Network Masters
KNOWLEDGE AND TECHNOLOGY TOGETHER

Cyber Security Expert
Duration: 150 Hrs

Network Fundamentals

1.1 Explain the role and function of network components
1.1.a Routers
1.1.b L2 and L3 switches
1.1.c Next-generation firewalls and IPS
1.1.d Access points
1.1.e Controllers (Cisco DNA Center and WLC)
1.1.f Endpoints
1.1.g Servers
1.2 Describe characteristics of network topology architectures
1.2.a 2 tier
1.2.b 3 tier
1.2.c Spine-leaf
1.2.d WAN
1.2.e Small office/home office (SOHO)
1.2.f On-premises and cloud
1.3 Compare physical interface and cabling types
1.3.a Single-mode fiber, multimode fiber, copper
1.3.b Connections (Ethernet shared media and point-to-point)
1.3.c Concepts of PoE
1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
1.5 Compare TCP to UDP
1.6 Configure and verify IPv4 addressing and subnetting
1.7 Describe the need for private IPv4 addressing
1.8 Configure and verify IPv6 addressing and prefix
1.9 Compare IPv6 address types
1.9.a Global unicast
1.9.b Unique local
1.9.c Link local
1.9.d Anycast
1.9.e Multicast
1.9.f Modified EUI 64
1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)
1.11 Describe wireless principles
1.11.a Nonoverlapping Wi-Fi channels
1.11.b SSID
1.11.c RF
1.11.d Encryption
1.12 Explain virtualization fundamentals (virtual machines)

1.13 Describe switching concepts
1.13.a MAC learning and aging
1.13.b Frame switching
1.13.c Frame flooding
1.13.d MAC address table

Network Access
2.1 Configure and verify VLANs (normal range) spanning multiple switches
2.1.a Access ports (data and voice)
2.1.b Default VLAN
2.1.c Connectivity
2.2 Configure and verify interswitch connectivity
2.2.a Trunk ports
2.2.b 802.1Q
2.2.c Native VLAN
2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations
2.5.a Root port, root bridge (primary/secondary), and other port names
2.5.b Port states (forwarding/blocking)
2.5.c PortFast benefits
2.6 Compare Cisco Wireless Architectures and AP modes
2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP, HTTPS, console, and TACACS+/RADIUS)
2.9 Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

IP Connectivity
3.1 Interpret the components of routing table
3.1.a Routing protocol code
3.1.b Prefix
3.1.c Network mask
3.1.d Next hop
3.1.e Administrative distance
3.1.f Metric
3.1.g Gateway of last resort
3.2 Determine how a router makes a forwarding decision by default
3.2.a Longest match
3.2.b Administrative distance
3.2.c Routing protocol metric

3.3 Configure and verify IPv4 and IPv6 static routing
3.3.a Default route
3.3.b Network route
3.3.c Host route
3.3.d Floating static
3.4 Configure and verify single area OSPFv2
3.4.a Neighbor adjacencies
3.4.b Point-to-point
3.4.c Broadcast (DR/BDR selection)
3.4.d Router ID
3.5 Describe the purpose of first hop redundancy protocol

IP Services
4.1 Configure and verify inside source NAT using static and pools
4.2 Configure and verify NTP operating in a client and server mode
4.3 Explain the role of DHCP and DNS within the network
4.4 Explain the function of SNMP in network operations
4.5 Describe the use of syslog features including facilities and levels
4.6 Configure and verify DHCP client and relay
4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping
4.8 Configure network devices for remote access using SSH
4.9 Describe the capabilities and function of TFTP/FTP in the network

Security Fundamentals
5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
5.2 Describe security program elements (user awareness, training, and physical access control)
5.3 Configure device access control using local passwords
5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
5.5 Describe remote access and site-to-site VPNs
5.6 Configure and verify access control lists
5.7 Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
5.8 Differentiate authentication, authorization, and accounting concepts
5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)
5.10 Configure WLAN using WPA2 PSK using the GUI

Automation and Programmability
6.1 Explain how automation impacts network management
6.2 Compare traditional networks with controller-based networking
6.3 Describe controller-based and software defined architectures (overlay, underlay, and

fabric)
6.3.a Separation of control plane and data plane
6.3.b North-bound and south-bound APIs
6.4 Compare traditional campus device management with Cisco DNA Center enabled device management
6.5 Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)
6.6 Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible
6.7 Interpret JSON encoded data

Cyber Security:

Module 1 / Threats, Attacks, and Vulnerabilities
Indicators of Compromise
• Why is Security Important?
• Security Policy
• Threat Actor Types
• The Kill Chain •
Social Engineering
• Phishing
• Malware Types
• Trojans and Spyware
• Open Source Intelligence
• Labs
• VM Orientation
• Malware Types
Critical Security Controls
• Security Control Types
• Defense in Depth
• Frameworks and Compliance
• Vulnerability Scanning and Pen Tests
• Security Assessment Techniques
• Pen Testing Concepts
• Vulnerability Scanning Concepts
• Exploit Frameworks
• Lab
• Using Vulnerability Assessment Tools
Security Posture Assessment Tools
• Topology Discovery
• Service Discovery
• Packet Capture
•Packet Capture Tools

