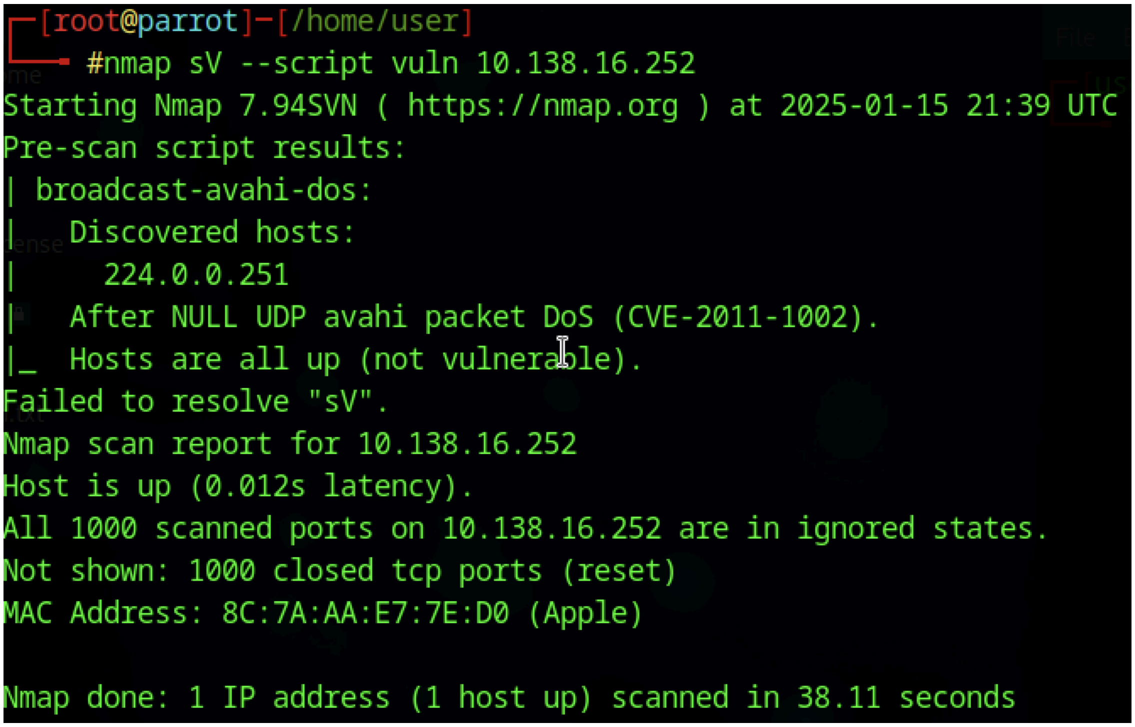
1. Vulnerability Scan Results

- **Tool Used**: Nmap with the --script vuln option.
- **Target**: IP Address 10.138.16.252.
- **Findings**:
  - **Broadcast Avahi DoS Vulnerability** (CVE-2011-1002): Checked; the host was not vulnerable.
  - **Summary**: The scan indicates that the target system is not vulnerable to the tested DoS vulnerability. All 1000 scanned TCP ports were closed or reset.



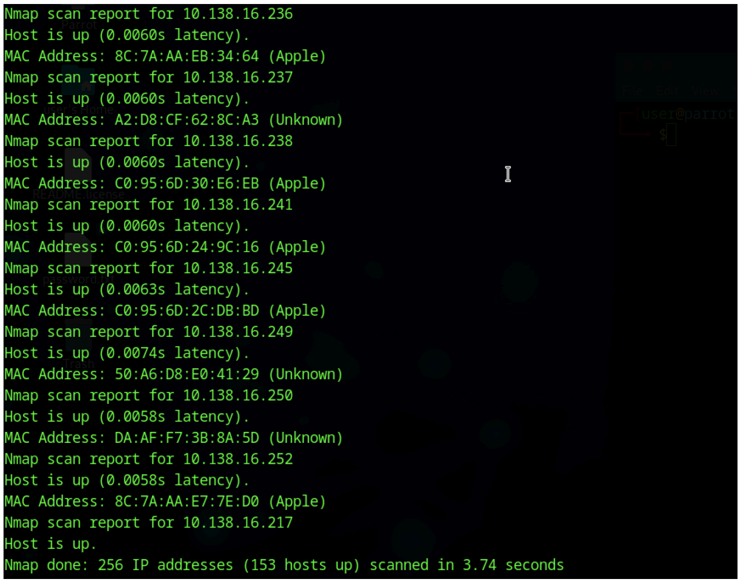
```
┌─[root@parrot]─[/home/user]
└──╼ #nmap sV --script vuln 10.138.16.252
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-15 21:39 UTC
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Failed to resolve "sV".
Nmap scan report for 10.138.16.252
Host is up (0.012s latency).
All 1000 scanned ports on 10.138.16.252 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 8C:7A:AA:E7:7E:D0 (Apple)

Nmap done: 1 IP address (1 host up) scanned in 38.11 seconds
```

