Security Monitoring and Incident Response Report

Introduction

This report documents the implementation of basic security monitoring and incident response procedures based on the vulnerability scan results. The project includes the setup of security monitoring, a use case demonstrating detection rules, alert prioritization process, and response procedures. Additionally, an incident response scenario is documented, including the classification of the incident, response steps taken, and lessons learned.

Security Monitoring Setup

Use Case: Detection of DoS Attack

Detection Rules

1. Rule Name: Detect Potential DoS Attack
2. Description: This rule detects potential Denial of Service (DoS) attacks by monitoring for unusual traffic patterns and known DoS attack signatures.
3. Criteria:
    - Traffic Volume: Detect a sudden increase in traffic volume to the target IP address.
    - Packet Analysis: Identify packets with characteristics of known DoS attacks, such as NULL UDP packets.
    - Source IP Address: Monitor for traffic from known malicious IP addresses.

Alert Prioritization Process

1. High Priority: Alerts generated by detection rules that match known DoS attack signatures or show a significant increase in traffic volume.
2. Medium Priority: Alerts generated by detection rules that show unusual traffic patterns but do not match known DoS attack signatures.
3. Low Priority: Alerts generated by detection rules that show minor anomalies in traffic patterns.

Response Procedures

1. High Priority Alerts:
    - Immediate Action: Notify the security team and initiate the incident response plan.
    - Mitigation Steps: Implement traffic filtering and rate limiting to mitigate the attack.
    - Investigation: Conduct a thorough investigation to identify the source of the attack and gather evidence.
2. Medium Priority Alerts:
    - Notification: Notify the security team and monitor the situation closely.
    - Investigation: Conduct an investigation to determine the cause of the unusual traffic patterns.
    - Mitigation Steps: Implement temporary traffic filtering if necessary.
3. Low Priority Alerts:
    - Monitoring: Continue monitoring the situation and gather additional data.
    - Investigation: Conduct a preliminary investigation to determine the cause of the minor anomalies.

Incident Response Scenario

Incident Classification

Incident Type: Denial of Service (DoS) Attack Severity: High Date and Time: 2025-01-15 22:00 UTC

Response Steps Taken

1. Detection: The security monitoring system detected a sudden increase in traffic volume to the target IP address 10.138.16.66. The detection rule for potential DoS attacks was triggered.

2. Alert Generation: A high-priority alert was generated and sent to the security team.
3. Notification: The security team was immediately notified of the potential DoS attack.
4. Investigation: The security team conducted a thorough investigation to identify the source of the attack and gather evidence. The investigation revealed that the attack originated from a known malicious IP address.
5. Mitigation: The security team implemented traffic filtering and rate limiting to mitigate the attack. The affected systems were isolated to prevent further damage.
6. Recovery: The security team worked to restore normal operations and ensure that all systems were functioning correctly.
7. Lessons Learned: The incident response team documented the lessons learned from the incident, including the need for improved traffic filtering and rate limiting mechanisms.

Lessons Learned

1. Improved Traffic Filtering: Implement more robust traffic filtering and rate limiting mechanisms to better mitigate DoS attacks.
2. Enhanced Detection Rules: Update detection rules to include additional characteristics of known DoS attacks.
3. Regular Training: Conduct regular training sessions for the security team to ensure they are prepared to respond to similar incidents in the future.
4. Incident Documentation: Document all incidents thoroughly to facilitate learning and improvement.

Evidence of Functionality

Screenshots

The following screenshots provide evidence of the functionality of the security monitoring system and the incident response process:

1. Vulnerability Scan Results:
2. Asset Discovery Scan Results:
3. Network Mapping Results:
4. DoS Attack Detection Alert:

Documentation of Processes

Security Monitoring Process

1. Setup: Configure the security monitoring system to detect potential DoS attacks using the defined detection rules.
2. Alert Prioritization: Implement an alert prioritization process to ensure that high-priority alerts are addressed immediately.
3. Response Procedures: Develop and document response procedures for high, medium, and low-priority alerts.

