+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 10/06/2024

Sign up

KLCP™ Certification Training (PEN-103)

ALL-IN-ONE: EXAM INCLUDED IN PRICE WITH PEN-103 COURSE

2 days (14 hours)

PRESENTATION

Would you like to demonstrate your offensive security skills and master Kali Linux tools? Our KLCP certification training (PEN-103) will enable you to acquire a wide range of skills and knowledge essential for penetration testing and IT security.

During this training course, you'll learn how to use and configure Kali Linux, manually exploit vulnerabilities, and conduct comprehensive penetration tests. You'll develop in-depth skills in recognizing, scanning, exploiting and post-exploiting targets.

This course will also teach you how to secure systems and networks, use advanced Kali Linux tools for network analysis and security testing, and understand the key concepts of IT security.

After completing our preparation course, you'll be ready to take the Kali Linux Certified Professional (KLCP) certification.

OBJECTIVES

- Understanding and using Kali Linux tools for security testing
- Recognizing and exploiting network and web vulnerabilities
- Master the basic concepts of IT security
- Perform complete penetration tests, from reconnaissance to post-exploitation
- Obtain Kali Linux Certified Professional (KLCP) certification

TARGET AUDIENCE

- Pentesters
- Ethical hackers
- System and network administrators
- Developers and technical architects
- IT Security Analysts

Prerequisites

- Basic knowledge of Linux and operating systems
- Basic knowledge of computer networks
- Fluency in technical English

Software requirements

- **Kali Linux** --> Download here

Note: Ambient IT does not own KLCP™, this certification belongs to OffSec ® Services LLC.

KLCP™ CERTIFICATION TRAINING PROGRAM

INTRODUCTION TO WEB-103

- Introduction to PEN-103 certification and its objectives
- Understanding of basic IT security concepts
- Recognizing the mindset required of a safety professional
- Introduction to the concepts of the security triad: Confidentiality, Integrity, Availability (CIA)
- Key terminology and unique domain features
- Introduction to basic Kali Linux tools
- Lab overview and VPN configuration

GETTING STARTED WITH BASIC TOOLS

- Modifying and configuring the /etc/hosts file
- Host file modification validation tests
- Introduction to proxies and using Burp Suite
- Using Nmap to scan and run NSE scripts
- The concept of word lists and their use with Gobuster
- Using Wfuzz for file and directory discovery
- Using hakrawler for crawling and spidering

WEB PENETRATION TESTING

- Introduction to web penetration testing concepts
- Identification and exploitation of XSS (Cross-Site Scripting) vulnerabilities
- Using JavaScript to exfiltrate data
- Exploiting reflected and stored servers XSS
- Introduction and exploitation of CSRF (Cross-Site Request Forgery) attacks
- Understanding and exploiting weak CORS policies
- Case study in web vulnerability exploitation

NETWORK SCANS AND ANALYSIS

- Introduction to network scanning tools
- Advanced use of Nmap for discovery and enumeration
- Network packet analysis with Wireshark
- Monitoring network connections with Netstat and lsof
- Network performance tests with iperf and hping
- Setting up and using WiFi tools (aircrack-ng suite)
- Network vulnerability analysis with OpenVAS

SECURITY AND SYSTEM ADMINISTRATION

- Security concepts and basic administration under Linux
- User and permissions management
- Firewall configuration (iptables, ufw)
- Cryptography: using GPG and OpenSSL
- Securing network services (SSH, FTP, Web)
- Security auditing and logging with syslog
- Advanced security tools (Metasploit Framework)

OPERATING AND POST-OPERATION TECHNIQUES

- Introduction to operating techniques
- Using Metasploit to exploit vulnerabilities
- Manual operating techniques and scripts
- Maintaining access and elevating privileges
- Lateral movement and persistence on compromised systems
- Data infiltration and circumvention of security measures
- Cleaning and anti-forensic techniques

PRACTICES AND SIMULATIONS

- Setting up a secure laboratory environment
- Simulation of realistic penetration test scenarios
- Practical exercises with Kali Linux tools
- Participation in Capture The Flag (CTF) challenges
- Analysis of real-life security incidents
- Review and preparation for the KLCP exam
- Q&A session for clarification and final revisions

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.