**PROJECT: HOME NETWORK SECURITY AUDIT**

**Description:**

**Conducted a comprehensive security audit of a home network by scanning all connected devices with Nmap, identifying open ports, and checking for potential vulnerabilities. Implemented recommendations to enhance network security.**

**NOTE: For security and privacy reasons, all IP addresses, MAC addresses, and device hostnames have been anonymized in this report. The data presented is for educational and illustrative purposes only.**

**TOOLS NEEDED:**

1. **Router Admin Interface** – To view connected devices and modify network settings
2. **Penetration Testing Linux Distro (Optional): Kali Linux** – Comes pre-installed with Nmap
3. **Any PC/Laptop/Smartphone connected to your home network**

**SETUP – STEP-BY-STEP**

**STEP 1: PREPARE YOUR ENVIRONMENT**

* Download and install VirtualBox, then set up Kali Linux (includes Nmap).
* Using Kali Linux in a VM is a safe and convenient way to run the audit.
* your device to your home Wi-Fi or via Ethernet.

**STEP-2: IDENTIFY YOUR NETWORK RANGE**

What are we doing?

We want to know the IP address and subnet your Kali Linux VM is using to connect to your home network. This tells us the range of IP addresses where all devices will be.

Why?

We need to scan the entire network subnet to find all connected devices. Without this info, we can’t scan the right network.

