uCertify

Course Outline

Kali Linux Penetration Testing Bible

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

   Syllabus

   Chapter 1: Introduction

   Chapter 2: Mastering the Terminal Window

   Chapter 3: Bash Scripting

   Chapter 4: Network Hosts Scanning

   Chapter 5: Internet Information Gathering

   Chapter 6: Social Engineering Attacks

   Chapter 7: Advanced Enumeration Phase

   Chapter 8: Exploitation Phase

   Chapter 9: Web Application Vulnerabilities

   Chapter 10: Web Penetration Testing and Secure Software Development Lifecycle

   Chapter 11: Linux Privilege Escalation

   Chapter 12: Windows Privilege Escalation

   Chapter 13: Pivoting and Lateral Movement

   Chapter 14: Cryptography and Hash Cracking

   Chapter 15: Reporting

   Chapter 16: Assembly Language and Reverse Engineering

   Chapter 17: Buffer/Stack Overflow

   Chapter 18: Programming with Python

1. Course Objective

Become an expert in penetration testing with the course Kali Linux Penetration Testing Bible. Designed for red teamers, ethical hackers, and defensive specialists, this course offers interactive lessons, quizzes, and hands-on labs to enhance your skills. Explore the powerful tools of Kali Linux, master pentesting techniques, and gain expertise in digital forensics and reverse engineering. Stay ahead in the field of cybersecurity by learning how to identify vulnerabilities and automate testing.

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. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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

10. 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

- What Does This Course Cover?

Chapter 2: Mastering the Terminal Window

- Kali Linux File System
- Managing Users and Groups in Kali
- Files and Folders Management in Kali Linux
- Remote Connections in Kali
- Kali Linux System Management

- Networking in Kali Linux
- Summary

Chapter 3: Bash Scripting

- Basic Bash Scripting
- Printing to the Screen in Bash
- Variables
- Script Parameters
- User Input
- Functions
- Conditions and Loops
- Summary

Chapter 4: Network Hosts Scanning

- Basics of Networking
- Network Scanning
- DNS Enumeration
- Summary

Chapter 5: Internet Information Gathering

- Passive Footprinting and Reconnaissance
- Summary

Chapter 6: Social Engineering Attacks

- Spear Phishing Attacks
- Payloads and Listeners
- Social Engineering with the USB Rubber Ducky
- Summary

Chapter 7: Advanced Enumeration Phase

- Transfer Protocols
- E?mail Protocols
- Database Protocols
- CI/CD Protocols
- Web Protocols 80/443
- Graphical Remoting Protocols
- File Sharing Protocols

- Summary

Chapter 8: Exploitation Phase

- Vulnerabilities Assessment
- Services Exploitation
- Summary

Chapter 9: Web Application Vulnerabilities

- Web Application Vulnerabilities
- Summary

Chapter 10: Web Penetration Testing and Secure Software Development Lifecycle

- Web Enumeration and Exploitation
- Secure Software Development Lifecycle
- Summary

Chapter 11: Linux Privilege Escalation

- Introduction to Kernel Exploits and Missing Configurations
- Kernel Exploits

- SUID Exploitation
- Overriding the Passwd Users File
- CRON Jobs Privilege Escalation
- sudoers
- Exploiting Running Services
- Automated Scripts
- Summary

Chapter 12: Windows Privilege Escalation

- Windows System Enumeration
- File Transfers
- Windows System Exploitation
- Summary

Chapter 13: Pivoting and Lateral Movement

- Dumping Windows Hashes
- Pivoting with Port Redirection
- Summary

Chapter 14: Cryptography and Hash Cracking

- Basics of Cryptography
- Cracking Secrets with Hashcat
- Summary

Chapter 15: Reporting

- Overview of Reports in Penetration Testing
- Scoring Severities
- Report Presentation
- Summary

Chapter 16: Assembly Language and Reverse Engineering

- CPU Registers
- Assembly Instructions
- Data Types
- Memory Segments
- Addressing Modes
- Reverse Engineering Example

- Summary

Chapter 17: Buffer/Stack Overflow

- Basics of Stack Overflow
- Stack Overflow Exploitation
- Summary

Chapter 18: Programming with Python

- Basics of Python
- Running Python Scripts
- Debugging Python Scripts
- Practicing Python
- Python Basic Syntaxes
- Variables
- More Techniques in Python
- Summary

Chapter 19: Pentest Automation with Python

- Penetration Test Robot

- Summary

Chapter 20: APPENDIX A: Kali Linux Desktop at a Glance

- Downloading and Running a VM of Kali Linux
- Kali Xfce Desktop
- Summary

Chapter 21: APPENDIX B: Building a Lab Environment Using Docker

- Docker Technology
- Summary

Chapter 22:

11. Practice Test

Here's what you get

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.

12. 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

Mastering the Terminal Window

- Managing Users Using Users Commands
- Changing the Permissions of a File Using the chmod Command

Network Hosts Scanning

- Performing Port Scanning and Identifying Live Hosts

- Performing Zone Transfer Using dig

Internet Information Gathering

- Using Maltego
- Using Google Hacking Database (GHDB)
- Using Shodan to Find Webcams
- Using the Information Gathering Tool

Social Engineering Attacks

- Gathering Information Using the Social Engineering Toolkit
- Analyzing Malware Using VirusTotal
- Creating Reverse and Bind Shells Using Netcat

Advanced Enumeration Phase

- Performing Session Hijacking Using Burpsuite

Exploitation Phase

- Performing Vulnerability Scanning Using OpenVAS
- Searching Exploits Using searchsploit
- Securing the FTP Service
- Using the msfvenom Program

Web Application Vulnerabilities

- Exploiting Local File Inclusion and Remote File Inclusion Vulnerabilities
- Conducting Cross-Site Request Forgery Attacks
- Exploiting Command Injection Vulnerabilities
- Exploiting a Website Using SQL Injection
- Attacking a Website Using XSS Injection

Linux Privilege Escalation

- Creating a Shell Script and cron Job

Windows Privilege Escalation

- Using Basic Enumeration Commands
- Displaying Networking Information
- Using Meterpreter to Display the System Information

Pivoting and Lateral Movement

- Using Mimikatz
- Cracking Passwords Using Cain and Abel

Cryptography and Hash Cracking

- Performing Symmetric Encryption
- Examining Asymmetric Encryption
- Observing a SHA256-Generated Hash Value
- Observing an MD5-Generated Hash Value

Pentest Automation with Python

- Finding Live Hosts by Using the Ping Sweep in Python

Here's what you get

32	32	59
LIVE LABS	VIDEO TUTORIALS	MINUTES

GET IN TOUCH:

3187 Independence Drive
Livermore, CA 94551,
+1-415-763-6300
support@ucertify.com
www.ucertify.com