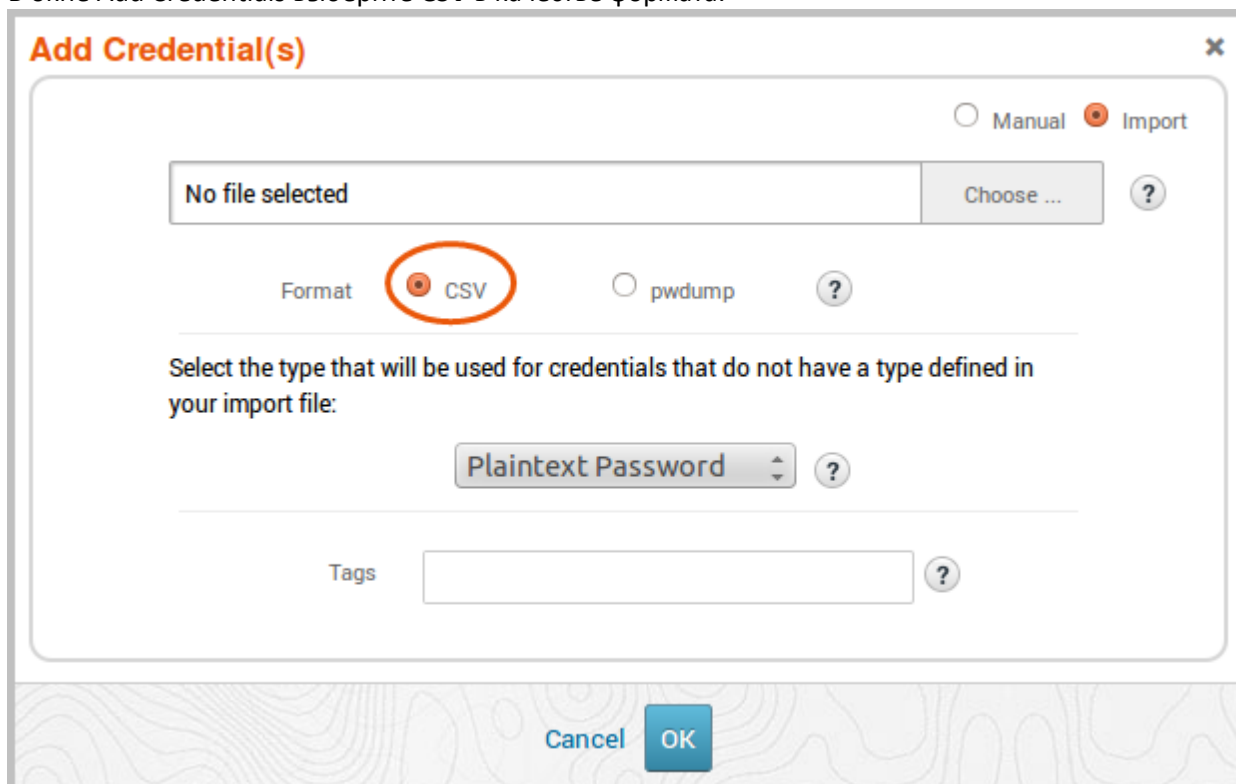
3. Выберите опцию **Import**.



4. Нажмите кнопку **Choose** и перейдите в местоположение ZIP-файла, который вы хотите импортировать.



5. Выберите файл и нажмите **Open**.
6. В окне Add Credentials выберите **CSV** в качестве формата.



7. Нажмите выпадающее меню **Password Type** и выберите тип, который вы хотите назначить учётным данным, не имеющим тип, определённый в вашем файле импорта. Любые учётные данные, содержащие приватный тип данных, должны иметь тип, определённый для него. Этот параметр

позволяет вам установить тип по умолчанию для всех учётных данных, имеющих тип пустого поля в файле импорта.

- Введите теги для учётной пары (credential pair). (Необязательно)

Чтобы ввести тег, начните печатать его имя в поле **Tag**. Пока вы печатаете, Metasploit Pro автоматически подсказывает теги, которые могут быть похожи на те, которые вы ищете. Если такого тега не существует, Metasploit Pro создаст его.

- Нажмите **ОК**.

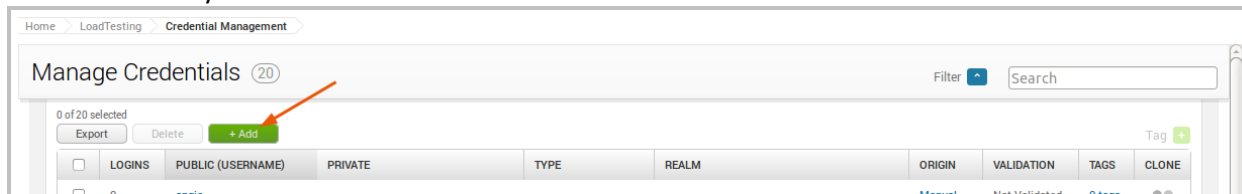
CSV-файл импортирован в проект. Вы можете перейти на страницу Manage Credentials, чтобы просмотреть импортированные учётные данные.

Импорт созданного вручную файла учётных данных

Если у вас есть список учётных данных, который вы создали вручную, его можно импортировать на странице Manage Credentials. Загружаемый файл учётных данных должен быть CSV-файлом, который содержит следующую строку заголовка: username,private_data.

Чтобы импортировать созданный вручную файл учётных данных:

- В рамках проекта перейдите в **Credentials > Manage** для доступа к области Manage Credentials.
- Нажмите кнопку **Add**.



Появится окно **Add Credentials**.

- Выберите опцию **Import**.

Add Credential(s)

☐ Manual ☒ Import

No file selected Choose ...

Format ☒ CSV ☐ pwdump

Select the type that will be used for credentials that do not have a type defined in your import file:

Plaintext Password

Tags

Cancel OK

- Нажмите кнопку **Choose** и перейдите в местоположение CSV-файла, который вы хотите импортировать.

Add Credential(s)

☐ Manual ☒ Import

No file selected Choose ...

Format ☒ CSV ☐ pwdump

Select the type that will be used for credentials that do not have a type defined in your import file:

Plaintext Password

Tags

Cancel OK

CSV-файл должен содержать следующую строку заголовка: username,private_data.

- Выберите файл и нажмите **Open**.
- В окне Add Credentials выберите **CSV** в качестве формата.

Add Credential(s)

☐ Manual ☒ Import

No file selected Choose ... ?

Format ☒ **CSV** ☐ pwdump ?

Select the type that will be used for credentials that do not have a type defined in your import file:

Plaintext Password ?

Tags ?

Cancel OK

- Введите теги для учётной пары (credential pair). (Необязательно)
Чтобы ввести тег, начните печатать его имя в поле **Tag**. Пока вы печатаете, Metasploit Pro автоматически подсказывает теги, которые могут быть похожи на те, которые вы ищете. Если такого тега не существует, Metasploit Pro создаст его.
- Нажмите **OK**.

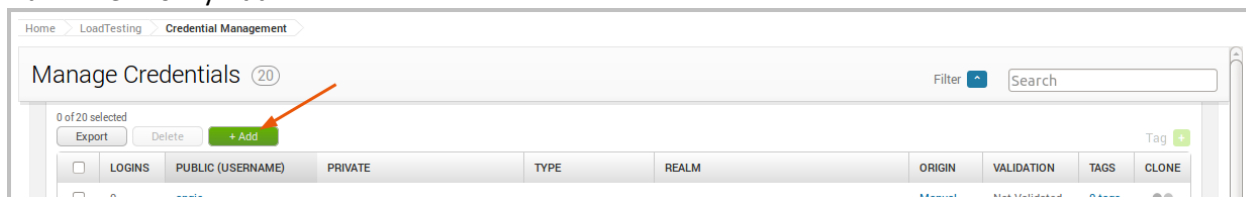
CSV-файл импортирован в проект. Вы можете перейти на страницу Manage Credentials, чтобы просмотреть импортированные учётные данные.

Импорт файла PWDump

PWDump – текстовый файл, содержащий учётные данные, имеющие логины, связанные с ними. Файл PWDump, который вы загружаете, должен быть экспортирован из Metasploit Pro. Другие типы дампов паролей не поддерживаются.

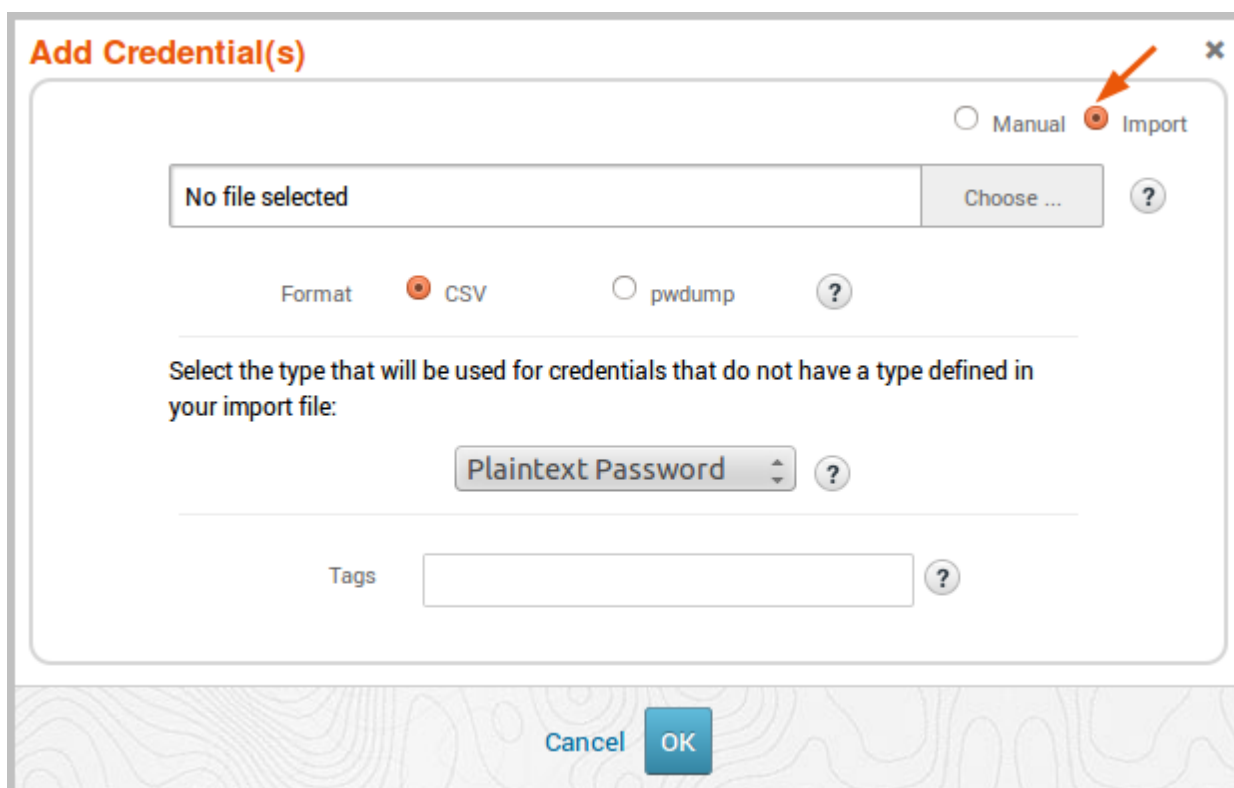
Чтобы импортировать файл PWDump:

- В рамках проекта перейдите в **Credentials > Manage** для доступа к области Manage Credentials.
- Нажмите кнопку **Add**.



Появится окно **Add Credentials**.

- Выберите опцию **Import**.



Add Credential(s)

☐ Manual ☒ Import

No file selected Choose ... ?

Format ☒ CSV ☐ pwdump ?

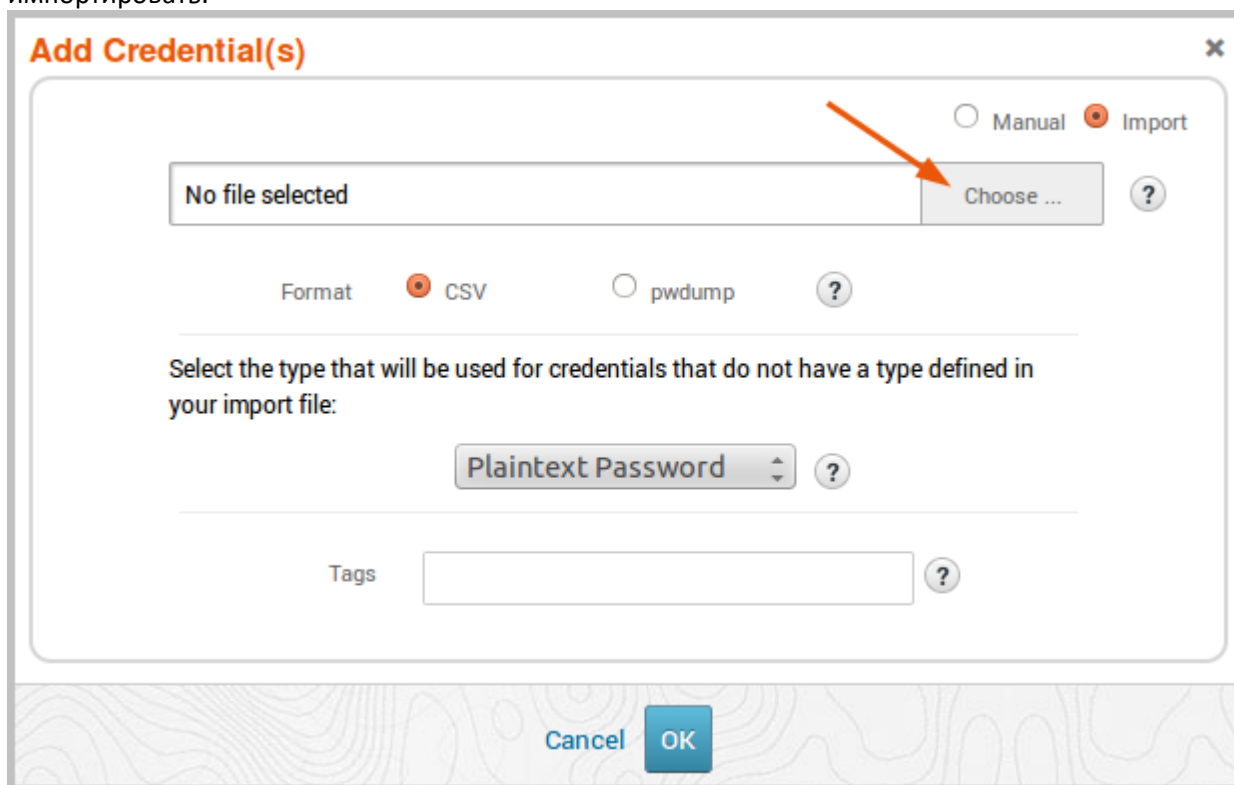
Select the type that will be used for credentials that do not have a type defined in your import file:

Plaintext Password ?

Tags ?

Cancel OK

4. Нажмите кнопку **Browse** и перейдите к местоположению файла PWDump, который вы хотите импортировать.



Add Credential(s)

☐ Manual ☒ Import

No file selected Choose ... ?

Format ☒ CSV ☐ pwdump ?

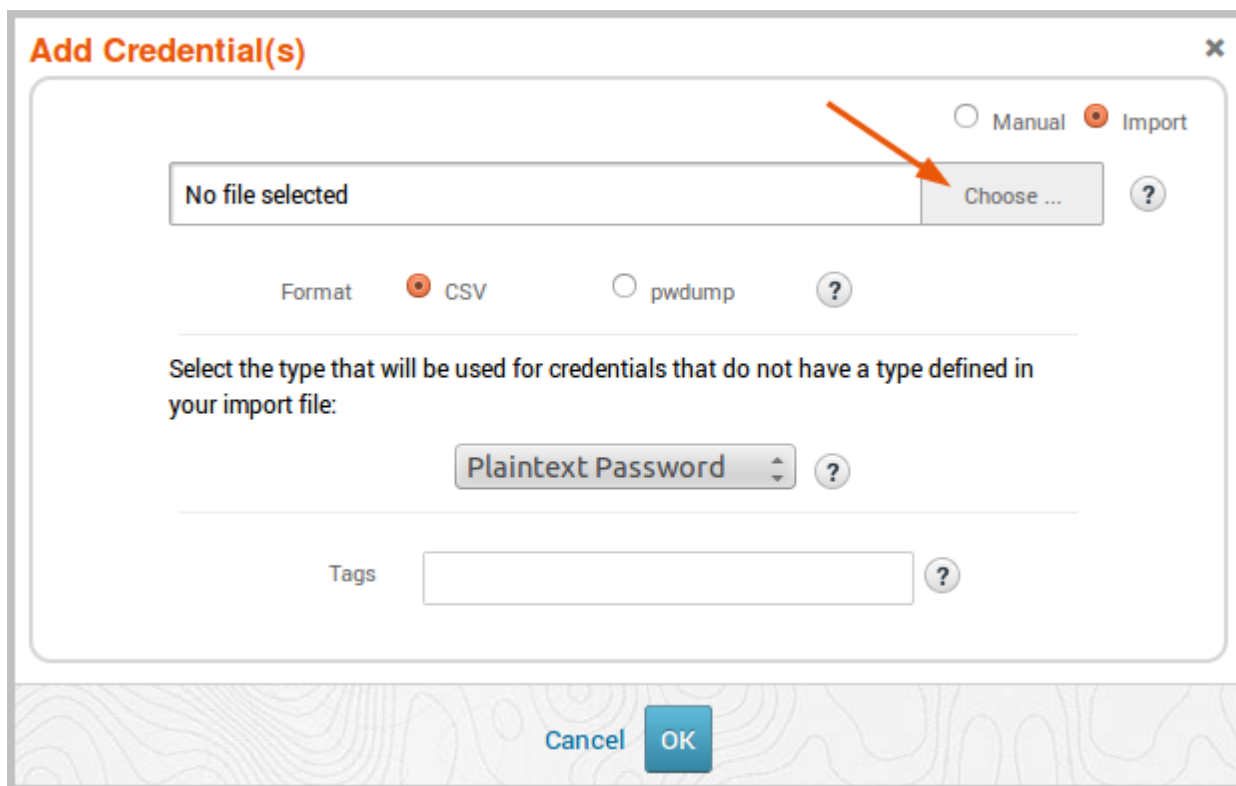
Select the type that will be used for credentials that do not have a type defined in your import file:

Plaintext Password ?

Tags ?

Cancel OK

5. Выберите файл и нажмите **Open**.
6. Выберите формат **pwdump**.



7. Введите теги для учётной пары (credential pair). (Необязательно)
Чтобы ввести тег, начните печатать его имя в поле **Tag**. Пока вы печатаете, Metasploit Pro автоматически подсказывает теги, которые могут быть похожи на те, которые вы ищете. Если такого тега не существует, Metasploit Pro создаст его.
8. Нажмите **OK**.

PWDump-файл импортирован в проект. Вы можете перейти на страницу Manage Credentials, чтобы просмотреть импортированные учётные данные.

Экспорт всех учётных данных

Существует несколько способов экспорта всех учётных данных из проекта. Вы можете сделать это на уровне проекта путём экспорта ZIP-файла рабочей области, который будет содержать всю информацию, хранящуюся в проекте - такую как данные хоста, собранные данные и отчёты, а также папку, содержащую учётные данные.

Если вы хотите экспортировать только учётные данные из проекта, вы можете экспортировать их со страницы Manage Credentials. Когда вы экспортируете учётные данные, Metasploit Pro создаёт файл манифеста и автоматически сжимает его в ZIP-файл, что позволяет вам импортировать файл без дополнительных изменений.

Чтобы экспортировать все учётные данные:

1. В рамках проекта перейдите в **Credentials > Manage** для доступа к области Manage Credentials. Нажмите кнопку **Export**.
3. Введите имя файла в поле **File Name**, если вы хотите указать придуманное вами имя. В противном случае будет использовано автоматически сгенерированное имя файла.

Export [X]

File Name:

Format: ☒ CSV ☐ pwdump (logins only)

Rows: ☐ Selected ☒ All

Cancel OK

4. Для параметра **Format** выберите CSV.

Export [X]

File Name:

Format: ☒ CSV ☐ pwdump (logins only)

Rows: ☐ Selected ☒ All

Cancel OK

5. Для параметра **Row** выберите All.

Export [X]

File Name:

Format: ☒ CSV ☐ pwdump (logins only)

Rows: ☐ Selected ☒ All

Cancel OK

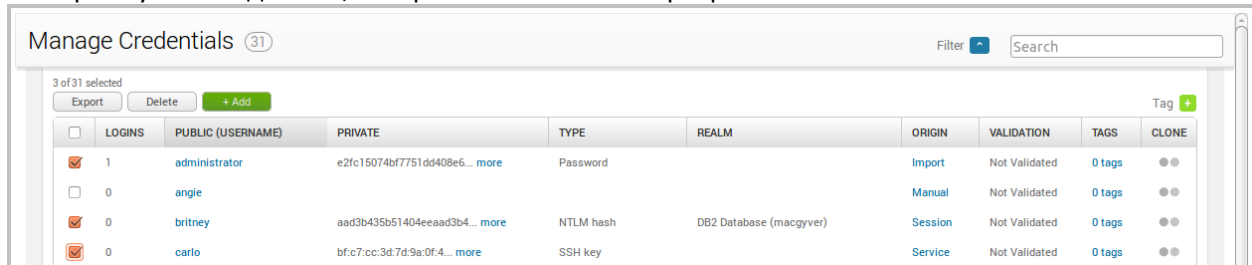
6. Нажмите **OK**, чтобы начать экспорт.

Экспорт начнётся автоматически. Ваша система может предложить вам сохранить файл, если она не настроена для автоматической загрузки.

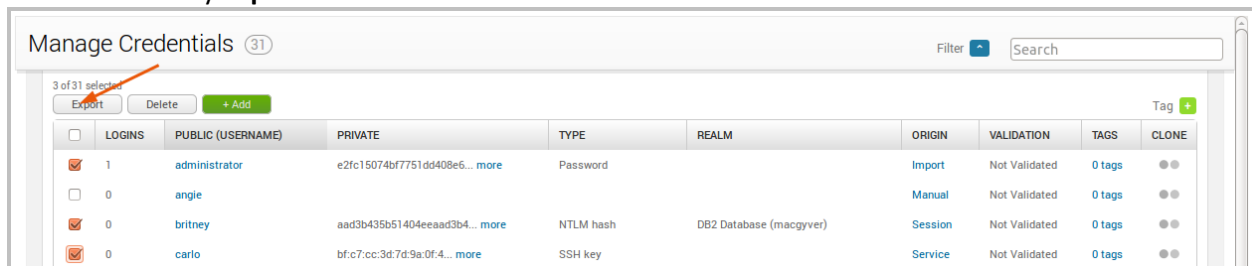
Экспорт выбранных учётных данных

Вы можете экспортировать определённые учётные данные из проекта на странице Manage Credentials.

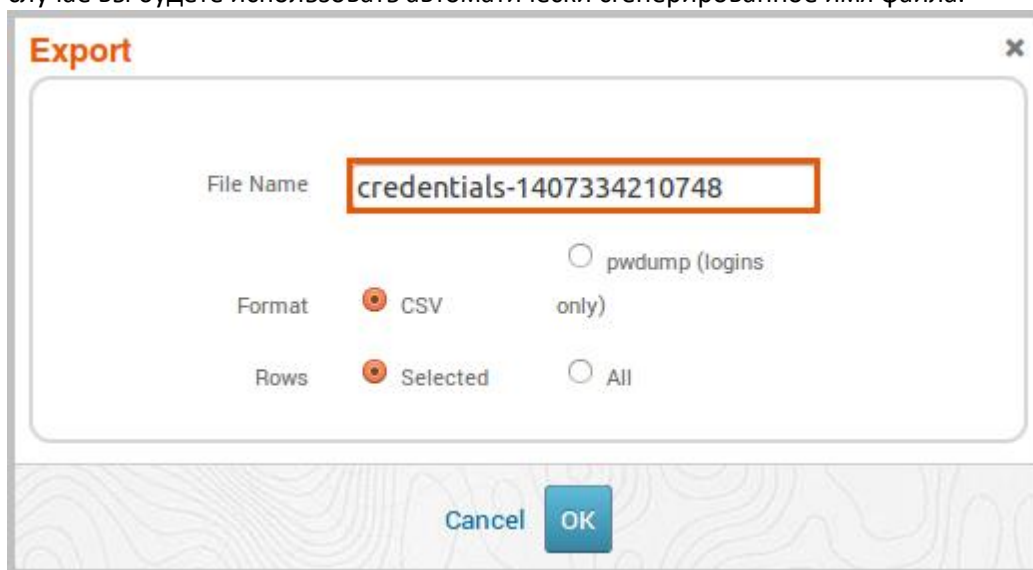
1. В рамках проекта перейдите в **Credentials > Manage** для доступа к области Manage Credentials.
2. Выберите учётные данные, которые вы хотите экспортировать.



3. Нажмите кнопку **Export**.



4. Введите имя файла в поле **File Name**, если вы хотите указать придуманное вами имя. В противном случае вы будете использовать автоматически сгенерированное имя файла.



5. Для параметра **Format** выберите CSV.

Export

File Name:

Format: ☒ CSV ☐ pwdump (logins only)

Rows: ☒ Selected ☐ All

Cancel OK

6. Для параметра **Row** выберите Selected.

Export

File Name:

Format: ☒ CSV ☐ pwdump (logins only)

Rows: ☒ Selected ☐ All

Cancel OK

7. Нажмите **OK**, чтобы начать экспорт.

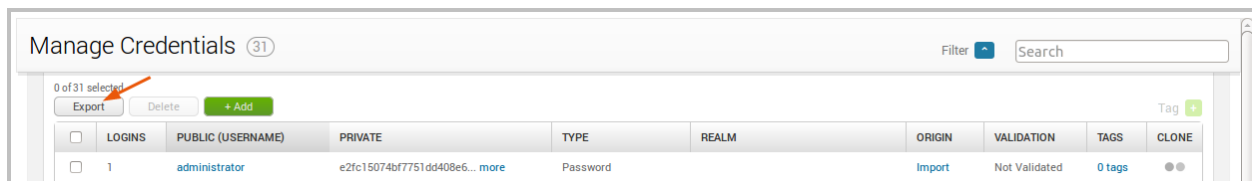
Экспорт начнётся автоматически. Ваша система может предложить вам сохранить файл, если она не настроена для автоматической загрузки.

Экспорт файла PWDump

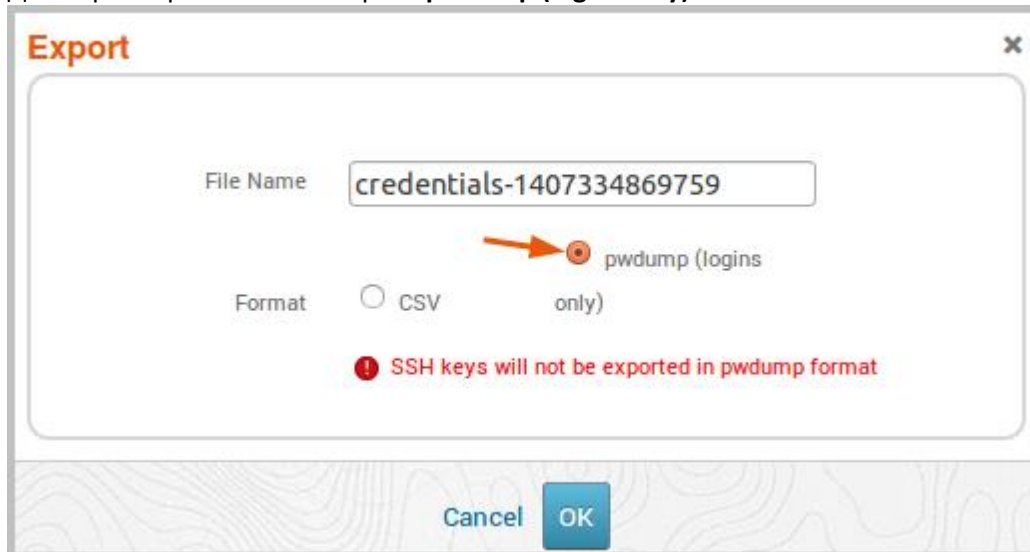
PWDump - это тип экспорта в Metasploit Pro, который работает только с учётными данными, имеющими логин. Metasploit Pro экспортирует PWDump как текстовый файл, который может быть импортирован в другие проекты.

Чтобы экспортировать PWDump:

1. В рамках проекта перейдите в **Credentials > Manage** для доступа к области Manage Credentials.
2. Нажмите кнопку **Export**.



3. Для параметра **Format** выберите **pwdump (logins only)**.



4. Нажмите **ОК**, чтобы начать экспорт.

Экспорт начнётся автоматически. Ваша система может предложить вам сохранить файл, если она не настроена для автоматической загрузки.

Создание файла учётных данных CSV для импорта

Вы можете создавать CSV-файлы для импорта учётных данных в проект. Например, если у вас есть список слов или паролей, которые вы хотите добавить в проект, вам нужно будет создать файл CSV для этих учётных данных. Для создания файла CSV вы можете использовать программу для работы с электронными таблицами – например, Microsoft Excel или Google Docs.

Файл CSV должен содержать в головном ряду username, private_data, что определит распределение полей в таблице. На следующем рисунке показан пример списка учётных данных, который был создан в Microsoft Excel:

	A	B
1	username	private_data
2	administrator	administrator
3	guest	guest
4	username	password
5	admin	admin
6	root	
7		password

Как вы можете видеть, первая строка содержит головной ряд. Следующие строки содержат данные, указанные каждым заголовком. Если вы хотите оставить имя пользователя или пароль пустыми, вы можете ничего не вводить.

Когда вы закончите создание файла, вам нужно будет сохранить его с расширением .csv, чтобы можно было импортировать его в проект. Сведения о том, как импортировать CSV-файл в проект, см. в разделе «[Импорт и экспорт учётных данных](#)».

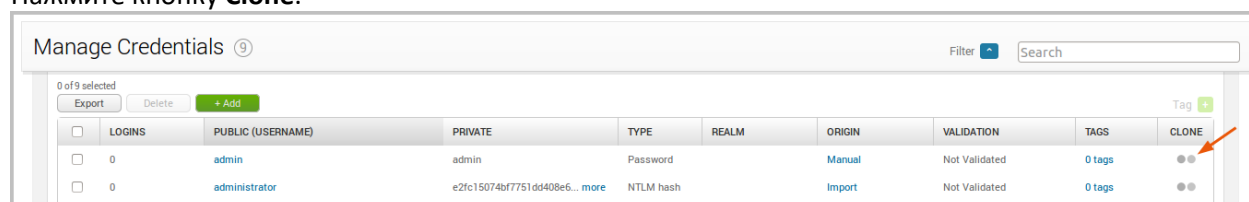
Клонирование и редактирование учётных данных

Клонирование - полезная функция, если вы хотите сделать копию учётных данных с некоторыми незначительными изменениями. Например, если у вас есть учётная пара (credential pair), например admin:admin, вы можете добавить вариант, например admin1:admin1. Самый быстрый способ сделать это - клонировать оригинальную пару учётных данных и настроить публичные и приватные данные для неё.

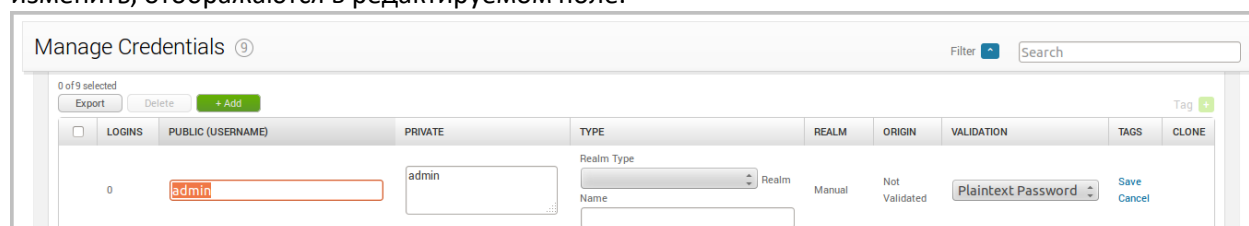
Примечание: Учётные данные не могут быть изменены после сохранения их в проекте. Единственный способ редактировать учётные данные – это клонировать и изменять их. Если есть изменения, которые необходимо внести в учётные данные, вам нужно будет клонировать их, редактировать клон, сохранить клон и удалить оригинальные учётные данные.

Чтобы клонировать учётные данные:

1. В рамках проекта перейдите в **Credentials > Manage** для доступа к области Manage Credentials. Когда появится страница Manage Credentials, найдите строку, содержащую учётные данные, которые вы хотите клонировать.
3. Нажмите кнопку **Clone**.



Дубликат учётных данных создаётся и добавляется в таблицу. Любые данные, которые вы можете изменить, отображаются в редактируемом поле.



4. Отредактируйте любое из следующих полей: Public (имя пользователя), Private (пароль), Realm, Origin и Password Type. Вы должны изменить одно из полей, потому что проект не может содержать дубликаты точной записи учётных данных. Вы не сможете сохранить учётные данные, если они не уникальны. Например, у вас может быть две записи для admin/admin, пока область или приватный тип различны.
5. Нажмите **Save**, когда закончите.

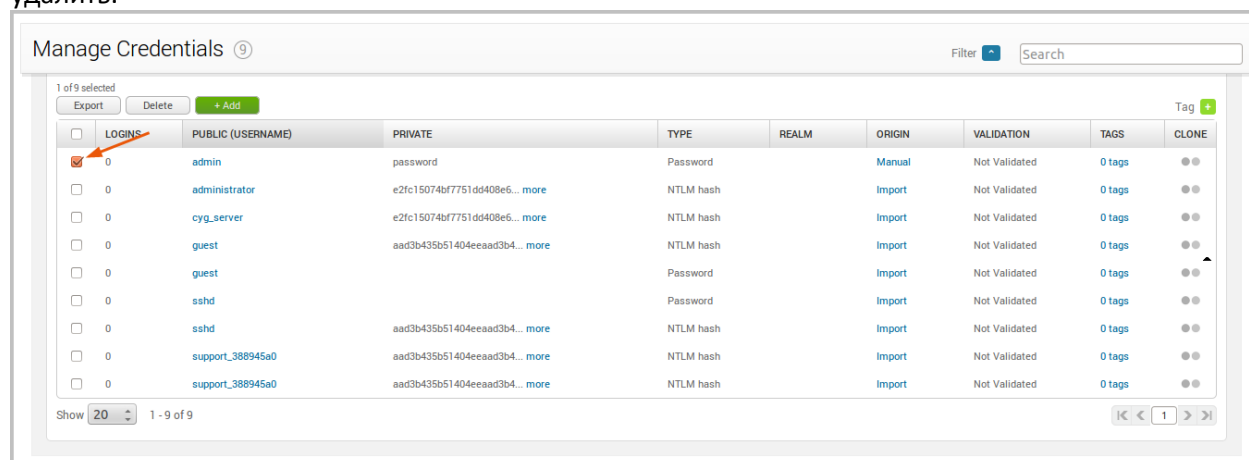
Учётные данные добавлены в проект и отображаются на странице Manage Credentials.

Удаление учётных данных

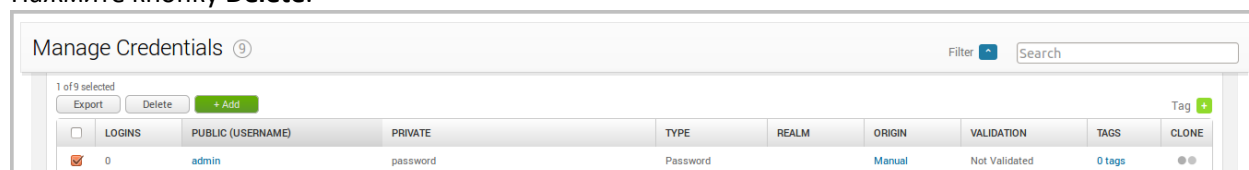
Если есть учётные данные, которые вам больше не нужно хранить в проекте, их можно удалить. Они удаляются из проекта навсегда, и не могут быть восстановлены.

- 1) В рамках проекта перейдите в **Credentials > Manage** для доступа к области Manage Credentials.

Когда появится страница Manage Credentials, выберите учётные данные, которые вы хотите удалить.



3) Нажмите кнопку **Delete**.



Когда появится окно подтверждения, нажмите «ОК», чтобы удалить учётные данные из рабочей области. Учётные данные, включая все их логины, будут удалены из проекта. Вы должны быть абсолютно уверены, что хотите удалить учётные данные. Вы не сможете восстановить удалённые учётные данные.

Повторное использование учётных данных

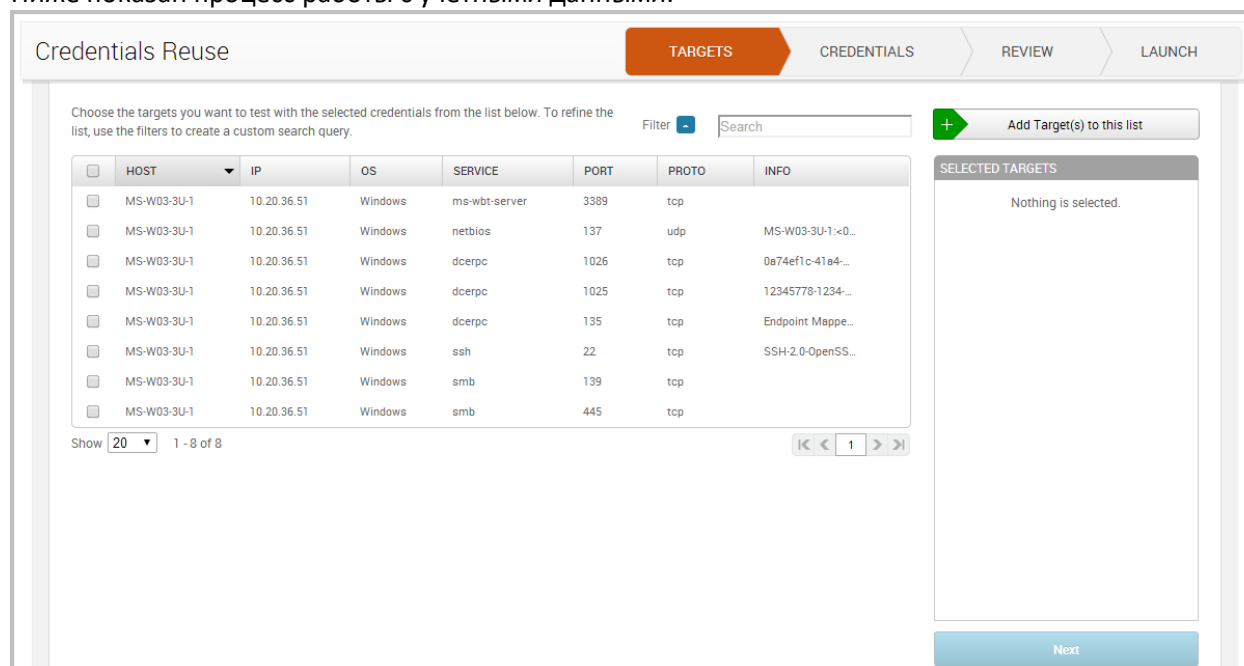
С чрезвычайно более строгими требованиями к паролю повторное использование учётных данных становится общей проблемой во многих организациях. Пользователи, «утонувшие» в сложной парольной политике, могут прибегать к повторному использованию одного и того же пароля для нескольких учётных записей, чтобы можно было легко управлять своими учётными данными. Это может привести к серьёзным проблемам безопасности, когда эти учётные данные будут скомпрометированы. Например, если злоумышленник получил действительные учётные данные для одной цели, он может попробовать их же и для других целей - для дальнейшей компрометации сети.

Чтобы помочь организации проверить свои пароли, вы можете повторно использовать учётные данные для определения дополнительных целей, которые будут уязвимы, если определённые учётные данные будут скомпрометированы. Повторное использование учётных данных - это функция Metasploit Pro, которая повторно использует проверенные учётные данные для попытки аутентификации для дополнительных целей. Эта функция полезна, если у вас есть проверенные или известные учётные данные, которые вы хотите использовать для набора целей. Например, если вы смогли получить хэш-файл NTLM для цели, вы должны попытаться повторно использовать этот хэш для других целей SMB. Если системный администратор обычно развёртывает для системы конфигурацию по умолчанию, вероятность того, что учётные данные будут работать, высока.

Процесс работы с повторным использованием учётных данных

Повторное использование учётных данных предоставляет управляемый рабочий процесс для требуемых задач, которые необходимо настроить. Каждая задача в рабочем процессе отображается на отдельной вкладке. Вы можете щёлкнуть любую вкладку, чтобы переключаться между различными задачами в рабочем процессе; однако вы должны выполнить каждую задачу, прежде чем сможете перейти к следующей.

Ниже показан процесс работы с учётными данными:



Рабочий процесс довольно прост, и состоит из четырёх этапов:

1. Выберите цели, для которых вы хотите использовать учётные данные.
2. Выберите учётные данные, которые вы хотите использовать для аутентификации выбранных целей.
3. Настройте параметры повторного использования, такие как ограничение времени ожидания и лимиты проверок, и информацию о цели, которые вы хотите использовать.
4. Запустите задачу.

Целевые задачи повторного использования учётных данных

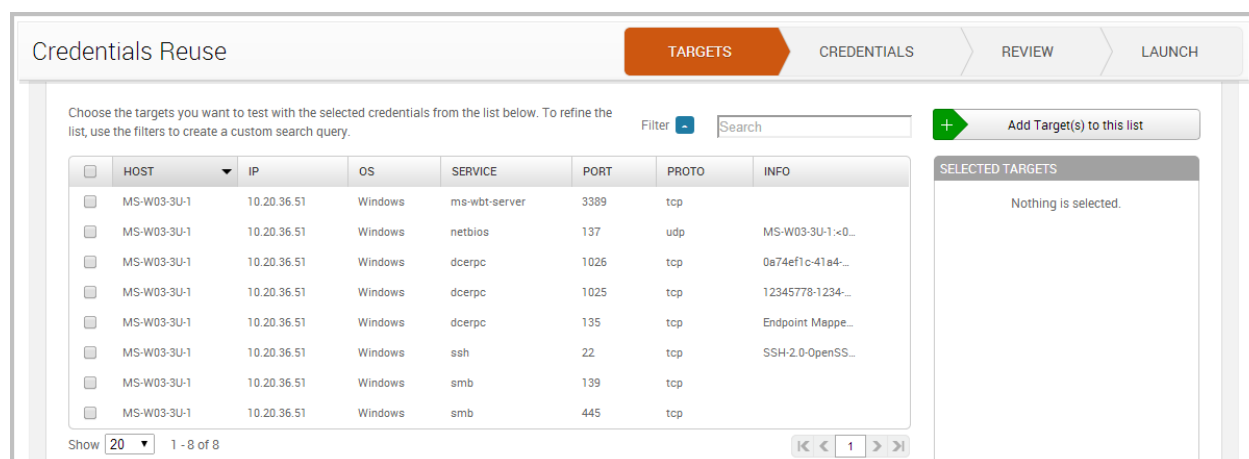
Повторное использование учётных данных задействует несколько сканеров логинов от Metasploit Framework, что даёт возможность нацелиться на следующие службы: AFP, DB2, FTP, HTTP, HTTPS, MSSQL, MySQL, POP3, PostgreSQL, SMB, SNMP, SSH, Telnet, VNC и WinRM.

Цели, у которых нет сканера логинов – как, например, DCERPC – будут пропущены.

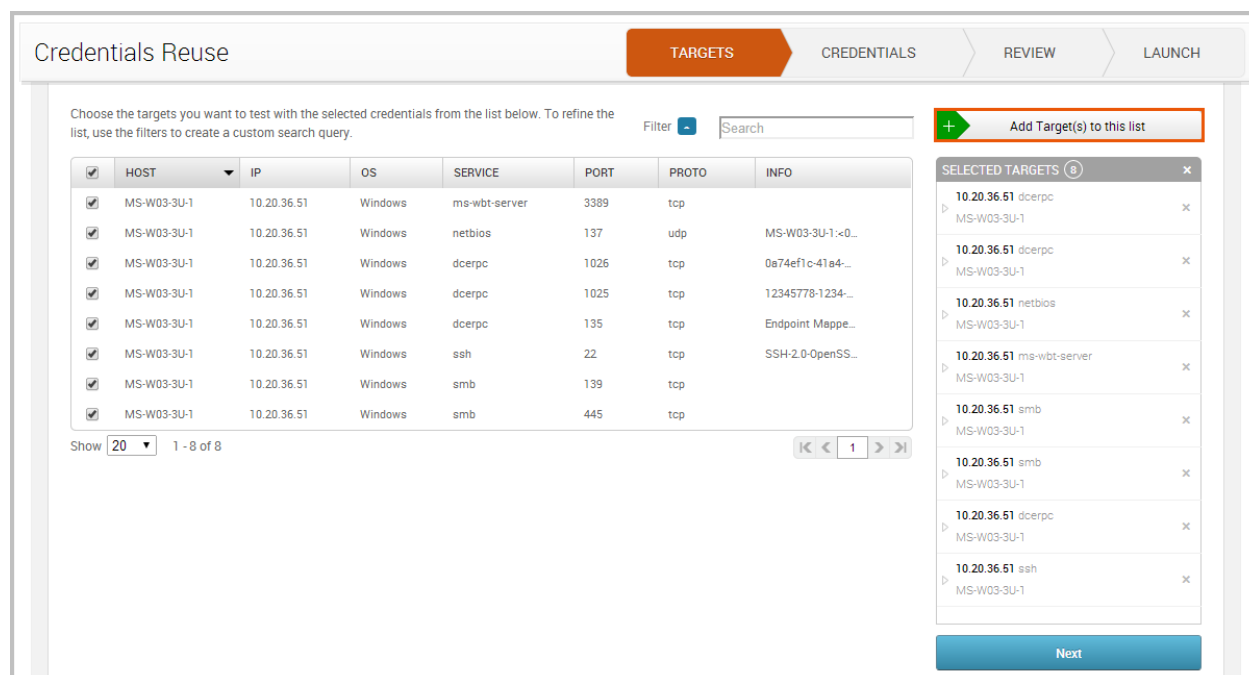
Настройка и запуск повторного использования учётных данных

1. В рамках проекта выберите **Credentials > Reuse**.

Появляется рабочий процесс повторного использования учётных данных. Сначала отображается вкладка **Targets**, и показывает вам цели, доступные в проекте. В этот момент целями являются службы. Metasploit Pro извлекает эти данные из данных хоста и службы, которые хранятся в проекте.



- Выберите задачи, для которых вы хотите использовать учетные данные. Вы можете выбрать неограниченное (произвольное) количество задач. По окончании выбора задач, нажмите кнопку **«Add Target(s) to this list (Добавить задачи к этому списку)»**. Задачи будут добавлены в список **«Selected Targets (Выбранные задачи)»**.



Вы можете использовать флажок **«Select All (Выбрать все)»** для выбора всех задач в проекте и стрелки страничной навигации, чтобы просмотреть список задач. Если вы хотите просмотреть все задачи в проекте, выберите опцию **«All (Все)»** в раскрывающемся списке **«Show (Показать)»**.

☒	HOST	IP	OS	SERVICE	PORT	PROTO	INFO
☒	MS-W03-3U-1	10.20.36.51	Windows	ms-wbt-server	3389	tcp	
☒	MS-W03-3U-1	10.20.36.51	Windows	netbios	137	udp	MS-W03-3U-1:<0...
☒	MS-W03-3U-1	10.20.36.51	Windows	dcerpc	1026	tcp	0a74ef1c-41a4...
☒	MS-W03-3U-1	10.20.36.51	Windows	dcerpc	1025	tcp	12345778-1234...
☒	MS-W03-3U-1	10.20.36.51	Windows	dcerpc	135	tcp	Endpoint Mappe...
☒	MS-W03-3U-1	10.20.36.51	Windows	ssh	22	tcp	SSH-2.0-OpenSS...
☒	MS-W03-3U-1	10.20.36.51	Windows	smb	139	tcp	
☒	MS-W03-3U-1	10.20.36.51	Windows	smb	445	tcp	

Show 20 1 - 8 of 8

1

Вы также можете нажать кнопку «Filter (Фильтр)», чтобы найти задачи по хосту, службе, порту, операционной системе, протоколу или ключевому слову.

Credentials Reuse

TARGETS CREDENTIALS

Choose the targets you want to test with the selected credentials from the list below. To refine the list, use the filters to create a custom search query.

Filter

Search

HOST NAME

Enter key word

SERVICE NAME

Enter service name

PORT

Enter port number

OS

Enter OS info

TEXT INFO

Enter key word

PROTOCOL

Enter protocol name

Reset Filter

- По окончании выбора задач, нажмите кнопку «**Next (Далее)**».

Отобразится вкладка «Credentials (Учетные данные)», на которой будут показаны все доступные в проекте учетные записи.

- Выберите учетные данные, которые вы хотите повторно использовать. Вы можете выбрать неограниченное (произвольное) количество учетных записей. По окончании выбора учетных записей, нажмите кнопку «**Add Credential(s) to this list** (Добавить учетные записи к этому списку)». Задачи будут добавлены в список «Selected Credentials list (Список выбранных учетных записей)».

Credentials Reuse

TARGETS

CREDENTIALS

REVIEW

LAUNCH

Choose the credentials that Metasploit will attempt to use to authenticate to the selected target list below.

Filter

Search

+

Add Credential(s) to this list

☒	PUBLIC (USERNAME)	PRIVATE	TYPE	REALM	REALM TYPE	TAGS
☒	administrator	e2fc15074bf7751dd408e6... more	NTLM hash			0 tags
☒	cyg_server	e2fc15074bf7751dd408e6... more	NTLM hash			0 tags
☒	guest	aad3b435b51404eeaad3b4... more	NTLM hash			0 tags
☒	guest		Password			0 tags
☒	sshd	aad3b435b51404eeaad3b4... more	NTLM hash			0 tags
☒	sshd		Password			0 tags
☒	support_388945a0	aad3b435b51404eeaad3b4... more	NTLM hash			0 tags

Show

20

1 - 7 of 7

<<

<

1

>

>>

SELECTED CREDENTIALS (7)

sshd

No Realm

×

guest

No Realm

×

cyg_server e2fc15074bf7751dd408e6b105...

No Realm

×

sshd aad3b435b51404eeaad3b435b51404e...

No Realm

×

support_388945a0 aad3b435b51404eeaad3...

No Realm

×

guest aad3b435b51404eeaad3b435b51404...

No Realm

×

administrator e2fc15074bf7751dd408e6b1...

No Realm

×

Next

Вы можете использовать флажок **«Select All (Выбрать все)»**, чтобы выбрать все задачи в проекте и стрелки страничной навигации, чтобы просмотреть список учетных данных. Если вы хотите просмотреть все учетные записи в проекте, выберите опцию **«All (Все)»** в раскрывающемся списке **«Show (Показать)»**.

☒

PUBLIC (USERNAME)

▲

PRIVATE

TYPE

REALM

REALM TYPE

TAGS

☒	administrator	e2fc15074bf7751dd408e6... more	NTLM hash			0 tags
☒	cyg_server	e2fc15074bf7751dd408e6... more	NTLM hash			0 tags
☒	guest	aad3b435b51404eeaad3b4... more	NTLM hash			0 tags
☒	guest		Password			0 tags
☒	sshd	aad3b435b51404eeaad3b4... more	NTLM hash			0 tags
☒	sshd		Password			0 tags
☒	support_388945a0	aad3b435b51404eeaad3b4... more	NTLM hash			0 tags

Show

20

1 - 7 of 7

<<

<

1

>

>>

Вы также можете нажать кнопку **«Filter (Фильтр)»**, чтобы найти учетные записи по статусу проверки, имени пользователя, паролю, скрытому типу, области и тегу (метке).

5. По окончании выбора учетных данных, нажмите кнопку **«Next»**.
Отобразится вкладка **«Review (Просмотр)»** с выводом параметров, которые можно установить для многократного использования учетных данных, а также задачи и учетные записи, которые вы выбрали.

6. Если вы хотите управлять настройками лимитирования времени для многократного использования учетных данных, вы можете настроить любую из следующих опций:
 - **Service Timeout** - устанавливает тайм-аут (в секундах) для каждой задачи.
 - **Overall Timeout** - устанавливает тайм-аут для всей задачи Credentials Reuse.
 - **Validate one credential per service** – Ограничивает до одной количество учетных записей, которым разрешен доступ к службе на хосте. Как только учетная запись прошла проверку на доступ к службе, Credentials Reuse прекратит тестирование других учетных записей.
7. Просмотрите задачи и учетные данные, которые вы выбрали для Credentials Reuse.

Если вы хотите что-либо удалить, вы можете нажать кнопку «X», расположенную рядом с задачей или учетной записью, или же вы можете нажать кнопку «X», расположенную сверху каждого списка, чтобы удалить все задачи или учетные данные.

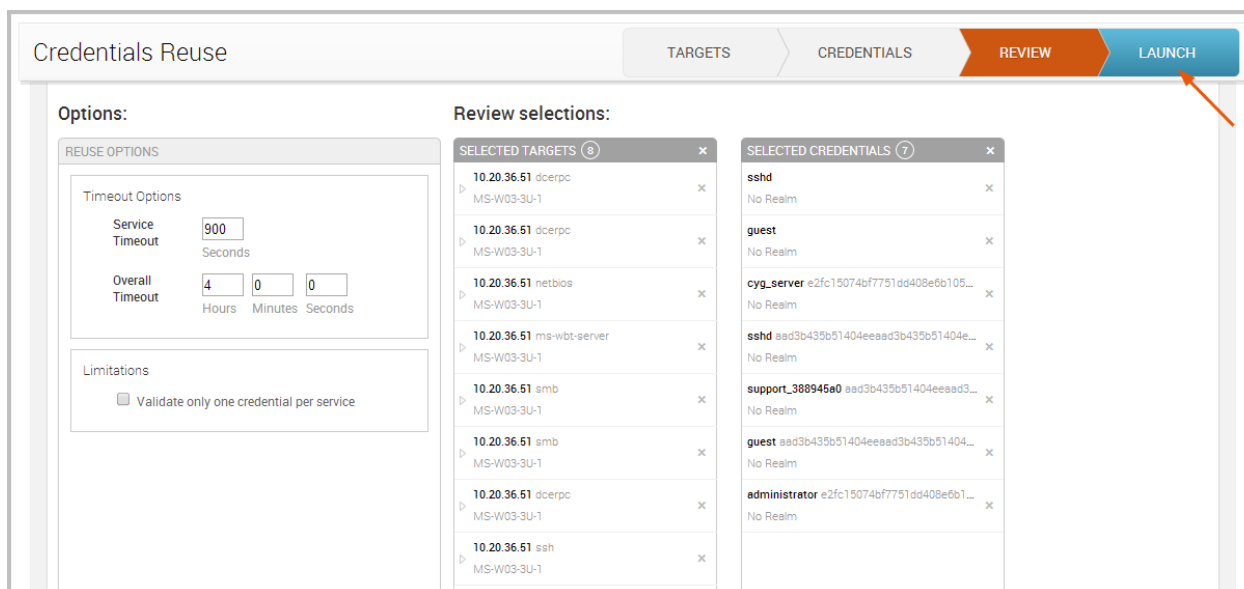
Review selections:

SELECTED TARGETS 8	SELECTED CREDENTIALS 7
10.20.36.51 dcerpc MS-W03-3U-1 10.20.36.51 dcerpc MS-W03-3U-1 10.20.36.51 netbios MS-W03-3U-1 10.20.36.51 ms-wbt-server MS-W03-3U-1 10.20.36.51 smb MS-W03-3U-1 10.20.36.51 smb MS-W03-3U-1 10.20.36.51 dcerpc MS-W03-3U-1 10.20.36.51 ssh MS-W03-3U-1	sshd No Realm guest No Realm cyg_server e2fc15074bf7751dd408e6b105... No Realm sshd aad3b435b51404eeaad3b435b51404e... No Realm support_388945a0 aad3b435b51404eeaad3... No Realm guest aad3b435b51404eeaad3b435b51404... No Realm administrator e2fc15074bf7751dd408e6b1... No Realm

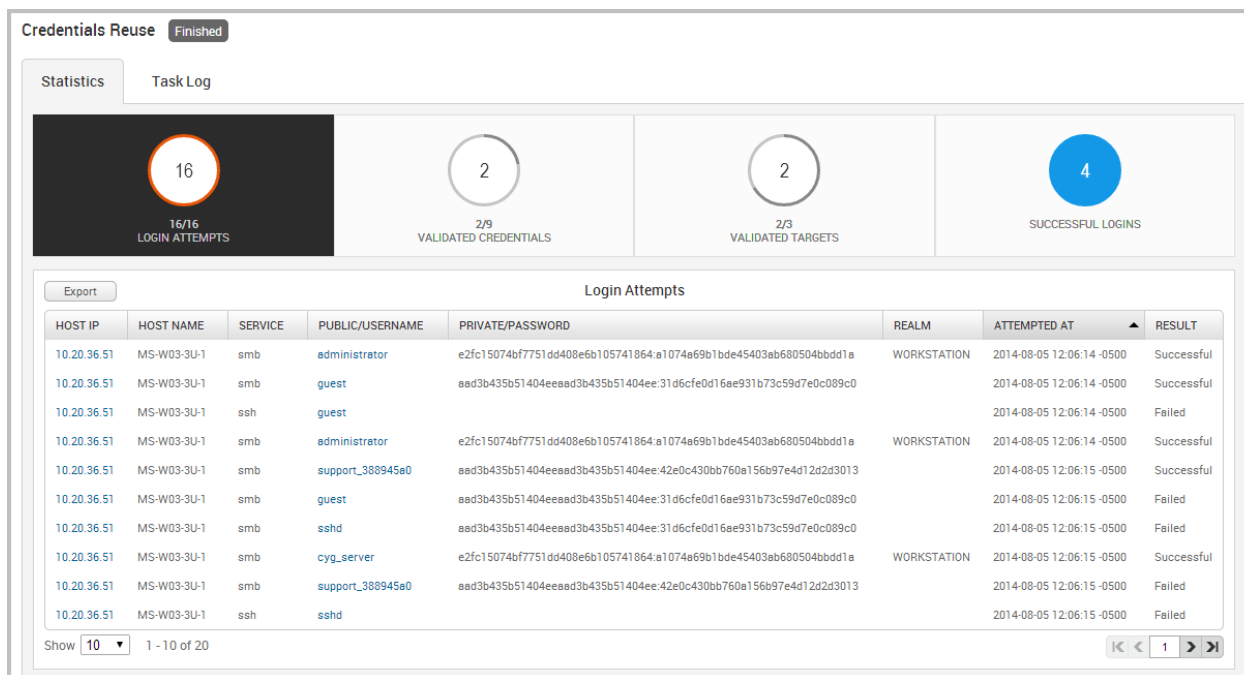
Если вы хотите добавить задачи или учетные записи, вы можете либо кликнуть по вкладке нужного элемента, чтобы его добавить, либо нажать на ссылку «**Go back and edit** (Вернуться и редактировать)», расположенную внизу списков выбранных задач (**Selected Targets**), и выбранных учетных данных (**Selected Credentials**).

