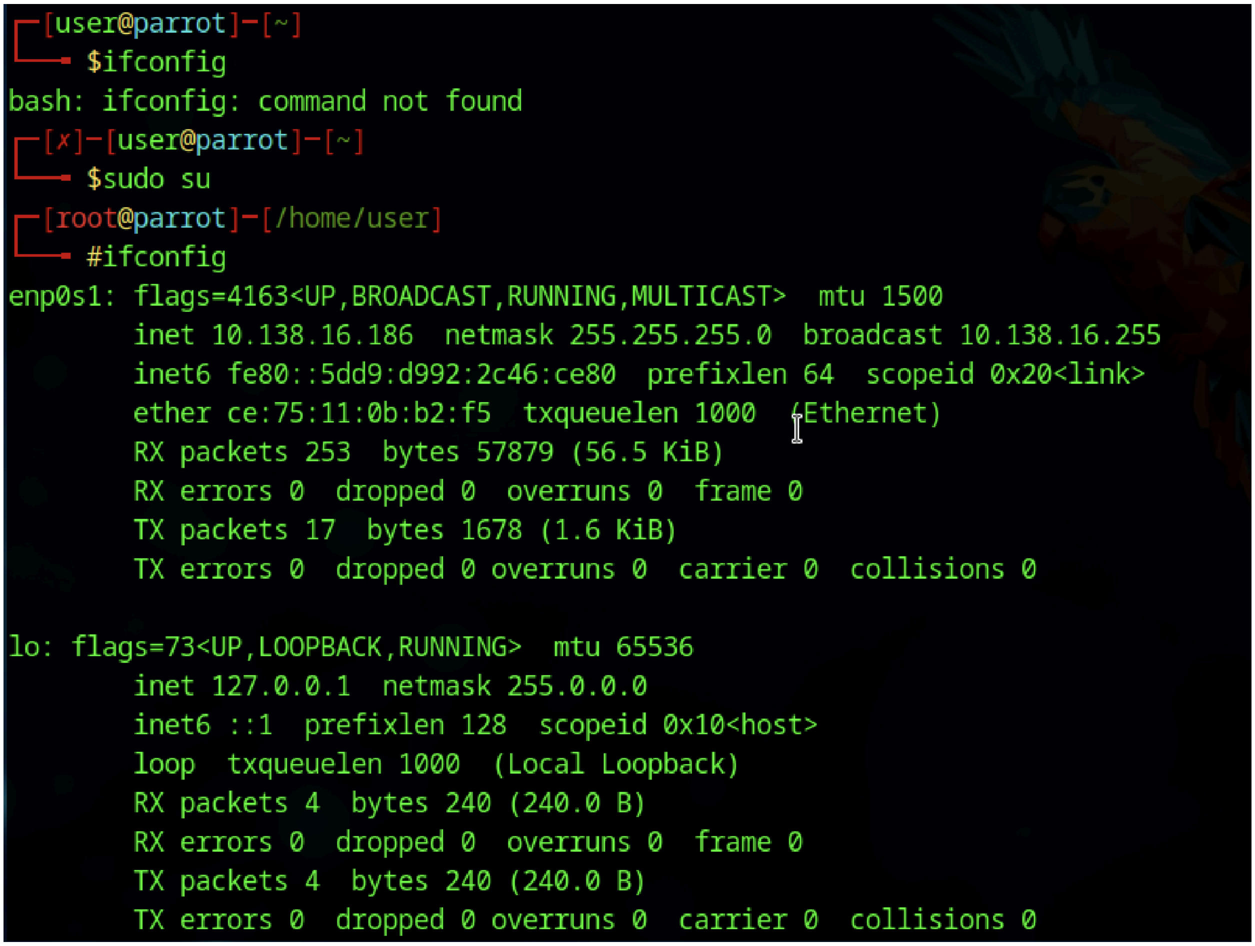
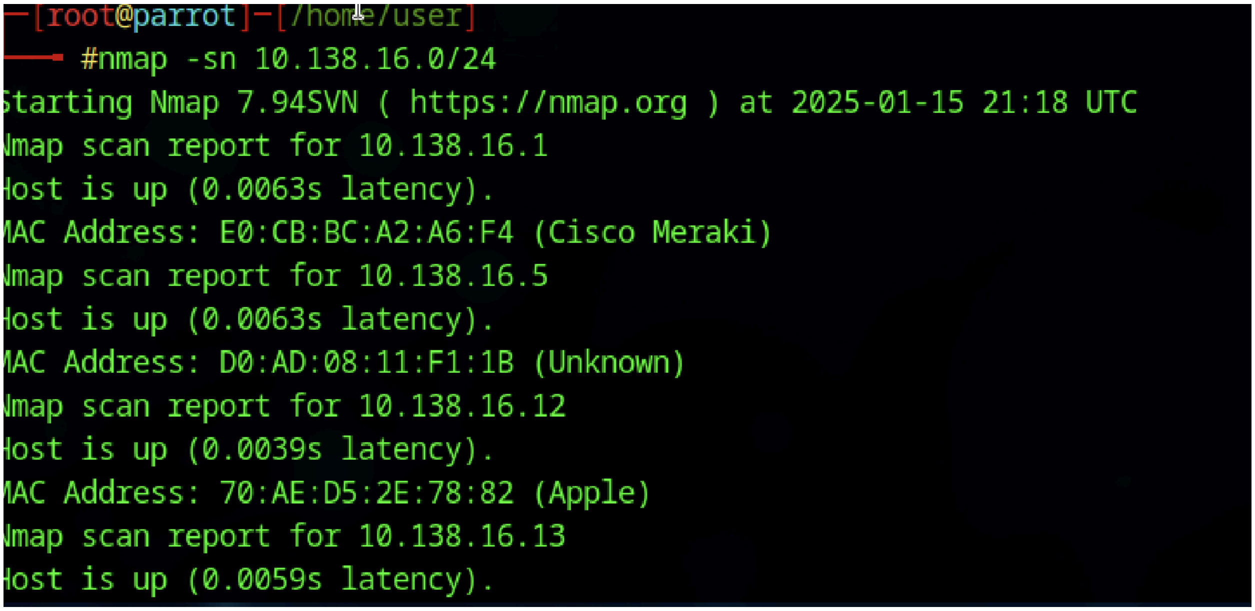
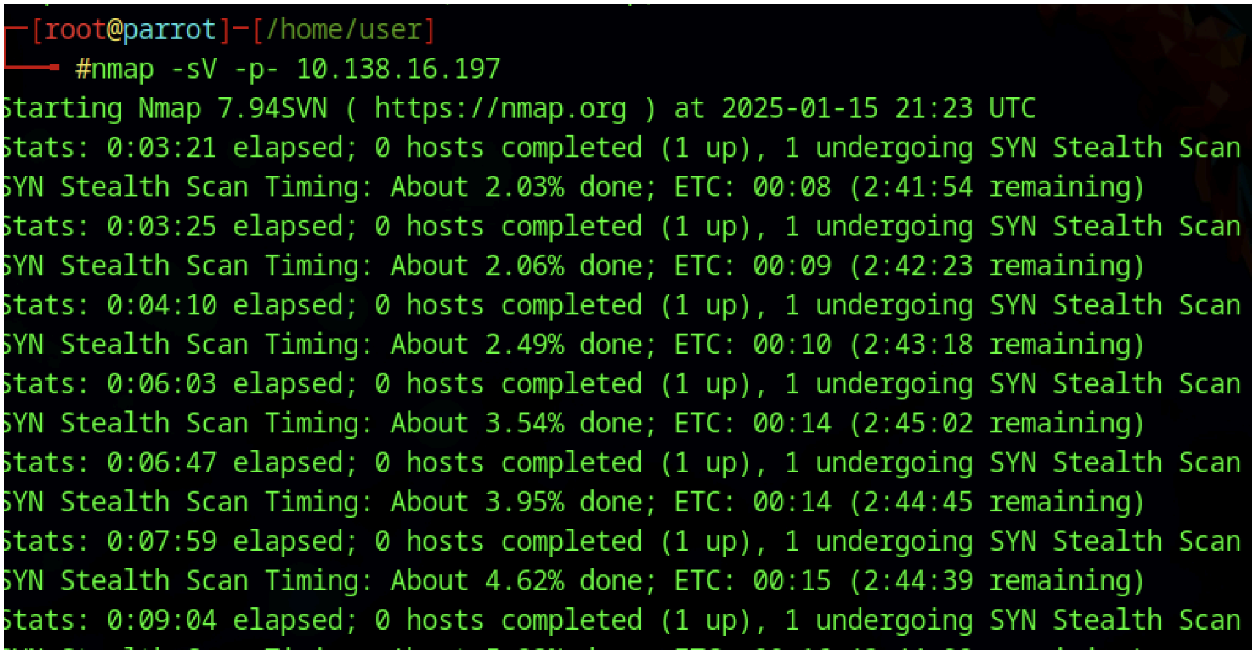


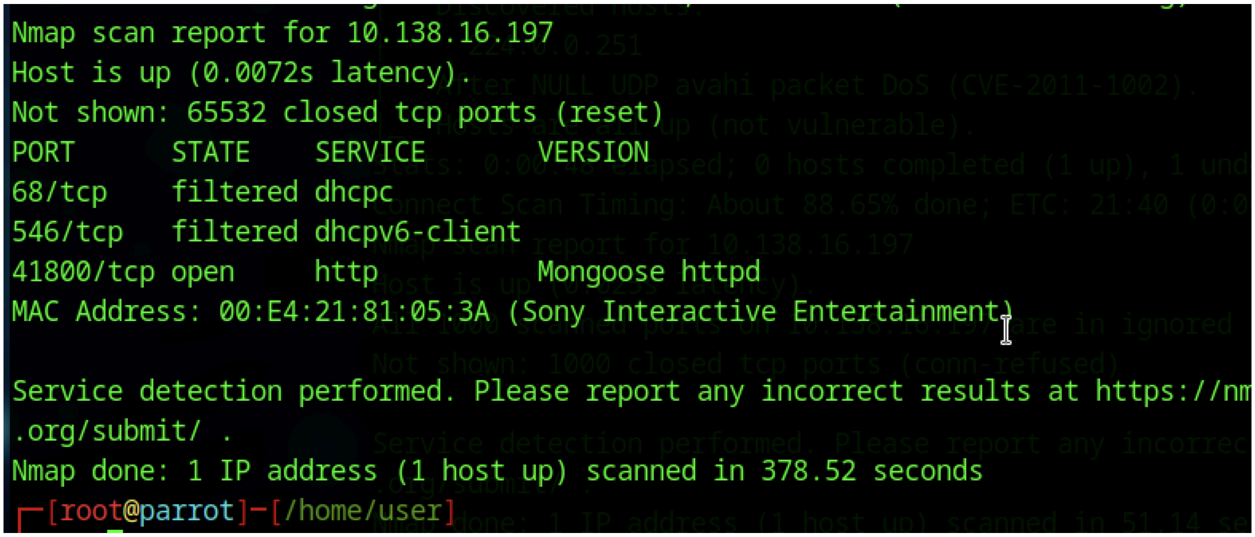
```
┌─[user@parrot]─[~]
└──╼ $ifconfig
bash: ifconfig: command not found
┌─[✗]─[user@parrot]─[~]
└──╼ $sudo su
┌─[root@parrot]─[/home/user]
└──╼ #ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.138.16.186  netmask 255.255.255.0  broadcast 10.138.16.255
        inet6 fe80::5dd9:d992:2c46:ce80  prefixlen 64  scopeid 0x20<link>
        ether ce:75:11:0b:b2:f5  txqueuelen 1000  (Ethernet)
        RX packets 253  bytes 57879 (56.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17  bytes 1678 (1.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



```
─[root@parrot]─[/home/user]
──╼ #nmap -sn 10.138.16.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-15 21:18 UTC
Nmap scan report for 10.138.16.1
Host is up (0.0063s latency).
MAC Address: E0:CB:BC:A2:A6:F4 (Cisco Meraki)
Nmap scan report for 10.138.16.5
Host is up (0.0063s latency).
MAC Address: D0:AD:08:11:F1:1B (Unknown)
Nmap scan report for 10.138.16.12
Host is up (0.0039s latency).
MAC Address: 70:AE:D5:2E:78:82 (Apple)
Nmap scan report for 10.138.16.13
Host is up (0.0059s latency).
