Sysadmin Essentials: Monitoring Log Files

Cybersecurity
Linux 3 Day 3

Today’s Objectives

By the end of class, you will be able to:

- □ Filter cron log message using `journalctl` and `ryslog`
- □ Analyze and troubleshoot cron logs using `logwatch`
- □ Review the past three weeks of Linux lessons.

A Better Way to Administer Log Files

Journalctl

Amidst thousands of incoming messages, filtering is an efficient way to monitor and troubleshoot problems.

- `Jounalctl` and `rsyslog` administer logs via filtering.
- The `jounalctl` utility displays entries in the journal managed by the `journald` daemon
- Sysadmins use journalctl to display and filter logs from various service.
- Journal records are structured and indexed, allowing for output in different formats such as JSON.

Filtering Cron Logs Demo

Next, we’ll demonstrate the following:

01 Filtering for the cron service.

02 Journalctl filtering options

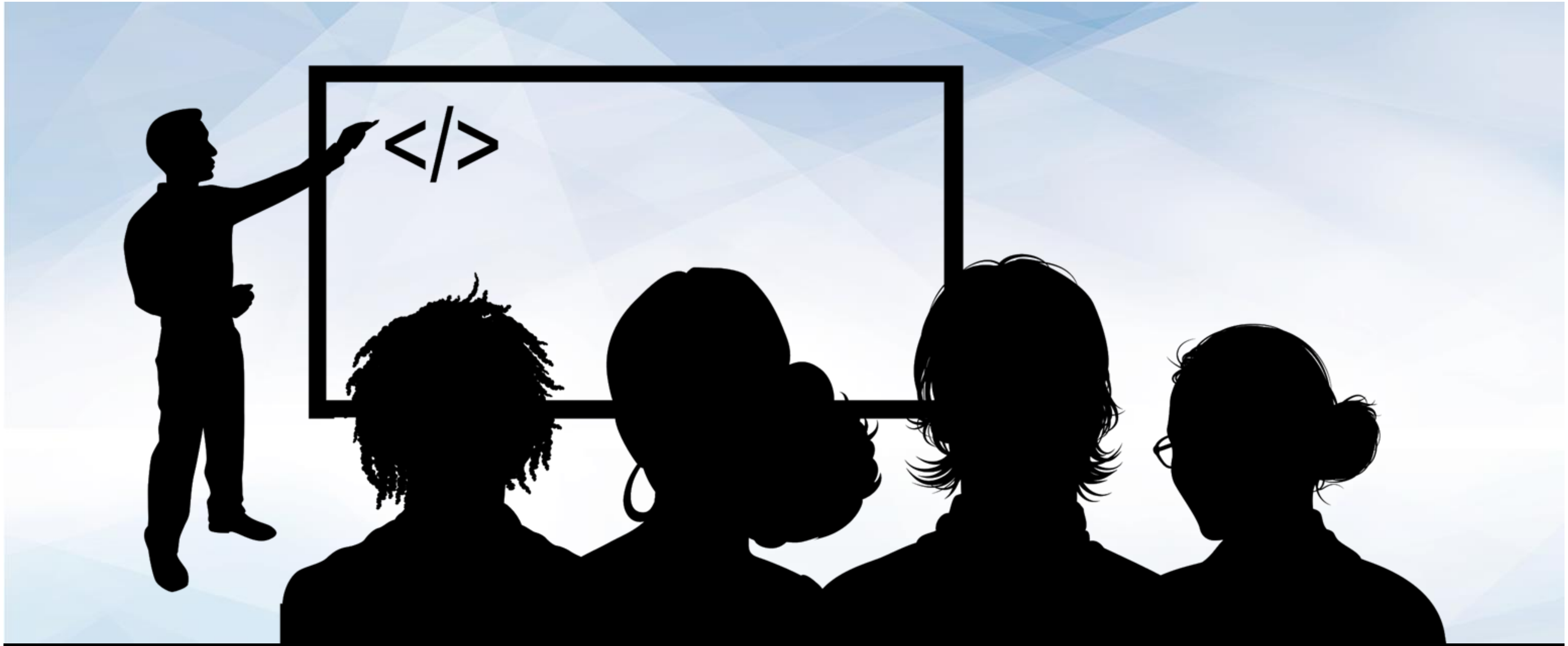
03 Viewing cron logs using predefined Strings

04 Viewing cron logs by time.

05 Formatting the Output with a log management system

06 Persist journalctl logs

07 Filtering cron logs with ryslog



Instructor Demonstration

Journctl

Activity: Filtering Log Files

In this activity, you will use journalctl to filter cron logs.

