Report on Home Network Vulnerability Scan

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

Conducted a scan on IP range 192.168.100.* using NMAP tool using the options below :

- `-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 goal of the scan was to detect any open ports or services running on the devices within my network that could pose security issues and asses operating systems running on my devices.

Vulnerabilities Detected Include :

192.168.100.1 (Huawei Home Gateway)

Open Telnet (port 23) service detected.

Vulnerability: Telnet sends data in plaintext making it easier to intercept data while in transist.

Recommendation: Switch to a secure protocol like SSH.

192.168.100.4 (Windows 10 Machine)

Open MySQL (port 3306) service detected.

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

Recommendation: Restrict MySQL access to trusted hosts .

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

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

Recommendation: Implement firewall rules to minimize access to the open services.

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).