Monitor and Respond to Network Security Events

Report: Monitoring and Responding to Network Security Events

1. Introduction

This report describes the monitoring of network security events, identifies a security incident, and details the steps taken for incident response.

2. Security Incident Overview

- **Date and Time:** 2024-12-03, 12:45 PM

- **Incident Type:** Unauthorized login attempt

- **Source IP:** 203.0.113.45

- **Target System:** Web server (192.168.1.10)

3. Event Monitoring and Identification

The security monitoring system detected repeated failed login attempts to the web server. The following log entries were observed:

Log Sample:

[2024-12-03 12:45:01] Failed login attempt from IP: 203.0.113.45
[2024-12-03 12:45:05] Failed login attempt from IP: 203.0.113.45
[2024-12-03 12:45:10] Failed login attempt from IP: 203.0.113.45
[2024-12-03 12:45:15] Account lock triggered for user: admin

4. Incident Response Steps

1. **Initial Analysis:**

   - Reviewed logs to confirm the incident was a brute-force attack.

   - Verified no successful login occurred.

2. **Immediate Actions:**

   - Blocked the source IP (203.0.113.45) using the firewall:

   sudo iptables -A INPUT -s 203.0.113.45 -j DROP

   - Notified the system administrator about the attempted breach.

3. **Investigation:**

   - Checked the integrity of the web server for unauthorized changes or malware.

   - Reviewed user accounts to ensure no compromise occurred.

4. **Mitigation:**

   - Enabled account lockout after 3 failed login attempts.

   - Updated the server's SSH configuration to disable password authentication and require key-based authentication.

5. **Documentation and Reporting:**

- Logged the incident and response steps in the security event management system.

- Informed stakeholders of the resolution.

5. Conclusion and Recommendations

The network monitoring system successfully detected a brute-force attack. Swift action prevented unauthorized access, and further security measures were implemented to reduce future risks.

Recommendations:

- Regularly review and update firewall rules.

- Implement multi-factor authentication (MFA) for all users.

- Conduct regular security audits.

If you need this tailored further into a professional format or any additional customization, feel free to ask!