Vulnerability Scan Report

Introduction

This report summarizes the results of a vulnerability scan performed on the home network using Nmap. The objective was to identify open ports, services, and potential vulnerabilities across devices connected to the network.

Problem Definition

The task involved scanning the home network to identify potential security vulnerabilities. The scan was intended to detect open ports, services, and operating systems, and to assess the security risks associated with these findings.

Task Definition

A scan was conducted on the IP range 192.168.100.* using the Nmap tool with the following options:

- `-sV`: Probe open ports to determine service and version information.

- `-T4`: Aggressive timing for faster scans.

- `-O`: OS detection.

- `-F`: Fast scan, fewer ports.

- `--version-light`: Reduce intensity of version detection to speed up the scan.

The primary goal of the scan was to identify any open ports or services on devices within the network that could pose security risks and assess the operating systems running on the devices.

Vulnerabilities Identified

1. Device: 192.168.100.1 (Huawei Home Gateway)

Open Telnet (port 23) service detected.

Vulnerability: Telnet is an insecure protocol that sends data in plaintext, making it highly vulnerable to interception.

Remediation: Disable Telnet and switch to a secure protocol like SSH.

2. Device: 192.168.100.4 (Windows 10 Machine)

Open MySQL (port 3306) service detected.

Vulnerability: MySQL is accessible without proper authorization, which can allow unauthorized access to the database.

Remediation: Restrict MySQL access to trusted hosts and implement strong authentication.

Open Microsoft Windows services like MSRPC (port 135), NetBIOS (port 139), and SMB (port 445) detected.

Vulnerability: These services are often targeted in attacks such as ransomware and data exfiltration.

Remediation: Close unnecessary ports and enforce strict firewall rules.

Results and Tools Used

The scan detected three devices on the network. Nmap was used due to its efficiency in identifying services, ports, and operating systems. Below are the key findings:

- 192.168.100.1: Huawei router with Telnet and DNS services.

- 192.168.100.4: Windows 10 machine with open RPC, NetBIOS, SMB, MySQL, and HTTP services.

- 192.168.100.5: Device with no open ports (all ports closed).