Train Signal - Cisco CCNA Security 640-553:IINS raining

You cannot be a Cisco Network Administrator without knowing Cisco Security. Today, security knowledge is no longer a luxury, it is a necessity in nearly any IT position. Any job applicant, from the most experienced network admin to the entry level junior admin will be required to demonstrate a substantial amount of knowledge concerning security elements. Passing the CCNA Security exam and proving your security knowledge is difficult. That's why I have created this comprehensive course that shows you how to tackle the diverse security issues that you will face on the exam and in the real world. As with all Train Signal courses, this CCNA Security course presents the same combination of clearly explained theory and an abundance of "real world" lab examples using the new Security Device Manager (SDM) and the Command Line. This exciting course contains over 13 hours of video instruction where I break down network security theory as you work hands on with real Cisco routers & switches... and secure your own network! Video 1 Hackers - Their Motives and Methods Learn about Hacker Roles and why they hack. Discover what your Network Security Goals should be, and how to implement Network Security Best Practices to achieve those goals to keep from suffering the consequences of ineffective network security. - Why Do Hackers Hack? - General Network Security Goals - The Consequences of Ineffective Network Security - Where Network Attacks Originate From - Social Engineering Attacks - Trojan Horses and Privilege Escalation Attacks - Using Ping Sweeps and Port Scans on Your Own Network - Best Practices Video 2 Introduction to SDM (Security Device Manager) Improve productivity, simplify router deployments, and troubleshoot complex connectivity issues using the Security Device Manager. Plus, launch, login, and tour SDM and discover some Real World SDM issues as you learn to manage your router away from the Command Line. - Cisco's Security Device Manager (SDM) - Pre-installation Configuration - Installing SDM - Launching and Loading SDM - SDM Settings - User Preferences - SDM Configure Window - Additional Tasks Tab - SDM Monitor Window - SDM in Internet Explorer Problem Video 3 Authentication, Authorization, and Accounting (AAA) Learn how Authentication works in AAA, what happens when you specify different devices used for Authentication, and discover commands used in Authentication, Authorization, and Accounting that will be useful in the real world and on the exam. Plus, configure TACAS+ and RADIUS security protocols. - What is AAA? - TACAS+ vs. RADIUS - TACAS+ and RADIUS Configuration - Authentication Configuration - No Authentication Option - Telnet Login Problem - Real World Not About AAA Lists - Using AAA for Privileged EXEC Mode and PPP - Accounting - Authorization - Configuring AAA with SDM Video 4 Layer 2 Security Learn how to prevent security threats like CAM Overflow attacks by configuring and implementing Port Security, Sticky Addresses, Lightweight Extensible Authentication Protocol (LEAP), and SPAN. Plus, discover the relationship between DHCP Snooping, Dynamic ARP Inspection, and IP Source Guard and learn to configure and operate Root Guard and BPDU Guard. - Basic L2 Security Features - Cisco Password Rules Review - Preventing CAM Overflow Attacks with Port Security - Port Security - Configuring Port Security - Misconfiguring Port Security - Aging Time for Secure Addresses - Sticky Addresses - Configuring MAC Table Event Notification - Dot1x Port-Based Authentication - Cisco Lightweight Extensible Authentication Protocol (LEAP) - Extensible Authentiaction Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) - Local SPAN Configuration - Remote SPAN Configuration - Filtering Intra-VLAN Traffic - VLAN Access List (VACL) - Private VLAN - DHCP Snooping - Dynamic ARP Inspection - IP Source Guard - MAC Address Flooding Attacks - VLAN Hopping - Root Guard - BPDU Guard Video 5 Layer 3 Security This is one of the most important Videos in the course because of the volume of detailed information that you will use on the exam and in the real world. Learn about "Salting" your MD5 to make an encrypted password even stronger and discover how Network Time Protocol (NTP) will be important in your security deployment. Plus, learn to configure and use Superviews, Autosecure, Security Audits, and One-Step Lockdown via SDM to thwart ICMP based attacks, IP Spoofing, and Recon Attacks. - Configuring Enable Password - Privileged Level Password vs. Privleged Level Secret - Encrypting Passwords - Strong Passwords vs. Weak Passwords - Creating and Testing Minimum Length Password Policy - "Salting" your MD5 - Network Time Protocol (NTP) - Configuring NTP Master Time Source - Synchronizing System Clocks - Configuring Peering with NTP Peers Command - Other Clock Commands - Telnet and SSH - Creating Banners - Different Types of Network Attacks - Denial of Services (DoS) Attack and SYN Flooding Attack - TCP Intercept Defense - ICMP (Ping) Sweep, Port Scan and Port Sweep - Ping of Death vs. Invite of Death and Ping Floods - Smurf Attacks - Availability Attacks: Don't Forget the Physical Layer! - IP Spoofing - IP Source Routing - Packet Sniffers and Queries - Other Confidentiality Attacks - Password Attacks - Salami Attack - Other Network Attacks Types - Trust Exploitation - Superviews - Role-Based CLI Views - AutoSecure - One-Step Lockdown - Security Audit - NTP and SSH in SDM - Differences Between SDM and AutoSecure - SNMP - Logging - Viruses and Worms - Cisco IOS Logging Enhancements - Buffer Overflow - Cisco IOS Resilient Conofiguration and Login Enhancements - exec-timeout Command Video 6 The

