Vulnerability Assessment Report

Introduction

This report documents the vulnerability assessment conducted using Nmap on a target system. The assessment includes a vulnerability scan, asset discovery scan, and basic network mapping. The methodology used, findings, and potential security implications are detailed below.

Methodology

Vulnerability Scan

Tool Used: Nmap Scan Configuration:

- Command: `sudo nmap -sV -p- 10.138.16.66`
- Options:
    - `-sV`: Service version detection.
    - `-p-`: Scan all 65535 ports.

Date and Time: 2025-01-15 21:40 UTC

Asset Discovery Scan

Tool Used: Nmap Scan Configuration:

- Command: `sudo nmap -sn 10.138.16.66`
- Options:
    - `-sn`: No port scan, only host discovery.

Date and Time: 2025-01-15 21:26 UTC

Network Mapping

Tool Used: Nmap Scan Configuration:

- Command: `sudo nmap -sP 10.138.16.66`
- Options:
    - `-sP`: Ping scan to discover live hosts.

Date and Time: 2025-01-15 21:32 UTC

Findings

Vulnerability Scan Results

Target IP: 10.138.16.66 Host Status: Up Latency: 0.000030s

Open Ports: None Closed Ports: 65535

Pre-scan Script Results:

- broadcast-avahi-dos:
    - Discovered Hosts: 224.0.0.251
    - Vulnerability: After NULL UDP avahi packet DoS (CVE-2011-1002).
    - Status: Hosts are all up (not vulnerable).

Summary: The vulnerability scan did not identify any open ports or significant vulnerabilities on the target system. The pre-scan script detected a potential Denial of Service (DoS) vulnerability related to the Avahi service, but the hosts were found to be not vulnerable.

Asset Discovery Scan Results

Target IP: 10.138.16.66 Host Status: Up Latency: 0.000010s

Summary: The asset discovery scan confirmed that the target host is up and reachable. No additional services or open ports were identified.

Network Mapping Results

Target IP: 10.138.16.66 Host Status: Up Latency: 0.000010s

Summary: The network mapping scan confirmed the presence of the target host on the network. No additional hosts or services were discovered.

Vulnerability Classification

Potential Vulnerabilities

1. Denial of Service (DoS) Vulnerability:
    - CVE: CVE-2011-1002
    - Description: A NULL UDP avahi packet DoS vulnerability was detected. However, the hosts were found to be not vulnerable.
    - Impact: If exploited, this vulnerability could cause a denial of service, leading to system unavailability.
    - Mitigation: Ensure that the Avahi service is updated to the latest version and apply necessary patches.

Potential Security Implications

1. Denial of Service (DoS):
    - Although the scan indicated that the hosts are not vulnerable, the presence of a DoS vulnerability in the network can lead to service disruption if exploited. Regular patching and updating of services are crucial to mitigate such risks.
2. Network Security:
    - The absence of open ports suggests a well-configured firewall or security policy. However, continuous monitoring and regular vulnerability assessments are essential to maintain network security.

