1. Objective

The objective of this reconnaissance activity was to identify exposed services, enumerate available assets, and document the attack surface of the target machine using passive and active information-gathering techniques.

2. Tools Used

- Nmap
- Shodan (theoretical OSINT reference)
- Maltego (asset mapping simulation)

3. Domain / Target Information

Target Name: Metasploitable 2
IP Address: 10.33.226.229
Operating System (Detected): Linux (Ubuntu-based)

Since the target is an internal IP, WHOIS and public DNS information were not applicable.

```
┌──(gyanesh㉿kali)-[~/cyart]
└─$ sudo nmap 10.33.226.229 -O
[sudo] password for gyanesh:
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-12 21:03 +0530
Nmap scan report for 10.33.226.229
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:73:BA:83 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.49 seconds
```

4. Subdomain Enumeration

Because the target is an IP-based lab system without a registered domain name, no DNS records or subdomains were identified.

Commands executed:

nslookup 10.33.226.229

Result:

- No domain name associated
- No DNS entries found

5. Exposed Services Identification

An Nmap service/version scan was performed:

nmap -sS -sV -O 10.33.226.229

Identified Open Ports:

Port	Service	Version	Risk Level
21	FTP	vsftpd 2.3.4	Critical
22	SSH	OpenSSH 4.7p1 Debian 8ubuntu1	Medium
23	Telnet	Linux telnetd	High
25	SMTP	Postfix smtpd	Medium
53	DNS	ISC BIND 9.4.2	Medium
80	HTTP	Apache httpd 2.2.8 (Ubuntu)	High
111	RPCBind	rpcbind 2	Medium
139	SMB	Samba smbd 3.X – 4.X	High
445	SMB	Samba smbd 3.X – 4.X	High
512	RSH	netkit-rsh rexecd	High
513	Rlogin	rlogind	High
514	TCPWrapped	Unknown	Medium
1099	Java RMI	GNU Classpath grmiregistry	High
1524	Bind Shell	Metasploitable root shell	Critical
2049	NFS	NFS v2-4	High
2121	FTP	ProFTPD 1.3.1	High

Port	Service	Version	Risk Level
3306	MySQL	MySQL 5.0.51a-3ubuntu5	High
5432	PostgreSQL	PostgreSQL 8.3.0 – 8.3.7	High
5900	VNC	VNC protocol 3.3	High
6000	X11	Access denied	Medium
6667	IRC	UnrealIRCd	Critical
8009	AJP13	Apache JServ Protocol v1.3	High
8180	HTTP	Apache Tomcat/Coyote JSP engine 1.1	High

Observations:

- Multiple outdated services detected
- Telnet enabled (insecure protocol)
- FTP version vulnerable to backdoor exploit
- Database services exposed

6. Web Service Reconnaissance

The web server was accessed via:

http://10.33.226.229

Observed:

- Apache default page
- Vulnerable web applications (DVWA, Mutillidae)
- Test directories

7. Asset Mapping Log

Timestamp | Tool | Finding

---|---|---

2026-02-12 12:00:00 | Ping | Host reachable

2026-02-12 12:05:00 | Nmap | Multiple ports open

2026-02-12 12:10:00 | Browser | Apache web server accessible

2026-02-12 12:15:00 | Nmap -O | Linux OS detected

8. Reconnaissance Checklist

- ☑ Host availability check
- ☑ Service discovery (Nmap)
- ☑ OS detection
- ☑ Web service enumeration
- ☑ Documentation of findings
- ☑ Attack surface identification

Word Recon Summary

The reconnaissance phase revealed multiple exposed services including FTP, SSH, Telnet, HTTP, and database ports on the Metasploitable 2 system. Several outdated and insecure services significantly increased the attack surface. Web applications and database services were publicly accessible, indicating high exploitation potential within the internal lab environment.