Intrusion Prevention System (IPS) Learn the differences between Intrusion Detection (IDS) and Intrusion Prevention (IPS) and how they operate. Plus, discover the different approaches to identifying malicious traffic and learn to use NIPS, HIPS and Honeypots to stop it. We'll also configure your Intrusion Prevention System using the Security Device Manager (SDM) and we'll use the Command Line to verify this IPS configuration. - Intrusion Detection (IDS) vs. Intrusion Prevention (IPS) - Signatures and Signature Types - NIPS and HIPS - Honeypots - Configuring IPS in SDM - Editing IPS Rules - Editing Global Settings - SDEE Message Logs - Viewing Signatures - Editing and Deleting Signatures - Verifying Your IPS Configuration Video 7 Firewalls Learn to enable a Cisco router to act as a firewall using the Cisco IOS Firewall Set. Plus, discover concepts relatively new to Cisco like Zone-based Firewalls that are meant to phase out CBAC and the "ip inspect" command. We'll also configure and edit a firewall using the Security Device Manager's (SDM) Basic Firewall Wizard and we'll draw distinctions between the Basic Firewall Wizard and SDM's Advanced Firewall Wizard. - Firewall Basics - Stateless and Stateful Firewalls - Application Layer Gateway (ALG) - The Cisco IOS Firewall Feature Set Components - Authentication Proxy - Plan for Firewall Success Then Succeed! - ACL Review - Extended ACL Review - Extended Access Control Lists - Real-World ACL Success Tips - Introduction to Turbo ACLs - CBAC and "ip inspect" command - Real-World Tips and Best Practices - TCP and UDP Generic Inspection - Deep Pocket Inspection (DPI) - Zone-Based Firewall Configuration - Class Maps and Policy Maps - Basic Zone Commands - Configuring Zone Pairs - Configuring Firewall with SDM's Basic Firewall Wizard - Editing Firewall with SDM - SDM's Advanced Firewall Wizard - Watch Your Directions - More Tips - ICMP Inspection - Final Note Video 8 Cryptography and Virtual Private Networks (VPNs) Learn how Asymetric and Symetric Algorithms can be used to implement Cryptography Techniques that help encrypt clear text passwords. Plus, configure your own IKE policy using the Command Line and get your hands dirty by using the Security Device Manager (SDM) to configure Site-to-Site VPN and Generic Routing Encapsulation (GRE) over IPsec. - Cryptography Techniques - Asymmetric and Symmetric Algorithms - RSA Algorithm - Diffie-Hellman (DH) - A Word or Two About SHA - What is VPN? - VPN Terminology and Theory - Introduction to PKI and the Certificate of Authority - Public Key Cryptography Standards (PKCS) - Internet Key Exchange (IKE) - Steps to Configure Site-to-Site VPN - Configuring IKE Policy Using Command Line - Policy Match Criteria - Crypto ACLs - Mirror Configuration - Creating Crypto Map - Using SDM to Configure Site-to-Site VPN - Generating Mirror in SDM - Testing Our Configuration - Verifying SDM Configuration Using Command Line - The Return of Generic Routing Encapsulation (GRE) Over IPSec - Using SDM to Configure GRE over IPSec Video 9 Introduction to Voice and SAN Security You do not need to be an expert in Voice Networking or Storage Area Networking (SAN) to learn how to keep these types of networks secure. Learn the differences between FCAP and FCPAP, discover the details of LUN and LUN Masking, and delve deeper into VoIP (Voice Over IP). Whatever your experience level may be, this detailed overview of Voice and SAN Networking will provide you the insight you need to get into one of the fastest growing areas in the IT field. - Voice Over IP Overview - Gateways and Gatekeepers - VoIP Protocols - Typical VoIP Attacks and Precautions - Introduction to Storage Area Networking (SAN) - SAN Transport Technologies and Protocols - SAN Security - LUNS and LUN Masking - SAN Zones - Virtual SANs (VSANs) - FCAP and FCPAP Video 10 Introduction to Cisco Network Solutions This Video will introduce you to Cisco Network Solutions including: ASA 5500, Cisco Self-Defending Network, Cisco Security Management Suite, and Cisco Security Agent. Plus, learn about the five phases of the Cisco SDLC (System Development Life Cycle) and discover the differences between Quantitative Risk Analysis and Qualitative Risk Analysis. - System Development Life Cycle - Cisco SDLC Phase 1 - Initiation - Cisco SDLC Phase 2 - Acquisition and Development - Cisco SDLC Phase 3 - Implementation - Cisco SDLC Phase 4 - Operation and Maintenance - Cisco SDLC Final Phase - Disposition - Disaster Recover - Hot, Warm and Cold Sites - Risk Analysis - Quantitative and Qualitative - Cisco Self-Defending Network - Cisco Security Management Suite - IronPort - Cisco Security Agent - Cisco Security Agent Interceptors - Cisco ACS - "in-band" and "out of band" Download **[This hidden password content is only available for our VIP member. Become VIP Member NOW**