Understanding Cisco Cybersecurity Fundamentals - On Demand (SECFND 1.0)

Modality: On Demand

Duration: 40 Hours

CLC: 15 Units

About the course:

To polish your skills and enhance the fundamental knowledge of Cisco technologies and its products, we have created the “Cisco Cybersecurity Fundamentals” course. Students who are part of this e-learning program will be given significant information about Cisco as well as about Cisco products which will help them with Cisco exam preparation.

The Cisco online learning course includes several interesting lab-exercises to keep the student engage and focused in the course.

Course Outline:

Module 1: TCP/IP and Cryptography Concepts

Objective: Describe the concepts and usage of the TCP/IP protocol suite, network infrastructure, TCP/IP attacks, and cryptography.

Lesson 1: Understanding the TCP/IP Protocol Suite

Objective: Describe the TCP/IP protocol suite and its functions.

This lesson includes these topics:

OSI Model
Objective: Describe the OSI model and its function.
TCP/IP Model
Objective: Explain the TCP/IP protocol suite.
Introduction to the Internet Protocol
Objective: Explain Internet Protocol characteristics.
IP Addressing
Objective: Explain IPv4 addressing concepts.
IP Address Classes
Objective: Explain IPv4 address classes.
Reserved IP Addresses
Objective: Describe IPv4 reserved addressing space.
Public and Private IP Addresses
Objective: Describe the difference between public and private IP address space.
IPv6 Addresses

Objective: Describe IPv6 addressing.

Introduction to the Transmission Control Protocol

Objective: Describe TCP protocol characteristics.

TCP Three-Way Handshake

Objective: Explain the TCP three-way handshake process.

Introduction to the User Datagram Protocol

Objective: Describe the UDP protocol and how it differs from TCP.

TCP and UDP Ports

Objective: Explain the use of TCP and UDP ports in network communications. List some of the well-known ports.

Address Resolution Protocol

Objective: Explain how ARP provides the essential service of mapping IP addresses to physical addresses on a network.

Host-to-Host Packet Delivery Using TCP

Objective: Describe the steps required for host-to-host packet delivery using TCP.

Dynamic Host Configuration Protocol

Objective: Describe how the DHCP protocol functions.

Domain Name System

Objective: Decribe basic DNS function and operation.

Internet Control Message Protocol

Objective: Describe the use and role of ICMP.

Packet Capture Using tcpdump

Objective: This topic analyzes packet captures using tools such as tcpdump.

Wireshark

Objective: Describe how Wireshark is used to capture packets live and to open PCAP files.

Lesson 2: Understanding the Network Infrastructure

Objective: Describe network devices and the protocols running inside the network infrastructure and investigate the logs that network devices generate.

This lesson includes these topics:

Analyzing DHCP Operations

Objective: Describe attacks that target the Dynamic Host Configuration Protocol and how to monitor DHCP exchanges.

IP Subnetting

Objective: Describe how to scale IP networks with IP subnetting.

Hubs, Bridges, and Layer 2 Switches

Objective: Describe hub, bridge, and layer 2 switch operation and concepts.

VLANs and Trunks

Objective: Describe the function of VLANs and trunks at layer 2.

Spanning Tree Protocols

Objective: Describe layer 2 spanning-tree protocol.

Standalone (Autonomous) and Lightweight Access Points

Objective: Describe Standalone (Autonomous) and Lightweight Access Points, and their security vulnerabilities.

Routers

Objective: Describe the use of routers and the routing process used in network communications.

Routing Protocols

Objective: Describe routing protocols and attacks that can be used against them.

Multilayer Switches

Objective: Describe how multilayer switches operate and how frame and packet forwarding take place on the switch.

NAT Fundamentals

Objective: Describe Network Address Translation (NAT) fundamental concepts.

Packet Filtering with ACLs

Objective: Describe the purpose of Access List Control lists.

ACLs with the Established Option

Objective: Describe ACL operation when using the established option.

Lesson 3: Understanding Common TCP/IP Attacks

Objective: Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts.

This lesson includes these topics:

Legacy TCP/IP Vulnerabilities

Objective: Describe legacy TCP/IP vulnerabilities.

IP Vulnerabilities

Objective: Describe vulnerabilities related to the IP protocol.

ICMP Vulnerabilities

Objective: Describe vulnerabilities related to the ICMP protocol.

