Cisco Networking Academy

CyberOps Associate (CA) Release Notes

Last updated July 23, 2020

Purpose

The CyberOps Associate course is designed for Cisco Networking Academy® students who are 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). Learners in this course are exposed to all of the foundational knowledge required to detect, analyze, and escalate basic cybersecurity threats using common open-source tools. This course aligns with the Cisco Certified CyberOps Associate (CBROPS) certification. Candidates need to pass the 200-201 CBROPS exam to achieve the Cisco Certified CyberOps Associate certification.

By the end of the course, students will be able to:

- 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.
- 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.

This course contains numerous opportunities for practicing and assessing student skills through various types of assessments, labs, and Packet Tracer activities.

These notes provide detailed information about this release, including curriculum content, known issues, and support information.

This 70-hour, instructor-led course includes videos, labs, Packet Tracer activities, Module Quizzes, Module Exams, a Skills Assessment Lab, and Final Exams.

Release Content

Table 1. Content Included in the Cyber Operations Associate Release

Component	Description
E-Learning Content	28 modules
Videos	30 videos
Labs	46 hands on and paper labs
Packet Tracer Activities	6 Packet Tracer activities. Minimum Packet Tracer version is 7.3.0 Simulation and modeling activities designed for skills exploration, acquisition, reinforcement.
Interactive Activities	9 Interactive activities
Check Your Understanding	46 CYUs CYUs are per topic, online, self-diagnostic quizzes to help learners gauge content understanding. CYU activities are designed to let students quickly determine if they understand the content and can proceed, or if they need to review. CYU activities ***do not*** affect student grades.
Module Quizzes	28 Module Quizzes Instructor Activated Assessments that assess content from multiple modules. These assessments provide learners the opportunity to apply and validate knowledge learned.
Module Group Exams	9 Module Group Exams These assessments provide learners the opportunity to apply and validate knowledge learned throughout the course.
Practice Final	1 practice final Unsecured. Not Dynamic.

Secured, Dynamic Final Exam	1 Dynamic Final Exam with Secured Activation Variables in the design of the exam allow an instructor to administer unique exams to each student and assess each student's learning individually. With Secured Activation, individual assessment item preview and review is disabled to improve validity and security of this summative assessment. Instructors are provided with a visual summary view of how students performed against the competencies outlined for the course.
200-201 Certification Practice Exam	1 Certification practice exam Unsecured. Dynamic.
Skills Assessment Lab	1
End-of-Course Feedback	1 end-of-course survey to provide feedback for the course.
Accessibility	New UI complies with WCAG 2.1 Level AA Guidelines. All pages contain accessible text and highly descriptive media transcripts. All PDF files in the curriculum have been created with accessible features. Videos have closed captioning available. UI is screen reader and keyboard accessible.
Certificate of Completion	The successful completion of the end-of-course assessment and end-of-course survey are required for receiving the Certificate of Completion.

Equipment List

This course uses one of two virtual machines (VM) for many of the labs. Only one VM is required to be run at a time in any lab that uses a VM. The lab or student PCs should meet the following requirements:

- Host computer using 64-bit processor with at least 8 GB of RAM and 40 GB of free disk space (see link to determine if your host computer has a 64-bit processor: https://www.computerhope.com/issues/ch001121.htm)
- Latest version of Oracle VirtualBox: http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html
- Internet connection
- Two virtual machines that are listed in the table below:

Table 2. Virtual Machine Requirements

Virtual Machine	RAM	Disk Space	Username	Password
CyberOps Workstation VM	1 GB	20 GB	analyst	cyberops
Security Onion VM	4 GB Minimum (8GB Highly Recommended)	20 GB	analyst	cyberops

Known Issues

Table 3. Known Issues

Known Issues and Caveats	Description
English Spelling	American-English spellings are interspersed in the text of the modules.
Closed Captions	Use the external video link if you are having issues with the embedded videos.
Packet Tracer Program	You must use Packet Tracer version 7.3.0 to load the Packet Tracer activities within this course and assessments.
CyberOps Skills Challenge Game v1.1	This course also contains the VMs and installation guides to run the optional CyberOps Skills Challenge game from that was developed with the CCNA CyberOps v1.1 course. The game and the VMs do not completely align with the CyberOps Associate course or certification but do provide opportunities for fun and practice with the fundamentals of cybersecurity knowledge and skills. The files are used as is and have not been updated. Consult the FAQ provided in the Instructor Resources for more information on the game.

Course Outline

Table 4. Course Outline

Module	Title
1	Course Introduction/The Danger
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	Principles of Network Security
8	Address Resolution Protocol
9	The Transport Layer

10	Network Services
11	Network Communication Devices
12	Network Security Infrastructure
13	Attackers and Their Tools
14	Common Threats and Attacks
15	Observing Network Operation
16	Attacking the Foundation
17	Attacking What We Do
18	Understanding Defense
19	Access Control
20	Threat Intelligence
21	Cryptography
22	Endpoint Protection
23	Endpoint Vulnerability Assessment
24	Technologies and Protocols
25	Network Security Data
26	Evaluating Alerts
27	Working with Network Security Data
28	Digital Forensics and Incident Analysis and Response

Updates in CyberOps Associate

This is the first version of the CyberOps Associate course; therefore, there are no updates.

Support

For general assistance with curriculum, classroom, or program issues, please contact the Networking Academy™ Support Desk by signing into the netacad.com™ learning environment and clicking the Support question mark (?).