Чтобы просмотреть дополнительную информацию для определенной задачи, вы можете нажать стрелку вниз, расположенную рядом с каждой задачей для отображения информации об операционной системе, порта и протокола.

- Нажмите кнопку «**Launch**» (Запустить), когда вы готовы к запуску Credentials Reuse. Кнопки запуска расположены также сверху и внизу списка заданий.



Когда вы запускаете Credentials Reuse, появляется окно «Findings» (Результаты), которое отображает статистику для выполняемой задачи. Вы можете щелкнуть по любому статистическому кружочку, для просмотра подробной информации по конкретному статистическому показателю.



Окно «Findings»(Результаты) отображает следующие статистические данные:

- **Login attempts** (Попытки входа) - Общее количество попыток входа в систему. Credentials Reuse будет отслеживать только попытки входа в систему для следующих служб: AFP, DB2, FTP, HTTP, HTTPS, MSSQL, MySQL, POP3, PostgreSQL, SMB, SNMP, SSH, telnet, VNC и WinRM. Поэтому Login attempts могут не содержать все задачи, которые вы выбрали. Login Attempts также показывает результаты по логину и времени последней попытки входа в систему.
- **Validated credentials** (Проверенные учетные данные) - Общее количество успешно авторизованных учетных данных.
- **Validated targets** (Проверенные задачи) - общее количество задач, которые были подтверждены.

- **Successful logins** (Успешные входы) - общее количество успешных входов в систему. Это число определяется из количества подтвержденных учетных данных и задач.

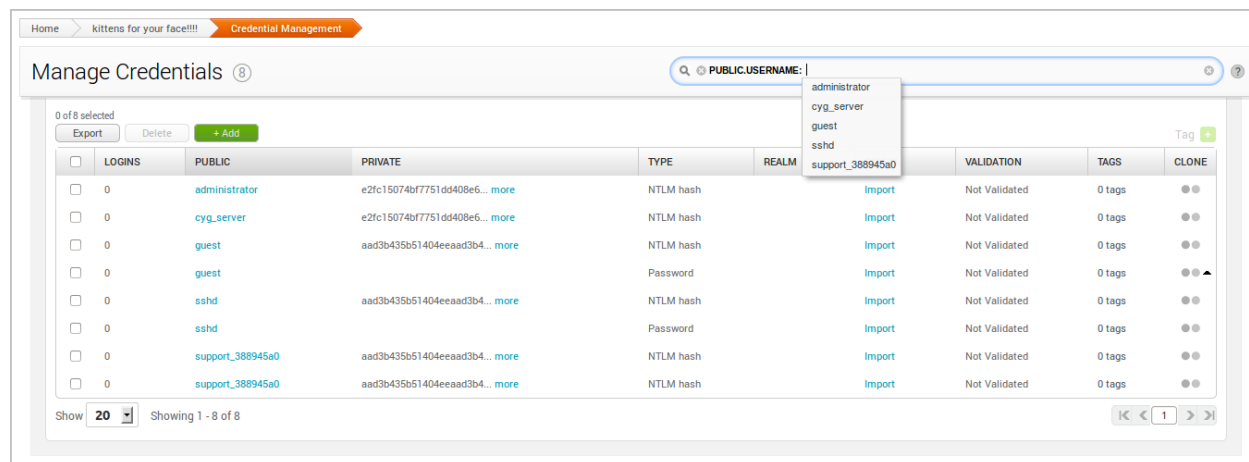
Примечание: Если Metasploit Pro может определить область учетных данных, он обновит их с помощью информации об области. Вы сможете увидеть обновленные учетные данные на странице «Manage Credentials page» (Управление учетными данными).

Поиск учетных данных

Вы можете создавать расширенные поисковые запросы, чтобы найти точные совпадения учетных данных на страницах Credential Management (Управление учетными данными) и Credentials Reuse (Многократное использование учетных данных). Эта возможность помогает сузить результаты поиска до поднабора данных, таких как определенные public (открытые) и private (закрытые).

Создание поискового запроса

Чтобы найти учетные данные, щелкните по полю «**Search** (Поиск)», расположенном на странице «Credential Management (Управление учетными данными)» или «Credentials Reuse (Многократное использование учетных данных)». Выпадающий список отображает доступные операторы поиска. Для продолжения вам нужно выбрать оператор поиска из списка. В поле поиска отображаются возможные ключевые слова, доступные для выбранного оператора. Вы можете выбрать ключевое слово из списка или начать вводить запрос, чтобы уточнить список.



Чтобы создать поисковый запрос для учетных данных, необходимо указать хотя бы один оператор поиска и ключевое слово. Оператор поиска определяет тип данных, которые вы хотите запросить, а ключевое слово указывает условие, используемое поиском для нахождения совпадающих записей. Вы можете использовать столько операторов поиска, сколько необходимо. Как только вы добавите оператор поиска к запросу, таблица автоматически обновит список учетных данных.

По умолчанию в поисковом запросе используется – соединитель «AND» между каждым оператором поиска. Например, запрос: "PUBLIC.USERNAME: John, PRIVATE.DATA: abc123" возвращает любое имя

пользователя, содержащее «John», у которого есть пароль «abc123». Однако, если запрос содержит несколько операторов одного и того же типа, между ними используется соединитель «OR». Например, запрос: "PUBLIC.USERNAME: John, PUBLIC.USERNAME: Mike, PRIVATE.DATA: abc123" возвращает имя пользователя, содержащее «Джон» или «Майк», который имеет пароль «abc123».

! Поисковый запрос автоматически добавляет соединитель «И» между каждым оператором поиска. Однако, если поисковый запрос использует два и более оператора поиска одного и того же типа, запрос использует соединитель «ИЛИ» между такими операторами.

Операторы поиска

Для учетных данных доступны следующие операторы поиска:

- public.username - Этот оператор поиска соответствует имени пользователя.
- private.data - этот оператор поиска соответствует скрытым данным.
- private.type. Этот оператор поиска соответствует скрытому типу данных.
- realm.key - Этот оператор поиска соответствует типу области.
- realm.value - этот оператор поиска соответствует имени области идентификации.
- tags.name - этот оператор поиска соответствует тегу.

Синтаксис поиска учетных данных

Вы должны использовать следующий синтаксис при поиске учетных данных:

<search operator>:<keyword>.

Например, если вы хотите найти все учетные записи, которые имеют значение admin, вам необходимо создать следующий запрос:

public.username: admin.

Этот запрос гарантирует, что поиск ведется только по столбцу Public в таблице учетных данных для ключевого слова administrator и возвращает только учетные данные, которые имеют administrator в качестве открытого значения.

Поиск открытых данных (по имени пользователя)

Чтобы искать по имени пользователя, ваш запрос должен использовать оператор public.username.

Например, запрос:

public.username: admin

выполняет поиск всех учетных данных, имеющих в имени «admin».

Поиск скрытых (непубличных) данных

Для поиска скрытых данных ваш запрос должен использовать оператор private.data.

Например, в запросе

private.data:abc123

выполняется поиск любых учетных записей, имеющих «abc123» в скрытых (непубличных) данных.

Поиск данных скрытого типа

Для поиска данных скрытого типа ваш запрос должен использовать оператор private.type.

Например, запрос

private.type:hash

выполняет поиск любых учетных данных, имеющих скрытый тип «hash(хэш)».

Поиск по типу области идентификации

Для поиска по типу области ваш запрос должен использовать оператор realm.key.

Например, запрос:

realm.type:DB2

ищет любые учетные данные, имеющие тип области «DB2 Database».

Поиск по имени области

Для поиска по имени области, ваш запрос должен использовать оператор realm.value.

Например, запрос:

realm.value:DC

выполняет поиск всех учетных данных, имеющих область идентификации с именем «DC».

Поиск учетных данных по определенному тегу

Для поиска учетных данных по определенному тегу ваш запрос должен использовать оператор tags.name.

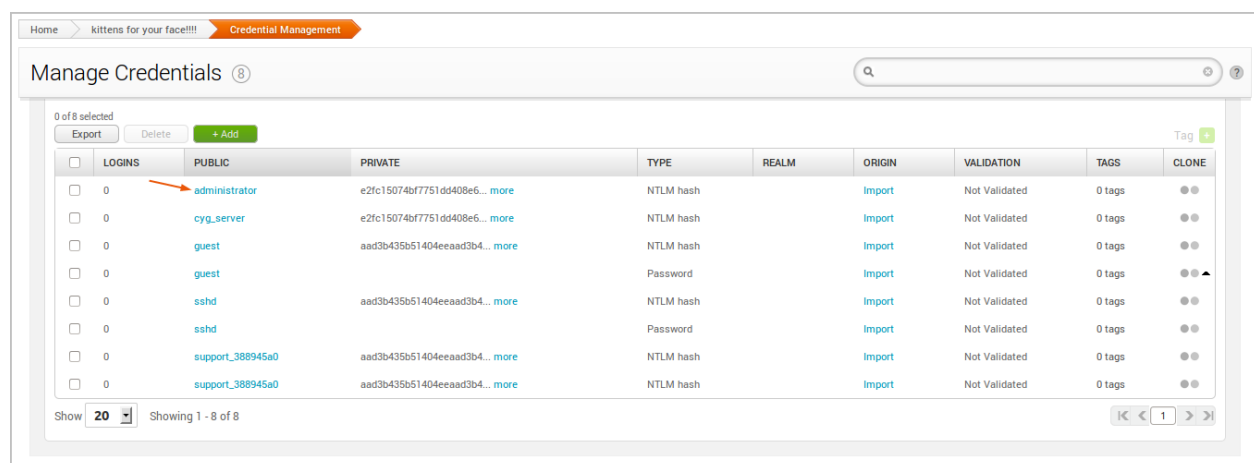
Например, запрос:

tags.name>window

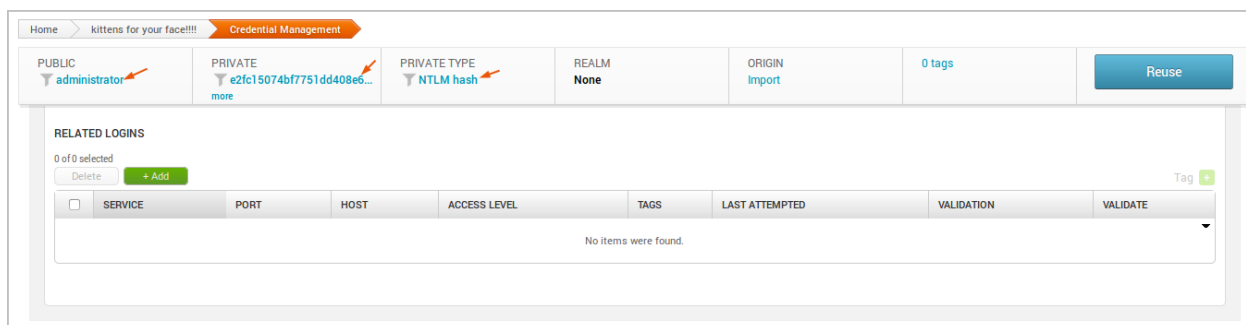
выполняет поиск любых учетных данных, имеющих тег «window».

Фильтрация по Метаданным учетных записей

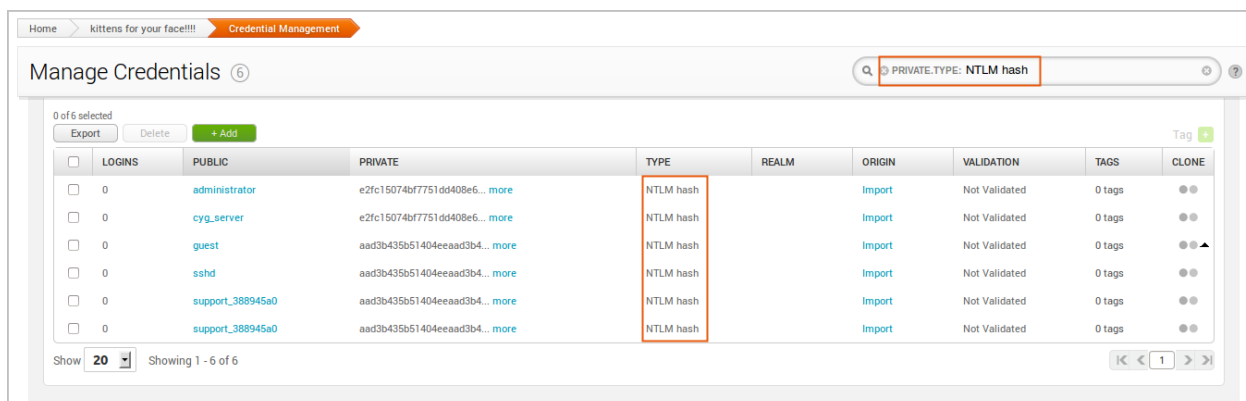
На странице учетной записи отображаются детали для отдельной учетной записи, например, метаданные и связанные с ними логины. Чтобы получить доступ к странице отдельной учетной записи, вам нужно кликнуть на private на странице Manage Credentials (Управление учетными данными), как показано ниже:



Когда вы нажимаете на private, страница учетной записи переходит в режим просмотра. Обратите внимание, значения public, private и private type отображаются как ссылки. Вы можете кликнуть по этим ссылкам, чтобы запросить другие учетные данные в проекте, имеющие такие же метаданные public, private или private type.



Появится страница «Manage Credentials (Управление учетными данными)» и отобразит результаты запроса. Фильтры будут предустановлены на основании запрошенного вами типа данных. Например, если вы просматриваете данные для public, такие как administrator, возможно вы захотите увидеть другие учетные данные в проекте, имеющие такой же public. Для этого вы можете просто нажать на public. Когда появится страница «Manage Credentials (Управление учетными данными)», вы можете выбрать дополнительные фильтры для дальнейшего сужения списка учетных записей.

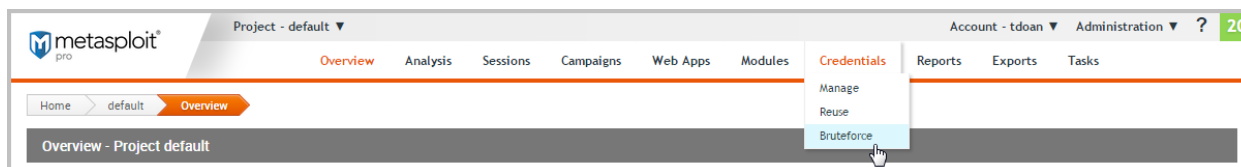


Брутфорс-атаки

Суть атаки «грубой силой» (брутфорс-атаки) заключается в автоматических и систематических попытках методом подбора угадать правильное имя пользователя и секретную комбинацию для службы. Их цель — подобрать действующие в системе логины и использовать их для получения доступа к сети с последующим извлечением конфиденциальных данных. Например, хэши паролей и токены. В рамках теста на проникновение важно оценить эффективность атаки «грубой силы» на сеть, чтобы в дальнейшем вы могли определить аудит парольной политики и распознать потенциальные векторы атак. Это позволит вам создать усовершенствованный список технических рекомендаций и провести анализ реального бизнес-риска. Для помощи в проведении атаки «грубой силы» вы можете использовать Bruteforce Workflow (рабочий процесс брутфорсинга), где предоставляется интерфейс с подсказками, который поможет вам настроить параметры атаки подбора паролей.

Доступ к Bruteforce Workflow

Чтобы получить доступ к Bruteforce Workflow, откройте панель вкладок проекта и выберите **Credentials** (Учетные данные) > **Bruteforce** (Атака грубой силы), как показано ниже.



Определение хостов для атаки грубой силой

Первое, что вам нужно сделать в Workflow Bruteforce — определить область атаки. Область применения определяет хосты в проекте, на которые необходимо ориентироваться во время атаки. Вы можете выбрать атаку на все хосты в проекте, или вручную определить их, если вы хотите получить детальное управление над областью атаки.

Чтобы атаковать все хосты в проекте, в разделе «Цели» выберите опцию «**Все хосты**», как показано ниже.

Чтобы атаковать определенные хосты в проекте, в разделе «Цели» выберите параметр «**Ввести целевые адреса**», как показано ниже. Вы можете ввести один адрес (192.168.1.1), диапазон (192.168.1.1-192.168.1.100), бесклассовую адресацию (192.168.1.0/24) или подстановочный знак (192.168.1*). Для разделения каждой записи необходимо использовать новую строку. Если вы хотите включить все хосты в проект, то это поле можно оставить пустым.

Bruteforce

Bruteforce systematically attempts to use credentials to authenticate to services on target hosts. Select the hosts and services you want to bruteforce and the credentials you want to use to attempt authentication.

TARGETS

CREDENTIALS

OPTIONS

0 targets selected

Select Host(s):

☐ All hosts

☒ Enter target addresses

Target addresses: ?

Excluded addresses:

Select Services:

☐ All Services

☐ AFP	☐ MSSQL	☐ SNMP
☐ DB2	☐ MySQL	☐ SSH
☐ FTP	☐ POP3	☐ Telnet
☐ HTTP	☐ Postgres	☐ VNC
☐ HTTPS	☐ SMB	☐ WinRM

0 possible combinations

☐ All credentials in this project

☐ Attempt factory defaults

☐ Add/Import credential pairs

Overall Timeout ?

HH

MM

SS

Hours Minutes Seconds

Service Timeout ?

SS

Seconds

Time Between Attempts ?

Normal (0 seconds)

☐ Apply mutation(s) ?

☐ Stop bruteforcing a target when a credential is guessed ?

☐ Get sessions if possible ?

LAUNCH

Исключение хостов из атаки грубой силы

В списке исключений определяются хосты, которые вы не хотите атаковать. Список исключений особенно полезен, если вы хотите определить диапазон для целевых хостов и исключить несколько хостов из диапазона. Например, если вы определили 192.168.0.0/24 как диапазон целевых адресов, но знаете, что не можете протестировать 192.168.0.1 и 198.168.0.2 из-за рисков блокировки, вы можете добавить их в список исключений.

Чтобы исключить хосты из атаки «грубой силы», в разделе **«Цели»** необходимо выбрать параметр **«Цели»**. В поле **«Исключенные адреса»** укажите хосты, которые вы хотите добавить в черный список, как показано ниже.

Bruteforce

Bruteforce systematically attempts to use credentials to authenticate to services on target hosts. Select the hosts and services you want to bruteforce and the credentials you want to use to attempt authentication.

TARGETS

CREDENTIALS

OPTIONS

0 targets selected

Select Host(s):

☐ All hosts

☒ Enter target addresses

Target addresses: ?

Excluded addresses:

Select Services:

☐ All Services

☐ AFP
☐ DB2
☐ FTP
☐ HTTP
☐ HTTPS

☐ MSSQL
☐ MySQL
☐ POP3
☐ Postgres
☐ SMB

☐ SNMP
☐ SSH
☐ Telnet
☐ VNC
☐ WinRM

0 possible combinations

☐ All credentials in this project

☐ Attempt factory defaults

☐ Add/Import credential pairs

Overall Timeout ?

Hours Minutes Seconds

Service Timeout ?

Seconds

Time Between Attempts ?

☐ Apply mutation(s) ?

☐ Stop bruteforcing a target when a credential is guessed

☐ Get sessions if possible ?

LAUNCH

Вы можете ввести один IP-адрес, диапазон адресов или бесклассовую адресацию. Если есть несколько адресов или диапазон адресов, используйте новую строку для разделения каждой записи.

Вы можете оставить поле «**Целевые адреса**» пустым, чтобы включить все хосты в проект, за исключением перечисленных в поле «**Исключенные адреса**».

Выбор служб для брутфорса

После выбора хостов для атаки, вам необходимо выбрать логины служб, которые вы хотите атаковать «грубой силой». Службы, предназначенные для целей атаки грубой силы, ограничены следующими протоколами: AFP, DB2, FTP, HTTP, HTTPS, MSSQL, MySQL, POP3, PostgreSQL, SMB, SNMP, SSH, Telnet, VNC и WinRM. Вы можете выбрать целью все службы или любое их сочетание. Попытка входа в систему происходит только в том случае, если служба открыта на хосте. В противном случае она пропускается.

Чтобы указать службы для атаки «грубой силы», необходимо выбрать их из списка «Службы», как показано ниже:

Bruteforce

Bruteforce systematically attempts to use credentials to authenticate to services on target hosts. Select the hosts and services you want to bruteforce and the credentials you want to use to attempt authentication.

TARGETS

0 targets selected

Select Host(s):

- ☒ All hosts
- ☐ Enter target addresses

Select Services:

- ☒ All Services
- ☐ AFP
- ☐ DB2
- ☐ FTP
- ☐ HTTP
- ☐ HTTPS
- ☐ MSSQL
- ☐ MySQL
- ☐ POP3
- ☐ Postgres
- ☐ SMB
- ☐ SNMP
- ☐ SSH
- ☐ Telnet
- ☐ VNC
- ☐ WinRM

CREDENTIALS

0 possible combinations

- ☐ All credentials in this project
- ☐ Attempt factory defaults
- ☐ Add/Import credential pairs

OPTIONS

Overall Timeout: HH MM SS ?
Hours Minutes Seconds

Service Timeout: SS ?
Seconds

Time Between Attempts: Normal (0 seconds) ?

- ☐ Apply mutation(s) ?
- ☐ Stop bruteforcing a target when a credential is guessed
- ☐ Get sessions if possible ?

LAUNCH

После того, как вы выбрали службы для атаки «грубой силы», общий подсчет целей обновляется в соответствии с разделом «Цели». Общее количество выбранных целей рассчитывается на основе количества хостов и выбранных вами служб.

Создание списка паролей для брутфорса

При атаке «грубой силы» используется список паролей (словарь), где содержится учетные данные, которые могут использоваться для атаки «грубой силы» на логины служб (атака по словарю). Вы можете найти списки паролей в Интернете, где, как правило, содержатся часто используемые учетные данные, например, admin/admin, или вы можете создать собственный список паролей, используя собранные данные о цели. Например, если вы смогли получить и взломать хэши NTLM из цели, вы должны добавить их в список паролей, чтобы во время атаки «грубой силы» была возможность попробовать использовать их против дополнительных целей.

С помощью Bruteforce Workflow вы можете использовать любую комбинацию следующих методов для создания списка паролей для атаки «грубой силы»:

- Вы можете выбрать все учетные данные, хранящиеся в проекте.
- Вы можете попробовать часто используемые настройки учетной записи.
- Вы можете импортировать список паролей.
- Вы можете вручную ввести список паролей.

Для попытки прохождения проверки в службе, во время атаки «грубой силы» пробуются каждая пара для учетных данных из списка паролей. Если проверка в службе с конкретными учетными данными пройдена, учетные данные сохраняются в проекте, а для службы создается логин. Во

время атаки «грубой силы» продолжается перебор списка паролей, пока все учетные данные не будут испробованы, или до тех пор, пока он не достигнет предела, который вы определили.

Общее количество выбранных учетных данных рассчитывается на основе прямого произведения выбранных вами учетных данных и количества примененных вами мутаций.

Использование всех учетных данных в проекте для атаки «грубой силы»

Чтобы настроить атаку «грубой силы» для использования всех учетных данных в проекте, необходимо в разделе «Учетные данные» в этом проекте выбрать параметр «Все учетные данные» в Bruteforce Workflow, как показано ниже.

The screenshot shows the 'Bruteforce' configuration window. It has three tabs: 'TARGETS', 'CREDENTIALS', and 'OPTIONS'. The 'CREDENTIALS' tab is active, showing '778 possible combinations'. Under 'Select Host(s):', 'All hosts' is selected. Under 'Select Services:', a grid of checkboxes lists various protocols like AFP, DB2, FTP, HTTP, HTTPS, MSSQL, MySQL, POP3, Postgres, SMB, SNMP, SSH, Telnet, VNC, and WinRM. In the 'CREDENTIALS' section, 'All credentials in this project' is checked, with 'Attempt factory defaults' and 'Add Import credential pairs' as options. The 'OPTIONS' section on the right includes settings for 'Overall Timeout', 'Service Timeout', 'Time Between Attempts' (set to 'Normal (0 seconds)'), and checkboxes for 'Apply mutation(s)', 'Stop bruteforcing a target when a credential is guessed', and 'Get sessions if possible'. A 'LAUNCH' button is at the bottom right.

Ввод учетных данных вручную для атаки «грубой силы»

Вы можете вручную создать список паролей для атаки «грубой силы». Чтобы вручную добавить пары учетных данных для атаки «грубой силы», в разделе «Учетные данные» выберите параметр «Добавить/Импортировать учетные данные». После этого отобразится текстовое поле «Добавить учетные данные вручную», как показано ниже.

Bruteforce

Bruteforce systematically attempts to use credentials to authenticate to services on target hosts. Select the hosts and services you want to bruteforce and the credentials you want to use to attempt authentication.

TARGETS

0 targets selected

Selected Host(s):

- ☒ All hosts
- ☐ Enter target addresses

Select services:

- ☒ All services
- ☒ AFP
- ☒ HTTP
- ☒ MySQL
- ☒ SMB
- ☒ SSH PUBKEY
- ☒ WinRM
- ☒ DB2
- ☒ HTTPS
- ☒ POP3
- ☒ SNMP
- ☒ Telnet
- ☒ FTP
- ☒ MSSQL
- ☒ Postgres
- ☒ SSH
- ☒ VNC

CREDENTIALS

0 possible combinations

- ☐ All credentials in this project
- ☐ Attempt factory defaults
- ☒ Add/Import credential pairs

Credentials (100 lines max)

Enter a space and new line delimited list of credential pairs.

Example:

```
username pass
username pass1 pass2
realm/username pass
realm/username pass1 pass2
```

Import Credentials from a file:

No file selected... Choose ...

- ☐ Use <BLANK> as password
- ☐ Use username as password

OPTIONS

Overall Timeout: 4 0 0 ?

Service Timeout: 900 ?

Time Between Attempts: Normal (0 seconds) ?

- ☐ Apply mutation(s) ?
- ☐ Stop bruteforcing a target when a credential is guessed ?
- ☐ Get session if possible ?

Вы можете предоставить разграниченный список пар учетных данных с размещением с интервалами и новыми строками. Первое слово на каждой строке обрабатывается как имя пользователя. Каждое слово, следующее за именем пользователя, является паролем. Вы можете ввести до 100 пар учетных данных в текстовом поле. Если вам нужно добавить более 100 учетных пар, необходимо создать файл учетных данных и импортировать его. Дополнительные сведения об импорте файла учетных данных смотрите в разделе [«Импорт списка паролей для атаки «грубой силы»»](#).

Вы должны следовать следующим правилам синтаксиса, когда вручную вводите список паролей:

- Чтобы определить пару учетных данных, используйте следующий формат: имя пользователя пароль.
- Чтобы указать несколько паролей для имени пользователя, введите имя пользователя, а за ним сразу пароли. Каждый пароль должен быть разделен пробелом.
- Каждая учетная запись должна начинаться с новой строки.
- Каждый элемент должен быть разделен пробелом.
- Чтобы указать пустое имя пользователя, используйте <BLANK>.
- Чтобы указать имя пользователя с пустым паролем, введите только имя пользователя.

Пример списка паролей

Username

<BLANK> pass

username pass

username pass1 pass2

[Импорт списка паролей для атаки грубой силы](#)

Список паролей (словарь) — это текстовый файл, содержащий пары учетных данных. Вы можете вручную создать список паролей, используя базовый текстовый редактор, например Блокнот, или вы можете загрузить список паролей из Интернета.

Список паролей должен соответствовать следующим правилам:

- В каждой учетной паре должен использоваться следующий формат: имя пользователя/пароль.
- Каждая учетная пара должна начинаться с новой строки.
- Каждый элемент должен быть разделен пробелом.
- Пустое имя пользователя должно быть обозначено как <BLANK>.
- Пустой пароль не обязательно так обозначать
- Имя пользователя без пароля служит признаком пустого пароля.

Чтобы импортировать список паролей, необходимо в разделе «Учетные данные» выбрать параметр «Добавить/Импортировать учетные данные». Нажмите кнопку «Выбрать файл», как показано ниже.

The screenshot shows the Bruteforce application interface. The 'CREDENTIALS' tab is active. In the 'CREDENTIALS' section, the 'Add/Import credential pairs' checkbox is checked. Below it, there is a text area for entering credentials and a button labeled 'Choose...' for selecting a file. An orange arrow points to the 'Choose...' button. The OPTIONS section contains various timeout and attempt settings.

Когда отобразится окно каталога, перейдите к расположению файла, который вы хотите импортировать. Выберите и нажмите кнопку «Импорт».

Использование заводских настроек для атаки «грубой силы»

Учетные данные по умолчанию — это пары имени пользователя и пароля, которые поставляются с операционной системой, базой данных или программным обеспечением. Зачастую эти заводские настройки по умолчанию одинаковы для всех версий программного обеспечения, публично задокументированы и часто остаются без изменений. Поэтому, поставщики всегда рекомендуют изменить пароль по умолчанию до того, как система будет внедрена в производственную окружающую среду. Однако не все придерживаются этих указаний, и системы часто устанавливают с настройками конфигурации по умолчанию, благодаря чему они становятся основными целями для атаки «грубой силы».

Чтобы помочь вам определить системы, использующие конфигурацию по умолчанию, атака «грубой силы» включает в себя опцию под названием «Попытка взлома заводских настроек по умолчанию», что позволяет вам использовать службы атаки «грубой силы», используя общие учетные данные по умолчанию. В следующем разделе перечислены учетные данные, которые будут проверяться для каждой службы (если эта опция включена).

Bruteforce

Bruteforce systematically attempts to use credentials to authenticate to services on target hosts. Select the hosts and services you want to bruteforce and the credentials you want to use to attempt authentication.

TARGETS

CREDENTIALS

OPTIONS

0 targets selected

Select Host(s):

☒ All hosts

☐ Enter target addresses

Select Services:

☐ All Services

☐ AFP	☐ MSSQL	☐ SNMP
☐ DB2	☐ MySQL	☐ SSH
☐ FTP	☐ POP3	☐ Telnet
☐ HTTP	☐ Postgres	☐ VNC
☐ HTTPS	☐ SMB	☐ WinRM

1,150 combinations

☐ All credentials in this project

☒ Attempt factory defaults

☐ Add/Import credential pairs

Overall Timeout ?
Hours Minutes Seconds

Service Timeout ?
Seconds

Time Between Attempts ?

☐ Apply mutation(s) ?

☐ Stop bruteforcing a target when a credential is guessed

☐ Get sessions if possible ?

LAUNCH

Учетные данные по умолчанию для Axis2

Следующие имена пользователей и пароли являются стандартными значениями по умолчанию для Axis2:

- Имя пользователя - 'admin'
- Пароли - 'axis2'

Учетные данные по умолчанию для DB2

Следующие имена пользователей и пароли являются стандартными значениями по умолчанию для DB2:

- Имя пользователя - 'admin', 'dasusr1', 'db2admin', 'db2fenc1' и 'db2inst1'
- Пароли - 'admin', 'dasusr1', 'db2admin', 'db2fenc1', 'db2inst1', 'db2pass', 'db2password' и 'db2pw'

Учетные данные по умолчанию для FTP

Следующие имена пользователей и пароли являются стандартными значениями по умолчанию для FTP:

- Имя пользователя - 'admin', 'anonymous', 'ftp', 'ftp_admi', 'ftp_inst', 'ftp_nmc', 'ftp_oper', 'ftpuser', 'login', 'rapport', 'root', 'user' и 'xbox'
- Пароли - '1234', 'access', 'chrome@example.com', 'Exabyte', 'ftp', 'help1954', 'IEUser @', 'kilo1987', 'mozilla@example.com', 'pass', 'password', 'pbxk1064', 'r@p8p0r', 'tuxalize', and 'xbox'

Настройки по умолчанию для HTTP

Для HTTP по умолчанию используются следующие имена пользователей и пароли:

- Имена пользователя - 'admin', 'apc', 'axis2', 'cisco', 'connect', 'manager', 'newuser', 'pass', 'private', 'root', 'security', 'sitecom', 'sys', 'system', 'tomcat', 'user', 'wampp', 'xampp', and 'xampp-dav-unsecure'
- Пароли - '1234', 'admin', 'apc', 'cisco', 'connect', 'default', 'letmein', 'manager', 'none', 'pass', 'password', 'ppmax2011', 'root', 'sanfran', 'security', 'sitecom', 'sys', 'system', 'tomcat', 'turnkey', 'user', 'wampp', and 'xampp'

Настройки по умолчанию для MSSQL

Для MSSQL используются следующие настройки по умолчанию:

- Usernames - 'Administrator', 'ARAdmin', 'entldbdbo', 'entldbreader', 'mon_user', 'probe', 'repl_publisher', 'repl_subscriber', 'sa', и 'WinCCConnect'
- Passwords - '2WSXcder', 'AR#Admin#', 'blank', 'dbopswd', 'pass', 'pass1', 'password', 'rdprswd'

Настройки по умолчанию для MySQL

Для MySQL используются следующие имена пользователей и пароли:

- Имена пользователей - 'admin', 'mysql', и 'root'
- Пароли - 'blank', 'pass', 'pass1', 'password', и 'vicidia1now'

Настройки по умолчанию для PostgreSQL

Для PostgreSQL используются следующие имена пользователей и пароли:

- Имена пользователей - 'admin', 'postgres', 'scott', и 'tom'
- Пароли - 'admin', 'password', 'postgres', и 'tiger'

Настройки по умолчанию для SMB

Для SMB используются следующие имена пользователей и пароли:

- Имена пользователей - 'backup' и 'helpdesk'
- Пароли - 'backup' и 'hpinvent'

Настройки по умолчанию для SNMP

- Для SNMP используются следующие имена пользователей и пароли:
Имена пользователей - <BLANK>
- Пароли - '0392a0', '1234', '2read', '4changes', 'access', 'adm', 'Admin', 'admin', 'agent', 'agent_steal', 'all', 'all private', 'all public', 'ANYCOM', 'apc', 'bintec', 'blue', 'c', 'C0de', 'cable-d', 'canon_admin', 'cc', 'CISCO', 'cisco', 'community', 'core', 'CR52401', 'debug', 'default', 'dilbert', 'enable', 'field', 'field-service', 'freekevin', 'fubar', 'guest', 'hello', 'hp_admin', 'IBM', 'ibm', 'ILMI', 'ilmi', 'Intermec', 'intermec', 'internal', 'I2', 'I3', 'manager', 'mngt', 'monitor', 'netman', 'network', 'NoGaH\$@!', 'none', 'openview', 'OrigEquipMfr', 'pass', 'password', 'pr1v4t3', 'private', 'PRIVATE', 'Private', 'proxy', 'pub1lc', 'public', 'PUBLIC', 'Public', 'read', 'read-only', 'read-write', 'readwrite', 'red', 'regional', 'rmon', 'rmon_admin', 'ro', 'root', 'router', 'rw', 'rwa', 's!a@m#n\$p%c', 'san-fran', 'sanfran', 'scotty', 'SECRET', 'Secret', 'secret', 'SECURITY', 'Security', 'security', 'seri', 'SNMP', 'snmp', 'SNMP_trap', 'snmpd', 'snmptrap', 'solaris', 'SUN', 'sun', 'superuser', 'SWITCH', 'Switch', 'switch', 'SYSTEM', 'System', 'system', 'tech', 'TENmanUFactOryPOWER', 'TEST', 'test', 'test2', 'tiv0li', 'tivoli', 'trap', 'world', 'write', 'xyzy', и 'yellow'

Для SSH используются следующие настройки по умолчанию

Для SSH используются следующие имена пользователей и пароли:

- Имена пользователей - 'admin', 'administrator', и 'root'
- Пароли - '1234', 'admin', 'changeme123', 'password', 'password1', 'password123', 'password123!', и 'toor'

Настройки по умолчанию для Telnet

Для telnet используются следующие имена пользователей и пароли:

- Имена пользователей - 'admin', 'administrator', 'Alphanetworks', 'cisco', 'helpdesk', 'pix', и 'root'
- Пароли - '100', 'admin', 'changeme123', 'cisco', 'password', 'password1', 'password123', 'password123!', 'sanfran', 'root', 'wrgg15_di524', 'wrgg19_c_dlwbr_dir300', и 'wrgn22_dlwbr_dir615'

Настройки по умолчанию для VNC

Для VNC используются следующие имена пользователей и пароли:

- Имена пользователей - 'admin', 'administrator', and 'root'
- Пароли - '100', '1234', 'admin', 'changeme123', 'password', 'password1', 'password123', 'password123!', и 'toor'

Настройки по умолчанию для WinRM

Для WinRM используются следующие имена пользователей и пароли:

- Имена пользователей - 'admin', 'administrator', and 'root'
- Пароли - '1234', 'admin', 'changeme123', 'password', 'password1', 'password123', 'password123!', и 'toor'

Использование пустых паролей при хакерских атаках методом перебора («грубой силы»)

Для генерации пустых паролей для каждого имени пользователя в списке паролей, рекомендуем подключить в качестве опции пароля Use <BLANK>, как показано на примере ниже. Например, если в списке паролей прописана по умолчанию пара наподобие 'admin'/'admin', взломщики могут воспользоваться опцией admin/'<BLANK>'.

The screenshot shows the Bruteforce application interface with three tabs: TARGETS, CREDENTIALS, and OPTIONS. The CREDENTIALS tab is active, showing 0 possible combinations. Under 'All credentials in this project', the 'Add/Import credential pairs' checkbox is checked. Below this, there is a text area for 'Credentials (100 lines max)' with an example of a list of credential pairs. At the bottom, under 'Import Credentials from a file:', there is a 'No file selected...' button and a 'Choose...' button. A red arrow points to the 'Use <BLANK> as password' checkbox, which is checked. Below it, the 'Use username as password' checkbox is unchecked.

Использование имени пользователя в качестве пароля

Для использования имени пользователя в качестве пароля рекомендуем подключить опцию «Использовать имя пользователя в качестве пароля» как показано на примере ниже. Например, если в списке паролей по умолчанию указана пара 'user'/'pass', взломщики могут воспользоваться 'user'/'user'.

The screenshot shows the Bruteforce application interface with three main tabs: TARGETS, CREDENTIALS, and OPTIONS. The CREDENTIALS tab is active, showing options for credential combinations and a list of services. A red arrow points to the 'Use username as password' checkbox, which is checked.

TARGETS

0 targets selected

Selected Host(s):

- ☒ All hosts
- ☐ Enter target addresses

Select services:

- ☒ All services
- ☒ AFP
- ☒ HTTP
- ☒ MySQL
- ☒ SMB
- ☒ SSH PUBKEY
- ☒ WinRM
- ☒ DB2
- ☒ HTTPS
- ☒ POP3
- ☒ SNMP
- ☒ Telnet
- ☒ FTP
- ☒ MSSQL
- ☒ Postgres
- ☒ SSH
- ☒ VNC

CREDENTIALS

0 possible combinations

- ☐ All credentials in this project
- ☐ Attempt factory defaults
- ☒ Add/Import credential pairs

Credentials (100 lines max)

Enter a space and new line delimited list of credential pairs.

Example:

```
username pass
username pass1 pass2
realm/username pass
realm/username pass1 pass2
```

Import Credentials from a file:

No file selected... Choose ...

☐ Use <BLANK> as password

☒ Use username as password

OPTIONS

Overall Timeout: 4 Hours 0 Minutes 0 Seconds

Service Timeout: 900 Seconds

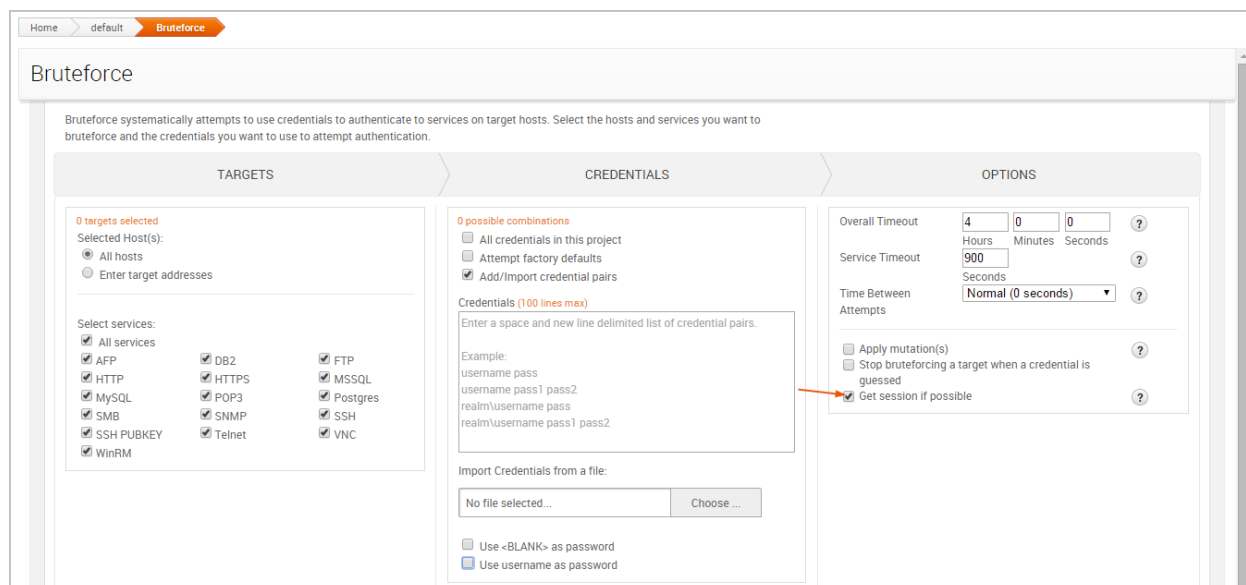
Time Between Attempts: Normal (0 seconds)

- ☐ Apply mutation(s)
- ☐ Stop bruteforcing a target when a credential is guessed
- ☐ Get session if possible

Получение доступа на основе предполагаемых настроек по умолчанию

Наряду с использованием предполагаемых настроек у Bruteforce есть опция открытия сессии в случае успешного подбора аутентификационных данных по умолчанию для доступа к определённым системам таким как MSSQL, MySQL, PostgreSQL, SMB, SSH, Telnet, WinRM, и некоторым HTTP сервисам, среди которых Tomcat, Axis2, или GlassFish. Открытые сессии могут использоваться для выполнения различных задач по эксплуатации сервиса, которые обычно встречаются на практике при компрометации: например, сбор дополнительной информации с хостинга и переноса данных на новые хосты.

Для открытия сервисов после успешного взлома настроек по умолчанию программой Bruteforce необходимо подключить опцию «Доступы к системе», если такая опция предусмотрена и указать количество доступов, которое необходимо использовать, как показано на примере ниже. Эта сессия будет оставаться открытой после завершения хакерской атаки, и её можно будет использовать для выполнения дальнейших действий.



Настройка выполняемых действий на случай взломов программой Bruteforce

Для настройки выполняемых действий на скомпрометированной системе можно воспользоваться следующими опциями:

- Тип входов: эта опция определяет тип входов после взлома системы. Можно выбрать одну из следующих опций:
- Meterpreter: эта расширенная многофункциональная начинка, которая может быть расширена при использовании и добавлять новые особенности по мере необходимости: расширять доступы, использовать функцию «dump password hashes», делать скриншоты, запускать и менять процессы и переносить файлы в новое место. В Meterpreter также есть оболочка управления для выполнения базовых заданий, таких как добавление новых аккаунтов пользователей или запуска скриптов.

Meterpreter также динамически запускается в существующих процессах используя технологию под названием «отражённая DLL инъекция», с помощью которой Meterpreter остаётся в памяти системы и его нельзя обнаружить системами предупреждения и обнаружения взломов.

- Command: эта функция предоставляет возможность запуска единичных команд на хостинге для выполнения простых задач, среди которых добавление новых аккаунтов пользователей или смена паролей. Эта управленческая оболочка предоставляет ограниченный доступ, но может быть обновлена до уровня оболочки Meterpreter для получения расширенного списка опций.

В отличие от Meterpreter, у этой оболочки есть опция запуска новых функций, которые можно легко обнаружить системами предупреждения и обнаружения взломов.

- Connection: Эта опция определяет как ваш Metasploit instance подключается к хостингу. Можно выбрать одну из следующих опций:
- Auto: Этот тип соединения использует систему обратного подключения при обнаружении NAT или файрвола; в других случаях используется bind-подключение.
- Bind – Этот тип подключения использует bind подключение. Необходимо использовать такой тип подключения при наличии прямого не запрещённого подключения к целевому хостингу.
- Reverse: Этот тип использует обратное подключение. Необходимо выбирать такое подключение, если хостинг находится за файрволом или NAT шлюзом, который будет предотвращать запросы от Metasploit instance на целевой хостинг.

- Контрольные порты: Эта опция определяет порты, используемые админом для ожидания будущих соединений. можно указать конкретный порт или несколько портов через запятую или целый набор портов. при указании набора портов из списка будет выбираться первый доступный порт.
- Контрольный хост: Эта опция определяет IP-адрес на который перенаправляется целевой хост. Обычно идёт речь о внешних IP локального сервера. При отсутствии указанного контрольного хоста используется внешний IP адрес локального сервера.

Настройка периода выполнения для атаки с помощью Bruteforce

Есть возможность контроля временного промежутка для общей задачи bruteforce и каждого конкретного сервиса. Вы можете настроить период выполнения с помощью опции «Действие Bruteforce» как показано ниже:

The screenshot shows the Bruteforce configuration window with three tabs: TARGETS, CREDENTIALS, and OPTIONS. The OPTIONS tab is active, and a red box highlights the timeout settings. The settings are as follows:

Setting	Value	Unit
Overall Timeout	HH:MM:SS	Hours, Minutes, Seconds
Service Timeout	SS	Seconds
Time Between Attempts	Normal (0 seconds)	Dropdown menu

Other options visible in the OPTIONS tab include:

- ☐ Apply mutation(s)
- ☐ Stop bruteforcing a target when a credential is guessed
- ☐ Get sessions if possible

A blue LAUNCH button is located at the bottom right of the configuration area.

Для настройки периода выполнения доступны следующие опции:

- Сервисный период – устанавливает период выполнения в минутах для каждого сервиса.
- Общий период- устанавливает максимальный период времени в минутах для запуска bruteforce. При подключении опции общего простоя программа Bruteforce будет использовать максимум попыток в установленный период. Bruteforce не сможет воспользоваться всеми попытками, если установлены временные лимиты.
- Период простоя между попытками – устанавливает время простоя в секундах между каждыми попытками входа. Вы можете один из представленных временных лимитов: нормальный (0 секунд), скрытый (5 секунд), Медленный (10 секунд), и сверх-медленный (60 секунд).

При отсутствии настроек временных рамок, «Рабочий процесс Bruteforce» устанавливается по умолчанию на 0 и не регулирует временные рамки.

Применение правил мутации для атак с помощью программы Bruteforce

В большинстве случаев организации используют различные вариации для настроек аккаунта по умолчанию или используют leetspeak в качестве иконок. Для выполнения определённых сценариев можно использовать правила мутаций для создания различных перестановок по настройкам приватности.

Правило мутации прибавляет, добавляет к началу и заменяет символы в настройках приватности. Эти настройки приватности можно эффективно использовать для создания большего списка паролей, используя установленную базу слов. Например, если вы определили, что организация обычно использует пароли с названием компании, вы можете добавить название компании в список и использовать мутации для автоматической генерации различных вариаций. Таким образом, в зависимости от применяемых правил мутации настройки конфиденциальности как "myscompany" могут иметь несколько вариаций наподобие "myscompany2014", "myscompany1", "myscomp@ny" и т.д.

Существует несколько различных типов правил мутации, доступных для применения. Например, присоединение цифр в конец/в начало к скрытому значению, применение leetspeak-замен к скрытому значению и присоединение текущего года в конец или в начало к скрытому значению. Правила мутации по умолчанию отключены, поэтому нужно включить опцию мутации и выбрать правила, которые планируется использовать. После активации правил мутации они будут применены к учётным данным, которые были выбраны для брутфорс-атаки

Применение leetspeak-замен

Leetspeak - альтернативный алфавит, который можно использовать для замены букв спецсимволами и цифрами.

Активация опции **1337 speak** позволяет выполнить отдельные leetspeak-замены применительно к скрытому значению. При активации опции **1337 speak** в отношении каждого скрытого значения применяются следующие правила:

- Правило мутации меняет все вхождения буквы "a" на "@".
- Правило мутации меняет все вхождения буквы "a" на "4".
- Правило мутации меняет все вхождения буквы "e" на "3".
- Правило мутации меняет все вхождения буквы "l" на "1".
- Правило мутации меняет все вхождения буквы "o" на "0".
- Правило мутации меняет все вхождения буквы "s" на "5".
- Правило мутации меняет все вхождения буквы "s" на "\$".
- Правило мутации меняет все вхождения буквы "t" на "7".

Каждое правило leetspeak применяется индивидуально. Например, если скрытым значением является "myscompany", то правило мутации leetspeak создает две замены: "mys0mpany" и "myscomp@ny". Система не комбинирует правила leetspeak для создания "mys0mp@ny".

Присоединение спецсимволов в начало (!#*)

Активация опции **Prepend Special Characters** позволяет присоединить спецсимвол к началу скрытого значения. При активации правило присоединяет восклицательный знак (!), хэш-символ (#), амперсанд (&) и звездочку (*) в начало скрытого значения. Например, если скрытым значением является "mycompany", создаются следующие перестановки: "!mycompany", "#mycompany", "&mycompany" и "*mycompany".

Присоединение спецсимволов в конец (!#*)

Активация опции **Append Special Characters** позволяет присоединить спецсимвол к концу скрытого значения. При активации правило присоединяет восклицательный знак (!), хэш-символ (#), амперсанд (&) и звездочку (*) в конец скрытого значения. Например, если скрытым значением является "mycompany", создаются следующие перестановки: "mycompany!", "mycompany#", "mycompany&" и "mycompany*".

Присоединение одноразрядного числа в начало

Активация опции **Prepend a Single Digit** позволяет присоединить одноразрядное число к началу скрытого значения. При активации правило присоединяет числа от 0 до 9 в начало скрытого значения. Например, если скрытым значением является "mycompany", создаются следующие перестановки: "mycompany0", "mycompany1", "mycompany2", "mycompany3" и так далее.

Присоединение одноразрядного числа в конец

Активация опции **Append Single Digit** позволяет присоединить одноразрядное число к концу скрытого значения. При активации правило присоединяет числа от 0 до 9 в конец скрытого значения. Например, если скрытым значением является "mycompany", создаются следующие перестановки: "0mycompany", "1mycompany", "2mycompany", "3mycompany" и так далее.

Присоединение чисел в начало

Активация опции **Prepend Digits** позволяет присоединить три числа к началу скрытого значения. Например, если скрытым значением является "mycompany", создаются следующие перестановки: "mycompany000", "mycompany001", "mycompany002", "mycompany003" и так далее.

Примечание: При активации это правило может сгенерировать до 1000 перестановок применительно к одному скрытому значению.

Присоединение чисел в конец

Активация опции **Append Digits** позволяет присоединить три числа к концу скрытого значения. Например, если скрытым значением является "mycompany", создаются следующие перестановки: "000mycompany", "001mycompany", "002mycompany", "003mycompany" и так далее.

Примечание: При активации это правило может сгенерировать до 1000 перестановок применительно к одному скрытому значению.

Присоединение текущего года в начало

Активация опции **Prepending Current Year** позволяет присоединить текущий год к началу скрытого значения. Например, если скрытым значением является "myscompany", создаются следующие перестановки: "2014myscompany", "2014myscompany", "2014myscompany", "2014myscompany" и так далее.

Присоединение текущего года в конец

Активация опции **Append Current Year** позволяет присоединить текущий год к концу скрытого значения. Например, скрытым значением является "myscompany", будут созданы следующие перестановки: "myscompany2014", "myscompany2014", "myscompany2014", "myscompany2014" и так далее.

Запуск брутфорс-атаки

Кнопка запуска на странице конфигурации брутфорса активируется, когда заполняются все обязательные поля. При готовности запустить брутфорс-атаку, нажмите кнопку "Запустить" / Launch.

Bruteforce

Bruteforce systematically attempts to use credentials to authenticate to services on target hosts. Select the hosts and services you want to bruteforce and the credentials you want to use to attempt authentication.

TARGETS

CREDENTIALS

OPTIONS

64 targets selected

Select Host(s):

☒ All hosts
 ☐ Enter target addresses

Select Services:

☒ All Services
☒ AFP ☒ MSSQL ☒ SNMP
☒ DB2 ☒ MySQL ☒ SSH
☒ FTP ☒ POP3 ☒ Telnet
☒ HTTP ☒ Postgres ☒ VNC
☒ HTTPS ☒ SMB ☒ WinRM

778 possible combinations

☒ All credentials in this project
☐ Attempt factory defaults
☐ Add Import credential pairs

Overall Timeout

HH

MM

SS

?

Hours Minutes Seconds

Service Timeout

SS

?

Seconds

Time Between Attempts

Normal (0 seconds)

▼

?

☐ Apply mutation(s) ?

☒ Stop bruteforcing a target when a credential is guessed

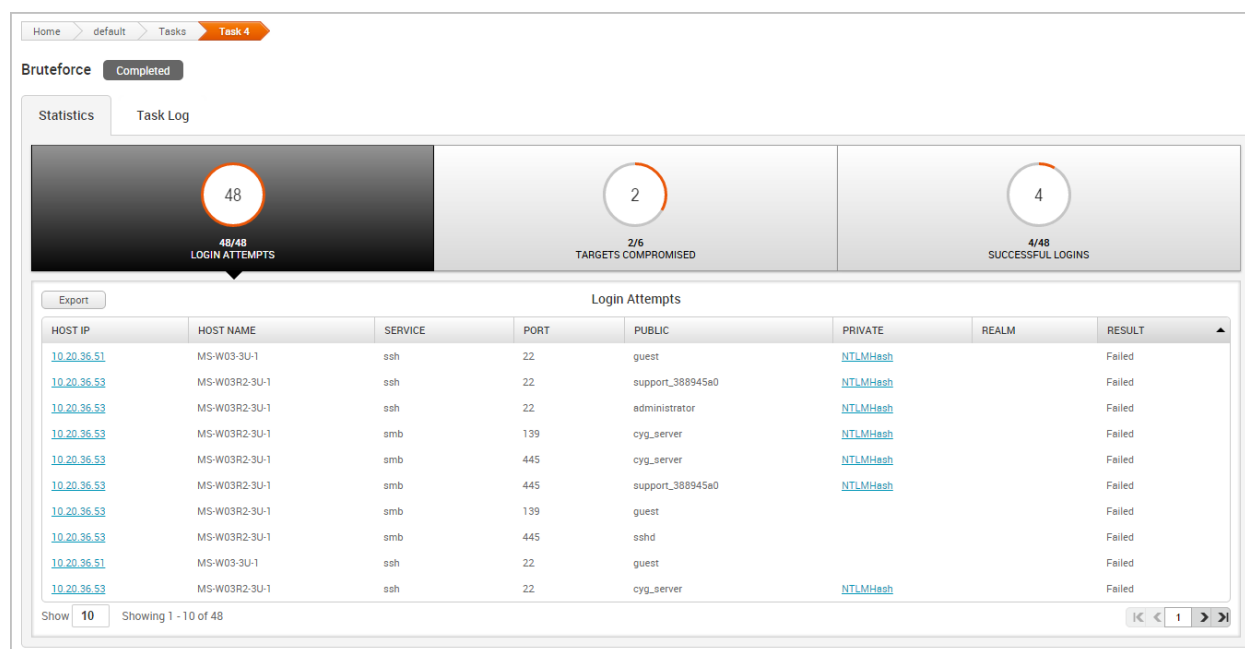
☐ Get sessions if possible ?