* Represent Device names- RED

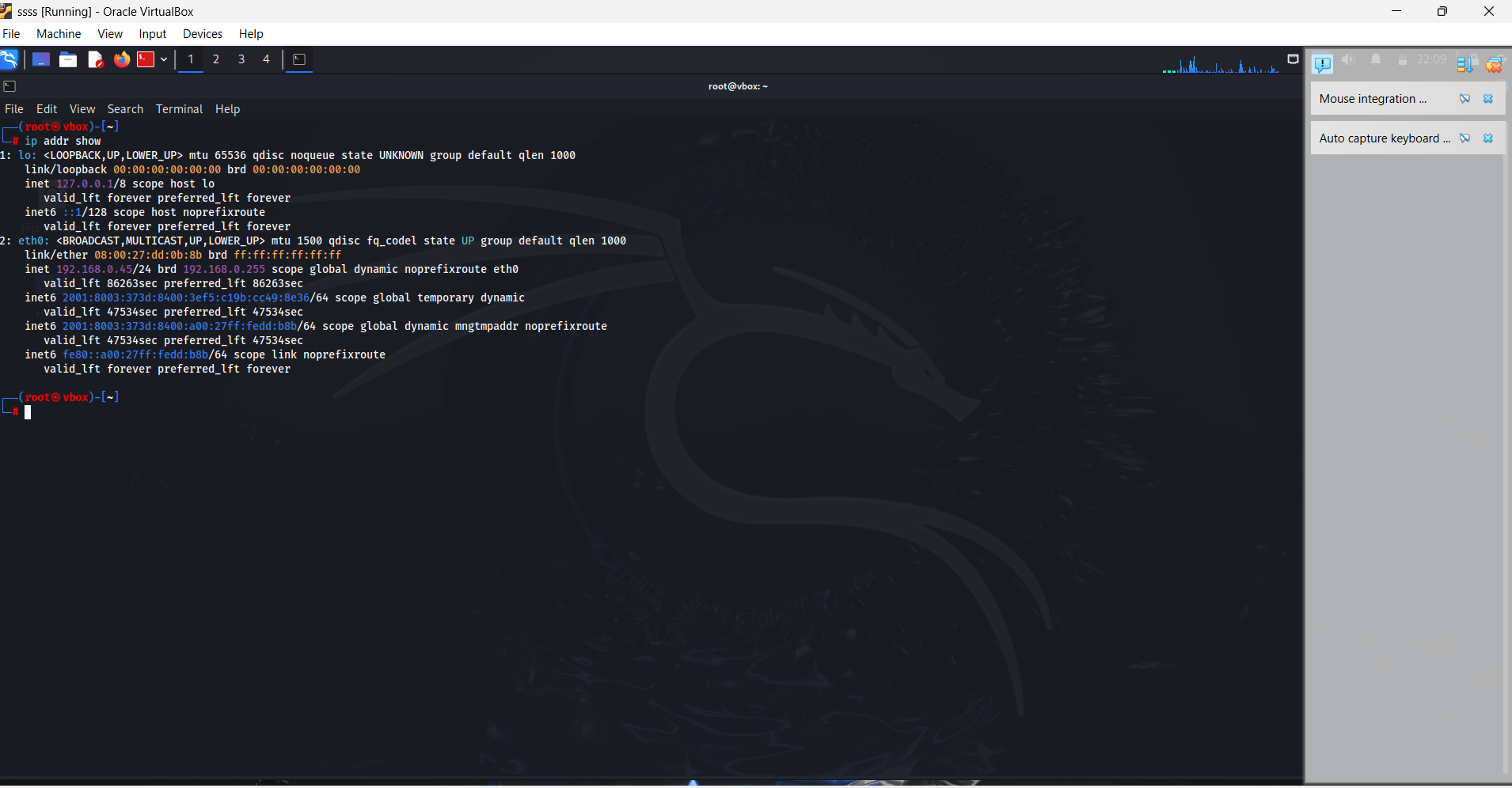


* Represent Vendor Info - BLUE



* Represent IP &MAC Addresses - YELLOW





shows ip range here in output



We will use command: ip addr show

Look for the network interface connected to your home network (likely eth0 or wlan0).

Note the IP address, for example: 192.168.xx.xx/24

**STEP 2: SCAN YOUR NETWORK FOR LIVE DEVICES**

Now, scan your entire local subnet to discover all active devices.

Replace 192.168.xx.xx/24 (example) with your network range if different:



****



Device 1



192.168.xx.x1



This will ping all devices and show which are online.

For example: Above image shows for phone ip address is 192.168.xx.xx and MAC address xx.xx.xx.xx.

**Step 3: Review Discovered Devices**

Look at the output — it’ll list IPs and device MAC addresses (often with vendor info).

Make a list of devices you recognize (laptop, phone, smart TV, etc.) and note any unknown devices.

**Example Output Summary:**

|  |  |  |  |
| --- | --- | --- | --- |
| Device | IP Address | MAC Address | Vendor |
| Phone-1 | 192.168.xx.xx | xx:xx:xx:xx:xx:xx | Unknown |
| Laptop-1 | 192.168.xx.xx | xx:xx:xx:xx:xx:xx | Unknown |
| Laptop-2 | 192.168.xx.xx | xx:xx:xx:xx:xx:xx | Vendor-3 |
| Laptop-3 | 192.168.xx.xx | xx:xx:xx:xx:xx:xx | Vendor-4 |
| Laptop-4 | 192.168.xx.xx | xx:xx:xx:xx:xx:xx | Vendor-5 |
| Phone-2 | 192.168.xx.xx | xx:xx:xx:xx:xx:xx | Vendor-6 |

**STEP 4: SCAN OPEN PORTS ON A DEVICE**

**Pick one device IP from the previous scan to check its open ports and running services.**

**Use command (sudo nmap -sV ip…) on Phone-1.**



**(*Note: IP redacted for privacy*)**

****



Ports open:

49152/tcp -open

62078/tcp -open

Both ports on **Device 1** returned as **tcpwrapped**, it means Nmap could see that the ports are open, but the service refused to provide version info—likely due to access restrictions or protection mechanisms like a firewall.

**What is tcpwrapped?**

* The term **tcpwrapped** indicates that Nmap connected to the port but was unable to determine what service is running.
* This often means the service **requires authentication** or has **access control mechanisms** in place (e.g., a firewall or intrusion prevention system) that block Nmap's probing.

