Security Certification Training Programs

HCIA-Security Training

Training Path

١	Security information and security overview	Lecture,Practice	٢,٠ days
٢	Operation System and Host Security	Lecture,Demonstration	١,٠ day
٣	Network Security Basis	Lecture,Practice	٣,٠ days
٤	Application of Encryption and Decryption	Lecture,Practice	٢,٠ days
٥	Security Operation and Analysis	Lecture,Case study	٢,٠ days

Target Audience

Cyber security junior engineer who hopes to have information security capabilities

Prerequisites

- Basic knowledge of TCP/IP.
- Basic knowledge of Routing and Switching.
- .

Objectives

On completion of this program, the participants will be able to:

- Understand the basic concepts of information security
- Understand information security common specifications
- Configure network devices

- Know some common security attacks
- Know the basic component of operating system
- Understanding the common risks and defense methods of operating systems
- Understand basic firewall technology and configuration
- Understand NAT technology
- Understand firewall dual-system hot back principles
- Know basic network instructions
- Understand encryption principles
- Understand encryption application and practice the related configurations
- Understand the basic process of security operation and maintenance
- Understanding of safety analysis methods and evidence collection methods

Training Contents

Security information and security overview

- Basic Concepts of Information Security
  - Information and Information Security
  - Information Security Risks and Management
- Information Security Standards and Specifications
  - Information Security Standards and Specifications
  - ISO ٢٧٠٠١ ISMS
  - Graded Protection of Information Security
  - Other Standards
- Basic Network Concepts
  - TCP/IP Architecture
  - Common Network Protocols
- Common Network Devices
  - Basic Network Devices
  - Initial Device Login
- Common Information Security Threats
  - Current Situation of Information Security Threats
  - Threats to Network Security
  - Threats to Application Security
  - Threats to Data Transmission and Device Security
- Threat Defense and Information Security Development Trends
  - Security Threat Defense
  - Information Security Awareness

    - Information Security Development Trends

Operation System and Host Security

- Operating System Overview
    - Operating System ١٠١
    - Windows Operating System
    - Linux Operating System
- Common Server Types and Threats
    - Server Overview
    - Common Server Software
    - Server Security Threats
    - Vulnerabilities and Patches
- Host Firewalls and Antivirus Software
    - Windows Firewalls
    - Linux Firewalls
    - Antivirus Software

Network Security Basis

- Introduction to Firewalls
    - Firewall Overview
    - Principle of Firewall Forwarding
    - Firewall Security Policies and Application
    - ASPF
- Network Address Translation
    - NAT Principle
    - Source NAT
    - Server Mapping
    - Application Scenarios
- Dual-System Hot Standby
    - Technical Principles of Dual-System Hot Standby
    - Basic Networking and Configuration of Dual-System Hot Standby
- Firewall User Management
    - User Authentication and AAA Technical Principles
    - User Authentication Management and Application
- Overview of Intrusion Prevention
    - Intrusion Overview
    - Intrusion Prevention System Overview
    - Network Antivirus Overview

Application of Encryption and Decryption

- Encryption and Decryption Mechanisms
  - Encryption Technology Development
  - Encryption and Decryption Mechanisms
  - Common Encryption and Decryption Algorithms
- Public Key Infrastructure (PKI) Certificate System
  - Digital Certificate
  - PKI System Structure
  - PKI Implementation
- Application of Cryptographic Technologies
  - Application of Cryptography
  - VPN Overview
  - VPN Configuration

Security Operation and Analysis

- Introduction to Security Operations
  - Concept of Security Operations
  - Basic Requirements for Security Operations
  - Content of Security Operations
- Data Monitoring and Analysis
  - Proactive Analysis
  - Passive Collection
  - Data Analysis
- Digital Forensics
  - Cyber crime
  - Overview of Digital Forensics
  - Digital Forensic Process
- Cyber Security Emergency Response
  - Background of Cyber Security Emergency Response
  - Overview of Cyber Security Emergency Response
  - Process of Cyber Security Emergency Response
- Case Workshop
  - Discussion on Information Security Deployment Procedure
  - Discussion on Cyber Security Cases

Duration

١٠ working days

Class Size

Max ۱۲