INFOSEC Boot Camps
CERTIFICATION TRAINING

Get live, expert instruction from anywhere.

Certified Penetration Testing Professional (C|PENT) Boot Camp

Master AI-Driven Pentesting with Proven Methodologies for Real-World Success. The C|PENT program enables you to gain mastery in a complete hands-on pen testing methodology and master AI pen testing skills mapped to all pen testing phases.

Course description

The Certified Penetration Testing Professional (C|PENT) is the world's most comprehensive pen testing program with guided learning in labs. Unlike many other certifications, C|PENT covers the complete pen testing methodology from planning, scoping, and rules of engagement to the test execution and report writing phase of a pen testing assignment. The program includes all skill sets required to manage and execute a complete pen test assignment. C|PENT leverages cutting-edge AI tools like ChatGPT, ShellGPT, and PentestGPT to enhance efficiency, automate tasks, and simulate real-world cyber threats. AI techniques are mapped to all technical domains of C|PENT, with unique labs for practical application.

Who should attend

- Penetration Tester
- Penetration Testing Consultant
- Penetration Testing Engineer
- Security Penetration Testing Consultant/Architect
- Vulnerability Assessment and Penetration Testing (VAPT) Analyst/Engineer
- QA Security Tester
- Web Application Penetration Tester
- Vulnerability Assessment Specialist
- Red Team - VAPT Security Consultant
- General Interest audience

Boot camp at a glance

What you'll learn

- Introduction to Penetration Testing and Methodologies
- Penetration Testing Scoping and Engagement
- Open Source Intelligence (OSINT) and Attack Surface Mapping
- Social Engineering Penetration Testing
- Web Application and API Penetration Testing

Delivery methods

- Online

Training duration

- Immediate access to course materials
- 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

- Five days of expert, live instruction in penetration testing
- 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 1,400+ additional courses and labs)
- Knowledge Transfer Guarantee

Prerequisites

Candidates should have strong understanding of networking concepts and protocols, familiarity with Windows and Linux operating systems, and basic scripting knowledge. 2-3 years of information security experience is recommended.

Certification details

The Certified Penetration Testing Professional (CPENT) Exam 412-80 certification features:

Exam Format:

- Duration: 24 Hours or Choose 2 Sessions of 12 Hours Each
- Report Submission: Submit Pentesting Report within 7 Days of Examination
- Test Format: 100% Practical Exam
- Dual Certification: Score more than 90% and get one more certification: Licensed Penetration Tester

Testing Domains: The exam validates skills across five unique multi-disciplinary courses:

- Active Directory (AD) Range
- Binaries Range
- IoT Range
- Web Range
- CTF (Capture the Flag) Range

What you'll learn

- Plan and scope penetration testing engagements with proper ROE and legal considerations
- Conduct reconnaissance using OSINT and AI tools to map attack surfaces and identify vulnerabilities
- Exploit web applications and APIs to uncover injection flaws and authentication weaknesses
- Bypass security controls including firewalls, IDS/IPS, and network filtering devices
- Perform privilege escalation on Windows, Linux, and Active Directory environments
- Execute binary exploitation through reverse engineering and buffer overflow techniques
- Implement lateral movement and pivoting to access segmented and hidden networks
- Document findings in professional reports with risk assessments and remediation recommendations

Learn from experts

We don't just have great instructors, our instructors have years of industry experience and are recognized as experts. Over the past 15 years, we've helped tens of thousands of students get certified and advance their careers.

Skill up and get certified, guaranteed

Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.

100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

C|PENT 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 Introduction to Penetration Testing and Methodologies Penetration Testing Scoping and Engagement	Social Engineering Penetration Testing Web Application Penetration Testing	Perimeter Defense Evasion Techniques	Linux Exploitation and Privilege Escalation Reverse Engineering, Fuzzing & Binary Exploitation	Report Writing and Post Testing Actions
Afternoon session	Open Source Intelligence (OSINT) and Attack Surface Mapping	API and Java Web Token Penetration Testing	Windows Exploitation and Privilege Escalation Active Directory Penetration Testing	Lateral Movement and Pivoting IoT Penetration Testing	Recap & Review Practice Exam

Schedule may vary from class to class

The C|PENT program is aligned with Cyber Kill Chain (CKC) and MITRE ATT&CK frameworks and is globally recognized by organizations like NCSC, NICE, CREST, and more.

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

During your boot camp

Advanced pentesting techniques

- Pivoting & Double Pivoting - Move across hidden networks by identifying filtering rules and manually setting up advanced pivoting techniques
- Privilege Escalation - The latest methods of privilege escalation
- Evasion Techniques - Learn to bypass modern security defenses by weaponizing exploits
- Attack Automation - Master scripting for penetration testing with Python, PowerShell, Bash, and Metasploit
- Weaponizing Exploits - Build custom tools and develop offensive security strategies
- Professional Reporting - Writing pentesting reports is a critical part of the pentesting process
- Advanced Windows Attacks - Gain access to an AD forest, bypass PowerShell defenses, and execute attacks like Silver/Golden Ticket and Kerberoasting
- Attacking IoT Systems - Identify and exploit IoT devices by extracting and reverse-engineering firmware
- Advanced Binary Exploitation - Find vulnerable binaries, reverse engineer them, and write exploits for 32/64-bit programs while bypassing protections
- Bypassing Filtered Networks - Identify segmentation rules, penetrate web zones, and extract critical data

AI skills learned

- Collect and analyze open-source intelligence (OSINT) for reconnaissance
- Automate the network scanning process by generating the script and commands using AI tools
- Identify potential attack surfaces
- Identify and prioritize vulnerabilities across networks, applications, and systems
- Perform various attacks on networks, applications, and systems
- Perform social engineering attacks using AI tools
- Implement AI-driven tools for brute force and dictionary attacks to crack passwords efficiently
- Perform Active Directory enumeration
- Apply AI in reverse engineering to understand binary structures and application flows
- Utilize AI to automate fuzzing processes to identify software bugs and vulnerabilities

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, get a head start on your next certification goal or start earning 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