TCP Vulnerabilities

Objective: Describe vulnerabilities related to the TCP protocol.

UDP Vulnerabilities

Objective: Describe vulnerabilities related to the UDP protocol.

Attack Surface and Attack Vectors

Objective: Describe the attack surface and its relation to an organizations vulnerability.

Reconnaissance Attacks

Objective: Describe how network data is collected through a reconnaissance attack.

Access Attacks

Objective: Describe how an access attack is used to gain unauthorized access.

Man-in-the-Middle (MITM) Attacks

Objective: Describe MITM attacks.

Denial of Service and Distributed Denial of Service

Objective: Describe how DoS and DDoS attacks are used against networks.

Reflection and Amplification Attacks

Objective: Describe how a reflection attack is used against IP hosts.

Spoofing Attacks

Objective: Describe the concepts and uses of spoofing attacks.

DHCP Attacks

Objective: Describe the concepts and use of DHCP attacks.

Lesson 4: Understanding Basic Cryptography Concepts

Objective: Describe the basic concepts and uses of cryptography.

This lesson includes these topics:

Impact of Cryptography on Security Investigations
Objective: Describe the impact of cryptography on security investigations.
Cryptography Overview
Objective: Describe cryptography concepts.
Hash Algorithms
Objective: Describe hashing mechanisms and algorithms.
Encryption Overview
Objective: Describe encryption usage and features.
Cryptanalysis
Objective: Describe the use of cryptanalysis to break codes to decipher encrypted data.
Symmetric Encryption Algorithms
Objective: Describe the use of symmetric encryption algorithms.
Asymmetric Encryption Algorithms
Objective: Describe the use of asymmetric cryptographic algorithms.
Diffie-Hellman Key Agreement
Objective: Describe the Diffie-Hellman key agreement and Diffie-Hellman groups.
Use Case: SSH
Objective: Describe uses of the SSH protocol.
Digital Signatures
Objective: Describe the basic security services offered with the use of digital signatures.
PKI Overview
Objective: Describe PKI components and use.
PKI Operations
Objective: Describe PKI operations.
Use Case: SSL/TLS
Objective: Describe a use case for SSL/TLS.
Cipher Suite
Objective: Describe cipher suite concepts.
Key Management
Objective: Describe key management for the secure generation, verification, exchange, storage, and destruction of keys.
NSA Suite B
Objective: Describe NSA Suite B cryptographic algorithms.

Module 2: Network Applications and Endpoint Security

Lesson 1: Describing Information Security Concepts

Objective: Describe information security concepts and strategies within the network.

This lesson includes these topics:

Information Security Confidentiality, Integrity, and Availability
Objective: Describe the Information Security CIA triad.

Personally Identifiable Information
Objective: Describe PII as it relates to information security.
Risk
Objective: Describe risk as a function of the likelihood of a given threat source's exercising a particular potential vulnerability.
Vulnerability Assessment
Objective: Describe vulnerability assessment in the context of information security.
CVSS v3.0
Objective: Describe the CVSS.
Access Control Models
Objective: Describe basic models for implementing access controls over network resources.
Regulatory Compliance
Objective: Describe compliance regulations and their effects on an organization.
Information Security Management
Objective: Describe frameworks for information security management.
Security Operations Center
Objective: Describe the SOC components of people, processes, and technologies, and the reason for the SOC.
Challenge

Lesson 2: Understanding Network Applications

Objective: This lesson describes the use of network applications and how the security analyst can use this knowledge to detect malicious behavior.

This lesson includes these topics:

DNS Operations
Objective: Explain DNS terminology and operations.
Recursive DNS Query
Objective: Describe the process of recursive DNS queries.
Dynamic DNS
Objective: Describe the automated discovery and registration process of the client public IP addresses via DDNS.
HTTP Operations
Objective: Describe HTTP operations and traffic analysis to identify anomalies in the HTTP traffic.
HTTPS Operations
Objective: Describe the use of and operation of HTTPS traffic.
Web Scripting
Objective: Describe how web scripting can be used to deliver malware.
SQL Operations
Objective: Describe how SQL is used to query, operate, and administer relational database management systems as well as how to recognize SQL based attacks.
SMTP Operations
Objective: Describe how the mail delivery process works, and SMTP conversations.

