

Risk Analysis of Open Ports

Device 1: 192.168.31.10

Open Ports:

- 22/tcp (SSH)
- 80/tcp (HTTP)

Risk Analysis:

- Port 22 (SSH) – Medium Risk: Can be brute forced; allows remote login.
- Port 80 (HTTP) – Medium Risk: Exposes web interface; may reveal sensitive info.

Device 2: 192.168.31.238

Open Ports:

- 445/tcp (SMB)
- 139/tcp (NetBIOS)

Risk Analysis:

- Port 445 (SMB) – High Risk: Common ransomware target (e.g., WannaCry).
- Port 139 (NetBIOS) – High Risk: Leaks system information; file sharing vulnerabilities.

Device 3: 192.168.31.70

Open Ports:

- 443/tcp (HTTPS)

Risk Analysis:

- Port 443 (HTTPS) – Low Risk: Secure protocol; low risk unless outdated.

Device 4: 192.168.31.22

Open Ports:

- 5555/tcp (ADB)

Risk Analysis:

- Port 5555 (ADB) – Critical Risk: Allows full remote control of Android device.

Overall Summary:

High risk ports detected: 445, 139, 5555.

Medium risk ports detected: 22, 80.

Low risk ports detected: 443.