Risk Management Report

Introduction

This report documents the risk management strategies developed and applied based on the vulnerability scan results. The project includes the identification of risks, treatment recommendations, mitigation steps, and a risk monitoring procedure. All assessments and procedures are clearly documented with justifications for the decisions made.

Identification of Risks

Critical Risks

1. Denial of Service (DoS) Vulnerability
    - Description: A NULL UDP avahi packet DoS vulnerability (CVE-2011-1002) was detected during the vulnerability scan. Although the hosts were found to be not vulnerable, the presence of this vulnerability in the network poses a significant risk.
    - Explanation: If exploited, this vulnerability could cause a denial of service, leading to system unavailability and potential disruption of services. This can result in financial losses, reputational damage, and loss of user trust.
    - Treatment Recommendations:
        - Patch Management: Ensure that the Avahi service is updated to the latest version and apply necessary patches.
        - Network Segmentation: Implement network segmentation to isolate critical systems and reduce the attack surface.
        - Intrusion Detection Systems (IDS): Deploy IDS to detect and respond to potential DoS attacks in real-time.
    - Mitigation Steps:
        - Regular Patching: Schedule regular patching and updating of the Avahi service and other network services.
        - Network Monitoring: Implement continuous network monitoring to detect and respond to potential DoS attacks.
        - Incident Response Plan: Develop and maintain an incident response plan to quickly address and mitigate DoS attacks.

2. Lack of Open Ports
    - Description: The vulnerability scan did not identify any open ports on the target system. While this indicates a well-configured firewall or security policy, it also poses a risk of overlooking potential vulnerabilities.
    - Explanation: The absence of open ports suggests that the system is well-protected. However, it is essential to ensure that all ports are properly configured and that no potential vulnerabilities are overlooked. Unidentified vulnerabilities can be exploited by attackers, leading to unauthorized access and data breaches.
    - Treatment Recommendations:
        - Comprehensive Vulnerability Scanning: Conduct comprehensive vulnerability scans regularly to identify and address potential vulnerabilities.
        - Firewall Configuration Review: Periodically review and update the firewall configuration to ensure that all ports are properly configured and secured.
        - Penetration Testing: Perform regular penetration testing to identify and mitigate potential vulnerabilities that may not be detected through automated scans.
    - Mitigation Steps:
        - Regular Vulnerability Assessments: Schedule regular vulnerability assessments to identify and address potential vulnerabilities.
        - Firewall Configuration Audits: Conduct periodic audits of the firewall configuration to ensure that all ports are properly configured and secured.
        - Penetration Testing: Include penetration testing as part of the regular security assessment process to identify and mitigate potential vulnerabilities.

Risk Monitoring Procedure

Risk Monitoring Procedure for DoS Vulnerability

1. Objective: To monitor and track the risk associated with the DoS vulnerability (CVE-2011-1002) and ensure that appropriate mitigation steps are in place.
2. Scope: This procedure applies to all network systems and services that are potentially affected by the DoS vulnerability.

3. Responsibilities:
    - Network Administrator: Responsible for implementing and maintaining the risk monitoring procedure.
    - Security Team: Responsible for conducting regular vulnerability assessments and penetration testing.
    - IT Management: Responsible for ensuring that all recommended mitigation steps are implemented and maintained.
4. Procedure:
    - Step 1: Initial Assessment: Conduct an initial assessment to identify systems and services that are potentially affected by the DoS vulnerability.
    - Step 2: Patch Management: Ensure that all affected systems and services are updated to the latest version and apply necessary patches.
    - Step 3: Network Monitoring: Implement continuous network monitoring to detect and respond to potential DoS attacks in real-time.
    - Step 4: Incident Response Plan: Develop and maintain an incident response plan to quickly address and mitigate DoS attacks.
    - Step 5: Regular Reviews: Conduct regular reviews of the risk monitoring procedure to ensure its effectiveness and make necessary adjustments.
5. Documentation: All findings, recommendations, and mitigation steps must be clearly documented and maintained for future reference.

Justification for Decisions Made

1. Patch Management: Regular patching and updating of services are crucial to mitigate known vulnerabilities and ensure the security of the network.
2. Network Segmentation: Implementing network segmentation helps isolate critical systems and reduce the attack surface, making it more difficult for attackers to exploit vulnerabilities.
3. Intrusion Detection Systems (IDS): Deploying IDS helps detect and respond to potential attacks in real-time, enhancing the overall security posture of the network.
4. Comprehensive Vulnerability Scanning: Conducting comprehensive vulnerability scans regularly ensures that potential vulnerabilities are identified and addressed promptly.
5. Firewall Configuration Review: Periodically reviewing and updating the firewall configuration ensures that all ports are properly configured and secured, reducing the risk of unauthorized access.