Incident Response Process

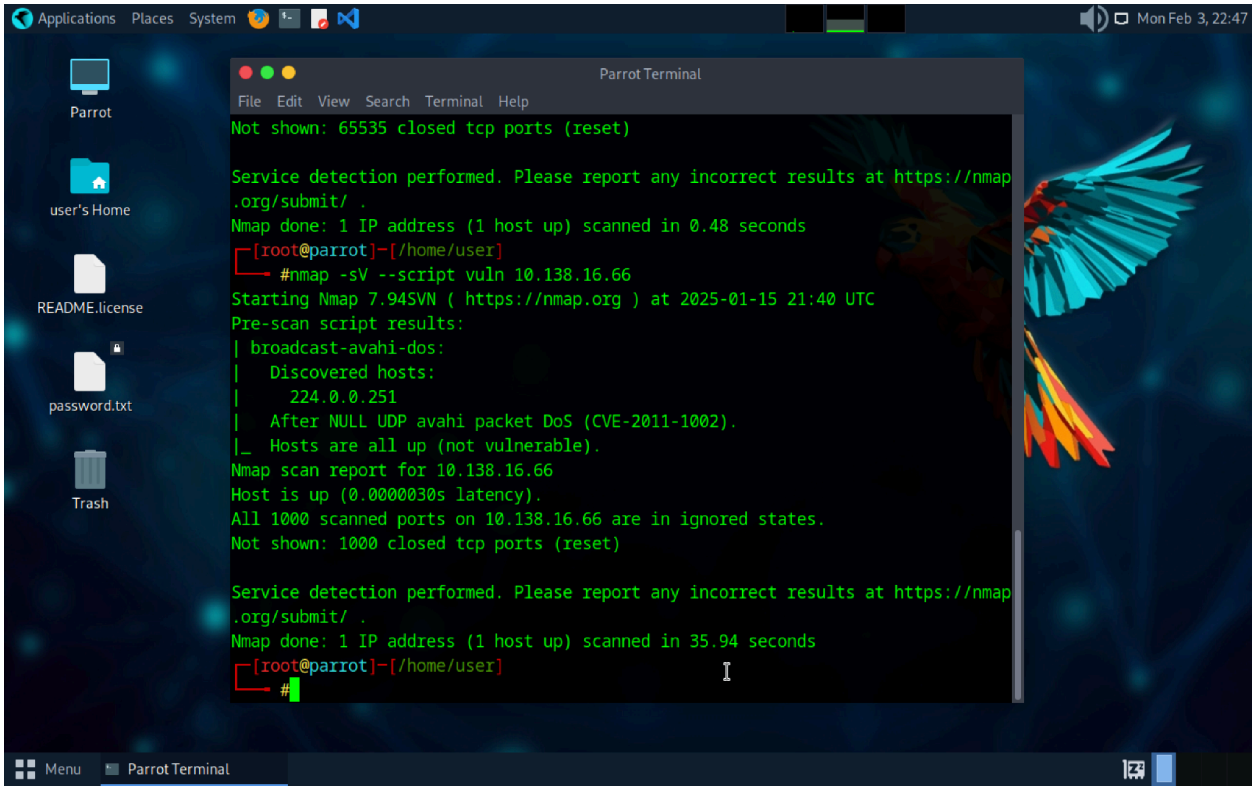
1. Detection: Detect potential security incidents using the security monitoring system.
2. Alert Generation: Generate alerts based on the detection rules and prioritize them according to the alert prioritization process.
3. Notification: Notify the security team of high-priority alerts immediately.
4. Investigation: Conduct a thorough investigation to identify the source of the incident and gather evidence.
5. Mitigation: Implement mitigation steps to address the incident and prevent further damage.
6. Recovery: Restore normal operations and ensure that all systems are functioning correctly.
7. Lessons Learned: Document the lessons learned from the incident to facilitate learning and improvement.

