Task 1 – Basic Network Scanning with Nmap

1. Introduction

Network scanning is a fundamental activity in cybersecurity that helps security professionals understand the exposure of systems within a network. One of the most widely used tools for this purpose is Nmap (Network Mapper). Nmap is an open-source utility used for network discovery, host identification, port scanning, and service enumeration. It is commonly used by system administrators to audit networks and by security analysts to identify potential vulnerabilities.

This report documents Task 1 – Basic Network Scanning with Nmap, which focuses on identifying open ports and running services on a target system within a controlled virtual environment. The activity was performed ethically and strictly for educational and learning purposes.

---

2. Objective

The objective of this task is to:

- Perform a basic network scan using Nmap.
- Identify whether the target system is reachable on the network.
- Detect open TCP ports and enumerate running services.
- Analyze the security implications of the scan results.
- Understand how network exposure affects the attack surface of a system.

---

3. Environment Setup

The scanning activity was conducted in a virtualized lab environment to ensure safety and isolation from real-world networks.

3.1 Attacker System

- Operating System: Kali Linux
- Deployment: Oracle VirtualBox Virtual Machine
- Purpose: Used to execute Nmap scanning commands

3.2 Target System

- Target IP Address: 192.168.232.128
- Network Type: Host-only / Internal network (VirtualBox)
- State: Powered on and reachable

This setup ensures that scanning activities do not impact external or unauthorized systems.

---

4. Tool Used

Nmap (Network Mapper)

Nmap is a powerful network scanning tool capable of:

- Discovering hosts on a network
- Scanning TCP and UDP ports
- Detecting running services and versions
- Performing OS detection and script-based vulnerability checks

In this task, Nmap was used specifically for TCP SYN scanning and service version detection.

---

5. Commands Executed

Two primary commands were executed during this task:

1. ip a – Used to verify the IP address and network configuration of the Kali Linux system.
2. nmap -sS -sV 192.168.232.128 – Used to scan the target system for open TCP ports and running services.

---

6. Command Explanation

6.1 ip a

The ip a command displays detailed information about:

- Network interfaces
- Assigned IP addresses
- Interface status (UP/DOWN)

This step ensures that the attacker machine is properly connected to the target network before scanning.

6.2 nmap -sS -sV 192.168.232.128

- -sS (TCP SYN Scan):
    - Performs a stealthy scan by sending SYN packets.
    - Does not complete the TCP handshake.
    - Faster and less detectable than a full TCP connect scan.

- -sV (Service Version Detection):
    - Attempts to identify the service and version running on open ports.
    - Useful for vulnerability assessment and patch verification.
- Target IP: Specifies the system to be scanned.

---

7. Scan Results

The Nmap scan produced the following results:

- The target host was reachable and responsive.
- No open TCP ports were detected during the scan.
- All scanned ports were found in a closed state.
- No services or service versions were identified.

These results indicate that the target system is active on the network but does not expose any listening services over TCP.

---

8. Security Significance

The scan findings have important security implications:

- Closed Ports:
    - Closed ports indicate that no services are actively listening.
    - This significantly reduces opportunities for attackers.
- Reduced Attack Surface:
    - Fewer exposed services mean fewer potential vulnerabilities.
    - Limits vectors such as remote exploitation and brute-force attacks.
- Baseline Security Posture:
    - A system with no unnecessary open ports represents a strong security baseline.
    - Ideal for hardened systems or newly deployed machines.
- Defense-in-Depth Support:
    - When combined with firewalls and intrusion detection systems, closed ports enhance overall security.

---

9. Limitations of the Scan

While the scan provided useful insights, it has certain limitations:

- Only TCP ports were scanned; UDP services were not assessed.
- Firewall rules may block or filter scan responses.
- Services may be bound to localhost only, making them invisible to remote scans.

Further scans such as UDP scanning, firewall evasion techniques, or authenticated scans could provide deeper visibility.

---

10. Conclusion

This task successfully demonstrated the use of Nmap for basic network scanning and service enumeration. The target system was found to be reachable but did not expose any open TCP services, indicating a secure configuration with a minimal attack surface.

Regular network scanning is a critical practice in cybersecurity. It helps organizations identify misconfigurations, detect unauthorized services, and maintain a strong security posture. This exercise reinforces the importance of proactive security assessments and provides a solid foundation for advanced network reconnaissance techniques.