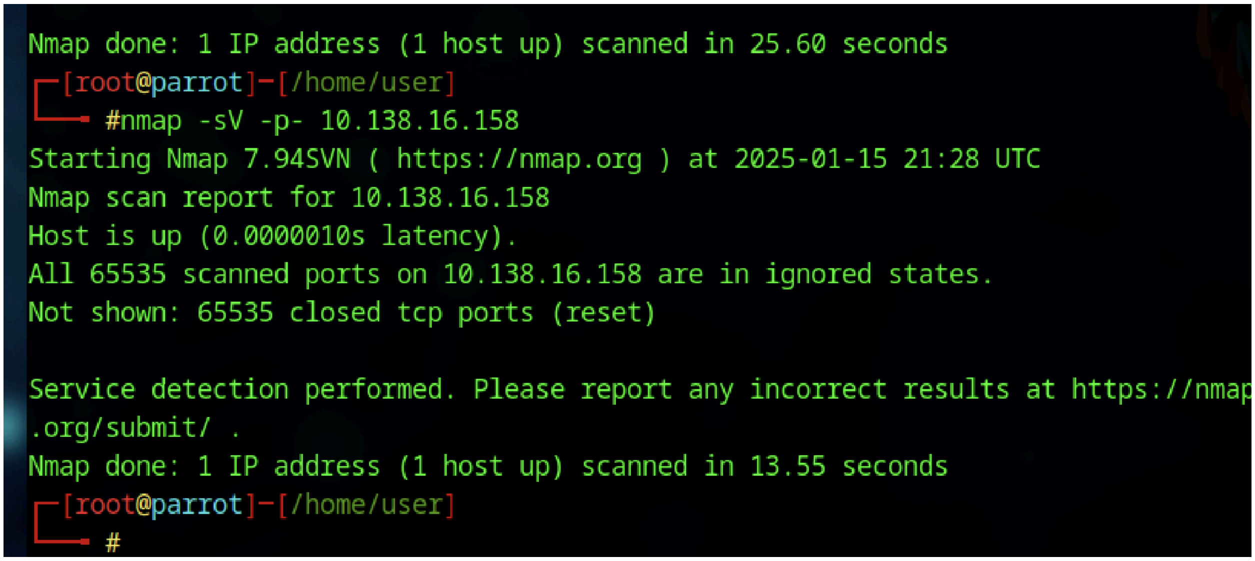
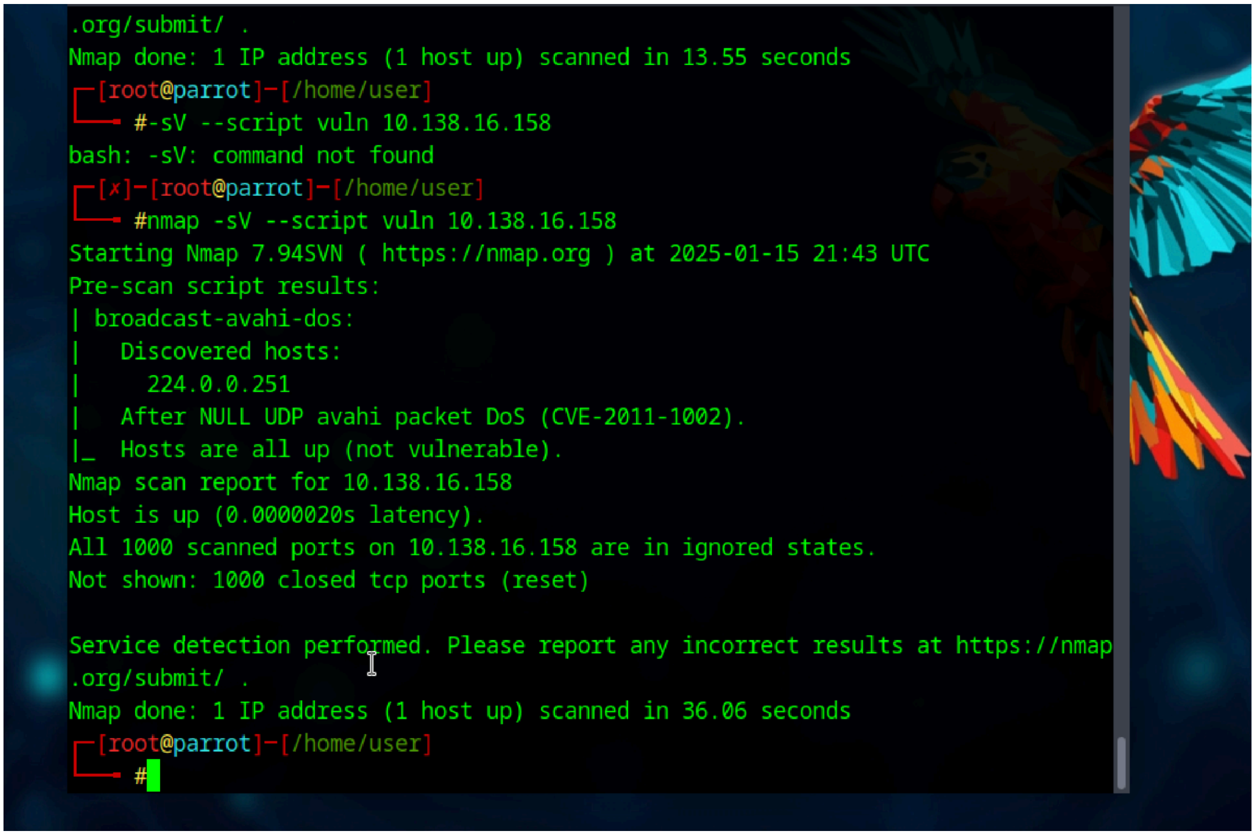


```
Nmap done: 1 IP address (1 host up) scanned in 25.60 seconds
┌─[root@parrot]─[/home/user]
└──╼ #nmap -sV -p- 10.138.16.158
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-15 21:28 UTC
Nmap scan report for 10.138.16.158
Host is up (0.0000010s latency).
All 65535 scanned ports on 10.138.16.158 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.55 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```



