CCNA Cybersecurity Operations 1.1 Scope and Sequence

Last updated June 18, 2018

Introduction

Today's organizations are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. Teams of people in Security Operations Centers (SOCs) keep a vigilant eye on security systems, protecting their organizations by detecting and responding to cybersecurity threats. CCNA Cybersecurity Operations prepares candidates to begin a career working with associate-level cybersecurity analysts within security operations centers.

Target Audience

The Cisco CCNA® Cybersecurity Operations 1.0 (CyberOps) course is designed for Cisco Networking Academy® students seeking career-oriented, entry-level security analyst skills. Target students include individuals enrolled in technology degree programs at institutions of higher education and IT professionals who want to pursue a career in the Security Operation Center (SOC).

Prerequisites

CCNA Cybersecurity Operations students should have the following skills and knowledge:

- PC and Internet navigation skills
- Basic Windows and Linux system concepts
- Basic Networking concepts
- Binary and Hexadecimal understanding
- Awareness of basic programming concepts
- Awareness of basic SQL queries

Target Certifications

This course aligns with the CCNA Cyber Ops certification. Candidates need to pass the 210-250 SECFND exam and the 210-255 SECOPS exam to achieve the CCNA Cyber Ops certification.

Curriculum Description

The course has many features to help students understand these concepts:

- Rich multimedia content, including interactive activities, videos, games, and quizzes, addresses a variety of learning styles and help stimulate learning and increase knowledge retention
- Virtual environments simulate real-world cybersecurity threat scenarios and create opportunities for ethical hacking, security monitoring, analysis and resolution
- Hands-on labs help students develop critical thinking and complex problem solving skills
- Innovative assessments provide immediate feedback to support the evaluation of knowledge and acquired skills

- Technical concepts are explained using language that works well for learners at all levels and embedded interactive activities break up reading of the content and help reinforce understanding
- The curriculum encourages students to consider additional IT education, but also emphasizes applied skills and hands-on experience
- Cisco Packet Tracer activities are designed for use with Packet Tracer 7.0 or later.

Curriculum Objectives

CCNA Cybersecurity Operations 1.0 covers knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a Security Operations Center (SOC).

Upon completion of the *CCNA Cybersecurity Operations 1.0* course, students will be able to perform the following tasks:

- Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
- Explain the role of the Cybersecurity Operations Analyst in the enterprise.
- Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses.
- Explain the features and characteristics of the Linux Operating System.
- Analyze the operation of network protocols and services.
- Explain the operation of the network infrastructure.
- Classify the various types of network attacks.
- Use network monitoring tools to identify attacks against network protocols and services.
- Use various methods to prevent malicious access to computer networks, hosts, and data.
- Explain the impacts of cryptography on network security monitoring.
- Explain how to investigate endpoint vulnerabilities and attacks.
- Evaluate network security alerts.
- Analyze network intrusion data to identify compromised hosts and vulnerabilities.
- Apply incident response models to manage network security incidents.

Virtual Machine Lab Requirements

This course uses a single virtual machine (VM) for many of the labs through Chapter 10. Three additional VMs are added in Chapter 11. There is also a single VM option available for lab or student PCs that do not meet the following requirements:

- Host computer with at least 8 GB of RAM and 45 GB of free disk space
- Latest version of Oracle VirtualBox: http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html
- Internet connection
- Five virtual machines listed in the table below:

Table 1. Virtual Machine Requirements

Virtual Machine	RAM	Disk Space	Username	Password
CyberOps Workstation VM	1 GB	7 GB	analyst	cyberops
Kali	1 GB	10 GB	root	cyberops
Metasploitable	512 KB	8 GB	msfadmin	msfadmin
Security Onion	4 GB	10 GB	analyst	cyberops
Security Onion (Alternative)*	3 GB	10 GB	analyst	cyberops

*Chapter 12 labs 12.4.1.1 and 12.4.1.2 provide an option of using only one Alternative Security Onion VM.

For the best learning experience, we recommend a typical class size of 12 to 15 students and a ratio of one Lab PC per student. At most, two students can share one Lab PC for the hands-on labs. Some lab activities require the student Lab PCs to be connected to a local network.

