uCertify

Course Outline

Cybersecurity – Attack and Defense Strategies

20 May 2024

1. Course Objective
2. Pre-Assessment
3. Exercises, Quizzes, Flashcards & Glossary

   Number of Questions
4. Expert Instructor-Led Training
5. ADA Compliant & JAWS Compatible Platform
6. State of the Art Educator Tools
7. Award Winning Learning Platform (LMS)
8. Chapter & Lessons

1. Course Objective

The Cybersecurity – Attack and Defense Strategies course delves into the intricacies of cybersecurity by exploring both offensive and defensive strategies. This course is meticulously crafted to empower you with the expertise required to safeguard systems, networks, and data from cyber threats while gaining insights into the tactics employed by cyber attackers. Whether you are venturing into cybersecurity or aiming to advance your competencies, this course equips you with the skills necessary to excel in the cybersecurity domain.

2. Pre-Assessment

Pre-Assessment lets you identify the areas for improvement before you start your prep. It determines what students know about a topic before it is taught and identifies areas for improvement with question assessment before beginning the course.

3. Exercises

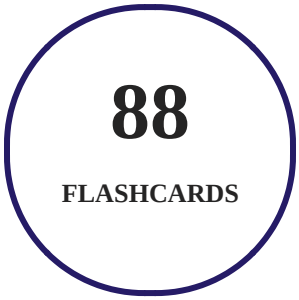
There is no limit to the number of times learners can attempt these. Exercises come with detailed remediation, which ensures that learners are confident on the topic before proceeding.

4. 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.

5. 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.



6. 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.

7. 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.

8. 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.

9. 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.

10. 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

11. 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: Preface

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

Chapter 2: Security Posture

- Why security hygiene should be your number one priority
- The current threat landscape
- Cybersecurity challenges
- Enhancing your security posture
- The Red and Blue Teams
- Summary
- References

Chapter 3: Incident Response Process

- The incident response process
- Handling an incident
- Post-incident activity
- Considerations for incident response in the cloud
- Summary
- References

Chapter 4: What is a Cyber Strategy?

- How to build a cyber strategy
- Why do we need to build a cyber strategy?
- Best cyber attack strategies
- Best cyber defense strategies
- Benefits of having a proactive cybersecurity strategy
- Top cybersecurity strategies for businesses
- Conclusion
- Further reading

Chapter 5: Understanding the Cybersecurity Kill Chain

- Understanding the Cyber Kill Chain
- Security controls used to stop the Cyber Kill Chain
- Threat life cycle management
- Concerns about the Cybersecurity Kill Chain
- How the Cyber Kill Chain has evolved
- Tools used during the Cyber Kill Chain
- Comodo AEP via Dragon Platform
- Summary

- Further reading
- References

Chapter 6: Reconnaissance

- External reconnaissance
- Internal reconnaissance
- Tools used for reconnaissance
- Passive vs. active reconnaissance
- How to combat reconnaissance
- How to prevent reconnaissance
- Summary
- References

Chapter 7: Compromising the System

- Analyzing current trends
- Performing the steps to compromise a system
- Mobile phone (iOS/Android) attacks
- Summary

- Avoiding alerts
- Performing privilege escalation
- Summary
- References

Chapter 11: Security Policy

- Reviewing your security policy
- Educating the end user
- Policy enforcement
- Monitoring for compliance
- Continuously driving security posture enhancement via security policy
- Summary
- References

Chapter 12: Network Security

- The defense-in-depth approach
- Physical network segmentation
- Securing remote access to the network
- Virtual network segmentation

- Zero trust network
- Hybrid cloud network security
- Summary
- References

Chapter 13: Active Sensors

- Detection capabilities
- Intrusion detection systems
- Intrusion prevention system
- Behavior analytics on-premises
- Behavior analytics in a hybrid cloud
- Summary
- References

Chapter 14: Threat Intelligence

- Introduction to threat intelligence
- Open-source tools for threat intelligence
- Microsoft threat intelligence

- Summary
- References

Chapter 15: Investigating an Incident

- Scoping the issue
- Investigating a compromised system on-premises
- Investigating a compromised system in a hybrid cloud
- Proactive investigation (threat hunting)
- Lessons learned
- Summary
- References

Chapter 16: Recovery Process

- Disaster recovery plan
- Live recovery
- Contingency planning
- Business continuity plan
- Best practices for disaster recovery
- Summary

- Further reading
- References

Chapter 17: Vulnerability Management

- Creating a vulnerability management strategy
- Elements of a vulnerability strategy
- Differences between vulnerability management and vulnerability assessment
- Best practices for vulnerability management
- Vulnerability management tools
- Conclusion
- Summary
- Further reading
- References

Chapter 18: Log Analysis

- Data correlation
- Operating system logs
- Firewall logs

- Web server logs
- Amazon Web Services (AWS) logs
- Azure Activity logs
- Google Cloud Platform Logs
- Summary
- References

12. Practice Test

Here's what you get

65	65
PRE-ASSESSMENTS QUESTIONS	POST-ASSESSMENTS QUESTIONS

Features

Each question comes with detailed remediation explaining not only why an answer option is correct but also why it is incorrect.

Unlimited Practice

Each test can be taken unlimited number of times until the learner feels they are prepared. Learner can review the test and read detailed remediation. Detailed test history is also available.

Each test set comes with learn, test and review modes. In learn mode, learners will attempt a question and will get immediate feedback and complete remediation as they move on to the next question. In test mode, learners can take a timed test simulating the actual exam conditions. In review mode, learners can read through one item at a time without attempting it.

13. 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

Security Posture

- Performing a Phishing Attack

What is a Cyber Strategy?

- Simulating the DDoS Attack
- Using OWASP ZAP

Understanding the Cybersecurity Kill Chain

- Using Nikto
- Cracking a Linux Password Using John the Ripper
- Using the EternalBlue Exploit in Metasploit
- Cracking Password Using Hydra
- Using Sparta
- Using Kismet

Reconnaissance

- Performing Reconnaissance on a Network
- Installing a Wardriving Application and Analyzing a Site Survey Capture
- Gathering OSINT
- Sniffing a Network with Wireshark
- Using the masscan Command
- Capturing Network Packets Using tcpdump
- Performing Nmap Port Scanning
- Using theHarvester
- Conducting Vulnerability Scanning Using Nessus
- Using Cain and Abel
- Using nslookup for Passive Reconnaissance

Compromising the System

- Using the Armitage Tool for Intrusion Detection
- Cracking Windows Password Using Ophcrack
- Conducting a Cross-Site Request Forgery Attack
- Exploiting a Website Using SQL Injection

Lateral Movement

- Understanding Lateral Movement

Privilege Escalation

- Understanding LPE

Network Security

- Configuring VLANs
- Configuring a Network Firewall
- Configuring a VPN

Active Sensors

- Performing Intrusion Detection

Threat Intelligence

- Examining MITRE ATT&CK

Investigating an Incident

- Using the NETSH Command
- Using the PING Command

Recovery Process

- Using the chntpw Command

Vulnerability Management

- Performing Vulnerability Scanning Using OpenVAS

Log Analysis

- Analyzing Linux Logs for Security Intelligence
- Viewing Windows Event Logs

Here's what you get

37

LIVE LABS

14. Post-Assessment

After completion of the uCertify course Post-Assessments are given to students and often used in conjunction with a Pre-Assessment to measure their achievement and the effectiveness of the exam.

GET IN TOUCH:

3187 Independence Drive
Livermore, CA 94551,
United States

+1-415-763-6300

support@ucertify.com

www.ucertify.com