CCNA Cyber Ops Certification (Coming Soon)

Modality: On Demand

Duration:

This course is for professionals planning to enroll in the 210-250 SECFND Exam & 210-255 SECOPS Exam leading to the 210-250 SECFND & 210-255 SECOPS Certification. The official exam voucher is not included in this course. However, the official exam voucher can be purchased separately on request.

About this Course:

This course introduces IT Professionals to the concepts of cybersecurity relating to TCP/IP Protocols, Threat Analysis, Identification of Malicious Activities, Effective Attack Responses, Vulnerability Fixes, Event Correlation, and many more. This course is designed for professionals who want to embark on a professional road leading to cybersecurity expert. This course provides professionals and students with all the skills needed to function as an entry-level security team member.

Course Objectives:

The core objective of this course is to help professionals gain the knowledge and understanding of the following key concepts:

- Network Security Concepts Identification
- TCP/IP Essentials and Cryptography Principles
- Log Data Interpretation and Endpoint Attacks
- Data, Source, and Event Identification and Security Monitoring
- Security Vulnerabilities and Remote Exploits
- Key Concepts, Tools, and Infrastructure of SOC
- Threat-Centric SOC Basic Incident Analysis
- Attack Vectors and Basic Event Normalization
- Mitigating Malicious Activity and Types of SOC Metrics
- Automating SOC Workflow Management System

Audience:

- Cisco Channel Partners & Security Analyst
- Network Defense Analyst and Future Incident Responders
- IT Professionals and Network Security Experts
- Network Defense Infrastructure Professionals
- Security Operation Center Professionals

Job Roles:

- Information Security Analyst – Average Annual Salary $80,865

- Network Security Engineer – Average Annual Salary $83,114
- Security Engineer – Average Annual Salary $129,847
- Cybersecurity Engineer – Average Annual Salary $130,000

Prerequisites:

Professionals planning to enroll in this course must have the fundamental knowledge of technology and a certification in any one of the following courses:

- Cisco CCENT Certification
- CompTIAA+, CompTIA Network+, and CompTIA Server+ Certification
- Microsoft Specialist, MCSE, and MCSA Certification
- Cisco CCNA1 and Cisco CCNA2 Certification
- Oracle Linux OCP and OCA Certification and Red Hat (RHCE, RHCSA, & RHCA) Certification
- Professional Institute (LPI), Linux Foundation (LFCE & LFCS), & CompTIA Linux+ Certification

In addition to this obligatory prerequisites, it is also recommended that professionals have a sound knowledge of Windows Operating System, Cisco Fundamental Concepts, and Networking Devices.

Course Outline:

210-250 SECFND

This course allows learners to understand common security concepts, and start to

learn the basic security techniques used in a Security Operations Center (SOC) to

find threats on a network using a variety of popular security tools within a "real-life"

network infrastructure.

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
  - Classroom Live Labs

Guided Lab 1: Explore the TCP/IP Protocol Suite

- Topology
- Task 1: Examine the Network Configuration on Inside-Win
- Task 2: Examine the Network Configuration on Inside-Kali
- Task 3: Verify That Peers Are Not Yet in ARP Cache
- Task 4: Initialize the Packet Capture Process
- Task 5: Generate and Capture Local LAN Traffic
- Task 6: Examine Packet Summaries
- Task 7: Examine Ethernet Headers
- Task 8: Examine an IP Header
- Task 9: Examine an ICMP Header and Data
- Task 10: Capture Communication with a Remote LAN
- Task 11: Examine How the Communication Started
- Task 12: Examine a TCP Connection
- Task 13: Examine the First HTTP Transactions
- Task 14: Examine TCP Connections
- Task 15: Compare and Contrast TCP and UDP
- Challenge

Guided Lab 2: Explore the Network Infrastructure

- Topology
- Task 1: Explore Network Switch Operation
- Task 2: Explore VLANs
- Task 3: Explore Trunking
- Task 4: Explore Routing
- Task 5: Explore NAT
- Task 6: Explore Firewalling
- Task 7: Explore DHCP Operation
- Challenge

Guided Lab 3: Explore TCP/IP Attacks

- Topology
- Task 1: Footprinting
- Task 2: Fingerprinting
- Task 3: Discrete OS Scanning
- Task 4: Malicious Route Injection
- Task 5: ARP Cache Poisoning
- Challenge