Lesson 3: Understanding Common Network Application Attacks

Objective: This lesson discusses several network application-based attacks. The security analyst needs to be aware of and able to detect these types of attacks.

This lesson includes these topics:

Password Attacks
Objective: Describe password attacks such as brute force and dictionary attacks.
Pass-the-Hash Attacks
Objective: Describe pass-the-hash attacks.
DNS-Based Attacks
Objective: Describe DNS-based attacks.
DNS Tunneling
Objective: Describe DNS tunneling and its use to exfiltrate data out of their networks.
Web-Based Attacks
Objective: Describe web-based attacks and their risk to businesses.
Malicious iFrames
Objective: Describe malicious scripts that are hidden inside inline frames.
HTTP 302 Cushioning
Objective: Describe web site redirection with HTTP 302 cushioning.
Domain Shadowing
Objective: Describe the domain shadowing process used to hijack users' domain registration logins to create subdomains.
Command Injections
Objective: Describe command injection used to execute arbitrary commands on vulnerable web applications.
SQL Injections
Objective: Describe how SQL injections are used against databases.
Cross-Site Scripting and Request Forgery
Objective: Describe how cross-site scripting and request forgery are used to threaten the security of web applications.
Email-Based Attacks
Objective: Describe how email-based attacks are used against enterprises.

Lesson 4: Understanding Windows Operating System Basics

Objective: This lesson focuses on the Windows operating system feature and functionality.

This lesson includes these topics:

Windows Operating System History
Objective: Describe the history on the Windows operating systems and vulnerabilities.
Windows Operating System Architecture
Objective: Describe the Windows OS architecture and components.
Windows Processes, Threads, and Handles
Objective: Describe Windows processes, threads, and handles.
Windows Virtual Memory Address Space
Objective: Describe virtual memory allocation in the Windows OS.
Windows Services

Objective: Describe Windows services and how they are used.

Windows File System Overview

Objective: Describe the functionality of Windows NTFS.

Windows File System Structure

Objective: Describe the Windows NTFS structure.

Windows Domains and Local User Accounts

Objective: Describe Windows domains and local user accounts.

Windows Graphical User Interface

Objective: Describe the Windows graphical user interface and its use.

Run as Administrator

Objective: Describe how to perform tasks in Windows which may require administrator privileges.

Windows Command Line Interface

Windows PowerShell

Objective: Describe the features of the Windows PowerShell.

Windows net Command

Objective: Describe how the net command is used for Windows administration and maintenance.

Controlling Startup Services and Executing System Shutdown

Objective: Describe how to control Windows startup services, and execute a system shutdown.

Controlling Services and Processes

Objective: Describe how to control Windows services and processes that are operating on a host.

Monitoring System Resources

Objective: Describe how to monitor Windows system resources with the use of Windows Task Manager.

Windows Boot Process

Objective: Describe the Windows boot process, starting services, and registry entries.

Windows Networking

Objective: Describe how to configure Windows networking properties.

Windows netstat Command

Objective: Describe how to use the netstat command to view running networking functions.

Accessing Network Resources with Windows

Objective: Describe how access Windows network resources and perform remote functions.

Windows Registry

Objective: Describe the use of the Windows registry.

Windows Event Logs

Objective: Describe how the Windows Event Viewer is used to browse and manage event logs.

Windows Management Instrumentation

Objective: Describe how the Windows Management Instrumentation is used for management of data and operations on Windows-based operating systems.

Common Windows Server Functions

Objective: Describe common Windows server functions and features.

Common Third-Party Tools

Objective: Describe commonly used third-party tools to manage to manage Windows operating systems.

Lesson 5: Understanding Linux Operating System Basics

Objective: Provide an overview of the Linux Operating System.

This lesson includes these topics:

History and Benefits of Linux

Objective: Provide brief history and benefits of Linux operating system

Linux Architecture

Objective: Describe Linux architecture.

Linux File System Overview

Objective: Provide an overview of the Linux file system.

Basic File System Navigation and Management Commands

Objective: Describe basic file system navigation and management commands in Linux.

File Properties and Permissions

Objective: Describe Linux file properties and permissions.

Editing File Properties

Objective: Describe Linux commands that you can use to manage file permissions and ownership.

Root and Sudo

Objective: Describe Root and Sudo commands in Linux.

