

Network Vulnerability Scanning – Detailed Report

Cyber Security Internship – Task 9

Tool Used: Nmap

Environment: Local Network / Kali Linux Lab

Author: Mohammed Nihal

Abstract

This report presents a detailed network vulnerability scanning exercise conducted using Nmap. The objective was to discover active hosts, identify open ports, detect running services, and evaluate potential network-level security risks. The scan was performed in a controlled lab environment on authorized systems to ensure ethical compliance.

1. Introduction

Network vulnerability scanning is a critical phase of network security assessment and penetration testing. It helps security professionals understand the exposed attack surface of a system by identifying open ports, running services, and operating systems. Attackers often begin their intrusion attempts with reconnaissance, making proactive scanning an essential defensive practice.

2. Overview of Nmap

Nmap (Network Mapper) is an open-source tool widely used for network discovery and security auditing. It supports various scanning techniques, including host discovery, port scanning, service version detection, operating system fingerprinting, and vulnerability detection using NSE scripts.

3. Scanning Environment

The scanning environment consisted of a Kali Linux system connected to a private network. The target host resided within a local IP range. All scans were conducted on systems owned by the user, ensuring that the activity was legal and ethical.

4. Scanning Methodology

A structured scanning methodology was followed. The process included host discovery to confirm live systems, TCP port scanning to identify open ports, service version detection to enumerate applications, and operating system detection to identify the underlying platform. Scan results were saved for analysis.

5. Scan Results and Observations

The Nmap scan confirmed that the target host was active on the network. However, all scanned TCP ports were found to be closed. This indicates that no services were actively listening for incoming connections. Such a configuration significantly reduces the system's exposure to network-based attacks.

6. Service and Operating System Detection

Service version detection and operating system fingerprinting were attempted using Nmap. Due to the absence of open ports, Nmap was unable to determine service versions or accurately identify the operating system. This behavior is expected and highlights the effectiveness of closed-port configurations.

7. Vulnerability and Risk Analysis

No direct network-level vulnerabilities were identified during the scan due to the lack of exposed services. Closed ports limit the opportunities for attackers to exploit known service vulnerabilities. However, network security is dynamic, and vulnerabilities may arise if new services are enabled in the future.

8. Importance of Network Scanning

Regular network vulnerability scanning helps organizations identify misconfigurations, detect unauthorized services, and assess overall security posture. It enables proactive risk management and supports compliance with security best practices.

9. Conclusion

This task provided hands-on experience with network vulnerability scanning using Nmap. Even though no open ports were detected, the scan demonstrated the importance of reconnaissance in evaluating network security. Consistent scanning and monitoring are essential for maintaining a strong security posture in evolving network environments.