



# CompTIA PenTest+ Course Outline



# ERIC REED

CYBERSECURITY TRAINING  
PASS ON THE FIRST ATTEMPT!™



## COMPANY OVERVIEW

For over 25 years, Eric Reed Cybersecurity Training has been a trusted leader in cybersecurity education, equipping more than 60,000 professionals with the skills needed to defend against emerging cyber threats. Our mission is to empower individuals and organizations with comprehensive, hands-on training that translates directly to real-world success. Recognized with multiple industry awards—including an unprecedented 10-time EC Council Instructor of the Year and 7-time Circle of Excellence honoree—we combine innovative delivery methods with a passion for excellence to ensure our students achieve certification success on the first attempt



## COMPTIA PENTEST+

CompTIA PenTest+ is designed for cybersecurity professionals focusing on penetration testing, vulnerability assessment, and ethical hacking.



ONLINE LIVE  
LEARNING



ON-DEMAND  
LIVE LEARNING

## ONLINE LIVE & ON-DEMAND LIVE

All the benefits of live, instructor-led training with the convenience of on-demand.

- **Online Live:** Attend our scheduled sessions in real time (Monday–Friday). Get immediate interaction with the instructor and fellow students.
- **On-Demand Live:** Access recordings of the most recent live sessions on your own schedule, while still having direct instructor support.
- **Flexible Scheduling:** Choose a structured approach—one-week bootcamp (M–F), two nights a week for five weeks, or every Saturday for five weeks. Need more wiggle room? Adjust any schedule to fit your lifestyle!



## COURSE OBJECTIVES

- Conduct reconnaissance and vulnerability assessments.
- Perform penetration testing on networks, applications, and devices.
- Exploit security vulnerabilities and document findings.
- Implement security countermeasures based on test results.
- Report and communicate penetration test results effectively.



## SALARY RANGE

PenTest+ → \$90,000 - \$125,000

*These figures are approximate and depend on location, experience, and job role. Higher salaries are usually seen in major tech hubs and with significant experience.*



## JOB ROLES

- Penetration Tester
- Red Team



*"It's was a great class that covered all aspects of security. Most importantly, I appreciate the fact that you are giving up your own time to assist us and maintain a sharedrive with the latest security tools and informative papers even after the class is over. I was able to pass the test after one week of attending the training."*

*-Shadi Ehalabi*

## Contact Us

- 📞 (707) 722-7333
- ✉ info@ericreedlive.com
- 📍 1401 61st St S  
Gulfport, FL 33707



[WWW.LINKEDIN.COM/IN/ERICREEDLIVE/](https://www.linkedin.com/in/ericreedlive/)



# CompTIA PenTest+ Course Outline



## COMPTIA PENTEST+ COURSE OUTLINE

### 1 - Scoping Organizational/Customer Requirements

- Define Organizational PenTesting
- Acknowledge Compliance Requirements
- Compare Standards and Methodologies
- Describe Ways to Maintain Professionalism



### 2 - Defining the Rules of Engagement

- Assess Environmental Considerations
- Outline the Rules of Engagement
- Prepare Legal Documents



### 3 - Footprinting and Gathering Intelligence

- Discover the Target
- Gather Essential Data
- Compile Website Information
- Discover Open-Source Intelligence Tools



### 4 - Evaluating Human and Physical Vulnerabilities

- Exploit the Human Psyche
- Summarize Physical Attacks
- Use Tools to Launch a Social Engineering Attack



### 5 - Preparing the Vulnerability Scan

- Plan the Vulnerability Scan
- Detect Defenses
- Utilize Scanning Tools



### 6 - Scanning Logical Vulnerabilities

- Scan Identified Targets
- Evaluate Network Traffic
- Uncover Wireless Assets



### 7 - Analyzing Scanning Results

- Discover Nmap and NSE
- Enumerate Network Hosts
- Analyze Output from Scans



### 8 - Avoiding Detection and Covering Tracks

- Evade Detection
- Use Steganography to Hide and Conceal
- Establish a Covert Channel



### 9 - Exploiting the LAN and Cloud

- Enumerate Hosts
- Attack LAN Protocols
- Compare Exploit Tools
- Discover Cloud Vulnerabilities
- Explore Cloud-Based Attacks



# CompTIA PenTest+ Course Outline



## 10 - Testing Wireless Networks

Discover Wireless Attacks

Explore Wireless Tools



## 11 - Targeting Mobile Devices

Recognize Mobile Device Vulnerabilities

Launch Attacks on Mobile Devices

Outline Assessment Tools for Mobile Devices



## 12 - Attacking Specialized Systems

Identify Attacks on the IoT

Recognize Other Vulnerable Systems

Explain Virtual Machine Vulnerabilities



## 13 - Web Application-Based Attacks

Recognize Web Vulnerabilities

Launch Session Attacks

Plan Injection Attacks

Identify Tools



## 14 - Performing System Hacking

System Hacking

Use Remote Access Tools

Analyze Exploit Code



## 15 - Scripting and Software Development

Analyze Scripts and Code Samples

Create Logic Constructs

Automate Penetration Testing



## 16 - Leveraging the Attack: Pivot and Penetrate

Test Credentials

Move Throughout the System

Maintain Persistence



## 17 - Communicating During the PenTesting Process

Define the Communication Path

Communication Triggers

Use Built-In Tools for Reporting



## 18 - Summarizing Report Components

Identify Report Audience

List Report Contents

Define Best Practices for Reports



## 19 - Recommending Remediation

Employ Technical Controls

Implement Administrative and Operational Controls

Apply Physical Controls



## 20 - Performing Post-Report Delivery Activities

Conduct Post-Engagement Cleanup

Execute Follow-Up Actions