CCIE Security - Lab Preparation

Duration: 5 Days **Course Code: CCIESEC** **Version: 4.0**

Overview:

This intense course is designed to prepare CCIE candidates for the one-day Security "hands-on" lab exam. Over six days candidates will solidify their existing knowledge, expose their weaknesses and gain vital test taking strategies. Each candidate will work through challenging scenarios on their own vRack of equipment. Each student will be given dedicated access to their individual vRack throughout the course.

Target Audience:

This class is designed for candidates who are within 6 months of their lab date. The class does not cover introductory material and candidates are expected to have at a minimum a CCSP level knowledge of the topics covered in order to receive the full benefit of the class.

Objectives:

- After completing this course delegates should be able to:
- This course consists of sereval hours od lecture per day and up to 10 hours of more of hands-on preparation per day. Be prepared to stay late every evening. During the course the instructor will identify some of the most commen mistakes that candidates make and at the end of the week, will provide each individual an assessment of their readiness.

Prerequisites:

The skills and knowledge required for delegates to sit this course are as follows;

- At least 2 years hands-on experience with Cisco Security and SAFE Blueprint architecture.
- Students should have passed the CCIE Security Written exam and may already hold some of the security certifications such as CCSP, etc.

Testing and Certification

This course will prepare delegates for the following exams;
Cisco CCIE Security Lab Exam Blueprint v2.0

Content:

ASA/PIX Firewall

- Initial Configuration of PIX/ASA
- Routing
- Translations and Connections
- Access Control Lists and Object Groups
- Deep Packet Inspection
- Control URL's and FTP commands using MPF
- Running BGP thru the Firewall
- TCP Normalization
- Transparent Firewall
- ARP inspection on Firewall
- Virtual Firewalls (Security Contexts)
- Active/Standby Failover
- Statefull Failover
- Active/Active Failover

IPSEC/VPN

- LAN-to-LAN IPSec using NAT-T
- IPSec Hairpinning
- EZVPN in Client and Network Extension Mode
- QoS with IPSec
- DMVPN thru the Firewall
- Basic Configuration of VPN Concentrator
- Routing on the Concentrator
- Administration and Filtering on the Concentrator
- LAN-to-LAN Tunnel on the Concentrator
- EZVPN on the Concentrator in Client Mode
- EZVPN on the Concentrator in Network Extension Mode without XAUTH
- Remote Access on the Concentrator with RRI and Split Tunnelling

IPS Sensor

- IPS in Promiscuous Mode
- SPAN/RSPAN
- Blocking Using ASA
- IPS in Inline Mode – Interface Pair and Inline VLAN Pair
- Signature Tuning
- Custom Stream Signatures
- Custom HTTP Signatures
- Custom Packet Signatures

Access Management

- Configuring ACS for Network Devices
- Configuring Users and Groups on ACS Server
- Configuring Routers, Switches and ASA/PIX for Management Authentication using ACS Server
- Configuring Command Authorization based on the ACS server
- Configuring Accounting based on the ACS Server
- Configuring Authentication Proxy on the ASA
- Configuring Authentication on the Concentrator from the ACS Server
- Configuring NAC-802.1X Authentication on the Switch

Advanced Network Security and Network Attacks

- Preventing IP Spoofing
- Configuring NAT on Routers
- Configuring IP TCP Intercept
- Blocking ICMP Attacks
- Port Security on the Switches
- DHCP Snooping
- Dynamic ARP Inspection(DAI)
- IP Source Guard
- Mitigating Attacks using CAR
- Mitigating Attacks using NBAR
- IOS Firewall

Blocking attacks using PBR

Additional Information:

Recommended Knowledge prior to Training
Recommended Courses, Reading or Hands-on Experience on the Following Topics: Cisco Secure Virtual Private Networks (CSVPN) Implementing Cisco Intrusion Prevention System v5.0 (IPS) Securing Cisco Network Devices (SND) Securing Networks with PIX and ASA (SNPA) Securing Networks with Cisco Routers and Switches (SNRS)
Students are required to have the solid basic understanding of Security Devices, PIX/ASA, VPN Concentrator, IOS FW, Catalyst 3550
Protocols: OSPF, RIP, EIGRP, BGP, IPSec, GRE, ACL's, CBAC, NAT
Basic understanding of ACS Server, IPS
All of the IOS Router basic features and Solid troubleshooting skills

Further Information:

For More information, or to book your course, please call us on 353-1-814 8200

info@globalknowledge.ie

www.globalknowledge.ie

Global Knowledge, 3rd Floor Jervis House, Millennium Walkway, Dublin 1