**Security Interpretation:**

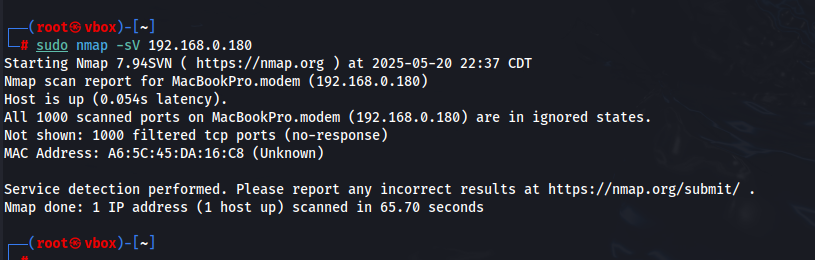
* These ports are **open**, but the services are **protected**, which is better than fully exposed services.
* Since **62078** is commonly used for **Apple device syncing** (e.g., iPhone), and **49152** is a dynamic/private port, these results are expected if the device is an Apple phone or tablet.

**Recommendations:**

* If this is a **personal and known device** (e.g., your iPhone), no immediate concern.
* If the device is **unknown**, further investigation is recommended:
  + Identify the device type via MAC address/vendor.
  + Log into your router and **disable or isolate unknown devices**.
* For enhanced privacy, consider setting up a **Guest Wi-Fi** for smart or unknown devices.

--------------------------------------------------------------------------------------------------------------------------------------

**Device 2: Port Scan Results**

****



Command Used:

(sudo nmap -sV 192.168.X.X)

**(*IP redacted for privacy*)**

**Scan Output Summary:**

Host is up (0.012s latency).

All 1000 scanned ports on 192.168.X.X are in ignored states.

Not shown: 1000 filtered tcp ports (no-response).

**What does this mean?**

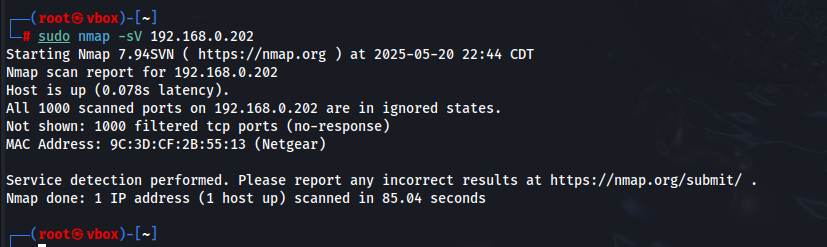
* **"Host is up"** confirms that the device is online and responding to pings or ARP requests.
* **"1000 filtered TCP ports"** means that **no ports responded to Nmap's probes**.
* "Filtered" typically indicates that:
  + A **firewall is blocking** the scan.
  + The host is **dropping packets silently** (not rejecting or accepting them).
  + There are **no open ports** visible due to access control or security settings.

**Recommendations:**

* If the device is known and trusted, no further action is required.
* If it is an **unknown device**, you may still want to:
  + Identify it via the MAC address.
  + Review your router’s connected device list.
  + Use ARP spoofing protection or Guest Wi-Fi segmentation if needed.

------------------------------------------------------------------------------------------------------------------------------

