Список всех модулей CrackMapExec

spy-soft.net/crackmapexec-modules-library

8 июня 2024 г.

Мы уже рассказывали, как установить и использовать CrackMapExec на Kali Linux. В этой статье вы найдете полный список всех модулей CrackMapExec, доступных в последней публичной версии этого отличного инструмента, который используется для пентеста в локальных сетях.

Еще по теме: Пример атак Kerberoasting и AS-REP Roasting

CrackMapExec (или CME) включает в себя множество модулей, что делает этот инструмент столь полезным. Надеюсь, этот список поможет ориентироваться среди всех модулей.

Модули CrackMapExec

В последней версии CME имеется всего 68 модулей. Все эти модули относятся к категории постэксплуатации, дополняя мощные возможности CME по перебору паролей и атаке методом распыления паролей. На этой странице, однако, вы найдете информацию только о модулях.

Ниже вы найдете список модулей CME, доступных при использовании инструмента. CME в настоящее время поддерживает следующие сетевые протоколы:

- LDAP (порт 389 или 636) — 5 модулей
- MSSQK(порт 1433) — 23 модуля
- SMB (порт 135, 139 или 445) — 39 модулей
- SSH (порт 22) — 1 модуль
- WinRM (порт 5985 или 5986) — 0 модулей

Модули CME LDAP

Вот список всех модулей CrackMapExec, которые могут использоваться с протоколом LDAP:

```
# cme ldap -L
[*] MAQ                  Извлекает атрибут MachineAccountQuota на уровне домена
[*] adcs                 Находит службы регистрации PKI в Active Directory
[*] get-desc-users       Получает описание пользователей. Может содержать пароли
[*] laps                 Извлекает пароли LAPS
[*] user-desc            Получает описания пользователей, хранящиеся в Active Directory
```

Модули CME MSSQL

Вот список всех модулей CrackMapExec, которые могут использоваться с протоколом MSSQL:

```
#cme mssql -L
[*] Get-ComputerDetails       Перечисляет информацию о системе
[*] empire_exec               Использует RESTful API Empire для создания
запускающего механизма для указанного слушателя и выполняет его
[*] enum_chrome               Расшифровывает сохраненные пароли Chrome с
помощью Get-ChromeDump
[*] get_keystrokes            Логирует нажатия клавиш, время и активное окно
[*] get_netdomaincontroller   Перечисляет все контроллеры домена
[*] get_netrdpsession         Перечисляет все активные сеансы RDP
[*] get_timedscreenshot       Делает скриншоты через регулярные интервалы
[*] invoke_sessiongopher      Извлекает сохраненную информацию о сеансах
для PuTTY, WinSCP, FileZilla, SuperPuTTY и RDP с помощью SessionGopher
[*] invoke_vnc                Внедряет клиент VNC в память
[*] met_inject                Загружает stager Meterpreter и внедряет его в память
[*] mimikatz                  Извлекает все логин-пароли из памяти
[*] mimikatz_enum_chrome      Расшифровывает сохраненные пароли Chrome
с помощью Mimikatz
[*] mimikatz_enum_vault_creds Расшифровывает сохраненные учетные
данные в Windows Vault/Credential Manager
[*] mimikittenz               Выполняет Mimikittenz
[*] mssql_priv                Перечисляет и эксплуатирует привилегии MSSQL
[*] multirdp                  Патчит терминальные службы в памяти для разрешения
нескольких пользователей RDP
[*] netripper                 Захватывает учетные данные с помощью API-хука
[*] pe_inject                 Загружает указанный DLL/EXE и внедряет его в память
[*] rid_hijack                Выполняет перехват RID для установки постоянного
присутствия
[*] shellcode_inject          Загружает указанный raw shellcode и внедряет его в
память
[*] test_connection           Пингует хост
[*] tokens                    Перечисляет доступные токены
[*] web_delivery              Запускает нагрузку Metasploit с использованием
модуля exploit/multi/script/web_delivery
```