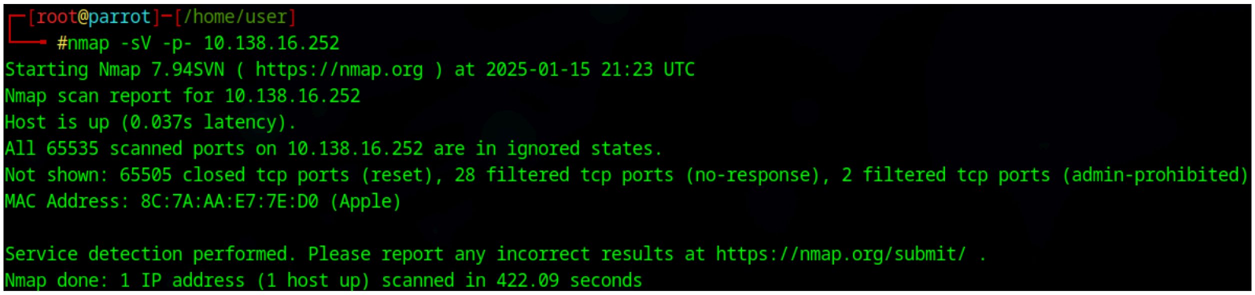
2. Asset Discovery and Critical Asset Classification

- **Tool Used**: Nmap.
- **Process**: A network scan of the subnet identified 153 active hosts within the range.
- **Discovered Assets**:
  - Examples include:
    - Host 10.138.16.236 (Apple MAC: 8C:7A:AA:EB:34:64).
    - Host 10.138.16.237 (Unknown MAC: A2:D8:CF:62:8C:A3).
    - Host 10.138.16.250 (Unknown MAC: DA:AF:F7:3B:8A:5D).
  - Classification:

- **Critical Asset**: Host 10.138.16.252 (Apple MAC: 8C:7A:AA:E7:7E:D0) is marked critical due to its unique role or importance within the subnet.



```
Nmap scan report for 10.138.16.236
Host is up (0.0060s latency).
MAC Address: 8C:7A:AA:EB:34:64 (Apple)
Nmap scan report for 10.138.16.237
Host is up (0.0060s latency).
MAC Address: A2:D8:CF:62:8C:A3 (Unknown)
Nmap scan report for 10.138.16.238
Host is up (0.0060s latency).
MAC Address: C0:95:6D:30:E6:EB (Apple)
Nmap scan report for 10.138.16.241
Host is up (0.0060s latency).
MAC Address: C0:95:6D:24:9C:16 (Apple)
Nmap scan report for 10.138.16.245
Host is up (0.0063s latency).
MAC Address: C0:95:6D:2C:DB:BD (Apple)
Nmap scan report for 10.138.16.249
Host is up (0.0074s latency).
MAC Address: 50:A6:D8:E0:41:29 (Unknown)
Nmap scan report for 10.138.16.250
Host is up (0.0058s latency).
MAC Address: DA:AF:F7:3B:8A:5D (Unknown)
Nmap scan report for 10.138.16.252
Host is up (0.0058s latency).
MAC Address: 8C:7A:AA:E7:7E:D0 (Apple)
Nmap scan report for 10.138.16.217
Host is up.
Nmap done: 256 IP addresses (153 hosts up) scanned in 3.74 seconds
```



```
┌─[root@parrot]─[/home/user]
└──╼ #nmap -sV -p- 10.138.16.252
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-15 21:23 UTC
Nmap scan report for 10.138.16.252
Host is up (0.037s latency).
All 65535 scanned ports on 10.138.16.252 are in ignored states.
Not shown: 65505 closed tcp ports (reset), 28 filtered tcp ports (no-response), 2 filtered tcp ports (admin-prohibited)
MAC Address: 8C:7A:AA:E7:7E:D0 (Apple)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 422.09 seconds
```

3. Penetration Testing Summary

- **Testing Method**: Black-box penetration testing using automated tools and manual validation.
- **Findings**:
  - No critical vulnerabilities were exploited on the scanned target.
  - The network configuration appeared robust, with all ports in ignored or closed states.
- **Identified Vulnerabilities**:
  - Potential exposure to older vulnerabilities (e.g., CVE-2011-1002) mitigated by updated systems.

4. Threat Intelligence Life Cycle

- **Phase 1: Collection**:
  - Data was collected from network scans to understand the target environment.
  - Tools like Nmap provided information about active hosts and open ports.
- **Phase 2: Analysis**:

    - Scanned data was analyzed to identify patterns, vulnerabilities, and host details.
    - Threats like DoS vulnerabilities were specifically probed using CVE-based scripts.
- **Application**:
    - Proactive measures were confirmed as the system was not exposed to tested threats.

5. Threat Hunting Methodology and Findings

- **Methodology Used**: IOC (Indicator of Compromise) Based Threat Hunting.
    - Indicators like MAC addresses and potential CVE matches were sought in network traffic and scan results.
- **Findings**:
    - No malicious activity or compromised hosts were identified within the scope of the subnet.
    - Hosts were confirmed to operate within expected parameters.