ProLUG 101

Unit 13 Worksheet

Instructions

Fill out this sheet as you progress through the lab and discussions. Hold onto all of your work to send to me at the end of the course.

Discussion Questions:

Unit 13 Discussion Post 1: Your security team comes to you with a discrepancy between the production security baseline and something that is running on one of your servers in production. There are 5 servers in a web cluster and only one of them is showing this behavior. They want you to account for why something is different.

1. How are you going to validate that the difference between the systems?
2. What are you going to look at to explain this?
3. What could be done to prevent this problem in the future?

Unit 13 Discussion Post 2: Your team has been giving you more and more engineering responsibilities. You are being asked to build out the next set of servers to integrate into the development environment. Your team is going from RHEL 8 to Rocky 9.4.

1. How might you start to plan out your migration?
2. What are you going to check on the existing systems to baseline your build?
3. What kind of validation plan might you use for your new Rocky 9.4 systems?

Definitions/Terminology

- Hardening
- Pipeline
- Change management (IT)
- Security Standard
- Security Posture
- Acceptable Risk
    - NIST 800-53

- STIG
- CIS Benchmark
- OpenSCAP
- SCC Tool
- HIDS
- HIPS

Notes During Lecture/Class:

Links:

Terms:

Useful tools:

Lab and Assignment

Unit 13 Lab System Hardening

Continue working on your project from the Project Guide

Topics:

1. System Stability
2. System Performance
3. System Security
4. System monitoring
5. Kubernetes
6. Programming/Automation

You will research, design, deploy, and document a system that improves your administration of Linux systems in some way.

Digging Deeper (optional)

1. Run through this lab: https://killercoda.com/het-tanis/course/Linux-Labs/107-server-startup-process
    a. How does this help you better understand the discussion 13-2 question?
2. Run through this lab: https://killercoda.com/het-tanis/course/Linux-Labs/203-updating-golden-image
    a. How does this help you better understand the process of hardening systems?

Reflection Questions

1. What questions do you still have about this week?

2. How can you apply this now in your current role in IT? If you're not in IT, how can you look to put something like this into your resume or portfolio?