Document Generated: 06/10/2026

Learning Style: On Demand

Technology: Linux Foundation

Difficulty: Beginner

Course Duration: 24 Hours

Mastering Infrastructure Security: Strategies, Tools, and Practices (SKF200)

About This Course:

By the end of this course, you should be able to fortify digital architectures against contemporary and emerging threats as well as navigate the intricate landscape of infrastructure security.

Course Objectives:

- Explore the fundamental elements needed to establish and maintain a secure infrastructure configuration and the principles and techniques of network penetration testing to identify potential security vulnerabilities.

Audience:

- This course is designed for developers aiming to deepen their understanding of infrastructure security and management. It is ideal for those who wish to enhance their knowledge in network penetration testing and infrastructure security skills.

Prerequisites:

- None

Course Outline:

- Chapter 1. Course Introduction
- Chapter 2. Introduction to Infrastructure & Ops Security
- Chapter 3. Phases of Hacking
- Chapter 4. Reconnaissance - The First Step of Hacking
- Chapter 5. Scanning, Identifying Vulnerabilities, and Mapping the Network
- Chapter 6. Gaining Access: The Art of Exploitation
- Chapter 7. Mapping and Information Gathering
- Chapter 8. Service Enumeration and Subdomain Takeover
- Chapter 9. Default Pages, Backup Files, and Application Versions
- Chapter 10. Command Injection Attacks
- Chapter 11. Privilege Escalation - Linux
- Chapter 12. Privilege Escalation - Windows
- Chapter 13. Security, TLS, and Configuration

- Chapter 14. Labs - Basic to Advanced