Pearson | Live Virtual Training

Train with Confidence and Advance Your Career

Certified Ethical Hacker (CEH) Certification Crash Course

This live and interactive training is designed to help you prepare for the EC-Council Certified Ethical Hacker (CEH) version 10 certification exam. In this training, we will review

- Key topics and methodologies that you need to master the CEHv10 exam objectives
- Step-by-step examples of security penetration testing methodologies and concepts
- Sample questions for each of the topics covered in the exam

Learn how to craft exploits used by ethical hackers to perform real-world penetration testing engagements. Understand the methods for conducting wired and wireless network assessments, hacking web servers, and web applications. Explore attack techniques against mobile devices, IoT devices, and cloud deployments.

This Live Virtual Training is for:

- Participants with an understanding of cybersecurity fundamentals.
- Candidates studying for the Certified Ethical Hacker (CEH) version 10 certification.
- Anyone interested in cybersecurity and penetration testing (ethical hacking) will benefit from this training.
- Professionals wanting to learn different methodologies and best practices to perform security penetration testing assessments.

You will learn:

- The main topics covered in the CEHv10 exam.
- Main topics through step-by-step demonstrations.

Prerequisites:

- Course participants should have a basic understanding of cybersecurity and networking concepts./qw2

**Note – Live virtual training is a crash course intended to be part of a candidate's larger study & prep plan toward certification.*

Price: CAD 940 for the live virtual training course, which includes access to Pearson self-study materials (i.e. video training).

Schedule: November 11 and 12, 2019 (8 hours total, 4 hours each day)

Course times: 3 pm – 7 pm PST

About the Instructor:

Omar Santos is a Principal Engineer in the Cisco Product Security Incident Response Team (PSIRT) within Cisco's Security Research and Operations. He mentors and leads engineers and incident managers during the investigation and resolution of security vulnerabilities in all Cisco products, including cloud services. Omar has been working with information technology and cybersecurity since the mid-1990s. Omar has designed, implemented, and supported numerous secure networks for Fortune 100 and 500 companies and the U.S. government. Before his current role, he was a Technical Leader within the World-Wide Security Practice and the Cisco Technical Assistance Center (TAC), where he taught, led, and mentored many engineers. Omar is the author of several books and video courses.

Course Set-up:

- The course setup instructions are documented at https://cehreview.com/setup
- Attendees also need a reliable Internet connection and a web browser.

Course Outline:

Section 1: Introduction to Ethical Hacking and the CEHv10 exam (**30 minutes)**

- An introduction to ethical hacking and penetration testing methodologies.
- Reviewing what is new in the CEHv10 exam.

Section 2: Foot-printing, Enumeration, Reconnaissance, and Network Scanning **(50 minutes)**

- Introducing passive and active reconnaissance.
- Reviewing network scanning and system enumeration.
- Reviewing example questions.

Break 10 minutes

Section 3: Vulnerability Analysis and System Hacking **(40 minutes)**

- Reviewing vulnerability analysis methodologies and system hacking.
- Reviewing example questions.

Section 4: Social Engineering **(40 minutes)**

- Introducing social engineering.
- Reviewing social engineering tools and methodologies.
- Reviewing example questions.

Break 10 minutes

Section 5: Denial-of-Service (**30 minutes)**

- Introducing denial of service (DoS) attacks.
- Reviewing examples of DoS attacks.
- Reviewing example questions.

Section 6: Session Hijacking, Evading IDS, IPS, Firewalls, and Honeypots **(30 minutes)**

- Introducing session hijacking.
- Reviewing how to evade intrusion detection systems (IDS), intrusion prevention systems (IPS), and honeypots.
- Reviewing example questions.

Break 10 minutes

Section 7: Cryptography **(30 minutes)**

- Introducing cryptography concepts.
- Reviewing cryptographic vulnerabilities.
- Reviewing example questions.

Section 8: Hacking Wireless Networks **(40 minutes)**

- Introducing wireless network vulnerabilities.
- Reviewing how to hack wireless networks.
- Reviewing example questions.

Break 10 minutes

Section 9: Hacking Web Servers and Web Applications **(60 minutes)**

- Reviewing how to hack web servers.
- Reviewing how to hack web applications.
- Review example questions.

Break 10 minutes

Section 10: Hacking Mobile Platforms **(30 minutes)**

- Introducing mobile security.
- Reviewing mobile hacking methodologies and techniques.
- Reviewing example questions.

Section 11: IoT Hacking **(30 minutes)**

- Introducing IoT security.
- Reviewing IoT hacking methodologies and techniques.
- Reviewing example questions.

Section 12: Cloud Computing **(30 minutes)**

- Introducing cloud computing.
- Reviewing cloud security concepts.

- Reviewing example questions