

# Nmap Scan Report

## Environment Summary

| Attribute       | Details                          |
|-----------------|----------------------------------|
| Scan Date       | 23 October 2025                  |
| Scan Tool       | Nmap v7.94 (Kali Linux)          |
| Attacker System | Kali Linux (192.168.56.101)      |
| Target System   | Metasploitable2 (192.168.56.102) |
| Network Mode    | VirtualBox Host-Only Adapter     |
| MAC Address     | 08:00:27:4C:8F:8C (Oracle Corp)  |

## Reconnaissance Summary:

Reconnaissance is the first phase of a security assessment, used to gather information about the target system before active scanning. It is divided into Passive and Active technique.

### 1. Passive Reconnaissance

- Tools Used: whois, nslookup, Google Dorking, Shodan
- Purpose: Collect information without directly interacting with the target
- Execution & Findings:
  - whois: Not applicable for private IP (192.168.56.102) — no public registration
  - nslookup 192.168.56.102: No DNS records found (expected in isolated lab setup)
  - Google Dorking: Not applicable — target is not publicly hosted
  - Shodan: No results — target IP is private and not indexed

> Note: Passive recon confirmed that the target is an internal lab system with no public exposure.

### 2. Active Reconnaissance

- Tools Used: nmap -sn, telnet, nc (netcat)
- Purpose: Interact with the target to confirm host status and identify services
- Execution & Findings:

> Active recon validated the target's availability and revealed service banners useful for vulnerability mapping.

```
kali@kali: ~  
Session Actions Edit View Help  
[kali@kali]~  
$ nmap -sn 192.168.56.102  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 13:00 EDT  
Nmap scan report for 192.168.56.102  
Host is up (0.0018s latency).  
MAC Address: 08:00:27:4C:8F:8C (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)  
Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds  
[kali@kali]~  
$ telnet 192.168.56.102  
Trying 192.168.56.102 ...  
Connected to 192.168.56.102.  
Escape character is '^['.  
  
metasploit  
  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started
```

## 🔍 Scan Breakdown

### 1. TCP SYN Scan (-sS)

- Command: `nmap -sS 192.168.56.102`
- Purpose: Stealth scan using raw packets (requires root)
- Findings:

```
Session Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
[kali@kali]~  
$ nmap -sS 192.168.56.102  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 11:57 EDT  
Nmap scan report for 192.168.56.102  
Host is up (0.0013s 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
```

```
Session Actions Edit View Help  
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  
MAC Address: 08:00:27:4C:8F:8C (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)  
Nmap done: 1 IP address (1 host up) scanned in 13.67 seconds  
[kali@kali]~  
$
```

### 2. TCP Connect Scan (-sT)

- Command: `nmap -sT 192.168.56.102`
- Purpose: Full TCP connection (used when not root)
- Findings:

```
kali@kali: ~  
Session Actions Edit View Help  
[kali@kali]~$ sudo nmap -sT 192.168.56.102  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 12:02 EDT  
Nmap scan report for 192.168.56.102  
Host is up (0.0088s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
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  
MAC Address: 08:00:27:4C:8F:8C (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)  
Nmap done: 1 IP address (1 host up) scanned in 14.37 seconds  
[kali@kali]~$
```

### 3. Service Version Detection (-sV)

- Command: `sudo nmap -sV 192.168.56.102`
- Purpose: Identify software versions running on open ports.
- Findings:

```
kali@kali: ~  
Session Actions Edit View Help  
[kali@kali]~$ sudo nmap -sV 192.168.56.102  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 12:43 EDT  
Nmap scan report for 192.168.56.102  
Host is up (0.00083s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache/2.2.22 ((Ubuntu) DAV/2)  
111/tcp    open  rpcbind      2 (RPC #100000)  
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)  
512/tcp    open  exec         netkit-rsh rexecd  
513/tcp    open  login        Netkit rshd  
514/tcp    open  shell        GNU Classpath grmiregistry  
1099/tcp   open  java-rmi     Metasploitable root shell  
1524/tcp   open  bindshell    2-4 (RPC #100003)  
2049/tcp   open  nfs          ProFTPD 1.3.1  
2121/tcp   open  ftp          ProFTPD 1.3.1  
3306/tcp   open  mysql        MySQL 5.0.51a-3ubuntu5  
5432/tcp   open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp   open  vnc          VNC (protocol 3.3)  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs : Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
Service detection performed. Please report any incorrect results at https://n  
map.org/submit/  
Nmap done: 1 IP address (1 host up) scanned in 25.70 seconds  
[kali@kali]~$
```

### 4. OS Detection (-O)

- Command: `sudo nmap -O 192.168.56.102`
- Purpose: Identify operating system via TCP/IP fingerprinting.
- Findings:

```
kali@kali: ~  
Session Actions Edit View Help  
[kali@kali]~$ sudo nmap -O 192.168.56.102  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 12:34 EDT  
Nmap scan report for 192.168.56.102  
Host is up (0.0023s 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  
MAC Address: 08:00:27:4C:8F:8C (PCS Systemtechnik/Oracle VirtualBox virtual N  
IC)  
OS: Linux 3.2-6.1  
OS CPE: cpe:/o:linux:linux_kernel  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs : Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
Nmap done: 1 IP address (1 host up) scanned in 12.05 seconds  
[kali@kali]~$
```

### Security Observations:

| Service            | Port(s)  | Risk Summary                               |
|--------------------|----------|--|
| FTP (vsftpd 2.3.4) | 21       | Known backdoor vulnerability               |
| Telnet             | 23       | Transmits credentials in plaintext         |
| Samba              | 139, 445 | Vulnerable to remote code execution        |
| Apache & MySQL     | 80, 3306 | Outdated versions                          |
| PostgreSQL         | 5432     | May expose sensitive data if misconfigured |

### Recommendations:

- Disable insecure services: Telnet and FTP should be removed; use SSH/SFTP instead.
- Patch outdated software: Upgrade Apache, Samba, MySQL, PostgreSQL to secure versions.
- Apply firewall rules: Use iptables or ufw to restrict access to sensitive ports.
- Run deeper scans: Use OpenVAS or Nessus Essentials for CVE-based vulnerability analysis.
- Maintain documentation: Archive scan logs, screenshots, and remediation steps for audit and learning.