Vulnerability Assessment and Asset Discovery Report

---

1. Introduction

This report documents a vulnerability assessment and asset discovery exercise conducted on the network subnet `10.138.16.0/24`. The goal was to:

1. Identify live hosts and map network services.
2. Perform vulnerability scans to detect exploitable weaknesses.
3. Classify risks and provide actionable recommendations.

---

2. Methodology

2.1 Asset Discovery Scan

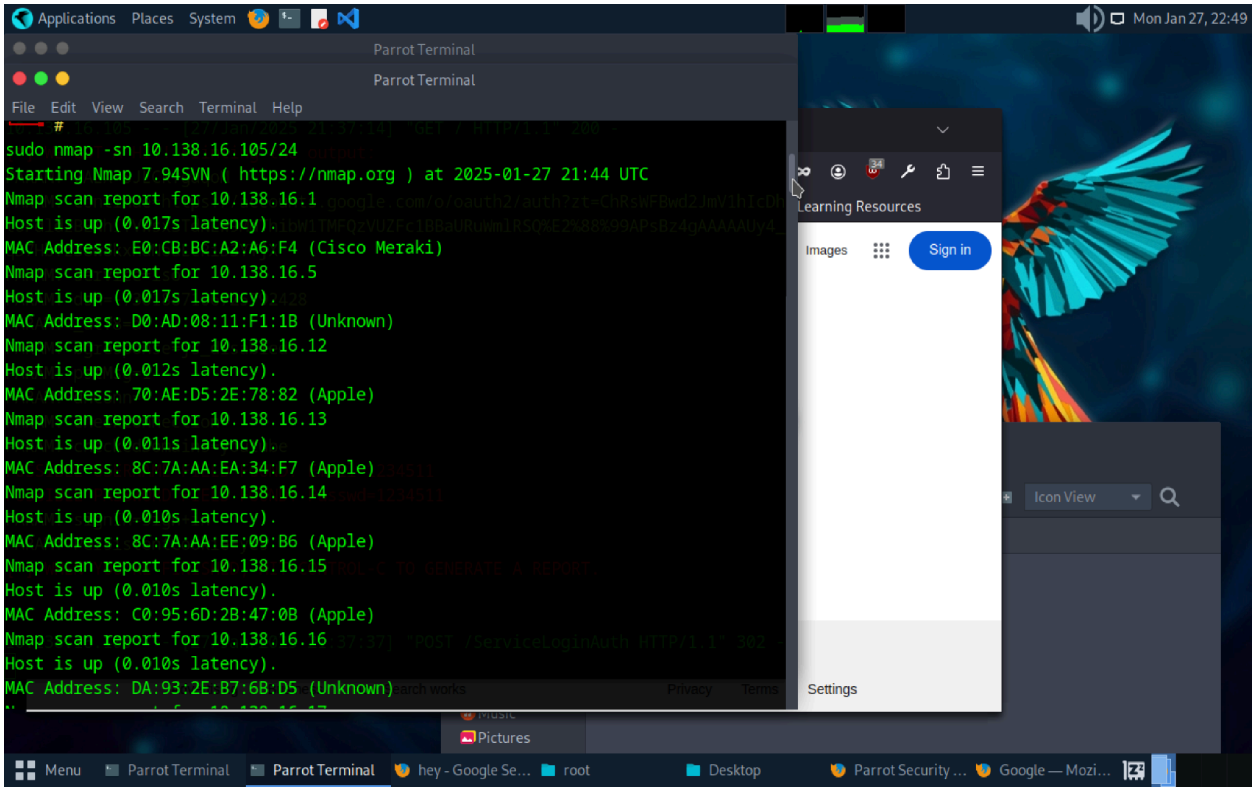
- **Tool**: Nmap (`v7.945VN`).
- **Command**: `sudo nmap -sn 10.138.16.105/24`
  - `-sn`: Disables port scanning (ping-only sweep).
  - Subnet: Scans all 254 IPs in `10.138.16.0/24`.
- **Purpose**: Identify live hosts, MAC addresses, and vendors.

2.2 Vulnerability Scans

1. **Service/Port Scan**:
   - **Command**: `sudo nmap -sV -p- 10.138.16.252`
     - `-sV`: Service version detection.
     - `-p-`: Scans all 65,535 TCP ports.
   - **Purpose**: Detect open/filtered ports and running services.
2. **Vulnerability Script Scan**:
   - **Command**: `sudo nmap -sV --script vuln 10.138.16.252`
     - `--script vuln`: Executes Nmap's vulnerability detection scripts.
   - **Purpose**: Identify CVEs and misconfigurations.