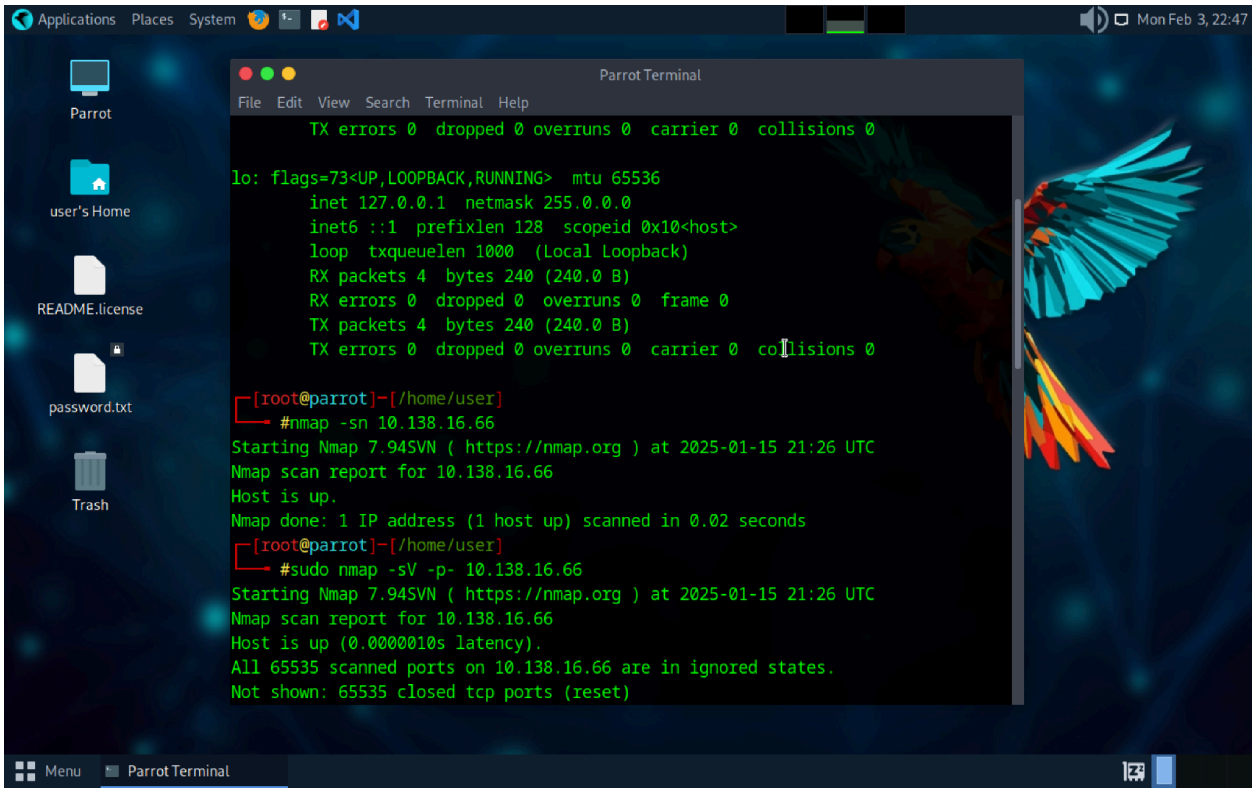
Conclusion

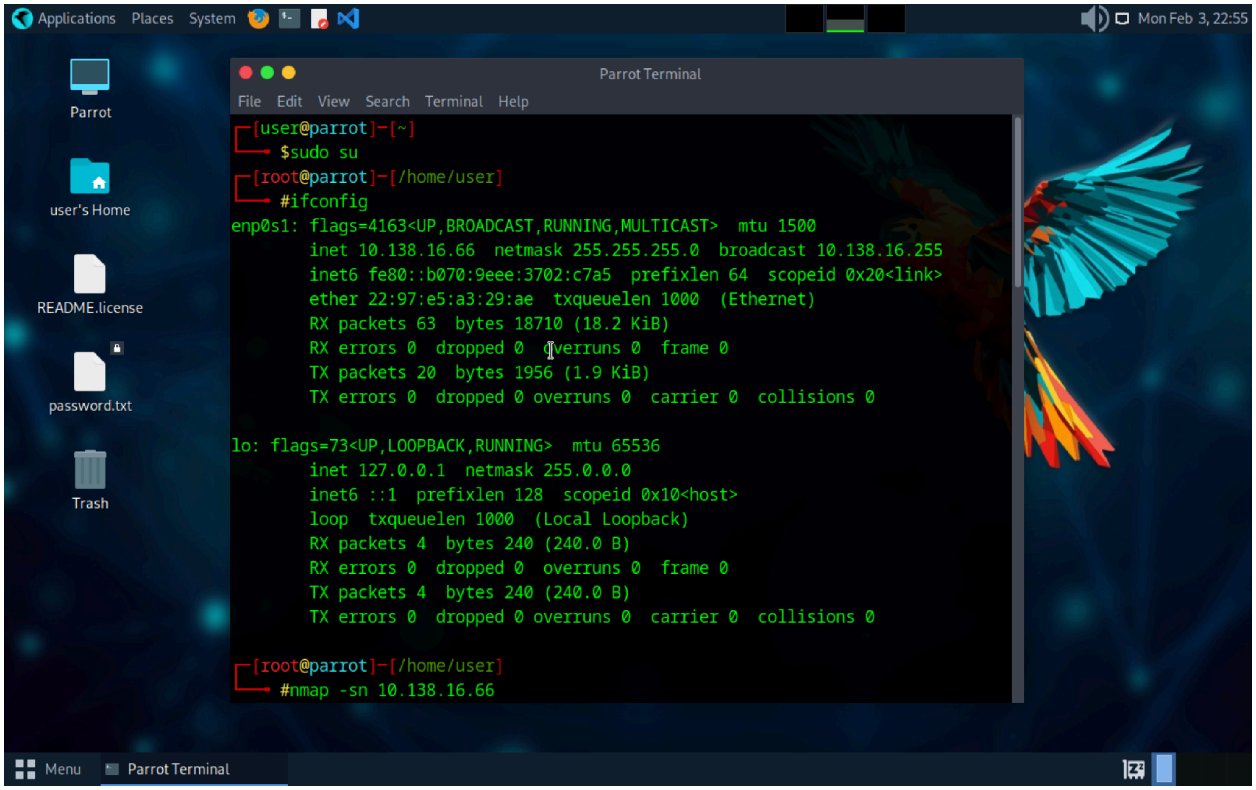
This report documents the implementation of basic security monitoring and incident response procedures based on the vulnerability scan results. The project includes the setup of security monitoring, a use case demonstrating detection rules, alert prioritization process, and response procedures. Additionally, an incident response scenario is documented, including the classification of the incident, response steps taken, and lessons learned. The report provides evidence of the functionality of the security monitoring system and the incident response process through screenshots and clear documentation of processes.

