

# uCertify

## Course Outline

### IDS and IPS with Snort 3



20 May 2026

1. Exercises, Quizzes, Flashcards & Glossary

Number of Questions

2. Expert Instructor-Led Training

3. ADA Compliant & JAWS Compatible Platform

4. State of the Art Educator Tools

5. Award Winning Learning Platform (LMS)

6. Chapter & Lessons

Syllabus

Chapter 1: Introduction

Chapter 2: Introduction to Intrusion Detection and Prevention

Chapter 3: The History and Evolution of Snort

Chapter 4: Snort 3 – System Architecture and Functionality

Chapter 5: Installing Snort 3

Chapter 6: Configuring Snort 3

Chapter 7: Data Acquisition

Chapter 8: Packet Decoding

Chapter 9: Inspectors

Chapter 10: Stream Inspectors

Chapter 11: HTTP Inspector

Chapter 12: DCE/RPC Inspectors

Chapter 13: IP Reputation

Chapter 14: Rules

Chapter 15: Alert Subsystem

Chapter 16: OpenAppID

Chapter 17: Miscellaneous Topics on Snort 3

Videos and How To

7. Live labs

Lab Tasks

Here's what you get

## 1. Exercises

There is no limit to the number of times learners can attempt these. Exercises come with detailed remediation, which ensures that learners are confident on the topic before proceeding.

**49**  
EXERCISES

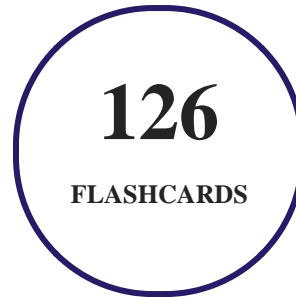
## 2. Quiz

Quizzes test your knowledge on the topics of the exam when you go through the course material. There is no limit to the number of times you can attempt it.

**223**  
QUIZ

## 3. flashcards

Flashcards are effective memory-aiding tools that help you learn complex topics easily. The flashcard will help you in memorizing definitions, terminologies, key concepts, and more. There is no limit to the number of times learners can attempt these. Flashcards help master the key concepts.



#### 4. Glossary of terms

uCertify provides detailed explanations of concepts relevant to the course through Glossary. It contains a list of frequently used terminologies along with its detailed explanation. Glossary defines the key terms.



#### 5. Expert Instructor-Led Training

uCertify uses the content from the finest publishers and only the IT industry's finest instructors. They have a minimum of 15 years real-world experience and are subject matter experts in their fields. Unlike a live class, you can study at your own pace. This creates a personal learning experience and gives you all the benefit of hands-on training with the flexibility of doing it around your schedule 24/7.

#### 6. ADA Compliant & JAWS Compatible Platform

uCertify course and labs are ADA (Americans with Disability Act) compliant. It is now more accessible to students with features such as:

- Change the font, size, and color of the content of the course
- Text-to-speech, reads the text into spoken words
- Interactive videos, how-tos videos come with transcripts and voice-over
- Interactive transcripts, each word is clickable. Students can clip a specific part of the video by clicking on a word or a portion of the text.

JAWS (Job Access with Speech) is a computer screen reader program for Microsoft Windows that reads the screen either with a text-to-speech output or by a Refreshable Braille display. Student can easily navigate uCertify course using JAWS shortcut keys.

## 7. State of the Art Educator Tools

uCertify knows the importance of instructors and provide tools to help them do their job effectively. Instructors are able to clone and customize course. Do ability grouping. Create sections. Design grade scale and grade formula. Create and schedule assessments. Educators can also move a student from self-paced to mentor-guided to instructor-led mode in three clicks.

## 8. Award Winning Learning Platform (LMS)

uCertify has developed an award winning, highly interactive yet simple to use platform. The SIIA CODiE Awards is the only peer-reviewed program to showcase business and education technology's finest products and services. Since 1986, thousands of products, services and solutions have been recognized for achieving excellence. uCertify has won CODiE awards consecutively for last 7 years:

- **2014**
  1. Best Postsecondary Learning Solution
- **2015**
  1. Best Education Solution

2. Best Virtual Learning Solution
3. Best Student Assessment Solution
4. Best Postsecondary Learning Solution
5. Best Career and Workforce Readiness Solution
6. Best Instructional Solution in Other Curriculum Areas
7. Best Corporate Learning/Workforce Development Solution

- **2016**

1. Best Virtual Learning Solution
2. Best Education Cloud-based Solution
3. Best College and Career Readiness Solution
4. Best Corporate / Workforce Learning Solution
5. Best Postsecondary Learning Content Solution
6. Best Postsecondary LMS or Learning Platform
7. Best Learning Relationship Management Solution

- **2017**

1. Best Overall Education Solution
2. Best Student Assessment Solution
3. Best Corporate/Workforce Learning Solution
4. Best Higher Education LMS or Learning Platform

- **2018**

1. Best Higher Education LMS or Learning Platform
2. Best Instructional Solution in Other Curriculum Areas
3. Best Learning Relationship Management Solution

- **2019**

1. Best Virtual Learning Solution
2. Best Content Authoring Development or Curation Solution
3. Best Higher Education Learning Management Solution (LMS)

- **2020**

1. Best College and Career Readiness Solution
2. Best Cross-Curricular Solution
3. Best Virtual Learning Solution

## 9. Chapter & Lessons

uCertify brings these textbooks to life. It is full of interactive activities that keeps the learner engaged. uCertify brings all available learning resources for a topic in one place so that the learner can efficiently learn without going to multiple places. Challenge questions are also embedded in the chapters so learners can attempt those while they are learning about that particular topic. This helps them grasp the concepts better because they can go over it again right away which improves learning.