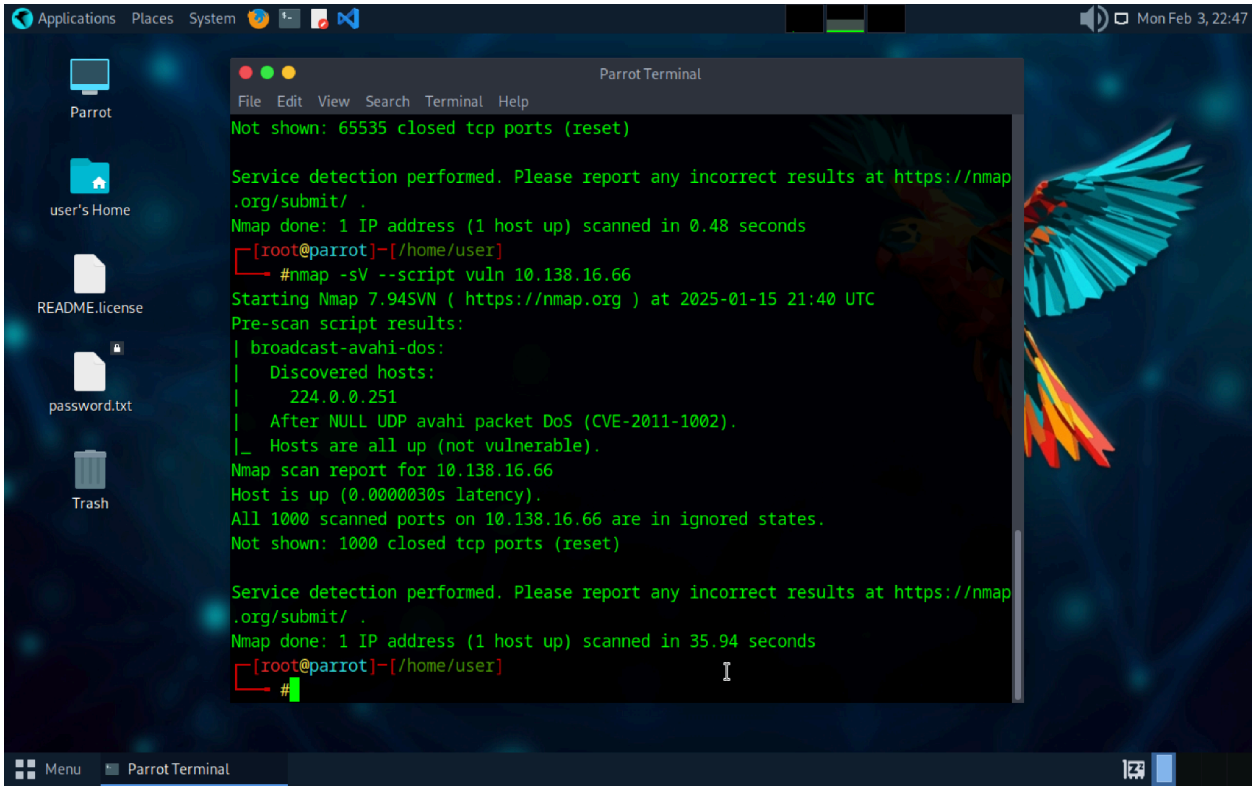
6. Penetration Testing: Performing regular penetration testing helps identify and mitigate potential vulnerabilities that may not be detected through automated scans.

