Monitor and Respond to Network Security Events

1. Executive Summary

This report outlines the monitoring of network security events in a simulated environment, focusing on identifying and responding to a brute force attack. Using mock data from a SIEM (Security Information and Event Management) tool, the report provides details about the incident, response actions, and recommendations for improving security posture. Screenshots and logs are included to substantiate findings.

2. Environment Overview

- **Network Setup:**
  - Firewall: Configured to log and alert on suspicious activities.
  - SIEM Tool: Mocked instance of Splunk for log collection and analysis.
  - Systems Monitored: Web server (192.168.1.10) and authentication server (192.168.1.20).
- **Monitoring Methodology:**
  - Real-time log ingestion from network devices and servers.
  - Automated alerts for failed authentication attempts exceeding predefined thresholds.

3. Incident Details

Incident Type: Brute Force Attack on the Authentication Server.
Date and Time: January 26, 2025, 03:45 AM (UTC).
Source IP Address: 203.0.113.45 (mocked).
Target System: Authentication Server (192.168.1.20).
Attack Vector: Repeated login attempts using a dictionary of common passwords.
Impact:

- Temporary lockout of multiple user accounts due to failed login attempts.
- Increased CPU usage on the authentication server during the attack period.

4. Detection and Analysis

Logs Analysis:

- Sample log entries (mocked):

Jan 26 03:45:12 auth-server sshd[12345]: Failed password for invalid user admin from 203.0.113.45 port 45789 ssh2
Jan 26 03:45:13 auth-server sshd[12345]: Failed password for invalid user root from 203.0.113.45 port 45790 ssh2
Jan 26 03:45:14 auth-server sshd[12345]: Failed password for user test from 203.0.113.45 port 45791 ssh2
Jan 26 03:45:15 auth-server sshd[12345]: Failed password for

invalid user guest from 203.0.113.45 port 45792 ssh2

Key Findings:

- Over 100 failed login attempts detected within a 2-minute window.
- The source IP (203.0.113.45) exhibited anomalous behavior compared to normal traffic patterns.
- No successful login was observed during the attack.

Screenshot: (Splunk screenshot displaying a spike in failed login attempts and the attacker's IP address.)

5. Incident Response Steps

Step 1: Detection

- An alert triggered by the SIEM tool flagged excessive failed login attempts.

Step 2: Containment

- Blocked the source IP (203.0.113.45) at the firewall level.
- Enabled rate limiting for SSH connections to mitigate future attacks.

Step 3: Eradication

- Conducted a system scan to ensure no successful compromise occurred.
- Implemented stricter account lockout policies.

Step 4: Recovery

- Restored temporarily locked accounts after verification.
- Monitored for any residual malicious activity.

Step 5: Post-Incident Analysis

- Reviewed logs and updated the SIEM rule set to include:
  - Alerts for failed logins from a single IP exceeding 10 attempts in 1 minute.
  - Geo-blocking for non-essential regions.

6. Recommendations

1. **Harden Authentication Mechanisms:**
   - Enforce multi-factor authentication (MFA) for all users.
   - Disable root login via SSH.
2. **Improve Monitoring:**
   - Implement additional threat intelligence feeds for identifying known malicious IPs.
3. **Conduct Regular Security Audits:**
   - Schedule quarterly vulnerability assessments to identify weaknesses.
4. **User Awareness:**
   - Educate users about strong passwords and recognizing phishing attempts.

7. Supporting Evidence

1. Logs:

- Raw log data from the authentication server during the attack period.

2. Screenshots:

- Graph from Splunk showing the failed login spike.
- Firewall configuration screenshot showing the blocked IP address.

8. Conclusion

The mock brute force attack was successfully identified and mitigated through real-time monitoring and prompt response actions. Implementing the recommended measures will strengthen the network's resilience against similar threats in the future.