```



```
┌─[root@parrot]─[/home/user]
└──╼ #nmap -sV -p- 10.138.16.197
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-15 21:23 UTC
Stats: 0:03:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.03% done; ETC: 00:08 (2:41:54 remaining)
Stats: 0:03:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.06% done; ETC: 00:09 (2:42:23 remaining)
Stats: 0:04:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.49% done; ETC: 00:10 (2:43:18 remaining)
Stats: 0:06:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.54% done; ETC: 00:14 (2:45:02 remaining)
Stats: 0:06:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.95% done; ETC: 00:14 (2:44:45 remaining)
Stats: 0:07:59 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 4.62% done; ETC: 00:15 (2:44:39 remaining)
Stats: 0:09:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
```



```
Nmap scan report for 10.138.16.197
Host is up (0.0072s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE    SERVICE        VERSION
68/tcp    filtered dhcpc
546/tcp   filtered dhcpv6-client
41800/tcp open     http           Mongoose httpd
MAC Address: 00:E4:21:81:05:3A (Sony Interactive Entertainment)

Service detection performed. Please report any incorrect results at https://nm
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 378.52 seconds
┌─[root@parrot]─[/home/user]
```

Methodology Used:

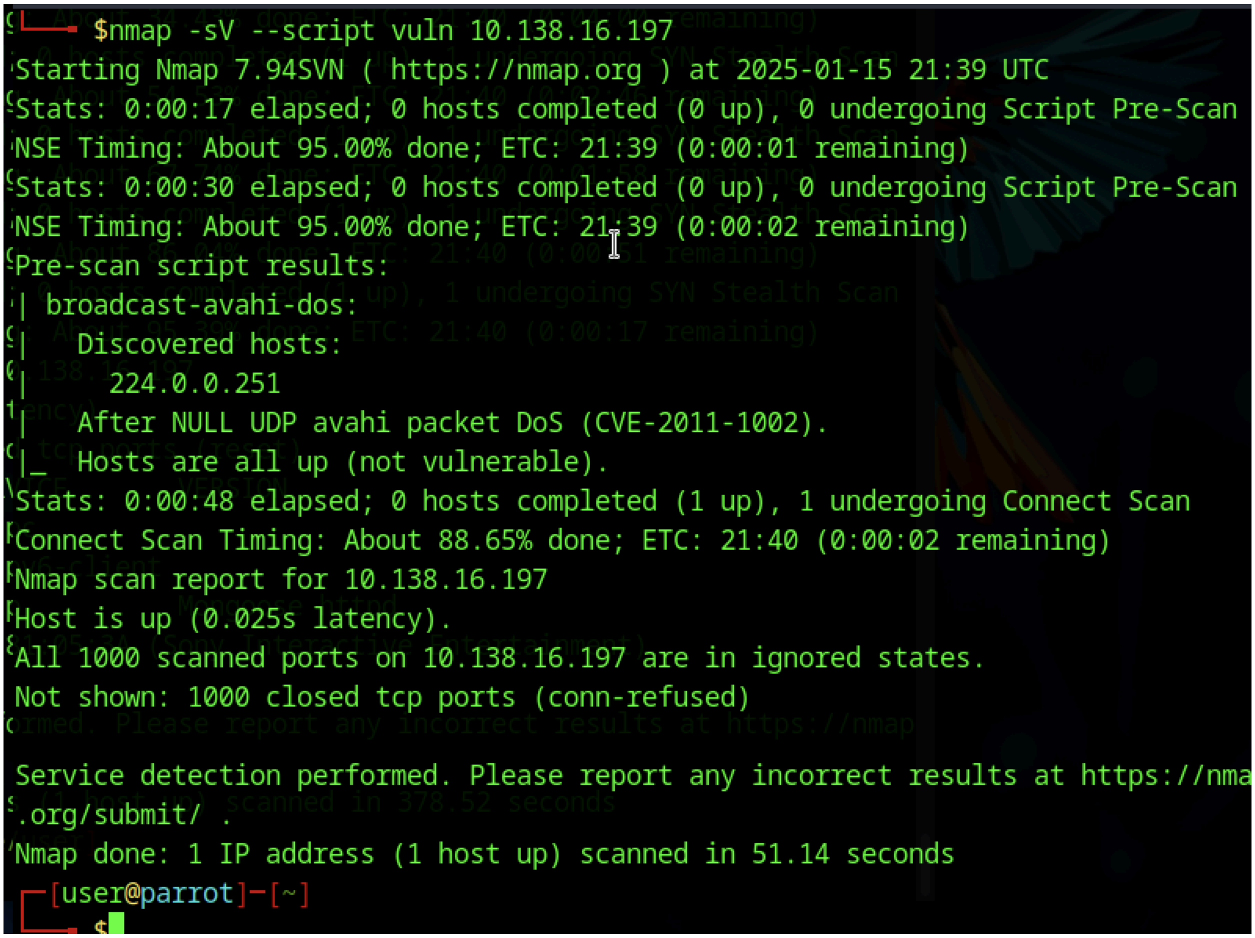
1. **Nmap Tool**:
   - The scan was performed using **Nmap (Network Mapper)**, a tool commonly used for network discovery and security auditing.
2. **Host Identification**:
   - The tool identified the target host at the IP address **10.138.16.197**. It confirmed the host is reachable (latency: 0.0072 seconds).
3. **Port Scanning**:
   - The scan revealed:
     - **65532 closed TCP ports** were detected.
     - Specific ports:

- **68/tcp** (DHCP) - Filtered.
