INFOSEC Boot Camps
CERTIFICATION TRAINING

Get live, expert instruction from anywhere.

Ethical Hacking (CEH) Boot Camp

Discover vulnerabilities before the bad guys do! Our most popular information security and hacking training goes in-depth into the techniques used by malicious, black-hat hackers with attention-getting lectures and hands-on labs.

Course description

This boot camp teaches you how to use the tools and techniques used by cybercriminals to perform a white-hat, ethical hack on your organization. You'll learn ethical hacking methodologies and gain hands-on hacking experience in our cloud-hosted cyber range, including reconnaissance, gaining access to systems, exploiting vulnerabilities and exfiltrating data.

You'll leave with the ability to quantitatively assess and measure threats to information assets — and discover where your organization is most vulnerable to hacking. This boot camp also prepares you to earn the highly sought after EC-Council Certified Ethical Hacker (CEH) professional certification.

Who should attend

- Penetration and vulnerability testers
- Cybersecurity analysts
- Cybersecurity consultants
- Offensive security professionals
- Anyone with a desire to learn about ethical hacking and develop their penetration testing skills

Boot camp at a glance

Hands-on training

- Practice your skills in the Ethical Hacking cyber range
- Dozens of hands-on exercises and Capture the Flags (CTFs)
- Compromise web servers, virtual machines, databases, routers and more!

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 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 live, expert ethical hacking instruction
- Exam Pass Guarantee
- Exam voucher
- 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
- Exposure to the Linux Operating System or other Unix-based operating system
- Grasp of the TCP/IP protocols

Learn by doing in the cyber range

Hundreds of exercises in over 20 separate hands-on labs bring you up to speed with the latest threats to which your organization is most vulnerable. Practice penetration testing in our virtualized environment that simulates a full range of servers and services used in a real company. Learn how to compromise web servers, virtual machines, databases, routers and firewalls, and then put it all together in an un-scripted evening Capture the Flag (CTF) exercise.

CTF exercises are an opportunity for you to practice your hacking skills in a real-world environment. Infosec sets up a mock company that you can freely attack without having to worry about damaging production systems. The purpose of the CTF exercises is to ensure you understand how to apply the skills you learned during the day to a real-world, ethical hacking scenario.

Meets 8570.1 requirements

Attention DoD Information Assurance workers! This boot camp helps meet U.S. Department of Defense Directive 8570.1 requirements for department employees or contractors engaged in work related to information security. The directive specifies Certified Ethical Hacker (CEH) as an approved baseline certification for CCSP Analyst, CSSP Infrastructure Support, CSSP Incident Responder, and CSSP Auditor.

Best course evaluations in the industry

Over 98% of Infosec students attending our Ethical Hacking Boot Camp rate it 10 out of 10 stars. Students often report this is the best course they have ever attended, even those with over 20 years of experience in the IT field.

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 have never had a better experience in any previous training. The instructor gave the information needed for the test and also shared his real-world experience to bring it together. I would not hesitate recommending this class to anyone interested in CEH.

Chris Young
Maintech

I thoroughly enjoyed the Ethical Hacking class. I would venture to say it is one of the best technical classes I have ever attended. I feel very confident that I will be able to take my learning experience and be better able to defend our company assets.

Jeremy Kicklighter
ACI Worldwide

The course materials were excellent. The class format was fantastic. The instructor not only prepared us for the examination but also spent a considerable amount of time in learning practical skills for the real world.

Stephen Field
Thomas Compliance Associates, Inc.

GREAT labs. They were relevant to issues faced in the security industry. The classroom instructor had great knowledge and real-world experience to share, which made the class exciting and relevant.

Brian McKee
Runzheimer International

This. Was. Great. Very nice fluctuation of the way and speed the instructor delivered content. Great for me (who has little experience) and great for those who were already skilled in the knowledge/content being delivered. Thanks!

Chalice Ebow
Nexen Petroleum USA

Ethical Hacking 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 to ethical hacking Pentesting process	Network scanning	Exploitation	Deep target penetration and covering tracks	Scripting Post-engagement activities Exam review
Afternoon session	Passive reconnaissance and OSINT	Target system identification, service enumeration and vulnerability scanning	Password security, social engineering, and physical security	Web application attacks	Take CEH exam
Evening session	CTF Exercises	CTF Exercises	CTF Exercises	CTF Exercises	

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 ethical hacking prep course, the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

Day 1

The first half of day one focuses on learning the job duties required of a penetration tester. You will learn the ins and outs of the various penetration testing methodologies required in order for an ethical hack to be used in a business or government setting. You will also delve deep into technical material, learning how to perform network reconnaissance against modern infrastructure.

