Final Nmap Network Scan Report (IP Addresses Hidden)

1. Introduction

This report summarizes a network scan performed using Nmap to discover active devices, open ports, and potential security risks. The scan used a TCP SYN method, which is efficient and commonly used for network auditing.

2. Scan Method Used

A TCP SYN scan was performed across the local network. Results were saved to a text file. For privacy, all IP addresses have been removed in this report.

3. Scan Summary

- Total devices detected: 6

- Scan duration: Approximately 49 seconds

- The network contained a mix of router, smartphone, IoT, and computer devices.

4. Device Findings (IPs Hidden)

Device 1:

- Status: Reachable

- Open Ports: DNS, HTTP, HTTPS

- Several ports were filtered for security.

- Likely Device: Router/Modem

- Vendor Identified: DZS

Device 2:

- Status: Reachable

- No open ports detected

- Vendor: Motorola Mobility

- Likely Device: Smartphone

Device 3:

- Status: Reachable

- Open Ports: HTTP, HTTPS-Alt, AJP13, others commonly used by IoT or streaming devices.

- Vendor: Hon Hai Precision

- Likely Device: Smart TV or Set-top Box

Device 4:

- Status: Reachable

- No visible open ports

- Vendor: Unknown

- Likely Device: Consumer device with blocked ports

Device 5:

- Status: Reachable

- Open Ports: iPhone sync service ports and a high port number

- Likely Device: iPhone

Device 6:

- Status: Reachable

- Open Ports: MSRPC, SMB, NetBIOS, MySQL

- Likely Device: Windows computer running MySQL services

5. Security Risk Analysis

High-Risk Ports:

- SMB (445) and NetBIOS (139) can lead to ransomware or unauthorized access risks.

- IoT debugging port (5555) is unsafe if publicly exposed.

Medium Risk:

- MySQL port (3306) should not be open unless required.

Low Risk:

- Standard router service ports such as HTTP and HTTPS are normal.

6. Conclusion

The scan successfully discovered several active devices in the network. Some devices expose ports that could pose security risks if improperly configured. It is recommended that unnecessary ports be closed, especially on Windows machines and IoT devices, to minimize vulnerabilities.

This report excludes IP addresses for privacy and presents findings in a human-friendly manner.