

# uCertify

## Course Outline

### The Ultimate Kali Linux



04 Aug 2025

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: Preface

Chapter 2: Introduction to Ethical Hacking

Chapter 3: Building a Penetration Testing Lab

Chapter 4: Setting Up for Advanced Penetration Testing Techniques

Chapter 5: Passive Reconnaissance

Chapter 6: Exploring Open-Source Intelligence

Chapter 7: Active Reconnaissance

Chapter 8: Performing Vulnerability Assessments

Chapter 9: Understanding Network Penetration Testing

Chapter 10: Performing Network Penetration Testing

Chapter 11: Post-Exploitation Techniques

Chapter 12: Delving into Command and Control Tactics

Chapter 13: Working with Active Directory Attacks

Chapter 14: Advanced Active Directory Attacks

Chapter 15: Advanced Wireless Penetration Testing

Chapter 16: Social Engineering Attacks

Chapter 17: Understanding Website Application Security

Chapter 18: Advanced Website Penetration Testing

Chapter 19: Best Practices for the Real World

Chapter 20: Appendix

Videos and How To

7. Live labs

Lab Tasks

Here's what you get

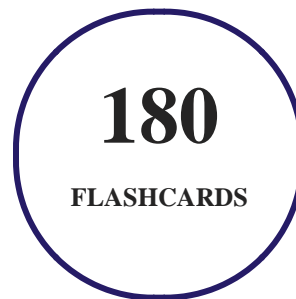
## 1. Exercises

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.



## 2. 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.



## 3. 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.



#### 4. 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.

#### 5. 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.

## 6. 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.

## 7. 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

## 8. 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: Introduction to Ethical Hacking

- Understanding the need for cybersecurity
- Exploring cybersecurity terminology
- Identifying threat actors and their intent
- Understanding what matters to threat actors
- Exploring the importance of penetration testing
- Penetration testing methodologies
- Discovering penetration testing approaches
- Types of penetration testing
- Exploring the phases of penetration testing
- Understanding the Cyber Kill Chain framework

- Summary

## Chapter 3: Building a Penetration Testing Lab

- An overview of the lab setup and technologies used
- Setting up a hypervisor and virtual networks
- Setting up and working with Kali Linux
- Setting up a vulnerable web application
- Deploying Metasploitable 2 as a vulnerable machine
- Building and deploying Metasploitable 3
- Summary

## Chapter 4: Setting Up for Advanced Penetration Testing Techniques

- Building an Active Directory red team lab
- Setting up a wireless penetration testing lab
- Summary

## Chapter 5: Passive Reconnaissance

- The importance of reconnaissance
- Exploring passive reconnaissance



- Creating a sock puppet
- Anonymizing internet-based traffic
- Summary

## Chapter 6: Exploring Open-Source Intelligence

- Google hacking techniques
- Domain reconnaissance
- Sub-domain harvesting
- Identifying organizational infrastructure
- Harvesting employees' data using Hunter
- Automating social media reconnaissance with Sherlock
- Summary

## Chapter 7: Active Reconnaissance

- Understanding active information
- Profiling websites using EyeWitness
- Exploring active scanning techniques
- Using scanning evasion techniques
- Enumerating network services

- Discovering data leaks in the cloud
- Summary

## Chapter 8: Performing Vulnerability Assessments

- Getting started with Nessus
- Vulnerability identification using Nmap
- Working with Greenbone Vulnerability Manager
- Using web application scanners
- Summary

## Chapter 9: Understanding Network Penetration Testing

- Introduction to network penetration testing
- Working with bind and reverse shells
- Antimalware evasion techniques
- Working with wireless adapters
- Managing and Monitoring wireless modes
- Summary

## Chapter 10: Performing Network Penetration Testing

- Exploring password-based attacks
- Performing host discovery
- Identifying and exploiting vulnerable services
- Summary

## Chapter 11: Post-Exploitation Techniques

- Pass-the-hash techniques
- Post exploitation using Meterpreter
- Data encoding and exfiltration
- Summary

## Chapter 12: Delving into Command and Control Tactics

- Understanding C2
- Setting up C2 operations
- Post-exploitation using Empire
- Working with Starkiller
- Summary

## Chapter 13: Working with Active Directory Attacks

- Understanding Active Directory
- Enumerating Active Directory
- Leveraging network-based trust
- Summary