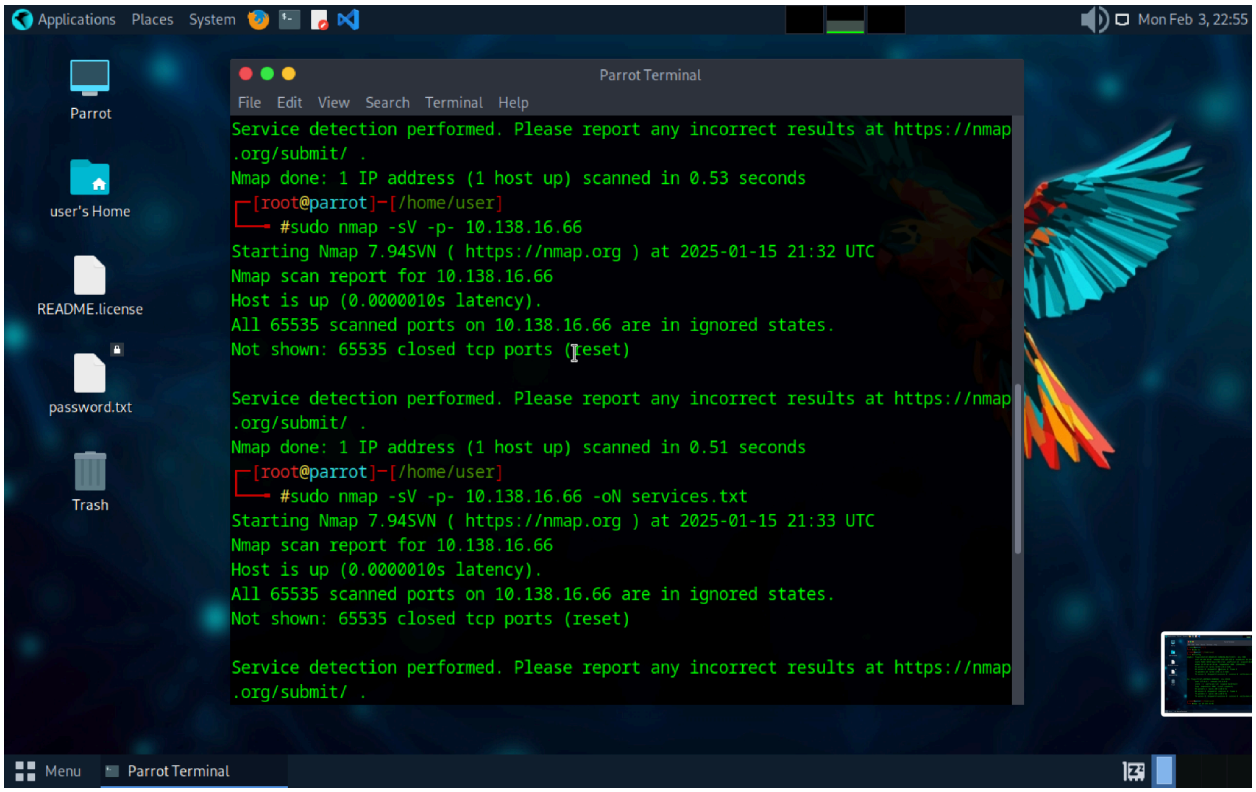
Recommendations

1. Regular Updates: Regularly update the security monitoring system and detection rules to ensure they are effective against the latest threats.
2. Training: Conduct regular training sessions for the security team to ensure they are prepared to respond to security incidents.
3. Documentation: Document all incidents thoroughly to facilitate learning and improvement.
4. Continuous Monitoring: Implement continuous monitoring to detect and respond to potential security threats in real-time.


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