LAUNCH

При возникновении каких-либо проблем с конфигурацией атаки, рядом с некорректно настроенным параметром появится предупреждение. Чтобы появилась возможность запустить брутфорс-атаку, необходимо устранить проблему.

Трактовка результатов брутфорса

После запуска брутфорс-атаки появляется окно результатов, в котором в режиме реального времени отображаются результаты атаки и связанные с ней события. Чтобы упростить ознакомление с данными, окно результатов состоит из двух основных вкладок: вкладки "Статистика" / Statistics и вкладки "Журнал регистрации задач" / Task Log.

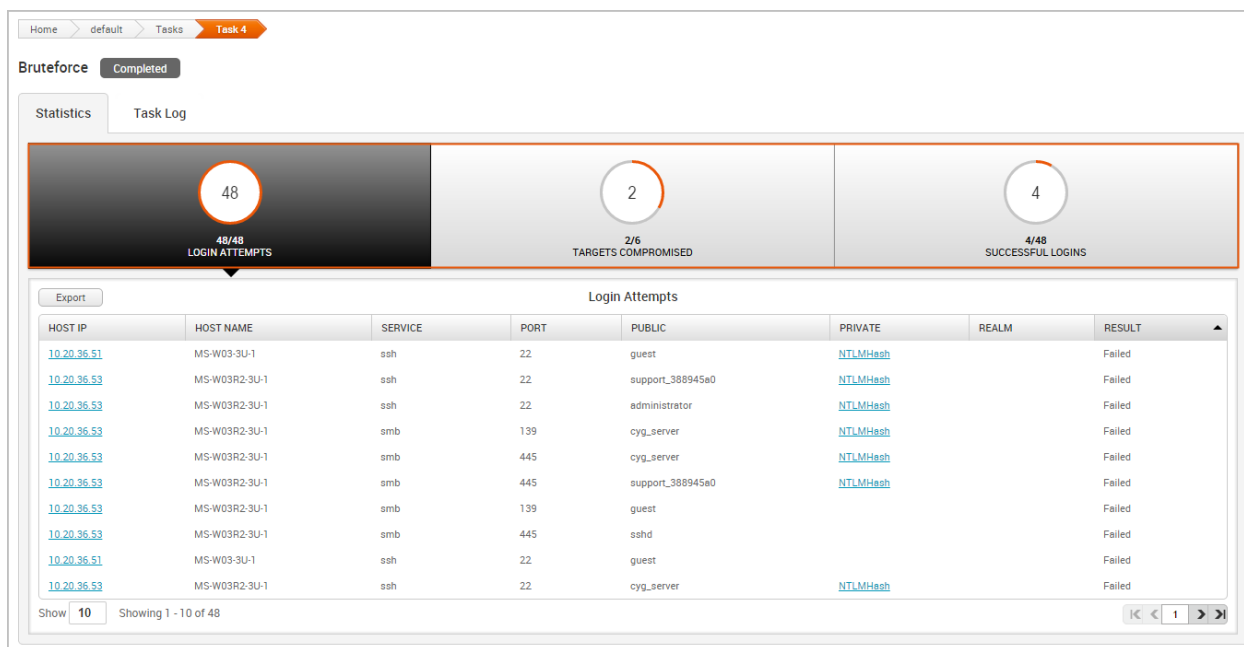


Вкладка статистики

Вкладка "Статистика" / Statistics позволяет вести мониторинг результатов в режиме реального времени в разрезе следующих параметров:

- Общее количество попыток логина.
- Общее количество скомпрометированных целей.
- Общее количество успешных логинов.

Каждый статистический показатель отображается в отдельной вкладке. Можно кликнуть по вкладке, чтобы просмотреть соответствующую таблицу для каждого статистического показателя.



Просмотр таблицы попыток логина

В таблице "Попытки логина" / Login Attempts отображается каждый логин, попытка осуществить который была предпринята в ходе брутфорс-атаки. Для каждого логина указана следующая информация:

- IP каждого хоста
- Имя хоста
- Имя службы
- Служебный порт
- Открытое значение
- Скрытое значение
- Тип области применения приложения
- Результат попытки входа в систему

Просмотр таблицы скомпрометированных целей

Таблица "Скомпрометированные цели" / Targets Compromised отображает каждую цель, в случае которой в ходе брутфорс-атаки удалось успешно пройти аутентификацию. Для каждой скомпрометированной цели указана следующая информация:

- IP хоста
- Имя хоста
- Операционная система
- Имя сервиса
- Сервисный порт

- Количество захваченных учёных данных
- Сеансы *

* Если брутфорс-атака будет предварительно настроена для получения сеансов, таблица Targets Compromised будет включать столбец "Сеансы" / Sessions, в котором указано общее количество сеансов, открытых в рамках каждой цели. Можно навести курсор на счетчик сеансов, чтобы просмотреть список ссылок для доступа к странице подробных сведений по каждому сеансу.

Просмотр таблицы успешных логинов

В таблице "Успешные логины" / Successful Logins отображаются все логины, валидация которых с помощью брутфорс-атаки завершилась успехом. Для каждого логина указана следующая информация:

- IP хоста
- Имя хоста
- Операционная система
- Имя сервиса
- Сервисный порт
- Открытое значение
- Скрытое значение
- Тип области применения приложения
- Детали сеанса *

* Если брутфорс-атака будет предварительно настроена для получения сеансов, таблица Targets Compromised будет включать столбец "Переход к сеансам" / Go to Sessions, в котором отображается ссылка для каждого открытого сеанса. Можно кликнуть по ссылке, чтобы перейти к странице с подробной информацией о сеансе. Если вы не настроили брутфорс-атаку для получения сеансов, в таблице Targets Compromised будет столбец "Попытка сеанса" / Attempt Session, который позволяет провести валидацию логина из окна результатов.

Вкладка журнала регистрации задач

Журнал регистрации задач используется для отслеживания активности в рамках брутфорс-атаки. В нем приводится информация о цели, которая подвергается брутфорсу и результат для каждой попытки угадывания перебором. Успешный логин будет выделен желтым цветом, как показано ниже:

Bruteforce Findings

Statistics

Task Log

Bruteforce	Complete	Started: 2014-04-18 16:28:15 UTC Duration: 9 minutes
------------	----------	---

```

[*] [2014.12.03-14:23:00] Preparing attack space...
[*] [2014.12.03-14:23:00] Starting Bruteforce of 3 services of types: SMB SSH
[*] [2014.12.03-14:23:00] 10.20.36.53:445 SUCCESSFUL - WORKSTATION\administrator:e2fc15074bf7751dd408e6b105741864:a1074a69b1bde45403ab680504bbdd1a
[*] [2014.12.03-14:23:00] 10.20.36.53:139 SUCCESSFUL - WORKSTATION\administrator:e2fc15074bf7751dd408e6b105741864:a1074a69b1bde45403ab680504bbdd1a
[*] [2014.12.03-14:23:00] 10.20.36.53:22 INCORRECT - administrator:
[*] [2014.12.03-14:23:01] 10.20.36.53:445 INCORRECT - WORKSTATION\admin:1234
[*] [2014.12.03-14:23:01] 10.20.36.53:445 INCORRECT - WORKSTATION\admin:admin
[*] [2014.12.03-14:23:01] 10.20.36.53:139 INCORRECT - WORKSTATION\admin:1234
[*] [2014.12.03-14:23:01] 10.20.36.53:445 INCORRECT - WORKSTATION\admin:changeme123
[*] [2014.12.03-14:23:01] 10.20.36.53:445 INCORRECT - WORKSTATION\admin:password
[*] [2014.12.03-14:23:01] 10.20.36.53:139 INCORRECT - WORKSTATION\admin:admin
[*] [2014.12.03-14:23:01] 10.20.36.53:445 INCORRECT - WORKSTATION\admin:password1
[*] [2014.12.03-14:23:01] 10.20.36.53:139 INCORRECT - WORKSTATION\admin:changeme123
[*] [2014.12.03-14:23:01] 10.20.36.53:22 INCORRECT - admin:1234
[*] [2014.12.03-14:23:01] 10.20.36.53:445 INCORRECT - WORKSTATION\admin:password123
[*] [2014.12.03-14:23:01] 10.20.36.53:139 INCORRECT - WORKSTATION\admin:password
[*] [2014.12.03-14:23:01] 10.20.36.53:445 INCORRECT - WORKSTATION\admin:password123!

```

Журнал регистрации задач также используется для документирования любых ошибок или сбоев, которые произошли во время атаки, и может использоваться для устранения любых проблем, связанных проведением брутфорса. Это особенно полезно, если, к примеру, атака велась в течение длительного времени, наблюдаются "зависания", или работа системы не завершается.

Заданные пользователем мутации элемента учетных данных

Мутации элемента учетных данных модифицируют пароли в списке слов. Вы можете использовать их для создания многочисленных перестановок пароля, таких как замена букв цифрами (когда "password" превращается в "passw0rd"), что позволяет создавать большой список слов на основе небольшого набора паролей. Мутации элемента учетных данных также позволяют добавлять числа и спецсимволы к паролю, менять строчные буквы на прописные (и обратно), а также управлять длиной пароля.

Metasploit Pro предлагает несколько готовых мутаций, которые можно использовать "из коробки". Однако при желании создать заданный пользователем список учётных данных, подвергшихся мутации, нужно будет пропустить свой список слов через инструмент для взлома паролей вроде John the Ripper. John the Ripper применит набор правил модификации к списку слов и выдаст список подвергшихся мутации учётных данных, которые затем можно будет импортировать в проект.

John the Ripper

John the Ripper - бесплатный инструмент для взлома паролей, который доступен пользователям многих разновидностей Unix, Windows, DOS, BeOS и OpenVMS. John the Ripper обычно используется для обнаружения слабых паролей и хэшей, но его также можно применять для генерации подвергшегося мутации списка слов с целью последующего импорта в Metasploit Pro для использования функции Bruteforce Guess.

Скачивание и установка John the Ripper

Установочный пакет Metasploit включает двоичные файлы John the Ripper 1.7.8, которые расположены по адресу `path/to/metasploit/apps/pro/msf3/data/john`. Чтобы запустить John the Ripper, нужно просто вызвать двоичный файл в каталоге, из которого запускается инструмент, для обработки цели. Если понадобится наиболее свежая версия John the Ripper, нужно будет установить ее. Комплексная инструкция по установке John the Ripper расположена по адресу <http://www.openwall.com/john/doc/INSTALL.shtml>. Однако при желании изучить этот процесс помощью настоящего руководства продолжайте чтение.

Для начала нужно будет скачать John the Ripper по адресу <http://www.openwall.com/john/>. Доступны бесплатная, улучшенная членами сообщества и коммерческая версии John the Ripper. Загрузите подходящую версию для своей системы.

John the Ripper распространяется в основном в форме исходного кода и загружается в виде архивного файла. После загрузки архивного файла нужно будет извлечь его содержимое. Чтобы запустить John the Ripper, просто вызовите приложение из места извлечения.

Установка John the Ripper в Linux

Откройте терминал и введите следующее:

```
sudo -sH
cd /opt
wget http://www.openwall.com/john/j/john-1.8.0.tar.gz
tar -xvzf john-1.8.0.tar.gz
mv john-1.8.0 john
rm john-1.8.0.tar.gz
```

Примечание. При использовании иной версии John the Ripper замените 1.8.0 на версию, которую вы используете.

```
cd /opt/john/src
make
```

Команда `make` отображает список целей. Выберите оптимальную для своей архитектуры и повторите команду `make` с выбранным вами объектом. Например, для системы x86-64 для Linux введите следующее:

```
make clean linux-x86-64
```

Теперь John the Ripper установлен на вашей Linux-системе и готов к использованию.

Установка John the Ripper в Windows

1. Перейдите на <http://www.openwall.com/john> и скачайте самый свежий установочный пакет для Windows.

Бинарные файлы для Windows будут доступны в ZIP-файле.

2. Разместите скачанный файл на диске C: \. Результирующая директория будет иметь примерно такой вид
C:\john179.

При использовании другой версии John the Ripper замените john179 на версию, которую вы используете.

3. Переименуйте директорию в john. Результирующая директория будет выглядеть следующим образом C:\john.

Теперь John the Ripper установлен на вашей Windows-системе и готов к использованию.

Использование John the Ripper в Linux

Откройте терминал командной строки и введите следующее:

```
sudo -sH
cd /path/to/john/run
./john
```

Примечание: Замените /path/to/ адресом установки John the Ripper.

John the Ripper отобразит список доступных опций. Для получения дополнительной информации об опциях John the Ripper посетите <http://www.openwall.com/john/doc/OPTIONS.shtml>.

Использование John the Ripper в Windows

Откройте терминал командной строки (**Start > Run > cmd**) и введите следующее:

```
cd \path\to\john\run
john
```

Примечание: Замените \path\to\ адресом установки John the Ripper.

John the Ripper отобразит список доступных опций. Для получения дополнительной информации об опциях John the Ripper посетите <http://www.openwall.com/john/doc/OPTIONS.shtml>.

Заданные пользователем правила мутации

После установки John the Ripper и подтверждения работоспособности этого инструмента, нужно добавить правила мутации в конфигурационный файл John the Ripper. Правило позволяет выполнить определенный тип мутации в отношении слова. Например, можно создать правило, которое присоединяет конкретные спецсимволы вроде [!@#%&*()+=.?] в конец каждого слова в списке слов.

Чтобы определить заданные пользователем правила мутации, нужно будет создать наборы правил в конфигурационном файле John the Ripper. Набор правил - это логическая группировка связанных правил мутации. Все правила мутации должны содержаться в наборе правил. Например, нужно создать отдельные наборы правил для правил, которые присоединяют символы в конец, правил, которые присоединяют символы в начало, и правил, которые управляют длиной символов. Нужно будет представить набор правил как часть параметра правил при создании списка слов как следующем примере:

```
./john --wordlist=[path to word list] --stdout --rules:[ruleset name] > [path to output list]
```

Требования к заданному пользователем набору правил

Каждый раздел с набором правил должен начинаться с типа и имени такого набора, заключенных в скобки. При работе с набором правил нужно использовать следующий формат: [List. Rules: <name>], где <name> заменяется именем набора правил.

Например, при наличии набора правил с именем AppendLowercaseNumbers раздел в конфигурационном файле John the Ripper должен быть прописан следующим образом [List.Rules:AppendNumbers].

Таким образом, ваш набор правил будет выглядеть примерно так:

```
[List.Rules:AppendLowercaseNumbers]
#lowercase and add numbers to the end of a password
I$[0-9]
I$[0-9]$[0-9]
I$[0-9]$[0-9]$[0-9]
I$[0-9]$[0-9]$[0-9]$[0-9]
```

Вот несколько дополнительных правил форматирования, которые следует запомнить:

- Названия разделов не являются регистрозависимыми.
- Строки комментариев начинаются с хэша (" #") или точки с запятой (" ;").
- Пустые строки игнорируются.
- Наборы правил могут быть размещены в произвольной части конфигурационного файла John the Ripper, но рекомендуется добавлять их в нижнюю часть файла.

[Получение доступа к файлу конфигурации John the Ripper](#)

Чтобы получить доступ к конфигурационному файлу John the Ripper, перейдите в директорию /path/to/john/run. Файл конфигурации будет называться john.conf либо john.ini - в зависимости от вашей операционной системы. Нужно открыть файл конфигурации с помощью текстового редактора вроде Vim (Linux) или "Блокнота" (Windows).

```
sudo -sH
cd /opt/john/run
vim john.conf
```

В случае отсутствия Vim можно установить его с помощью следующей команды: apt-get install vim.

Файл конфигурации состоит из нескольких разделов. Каждый раздел имеет уникальную функцию, и ему присваивается имя раздела, заключенное в квадратные скобки, как показано ниже:

```
# This file is part of John the Ripper password cracker,
# Copyright (c) 1996-2006,2008-2013 by Solar Designer
#
# Redistribution and use in source and binary forms, with or without
# modification, are permitted.
#
# There's ABSOLUTELY NO WARRANTY, express or implied.
#
# Please note that although this configuration file is under the cut-down BSD
# license above, many source files in John the Ripper are under GPLv2.
# For licensing terms for John the Ripper as a whole, see doc/LICENSE.
#

[Options]
# Wordlist file name, to be used in batch mode
Wordlist = $JOHN/password.lst
# Use idle cycles only
Idle = Y
# Crash recovery file saving delay in seconds
Save = 600
# Beep when a password is found (who needs this anyway?)
Beep = N

# "Single crack" mode rules
[List.Rules:Single]
# Simple rules come first...
:
-s x**
-c (?a c Q
-c l Q
-s-c x** /?u l
```

Основные синтаксические правила John the Ripper

У John the Ripper имеется отличная документация, в которой объясняется синтаксис для построения правил. Дополнительные сведения об этом можно получить, перейдя по адресу <http://www.openwall.com/john/doc/RULES.shtml>. Настоятельно рекомендуется изучить эту документацию, прежде чем создавать свои собственные заданные пользователем правила.

Чтобы помочь вам приступить к работе, кратко рассмотрим некоторые потенциально полезные команды:

- \$ присоединяет в конец слова символ или число. Можно определить один символ, например, \$1, который присоединит цифру 1 в конец к паролю. Также можно определить группу символов, например \${0-9}, которая присоединит 0, 1, 2, 3, 4, 5, 6, 7, 8 и 9 в конец к паролю.
- ^ присоединяет в начало слова символ или число. Можно определить один символ, например, ^1, который присоединит цифру 1 в начало к паролю. Также можно определить группу символов,

например `$[0-9]`, которая присоединит 0, 1, 2, 3, 4, 5, 6, 7, 8 и 9 в начало к паролю.

- `l` преобразует все буквы в слове в буквы нижнего регистра.
- `s` преобразует все буквы в слове в буквы верхнего регистра.
- `C` меняет регистр первого символа в слове на нижний, а регистр остальных – на верхний.
- `t` меняет регистр всех символов в слове на противоположный.

Допускается использование произвольной комбинации команд внутри правила. Например, можно создавать правила, которые присоединяют цифры в начало и в конец к паролю. Например, `^[0-9]$[0-9]`. Каждое правило должно прописываться в новой строке.

Создание заданных пользователем правил мутации

Продолжим, добавляя некоторые правила мутации в конфигурационный файл John the Ripper.

Рассмотрим следующие мутации:

- Присоединение в конец пароля цифры.
- Присоединение в начало пароля цифры.
- Присоединение в конец пароля спецсимволов.
- Присоединение в начало пароля спецсимволов.
- Смена регистра пароля на нижний и присоединение к нему спецсимволов и цифр.
- Смена регистра пароля на верхний и присоединение к нему спецсимволов и цифр.

Чтобы добавить эти правила, откройте конфигурационный файл John the Ripper с помощью текстового редактора и прокрутите вниз до конца файла. Можно скопировать и вставить любое из этих правил в конфигурационный файл John the Ripper или использовать их в качестве примеров для создания собственных правил. Не забудьте сохранить изменения после добавления правил в конфигурационный файл John the Ripper.

Примечание: Прежде чем вносить какие-либо изменения в конфигурационный файл John the Ripper, сделайте копию исходного файла на случай необходимости восстановления значений.

Присоединение в конец пароля цифр

```
[List.Rules:AppendNum]
```

```
#Appends one, two, and three numbers to a password $[0-9]
```

```
$[0-9]$[0-9]
```

```
$[0-9]$[0-9]$[0-9]
```

Присоединение в начало пароля цифр

```
[List.Rules:PrependNum]
```

```
#Prepends one, two, and three numbers to a password
```

```
^[0-9]
```

```
^[0-9]^[0-9]
```

```
^[0-9]^[0-9]^[0-9]
```

Присоединение в конец пароля спецсимволов

```
[List.Rules:AppendSpecialChar]
```

```
#Appends one, two, and three special character to a password
```

```
$[!@#%&*()+=.~?]
```

```
$[!@#%&*()+=.~?]$[!@#%&*()+=.~?]
```

```
$[!@#%&*()+=.~?]$[!@#%&*()+=.~?]$[!@#%&*()+=.~?]
```

Присоединение в начало пароля спецсимволов

```
[List.Rules:PrependSpecialChar]
```

```
#Prepends one, two, and three special character to a password
```

```
^[!@#%&*()+=.~?]
```

```
^[!@#%&*()+=.~?]^[!@#%&*()+=.~?]
```

```
^[!@#%&*()+=.~?]^[!@#%&*()+=.~?]^[!@#%&*()+=.~?]
```

Смена регистра пароля на нижний и присоединение к нему цифр и спецсимволов

```
[List.Rules:LowercaseNumChar]
```

```
#Lowercases all of the letters of the password and adds a number and/or special character to it
```

```
|
```

```
|$[0-9]
```

```
|$[0-9]$[0-9]
```

```
|$[!@#%&*()+=.~?]
```

```
|$[!@#%&*()+=.~?]$[!@#%&*()+=.~?]
```

```
|$[0-9]$[!@#%&*()+=.~?]
```

```
|$[0-9]$[0-9]$[!@#%&*()+=.~?]$[!@#%&*()+=.~?]
```

Смена регистра пароля на верхний и присоединение к нему цифр и спецсимволов

```
List.Rules:UppercaseNumChar]
```

#Uppercases all of the letters of the password and adds a number and/or special character to it

```
u
u$[0-9]
u$[0-9]$[0-9]
u$[!@#%&^*()+=?.?]
u$[!@#%&^*()+=?.?]$[!@#%&^*()+=?.?]
u$[0-9]$[!@#%&^*()+=?.?]
u$[0-9]$[0-9]$[!@#%&^*()+=?.?]
```

Генерация подвергнувшегося мутации списка слов

При готовности создать подвергшийся мутации список слов нужно будет выполнить следующее: --wordlist= [path to the pre-mutated wordlist] --stdout --rules:[rule set name] > [path to the generated list]. Нужно будет вызвать John the Ripper, используя соответствующий метод для вашей операционной системы.

John the Ripper сгенерирует список слов, используя указанные вами правила. При желании применить все правила в файле конфигурации к списку слов можно просто указать опцию -rules.

Генерация списка слов в Linux

```
./john --wordlist=[path to the wordlist] --stdout --rules:[rule set name]
> [path to the generated list]
```

Квадратные скобки и их содержимое нужно заменить соответствующей информацией. Например:

```
./john --wordlist=password.lst --stdout --rules:PrependSpecialChar >
/home/usr/Desktop/mutatedpswds.lst
```

Генерация списка слов в Windows

```
john --wordlist=[path to the wordlist] --stdout --rules:[rule set name] > [path to the generated list]
```

Квадратные скобки и их содержимое нужно заменить соответствующей информацией. Например:

```
john --wordlist=password.lst --stdout --rules:PrependSpecialChar > /Desktop/mutatedpswds.lst
```

Импорт списков слов из John the Ripper в проект

Теперь, когда у вас есть подвергнутый мутации список слов, можете импортировать его в проект и использовать при брутфорсе.

1. Перейдите на экран "Управление учётными данными" / **Manage Credentials**.
2. Нажмите кнопку "Добавить" / **Add**.
3. Когда появится окно "Добавить учётные данные" / **Add Credentials**, выберите опцию "Импорт" / **Import**.
4. Нажмите кнопку "Обзор" / **Browse** и перейдите к расположению списка слов, который вы хотите импортировать. Это должен быть .txt-файл или .lst-файл.
5. Выберите файл и нажмите "Открыть" / **Open**.
6. В окне "Добавить учётные данные" в качестве формата выберите "Список слов" / **Wordlist**.
7. Выберите раскрывающееся меню "Тип файла" / **File Type** и выберите "Пароли" / **Passwords**.
8. Введите теги для паролей в списке слов (опционально).

Теги помогут легко найти и идентифицировать определенные пароли. Чтобы ввести тег, начните вводить имя тега, который хотите использовать в поле "Тег" / **Tag**. При вводе информации в поле поиска Metasploit Pro автоматически прогнозирует теги, которые могут быть похожи на те, которые вы ищете. Если тега не существует, Metasploit Pro создает его.

9. Нажмите **OK**.

Список слов импортируется в проект. Вы можете перейти на страницу "Управление учётными данными" / **Manage Credentials**, чтобы просмотреть импортированные учётные данные.

Credentials Domino MetaModule

Модуль Credentials Domino MetaModule позволяет определить, насколько далеко может проникнуть злоумышленник в сети, если ему удастся получить конкретный элемент учетных данных. Этот модуль выполняет итеративную атаку на основе учетных данных для определения направлений атаки, возможность осуществления которых возникает при условии успешного перехвата сеанса или захвата элемента учетных данных с определенного хоста. Модуль призван помочь при оценке влияния атаки на основе учётных данных, информируя пользователя о количестве хостов, которые могут быть скомпрометированы, и количестве уникальных учётных данных, которые могут быть захвачены за счет использования конкретного элемента учетных данных.

Чтобы запустить MetaModule Credentials Domino, в распоряжении проекта должен быть, как минимум, один действительный логин или один открытый сеанс, который можно рассматривать в качестве отправной точки. Как уже упоминалось ранее, Credentials Domino MetaModule выполняет итеративную атаку. Это означает, что модуль многократно циклически проходит по сети и пытается аутентифицировать каждый хост с помощью разных элементов учетных данных. Каждая итерация

представляет собой один циклический проход по сети с применением уникального элемента учетных данных. Модуль Credentials Domino MetaModule продолжает работать до тех пор, пока не откроет сеанс на каждом целевом хосте или не достигнет условия прерывания.

Во время первой итерации, если вы решите начать с действующего логина, MetaModule Credentials Domino сразу же попытается использовать его для аутентификации и открытия сеанса на каждом целевом хосте. Если Credentials Domino MetaModule удастся успешно пройти аутентификацию и открыть сеанс, метамодуль захватывает учетные данные от хоста и сохраняет их в проекте. После успешного открытия метамодулем сеанса на хосте, он больше не будет пытаться взаимодействовать с соответствующим хостом. Однако если пользователь решит начать с открытого сеанса, MetaModule начнет со сбора учётных данных из сеанса. Затем он будет пробовать воспользоваться каждым захваченным элементом учетных данных, пока не сможет найти успешный логин. Метамодуль использует успешный элемент учетных данных для запуска следующей итерации.

Чтобы помочь пользователям при оценке влияния на сеть, метамодуль предлагает специализированный отчет, в котором документируются технические выводы и результаты атаки. Кроме того, модуль в режиме реального времени демонстрирует результаты по скомпрометированным хостам и захваченным учетным данным через окно результатов, а также предлагает визуализацию паттернов атак, установить возможность проведения, которых модулю Credentials Domino MetaModule удалось после анализа целевой сети.

Получение доступа к Credentials Domino MetaModule

Получить доступ к Credentials Domino MetaModule можно со страницы метамодулей. Чтобы перейти на страницу метамодулей, во вкладке "Проект" / **Project** выберите "Модули" / **Modules** > "Метамодули" / **MetaModules**. Найдите Credentials Domino MetaModule и нажмите кнопку "Запустить" / **Launch**.

The screenshot shows the 'MetaModules Overview' page. At the top, there are navigation links: 'Home', 'kittens for your face', and 'MetaModules Overview'. Below the navigation, the 'MetaModules' section is displayed. On the left, there are 'Categories' (Auditing (5), Credentials (5), Discovery (5), Intrusion (1)) and a 'Safety Rating' section with star ratings and counts. The main area contains several module cards, each with a title, category, description, safety rating, and a 'Launch' button.

Module Name	Category	Description	Safety Rating	Launch Button
Segmentation and Firewall Testing	Discovery Auditing	Runs a full Nmap SYN scan against an external server hosted by Rapid7 that acts as an egress scan target. Use this MetaModule to discover outbound ports more...	★★★★★ (3)	Launch
Credentials Domino	Credentials Auditing	Uses a valid login or an active session to perform an iterative credentials attack that collects credentials from compromised hosts. It reuses collected more...	★★★★★	Launch
SSH Key Testing	Credentials Discovery Auditing	Attempts to log in to systems with a recovered SSH key and records the success and failure results for each service. You will need to specify the user name, SSH more...	★★★★★	Launch
Single Credentials Testing	Credentials Discovery Auditing	Tests the usage level for a set of weak or exposed credentials. It tries to log in to a range of hosts and services that you specify and records the success and fa more...	★★★★★	Launch
Pass the Hash	Credentials Discovery Auditing	Attempts to log in to hosts with a recovered Windows SMB hash or Postgres MD5 hash and reports the hosts that were successfully authenticated. You must pr more...	★★★★★	Launch
Passive Network Discovery	Discovery	Sniffs traffic to discover hosts and services on a local network. Since it does not send any packets, you can run this app to conduct a stealthy network discovery more...	★★★★★	Launch
Known Credentials Intrusion	Credentials Intrusion	Systematically logs in to as many hosts and services as possible using the known good credentials for this project. Run this MetaModule to reuse crede more...	★★★★★	Launch

При появлении окна конфигурации Credentials Domino MetaModule в нем будет отображена форма "Выбор первоначального хоста" / Select Initial Host. Каждая операция конфигурирования предполагает взаимодействие с отдельной вкладкой, благодаря чему пользователь может переключаться между различными формами конфигурации, кликая по любой соответствующей вкладке.

Выбор первоначального хоста для Credentials Domino MetaModule

Начать конфигурирование Credentials Domino MetaModule следует с выбора хоста с логином или сеансом, который вы хотите использовать. На вкладке "Выбор первоначального хоста" / Select Initial Host, можно увидеть список всех хостов в проекте, которые либо имеют действительные логины, либо открытые сеансы.

Credentials Domino

Performs an iterative credentials-based attack against a set of targets using a valid login or open session.

Select Initial Host

Choose a host from the list below

Scope

Settings

☒ Generate Report

HOST IP	HOST NAME	OS	SERVICES	LOGINS	SESSIONS	TAGS
10.20.36.53	MS-W03R2-3U-1	Windows 2003 R2	3 services	7 logins	1 session	0 tags

Show 10 Showing 1 - 1 of 1

Cancel Launch

Выберите хост, который должен использовать метамодуль. После выбора хоста будет отображена подробная информация о логине и сеансе для хоста.

Credentials Domino

Performs an iterative credentials-based attack against a set of targets using a valid login or open session.

Select Initial Host [< Back to full list](#)

Scope

Settings

☒ Generate Report

HOST IP	HOST NAME	OS	SERVICES	LOGINS	SESSIONS	TAGS
10.20.36.53	MS-W03R2-3U-1	Windows 2003 R2	3	7	1	0

Choose the login or session you want to use to start the attack.

PUBLIC	PRIVATE	REALM	SERVICE	PORT
☐ support_388945a0	aad3b435b51404eeaad3b435b51404		smb	445
☐ sshd	aad3b435b51404eeaad3b435b51404		smb	445
☐ sshd			smb	445
☐ guest			smb	445
☐ guest	aad3b435b51404eeaad3b435b51404		smb	445
☐ cyg_server	e2fc15074bf7751dd408e6b1057418e		smb	445
☐ administrator	e2fc15074bf7751dd408e6b1057418e		smb	445

Show 10 Showing 1 - 7 of 7

Cancel Launch

Выберите логин или сеанс, которые должен использовать метамодуль для начала атаки.

Credentials Domino

Performs an iterative credentials-based attack against a set of targets using a valid login or open session.

Select Initial Host [< Back to full list](#)

Scope

Settings

☒ Generate Report

HOST IP	HOST NAME	OS	SERVICES	LOGINS	SESSIONS	TAGS
10.20.36.53	MS-W03R2-3U-1	Windows 2003 R2	3	7	1	0

Choose the login or session you want to use to start the attack.

PUBLIC	PRIVATE	REALM	SERVICE	PORT
☐ support_388945a0	aad3b435b51404eeaad3b435b51404		smb	445
☐ sshd	aad3b435b51404eeaad3b435b51404		smb	445
☐ sshd			smb	445
☐ guest			smb	445
☐ guest	aad3b435b51404eeaad3b435b51404		smb	445
☐ cyg_server	e2fc15074bf7751dd408e6b1057418e		smb	445
☒ administrator	e2fc15074bf7751dd408e6b1057418e		smb	445

Show 10 Showing 1 - 7 of 7

Cancel Launch

Определение области применения Credentials Domino MetaModule

Область применения устанавливает хосты, на которые планируется нацелить метамодуль во время атаки. Чтобы определить область применения, следует использовать поля "Целевые адреса" / **Target Addresses** и "Исключенные адреса" / **Excluded Addresses**.

Credentials Domino

Performs an iterative credentials-based attack against a set of targets using a valid login or open session.

Select Initial Host

Scope

Settings

☒ Generate Report

Enter the hosts you want to attack

Target addresses

Excluded addresses ?

High Value Hosts ?

Enter IP range or address(es) of high value hosts.

High Value Host Tags ?

Enter the tags you applied to high value hosts.

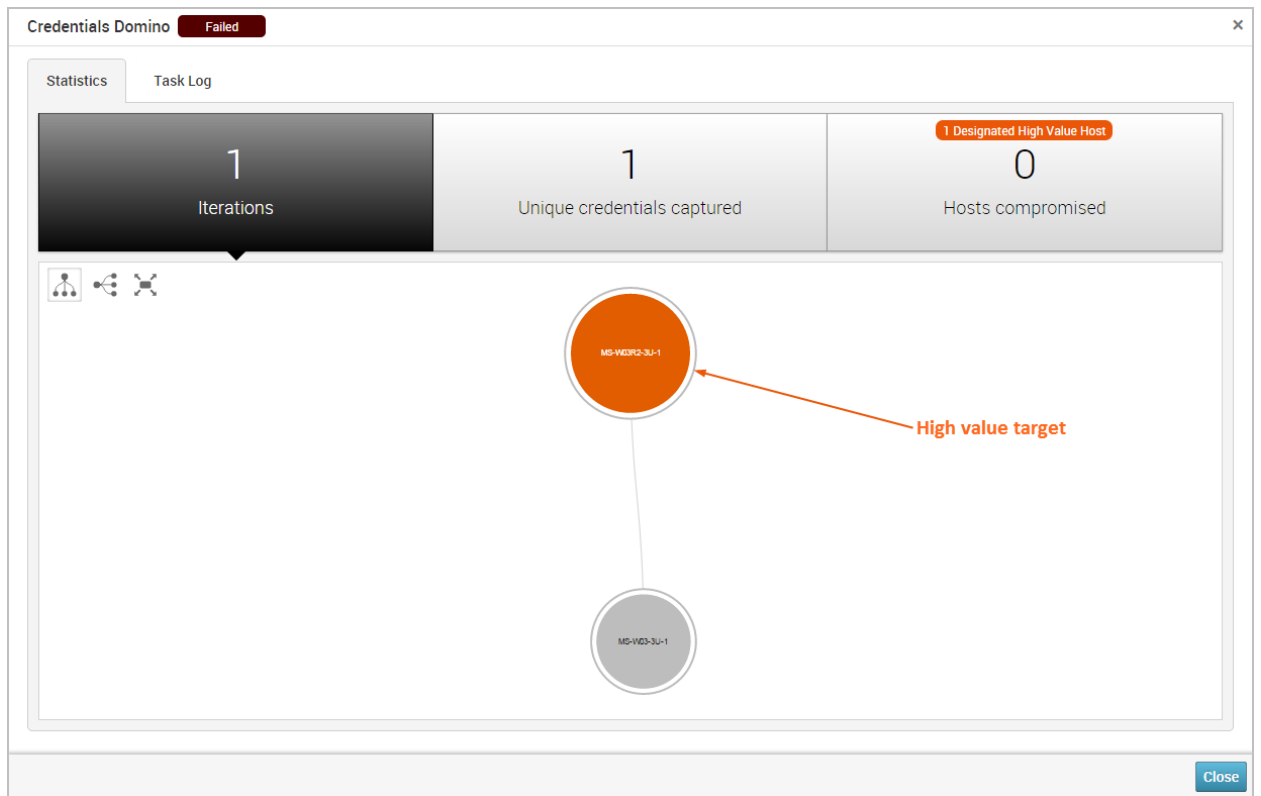
Cancel Launch

При наличии конкретных хостов, которые нужно атаковать, можно ввести их в поле "Целевые адреса" / **Target Addresses**. Можно ввести один адрес (192.168.1.1), диапазон адресов (192.168.1.1-192.168.1.100), CIDR-нотацию (192.168.1.0/24) или подстановочный символ (192.168.1.*). Необходимо использовать новую строку для отделения каждой записи. При желании включить все хосты проекта можно оставить это поле пустым.

Присвоение статуса "Особо важный хост" в Credentials Domino MetaModule

"Особо важный хост" / High Value Host - это статус, который пользователь присваивает хосту при необходимости выделить соответствующий хост в окне Credentials Domino Findings и в отчете Credentials Domino MetaModule. Присвоение статуса "Особо важный хост" помогает быстро определить воздействие конкретной пары захваченных элементов учетных данных по отношению к критически важным хостам. Присвоение статуса "Особо важный хост" позволяет указать на то, что хост имеет максимально важное значение для организации, и любая атака на хост может негативно повлиять на работу такой организации. Например, контроллеры доменов и серверы, содержащие конфиденциальную финансовую информацию, могут рассматриваться как особо важные хосты.

Все особо важные хосты будут выделены оранжевым цветом в окне "Результаты" / Findings, как показано ниже:



Есть несколько способов присвоить хосту статус High Value Host:

- Применение хостовых тегов - Можно применять теги к хостам, которые имеют критически важное значение для организации, что позволяет вести отслеживание таких хостов, группировать их и готовить по ним отчеты в зависимости от того, как такие хосты влияют на организацию. Теги позволяют осуществлять просмотр и фильтрацию хостов на уровне проекта.

Например, можно присвоить всем серверам учета тег вроде accounting. Также можно создать и применить теги критичности, такие как "Высокая" / High, "Средняя" / Medium и "Низкая" / Low, чтобы изолировать хосты на основе уровней их критичности.

Credentials Domino

Performs an iterative credentials-based attack against a set of targets using a valid login or open session.

Select Initial Host

Scope

Settings

☒ Generate Report

Enter the hosts you want to attack

Target addresses

10.20.36.*

Excluded addresses

High Value Hosts

Enter IP range or address(es) of high value hosts.

High Value Host Tags

Enter the tags you applied to high value hosts.

high

Cancel Launch

- Определение особо важных хостов в Credentials Domino MetaModule - Также можно присваивать статус High Value Host хостам, исходя из их адресов. Можно ввести диапазон адресов, один адрес или список адресов, каждый элемент которого прописывается в новой строке.

Например, если известен IP-адрес конкретного хоста, который представляет особый интерес, можно указать его при настройке области применения Credentials Domino MetaModule. Используйте этот метод при желании вручную определить хосты, которым необходимо присвоить статус High Value Hosts и при этом необходимо избежать использования тегов.

Credentials Domino

Performs an iterative credentials-based attack against a set of targets using a valid login or open session.

Select Initial Host

Enter the hosts you want to attack

Target addresses

10.20.36.*

Excluded addresses

High Value Hosts

Enter IP range or address(es) of high value hosts.

10.20.36.53

High Value Host Tags

Enter the tags you applied to high value hosts.

Generate Report

Cancel Launch

Настройка параметров нагрузки для Credentials Domino MetaModule

Можно определить нагрузку, которую Credentials Domino MetaModule должен передавать во время атаки. Чтобы настроить параметры нагрузки, можно использовать следующие опции во вкладке "Настройки" / Settings:

- Тип нагрузки / Payload Type: этот параметр определяет тип нагрузки, которую метамодуль передает цели. Можно выбрать одну из следующих опций:

■ **Meterpreter:** Данный тип нагрузки представляет собой усовершенствованную интерактивную оболочку, которая позволяет осуществлять широкий спектр действий после эксплуатации уязвимости (post-exploitation). Например, с ее помощью можно выполнять эскалацию привилегий, получать дампы хэшей паролей, делать скриншоты, выполнять запуск и миграцию процессов, а также закачивать файлы в хранилище цели. Meterpreter также предлагает возможности командной оболочки для решения базовых задач, таких как добавление учетной записи пользователя или выполнение скрипта.

Кроме того, Meterpreter выполняет динамическую самозагрузку в существующий процесс на целевом хосте, используя метод под названием DLL-инъекция с отражением, позволяющий полностью находиться в памяти и оставаться незамеченным системами обнаружения и предотвращения проникновений.

■ **Команда / Command:** Этот тип нагрузки предоставляет доступ к командной оболочке, которую пользователь может использовать для запуска отдельных команд на хосте с целью выполнения простых задач, таких как добавление учетной записи пользователя или изменение пароля.

Командная оболочка предоставляет ограниченные возможности, но допускает последующий апгрейд до оболочки Meterpreter с дополнительными опциями.

В отличие от Meterpreter, командная оболочка может запустить новый процесс, который может быть легко обнаружен системами обнаружения и предотвращения проникновений.

- Соединение / Connection: Эта опция определяет, как экземпляр Metasploit пользователя подключается к хосту. Можно выбрать одну из следующих опций:

- Авто / Auto: Этот тип соединения использует обратное соединение при обнаружении NAT или файрвола; в противном случае он используется привязку соединения.

- Привязка / Bind: Этот тип соединения использует привязку. Его следует использовать при наличии прямого неограниченного соединения с целевым хостом.

- Обратное / Reverse: Этот тип соединения использует обратное соединение. Его следует использовать, если хосты находятся за файрволом или NAT-шлюзом, которые предотвратят передачу запросов с экземпляра Metasploit пользователя в направлении цели.

- Порты прослушивания / Listener Ports: Эта опция определяет порты, которые слушатель использует для ожидания входящих соединений.

Можно указать конкретный порт, список разделенных запятыми портов или диапазон портов.

Если вводится диапазон портов, из диапазона выбирается первый доступный открытый порт.

- Хост прослушивания / Listener Host: Эта опция определяет IP-адрес, к которому целевой хост подключается обратно. Обычно для этого используется внешний IP-адрес локального устройства пользователя. Если хост прослушивания не указан, MetaModule автоматически использует внешний IP-адрес локального устройства пользователя.

- Очистка сеансов / Clean up Sessions: Эта опция позволяет закрыть все открытые сеансы после завершения работы MetaModule. Эта опция включена по умолчанию. При желании сохранить сеансы открытыми, отмените выбор этой опции.

Установка условий прерывания для Credentials Domino MetaModule

Можно контролировать количество циклических проходов Credentials Domino MetaModule по целевой сети, задавая условия по итерациям и таймауту. Если условия по итерациям или таймауту не будут заданы, Credentials Domino MetaModule будет работать до тех пор, пока не исчерпает все комбинации элементов учетных данных и хостов. В зависимости от объема атаки и количества захваченных учетных данных атака может предполагать прохождение через большое количество итераций.

Чтобы установить условия прерывания, нужно использовать следующие параметры, которые находятся на вкладке "Настройки" / Settings:

- Количество итераций / Number of Iterations: Эта опция устанавливает лимит по количеству итераций, попытки осуществить которые будет предпринимать метамодуль. Можно оставить поля пустыми при необходимости продолжения метамодулем работы до тех пор, пока у него не закончатся учетные данные для перебора.

- **Совокупный таймаут / Overall Timeout:** Данная опция устанавливает лимит по продолжительности работы метамодуля в целом.

При указании таймаута можно использовать следующий формат: ЧЧ:ММ:СС (НН:ММ:СС). Можно оставить поля пустыми, чтобы не устанавливать лимит по таймауту.

- **Таймаут службы / Service Timeout:** Эта опция устанавливает таймаут в секундах для каждой цели. Можно оставить поля пустыми, чтобы не устанавливать лимит по таймауту.

Включение сгенерированного отчета Credentials Domino MetaModule

В отчете Credentials Domino MetaModule приведены выводы и технические результаты атаки на основе учетных данных. Вы можете просмотреть отчет, чтобы определить, как подтвержденный вход или открытый сеанс повлияли на целевую сеть.

Чтобы включить отчет Credentials Domino MetaModule, вам просто нужно включить соответствующий параметр отчета.

Credentials Domino

Performs an iterative credentials-based attack against a set of targets using a valid login or open session.

Select Initial Host

Scope

Settings

☒ **Generate Report**

Report is **enabled**

☐ HTML ☒ PDF ☐ RTF ☐ WORD

Name* CredentialsDominoMetaModule-20150629124639 ?

Sections ?

- ☒ Cover Page
- ☒ Executive Summary
- ☒ Project Summary
- ☒ Run Selections
- ☒ Findings Summary
- ☒ Summary Charts
- ☒ Compromised High Value Hosts
- ☒ Uncompromised High Value Hosts
- ☒ All Compromised Hosts
- ☒ All Uncompromised Hosts
- ☒ Appendix: Report Options

Options

- ☐ Include charts

Excluded addresses ?

Email Report ?

Cancel Launch

Если вы выберете автоматическое генерирование отчета, вы можете настроить отчет с помощью любого из следующих параметров:

- **Формат:** Отчет может быть создан как файл в формате HTML, PDF или RTF. Вы должны выбрать хотя бы один формат для отчета.
- **Название:** Отчету назначено название по умолчанию, в зависимости от метамодуля и текущей даты. Вы можете использовать название по умолчанию или указать собственное название отчета.

- **Разделы:** Отчет включает следующие разделы: Титульный лист, Краткое описание проекта, Обобщение результатов, Аналитические службы и Сводные таблицы хостов, Подтвержденные службы и Сведения о хосте и Приложение. По умолчанию отчет включает все эти разделы. Вы можете отменить выбор любых разделов, которые не хотите включать в отчет.
- **Скрыть обнаруженные учетные данные:** в отчете отображаются все полученные учетные данные в виде обычного текста. Если вы хотите скрыть учетные данные из отчета, вы должны включить этот параметр.
- **Включить графики:** Отчет содержит несколько диаграмм и графиков, демонстрирующих результаты атаки. Если вы не хотите включать диаграммы и графики в отчет, вы должны включить этот параметр.
- **Исключенные адреса:** Отчет содержит данные для всех хостов, включенных в область. При наличии определенных хостов, данные, которые вы не хотите включать в отчет, вы можете перечислить в этом поле.
- **Отправка отчета по электронной почте:** Вы можете отправить отчет по электронной почте после его создания. Чтобы отправить отчет по электронной почте, в этом поле необходимо ввести список адресов электронной почты с разделением запятыми.

Обратите внимание, что для использования у вас уже должен быть установлен локальный почтовый сервер или служба ретрансляции сообщений электронной почты, настроенные для Metasploit Pro. Чтобы определить параметры вашего почтового сервера, перейдите по пути «Администрирование»> «Глобальные настройки»> «Настройки SMTP».

!!Из метамодуля вы можете генерировать только отчет метамодуля. Если вы не включите сгенерированный отчет при настройке метамодуля, вы не сможете сделать это позже.

Запуск Credentials Domino MetaModule

При готовности к запуску Credentials Domino MetaModule нажмите на кнопку "Запустить".

Credentials Domino

Performs an iterative credentials-based attack against a set of targets using a valid login or open session.

Select Initial Host

Scope

Settings

☒ Generate Report

Report is **enabled**

HTML ☐ PDF ☒ RTF ☐ WORD

Name* CredentialsDominoMetaModule-20150629124639 ?

Sections ?

- ☒ Cover Page
- ☒ Executive Summary
- ☒ Project Summary
- ☒ Run Selections
- ☒ Findings Summary
- ☒ Summary Charts
- ☒ Compromised High Value Hosts
- ☒ Uncompromised High Value Hosts
- ☒ All Compromised Hosts
- ☒ All Uncompromised Hosts
- ☒ Appendix: Report Options

Options

- ☐ Include charts

Excluded addresses ? Email Report ?

Cancel Launch

Понимание результатов Credentials Domino MetaModule

После запуска Credentials Domino MetaModule появится окно результатов, в котором будут отображены результаты и события для атаки в режиме реального времени. Вы можете быстро заметить влияние атаки на целевую сеть и определить возможные маршруты атаки.

Для упрощения просмотра данных окно результатов состоит из двух основных вкладок: вкладки «Статистика» и вкладки «Журнал задач».

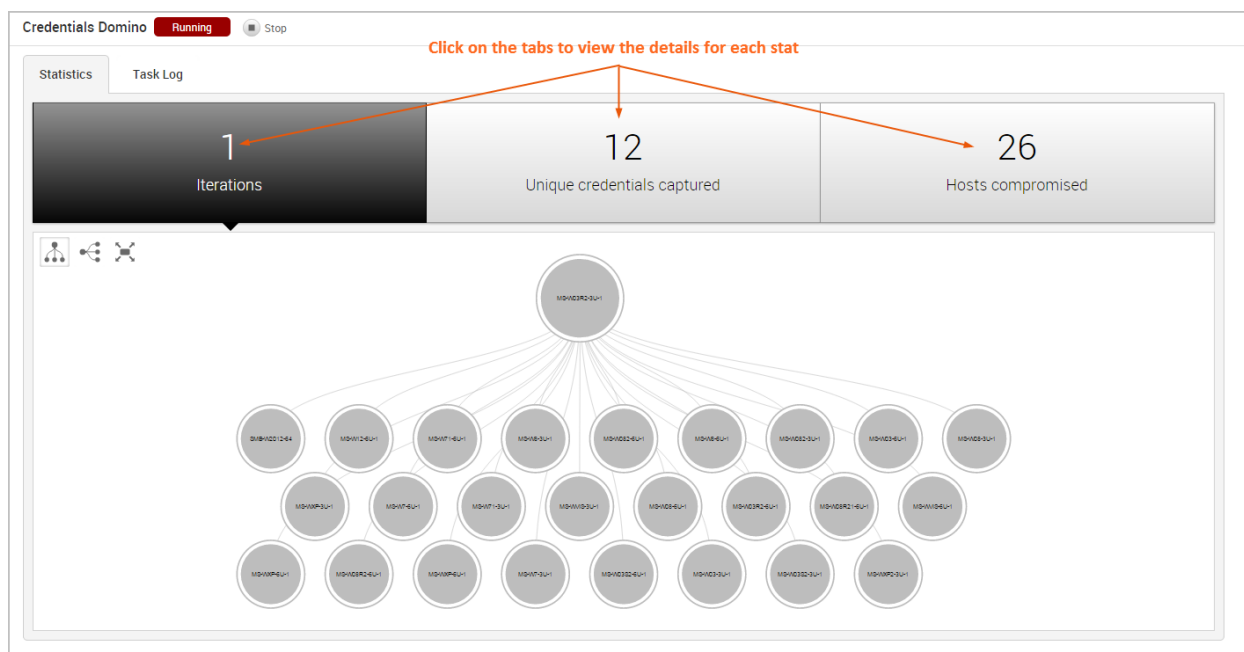


Статистика

Вкладка «Статистика» отслеживает результаты для атаки в режиме реального времени. В нем отображается следующая статистика:

- Общее число итераций, выполняемых метамодулем
- Общее количество зарегистрированных учетных данных
- Общее количество взломанных хостов

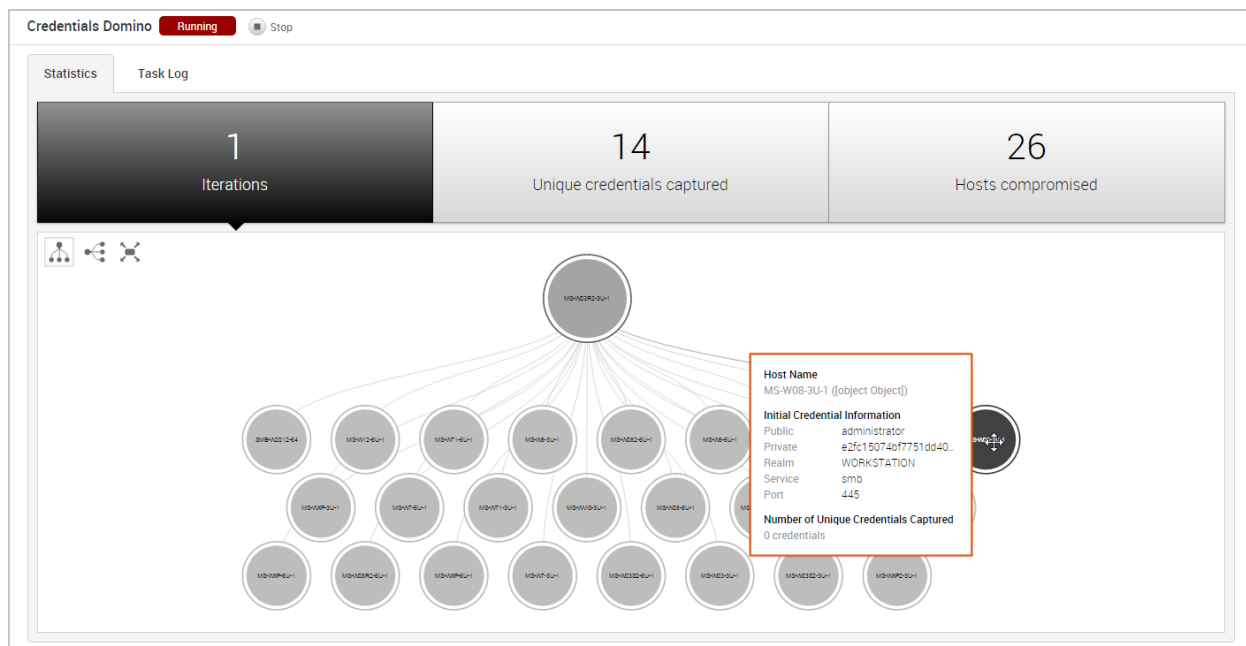
Каждая статистика отображается на отдельной вкладке. Вы можете кликнуть любую вкладку, чтобы просмотреть соответствующие данные статистики.



Просмотр и Визуализация атак

Для упрощения просмотра маршрутов атак, которые метамодулю удалось установить, результаты, представленные ниже, включают визуализацию атаки, которая наглядно показывает взаимосвязь и иерархию между каждым взломанным хостом в сети. Визуализация использует древовидную структуру и представляет каждый нод как нод в дереве. Исходный нод - это исходный хост, который метамодуль использовал для начала атаки.

Визуализация атаки использует иерархический формат для подключения хостов, которые связаны с другими хостами. Соединение между двумя узлами создается, когда учетные данные одного хоста используются для взлома другого нода. Вы можете навести указатель на нод при визуализации атак, чтобы выделить маршрут атаки, который использовался для взлома хоста.

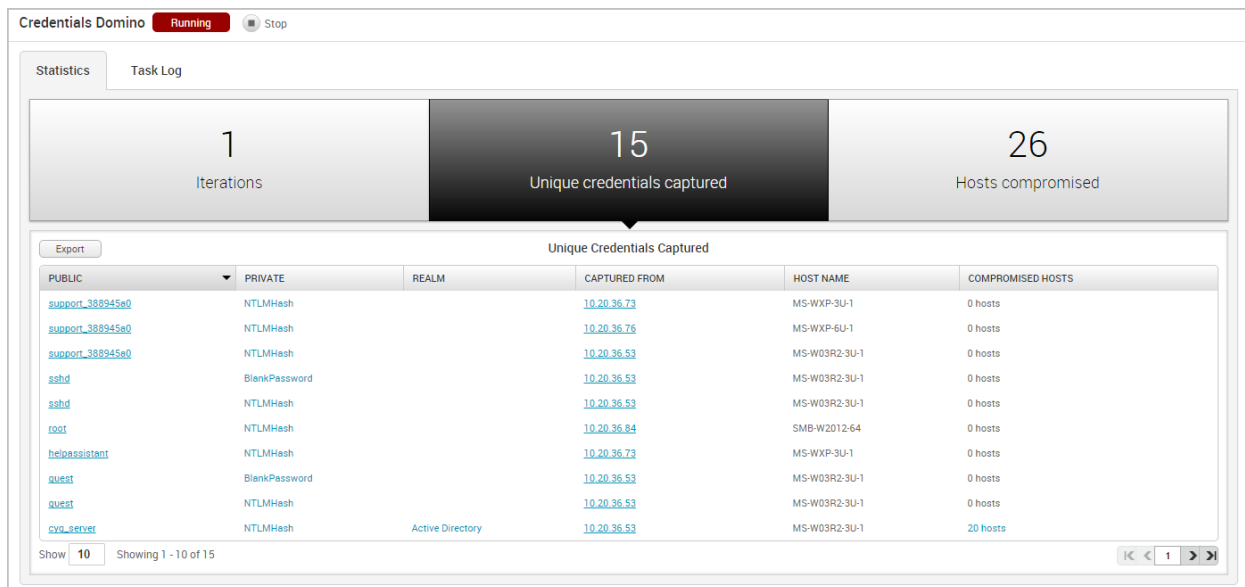


Каждая итерация представляет собой уровень на дереве, поэтому визуализация атаки может стать довольно объемной, если метамодуль выполнил несколько итераций атаки. Например, если метамодуль выполнил 20 итераций атаки, в визуализации атаки будет представлено 20 уровней. Если это произойдет, вы можете прокрутить или дважды кликнуть по дереву, чтобы увеличить его размер для просмотра меньшего набор узлов, или можете навести курсор на определенный нод, чтобы просмотреть сведения об этом узле, такие как имя хоста, операционная система, информация об учетных данных и зарегистрированные учетные данные.

