CCIE Security - Lab Preparation

Duration: 5 Days Course Code: CCIESEC

Overview:

The CCIE Security program is a program intended to recognize the Cisco network security experts who have the necessary skills to test, deploy, configure, maintain, and troubleshoot Cisco network security appliances and Cisco IOS Software devices that establish the security posture of the network.

CISCO Exam Covered: CCIE Security Lab Exam v.4
Course Delivery Method:This boot camp is a combination of lecture and hands-on labs.
Students Will Receive: Advanced CCIE Security Workbook v4 (Technology Focused)
Boot Camp Hours: Monday – Friday 9:30 AM – 9:00 PM
Follow On Certification: There is no follow on Certification

Target Audience:

Candidates that need to acquire their CCIE Security certificate. Network engineers/designers that need to raise their knowledge to an expert-level.

Prerequisites:

There are no formal prerequisites for Cisco CCIE certification. Candidates must first pass a written qualification exam and then pass the corresponding hands-on lab exam. Candidates are expected to have an in-depth understanding of the exam topics and are strongly encouraged to have three to five years of job experience before attempting certification.

Testing and Certification

Recommended preparation for exam(s):

- CCIE Security Lab Exam v.4

Content:

System Hardening and Availability

- Routing plane security features (e.g. protocol authentication, route filtering)
- Control Plane Policing
- Control Plane Protection and Management Plane Protection
- Broadcast control and switchport security
- Additional CPU protection mechanisms (e.g. options drop, logging interval)
- Disable unnecessary services
- Control device access (e.g. Telnet, HTTP, SSH, Privilege levels)
- Device services (e.g. SNMP, Syslog, NTP)
- Transit Traffic Control and Congestion Management

Threat Identification and Mitigation

- Identify and protect against fragmentation attacks
- Identify and protect against malicious IP option usage
- Identify and protect against network reconnaissance attacks
- Identify and protect against IP spoofing attacks
- Identify and protect against MAC spoofing attacks
- Identify and protect against ARP spoofing attacks
- Identify and protect against Denial of Service (DoS) attacks
- Identify and protect against Distributed Denial of Service (DDoS) attacks
- Identify and protect against Man-in-the-Middle (MiM) attacks
- Identify and protect against port redirection attacks
- Identify and protect against DHCP attacks
- Identify and protect against DNS attacks
- Identify and protect against MAC Flooding attacks
- Identify and protect against VLAN hopping attacks
- Identify and protect against various Layer2 and Layer3 attacks
- NBAR
- NetFlow
- Capture and utilize packet captures

Intrusion Prevention and Content Security

IPS 4200 Series Sensor Appliance

- Initialize the Sensor Appliance
- Sensor Appliance management
- Virtual Sensors on the Sensor Appliance
- Implementing security policies
- Promiscuous and inline monitoring on the Sensor Appliance
- Tune signatures on the Sensor Appliance
- Custom signatures on the Sensor Appliance

Identity Management

Identity Based Authentication/Authorization/Accounting

- Cisco Router/Appliance AAA
- RADIUS
- TACACS+

Device Admin (Cisco IOS Routers, ASA, ACS5.x)

Network Access (TrustSec Model)

- Authorization Results for Network Access (ISE)
- 802.1X (ISE)
- VSAs (ASA / Cisco IOS / ISE)
- Proxy-Authentication (ISE/ASA/Cisco IOS)

Cisco Identity Services Engine (ISE)

- Profiling Configuration (Probes)
- Guest Services
- Posture Assessment
- Client Provisioning (CPP)
- Configuring AD Integration/Identity Sources

Perimeter Security and Services

Cisco ASA Firewall

- Basic firewall Initialization
- Device management
- Address translation (nat, global, static)
- Access Control Lists
- IP routing/Route Tracking
- Object groups
- VLANs
- Configuring Etherchannel
- High Availability and Redundancy
- Layer 2 Transparent Firewall
- Security contexts (virtual firewall)
- Modular Policy Framework
- Identity Firewall Services
- Configuring ASA with ASDM
- Context-aware services
- IPS capabilities
- QoS capabilities

Cisco IOS Zone Based Firewall

- Network, Secure Group and User Based Policy
- Performance Tuning
- Network, Protocol and Application Inspection

Perimeter Security Services

- Cisco IOS QoS and Packet marking techniques
- Traffic Filtering using Access-Lists
- Cisco IOS NAT
- uRPF
- PAM – Port to Application Mapping
- Policy Routing and Route Maps

Confidentiality and Secure Access

- IKE (V1/V2)
- IPsec LAN-to-LAN (Cisco IOS/ASA)
- Dynamic Multipoint VPN (DMVPN)
- FlexVPN
- Group Encrypted Transport (GET) VPN
- Remote Access VPN
- Easy VPN Server (Cisco IOS/ASA)
- VPN Client 5.X
- Clientless WebVPN
- AnyConnect VPN
- EasyVPN Remote
- SSL VPN Gateway
- VPN High Availability
- QoS for VPN
- VRF-aware VPN
- MacSec
- Digital Certificates (Enrollment and Policy Matching)
- Wireless Access
- EAP methods
- WPA/WPA-2

WIPS

- Actions on the Sensor Appliance
- Signature engines on the Sensor Appliance
- Use IDM/IME to the Sensor Appliance
- Event action overrides/filters on the Sensor Appliance
- Event monitoring on the Sensor Appliance

VACL/SPAN ; RSPAN on Cisco switches

WSA

- Implementing WCCP
- Active Dir Integration
- Custom Categories
- HTTPS Config
- Services Configuration (Web Reputation)
- Configuring Proxy By-pass Lists
- Web proxy modes
- App visibility and control

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.co.uk

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK