CETPA INFOTECH PVT. LTD.

CURRICULUM FOR CCNA SECURITY

IMPLEMENTING CISCO IOS NETWORK SECURITY

1.0 COMMON SECURITY THREATS

1.1 Describe common security threats
1.1.a Common threats to the physical installation
1.1.b Mitigation methods for common network attacks
1.1.c Email-based threats
1.1.d Web-based attacks
1.1.e Mitigation methods for Worm, Virus, and Trojan Horse attacks
1.1.f Phases of a secure network lifecycle
1.1.g Security needs of a typical enterprise with a comprehensive security policy
1.1.h Mobile/remote security
1.1.i DLP

2.0 SECURITY AND CISCO ROUTERS

2.1 Implement security on Cisco routers
- 2.1.a CCP Security Audit feature
- 2.1.b CCP One-Step Lockdown feature
- 2.1.c Secure router access using strong encrypted passwords, and using IOS login enhancements, IPV6 security.
- 2.1.d Multiple privilege levels
- 2.1.e Role-based CLI
- 2.1.f Cisco IOS image and configuration files

2.2 Describe securing the control, data and management plane
2.3 Describe CSM
2.4 Describe IPv4 to IPv6 transition
- 2.4.a Reasons for IPv6
- 2.4.b Understanding IPv6 addressing
- 2.4.c Assigning IPv6 addresses
- 2.4.d Routing considerations for IPv6

3.0 AAA ON CISCO DEVICES

3.1 Implement authentication, authorization, and accounting (AAA)
3.2 Describe TACACS+
3.3 Describe RADIUS
3.4 Describe AAA
- 3.4.a Authentication
- 3.4.b Authorization
- 3.4.c Accounting

3.5 Verify AAA functionality.

4.0 IOS ACLS

4.1 Describe standard, extended, and named IP IOS ACLs to filter packets
- 4.1.a IPv4
- 4.1.b IPv6
- 4.1.c Object groups
- 4.1.d ACL operations
- 4.1.e Types of ACLs (dynamic, reflexive, time-based ACLs)
- 4.1.f ACL wild card masking
- 4.1.g Standard ACLs
- 4.1.h Extended ACLs
- 4.1.i Named ACLs
- 4.1.j VLSM

4.2 Describe considerations when building ACLs
- 4.2.a Sequencing of ACEs
- 4.2.b Modification of ACEs

4.3 Implement IP ACLs to mitigate threats in a network
- 4.3.a Filter IP traffic
- 4.3.b SNMP
- 4.3.c DDoS attacks
- 4.3.d CLI
- 4.3.e CCP
- 4.3.f IP ACLs to prevent IP spoofing
- 4.3.g VACLs

5.0 SECURE NETWORK MANAGEMENT AND Reporting

5.1 Describe secure network management
- 5.1.a In-band
- 5.1.b Out of band
- 5.1.c Management protocols
- 5.1.d Management enclave
- 5.1.e Management plane

5.2 Implement secure network management
- 5.2.a SSH
- 5.2.b syslog
- 5.2.c SNMP
- 5.2.d NTP
- 5.2.e SCP
- 5.2.f CLI
- 5.2.g CCP
- 5.2.h SSL

6.0 COMMON LAYER 2 ATTACKS

6.1 Describe Layer 2 security using Cisco switches
- 6.1.a STP attacks
- 6.1.b ARP spoofing
- 6.1.c MAC spoofing
- 6.1.d CAM overflows
- 6.1.e CDP/LLDP

6.2 Describe VLAN Security
- 6.2.a Voice VLAN
- 6.2.b PVLAN
- 6.2.c VLAN hopping
- 6.2.d Native VLAN

6.3 Implement VLANs and trunking
- 6.3.a VLAN definition
- 6.3.b Grouping functions into VLANs
- 6.3.c Considering traffic source to destination paths
- 6.3.d Trunking
- 6.3.e Native VLAN
- 6.3.f VLAN trunking protocols
- 6.3.g Inter-VLAN routing

6.4 Implement Spanning Tree
- 6.4.a Potential issues with redundant switch topologies
- 6.4.b STP operations
- 6.4.c Resolving issues with STP

7.0 CISCO FIREWALL TECHNOLOGIES

7.1 Describe operational strengths and weaknesses of the different firewall technologies
- 7.1.a Proxy firewalls
- 7.1.b Packet and stateful packet
- 7.1.c Application firewall
- 7.1.d Personal firewall

7.2 Describe stateful firewalls
- 7.2.a Operations
- 7.2.b Function of the state table

7.3 Describe the types of NAT used in firewall technologies
- 7.3.a Static
- 7.3.b Dynamic
- 7.3.c PAT

7.4 Implement Zone Based Firewall using CCP
- 7.4.a Zone to zone
- 7.4.b Self zone

7.5 Implement the Cisco Adaptive Security Appliance (ASA)
- 7.5.a NAT
- 7.5.b ACL
- 7.5.c Default MPF
- 7.5.d Cisco ASA sec level

7.6 Implement NAT and PAT
- 7.6.a Functions of NAT, PAT, and NAT Overload
- 7.6.b Translating inside source addresses
- 7.6.c Overloading Inside global addresses

8.0 CISCO IPS

8.1 Describe IPS deployment considerations
- 8.1.a SPAN
- 8.1.b IPS product portfolio
- 8.1.c Placement
- 8.1.d Caveats

8.2 Describe IPS technologies
- 8.2.a Attack responses
- 8.2.b Monitoring options
- 8.2.c syslog
- 8.2.d SDEE
- 8.2.e Signature engines
- 8.2.f Signatures
- 8.2.g Global correlation and SIO
- 8.2.h Network-based
- 8.2.i Host-based

8.3 Configure Cisco IOS IPS using CCP
- 8.3.a Logging
- 8.3.b Signatures

9.0 VPN TECHNOLOGIES

9.1 Describe the different methods used in cryptography
- 9.1.a Symmetric
- 9.1.b Asymetric
- 9.1.c HMAC
- 9.1.d Message digest
- 9.1.e PKI

9.2 Describe VPN technologies
- 9.2.a IPsec
- 9.2.b SSL

9.3 Describe the building blocks of IPSec
- 9.3.a IKE
- 9.3.b ESP
- 9.3.c AH
- 9.3.d Tunnel mode
- 9.3.e Transport mode

9.4 Implement an IOS IPSec site-to-site VPN with pre-shared key authentication
- 9.4.a CCP
- 9.4.b CLI

9.5 Verify VPN operations.

9.6 Implement SSL VPN using ASA device manager
- 9.6.a Clientless
- 9.6.b Any Connect

HEAD OFFICE: 200 Purwavali, 2nd Floor, (Opp. Railway Ticket Agency), Railway Road, Ganeshpur, Roorkee – 247667 Ph. No.: 09219602769, 01332-270218 Fax - 1332 – 274960.

CORPORATE OFFICE: D-58, Sector-2, Near Red FM. Noida -201301, Uttar Pradesh Contact Us: +91-9212172602 , 0120-4535353

BRANCH OFFICE: 401 A, 4th Floor, Lekhraj Khazana, Faizabad Road, Indira Nagar, Lucknow-226016 (U.P.), Ph. No: +91-522-6590802, +91-9258017974, Fax No: +91-522-6590802

BRANCH OFFICE: 105, Mohit Vihar, Near Kamla Palace, GMS Road, Dehradun-248001, UK Contact: +91-9219602771, 0135-6006070

Toll Free- 1800-8333-999 (from any network)