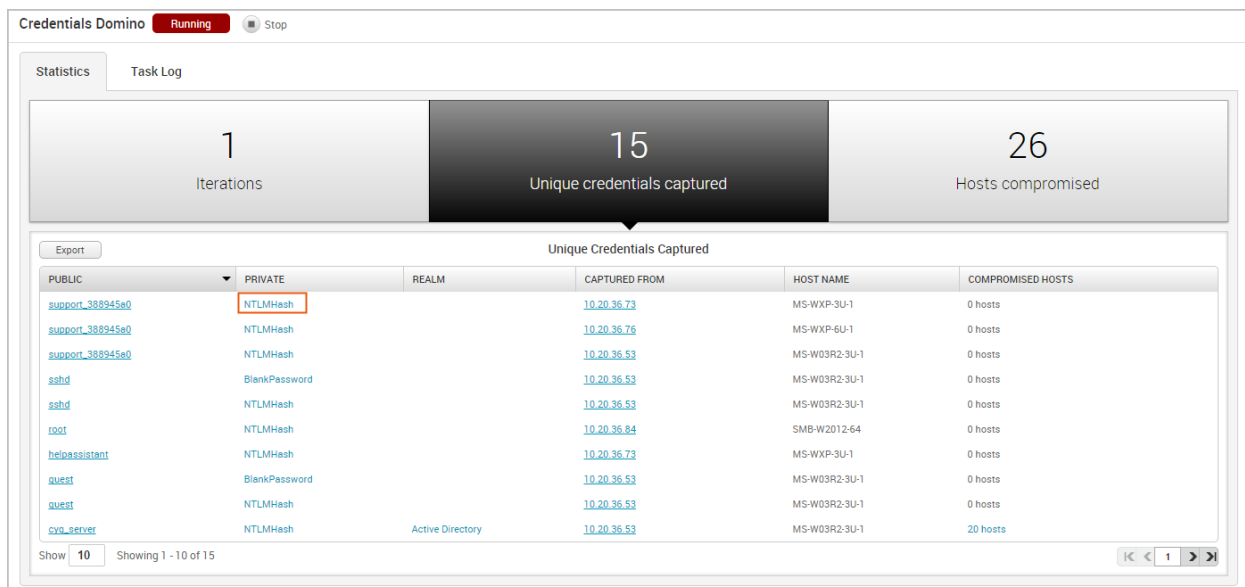
Просмотр уникальных зарегистрированных учетных данных

Domino отслеживает учетные данные, которые не имеют общих открытых, закрытых и поименованных данных с другими зарегистрированными учетными данными. Он отображает этот подсчет на вкладке «Уникальные зарегистрированные учетные данные» и постоянно обновляет подсчет в режиме реального времени.

Для каждого уникальных зарегистрированных учетных данных в таблице Уникальных зарегистрированных учетных данных отображается общедоступное значение, скрытое значение, поименованный тип, исходный IP-адрес хоста, имя исходного хоста и количество хостов, с которых были получены учетные данные.



Если учетные данные являются хешем или SSH-ключом, то поле "Скрытое" (Private) отображает тип учетных данных вместо скрытого значения. Вы можете кликнуть по скрытому типу, чтобы просмотреть скрытое значение.



Просмотр взломанных хостов

Метамодуль Credentials Domino отслеживает хосты, на которых он смог открыть сеансы. Он отображает этот подсчет на вкладке «Взломанные хосты» и постоянно обновляет подсчет в режиме реального времени.

Credentials Domino **Running** 

Statistics Task Log

1
Iterations

27
Unique credentials captured

26
Hosts compromised

Export ☐ Show High Value Hosts only

HOST IP	HOST NAME	OS	SERVICE	PORT	PUBLIC	PRIVATE	REALM	CREDENTIALS LOOTED	SESSIONS
10.20.36.84	SMB-W2012-64	Windows 2008	smb	445	administrator	NTLMHash	Active Directory	3 credentials	1 session
10.20.36.76	MS-WXP-6U-1	Windows XP	smb	445	cva_server	NTLMHash	Active Directory	1 credential	1 session
10.20.36.75	MS-W03S2-6U-1	Windows 2003 R2	smb	139	cva_server	NTLMHash	Active Directory	1 credential	1 session
10.20.36.74	MS-WXP-6U-1	Windows XP	smb	139	cva_server	NTLMHash	Active Directory	0 credentials	1 session
10.20.36.73	MS-WXP-3U-1	Windows XP	smb	139	administrator	NTLMHash	Active Directory	2 credentials	1 session
10.20.36.72	MS-WXP2-3U-1	Windows XP	smb	445	administrator	NTLMHash	Active Directory	0 credentials	1 session
10.20.36.71	MS-WVIS-6U-1	Windows Vista	smb	445	cva_server	NTLMHash	Active Directory	0 credentials	1 session
10.20.36.70	MS-WVIS-3U-1	Windows Vista	smb	445	cva_server	NTLMHash	Active Directory	0 credentials	1 session
10.20.36.68	MS-W8-6U-1	Windows 8	smb	445	cva_server	NTLMHash	Active Directory	0 credentials	1 session
10.20.36.67	MS-W8-3U-1	Windows 8	smb	445	cva_server	NTLMHash	Active Directory	2 credentials	1 session

Show 10 Showing 1 - 10 of 26

В таблице Взломанных хостов перечислены IP-адрес хоста, имя хоста, операционная система, название службы, порт, общедоступный, закрытый, поименованный тип, количество украденных (захваченных) учетных данных и ссылка на сеанс для каждого взломанного хоста.

Чтобы просмотреть список учетных данных, которые были захвачены с хоста, вы можете навести курсор на подсчет учетных данных в столбце «Учетные данные».

Credentials Domino **Completed**

Statistics Task Log

3
Iterations

37
Unique credentials captured

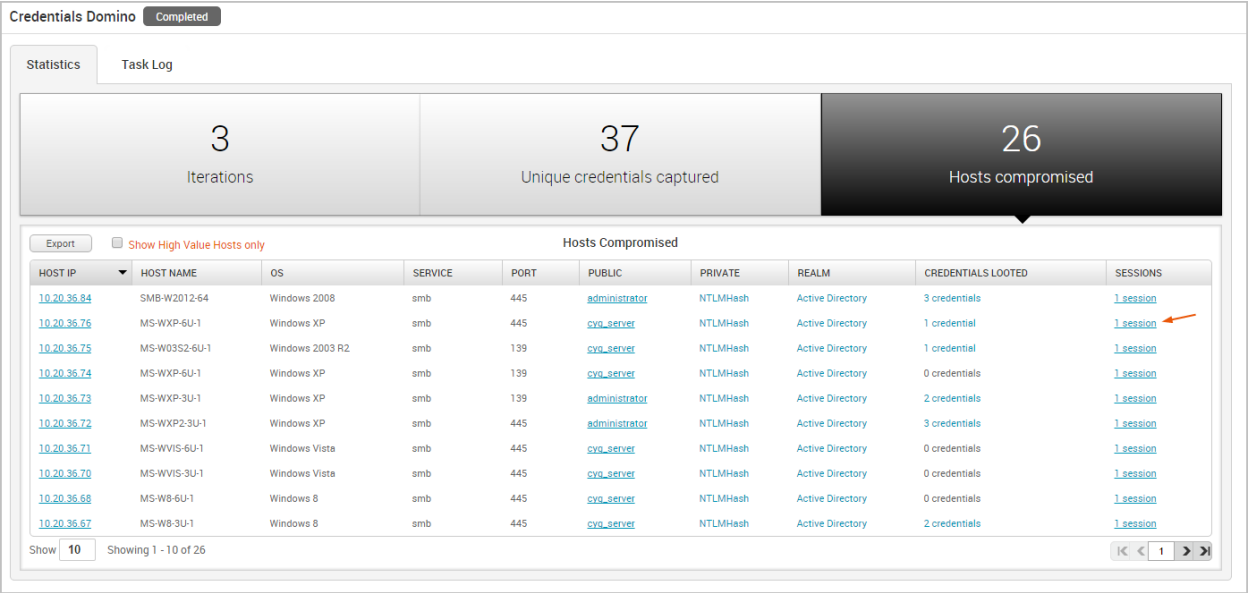
26
Hosts compromised

Export ☐ Show High Value Hosts only

HOST IP	HOST NAME	OS	SERVICE	PORT	PUBLIC	PRIVATE	REALM	CREDENTIALS LOOTED	SESSIONS
10.20.36.84	SMB-W2012-64	Windows 2008	smb	445	administrator	NTLMHash	Active Directory	3 credentials	1 session
10.20.36.76	MS-WXP-6U-1	Windows XP	smb	445	cva_server	NTLMHash	Active Directory	1 credential	1 session
10.20.36.75	MS-W03S2-6U-1	Windows 2003 R2	smb	139	cva_server	NTLMHash	Active Directory	1 credential	1 session
10.20.36.74	MS-WXP-6U-1	Windows XP	smb	139	cva_server	NTLMHash	Active Directory	0 credentials	1 session
10.20.36.73	MS-WXP-3U-1	Windows XP	smb	139	administrator	NTLMHash	Active Directory	2 credentials	1 session
10.20.36.72	MS-WXP2-3U-1	Windows XP	smb	445	administrator	NTLMHash	Active Directory	3 credentials	1 session
10.20.36.71	MS-WVIS-6U-1	Windows Vista	smb	445	cva_server	NTLMHash	Active Directory	0 credentials	1 session
10.20.36.70	MS-WVIS-3U-1	Windows Vista	smb	445	cva_server	NTLMHash	Active Directory	0 credentials	1 session
10.20.36.68	MS-W8-6U-1	Windows 8	smb	445	cva_server	NTLMHash	Active Directory	0 credentials	1 session
10.20.36.67	MS-W8-3U-1	Windows 8	smb	445	cva_server	NTLMHash	Active Directory	2 credentials	1 session

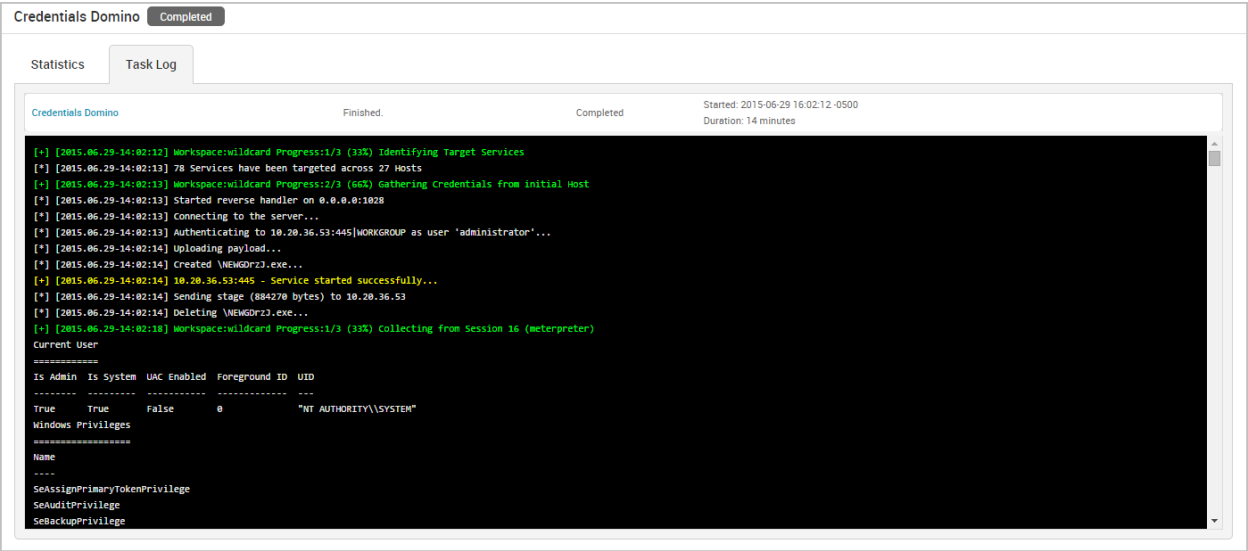
Show 10 Showing 1 - 10 of 26

Для доступа к странице сведений для открытого сеанса кликните ссылку сеанса в столбце «Сеанс».



Журнал задач

Журнал задач отслеживает действия для метамодуля, такие как комбинации пар хостов и учетных данных, которые были проверены (использованы), и результаты этих попыток. Журнал задач также документирует любые ошибки или сбои, произошедшие во время атаки, и может использоваться для устранения любых проблем, связанных с запуском метамодуля. Это особенно полезно, если, например, метамодуль работает в течение длительного времени, подвисает или не закрывается.



Метамодуль проверки единых учетных данных

Метамодуль проверки единых учетных данных обрабатывает известную пару учетных данных для выявления дополнительных систем, которые могут быть аутентифицированы. Вы можете запустить этот метамодуль, чтобы продемонстрировать, как повторное использование паролей может выявить серьезные недостатки в средствах обеспечения безопасности предприятия. Один

взломанный пароль позволяет с легкостью взломать другие системы, использующие один и тот же пароль.

Чтобы использовать Метамодуль проверки единых учетных данных, вам необходимо предоставить ему известную пару учетных данных, которую вы вскрыли с помощью Discovery Scan, методом грубого подбора или фишинг-атаки. Когда вы настраиваете этот метамодуль, вам необходимо определить целевые хосты и службы, которые вы хотите попытаться аутентифицировать. После завершения работы, метамодуль создает отчет, в котором указаны хосты, на которых он смог аутентифицировать учетные данные.

Риски блокировки

Блокировка учетной записи отключает учетную запись и не позволяет вам получить доступ к учетной записи в течение периода блокировки. Когда вы настраиваете метамодуль проверки единых учетных данных, вы должны учесть риск блокировки для выбранных вами служб.

Каждая служба подразделяется на следующие типы рисков блокировки:

- Низкий уровень риска: Любая служба, которая обычно не осуществляет принудительную блокировку учетных записей, такая как AFP, DB2, EXEC, FTP, HTTP, HTTPS, LOGIN, Oracle, Postgres, SHELL, SNMP, SSH_PUBKEY, Telnet и VNC.
- Средний уровень риска: Любая служба, которая обычно осуществляет принудительно блокировку учетных записей, такая как MSSQL, MySQL, POP3, и SSH.
- Высокий уровень риска: Любая служба, использующая проверку подлинности Windows, например PC Anywhere, SMB, vmauthd, and WinRM.

Запуск Метамодуля проверки единых учетных данных

1. В проекте выберите «Модули» > «Метамодули».
2. Найдите Метамодуль проверки единых учетных данных и нажмите кнопку «Запустить». Появится окно тестирования отдельных учётных данных.

MetaModules

Categories:

- ☐ Auditing (1)
- ☐ Credentials (2)
- ☐ Discovery (4)
- ☐ Intrusion (2)
- ☐ Penetration Testing (2)

Safety Rating:

- ★★★★★ (1)
- ★★★★★ & up (2)
- ★★★★★ & up (6)
- ★★★★★ & up (6)
- ★★★★★ & up (6)

SSH Key Testing

Credentials

This MetaModule attempts to log in to systems with a recovered SSH key and records the success and failure results for each service. You will need to specify the user name, SSH key filename, and range of hosts that you want to test.

Safety Rating: ★★★★★

Launch

Single Password Testing

Discovery | Credentials

This MetaModule tests the usage level for a set of weak or exposed credentials. It tries to log in to a range of hosts and services that you specify and records the success and failure results for each service.

Safety Rating: ★★★★★

Launch

Pass the Hash

Discovery | Intrusion

This MetaModule attempts to log in to as many hosts as possible with a recovered Windows SMB hash. It reports the hosts that it was able to successfully authenticate. You specify a username, SMB hashed password, and the range of hosts that you want to test.

Safety Rating: ★★★★★

Launch

Passive Network Discovery

Discovery | Intrusion | Auditing

This MetaModule sniffs traffic to discover hosts and services on a local network. Since it does not send any packets, you can run this app to conduct a stealthy network discovery scan and identify any hosts, services, and clear-text credentials.

Safety Rating: ★★★★★

Launch

Firewall Egress Testing

Penetration Testing | Discovery

This MetaModule runs a full Nmap SYN scan against an external server hosted by Rapid7 that acts as an egress scan target. Use this MetaModule to discover outbound ports on a firewall that an attacker can use to exfiltrate information. You will need to specify the ports and protocols that you want to audit.

Safety Rating: ★★★★★

Launch

Known Credentials Intrusion

Penetration Testing

This MetaModule systematically logs in to as many hosts and services as possible using the known good credentials for this project. Run this MetaModule to reuse credentials that you have collected from compromised machines. For the best results, you should run a bruteforce attack or phishing attack to collect as many credentials as you can before you run this MetaModule.

Safety Rating: ★★★★★

Launch

3. На вкладке «Область» введите диапазон целевых адресов, который вы хотите использовать для тестирования. Диапазон целевых адресов должен соответствовать хостам в рабочей области.

Single Credentials Tester

Attempts to use a known credential pair to authenticate services on a range of target hosts and reports the ones it was able to authenticate.

Scope

Address Range

Service and Ports

Credentials

☒ Generate Report

Advanced ⌵

Cancel **Launch**

4. Перейдите на вкладку «Службы и порты». Появится форма Служб.

Single Credentials Tester

Attempts to use a known credential pair to authenticate services on a range of target hosts and reports the ones it was able to authenticate.

Scope

Service and Ports

Credentials

☒ Generate Report

Select Services

Low Lockout Risk

☒ AFP	☒ DB2	☒ EXEC	☒ FTP	☒ HTTP
☒ HTTPS	☒ LOGIN	☒ Oracle	☒ Postgres	☒ SHELL
☒ SNMP	☒ SSH_PUBKEY	☒ Telnet	☒ VNC	

Medium Lockout Risk

☒ MSSQL	☒ MySQL	☒ POP3	☒ SSH
---	---	--	---

High Lockout Risk

☒ PCAnywhere_Data	☒ SMB	☒ VMAuthd	☒ WinRM
---	---	---	---

Cancel Launch

5. Выберите службы, которые вы хотите попытаться аутентифицировать. Все службы классифицируются в зависимости от их риска блокировки, что служит вероятностью того, что служба обеспечивает принудительную блокировку учетных записей.

6. Перейдите на вкладку «Учетные данные». Появится форма "Учетные данные".

7. Вы можете выбрать один из следующих параметров, чтобы предоставить метамодулю учетные данные:

- Введите известную пару учетных данных: Вам необходимо вручную ввести комбинацию имени пользователя и пароля для использования метамодулем. Используйте этот метод для учетных данных, полученных в результате фишинг-атак.
- Выберите существующую пару учетных данных: Вы можете выбрать комбинацию имени пользователя и пароля из списка известных учетных данных. Эти учетные данные были получены в результате грубого подбора, с помощью discovery scan или импорта данных.

Single Credentials Tester ✕

Attempts to use a known credential pair to authenticate services on a range of target hosts and reports the ones it was able to authenticate.

Scope*
Service and Ports
Credentials
☒ Generate Report

Credentials

☒ Enter a known credential pair
☐ Choose an existing credential pair

Username

Password
☐ Display password

Domain

Cancel Launch

8. Перейдите на вкладку «Отчет». Появится форма конфигурации отчета.

Single Credentials Tester ✕

Attempts to use a known credential pair to authenticate services on a range of target hosts and reports the ones it was able to authenticate.

Scope*
Service and Ports
Credentials
☒ **Generate Report**

Report is enabled PDF RTF HTML

Report name

Sections

☒ Cover Page
☒ Project Summary
☒ Findings Summary
☒ Authenticated Services and Hosts Summary Charts

☒ Authenticated Services and Hosts Details
☒ Appendix: Report Options Selected

Options

☐ Mask discovered passwords
☒ Include charts and graphs

Excluded Addresses

☐ **Email Report** ?
Email Addresses

Cancel Launch

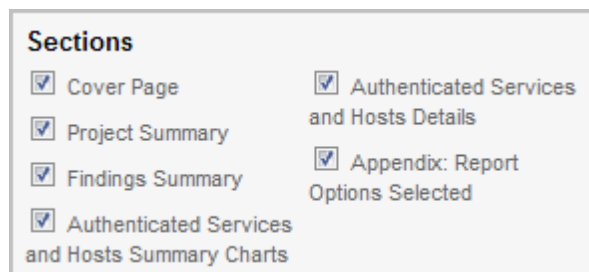
9. Введите название отчета в поле «Название отчета», если вы хотите использовать

пользовательское название отчета. В противном случае метамодуль использует название отчета по умолчанию.

10. Выберите формат PDF, Word, RTF или HTML в качестве формата отчета.

11. В области Разделы отмените выбор любых разделов, которые вы не хотите включать в отчет.

Пропустите этот шаг, если вы хотите сгенерировать все разделы отчета.



12. Выберите параметр «Отправить по электронной почте», если вы хотите отправить отчет по электронной почте отчет после его генерирования. Если вы включите этот параметр, вам необходимо предоставить список адресов электронной почты, с разделением запятыми.

Примечание: Если вы хотите отправить отчет по электронной почте, вы должны настроить локальный почтовый сервер или службу ретрансляции сообщений электронной почты для использования Metasploit Pro. Чтобы определить параметры вашего почтового сервера, выберите «Администрирование» > «Глобальные настройки» > «Настройки SMTP».

13. Нажмите кнопку «Запустить».

При запуске метамодуля, появляется окно «Результаты», в котором отображена статистика и режим задач в режиме реального времени для запуска метамодуля. Вы можете отслеживать общее количество хостов, которые метамодуль попытался аутентифицировать, общее количество попыток входа и общее количество успешных входов.

Если вы хотите просмотреть все данные о событии, вы можете кликнуть вкладку «Журнал задач».

После завершения работы метамодуля, вы должны перейти в область "Отчеты" для просмотра Отчета проверки единых учетных данных. На первых страницах отчета показаны графики и таблицы с высокоуровневой разбивкой аутентифицированных служб и хостов. Для более тщательного просмотра взломанных хостов вы можете перейти в раздел Аутентифицированный службы и Данные о хостах», в котором показаны аутентифицированные службы, и сеансы, открытые на каждом хосте.

Метамодуль проверки SSH-ключей

Аутентификация с открытым SSH-ключом обеспечивает безопасный способ входа на удаленный хост. Она использует пару SSH-ключей для аутентификации входа вместо традиционной комбинации имени пользователя и пароля. Пара SSH-ключей состоит из закрытого и открытого SSH-ключа. Закрытый SSH-ключ хранится на локальном компьютере и позволяет вам входить в удаленные системы, на которых установлен соответствующий открытый ключ.

Если вы получите незашифрованный закрытый SSH-ключ со взломанного целевого компьютера, вы можете запустить Метамодуль проверки SSH-ключей. Этот метамодуль позволяет вам вводить логины методом подбора на разных хостах для выявления удаленных компьютеров, которые могут быть аутентифицированы с помощью закрытого ключа. Во время работы метамодуля, отображает статистику в режиме реального времени по количеству целевых хостов, количеству сделанных попыток входа и количеству успешных логинов. После завершения работы, метамодуль создает полный отчет, в котором представлены подробные данные хостов, которые ему удалось успешно аутентифицировать.

Запуск Метамодуля проверки SSH-ключей

Прежде чем вы сможете запустить MetaModule проверки SSH-ключей, вы должны либо иметь закрытый SSH-ключ, который можете загрузить в свой проект, либо ваш проект должен содержать личный украденный SSH-ключ, полученный с помощью Discovery Scan, путем грубого подбора или каким-либо другим эксплойт-методом.

1. В проекте выберите «Модули»> «Метамодули».
2. Найдите Метамодуль проверки SSH-ключей и нажмите кнопку «Запустить». Появится окно тестирования SSH-ключа.

The screenshot displays the 'MetaModules' interface. On the left, there is a sidebar with 'Categories' (Auditing (1), Credentials (2), Discovery (4), Intrusion (2), Penetration Testing (2)) and 'Safety Rating' (5 star ratings with counts). The main area shows six modules in a grid:

- SSH Key Testing** (Credentials): Description of attempting login with a recovered SSH key. Safety Rating: 3 stars. 'Launch' button.
- Single Password Testing** (Discovery | Credentials): Description of testing usage level for weak credentials. Safety Rating: 3 stars. 'Launch' button.
- Pass the Hash** (Discovery | Intrusion): Description of attempting login with a recovered Windows SMB hash. Safety Rating: 3 stars. 'Launch' button.
- Passive Network Discovery** (Discovery | Intrusion | Auditing): Description of sniffing traffic to discover hosts and services. Safety Rating: 3 stars. 'Launch' button.
- Firewall Egress Testing** (Penetration Testing | Discovery): Description of running a full Nmap SYN scan against an external server. Safety Rating: 5 stars. 'Launch' button.
- Known Credentials Intrusion** (Penetration Testing): Description of systematically logging in with known good credentials. Safety Rating: 3 stars. 'Launch' button.

3. На вкладке «Область» введите диапазон целевых адресов, который вы хотите использовать для тестирования.

Single SSH Key Tester

Finds all systems which can be logged into using a recovered private SSH Key, and a range of hosts to try. It reports back on which hosts it was able to successfully authenticate.

Scope

Address Range: 192.168.56.0/24

Advanced ▾

☒ Generate Report

Cancel Launch

4. Перейдите на вкладку «Учетные данные». Появится форма "Учетные данные".
5. Выберите один из следующих параметров, чтобы предоставить метамодулю секретный SSH-ключ:
 - Введите пару известных учетных данных. Вам нужно вручную ввести имя пользователя, а затем перейти к местоположению закрытого ключа, который вы хотите, чтобы метамодуль использовал.
 - Выберите существующий SSH-ключ. Вы можете выбрать имя пользователя и SSH-ключ из списка украденных ключей. Эти ключи были получены в результате грубого подбора, с помощью discovery scan или эксплойта системы.

Single SSH Key Tester

Attempts to log in to systems on a target range with a recovered private SSH key and reports the hosts that it was able to successfully authenticate.

Scope*

Credentials

☒ Generate Report

Credentials

☒ Enter a known credential pair
☐ Choose an existing SSH key

User name

root

metasploitable2_root.key

Choose Key file...

Domain

Cancel

Launch

6. Перейдите на вкладку «Отчет». Появится форма конфигурации отчета.

7. Введите название отчета в поле «Название отчета», если вы хотите использовать пользовательское название отчета. В противном случае метамодуль использует название отчета по умолчанию.

8. Из PDF, HTML или RTF выберите формат, в котором вы желаете сгенерировать отчет.

9. В области Разделы отмените выбор любых разделов, которые вы не хотите включать в отчет. Пропустите этот шаг, если вы хотите сгенерировать все разделы отчета.

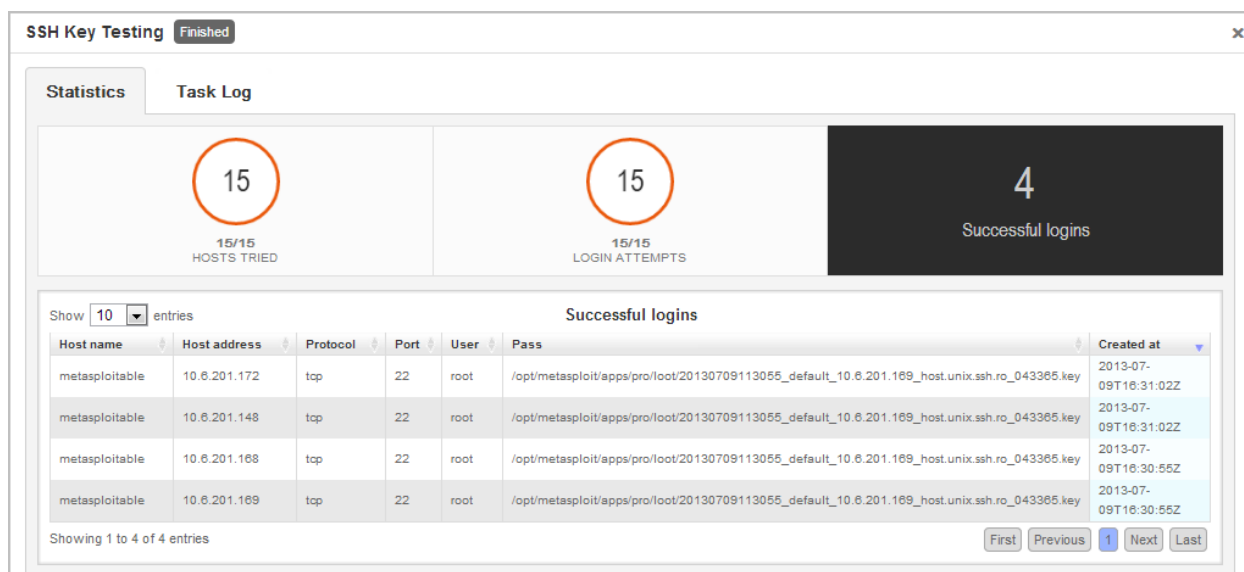
10. Выберите параметр «Отправить по электронной почте», если вы хотите отправить отчет по электронной почте отчет после его генерирования. Если вы включите этот параметр, вам необходимо предоставить список адресов электронной почты, с разделением запятыми.

Примечание: Если вы хотите отправить отчет по электронной почте, вы должны настроить локальный почтовый сервер или службу ретрансляции сообщений электронной почты для использования Metasploit Pro. Чтобы определить параметры вашего почтового сервера, выберите «Администрирование»> «Глобальные настройки»> «Настройки SMTP».

11. Нажмите кнопку «Запустить».

При запуске метамодуля, появляется окно «Результаты», в котором отображена статистика и режим задач в режиме реального времени для запуска метамодуля. Вы можете отслеживать общее количество хостов, которые метамодуль попытался аутентифицировать, общее количество попыток

входа и общее количество успешных входов. Если вы хотите просмотреть все данные о событии, вы можете кликнуть вкладку «Журнал задач».



После завершения работы метамодуля, вы должны перейти в область "Отчеты" для просмотра Отчета проверки SSH-ключа. На первых страницах отчета показаны графики и таблицы с высокоуровневой разбивкой взломанных хостов и служб. Для более детального просмотра хостов, вы можете перейти в раздел «Аутентифицированные службы и Данные о хостах», в котором показаны аутентифицированные службы, и сеансы, открытые на каждом хосте.

Метамодуль взлома известных учетных данных

Метамодуль взлома известных учетных данных входит в список указанных служб и пытается открыть сеансы на множестве хостов с известными учетными данными в проекте. Вы можете запустить этот MetaModule, если вы хотите быстро получить командные оболочки на хостах вашего проекта.

Чтобы запустить MetaModule взлома известных учетных данных, проект должен уже содержать учетные данные, которые вы либо собрали с помощью Discovery Scan, путем подбора, либо импорта данных. Метамодуль взлома известных учетных данных попытается выполнить аутентификацию каждой службы, которая была перечислена для каждого хоста. Если метамодуль может успешно войти в службу, он попытается открыть сеанс в целевой системе, который вы можете использовать для выполнения таких действий, как настройка точки доступа VPN, сбор системных данных или запуск оболочки для взаимодействия с целевой системой. Он открывает по одному сеансу в каждой целевой системе, и он переместится на следующий хост в тесте, если сеанс уже установлен для хоста.

Во время работы метамодуля, отображает статистику в режиме реального времени по количеству целевых хостов, количеству сделанных попыток входа и количество открытых сеансов. После завершения работы, метамодуль создает полный отчет, в котором представлены подробные данные хостов, в которых ему удалось открыть сеанс. Вы можете передать этот отчет своей организации, чтобы обозначить слабые пароли и помочь устранить изъяны в ее инфраструктуре безопасности.

Запуск Метамодуля взлома известных учетных данных

Перед запуском Метамодуля взлома известных учетных данных вы должны запустить Discovery Scan в диапазоне целевой сети или импортировать существующие данные хоста. Это действие приведет к заполнению проекта необходимой информацией о хосте, такой как открытые порты и службы, которые метамодулю необходимо запустить.

1. В проекте выберите «Модули»> «Метамодули».
 2. Найдите Метамодуль взлома известных учетных данных и нажмите кнопку «Запустить».
- Появится окно взлома известных учетных данных.

The screenshot displays the 'MetaModules' section of a software interface. On the left, there is a sidebar with 'Categories' (Auditing (1), Credentials (2), Discovery (4), Intrusion (2), Penetration Testing (2)) and 'Safety Rating' (5 stars (1), 4 stars & up (2), 3 stars & up (6), 2 stars & up (6), 1 star & up (6)). The main area contains six module cards, each with a title, description, safety rating, and a 'Launch' button:

- SSH Key Testing** (Credentials): Attempts to log in with a recovered SSH key. Safety Rating: 3 stars.
- Single Password Testing** (Discovery | Credentials): Tests usage level for a set of weak or exposed credentials. Safety Rating: 3 stars.
- Pass the Hash** (Discovery | Intrusion): Attempts to log in with a recovered Windows SMB hash. Safety Rating: 3 stars.
- Passive Network Discovery** (Discovery | Intrusion | Auditing): Sniffs traffic to discover hosts and services. Safety Rating: 4 stars.
- Firewall Egress Testing** (Penetration Testing | Discovery): Runs a full Nmap SYN scan against an external server. Safety Rating: 5 stars.
- Known Credentials Intrusion** (Penetration Testing): Systematically logs in with known good credentials. Safety Rating: 3 stars.

3. На вкладке «Область» введите диапазон целевых адресов, который вы хотите использовать для тестирования.

Known Credential Intrusion

Uses known credentials to compromise hosts across the entire network. You can run this MetaModule to reuse credentials that you obtained from bruteforce attacks, phishing attacks, or exploited hosts.

Scope

Address Range

10.6.201.0/24

Payload

Advanced ▾

☒ Generate Report

Cancel

Launch

4. Перейдите на вкладку «Полезная информация», чтобы настроить параметры полезной информации.

Known Credential Intrusion

Uses known credentials to compromise hosts across the entire network. You can run this MetaModule to reuse credentials that you obtained from bruteforce attacks, phishing attacks, or exploited hosts.

Scope*

Payload

☒ Generate Report

Payload Settings

Payload type

Meterpreter ▾

Connection

Auto ▾

Listener Ports

1024-85535

Listener Host

Cancel

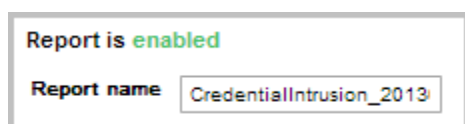
Launch

5. Укажите следующие параметры, которые вы хотите использовать для полезной информации:

- Тип полезной информации - Выберите Meterpreter для Windows или командную оболочку для Linux-систем.
- Соединение - Выберите один из следующих типов соединений:
 - Автоматически - Автоматически выбирает тип полезной информации. В большинстве случаев опция «Автоматически» выбирает полезную информацию с обратной оболочкой (реверс-шелл), потому что существует большая вероятность установить соединение между целевой машиной и атакующей машиной.
 - Reverse - выберите этот параметр, если целевые системы находятся в рамках брандмауэра или используют NAT. Как правило, полезная информация с обратной оболочкой будет работать в большинстве ситуаций.
 - Bind - Выберите этот параметр, если целевые устройства не могут инициировать соединение.
- Порты прослушивания - Порт, на котором вы хотите, чтобы слушатель прослушивал входящие подключения. По умолчанию выбраны порты 1024-65535; однако вы можете указать определенный порт, который вы хотите, чтобы слушатель использовал, например 4444.
- Хост прослушивания - IP-адрес, к которому вы хотите подключить целевую машину. Обычно это будет IP-адрес вашей локальной машины. Если вы не укажете хост прослушивания, метамодуль автоматически использует IP-адрес вашего локального компьютера.

6. Перейдите на вкладку «Создать отчет». Появится форма конфигурации отчета.

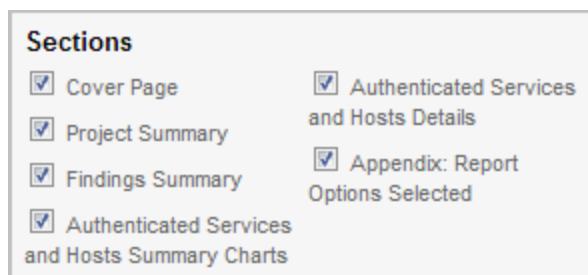
7. Введите название отчета в поле «Название отчета», если вы хотите использовать пользовательское название отчета. В противном случае метамодуль использует название отчета по умолчанию.



8. Из PDF, HTML или RTF выберите формат, в котором вы желаете создать отчет.

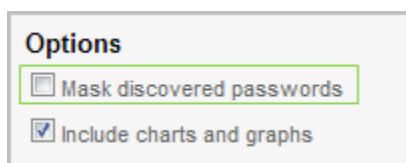


9. В области Разделы отмените выбор любых разделов, которые вы не хотите включать в отчет. Пропустите этот шаг, если вы хотите сгенерировать все разделы отчета.



10. В области «Параметры» выберите параметр «Скрыть обнаруженные пароли», если вы хотите скрыть любые пароли, содержащиеся в отчете. В отчете пароль заменяется на **СКРЫТ**. По

умолчанию этот параметр отключен. Вы должны включить этот параметр, если планируете распространять отчет.



11. Выберите параметр «Отправить по электронной почте», если вы хотите отправить отчет по электронной почте отчет после его генерирования. Если вы включите этот параметр, вам необходимо предоставить список адресов электронной почты, с разделением запятыми.

Если вы хотите отправить отчет по электронной почте, вы должны настроить локальный почтовый сервер или службу ретрансляции сообщений электронной почты для использования Metasploit Pro. Чтобы определить параметры вашего почтового сервера, выберите «Администрирование»> «Глобальные настройки»> «Настройки SMTP».

12. Нажмите кнопку «Запустить».

Метамодуль тестирования сегментации и брандмауэра

Когда брандмауэры имеют плохо настроенную или слабую политику фильтрации исходящего трафика, они открывают сеть вплоть до атак из обратных оболочек, эксфильтрации данных и других форм использования. Чтобы выявить открытые порты, разрешающие исходящий трафик, и убедиться, что ваши политики фильтрации исходящего трафика правильно блокируют трафик, вы можете запустить метамодуль для тестирования сегментации и брандмауэра.

Метамодуль запускает Nmap SYN-сканирование для выходной цели, чтобы открыть внешние порты, открытые с внутреннего хоста. Он определяет состояние портов в вашем брандмауэре на основе трафика, полученного сервером. Если сервер получает трафик, то метамодуль обозначает порт как открытый. Если брандмауэр блокирует трафик, метамодуль обозначает порт как отфильтрованный. Метамодуль отмечает остальные порты как нефильТРованные или закрытые в зависимости от их ответа на соединения. После завершения работы, метамодуль генерирует отчет, который предоставляет вам полную картину распределения состояния портов и нефильТРованных портов.

Egress Scan Target

Egress target, egadz.metasploit.com - это сервер, размещенный в Rapid7 и настроенный на открытие всех 65535 портов. Каждый порт настроен на ответ с одним пакетом SYN-ACK. В своей конфигурации по умолчанию метамодуль инициирует сканирование портов, используя 1000 наиболее распространенных портов по умолчанию Nmap; однако, если вам нужно включить дополнительные порты, вы можете определить собственный диапазон портов.

Состояния портов

Метамодуль тестирования сегментации и брандмауэра использует следующие состояния для классификации портов.

1. **Открыт:** Порту присваивается состояние "Открыт", если он разрешает трафик из сети, и сервер EGADZ его получает. Открытое состояние указывает на то, что существует приложение, которое активно принимает TCP-соединения, датаграммы UDP или ассоциации SCTP.
2. **Отфильтрован:** Порт присваивается состояние "Отфильтрован", если он отключает трафик, прежде чем он дойдет до желаемого порта на сервере EGADZ. Он не получит ответа от сервера EGADZ. Как правило, порт имеет состояние "Отфильтрован", если специальное устройство брандмауэра, правила маршрутизатора или программное обеспечение брандмауэра на основе хоста успешно заблокировали отправку трафика от порта.
3. **Закрыт:** Порту присваивается состояние "Закрыт", если он разрешает трафик через порт, но не существует приложения или службы, привязанных к порту. Закрытый порт может использоваться для определения того, находится ли хост на IP-адресе.
4. **Неотфильтрованный:** Порту присваивается неотфильтрованный трафик, если он разрешает трафик через порт, но невозможно определить, открыт ли порт или закрыт.

Настройка сервера тестирования выхода (egress)

Метамодуль тестирования выхода брандмауэра использует внешний сервер, размещенный на Rapid7, для определения открытых выходных портов с внутреннего хоста. В некоторых случаях вы также захотите настроить собственный сервер тестирования выхода. Например, если вы хотите протестировать выход между разными конечными точками или если вы не хотите отправлять данные на сервер в Интернете, вы можете настроить собственный сервер тестирования выхода.

Чтобы помочь вам настроить пользовательский сервер тестирования выхода, Metasploit Pro предоставляет вам сценарий, который можно запустить на сервере Ubuntu 12.04 LTS. Сценарий можно загрузить на странице «Проекты» в Metasploit Pro.

Требования к серверу тестирования выхода

Чтобы настроить сервер тестирования выхода вы должны выполнить следующие задачи:

1. Настроить машину с установленным Linux с вашим любимым дистрибутивом.
2. Добавьте на машину с установленным Linux два сетевых интерфейса или сетевые адаптеры. Каждый сетевой интерфейс должен иметь IP-адрес.

Для получения дополнительной информации о настройке сетевого интерфейса на виртуальной машине, ознакомьтесь с документацией к вашему программному обеспечению для виртуализации.

3. Назначьте один IP-адрес в качестве административного интерфейса. Этот интерфейс будет использоваться для управления сервером тестирования выхода. Он должен быть назначен интерфейсу eth0.
4. Назначьте второй IP-адрес в качестве сервера тестирования выхода. Этот интерфейс должен быть назначен интерфейсу eth1.
5. Загрузите и запустите сценарий сервера тестирования выхода.

Настройка пользовательской выходной цели (Egress Target)

Чтобы настроить пользовательскую выходную цель, вам понадобится диалоговое окно Ubuntu 12.04, с двумя IP-адресами.

Эти два IP-адреса необходимы для следующих интерфейсов:

1. Интерфейс администратора: Обычно его можно найти в интерфейсе eth0, и он будет использоваться для управления выходным сервером.
2. Выходной сервер: Обычно его можно найти в интерфейсе eth1 или в виртуальном интерфейсе, таком как eth0: 1 Это IP-адрес, который вы отсканируете из Метамодуля тестирования сегментации и брандмауэра.

После настройки диалогового окна с двумя адресами, выполните следующие действия:

1. Войдите в веб-интерфейс Metasploit Pro.
2. Нажмите кнопку «Сценарий настройки цели сегментации», расположенную в разделе «Глобальные инструменты».

Процесс загрузки начнется автоматически.

Если ваш браузер не настроен на автоматическую загрузку файлов, появится диалоговое окно и предложит сохранить файл. Вам нужно будет сохранить файл на свой компьютер.

3. Следуйте инструкциям, указанным в сценарии create-egadz.sh, чтобы настроить выходную цель.
4. Убедитесь, что вы можете настроить выходную цель с помощью инструкций.

После настройки выходной цели, вы можете запустить Метамодуль сегментации и тестирования брандмауэра.

Запуск Метамодуля сегментации и тестирования брандмауэра

1. В проекте выберите «Модули»> «Метамодули».
2. Найдите Метамодуль сегментации и тестирования брандмауэра и нажмите кнопку «Запустить».

The screenshot shows the Metasploit Pro interface. At the top, there's a navigation bar with 'Project - default', 'Account - tdoan', and 'Administration'. Below this is a breadcrumb trail: 'Home > default > MetaModules Overview'. On the left, under 'MetaModules', there are categories: Auditing (4), Credentials (4), Discovery (5), and Intrusion (1). Below these are safety ratings: 5 stars (2), 4 stars & up (2), 3 stars & up (6), 2 stars & up (6), and 1 star & up (6). The main area displays six modules in a grid:

- Segmentation and Firewall Testing** (Discovery | Auditing): Runs a full Nmap SYN scan against an external server hosted by Rapid7 that acts as an egress scan target. Use this MetaModule to discover outbound ports on a firewall that an attacker can use to exfiltrate information. [more...](#) Safety Rating: 5 stars. [Launch](#)
- SSH Key Testing** (Credentials | Discovery | Auditing): Attempts to log in to systems with a recovered SSH key and records the success and failure results for each service. You will need to specify the user name, SSH key filename, and range of hosts that you want to test. [more...](#) Safety Rating: 3 stars. [Launch](#)
- Single Password Testing** (Credentials | Discovery | Auditing): Tests the usage level for a set of weak or exposed credentials. It tries to log in to a range of hosts and services that you specify and records the success and failure results for each service. Safety Rating: 3 stars. [Launch](#)
- Pass the Hash** (Credentials | Discovery | Auditing): Attempts to log in to as many hosts as possible with a recovered Windows SMB hash. It reports the hosts that it was able to successfully authenticate. You specify a username, SMB hashed password, and [more...](#) Safety Rating: 3 stars. [Launch](#)
- Passive Network Discovery** (Discovery): Sniffs traffic to discover hosts and services on a local network. Since it does not send any packets, you can run this app to conduct a stealthy network discovery scan and identify any hosts, services, and clear-text credentials. Safety Rating: 5 stars. [Launch](#)
- Known Credentials Intrusion** (Credentials | Intrusion): Systematically logs in to as many hosts and services as possible using the known good credentials for this project. Run this MetaModule to reuse credentials that you have collected from compromised machines. [more...](#) Safety Rating: 3 stars. [Launch](#)

Появится окно конфигурации Сегментации и тестирования брандмауэра.

3. На вкладке «Конфигурация сканирования» выберите одну из следующих целевых опций сканирования:

- Использовать выходную цель по умолчанию - Метамодуль работает в отношении выходного сервера, который Metasploit настроил для тестирования исходящего трафика.
- Использовать пользовательскую выходную цель - Метамодуль работает в отношении выходного сервера, который вы настроили для тестирования исходящего трафика. Вы можете указать IP или полное доменное имя. Чтобы узнать, как настроить целевую выходную цель, перейдите в область «Глобальные инструменты» на странице «Проекты» и загрузите сценарий настройки цели сегментации. Вы можете следовать инструкциям, приведенным в сценарии, для создания пользовательского выходного сервера.

4. На вкладке «Конфигурация сканирования» выберите один из следующих параметров диапазона портов:

- Использовать набор портов nmap по умолчанию: Сканирует 1000 наиболее распространенных портов Nmap.
- Использовать пользовательский диапазон портов: Сканирует диапазон портов, которые определяете вы.

Segmentation and Firewall Testing

Runs an Nmap SYN scan against an egress target to identify the ports that allow egress traffic out of the network.

Scan Config

☒ Generate Report

Scan Target

☒ Use default egress target (egadz.metasploit.com)
☐ Use a custom egress target

Port Range

☒ Use default nmap port set
☐ Use a custom port range

Cancel

Launch

5. Перейдите на вкладку «Создать отчет». Появится форма конфигурации отчета.
6. Введите название отчета в поле «Название отчета», если вы хотите использовать пользовательское название отчета. В противном случае метамодуль использует название отчета по умолчанию.

7. В области Разделы отмените выбор любых разделов, которые вы не хотите включать в отчет. Пропустите этот шаг, если вы хотите сгенерировать все разделы отчета.

8. Выберите параметр «Отправить по электронной почте», если вы хотите отправить отчет по электронной почте отчет после его генерирования. Если вы включите этот параметр, вам необходимо предоставить список адресов электронной почты, с разделением запятыми.

Если вы хотите отправить отчет по электронной почте, вы должны настроить локальный почтовый сервер или службу ретрансляции сообщений электронной почты для использования Metasploit Pro. Чтобы определить параметры почтового сервера, выберите «Администрирование»> «Глобальные настройки»> «Настройки SMTP».

9. Нажмите кнопку «Запустить».

Экспорт данных

Экспорт данных позволяет вам регулярно создавать резервные копии данных проекта и создавать архив ваших тестов. Когда вы экспортируете данные из проекта, его содержимое копируется и сохраняется в файл, который может быть импортирован в другие проекты или передан другим вариантам Metasploit Pro. Все экспортируемые данные можно загрузить из области "Экспорт" веб-интерфейса или из каталога экспортированных данных.

Каталог экспортированных данных

Когда Metasploit Pro создает экспорт, он сохраняет копию файла в `/path/to/Metasploit/apps/pro/exports`. Файлы, которые хранятся в этом каталоге, будут соответствовать списку экспортированных данных, отображаемому в веб-интерфейсе.

Вы можете перейти в каталог экспортированных данных для загрузки или просмотра экспортированных данных; однако вы не должны вносить какие-либо изменения непосредственно в каталог экспортированных данных, назначенный по умолчанию. Если вам нужно изменить экспортные файлы, вы должны создать копию каталога экспортированных данных и внести изменения из нового каталога. Любые изменения, которые вы вносите непосредственно в экспортные файлы, могут вызывать несоответствия между метаданными, отображаемыми для файла в веб-интерфейсе и самим файлом.

Если вам нужно удалить экспортированные данные из проекта, вы должны сделать это из веб-интерфейса. Не удаляйте их непосредственно из каталога экспортированных данных.

Просмотр экспортированных данных, сгенерированных с помощью Metasploit Pro 4.8 и более ранних версий

Все экспортированные данные, сгенерированные с помощью Metasploit Pro 4.8 и более ранних версий, хранятся в директории `/path/to/Metasploit/apps/pro/reports`. Эти экспортированные данные были созданы с помощью более старой версии Metasploit Pro и не были перенесены в каталог экспортированных данных, который был добавлен в Metasploit Pro 4.9. Эти файлы не будут отображаться или доступны из веб-интерфейса.

Журналы экспортированных данных

В журнале экспортированных данных хранятся исторические записи всех событий, связанных с экспортом. Metasploit Pro автоматически обновляет журнал экспортированных данных всякий раз, когда вы экспортируете данные из проекта. Если у вас возникли проблемы с экспортом, вы можете просмотреть журнал экспортированных данных, чтобы найти ошибки трассировки стека и устранить их.

Просмотр журнала экспорта

Найти и просмотреть журнал экспорта можно в следующей директории:
`/path/to/Metasploit/apps/pro/ui/log`. Файл журнала называется `exports.log`.

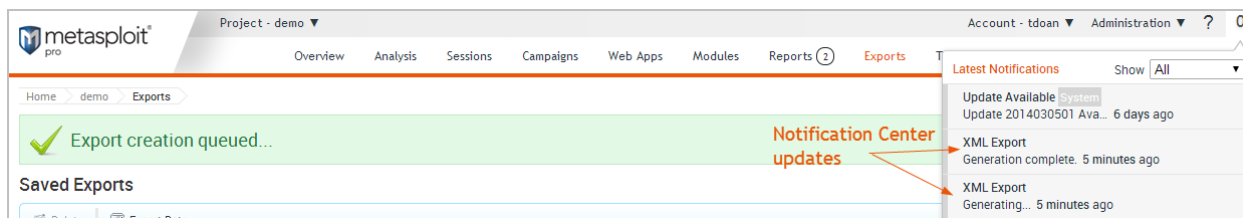
Очистка журнала экспорта

Чтобы очистить журнал экспорта, вам понадобится убрать его из директории, расположенной по адресу `/path/to/Metasploit/apps/pro/ui/log`. Metasploit Pro сгенерирует новый журнал экспорта, если обнаружит его отсутствие.

Внимание: до удаления файла `exports.log`, обязательно сделайте его копию на случай необходимости просмотреть историю позже.

Сигналы центра оповещений для экспорта

Центр оповещений предупредит вас, когда процесс экспорта запущен, завершен или остановлен из-за ошибки. Центр оповещений представлен иконкой в правом верхнем углу общей панели управлений и горит зеленым при наличии непрочитанных предупреждений. Вы можете кликнуть на иконку Центра оповещений, чтоб просмотреть список оповещений по всем проектам.



Центр оповещения показывает следующие сигналы при экспорте:

- Экспорт запущен – этот сигнал оповещает о начале экспорта.
- Экспорт завершен – этот сигнал оповещает о том, что экспорт завершен без ошибок и готов к скачиванию. Вы можете кликнуть на соответствующее предупреждение, чтобы открыть страницу экспорта с полным списком всех экспортированных файлов, сгенерированных для текущего проекта. Вы можете отсортировать их по дате создания, чтобы найти самый последний экспортированный файл.
- Проблема с экспортом – этот сигнал оповещает, что во время экспортирования возникли неполадки и процесс не был завершен. Для поиска причин неполадки нужно просмотреть журнал экспорта.

Для получения дополнительной информации о журнале экспорта читайте [раздел Журналы Экспорта](#).

Методы экспорта

Metasploit Pro предлагает вам следующие методы экспорта:

- Экспорт в XML файл, содержащий все атрибуты большинства объектов в проекте и подходящий для импорта в другой проект. Экспорт в XML особенно удобен при работе с большими объемами данных, которые вы хотите использовать в другом проекте или отправить в другую инстанцию Metasploit Pro. К примеру, вы можете экспортировать в XML проектные данные, если вы хотите использовать информацию о сканировании из определенного проекта.
- ZIP-архив рабочего пространства. Это ZIP-файл, содержащий XML, loot-файлы, файлы отчетов и журналы задач. Этот метод экспорта удобен тем, что можно быстро продублировать все данные проекта или поделиться ими с другой инстанцией Metasploit Pro.
- Скрипт повтора – пакетный файл с повтором задач, которые открывали сессии на отслеживаемых хостах. Скрипт повтора состоит из нескольких файлов ресурсов (.rc). Metasploit Pro создает файлы ресурсов для каждой открытой сессии. Вы можете запустить скрипт повтора из консоли Pro или msfconsole.

- PWDump. Это текстовый файл, содержащий все данные администраторов проекта, включая пароли в виде простого текста, SMB хэши и ключи SSH. Административные данные можно скрыть, чтобы были перечислены только имена пользователей.

Экспорт в XML

Когда вы экспортируете проект в виде XML файла, он содержит большую часть информации из аналитического раздела проекта, с несколькими исключениями. Экспортированный XML файл содержит большую часть объектов из базы данных проекта, а также их атрибуты. В нем нет файлов, связанных с объектами в проекте (журналы задач, сгенерированные отчеты и loot-файлы).

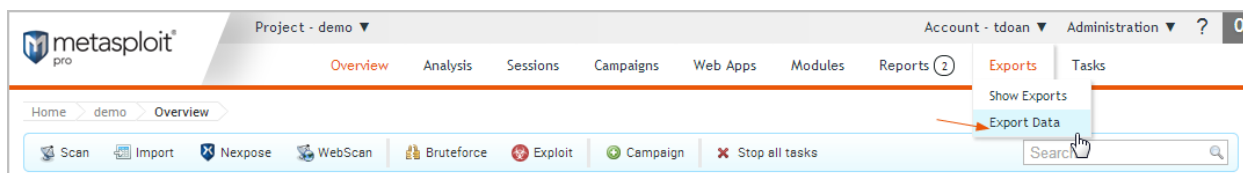
При просмотре экспортированного XML файл вы увидите следующие объекты:

- Хосты – детализированная информация по каждому хосту в проекте, включая следующие атрибуты: записи, тэги, уязвимости, данные администратора и сессии. Сюда также включаются другие данные: ID хоста, адрес, MAC адрес, название события и имя пользователя, инициировавшего задачу.
- События – журнал событий в проекте. Каждое событие включает ID рабочего пространства, дату создания события, название события и имя пользователя, инициировавшего задачу.
- Сессии – детализированная информация по каждой сессии в проекте, включая следующие атрибуты: ID хоста, тип сессии, использованные модули, описание сессии, использованные порты и время открытия и закрытия сессии.
- Сервисы – детализированная информация по каждому сервису, обнаруженному в проекте, включая ID хоста, номер порта, тип протокола, состояние, название сервиса, дату создания и дату модификации.
- Данные администратора – детализированная информация по каждому блоку административных данных, сохраненных в проекте, включая ID блока данных, ID сервиса, имя пользователя, пароль, дату создания и дату модификации.
- Вебсайты – детализированная информация по каждому обнаруженному веб серверу, включая ID вебсайта, ID сервиса, адрес хоста, адрес VHOST, HTTP порт, дату создания и дату модификации.
- Веб формы – детализированная информация по каждой обнаруженной веб форме, включая ID веб формы, путь к форме, тип запроса, адрес VHIST, HTTP порт, контент страницы, дату создания и дату модификации.
- Веб уязвимости – детализированная информация по каждой обнаруженной уязвимости, включая категорию уязвимости, описание уязвимости, (позиция в рейтинге доверия?), метод запроса, название уязвимости, HTTP порт, адрес VHOST и vulnerability blame.

Внимание: у некоторых объектов могут быть дополнительные атрибуты, но в списке выше перечислены основные атрибуты для каждого объекта.

Создание XML файла с данными проекта

1. Откройте проект, из которого вы хотите экспортировать данные.
2. Выберите Exports > Export Data в панели вкладок. Появится страница экспорта данных.