## Chapter 14: Advanced Active Directory Attacks

- Understanding Kerberos
- Abusing trust on IPv6 with Active Directory
- Attacking Active Directory
- Domain dominance and persistence
- Summary

## Chapter 15: Advanced Wireless Penetration Testing

- Introduction to Wireless Networking
- Performing Wireless Reconnaissance
- Compromising WPA/WPA2 Networks
- Performing AP-less Attacks
- Exploiting Enterprise Networks

- Setting Up a Wi-Fi Honeypot
- Exploiting WPA3 Attacks
- Summary

## Chapter 16: Social Engineering Attacks

- Fundamentals of social engineering
- Types of social engineering
- Planning for each type of social engineering attack
- Defending against social engineering
- Exploring social engineering tools and techniques
- Summary

## Chapter 17: Understanding Website Application Security

- Understanding web applications
- Exploring the OWASP Top 10: 2021
- Getting started with FoxyProxy and Burp Suite
- Understanding injection-based attacks
- Exploring broken access control attacks
- Discovering cryptographic failures

- Understanding insecure design
- Exploring security misconfiguration
- Summary

## Chapter 18: Advanced Website Penetration Testing

- Identifying vulnerable and outdated components
- Exploiting identification and authentication failures
- Understanding software and data integrity failures
- Exploring server-side request forgery
- Understanding security logging and monitoring failures
- Understanding cross-site scripting
- Automating SQL injection attacks
- Performing client-side attacks
- Summary

## Chapter 19: Best Practices for the Real World

- Guidelines for penetration testers
- Penetration testing checklist

- Creating a hacker's toolkit
- Setting up remote access
- Next steps ahead
- Summary

## Chapter 20: Appendix

- Setting Up a Penetration Testing Lab on Ubuntu Desktop
- An overview of the lab setup and technologies used
- Setting up a hypervisor and virtual networks
- Setting up Kali Linux on Ubuntu
- Setting up Metasploitable 3 on Ubuntu
- Summary

## Videos and How To

uCertify course includes videos to help understand concepts. It also includes How Tos that help learners in accomplishing certain tasks.

**2**

VIDEOS

**03**

MINUTES

## 9. 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

### **Building a Penetration Testing Lab**

- Setting Up a Vulnerable Web Application

### **Passive Reconnaissance**

- Setting Up TOR Services and TOR Browser on Kali Linux
- Setting Up Proxychains

### **Exploring Open-Source Intelligence**

- Using DNSRecon for DNS Enumeration
- Performing Automation using SpiderFoot
- Exploiting DNS Zone Transfer
- Performing Sub-domain Enumeration with Knockpy
- Performing Enumeration with DNSMap
- Using Netcraft to Profile a Targeted Organization/Domain
- Using theHarvester for Data Collection



## **Active Reconnaissance**

- Changing MAC Address using MAC Changer
- Performing Live Host Discovery

## **Performing Vulnerability Assessments**

- Conducting Vulnerability Scanning Using Nessus
- Performing Vulnerability Scanning Using OpenVAS

## **Understanding Network Penetration Testing**

- Setting Up Bind and Reverse Shells
- Working with Remote Shells Using Netcat

## **Performing Network Penetration Testing**

- Performing Host Discovery on a Targeted Network

## **Post-Exploitation Techniques**

- Working with Impacket for Pass-the-Hash Attack

## **Delving into Command and Control Tactics**

- Performing Penetration Testing with the Empire Server and Starkiller

## **Working with Active Directory Attacks**

- Exploiting SMB
- Exploiting SAM Database

## **Advanced Active Directory Attacks**

- Passing the Hash Using Mimikatz

## **Advanced Wireless Penetration Testing**

- Setting Up a Honeypot on Kali Linux

### Social Engineering Attacks

- Performing a Phishing Attack
- Performing Social Engineering Attack

### Understanding Website Application Security

- Setting Up FoxyProxy for Proxy Configuration
- Exploiting a Website Using SQL Injection

### Advanced Website Penetration Testing

- Identifying Vulnerable and Outdated Components
- Attacking a Website Using XSS Injection
- Performing a Client-Side Attack Using BeEF

## Here's what you get

**30**

LIVE LABS

**30**

VIDEO TUTORIALS

**01:52**

HOURS

You can't stay away! Get



3187 Independence Drive  
Livermore, CA 94551,  
United States



+1-415-763-6300



support@ucertify.com



www.ucertify.com