- Remote Access Trojans
- Honeypots and Honeynets
- Labs
- Using Network Scanning Tools 1
- Using Network Scanning Tools 2
- Using Steganography Tools

Incident Response

- Incident Response Procedures
- Preparation Phase
- Identification Phase
- Containment Phase
- Eradication and Recovery Phases

Module 2 / Identity and Access Management

Cryptography

- Uses of Cryptography
- Cryptographic Terminology and Ciphers
- Cryptographic Products
- Hashing Algorithms
- Symmetric Algorithms
- Asymmetric Algorithms
- Diffie-Hellman and Elliptic Curve
- Transport Encryption
- Cryptographic Attacks
- Lab
- Implementing Public Key Infrastructure Public Key Infrastructure
- PKI Standards
- Digital Certificates
- Certificate Authorities
- Types of Certificate
- Implementing PKI
- Storing and Distributing Keys
- Key Status and Revocation
- PKI Trust Models
- PGP / GPG
- Lab
- Deploying Certificates and Implementing Key Recovery

Identification and Authentication

- Access Control Systems
- Identification
- Authentication
- LAN Manager / NTLM
- Kerberos

- PAP, CHAP, and MS-CHAP
- Password Attacks
- Token-based Authentication
- Biometric Authentication
- Common Access Card
- Lab
- Using Password Cracking Tools

Identity and Access Services

- Authorization
- Directory Services
- RADIUS and TACACS+
- Federation and Trusts
- Federated Identity Protocols

Account Management

- Formal Access Control Models
- Account Types
- Windows Active Directory
- Creating and Managing Accounts
- Account Policy Enforcement
- Credential Management Policies
- Account Restrictions
- Accounting and Auditing
- Lab
- Using Account Management Tools

Module 3 / Architecture and Design (1)

Secure Network Design

- Network Zones and Segments
- Subnetting
- Switching Infrastructure
- Switching Attacks and Hardening
- Endpoint Security
- Network Access Control
- Routing Infrastructure
- Network Address Translation
- Software Defined Networking
- Lab
- Implementing a Secure Network Design

Firewalls and Load Balancers

- Basic Firewalls
- Stateful Firewalls
- Implementing a Firewall or Gateway

- Web Application Firewalls
- Proxies and Gateways
- Denial of Service Attacks
- Load Balancers
- Lab
- Implementing a Firewall

IDS and SIEM

- Intrusion Detection Systems
- Configuring IDS
- Log Review and SIEM
- Data Loss Prevention
- Malware and Intrusion Response
- Lab
- Using an Intrusion Detection System

Secure Wireless Access

- Wireless LANs
- WEP and WPA
- Wi-Fi Authentication
- Extensible Authentication Protocol
- Additional Wi-Fi Security Settings
- Wi-Fi Site Security
- Personal Area Networks

Physical Security Controls

- Site Layout and Access
- Gateways and Locks
- Alarm Systems
- Surveillance
- Hardware Security
- Environmental Controls

Module 4 / Architecture and Design (2)

Secure Protocols and Services

- DHCP Security
- DNS Security
- Network Management Protocols
- HTTP and Web Servers
- SSL / TSL and HTTPS
- Web Security Gateways
- Email Services
- S/MIME
- File Transfer
- Voice and Video Services
- VoIP

• Labs
• Implementing Secure Network Addressing Services
• Configuring a Secure Email Service
Secure Remote Access • Remote Access Architecture
• Virtual Private Networks
• IPSec
• Remote Access Servers
• Remote Administration Tools
• Hardening Remote Access Infrastructure
• Lab
• Implementing a Virtual Private Network
Secure Systems Design
• Trusted Computing
• Hardware / Firmware Security
• Peripheral Device Security
• Secure Configurations
• OS Hardening
• Patch Management
• Embedded Systems
• Security for Embedded Systems
Secure Mobile Device Services
• Mobile Device Deployments
• Mobile Connection Methods
• Mobile Access Control Systems
• Enforcement and Monitoring
Secure Virtualization and Cloud Services
• Virtualization Technologies
• Virtualization Security Best Practices
• Cloud Computing
• Cloud Security Best Practices

Module 5 / Risk Management
Forensics
• Forensic Procedures
• Collecting Evidence
• Capturing System Images
• Handling andm Analyzing Evidence
• Lab
• Using Forensic Tools
Disaster Recovery and Resiliency
• Continuity of Operations Plans
• Disaster Recovery Planning
• Resiliency Strategies