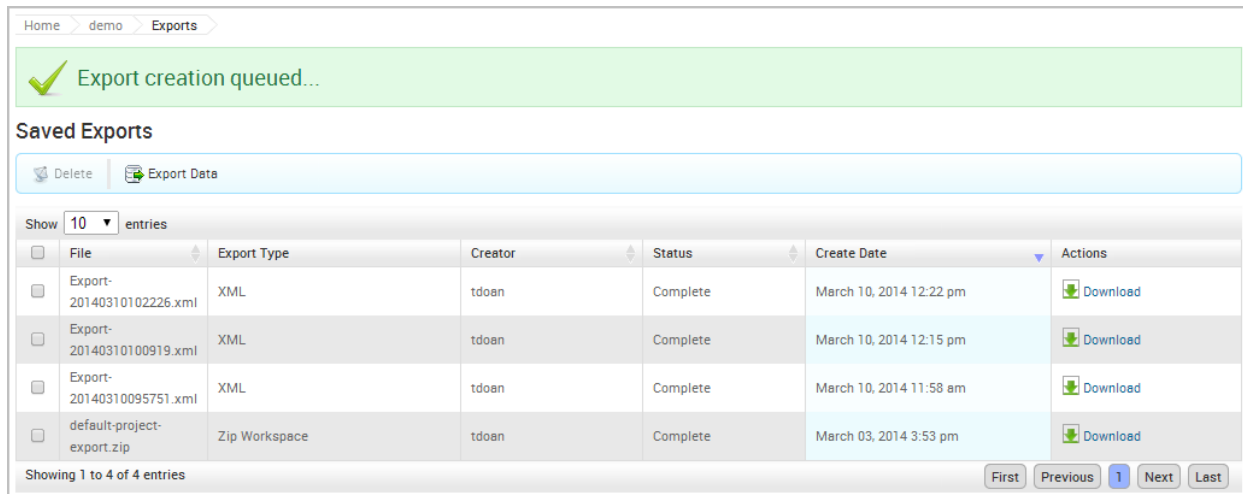
3. Выберите XML Export из предложенных форматов для экспорта.

Export Type

Export type* ?

4. Замените название файла на новое. Если не хотите, то можно оставить название по умолчанию. (Необязательно).
5. Определите хосты, которые вы хотите включить в файл, в поле «Included Addresses». (Необязательно).
6. Определите хосты, которые вы хотите исключить из файла, в поле «Excluded Addresses». (Необязательно).
7. Выберите опцию «Mask credentials» в настройках экспорта, если вы не хотите включать данные администраторов в экспортируемый файл.
Все скрытые данные будут заменены на ****MASKED**** в XML файле. Если вы импортируете его в проект, то данные администраторов не будут в него включены.
8. Нажмите на кнопку «Export Data».

Когда начнется экспортирование, вы попадете назад на страницу «Exports», где будет отображено сообщение «Export creation queued»/«Процесс экспорта в очереди».



Иконка Центра оповещений загорится зеленым и предупредит о начале и завершении экспортирования. Вы можете кликнуть на иконку Центра оповещения, чтобы просмотреть полный список всех предупреждений. Когда экспорт будет завершен, вы можете кликнуть на сообщение или выбрать Exports > Show Exports в панели вкладок, чтобы перейти в раздел экспорта.

По завершении экспорта, он появляется в списке «Exports List». Для создания автоматического имени используется следующий принцип: export-[текущие дата и время]. Если вы не видите операцию экспорта в самом верху списка, кликните на столбец «Create Date»/ «Дата создания», чтобы упорядочить список по дате создания.

Если во время экспорта произойдет ошибка и он не будет завершен, вы сможете просмотреть журнал экспорта для идентификации и поиска решения возникающих проблем. Для дополнительной информации по журналам экспорта, читайте раздел «[Export Logs](#)».

ZIP-архив рабочего пространства

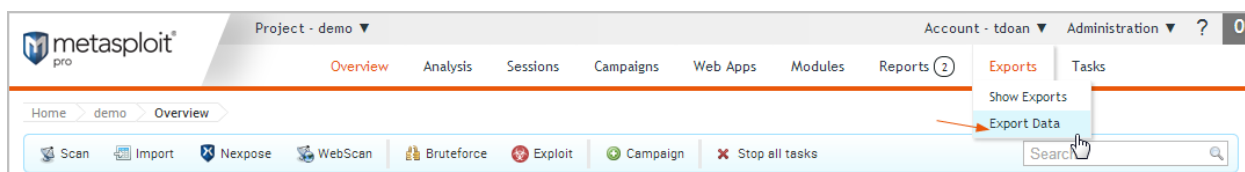
ZIP-архив содержит отчет в виде XML, где есть все атрибуты для большинства объектов в проекте и любые связанные директории, содержащие loot-файлы, файлы отчетов и журналы задач. Вы можете экспортировать рабочее пространство в ZIP, чтобы создать копию проекта, его данных и файлов. Это удобно при резервном копировании найденных уязвимостей и импорте данных в другие проекты.

Когда вы экспортируете проект, Metasploit Pro генерирует ZIP файл, содержащий:

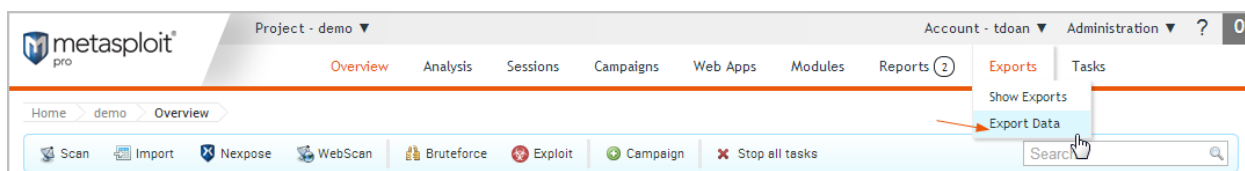
- Экспортированный XML файл – содержит большинство объектов проекта, включая хосты, сервисы, сессии, данные администраторов, данные модулей и события.
- Директорию отчетов – содержит все сгенерированные отчеты по проекту.
- Директорию задач – содержит текстовые файлы с деталями по каждой запущенной задаче.
- Директорию Loot – содержит loot-файлы проекта, включая хэши и SHN ключи.

Создание ZIP-архива проекта

1. Откройте проект, из которого вы хотите экспортировать рабочее пространство.
2. Выберите Exports > Export Data на панели вкладок. Появится окно экспорта данных.



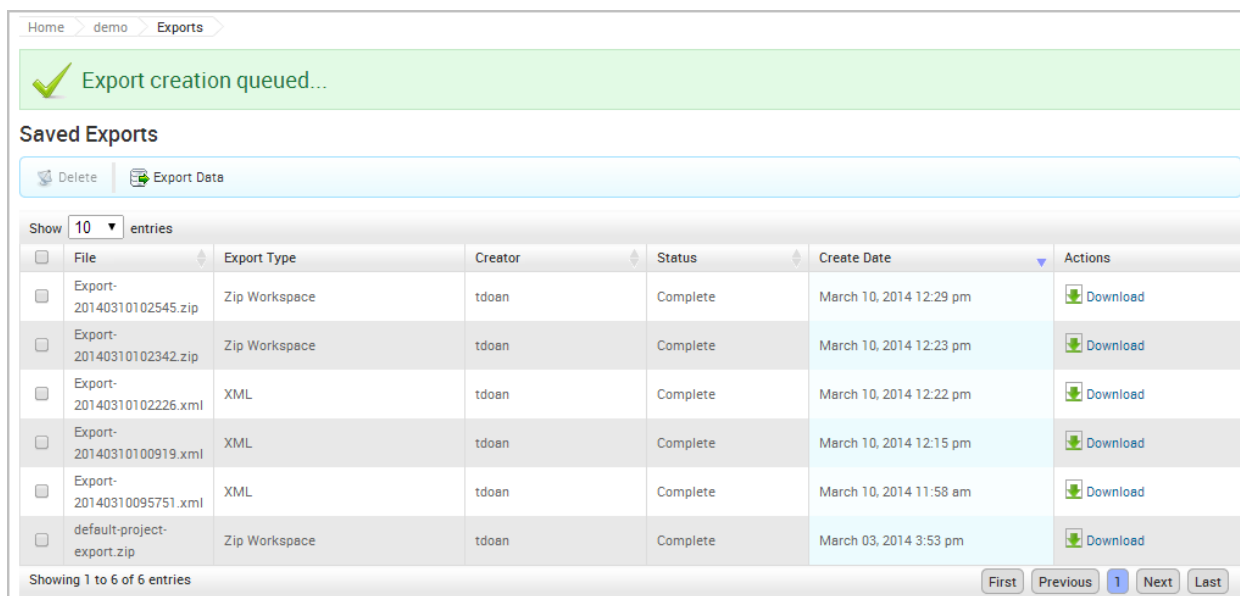
3. Выберите «ZIP Workspace»/ «Архивировать рабочее пространство» из списка форматов для экспорта.



4. Замените название файла на новое. Если не хотите, то можно оставить название по умолчанию. (Необязательно).
5. Определите адреса, которые вы хотите включить в файл, в поле «Included Addresses». (Необязательно).
6. Определите адреса, которые вы хотите исключить из файла, в поле «Excluded Addresses». (Необязательно).
7. Выберите опцию «Mask credentials» в настройках экспорта, если вы не хотите включать данные администраторов в экспортируемый файл.
8. Нажмите на кнопку «Export Data».

Когда начнется экспортирование, вы попадете назад на страницу «Exports», где будет отображено сообщение «Export creation queued»/«Процесс экспорта в очереди».

Иконка Центра оповещений загорится зеленым и предупредит о начале и завершении экспортирования. Вы можете кликнуть на иконку Центра оповещения, чтобы просмотреть полный список всех предупреждений. Когда экспорт будет завершен, вы можете кликнуть на сообщение или выбрать Exports > Show Exports в панели вкладок, чтобы перейти в раздел экспорта.



По завершении экспорта, ZIP-архив появляется в списке «Exports List». Для создания автоматического имени используется следующий принцип: export-[текущие дата и время]. Если вы не видите операцию экспорта в самом верху списка, кликните на столбец «Create Date»/ «Дата создания», чтобы упорядочить список по дате создания.

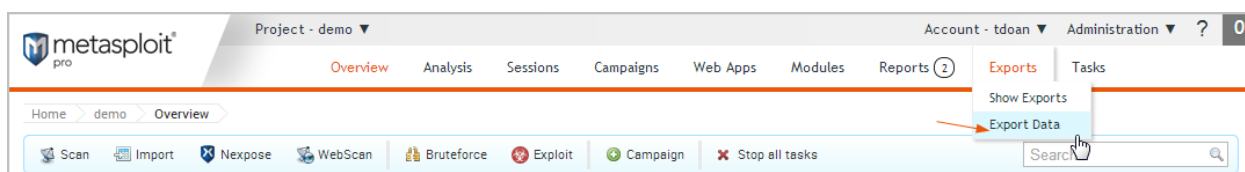
Если во время экспорта произойдет ошибка и он не будет завершен, вы сможете просмотреть журнал экспорта для идентификации и поиска решения возникающих проблем. Для дополнительной информации по журналам экспорта, читайте раздел «[Export Logs](#)».

Скрипты повтора

Скрипт повтора – это пакетный файл, запускающий все задачи, открывшие сессии на целевом хосте. Вы можете экспортировать скрипт для автоматизации успешных атак посредством Pro Console или MSFConsole. Когда вы экспортируете скрипт повтора, Metasploit Pro создает специальный файл ресурсов для каждой открытой сессии и сжимает их в ZIP-архиве.

Экспортирование скриптов повтора

1. Откройте проект, из которого вы хотите экспортировать рабочее пространство.
2. Выберите Exports > Export Data на панели вкладок. Появится окно экспорта данных.



3. Выберите «Replay Script»/ «Скрипт повтора» из списка форматов для экспорта.

4. Определите хосты, которые вы хотите включить в скрипт, в поле «Included Addresses». (Необязательно).
5. Определите хосты, которые вы хотите исключить из скрипта, в поле «Excluded Addresses». (Необязательно).
6. Выберите опцию «Mask credentials» в настройках экспорта, если вы не хотите включать данные администраторов в экспортируемый файл.
7. Нажмите на кнопку «Export Data».

Когда начнется экспортирование, вы попадете назад на страницу «Exports», где будет отображено сообщение «Export creation queued»/«Процесс экспорта в очереди».

Иконка Центра оповещений загорится зеленым и предупредит о начале и завершении экспортирования. Вы можете кликнуть на иконку Центра оповещения, чтобы просмотреть полный список всех предупреждений. Когда экспорт будет завершен, вы можете кликнуть на сообщение или выбрать Exports > Show Exports в панели вкладок, чтобы перейти в раздел экспорта.

По завершении экспорта, ZIP-архив появляется в списке «Exports List». Для создания автоматического имени используется следующий принцип: export-[текущие дата и время]. Если вы не видите операцию экспорта в самом верху списка, кликните на столбец «Create Date»/ «Дата создания», чтобы упорядочить список по дате создания.

Если во время экспорта произойдет ошибка и он не будет завершен, вы сможете просмотреть журнал экспорта для идентификации и поиска решения возникающих проблем. Для дополнительной информации по журналам экспорта, читайте раздел [«Export Logs»](#).

Запуск скрипта повтора при помощи Pro Console или MSFConsole

Для запуска скрипта повтора используется команда «Resource». Она загружает пакетный файл и прогоняет его через Pro Console или MSFConsole. Команда обязательно должна включать в себя путь к скрипту. К примеру, вы можете ввести в консоли «resource /path/to/session_ID_IP.rc» для загрузки повтора и запуска команд, сохраненных в файле.

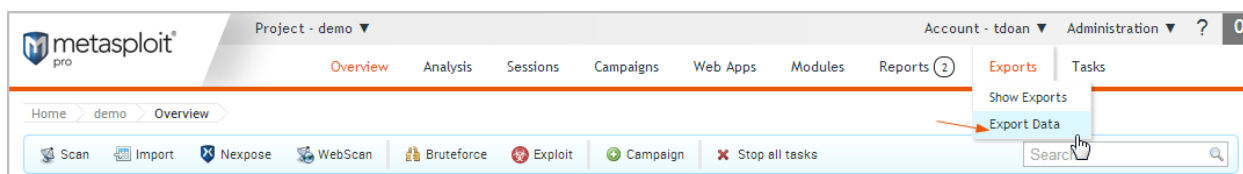
! Чтобы запустить файл ресурса, нужно извлечь его из ZIP-архива.

PWDumps

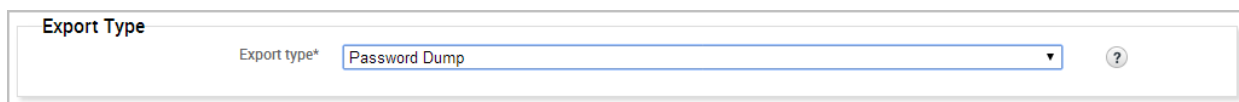
PWDumps – это текстовый файл, содержащий все данные администраторов проекта, включая пароли открытым текстом, SMB хэши и SSH ключи. Вы можете экспортировать файл PWDump, чтобы настроить оффлайновый взлом пароля при помощи инструментов типа «John the Ripper».

Экспортирование в файл PWDump

1. Откройте проект, из которого вы хотите экспортировать данные.
2. Выберите Exports > Export Data на панели вкладок. Появится окно экспорта данных.



3. Выберите «PWDump» из списка форматов для экспорта.



The image shows a web interface element labeled 'Export Type'. It features a dropdown menu with the text 'Export type*' and 'Password Dump' selected. A question mark icon is visible to the right of the dropdown.

4. Определите хосты, которые вы хотите включить в файл, в поле «Included Addresses». (Необязательно).
5. Определите хосты, которые вы хотите исключить из файла, в поле «Excluded Addresses». (Необязательно).
6. Нажмите на кнопку «Export Data».
7. Когда начнется экспортирование, вы попадете назад на страницу «Exports», где будет отображено сообщение «Export creation queued»/«Процесс экспорта в очереди».

Иконка Центра оповещений загорится зеленым и предупредит о начале и завершении экспортирования. Вы можете кликнуть на иконку Центра оповещения, чтобы просмотреть полный список всех предупреждений. Когда экспорт будет завершен, вы можете кликнуть на сообщение или выбрать Exports > Show Exports в панели вкладок, чтобы перейти в раздел экспорта.

По завершении экспорта, файл PWDump появляется в списке «Exports List». Для создания автоматического имени используется следующий принцип: export-[текущие дата и время]. Если вы не видите операцию экспорта в самом верху списка, кликните на столбец «Create Date»/ «Дата создания», чтобы упорядочить список по дате создания.

Если во время экспорта произойдет ошибка и он не будет завершен, вы сможете просмотреть журнал экспорта для идентификации и поиска решения возникающих проблем. Для дополнительной информации по журналам экспорта, читайте раздел «Export Logs» на странице 199.

Просмотр экспортированных данных

Для просмотра всех экспортированных данных выберите Exports > Show Exports на панели вкладок. В списке «Data Exports» будут отображены все экспортированные данные, связанные с проектом. Вы можете кликнуть на кнопки «Download»/ «Скачать» или «View»/ «Просмотр» для работы с любым файлом.

Социальная инженерия

Социальная инженерия – это метод атаки, эксплуатирующий различные каналы связи (e-mail, веб-странички или USB ключи) для того, чтобы заставить жертву поделиться важной персональной информацией или сделать что-то, что позволит атакующему найти уязвимость в системе. Проведение тестов из области социальной инженерии позволяет оценить, насколько хорошо сотрудники следуют рекомендациям по безопасности, и идентифицировать уязвимости, созданные людьми и бизнес-процессами в организации.

Данные, собранные при помощи правильного использования приемов социальной инженерии, позволяют получить информативную картину рисков и уязвимостей, существующих в инфраструктуре и кодексе безопасности организации, которая сможет использовать результаты теста для усиления собственной политики безопасности, улучшения IT-защиту и повышения эффективности программ обучения персонала в области безопасности.

В Metasploit Pro вы можете создавать и проводить кампании в области социальной инженерии. Кампания – это логическое объединение методов и приемов, которые вы будете использовать для фишинга и атак на группы людей. Вы можете создавать кампании при помощи следующих компонентов:

- Механизмы доставки совершения атак: электронная почта, веб-странички и отдельные файлы.
- Шаблоны: HTML-оболочки, содержащие шаблонные сообщения. Оболочки можно быстро размножить в рамках кампании в проекте. Вы можете создавать и использовать шаблоны для быстрого создания веб страниц и электронных писем.
- Target List/Список целей определяет получателей и их электронные адреса, на которые будут отправлены сообщения.

Методики социальной инженерии

Главное задачей социальной инженерии является заставить цель совершить какое-то запрещенное действие, что позволит вам проникнуть в систему или получить от цели важную информацию.

Социальная инженерия обычно использует атаки по электронной почте, стараясь выявить уязвимости на стороне целевой организации. Это позволяет впоследствии атаковать по тем направлениям, которые доступны только локальным пользователям. Такие атаки обычно проводятся с применением файлов с измененным расширением для получения доступа к локальным файлам и приложениям, сохраненным на компьютере жертвы. Иногда применяются фишинговые тактики для сбора информации от самих пользователей. К примеру, вы можете приложить PDF-файл с эксплойтом типа Cooltype к электронному письму и отправить его группе людей. Когда получатель откроет инфицированный документ PDF, эксплойт запускает сессию на его компьютере, если он уязвим к эксплойту Cooltype.

Оптимальные методы вы подбираете сами, основываясь на целях и задачах социальной инженерии. К примеру, если вы хотите проверить, правильно ли в организации обрабатывают электронные письма с бизнес-предложениями и рекламой, вы можете организовать подобную фишинговую атаку. Если требуется оценка того, насколько хорошо в организации следуют к проверенным рекомендациям безопасности, вы можете сгенерировать независимый файл приложения, загрузить его на USB-носитель и подбросить его тестируемой группе. Несколько широко используемых методов социальной инженерии представлены ниже.

Фишинг

Фишинг – это метод захвата важной персональной информации вроде имен пользователей, паролей или данных кредитных карт напрямую от цели. В этом случае цель получает электронное письмо, замаскированное под реальное сообщение от источника, которому можно доверять (банк или государственная организация). Электронное письмо содержит ссылку на мошеннический веб сайт, который выглядит идентично официальному сайту организации, от которой пришло письмо. Имитируются стиль, логотип и основные изображения. Если фишинговая атака увенчалась успехом, цель заполнит веб форму и добровольно предоставит злоумышленнику все необходимые данные для продолжения атаки.

Чтобы настроить фишинговую атаку в Metasploit Pro, вам понадобится создать кампанию, содержащую следующие компоненты:

- Электронное письмо. Можно задать содержимое, которое вы хотите отправить в теле письма, и список получателей, которые будут подвергнуты атаке. Кампания не может содержать больше одного такого компонента.
- Веб-страничка. Можно задать путь к страничке, содержимое HTML и URL для перенаправления. Веб-страница, которую вы создаете, должна содержать форму, которую будет заполнять цель для передачи информации.

Эксплойты для использования на компьютере пользователя

Такие эксплойты используются для поиска уязвимостей в программном обеспечении цели (браузеры, приложения для управления электронной почтой, медиа проигрыватели). В случае использования эксплойтов жертва должна посетить зараженный вебсайт, чтобы запустить эксплойт. Эта форма кибератаки отличается от традиционного способа использования эксплойтов. В нашем случае необходимо наладить связь между атакующим компьютером и компьютером пользователя. Традиционные эксплойты не предусматривают взаимодействия с целью.

Когда цель посещает веб-страницу, содержащую эксплойт, запускается сессия на компьютере-клиенте, открывая атакующему доступ к интерфейсу операционной системы, если она уязвима для эксплойта. Во время открытой сессии вы сможете делать скриншоты, заполучить файлы паролей и атаковать другие звенья сети.

Для использования определенных типов файлов и эксплойтов в Metasploit Pro вы можете создать кампанию со следующими компонентами:

- Электронное письмо. Можно задать содержимое, которое вы хотите отправить в теле письма, и список получателей, которые будут подвергнуты атаке. Можно добавить ссылку на вебсайт, где будет размещен эксплойт.
- Веб-страничка (Необязательно). Можно задать содержимое HTML и URL для отслеживания.

Файлы с прикрепленным эксплойтом

Подобный вид эксплойтов ориентирован на использование уязвимостей в программах, открывающих определенные типы файлов (PDF, DOC, JPEG и другие). Эксплойт запускается, когда цель открывает файл, с присоединенным к нему эксплойтом. К примеру, можно прикрепить к обычному документу Word эксплойт типа MS11-006 и вложить документ в электронное письмо. Когда цель скачает и просматривает документ, атакующий получает доступ к интерфейсу операционной системы.

Чтобы провести атаку при помощи вложенных в e-mail файлов, вы можете создать кампанию со следующими компонентами:

- Электронное письмо. К нему прикрепляется файл с эксплойтом. В кампании также указываются адреса целей для атаки.
- Портативный файл. Генерируется файл с обычным расширением и прикрепленным к нему эксплойтом. Файл можно хранить на USB-носителе.

Подписанные Java-апплеты

Модуль «Java Signed Social Engineering Code Execution» создает файл с расширением .jar и подписывает его. Вам достаточно просто доставить подписанный Java-апплет цели при помощи веб-странички, содержащей тэг апплета. Когда цель попадает на страницу, виртуальная машина Java спрашивает, доверяет ли пользователь подписанному апплету. Если цель запускает его, открывается сессия доступа к компьютеру жертвы.

Портативные файлы

Обычно они используются для подброса USB-накопителей. Портативным файлом может быть приложение или прикрепленный к файлу эксплойт, загруженные на USB-накопитель. Когда цель открывает файл с накопителя, между атакующим и компьютером пользователя открывается канал связи.

Чтобы создать портативный файл в Metasploit Pro, вам нужно создать кампанию, содержащую следующие компоненты:

- Портативный файл. Генерируется файл приложения или с эксплойтом.

Терминология в социальной инженерии

До начала работы с кампаниями вам следует ознакомиться с основными терминами из мира социальной инженерии.

Кампания/Campaign

Кампания представляет собой группу взаимосвязанных компонентов, используемых для проведения атаки. Кампания может содержать только 1 компонент электронной почты, но может иметь несколько веб страниц и используемых портативных файлов.

Отслеживание кликов/Click Tracking

Это метод тестирования проверки безопасности, заключающийся в подсчете количества целей, которые кликают на предоставленную ссылку. Веб странички ведут подсчет количества визитов и помогают организации идентифицировать насколько сотрудники и члены организации подвержены атакам на фронте социальной инженерии.

Шаблон электронного письма/e-mail template

Шаблон электронного письма содержит подготовленный заранее HTML-контент.

Файл-приложение/executable

Файл-приложение автоматически запускается после открытия целью файла. Задачей файла является установление связи между компьютером атакующего и компьютером цели.

Файл с прикрепленным эксплойтом/File Format Exploit

Это файл с обычным расширением и привязанным к нему эксплойтом, использующим для проникновения уязвимости приложений, открывающих файл. Чаще всего используются уязвимости Microsoft Word и Adobe PDF.

Цель/Human Target

Цель-человек является жертвой атаки и может быть частью настроенной кампании.

Фишинговая атака

Фишинг – это метод захвата важной персональной информации вроде имен пользователей, паролей или данных кредитных карт напрямую от цели. В этом случае цель получает электронное письмо, замаскированное под реальное сообщение от источника, которому можно доверять (банк или государственная организация). Электронное письмо содержит ссылку на мошеннический веб сайт, который выглядит идентично официальному сайту организации, от которой пришло письмо. Имитируются стиль, логотип и основные изображения.

Портативный файл

Специально сгенерированный файл-приложение или файл с эксплойтом. Может распространяться по электронной почте или же на USB-носителе. Когда цель открывает файл, запускается приложение, устанавливающее связь между компьютером атакующего и компьютером цели.

Файл ресурса/Resource File

Файл ресурса может представлять собой шаблон веб страницы, электронного письма или же список целей. Это файл, который вы можете использовать в нескольких кампаниях. У каждого проекта свой набор файлов ресурсов. Эти файлы нельзя использовать в разных проектах.

Список целей/Target List

Список целей содержит цели, которые вы хотите включить в кампании. Можно использовать списки для того, чтобы точно указать получателей для электронных писем во время массовой атаки.

Отслеживание GIF/Tracking GIF

Установка куки в браузер при открытии целью электронного письма.

Отслеживание ссылки/Tracking Link

Состоит из URL-пути к веб странице и строки отслеживания. Когда цель кликает URL, система устанавливает куки для отслеживания этого и последующих визитов.

Строка отслеживания/Tracking String

Это 64-битная строка с информацией об ID цели и ID электронного письма. Кампании используют строки отслеживания для мониторинга активности цели.

Посещение/Visit

Фиксируется при нажатии ссылки и открытии веб страницы целью.

Веб шаблон/Web Template

Содержит предварительно подготовленное HTML содержимое, которое можно вставить в веб страничку.

Управление кампаниями

В Metasploit Pro вы можете создавать и запускать кампании для проведения атак в области социальной инженерии. Кампании содержат электронные письма, веб страницы и портативные файлы – все это необходимо для проведения атаки против группы целей. Вы можете настроить кампании таким образом, чтобы совершать фишинговые атаки, запускать эксплойты на компьютерах целей, использовать подписанные java-апплеты, генерировать файлы-приложения с загрузкой на USB-носители, а также отправлять электронные письма с инфицированными вложениями.

Кампания отслеживает количество целей, ставших жертвами атаки и представляет результаты отслеживания в виде специального отчета по социальной инженерии. Вы можете просмотреть отчет для оценки показателей кампании, узнать о рекомендуемых методах переобучения персонала и определить общую эффективность кампании. Дополнительно, страница кампании обновляется в реальном времени и показывает релевантную статистику, что позволяет максимально эффективно управлять кампанией. К примеру, вы можете посмотреть количество

получателей электронного письма, открывших само письмо или заполнивших веб форму при симуляции фишинговой атаки.

Кампания – это группа взаимосвязанных компонентов, необходимых для подброса эксплойтов или фишинга, направленных на группу целей. Кампания может быть составлена из нескольких компонентов: электронного письма, веб страниц и портативных файлов. Компоненты, которые добавляете к кампании, должны подбираться с учетом целей и задач самой атаки.

Ограничения кампаний

Есть несколько ограничений при создании кампаний:

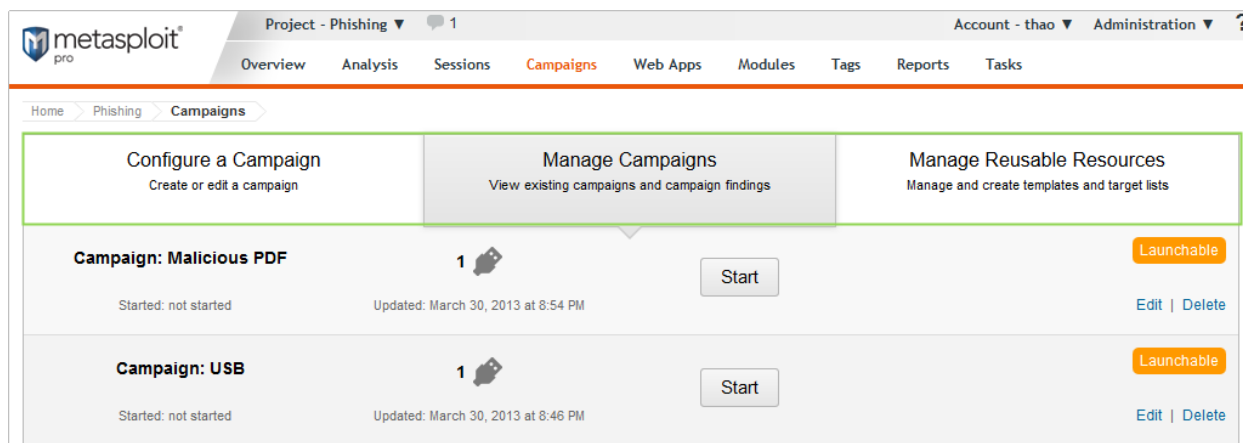
- Кампания не может содержать больше одного электронного письма.
- Кампания для фишинга не может содержать больше одного электронного письма, но может иметь 2 веб страницы. Одна из них используется в качестве лендинга, а другая в качестве страницы для перенаправления. Если вам необходимы дополнительные странички для перенаправления, используйте конструктор кампаний.
- В каждой отдельно установленной версии Metasploit Pro можно вести не больше 1 кампании одновременно.

Панель кампании

Панель кампании содержит интерфейсы и инструменты, необходимые для настройки кампаний по социальной инженерии. Панель обеспечивает доступ к кампаниям, спискам целей и файлам ресурсов в проекте. Панель кампании представлена в виде блока задач, модальных окон, виджетов для кампании и активные ссылки.

Блок задач кампании

В панели кампании под блоком главных задач расположен блок задач кампании. Каждая вкладка в этом блоке отвечает за управление важными функциональными составляющими в области социальной инженерии. Кликайте на вкладки для быстрого переключения между вкладками «управление кампанией»/«campaign configuration», «конфигурация кампании»/«campaign management» и «элементы кампании»/«campaign elements».

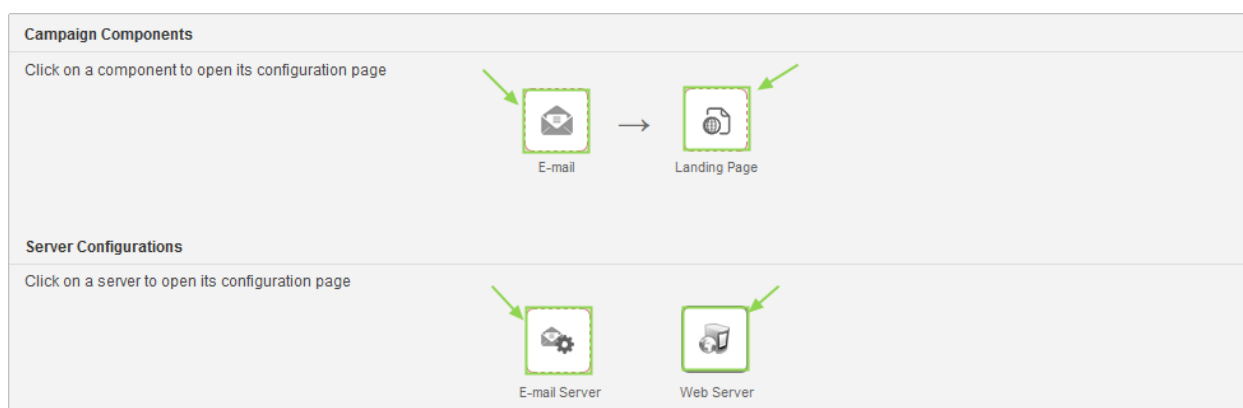


В блоке располагаются несколько важных вкладок:

- Конфигурирование кампании. Отображает редактор кампании. используйте его для создания новых кампаний и корректировки активных.
- Управление кампанией. Отображает список текущих кампаний в проекте. Напротив каждой позиции списка расположены активная ссылка. Используйте их для редактирования, удаления, сброса, предпросмотра, остановки или запуска кампании.
- Управление ресурсами кампании. Обеспечивает доступ к интерфейсу управления ресурсами кампании, включая шаблоны электронных писем, шаблоны веб страниц и инфицированные файлы.

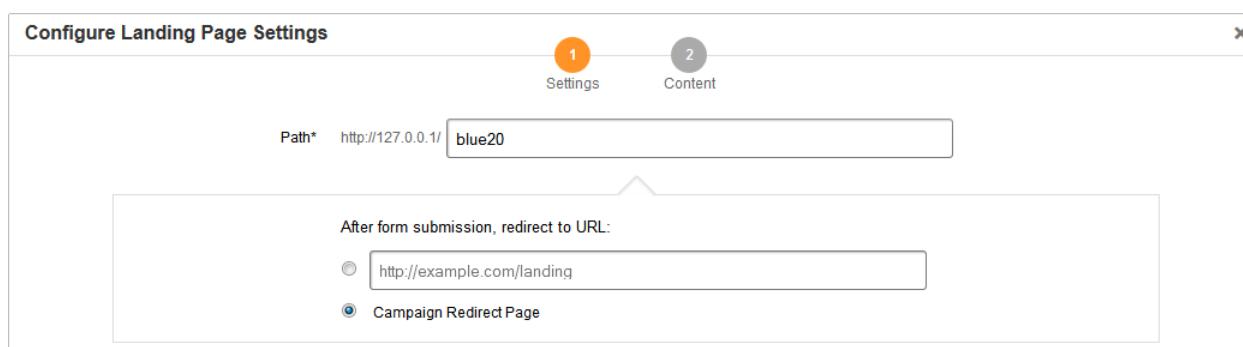
Виджет кампании.

Это иконка отображающая компонент кампании. Когда вы кликаете на виджет, открывается модальное окно с конфигурацией выбранного компонента кампании.



Модальные окна

Модальное окно представляет собой всплывающее окно, требующее обязательно взаимодействия для возврата обратно в главное окно. Обычно модальные окна используются для отображения предупреждений или подтверждения действий в Windows. В Metasploit Pro модальное окно будет для вас проводником по процессу настройки компонентов кампании. Чтобы выйти из модального окна, вы должны заполнить обязательные к заполнению поля формы или просто кликнуть на «X», чтобы закрыть окошко.



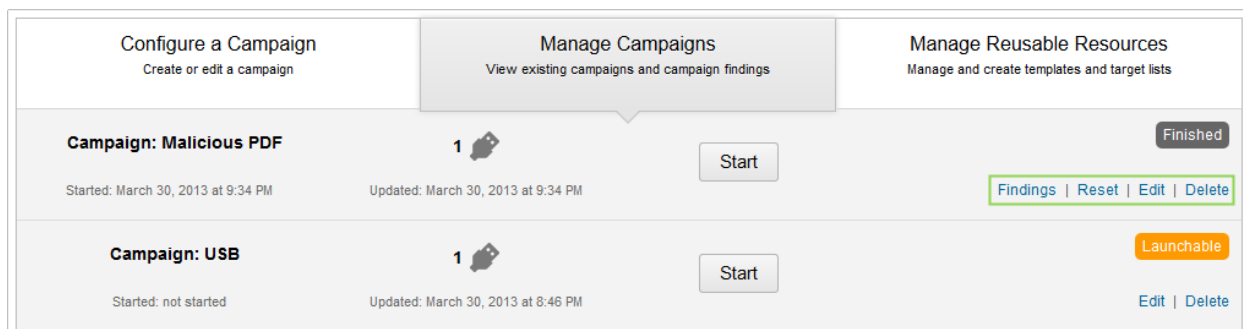
Активные ссылки

Это интерактивная ссылка, позволяющая выполнить задачу по клику мыши. Каждая кампания сопровождается набором активных ссылок:

- «Старт/Start» – запуск кампании.
- «Стоп/Stop» – остановка кампании.
- «Предпросмотр/Preview» – предварительный просмотр электронных писем и веб страниц.

- «Сброс/Reset» – сброс текущей статистики и данных кампании.
- «Редактировать/Edit» – редактирование текущей конфигурации компонентов кампании.

На изображении показаны активные ссылки, доступные вам при работе с кампанией.



Состояние кампании

Состояния описывают текущий статус кампании. В каждый отдельно взятый момент времени кампания может быть в одном из следующих состояний:

- Несконфигурированная/Unconfigured – кампания не содержит никаких компонентов или содержит ненастроенные компоненты.
- «Подготавливается/Preparing» – кампания почти готова к запуску.
- «Готова к запуску/Launchable» – кампания полностью готова к запуску.
- «Работает/Running» – кампания выполняется.

Для кампаний с активными веб страницами это означает, что веб страницы находятся в режиме онлайн и доступны компьютерам в кампании.

Для кампаний с электронными письмами это означает, что Metasploit Pro совершил рассылку писем всем целям в списке через предоставленный почтовый сервис.

Для кампаний, содержащих портативные файлы, это означает, что обработчик готов ко входящим соединениям с целевыми компьютерами.

- «Закончена/Finished» – Кампания более не активна.

Для кампаний с веб страницами это означает, что веб страницы более недоступны и не могут быть никем просмотрены.

Для кампаний, содержащих портативные файлы, это означает, то обработчик более не принимает входящие соединения.

Создание кампании

1. В проекте выберите «Кампании/Campaigns» в меню задач.
2. Когда откроется панель «Управление кампаниями/Manage Campaigns», кликните на вкладку «Настроить кампанию/Configure a Campaign».
3. Когда откроется панель «Настроить кампанию/Configure a Campaign», введите название для кампании в поле «Имя/Name».
4. Выберите один из следующих вариантов настройки:

- «Фишинговая кампания/Phishing Campaign» – Metasploit Pro автоматически создаст кампанию со всеми необходимыми компонентами для настройки фишинговой атаки. Фишинговая кампания состоит из компонента электронной почты и двух компонентов веб-страниц, которые настраиваются в качестве лендинга и странички для перенаправления.
- «Своя кампания/Custom Campaign» - вы самостоятельно создаете кампанию и добавляете необходимые вам компоненты. К примеру, если вам нужно сгенерировать портативный файл или файл с прикрепленным экслойтом.
Теперь вы готовы к настройке кампании. Если кампания пуста, вам нужно будет добавить к ней компонент, чтобы она стала активной. К примеру, если вам нужно сгенерировать файл-приложение для запуска с USB-носителя, вы можете добавить к кампании соответствующий компонент.

Редактирование названия кампании

1. В проекте выберите «Кампании/Campaigns» в меню задач.
2. Когда откроется панель «Управление кампаниями/Manage Campaigns», найдите кампанию, название которой нужно изменить.
3. Кликните на активную ссылку «Редактировать/Edit».
4. На странице конфигурации кампании удалите текущее название в поле «Имя/Name».
5. Введите в поле новое желаемое имя.
6. Нажмите на кнопку «Сохранить/Save».

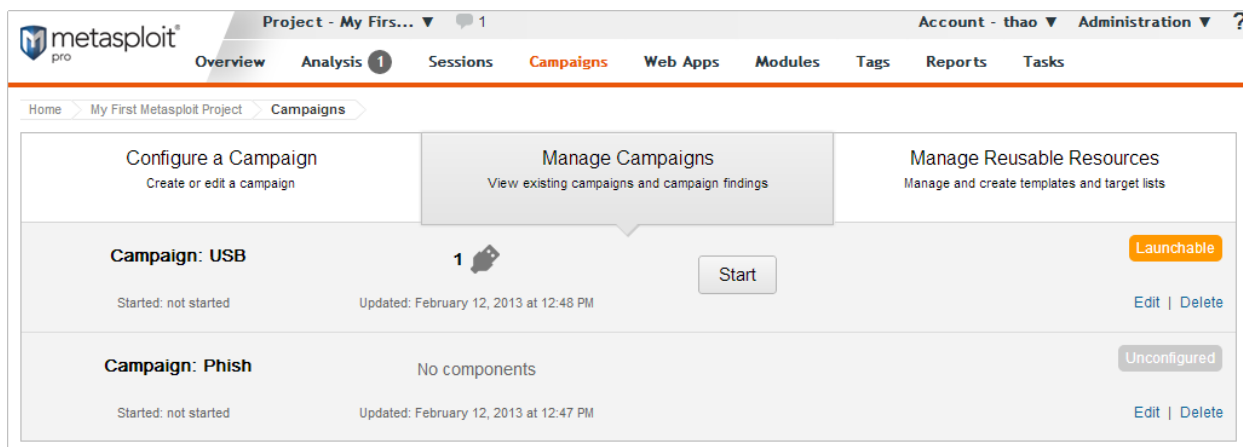
Запуск и работа кампании

1. В проекте выберите «Кампании/Campaigns» в меню задач.
2. Когда откроется панель «Управление кампаниями/Manage Campaigns», найдите кампанию, которую нужно запустить. Заметьте, состояние кампании должно быть «Готова к запуску/Launchable», что будет означать полную готовность всех компонентов к запуску.
3. Кликните на активную ссылку «Старт/Start».

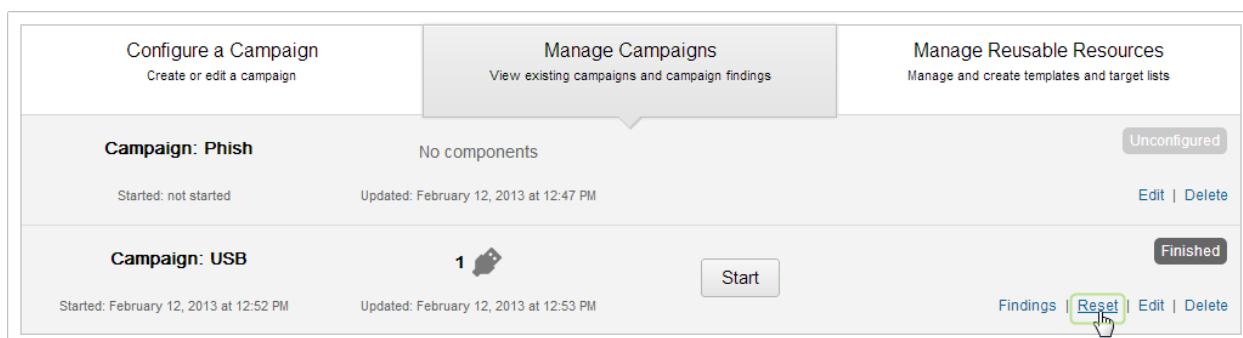
Очистка данных кампании

При сбросе кампании вы потеряете всю статистику и данные, собранные во время кампании. Сброс удаляет все данные из форм, статистику фишинговых атак, а также статистику отслеживания электронных писем.

1. В проекте выберите «Кампании/Campaigns» в меню задач.
2. Когда откроется панель «Управление кампаниями/Manage Campaigns», найдите кампанию, которую нужно сбросить.



3. Нажмите на активную ссылку «Сброс/Reset».



4. Когда появится окно подтверждения, кликните «ОК», чтобы подтвердить полный сброс данных кампании.

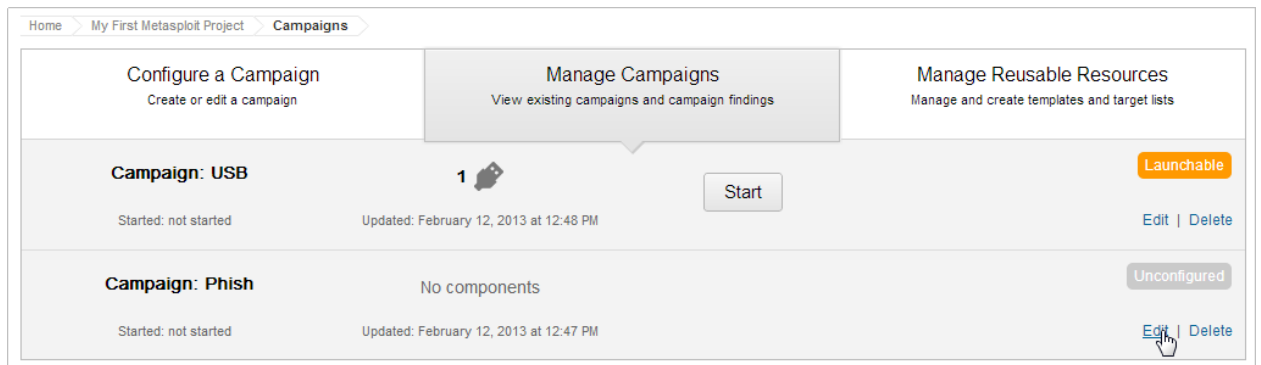
Просмотр результатов кампании

1. В проекте выберите «Кампании/Campaigns» в меню задач.
2. Когда откроется панель «Управление кампаниями/Manage Campaigns», найдите кампанию, результаты которой вам интересны.
3. Кликните на активную ссылку «Собранные данные/Findings». Появится окно с отображением всей статистики по кампании. Вы увидите общее количество целей, получивших электронные письма, количество открытых писем, визитов на фишинговых веб-страницах, а также заполненные онлайн формы.
4. Кликните на окошко со статистикой для получения информации касательно группы пользователей, имеющей отношение к данному типу статистики. К примеру, если вы хотите увидеть собранные данные по получателям писем, заполнившем форму, вы увидите имена и электронные адреса целей, заполнивших веб форму. Если вы кликните на их электронные адреса, то увидите дату заполнения.
5. Кликните кнопку «Закончить/Done», чтобы закрыть окно результатов.

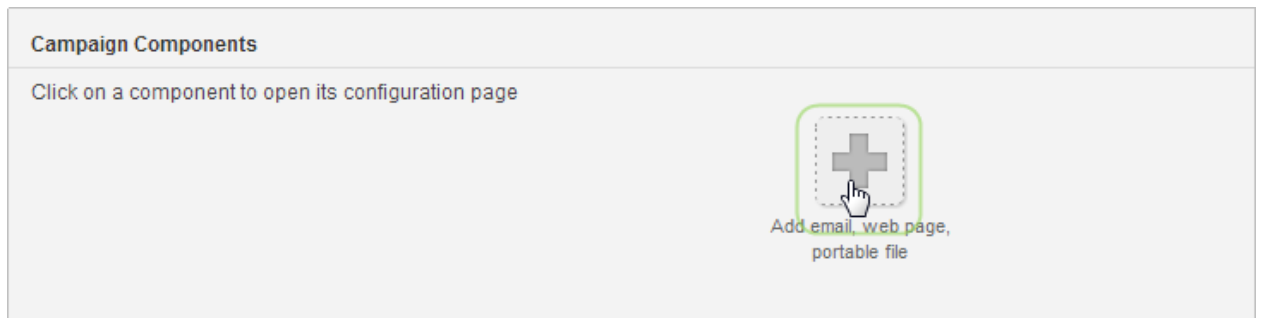
Добавление компонента кампании

1. В проекте выберите «Кампании/Campaigns» в меню задач.

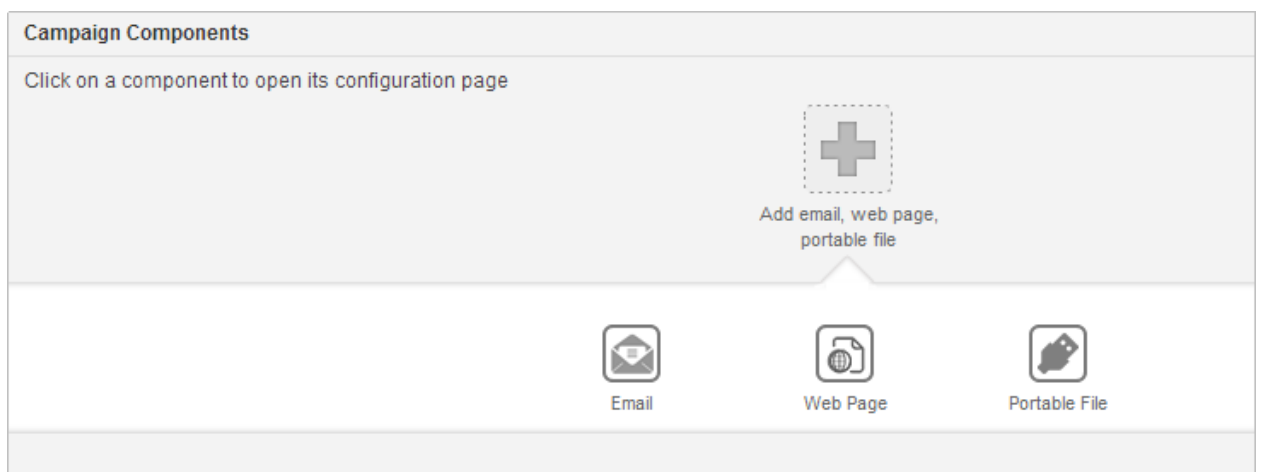
2. Когда откроется панель «Управление кампаниями/Manage Campaigns», найдите кампанию, которую надо отредактировать.



3. Кликните на активную ссылку «Редактировать/Edit». На странице конфигурации кампании, кликните соответствующую активную ссылку для добавления электронного письма, веб-страницы или портативного файла. Вы можете добавлять компоненты только в свои кампании с собственными настройками. Вы не сможете добавить компоненты в фишинговую кампанию по умолчанию.



4. Кликните на компонент, который вы хотите добавить. После добавления вы автоматически перейдете на страницу конфигурирования компонента. Следуйте инструкциям на экране для настройки компонента.



Удаление компонентов кампании

5. В проекте выберите «Кампании/Campaigns» в меню задач.
6. Когда откроется панель «Управление кампаниями/Manage Campaigns», найдите кампанию, которую нужно отредактировать.
7. Кликните на активную ссылку «Редактировать/Edit».
8. На странице конфигурации кампании, кликните соответствующую активную ссылку «Редактировать/Edit», расположенную под вкладкой программных компонентов. У каждой иконки есть небольшой красный крест. Это кнопка для удаления компонентов.
9. Нажмите кнопку «X», соответствующую ненужному компоненту.
10. Нажмите кнопку «Готово/Done» по завершении редактирования.

Остановка кампании

1. В проекте выберите «Кампании/Campaigns» в меню задач.
2. Когда откроется панель «Управление кампаниями/Manage Campaigns», найдите кампанию, которую нужно остановить.
3. Кликните на активную ссылку «Стоп/Stop».

Отправка электронного письма с уведомлением о начале кампании

До настройки уведомлений по почте вам следует проверить настройки SMTP вашего почтового сервера, они должны быть настроены под metasploit Pro. Зайдите в Administration > Global Settings и проверьте параметры SMTP.

1. В меню конфигурирования кампании найдите панель уведомлений.
2. Выберите «Уведомлять других до запуска кампании/Notify others before launching the campaign».
3. Когда появится окно настройки уведомлений, введите в поле «Кому/To» электронные адреса людей, которых нужно оповестить о начале кампании, через запятую. К примеру, вы можете ввести joe@rapid7.com, mary@rapid7.com, jon@rapid7.com.
4. В поле «Тема/Subject» введите тему отправляемого электронного письма. По умолчанию Metasploit Pro использует стандартные темы.
5. В поле «Сообщение/Message» вводится тело письма, которое будет отправлено по электронной почте. К примеру, вам может понадобиться отправить фразу типа «Объявляем о старте нашей программы проверки безопасности. За любыми деталями обращайтесь к Ивану Иванову».
6. После завершения редактирования нажмите кнопку «Сохранить/Save».

Загрузка инфицированного файла

1. В проекте выберите «Кампании/Campaigns» в меню задач.
2. Кликните на вкладку «Управлять ресурсами/Manage Reusable Resources».
3. Из открывшегося ниспадающего меню выберите «Инфицированные файлы/Malicious Files».
4. Кликните кнопку «Новый инфицированный файл/New Malicious File».
5. В поле «Имя/Name» ведите название импортируемого файла. Имя файла должно включать расширение. К примеру, если вы загружаете файл-приложение, то имя должно включать расширение .exe.

6. Кликните кнопку «Просмотреть/Browse», чтобы найти расположение импортируемого файла. После его нахождения кликните кнопку «Открыть/Open». Путь к файлу появится в соответствующем поле.
7. Кликните кнопку «Сохранить/Save».

Удаление кампании

1. В проекте выберите «Кампании/Campaigns» в меню задач.
2. Когда откроется панель «Управление кампаниями/Manage Campaigns», найдите кампанию, которую нужно удалить.
3. Нажмите кнопку «Удалить/Delete».
4. Подтвердите ваше решение в появившемся окне, кликните «ОК» для продолжения. Все списки целей и компоненты кампании будут удалены из проекта. Вы больше не сможете просмотреть, запустить или отредактировать удаленную кампанию.

Экспорт собранных во время кампании данных в файл CSV

1. В проекте выберите «Кампании/Campaigns» в меню задач.
2. Когда откроется панель «Управление кампаниями/Manage Campaigns», найдите кампанию, данные которой нужно экспортировать.
3. Нажмите кнопку «Собранные данные/Findings».
4. В окне статистики выберите данные для экспорта. К примеру, если вам нужно выгрузить список целей, открывших электронное письмо, кликните на число получателей, открывших полученное письмо в окне статистики. Появятся список целей и кнопка «Экспорт данных/Data Export».
5. Нажмите кнопку «Экспорт данных/Data Export».
6. В открывшемся окне выберите опцию «Сохранить файл/Save File» и кликните «ОК». Выбранные данные будут сохранены в файл в директории «Загрузки» вашей операционной системы.

Экспорт разосланных электронных писем кампании в файл CSV

1. В проекте выберите «Кампании/Campaigns» в меню задач.
2. Когда откроется панель «Управление кампаниями/Manage Campaigns», найдите кампанию, данные которой нужно экспортировать.
3. Нажмите кнопку «Собранные данные/Findings».
4. В окне статистики кликните на число отосланных писем. Появятся список целей и кнопка «Экспорт данных/Data Export».
5. Нажмите кнопку «Экспорт данных/Data Export».
6. В открывшемся окне выберите опцию «Сохранить файл/Save File» и кликните «ОК». Выбранные данные будут сохранены в файл в директории «Загрузки» вашей операционной системы.

Экспорт списка целей, открывших электронное письмо, в файл CSV

1. В проекте выберите «Кампании/Campaigns» в меню задач.
2. Когда откроется панель «Управление кампаниями/Manage Campaigns», найдите кампанию, данные которой нужно экспортировать.
3. Нажмите кнопку «Собранные данные/Findings».
4. В окне статистики кликните на число целей, открывших письмо. Появятся список целей и кнопка «Экспорт данных/Data Export».
5. Нажмите кнопку «Экспорт данных/Data Export».
6. В открывшемся окне выберите опцию «Сохранить файл/Save File» и кликните «ОК». Выбранные данные будут сохранены в файл в директории «Загрузки» вашей операционной системы.

Экспорт списка целей, кликнувших на ссылку, в файл CSV

1. В проекте выберите «Кампании/Campaigns» в меню задач.
2. Когда откроется панель «Управление кампаниями/Manage Campaigns», найдите кампанию, данные которой нужно экспортировать.
3. Нажмите кнопку «Собранные данные/Findings».
4. В окне статистики кликните на число целей, кликнувших ссылку. Появятся список целей и кнопка «Экспорт данных/Data Export».
5. Нажмите кнопку «Экспорт данных/Data Export».
6. В открывшемся окне выберите опцию «Сохранить файл/Save File» и кликните «ОК». Выбранные данные будут сохранены в файл в директории «Загрузки» вашей операционной системы.

Экспорт целей, заполнивших веб форму, в файл CSV

1. В проекте выберите «Кампании/Campaigns» в меню задач.
2. Когда откроется панель «Управление кампаниями/Manage Campaigns», найдите кампанию, данные которой нужно экспортировать.
3. Нажмите кнопку «Собранные данные/Findings».
4. В окне статистики кликните на число целей, заполнивших веб форму. Появятся список целей и кнопка «Экспорт данных/Data Export».
5. Нажмите кнопку «Экспорт данных/Data Export».
6. В открывшемся окне выберите опцию «Сохранить файл/Save File» и кликните «ОК». Выбранные данные будут сохранены в файл в директории «Загрузки» вашей операционной системы.

Наилучшие стратегии для атак при помощи социальной инженерии

Социальная инженерия – это метод атаки, заставляющий ничего не подозревающего человека передать злоумышленникам ценную информацию или совершить действие, создающее угрозу безопасности всей системы. Типичные методы атак при помощи социальной инженерии подразумевают какой-то определенный способ доставки ссылки или файла, но можно

использовать и другие механизмы. Нередко применяются телефонные звонки и даже личные визиты.

Социальная инженерия превратилась в очень опасный инструмент злоумышленника. Подобная динамика стала возможной из-за особенностей современных систем безопасности. Все больше организаций смещают фокус в разработке систем безопасности на самое слабое звено – своих сотрудников.

