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.

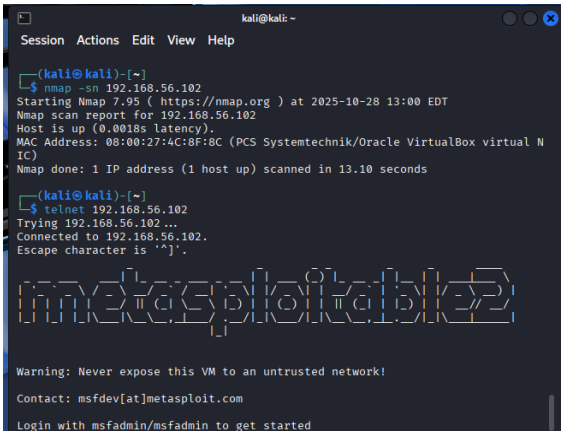
2. Active Reconnaissance

- 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.



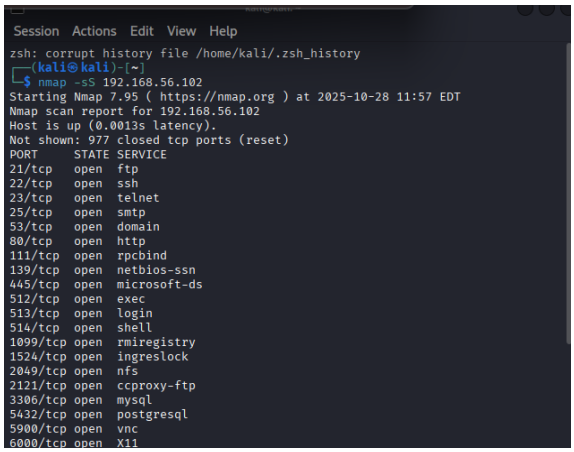
🔍 Scan Breakdown

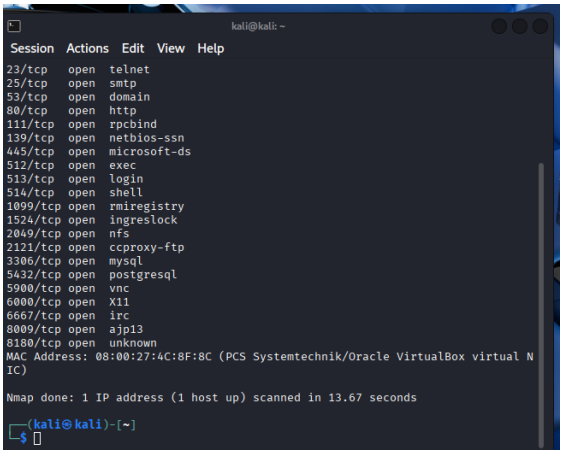
1. TCP SYN Scan (-sS)

- Command: nmap -sS 192.168.56.102

- Purpose: Stealth scan using raw packets (requires root)

- Findings:



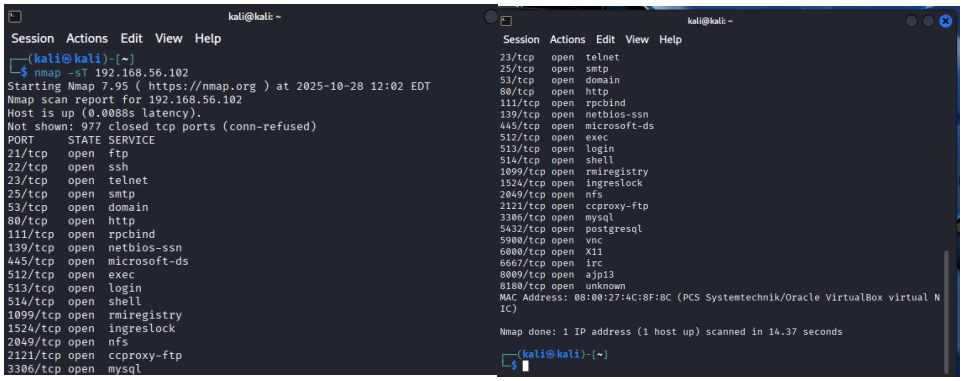


2. TCP Connect Scan (-sT)

- Command: nmap -sT 192.168.56.102

- Purpose: Full TCP connection (used when not root)

- Findings:

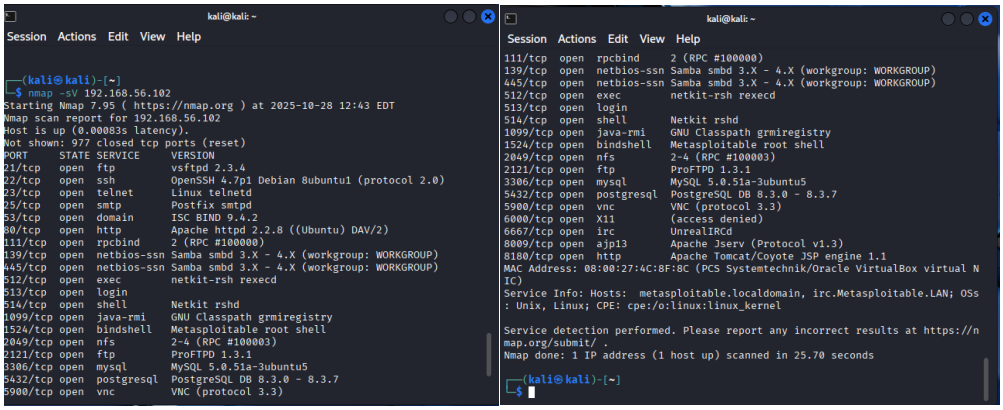


3. Service Version Detection (-sV)

- Command: sudo nmap -sV 192.168.56.102

- Purpose: Identify software versions running on open ports.

- Findings:

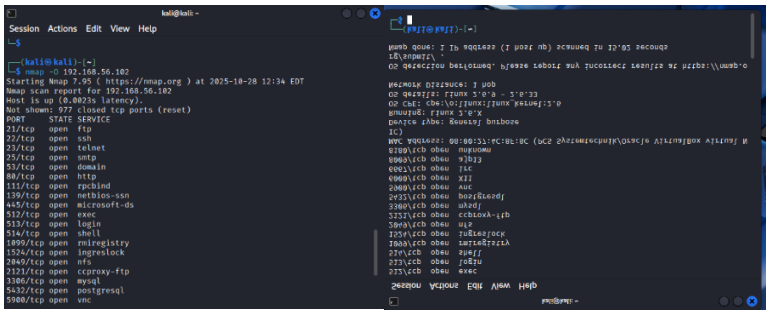


4. OS Detection (-O)

- Command: sudo nmap -O 192.168.56.102

- Purpose: Identify operating system via TCP/IP fingerprinting.

- Findings:



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.