Over 35 Years Of Technology Training

**Document Generated: 12/08/2025**

**Learning Style: On Demand**

**Technology:**

**Difficulty: Beginner**

**Course Duration:**

# Linux Security Fundamentals (LFS216)

## About this Course:

This program is a detailed look at the security issues that can affect nearly every device, particularly with the smooth communication we are seeking from the Internet. Some of the Linux securing features are either integrated into the Linux Kernel or introduced by the numerous Linux Distributions.

## Course Objectives:

This course is a comprehensive look at the security challenges that can affect almost every system, especially with the seamless connectivity we seek from the Internet. The class starts with an overview of computer security and touches on how security affects everyone in the chain of development, implementation, administration and the end user. After completing this advanced Linux security training students will be able to assess your current security needs, evaluate your current security readiness and implement security options as required

## Audience:

This advanced Linux security course is for everyone involved with any security related tasks including implementation technicians, developers and managers will gain additional expertise from this course.

## Prerequisites:

To make the most of this course, you will need to be able to: Download files from the Internet, configure virtual machines, import a virtual appliance and a “host only” virtual private network. Basic Linux command line skills (covered in LFS201

## Course Outline:

Chapter 1. Course Introduction

Chapter 2. Security Basics

Chapter 3. Threats and Risk Assessment

Chapter 4. Physical Access

Chapter 5. Logging

Chapter 6. Auditing and Detection

Chapter 7. Application Security

Chapter 8. Kernel Vulnerabilities

Chapter 9. Authentication

Chapter 10. Local System Security

Chapter 11. Network Security

Chapter 12. Network Services Security

Chapter 13. Denial of Service

Chapter 14. Remote Access

Chapter 15. Firewalling and Packet Filtering

Chapter 16. Response and Mitigation

Chapter 17. Compliance Testing with OSCAP