LIONFISH CYBER SECURITY™
Training Center

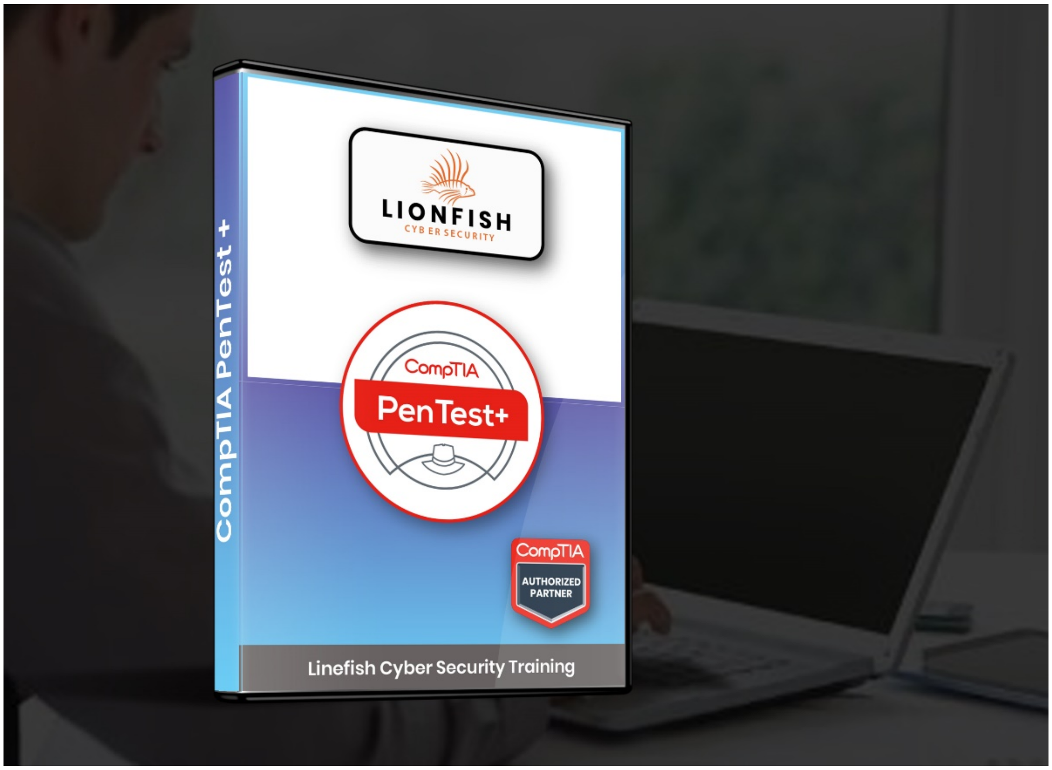
CompTIA AUTHORIZED PARTNER

Lionfish Cyber Security Course Syllabus:

CompTIA PenTest+ (PT0-001)

Interactive and entertaining talk-show style format presented by industry leading experts.

- 40+ hours of virtual training, practice exams and study.
- Receive a Certificate of completion
- Presented by highly qualified, industry leading experts
- 12 Months Access *(Unless indicated otherwise)*
- * The CompTIA bundle comes with practice exams.



Description

CompTIA PenTest+ assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks.

Curriculum Overview

CompTIA PenTest+ is for cybersecurity professionals tasked with penetration testing and vulnerability management. CompTIA PenTest+ is the only penetration testing exam taken at a Pearson VUE testing center with both hands-on, performance-based questions and multiple-choice, to ensure each candidate possesses the skills, knowledge, and ability to perform tasks on systems. PenTest+ exam also includes management skills used to plan, scope, and manage weaknesses, not just exploit them. PenTest+ is unique because our certification requires a candidate to demonstrate the hands-on ability and knowledge to test devices in new environments such as the cloud and mobile, in addition to traditional desktops and servers. CompTIA PenTest+ assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks. Successful candidates will have the intermediate skills required to customize assessment frameworks to effectively collaborate on and report findings. Candidates will also have the best practices to communicate recommended strategies to improve the overall state of IT security. CompTIA PenTest+ meets the ISO 17024 standard. Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program.