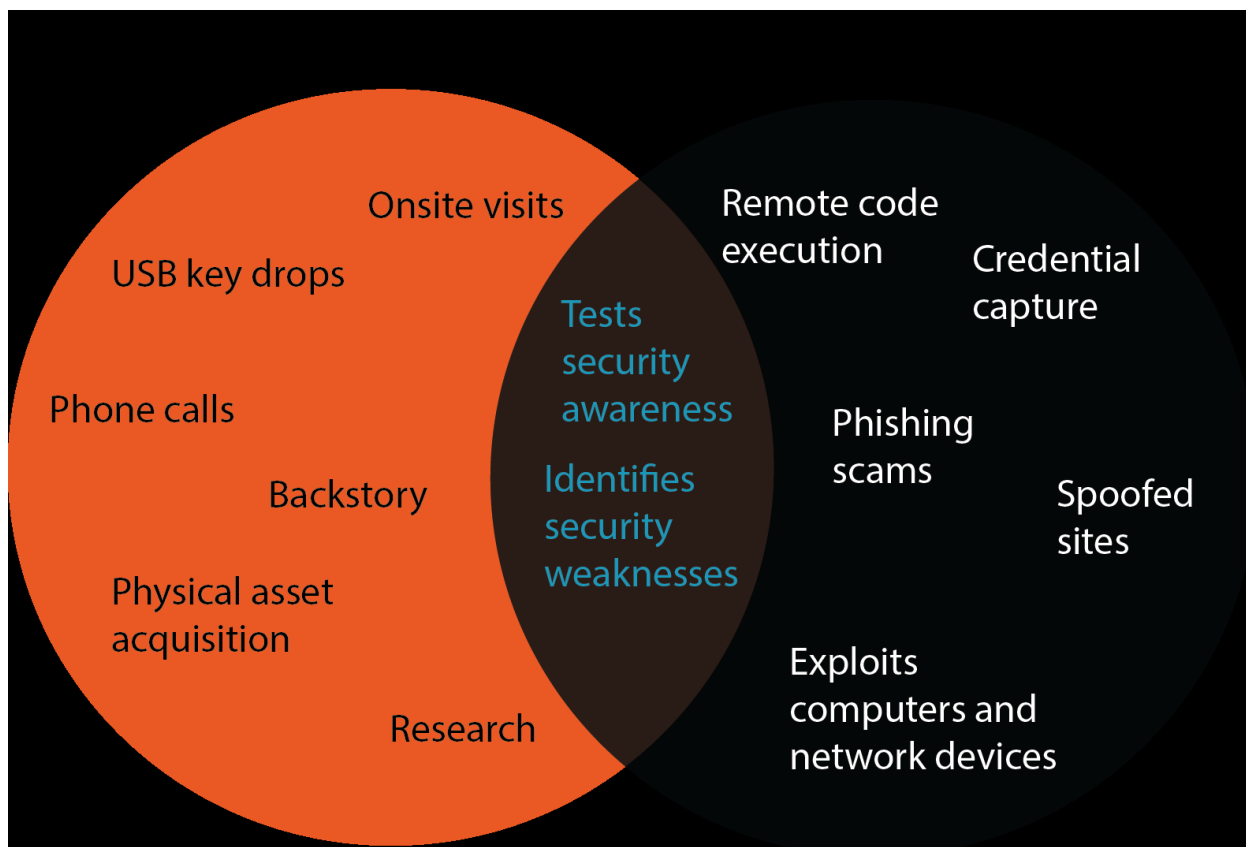
В ходе работы по тестированию систем безопасности той или иной организации вас могут попросить провести полноценное тестирование физической и IT-инфраструктур на предмет сопротивления атакам из области социальной инженерии.

До начала разработки конкретного плана необходимо провести серию встреч с руководством организации для идентификации основных целей и задач тестирования. Большинство организаций захотят измерить эффективность обучающих программ и выявить существующие слабости в используемых руководствах по безопасности и в самой IT-инфраструктуре.

После постановки четкой цели и достижения полного понимания задачи вы сможете построить план атак, позволяющий сконцентрировать внимание на определенных аспектах системы безопасности.

Принято различать две основные формы тестирования на возможность проникновения при помощи методов социальной инженерии: цифровая и физическая. Цифровое тестирование сводится к проверке IT-инфраструктуры и степени ответственности сотрудников и членов организации по отношению к рекомендациям в области безопасности. Физические тесты заключаются в поведенческом анализе и оценке оборудования и помещений организации в отношении обеспечения безопасности.

В зависимости от задач тестирования, можно использовать только одну форму или обе.

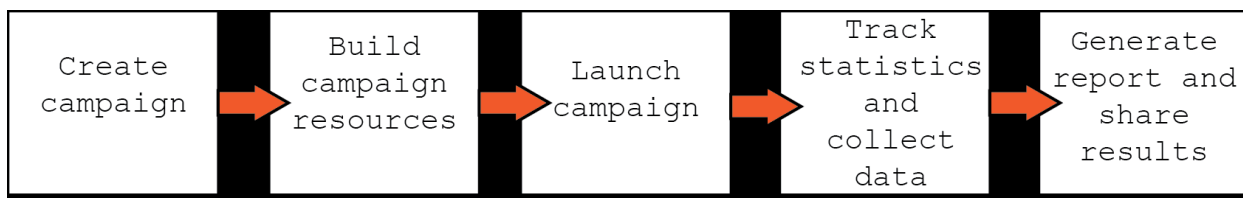


К примеру, если организация хочет измерить ответственность сотрудников и то, как они следуют рекомендациям по безопасности, то может потребоваться разработка долгосрочного масштабного плана тестирования с проработкой фундамента для использования социальной инженерии. После выстраивания фундаментальной стратегии можно начинать применение приемов социальной инженерии, включая подброс USB-носителей, фишинговые тактики и другие приемы для полноценного разнонаправленного тестирования всего периметра цифровой безопасности.

Социальная инженерия вместе с Metasploit Pro

Основной функционал Metasploit Pro в отношении социальной инженерии сфокусирован на проведении атак с вовлечением компьютера пользователя. Большинство таких атак связаны с использованием какого-либо механизма доставки: электронного письма, рассылки ссылок в мессенджерах, передачи инфицированного файла на физическом носителе. При помощи Metasploit Pro можно создавать и отправлять тысячи электронных писем и файлов, обычно ассоциируемых со взломами и кражей информации.

В Metasploit Pro атаки проводятся при помощи специальных кампаний. Это рабочие пространства, где можно оперативно управлять различными типами атак. В наличии инструменты для быстрого создания всех необходимых для атаки ресурсов – электронных писем, шаблонов веб страниц, шаблонов писем, инфицированных файлов и списков целей для атак.



Чтобы понять, как конкретно строится работа с Metasploit Pro, нужно осветить социальную инженерию в целом, ее основные методики и особенности. Уделим внимание и практическим советам по организации наиболее эффективных программ тестирования систем безопасности.

Фишинг

Если вы внимательно изучите папку «СПАМ» в почтовом ящике, то найдете огромное количество фишинговых электронных писем, содержание которых вызывает доверие. Они похожи на письма от уважаемых банков, «друзей» из Нигерии, да и вообще от кого угодно, с кем вы могли поделиться какой-либо конфиденциальной информацией.

Эти электронные письма выглядят идентично настоящим рассылкам от уважаемых компаний. Задачей фейковых писем является убедить пользователя в том, что они настоящие. Они даже могут иметь хорошо подобранный обратный почтовый адрес, красивое оформление, логотипы и отлично написанный контент.



Конечно и единственной задачей этого письма является вынуждение получателя кликнуть на ссылку в письме. Эта ссылка приведет пользователя на фальшивый сайт, где будут созданы все условия для незаметной кражи информации.

Metasploit Pro позволяет вам заняться превентивной защитой. Вы сможете создавать и отправлять фишинговые электронные письма за несколько минут. Для этого внедрены специальные компоненты, включая шаблоны писем для отправки, шаблоны веб страниц, возможность настроить SMTP сервер и подготовить обширный список целей для атак.

Теперь вы знаете, как Metasploit Pro может вам помочь. Пройдемся по нескольким прикладным методами повышения эффективности фишинга в рамках тестирования систем безопасности.

Фишинг. Совет №1. Клонировать, клонируйте и клонируйте

Одним из мощнейших инструментов среди функционала для социальной инженерии является инструмент для создания клонов реальных веб страниц. Для создания хорошего клона достаточно просто предоставить программе ссылку на ресурс, а все остальное будет сделано за вас. Metasploit Pro делает копию HTML-кода странички и импортирует ее в проект. После импорта данных вы сможете его отредактировать для еще большей аутентичности.

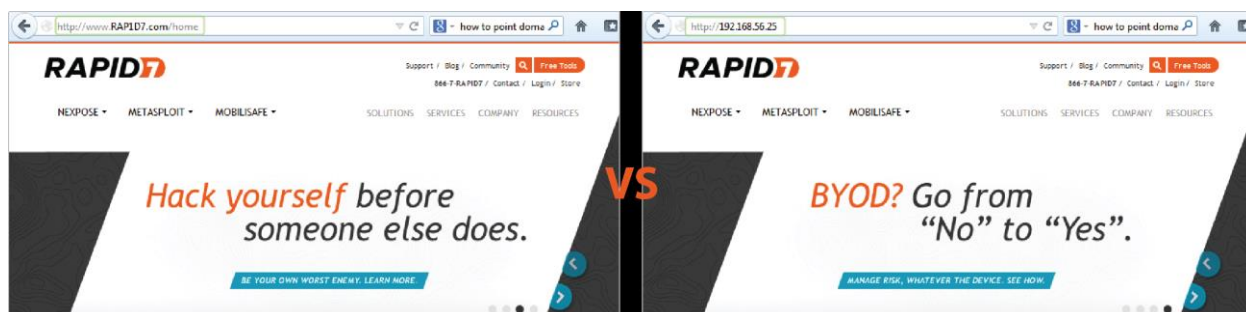
Главная задача этого сайта заставить пользователя поверить в то, что он настоящий. Очень важно, чтобы клонированный сайт был абсолютной внешней репликой реального. Именно поэтому для эффективного фишинга нужно клонировать страницы, а не писать их «с нуля». После копирования сайта с интернета, все необходимые для работы клона ресурсы будут размещены на сервере-клоне, что позволяет быстро редактировать внешний вид веб страницы и запустить его в кратчайшие сроки.



Фишинг. Совет №2. Используйте реалистичный домен

Одним из самых простых способов определить мошенника является быстрый взгляд, кинутый на адресную строку браузера. Очень важно использовать доменное имя близкое по внешнему виду к реальному. К примеру, фальшивый домен для Rapid7 будет выглядеть как RAP1D7 или RAPID7. Если сравнить между собой адреса «http://196.184.132.24/home» и «http://www.RAPID7.com/home», то второй выглядит намного безопаснее для посещения.

Большинство людей смогут быстро отличить фальшивый URL от реального. Тестирование с применением сайтов с качественно подобранными доменами позволяет оценить способность цели обращать внимание на важные детали и выявлять подозрительные ссылки.



Для того, чтобы Metasploit Pro смог использовать определенное доменное имя, нужно его купить. После покупки вы сможете использовать адрес при работе с установленной у вас копией Metasploit.

Фишинг. Совет №3. Бейте по малым аудиториям

Не сводите свою IT команду с ума. Используйте небольшие списки целей для большинства своих тестов. С небольшим списком целей намного проще избежать подозрений и проблем с персоналом.

Ограничивая количество целей для атак, вы можете контролировать размеры и демографию контрольных групп. К примеру, вы можете создать отдельный список целей для своей IT команды, у которой могут быть свои цели и задачи, отличные от общеорганизационных.

При необходимости вы можете проводить и крупномасштабные тесты. В этом случае симулируется реальная атака с вовлечением большого количества целей. Такие масштабные мероприятия помогают определить текущее состояние систем безопасности и идентифицировать проблемные зоны в IT инфраструктуре.

Resource: Target Lists			Delete New Target List
☐	Name	# Targets	Created
☐	Dev_Team	1	February 11, 2013 at 7:52 AM
☐	Exec_Team	1	February 11, 2013 at 7:51 AM
☐	IT_Team	1	February 11, 2013 at 7:51 AM
☐	HR_Team	1	February 11, 2013 at 7:50 AM
Showing 1 to 4 of 4 entries			
First Previous 1 Next Last			

Фишинг. Совет №4. Используйте SMTP серверы для рассылок

Одна из самых часто возникающих проблем при проведении тестирования в области социальной инженерии заключается в невозможность рассылать письма посредством локального сервера. Большинство почтовых серверов проводят обратную проверку DNS адресов для того, чтоб удостовериться, что IP адрес хостинга Metasploit Pro соответствует доменному имени электронного адреса, который пытаетесь использовать для рассылок. Если при проверке DNS обнаруживается проблема, то письмо не принимается.

Из-за высокой степени защиты почтовых серверов от спама и подозрительных рассылок эффективно разослать большое количество фишинговых писем не получится. Чтобы обойти эту проблему, используйте SMTP сервисы для рассылок. Примерами можно считать Sendgrid и JangoSMTP или даже Mandrill. Публично доступные сервисы вроде Gmail, Hotmail, Mail.ru, Yandex или Yahoo использовать нельзя, там очень высокие требования к безопасности и при малейшем намеке на мошенничество или фишинг адрес попадает в черный список.

Вне зависимости от того, какого провайдера услуг вы выберете, нужно всегда проверять с каким процентом успешности доставляются письма. Следите за тем, чтобы количество попаданий в spam фильтры стремилось к нулю.

Фишинг. Совет №5. Собирайте ценную информацию

Если вы хотите использовать фишинг для тестирования и последующего усиления безопасности в компании, используйте фальшивые веб страницы для реального сбора персональной информации. К сожалению, ничто не провоцирует людей быть осторожнее кроме личного опыта жертвы кражи персональных данных.

Фишинговая кампания уже снабжена всем необходимым для оперативной рассылки и редиректа пользователей на фальшивый сайт. Сбор данных ведется в реальном времени, а потому вы сможете

очень быстро идентифицировать людей, которые вводят свои личные данные. Вы также увидите, какую именно информацию они вводят.

Архитектура Metasploit Pro не позволяет нам скрыть персональные данные от администратора. Данные из форм не включаются в отчет по умолчанию, но вы можете использовать опции настроек при создании своей собственной кампании и выбрать, какая информация будет включена в отчеты. Часть данных необходимо скрывать. Помните, что номера кредитных карт и пароли разглашать нельзя ни в коем случае.

Фишинг. Совет №6. Обязательно имитируйте стиль и текст ссылки при наведении курсора

Самый простой способ быстро разоблачить мошенника – просто навести мышку на ссылку и увидеть реальный URL. Для того, чтобы еще больше запутать цели, меняйте текст ссылки, появляющийся при наведении на нее мыши, на заслуживающий доверия. При помощи стилизации можно ввести любой текст.

К примеру, если ваша копия Metasploit Pro установлена на веб сервере, который не ведет к DNS серверу, то адрес будет выглядеть плохо. Что-то в стиле «<http://1.2.3.4/blue123>» трудно принять за заслуживающий доверия. Просто заменить всплывающий текст на URL «<http://www.rapid7.com>» достаточно легко, а выглядеть все начинает намного солиднее, как будто бы он ведет на реальный сайт.

USB-приманка

В любом офисе можно найти огромное количество флэшек, разбросанных по всему помещению. USB-накопители лежат рядом с копиями, кофе-машинками, просто бесхозно валяются на столах и шкафах. Можно подумать, что хозяин просто забыл или не там положил свой USB-накопитель. Если вы найдете такую флэшку, то первым делом вставьте ее в компьютер и посмотрите, что на ней есть.

При просмотре содержимого флэшки вы можете увидеть файл с названием, которое может вас заинтересовать. Вам будет интересно открыть файл с названием «Резюме_Сергей.pdf» потому, что он может содержать важную персональную информацию о владельце флэшки. К сожалению, такие файлы не так безобидны, как кажутся. Открытие такого файла может заразить компьютер вредоносной программой и открыть к нему доступ злоумышленникам.

Использование USB-накопителя в качестве приманки полностью основано на человеческом любопытстве. Большинство схем подброса файлов таким образом требуют от злоумышленника обязательного наличия доступа к офисному помещению. В некоторых случаях для проникновения на территорию организации люди переодеваются в технических работников или врут о том, что них там работают друзья или родственники.

Во время тестирования безопасности в области социальной инженерии необходимо использовать метод USB-приманки для повышения бдительности и усиления дисциплины в отношении рекомендаций по безопасности. Все это существенно укрепляет защиту организации.

Кроме фишинга Metasploit Pro позволяет вам создавать инфицированные файлы. Это может быть файл-приложение или же просто зараженный файл, который легко закачать на флэшку. Можно создать файл со стандартным расширением и привязать к нему эксплойт. Примером является использование PDF документа в качестве контейнера для эксплойта Adobe Cooltype. Для

проведения тестирования достаточно просто загрузить файл на USB-носитель и оставить его там, где чаще всего проводят время сотрудники.

Это общее описание методик подброса зараженных файлов при помощи обыкновенной флешки. Теперь несколько советов по тому, как сделать USB-приманку заметнее.

USB-приманка. Совет №1. Аккуратно планируйте атаку

Как и в случае с другими тестами на проникновение, исследование обстановки и планирование играют ключевую роль. Для успешного подброса вам придется самостоятельно проникать на незнакомую территорию и физически подбрасывать файл, а этом сильно отличается от фишинга.

Двумя главными задачами можно считать исследование локации и определить потенциально уязвимые системы.

Чтобы подброс USB-ключа был успешным, следует найти зону с наибольшей проходимостью. Такие локации обеспечивают большую вероятность того, что кто-то подберет USB-накопитель и использует его на своем компьютере. Иногда, при отсутствии доступа к определенному объекту, требуется придумать себе «легенду», чтобы проникнуть на территорию. Можно притвориться работником технической службы или курьером, а это потребует необходимости использовать соответствующую униформу.

На этапе предварительного исследования территории необходимо спросить у самого себя:

«Как я попаду внутрь?»

«Какую легенду мне лучше всего использовать?»

«Где находятся места с наибольшей проходимостью?»

«Кто может попытаться меня остановить?»

Поиск ответов на эти вопросы поможет вам подготовиться к подбросу USB-флешку по максимуму.

Раз вы не можете быть уверенными в том, кто воспользуется подброшенным устройством, вы не сможете знать наперед, подойдет ли получения доступа тот или иной эксплойт. Важно собрать побольше информации о том, какие системы и программы используются в организации для подбора самых эффективных эксплойтов. Если вам известно, что на большинстве компьютеров установлена ОС Windows, вы можете использовать эксплойты, разработанные специально для этой системы. Для организаций, широко применяющих Adobe Reader, нужно искать другой подход – инфицированные PDF файлы.

С достаточно детальным исследованием вы сможете разработать эффективную стратегию нападения и собрать много полезной информации для организации.

USB-приманка. Совет №2. Называйте файлы интересно

Когда кто-то находит USB-накопитель, первым желанием нашедшего будет просмотреть содержимое. Поэтому вам следует использовать интересные названия для файлов. Можно использовать простой прием: назвать файл «Зарплата.exe» или «На увольнение.pdf». Такие названия заставят любопытного пользователя открыть их.

Инфицированные вложения

Так называют зараженные файлы или приложения, которые вкладываются в электронное письмо, отправляемое цели. Само письмо составляется в виде сообщения от доверенного источника с вложением, которое должно быть немедленно скачано.

Некоторые по-настоящему эффективные атаки начинаются с безобидного действия – открытия вложения в письме. Вложенный файл содержит эксплойты, доставляющие инфицированные данные к системе цели, что делает эту систему уязвимой к вирусам, шпионскому ПО, троянам и другим вредоносным программам. В некоторых случаях атака инициирует цепочку событий, ведущую к инфицированию всей сети.

Сам получатель может даже не заметить, что вложение может быть опасным, ведь оно приходит от знакомого источника. Как и в случае с фишинговыми атаками, злоумышленник манипулирует восприятием получателя, старается сделать так, чтобы письмо выглядело аутентично, а само вложение – заслуживающим доверия. Персонализированные корпоративные электронные письма с финансовыми отчетами или выписками по социальному страхованию могут сбить с толку получателя и заставить его скачать файлы. Такие письма работают лучше, чем просто торговые предложения и реклама.

При тестировании систем защиты нужно оценить потенциальные для организации риски, связанные с атаками при помощи электронной почты, а затем выработать оптимальные решения для минимизации этих рисков. Важно обеспечить сотрудников необходимыми навыками, необходимыми для снижения риска, который они сами создают для своей компании. Одновременно, следует стараться идентифицировать наиболее очевидные критические уязвимости, требующие к себе немедленного внимания со стороны организации.

Теперь вы знаете о том, что такое инфицированные вложения. Пройдемся по прикладным советам, которые помогут вам создавать такие вложения и правильно составлять письма.

Инфицированные вложения. Совет №1. Создавайте убедительные письма

Чтобы воспользоваться доверием и любопытством цели, нужно создать электронное письмо, которое будет выглядеть убедительно, но также содержать информацию, способную заинтересовать цель.

Любое электронное письмо должно содержать логотип, стиль текста и цвета организации, от которой отправляются письма. Желательно использовать актуальные письма, их заглавия, футеры и подписи в качестве ориентира. Такие мелочи заставляют пользователя верить в то, что письмо пришло от верифицированного знакомого источника.

Чтобы убедить цель открыть вложение, вам нужно сделать интересным и любопытным, чтобы цели хотелось его открыть. Чаще всего люди заинтересованы в информации, затрагивающей их напрямую. К примеру, электронные письма о бонусах, с вложениями типа «2018_бонусы_сотрудникам.pdf» скорее всего получит намного больше прямых просмотров, чем письма о новых корпоративных буклетах и инструкциях.

Инфицированные вложения. Совет №2. Почаще применяйте файлы с вложенными эксплойтами

В зависимости от собранной о системах и ПО на компьютерах выбранных целей нужно правильно подбирать эксплойты и доставлять в файлах со стандартными расширениями. К примеру, большинство компьютеров в крупных организациях используют Microsoft Windows или Adobe

Reader. Когда вы выбираете расширение для файла с вложенным эксплойтом, учитывайте вероятность того, что у цели будет необходимое программное обеспечение для открытия файла.

Инфицированные вложения. Совет №3. Архивируйте вложенные файлы

Большинство почтовых сервисов не будут доставлять письма с вложенными файлами-приложениями. Если вам нужно использовать такой формат файла, используйте ZIP-архивирование. Это снижает вероятность того, что вложение будет идентифицировано как вредоносное.

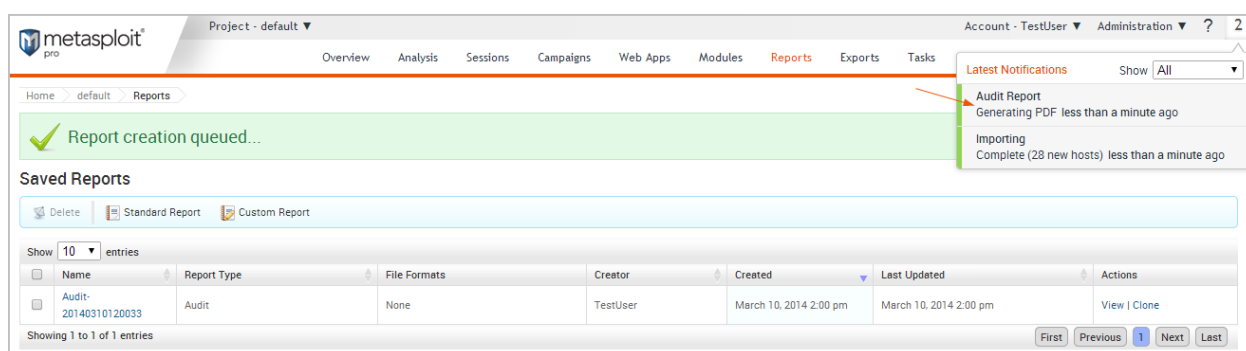
Отчеты

Отчет представляет все данные проекта в простом для понимания формате. В нем все собранные данные группируются в релевантных секциях, а статистика отображается в графиках. Это позволяет быстро суммировать результаты работы. Отчеты чрезвычайно полезно в тех случаях, когда нужно оперативно отправить данные людям, у которых нет Metasploit Pro или для получения полного представления о ходе тестирования.

Все задачи, относящиеся к отчетам, осуществляются в разделе отчетов в веб-интерфейсе. Туда входят следующие функции: создание, скачивание, отправление по электронной почте и удаление отчетов.

Сигналы Центра Оповещений при работе с отчетами

Когда вы создаете отчет, Центр оповещений обязательно предупредит вас о том, когда процесс начинается, завершается или останавливается из-за ошибки. Центр оповещений представлен в виде иконки в верхнем правом углу общей панели инструментов и отображает общее количество непрочитанных оповещений. Вы можете кликнуть на иконку для отображения списка предупреждений.



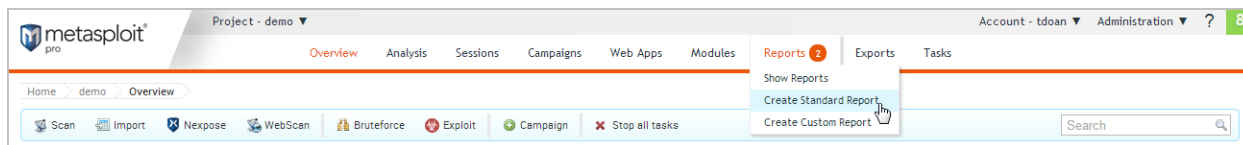
Следующие сигналы Центра оповещений относятся к отчетам:

- Отчет начат/Report Started. Этот сигнал означает, что процесс составления отчета начат.
- Отчет завершен/Report Finished. Этот сигнал означает, что отчет был создан без ошибок и готов для просмотра и скачивания. вы можете кликнуть на оповещение для открытия отчета. Когда вы открываете отчете из Центра оповещений, отображается общий вид отчета и доступные форматы. Вы можете кликнуть на иконку любого формата, чтобы просмотреть в нем созданный отчет.
- Проблема с отчетом/Problem with report. Этот сигнал означает, что с произошла какая-то проблем при создании отчета и он не мог быть завершен в штатном порядке. Вам нужно

будет просмотреть журнал отчетов для идентификации проблемы. Для получения дополнительной информации о журналах отчетов, читайте раздел Журналы Отчетов.

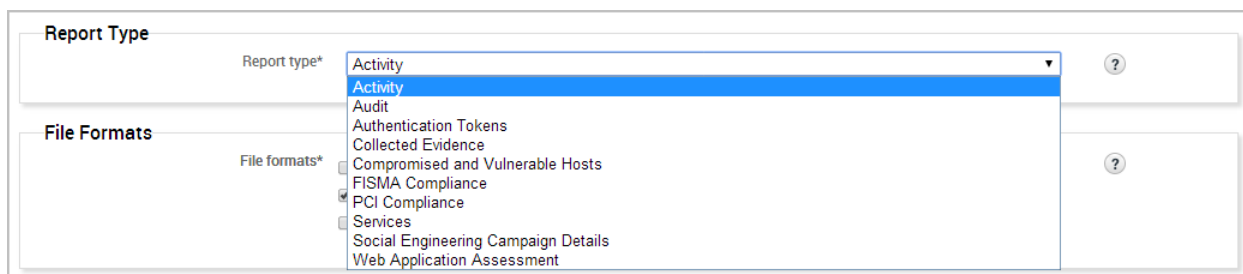
Создание стандартного отчета

1. Откройте проект, для которого нужно создать отчет.
2. Откройте Reports > Create Standard Report во вкладке «Проекты/Projects».



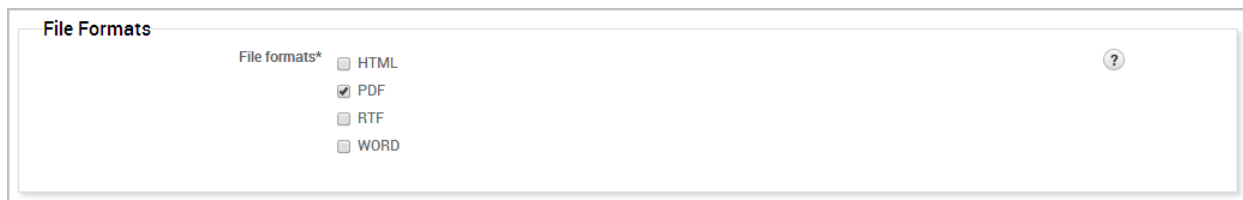
Страница отчетов будет открыта с выбором опции «Создание стандартного отчет/Generate Standard Report» по умолчанию.

3. Кликните «Тип отчета/Report type» для открытия ниспадающего меню и выберите нужный вам тип отчета.



Для получения дополнительной информации о типах отчетов, читайте раздел Типы отчетов Metasploit.

4. Выберите файловые форматы, в которых будет представлен отчет.



Вы можете создавать отчет в нескольких форматах одновременно. Большинство отчетов может быть создано в форматах PDF, Word, RTF или HTML, но отчет типа «Оценка веб приложения/Web Application Assessment» не может быть выгружено в формате Word.

5. Введите название отчета в поле «Название отчета/Report Name». (Необязательно)



Если вы не укажете имя, то Metasploit Pro воспользуется типом отчета и время создания для формирования названия. К примеру, отчет по аудиту будет назван Audit-20180106140552.

6. Используйте поле «Включенные адреса/Included addresses», чтобы указать точный перечень хостов, для которых вы хотите создать отчет. (Необязательно)

К примеру, вы можете ввести в данное поле перечень адресов, которые вам не нужны отчеты. Все остальные адреса не будут включены в отчет.

7. Используйте поле «Исключенные адреса/Excluded addresses», чтобы точно указать хосты, которые вы хотите исключить из отчета.

К примеру, вы можете исключить только определенные хосты из отчета. Укажите их в данном поле. Все остальные хосты будут включены в отчет.

8. Кликните на «Кампании/Campaigns». В выпадающем меню выберите кампании, которые вы хотите включить в отчет (только для отчетов по социальной инженерии). В этом случае отчет будет отображать кампании из вашего проекта.
9. Кликните на «Cover Logo» и выберите логотип, которые вы хотите использовать для заглавной страницы отчета.



Если вы не загружали никаких лого в проект, то нужно загрузить логотип, которые вы хотите использовать, в раздел «Custom Report Collateral» в проекте. Для получения дополнительной информации по загрузке логотипов, читайте раздел [«Пользовательские Лого/Custom Logo»](#).

10. Выберите секции отчета, которые вы хотите включить в отчет.
1. Доступные для выбора секции отчета будут меняться в зависимости от типа отчета. Для получения дополнительной информации о секциях отчета для каждого проекта читайте раздел «Разбираемся в содержимом отчета/Understanding Report Content» на странице 1.
11. Включайте и выключайте опции, чтобы выбрать нужные данные для составления отчета.

Форма создания отчета отобразит все опции, доступные для текущего отчета. Следующие опции могут быть доступны для выбора:

- Скрыть обнаруженные пароли. Из отчета удаляются все личные данные, включая пароли открытым тестом, хэши и ключи SSH. Отчет отображает имя пользователя и пустое поле для пароля.
 - Включить детали сессии. Показывает детали для каждой сессии, открытой Metasploit Pro, включая тип сессии и модуль атаки, использованный для ее открытия.
 - Включить графики. Дополняет отчеты круговыми диаграммами и другими видами визуализации данных для сопровождения статистических данных в проекте.
 - Включить HTML-код для веб страниц (в дополнение к предпросмотру изображений). Включает в отчет оригинальный код в виде обычного текста, а также изображение с предпросмотром странички. (Только для отчетов по социальной инженерии).
12. Введите адреса электронной почты, на которые нужно отправить отчет после создания. (Необязательно).

Используйте точку или точку с запятой для написания нескольких адресов подряд.

Чтобы отправить отчет по электронной почте, в общих настройках должен быть указан активный почтовый сервер.

Для получения дополнительной информации по настройке почтового сервера, читайте раздел «Ввод настроек SMTP/Defining SMTP Settings».

13. Создание отчета.

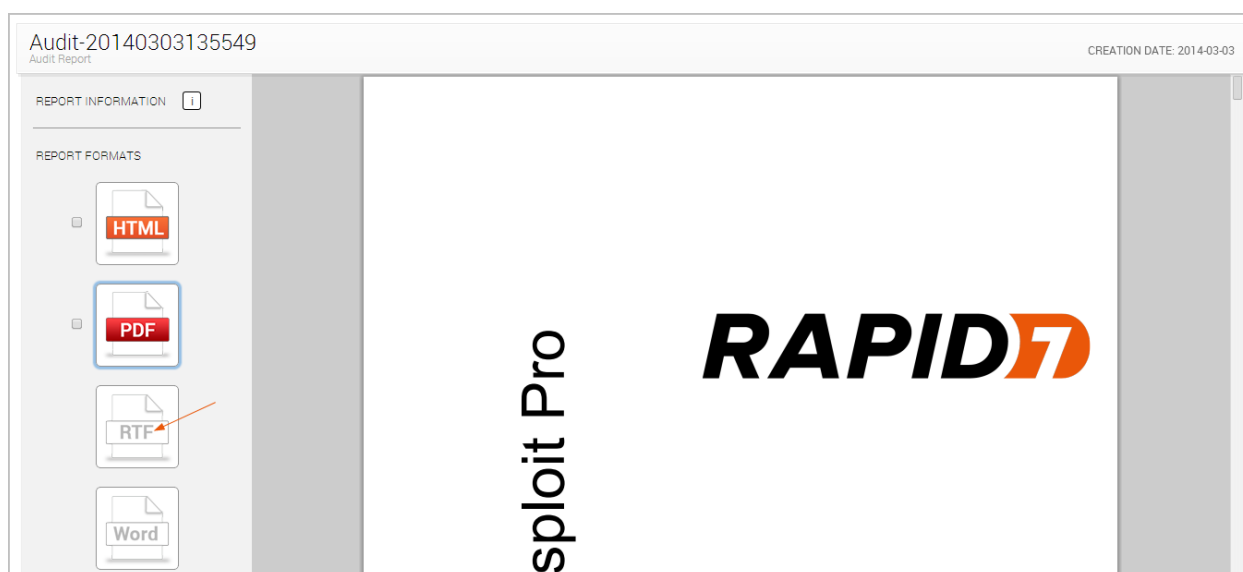
Когда процесс создания отчета будет запущен, веб интерфейс перенаправит вас на вкладку «Просмотр отчетов/View Reports». После этого вы сможете свободно переходить на другие вкладки Metasploit Pro. Центр оповещений отправит сигнал, когда процесс создания будет завершен.

По завершении создания вы можете кликнуть на иконку Центра оповещений, чтобы просмотреть сообщение или перейти в Reports > Show Reports во вкладке управления проектом для перехода в раздел отчетов.

Если по ходу создания отчета произойдет ошибка, вы сможете просмотреть журнал отчетов для идентификации проблемы. Для получения дополнительной информации о журналах отчетов, читайте раздел Журналы Отчетов.

Создание отчета в нескольких форматах

1. Откройте проект, содержащий отчет, который нужен вам в нескольких форматах.
2. Выберите Reports > Show Reports во вкладке управления проектом. Появится страница управления отчетами.
3. Найдите отчет, который нужен вам в нескольких форматах.
Нужная строка содержит мета-данные и форматы, доступные для данного отчета.
4. Кликните имя проекта, чтобы открыть его.
Будет открыта форма просмотра. Все доступные форматы будут отображены в боковой панели. Форматы с цветной иконкой и стоящей рядом галочкой уже были сгенерированы. Серые иконки означают, что форматы еще не использовались.
5. Кликните на интересующий вас формат файла. Можно создавать не больше 1 типа файла за раз.



Когда процесс создания отчета начнется, иконка формата будет заменена на индикатор прогресса. Иконка появится опять, когда отчет будет готов для просмотра и скачивания.

Теперь вы можете перейти в любой другой раздел Metasploit Pro при желании. Центр оповещений сообщит вам о завершении создания отчета.

Когда процесс будет завершен, вы можете кликнуть на иконку Центра оповещений для просмотра последних сообщений или перейти в Reports > Show Reports во вкладке управления проектом, чтобы попасть в раздел отчетов.

Если по ходу создания отчета произойдет ошибка, вы сможете просмотреть журнал отчетов для идентификации проблемы. Для получения дополнительной информации о журналах отчетов, читайте раздел Журналы Отчетов.

Создание отчетов Мета-модулей

Мета-модуль оснащен удобным интерфейсом, который позволяет быстро освоить проведение отдельных тестов на проникновение. Каждый мета-модуль берет на себя только главный функционал модуля (например, тестирование паролей), но позволяет вам быстро настроить и запустить модуль в кратчайшие сроки. Каждый мета-модуль включает в себя специализированный отчет с данными, релевантными к запуску и работе этого конкретного мета-модуля.

Отчеты мета-модулей создаются самим модулем по ходу его работы. После того, как мета-модуль создает отчет, вы можете просмотреть его в Разделе отчетов/Reports area. Для получения дополнительной информации об отчетах мета-модулей, читайте раздел Отчеты мета-модулей.

Known Credentials Intrusion

Uses known credentials to compromise hosts across the entire network. You can run this MetaModule to reuse credentials that you obtained from bruteforce attacks, phishing attacks, or exploited hosts.

Scope*

Payload

☒ Generate Report

Report is **enabled** ☐ HTML ☒ PDF ☐ RTF

Name* AuthMetaModule-20140311090337 ?

Sections ?

- ☒ Cover Page
- ☒ Project Summary
- ☒ Findings Summary
- ☒ Authenticated Services and Hosts Summary Charts
- ☒ Authenticated Services and Hosts Details
- ☒ Appendix: Report Options Selected

Options

- ☐ Mask discovered credentials
- ☒ Include charts

Excluded addresses ?

Email Report ?

Cancel Launch

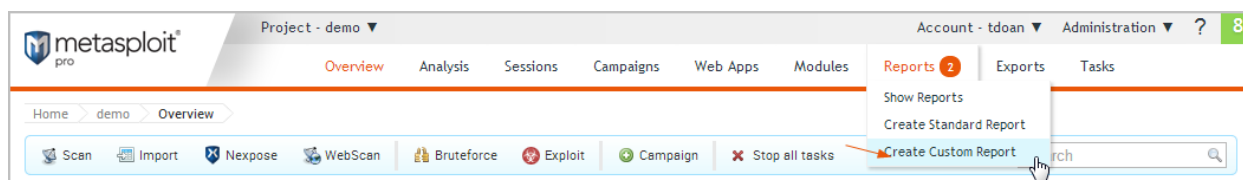
Создание пользовательского отчета

Пользовательский отчет создается при помощи загруженного пользователем шаблона отчетов JasperReports. Шаблон определяет разметку отчета и включаемые в него секции. Вы можете создать шаблон отчета с нуля при помощи инструментов типа iReport. Для получения дополнительной информации о своих отчетах, читайте раздел Пользовательские отчеты.

До начала создания своего отчета нужно загрузить шаблон, который вы хотите использовать, в раздел «Custom Report Collateral» в проекте. Если проект не содержит никаких загруженных шаблонов, форма предупредит вас об отсутствии пользовательских шаблонов. Необходимо загрузить подходящий шаблон JRXML для продолжения. Для дополнительной информации о загрузке пользовательских шаблонов, читайте раздел Загрузка шаблонов.

Чтобы создать пользовательский отчет:

1. Откройте проект, данные которого войдут в отчет.
2. Перейдите в Reports > Create Custom Report во вкладке управления проектом. Появится форма «Новый пользовательский отчет/New Custom Report».



3. Выберите шаблон, по которому будет создан отчет.
4. Выберите необходимые файловые форматы отчетов.

 The screenshot shows a form titled 'File Formats'. It contains a section 'File formats*' with four checkboxes: HTML, PDF (which is checked), RTF, and WORD. There is a help icon (?) to the right of the checkboxes.

Вы можете выбрать несколько форматов. Все они будут созданы одновременно.

5. Введите название отчета в поле «Название отчета/Report Name». (Необязательно)

 The screenshot shows a form with a label 'Name' and an input field. The input field contains the text 'Custom-20140310125739'. There is a help icon (?) to the right of the input field.

Если вы не укажете имя, то Metasploit Pro воспользуется типом отчета и время создания для формирования названия. К примеру, отчет может быть назван Custom-20180106140552.

6. Используйте поле «Включенные адреса/Included addresses», чтобы указать точный перечень хостов, для которых вы хотите создать отчет. (Необязательно)
К примеру, вы можете ввести в данное поле перечень адресов, которые вам не нужны отчеты. Все остальные адреса не будут включены в отчет.
7. Используйте поле «Исключенные адреса/Excluded addresses», чтобы точно указать хосты, которые вы хотите исключить из отчета. (Необязательно)
К примеру, вы можете исключить только определенные хосты из отчета. Укажите их в данном поле. Все остальные хосты будут включены в отчет.
8. Кликните на «Cover Logo» и выберите логотип, которые вы хотите использовать для заглавной страницы отчета.



Если вы не выберете определенный логотип, будет использоваться лого Rapid7 по умолчанию.

9. Введите адреса электронной почты, на которые нужно отправить отчет после создания. (Необязательно).

Используйте точку или точку с запятой для написания нескольких адресов подряд. Чтобы отправить отчет по электронной почте, в общих настройках должен быть указан активный почтовый сервер. Для получения дополнительной информации по настройке почтового сервера, читайте раздел «Ввод настроек SMTP/Defining SMTP Settings» для почтового сервера.

10. Создайте отчет.

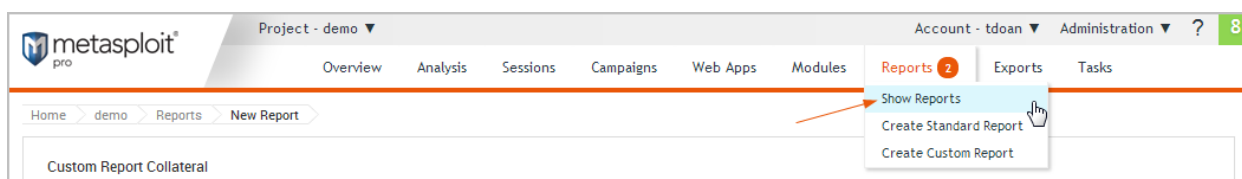
Когда процесс создания отчета будет запущен, веб интерфейс перенаправит вас на вкладку «Просмотр отчетов/View Reports». После этого вы сможете свободно переходить на другие вкладки Metasploit Pro. Центр оповещений отправит сигнал, когда процесс создания будет завершен.

По завершении создания вы можете кликнуть на иконку Центра оповещений, чтобы просмотреть сообщение или перейти в Reports > Show Reports во вкладке управления проектом для перехода в раздел отчетов.

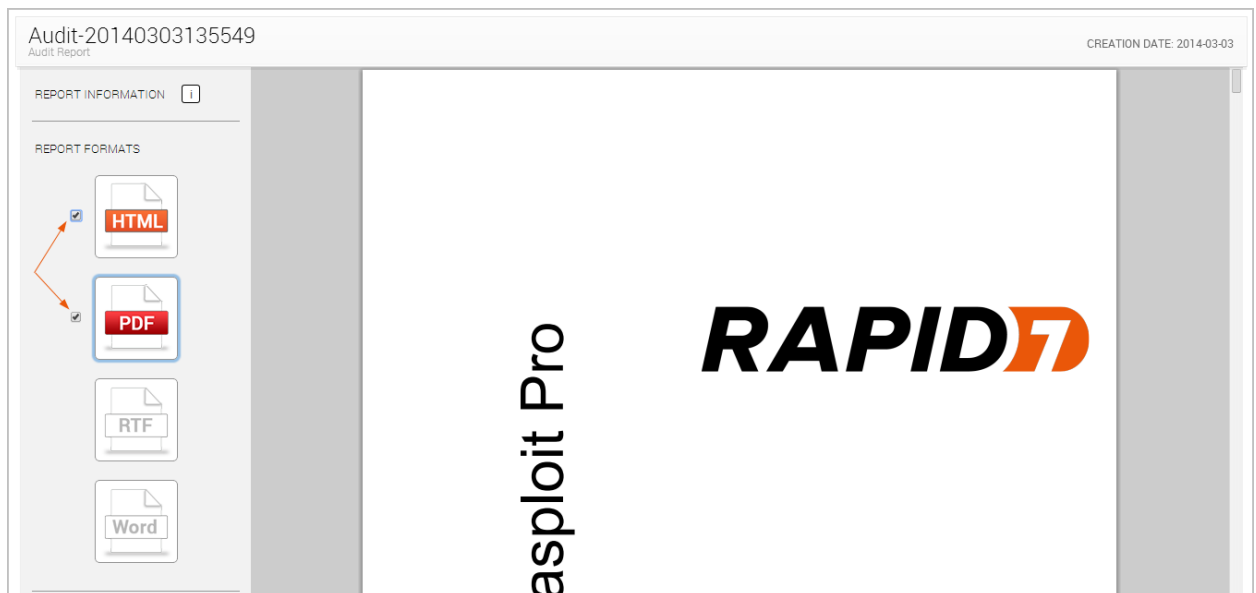
Если по ходу создания отчета произойдет ошибка, вы сможете просмотреть журнал отчетов для идентификации проблемы. Для получения дополнительной информации о журналах отчетов, читайте раздел Журналы Отчетов на странице 1.

Скачивание отчета

1. Откройте проект с отчетом, который вы хотите скачать.
2. Перейдите в Reports > Show Reports во вкладке управления проектом.

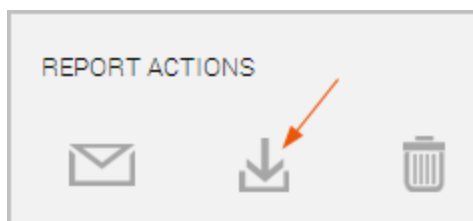


3. Найдите строку отчета, который нужно просмотреть. Строка отображает мета-данные и файловые форматы, доступные для данного отчета.
4. Кликните на имя отчета, чтоб открыть его. Откроется форма просмотра отчета с предпросмотром.
5. Выберите форматы, которые вы хотите скачать.



Форматы, доступные для данного отчета, будут отмечены галочкой.

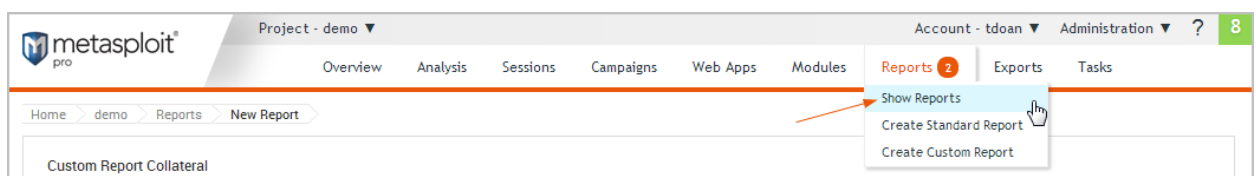
6. Кликните кнопку «Скачать/Download», расположенную под панелью «Действия с отчетом/Report Actions».



Процесс скачивания начнется автоматически. Если ваш браузер не настроен на автоматическую скачку, появится диалоговое окно с подтверждением, чтобы вы подтвердили скачивание. Скачанный отчет необходимо скачать на компьютере.

Просмотр отчета

1. Откройте проект с отчетом, который вы хотите просмотреть.
2. Перейдите в Reports > Show Report во вкладке управления проектом. Появится страница отчетов.



3. Найдите строку с отчетом, который нужно просмотреть.

Saved Reports

Delete Standard Report Custom Report

Show 10 entries

☐	Name	Report Type	File Formats	Creator	Created	Last Updated	Actions
☐	AuthenticationTokens-20140311091720	Authentication Tokens	PDF	tdoan	March 11, 2014 11:17 am	March 11, 2014 11:18 am	View Clone
☐	Audit-20140311091707	Audit	PDF	tdoan	March 11, 2014 11:17 am	March 11, 2014 11:17 am	View Clone
☐	Audit-20140310120033	Audit	PDF, HTML, RTF	TestUser	March 10, 2014 2:00 pm	March 11, 2014 11:22 am	View Clone

Showing 1 to 3 of 3 entries

First Previous 1 Next Last

В строке отображаются метаданные и форматы файлов, созданные для проекта.

4. Кликните на нужный формат для просмотра в нем отчета.

Отчет будет открыт в браузере.

Отправка отчета по почте

Вы можете быстро отправить отчет, как только он будет создан. Стандартные и пользовательские отчеты снабжены функцией «Отправить по почте/Email Report», позволяющей вам отправить письмо с отчетом списку получателей.

Email Report

Recipients

?

Если введены верные настройки почтового сервера в вашей копии программы Metasploit Pro, отчет будет автоматически отправлен получателям в вашем списке.

Настройка почтового сервера

Чтобы максимально использовать все функции электронной почты, необходимо настроить доступ к локальному или веб почтовому серверу. Вам понадобятся адрес и порт почтового адреса, доменное имя хоста сервера, а также необходимые данные для доступа к нему.

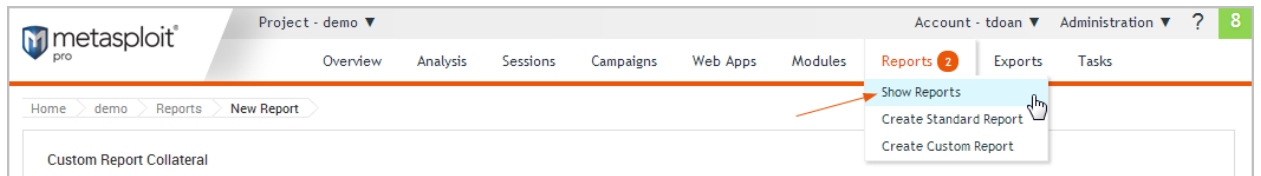
Для получения дополнительной информации по поводу настройки сервера читайте раздел Назначение настроек SMTP для почтового сервера.

Клонирование настроек отчета

Вы можете клонировать отчет, чтобы создать копию настроек отчета. Клонирование позволяет вам использовать заново или перезапускать уже сгенерированные отчеты. Вы можете модифицировать конфигурацию или запустить ее «как есть».

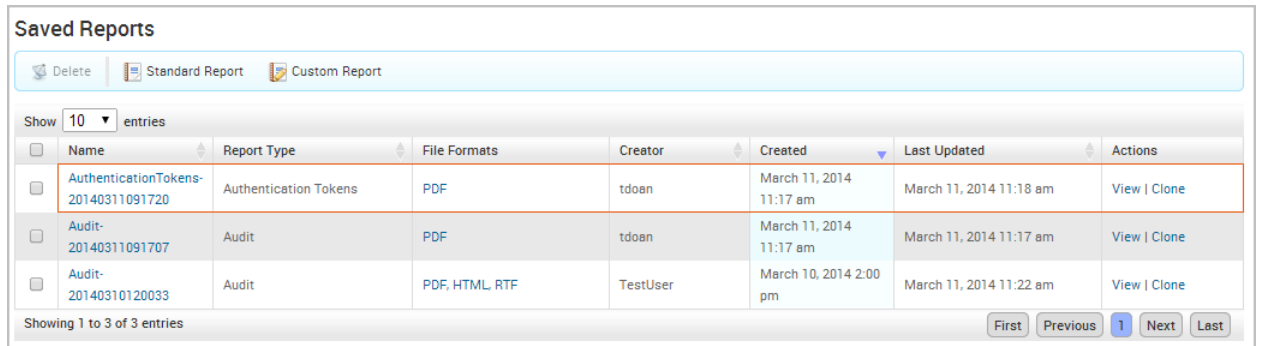
Чтобы клонировать отчет:

1. Откройте проект с отчетом, который нужно клонировать.
2. Перейдите в Reports > Show Reports во вкладке управления проектом.

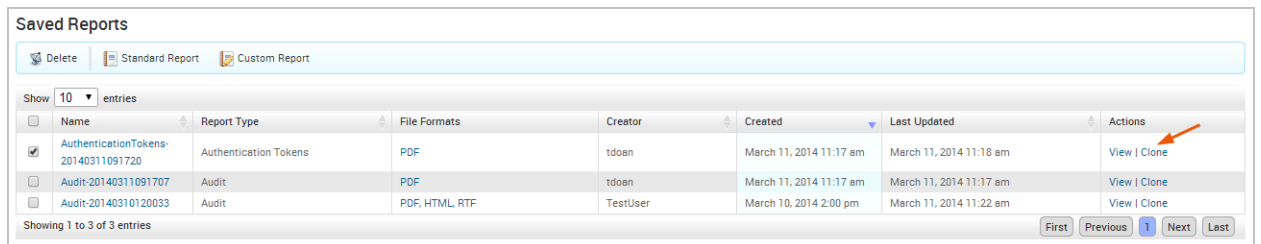


Появится страница отчетов.

3. Найдите строку нужного вам отчета.



4. Кликните активную ссылку «Клонировать/Clone» в колонке действий.



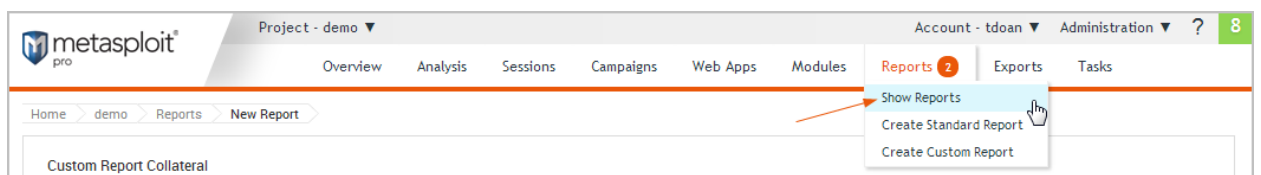
Появится форма создания нового отчета. Форма сохранит конфигурацию настроек, которая была использована для создания этого отчета.

Удаление отчетов

Когда вы удаляете отчет, он будет навсегда удален из директории отчетов. Вы более не сможете просмотреть его из раздела отчетов в веб интерфейсе. До удаления отчета убедитесь в том, что все необходимые вам данные у вас сохранены.

Чтобы удалить отчет:

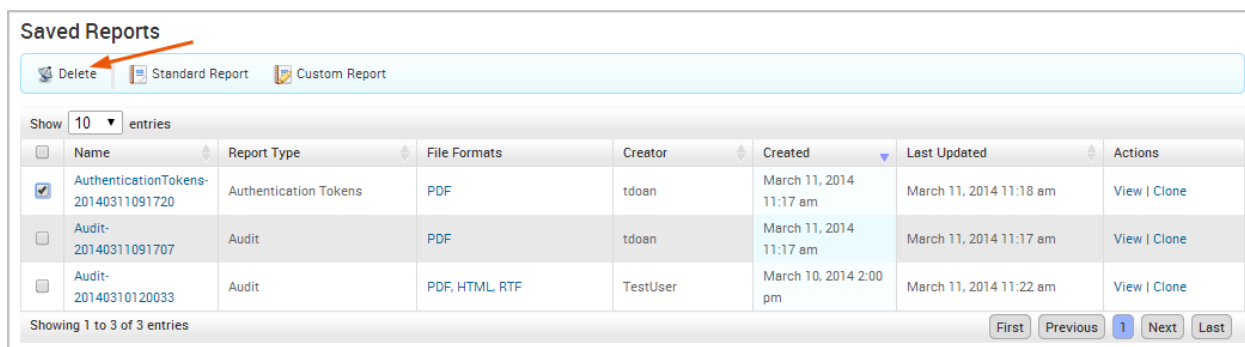
1. Откройте проект с отчетом, который нужно удалить.
2. Перейдите в Reports > Show Reports во вкладке управления проектом.



Появится страница отчетов.

3. Найдите строку нужного вам отчета.

4. Кликните активную ссылку «Удалить/Delete» в панели быстрых действий.



Вам будет необходимо подтвердить действие.

5. Кликните «ОК» для удаления.

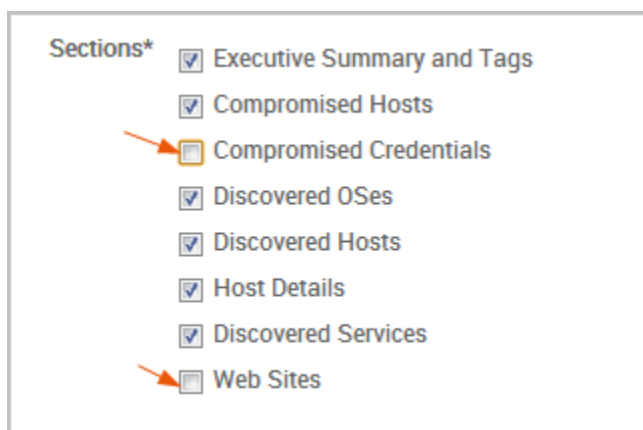
Изменение стандартных отчетов

Стандартный отчет основан на шаблоне по умолчанию от Metasploit Pro. Шаблон определяет внешний вид и форму отчета. Все отчеты также снабжаются титульной страницей и включают в себя набор опций для контроля над данными, включаемыми в отчет. Вы можете изменить некоторые составляющие стандартного отчета. Изменить можно логотип и секции данных в отчете.

Если вам нужно модифицировать разметку отчета, то необходимо использовать пользовательские шаблоны. Для получения дополнительной информации о пользовательских шаблонах читайте раздел [Работа с пользовательскими шаблонами](#).

Исключение секций данных в отчете

Отчет состоит из нескольких секций. Каждая секция разделяет содержимое отчета на несколько важных типов информации. Когда вы просматриваете раздел «Новый отчет», вы увидите секции, доступные для включения в отчет. По умолчанию, выбраны все секции. Если вы хотите, чтобы отчет отображал только определенные секции, то вы можете исключить те, что вам не нужны.