Learners can do Flashcards, Exercises, Quizzes and Labs related to each chapter. At the end of every lesson, uCertify courses guide the learners on the path they should follow.

### Syllabus

#### Chapter 1: Introduction

- Who this course is for
- What this course covers
- To get the most out of this course
- Conventions used

#### Chapter 2: Introduction to Intrusion Detection and Prevention

- The need for information security
- Defense-in-depth strategy

- The role of network IDS and IPS
- Types of intrusion detection
- The state of the art in IDS/IPS
- IDS/IPS metrics
- Evasions and attacks
- Summary

### Chapter 3: The History and Evolution of Snort

- The beginning of Snort
- Snort 1 – key features and limitations
- Snort 2 – key features, improvements, and limitations
- The need for Snort 3
- Summary

### Chapter 4: Snort 3 – System Architecture and Functionality

- Design goals
- Key components
- Snort 3 system architecture

- Summary

## Chapter 5: Installing Snort 3

- Choosing an OS for installing Snort 3
- Snort 3 installation process
- Installing Snort 3 on CentOS
- Installing Snort 3 on Kali (Debian)
- Summary

## Chapter 6: Configuring Snort 3

- Configuring Snort 3 – how?
- Configuring Snort 3 – what?
- Configuring your environment
- Optimal configuration and tuning
- Managing multiple policies and configurations
- Summary

## Chapter 7: Data Acquisition

- The functionality of the DAQ layer

- The performance of the DAQ Layer
- Packet capture in Snort
- The Snort 3 implementation of the DAQ layer
- Configuring DAQ
- Summary

## Chapter 8: Packet Decoding

- OSI layering and packet structure
- The role of packet decoding (Codecs)
- Packet decoding in Snort 3
- EthCodec – a layer 2 codec
- IPv4Codec – a layer 3 codec
- TcpCodec – a layer 4 codec
- Code structure and other codecs
- Summary

## Chapter 9: Inspectors

- The role of inspectors
- Types of inspectors

- Snort 3 inspectors
- Summary

## Chapter 10: Stream Inspectors

- Relevant protocols for the stream inspector
- The stream inspectors
- Summary

## Chapter 11: HTTP Inspector

- Basics of HTTP
- HTTP inspector
- HTTP inspector configuration
- Summary

## Chapter 12: DCE/RPC Inspectors

- A DCE/RPC overview
- DCE/RPC inspectors
- DCE/RPC rule options
- Summary

## Chapter 13: IP Reputation

- Background
- Configuration of the IP reputation inspector module
- Functionality of the IP reputation inspector
- IP reputation inspector – alerts and pegs
- Summary

## Chapter 14: Rules

- Snort rule – the structure
- Rule header
- Rule options
- Recommendations for writing good rules
- Summary

## Chapter 15: Alert Subsystem

- Post-inspection processing
- Alert formats
- Summary

## Chapter 16: OpenAppID

- The OpenAppID feature
- Design and architecture
- Summary

## Chapter 17: Miscellaneous Topics on Snort 3

- Snort 2 to Snort 3 migration
- Troubleshooting Snort 3
- Summary

## 10. Live Labs

The benefits of live-labs are:

- Exam based practical tasks
- Real equipment, absolutely no simulations
- Access to the latest industry technologies
- Available anytime, anywhere on any device
- Break and Reset functionality
- No hardware costs

## Lab Tasks

## **Introduction to Intrusion Detection and Prevention**

- Analyzing Malware Using VirusTotal
- Performing Static Analysis with Ghidra
- Using Syslog to Centralize Network Logs
- Creating Basic WAF Rules for a Web Application
- Using the Metasploit RDP Post-Exploitation Module
- Performing Reconnaissance on a Network
- Configuring iptables to Allow or Deny Traffic
- Configuring Firewall Rules and Monitoring Network Logs Using pfSense
- Viewing Linux Event Logs
- Simulating a DoS Attack
- Analyzing a Phishing Attack

## **The History and Evolution of Snort**

- Configuring Snort 2

## **Installing Snort 3**

- Configuring Snort 3

## **Packet Decoding**

- Decoding Ethernet Frames in Snort 3
- Analyzing TCP Segments in Snort 3

## **Inspectors**

- Exploring Snort 3 Inspectors

## **HTTP Inspector**

- Capturing and Analyzing Network Traffic Using Wireshark

## **IP Reputation**

- Configuring the IP Reputation Inspector in Snort 3

### Alert Subsystem

- Viewing Snort Alerts in Unified2 Format

## Here's what you get

**19**

LIVE LABS

**19**

VIDEO TUTORIALS

**36**

MINUTES

You can't stay away! Get

 3187 Independence Drive  
Livermore, CA 94551,  
United States



+1-415-763-6300



support@ucertify.com



www.ucertify.com