Disks and File Systems

Objective: Describe Linux storage disks and file systems.

System Initialization

Objective: Describe the Linux boot process.

Emergency/Alternate Startup Options

Objective: Describe alternate startup options in case Linux is experiencing problems or has been compromised.

Shutting Down the System

Objective: Describe properly procedure to shut down a Linux-based system when you need to bring the system down for maintenance or troubleshooting.

System Processes

Objective: Describe Linux system processes.

Interacting with Linux

Objective: Describe mechanisms for interacting with the Linux operating system.

Linux Command Shell Concepts

Objective: Explore important concepts about the Linux shell and its usage.

Piping Command Output

Objective: Explore Linus Piping command output.

Other Useful Command Line Tools

Objective: Describe other useful Linux command line tools.

Overview of Secure Shell Protocol

Objective: Provide an overview of Secure Shell Protocol.

Networking

Objective: Describe Linux f tools and features for managing virtually every aspect of networking and connectivity configuration.

Managing Services in SysV Environments

Objective: Describe the process of managing services in SysV environments.

Viewing Running Network Services

Objective: Describe tools to track the services running in your Linux installation.

Name Resolution: DNS

Objective: Provide an overview of the Domain Name System.

Testing Name Resolution

Objective: Explore the Linux operating system tools to test name resolution.

Viewing Network Traffic

Objective: Explore Linux tools to viewing network traffic.

System Logs

Objective: Explore logging functionality in context to Linux systems.

Configuring Remote syslog

Objective: Configure remote syslog in context to Linux systems.

Running Software on Linux

Objective: Describe requirements to run software in a Linux installation.

Executables vs. Interpreters

Objective: Explore Linux executable files and interpreters that can execute code.

Using Package Managers to Install Software in Linux

Objective: Describe package managers to install software in Linux.

System Applications

Objective: Describe system applications used to serve clients in context to Linux.

Lightweight Directory Access Protocol

Objective: Provide an overview of the Lightweight Directory Access Protocol.

Lesson 6: Understanding Common Endpoint Attacks

Objective: Describe various attack techniques against the endpoints.

This lesson includes these topics:

Classify Attacks, Exploits, and Vulnerabilities

Objective: Classify attacks, exploits, and vulnerabilities in context to endpoint attacks.

Buffer Overflow

Objective: Describe buffer overflow vulnerability.

Malware

Objective: Describe malware in context to endpoint attacks.

Reconnaissance

Objective: Describe reconnaissance in context to endpoint attacks.

Gaining Access and Control

Objective: Describe gaining access and control in context to endpoint attacks.

Gaining Access via Social Engineering

Objective: Describe how social engineering is used to gain access to endpoints.

Social Engineering Example: Phishing

Objective: Describe phishing as an example of social engineering.

Gaining Access Via Web-Based Attacks

Objective: Describe how attacker can gain access via web-based attacks.

Exploit Kits

Objective: Describe how attackers can use exploit kit to discover and exploit vulnerabilities in an endpoint.

Rootkits

Objective: Describe rootkit as an attacker tool.

Privilege Escalation

Objective: Describe mechanisms that attackers can use to escalate privileges.

Pivoting

Objective: Describe how attackers use pivoting technique to expand their access in a network.

Post-Exploitation Tools Example

Objective: Provide example of tools used in the post-exploitation phase of an attack.

Exploit Kit Example: Angler

Objective: Describe Angler exploit kit chain of events.

Lesson 7: Understanding Network Security Technologies

Objective: Describe how various network security technologies work together to guard against attacks.

This lesson includes these topics:

Defense-in-Depth Strategy

Objective: Describe the traditional Defense-in-Depth approach to provide a layered security by using multiple security mechanisms.

Defend Across the Attack Continuum

Objective: Describe the security model that works across the attack continuum.

Authentication, Authorization, and Accounting

Objective: Describe AAA.

Identity and Access Management

Objective: Describe Identity and Access Management solutions.

Stateful Firewall

Objective: Describe stateful firewalls.

Network Taps

Objective: This topic describes network taps.

Switched Port Analyzer

Objective: This topic describes switched port analyzer.

Remote Switched Port Analyzer

Objective: This topic describes remote switched port analyzer.

Intrusion Prevention System

Objective: Describe Intrusion Prevention Systems.