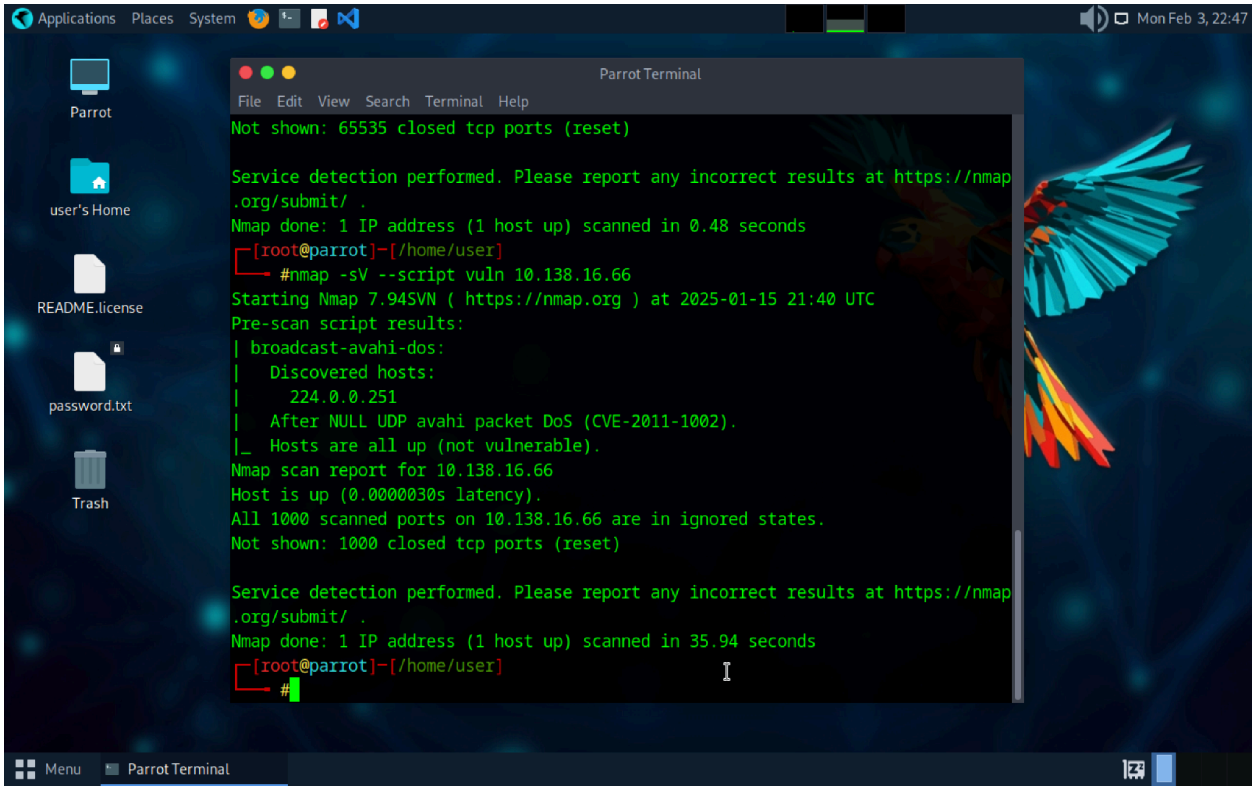
Conclusion

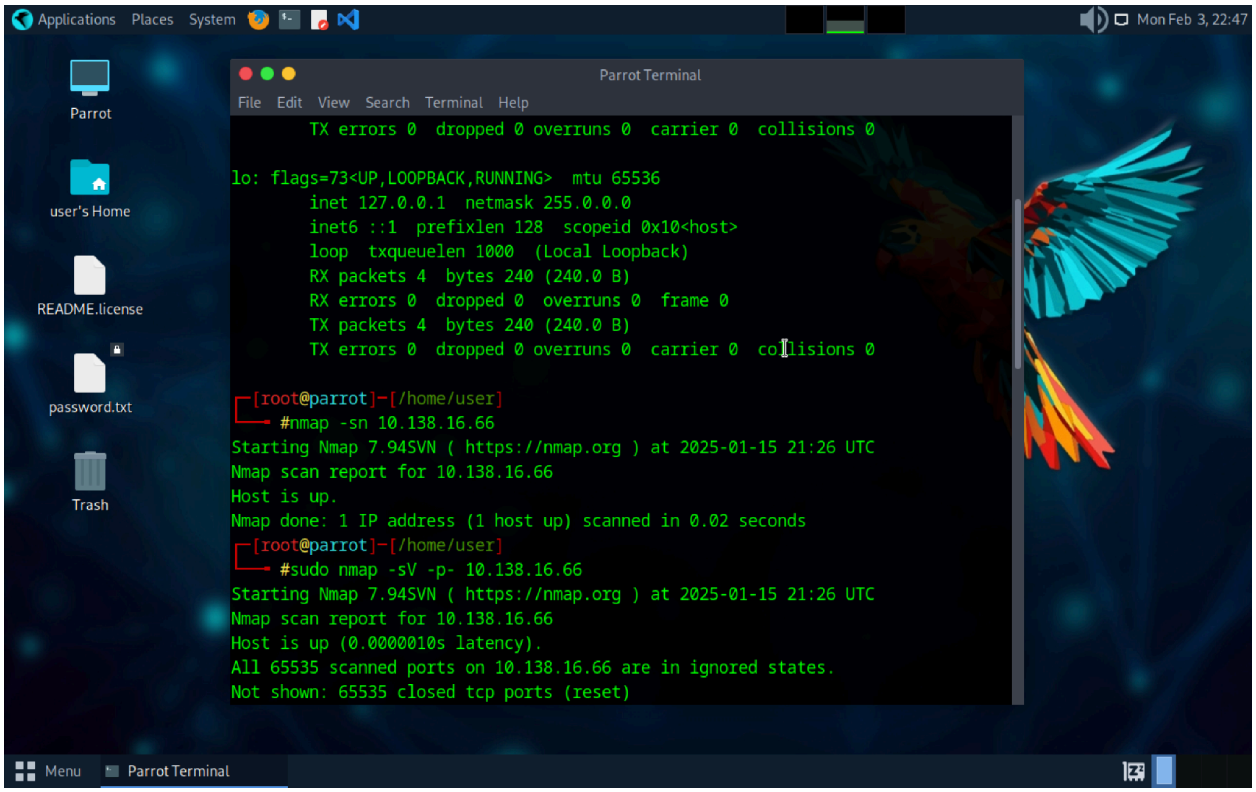
The vulnerability assessment conducted using Nmap did not identify any significant vulnerabilities or open ports on the target system. The pre-scan script detected a potential