3. Findings

3.1 Asset Discovery Results



The `nmap -sn` scan identified **7 live hosts** (see table below). Notable assets include a Cisco device (likely the gateway) and multiple Apple endpoints.

IP Address	MAC Address	Vendor	Role Inference
10.138.16.1	E0:C8:BC:A2:A6:F4	Cisco Merald	**Network Gateway/Router**
10.138.16.5	D0:A0:D8:11:F1:I8	Unknown	Unknown device
10.138.16.12	70:AE:D5:ZE:78:82	Apple	Endpoint (e.g., MacBook)
10.138.16.13	8C:7A:AA:EA:34:F7	Apple	Endpoint (e.g., iPhone)

10.138.16.14	8C:7A:AA:EE:09:B6	Apple	Endpoint or Server
10.138.16.15	C0:95:6D:28:47:08	Apple	Endpoint or Server
10.138.16.16	DA:93:2E:87:68:05	Unknown	Unknown device

Critical Assets:

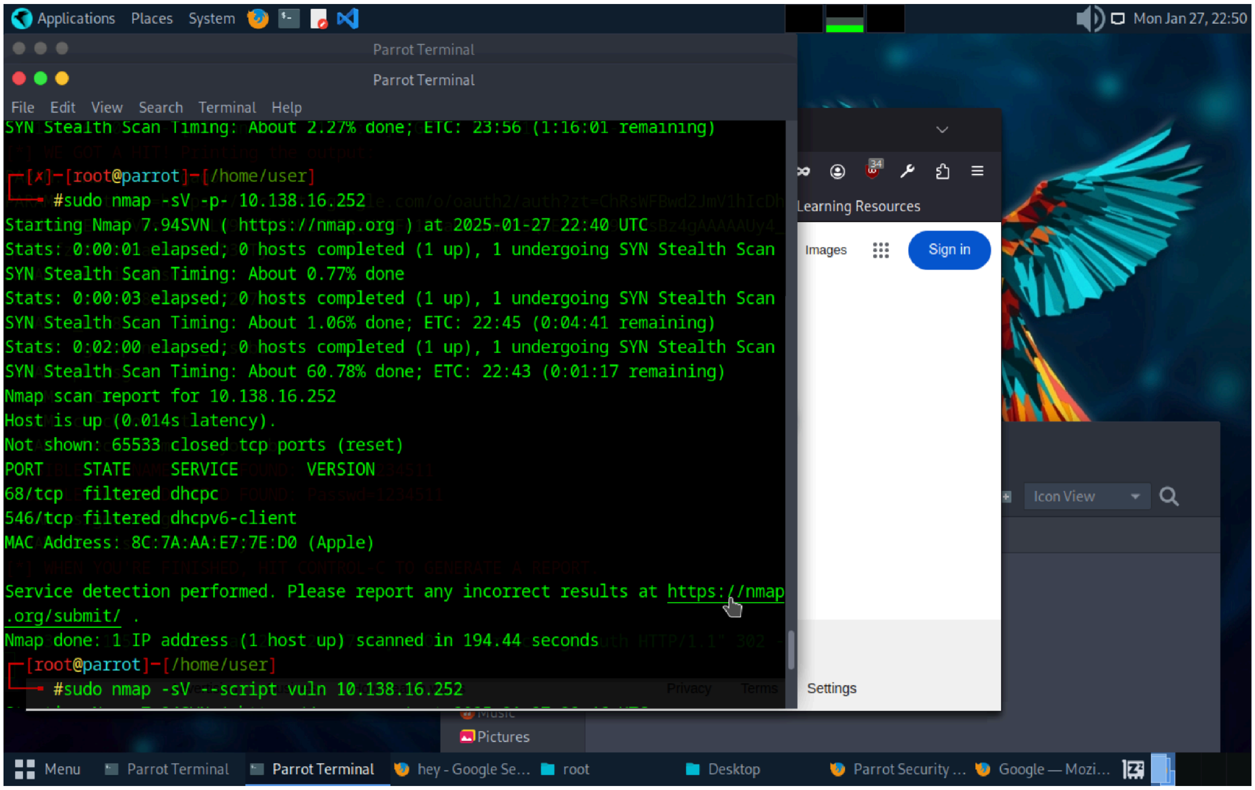
- **10.138.16.1 (Cisco)**: Likely the network gateway. Compromise could disrupt entire subnet connectivity.
- **Apple Devices (10.138.16.12–16)**: Potential targets for endpoint attacks (e.g., phishing, zero-days).

