CBT Nuggets - Cisco CCNA Security Exam Pack 640-553: IINS

Jump into security with Jeremy Cioara's Cisco CCNA Security video series. Jeremy puts you in the mind of hackers and intruders and shows you how to defeat these black hats. Soon you'll be recognizing different types of attackers and threats and eliminating the damage that can follows security breaches. Jeremy's videos move from one "cool topic" to the next -- showing you the big picture involved in securing your network. By the time you've finished watching the full series, you'll have a terrific foundation in Cisco security. And you'll be respected for the confidentiality, integrity and availability that you bring to your organization's network data. This training is mapped to Cisco CCNA Security exam 640-533 IINS, so you'll be ready to pass the certification test. **What You'll Learn** Video 1: Welcome to CCNA Security: Cisco Certification and Getting the Most from This Series|32:45 With every new program, there is typically an included "Read Me First" text file. In the same sense, consider this nugget the "Watch Me First" of the series. This nugget presents the strategies you can use for getting the most from the series, changes to the Cisco certification program, and the ideal CCNA Security lab environment. Video 2: Welcome to CCNA Security: Understanding the Threats|31:18 It's impossible to defend against something you don't understand. In this nugget, Jeremy defines the goal behind having a secure network and the categories of intruders and attacks. Video 3: Welcome to CCNA Security: Understanding the Threats, Part 2|27:49 Jeremy continues defining the properties of a secure network by discussing many of the network attacks you can face and a general mitigation strategy. In addition, Jeremy discusses the components behind the Cisco Self-Defending Network system. Video 4: Foundation Router Security: Using SDM to Lock Down Your Router|41:22 The Cisco Security Device Manager (SDM) is a powerful graphic interface you can use to manage your router and perform complex tasks with the click of a mouse button. This nugget walks through the process of configuring your router to support Cisco SDM and using the SDM to perform a security audit or one-step lockdown of your device. Video 5: Foundation Router Security: Implementing Secure Router Management|47:46 One of the first areas of security you should consider is the management traffic between you and the network devices. In this nugget, Jeremy describes creating an Out Of Band (OOB) management network and three areas of network management: syslog, SNMP, and SSH. Video 6: Foundation Router Security: Understanding and Implementing AAA|43:22 AAA is more than just roadside assistance; it represents authentication, authorization, and accounting (AAA) methods you can use on a Cisco device. This nugget describes the concepts behind AAA and walks through the setup of a AAA device and the Cisco ACS TACACS+ server. Video 7: Foundation Router Security: Using IOS-based Tools for Administrative Access|32:21 While server security is essential, network security is of the utmost importance. One of the first network areas requiring more security is the area of administrative access. By default Cisco switches and routers will allow someone to attempt to logon to the device infinitely. This nugget focuses on locking down this logon prompt, configuring role-based access (sub-administrators), and securing the IOS and configuration files on your devices. Video 8: Foundation Router Security: Becoming an ACL Wizard|49:15 Understanding the implementation of Access Control Lists (ACLs) is critical for any Cisco environment, however, you can apply ACLs in more ways than one. In this nugget, Jeremy walks through guidelines for using ACLs followed by four practical scenarios of ACL implementation. Video 9: Foundation Switch Security: Locking Down the Catalyst Switch|29:51 In this nugget, all eyes turn to the internal network as Jeremy discusses Layer 2 security for your network. This initial nugget explores the reasons for L2 security, common attacks at L2, and concludes with one of the core mitigation techniques: port security. Video 10: Foundation Switch Security: Locking Down the Catalyst Switch, Part 2|38:49 Layer 2 security continues as Jeremy builds multiple layers of security at the switch level including Spanning Tree Protocol (STP) protection, Rogue DHCP server control, Storm Control, SPAN, and Private VLANs. Video 11: Foundation Switch Security: Understanding NAC, Cisco CSA. and VoIP Security|34:29 The evolution of network attacks have dictated an entire new generation of Layer 2 security methods. In this nugget, Jeremy discusses these newer forms of security such as Network Admission Control (NAC), 802.1x, the Cisco Security Agent (CSA), and VoIP security. Video 12: Security Services: Implementing Router-Based Firewalls|22:35 The security focus moves from the switch environment to the routed network. This initial nugget discusses Cisco's two firewall strategies: The Cisco IOS Classic Firewall and the Zone-based Firewall. Video 13: Security Services: Implementing Router-Based Firewalls, Part 2|01:00:46 Cisco's Zone-based Firewall strategy is a completely new style of firewall for IOS routers. This nugget walks through the implementation of the new Zone-based Firewall on live Cisco gear. Video 14: Security Services: Implementing Router-Based IPS|52:00 The Cisco Integrated Service Router (ISR) product line was designed to implement many traditionally separate network functions into a single device. This made the implementation of Intrusion Prevention System (IPS) a natural one. In this nugget, Jeremy discusses the place and configuration of Cisco IPS on an ISR device. Video 15: Security Services: Understanding VPN Components - IPSec and Encryption|51:49 (VPNs) have become a commonplace technology to allow remote users to access a network and bridge multiple offices connected to the Internet into a seamless network fabric. The

architecture behind VPN technology is anything but commonplace. In this nugget, Jeremy discusses the IP Security (IPSec) protocol used to create VPN connections, focusing specifically on the encryption capabilities. Video 16: Security Services: Understanding VPN Components - Digital Signatures and PKI|31:48 The VPN discussion continues as Jeremy explains the ideas behind the Public Key Infrastructure (PKI) and certificate-based authentication. Video 17: Security Services: Understanding VPN Architecture|19:09 This final, conceptual nugget on VPN technology focuses on the process devices go through when establishing a VPN connection. Special attention is given to the important concepts of identifying interesting traffic and the Internet Key Exchange (IKE) phases. Video 18: Security Services: Implementing Site-to-Site VPNs via Command Line|50:21 It's time to put the VPN concepts into action! In this nugget, Jeremy walks through the step-by-step process to configure a site-to-site VPN using the command line interface. Video 19: Security Services: Implementing Site-to-Site VPNs via SDM|17:10 Once you have seen the command-line configuration of a site-to-site VPN, this nugget shows you the "easy configuration method" by setting up the same VPN using the Cisco Security Device Manager (SDM) graphic interface. Video 20: A Final Word to CCNA Security Test Takers|06:10 To conclude the CCNA Security series, Jeremy gives some final tips to those focused on the certification exam. Download **[This hidden password content is only available for our VIP member. Become VIP Member NOW**