DoS vulnerability related to the Avahi service, but the hosts were found to be

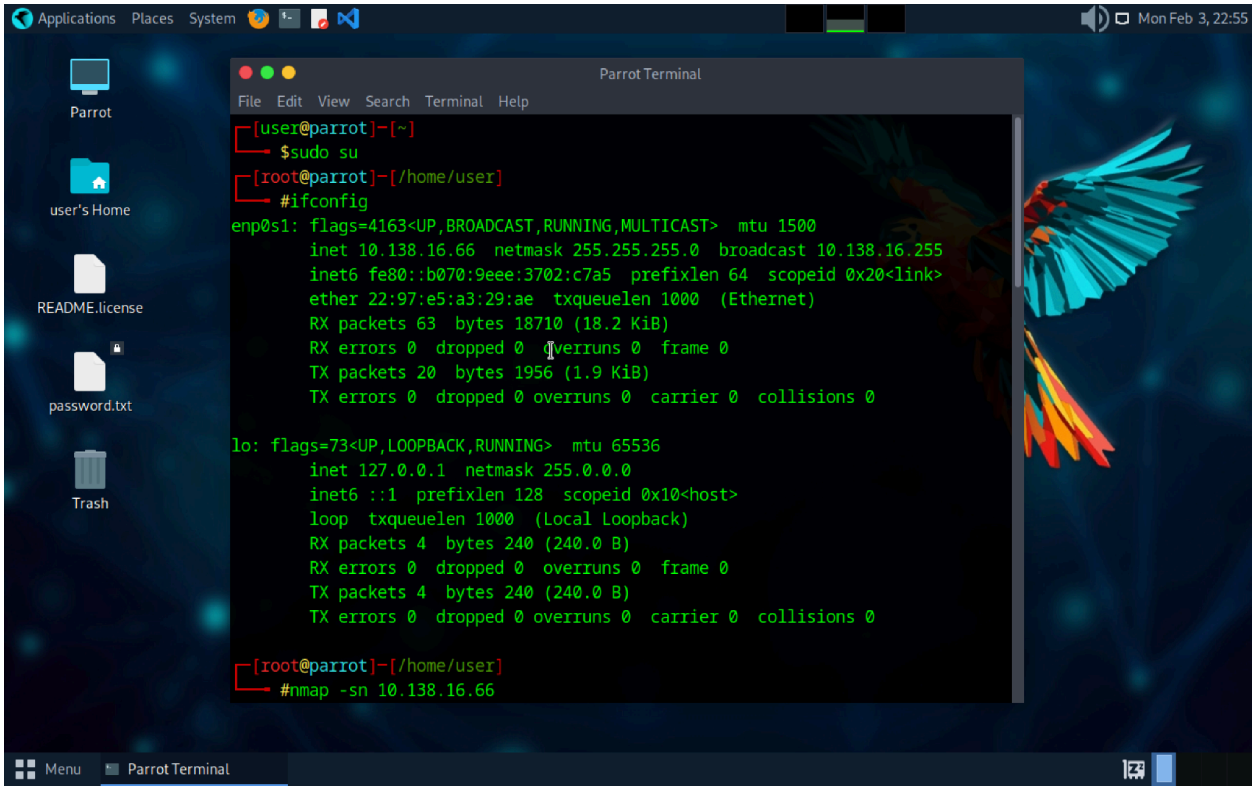
not vulnerable. Regular vulnerability assessments and timely patching of services are recommended to maintain the security posture of the network.