• Recovery Sites
• Backup Plans and Policies
• Resiliency and Automation Strategies
Risk Management
• Business Impact Analysis
• Identification of Critical Systems
• Risk Assessment
• Risk Mitigation
Secure Application Development
• Application Vulnerabilities
• Application Exploits
• Web Browser Exploits
• Secure Application Design
• Secure Coding Concepts
• Auditing Applications
• Secure DevOps
• Lab
• Identifying a Man-in-the-Browser Attack
Organizational Security
• Corporate Security Policy
• Personnel Management Policies
• Interoperability Agreements
• Data Roles
• Data Sensitivity Labeling and Handling
• Data Wiping and Disposal
• Privacy and Employee Conduct Policies
• Security Policy Training
- Utilize Attack Frameworks and Indicator Management
- Utilize Threat Modeling and Hunting Methodologies
- Analyzing Security Monitoring Data
- Analyze Network Monitoring Output
- Analyze Appliance Monitoring Output
- Analyze Endpoint Monitoring Output
- Analyze Email Monitoring Output

Ethical Hacking:

1. Introduction to Ethical Hacking
- Information Security Overview
- Hacking Methodologies and Frameworks
- Hacking Concepts
- Ethical Hacking Concepts

- Information Security Controls
- Information Security Laws and Standards

2. Footprinting and Reconnaissance

- Footprinting Concepts
- Footprinting through Search Engines
- Footprinting through Web Services
- Footprinting through Social Networking Sites
- Website Footprinting
- Email Footprinting
- Who is Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting Tools
- Footprinting Countermeasures

3. Scanning Networks

- Network Scanning Concepts
- Scanning Tools
- Host Discovery
- Port and Service Discovery
- OS Discovery (Banner Grabbing/OS Fingerprinting)
- Scanning Beyond IDS and Firewall
- Network Scanning Countermeasures

4. Enumeration

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP and NFS Enumeration
- SMTP and DNS Enumeration
- Other Enumeration Techniques
- Enumeration Countermeasures

5. Vulnerability Analysis

- Vulnerability Assessment Concepts
- Vulnerability Classification and Assessment Types
- Vulnerability Assessment Tools
- Vulnerability Assessment Reports

6. System Hacking

- Gaining Access
- Escalating Privileges
- Maintaining Access
- Clearing Logs

7. Malware Threats

- Malware Concepts
- APT Concepts
- Trojan Concepts
- o Worm Makers
- Fileless Malware Concepts
- Malware Analysis
- Malware Countermeasures
- Anti-Malware Software

8. Sniffing

- Sniffing Concepts
- Sniffing Technique: MAC Attacks
- Sniffing Technique: DHCP Attacks
- Sniffing Technique: ARP Poisoning
- Sniffing Technique: Spoofing Attacks
- Sniffing Technique: DNS Poisoning
- Sniffing Tools

9. Social Engineering

- Social Engineering Concepts
- Social Engineering Techniques
- Insider Threats
- Impersonation on Social Networking Sites
- Identity Theft
- Social Engineering Countermeasures

10. Denial-of-Service

- DoS/DDoS Concepts
- Botnets
- DoS/DDoS Attack Techniques
- DDoS Case Study
- DoS/DDoS Attack Countermeasures

11.Session Hijacking

- Session Hijacking Concepts
- Application-Level Session Hijacking
- Network-Level Session Hijacking
- Session Hijacking Tools
- Session Hijacking Countermeasures

12. Evading IDS, Firewalls, and Honeypots

- IDS, IPS, Firewall, and Honeypot Concepts
- IDS, IPS, Firewall, and Honeypot Solutions
- Evading IDS
- Evading Firewalls
- Evading NAC and Endpoint Security
- IDS/Firewall Evading Tools
- Detecting Honeypots
- IDS/Firewall Evasion Countermeasures

13. Hacking Web Servers

- Web Server Concepts
- Web Server Attacks
- Web Server Attack Methodology
- Web Server Attack Countermeasures

14. Hacking Web Applications

- Web Application Concepts
- Web Application Threats
- Web Application Hacking Methodology
- Web API, Webhooks, and Web Shell
- Web Application Security

15. SQL Injection

- SQL Injection Concepts
- Types of SQL Injection
- SQL Injection Methodology
- SQL Injection Tools
- SQL Injection Countermeasures

16. Hacking Wireless Networks

- Wireless Concepts
- Wireless Encryption
- Wireless Threats

- Wireless Hacking Methodology
- Wireless Hacking Tools
- Bluetooth Hacking
- Wireless Attack Countermeasures
- Wireless Security Tools

17. Hacking Mobile Platforms

- Mobile Platform Attack Vectors
- Hacking Android OS
- Hacking iOS
- Mobile Device Management
- Mobile Security Guidelines and Tools

18. IoT and OT Hacking

- IoT Hacking
- IoT Concepts
- IoT Attacks
- IoT Hacking Methodology
- OT Hacking
- OT Concepts
- OT Attacks
- OT Hacking Methodology

19. Cloud Computing

- Cloud Computing Concepts
- Container Technology
- Manipulating Cloud Trial Service
- Cloud Security

20. Cryptography

- Cryptography Concepts
- Encryption Algorithms
- Cryptography Tools
- Email Encryption
- Disk Encryption
- Cryptanalysis
- Cryptography Attack Countermeasures