Lectures include:

- Security testing methodologies
- The ethical hacking profession
- Planning and scoping an engagement
- Legal and compliance considerations
- Ethical hacking methodologies
- Tools of the trade
- Linux overview
- Passive intelligence gathering
- Abusing DNS and SNMP
- Security testing methodologies

Some of the hands-on lab exercises include

- Linux fundamentals
- Passive intelligence gathering
- Understanding the Domain Naming System
- Enumerating DNS entries to develop a focused attack strategy
- Attacking the Domain Naming System
- Discovering SNMP vulnerabilities and flaws
- Enumerating SNMP information
- Brute forcing SNMP community strings
- Capture the Flag exercises

Day 2

Having learned how to gather information about several targets, we begin day two with narrowing our attack by finding potentially vulnerable systems/services. You will master the art of network scanning and service identification, and gain a deeper understanding of how systems communicate using the TCP and UDP protocols.

Lectures include:

- Understanding TCP packets and structures
- Passive network discovery and scanning
- TCP scanning
- Using differences in RFC implementations to your advantage
- Scanning through firewalls
- How to prevent the discovery of your reconnaissance activities
- Using zombies to mask network scanning
- Avoiding IDS/IPS detection
- Proper identification of services
- Vulnerability identification

Some of the hands-on lab exercises include:

- Packet analysis
- Obtaining authentication credentials via packet capture
- Network scanning
- Target scanning of potentially vulnerable targets
- Remaining undetected while performing a network scan
- Enumerating services and identifying vulnerabilities
- Capture the Flag exercises

Day 3

After gathering information about your target system, you will put all that hard work to use when you learn how to exploit those vulnerabilities. You will learn the skills to demonstrate a successful exploit of a vulnerability as well as how to gather additional credentials to exploit vulnerabilities in other systems. You will also learn useful social engineering techniques, including phishing, and methods of attacking physical security.

Lectures include:

- Vulnerability life cycles
- Types of vulnerabilities
- Flaws in encryption
- Configuration errors
- Buffer overflows
- Stack overflows
- Vulnerability mapping
- Exploit utilization and delivery methods
- Client side exploits
- Server side exploits
- Password security
- Social engineering techniques
- Attacking physical controls
- Hashing
- Rainbow tables
- Attacking Windows password security
- Weaknesses in Windows authentication protocols

Some of the hands-on lab exercises include:

- Gaining unauthorized access to systems
- Use of various payloads to increase privileges
- Keystroke logging
- DLL injection attack
- Exploit server side applications
- Gather password hashes
- Exploit weaknesses in authentication protocols
- Capture the Flag exercises

Day 4

After compromising a target, you will extend your access to all vulnerable systems at your target organization and learn how to covertly exfiltrate data. The second half of day four covers attacking web based applications and understanding SQL injection.

Lectures include:

- Use of Trojans
- Redirecting ports to thwart firewall rules
- Avoiding anti-virus detection
- Lateral movement and persistence
- Use of keyloggers
- IDS operations and avoidance
- Encrypting your communications
- Protocol abuse for covert communications
- Creating custom encryption tunneling applications
- E-shoplifting
- XSS attacks
- Cross site forgery
- Circumventing authentication
- SQL injection discovery and exploitation
- SQL data extraction

Some of the hands-on lab exercises include:

- Use of Trojans
- IDS usage and avoidance
- Data transmission encryption techniques
- Creating a custom covert channel
- Web application parameter tampering
- Cross site scripting attacks
- SQL injection
- Chaining exploits
- Exploiting extended stored procedures
- Capture the Flag exercises

Day 5

Day five is dedicated toward wireless security, using basic scripts for ethical hacking, covering your tracks and post-engagement activities. You will master the ability to sniff data, clean up all traces of your activities and learn best practices for writing reports and recommending mitigation strategies.

Lectures include:

- Sniffing in different environments
- Attack sniffers
- Man-in-the-middle attacks
- Wireless networking
- Shared key authentication weaknesses
- WEP/WPA/WPA2 cracking
- Anti-forensics
- Log modification/deletion
- Rootkits
- Introduction to scripting
- Common script components
- Writing effective reports
- Providing mitigation recommendations
- CEH exam review

Some of the hands-on lab exercises include:

- ARP spoofing and man in the middle
- Specialized sniffing
- DNS spoofing
- Phishing attacks

The day finishes with the CEH examination given onsite at the training location or online from home.

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