UNDERSTANDING CISCO CYBER SECURITY FUNDAMENTALS

DURATION: 5 DAYS

COURSE OVERVIEW

The Understanding Cisco Cyber security Fundamentals (SECFND) v1.0 course provides you with an understanding of network infrastructure devices, operations and vulnerabilities of the TCP/IP protocol suite, basic information security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data that are used to investigate security incidents.

After completing this course, you will have basic knowledge that is required to perform the job role of an entry-level cybersecurity analyst in a threat-centric security operations center.

TARGET AUDIENCE

Individuals looking to understand the basic principles of cyber security or study for the Cisco CCNA Cyber Ops Certification.

COURSE OBJECTIVES

After completing this course you should be able to:

1. Describe, compare and identify various network concepts
2. Fundamentals of TCP/IP
3. Describe and compare fundamental security concepts
4. Describe network applications and the security challenges
5. Understand basic cryptography principles.
6. Understand endpoint attacks, including interpreting log data to identify events in Windows and Linux
7. Develop knowledge in security monitoring, including identifying sources and types of data and events
8. Know various attack methods, security weaknesses, evasion methods, and remote versus local exploits

COURSE CONTENT

TCP/IP and Cryptography Concepts

1. Understanding the TCP/IP Protocol Suite

2. Understanding the Network Infrastructure
3. Understanding Common TCP/IP Attacks
4. Understanding Basic Cryptography Concepts

Network Applications and Endpoint Security

1. Describing Information Security Concepts
2. Understanding Network Applications
3. Understanding Common Network Application Attacks
4. Understanding Windows Operating System Basics
5. Understanding Linux Operating System Basics
6. Understanding Common Endpoint Attacks
7. Understanding Network Security Technologies
8. Understanding Endpoint Security Technologies

Security Monitoring and Analysis

1. Describing Security Data Collection
2. Describing Security Event Analysis

Labs

Lab 1: Explore the TCP/IP Protocol Suite
Lab 2: Explore the Network Infrastructure
Lab 3: Explore TCP/IP Attacks
Lab 4: Explore Cryptographic Technologies
Lab 5: Explore Network Applications
Lab 6: Explore Network Application Attacks
Lab 7: Explore the Windows Operating System
Lab 8: Explore the Linux Operating System
Lab 9: Explore Endpoint Attacks
Lab 10: Explore Network Security Technologies
Lab 11: Explore Endpoint Security
Lab 12: Explore Security Data for Analysis

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

1. Skills and knowledge equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1)
2. Working knowledge of the Windows operating system
3. Working knowledge of Cisco IOS networking and concepts

TEST CERTIFICATION

Recommended as preparation for the following exams:

210-250 - SECFND

This is one of two exams required to achieve the CCNA Cyber Ops Certification