Guided Lab 4: Explore Cryptographic Technologies

- Topology
- Task 1: Demonstrate Hash Algorithms
- Task 2: Examine Hash Collisions
- Task 3: Explore MD5 and Enable Secret

- Task 4: Demonstrate Symmetric Encryption
- Task 5: Demonstrate Asymmetric Encryption
- Task 6: Create a Key Pair and Digital Signature
- Task 7: Explore Public-Key Infrastructure
- Task 8: Capture Packets from an SSL/TLS Connection
- Task 9: Analyze SSL/TLS Negotiation
- Challenge

Guided Lab 5: Explore Network Applications

- Topology
- Task 1: Prepare to Send an Email Manually
- Task 2: Send an Email Manually
- Task 3: Follow the Email Path
- Task 4: Examine the Email
- Task 5: Send One Email the Normal Way
- Task 6: Examine Hypertext Markup Language
- Task 7: Examine Cascading Style Sheets
- Task 8: Examine JavaScript
- Task 9: Examine PHP
- Task 10: Examine Structured Query Language
- Task 11: Examine URLs
- Task 12: Capture HTTP Traffic for Analysis
- Task 13: HTTP Requests: GET and POST
- Challenge

Guided Lab 6: Explore Network Application Attacks

- Objective: This lab will explore several different classes of attacks against a targeted
- web server.
- Topology
- Task 1: Explore Vulnerability Scanning
- Task 2: Examine the Footprints of a Vulnerability Scan
- Task 3: Leverage the Vulnerability Scan Results
- Task 4: Perform an Offline Password Attack
- Task 5: Perform an Online Password Attack
- Task 6: Perform a Command Injection
- Task 7: Perform an SQL Injection
- Task 8: Account Access Via Cookie Manipulation
- Task 9: Explore Reflected Cross-Site Scripting
- Task 10: Explore Persistent Cross-Site Scripting
- Challenge

Guided Lab 7: Explore the Windows Operating System

- Objective: This lab will focus on exploring the Windows operating system and
- services discussed in the lesson.
- Topology

- Task 1: Prepare the Inside-Win VM
- Task 2: Explore Processes
- Task 3: Explore Threads
- Task 4: Explore the Registry Database
- Task 5: Explore Handles
- Task 6: Explore Windows Services
- Task 7: Explore Windows Users, Groups, and Permissions
- Task 8: Explore Windows Network Activity from the CLI
- Task 9: Explore Windows Network Activity from the GUI
- Challenge

Guided Lab 8: Explore the Linux Operating System

- Objective: This lab exercise provides you a structured experience with the Linux
- operating system basics.
- Topology
- Task 1: Bash Shell
- Task 2: Navigate Linux Directories
- Task 3: Basic File and Directory Operations
- Task 4: File System Permissions
- Task 5: Modify Permissions
- Task 6: I/O Piping and Redirection
- Task 7: grep Command
- Task 8: Linux Processes
- Task 9: netstat Command
- Challenge

Guided Lab 9: Explore Endpoint Attacks

- Topology
- Task 1: Perform Reconnaissance
- Task 2: Exploit a Misconfiguration
- Task 3: Exploit a Back Door
- Task 4: Escalate a Privilege Escalation
- Task 5: Exploit an Operating System Flaw
- Task 6: Use a Pivot
- Task 7: Employ Social Engineering/Phishing
- Task 8: Establish Persistence
- Task 9: Tunnel Exfiltrated Data
- Challenge

Guided Lab 10: Explore Network Security Technologies

- Topology
- Task 1: Examine Interface Access Policy on the ABC-ASA
- Task 2: Demonstrate Stateful Inspection of TCP
- Task 3: Examine Application Policy on the ABC-ASA
- Task 4: Examine Remote Access VPNs

- Task 5: Examine Network IDS
- Task 6: Examine the Squid Web Proxy
- Challenge

Guided Lab 11: Explore Endpoint Security

- Objective: Explore the behavior of two endpoint security applications that are part
- of the base Windows operating system distribution: Windows Defender and
- Windows Firewall.
- Topology
- Task 1: Explore Windows Defender
- Task 2: Explore Windows Firewall
- Task 3: Explore IPtables and TCP wrappers
- Challenge

