INFOSOFT IT SOLUTIONS

Training | Projects | Placements

Revathi Apartments, Ameerpet, 1st Floor, Opposite Annapurna Block,

Infosoft It solutions, Software Training & Development Institute, **9059683947|9182540872**

Cisco CCNA Security

Security Concepts

- **Security Threats Facing Modern Network Infrastructures**

    - Describe various types of threats (e.g., social engineering, malware, phishing)

    - Explain threat actors and their motivations

- **Security Principles**

    - Describe confidentiality, integrity, and availability (CIA) concepts

    - Explain the principle of least privilege and how it applies to security policies

- **Security Program Elements**

    - Describe the components of a security program (policies, procedures, awareness)

    - Explain risk management processes and practices

Secure Access

- **Secure Management and Reporting**

  - Configure and verify secure access management protocols (SSH, HTTPS)

  - Describe logging and monitoring capabilities

- **AAA Concepts**

  - Describe AAA concepts (authentication, authorization, and accounting)

  - Configure and verify local AAA (including privilege levels, authentication methods)

- **802.1X Authentication**

  - Configure and verify 802.1X authentication protocols

Virtual Private Networks (VPNs)

- **VPN Concepts**

  - Describe VPN concepts and technologies (IPsec, SSL/TLS, GRE)

  - Describe VPN deployments (site-to-site, remote access VPNs)

- **Implementing VPNs**
  - Configure and verify site-to-site VPNs using CLI
  - Configure and verify remote access VPNs using CLI

Secure Routing and Switching

- **Security on Cisco Routers**
  - Configure and verify router security features (ACLs, NAT, PAT)
  - Implement secure routing protocols (RIP, EIGRP, OSPF)

- **Security on Cisco Switches**
  - Configure and verify switch security features (port security, DHCP snooping, DAI)
  - Implement VLAN security features (PVLANs, trunking)

Cisco Firewall Technologies

- **Firewall Technologies**
  - Describe firewall technologies (stateful, stateless)
  - Describe types of firewall deployment scenarios (edge, campus, data center)

- **Implementing Firewall Technologies**
  - Configure and verify Cisco ASA (Adaptive Security Appliance) and Cisco FTD (Firepower Threat Defense) using CLI

IPS (Intrusion Prevention Systems)

- **IPS Concepts**
  - Describe IPS deployment strategies
  - Explain IPS technologies and features
- **Implementing IPS**
  - Configure and verify Cisco IPS using CLI

Content and Endpoint Security

- **Content Security Concepts**
  - Describe web and email content security features and functions
  - Describe web security controls and policies
- **Implementing Content Security**
  - Configure and verify Cisco WSA (Web Security Appliance) and Cisco ESA (Email Security Appliance)

Secure Network Design

- **Design Principles**

    - Describe network security design considerations (defense in depth, segregation of duties)

    - Explain the concepts of trust boundaries and zoning

- **Implementing Secure Network Design**

    - Implement secure network architecture (DMZ, VPN, VLANs)

Security Management

- **Monitoring and Reporting**

    - Configure and verify network monitoring tools

    - Configure and verify network management protocols (SNMP, syslog)

- **Troubleshooting and Incident Response**

    - Describe common security threats and mitigation techniques

    - Troubleshoot security issues using appropriate tools and resources

Secure Wireless Networks

- **Wireless Security Concepts**

    o Describe wireless security protocols and authentication methods

    o Explain the concepts of SSID, MAC filtering, and encryption methods

- **Implementing Secure Wireless Networks**

    o Configure and verify wireless security settings (WPA, WPA2, WPA3)

Additional Topics

- **Security Policies and Compliance**

    o Describe regulatory compliance requirements (GDPR, HIPAA, PCI DSS)

    o Explain the importance of security policies, standards, guidelines, and procedures

- **Threat Intelligence and Incident Response**

    o Describe threat intelligence sources and types

    o Explain the incident response process and procedures