Threat Detection Lab – Phase 1: Sudo Monitoring

Generated on: 2025-05-08 21:05:38

# 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

- 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

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

Command:  
sudo ls /root

Explanation:  
This command lists the contents of the /root directory (accessible only to the root user).

# 4. Log Review

Command:  
sudo ausearch -k sudo\_monitoring

# 5. Screenshots

- Sudo\_Rule\_Configured.png  
- 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 triggered.  
Control Validation: The configuration satisfied NIST controls AU-6, AU-12, and SI-4.