Objectives

- Planning and Scoping Penetration Tests
- Conducting Passive Reconnaissance
- Performing Non-Technical Tests
- Conducting Active Reconnaissance
- Analyzing Vulnerabilities
- Penetrating Networks
- Exploiting Host-Based Vulnerabilities
- Testing Applications
- Completing Post-Exploit Tasks
- Analyzing and Reporting Pen Test Results

Prerequisites

Although not a prerequisite the CompTIA PenTest+ (PT0-001) Certification is aimed at an IT security professional who has:

- Network+, Security+ or equivalent knowledge
- Minimum of 3-4 years of hands-on information security or related experience

Target Audience

This course is designed for IT professionals who want to develop penetration testing skills to enable them to identify information-system vulnerabilities and effective remediation techniques for those vulnerabilities. Target students who also need to offer practical recommendations for action to properly protect information systems and their contents will derive those skills from this course. This course is also designed for individuals who are preparing to take the CompTIA PenTest+ certification exam PT0-001, or who plan to use PenTest+ as the foundation for more advanced security certifications or career roles. Individuals seeking this certification should have three to four years of hands-on experience performing penetration tests, vulnerability assessments, and vulnerability management

Syllabus

	CompTIA PenTest+ (PT0-001)
#	Episode Name
	Introduction to Ethical Hacking & CompTIA PenTest+ (PT0-001)
1	Promo
2	Introduction
	Chapter 1 - Planning and Scoping
1	Planning a Pen Test
2	Rules of Engagement
3	Resources and Budgets
4	Impact and Constraints
5	Support Resources
6	Legal Groundwork
7	Scope Considerations

Chapter 2 - Surveying the Target

Chapter 3 - Selecting Your Attack Vector

21	Persistence and Stealth
	Chapter 4 - Selecting Pen Testing Tools
1	Nmap Scoping and Output Options
2	Pen Testing Toolbox
3	Using Kali Linux
4	Scanners and Credential Tools
5	Code Cracking Tools
6	Open Source Research Tools
7	Wireless and Web Pen Testing Tools
8	Remote Access Tools
9	Analyzers and Mobile Pen Testing Tools
10	Other Pen Testing Tools
11	Using Scripting in Pen Testing
12	Bash Scripting Basics
13	Bash Scripting Techniques
14	PowerShell Scripts
15	Ruby Scripts
16	Python Scripts
17	Scripting Languages Comparison
	Chapter 5 - Reporting and Communication
1	Writing Reports
2	Post Report Activities
3	Mitigation Strategies
4	Communication

Prepare for the CompTIA PenTest+ exam with the excellent practice tests. Enabling you to practice on test questions and assess your skill and knowledge of the material. Get certified the best way

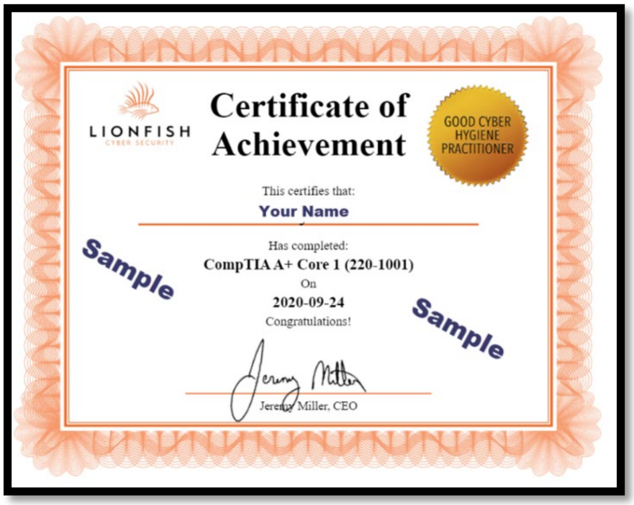
- Applies to the current N10-007 exam
- Includes many practices questions
- Requires Windows, macOS, Chrome OS, or Linux (iOS and Android not supported)
- Single-user license

Learn includes:

- **Interactive learning with flashcards and performance-based questions.**
- **Videos that demonstrate key concepts and processes.**
- **Customizable learning plan.**
- **Easy self-assessments.**
- **Learning progress analytics and reporting.**

LIONFISH
CYBER SECURITY™
Training Center

Sample Certificate upon completions of each course



LIONFISH
CYBER SECURITY

Certificate of Achievement

GOOD CYBER HYGIENE PRACTITIONER

This certifies that:

Your Name

Has completed:

CompTIA A+ Core 1 (220-1001)

On

2020-09-24

Congratulations!

Jeremy Miller

Jeremy Miller, CEO

To learn more, contact us at 877-732-6772 or info@lionfishcybersecurity.com

www.LionfishCyberSecurity.com

LIONFISH
CYBER SECURITY™

This institution is regulated by the Office for Career and Technical Schools - 10 N Senate Avenue, Suite SE 308, Indianapolis 46204 - OCTS@dwd.in.gov
http://www.in.gov/dwd/2731.htm

101 West Ohio Street,
Suite 2000, Indianapolis,
In 46204

CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
RPO
REGISTERED

CMMC-AB Registered Provider Organization™