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

Updated on 24/04/2024

Sign up

Kali Linux training

3 days (21 hours)

Presentation

Our Kali Linux training course offers you a unique opportunity to master the Linux distribution specialized in computer security and ethical hacking.

Kali Linux gives you access to a host of advanced, up-to-date security tools, enabling you to carry out in-depth security tests, audits and analyses of networks and computer systems.

During this training course, we'll guide you through the essential aspects of Kali Linux, from its basics to its advanced applications in professional scenarios.

We'll take a detailed look at its architecture, installation and configuration methods, and the practical use of its tools and functions. You'll also learn about best practices in security and ethical hacking.

As with all our training courses, our Kali Linux training course will introduce you to its latest version and new features (at the time of writing: Kali Linux 2024).

Objectives

- Understand the importance of Kali Linux in cybersecurity and the differences between Black Hat and White Hat practices.
- Installing, configuring and securing a Kali Linux installation
- Master the use of scanning tools such as Nmap and Nessus
- Learn the basics of vulnerability exploitation with Metasploit

Target audience

- Pentesters

- Security Analysts
- System administrators

Prerequisites

- Basic knowledge of computers and Linux operating systems
- Familiarity with IT security concepts
- Ability to use the Unix/Linux command line
- Software development experience would be beneficial

KALI LINUX TRAINING PROGRAM

INTRODUCTION TO KALI LINUX

- Introducing Kali Linux and its importance in cybersecurity
- Differences between Black Hat and White Hat practices
- Overview of Kali Linux operating modes
- Legal framework for penetration and security testing
- Guidance on the structure of the training program

INSTALLING AND CONFIGURING KALI LINUX

- How to install Kali Linux on a virtual machine
- Initial configuration and system updates
- Customize your working environment
- Network settings and Internet connection
- Securing the Kali Linux installation

VULNERABILITY DISCOVERY WITH KALI LINUX

- Introduction to systems vulnerability testing
- Using scan tools such as Nmap and Nessus
- Interpreting results and identifying faults
- Creation of vulnerability reports
- Best practices in vulnerability management

NETWORK ANALYSIS TECHNIQUES

- Network fundamentals and use of basic commands
- Practice of the Man in the Middle (MitM) attack
- MAC spoofing techniques and MAC address changes
- Traffic analysis with Wireshark
- Kali Linux-specific network tools

EXPLOITATION OF VULNERABILITIES

- Basic principles of vulnerability exploitation
- Using Metasploit to exploit vulnerabilities
- Building payloads and listening for incoming connections
- Remote control and elevation of privileges
- Post-operation documentation and reporting

BRUTE FORCE ATTACKS

- Understanding brute force attacks and their implications
- Installing and using Patator and Thc-Hydra
- Configure attacks against various services (SSH, FTP, HTTP)
- Protective measures against brute force attacks
- Analysis of results and corrective measures

WIRELESS NETWORK SECURITY

- Introduction to WiFi network security
- Introducing Kali Linux-compatible hardware for WiFi testing
- Using tools such as Aircrack-ng and Reaver
- Techniques for securing and preventing attacks on wireless networks
- Setting up a test attack and analyzing countermeasures

SCRIPTING AND AUTOMATION

- Introduction to scripting with Bash and Python
- Automate repetitive tasks with scripts
- Development of customized tools for safety testing
- Results management with scripts and reporting tools
- Practical scripting exercises applied to cybersecurity

REVISION AND PRACTICE

- Review of key concepts and tools studied during training
- Setting up a test laboratory to practice the techniques learned
- Simulating a safety assessment on a fictitious system
- Feedback and discussion of case studies
- Tips for technology watch and continuous progress in cybersecurity

Companies concerned

This training 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.