CCNA Security (Implementing Cisco Network Security)

CCNA Security (Implementing Cisco Network Security)	Exam : 210-260

Security Concepts

Common security principles

.a Describe confidentiality, integrity, availability (CIA)

.b Describe SIEM technology

.c Identify common security terms

.d Identify common network security zones

Common security threats

.a Identify common network attacks

.b Describe social engineering

.c Identify malware

.d Classify the vectors of data loss/exfiltration

Cryptography concepts

.a Describe key exchange

.b Describe hash algorithm

.c Compare and contrast symmetric and asymmetric encryption

.d Describe digital signatures, certificates, and PKI

Describe network topologies

.a Campus area network (CAN)

.b Cloud, wide area network (WAN)

.c Data center

.d Small office/home office (SOHO)

.e Network security for a virtual environment

Secure Access

Secure management

.a Compare in-band and out-of band

.b Configure secure network management

.c Configure and verify secure access through SNMP v

using an ACL

.d Configure and verify security for NTP

.e Use SCP for file transfer

AAA concepts

.a Describe RADIUS and TACACS+ technologies

.b Configure administrative access on a Cisco router using TACACS+

.c Verify connectivity on a Cisco router to a TACACS+ server

.d Explain the integration of Active Directory with AAA

.e Describe authentication and authorization using ACS and ISE

X authentication

.a Identify the functions

X components

BYOD

.a Describe the BYOD architecture framework

.b Describe the function of mobile device management (MDM)

VPN

VPN concepts

.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)

.b Describe hairpinning, split tunneling, always-on, NAT traversal

Remote access VPN

.a Implement basic clientless SSL VPN using ASDM

.b Verify clientless connection

.c Implement basic AnyConnect SSL VPN using ASDM

.d Verify AnyConnect connection

.e Identify endpoint posture assessment

Site-to-site VPN

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

.b Verify an IPsec site-to-site VPN

Secure Routing and Switching

Security on Cisco routers

.a Configure multiple privilege levels

.b Configure Cisco IOS role-based CLI access

.c Implement Cisco IOS resilient configuration

Securing routing protocols

.a Implement routing update authentication on OSPF

Securing the control plane

.a Explain the function of control plane policing

Common Layer attacks

.a Describe STP attacks

.b Describe ARP spoofing

.c Describe MAC spoofing

.d Describe CAM table (MAC address table) overflows

.e Describe CDP/LLDP reconnaissance

.f Describe VLAN hopping

.g Describe DHCP spoofing

Mitigation procedures

.a Implement DHCP snooping

.b Implement Dynamic ARP Inspection

.c Implement port security

.d Describe BPDU guard, root guard, loop guard

.e Verify mitigation procedures

VLAN security

.a Describe the security implications of a PVLAN

.b Describe the security implications of a native VLAN

Cisco Firewall Technologies

Describe operational strengths and weaknesses of the different firewall technologies

.a Proxy firewalls

.b Application firewall

.c Personal firewall

Compare stateful vs. stateless firewalls

.a Operations

.b Function of the state table

Implement NAT on Cisco ASA

.x

.a Static

.b Dynamic

.c PAT

.d Policy NAT

e Verify NAT operations

Implement zone-based firewall

.a Zone to zone

.b Self zone

Firewall features on the Cisco Adaptive Security Appliance (ASA)

.x

.a Configure ASA access management

.b Configure security access policies

.c Configure Cisco ASA interface security levels

.d Configure default Cisco Modular Policy Framework (MPF)

.e Describe modes of deployment (routed firewall, transparent firewall)

.f Describe methods of implementing high availability

.g Describe security contexts

.h Describe firewall services

IPS

Describe IPS deployment considerations

.a Network-based IPS vs. host-based IPS

.b Modes of deployment (inline, promiscuous - SPAN, tap)

.c Placement (positioning of the IPS within the network)

.d False positives, false negatives, true positives, true negatives

Describe IPS technologies

.a Rules/signatures

.b Detection/signature engines

.c Trigger actions/responses (drop, reset, block, alert, monitor/log, shun)

.d Blacklist (static and dynamic)

Content and Endpoint Security

.b Personal firewall/HIPS

.c Hardware/software encryption of local data

Describe mitigation technology for email-based threats

.a SPAM filtering, anti-malware filtering, DLP, blacklisting, email encryption

Describe mitigation technology for web-based threats

.a Local and cloud-based web proxies

.b Blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, TLS/SSL decryption

Describe mitigation technology for endpoint threats

.a Anti-virus/anti-malware