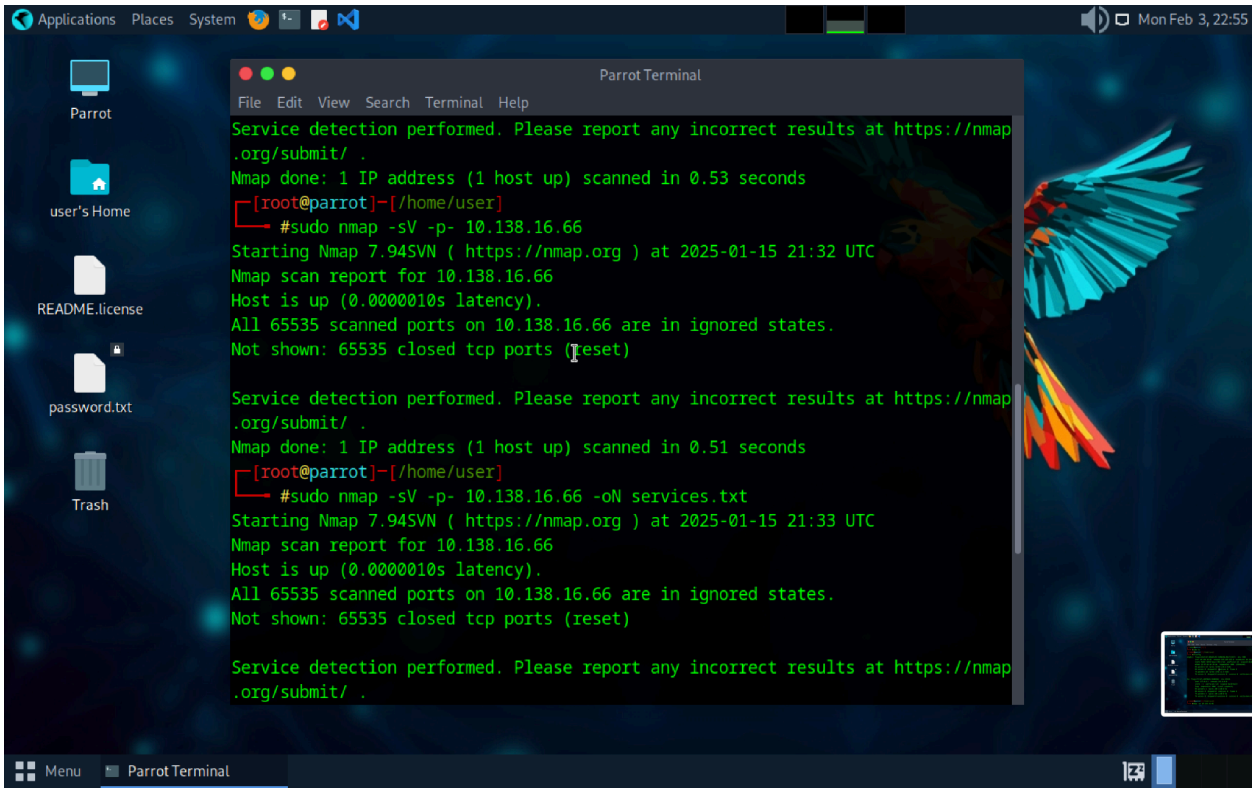
Recommendations

1. Regular Vulnerability Assessments:
    - Conduct regular vulnerability assessments to identify and mitigate potential security risks.
2. Patch Management:
    - Ensure that all services and applications are updated to the latest versions and apply necessary patches promptly.
3. Network Monitoring:
    - Implement continuous network monitoring to detect and respond to potential security threats in real-time.
4. Firewall Configuration:
    - Maintain a robust firewall configuration to prevent unauthorized access and protect against potential attacks.


Applications Places System
Mon Feb 3, 22:47
Parrot
user's Home
README.license
password.txt
Trash
Parrot Terminal
File Edit View Search Terminal Help
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 0.48 seconds
[root@parrot]-[/home/user]
#nmap -sV --script vuln 10.138.16.66
Starting Nmap 7.94SVN (https://nmap.org) at 2025-01-15 21:40 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 10.138.16.66
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.138.16.66 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 35.94 seconds
[root@parrot]-[/home/user]
#
Menu
Parrot Terminal


Applications Places System
Mon Feb 3, 22:47
Parrot
user's Home
README.license
password.txt
Trash
Parrot Terminal
File Edit View Search Terminal Help
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 10.138.16.66
Starting Nmap 7.94SVN (https://nmap.org) at 2025-01-15 21:26 UTC
Nmap scan report for 10.138.16.66
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
[root@parrot]-[/home/user]
#sudo nmap -sV -p- 10.138.16.66