Модули CME SMB

Вот список всех модулей CrackMapExec, которые могут использоваться с протоколом SMB:

```
#cme smb -L
[*] Get-ComputerDetails       Перечисляет информацию о системе
[*] bh_owned                  Устанавливает скомпрометированный компьютер как
принадлежащий Bloodhound
[*] bloodhound                Выполняет сценарий разведки BloodHound на цели и
возвращает результаты на машину атакующего
[*] empire_exec               Использует RESTful API Empire для создания
запускающего механизма для указанного слушателя и выполняет его
[*] enum_avproducts           Собирает информацию о всех решениях защиты
конечных точек, установленных на удаленном хосте(ах) через WMI
[*] enum_chrome               Расшифровывает сохраненные пароли Chrome с
помощью Get-ChromeDump
[*] enum_dns                  Использует WMI для дампа DNS с сервера DNS AD
```

```
[*] get_keystrokes           Логирует нажатия клавиш, время и активное окно
[*] get_netdomaincontroller  Перечисляет все контроллеры домена
[*] get_netrdpsession        Перечисляет все активные сеансы RDP
[*] get_timedscreenshot      Делает скриншоты через регулярные интервалы
[*] gpp_autologin            Ищет информацию о автологоне в файле registry.xml
на контроллере домена и возвращает имя пользователя и пароль.
[*] gpp_password             Извлекает текстовый пароль и другую информацию
для учетных записей, настроенных через Preferences Group Policy.
[*] invoke_sessiongopher     Извлекает сохраненную информацию о сеансах
для PuTTY, WinSCP, FileZilla, SuperPuTTY и RDP с помощью SessionGopher
[*] invoke_vnc               Внедряет клиент VNC в память
[*] lsassy                   Дампит lsass и парсит результат удаленно с помощью
lsassy
[*] met_inject               Загружает stager Meterpreter и внедряет его в память
[*] mimikatz                 Извлекает все логин-пароли из памяти
[*] mimikatz_enum_chrome     Расшифровывает сохраненные пароли Chrome
с помощью Mimikatz
[*] mimikatz_enum_vault_creds Расшифровывает сохраненные учетные
данные в Windows Vault/Credential Manager
[*] mimikittenz              Выполняет Mimikittenz
[*] multirdp                 Патчит терминальные службы в памяти для разрешения
нескольких пользователей RDP
[*] netripper                Захватывает учетные данные с помощью API-хука
[*] pe_inject                Загружает указанный DLL/EXE и внедряет его в память
[*] rdp                      Включает/выключает RDP
[*] rid_hijack               Выполняет перехват RID для установки постоянного
присутствия
[*] runasppl                 Проверяет, установлен ли реестровый ключ RunAsPPL
[*] scuffy                   Создает и дампит произвольный файл .scf с атрибутом
иконки, содержащим путь UNC к указанному серверу SMB для всех
записываемых долей
[*] shellcode_inject         Загружает указанный raw shellcode и внедряет его в
память
[*] slinky                   Создает ярлыки Windows с атрибутом иконки,
содержащим путь UNC к указанному серверу SMB для всех записываемых
долей
[*] spider_plus              Список файлов на целевом сервере (исключая `DIR`
директории и `EXT` расширения) и сохранение их в `OUTPUT` директорию,
если они меньше `SIZE`
[*] spooler                  Определяет, включен ли принт-спулер или нет
[*] test_connection          Пингует хост
[*] tokens                   Перечисляет доступные токены
[*] uac                      Проверяет статус UAC
[*] wdigest                  Создает/удаляет реестровый ключ 'UseLogonCredential',
разрешающий дампинг учетных данных WDigest на Windows >= 8.1
[*] web_delivery             Запускает нагрузку Metasploit с использованием
модуля exploit/multi/script/web_delivery
[*] webdav                   Проверяет, запущен ли сервис WebClient на цели
[*] wireless                 Получает ключ всех беспроводных интерфейсов
```

Модули CME SSH

Вот список всех модулей CrackMapExec, которые могут использоваться с протоколом SSH:

```
# cme ssh -L
[*] mimipenguin дампит учетные данные в памяти в открытом виде
```

Модули CME WinRM

Вот список всех модулей CrackMapExec, которые могут использоваться с протоколом WinRM:

```
# cme winrm -L
```

Как видите, на данный момент модулей нет.

Заключение

CrackMapExec — это все еще активно поддерживаемый проект с потенциальными новыми функциями и модулями в будущем. Я постараюсь обновлять эту статью, но если вы найдете что-то, чего не хватает, пожалуйста, не оставьте комментарий ниже.

ПОЛЕЗНЫЕ ССЫЛКИ:

- Информации об учетных записях и SMB в CrackMapExec
- Извлечение паролей из дампа памяти используя MimiPenguin