Guided Lab 12: Explore Security Data for Analysis

- Objective: This lab focuses on the analysis of event data for investigation of a
- security event.
- Topology
- Task 1: Explore Alert Data
- Task 2: Extracted Content
- Task 3: Sandbox Analysis
- Task 4: Transaction Data
- Task 5: Session Data
- Task 6: Full Packet Capture
- Challenge

210-255 SECOPS

Module 1: SOC Overview

- Lesson 1: Defining the Security Operations Center
- Lesson 2: Understanding NSM Tools and Data
- Lesson 3: Understanding Incident Analysis in a Threat-Centric SOC
- Lesson 4: Identifying Resources for Hunting Cyber Threats

Module 2: Security Incident Investigations

- Lesson 1: Understanding Event Correlation and Normalization
- Lesson 2: Identifying Common Attack Vectors
- Lesson 3: Identifying Malicious Activity
- Lesson 4: Identifying Patterns of Suspicious Behavior
- Lesson 5: Conducting Security Incident Investigations

Module 3: SOC Operations

- Lesson 1: Describing the SOC Playbook
- Lesson 2: Understanding the SOC Metrics
- Lesson 3: Understanding the SOC WMS and Automation
- Lesson 4: Describing the Incident Response Plan
- Lesson 5: Appendix A—Describing the Computer Security Incident Response Team
- Lesson 6: Appendix B—Understanding the use of VERIS

Classroom Live Labs

- Guided Lab 1: Explore Network Security Monitoring Tools
    - Task 1: Prepare the Lab Environment
    - Task 2: Analyze Alerts
    - Task 3: Extract Content from Packet Captures
    - Task 4: Analyze Malware
    - Task 5: Search Bro Data Using ELSA
    - Challenge
- Discovery 1: Investigate Hacker Methodology
    - Task 1: Scanning and Analyzing Reconnaissance Activity
    - Task 2: Analyzing the Weaponization, Delivery, and Exploitation Phases of the
- Kill Chain Model
    - Task 3: Persistence on the Target Machine
    - Task 4: Host-Based Analysis
    - Task 5: Identifying Data Exfiltration
    - Challenge
- Discovery 2: Hunt Malicious Traffic
    - Task 1: Threat Simulation
    - Task 2: Combing Network Traffic with ELSA
    - Task 3: Pivot to Wireshark with capME!
    - Task 4: Analyzing Exfiltration Data
    - Task 5: Confirm A Backdoor
    - Challenge
- Discovery 3: Correlate Event Logs, PCAPs, and Alerts of an Attack
    - Task 1: Examine OSSEC Alerts
    - Task 2: Find and Correlate Additional Activity
    - Challenge
- Discovery 4: Investigate Browser-Based Attacks
    - Task 1: Setting up Security Onion
    - Task 2: SQL Injection
    - Task 3: Cross Site Scripting Attack
    - Task 4: Local File Inclusion and Directory Traversal
    - Challenge
- Discovery 5: Analyze Suspicious DNS Activity
    - Task 1: Investigate DNS Fast Fluxing
    - Task 2: Perform DNS Exfiltration
    - Task 3: Analyze DNS Exfiltration Activities
    - Challenge
- Discovery 6: Investigate Suspicious Activity Using Security Onion
    - Task 1: Identify Suspicious Domain Names

        - Task 2: Identify Suspicious User Agents
        - Task 3: Upload Malware to Malwr.com
        - Challenge
    - Discovery 7: Investigate Advanced Persistent Threats
        - Task 1: Investigate Sguil Alerts
        - Task 2: Investigate Suspicious Packet Captures
        - Task 3: Implement New Custom Snort Rule
        - Challenge
    - Discovery 8: Explore SOC Playbooks
        - Task 1: Access ELSA on the Security Onion VM
        - Task 2: Play: 404s Indicating Web Recon
        - Task 3: Play: Posts to Dynamic DNS Sites
        - Task 4: Play: DNS over TCP
        - Task 5: Play: HTTP Header Host Field Containing IP Address
        - Task 6: Play: Known Botnet C2 Domains (Manual Play)
        - Task 7: Play: Explore the Raw Bro Log Files
        - Task 8: Play: Known Botnet C2 Domains (Semi-Automated Play)
        - Task 9: Play: Malicious Files (Manual Play)
        - Task 10: Play: Malicious Files (Semi-Automated Play)
        - Task 11: Play: Large File Transfers (Semi-Automated Play)
        - Challenge
        - Challenge