Starting Nmap 7.94SVN (https://nmap.org) at 2025-01-15 21:26 UTC
Nmap scan report for 10.138.16.66
Host is up (0.0000010s latency).
All 65535 scanned ports on 10.138.16.66 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
Menu
Parrot Terminal


Applications Places System
Mon Feb 3, 22:55
Parrot
user's Home
README.license
password.txt
Trash
Parrot Terminal
File Edit View Search Terminal Help
[user@parrot]-[~]
$sudo su
[root@parrot]-[/home/user]
#ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.138.16.66 netmask 255.255.255.0 broadcast 10.138.16.255
inet6 fe80::b070:9eee:3702:c7a5 prefixlen 64 scopeid 0x20<link>
ether 22:97:e5:a3:29:ae txqueuelen 1000 (Ethernet)
RX packets 63 bytes 18710 (18.2 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 20 bytes 1956 (1.9 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 10.138.16.66
Menu
Parrot Terminal


Applications Places System
Mon Feb 3, 22:55
Parrot
user's Home
README.license
password.txt
Trash
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 0.53 seconds
[root@parrot]-[/home/user]
#sudo nmap -sV -p- 10.138.16.66
Starting Nmap 7.94SVN (https://nmap.org) at 2025-01-15 21:32 UTC
Nmap scan report for 10.138.16.66
Host is up (0.0000010s latency).
All 65535 scanned ports on 10.138.16.66 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 0.51 seconds
[root@parrot]-[/home/user]
#sudo nmap -sV -p- 10.138.16.66 -oN services.txt
Starting Nmap 7.94SVN (https://nmap.org) at 2025-01-15 21:33 UTC
Nmap scan report for 10.138.16.66
Host is up (0.0000010s latency).
All 65535 scanned ports on 10.138.16.66 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Menu
Parrot Terminal