Document Generated: 12/24/2024

Learning Style: Virtual Classroom

Provider: Linux Foundation

Difficulty: Intermediate

Course Duration: 4 Days

Linux Security (LFS416)

About this Course:

Security is the leading concern of business enterprises and resolving cybersecurity concerns is the utmost priority of any business and organization. Data protection and information security is becoming more and more complicated with the advancements in information technology. This course is designed for IT professionals and candidates striving to gain better knowledge and understanding of Linux System Security Essentials. Business direly needs professionals who can adequately implement robust security measures and protect viable business data. On average, a Linux Security Administrator earns $92,966 annually.

This course covers key concepts of Linux Security such as Security-Enhancing Techniques & Tools, Server Hardening, Monitoring Deployment, Security Attack Detection Practices, and Linux Response Strategy & Security Policy Development. This intermediate-level course provides professionals with practical knowledge of adopting a technical security approach and effectively corresponding to security holes and attack vectors in the Linux System. Professionals will develop the skillset required to mitigate security risks and resolve security vulnerabilities.

Course Objectives:

The core objective of this course is to help professionals develop a better understanding and sound knowledge of the following key concepts:

- Enterprise Security Risk Assessment in Linux Ecosystem
- Security-Enhancing Tools and Techniques
- Server Hardening and Security Threats & Vulnerabilities
- Monitoring Deployment and Implementing Attack Detection Practices & Tools
- Linux Response Strategy and Security Policy Development
- Configuring Linux Systems for DISA STIG & HIPAA Compliance

Audience:

This course is tailored for the following group of professionals and interested candidates:

- Linux Security Administrator
- IT Professionals & Experts
- Cybersecurity Professionals

Prerequisites:

Professionals planning to enroll in the Linux Security (LFS416) course must comply with the following prerequisites:

- Fundamental Knowledge of Local System Administration
- Conceptual Knowledge of Networking Systems
- Practical Experience of working with Linux & Unix

- Certification in Linux System Administration (LFS301) or Equivalent Knowledge
- Certification in Linux Network Management (LFS311) or Equivalent Knowledge

Course Outline:

Introduction

- Linux Foundation
- Linux Foundation Training
- Linux Foundation Certifications
- Linux Foundation Digital Badges
- Laboratory Exercises, Solutions and Resources
- Things Change in Linux and Open Source Projects
- ELearning Course: LFS260
- Platform Details

Cloud Security Overview

- Multiple Projects
- What is Security?
- Assessment
- Prevention
- Detection
- Reaction
- Classes of Attackers
- Types of Attacks
- Attack Surfaces
- Hardware and Firmware Considerations
- Security Agencies
- Manage External Access
- Labs

Preparing to Install

- Image Supply Chain
- Runtime Sandbox
- Verify Platform Binaries
- Minimize Access to GUI
- Policy Based Control
- Labs

Installing the Cluster

- Update Kubernetes
- Tools to Harden the Kernel
- Kernel Hardening Examples
- Mitigating Kernel Vulnerabilities
- Labs

Securing the kubeapiserver

- Restrict Access to API
- Enable Kubeapiserver Auditing
- Configuring RBAC
- Pod Security Policies
- Minimize IAM Roles
- Protecting etcd
- CIS Benchmark
- Using Service Accounts
- Labs

Networking

- Firewalling Basics
- Network Plugins
- Mitigate Brute Force Login Attempts
- Ingress Objects
- Pod to Pod Encryption
- Restrict Cluster Level Access
- Labs

Workload Considerations

- Minimize Base Image
- Static Analysis of Workloads
- Runtime Analysis of Workloads
- Container Immutability
- Mandatory Access Control
- SELinux
- AppArmor
- Generate AppArmor Profiles
- Labs

Issue Detection

- Understanding Phases of Attack
- Preparation
- Understanding an Attack Progression
- During an Incident
- Handling Incident Aftermath
- Intrusion Detection Systems
- Threat Detection
- Behavioral Analytics
- Labs

Domain Reviews

- Preparing for the Exam
- Labs

Credly Badge:

Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges