Network : Administrator

Network	Administrator	5	20 days	- Compare and contrast OSI and TCP/IP models - Compare and contrast TCP and UDP protocols - Describe the impact of infrastructure components in an enterprise network a. Firewalls b. Access points c. Wireless controllers - Communication Types a. Unicast b. Multicast c. Broadcast - Describe and verify switching concepts - Troubleshoot interface and cable issues (collisions, errors, duplex, speed) - VLANs, VTP, VTPv3, Trunk, Access, STP - EthernChannel - STP Security - Subnetting, VLSM - Static Routing, Default Route - Dynamic Routing (OSPF, EIGRP) - NAT, PAT - DNS, DHCP, NTP - TFTP, HSRP, GLBP
				1 . Network Design Methodologies - Cisco Design Lifecycle - SNMP, NetFlow 2. Design a basic campus - Layer 2 Layer 3 demarcation - Spanning Tree - EtherChannel - FHRP 3.Design a basic enterprise network - Layer 3 protocols and redistribution - Topologies (hub and spoke, point to point, Full mesh) 4.Considerations for Expanding and Existing Network - Describe security control integration consideration - Describe data center components
				- Use Cisco IOS troubleshooting tools - Debug, conditional debug - Ping and trace route with extended options - LAN and VLAN - Traffic monitoring, SNMPv3, Syslog and NetFlow - SPAN and RSPAN - Telnet , SSH, HTTPS - IP SLA - Tracking objects - Device Memory Types - Diagnose the root cause of networking issues - Design and implement valid solutions - Verify and monitor resolution
				-Network Security Devices -Network Design Security -Risk Calculation -Forensics -Incident Response

				-Security Awareness -Physical and Environmental Security -Risk Management -Malware -Attack Types -Social Engineering -Application Attacks -Penetration Testing -Host Security -Data Security -Vulnerability Scanning -Authentication Services & Protocols -Authentication Methods -Authorization Models -Cryptography
				- Footprinting - Scanning - Enumeration - System Hacking - Trojans and Backdoors - Sniffers - Denial of Service - Social Engineering - Session Hijacking
				- Threat Management -Topology discovery, OS fingerprinting, Service discovery, and packet capture -Router/Firewall ACLs review, Log review, Phishing, and DNS harvesting -Social media profiling and social engineering -Tools -NMAP, Host Scanning, Network mapping, Syslog, Vulnerability scanner, IDS/IPS, Packet analyzer, and HIDS/NIDS -Honeypot, endpoint security, Group policies -Hardening -Mandatory Access Control, Compensating Controls, Blocking unused ports/services, and Pathing -Network Access Control (NAC), Penetration Testing, Reverse Engineering, and Risk evaluation - Identification of requirements (vulnerability), Establish scanning frequency - Configuring tools to perform scans according to specification - Execute Scanning, and Generate reports - Remediation, and Ongoing scanning and continuous monitoring - Threat classification, Factors contributing to incident severity and prioritization, Forensics kits, and forensitc investigation suite - Common network-related symptoms, commont host-related symptoms, and common application-related symptoms - Contanment techniques, Eradication techniques, validation (patching, permission, scanning, verify logging/communication to security monitoring) -Corrective actions, and Incident summary report Day5 - Security Architecture and Tools Sets - Regulatory compliance, Frameworks, Policies, Controls, Procedures, Verification and quality control - Security issues associated with context-based authentication / identities / identity repositories / federation and single sign-on - Exploits, Security data analytics, Defense in depth
				- Information Security risks - Information Security importance

				- Consequences of security breaches - Physical Security in the workplace - Security-conscious work habits - Physical security outside the workplace - Risks of carrying electronic devices - Communication Security - The risks of email - Personnel Security - Social Engineering
				- Understanding Secure OS - Function, configuration and feature of CA Access Control - How to set policy of file access control - Analysis of violation log and countermeasures - How to set policy of process access control - Analysis of violation log and countermeasures - How to set policy of TCP access control - Analysis of violation log and countermeasures - Fault analysis technique - How to cope with fault