Linux Security (LFS416)

Modality: Virtual Classroom

Duration: 4 Days

SATV Value:

CLC:

NATU:

SUBSCRIPTION: No

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
- Laboratory Exercises, Solutions and Resources
- E-Learning Course: LFS216
- Distribution Details
- Labs

Security Basics

- What is Security?
- Assessment
- Prevention
- Detection
- Reaction
- Labs

Threats and Risk Assessment

- Classes of Attackers
- Types of Attacks
- Trade Offs
- Labs

Physical Access

- Physical Security
- Hardware Security
- Understanding the Linux Boot Process
- Labs

Logging

- Logging Overview
- Syslog Services
- The Linux Kernel Audit Daemon
- Linux Firewall Logging
- Log Reports
- Labs

Auditing and Detection

- Auditing Basics
- Understanding an Attack Progression
- Detecting an Attack
- Intrusion Detection Systems
- Labs

Application Security

- Bugs and Tools
- Tracking and Documenting Changes
- Resource Access Control
- Mitigation Techniques
- Policy Based Access Control Frameworks
- Real World Example
- Labs

Kernel Vulnerabilities

- Kernel and User Spaces
- Bugs
- Mitigating Kernel Vulnerabilities
- Vulnerabilities Examples
- Labs

Authentication

- Encryption and Authentication
- Passwords and PAM
- Hardware Tokens
- Biometric Authentication
- Network and Centralized Authentication
- Labs

Local System Security

- Standard UNIX Permissions
- Administrator Account

- Advanced UNIX Permissions
- Filesystem Integrity
- Filesystem Quotas
- Labs

Network Security

- TCP/IP Protocols Review
- Remote Trust Vectors
- Remote Exploits
- Labs

Network Services Security

- Network Tools
- Databases
- Web Server
- File Servers
- Labs

Denial of Service

- Network Basics
- DoS Methods
- Mitigation Techniques
- Labs

Remote Access

- Unencrypted Protocols
- Accessing Windows Systems
- SSH
- IPSEC VPNs
- Labs

Firewalling and Packet Filtering

- Firewalling Basics
- iptables
- Netfilter Implementation
- Netfilter rule management
- Mitigate Brute Force Login Attempts
- Labs

Response and Mitigation

- Preparation
- During an Incident

- Handling Incident Aftermath
- Labs

Compliance testing with OSCAP

- Compliance Testing
- SCAP Introduction
- OpenSCAP
- SCAP Workbench
- Command Line Scan
- Labs