Security Monitoring and Incident Response

Project Overview

This project demonstrates the setup of basic security monitoring, including a use case with detection rules, alert prioritization, and response procedures. It also documents an incident response scenario, covering incident classification, response steps, and lessons learned. The implementation emphasizes practical application and clear documentation.

Part 1: Security Monitoring Implementation.

1.1 System Setup

For this project, we'll use a combination of tools to simulate a basic security monitoring environment.

- **Vulnerability Scanning**: Nmap will be used to identify potential vulnerabilities. (Based on "Apply Vulnerability Assessment Techniques.pdf")
- **Log Monitoring**: A simple approach using system logs will be demonstrated. In a real-world scenario, this would involve a SIEM (Security Information and Event Management) system.
- **Intrusion Detection**: For simplicity, we will use a basic host-based intrusion detection system (HIDS) concept.

1.2 Use Case: Detection of Unauthorized Access

- **Detection Rules**:
    - Monitor SSH logs for failed login attempts. A threshold of 5 failed attempts within 60 seconds will trigger an alert.
    - ```
      grep "Failed password" /var/log/auth.log | awk '{print $11}' | sort | uniq -c | awk '$1 >= 5 {print $2}'
      ```
- **Alert Prioritization**:
    - Priority: High
    - Reason: Multiple failed login attempts to SSH indicate a potential brute-force attack, which can lead to unauthorized access.
- **Response Procedures**:
    - **Detection**: The above detection rule identifies the source IP address.
      ```

- **Notification**: Automatically send an alert to the security team via email/SMS.
- **Containment**:
  - Block the offending IP address at the firewall.
  - `iptables -A INPUT -s [Offending IP] -j DROP`
- **Investigation**:
  - Investigate the logs to determine the extent of the attack.
  - Check for any successful logins from the same IP.
- **Recovery**:
  - If necessary, restore the system from a clean backup.
  - Ensure all systems are patched and updated.
- **Post-Incident Activity**: Document the incident and review security measures.

1.3 Evidence of Functionality

- **Log Excerpt**: (Example)
  ```
  Feb 20 10:00:01 ubuntu sshd[2043]: Failed password for
  invalid user testuser from 192.168.1.5 port 22
  ```
- `Feb 20 10:00:05 ubuntu sshd[2043]: Failed password for invalid user testuser from 192.168.1.5 port 22`
- `Feb 20 10:00:08 ubuntu sshd[2043]: Failed password for invalid user testuser from 192.168.1.5 port 22`
- `Feb 20 10:00:12 ubuntu sshd[2043]: Failed password for invalid user testuser from 192.168.1.5 port 22`
- `Feb 20 10:00:15 ubuntu sshd[2043]: Failed password for invalid user testuser from 192.168.1.5 port 22`
-
-
- **Firewall Rule**: (Example)
  - Command: `iptables -L`
  - Output:
- `Chain INPUT (policy ACCEPT)`
- `target     prot opt source               destination`

- `DROP  all  --  192.168.1.5  anywhere`
-
-

Part 2: Incident Response Scenario

2.1 Incident Classification

- **Incident Type**: Unauthorized Access
- **Incident Summary**: A user reported that their account was locked out after multiple failed login attempts.
- **Based on documents**: The "Develop and Apply Risk Management Strategies.pdf" and "Identify and Analyze Cyber Threats.pdf" documents highlight the risks of weak credentials and phishing attacks, which could lead to this type of incident.

2.2 Response Steps Taken

1. **Preparation**: The security team was already trained on incident response procedures and had access to necessary tools.
2. **Identification**:
    - The SIEM system alerted the security team to the account lockout and the associated IP address.
    - Logs were analyzed to confirm the multiple failed login attempts.
3. **Containment**:
    - The user's account was temporarily disabled.
    - The offending IP address was blocked at the firewall.
4. **Eradication**:
    - The user's password was reset.
    - A full system scan was performed to check for any malware or other signs of compromise.
5. **Recovery**:
    - The user's account was re-enabled after verifying their identity.
    - The user was trained on creating strong passwords and identifying phishing attempts.

6. **Post-Incident Activity**:
    - A post-incident report was created, documenting the incident and the response steps taken.
    - A meeting was held to discuss lessons learned and identify areas for improvement.

2.3 Lessons Learned

- **Strengthen Password Policies**: The incident highlighted the need for stronger password policies, including complexity requirements and regular password changes.
- **Improve User Awareness Training**: The user might have been a victim of a phishing attack. Regular security awareness training is crucial.
- **Enhance Monitoring**: While the SIEM system did detect the incident, additional monitoring rules could be implemented to detect similar attacks earlier.
- **Implement Multi-Factor Authentication (MFA)**: MFA could prevent this type of attack even if the attacker knew the user's password.