Potential risks on open ports

IP: `192.168.0.1`

- **Open Ports:**
  - `23/tcp` → `telnet`
    → **BusyBox telnetd 1.14.0 or later (TP-LINK router)**
    High Risk: Plaintext access, often default/weak creds.

  - `53/tcp` → `tcpwrapped`
    → **PowerDNS Recursor 4.1.11**
    Medium Risk: Could allow DNS enumeration or amplification.

  - `80/tcp` → `http`
    → **TP-LINK WAP HTTP config**
    Medium Risk: Exposes router config via web, potential admin panel.

  - `1900/tcp` → `upnp`
    → **Portable SDK for UPnP devices 1.6.19**
    High Risk: UPnP is often exploitable, especially on TP-LINK.

- **MAC Address:** `40:3F:8C:CE:EE:12`

- **OS/Device Info:** Linux (3.10.14), TP-LINK router, WAP

IP: `192.168.0.100`

- **Open Ports:**
  - `1234/tcp` → `http`
    → **Node.js Express Framework (application/json)**
    Medium Risk: Custom API? May allow CORS abuse, info leakage, or injection.

  - `5900/tcp` → `vnc`
    → **VNC (protocol 3.8)` with authentication**

High Risk: VNC is easily brute-forced or sniffed if not tunneled.

  - `5985/tcp` → `http`
    → **Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)**
    Medium Risk: Used for WinRM; can be abused for remote code execution.

  - `7070/tcp` → `ssl/realserver?`
    → **TLS cert: AnyDesk Client (valid till 2074)**
    Medium-High Risk: Possibly exposed AnyDesk agent; check for RCE or misuse.

- **MAC Address:** `E4:C7:67:6B:33:93`

- **OS Info:** Windows OS

IP: `192.168.0.106`

- Host is up

All 1000 ports closed (no open ports)