IINS (IMPLEMENTING CISCO IOS NETWORK SECURITY) 3.0

Objetivo

Neste curso, você vai aprender sobre a concepção, implementação e acompanhamento de uma política de segurança abrangente usando recursos de segurança do Cisco IOS e suas tecnologias como exemplos. Você também vai aprender sobre os controles de segurança em dispositivos IOS da Cisco, bem como uma introdução funcional para o Cisco Adaptive Security Appliance (ASA). Este curso permite que você realize tarefas básicas para proteger uma rede utilizando os recursos de segurança Cisco IOS, que estão disponíveis através de interfaces gráficas em Cisco ASA, e a interface de linha de comando (CLI) em roteadores e switches Cisco. Também é abrangido em forma introdutória solução VPN site-to-site em Router IOS Cisco e Cisco ASA Firewall. São apresentados exemplos de malware, e os algoritmos de assinatura digital (hashing) e as técnicas criptográficas. O curso tem como base as versões atuais do Router e Switch Cisco IOS, Cisco ASA Firewall e Cisco AnyConnect. Ao completar o curso, o aluno vai estar preparado para: • Conceitos básicos em segurança de rede; • Prover um roteamento seguro e na infraestrutura de comutação (Switching); • Implantar serviços de autenticação, autorização e estatísticas básicas; • Implantar serviços básicos de firewall; • Implantar serviços básicos de VPN site-to-site básico e VPN de acesso remoto; • Serviços de segurança, como proteção contra intrusão, segurança de conteúdo e gerenciamento de identidade; • Desenvolver uma política de segurança abrangente para combater as ameaças contra a segurança da informação em redes; • Configurar roteadores com recursos de segurança do software Cisco IOS; • Apresentar o Cisco ASA Firewall para uso em uma rede de produção; • Configurar o firewall Cisco ASA para acesso básico em VPN SSL; • Configurar um firewall baseado em zona Cisco IOS (ZBF) para executar operações básicas de segurança em uma rede; • Configurar VPN site-to-site usando os recursos do Cisco IOS; • Configurar recursos de segurança em Cisco IOS para mitigar os riscos de ataques nas camadas 2 e 3; • Implementar acesso seguro ao Cisco IOS e ASA Firewall; • Apresentar os produtos ESA (Email Security Appliance), WSA (Web Security Appliance) e CWS (Cisco Web Security); • Utilizar o processo AAA (Autenticação, Autorização e Contabilidade) usando o banco de dados local, bem como o Cisco Secure ACS 5.X (Ou ISE);

Público Alvo

Este curso apresenta em formato introdutório os profissionais que estão envolvidos na gestão de segurança em soluções Cisco com roteadores e firewalls, que envolve as atividades de instalação, configuração, operação e solução de problemas em segurança. Esse público inclui: • Engenheiros de rede; • Administradores de rede; • Operadores de suporte. Curso recomendado para os profissionais que buscam a preparação para a realização do exame de certificação CCNA Security.

Pré-Requisitos

Para um melhor aproveitamento desse curso é recomendado que o aluno possua os seguintes habilidades e conhecimentos prévios: • Ter participado do treinamento ICND1, ou possuir conhecimentos equivalentes. • Conhecimento básicos de Windows.

Carga Horária

40 horas (5 dias).

Conteúdo Programático

Module 1: Security Concepts

Lesson 1: Threatscape
• Threatscape Overview
• DoS and DDoS
• Spoofing
• Reflection and Amplification Attacks
• Social Engineering
• Evolution of Phishing
• Password Attacks
• Reconnaissance Attacks
• Buffer Overflow Attacks
• Man-in-the-Middle Attacks
• Malware
• Vectors of Data Loss and Exfiltration
• Hacking Tools
• Other Considerations

Lesson 2: Threat Defense Technologies
• Firewalls
• Intrusion Prevention Systems
• Content Security
• VPNs
• Endpoint Security
• Logging
• Summary

Lesson 3: Security Policy and Basic Security Architectures
• Information Security Overview
• Classifying Assets, Vulnerabilities, and Countermeasures
• Managing Risk
• Regulatory Compliance
• Principles of Secure Network Design
• Security Policy
• Security Zones
• The Functional Planes of the Network

Lesson 4: Cryptographic Technologies
• Cryptography Overview
• Hash Algorithms
• Encryption Overview
• Cryptanalysis
• Symmetric Encryption Algorithms
• Asymmetric Encryption Algorithms
• Use Case: SSH
• Digital Signatures

- PKI Overview
- PKI Operations
- Use Case: SSL/TLS
- Key Management

Module 2: Secure Network Devices

Lesson 1: Implementing AAA
- Introduction to AAA
- AAA Databases
- AAA Protocols
- AAA Servers
- SSH Configuration and Operation on IOS
- IOS Authorization with Privilege Levels
- Implementing Local AAA Authentication and Authorization
- Authorization with Role-Based CLI
- TACACS+ on IOS
- Discovery 2: Configure and Verify AAA

Lesson 2: Management Protocols and Systems
- IOS File System
- Copying Files to and from Network Devices
- Validating IOS Images Using MD5
- Digitally Signed Images
- IOS Resilient Configuration
- NTP
- Syslog
- Memory and CPU Threshold Notifications
- Netflow
- Configuration Management Protocol Options
- HTTPS Configuration and Operation
- SNMPv3 Configuration and Operation
- Locking Down Management Access with ACLs
- Other Password Considerations

Lesson 3: Securing the Control Plane
- The Control Plane
- Control Plane Policing
- Control Plane Protection
- Authenticating Routing Protocols
- OSPF Route Authentication
- EIGRP Route Authentication
- Discovery 4: Securing Routing Protocols

