ETHICAL HACKING BOOT CAMP

COURSE SYLLABUS

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

Delivery Methods
Classroom
Live Online
Mentored Online

Duration
5 Days

Certification
Certified Ethical Hacker

COURSE DESCRIPTION

Our most popular information security and hacking training covers the techniques used by malicious, black hat hackers with high energy lectures and hands-on lab exercises. While these hacking skills can be used for malicious purposes, this class teaches you how to use the same hacking techniques to perform a white-hat, ethical hack, on your organization. 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 in this network security training course.

The goal of this course is to help you master a repeatable, documentable penetration testing methodology that can be used in an ethical penetration testing or hacking situation. This ethical hacking training course has a significant return on investment, since you gain hacking skills that are highly in demand, as well as, the EC-Council Certified Ethical Hacker.

INFOSEC INSTITUTE
866-471-0059

CONSTANTLY UPDATED TRAINING

Black Hat hackers are always changing their tactics to get one step ahead of the good guys. InfoSec Institute updates our course materials regularly to ensure that you learn about the current threats to your organization's networks and systems.

HANDS-ON LABS WITH IN-CLASSROOM EQUIPMENT

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 on 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, firewalls, and then put it all together in an unscripted evening CTF (Capture The Flag) exercise.

NIGHTLY CAPTURE THE FLAG EXERCISES

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

LEARN FROM EXPERTS

We don't just have great instructors, our instructors have years of industry experience and are recognized as experts. InfoSec Institute instructors have authored two of the top Network Security and Ethical Hacking books.

BEST COURSE EVALUATIONS IN THE INDUSTRY

Over 98% of InfoSec Institute students attending our Ethical Hacking course give 10 out of 10 positive feedback. It is quite frequent that we hear that students feel this is the best IT course they have ever attended, even with students with over 20 years of experience in the IT field.

Certified Ethical Hacker

In any hands on hacking training course, it is important to have the opportunity to prove to current or potential employers that you have the skills you say you do. This course prepares you for the top hacking certification in the industry, the CEH. The exam is given on-site, we have achieved a 93% pass rate for these certifications. Contact us to learn more about the requirements for the Certified Ethical Hacker.

We make sure you are fully prepared to pass the CEH. InfoSec Institute goes way beyond the material covered in the CEH to give you a more well-rounded exposure to hacking and penetration testing.

INFOSEC
INSTITUTE

866-471-0059

IDC lists InfoSec Institute as a Major Player in their Security Training Vendor Assessment.

"The quality of its instructors and training materials are viewed as the best of all vendors, as are its options for on-site and self-paced training. In addition, InfoSec Institute is perceived to be the best vendor for certification test preparation, classroom locations, facilities, and practice labs."

IDC Analyze the Future

"The real-time hands-on knowledge made the training more meaningful. Students were able to practice the skills and knowledge in the lab time and bring them back to their working environment. Thank you!"

YIDING EDWARD LI

ETHICAL HACKING BOOT CAMP (CEH V9)

PREREQUISITES

- Firm understanding of the Windows Operating System
- Exposure to the Linux Operating System or other Unix-based OS
- Grasp of the TCP/IP protocols
- Desire to learn about the hacking and network security profession, stay ethical, and get great security training!

CERTIFIED ETHICAL HACKING VERSION 10 COURSE SCHEDULE

Schedule	Day 1	Day 2	Day 3	Day 4	Day 5
8:30 - 12:30	Introduction to Ethical Hacking Information Gathering	Network Scanning	Exploitation	Deep Target Penetration and Covering Tracks	Penetration Testing Final Review
12:30	Lunch Provided	Lunch Provided	Lunch Provided	Lunch Provided	Lunch Provided
1:30 - 5:30	Using and Abusing DNS and SNMP	Target System Identification and Service Enumeration	Password Security	Web Application Attacks	CEH Exam Return Home
5:30 - 7:00	Break	Break	Break	Break	
7:00 - 10:00	CTF Exercises	CTF Exercises	CTF Exercises	CTF Exercises	

SCHEDULE MAY VARY FROM CLASS TO CLASS

WHAT'S INCLUDED

- Guaranteed access to Expert Instruction in an intimate learning setting not offered at any of our competitors.
- Boot camp style training - Course runs from 8am to 5pm daily with optional ethical hacking capture the flag exercises to 10:30pm.
- Certified Ethical Hacker exam fee.
- Lecture, Lab Exercise and Text book --- Share your new skills with friends and colleagues!

INFOSEC INSTITUTE

866-471-0059

ETHICAL HACKING COURSE DETAILS

Day 1 - Penetration Testing and Network Reconnaissance

The first half of Day 1 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. Some of the Day 1 lectures include:

Security testing methodologies:

- The Ethical Hacking Profession
- Ethical Hacking Methodologies
- Tools of the Trade
- Linux Overview
- Passive Intelligence Gathering
- Abusing DNS
- Abusing SNMP
- Security testing methodologies

Some of the instructor-led hands-on lab exercises:

- 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 - Network Scanning, Target System Identification, and Service Enumeration

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, service identification, and 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 for Day 2 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 - The Art of Exploitation and Password Security

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. 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
- Hashing
- Rainbow tables
- Attacking Windows password security
- Weaknesses in Windows authentication protocols
- Rainbow tables

ETHICAL HACKING COURSE DETAILS (CONTINUED)

Some of the hands-on lab exercises for Day 3 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!