Чтобы исключить из отчета какую-то определенную секцию, уберите выделение с тех секций, которые вам не нужны в отчете. При создании нового отчета вы более не увидите секций, которые вы убрали. Сам отчет покажет только те секции, для которых имеются необходимые данные.

Для получения дополнительной информации о секциях отчета читайте раздел Типы отчетов Metasploit.

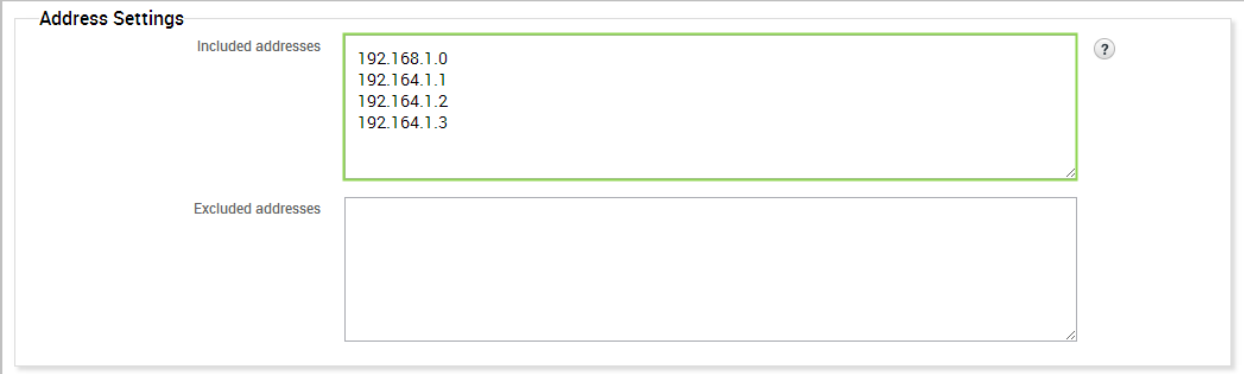
Исключение и включение хостов

При создании отчета Metasploit Pro автоматически включает данные со всех хостов проекта. Если вы хотите ограничить данные и включить в отчет только определенные хосты, необходимо создать специальный список исключений или включений.

Создание списков включенных хостов

«Список включений/Inclusion List» определяет хосты, которые вы хотите включить в отчет. Только данные с этих определенных хостов будут включены в отчет.

Создать список можно в интерфейсе формы «Новый отчет/New Report». Используйте поле «включенные адреса/included addresses» для определения хостов, которые вы хотите включить в отчет. Вы можете ввести всего один IP-адрес или список адресов, а также список CIDR. Если в вашем списке несколько адресов, то используйте новую строку в качестве разделителя.



Создание списков исключенных хостов

«Список исключений/Exclusion List» определяет хосты, которые вы хотите исключить из отчета. Данные со всех хостов будут включены в отчет кроме данных хостов из списка.

Создать список можно в интерфейсе формы «Новый отчет/New Report». Используйте поле «исключенные адреса/excluded addresses» для определения хостов, которые вы хотите исключить из отчета. Вы можете ввести всего один IP-адрес или список адресов, а также список CIDR. Если в вашем списке несколько адресов, то используйте новую строку в качестве разделителя.

Address Settings

Included addresses

Excluded addresses

- 192.164.1.1
- 192.164.1.2
- 192.164.1.3

Удаление личных данных из отчета

Вы можете скрыть личные данные, которые не хотите оставлять в отчете. К ним могут относиться пароли открытым текстом и хэши в отчетах типа Audit, Authentication Tokens, FISMA и PCI.

Чтобы скрыть личные данные в отчете, нужно выбрать опцию «маскировка личных данных/credential masking» в форме «Новый отчет/New Report». Выберите опцию «Скрыть собранные личные данные/Mask discovered credentials», чтобы активировать маскировку.

Options

- ☒ Mask discovered credentials
- ☒ Include session details
- ☒ Include charts

Когда она активна, информация в отчетах не будет представляться открытым текстом. К примеру, когда вы просматриваете отчет по аудиту, все собранные личные данные будут показывать только найденные адреса хостов, сервисы и имена пользователей. Пароли, хэши и SSH ключи будут пустыми.

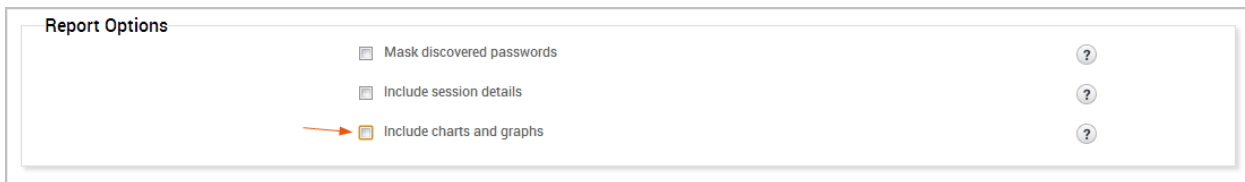
Host address	Service	Username	Password / Hash / Key
50.20.37.50	ssh/22	service	[Masked password]
50.20.37.50	ssh/22	klog	[Masked password]
50.20.37.50	ssh/22	user	[Masked password]

В других отчетах типа PCI и FISMA эти данные будут заменены на <blank>.

Удаление графиков из отчетов

Графики помогают визуализировать статистические данные. Они очень помогают при презентации больших объемов информации. Вы можете включить их в отчет для упрощения визуализации данных и создания акцентов на определенных трендах в результатах работ. Metasploit Pro обычно создает отчеты с круговыми диаграммами для иллюстрации распределения данных между разными категориями данных.

Большинство отчетов, за исключением отчетов типа FISMA, PCI, Social Engineering, Web Application Assessment и Activity, снабжено графиками. По умолчанию, графики включены. Они будут сформированы автоматически там, где это возможно. Если вы хотите исключить их из отчета, просто выключите соответствующую опцию, для этого снимите выделение с опции «Включить графики/Include charts and graphs».



Report Options

- ☐ Mask discovered passwords
- ☐ Include session details
- ☒ Include charts and graphs

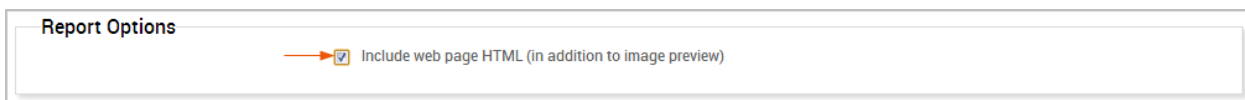
Включение HTML-кода веб страниц в отчеты по социальной инженерии

Отчеты типа Social Engineering представляют собранные данные для отдельно взятой кампании. Отчет включает в себя детали компонентов кампании, использованных при ее проведении, включая список целей, электронную почту и веб страницы, использованные при работе.

Содержимое списков целей и электронная почта будут автоматически включены в отчет. Если вы хотите включить в него HTML-код веб страниц, то нужно активировать соответствующую опцию. Когда она активирована, все веб страницы кампании будут отображены в этом виде. Предварительный просмотр веб страниц будет использован в том случае, если они использовались в кампании.

Внимание: если веб страница содержала вредоносный код (например, веб эксплойт, Java-апплет или файл-приложение), то он не будет включен в рендеринг страницы во время работы с формой «Новый отчет/new Report».

Если вы хотите включить сырой HTML, использованный для создания веб-страницы, вы можете активировать этот параметр на странице нового отчёта.



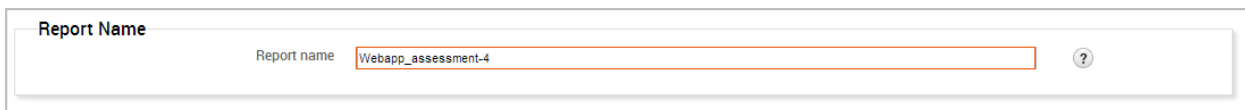
Report Options

- ☒ Include web page HTML (in addition to image preview)

Изменение названий отчетов

Metasploit Pro использует алгоритм для создания названий. Он включает в себя блоки «Тип отчет/report Type» и «Время создания/Timestamp». Выражается в форме: <report type>-<timestamp>. Это название используется для отображения отчета на странице отчетов.

Вы можете изменить название по умолчанию в поле «Название отчета/Report Name» при работе с формой «Новый отчет/New Report».



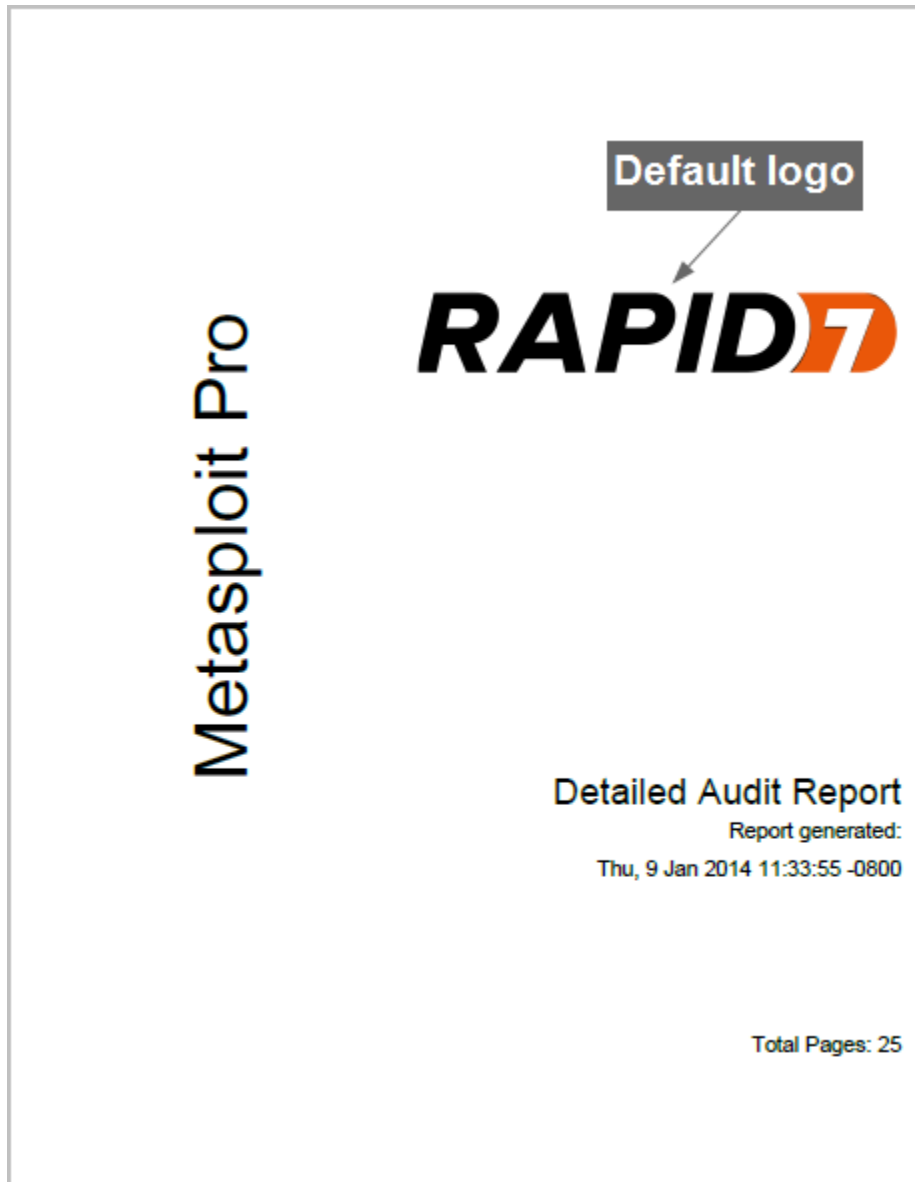
Report Name

Report name

Добавление пользовательского лого к отчету

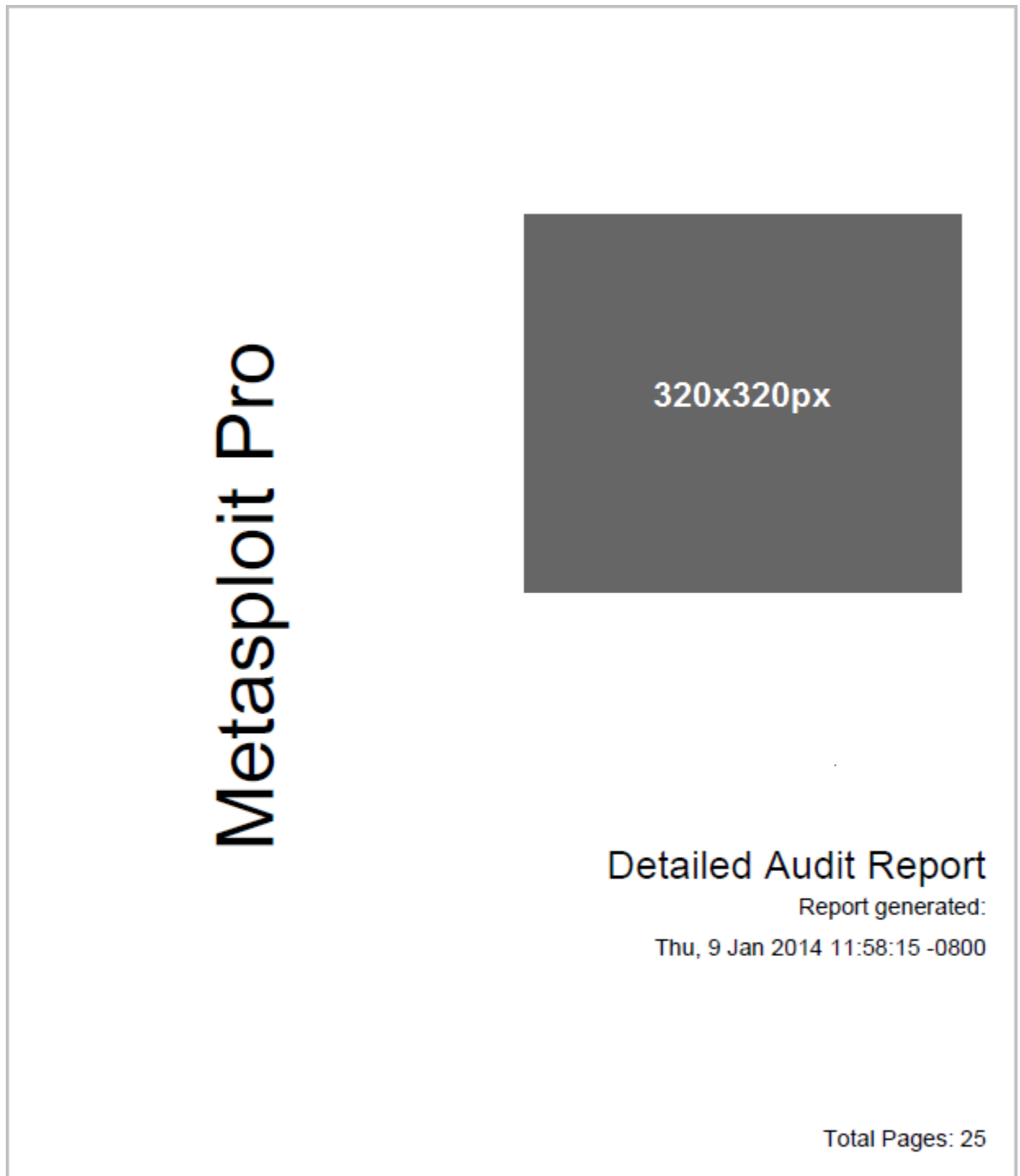
Все отчеты снабжаются титульной страницей, на которой отображены название, логотип и время создания. Титульная страница использует изображение Rapid7 в качестве лого по умолчанию.

Если вы хотите заменить лого по умолчанию, вы можете загрузить изображение в формате JPG, GIF или PNG. Загруженные логотипы можно использовать для брендирования отчетов вашей собственной символикой. Логотип размещается в правой части титульной страницы и замещает собой лого Rapid7.



Требования к логотипу

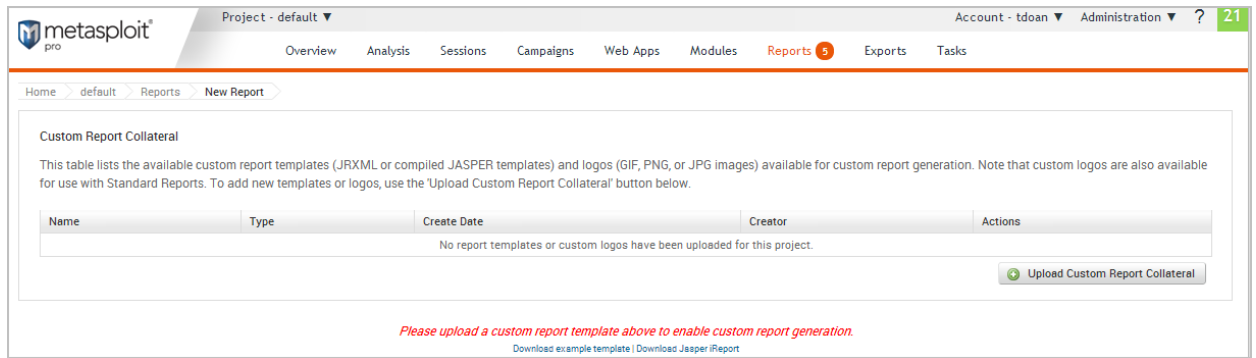
Площадь, отведенная логотипу, составляет 320x320 пикселей. Вы можете загрузить изображение больше этого размера, но лого будет подогнано так, чтобы поместиться на этой площади.



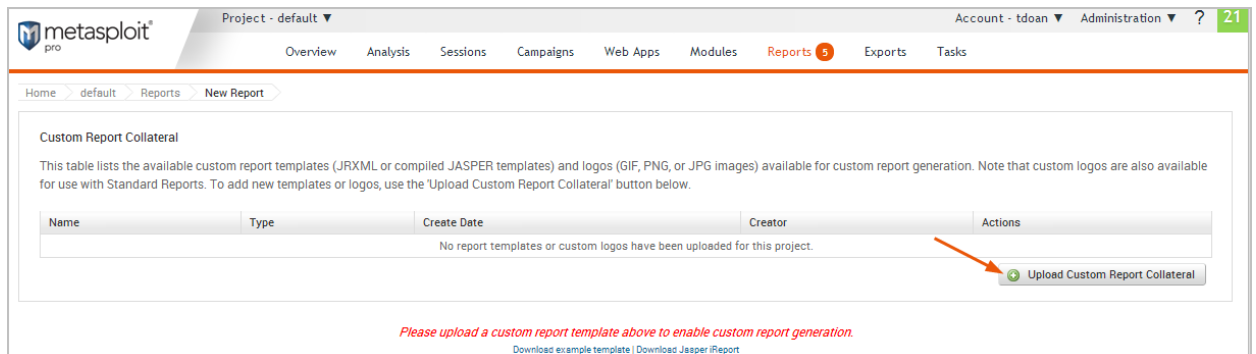
Если изображение больше отведенной площади, то высота изображения будет сохранена, но ширина будет изменена.

Загрузка пользовательского логотипа

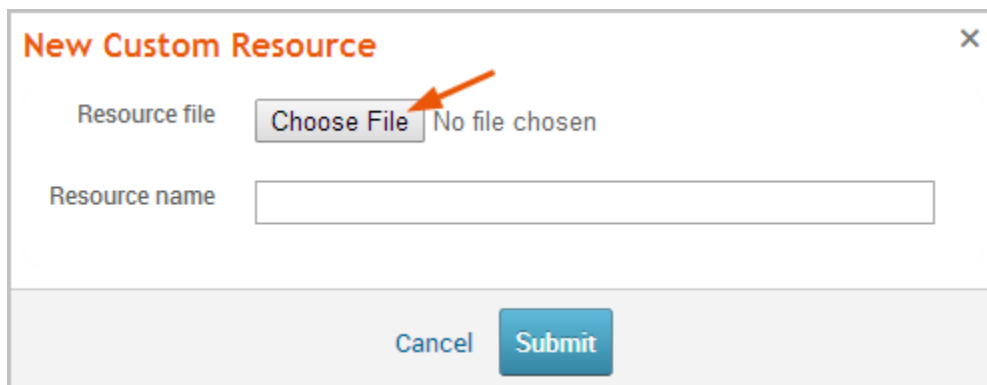
1. Откройте проект, для которого нужно загрузить лого.
2. Перейдите в Reports > Create Custom Report во вкладке управления проектами. Появится страница отчетов.
3. Найдите раздел «Custom Report Collateral».



4. Кликните «Upload Custom Report Collateral». Появится окно загрузки.



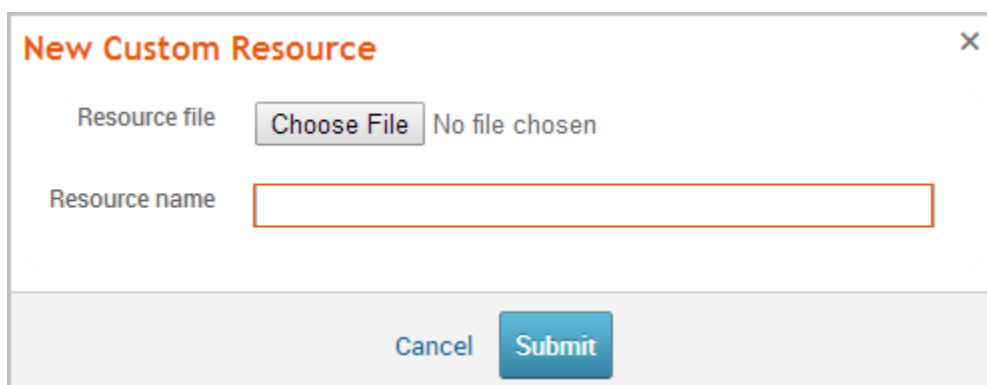
5. Кликните «Выбрать файл/Choose File». Откроется диалоговое окно.



6. Найдите необходимый вам файл.

Внимание: вы можете использовать только файлы в форматах GIF, JPEG, JPG или PNG.

7. Выберите файл логотипа и кликните на кнопку «Открыть/Open».
8. Введите название для файла в поле «Descriptive Name». (Необязательно).



Если вы не укажете имя файла, то в разделе «Custom Report Collateral» будет отображено оригинальное название.

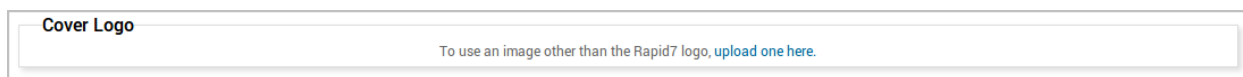
9. Кликните кнопку «Загрузить/Upload». Файл появится в разделе «Custom Report Collateral».

Добавление пользовательского лого к стандартному отчету

Чтобы использовать пользовательский логотип для титульной страницы, вам нужно кликнуть на «Custom report logo» в форме «Новый отчет/New Report» и выбрать нужное вам изображение. В выпадающем меню будут показаны все логотипы, загруженные в проект.



Если проект не содержит логотипы, то форма «Новый отчет/New Report» покажет вам ссылку на страницу «Пользовательские отчеты/Custom Reports», где вы сможете загрузить логотип.



Работа с пользовательскими шаблонами

Metasploit Pro распространяется вместе с набором уже подготовленных к работе стандартных отчетов, создаваемых при помощи шаблона Metasploit Pro с учетом всех современных норм тестирования систем безопасности. Стандартные отчеты могут не удовлетворять вашим собственным требованиям. Если вам нужны особые разметки и содержимое, вы можете использовать собственные шаблоны для отчетов. Пользовательские шаблоны позволяют вам применять корпоративный стиль к отчетам, контролировать, как и где отображается содержимое отчетов, а также изменять отчеты согласно вашим нормам соответствия.

Пользовательский шаблон представляет собой JRXML-файл. Это обычный XML-файл, созданный при помощи JasperReport. В нем содержится необходимая информация по структуре отображения содержимого, расположения изображений, а также по порядку запроса данных. Можно составить этот файл самостоятельно при помощи редактирования XML или воспользоваться редактором шаблонов для JasperReport типа iReport или Jaspersoft Studio для Eclipse.

Jasper Reports и iReport Designer

Metasploit Pro использует JasperReports 5.0. Это библиотека, написанная на Java, с открытым исходным кодом. JasperReports используется для компиляции данных и создания отчетов в форматах PDF, RTF, HTML и Word. Шаблон JRXML это файл стандартов XML, в котором определяются все элементы и атрибуты, контролирующие, где располагается содержимое. Вы можете создать JRXML-шаблон при помощи визуального дизайнера iReport Designer, разработанного ПО с открытым кодом от Jaspersoft.

iReport Designer позволяет вам работать с интуитивно понятным графическим интерфейсом для визуализации шаблонов отчетов без глубоких знаний библиотек JasperReports, XML или Java. Вы можете просто перетаскивать элементы отчета для создания разметки отчета и присоединять его к существующим источникам данных типа JDBC и XML для запроса данных к отчету. Это позволяет JRXML шаблонам импортировать данные в Metasploit Pro проект и использовать при создании пользовательских отчетов.

Скачивание Jasper iReport

Чтобы скачать iReport, пожалуйста, перейдите по адресу <http://jasperforge.org/projects/ireport>.

Ресурсы для JasperReports и iReports Designer

Чтобы создать пользовательский шаблон, нужно иметь определенные познания касательно JasperReports и iReports Designer. Есть несколько полезных ресурсов, которые помогут вам оперативно создавать шаблоны при помощи iReport Designer и понять, как именно работает JasperReports.

Чтобы получить дополнительную информацию по JasperReports и iReports Designer, используйте следующие ресурсы:

- Список документации для JasperReports – это полный список документации по JasperStudio, JasperReports Server, JasperReports Library и iReport Designer. Вы можете найти этот перечень здесь: <http://community.jaspersoft.com/documentation>.
- Список документации по работе с библиотеками JasperReports. Представлена техническая документация, вебинары и статьи, которые могут быть полезны при работе с JasperReports. Вы можете найти этот перечень здесь: <http://community.jaspersoft.com/wiki/jasperreports-library-reference-materials>
- Руководство и WIKI-справка для iReport Designer. Это wiki-ресурс с руководствами для работы с данным приложением. Вы можете найти этот перечень здесь: <http://community.jaspersoft.com/wiki/ireport-designer-tutorials-help>.
- Статья по работе с графиками содержит краткое описание и ссылки на редакторы графиков для JasperReports, iReport Designer и JasperReports Server. Читайте статью здесь: <http://mdahlman.wordpress.com/2011/04/17/chart-customizers-2/>.
- Документация по Groovy – это полностью Java-совместимый язык для скриптов, который можно использовать вместо Java для создания выражений для iReport. Чтобы побольше узнать о Groovy и iReport Designer, посетите <https://www.jaspersoft.com/training-services> или <https://www.jaspersoft.com/training>.
- JasperSoft тренинги. Вы можете пройти специальные тренинги. Для этого перейдите по адресу <https://www.jaspersoft.com/training-services> или <https://www.jaspersoft.com/training>.

Требования для создания шаблонов

Чтобы создать пользовательский шаблон, вам нужно будет следующее:

- Опыт работы с Jasper iReport, JasperReports, XML и SQL/XPath.
- Опыт работы с Java или Java-совместимым языком для скриптов, like Groovy или Javascript.

- Рабочая версия Jasper iReport.
- Доступ к базам данных Metasploit.

Настройка баз данных Metasploit и iReport Designer

Чтобы заполнить отчет данными, нужно иметь доступ к источнику данных, подключенному к Postgres-серверу Metasploit. Информация для postgres-сервера здесь:

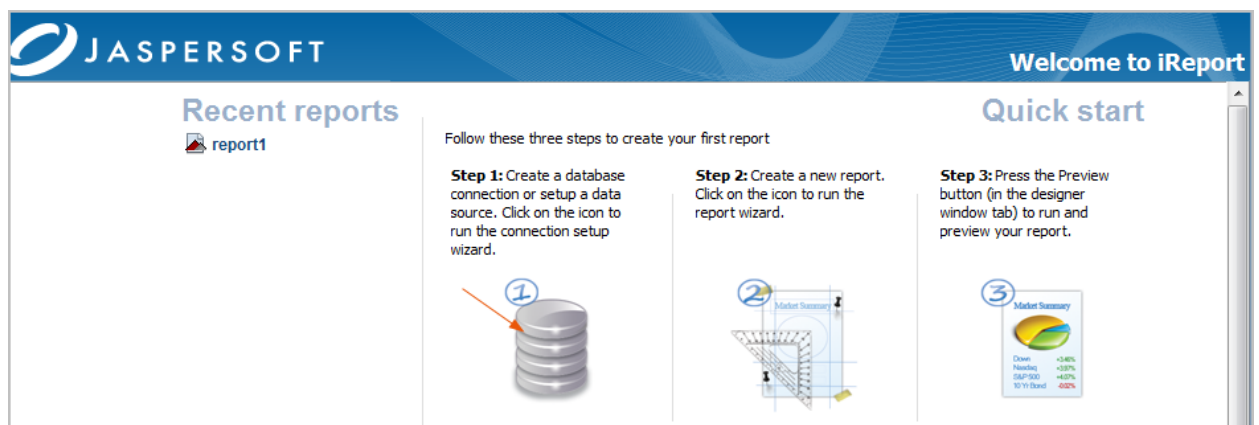
/path/to/metasploit/apps/pro/config/database.yml.

Вам понадобится следующая информация из файла database.yml:

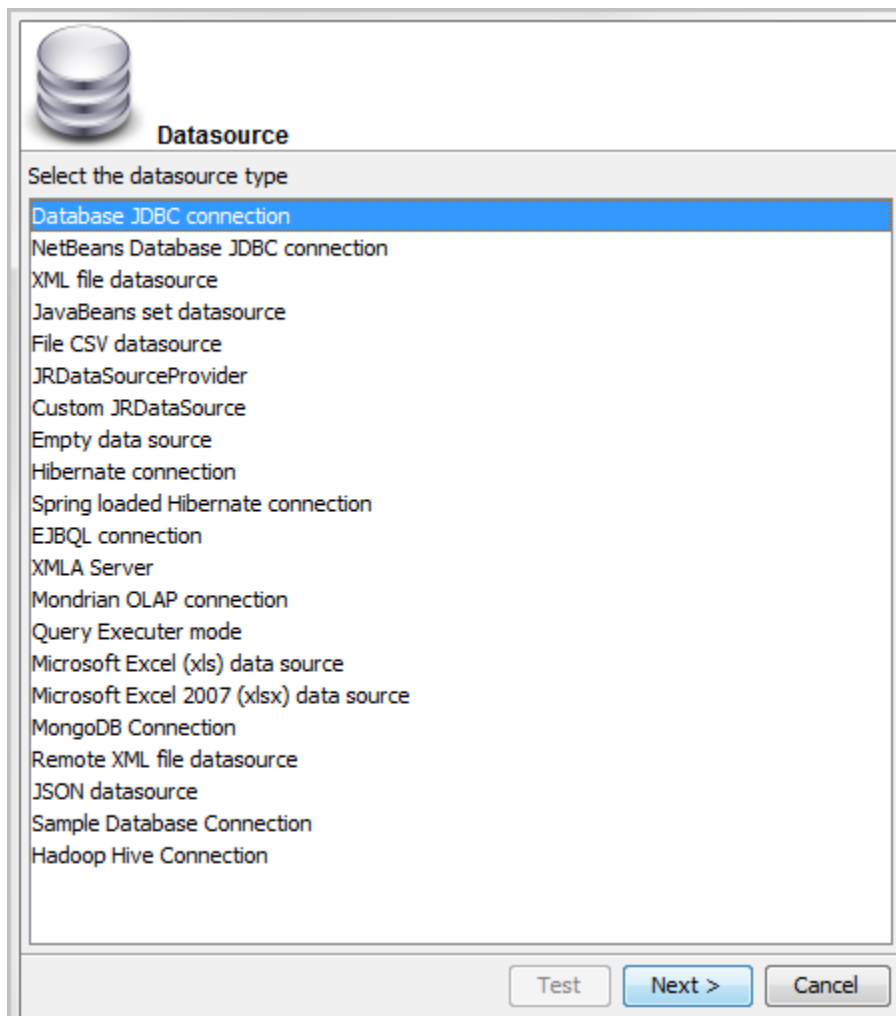
- Имя базы данных. По умолчанию называется msf3.
- Порт postgresql. Порт по умолчанию – 7337.
- Имя пользователя. По умолчанию имя пользователя – msf3.
- Пароль. Просмотрите файл database.yml, чтобы найти пароль к базе данных.

Как настроить источник данных для iReport Designer:

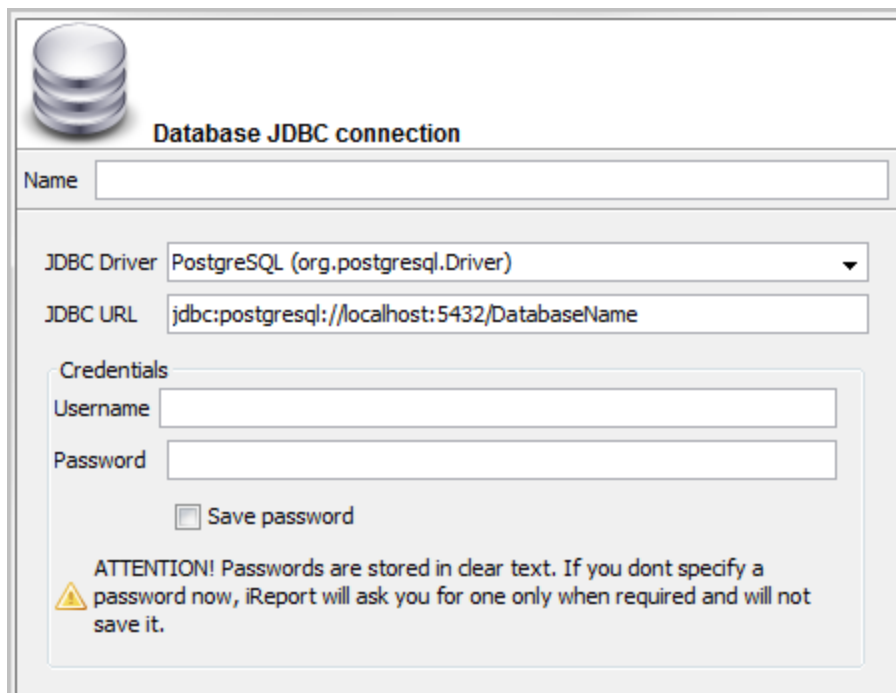
1. Откройте iReport Designer. Появится приветственное окно Quick Start.
2. Кликните на иконку соединения с базой данных. Появится окно «Источник данных/Data source».



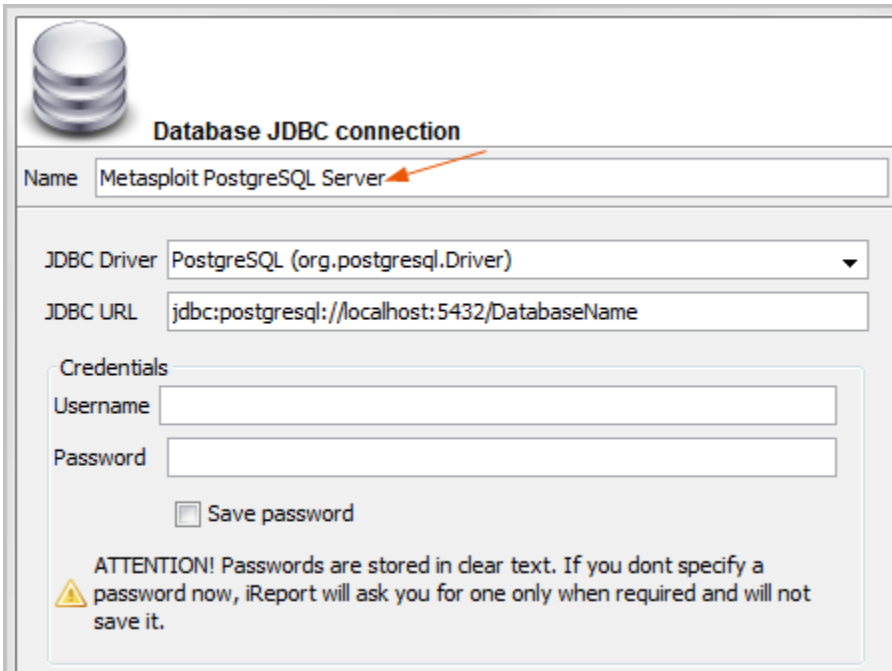
3. Выберите «Database JDBC» из списка источников данных.



4. Кликните «Далее/Next». Появится окно настройки соединения с базой JDBC.



5. Введите название для соединения в поле «Имя/Name».



The image shows a web form titled "Database JDBC connection" with a database icon. It contains several input fields: "Name" (Metasploit PostgreSQL Server), "JDBC Driver" (PostgreSQL (org.postgresql.Driver)), and "JDBC URL" (jdbc:postgresql://localhost:5432/DatabaseName). There is also a "Credentials" section with "Username" and "Password" fields, and a "Save password" checkbox. A warning message at the bottom states: "ATTENTION! Passwords are stored in clear text. If you dont specify a password now, iReport will ask you for one only when required and will not save it."

Database JDBC connection

Name

JDBC Driver

JDBC URL

Credentials

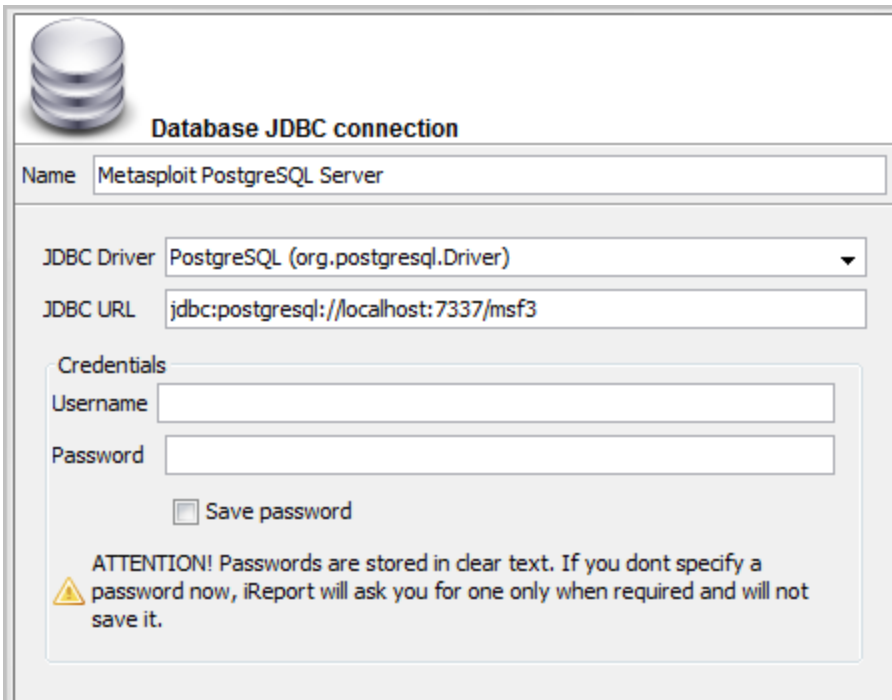
Username

Password

☐ Save password

ATTENTION! Passwords are stored in clear text. If you dont specify a password now, iReport will ask you for one only when required and will not save it.

6. Замените содержимое поля «JDBC URL» на jdbc:postgresql://localhost:7337/msf3.



The image shows the same web form as above, but with the "JDBC URL" field updated to "jdbc:postgresql://localhost:7337/msf3". All other fields and the warning message remain the same.

Database JDBC connection

Name

JDBC Driver

JDBC URL

Credentials

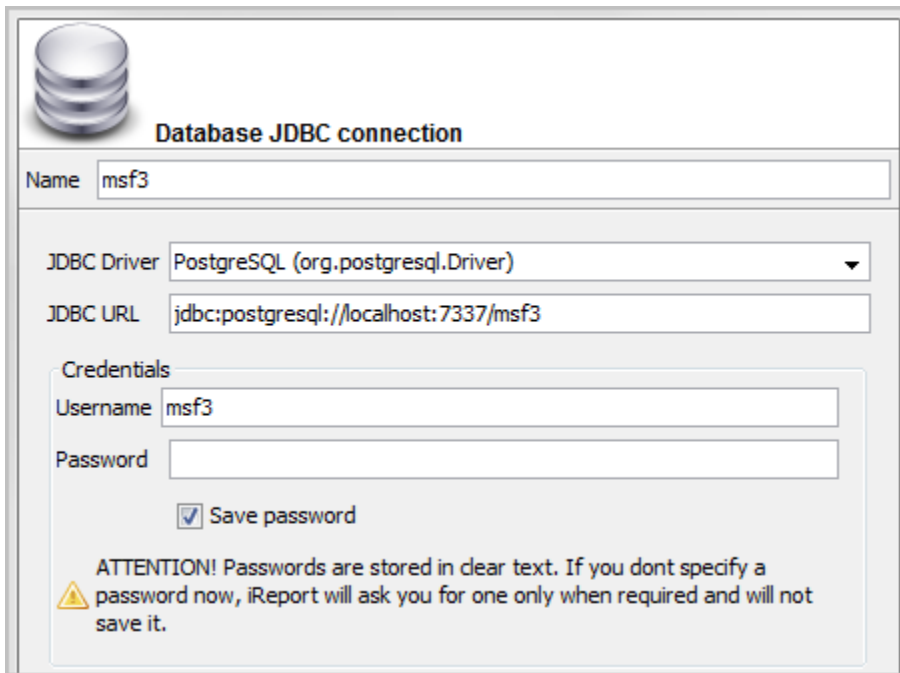
Username

Password

☐ Save password

ATTENTION! Passwords are stored in clear text. If you dont specify a password now, iReport will ask you for one only when required and will not save it.

7. Введите имя пользователя базы данных в поле «Имя пользователя/Username».



Database JDBC connection

Name

JDBC Driver

JDBC URL

Credentials

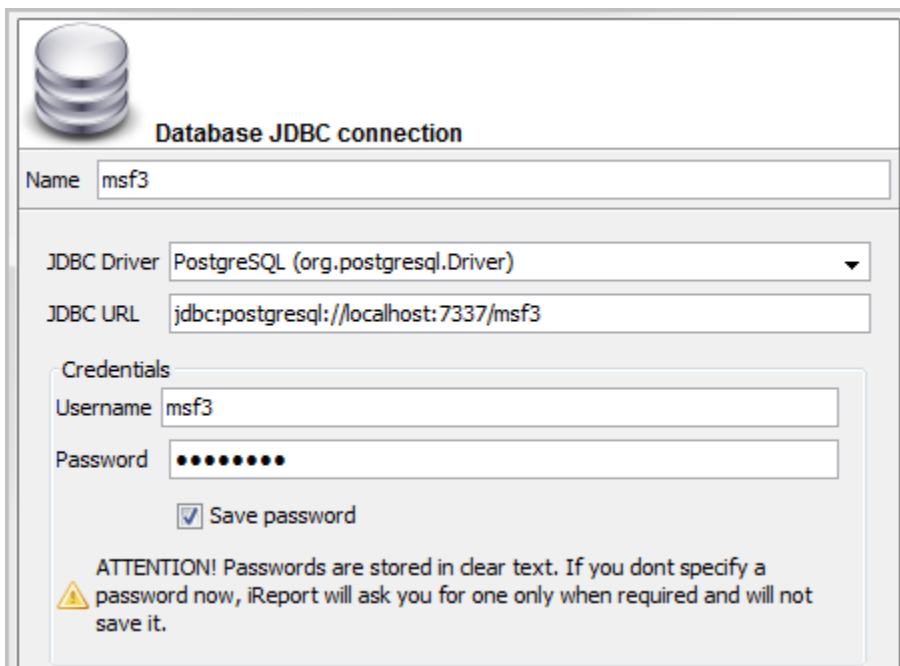
Username

Password

☒ Save password

ATTENTION! Passwords are stored in clear text. If you dont specify a password now, iReport will ask you for one only when required and will not save it.

8. Введите пароль от базы данных в поле «Пароль/Password».



Database JDBC connection

Name

JDBC Driver

JDBC URL

Credentials

Username

Password

☒ Save password

ATTENTION! Passwords are stored in clear text. If you dont specify a password now, iReport will ask you for one only when required and will not save it.

9. Протестируйте соединение.
Если соединение работает нормально, то появится окно с оповещением о том, что соединение было успешным. В другом случае, если соединение не состоялось, появляется окно с оповещением о том, что есть проблемы с настройками для баз данных. Внимательно проверьте соответствие информации в настройках баз данных с данными из файла database.yml.
10. Сохраните соединение, если оно было успешным.

Теперь вы готовы к созданию шаблона отчетов. Список ресурсов для создания шаблонов при помощи JasperReports и iReport Designer чуть выше.

Пользовательская директория ресурсов

Все пользовательские шаблоны и логотипы хранятся в директории

`/path/to/metasploit/apps/pro/reports/custom_resources.`

Вы можете зайти в директорию для скачивания или просмотра логотипов и шаблонов. Воздержитесь от изменений содержимого директории. Если вам нужно изменить логотип или шаблон, создайте копию директории и делайте изменения во вновь созданной.

Все изменения, которые вы делаете напрямую в директории с пользовательскими шаблонами, могут создать различия между метаданными, отображаемыми в веб интерфейсе, и файлами в директории. Не удаляйте их напрямую из директории.

Загрузка шаблонов

После создания пользовательского шаблона вам понадобится загрузить его в проект, который вы хотите использовать для создания пользовательского отчета. Шаблон будет использован только для проектов, в который вы его загрузили. Если вы хотите использовать шаблон для нескольких проектов, то вам придется импортировать его в каждый проект по отдельности.

Когда вы работаете с формой «Новый пользовательский отчет/New Custom Report», шаблон будет доступен в выпадающем меню «Шаблон отчета/Report Template».

Home > default > Reports > New Report

Custom Report Collateral

This table lists the available custom report templates (JRXML or compiled JASPER templates) and logos (GIF, PNG, or JPG images) available for custom report generation. Note that custom logos are also available for use with Standard Reports. To add new templates or logos, use the 'Upload Custom Report Collateral' button below.

Name	Type	Create Date	Creator	Actions
custom-template	Template	2014-01-16 13:42:47 -0800	tdoan	Download Delete

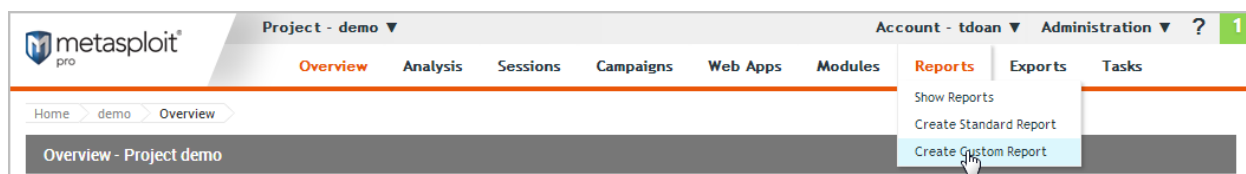
[Upload Custom Report Collateral](#)

Custom Report Template

Report template* custom-template ?

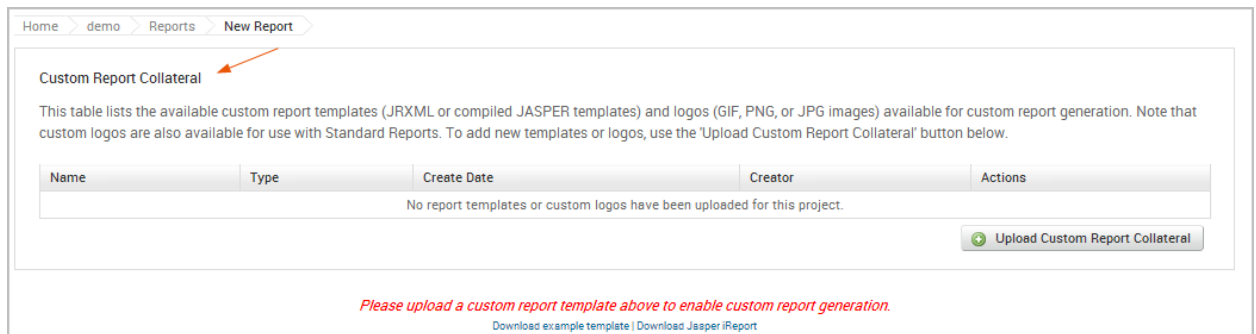
Чтобы загрузить шаблон:

1. Откройте проект, для которого нужно загрузить шаблон.
2. Перейдите в Reports > Create Custom Report во вкладке управления проектами.

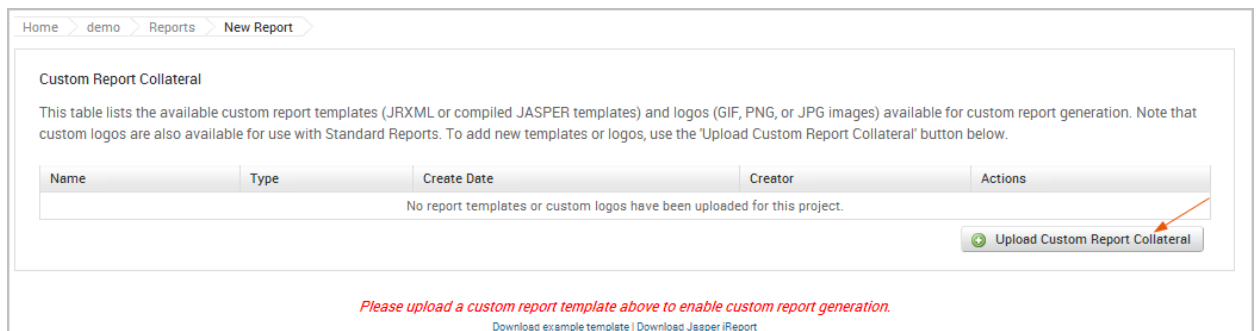


Появится страница отчетов с выбранной вкладкой «Создать пользовательский отчет/Generate Custom Report».

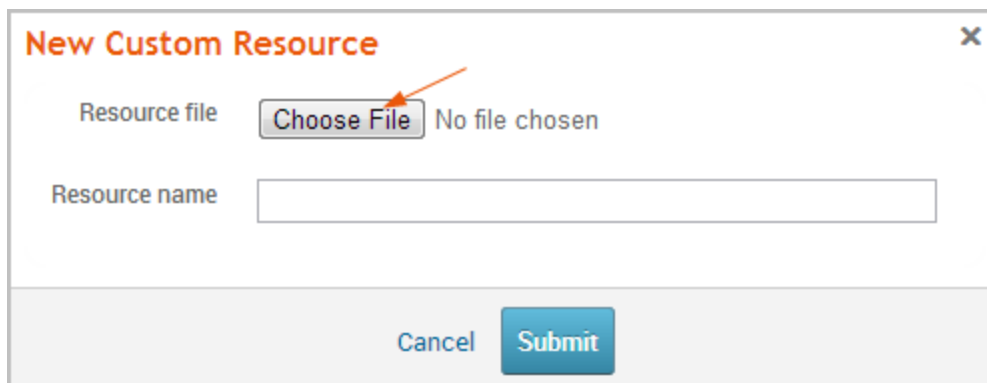
3. Найдите раздел «Custom Report Collateral». Если в вашем проекте нет никаких шаблонов, то вкладка «Новый Пользовательский отчет» не отобразит форму.



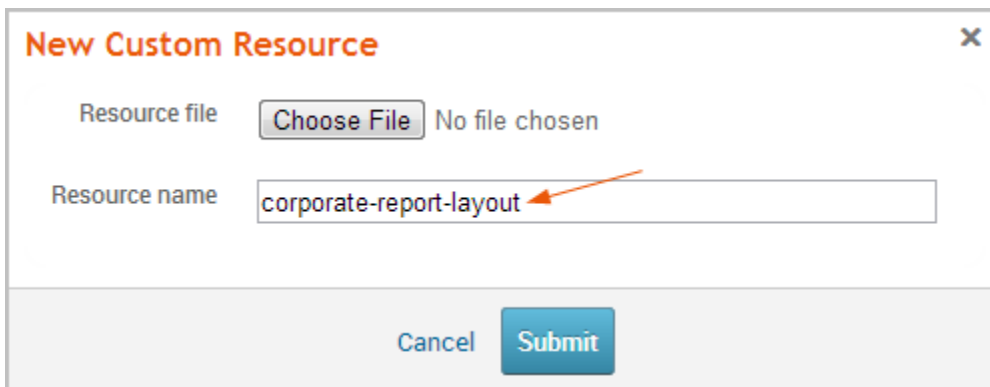
4. Кликните «Upload Custom Report Collateral». Появится окно загрузки.



5. Кликните «Выбрать файл/Choose File». Откроется диалоговое окно.



6. Найдите необходимый вам файл.
7. Выберите файл шаблона и кликните на кнопку «Открыть/Open». Файл должен иметь расширение JRXML.
8. Введите название для файла в поле «Descriptive Name». (Необязательно). Если вы не укажете имя файла, то в разделе «Custom Report Collateral» будет отображено оригинальное название.

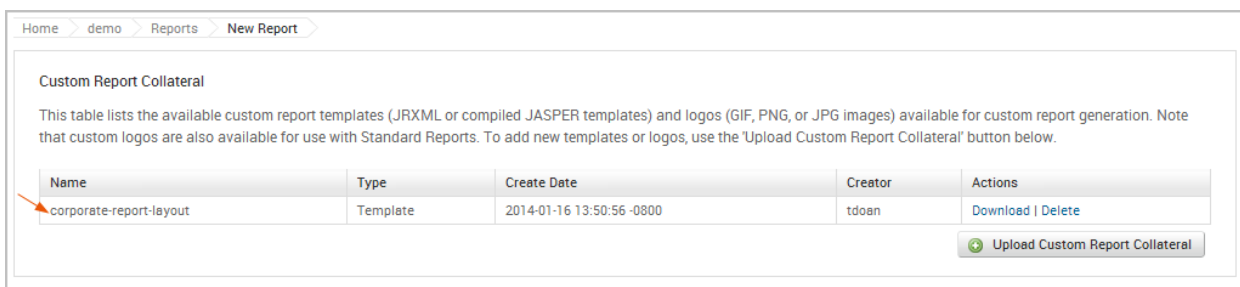


New Custom Resource

Resource file No file chosen

Resource name

9. Кликните кнопку «Submit». Файл появится в разделе «Custom Report Collateral».



Home > demo > Reports > New Report

Custom Report Collateral

This table lists the available custom report templates (JRXML or compiled JASPER templates) and logos (GIF, PNG, or JPG images) available for custom report generation. Note that custom logos are also available for use with Standard Reports. To add new templates or logos, use the 'Upload Custom Report Collateral' button below.

Name	Type	Create Date	Creator	Actions
corporate-report-layout	Template	2014-01-16 13:50:56 -0800	tdoan	Download Delete

Теперь вы можете создать пользовательский отчет. Для получения дополнительной информации о пользовательских отчетах читайте раздел «[Создание пользовательского отчета](#)».

Скачивание пользовательского шаблона для отчетов

1. Откройте проект, содержащий пользовательский шаблон проекта, который вам нужно скачать.
2. Перейдите в Reports > Show Reports во вкладке управления проектом. Появится страница отчетов с выбранной вкладкой «Создать пользовательский отчет/Generate Custom Report».



metasploit[®] pro

Project - demo ▼ Account - tdoan ▼ Administration ▼ ? 1

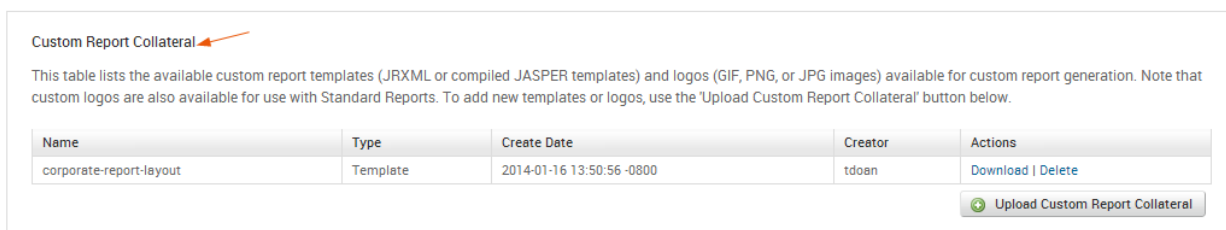
Overview Analysis Sessions Campaigns Web Apps Modules Reports Exports Tasks

Home > demo > Overview

Overview - Project demo

Show Reports
Create Standard Report
Create Custom Report

3. Найдите раздел «Custom Report Collateral».



Custom Report Collateral

This table lists the available custom report templates (JRXML or compiled JASPER templates) and logos (GIF, PNG, or JPG images) available for custom report generation. Note that custom logos are also available for use with Standard Reports. To add new templates or logos, use the 'Upload Custom Report Collateral' button below.

Name	Type	Create Date	Creator	Actions
corporate-report-layout	Template	2014-01-16 13:50:56 -0800	tdoan	Download Delete

4. Найдите строку содержащую пользовательский шаблон отчета, который вы хотите скачать.

Custom Report Collateral

This table lists the available custom report templates (JRXML or compiled JASPER templates) and logos (GIF, PNG, or JPG images) available for custom report generation. Note that custom logos are also available for use with Standard Reports. To add new templates or logos, use the "Upload Custom Report Collateral" button below.