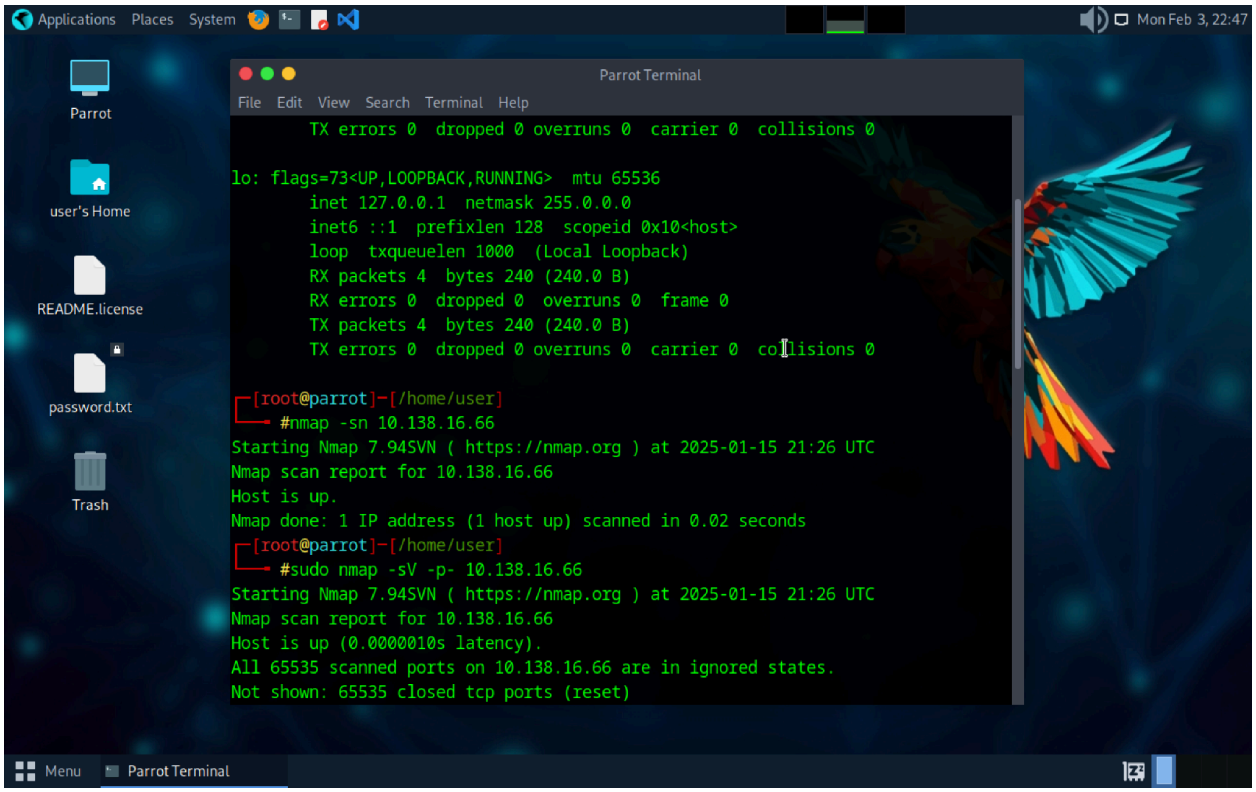
Conclusion

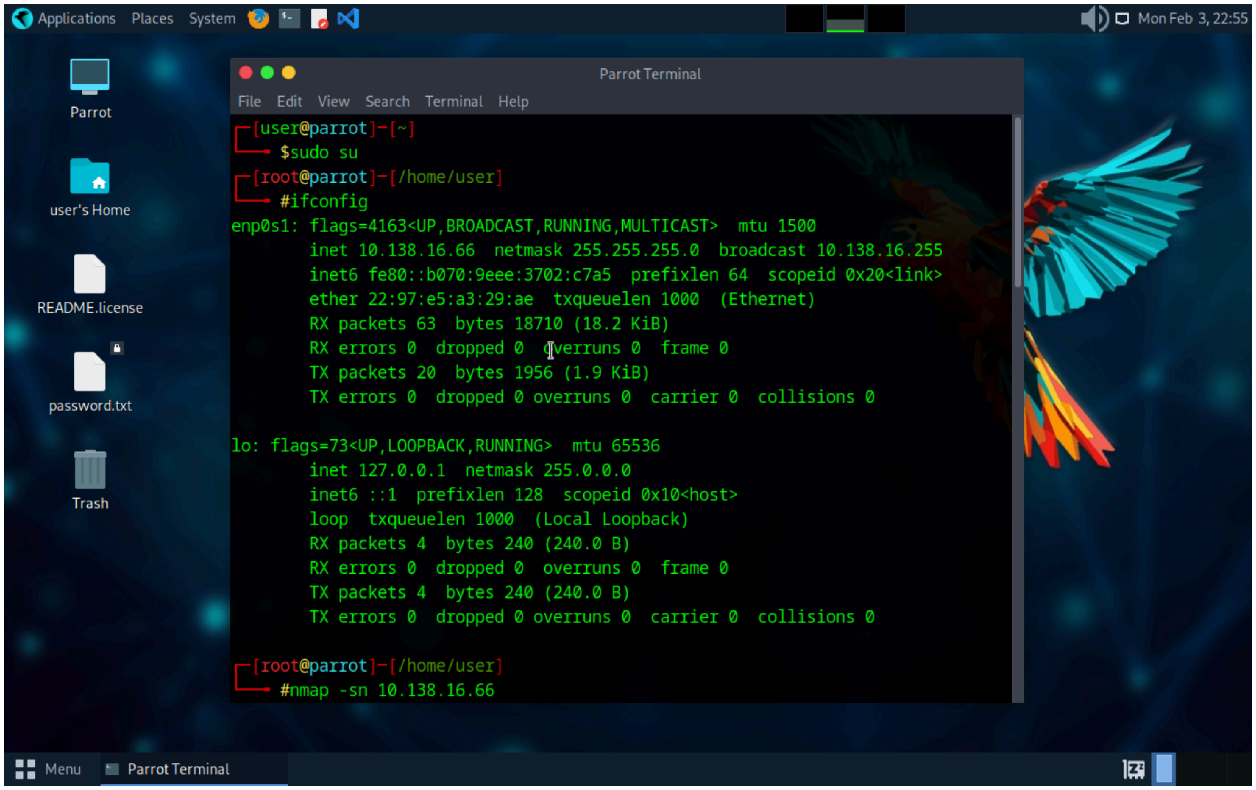
This risk management report provides a comprehensive overview of the risks identified from the vulnerability scan results, treatment recommendations, mitigation steps, and a risk monitoring procedure. The report is based on the scans conducted using Nmap, and the potential security implications are analyzed and explained. Regular vulnerability assessments, patch management, network monitoring, and incident response planning are essential to maintain the security posture of the network and mitigate identified risks.

