CompTIA Sec+ SY0-401, Part 1 of 8: Network Security [Deprecated/Replaced]

Meet the expert: Ryan Hendricks is an experienced instructor who teaches networking and security courses to IT professionals throughout the nation. He currently has the CompTIA Certified Technical Trainer (CTT+ Classroom) and the Cisco Certified Academy Instructor (CCAI) credentials. He holds certifications from (ISC)2, EC-Council, CompTIA, and Cisco. When not on the podium instructing, he delves into IT books, always looking to learn more and keep up with the latest security topics.

Prerequisites: This course assumes that the user has working knowledge of networks and networking. Ideally, the user should have their CompTIA Network+ certification, but can be replaced with networking experience.

Runtime: 01:57:16

Course description: In this course we will discuss the plethora of security devices found on the network. As a security professional you need to understand how these devices work, the methods used to implement security, and the design considerations needed when deploying them. We will cover all of these topics while keeping our focus on the security of the network. Security should be at the forefront of priorities, not an afterthought. This class will be a step in becoming a security conscientious individual. This course will cover the CompTIA Security+ objectives 1.1, 1.2, and 1.3.

Course outline:

Devices
- Introduction
- Switches
- Switches, Cont.
- Routers
- Routers, Cont.
- Firewalls
- Firewalls, Cont.
- Packet Filtering Firewall
- Packet Filtering Firewall, Cont.
- Stateful Firewall
- Stateful Firewall, Cont.
- Application Based Firewall
- App Based Firewall, Cont.
- Web Application Firewall
- Load Balancer
- Proxies
- Web Security Gateway
- VPN Concentrator
- Summary

Devices 2
- Introduction
- Intrusion Detection & Prevention
- IDS & IPS Rules
- IDS & IPS Rules, Example
- Network IDS & IPS Placement
- Detection Techniques
- Detection Techniques, Cont.
- Protocol Analyzer
- Protocol Analyzer, Cont.
- Spam Filter
- Unified Threat Management
- URL Filtering
- Content Inspection
- Malware Inspection
- Application Aware Devices
- Summary

Administration
- Introduction
- Rule-Based Management
- Rule Definitions, Cont.
- Explicit and Implicit Rules
- Firewall Rules
- Firewall Rules, Cont.
- Firewall Illustration
- VLAN Management
- VLAN Illustration
- VLANs
- Secure Router Configuration
- Access Control List
- ACLs, Cont.
- Port Security
- Port Security, Cont.
- 802.1x
- 802.1x, Cont.
- Flood Guards
- Loop Protection
- Loop Protection, Cont.
- Network Separation
- Network Separation, Cont.
- Log Analysis
- Log Analysis, Cont.
- Demo: Firewall Rules
- Demo: New Firewall Rule
- Summary

Design
- Introduction
- Demilitarized Zone
- DMZ illustration
- DMZ Devices
- Subnetting
- VLANs
- VLAN Illustration
- Network Address Translation
- NAT, Cont.
- Port Address Translation
- IPv4 Link-Local Range
- Remote Access
- Telephony
- Telephony, Cont.
- Network Access Control
- Virtualization
- Virtualization, Cont.
- Cloud Computing
- Essential Characteristics
- Service Model: SaaS
- Service Model: PaaS
- Service Model: IaaS
- Deployment Models
- Layered Security
- Summary