- HOME
- INFORMATION SECURITY TRAINING
- ETHICAL HACKING

# ETHICAL HACKING Boot Camp (CEH v7)

**SEC-200** 

"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 lab exercises"



#### WHAT'S ON THIS PAGE?

- Course Overview
- What You'll Learn
- Dates & Locations
- What Students Are Saying
- Certification & Compliance
- Prerequisites & Related Courses
- Pricing (What's Included?)

#### **GET QUOTE**

## **Ethical Hacking Course Overview**

COURSE LENGTH:

5-DAY

**CERTIFICATIONS:** 

**CEH** 

Our most popular information security and hacking training goes in-depth into the techniques us ed by malicious, black hat hackers with attention gettig 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 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.

#### The most current, up-to-date Ethical Hacking training available anywhere!

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 most current threats to your organization's networks and systems.

#### Learn from Experts in the field of Information Security:

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

#### FEATURED IN













Created and taught by Best-selling Industry Authors

- Over 90% Pass Rate Now CEHv7
- · On-site exam proctoring
- Over \$3000 in tools & software(details)

## FIND OUT PRICING ON-SITES OFFERED

"I was blown away by the instructor's knowledge and expertise. ... Would recommend to anyone thinking about being a pen tester"

#### **Connie Brown**

United States Air Force



#### What You'll LEARN

Run hacking attacks in our classroom labs, be a hacker for a week: Some of the hacking concepts you will learn to master during this hands on hacking course...

- Penetration testing methodologies
- · Stealthy network recon
- · Passive traffic identification
- Remote root vulnerability exploitation
- · Privilege escalation hacking
- IPv6 Vulnerabilities
- · Remote access trojan hacking
- Running shellcode in RAM vs. on disk
- · Wireless insecurity
- · Breaking IP-based ACLs via spoofing
- Abusing Windows Named Pipes for Domain Impersonation
- Evidence removal and anti-forensics
- · Attacking network infrastructure devices
- · Hacking by brute forcing remotely
- Hiding exploit payloads in jpeg and gif image files
- · Hacking Web Applications
- · Breaking into databases with SQL Injection
- · Cross Site Scripting hacking
- · Hacking into Cisco routers
- · Justifying a penetration test to management & customers
- CEH/CPT review
- Defensive techniques

#### What You'll DO

Some of the instructor-led hands-on hacking lab exercises in this security training experience:

- Capture the Flag hacking exercises every night!
- · Abusing DNS for host identification
- · Leaking system information from Unix and Windows
- Windows 2003 Server & Vista DNS Cache Poisoning Attacks
- · Unix, Windows and Cisco password cracking
- Remote buffer overflow exploit lab heap vs. stack overflows
- · Attacking Kerberos Pre-Auth Hashes
- Spoofing endpoints of communication tunnels
- Impersonation of other Users- Hijacking kernel tokens
- Attacking RDP (Remote Desktop Protocol) in Windows XP, 2003 & Vista
- Remote keylogging
- · Data mining authentication information from clear-text protocols
- Sniffing and hijacking SSL encrypted sessions
- · Breaking wireless security via hacking
- Malicious event log editing
- Client side IE & Firefox exploits
- Tunneling through IPSec VPNs by abusing ESP
- · Data retrieval with SQL Injection Hacking
- Calculating the Return on Investment (ROI) for an ethical hack

#### **Dates & Locations**

<u>Dates</u>	<u>Location</u>	Reserve a Seat!
Any Date!	Any Location!	Hacker Training Online - More Details Here
07/22/13-07/26/13	Dallas, TX	Reserve a Seat
07/22/13-07/26/13	Dulles, VA	Reserve a Seat
07/22/13-07/26/13	Live Online,	Reserve a Seat
07/29/13-08/02/13	Las Vegas, NV	Reserve a Seat
08/05/13-08/09/13	Orlando, FL	Reserve a Seat
08/12/13-08/16/13	Live Online,	Reserve a Seat
08/12/13-08/16/13	Dulles, VA	Reserve a Seat
08/26/13-08/30/13	Chicago, IL	Reserve a Seat

