uCertify

Penetration Testing Essentials

Lesson

Practice test

08 Jun 2023

8. 1 Introduction

   2 Introduction to Penetration Testing

   3 Introduction to Operating Systems and Networking

   4 Introduction to Cryptography

   5 Outlining the Pen Testing Methodology

   6 Gathering Intelligence

   7 Scanning and Enumeration

   8 Conducting Vulnerability Scanning

   9 Cracking Passwords

   10 Retaining Access with Backdoors and Malware

   11 Reporting

   12 Working with Defensive and Detection Systems

   13 Covering Your Tracks and Evading Detection

   14 Detecting and Targeting Wireless

   15 Dealing with Mobile Device Security

   16 Performing Social Engineering

   17 Hardening a Host System

   18 Hardening Your Network

   19 Navigating the Path to Job Success

   20 Building a Test Lab for Penetration Testing

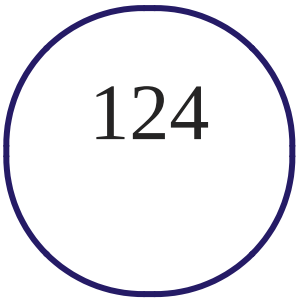
10.

1

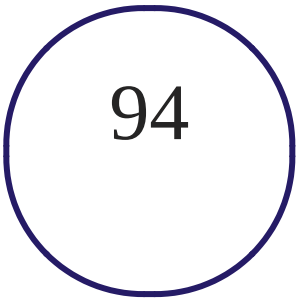
Master the concepts of IT penetration testing with the Penetration Testing Essentials course. The Penetration Testing Training offers an understanding of topics such as scanning and enumeration, intelligence gathering, cracking password, cryptography, reporting, retaining access with backdoors and malware, working with defensive and detecting sections, and many more. This penetration testing course will help you learn about the various ethical hacking methods currently being used on the front lines.

2

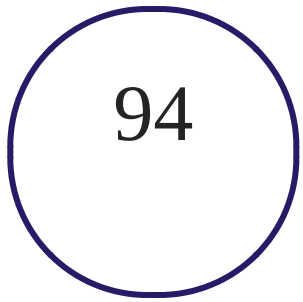
3



4



5



6

7

8

-

9

- **2014**
    1.
- **2015**
    4.
- **2016**

- **2017**
  3.
  4.
- **2018**
  3.
- **2019**
  3.
- **2020**
  3.

10

1: Introduction

2: Introduction to Penetration Testing

- Defining Penetration Testing
- Preserving Confidentiality, Integrity, and Availability
- Appreciating the Evolution of Hacking

3: Introduction to Operating Systems and Networking

- Comparing Common Operating Systems
- Exploring Networking Concepts

4: Introduction to Cryptography

- Recognizing the Four Goals of Cryptography
- The History of Encryption
- Speaking Intelligently About Cryptography
- Comparing Symmetric and Asymmetric Cryptography
- Transforming Data via Hashing
- A Hybrid System: Using Digital Signatures
- Working with PKI

5: Outlining the Pen Testing Methodology

- Determining the Objective and Scope of the Job
- Choosing the Type of Test to Perform
- Gaining Permission via a Contract
- Following the Law While Testing

6: Gathering Intelligence

- Introduction to Intelligence Gathering
- Examining a Company's Web Presence

- Finding Websites That Don't Exist Anymore
- Gathering Information with Search Engines
- Targeting Employees with People Searches
- Discovering Location
- Do Some Social Networking
- Looking via Financial Services
- Investigating Job Boards
- Searching Email
- Extracting Technical Information

7: Scanning and Enumeration

- Introduction to Scanning
- Checking for Live Systems
- Performing Port Scanning
- Identifying an Operating System
- Scanning for Vulnerabilities
- Using Proxies (Or Keeping Your Head Down)
- Performing Enumeration

8: Conducting Vulnerability Scanning

- Introduction to Vulnerability Scanning
- Recognizing the Limitations of Vulnerability Scanning
- Outlining the Vulnerability Scanning Process
- Types of Scans That Can Be Performed

9: Cracking Passwords

- Recognizing Strong Passwords
- Choosing a Password-Cracking Technique
- Executing a Passive Online Attack
- Executing an Active Online Attack
- Executing an Offline Attack
- Using Nontechnical Methods
- Escalating Privileges

10: Retaining Access with Backdoors and Malware

- Deciding How to Attack

- Installing a Backdoor with PsTools
- Opening a Shell with LAN Turtle
- Recognizing Types of Malware
- Launching Viruses
- Launching Worms
- Launching Spyware
- Inserting Trojans
- Installing Rootkits

11: Reporting

- Reporting the Test Parameters
- Collecting Information
- Highlighting the Important Information
- Adding Supporting Documentation
- Conducting Quality Assurance

12: Working with Defensive and Detection Systems

- Detecting Intrusions

- Recognizing the Signs of an Intrusion
- Evading an IDS
- Breaching a Firewall
- Using Honeypots: The Wolf in Sheep's Clothing

13: Covering Your Tracks and Evading Detection

- Recognizing the Motivations for Evasion
- Getting Rid of Log Files
- Hiding Files
- Evading Antivirus Software
- Evading Defenses by Entering Through a Backdoor
- Using Rootkits for Evasion

14: Detecting and Targeting Wireless

- An Introduction to Wireless
- Breaking Wireless Encryption Technologies
- Conducting a Wardriving Attack
- Conducting Other Types of Attack

- Choosing Tools to Attack Wireless
- Knocking Out Bluetooth
- Hacking the Internet of Things (IoT)

15: Dealing with Mobile Device Security

- Recognizing Current-Generation Mobile Devices
- Working with Android OS
- Working with Apple iOS
- Finding Security Holes in Mobile Devices
- Encountering Bring Your Own Device (BYOD)
- Choosing Tools to Test Mobile Devices

16: Performing Social Engineering

- Introduction to Social Engineering
- Exploiting Human Traits
- Acting Like a Social Engineer
- Targeting Specific Victims
- Leveraging Social Networking

- Conducting Safer Social Networking

17: Hardening a Host System

- Introduction to Hardening
- Three Tenets of Defense
- Creating a Security Baseline
- Hardening with Group Policy
- Hardening Desktop Security
- Backing Up a System

18: Hardening Your Network

- Introduction to Network Hardening
- Intrusion Detection Systems
- Firewalls
- Physical Security Controls

19: Navigating the Path to Job Success

- Choosing Your Career Path

- Build a Library
- Practice Technical Writing
- Display Your Skills

20: Building a Test Lab for Penetration Testing

- Deciding to Build a Lab
- Considering Virtualization
- Getting Starting and What You Will Need
- Installing Software

11

50	1	50
PRE-ASSESSMENTS QUESTIONS	**FULL LENGTH TESTS**	**POST-ASSESSMENTS QUESTIONS**

12

support@ucertify.com