Okay, let's craft a detailed report on implementing security monitoring and incident response, drawing from the provided documents.

Security Monitoring and Incident Response Report

1. Security Monitoring Setup and Use Case

- **Basic Security Monitoring:**
    - The "vulnerability assessment.pdf" document shows the use of Nmap for network scanning. While Nmap is a versatile tool, in a security monitoring context, its logs can be a source of information for detecting suspicious activity.
    - For example, repeated Nmap scans from an unusual IP address could indicate reconnaissance activity by an attacker.
- **Use Case: Detection of Port Scanning**
    - **Detection Rules:**
        - Detection rules would need to be implemented in a Security Information and Event Management (SIEM) system or an Intrusion Detection System (IDS).
        - A basic rule to detect port scanning could be: "Alert if the number of unique ports scanned on a host exceeds X within Y minutes from the same source IP address."
        - In this case, from "vulnerability assessment.pdf" document, we can see the Nmap commands used to scan the ports. For example "sudo nmap -p- 192.168.1.148".
    - **Alert Prioritization Process:**
        - **Severity:** High. Port scanning can be a precursor to an attack.
        - **Priority:** High. Security analysts should investigate these alerts promptly.
        - **Justification:** Repeated or broad port scans can indicate that an attacker is mapping the network to identify vulnerable services. This activity requires immediate attention to prevent potential exploitation.
    - **Response Procedures:**
        - **Initial Response:**
            - Alert the security team.
            - Identify the source IP address of the scanning activity.
            - Determine the target host(s).

        - **Investigation:**
            - Correlate the scanning activity with other logs (firewall, IDS, etc.) to identify any other suspicious behavior.
            - Assess the vulnerability status of the target host(s).
        - **Containment:**
            - If the scanning activity is deemed malicious, block the source IP address at the firewall.
            - Isolate the target host(s) if necessary.
        - **Remediation:**
            - Ensure that systems are patched and hardened to resist potential attacks.
            - Review and fine-tune security monitoring rules.
        - **Recovery:**
            - Restore any affected systems from backups, if necessary.
        - **Documentation:**
            - Document all actions taken during the incident response process.
- **Evidence of Functionality:**
    - To provide complete evidence, you would typically include:
        - SIEM/IDS screenshots showing the detection rule configuration.
        - Alert logs triggered by the port scanning activity.
        - Firewall logs showing blocked IP addresses.
        - Documentation of the response actions taken.

2. Incident Response Scenario

- **Incident Scenario:**
    - Compromise of a web server due to a known vulnerability (e.g., CVE-2017-14493 from "vulnerability assessment.pdf" document).
- **Classification of Incident:**
    - **Type:** Web server compromise
    - **Impact:** High (Potential data breach, service disruption)
    - **Severity:** Critical (Exploited vulnerability with a CVSS score of 9.8)
- **Response Steps Taken:**
    - **Detection:**

        - SIEM alerted on unusual web server activity and exploit attempt (IDS logs would show the attempt to exploit CVE-2017-14493).
    - **Containment:**
        - Isolated the affected web server from the network to prevent further damage or lateral movement.
        - Blocked the attacker's IP address at the firewall.
    - **Eradication:**
        - Patched the web server to remediate the vulnerability (CVE-2017-14493).
        - Scanned the server for malware and removed any malicious files.
    - **Recovery:**
        - Restored the web server from a clean backup to ensure no backdoors remained.
        - Brought the web server back online after thorough testing.
    - **Post-Incident Activity:**
        - Conducted a post-incident review to identify the root cause and improve security measures.
- **Lessons Learned:**
    - **Importance of Patch Management:** The incident highlighted the critical need for timely patching of vulnerabilities.
    - **SIEM Effectiveness:** The SIEM system played a crucial role in detecting the attack.
    - **Incident Response Plan:** The incident response plan facilitated a coordinated and effective response.
    - **Need for Improved Web Application Security:** Strengthen web application security measures (e.g., web application firewall, regular vulnerability scanning).
- **Evidence of Functionality:**
    - SIEM/IDS logs showing the detection of the exploit.
    - Firewall logs documenting the blocking of the attacker's IP.
    - Server logs before and after the incident.
    - Documentation of the incident response steps.

Sources and related content