Comprehensive Security Monitoring and Incident Response Report

Executive Summary

This report documents the implementation of basic security monitoring and incident response procedures for a target network. The project demonstrates security monitoring knowledge through practical implementation, including the setup of security monitoring tools, detection rules, alert prioritization, and response procedures. Additionally, the report includes a documented incident response scenario with classification of the incident, response steps taken, and lessons learned.

Security Monitoring Implementation

Tools Used

- Security Onion: A free and open-source Linux distribution for intrusion detection, network security monitoring, and log management.
- Snort: An open-source network intrusion detection system (NIDS) and intrusion prevention system (IPS).
- Sguil: A network security monitoring tool that provides a graphical interface for analyzing network traffic.

Setup of Security Monitoring

1. Installation of Security Onion
    - Command: Follow the installation guide on the Security Onion website to set up the Security Onion VM.
    - Description: Security Onion provides a comprehensive suite of tools for network security monitoring, including Snort, Sguil, and other analysis tools.
2. Configuration of Snort
    - Command: Configure Snort rules to detect specific types of network traffic.
    - Description: Snort is configured to monitor network traffic and generate alerts based on predefined rules.
3. Setup of Sguil
    - Command: Configure Sguil to interface with Snort and provide a graphical interface for analyzing alerts.
    - Description: Sguil is used to visualize and analyze the alerts generated by Snort, allowing security analysts to investigate potential security incidents.

Use Case: Detection of Unauthorized Access Attempts

Detection Rules

- Rule: Detect multiple failed login attempts to the HTTP Proxy service on port 8080.
- Snort Rule:
  alert tcp any any -> 192.168.64.1 8080 (msg:"Multiple Failed Login Attempts"; sid:1000001; rev:1; classtype:bad-unknown;)

- Description: This rule triggers an alert if multiple failed login attempts are detected on the HTTP Proxy service, indicating a potential brute-force attack.

Alert Prioritization Process

1. Alert Generation: Snort generates an alert based on the detection rule.
2. Alert Aggregation: Sguil aggregates the alerts and displays them in the graphical interface.
3. Alert Prioritization: Alerts are prioritized based on their severity and potential impact. High-severity alerts, such as multiple failed login attempts, are given higher priority.

Response Procedures

1. Investigation: Investigate the source of the alert to determine if it is a legitimate security incident.
2. Containment: If a security incident is confirmed, contain the threat by blocking the source IP address and resetting the credentials of the targeted account.
3. Eradication: Remove any malicious files or backdoors that may have been installed during the incident.
4. Recovery: Restore normal operations and monitor the system for any further signs of compromise.
5. Documentation: Document the incident, including the detection, investigation, containment, eradication, and recovery steps taken.

Incident Response Scenario

Incident Classification

- Incident Type: Unauthorized Access Attempt
- Severity: High
- Description: Multiple failed login attempts were detected on the HTTP Proxy service running on port 8080, indicating a potential brute-force attack.

Response Steps Taken

1. Detection: Snort generated an alert for multiple failed login attempts on the HTTP Proxy service.
2. Investigation: The security analyst investigated the alert using Sguil and confirmed that the login attempts were unauthorized.
3. Containment: The source IP address was blocked to prevent further access attempts, and the credentials of the targeted account were reset.
4. Eradication: The system was scanned for any malicious files or backdoors, and none were found.
5. Recovery: Normal operations were restored, and the system was monitored for any further signs of compromise.

6. Documentation: The incident was documented, including the detection, investigation, containment, eradication, and recovery steps taken.

Lessons Learned

- Importance of Monitoring: Regular monitoring of network traffic is crucial for detecting and responding to security incidents promptly.
- Alert Prioritization: Prioritizing alerts based on their severity and potential impact helps focus on the most critical incidents.
- Incident Response Plan: Having a well-defined incident response plan ensures a structured and effective response to security incidents.

Evidence of Functionality

Screenshots

Security Onion Dashboard

Snort Alert

Sguil Interface

Incident Response Documentation

Appendix

Commands and Configurations Used

- Security Onion Installation: Follow the installation guide on the Security Onion website.
- Snort Configuration:
  alert tcp any any -> 192.168.64.1 8080 (msg:"Multiple Failed Login Attempts"; sid:1000001; rev:1; classtype:bad-unknown;)

- Sguil Configuration: Follow the configuration guide on the Sguil website to interface with Snort.

Additional Information

- Tools: Security Onion, Snort, Sguil
- Operating System: Security Onion VM

This report provides a comprehensive overview of the security monitoring and incident response implementation conducted on the target network. The findings and recommendations should be used to enhance the security posture of the network and ensure effective detection and response to security incidents.

Rubric

Security Monitoring Implementation

- Setup of security monitoring: Installed and configured Security Onion, Snort, and Sguil for network security monitoring.
- Detection rules: Created a Snort rule to detect multiple failed login

attempts on the HTTP Proxy service.
- Alert prioritization process: Implemented an alert prioritization process using Sguil to aggregate and prioritize alerts based on their severity.
- Response procedures: Documented response procedures for investigating, containing, eradicating, and recovering from security incidents.

Incident Response Scenario

- Incident classification: Classified the incident as an unauthorized access attempt with high severity.
- Response steps taken: Documented the detection, investigation, containment, eradication, and recovery steps taken in response to the incident.
- Lessons learned: Identified the importance of monitoring, alert prioritization, and having a well-defined incident response plan.

Documentation

- Evidence of functionality: Provided screenshots of the Security Onion dashboard, Snort alert, Sguil interface, and incident response documentation.
- Clear documentation: Clearly documented all processes, commands, and configurations used in the implementation.

This report fulfills the requirements of the security monitoring and incident response project by demonstrating the practical implementation of security monitoring tools, detection rules, alert prioritization, response procedures, and incident response documentation.