INFOSEC Boot Camps
CERTIFICATION TRAINING

Get live, expert instruction from anywhere.

CompTIA Pentest+ Boot Camp

This intensive 5-day boot camp is designed for security consultants, penetration testers, vulnerability assessment analysts and IT professionals with 3-4 years of hands-on experience. Through expert-led lectures, interactive discussions and hands-on activities and labs, students will learn valuable information and in-demand skills. This course will help students enhance their penetration testing skill set, allowing them to confidently fulfill their responsibilities in a security consultant or penetration tester role.

Course description

Infosec's authorized CompTIA PenTest+ Boot Camp is an accelerated, in-depth training designed to help students who want to pass their PenTest+ certification exam and build their penetration testing skill set to confidently perform their job.

During this course, students will learn how to:

» Plan and scope a penetration testing engagement
» Perform vulnerability scanning and penetration testing using appropriate tools and techniques and then analyze the results
» Produce a written report containing proposed remediation techniques, effectively communicate results to the management team, and provide practical recommendations

Who should attend

Any professional who has 3-4 years of hands-on experience as a:

» Security consultant
» Penetration tester
» Vulnerability assessment analyst
» IT professional

Boot camp at a glance

What you'll learn

- ✓ Penetration testing engagement planning and execution
- ✓ The vulnerability scanning process
- ✓ Reporting best practices for remediation techniques

Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 5-day boot camp
- ✓ 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Boot Camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to hundreds of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

700+ IT and security courses

Earn CPEs and build new skills with hundreds of additional training courses.

What's included

- 5 days of expert live instruction
- Exam Pass Guarantee
- Exam voucher
- Unlimited practice exam attempts
- 100% Satisfaction Guarantee
- 90-day extended access to Boot Camp components including class recordings
- Free 90-day Infosec Skills subscription (access to 1400+ additional courses and labs)
- Knowledge Transfer Guarantee

Prerequisites

This course does not have any specific prerequisites, but it recommends that students have 3-4 years of hands-on experience in security roles.

CompTIA PenTest+ details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2	Day 3	Day 4	Day 5
Morning session	Introductions Scoping Organizational/ Customer Requirements Defining the Rules of Engagement	Scanning Logical Vulnerabilities Analyzing Scanning Results	Testing Wireless Networks Targeting Mobile Devices	Performing System Hacking Scripting and Software Development	Recommending Remediation Performing Post-Report Delivery Activities
Afternoon session	Footprinting and Gathering Intelligence Evaluating Human and Physical Vulnerabilities Preparing the Vulnerability Scan	Avoiding Detection and Covering Tracks Exploiting the LAN and Cloud	Attacking Specialized Systems Web Application-Based Attacks	Leveraging the Attack: Pivot and Penetrate Communicating During the PenTesting Process Summarizing Report Components	Exam Readiness Activities Q&A and course wrap-up

Schedule may vary from class to class

Before your boot camp

Start learning now. The moment they enroll, students will get immediate access to all the content in Infosec Skills, including an in-depth PenTest+ prep course. This content will help students prepare for the live boot camp, uncover knowledge gaps and maximize their training experience.

During your boot camp

Day 1

- Scoping Organizational/Customer Requirements
  - Define Organizational PenTesting
  - Acknowledge Compliance Requirements
  - Compare Standards and Methodologies
  - Describe Ways to Maintain Professionalism
- Defining the Rules of Engagement
  - Assess Environmental Considerations
  - Outline the Rules of Engagement
  - Prepare Legal Documents
- Footprinting and Gathering Intelligence
  - Discover the Target
  - Gather Essential Data
  - Compile Website Information
  - Discover Open-Source Intelligence Tools
- Evaluating Human and Physical Vulnerabilities
  - Exploit the Human Psyche
  - Summarize Physical Attacks
  - Use Tools to Launch a Social Engineering Attack
- Preparing the Vulnerability Scan
  - Plan the Vulnerability Scan
  - Detect Defenses
  - Utilize Scanning Tools

Day 2

- Scanning Logical Vulnerabilities
  - Scan Identified Targets
  - Evaluate Network Traffic
  - Uncover Wireless Assets
- Analyzing Scanning Results
  - Discover Nmap and NSE
  - Enumerate Network Hosts
  - Analyze Output from Scans

- Avoiding Detection and Covering Tracks
  - Evade Detection
  - Use Steganography to Hide and Conceal
  - Establish a Covert Channe
- Avoiding Detection and Covering Tracks
  - Evade Detection
  - Use Steganography to Hide and Conceal
  - Establish a Covert Channel

Day 3

- Testing Wireless Networks
  - Discover Wireless Attacks
  - Explore Wireless Tools
- Targeting Mobile Devices
  - Recognize Mobile Device Vulnerabilities
  - Launch Attacks on Mobile Devices.
  - Outline Assessment Tools for Mobile Devices
- Attacking Specialized Systems
  - Identify Attacks on the IoT
  - Recognize Other Vulnerable Systems
- Web Application-Based Attacks
  - Recognize Web Vulnerabilities
  - Launch Session Attacks
  - Plan Injection Attacks
  - Identify Tools

Day 4

- Performing System Hacking
  - System Hacking
  - Use Remote Access Tools
  - Analyze Exploit Code
- Scripting and Software Development
  - Analyzing Scripts and Code Samples
  - Create Logic Constructs
  - Automate Penetration Testing
- Leveraging the Attack: Pivot and Penetrate
  - Test Credentials
  - Move Throughout the System
  - Maintain Persistence
- Communicating During the PenTesting Process
  - Define the Communication Path
  - Communication Triggers
  - Use Built-In Tools for Reporting
- Summarizing Report Components
  - Identify Report Audience
  - List Report Contents
  - Define Best Practices for Reports

Day 5

- Recommending Remediation
  - Employ Technical Controls
  - Administrative and Operational Controls
  - Physical Controls
- Performing Post-Report Delivery Activities
  - Post-Engagement Cleanup
  - Follow-up Actions
- Exam Readiness Activities
  - Exam Experience
  - Group Practice Questions
  - Individual Practice Exams

After your boot camp

Students' access to Infosec Skills extends 90 days past their boot camp so they can take additional time to prepare for their exam, get a head start on their next certification goal or earn CPEs.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

INFOSEC