DESCRIPCIÓN:

El 640-553 Interconnecting Cisco Networking Devices Parte 2 (ICND2) es el examen asociado con Cisco Certified Network Associate Security (CCNA Security) el cual valida el nivel de asociación de conocimientos y habilidades requerido para asegurar las redes Cisco. Con la certificación CCNA Security, un profesional de las redes demostrará las habilidades necesarias para desarrollar la seguridad de una infraestructura, reconocer amenazas y vulnerabilidades de las redes, así como mitigar amenazas de seguridad. El currículum CCNA Security enfatiza en las tecnologías de seguridad básicas, la instalación, solución de problemas y seguimiento a los dispositivos de la red para mantener la integridad, confidencialidad y disponibilidad de los datos y dispositivos así como la competencia en las tecnologías que Cisco utiliza en su estructura de seguridad.

Nuestro programa de entrenamiento Cisco® CCDA® Security sigue estrictamente los currículos de entrenamiento Oficial de Cisco®.

CARACTERÍSTICAS DEL CURSO:

- Instructor altamente capacitado conduce presentaciones en video.
- Demostraciones prácticas de laboratorio.
- Prácticas Reales de Laboratorio
- Pruebas de repaso por capítulo.
- Material de apoyo.
- Soporte 24 x 7 en nuestra comunidad Mentoring.

PRERREQUISITOS

Se recomienda experiencia laboral en servicios de TI.

Nuestro curso es en Idioma inglés y modalidad en línea a través del portal educativo de BPUniversity.
Module 01 - Introduction to Network Security Principles

Introduction to Network Security Principles
Examining Network Security Fundamentals
Threats to Security
Addressing Internal Threats
External Threats
Threat Capabilities - More Dangerous and Easier to Use
Size of the Problem
The Evolution of Intent
Vulnerable Custom Applications
Network Security Objectives
Confidentiality
Integrity
Availability
Information Classification
Classification Levels
Classification Criteria
Information Classification Procedures
Distribution of Classified Materials
Information Classification Roles
Security Controls
Administrative Controls
Technical Controls
Physical Controls
Type of Controls
Computer Crime Investigations
Computer Crime Complications
Collection of Evidence
Types of Law
Ethics
Liability
Legal and Government Policy Issues
Section 1 - Review
Examining Network Attack Methodologies
Vulnerabilities, Risks, and Exploits
Main Vulnerability Categories
The Human Vulnerability Factor
Adversaries
Hackers, Crackers, and Phreakers
Computer Security Hackers
Motivations
Academic Hackers
Hobby Hackers

Thinking Like a Hacker
The Purpose of Defense in Depth
What Is Defense in Depth?
Examples of Defense in Depth
Early Defense in Depth Example
Defense in Depth Technical Example
Defense in Depth Non-Example
IP Spoofing
IP Spoofing - A Technical Discussion
IP Spoofing - Types of Attack
IP Source Routing Options
Man-in-the-Middle Attacks
Demo - MITM
Confidentiality Violations
Ping Sweeps and Port Scans
Packet Sniffers
Emanations Capturing
Overt and Covert Channels
Overt Channel Example
Stenography
Covert Channel Example
Phishing, Pharming, and Identity Theft
Integrity Violations
Trust Exploitation
Port Redirection
Password Attacks
Availability Violations
Botnets
DoS and DDoS Attacks
DDoS Example
TCP SYN Flooding
DoS Attacks Using ICMP
Smurf Attack
Electrical Power
Computing Environment
Best Practices to Defeat Hackers
Section 2 - Review
Examining Operations Security
Operations Security
Secure Network Lifecycle
Initiation Phase
Acquisition and Development Phase
Implementation Phase
Operations and Maintenance Phase
Disposition Phase
Principles of Operations Security
Separation of Duties
Rotation of Duties
Trusted Recovery
Change and Configuration Control
Network Security Testing and the System Development Life Cycle
Security Testing Techniques
Common Testing Tools
Nmap
SuperScan by Foundstone
Disaster Recovery and Business Continuity Planning
Disaster Recovery
Disruptions
Backups
Section 3 - Review
Understanding and Developing a Comprehensive Network Security Policy
Figure Out What You Are Protecting
Module 02 - Perimeter Security

