Updated on 08/10/2024

Sign up

PacketFence training

2 days (14 hours)

Our PacketFence training course offers a complete immersion in this open source network access management (NAC) solution, specially designed to secure and control connections in heterogeneous environments.

PacketFence automates network device detection and management, provides role-based access control and offers captive portals for user authentication, making it an essential tool for network administrators and IT security teams.

Thanks to its compatibility with the main network equipment (Cisco, Aruba, etc.), PacketFence can be easily integrated into existing infrastructures, while enabling fine-tuned security management, from anomaly detection to the isolation of suspect devices.

During this training course, you'll learn how to install, configure and manage PacketFence, integrate the solution with your network equipment, and define advanced security policies to better protect your critical resources.

You'll also discover how to use PacketFence to monitor incidents in real time and apply automatic sanctions to violations of network security rules.

This training course will enable you to develop key skills for strengthening the security of your network infrastructure, while optimizing the management of users and connected devices.

As with all our training courses, it will be accompanied by the latest resources and best practices in the field.

Objectives

- Master the basic principles of PacketFence and its installation
- Manage users, devices and guests via the captive portal
- Integrating PacketFence with network devices
- Configure and apply role-based network security policies
- Monitoring and maintaining PacketFence

Target audience

- Network administrators
- Safety engineers
- Systems and network technicians
- IT managers

Prerequisites

- Basic knowledge of TCP/IP networks
- Experience in network management or IT security
- Familiarity with network access concepts (VLAN, 802.1X) and network equipment (switches, routers)
- Experience with RADIUS and LDAP tools is a plus

PACKETFENCE TRAINING PROGRAM

Introduction to PacketFence

- Introduction to network security and access management
- PacketFence objectives: access control, guest management, device isolation
- PacketFence history and development
- Use cases in network environments
- Key features: fault detection, captive portal, equipment integration
- Technical requirements for installing PacketFence

Installation and initial configuration

- Preparing the server environment for PacketFence (OS, hardware)
- PacketFence installation via packages and sources
- Basic settings: IP addresses, SSL certificates and DNS
- Network interface configuration (management, isolation, registration)
- Connect to the PacketFence server and discover the web administration interface
- Checking initial operation

User and device management

- Creating and managing users in PacketFence
- Roles and permissions for users
- Peripherals management: add, track and audit
- Introduction to captive portal for user authentication
- Guest management and automatic device registration
- Use of APIs for integration with external systems

Integration with network equipment

- Integration with switches and access points (Cisco, Aruba, etc.)
- Setting dynamic VLAN mode for network segmentation
- Introduction to 802.1X and RADIUS management with PacketFence
- Using ACLs to manage network access
- Network device monitoring: detection and response
- Troubleshooting connections to network devices

Security and network access policies

- Definition of security policies based on roles and profiles
- Management of violations and sanctions: quarantine, blocking
- Configuring safety rules
- Introduction to authentication methods: SSO, LDAP, RADIUS
- Management of certificates and advanced security methods
- Implementation of real-time monitoring and alerts

Network monitoring and maintenance

- Using activity logs for monitoring and auditing
- Real-time incident monitoring and alert management
- Troubleshooting strategies for PacketFence network incidents
- PacketFence updates and maintenance (patches and new versions)
- Backing up and restoring PacketFence configuration
- Steps to production and best practices for deployment

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 forthcoming training course, within the limits imposed by the selected format. This

The questionnaire also enables us to anticipate any connection or internal security problems (intra-company or virtual classroom) that 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.