Copilot

Security Incident Report

Executive Summary

We conducted a thorough analysis of critical alerts investigated by the Senior Cybersecurity SOC Analyst. Leveraging various threat intelligence sources, we incorporated MITRE ATT&CK and OWASP Threat Modeling frameworks to contextualize our findings. Our research revealed potential DNS spoofing attacks (Alert #1) and unauthorized firewall ruleset modifications (Alert #2), indicating the involvement of threat actors evading security controls and establishing persistent access within targeted systems.

Overview of Critical Events

1. **Alert #1: DNS Spoofing Potential**
    - **Description**: A file integrity modification for "/etc/resolv.conf" may result in DNS spoofing attacks, potentially leading to malware infection, credential theft, or compromised user data.
    - **Recommendations**:
        - Restore the unaltered version of "/etc/resolv.conf" from a trusted backup or source control system.
        - Review and revise policies governing user and administrative access to critical configuration files.
        - Monitor DNS traffic and related logs for anomalous activity or suspicious queries.
2. **Alert #2: Unauthorized Firewall Ruleset Modifications**
    - **Description**: The previous state of firewall rulesets was restored, possibly due to unauthorized access, malicious intent, or improper change management processes.
    - **Recommendations**:
        - Investigate the cause of the firewall ruleset restoration.
        - Review and potentially revise policies governing firewall configurations.
        - Implement real-time monitoring and alerting for critical firewall ruleset changes.
        - Inform security teams about recent firewall rule changes and their impact on security controls.

Threat Actor Tactics, Techniques, and Procedures (TTPs)

The identified TTPs align with those used by threat actors engaged in DNS spoofing attacks and attempts to evade security controls through unauthorized firewall ruleset changes. Adversaries may be targeting the organization to gain access to sensitive data or disrupt critical systems.

Preventive Measures

To prevent future incidents:

- Establish a robust change management process with segregation of duties, least privilege principles, and documentation.
- Implement access control measures to minimize unauthorized access.
- Strengthen security monitoring capabilities with real-time alerting and automated response mechanisms.

By adopting these recommendations, the organization can enhance its security posture against DNS spoofing attacks and unauthorized firewall ruleset changes. Rapid detection, investigation, and response are vital in mitigating potential risks associated with these alerts and maintaining a robust security posture.

Triage Specialist’s Findings

As a Triage Specialist, I efficiently evaluated and prioritized security alerts based on severity, potential impact, and risk assessment criteria. The following events were identified:

1. **Alert: Integrity Checksum Changed**
    - Type: Wazuh Alert
    - Description: The file “/etc/resolv.conf” had its integrity checksum changed, potentially impacting system operations.
    - Severity: MEDIUM
    - Date: 2204-04-03T17:20:26
    - Tags: rule=550, agent_name=osi-0x01, agent_ip=192.168.133, agent_id=001, wazuh
2. **Alert: Previous State of Firewall Ruleset Restored**
    - Type: Wazuh Alert
    - Description: A previously saved version of a firewall ruleset was reapplied, restoring the firewall state.
    - Severity: MEDIUM
    - Date: 2024-04-10T07:34:16
    - Tags: rule=588, agent_name=osi-0x03, agent_ip=192.168.134, agent_id=001, wazuh

Recommendations for Further Investigation

For critical events, escalate to the Senior Cybersecurity SOC Analyst with detailed documentation and context. Continuously monitor the SIEM and other tools for related events.

Report generated by Copilot Security Reporting Tool.