Network Vulnerability Scanning Report

Objective

The objective of this task is to perform network vulnerability scanning using Nmap to identify open ports, services, operating systems, and potential security risks.

Tools Use

- Nmap VM kali linux
- Target: Own network/own system

Procedure

1. Scanned the local network to identify active hosts.
2. Identified open ports on the target system.
3. Detected running services and their versions.
4. Performed operating system detection.
5. Executed vulnerability scanning using Nmap scripts.
6. Saved the scan results for analysis.

Scan Results

- Multiple open ports were identified.
- Services such as HTTP, SSH, and FTP were detected.
- The target operating system was successfully identified.
- Potential vulnerabilities were observed due to exposed services.

Risk Analysis

- Open ports increase the attack surface.
- Outdated services may contain known vulnerabilities.
- Improperly configured services can be exploited by attackers.

Document Findings

- Close unused ports.
- Update and patch services regularly.
- Implement firewall rules.
- Use intrusion detection systems.
- Restrict access using network segmentation.