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

Empower yourself with the essential skills to fortify digital architectures against contemporary and emerging threats.

Duration: 3 Days

Prerequisites for this course

- General IT concepts, including operating systems, networking, and cloud computing.
- Programming Skills: While not a strict requirement, basic programming skills can be beneficial, especially in scripting languages such as Python or Bash.
- Fundamental networking principles, including TCP/IP, DNS, routing, and subnetting.
- Basic elements of infrastructure, like servers, databases, and network equipment, would be advantageous.
- Common security threats, vulnerabilities, and best practices for secure coding and infrastructure management.
- Ability to approach complex problems methodically, use logical reasoning, and implement effective solutions.

Outline for this course

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