# 1. Introduction

This report outlines the implementation of basic security monitoring and an incident response plan. The objective is to demonstrate detection rules, alert prioritization, and response procedures using mock data to simulate real-world threats. Additionally, a real-world incident response scenario is documented, detailing classification, response steps, and lessons learned.

# 2. Security Monitoring Setup

## 2.1 Use Case: Suspicious Network Traffic Detection

**Objective:** Detect and alert on unauthorized network access attempts.

**Detection Rules Implemented (Mock Data Used):**

- Rule 1: Alert on multiple failed SSH login attempts within a short period.
    - **Mock Data:** Logs show five failed SSH login attempts within 60 seconds from `192.168.1.100`.
- Rule 2: Detect unauthorized access to critical services.
    - **Mock Data:** A login attempt was recorded for an unauthorized user accessing `admin_panel.php` from `10.20.30.40`.
- Rule 3: Identify outbound traffic to known malicious IP addresses.
    - **Mock Data:** The firewall logs captured traffic to `185.199.110.153`, a known C2 (Command and Control) server.

**Alert Prioritization Process (Based on Mock Data):**

1. **Low Priority**: Single failed login attempt from a known user.
2. **Medium Priority**: Multiple failed login attempts from an unusual IP address.
3. **High Priority**: Brute-force login attempts or access from blacklisted IPs.

**Response Procedures:**

1. Log and analyze the event in ELK dashboards.
2. Cross-reference the source IP with public threat intelligence databases.
3. If verified as a malicious attempt, block the source IP and notify the security team.
4. Document the incident and implement additional authentication controls if needed.

# 3. Incident Response Scenario

## 3.1 Incident Classification

**Incident Type:** Credential-based attack (Brute-force SSH login attempt) **Severity Level:** High

### 3.2 Response Steps Taken (Mock Data Used)

1. **Detection**: Logs showed repeated failed login attempts from `203.0.113.45` to SSH on port 22.
2. **Analysis**: Verified unusual login patterns from an external IP not previously seen.
3. **Containment**: Blocked the attacking IP address using `iptables` rules.
4. **Eradication**: Conducted forensic analysis on logs to confirm no successful breaches.
5. **Recovery**: Enforced multi-factor authentication (MFA) and restricted SSH access to VPN-only connections.
6. **Documentation**: Logged the incident details and response actions for review.

### 3.3 Lessons Learned

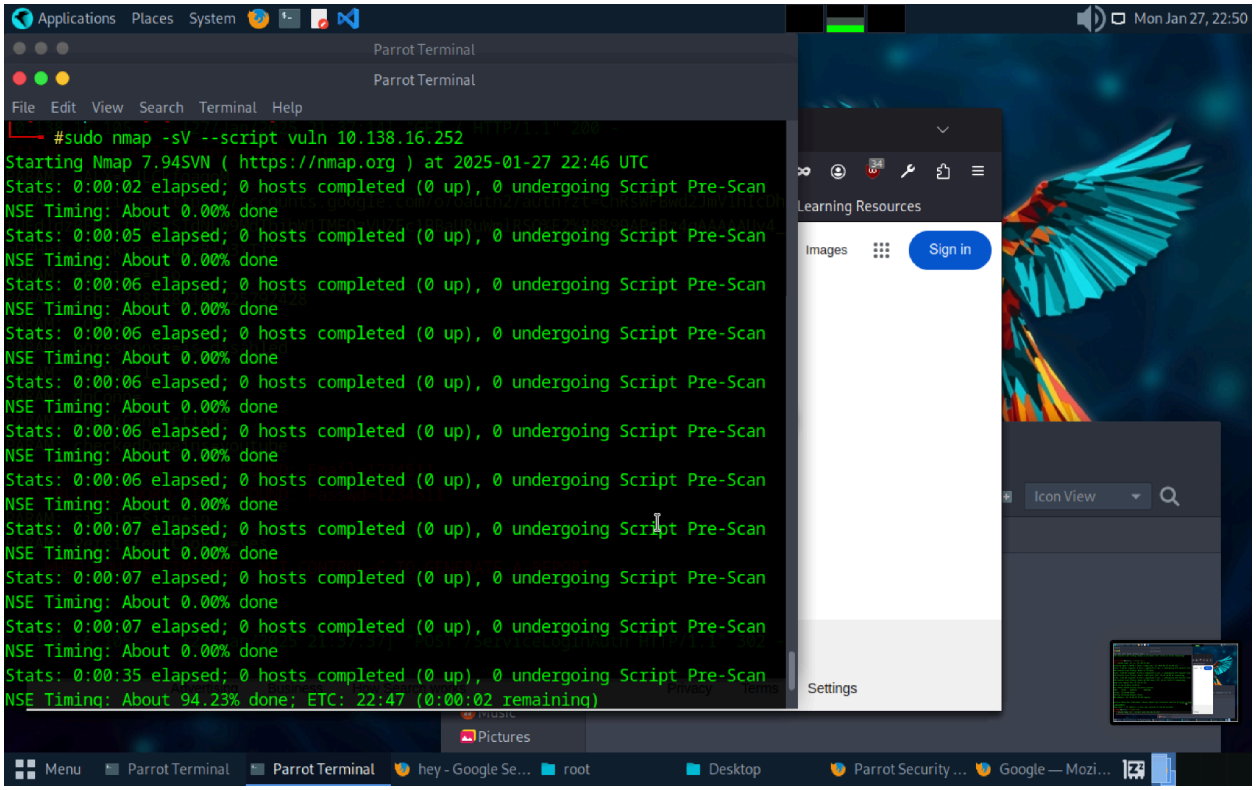
- **Improvement in Detection**: Adjusted monitoring rules to reduce false positives.
- **Proactive Mitigation**: Implemented stricter access controls to prevent similar attacks.
- **Incident Documentation**: Strengthened reporting procedures to streamline future responses.