IPS Evasion Techniques

Objective: Describe Intrusion Prevention Systems Evasion Techniques.

Snort Rules

Objective: Describe Intrusion Prevention Systems.

VPNs

Objective: Describe VPNs.

Email Content Security

Objective: Describe email content security.

Web Content Security

Objective: Describe web content security.

DNS Security

Objective: Describe DNS security.

Network-Based Malware Protection

Objective: Describe network-based malware protection.

Next Generation Firewall

Objective: Describe Next Generation Firewall.

Security Intelligence
Objective: Describe the use of security intelligence feed.
Threat Analytic Systems
Objective: Describe threat analytics systems
Network Security Device Form Factors
Objective: Describe the three network security device form factors: physical, virtual, and cloud.
Security Onion Overview
Objective: Describe the Security Onion open source security monitoring tool.
Security Tools Reference
Objective: Describe online security research tools.

Lesson 8: Understanding Endpoint Security Technologies

Objective: Provides basic understanding of endpoint security and be familiar with common endpoint security technologies.

This lesson includes these topics:

Host-Based Personal Firewall
Objective: Describe host-based personal firewall.
Host-Based Anti-Virus
Objective: Describe host-based anti-virus.
Host-Based Intrusion Prevention System
Objective: Describe host-based Intrusion Prevention System.
Application Whitelists and Blacklists
Objective: Describe application whitelists and blacklists.
Host-Based Malware Protection
Objective: Describe host-based malware protection.
Sandboxing
Objective: Describe sandboxing in context to network security.
File Integrity Checking
Objective: Describe how security analysts use file integrity checking tools.

Module 3: Security Monitoring and Analysis

Objective: This module discusses network security monitoring, data collection, and data analysis.

Lesson 1: Describing Security Data Collection

Objective: This lesson discusses security monitoring and analysis of logs and data collected from multiple sources.

This lesson includes these topics:

Network Security Monitoring Placement
Objective: Describe placement of network security monitoring devices on the network.
Network Security Monitoring Data Types
Objective: Describe the various types of data used in monitoring network security.

Intrusion Prevention System Alerts
Objective: Describe the importance and use of IPS alerts in network security monitoring.
True/False, Positive/Negative IPS Alerts
Objective: Describe true and false positive IPS alerts and their effects on security monitoring.
IPS Alerts Analysis Process
Objective: Describe the process of IPS alert analysis.
Firewall Log
Objective: Describe the context of a security incident in firewall syslog messages.
DNS Log
Objective: Describe the need for network DNS activity log analysis.
Web Proxy Log
Objective: Describe web proxy log analysis for investigating web-based attacks.
Email Proxy Log
Objective: Describe email proxy log analysis for investigating email-based attacks.
AAA Server Log
Objective: Describe AAA server log analysis.
Next Generation Firewall Log
Objective: Describe NGFW log analysis for incident investigation.
Applications Log
Objective: Describe application log analysis for detecting application misuse.
Packet Captures
Objective: Describe packet capture usage and benefits for investigating security incidents.
NetFlow
Objective: Describe the use of NetFlow for collection and monitoring of network traffic flow data.
Network Behavior Anomaly Detection
Objective: Describe network behavior anomaly monitoring for detecting deviations from the normal patterns.
Data Loss Detection Using Netflow Example
Objective: Decribe using NetFlow for data loss detection.
Security Information and Event Management Systems
Objective: Describe the deployment and use of SIEMs to collect, sort, process, prioritize, store, and report the alarms.

Lesson 2: Describing Security Event Analysis

Objective: Explore the different threat models that security operations organizations can reference when performing cybersecurity analysis.

This lesson includes these topics:

Cyber Kill Chain
Objective: Provide overview of the cyber kill chain model that describes the structure of an attack.
Advanced Persistent Threats
Objective: Describe advanced persistence threats characteristics.
Diamond Model for Intrusion Analysis
Objective: Describe the Diamond model for intrusion analysis.
Cybersecurity Threat Models Summary
Objective: Summarize cybersecurity threat models.

SOC Runbook Automation

Objective: Provide an overview of the SOC runbook automation.

Malware Reverse Engineering

Objective: Describe how malware reverse engineering can help protect or defend against future attacks.

Chain of Custody

Objective: Describe chain of custody for all evidence and interacting with law enforcement.

Challenge