**Device 3: Port Scan Results**

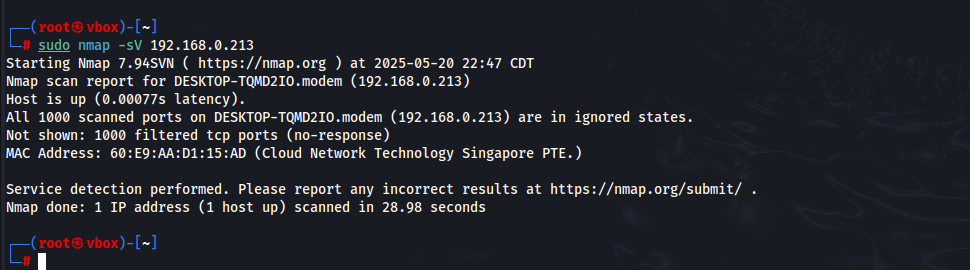
****



**Same output as Device – 2**

**--------------------------------------------------------------------------------------------**

**Device 4: Port Scan Results**

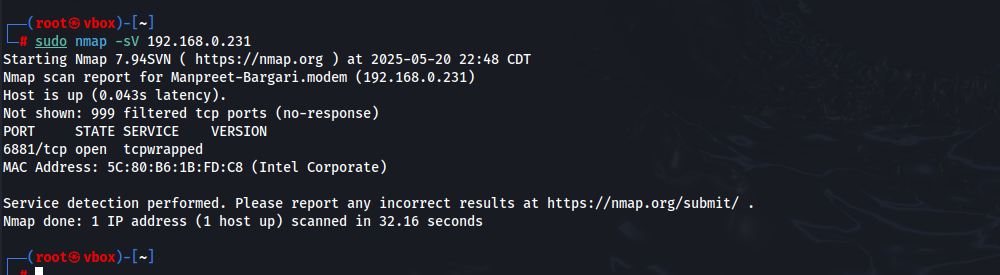
****



**Same output as Device - 2**

**--------------------------------------------------------------------------------------------**

**Laptop- 5:**

****



Open ports: 6881/tcp

**What is Port 6881?**

* Port **6881/tcp** is commonly associated with **BitTorrent** and other **peer-to-peer (P2P) file-sharing** services.
* Seeing this port open suggests the device may be running a **torrent client** or another P2P application.

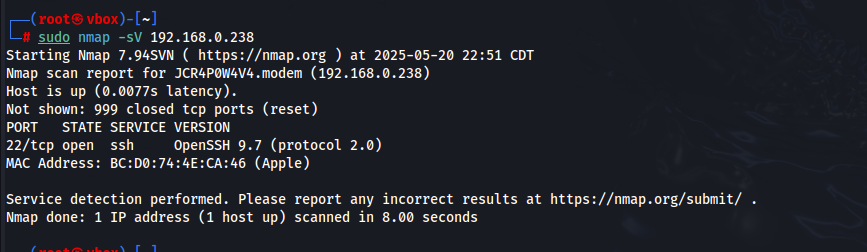
**Security Interpretation:**

* If Device 5 is a personal or known device and the user is intentionally running a torrent client, this is expected.
* However, P2P software can expose the device to:
  + **Malware** embedded in shared files.
  + **DDoS amplification risks.**
  + **Legal or copyright issues.**

**Recommendations:**

* If the use of torrenting is **intentional and safe**, consider:
  + Limiting port exposure to the internet via the router.
  + Enabling VPN when using P2P.
* If **torrenting is not expected or unknown**:
  + Investigate the device's software.
  + Consider disabling or removing the service.
  + Monitor the device’s network activity for unusual traffic.

Phone-2:





Open ports: 22/tcp-open

**🔐 What is Port 22 (SSH)?**

* **Port 22** is used for **Secure Shell (SSH)**, a protocol that allows remote login and secure command execution.
* **OpenSSH** is one of the most common and trusted SSH servers but must be configured securely

**🛡 Security Interpretation:**

* SSH being **open** is **not a vulnerability by itself**, **but**:
  + It should **not be accessible from the internet** unless absolutely necessary.
  + It **must** use strong **authentication methods** (e.g., public key, not just password).
  + The service should ideally be **configured to only accept trusted IPs**.

