Linux Security Monitoring and Auditing Lab Guide

1. Overview

This lab guide will provide you with hands-on experience in **Linux security monitoring** and **auditing** techniques. You will explore system-level auditing, log management, and security assessment tools to help you understand and analyze security events in Linux environments.

2. Learning Objectives

By completing this lab, you will:

- Understand the role of `auditd` for system-level auditing.
- Learn how to use tools like `journalctl`, `grep`, and **Lynis** for log management and system assessment.
- Gain practical experience in configuring auditing rules and analyzing audit logs for security-relevant events.

3. Prerequisites

- **VM Setup**: Use a virtual machine running Kali Linux or Ubuntu (e.g., Ubuntu 22.04 LTS/Kali Linux) or Debian for lab activities.
- **Linux CLI Basics**: Familiarity with basic Linux command-line operations (e.g., `cd`, `ls`, `sudo`, `nano`, `vim`) is required.
- **Internet Access**: Your VM will need internet access to install the necessary tools.

4. Lab Instructions

This lab must be completed **in groups**. Please maintain your assigned group and collaborate with your team members to complete the activities outlined in the lab guide.

To begin the lab, follow the steps outlined in the detailed guide available at the following GitHub link:

Access the Lab Guide

You are expected to discuss your findings and work through the lab together within your group. Upon completion, submit your group’s results as instructed in the lab guide.

Best of luck, and feel free to reach out if you have any questions!