09/09/13-09/13/13	Dulles, VA	Reserve a Seat
09/09/13-09/13/13	Live Online,	Reserve a Seat
09/16/13-09/20/13	Colorado Springs, CO	Reserve a Seat
09/23/13-09/27/13	San Diego, CA	Reserve a Seat
09/23/13-09/27/13	Baltimore, MD	Reserve a Seat
10/07/13-10/11/13	Live Online,	Reserve a Seat
10/07/13-10/11/13	Dulles, VA	Reserve a Seat
10/21/13-10/25/13	Atlanta, GA	Reserve a Seat
10/21/13-10/25/13	Baltimore, MD	Reserve a Seat
11/04/13-11/08/13	Live Online,	Reserve a Seat
11/04/13-11/08/13	New York City, NY	Reserve a Seat
11/04/13-11/08/13	Dulles, VA	Reserve a Seat
11/04/13-11/08/13	Chicago, IL	Reserve a Seat
11/11/13-11/15/13	Dallas, TX	Reserve a Seat
11/18/13-11/22/13	Baltimore, MD	Reserve a Seat
12/02/13-12/06/13	Orlando, FL	Reserve a Seat
12/09/13-12/13/13	Live Online,	Reserve a Seat
12/09/13-12/13/13	Dulles, VA	Reserve a Seat
12/16/13-12/20/13	Colorado Springs, CO	Reserve a Seat
01/04/31-01/04/31	Online,	Reserve a Seat
Any Date	Your Office!	Get Information for On-Site Training

#### The best in the world come train with us



**Ethical Hacking Locations Added Regularly** 

## See what our students are saying

More testimonials for Certified Ethical Hacker here

Booz | Allen | Hamilton

David P. Curly

Senior Consultant

Booz Allen Hamilton

"a must for any true

security professional"

"This was a phenomenal class! The instructor was extremely knowledgeable and crafted the exercises so that we truly learned the material. I have a whole new appreciation for how vulnerabilities are exploited. I have gained very practical skills and knowledge in this class which will help me tremendously in my job. I will highly recommend this course to all of my co-workers. This class should be a must for any true security professional. There were several moments during the week when I was amazed at how vulnerable systems truly are. The practical

labs and competition teams made the experience fun. I have learned some extremely valuable skills."

Find out more



#### **Aaron Bento**

**IBM Global Services** 

#### "hands-on experience was invaluable"

"The class was great! The instructor knew his his information very well. It was nice to have someone who is more than just book knowledge, someone who is just giving you the info for the cert test. His hands on experience in real world pen-testing was invaluable, as it gave a touch-stone to how the methods learned in class can be extended to real pen-testing."

Find out more



#### Virgil Sabas

SAIC

#### "nice to have a dedicated training laptop provided"

"I got a lot out of the real world scenarios presented in class. Jeremy is very knowledgeable in the field of penetration testing. Would definitely take classes again if he is the instructor. The course books are a great reference, and it was nice to have a dedicated training laptop provided by Infosec and not have to bring my own and waste time installing programs during class"

Find out more



#### Rummy Dabgotra

MTS Allstream

#### "invaluable to my career"

"Dan is an excellent instructor and incredibly knowledgeable. Great presenter and very helpful. The course was very intense but well structured. The hours were long but it really allows you to get your head wrapped around it. Slide notes were very good as well as the lab pre-info. The labs tied well into the course. The content and knowledge gained will be invaluable to my career."

Find out more

## **Certifications & Compliance**

#### Certified Ethical Hacker (CEH v8)



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 two hacking certification in the industry, the CEH. The exam is given on-site and we have achieved a 93% pass rate.