Instructions sent via Slack.

Suggested Time:
12 Minutes

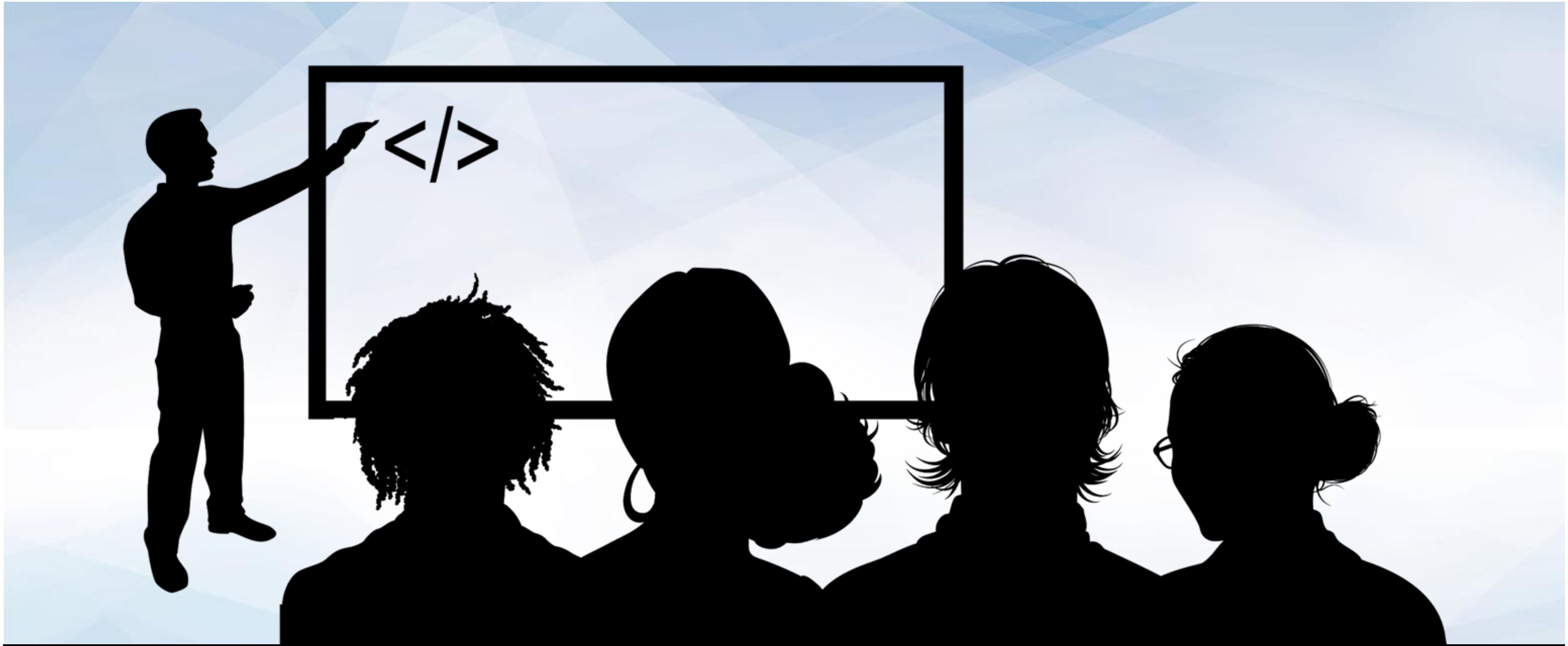
Times Up! Let’s Review.

Filtering Log Files

Take a Break!

Monitoring Cron Logs with logwatch

`logwatch` produces reports that can be filtered by services and viewed online or sent via email.



Instructor Demonstration

logwatch

Activity:Monitoring Cron Logs with logwatch

In this activity, you will use logwatch to manually monitor cron logs and email a digest to yourself.

Instructions sent via Slack.

Suggested Time:
20 Minutes

Times Up! Let’s Review.

logwatch Cron Monitor

Review Activity: **Linux**

In this activity, we will review the topics covered in the past three weeks of Linux lessons.

Instructions sent via Slack.

Suggested Time:
50 Minutes

Times Up! Let’s Review.

Linux