Perimeter Security
Securing Administrative Access to Cisco Routers
Router Security Principles
How Routers Enforce Perimeter Security Policy
Cisco Integrated Services Routers
Cisco Integrated Services Router Features
Cisco Secure ACS Prerequisites
Cisco Secure ACS 4.1 Homepage
Network Configuration
Interface Configuration
External Databases
Windows Database
Unknown User Policy
Group Setup
User Setup
Adding a AAA Server
Creating a AAA Login Authentication Policy
Applying an Authentication Policy
Creating a AAA Exec Authorization Policy
Creating a AAA Network Authorization Policy
AAA Accounting Configuration
AAA Configuration for TACACS+ Example
debag tacacs
debag tacacs events
Demo - AAA Authentication
Demo - Authentication Servers
Demo - ACS Server
Section 4 - Review
Implementing Secure Management and Reporting
Considerations for Secure Management and Reporting
Secure Management and Reporting Architecture
Secure Management and Reporting Guidelines
Syslog Systems
Cisco Security MARS
Cisco Security MARS Process Flow
Implementing Log Messaging for Security
Cisco Log Severity Levels
Log Message Format
Enabling Syslog Logging
Using Logs to Monitor Network Security
SNMPv1 and SNMPv2 Architecture
Community Strings
SNMPv3 Architecture
SNMP Security Models and Levels
Enabling SNMP with Cisco SDM
SNMP Trap Receiver
Secure Shell
Enabling SSH Using Cisco SDM
VTY Settings
Configuring an SSH Daemon Using the CLI
Manually Configuring Data and Time Settings
Network Time Protocol
Enabling NTP with Cisco SDM
Section 5 - Review
Locking Down the Router
Vulnerable Router Services and Interfaces
Management Service Vulnerabilities
Security Audit Home Page
Performing a Security Audit
Performing a One-Step Lockdown
Locking Down a Router Using Cisco Auto Secure
Limitations and Cautions
Module 03 - Network Security Using Cisco IOS Firewalls

Network Security Using Cisco IOS Firewalls
Introducing Firewall Technologies
What is a Firewall?
Expanding on the Definition
Firewall Benefits
Firewall Limitations
Firewalls in a Layered Defense Strategy
Static Packet Filtering Firewalls
Static Packet Filtering Example
Advantages and Disadvantages of Packet Filters
Application Layer Gateways
Proxy Server Communication Process
Advantages, Limitations, and Uses of Application Layer Gateways
Dynamic or Stateful Packet Filtering
Stateful Packet Filtering
Uses and Limitations of Stateful Packet Filters
Application Inspection Firewalls
Transparent Firewalls
Cisco IOS Firewall Features
Cisco Security Router Certifications
Cisco PIX 500 Series Security Appliances
Cisco ASA 5500 Series Adaptive Security Appliances
Firewall Best Practices
Section 1 - Review
Creating Static Packet Filters Using ACLs
Access Control Lists
Mitigating Threats Using ACLs
Outbound ACL Operation
Inbound ACL Operation
A List of Tests - Deny of Permit
Types of IP ACLs
Identifying ACLs
IP Access List Entry Sequence Numbering
ACL Configuration Guidelines
Wildcard Bits - How to Check the Corresponding Address Bits
Wildcard Bits to Match IP Subnets
Wildcard Bit Mask Abbreviations
Numbered Standard IPv4 ACL Configuration
Numbered Standard IPv4 ACL
Applying Standard ACLs to Control vty Access
Numbered Extended IPv4 ACL Configuration
Established Command
Displaying ACLs
Guidelines for Developing ACLs
ACL Caveats
ACL Editor - Access Rules
Standard Rule
Associate with an Interface (1)
Extended Rule
Associate with an Interface (2)
Routing Protocol Entries
IP Address Spoof Mitigation - Inbound
IP Address Spoof Mitigation - Outbound
Filtering ICMP Messages - Inbound
Filtering ICMP Messages - Outbound
Permitting Common Services
Router Service Traffic
Demo - ACL
Section 2 - Review
Configuring Cisco IOS Zone-Based Policy Firewall
Cisco IOS Zone-Based Policy Firewall
In the Beginning
Traditional Cisco IOS Firewall Stateful Inspection
The New Era: Cisco IOS Zone-Based Policy Firewall
Benefits of Zone-Based Policy Firewall
Zone-Based Policy Firewall Actions
Zone-Based Policy Firewall Rules for Application Traffic
Zone-Based Policy Firewall Rules for Router Traffic
Basic Firewall Configuration Wizard
Basic Firewall Interface Configuration
Applying Security Policy
Finishing the Wizard
Manually Configuring a Zone-Based Policy Firewall
Define Zones
Define Class Maps
Define Policy Maps
Assign Policy Maps to Zone Pairs
Reviewing the Cisco IOS Zone-Based Policy Firewall
Cisco IOS Zone-Based Firewall Policy Configuration
Viewing the Firewall Log
Monitoring the Cisco IOS Zone-Based Policy Firewall
Section 3 - Review
Module 03 - Review

