INFOSEC Skills

LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

GIAC GPEN Training Boot Camp

Infosec offers this five-day accelerated GPEN Boot Camp to train and prepare you for the GIAC® Penetration Tester (GPEN) certification exam, the prestigious security certification created and administered by the Global Information Assurance Certification.

Course description

Our GPEN Boot Camp focuses on preparing you for the GPEN exam through engaging lectures and hands-on exercises. Penetration testing is a critical part of any organization's IT security program and is required by multiple regulations and standards. You'll leave with the ability to discover, assess and mitigate threats to information assets. GPEN holders demonstrate an understanding of penetration-testing methodologies, the relevant legal issues and the ability to properly conduct a penetration test using best practice technical and non-technical techniques.

Our program is designed around the GPEN topic areas and provides you with a quick and proven method for mastering the huge range of knowledge defined in the GPEN Exam Certification Objectives & Outcome Statements. This intense, five-day total immersion training experience is the product of a wide range of leading industry experts and authors, and has a significant return on investment, since you gain pentesting skills that are highly in demand, as well as the GIAC Penetration Tester certification.

Boot camp at a glance

What you'll learn

- ✓ Utilize a process-oriented approach to penetration testing and reporting
- ✓ Obtain and attack password hashes and other password representations
- ✓ Conduct vulnerability scans and analyze the results

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

Who should attend

- Penetration testers
- IT security professionals whose responsibilities involve conducting security assessments
- Ethical hackers
- IT security auditors
- Incident responders and computer forensic investigators
- IT and information security professionals who want to expand their knowledge about offensive security

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

Infosec Skills 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 100s 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 100s of additional training courses.

What's included

- Five days of expert, live GPEN training
- Exam Insurance
- Exam Payment
- Unlimited practice exam attempts
- 100% Satisfaction Guarantee
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- 90-day extended access to all boot camp video replays and materials
- Onsite proctoring of exam
- Knowledge Transfer Guarantee

Prerequisites

- Firm understanding of the Windows operating system
- Basic understanding of Windows and Linux command line
- Working knowledge of computer networking and the TCP/IP protocols
- Basic understanding of cryptographic concepts

What you'll learn

- Penetration testing fundamentals
- Penetration testing process
- Penetration testing methodologies
- Penetration testing steps
- Reporting results
- Reconnaissance phase
- Finding and using publicly available information
- Passive recon methods
- Determining IP ranges
- Scanning tools and techniques
- Port scanning
- OS fingerprinting
- Service version scans
- Advanced scanning techniques
- Vulnerability scanning and mapping
- Types of exploits
- Finding and using exploits
- Metasploit framework components and terminology
- Exploitation process with Metasploit
- Creating and encoding payloads with msfvenom
- Delivering payloads
- Command shell vs. terminal access
- Using meterpreter payload
- Post-exploitation
- Basic password attacks (guessing)
- Obtaining and cracking password hashes
- Advanced password cracking tools and techniques
- Data exfiltration
- File manipulation and movement
- Using Windows command line
- Learning advanced command line skills
- Gathering target system information via command line
- Windows exploitation tools
- Leveraging PowerShell
- PowerShell introduction
- PowerShell capabilities for pentesting
- Advanced port-exploitation techniques with PowerShell
- Web application vulnerabilities overview
- Scanning for web application vulnerabilities
- Using proxies
- Exploiting injection flaws
- Exploiting XSS and CSRF
- Attacking wireless networks
- Wireless networks fundamentals
- Wireless encryption standards
- Wireless pentesting tools and techniques

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.

What our students are saying

I really appreciate that our instructor was extremely knowledgeable and was able to provide the information in a way that it could be understood. He also provided valuable test-taking strategies that I know not only helped me with this exam, but will help in all exams I take in the future.

Michelle Jemmott

Pentagon

Excellent! Our instructor had a vast background and related the materials to real life. Much better than just teaching the materials to pass an exam ... but he did that as well. He went out of his way in class. The extra materials really benefited us when we returned to our real jobs! Great experience!

John Peck

EPA

Very impressed with Infosec. My instructor did a great job delivering the information strategically and in a way for all to understand. I would definitely take another class/certification prep course.

Sylvia Swinson

Texeltek

The instructor was able to take material that prior to the class had made no sense, and explained it in real world scenarios that were able to be understood.

Erik Heiss

United States Air Force

The course was extremely helpful and provided exactly what we needed to know in order to successfully navigate the exam. Without this I am not confident I would have passed.

Robert Caldwell

Salient Federal Solutions

GPEN Boot Camp 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	Introduction Pentesting Process	Exploitation	Windows Command Line	Web App Pentesting	GPEN Exam Review
Afternoon session	Reconnaissance	Post-exploitation	PowerShell	Wireless Pentesting	GPEN Exam Review
Evening session	Optional group & individual study	Optional group & individual study	Optional group & individual study	Optional group & individual study	

Schedule may vary from class to class

Before your boot camp

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

During your boot camp

Day 1: Pentesting and reconnaissance

- Course overview
- Introduction to pentesting
  - Role of penetration tester
  - Penetration testing fundamentals
- Penetration testing process
  - Penetration testing methodologies
  - Penetration testing steps
  - Reporting results
- Reconnaissance phase
  - Finding and using publicly available information
  - Passive recon methods
  - Determining IP ranges
  - Scanning tools and techniques
  - Port scanning
  - OS fingerprinting
  - Service version scans
  - Advanced scanning techniques
  - Vulnerability scanning and mapping

Day 2: Exploitation

- Exploitation phase
  - Types of exploits
  - Finding and using exploits
  - Metasploit framework components and terminology
  - Metasploit modules
  - Exploitation process with Metasploit
  - Creating and encoding payloads with msfvenom
  - Delivering payloads
  - Command shell vs. terminal access
  - Using meterpreter payload
- Post-exploitation
  - Basic password attacks (guessing)
  - Obtaining and cracking password hashes

INFOSEC Skills
LIVE BOOT CAMPS

  - Advanced password cracking tools and techniques
  - Data exfiltration
  - File manipulation and movement

Day 3: Command line and PowerShell

- Using Windows command line
  - Learning advanced command line skills
  - Gathering target system information via command line
  - Windows exploitation tools
- Leveraging PowerShell
  - PowerShell introduction
  - PowerShell capabilities for pentesting
  - Advanced port-exploitation techniques with PowerShell

Day 4: Web app and wireless pentesting

- Web application pentesting
  - Web application vulnerabilities overview
  - Scanning for web application vulnerabilities
  - Using proxies
  - Exploiting injection flaws
  - Exploiting XSS and CSRF
- Attacking wireless networks
  - Wireless networks fundamentals
  - Wireless encryption standards
  - Wireless pentesting tools and techniques

Day 5: Exam review

- GPEN exam review

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