

[Show Menu](#)[/ The Danger / Introduction](#)[1 The Danger ^](#)[US HOW IT'S DONE](#)[1.1 War Stories v](#)[1.2 Threat Actors v](#)[1.3 Threat Impact v](#)[1.4 The Danger Summary v](#)[2 Fighters in the War Against Cybercrime v](#)[3 The Windows Operating System v](#)[4 Linux Overview v](#)[5 Network Protocols v](#)[6 Ethernet and Internet Protocol \(IP\) v](#)[7 Connectivity Verification v](#)[8 Address Resolution Protocol v](#)[9 The Transport Layer v](#)[10 Network Services v](#)

## Introduction

1.0.1

### First Time in This Course



CyberOps Associate v1.0 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 CyberOps Associate v1.0 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.

## 11 Network Communication Devices

Show Menu

### 1 The Danger

US HOW IT'S DONE

#### 1.1 War Stories

#### 1.2 Threat Actors

#### 1.3 Threat Impact

#### 1.4 The Danger Summary

### 2 Fighters in the War Against Cybercrime

### 3 The Windows Operating System

### 4 Linux Overview

### 5 Network Protocols

### 6 Ethernet and Internet Protocol (IP)

### 7 Connectivity Verification

### 8 Address Resolution Protocol

### 9 The Transport Layer

### 10 Network Services

- 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.
- Explain how 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.

1.0.2

## Student Resources



There are a number of tools and resources that are available to you that will help you in your journey as you develop your CyberOps skills and prepare for job opportunities.

### Lab Environment

In this course, two virtual machines (VM) are used: CyberOps Workstation and Security Onion. These VMs

11	Network Communication Devices	▼	provide all of the applications and latest security monitoring and network intrusion analysis capabilities needed for the course.
	Show Menu		
1	The Danger	^	The minimum RAM memory requirement to run CyberOps Workstation virtual machines is 1 GB. However, for the Security Onion virtual machine, 4 GB RAM is recommended. The RAM memory recommendation on Security Onion VM allows the services, such as network security monitoring (NSM), to function properly.
	US NOW IT'S DONE		
1.1	War Stories	▼	
1.2	Threat Actors	▼	Installation labs are available in the course and provide detailed steps to properly set up your VMs and the lab environment.
1.3	Threat Impact	▼	<b>About Security Onion</b>
1.4	The Danger Summary	▼	Security Onion is developed by Security Onion Solutions. <a href="#">Security Onion</a> is made available under GPL license. This course uses provides basic training in the use of Security Onion to validate the objectives of this course. For further training needs, visit the Security Onion Solutions developer site.
2	Fighters in the War Against Cybercrime	▼	<b>Packet Tracer</b>
3	The Windows Operating System	▼	Packet Tracer simulates the internal workings of a network and is used in this course. Download and install the latest version of Packet Tracer here: <a href="#">Packet Tracer Resources</a> .
4	Linux Overview	▼	If you are new to Packet Tracer, take this FREE, short, online course now: <a href="#">Introduction to Packet Tracer Course</a> .
5	Network Protocols	▼	You can use your smartphone, tablet, or desktop to access your course; however, Packet Tracer activities, as well as some other activities, quizzes, and exams are best experienced using a PC.
6	Ethernet and Internet Protocol (IP)	▼	<b>Join Our Communities</b>
7	Connectivity Verification	▼	Connect with and get help from other Networking Academy students from around the world with our <a href="#">Cisco Networking Academy Facebook page</a> .
8	Address Resolution Protocol	▼	Network with your peers at our <a href="#">Cisco Networking Academy LinkedIn page</a> .
9	The Transport Layer	▼	<b>Get a Job!</b>
10	Network Services	▼	

## 11 Network Communication Devices

Show Menu

### 1 The Danger

US NOW IT'S DONE

#### 1.1 War Stories

#### 1.2 Threat Actors

#### 1.3 Threat Impact

#### 1.4 The Danger Summary

### 2 Fighters in the War Against Cybercrime

### 3 The Windows Operating System

### 4 Linux Overview

### 5 Network Protocols

### 6 Ethernet and Internet Protocol (IP)

### 7 Connectivity Verification

### 8 Address Resolution Protocol

### 9 The Transport Layer

### 10 Network Services

Access [Career Resources](#) specifically tailored to help NetAcad students to be successful in the workplace.

