Программа подготовки специалистов в области безопасности компьютерных сетей, совместно с «IITC» - академией «CISCO System Inc.»

Учебный план курса «Защита информации в интернет сетях» (CISCO, Check-Point)

Программа курса.

Курс состоит из трех направлений:

1. **CCENT (Cisco)**

2. **CCNA Security (Cisco)**

3. **CCSA (Check-Point)**

Курс предназначен для выходцев из Советского Союза, желающих получить квалификацию (теоретический материал, сертификат и стажировку) в области информационной безопасности.

По окончании обучения и успешной сдачи экзаменов, учащиеся получат следующие международные сертификаты:

1. CCENT: Cisco Certified Entry Networking Technician

2. CCNA Security: Cisco Certified Network Associate Security

Программа курса:

1. Введение:

- Компьютер, принцип открытой архитектуры, составляющие.
- Использование программ Windows-2000/XP/NT и Office
- Использование операционной системы
- Использование Интернета.

2. CCENT:

Building a sample network

- Exploring the functions of networking
- Securing the network
- Understanding the host-to-host communication Model
- Understanding TCP-IP internet Layer
- Understanding TCP-IP Transport Layer
- Exploring the Packet Delivery Process

Ethernet Local Area Networks

- Understanding Ethernet
- Connecting to an Ethernet LAN
- Understanding the Challenges of Shared LANs
- Solving Network Challenges with Switched LAN Technology
- Exploring the Packet Delivery Process
- Operating Cisco IOS Software
- Starting a switch
- Understanding Switch Security
- Maximizing the Benefits of Switching
- Troubleshooting Switch Issues

Network Environment Management

- Discovering Neighbors on the Network
- Managing Router Startup and Configuration
- Managing Cisco Devices

3. CCNA Security:

Chapter 1

- Modern Network Security Threats
- Fundamental Principles of a Secure Network
- Worms, Viruses and Trojan Horses
- Attack Methodologies

Chapter 2

- Securing Network Devices
- Securing Device Access and Files
- Privilege Levels and Role-Based CL
- Monitoring Devices
- Using Automated Features

Chapter 3

- Authentication, Authorization and Accounting
- Purpose of AAA
- Configuring Local AAA
- Configure Server-Based AAA

Chapter 4

- Implementing Firewall Technologies
- Access Control Lists
- Firewall Technologies
- Context-Based Access Control
- Zone-Based Policy Firewall

Chapter 5

- Implementing Intrusion Perevention
- IPS Technologies
- Implementing IPS

Chapter 6

- Securing the Local Area Networks
- Endpoint Security Considerations
- Layer 2 Security Considerations
- Wireless, VoIP and SAN Security Considerations
- Configuring Switch Security
- SPAN and RSPAN

Chapter 7

- Cryptography
- Cryptographic Services
- Hashes and Digital Signatures and authentication
- Symmetric and Asymmetric Encryption

Chapter 8

- Implementing Virtual Private Networks
- VPNs
- IPSec VPN Components and Operation
- Implementing Site-to-Site IPSec VPNs
- Implementing SSL VPNs

Chapter 9

- Managing a Secure Network
- Secure Network Lifecycle
- Self-Defending Network
- Building a Comprehensive Security Policy

4. CCSA

Chapter 1—Check Point Technology Overview

- Describe Check Point's unified approach to network management and the key elements of this architecture
- Design a distributed environment
- Install the Security Gateway version R75 in a distributed environment

Chapter 2—Deployment Platforms

- Perform a backup and restore the current Gateway installation from the command line
- Identify critical files needed to purge or backup, import and export users and groups and add or delete administrators from the command line
- Deploy Gateways using sysconfig and cpconfig from the Gateway command line

Chapter 3—Introduction to the Security Policy

- Given the network topology, create and configure network, host and gateway objects
- Verify SIC establishment between the Security Management Server and the Gateway using SmartDashboard
- Create a basic Rule Base in SmartDashboard that includes permissions for administrative users, external services, and LAN outbound use
- Configure NAT rules on Web and Gateway servers
- Evaluate existing policies and optimize the rules based on current corporate requirements

- Maintain the Security Management Server with scheduled backups and policy versions to ensure seamless upgrades and minimal downtime

Chapter 4—Monitoring Traffic and Connections

- Use Queries in SmartView Tracker to monitor IPS and common network traffic and troubleshoot events using packet data
- Using packet data on a given corporate network, generate reports, troubleshoot system and security issues, and ensure network functionality
- Using SmartView Monitor, configure alerts and traffic counters, view a Gateway's status, monitor suspicious activity rules, analyze tunnel activity and monitor remote user access based on corporate requirements

Chapter 5—Using SmartUpdate

- Monitor remote Gateways using SmartUpdate to evaluate the need for upgrades, new installations, and license modifications
- Use SmartUpdate to apply upgrade packages to single or multiple VPN-1 Gateways
- Upgrade and attach product licenses using SmartUpdate

Chapter 6—Upgrading to R75

- Based on current products or platforms used in an enterprise network, perform a pre-installation compatibility assessment to upgrade to R75
- Given R71 licensing restrictions, obtain a license key
- Install a Contract File on platforms such as Windows, SecurePlatform, Linux, Solaris or IPSO

Chapter 7—User Management and Authentication

- Centrally manage users to ensure only authenticated users securely access the corporate network either locally or remotely
- Manage user access to the corporate LAN by using external databases

Chapter 8—Encryption and VPNs

- Select the most appropriate encryption algorithm when securing communication over a VPN based on corporate requirements
- Configure a certificate-based site-to-site VPN
- Establish VPN connections to partner sites in order to establish access to a central database by configuring Advanced IKE properties

Chapter 9—Introduction to VPNs

- Configure a pre-shared secret site-to-site VPN with partner sites
- Configure permanent tunnels for remote access to corporate resources
- Configure VPN tunnel sharing, given the difference between host-based, subunit-based and gateway-based tunnels

Chapter 10—Messaging and Content Security

- Configure Check Point Messaging Security to test IP Reputation, content based anti-spam, and zero hour virus detection
- Based on network analysis disclosing threats by specific sites, configure a Web-filtering and antivirus policy to filter and scan traffic

Организатор имеет право изменять, корректировать программу в случае необходимости.