Threat Detection Lab - Phase 1 & Phase 2 Report

Phase 1: Sudo Monitoring

Lab Objective:

To implement and test an audit rule that monitors privileged command execution using auditd and validate the logging process through various security controls.

1. Lab Environment:

- System Configuration:
  - Operating System: Ubuntu 24.04 LTS
  - Audit Tool: auditd
  - Security Framework: NIST SP 800-53 (Control Mapping AU-6, AU-12, SI-4)

2. Audit Rule Implementation:

Audit Rule:

To monitor privileged command execution using sudo, we configure an audit rule with auditctl.

Command Used:

sudo auditctl -w /usr/bin/sudo -p x -k sudo_monitoring

Explanation:

- -w: Watch a specified file or directory.
- /usr/bin/sudo: The path to the sudo binary.
- -p x: Monitor execution (execution permission).
- -k sudo_monitoring: Custom key for tracking this event.

3. Trigger Action:

To trigger the audit rule, I executed the sudo command as a non-root user.

Command:

sudo ls /root

Explanation:

This command lists the contents of the /root directory (accessible only to the root user). The system should log this action as it uses sudo for elevated privileges.

4. Log Review:

Command to review logs:

sudo ausearch -k sudo_monitoring

Explanation:

The ausearch command is used to search through audit logs for events tagged with the custom key sudo_monitoring. This helps identify any logged sudo usage events.

5. Screenshots:

- Screenshot 1: Sudo_Rule_Configured.png

- Screenshot 2: Sudo_Log_Result.png

6. Control Mapping:

- AU-6: Audit Review

- AU-12: Audit Generation

- SI-4: System Monitoring

7. Validation Summary:

- Audit Rule Validation: The sudo_monitoring audit rule was successfully configured and persisted across system reboots. The rule triggered successfully when executing the sudo command, and the event was captured in the audit logs.
- Control Validation: The implementation of this rule satisfied the requirements for the mapped NIST controls AU-6, AU-12, and SI-4 by ensuring the audit data was generated, stored, and accessible for future review.

Phase 2: /etc/passwd Monitoring & Failed Login Detection

Lab Objective:

In Phase 2, the goal is to enhance monitoring by tracking unauthorized access to the /etc/passwd file and detecting failed login attempts. These actions will be validated against NIST SP 800-53 controls to ensure that system security events are appropriately logged and monitored.

1. Lab Environment:

- System Configuration:
  - Operating System: Ubuntu 20.04 LTS (or your specific version)
  - Audit Tool: auditd
  - Security Framework: NIST SP 800-53 (Control Mapping AU-2, AU-12, SI-4, AC-7)

2. Audit Rule Implementation:

Audit Rule 1: Monitoring /etc/passwd Access

Command Used:

sudo auditctl -w /etc/passwd -p r -k passwd_watch

Purpose:

Monitor unauthorized access attempts to the sensitive file /etc/passwd.

Trigger Action 1: /etc/passwd Access

Command:

cat /etc/passwd

Log Review for /etc/passwd Access:

Command:

sudo ausearch -k passwd_watch

Audit Rule 2: Failed Login Detection

Command Used (Option 1):

sudo aureport -au

Command Used (Option 2):

sudo journalctl _SYSTEMD_UNIT=systemd-logind.service | grep "authentication failure"

Purpose:

Track failed login attempts to detect unauthorized access attempts.

Trigger Action 2: Failed Login Attempt

Command:

ssh fakeuser@localhost

Log Review for Failed Logins:

Command (Option 1):

sudo aureport -au

Command (Option 2):

sudo journalctl _SYSTEMD_UNIT=systemd-logind.service | grep "authentication failure"

3. Screenshots:

- Screenshot 1: Passwd_Rule_Configured.png

- Screenshot 2: Passwd_Log_Result.png

- Screenshot 3: Failed_Login_Log.png

4. Control Mapping:

- AU-2: Audit Records

- AU-12: Audit Generation

- SI-4: System Monitoring

- AC-7: Unsuccessful Login Attempts

5. Validation Summary:

- Audit Rule for /etc/passwd Access: The audit rule for monitoring /etc/passwd was successfully implemented, and access attempts were logged as expected.

- Audit Rule for Failed Login Detection: The audit rule for failed login attempts was successfully configured. The failed login was captured in both aureport and journalctl logs.

- Triggered Logs: Both rules were successfully triggered. Unauthorized access to /etc/passwd and failed login attempts were logged as expected.

- Control Validation: This phase meets the requirements of the mapped NIST controls (AU-2, AU-12, SI-4, AC-7) by ensuring that both critical file access and failed login attempts are logged and can be reviewed for suspicious activity.

6. Conclusion:

Phase 2 was successfully completed with the implementation of an audit rule to monitor access to /etc/passwd and tracking failed login attempts. Both audit rules were configured, tested, and validated against NIST SP 800-53 controls, improving system monitoring and security.

Next Steps:

- Extend Monitoring: Expand monitoring to other sensitive files like /etc/shadow and /etc/sudoers.
- Refine Documentation: Complete the lab report with detailed logs and analysis of the events that triggered the audit rules.