Nmap Network Scan Report

\*\*Date of Scan:\*\* May 26, 2025

\*\*Scan Command Used:\*\* nmap -sS 192.168.66.0/24

\*\*Total Hosts Scanned:\*\* 256

\*\*Hosts Up:\*\* 2

\*\*Scan Duration:\*\* 62.75 seconds

# Host: 192.168.66.1 (Your system)

|  |  |  |
| --- | --- | --- |
| Port | Service | Description |
| 135 | msrpc | Microsoft RPC (Remote Procedure Call) |
| 139 | netbios-ssn | NetBIOS Session Service |
| 445 | microsoft-ds | Microsoft Directory Services (SMB) |
| 902 | iss-realsecure | VMware Remote Console or security service |
| 912 | apex-mesh | Unknown (App-specific) |
| 7070 | realserver | RealMedia Server port (legacy) |

# Host: 192.168.66.254 (VMware Device)

No open ports detected — all scanned ports were filtered or unresponsive.

# Security Recommendations

|  |  |  |
| --- | --- | --- |
| Port(s) | Risk Level | Recommendation |
| 135, 139, 445 | High | Disable or restrict on public networks. These are often targeted by malware and ransomware. |
| 902 | Medium | Verify if VMware remote access is needed. Disable if not. |
| 912, 7070 | Unknown | Investigate the applications using these ports. If unused, close them for safety. |