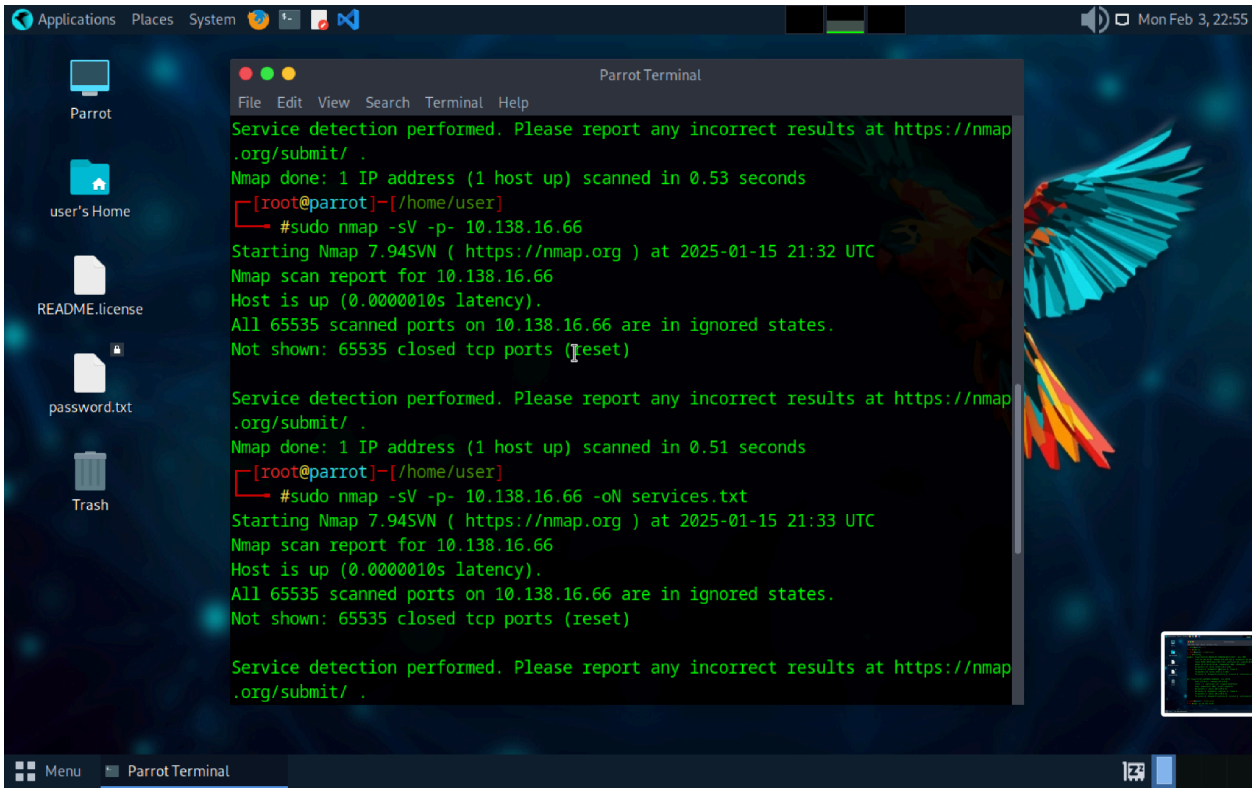
Recommendations

1. Regular Vulnerability Assessments: Conduct regular vulnerability assessments to identify and address 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. Incident Response Plan: Develop and maintain an incident response plan to quickly address and mitigate security incidents.
5. Firewall Configuration Audits: Conduct periodic audits of the firewall configuration to ensure that all ports are properly configured and secured.
6. Penetration Testing: Include penetration testing as part of the regular security assessment process to identify and mitigate potential vulnerabilities.


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