Module 3: Layer 2 Security

Lesson 1: Securing Layer 2 Infrastructure
- Introduction to Layer 2 Security

- Ethernet Switching Overview
- VLAN Overview
- VLAN Configuration
- 802.1Q Trunking
- Trunk Attacks
- Trunk Configuration and Attack Mitigation
- CDP
- ACL Primer
- ACLs on Switches
- MAC Address Abuse
- Port Security
- Private VLANs
- Private VLAN Edge
- Private VLAN Proxy Attack and Mitigation

Lesson 2: Securing Layer 2 Protocols
- STP Overview
- STP Attacks
- STP Attack Mitigation
- DHCP Overview
- DHCP Attacks
- DHCP Snooping
- ARP Overview
- ARP Cache Poisoning Attack
- Dynamic ARP Inspection

Module 4: Firewall

Lesson 1: Firewall Technologies
- Firewall Overview
- Packet Filters
- Stateful Firewalls
- Proxy Servers
- Next Generation Firewalls
- Logging

Lesson 2: Introducing the Cisco ASA v9.2
- Introducing the Cisco ASA Family of Security Appliances
- Cisco ASA Firewall Features
- Modes of Deployment
- Security Contexts
- High-Availability and Failover
- Configuring Management Access on the Cisco ASA
- Configuring Cisco ASA Interfaces
- NAT Fundamentals
- Configure NAT on Cisco ASA
- Configure Static NAT on Cisco ASA
- Configure Dynamic NAT on Cisco ASA

• Configure PAT on Cisco ASA
• Configure Policy NAT on Cisco ASA
• Verify NAT Operations

Lesson 3: Cisco ASA Access Control and Service Policies
• Overview of Interface Access Rules
• Configure Interface Access Rules
• Configure Object Groups
• Introducing Cisco ASA Modular Policy Framework
• Configuring Cisco MPF Service Policy Rules

Lesson 4: Cisco IOS Zone Based Firewall
• Zone-Based Policy Firewall Overview
• Zones and Zone Pairs
• Introduction to Cisco Common Classification Policy Language
• Default Policies, Traffic Flows, and Zone Interaction
• Cisco Common Classification Policy Language (C3PL) Configuration Overview
• Configuring Zone-Based Policy Firewall Class-Maps
• Configuring Zone-Based Policy Firewall Policy-Maps

Module 5: VPN

Lesson 1: IPsec Technologies
• IPsec VPNs
• IPsec Security Services
• IPsec Framework
• Internet Key Exchange
• IKE Phase 1
• ISAKMP Configuration
• IPsec Protocols
• IKE Phase 2
• IPsec Configuration
• Suite B Cryptographic Standard
• IKE Version 2
• IPsec with IPv6

Lesson 2: Site-to-Site VPN
• Site-to-Site Tunnel Negotiation Process
• Configuring Site-to-Site IPsec VPN
• Step 1: Ensure That ACLs Are Compatible with IPsec
• Step 2: Create ISAKMP IKE Phase 1 Policies
• Step 3: Configure Transform Sets
• Step 4: Create Crypto ACLs Using Extended ACLs
• Step 5: Configure IPsec Crypto Maps
• Verifying the IPsec Configuration
• Configuring Site-to-Site VPN on Cisco ASA
• Monitoring Site-to-Site VPN Configuration in ASDM

Lesson 3: Client Based Remote Access VPN
• Secure Sockets Layer and Transport Layer Security
• Basic Cisco AnyConnect SSL VPN
• Cisco AnyConnect SSL VPN Solution Components
• SSL VPN Server Authentication
• SSL VPN Client Authentication
• SSL VPN Client IP Address Assignment
• Basic AnyConnect SSL VPN Configuration Tasks

Lesson 4: Clientless Remote Access VPN
• Cisco Clientless SSL VPN
• Cisco Clientless SSL VPN Use Cases
• Cisco Clientless SSL VPN Resource Access Methods
• Basic Clientless SSL VPN Solution
• Server Authentication in Basic Clientless SSL VPN
• Client-Side Authentication in Basic Clientless SSL VPN
• Clientless SSL VPN URL Entry and Bookmarks
• Basic Access Control for Clientless SSL VPN
• Basic Clientless SSL VPN Configuration Tasks

Module 6: Advanced Topics

Lesson 1: Intrusion Detection and Protection
• Introduction to IPS
• IPS Terminology
• Evasion Techniques and Countermeasures
• Protecting the Network with FireSIGHT
• FireSIGHT Protection Before an Attack
• FireSIGHT Protection During an Attack
• FireSIGHT Protection After an Attack
• FireSIGHT Deployment Options
• Inline and Passive Mode Deployment Options
Lesson 2: Endpoint Protection
• Endpoint Security Overview
• Personal Firewalls
• Antivirus and Antispyware
• Centralized Endpoint Policy Enforcement
• Cisco AMP for Endpoints

Lesson 3: Content Security
• Cisco ESA Deployment
• Cisco ESA Overview
• Cisco ESA Features and Benefits
• Cisco ESA GUI Management
• Cisco ESA Mail Processing
• Cisco WSA Deployment
• Cisco WSA Overview
• Cisco WSA Features and Benefits

- Cisco WSA GUI Management
- Cisco CWS Deployment
- Cisco CWS Overview
- Cisco CWS Features and Benefits

Lesson 4: Advanced Network Security Architectures
- Modular Network Architectures
- Security Issues in Modern Networks
- Identity Management
- BYOD Challenge
- Cisco TrustSec