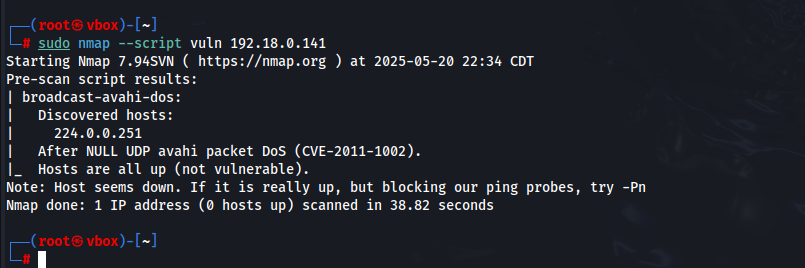
**✅ Recommendations:**

1. **Confirm it's intended**: If the device is a MacBook, Raspberry Pi, or Linux machine where remote access is needed, then this may be expected.
2. **Harden SSH Configuration**:
   * Disable password login (PasswordAuthentication no)
   * Use SSH keys for authentication
   * Change default port (optional, for obscurity)
   * Disable root login (PermitRootLogin no)
3. **Firewall Rules**:
   * Restrict port 22 to **local network IPs only**
   * Or, block it entirely if remote access isn’t needed
4. **Monitor for Unusual Logins**:
   * Check SSH logs (/var/log/auth.log) if available
   * Watch for brute-force attempts

**STEP 5: RUN VULNERABILITY SCAN ON THE DEVICE**

Check for vulnerabilities with Nmap’s scripting engine:

Device 1: (Phone-1)





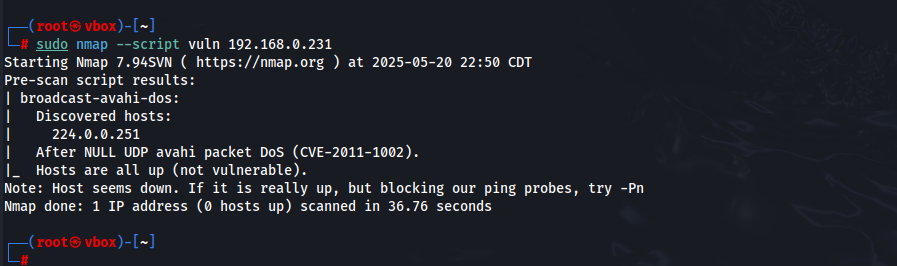
⚠️ **“Does not appear to be vulnerable”** – No known vulnerabilities were detected based on the scripts run.

⚠️ **“Some ports did not respond to vulnerability probes”** – The device or its firewall may be **blocking or filtering** deeper vulnerability checks.

# If ports are not responding to vuln probes, it's likely the **device has some firewalling** or **service hardening** in place — which is a **good sign** for security.

Device 2 & 3 & 4: Same output as device-1 : No Open ports detected and are not vulnerable.

DEVICE 5:

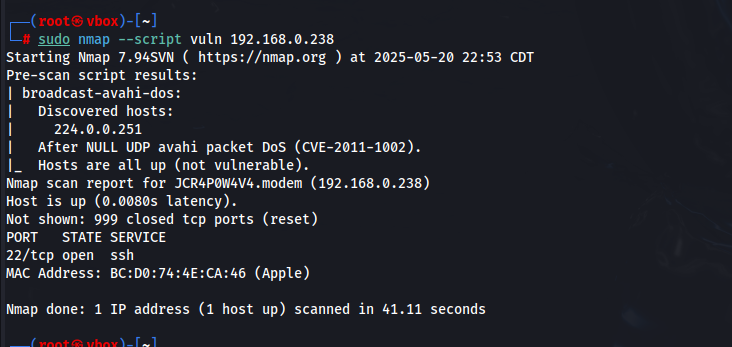




⚠️ **“Does not appear to be vulnerable”** – No known vulnerabilities were detected based on the scripts run.

⚠️ **“Some ports did not respond to vulnerability probes”** – The device or its firewall may be **blocking or filtering** deeper vulnerability checks.

Device 6:





It is a potential Risk.

**SSH Open on Apple Device** (22/tcp):

* Disable SSH if not needed:

**BitTorrent Port Open** (6881/tcp)

* Check if file-sharing apps are running.
* Disable if not intentionally in use to reduce exposure.

**Unknown Devices Detected**

* Double-check MAC addresses via router admin interface.
* If unknown devices persist, **change Wi-Fi password** and use **WPA3 encryption** if supported.

CONCLUSION:

This home network audit revealed open ports and services on several devices. Notably, SSH was enabled on an Phone-2 device, and peer-to-peer services were open on another. Appropriate actions were taken to disable unnecessary services, identify unknown devices, and strengthen overall network security.