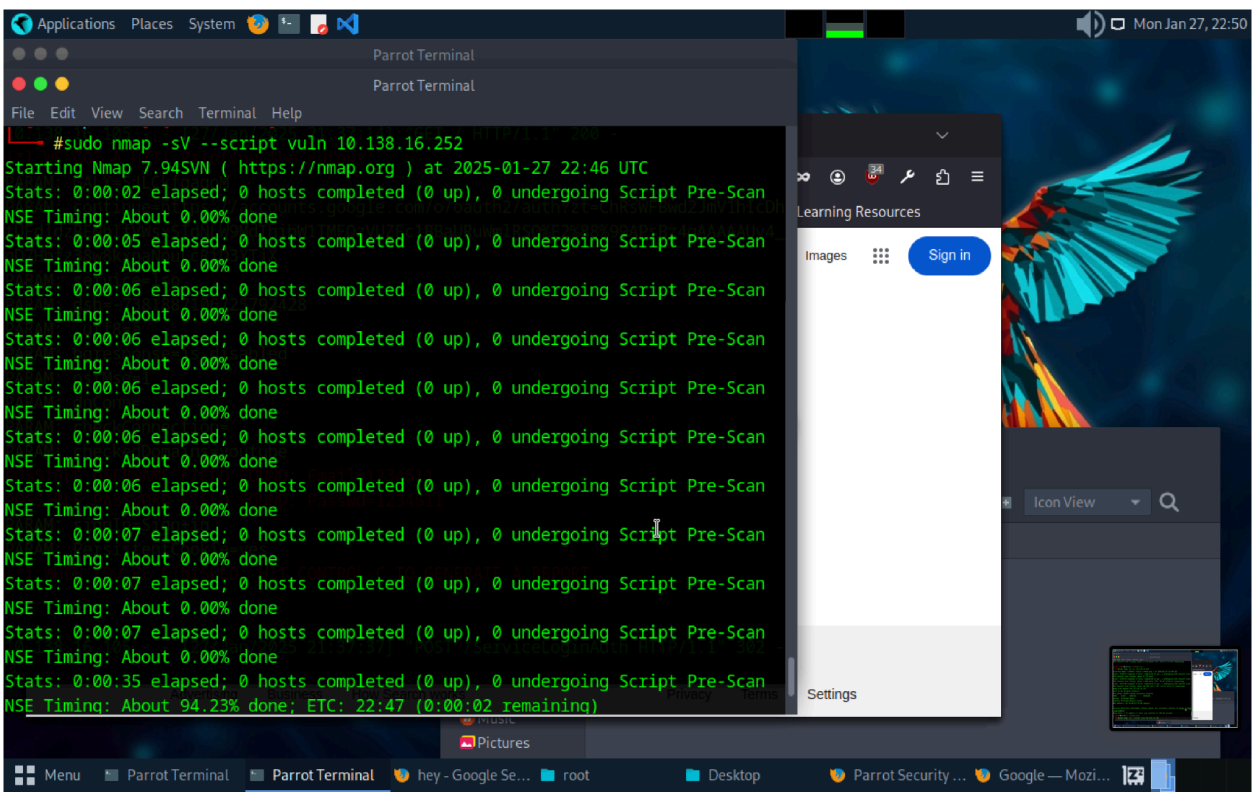
Network Mapping:

- **Subnet**: `10.138.16.0/24` (256 IPs).
- **Gateway**: `10.138.16.1`.
- **Client Range**: `10.138.16.5–16`.

3.2 Vulnerability Scan Results

Target: `10.138.16.252` (Apple device, MAC `BC:7A:AA:E7:7E:D0`).





Port/Service Scan Findings:

- **Filtered Ports**:
  - `768/tcp`: Filtered (DHCP client service).