Day 4 - Deep Target Penetration, Concealing our activities, and Web application attacks

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 4 covers attacking web based applications and understanding SQL injection. Lectures include:

- Use of Trojans
- Redirecting ports to thwart firewall rules
- Avoiding anti-virus detection
- 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
- CEH exam review

Some of the hands-on lab exercises for Day 4 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!

Day 5 - Web Application Hacking

Day 5 is dedicated toward wireless security, social engineering, and covering your tracks. You will master the ability to sniff data, trick users into giving you access to systems, and cleaning up all traces of your activities. 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

Some of the hands-on lab exercises for Day 5 include:

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

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

LIVE ONLINE TRAINING PLATFORM

InfoSec Institute provides the highest quality Live Online training offering in the industry. With our Live Online training courses, our goal has been to provide the exact same learning experience as our traditional classroom based courses.

In our Live Online courses, you directly learn from and interact with a live expert instructor, the same as you would if you attended the physical classroom course. The InfoSec Institute instructor is there to explain topics in greater detail, answer your questions, and provide personalized study and training plans for you as you progress through the course.

Some key advantages of InfoSec Institute's Live Online Training:

1. Exact same learning experience as being in a physical classroom class
2. Same courseware, labs, exam vouchers as classroom course delivered to you at no extra charge
3. Save on travel expenses, and train from the comfort of your home or work
4. High quality HD webcasting solution
5. Dedicated Live Online Facilitator available for entirety of your training course
6. Free re-sit guarantee – don't pass your exam, come back and re-sit the course for free

CORPORATE ON-SITE DISCOUNTS

Get ethical hacking training on-site for a fraction of the price of our publicly scheduled boot camps with 10 or more students!

Industry Recognition

These are just a few of the awards we've received.

InfoSec Institute's 100% Satisfaction & Human Capital Guarantee

InfoSec Institute is committed to you having the best possible training experience available. We offer students the opportunity to re-sit a Classroom-based or Live Online course tuition-free for up to one year or until the student obtains certification, whichever comes first. Our Human Capital Guarantee ensures a successful return on investment for employers. If an employer has paid the cost of a class for an employee who leaves within three (3) months of obtaining certification, InfoSec Institute will train an additional employee of the company at no tuition cost to the employer for up to 12 months. Any employer may request their InfoSec Institute graduate re-sit the course tuition-free within three (3) months of the completed training if the employee is not successfully performing a job duty related to the class that was taken.

INFOSEC
INSTITUTE

866-471-0059

AWARD WINNING TRAINING

- 2016 EC-Council Circle of Excellence
- 2016 TrainingIndustry.com - Top 20 IT Training Company
- 2015 TrainingIndustry.com - Top 20 IT Training Company
- 2014 TrainingIndustry.com - Top 20 IT Training Company
- 2014 Golden Bridge Award - Training and Education Innovation
- 2013 TrainingIndustry.com - Top 20 IT Training Company – WINNER
- 2013 SC Magazine Best Professional Training Program
- 2013 Golden Bridge Award - Training and Education Innovation
- 2013 Virtualization Review Reader's Choice Awards - Editor's Choice WINNER
- 2012 TrainingIndustry.com - Top 20 IT Training Company - WINNER
- 2012 Info Security Products Guide - Global Excellence - WINNER
- 2011 TrainingIndustry.com Top 20 IT Training Company
- 2011 SC Magazine Best Professional Training Program
- 2011 Global Excellence in Security Training - WINNER
- 2010 Best Professional Training Program - Finalist
- 2009 EC-Council ATC of the Year Award - "#1 Authorized Training Center in North America"
- 2009 EC-Council Instructor of the Year Award
- 2009 Best Professional Training Program - Finalist
- 2009 Global Excellence in Security Training - WINNER Security Products Awards
- 2008 Best Professional Training Program - Finalist
- 2008 Global Excellence in Security Training - WINNER
- 2007 Best Professional Training Program – Finalist
- 2006 Best Instructor Led Training Winner
- 2006 1st Runner up in the MCSE 2003 Boot Camp Category
- 2006 2nd Runner up in the CCNA Boot Camp Category
- 2005 Best Security Training Program SC Awards
- 2004 Best Instructor Led Training Windows IT Pro

"I am so impressed with my instructor and InfoSec CEH course. I started the course with minimal knowledge of the material, mainly self taught basics, and I am now leaving the class with gratification that I truly learned and grew knowledge that can be applied. Great course material! This course is well designed with abundant tools to help engage in the course and continue to learn the subject matter after the completion of the class. You will succeed not only in passaging the certification exams but also in applying what you learned in real life scenarios. InfoSec provides a course text book that utilizes and expands on the teachers slides, a step by step Lab Manual that gives you hands on experience of what you are learning, there is software given on disks to the students that allows students to continue practicing with the tools used in class, and the practice test questions truly help prepare for the test."

HELENE DAAGE

ETHICAL HACKING BOOT CAMP (CEH V9)

INFOSEC INSTITUTE

866-471-0059