Threat Detection Lab – Phase 2: /etc/passwd Monitoring & Failed Login Detection

# Lab Objective

Enhance monitoring by tracking unauthorized access to the /etc/passwd file and detecting failed login attempts. These actions are validated against NIST SP 800-53 controls.

# 1. Lab Environment

- 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: /etc/passwd Access  
Command:  
sudo auditctl -w /etc/passwd -p r -k passwd\_watch

Trigger Command:  
cat /etc/passwd

Log Review:  
sudo ausearch -k passwd\_watch

Audit Rule 2: Failed Login Detection  
Command Option 1:  
sudo aureport -au

Command Option 2:  
sudo journalctl \_SYSTEMD\_UNIT=systemd-logind.service | grep "authentication failure"

Trigger:  
ssh fakeuser@localhost

# 3. Screenshots

- Passwd\_Rule\_Configured.png  
- Passwd\_Log\_Result.png  
- 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

Both audit rules were configured and triggered successfully. Access attempts to /etc/passwd and failed login attempts were logged and validated against the mapped controls.

# 6. Conclusion

Phase 2 was successfully completed. Future steps include extending monitoring to other critical files and expanding documentation with detailed analysis.