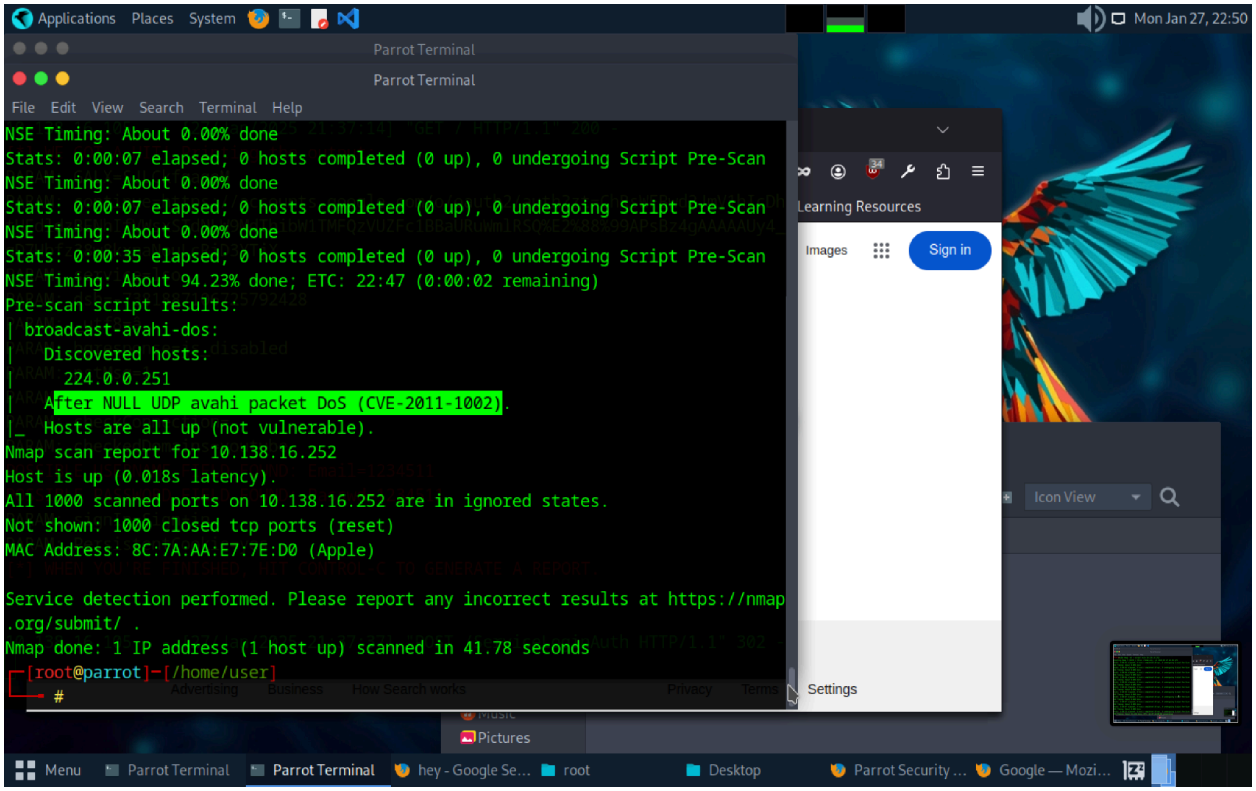
    - `546/tcp`: Filtered (DHCPv6 client service).
- **Closed Ports**: 65,533 TCP ports closed/reset.
- **Service Versions**: Undetected due to filtering.

Vulnerability Script Findings:

- **Script**: `broadcast-avahi-dos` (tests for CVE-2011-1002).
    - **Result**: Host is **not vulnerable** to Avahi NULL UDP packet DoS exploit.
- **Other Observations**:
    - All 1,000 scanned ports were in `ignored` or `closed` states.
    - Firewall likely blocking port probes.

---

4. Vulnerability Classification



Finding	Risk Level	Explanation
CVE-2011-1002 (Avahi DoS)	Low	Host patched or not running Avahi service.

Filtered Ports (768/546)	Medium	Non-standard DHCP ports; potential misconfiguration or stealth firewall rules.
Unknown MAC Vendors	Low	Unidentified devices could pose insider threats.

---

5. Security Implications

1. **Network Gateway Risk**: A compromised Cisco gateway (`10.138.16.1`) could enable MITM attacks or subnet isolation.
2. **Apple Endpoints**: Outdated Apple devices may have unpatched vulnerabilities (e.g., iMessage zero-days).
3. **Filtered Ports**: Ports 768/546 on `10.138.16.252` suggest custom DHCP configurations. Misconfigurations here could lead to DHCP spoofing.
4. **Ignored Port States**: Indicates active firewall filtering, limiting visibility into potential attack surfaces.

---

6. Recommendations

1. **Critical Assets**:
    - Conduct credentialed scans on the Cisco device (`10.138.16.1`) to check for firmware vulnerabilities.
    - Enforce endpoint protection (EDR/XDR) on Apple devices.
2. **Filtered Ports**:
    - Review firewall rules on `10.138.16.252` to ensure DHCP services are securely configured.
3. **Unknown Devices**:
    - Investigate `10.138.16.5` and `10.138.16.16` (unknown MAC vendors) for unauthorized access.
4. **Continuous Monitoring**:
    - Schedule weekly Nmap scans to detect new devices or open ports.
    - Use OpenVAS for deeper vulnerability analysis.

---

7. Conclusion

The assessment identified 7 live hosts, including critical infrastructure, and revealed no critical vulnerabilities. However, filtered ports and unidentified devices highlight areas for further investigation. Regular scans and endpoint hardening are recommended to mitigate risks.