

- Apply Vulnerability Assessment Techniques

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/user]
#ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.64.2 netmask 255.255.255.0 broadcast 192.168.64.255
    inet6 fd1b:7d22:a222:fcd:68ce:572:f78a:73e2 prefixlen 64 scopeid 0x0<
    global>
    ether 82:c:68:62:af:2e txqueuelen 1000 (Ethernet)
    RX packets 1489 bytes 1241798 (1.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 942 bytes 110628 (108.0 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]
#
```

```
Parrot Terminal
File Edit View Search Terminal Help

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.93 seconds
[root@parrot]~[/home/user]
#nmap -sV --script vuln 10.138.16.217
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).
Nmap scan report for 10.138.16.217
Host is up (0.018s latency).
All 1000 scanned ports on 10.138.16.217 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 8C:7A:AA:EB:D8:6A (Apple)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.34 seconds
[root@parrot]~[/home/user]
#
```

```
Parrot Terminal
File Edit View Search Terminal Help

Host is up.
Nmap done: 256 IP addresses (153 hosts up) scanned in 1.67 seconds
[root@parrot]~[/home/user]
#nmap -sV -p- [10.138.16.217]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-15 21:23 UTC
Failed to resolve "[10.138.16.217]".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.14 seconds
[root@parrot]~[/home/user]
#nmap -sV -p- 10.138.16.217
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-15 21:24 UTC
Nmap scan report for 10.138.16.217
Host is up (0.020s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
68/tcp    filtered dhcpc
546/tcp   filtered dhcpv6-client
MAC Address: 8C:7A:AA:EB:D8:6A (Apple)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.93 seconds
[root@parrot]~[/home/user]
#
```

- Asset Discovery Scan
  - Methodology:
    - The ifconfig command was initially used to identify the host's network interface details, including the IP address (192.168.64.2). Nmap was then utilized to conduct a network scan of the subnet, identifying live hosts and their basic details. The scan used the command nmap -sP

192.168.64.0/24, which performs a ping scan to discover systems within the network range.

- Findings:
  - The asset discovery identified multiple active hosts on the subnet, confirming the presence of 153 hosts out of 256 scanned IP addresses. This information provides a basic network mapping and an overview of potentially critical assets within the environment.
- Security Implications:
  - The discovered systems and their active states are critical for understanding the attack surface of the network. Ensuring these devices are secured and patched is necessary to reduce the likelihood of unauthorized access or exploitation.
- Vulnerability Scan
  - Methodology:
    - A targeted vulnerability scan was conducted on an identified host with IP 10.138.16.217. The following Nmap scans were performed:
  - 1. Service and Version Detection:
    - `nmap -sV -p- 10.138.16.217` to identify open ports and running services.
  - 2. Vulnerability Script Execution:
    - `nmap -sV --script vuln 10.138.16.217` to assess the target for known vulnerabilities using Nmap's vulnerability detection scripts.
- Findings:
  - Ports and Services:
    - The host showed no open TCP ports in the initial scan, with all detected ports either filtered or closed. This indicates strong firewall or network security configurations, limiting exposed services.
  - Vulnerability Assessment:
    - A pre-scan script result identified that the target was not vulnerable to the Avahi NULL UDP Packet DoS vulnerability (CVE-2011-1002). All other ports and services remained in ignored or filtered states, further confirming minimal exposure.
- Security Implications:
  - While the results show minimal vulnerabilities, the lack of open ports and identified services could either indicate a highly secure system or the presence of a host actively employing cloaking techniques. Continuous monitoring and deeper assessments may be required to validate these findings further.
- Conclusion and Documentation
  - The project effectively applied vulnerability assessment techniques through:
    - Asset Discovery: Identification and mapping of network systems and services.
    - Vulnerability Scanning: Detection of potential vulnerabilities and confirmation of secured configurations.