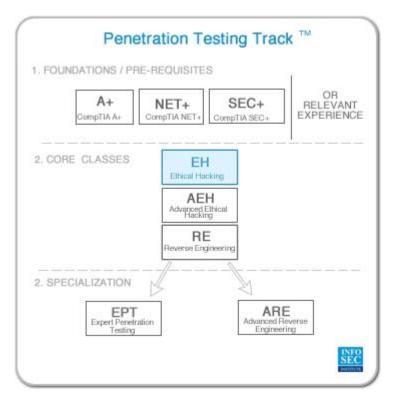
We make sure you are fully prepared to pass the <u>CEH v8</u>. InfoSec Institute goes way beyond the material covered in the CEH to give you a more well-rounded exposure to hacking and penetration testing.

Pricing for Certifed Ethical Hacker - including the CEH v7





## Related Courses, Tracks, & Prerequisites



#### 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!

#### Who This Class is For:

- Security Analyst
- Security Consultant
- Security Researcher

#### **Core Classes:**

- Ethical Hacking (SEC-200)
- Advanced Ethical Hacking (SEC-300)
- Reverse Engineering Malware (SEC-303)

#### Specialization:

- Advanced Reverse Engineering Malware (SEC-503)
- Web App Pen Testing (SEC-402)

See pricing & availability for Ethical Hacking (SEC-200) below

### **Instant Pricing**

Call (866)-471-0059 or fill out this short form for current pricing

#### YOU ALSO GET



\$3000 worth of tools and software!

InfoSec's Custom Hacking Tools Enterprise Suite, includes every program covered in the course for at home study. (558 Tools). Regular Price: *Hacking Tools Enterprise Suite available for individual purchase for only* \$1,499!

Full license for Immunity CANVAS (Normally sells for \$1450, included in most price quotes)

Core Impact SEL License



Course Materials, Test Fees and Class Guarantees!

Small class sizes (usually 10-20 Students), you get an intimate learning setting not offered by any of our competitors.

5 Full Days of Boot camp style training --- our instructors teach from 8am to 10:30pm every day. Course runs from 8am to 5pm daily with optional ethical capture the flag hacking exercises to 10:30pm.

All meals, snacks and refreshments included. Snacks not included in Las Vegas courses.

Certified Ethical Hacker exam fees.

Lecture, Lab Exercise and Text book --- Train your ethical friends and co-workers hacking!



Continued Access to the Course ONLINE

Total Access to Live Recorded Ethical Hacking Lectures:

InfoSec Institute's Ethical Hacking class is structured for maximum retention of knowledge learned in class. Because we believe in a commitment to your ongoing education after you attend a hands-on Ethical Hacking class, InfoSec Institute makes available for every student access to all of the Live Recorded lectures you attended in-class. These are available in online format for 30 days after the training session!

**GET YOUR QUOTE - INSTANTLY** 

#### Other Related Tools & Resources For Our Students

Be sure to check out our <u>R&D site</u>. We post tutorials, labs, white papers and articles to help you in your continued <u>ethical hacking training</u>. There are frequently forensics videos available. If you haven't taken a course with us yet, check out some of the types of thighs you'll be doing and learning about in class.

Application holes is a general category referring to specific programming errors or oversights that allow hackers to penetrate systems. (Throughout the list we separately cover holes in specific applications that we are able to exploit frequently (such as sendmail).) As part of a penetration test you identify applications running on remote systems. Once identified, you can perform a search for vulnerabilities and exploits that affect the applications. Application identification is often performed by capturing the application's banner, which frequently offers version information. By searching vulnerability databases and the Web for exploits specific to these versions, you can often find exploits or processes that can lead to a system compromise. For example, in one engagement we were initially unable to gain access to any of the systems in the company's demilitarized zone (DMZ), but we did identify several applications and versions that were running on the systems. After performing some research, we

discovered a vulnerability in the Compaq Web management service that enabled us to capture the backup SAM file out of the system's repair directory. The system OS was patched and configured correctly. However, the applications running on the system were not.