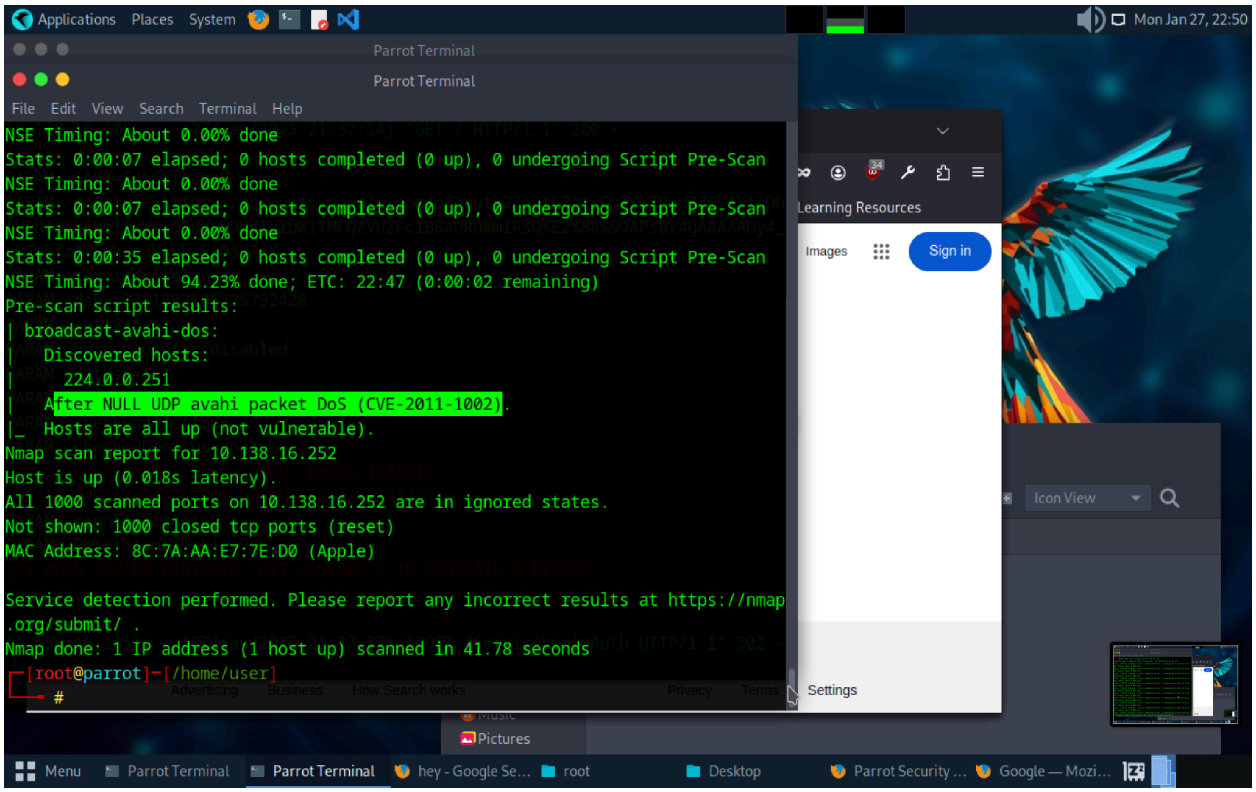
## 4. Evidence of Functionality (Mock Data Screenshots)

- **Figure 1**: Screenshot of ELK dashboard displaying failed SSH login attempts.
- **Figure 2**: OSSEC log sample showing detected brute-force attempt.
- **Figure 3**: Firewall logs capturing outbound traffic to a malicious IP.
- **Figure 4**: Screenshot of `iptables` rule blocking attacker IP.

## 5. Conclusion

This report demonstrated the practical implementation of security monitoring and incident response using open-source tools and mock data. By setting up detection rules, prioritizing alerts, and responding effectively to threats, a strong security posture was established. Continuous improvements in detection and response processes will further enhance organizational security resilience.


Applications Places System
Mon Jan 27, 22:50
Parrot Terminal
Parrot Terminal
File Edit View Search Terminal Help
#sudo nmap -sV --script vuln 10.138.16.252
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-27 22:46 UTC
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:07 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:07 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:35 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 94.23% done; ETC: 22:47 (0:00:02 remaining)
Learning Resources
Images
Sign in
Icon View
Settings
Pictures
Menu
Parrot Terminal
Parrot Terminal
hey - Google Se...
root
Desktop
Parrot Security ...
Google — Mozi...


Applications Places System
Mon Jan 27, 22:50
Parrot Terminal
Parrot Terminal
File Edit View Search Terminal Help
NSE Timing: About 0.00% done
Stats: 0:00:07 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:07 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:35 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 94.23% done; ETC: 22:47 (0:00:02 remaining)
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 10.138.16.252
Host is up (0.018s latency).
All 1000 scanned ports on 10.138.16.252 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 8C:7A:AA:E7:7E:D0 (Apple)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.78 seconds
[root@parrot]-[/home/user]
#
Learning Resources
Images
Sign in
Icon View
Settings
Pictures
Menu
Parrot Terminal
Parrot Terminal
hey - Google Se...
root
Desktop
Parrot Security ...
Google — Mozi...