Project Report: Basic Network Scanning with Nmap

Project Report: Basic Network Scanning with Nmap

1. Introduction
Network scanning is a fundamental activity in cybersecurity that helps identify live hosts, open ports, and running services in a network. This project demonstrates a basic Nmap scan performed on a lab virtual machine (VM) to understand how attackers or defenders can gather reconnaissance information.

The purpose of this report is to:
- Document the process of scanning a host using Nmap.
- Record and interpret the results.
- Highlight possible security risks.
- Suggest mitigation measures.

2. Tools & Environment
- Scanner Machine: Kali Linux (running on VirtualBox)
- Target Machine: Ubuntu/Debian-based VM (192.168.56.104)
- Tool Used: Nmap 7.95
- Network Setup: VirtualBox Host-only Adapter
- Date of Scan: 12th September 2025

3. Methodology
The following Nmap commands were executed step by step:
1. Host discovery (Ping Scan)
nmap -sn 192.168.56.104/24
- Discovered active hosts on the subnet.

2. Basic port scan
nmap 192.168.56.104
- Identified open ports on the target.

3. Full port scan
nmap -p- 192.168.56.104
- Checked all 65,535 TCP ports.

4. Service version detection
nmap -sV 192.168.56.104

5. Aggressive scan (OS detection, services, scripts, traceroute)
sudo nmap -A 192.168.56.104

6. Stealth full port scan
sudo nmap -sS -p 1-65535 -T4 192.168.56.104

7. Scan selected common ports
nmap -p 22,80,443,3306 192.168.56.104

8. Export results
nmap -sV -O 192.168.56.104 -oN nmap_scan_results.txt

4. Findings

Port: 80
State: Open
Service: HTTP
Version: Apache httpd 2.4.65
Notes: Directory listing enabled; suspicious files exposed

Ports 22, 443, 3306: Closed

Directory Listing Exposed Files:
- instagram.apk
- securefile.exe
- winAttack.exe
- winattack.exe

- zenserk.exe

These files appear suspicious/malicious and should not be downloaded or executed outside of a controlled sandbox environment.

5. Analysis & Risks
- Open HTTP (Port 80): Apache server is publicly accessible.
- Directory Listing Enabled: This is a misconfiguration; attackers can directly browse files.
- Malware Risk: .exe and .apk files suggest possible malware or unauthorized uploads.
- No Encryption (HTTPS closed): All traffic is in plaintext, vulnerable to interception.
- Limited Attack Surface: Other common services (SSH, MySQL) are closed, reducing exposure.

6. Recommendations
1. Disable directory listing: Update Apache config (Options -Indexes) and restart the service.
2. Remove malicious files: Delete or quarantine .exe and .apk files from /var/www/html/.
3. Enable HTTPS: Configure SSL/TLS using certbot or another CA.
4. Apply updates & patches: Run sudo apt update && sudo apt upgrade -y to patch vulnerabilities.
5. Use a firewall (UFW): Allow only required services (e.g., sudo ufw allow 80/tcp).
6. Audit logs: Review /var/log/apache2/ for unauthorized access attempts.
7. Segregate suspicious analysis: Open unknown files only in a sandbox VM or malware lab environment.

7. Ethical Considerations
This scan was performed only on a lab VM owned and controlled by the analyst. Unauthorized scanning of external systems is illegal and unethical. Always seek explicit permission before scanning systems you do not own.

8. Conclusion
This project demonstrated the process of scanning a local VM with Nmap, identifying an exposed Apache server with directory listing enabled. The presence of suspicious executables highlights the risks of poor configuration and unmonitored file hosting.

By applying remediation measures such as disabling directory listing, removing malicious files, and hardening the server, administrators can significantly reduce the attack surface and protect against exploitation.

Deliverables produced:
- nmap_scan_results.txt — Raw scan output
- README.md — Documentation of methods & results
- report.md — Compact 1-page summary
- Project Report (detailed document)