Find great job opportunities with Cisco and Cisco partners. Register now with [Talent Bridge](#).

Getting industry certification is a guarantee to employers that you have the technical skills to do the job. Check out our [Certifications and Vouchers](#) page.

#### More Courses

Choose a course, practice what you learn, and become an IT professional. Check out our [Course Catalog](#).

1.0.3

## Ethical Hacking Statement



The Cisco Networking Academy Program is focused on creating the global problem solvers needed to build, scale, secure, and defend the networks that are used in our businesses and daily lives. The need for well-trained cybersecurity specialists continues to grow at an exponential rate. Training to become a cybersecurity specialist requires in depth understanding and exposure to how cyber attacks occur, as well as how they are detected and prevented. These skills will naturally also include learning the techniques that threat actors use to circumvent data, privacy, and computer and network security.

In this course, learners will use tools and techniques in a “sandboxed”, virtual machine environment that allows them to create, implement, monitor, and detect various types of cyber attacks. The hands-on training is performed in this environment so that students can gain the necessary skills and knowledge needed to thwart these and future cyber attacks. Security holes and vulnerabilities that are created in this course should only be used in an ethical manner and only in this “sandboxed” virtual environment. Experimentation with these tools, techniques, and resources outside of the provided sandboxed virtual environment is at the discretion of the

11	Network Communication Devices	▼
	Show Menu	
1	The Danger	^
	US NOW IT'S DONE	
1.1	War Stories	▼
1.2	Threat Actors	▼
1.3	Threat Impact	▼
1.4	The Danger Summary	▼
2	Fighters in the War Against Cybercrime	▼
3	The Windows Operating System	▼
4	Linux Overview	▼
5	Network Protocols	▼
6	Ethernet and Internet Protocol (IP)	▼
7	Connectivity Verification	▼
8	Address Resolution Protocol	▼
9	The Transport Layer	▼
10	Network Services	▼

instructor and local institution. If the learner has any doubt about which computer systems and networks are part of the sandboxed virtual environment, they should contact their instructor prior to any experimentation.

Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

1.0.4

## Why Should I Take this Module?



Have you ever had something stolen? Perhaps you have had a wallet stolen or had your house robbed. Not only do you need to protect your physical property, you need to protect your information! Who is stealing information and why are they doing it? Maybe it is an individual just seeing if they are able to hack the information. Often it is for financial gain. There are many reasons. Keep reading this module to find out more about the threats and threat actors responsible for these attacks.





1.0.5

## What Will I Learn in this Module?



**Module Title:** The Danger  
**Module Objective:** Explain why networks and data are attacked.

Topic Title	Topic Objective

11	Network Communication Devices	▼	Topic Title	Topic Objective
	Show Menu		War Stories	Explain why networks and data are attacked.
			Threat Actors	Explain the motivations of the threat actors behind specific security incidents.
			Threat Impact	Explain the potential impact of network security attacks.
1	The Danger	^	<div>1.0.6</div> <h2>Class Activity - Top Hacker Shows Us How It's Done </h2> <p>In this class activity, you will view a TED Talk video that discusses various security vulnerabilities. You will also research one of the vulnerabilities mentioned in the video.</p> <div>  Top Hacker Shows ... </div>	
	US HOW IT'S DONE			
1.1	War Stories	▼		
1.2	Threat Actors	▼		
1.3	Threat Impact	▼		
1.4	The Danger Summary	▼		
2	Fighters in the War Against Cybercrime	▼	<div>  CyberOps Associate <div>1.1</div> War Stories  </div>	
3	The Windows Operating System	▼		
4	Linux Overview	▼		
5	Network Protocols	▼		
6	Ethernet and Internet Protocol (IP)	▼		
7	Connectivity Verification	▼		
8	Address Resolution Protocol	▼		
9	The Transport Layer	▼		
10	Network Services	▼		