SOFTCRAYONS
Tech Solutions Pvt. Ltd.

CCNA SECURITY+

@softcrayons

About Course

As a vendor-neutral credential, Security+ provides a broad base of knowledge suitable to multiple environments. The CCNA Security is also an early-level credential but is geared to Cisco systems and is therefore best suited to Cisco security professionals.

CCNA SECURITY+

CURRICULUM

1 Common Security Principles

- Describe confidentiality, integrity, availability (CIA)
- Describe SIEM technology
- Identify common security terms
- Identify common network security zones

2 Common Security Threats

- Identify common network attacks
- Describe social engineering
- Identify malware
- Classify the vectors of data loss/exfiltration

3 Cryptography Concepts

- Describe key exchange
- Describe hash algorithm
- Compare and contrast symmetric and asymmetric encryption
- Describe digital signatures, certificates, and PKI

SOFTCRAYONS
Tech Solutions Pvt. Ltd.

5 Describe Network Topologies

- Campus area network (CAN)
- Cloud, wide area network (WAN)
- Data center
- Small office/home office (SOHO)
- Network security for a virtual environment

6 Secure Management

- Compare in-band and out-of band
- Configure secure network management
- Configure and verify secure access through SNMP v3 using an ACL
- Configure and verify security for NTP
- Use SCP for file transfer

7 AAA Concepts

- Describe RADIUS and TACACS+ technologies
- Configure administrative access on a Cisco router using TACACS+
- Verify connectivity on a Cisco router to a TACACS+ server
- Explain the integration of Active Directory with AAA
- Describe authentication and authorisation using ACS and ISE

8 802.1X Authentication

Identify the functions 802.1X components

9 BYOD

Describe the BYOD architecture framework
Describe the function of mobile device management (MDM)

10 VPN Concepts

Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
Describe hairpinning, split tunneling, always-on, NAT traversal

11 Remote Access VPN

Implement basic clientless SSL VPN using ASDM
Verify clientless connection
Implement basic AnyConnect SSL VPN using ASDM
Verify AnyConnect connection
Identify endpoint posture assessment

12 Site-To-Site VPN

Implement an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls

Verify an IPsec site-to-site VPN

13 **4.1 Security On Cisco Routers**

Configure multiple privilege levels
Configure Cisco IOS role-based CLI access
Implement Cisco IOS resilient configuration

14 **Securing Routing Protocols**

Implement routing update authentication on OSPF

15 **Securing The Control Plane**

Explain the function of control plane policing

16 **Common Layer 2 Attacks**

Describe STP attacks
Describe ARP spoofing
Describe MAC spoofing
Describe CAM table (MAC address table) overflows
Describe CDP/LLDP reconnaissance
Describe VLAN hopping
Describe DHCP spoofing

17 **Mitigation Procedures**

Implement DHCP snooping

SOFTCRAYONS
Tech Solutions Pvt. Ltd.

- Implement Dynamic ARP Inspection
- Implement port security
- Describe BPDU guard, root guard, loop guard
- Verify mitigation procedures

18 VLAN Security

- Describe the security implications of a PVLAN
- Describe the security implications of a native VLAN

19 Cisco Firewall Technologies

- Proxy firewalls
- Application firewall
- Personal firewall

20 Compare Stateful Vs. Stateless Firewalls

- Operations
- Function of the state table

21 Compare Stateful Vs. Stateless Firewalls

- Operations
- Function of the state table

22 Implement NAT On Cisco ASA 9.X

- Static

- Dynamic
- PAT
- Policy NAT
- Verify NAT operations

23 Implement Zone-Based Firewall

- Zone to zone
- Self zone

24 Firewall Features On The Cisco Adaptive Security Appliance (ASA) 9.X

- Configure ASA access management
- Configure security access policies
- Configure Cisco ASA interface security levels
- Configure default Cisco Modular Policy Framework (MPF)
- Describe modes of deployment (routed firewall, transparent firewall)
- Describe methods of implementing high availability
- Describe security contexts
- Describe firewall services

25 Describe IPS Deployment Considerations

- Network-based IPS vs. host-based IPS
- Modes of deployment (inline, promiscuous - SPAN, tap)

- Placement (positioning of the IPS within the network)
- False positives, false negatives, true positives, true negatives

26 Describe IPS Technologies

- Rules/signatures
- Detection/signature engines
- Trigger actions/responses (drop, reset, block, alert, monitor/log, shun)
- Blacklist (static and dynamic)

27 Content And Endpoint Security

- Describe mitigation technology for email-based threats
- SPAM filtering, anti-malware filtering, DLP, blacklisting, email encryption

28 Describe Mitigation Technology For Web-Based Threats

- Local and cloud-based web proxies
- Blacklisting, URL filtering, malware scanning, URL categorisation, web application filtering, TLS/SSL decryption

29 Describe Mitigation Technology For Endpoint Threats

Anti-virus/anti-malware
Personal firewall/HIPS
Hardware/software encryption of local data

SOFTCRAYONS
Tech Solutions Pvt. Ltd.
www.softcrayons.com
info@softcrayons.com
(+91) 854 501 2345
693, Sector 14-A, Vasundhara,
Ghaziabad (U.P.), 201012
@softcrayons