Nmap Scan Analysis Report

Scan Target: 10.0.2.0/24

Tool Used: Nmap with Service Detection (nmap -sV --top-ports 100 10.0.2.0/24)

Scan Date: May 26, 2025

Host: 10.0.2.2

Open Ports and Services:

Port 135 is running Microsoft Windows RPC (msrpc). This service is used for DCOM & RPC and is commonly targeted by malware like the Blaster worm. It poses a high security risk.

Port 445 is hosting SMB file sharing (microsoft-ds). This port is vulnerable to well-known exploits like EternalBlue, which was used by ransomware such as WannaCry and NotPetya. It is considered high risk.

Port 7070 appears to be running an unknown service possibly named ssl/realserver. This may be a streaming or administrative interface and requires further investigation. It carries a medium risk.

Risk Summary:

Ports 135 and 445 expose critical Windows services that are often targeted by attackers.

Port 7070 is unknown and may be vulnerable or outdated despite being SSL-enabled.

Recommended Actions:

Restrict or firewall access to ports 135 and 445 unless absolutely necessary.

Identify and secure the service running on port 7070.

Host: 10.0.2.3

Open Ports and Services:

Port 53 is running a DNS service using dnsmasq version 2.78. This version is known to have vulnerabilities such as DNS cache poisoning, denial of service (DoS), and remote code execution (RCE). This presents a medium security risk.

Risk Summary:

The DNS service is outdated and may be affected by critical vulnerabilities if not updated.

Recommended Actions:

Upgrade dnsmasq to version 2.80 or later.

Regularly monitor DNS activity for suspicious behavior.

Host: 10.0.2.15

Open Ports:

No open ports detected. All 100 scanned ports are closed.

Risk Summary:

No services are currently exposed, indicating a secure state.

General Recommendations:

Keep all operating systems and services up to date with the latest security patches.

Use firewalls to block unnecessary ports and restrict access.

Perform deeper vulnerability checks using Nmap scripts like --script vuln.

Consider using a bridged network adapter in VirtualBox if you want to scan real LAN devices more effectively.

End of Report