Module 04 - Site-to-Site VPNs
Site-to-Site VPNs
Examining Cryptographic Services
Cryptology Overview
Cryptography History
Substitution Cipher
Vigenere Cipher
Transposition
One-Time Pads
Transforming Plaintext into Ciphertext
Cryptanalysis
Encryption Algorithm Features
Encryption Keys
Symmetric Encryption Algorithms
Asymmetric Encryption Algorithms
Block and Stream Ciphers
Choosing an Encryption Algorithm
Key Comparisons
Overview of Cryptographic Hashes
What Is Key Management?
Keyspaces
Key Length Issues
SSL Overview
SSL Tunnel Establishment
Section 1 - Review
Examining Symmetric Encryption
Symmetric Encryption Overview
Symmetric Encryption Key Lengths
Acceptable Key Lengths
DES
DES Modes
DES ECB vs. CBC Mode
DES Usage Guidelines
3DES
3DES Encryption Process
AES
SEAL
RC Algorithms
Section 2 - Review
Examining Cryptographic Hashes and Digital Signatures
Overview of Hash Algorithms and HMACs
What Is a Hash Function?
Hashing in Action
Hashed Message Authentication Code
HMAC in Action
Message Digest 5
Secure Hash Algorithm 1
MD5 and SHA-1 Compared
Hash and HMAC Best Practices
Overview of Digital Signatures
Digital Signatures in Action
Digital Signatures Example
Digital Signature Standard
Digital Signature Best Practices
Section 3 - Review
Examining Asymmetric Encryption and PKI
Asymmetric Encryption Overview
Asymmetric Encryption Algorithms
Public Key Confidentiality Scenario
Asymmetric Confidentiality Process
Public Key Authentication Scenario
Asymmetric Authentication Process
RSA Algorithm
RSA Digital Signatures
RSA Usage Guidelines
The DH Algorithm
The DH Key Exchange Algorithm
Trusted Third-Party Protocols
Trusted Third-Party Example
PKI Terminology and Components
PKI Topologies - Single - Root CA
PKI Topologies - Hierarchical Cas
PKI Topologies - Cross - Certified Cas
PKI and Usage Keys
PKI Server Offload
Overview of Standardization
X.509v3
Public-Key Cryptography Standards
Simple Certificate Enrollment Protocol
Identity Management Using Digital Certificates and CAs
Retrieving CA Certificates
Certificate Enrollment
Authentication Using Certificates
Features of Digital Certificates and CAs
Caveats of Digital Certificates and CAs
Applications of Certificates
Section 4 - Review
Examining IPSec Fundamentals
What Is a VPN?
Benefits of VPNs
Site-to-Site VPNs
Remote-Access VPNs
Cisco IOS SSL VPN
Cisco VPN Products
Cisco VPN-Enabled IOS Routers
Cisco ASA Adaptive Security Appliances
VPN Clients
Hardware-Based Encryption
What is IPSec?
IPSec Security Services
Encryption Algorithms
DH Key Exchange
Data Integrity
Authentication
IPSec Advantages
IPSec Versus SSL
IPSec Security Protocols
Authentication Header
AH Authentication and Integrity
Encapsulating Security Payload
ESP Protocol
Modes of Use - Tunnel Versus Transport Mode
Tunnel Mode
IPSec Framework
Internet Key Exchange
IKE Communication Negotiation Phases
IKE Phase 1
First Exchange - IKE Policy Is Negotiated
Second Exchange - DH Key Exchange
Third Exchange - Authenticate Peer Identity
IKE Phase 2
Section 5 - Review
Building a Site-to-Site IPSec VPN
Site-to-Site IPSec VPN
Site-to-Site IPSec Configuration
Step 1: Ensure That ACLs Are Compatible with IPSec
Step 2: Create ISAKMP (IKE) Policies
IKE Policy Negotiation
Configure PSKs
Site-to-Site IPSec Configuration - Phase 1
Step 3: Configure Transform Sets
Transform Set Negotiation
Purpose of Crypto ACLs
Step 4: Create Crypto ACLs Using Extended ACLs
Configure Symmetric Peer Crypto ACLs
Benefits of a SAN
SAN Basics
LUN Masking
World Wide Names
Fibre Channel Fabric Zoning
Virtual SANs
SAN Security Scope
SAN Management Threats
Fabric and Target Access Threats
Target Access Security - Zoning
IP Storage and Transmission Security
Section 2 - Review
Examining Voice Security
What is VoIP?
Business Case for VoIP
Components of a VoIP Network
Major VoIP Protocols
Threats to IP Telephony Endpoints
Spam over IP Telephony
SPIT Example
Fraud
SIP Vulnerabilities
Separate Voice VLAN
Protect IP Telephony with Firewalls
Protect IP Telephony with VPNs
Protect IP Telephony Endpoints
Protect IP Telephony Servers
Section 3 - Review
Mitigating Layer 2 Attacks
Why Worry About Layer 2 Security?
Domino Effect
VLAN Overview
VLAN Hopping by Rogue Trunk
VLAN Hopping by Double Tagging
Mitigating VLAN Hopping Network Attacks
Redundant Topology
Loop Resolution with STP
STP Operation
STP Root Bridge Selection
STP Manipulation
PortFast
BPDU Guard
Root Guard
Verifying BPDU Guard
CAM Table Overflow Attack
MAC Address Spoofing Attack
Port Security
Configuring Port Security
Configuring Port Security Aging
Port Security Example
Verifying Port Security
Notification of Intrusions
Switched Port Analyzer
Remote SPAN
Lan Storm
Storm Control

Layer 2 Security Best Practices
Demo - Layer 2 Security
Section 4 - Review
Module 06 - Review
Course Closure

Total Duration: 20 hrs 15 min