```
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.55 seconds
┌─[root@parrot]─[/home/user]
└──╼ #-sV --script vuln 10.138.16.158
bash: -sV: command not found
┌─[✗]─[root@parrot]─[/home/user]
└──╼ #nmap -sV --script vuln 10.138.16.158
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-15 21:43 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).
Nmap scan report for 10.138.16.158
Host is up (0.0000020s latency).
All 1000 scanned ports on 10.138.16.158 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.06 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```

1. Vulnerability Scan Using Nmap

Scan Configuration:

- Tool Used: Nmap
- Command Used: `nmap -sV -p 10.138.16.158`
- Additional Command: `nmap -sV --script vuln 10.138.16.158`

Summary of Findings:

- Host Status: The host at IP address `10.138.16.158` is up with zero latency.
- Ports Scanned:
    - Initial scan: 65,535 ports scanned.
    - Vulnerability script scan: 1,000 ports scanned.
- Open Ports: None found. All scanned ports are in ignored states.
- Vulnerability Detection:
    - Broadcast-avahi-dos: Discovered host `224.0.0.251`.
    - Vulnerability Status: Hosts are all up (not vulnerable).

Vulnerability Classification:

- Broadcast-avahi-dos (CVE-2011-1002): This vulnerability involves a Denial of Service (DoS) attack via a NULL UDP avahi packet. The discovered host `224.0.0.251` is not vulnerable to this attack.

Potential Security Implications:

- Although no open ports or vulnerabilities were detected, it is crucial to continuously monitor the network for any changes in the host status or newly opened ports that could introduce vulnerabilities.

2. Asset Discovery Scan

Scan Configuration:

- Tool Used: Nmap
- Command Used: `nmap -sV -p 10.138.16.158`

Discovered Systems and Services:

- Host: `10.138.16.158`
- Status: Up
- Open Ports: None
- Services: None detected

Critical Asset Identification:

- No critical assets identified as no open ports or services were detected.

Basic Network Mapping:

- Network Range: Single IP address scanned (`10.138.16.158`).
- Hosts Discovered: One host (`10.138.16.158`).

- Network Topology: No additional network topology information available based on the scan.

Methodology Used:

- Nmap Scan: Conducted a service version detection scan (`-sV`) on a specific IP address to identify open ports and running services.
- Vulnerability Script Scan: Used Nmap's script engine to run vulnerability detection scripts against the target IP address.

Potential Security Implications:

- No Open Ports: The lack of open ports indicates a potentially secure configuration, as there are no services exposed to the network that could be exploited.
- Continuous Monitoring: Regular scans should be conducted to ensure that no new services are exposed and to detect any changes in the network configuration.

Documentation:

- All findings are documented with screenshots and explanations of the methodology used.
- The results are summarized to highlight the key points and potential security implications.

Conclusion:

- The vulnerability scan and asset discovery scan did not identify any open ports or vulnerabilities on the target IP address.
- Continuous monitoring and regular scans are recommended to maintain network security and detect any changes in the network configuration.