hacker tool kit is essentially a set of tools placed on a compromised system to help escalate privileges or to attack other systems. The hacker tool kit usually consists of a port scanner (Nmap), Netcat (for creating listeners and back doors), and any other tools you used during your discovery and exploitation phase. Create a directory on the host system disguised by a name that will not alert a general user or system administrator. The file could also be hidden or streamed to further avoid detection. Just remember that when the test is over you will need to remove the tool kit, so remember where it is located. Now that you have administrator access on the compromised host, you can run the tools from the host remotely or just use it as a stepping stone using port redirection. Port redirection involves taking network traffic coming into a host on one port and directing out from the host on another. For example, if we were able to compromise an NT Web server inside of a packet-filtering firewall, we would use a port redirection tool such as Fpipe to accept connections on a specified port and resend them to a specified port on a specified machine. On the compromised Web server we could set up a Netcat listener on port 80. On the compromised system we would execute:

```
C:\>nc -1 80 -e cmd.exe
```

On the testing system outside the firewall, we could use Fpipe to make the connection to the Web server using a different source port that is not filtered by the firewall. The following command would establish a listener on port 25 on the test machine and then redirect the connection to port 80 on the target system using the source port of 25.

```
C:\>fpipe -l 25 -s 25 -r 80 webipaddress
```

By using telnet to connect to the test system on port 25 we obtain a command prompt on the Web server inside the firewall. The traffic travels to port 80 from port 25 and thereby is able to bypass the filtering on the firewall. Using port redirection such as this, you can bypass filtering rules on packet-filtering firewalls or routers. Also, by remotely using a compromised host as a testing platform you may be able to take advantage of trust relationships.

Buffer overflow attacks, also called data-driven attacks, can be run remotely to gain access and locally to escalate privileges. Buffer overflows in general are designed almost exclusively for UNIX because in order to write a successful buffer overflow, knowledge of the workings of the OS, specifically treatment of the TCP stack, or the target application's memory/buffer-handling processes is necessary. While there are buffer overflows for Windows and Windows-based applications such as the IIS Web server, they are more common on the UNIX environment. UNIX source code is generally available, whereas source code to Microsoft operating systems is generally not. This allows anyone interested to study and gain the knowledge needed to create buffer overflows for UNIX. A buffer overflow attack attempts to force the target host to change the flow of execution and execute code the attacker specifies. This is done by forcing the target to place so much data into the finite-capacity target buffer that it overflows (with data). This generally stalls or crashes the application through which data was loaded. The point is to redirect the kernel's pointer (which points to the next command to be executed) to a portion of that excessive data the hacker wants to have executed. This portion of data is called an egg. A buffer overflow is challenging to write, in part because it is OS and architecture specific.[1]

[1] For more specific information regarding the creation of a buffer overflow, refer to the landmark paper on this topic by Aleph1, "Smashing the Stack for Fun and Profit" in *Phrack* 49, available on the Web at <a href="http://www.phrack.org/default.htm">http://www.phrack.org/default.htm</a>.

These buffer overflows <u>cisa training</u> generally only need to be downloaded onto the target system, compiled, and executed. You do not necessarily have to have root privileges to successfully run them. The hard part in performing these attacks is to find a buffer overflow that will work against your particular target. As mentioned, these attacks are OS and architecture specific. Further, if you are launching against a particular application or service, the version and patch level must be taken into consideration. The exploit code mentioned earlier that overflows the <u>gethostbyname()buffer</u> of the rlogin service on Solaris 2.5.1 is not likely to work on the HPUX OS or even more current versions of Solaris.

Buffer overflow attacks are dangerous and effective. If you compile and launch a particular buffer overflow attack against a susceptible target (server, service, or application), it may need a bit of tweaking, but it will likely work. Use such exploits only when you are fully aware of what they are doing and all potential consequences. Further, any experimentation should be done only on machines that are under your own control. Buffer overflows can <u>cause systems to crash</u>, leading to a <u>denial-of-service condition</u>. Therefore, buffer overflows generally should not be attempted against production systems without the written permission of the client.