Name	Type	Create Date	Creator	Actions
corporate-report-layout	Template	2014-01-16 13:50:56 -0800	tdoan	Download Delete

[Upload Custom Report Collateral](#)

В строке отображаются метаданные и действия, которые вы можете совершить с пользовательским шаблоном.

5. Кликните кнопку «Скачать/Download».

Custom Report Collateral

This table lists the available custom report templates (JRXML or compiled JASPER templates) and logos (GIF, PNG, or JPG images) available for custom report generation. Note that custom logos are also available for use with Standard Reports. To add new templates or logos, use the "Upload Custom Report Collateral" button below.

Name	Type	Create Date	Creator	Actions
corporate-report-layout	Template	2014-01-16 13:50:56 -0800	tdoan	Download Delete

[Upload Custom Report Collateral](#)

Процесс скачивания начнется автоматически. Если ваш браузер не настроен на автоматическую скачку файлов, появится диалоговое окно, где нужно будет подтвердить ваше желание скачать и запустить файл. Вам нужно будет сохранить шаблон на вашем компьютере.

Удаление пользовательского шаблона для отчетов

1. Откройте проект с отчетом, который нужно удалить.
2. Перейдите в Reports > Create Custom Report во вкладке управления проектом. Появится страница отчетов с выбранной вкладкой «Создать пользовательский отчет/Generate Custom Report».

The screenshot shows the Metasploit web interface. The top navigation bar includes 'Overview', 'Analysis', 'Sessions', 'Campaigns', 'Web Apps', 'Modules', 'Reports', 'Exports', and 'Tasks'. The 'Reports' menu is open, showing options: 'Show Reports', 'Create Standard Report', and 'Create Custom Report'. The 'Create Custom Report' option is highlighted with a mouse cursor. The breadcrumb trail at the top reads 'Home > demo > Overview'.

3. Найдите раздел «Custom Report Collateral».

Custom Report Collateral

This table lists the available custom report templates (JRXML or compiled JASPER templates) and logos (GIF, PNG, or JPG images) available for custom report generation. Note that custom logos are also available for use with Standard Reports. To add new templates or logos, use the "Upload Custom Report Collateral" button below.

Name	Type	Create Date	Creator	Actions
corporate-report-layout	Template	2014-01-16 13:50:56 -0800	tdoan	Download Delete

[Upload Custom Report Collateral](#)

4. Найдите строку содержащую пользовательский шаблон отчета, который вы хотите удалить.

Custom Report Collateral

This table lists the available custom report templates (JRXML or compiled JASPER templates) and logos (GIF, PNG, or JPG images) available for custom report generation. Note that custom logos are also available for use with Standard Reports. To add new templates or logos, use the "Upload Custom Report Collateral" button below.

Name	Type	Create Date	Creator	Actions
corporate-report-layout	Template	2014-01-16 13:50:56 -0800	tdoan	Download Delete

 Upload Custom Report Collateral

5. Кликните активную ссылку «Удалить/Delete».

Custom Report Collateral

This table lists the available custom report templates (JRXML or compiled JASPER templates) and logos (GIF, PNG, or JPG images) available for custom report generation. Note that custom logos are also available for use with Standard Reports. To add new templates or logos, use the "Upload Custom Report Collateral" button below.

Name	Type	Create Date	Creator	Actions
corporate-report-layout	Template	2014-01-16 13:50:56 -0800	tdoan	Download Delete

 Upload Custom Report Collateral

Появится окно с подтверждением необходимости удалить файл. Нажмите «ОК».

Скачивание примера шаблона

Metasploit Pro идет вместе с примером шаблона, на который вы можете опираться при создании собственного шаблона. В примере есть простые примеры, позволяющие вам быстро разобраться, как происходит запрос данных, IP-адресов хостов, имен, операционных систем, сервисов и уязвимостей из проекта, а также как эта информация отображается в виде таблицы. Там также есть примеры того, как добавлять в отчет заглавие и футер.

Example JRXML Template

\$P{product_name}		Vulnerability and Service Survey Report (Sample)		
IP Address	Name	OS	Svcs	Vulns
\$F{address}	\$F{name}	\$F{os_name}	\$F	\$F{vuln_count}
Detail 1				
new java.util.Date() "Page ~\$V{PAGE_NUMBER}~" of ~\$V				

Report design

```
<queryString>
  <![CDATA[SELECT
hosts.id as id,
hosts.created_at as discovered,
HOST (CAST (hosts.address as inet)) as address,
COALESCE (hosts.name, HOST (CAST (hosts.address as inet))) as name,
COALESCE (hosts.os_name, '<Unknown>') as os_name,
(select count(*) from services where services.host_id = hosts.id) as service_count,
(select count(*) from vulns where vulns.host_id = hosts.id) as vuln_count
FROM hosts
WHERE hosts.workspace_id = $P{workspace_id} and
$P{host_address_clause}
ORDER BY vuln_count DESC, discovered
;]]>
</queryString>
```

Data query

Metasploit Pro		Vulnerability and Service Survey Report (Sample)		
IP Address	Name	OS	Svcs	Vulns
20.20.36.51	MS-W03-3U-1	Microsoft Windows	8	1
20.20.36.68	MS-W08-6U-1	Microsoft Windows	11	0
20.20.36.74	ms-wsp-6u-1	Microsoft Windows	5	0
20.20.36.57	MS-W08-3U-1	Microsoft Windows	12	0
20.20.36.59	MS-W08-6U-1	Microsoft Windows	12	0
20.20.36.58	MS-W08-6U-1	Microsoft Windows	12	0
20.20.36.52	MS-W03-3U-1	Microsoft Windows	7	0
20.20.36.79	WEBTARGET2	Microsoft Windows	14	0
20.20.36.55	MS-W03S2-3U-1	Microsoft Windows	6	0
20.20.36.54	MS-W03R2-6U-1	Microsoft Windows	7	0
20.20.36.70	ms-wvs-3u-1	Microsoft Windows	1	0
20.20.36.65	1 ms-ws08l6h-rp0d74	Microsoft Windows	12	0
20.20.36.76	MS-W7-3U-1	Microsoft Windows	6	0
20.20.36.56	MS-W08-3U-1	Microsoft Windows	12	0
20.20.36.53	MS-W08R2-3U-1	Microsoft Windows	7	0
20.20.36.61	MS-W08R2-6U-1	Microsoft Windows	13	0
20.20.36.63	MS-W71-3U-1	Microsoft Windows	12	0
20.20.36.62	MS-W72-6U-1	Microsoft Windows	14	0
20.20.36.60	MS-W08R21-6U-1	Microsoft Windows	13	0
20.20.36.66	MS-W7-6U-1	Microsoft Windows	12	0
20.20.36.75	MS-W03S2-6U-1	Microsoft Windows	8	0
20.20.36.71	MS-WV15-6U-1	Microsoft Windows	12	0
20.20.36.67	MS-W08-3U-1	Microsoft Windows	11	0
20.20.36.73	ms-wsp-3u-1	Microsoft Windows	6	0
20.20.36.64	MS-W71-6U-1	Microsoft Windows	12	0
20.20.36.78	SAPGATEWAYWIN	Microsoft Windows	15	0
20.20.36.1	10.20.36.1	Linux	1	0
20.20.36.72	ms-wsp2-3u-1	Microsoft Windows	5	0

Friday 17 January 2014

Page 1 of 1

Sample Report

Чтобы скачать пример шаблона:

1. Откройте любой проект.

2. Перейдите в Reports > Show Reports во вкладке управления проектом. Откроется страница отчетов.
3. Пролистайте страницу до самого низа.
4. Кликните на активную ссылку «Скачать пример шаблона/Download Template Link» под таблицей с отчетами.

Saved Reports

Delete Standard Report Custom Report

Show 10 entries

☐	Name	Report Type	File Formats	Creator	Created	Last Updated	Actions
☐	AuthenticationTokens-20140311091720_clone	Authentication Tokens	None	tdoan	March 11, 2014 11:45 am	March 11, 2014 11:45 am	View Clone
☐	AuthenticationTokens-20140311091720_clone	Authentication Tokens	None	tdoan	March 11, 2014 11:45 am	March 11, 2014 11:45 am	View Clone
☐	AuthenticationTokens-20140311091720_clone	Authentication Tokens	PDF	tdoan	March 11, 2014 11:45 am	March 11, 2014 11:45 am	View Clone
☐	AuthenticationTokens-20140311091720	Authentication Tokens	PDF	tdoan	March 11, 2014 11:17 am	March 11, 2014 11:18 am	View Clone
☐	Audit-20140311091707	Audit	PDF	tdoan	March 11, 2014 11:17 am	March 11, 2014 11:17 am	View Clone
☐	Audit-20140310120033	Audit	PDF, HTML, RTF	TestUser	March 10, 2014 2:00 pm	March 11, 2014 11:22 am	View Clone

Showing 1 to 6 of 6 entries

Download example template | Download Jasper iReport

First Previous 1 Next Last

Процесс скачивания начнется автоматически. Если ваш браузер не настроен на автоматическую скачку файлов, появится диалоговое окно, где нужно будет подтвердить ваше желание скачать и запустить файл. Вам нужно будет сохранить шаблон на вашем компьютере.

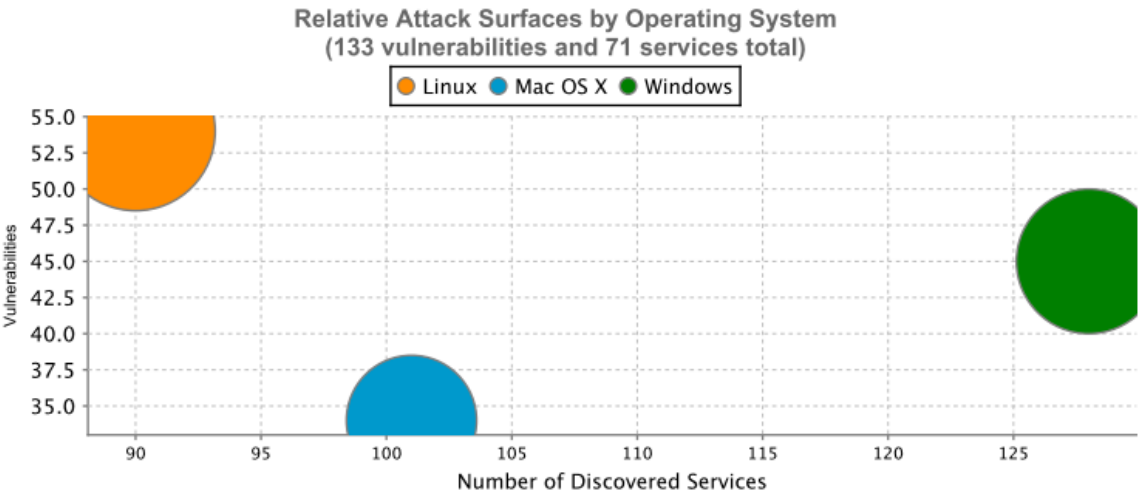
Отчеты по аудиту

Эта форма отчета используется для презентации собранных в проекте данных. Этот отчет будет полезным, если вам нужно получить детальную информацию о целевых хостах в проекте. Данные проекта разделены на две основные части: основные результаты и детализированные результаты.

Executive Summary

This report represents a security audit performed using Metasploit Pro from Rapid7, Inc. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

During this test, 30 hosts with a total of 71 exposed services were discovered. No modules were successfully run and 375 login credentials were obtained.

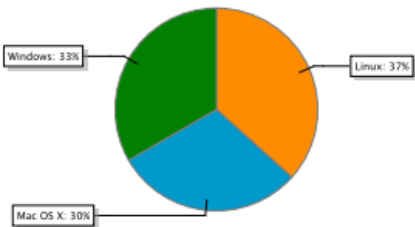


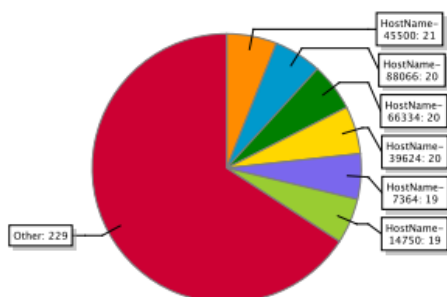
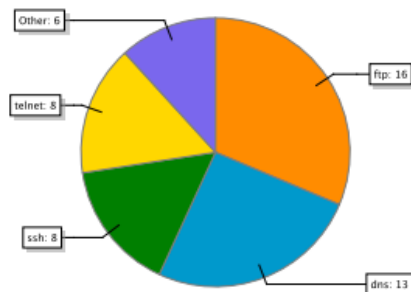
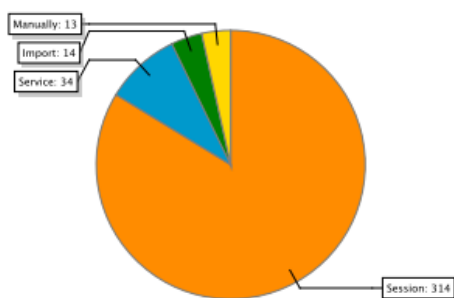
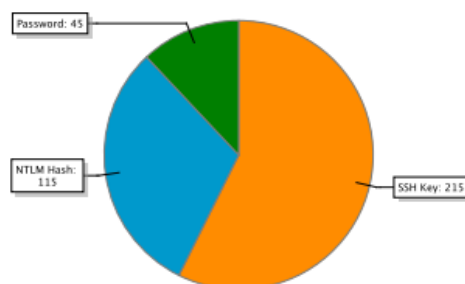
Major Findings

Discovered Operating Systems

Operating System	Hosts	Services	Vulnerabilities
Linux	11	90	54
Mac OS X	9	101	34
Windows	10	128	45

Host Frequency by OS (30 hosts total)



Credentials (375 total)**Credentials by Host****Credentials by Service****Credentials by Origin****Credentials by Type**

Основные результаты

В этой секции в виде таблиц и графиков отображены хост, операционная система и успешно собранные личные данные. Главной задачей этой секции является суммирование данных и идентификация критически важных данных в отчете.

Основные результаты содержат следующие виды данных:

- Потенциальные зоны для атак с учетом обнаруженных уязвимостей и сервисов на каждой операционной системе.
- Список хостов, сервисов и уязвимостей для каждой операционной системы.
- IP-адрес, имя, операционную систему, сервисы и уязвимости для каждого хоста в проекте.
- The публичные и приватные данные, тип области, источники, число хостов и служб для каждого типа личных данных, найденных в проекте. Все личные данные сгруппированы по типу. Это может быть пароль открытым текстом, NTLM хэш, non-replayable хэш или SSH ключ.
- Статистика по личным данным с сортировкой по хостам, источникам, сервисам и типам.

Детализированные результаты

В этой секции собраны подробные детали для каждого хоста в проекте. Сюда включаются следующие данные:

- Имена хостов, IP-адреса и все цели проекта.
- Детали личных данных, сохраненных в проекте, включая публичные (имена пользователей) и персональные (пароли), realm type, realm value, and origin.
- Открытые сервисы, обнаруженные на каждом хосте.
- Уязвимости, обнаруженные на каждом хосте.
- Веб уязвимости, обнаруженные на каждом хосте.
- Модули, которые смогли с успехом использовать уязвимости и начать сессию.
- Активность каждой сессии, включая информацию о том, когда они были начаты и закрыты, а также какие команды использовались при выполнении.

Опции для отчета по аудиту

Тип настроек	Опции
Форматы выгрузки	PDF, HTML, WORD, RTF
Опции отчетов	Скрыть обнаруженные личные данные – удаляет из отчета личные данные, включая пароли открытым текстом, хэши и SSH ключи. Включить данные сессии – показывает детали для каждой сессии, которую смог открыть Metasploit Pro, включая тип сессии и модуль, использованный для открытия сессии. Включить графики – включает в отчет круговые диаграммы и графики для отображения статистики данных, собранных в проекте.
Секции отчетов	Общая сводка Пораженные хосты Личные данные Обнаруженные операционные системы Обнаруженные хосты Детали хостов Обнаруженные сервисы Вебсайты

Отчет по личным данным

В этом отчете собраны личные данные, включая пароли открытым текстом, NTLM хэши, nonreplayable хэши и SSH ключи. Все данные отображены в одном отчете по личным данным. Он полезен в тех случаях, когда нужно получить полное представление о количестве личных данных в проекте в определенный момент времени и презентовать его в удобном виде (например, документ PDF).

Чтобы помочь вам разобраться с данными и найти ключевую информацию, в отчете организован следующие секции:

- Титульная страница
- Сводка по проекту
- Сводка по собранным личным данным
- Детали личных данных
- Логины
- Хосты
- Модули
-

Дополнительная информация

Сводка личных данных может быть представлена в виде круговой диаграммы для визуализации всей собранной информации. В диаграмме могут быть отображены следующие типы данных:

- Private Types – общее распределение приватной информации записей.
- Credential Origins - общее распределение источников записей в проекте.
- Хосты по логинам – общее распределение логинов среди хостов в проекте.
- Top Shared Credentials by Related Hosts – общее распределение учётных пар наиболее часто встречающихся у хостов.
- Логины по операционным системам – общее распределение логинов среди операционных систем.
- Логины по сервисам – общее распределение логинов по именам сервисов.

Детали личных данных

В этом разделе представлены подробные детали всех типов личных данных, собранных в проекте. Данные сгруппированы по типам: пароли открытым текстом, NTLM хэши, non-replayable хэши и SSH ключи. Каждый блок данных содержит следующие типы информации:

- Открытое значение
- Закрытое значение
- Тип области
- Ценность области
- Источник
- Число связанных хостов
- Число связанных служб

Детали логинов

В этом разделе показаны все логины, относящиеся к выбранным хостам, или логины, относящиеся ко всем хостам в рабочем пространстве, если определенные хосты не были выбраны. Каждый логин будет сопровожден информацией:

- Название сервиса
- Название хоста
- Дата создания логина
- Уровень доступа
- Публичная информация
- Персональная информация

Детали хостов

В этом разделе указан список хостов в проекте с хотя бы одним логином или типом личных данных. Каждый хост сопровождается следующими типами информации:

- Имя хоста
- IP-адрес хоста
- Дата добавления хоста
- Общее количество логинов для хоста
- Количество экземпляров личных данных, относящихся к хосту, от которого были получены логин, аутентификация сервиса или выгрузки сеанса.

Детали модулей

В этом разделе отображается информация касательно модулей, использованных для получения личных данных. Этот раздел разделен на две основные части: источники сеанса и источники служб.

Источники служб

Эта секция содержит список модулей, использованных для аутентификации в сервисах для получения личных данных. Эти личные данные обычно получены при помощи функций «Bruteforce Guess», «Credential Reuse» или «Get Session».

Каждый модуль сопровождается следующей информацией:

- Имя модуля
- Имя сервиса
- Количество логинов, относящихся к личным данным, добавленным модулем
- Время и дату добавления личных данных в проект. Они добавляются если аутентификация в сервисе была успешной.

Источники сеанса

Эта секция содержит список модулей, которые были использованы для открытия сессии и сбора личных данных с пораженных хостов.

Каждый модуль сопровождается следующей информацией:

- Имя модуля
- Дату и время открытия сессии
- Количество экземпляров личных данных, собранных модулем
- Количество логинов, относящихся к собранным личным данным, собранным модулем

Дополнительные данные.

Здесь приведены дополнительные детали отчета по личным данным. Например, список опций отчета, использованных для его создания и глоссарий с основными терминами.

Опции отчетов по личным данным

Тип настроек	Опции
Форматы выгрузки	PDF, HTML, WORD, RTF
Опции отчетов	Скрыть обнаруженные личные данные – удаляет из отчета личные данные, включая пароли открытым текстом, хэши и SSH ключи. Персональные данные замещаются словом *MASKED*.

	Включить графики – включает в отчет круговые диаграммы и графики для отображения статистики данных, собранных в проекте.
Секции отчетов	Титульная страница Общая сводка по проекту Сводка по личным деталям Пароли открытым текстом NLTМ хэши Не повторяющиеся хэши SSH ключи Детали логинов Детали хостов Детали модулей Источники служб Источники сеансов Дополнительные сведения: глоссарий Дополнительные сведения: использованные опции отчета

Отчет по соответствию нормам FISMA

Федеральный Акт по Контролю Безопасности Информации (FISMA) обеспечивает устойчивый фундамент, помогающий федеральным агентствам внедрять процессы и системы контроля, защищающие данные и информационные системы. Акт FISMA основан на наборе стандартов и рекомендаций от технологических агентств таких, как Национальный Институт Стандартов и Технологий (NIST). Эта организация разрабатывает стандарты и нормы типа Специальной Публикации 800-53 ревизия 4 (SP800-53r4), которые федеральные агентства могут использовать для разработки программ проверки соответствия нормам FISMA. Рекомендации, разработанные в NIST, определяют минимальные требования к менеджменту, контролю и ведению информационных систем.

Отчет по соответствию нормам FISMA помогает вам оценить, насколько организация следует определенным требованиям FISMA. Metasploit Pro сообщает о результатах проверки соответствия следующим требованиям к контролю над безопасностью:

- Контроль доступа/Access Control – AC7
- Бдительность и тренинги/Awareness and Training - AT-2
- Менеджмент конфигураций/Configuration Management - CM-7
- Идентификация и аутентификация/Identification and Authentication - IA-2, IA-5, and IA-7
- Оценка риска/Risk Assessment - RA-5
- Целостность систем и информации/System and Information Integrity - SI-2 and SI-10

Этот отчет представляет результаты в виде списка соответствий и несоответствий тем или иным нормам FISMA. Все результаты должны быть использованы в качестве дополнительных сведений к тестированию на соответствие нормам FISMA, но не в качестве результатов фактического аудита. Для получения дополнительной информации касательно требований FISMA, проверьте национальную базу данных уязвимостей: <http://web.nvd.nist.gov/view/800-53/Rev4>

Чтобы помочь вам быстрее найти необходимую информацию, отчет организован в виде двух основных секций:

- Общая сводка

- Детализация результатов

Общая сводка

Общая сводка содержит список соответствий и несоответствий каждому из требований FISMA, которые проверяются при помощи Metasploit Pro.

Детализация результатов

В этой секции представлены технические детали для каждого из требований FISMA, по которым Metasploit Pro составляет отчет. Отчет по соответствию нормам и требованиям FISMA перечисляет каждый хост, который не прошел по критериям каждого из требований.

Контроль доступа. FISMA AC-7

Этот норматив указывает максимальное количество неправильных попыток входа, совершенных пользователем. Норматив требует, чтобы этот показатель задавался каждой организацией на основе ее собственной политики безопасности. В этом отчете хост будет считаться непрошедшим тестирование, если он дает пользователям более 3 неудачных попыток на логин в течение 60 секунд.

Для каждого хоста, непрошедшего тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились попытки входа.
- Операционная система, используемая на хосте.
- Открытые и закрытые типы, ценность закрытых данных, тип источника и детали источника для всех личных данных, которые пробовали войти более 3 раз в течение 60 секунд.

Бдительность и тренинги. FISMA AT-2

Данный норматив требует, чтобы тренинги по повышению бдительности проводились для всех пользователей систем. Состав тренинговых программ разрабатывается организацией на основе ее потребностей и требований. Хосты будут считаться непрошедшим тест, если на нем обнаружены уязвимости, которые были успешно использованы.

Для каждого поста, непрошедшего тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились попытки входа
- Операционная система, используемая на хосте.
- Обнаруженная уязвимость.
- Модуль, использованный для атаки через уязвимость и время обнаружения уязвимости.

Менеджмент конфигураций. FISMA CM-7

Этот норматив требует, чтобы каждый хост имел одну главную функцию. Хост будет считаться непрошедшим тест, если на нем работает больше 1 основного сервиса (HTTP, HTTPS, DNS, FTP, MySQL, Postgres, DB2 и MSSQL). Исключением являются случаи, когда на хосте выполняются HTTP и HTTPS. Оба этих сервиса используются для поддержки приложений одновременно и могут работать вместе на одном и том же хосте.

Для каждого хоста, непрошедшего тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и имя хоста
- Операционная система, установленная на хосте
- Основные сервисы, выполняемые на хосте

Идентификация и аутентификация. FISMA - IA-2

Этот норматив требует, чтобы хосты идентифицировали и аутентифицировали только уникальных пользователей. Хост будет считаться непрошедшим тест, если он позволяет входить пользователям при помощи общепринятых имен пользователя (root, administrator, admin, tomcat, cisco, manager, SA, postgres или guest). Хост также будет считаться непрошедшим тест, если он запускает пользователей с незаполненным полем «Пароль».

Для каждого хоста, непрошедшего тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились попытки входа.
- Операционная система, используемая на хосте.
- Открытые и закрытые типы, ценность закрытых данных, тип источника и детали источника для всех личных данных, которые пробовали войти более 3 раз в течение 60 секунд.

Идентификация и аутентификация. FISMA - IA-5

Этот норматив требует, чтобы системные аутентификаторы (пароли и токены) правильно создавались, раздавались пользователям и контролировались. Эти требования позволяют удостовериться в том, что аутентификаторы не являются таковыми по умолчанию, а их создание сопровождается минимальными требованиями к созданию паролей. Хост будет считаться непрошедшим тест, если он позволяет входить пользователям при помощи общепринятых имен пользователя (root, administrator, admin, tomcat, cisco, manager, SA, postgres или guest). Хост также будет считаться непрошедшим тест, если он запускает пользователей с незаполненным полем «Пароль».

Для каждого хоста, непрошедшего тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились попытки входа.
- Операционная система, используемая на хосте.
- Открытые и закрытые типы, ценность закрытых данных, тип источника и детали источника для всех личных данных, которые пробовали войти более 3 раз в течение 60 секунд.

Идентификация и аутентификация. FISMA - IA-7

Этот норматив требует, чтобы механизмы аутентификации соответствовали современным требованиям к криптографии. Хост будет считаться непрошедшим тест, если на нем открыты и работают любые из следующих сервисов: telnet, shell, rhexec, rlogin или POP3. Хост также будет считаться непрошедшим тест, если на нем используется оборудование Cisco с работающим HTTP сервисом.

Для каждого хоста, непрошедшего тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились попытки входа.
- Операционная система, используемая на хосте.
- Основные сервисы, запущенные на хосте.

Оценка риска. FISMA RA-5

Этот норматив требует, чтобы тестирование на уязвимости проводилось регулярно. Хост будет считаться непрошедшим тест на соответствие, если на нем есть уязвимость, которая была успешно использована.

Для каждого хоста, непрошедшего тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились попытки входа.
- Операционная система, используемая на хосте.
- Уязвимость, которая была обнаружена.
- Модуль, который был использован для проникновения через уязвимость и время проникновения.

Целостность систем и информации. FISMA SI-2

Этот норматив требует, чтобы обо всех системах с обнаруженными уязвимостями и проблемами с безопасностью обязательно создавались отчеты. Все известные уязвимости должны быть исправлены при помощи последних обновлений от поставщика ПО. Хост будет считаться непрошедшим тест на соответствие, если на нем есть уязвимость, которая была успешно использована.

Для каждого хоста, непрошедшего тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились попытки входа.
- Операционная система, используемая на хосте.
- Уязвимость, которая была обнаружена.
- Модуль, который был использован для проникновения через уязвимость и время проникновения.

Целостность систем и информации. FISMA SI-10

Этот норматив требует, чтобы синтаксис и семантика при вводе в информационных системах соответствовала заданным значениям для форматов и содержимого. Хост будет считаться непрошедшим тест на соответствие, если на нем есть уязвимость, которая была успешно использована.

Для каждого хоста, непрошедшего тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились попытки входа.
- Операционная система, используемая на хосте.
- Уязвимость, которая была обнаружена.
- Модуль, который был использован для проникновения через уязвимость и время проникновения.

Опции отчета по соответствию нормам FISMA

Тип настроек	Опции
Форматы выгрузки	PDF, HTML, WORD, RTF
Опции отчетов	Скрыть обнаруженные личные данные – удаляет из отчета личные данные, включая пароли открытым текстом, хэши и SSH ключи. Персональные данные замещаются словом *MASKED*.
Секции отчетов	Общая сводка Детализация результатов

Отчет по соответствию нормам PCI

Данный отчет содержит информацию по собранным данным касательно соответствия систем безопасности нормам охраны безопасности данных в Индустрии Платежных Карт 2.0 (PCE-DSS 2.0), в которых перечислены все современные инструменты и измерения, позволяющие безопасно работать с данными обладателя карты. PCE-DSS 2.0 состоит из 12 основных требований, которые организованы в следующие группы:

1. Создание и техническая поддержка защищенной сети.
2. Защита персональных данных обладателей карт.
3. Поддержка программ менеджмента уязвимостей.
4. Внедрение усиленных мер контроля доступа.
5. Регулярные мониторинг и тестирование сетей.
6. Поддержка современных политик информационной безопасности.

Отчет по соответствию нормам PCI описывает уровень соответствия организации требованиям PCI-DSS по пунктам 1, 3 и 4. В отчете собрана информация по выбранному набору требований из каждого пункта. Отчет оценивает какие именно стандартные настройки вендора используются, как часто запрашиваются и используются последние патчи с обновлениями безопасности, а также то, насколько устойчивы к угрозам рекомендации по созданию сильных паролей и работе с пользователями. Отчет представлен в виде списка соответствий и несоответствий тем или иным требованиям PCI-DSS. Результаты тестирования должны быть использованы в качестве дополнительных сведений касательно тестирования на соответствие нормам PCI, но не в качестве результатов фактического тестирования.

Чтобы помочь вам быстрее найти необходимую информацию, отчет организован в нескольких секциях:

- Общая сводка.
- Сводка по соответствию требованиям.
- Сводка по состоянию хостов.
- Детализация результатов.

Общая сводка

Здесь представлено краткое содержание отчета.

Сводка по соответствию требованиям

В этом разделе представлен список соответствий и несоответствий требованиям PCI-DSS по следующим требованиям:

- 2.2.1 – Организация использует не более одной основной функции на отдельном сервере для предотвращения выполнения на одном сервере двух функций с разными уровнями безопасности.
- 2.3 – Организация шифрует административный доступ из неконсольных источников (браузеры и веб инструменты для менеджмента).
- 6.1. - Организация обеспечивает установку последних обновлений ПО, касающихся безопасности, для всех программных компонентов и программного обеспечения от всех поставщиков. Критически важные патчи устанавливаются в течение месяца после релиза.
- 8.2 – Организация использует хотя бы один из следующих методов аутентификации пользователей: пароль, секретное слово или двухфакторная аутентификация.
- 8.4 – Организация делает все пароли нечитаемыми для всех системных компонентов при хранении и передаче данных при помощи современных криптографических методов, соответствующим утвержденным стандартам.
- 8.5 – Организация использует правильное управление аутентификациями и паролями пользователей и администраторов на всех системных компонентах.
- 8.5.8 – Организация не использует групповые, переданные или простые пароли, аккаунты и другие методы аутентификации.

- 8.5.10 – Организация требует, чтобы минимальная длина пароля была не менее 7 символов.
- 8.5.11 – Организация требует, чтобы пароли содержали цифры и буквы алфавита.

Сводка по состоянию хостов

В этом разделе представлен список соответствий и несоответствий для каждого из хостов в проекте. Хост будет считаться прошедшим тест, если он соответствует всем требованиям PCS-DSS, которые проверяет Metasploit Pro. В ином случае он будет считаться непрошедшим тест.

Детализация результатов

В этом разделе представлены технические детали для каждого из требований PCS-DSS. Для каждого требования отчет составляет список хостов, которые не прошли отбор по критериям, установленным для каждого стандарта.

Требования PCI. 2.2.1

Этот норматив требует, чтобы на каждом хосте выполнялась только одна основная функция. Каждая отдельно взятая функция должна выполняться на отдельном сервере. В списке будут только те хосты, на которых выполняется больше одной функции, определяемой в качестве основного системного компонента.

Для каждого хоста, непрошедшего тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились попытки входа.
- Операционная система, используемая на хосте.
- Сервисы и порты, обнаруженные на хосте.

Требования PCI. 2.3

Этот норматив требует, чтобы все типы неконсольного административного доступа (Telnet и rlogin) были хорошо закодированы при помощи криптографии (SSH или SSL). В этой секции представлен список хостов, на которых не применяется шифровка данных или есть слушающий HTTP или оборудование Cisco.

Для каждого хоста, непрошедшего тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились попытки входа.
- Операционная система, используемая на хосте.
- Сервисы и порты, обнаруженные на хосте.

Требования PCI. 6.1

Этот норматив требует, чтобы все известные уязвимости были устранены при помощи последних обновлений от поставщиков оборудования. Эта секция отображает список хостов, на которых есть такие уязвимости.

Для каждого хоста, непрошедшего тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились попытки входа.
- Операционная система, используемая на хосте.
- Сервисы и порты, обнаруженные на хосте.

Требования PCI. 8.2

Эта секция отображает список хостов, на которых для аутентификации не используется пароль или двухфакторная аутентификация. Неудача в прохождении данного теста говорит о том, что целевой хост не использует пароли и секретные фразы для аутентификации.

Для каждого хоста, непрошедшего тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились попытки входа.
- Операционная система, используемая на хосте.
- Сервисы и порты, обнаруженные на хосте.
- Открытые и закрытые типы, ценность закрытых данных, тип источника и детали источника для всех личных данных.

Требования PCI. 8.4

Этот норматив требует, чтобы пароли хранились в зашифрованном виде. Эта секция отображает список хостов, на которых персональная информация используется для логина.

Для каждого хоста, непрошедшего тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились попытки входа.
- Операционная система, используемая на хосте.
- Сервисы и порты, обнаруженные на хосте.
- Открытые и закрытые типы, ценность закрытых данных, тип источника и детали источника для всех личных данных.

Требования PCI. 8.5.8

Этот норматив требует, чтобы в системах не использовались простые имена пользователей. Эта секция отображает личные данные, в которых содержится общие имена типа user, root, administrator, admin, tomcat, cisco, manager, sa, postgres или guest.

Для каждого набора личных данных, непрошедших тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились был осуществлен вход при помощи таких имен.
- Операционная система, используемая на хосте.
- Сервисы и порты, обнаруженные на хосте.
- Открытые и закрытые типы, ценность закрытых данных, тип источника и детали источника для всех личных данных.

Требования PCI. 8.5.10

Этот норматив требует, чтобы все пароли состояли из не менее чем 8 символов. Эта секция отображает пароли, в которых только 7 или менее символов.

Для каждого набора личных данных, непрошедших тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились был осуществлен вход при помощи таких имен.
- Операционная система, используемая на хосте.
- Сервисы и порты, обнаруженные на хосте.

- Открытые и закрытые типы, ценность закрытых данных, тип источника и детали источника для всех личных данных.

Требования PCI. 8.5.11

Этот норматив требует, чтобы все пароли состояли из цифр и букв алфавита. Эта секция отображает пароли, в которых нет цифр или букв.

Для каждого набора личных данных, непрошедших тест на соответствие, в секции будет предоставлена следующая информация:

- IP-адрес и название хоста, на котором производились был осуществлен вход при помощи таких имен.
- Операционная система, используемая на хосте.
- Сервисы и порты, обнаруженные на хосте.
- Открытые и закрытые типы, ценность закрытых данных, тип источника и детали источника для всех личных данных.

Опции отчета по нормам соответствия PCI

Тип настроек	Опции
Форматы загрузки	PDF, HTML, WORD, RTF
Опции отчетов	Скрыть обнаруженные личные данные – удаляет из отчета личные данные, включая пароли открытым текстом, хэши и SSH ключи. Персональные данные замещаются словом *MASKED*.
Секции отчетов	Общая сводка Сводка по соответствию требованиям Сводка по состоянию хостов Детализация результатов

Отчет мета-модуля Credentials Domino

Мета-модуль Credentials Domino производит итеративные атаки с использованием личных данных для определения наиболее уязвимых маршрутов атак при обнаружении личных данных, полученных во время открытой сессии от определенного хоста. Это позволяет вам идентифицировать цели, которые могут быть успешно атакованы, а также список дополнительных типов личных данных, которые можно получить при использовании уже собранных личных данных. Все результаты атак представлены в виде соответствующего отчета мета-модуля. Вы можете создать отчет, чтобы просмотреть все результаты в удобной форме (например, документ PDF).

Чтобы вам было проще найти необходимые данные, отчет организован в виде нескольких секций:

- Титульная страница
- Общая сводка
- Сводка по проекту
- Сводка по запускам
- Сводка по результатам
- Графики данных

- Успешно атакованные хосты повышенной значимости
- Неуспешно атакованные хосты повышенной значимости
- Все успешно атакованные хосты
- Все неуспешно атакованные хосты
- Дополнительные сведения

Общая сводка

В общей сводке приводится поверхностный обзор всех результатов работы мета-модуля, включая количество атакованных хостов, количество успешно атакованных хостов и количество успешно атакованных хостов повышенной значимости.

Сводка по проекту

В данном разделе указывается название проекта и имя пользователя, создавшего отчет.

Сводка по запускам

В этом разделе представлен список данных, собранных во время запусков мета-модуля Credentials Domino.

Сюда включены следующие данные:

- Время работы – общее время работы мета-модуля Credentials Domino.
- Итерации – количество циклов атак, произведенных при помощи мета-модуля Credentials Domino.
- Основной хост – хост с логином или сессией, которые использовал мета-модуль Credentials Domino для начала атаки.
- Входная точка – логин или сессия, которые использовал мета-модуль Credentials Domino для начала атаки.

Сводка по результатам

Здесь приведен обзор всех данных собранных при помощи мета-модуля Credentials Domino.

Сюда включены следующие данные:

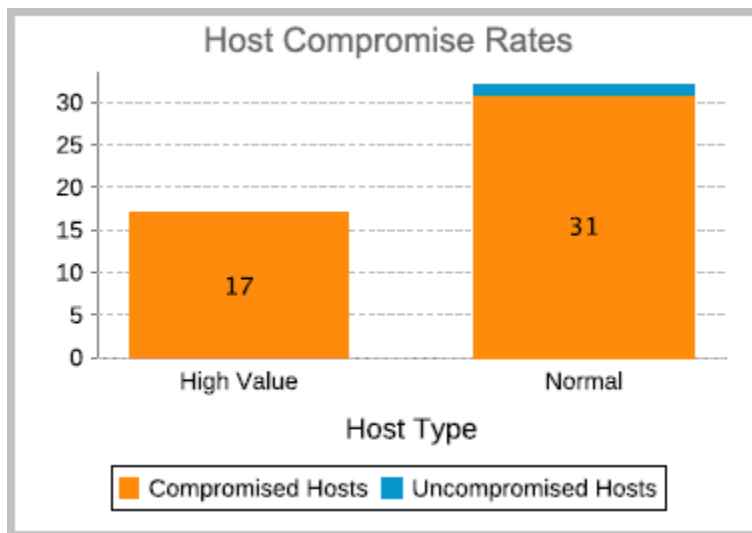
- Выбранные хосты – общее количество всех целевых хостов, выбранных для атаки.
- Хосты повышенной значимости – общее количество хостов повышенной важности, которые были атакованы.
- Собранные личные данные – общее количество экземпляров личных данных, собранных во время атаки.
- Успешно атакованные хосты – общее количество и процент хостов, на которых была успешно открыта сессия при проведении атаки.
- Успешно атакованные хосты повышенной значимости – общее количество и процент хостов повышенной значимости, на которых была открыта сессия при проведении атаки.

Графики данных

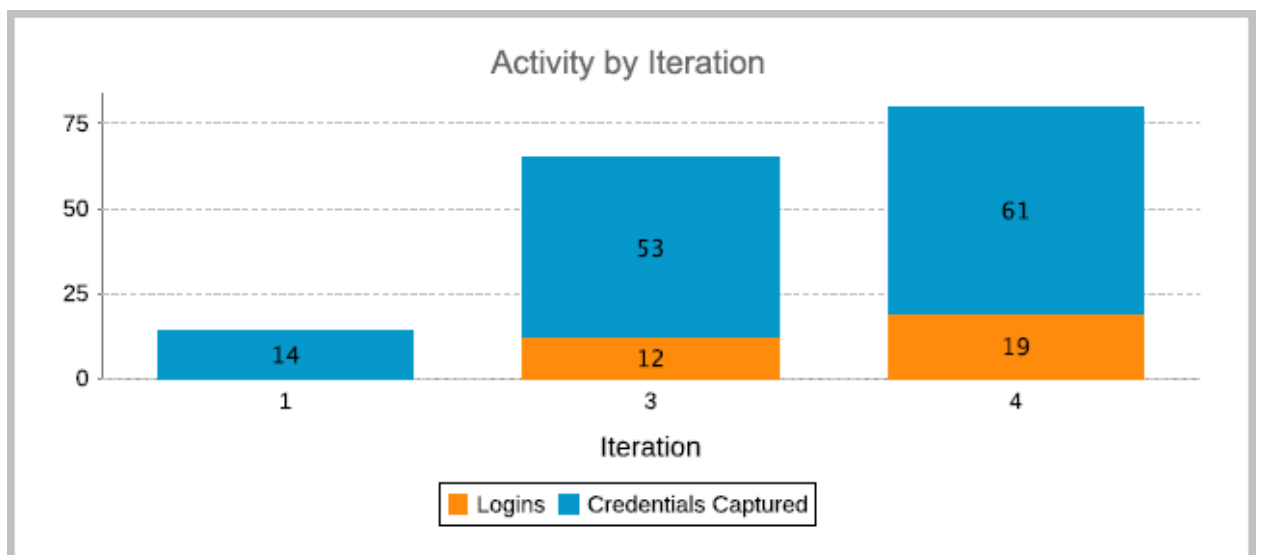
В этой секции в виде графиков представлена статистика: процент успешных атак на хосты и сервисы, а также активность во время каждого цикла атак.

Сюда входят следующие графики:

- Процент успеха – показывает соотношение хостов и хостов повышенной значимости, которые были успешно атакованы.



- Активность во время циклов атаки показывает общее количество входов и личных данных, захваченных во время каждого цикла атак.



Успешно атакованные хосты повышенной значимости

Это хосты, имеющие критическую важность для организации, это контроллеры доменов и серверы, на которых хранится ценная финансовая информация. Если вы определили такие хосты во время настройки мета-модуля Credentials Domino, то эти хосты будут включены в секцию хостов повышенной значимости и отмечены в отчете жирным красным тэгом. Эта секция представляет подробные данные для каждого хоста повышенной значимости, которые успешно атаковал мета-модуль.

Сюда включены следующие данные для каждого хоста:

- Имя хоста.
- IP-адрес хоста.
- Операционная система, используемая на хосте.
- Сервисы, подвергнутые атакам мета-модуля.
- Дата и время, когда мета-модуль получил доступ к цели.
- Общий объем захваченных личных данных.
- Цепь уязвимостей, в которой в хронологическом порядке перечислены хосты, использованные для получения доступа к этому хосту.

Неуспешно атакованные хосты повышенной значимости

В этой секции представлены подробные детали по хостам повышенной важности, на которых мета-модуль не смог открыть сессию.

Сюда включены следующие данные:

- Имя хоста.
- IP-адрес хоста.
- Операционная система, используемая на хосте.
- Дата и время, когда мета-модуль попытался атаковать цель.

Все успешно атакованные хосты

В этом разделе перечислены все хосты, которые мета-модуль смог успешно атаковать, чтобы заполнить личные данные для входа.

Сюда включены следующие данные:

- Имя хоста.
- IP-адрес хоста.
- Операционная система, используемая на хосте.
- Сервисы, подвергнутые атакам мета-модуля.
- Общий объем захваченных личных данных.
- Является ли он хостом повышенной значимости.

Все неуспешно атакованные хосты

В этом разделе перечислены все хосты, на которых мета-модулю не удалось открыть сессию.

Сюда включены следующие данные:

- Имя хоста.
- IP-адрес хоста.
- Операционная система, используемая на хосте.
- Сервисы, подвергнутые атакам мета-модуля.
- Время и даты, когда мета-модуль пытался провести атаку.
- Является ли он хостом повышенной значимости.

Дополнительные сведения

В этом разделе представлены дополнительные детали касательно отчета по работе мета-модуля Credentials Domino.

Опции отчета по работе Мета-модуля Credentials Domino

Тип настроек	Опции
Форматы выгрузки	PDF, HTML, WORD, RTF
Опции отчетов	Включить графики – включает в отчет круговые диаграммы и графики для отображения статистики данных, собранных в проекте.
Секции отчетов	Титульная страница Общая сводка Сводка по проекту Сводка по запускам Сводка по результатам Графики данных Успешно атакованные хосты повышенной значимости

	Неуспешно атакованные хосты повышенной значимости Все успешно атакованные хосты Все неуспешно атакованные хосты Дополнительные сведения
Настройки мета-модуля	Перечень всех настроек, использованных для запуска мета-модуля, включая: Максимальное число циклов Общее время ожидания Время ожидания на каждый сервис Включенные хосты Исключенные хосты Хосты повышенной значимости

Отчёт вторжения по **узнанным** учётным данным

В данном отчете представлены результаты использования всех полученных в проекте личных данных при атаках целевых хостов и сервисов.

Чтобы вам было проще найти необходимую информацию, отчет организован в виде нескольких секций:

- Сводка по проекту.
- Сводка по результатам.
- Графики с данными о сервисах и хостах, к которым был получен доступ.
- Детализированные данные о сервисах и хостах, к которым был получен доступ.
- Дополнительные сведения.

Сводка по проекту

В этом разделе показаны название проекта и пользователь, который создал отчет.

Сводка по результатам

В данном разделе перечислены следующие виды данных:

- Мета-модуль – запущенный мета-модуль.
- Время работы – общее время работы мета-модуля.
- Выбранные хосты – общее количество хостов, определенных в качестве целей для мета-модуля.
- Проверенные хосты – общее количество хостов, которые мета-модуль пытался атаковать.
- Сессий открыто – общее количество сессий, которые мета-модуль смог открыть на всех целевых хостах.

Графики с данными о сервисах и хостах, к которым был получен доступ

В этом разделе отображены в виде круговых диаграмм данные по 5 наиболее уязвимым хостам, на которых мета-модуль смог открыть сессию.

На изображении показан пример графика с данными о сервисах и хостах, к которым был получен доступ.

Детализированные данные о сервисах и хостах, к которым был получен доступ

В этом разделе перечислены технические детали по каждому из целевых хостов, на которых мета-модулю удалось открыть сессию. Отчет упорядочивает цели по имени хоста и перечисляет информацию о сессиях для каждого хоста.

Каждый хост сопровождается следующими данными:

- Время и дата добавления хоста в проект.
- Тип сессии, открытой между Metasploit и целью.
- Время и дата открытия сессии.
- Время и дата закрытия сессии.

Дополнительные сведения

В этом разделе представлены детали отчета Known Credentials Intrusion.

Опции отчета

Тип настроек	Опции
Форматы выгрузки	PDF, HTML, WORD, RTF
Опции отчетов	Скрыть обнаруженные личные данные – удаляет из отчета личные данные, включая пароли открытым текстом, хэши и SSH ключи. Персональные данные замещаются словом *MASKED*. Включить графики – включает в отчет круговые диаграммы и графики для отображения статистики данных, собранных в проекте.
Секции отчетов	Сводка по проекту Сводка по результатам Графики с данными о сервисах и хостах, к которым был получен доступ Детализированные данные о сервисах и хостах, к которым был получен доступ Дополнительные сведения
Выбранные сервисы	Список всех сервисов, к которым пытался подключиться мета-модуль.

Отчет по работе мета-модуля Single Password Testing

Данный отчет представляет результаты от использования определенного имени пользователя и простого пароля против целевых хостов и сервисов. В сводке отчета отображен график, демонстрирующий 5 наиболее уязвимых хостов и сервисом, к которым удалось подключиться. В отчет также включены технические детали по каждому целевому хосту, которые были успешно атакованы при помощи имени пользователя и пароля.

Чтобы вам было проще найти необходимые данные, отчет организован в виде следующих секций:

- Сводка по проекту
- Сводка по результатам
- Графики с данными о сервисах и хостах, к которым был получен доступ.
- Детализированные данные о сервисах и хостах, к которым был получен доступ.
- Дополнительные сведения.

Сводка по проекту

В этом разделе показаны название проекта и пользователь, который создал отчет.

Сводка по результатам

В данном разделе перечислены следующие виды данных:

- Мета-модуль – запущенный мета-модуль.
- Время работы – общее время работы мета-модуля.

- Выбранные имена пользователей – имена пользователей, при помощи которых мета-модуль пытался аутентифицироваться.
- Выбранные пароли – пароли, при помощи которых мета-модуль пытался аутентифицироваться.
- Выбранные хосты – общее количество хостов, определенных в качестве целей для мета-модуля.
- Выбранные личные данные – общее количество экземпляров личных данных, использованных при запуске мета-модуля.
- Успешные логины – количество успешных аутентификаций, выполненных модулем.

Графики с данными о сервисах и хостах, к которым был получен доступ

В этом разделе отображены в виде круговых диаграмм данные по 5 наиболее уязвимым хостам, на которых мета-модуль смог открыть сессию, а также 5 наиболее уязвимых сервисов, где мета-модуль умел залогиниться при помощи выбранных имен пользователей и паролей.

На изображении показан пример графика с данными о сервисах и хостах, к которым был получен доступ.

Детализированные данные о сервисах и хостах, к которым был получен доступ

В этом разделе перечислены технические детали по каждому из целевых хостов, на которых мета-модулю удалось открыть сессию при помощи выбранных имен пользователей и паролей. Цели упорядочены по имени. Для каждого хоста также указывается сервис, в котором успешно аутентифицировался мета-модуль.

Каждый хост сопровождается следующими данными:

- Номер порта
- Протокол
- Имя сервиса
- Время и дата попытки логина
- Результат логина
- Уровень доступа для логина

Дополнительные сведения

В этом разделе представлены детали отчета для мета-модуля Single Password Testing.

Опции отчета по работе мета-модуля Single Password Testing

Тип настроек	Опции
Форматы загрузки	PDF, HTML, WORD, RTF
Опции отчетов	Скрыть обнаруженные личные данные – удаляет из отчета личные данные, включая пароли открытым текстом, хэши и SSH ключи. Персональные данные замещаются словом *MASKED*. Включить графики – включает в отчет круговые диаграммы и графики для отображения статистики данных, собранных в проекте.
Секции отчетов	Сводка по проекту Сводка по результатам Графики с данными о сервисах и хостах, к которым был получен доступ Детализированные данные о сервисах и хостах, к которым был получен доступ Дополнительные сведения

Выбранные сервисы	Список всех сервисов, к которым пытался подключиться мета-модуль.
-------------------	---

Отчет по работе мета-модуля SSH Key Testing

Данный отчет представляет результаты использования определенного имени пользователя и SSH ключа против выбранных хостов и сервисов. В сводке отчета есть графики, показывающие 5 наиболее уязвимых хостов и сервисов, в которых успешно аутентифицировался мета-модуль при помощи имени пользователя и SSH ключа. В отчет также включены технические данные для каждого целевого хоста, на котором удалось использовать имя пользователя и SSh ключ.

Чтобы вам было проще найти необходимые данные, отчет организован в виде следующих секций:

- Сводка по проекту
- Сводка по результатам
- Графики с данными о сервисах и хостах, к которым был получен доступ.
- Детализированные данные о сервисах и хостах, к которым был получен доступ.
- Дополнительные сведения.

Сводка по проекту

В этом разделе показаны название проекта и пользователь, который создал отчет.

Сводка по результатам

В данном разделе перечислены следующие виды данных:

- Мета-модуль – запущенный мета-модуль.
- Время работы – общее время работы мета-модуля.
- Выбранные имена пользователей – имена пользователей, при помощи которых мета-модуль пытался аутентифицироваться.
- Выбранные SSH ключи – SSH ключи, при помощи которых мета-модуль пытался аутентифицироваться.
- Выбранные хосты – общее количество хостов, определенных в качестве целей для мета-модуля.
- Выбранные сервисы – общее количество сервисов, определенных в качестве целей для мета-модуля.
- Проверенные хосты – общее количество хостов, в которых пытался аутентифицироваться мета-модуль.
- Проверенные сервисы – общее количество сервисов, в которых пытался аутентифицироваться мета-модуль.
- Успешные логины – количество успешных аутентификаций, выполненных модулем.

Графики с данными о сервисах и хостах, к которым был получен доступ

В этом разделе отображены в виде круговых диаграмм данные по 5 наиболее уязвимым хостам, на которых мета-модуль смог открыть сессию, а также 5 наиболее уязвимых сервисов, где мета-модуль умел залогиниться при помощи выбранных имен пользователей и SSH ключей.

На изображении показан пример графика с данными о сервисах и хостах, к которым был получен доступ.

Детализированные данные о сервисах и хостах, к которым был получен доступ

В этом разделе перечислены технические детали по каждому из целевых хостов, на которых мета-модулю удалось открыть сессию при помощи выбранных имен пользователей и SSH ключей. Цели

упорядочены по имени. Для каждого хоста также указывается сервис, в котором успешно аутентифицировался мета-модуль.

Каждый хост сопровождается следующими данными:

- Номер порта
- Протокол
- Имя сервиса
- Время и дата попытки логина
- Результат логина
- Уровень доступа для логина

Дополнительные сведения

В этом разделе представлены детали отчета для мета-модуля Single Password Testing.

Опции отчета по работе мета-модуля SSH Key Testing

Тип настроек	Опции
Форматы выгрузки	PDF, HTML, WORD, RTF
Опции отчетов	Скрыть обнаруженные личные данные – удаляет из отчета личные данные, включая пароли открытым текстом, хэши и SSH ключи. Персональные данные замещаются словом *MASKED*. Включить графики – включает в отчет круговые диаграммы и графики для отображения статистики данных, собранных в проекте.
Секции отчетов	Сводка по проекту Сводка по результатам Графики с данными о сервисах и хостах, к которым был получен доступ Детализированные данные о сервисах и хостах, к которым был получен доступ Дополнительные сведения
Выбранные сервисы	Список всех сервисов, к которым пытался подключиться мета-модуль.

Отчет по прохождению хэшей

Данный отчет представляет результаты использования определенного имени пользователя и хэша против целевых хостов и сервисов. В сводке отчета есть графики, показывающие 5 наиболее уязвимых хостов и сервисов, в которых успешно аутентифицировался мета-модуль при помощи имени пользователя и хэша. В отчет также включены технические данные для каждого целевого хоста, на котором удалось использовать имя пользователя и хэш.

Чтобы вам было проще найти необходимые данные, отчет организован в виде следующих секций:

- Сводка по проекту
- Сводка по результатам
- Графики с данными о сервисах и хостах, к которым был получен доступ.
- Детализированные данные о сервисах и хостах, к которым был получен доступ.
- Дополнительные сведения.

Сводка по проекту

В этом разделе показаны название проекта и пользователь, который создал отчет.

Сводка по результатам

В данном разделе перечислены следующие виды данных:

- Мета-модуль – запущенный мета-модуль.
- Время работы – общее время работы мета-модуля.
- Выбранные имена пользователей – имена пользователей, при помощи которых мета-модуль пытался аутентифицироваться.
- Выбранные NLTМ хэши – NLTМ хэши, при помощи которых мета-модуль пытался аутентифицироваться.
- Выбранные хосты – общее количество хостов, определенных в качестве целей для мета-модуля.
- Выбранные сервисы – общее количество сервисов, определенных в качестве целей для мета-модуля.
- Проверенные хосты – общее количество хостов, в которых пытался аутентифицироваться мета-модуль.
- Проверенные сервисы – общее количество сервисов, в которых пытался аутентифицироваться мета-модуль.
- Успешные логины – количество успешных аутентификаций, выполненных модулем.

Графики с данными о сервисах и хостах, к которым был получен доступ

В этом разделе отображены в виде круговых диаграмм данные по 5 наиболее уязвимым хостам, на которых мета-модуль смог открыть сессию, а также 5 наиболее уязвимых сервисов, где мета-модуль умел залогиниться при помощи выбранных имен пользователей и хэша.

На изображении показан пример графика с данными о сервисах и хостах, к которым был получен доступ.

Детализированные данные о сервисах и хостах, к которым был получен доступ

В этом разделе перечислены технические детали по каждому из целевых хостов, на которых мета-модулю удалось открыть сессию при помощи выбранных имен пользователей и хэша. Цели упорядочены по имени. Для каждого хоста также указывается сервис, в котором успешно аутентифицировался мета-модуль.

Каждый хост сопровождается следующими данными:

- Номер порта
- Протокол
- Имя сервиса
- Время и дата попытки логина
- Результат логина
- Уровень доступа для логина

Дополнительные сведения

В этом разделе представлены детали отчета для мета-модуля Pass the Hash.

Опции отчета по работе мета-модуля Pass the Hash

Тип настроек	Опции
Форматы выгрузки	PDF, HTML, WORD, RTF

Опции отчетов	Скрыть обнаруженные личные данные – удаляет из отчета личные данные, включая пароли открытым текстом, хэши и SSH ключи. Персональные данные замещаются словом *MASKED*. Включить графики – включает в отчет круговые диаграммы и графики для отображения статистики данных, собранных в проекте.
Секции отчетов	Сводка по проекту Сводка по результатам Графики с данными о сервисах и хостах, к которым был получен доступ Детализированные данные о сервисах и хостах, к которым был получен доступ Дополнительные сведения
Выбранные сервисы	Список всех сервисов, к которым пытался подключиться мета-модуль.