- **546/tcp** (DHCPv6-client) - Filtered.
- **41800/tcp** (HTTP) - Open, running the **Mongoose HTTPD server**.

4. **MAC Address and Device Information**:
    - The MAC address **00:E4:21:81:05:3A** was detected.
    - The vendor information, **Sony Interactive Entertainment**, suggests the device might be related to PlayStation or other Sony hardware.
5. **Service Detection**:
    - A service detection scan identified an HTTP service (Mongoose HTTPD) on port 41800.

Potential Security Implications

1. **Open Port (41800/tcp)**:
    - An open HTTP port indicates a web server is running on the device.
    - **Vulnerability Risk**:
        - If the Mongoose HTTPD server has known vulnerabilities, it could be exploited for unauthorized access or attacks.
    - **Recommendation**:
        - Ensure the web server is updated with the latest patches and configured securely.
2. **Filtered Ports**:
    - **DHCP (68/tcp)** and **DHCPv6 (546/tcp)** are filtered, indicating possible firewall rules or security measures are in place. While this is generally good, misconfigured filters could still be exploited.
3. **Vendor-Specific Device (Sony Interactive Entertainment)**:
    - Devices like gaming consoles can sometimes run outdated or vulnerable firmware, especially if not regularly updated.
    - **Recommendation**:
        - Regularly update the device firmware and disable unnecessary services.
4. **Potential Exposure of Internal Network**:
    - Scanning an internal IP (10.x.x.x) indicates an internal network. If the scan results were shared or exposed externally, it could reveal sensitive network details to attackers.
5. **Mongoose HTTPD**:
    - While lightweight and efficient, Mongoose HTTPD has previously been targeted in exploits (depending on the version). Ensure that:
        - Authentication is enabled.
        - Only trusted connections are allowed.
        - Sensitive data is not served over HTTP.



```
└──╼ $nmap -sV --script vuln 10.138.16.197
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-15 21:39 UTC
Stats: 0:00:17 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 95.00% done; ETC: 21:39 (0:00:01 remaining)
Stats: 0:00:30 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 95.00% done; ETC: 21:39 (0:00:02 remaining)
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).
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 88.65% done; ETC: 21:40 (0:00:02 remaining)
Nmap scan report for 10.138.16.197
Host is up (0.025s latency).
All 1000 scanned ports on 10.138.16.197 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nma
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.14 seconds
┌─[user@parrot]─[~]
└──╼ $
```

Methodology Used

Command Used:

css

Copy code

```
nmap -sV --script vuln 10.138.16.197
```

1.
   - `-sV`: Enables service version detection to identify the software version of services running on the host.
   - `--script vuln`: Uses Nmap Scripting Engine (NSE) to run vulnerability detection scripts. These scripts look for known vulnerabilities like outdated software, misconfigurations, or exposed attack surfaces.
2. **Scan Execution**:
   - **Pre-scan Script Results**:
     - The `broadcast-avahi-dos` vulnerability (CVE-2011-1002) was tested, and the hosts were confirmed **not vulnerable**.
   - **Host Discovery**:

        - Identified the target host at IP **10.138.16.197**, confirming it is active with a latency of 0.025 seconds.
    - **Port Scan**:
        - All **1000 scanned TCP ports** were in "closed" status (connection refused).
        - This suggests that the host has either a strict firewall or no exposed services on common TCP ports.
3. **Vulnerability Assessment**:
    - Scripts checked for specific vulnerabilities but no issues were reported in the screenshot.

Potential Security Implications

1. **Effective Security Posture**:
    - Since all scanned TCP ports are closed, the system seems to be well-secured at the network level.
    - The **vulnerability script** confirms that the device is not exposed to the CVE-2011-1002 DoS attack. This indicates proper handling of known vulnerabilities.
2. **Use of `--script vuln`**:
    - This script searches for specific vulnerabilities and can reveal outdated software or misconfigurations if found. Regular use is helpful for:
        - Identifying weak points before attackers do.
        - Ensuring compliance with security best practices.
3. **Possibility of Targeting**:
    - If this scan were conducted on a network without authorization, it could be part of reconnaissance for malicious purposes. This highlights the need for monitoring tools to detect unauthorized scans.
4. **Firewall and IDS Configuration**:
    - While the closed ports indicate a secure setup, it’s crucial to ensure:
        - Firewalls are correctly configured and do not leak unnecessary information.
        - Intrusion Detection Systems (IDS) are in place to log and alert on port scans or vulnerability checks.