Course Outline

Table 2. Cybersecurity Operations 1.0 Course Outline

Chapter/Section	Goals/Objectives
Chapter 1. Cybersecurity and the Security Operations Center	**Explain the role of the Cybersecurity Operations Analyst in the enterprise.**
1.1 The Danger	Explain why networks and data are attacked.
1.2 Fighters in the War Against Cybercrime	Explain how to prepare for a career in Cybersecurity operations.
Chapter 2. Windows Operating System	**Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses.**
2.1 Windows Overview	Explain the operation of the Windows Operating System.
2.2 Windows Administration	Explain how to secure Windows endpoints.
Chapter 3. Linux Operating System	**Explain the features and characteristics of the Linux Operating System.**
3.1 Using Linux	Perform basic operations in the Linux shell.
3.2 Linux Administration	Perform basic Linux administration tasks.
3.3 Linux Clients	Perform basic security-related tasks on a Linux host.
Chapter 4. Network Protocols and Services	**Analyze the operation of network protocols and services.**
4.1 Network Protocols	Explain how protocols enable network operations.
4.2 Ethernet and Internet Protocol (IP)	Explain how the Ethernet and IP protocols support network communication.
4.3 Connectivity Verification	Use common testing utilities to verify and test network connectivity.

4.4 Address Resolution Protocol	Explain how the address resolution protocol enables communication on a network.
4.5 The Transport Layer and Network Services	Explain how transport layer protocols and network services support network functionality.
4.6 Network Services	Explain how network services enable network functionality.
Chapter 5. Network Infrastructure	**Explain the operation of the network infrastructure.**
5.1 Network Communication Devices	Explain how network devices enable wired and wireless network communication.
5.2 Network Security Infrastructure	Explain how devices and services are used to enhance network security.
5.3 Network Representations	Explain how networks and network topologies are represented.
Chapter 6. Principles of Network Security	**Classify the various types of network attacks.**
6.1 Attackers and Their Tools	Explain how networks are attacked.
6.2 Common Threats and Attacks	Explain the various types of threats and attacks.
Chapter 7. Network Attacks: A Deeper Look	**Use network monitoring tools to identify attacks that against network protocols and services.**
7.1 Observing Network Operation	Explain network traffic monitoring.
7.2 Attacking the Foundation	Explain how TCP/IP vulnerabilities enable network attacks.
7.3 Attacking What We Do	Explain how common network applications and services are vulnerable to attack.
Chapter 8. Protecting the Network	**Use various methods to prevent malicious access to computer networks, hosts, and data.**
8.1 Understanding Defense	Explain approaches to network security defense.
8.2 Access Control	Explain access control as a method of protecting a network.
8.3 Network Firewalls and Intrusion Prevention	Explain how firewalls and other devices prevent network intrusions.
8.4 Content Filtering	Explain how content filtering prevents unwanted data from entering the network.
8.5 Threat Intelligence	Use various intelligence sources to locate current security threats.
Chapter 9. Cryptography and the Public Key Infrastructure	**Explain the impacts of cryptography on network security monitoring.**
9.1 Cryptography	Use tools to encrypt and decrypt data.
9.2 Public Key Cryptography	Explain how the public key infrastructure (PKI) supports network security.
Chapter 10. Endpoint Security and Analysis	**Explain how to investigate endpoint vulnerabilities and attacks.**

10.1 Endpoint Protection	Use a tool to generate a malware analysis report.
10.2 Endpoint Vulnerability Assessment	Classify endpoint vulnerability assessment information.
Chapter 11. Security Monitoring	**Evaluate network security alerts.**
11.1 Technologies and Protocols	Explain how security technologies affect security monitoring.
11.2 Log Files	Explain the types of log files used in security monitoring
Chapter 12. Intrusion Data Analysis	**Analyze network intrusion data to identify compromised hosts and vulnerabilities**
12.1 Data Collection	Explain how security-related data is collected.
12.2 Data Preparation	Arrange a variety of log files in preparation for intrusion data analysis.
12.3 Data Analysis	Analyze intrusion data to determine the source of an attack.
Chapter 13. Incident Response and Handling	**Explain how network security incidents are handled by CSIRTs.**
13.1 Incident Response Models	Apply incident response models to an intrusion event.
13.2 CSIRTs and NIST 800-61r2	Apply standards specified in NIST 800-61r2 to a computer security incident.
13.3 Case-Based Practice	Given a set of logs, isolate a threat actor and recommend an incident response plan.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**