كلية المجتمع بجدة
Jeddah Community College

King Abdulaziz University

Certified Ethical Hacker V9

Certificate: Certified Ethical Hacker
Accreditor: EC Council
Duration: 5 Days
Language: English
Course Delivery: Blended

Course Description:

This is the world's most advanced ethical hacking course with 18 of the most current security domains any ethical hacker will ever want to know when they are planning to beef up the information security posture of their organization. In 18 comprehensive modules, the course covers 270 attack technologies, commonly used by hackers. You will scan, test, hack and secure your own systems. You will be taught the five phases of ethical hacking and the ways to approach your target and succeed at breaking in every time. The five phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

Audience:

"Security Officers, Auditors, Security Professionals, Site Administrators, and anyone who is concerned about the integrity of the network infrastructure"

Learning Objectives:

- The Ethical Hacking and Countermeasures course prepares candidates for the CEH exam offered by EC-Council.
- The course focuses on hacking techniques and technology from an offensive perspective.
- The advanced security course is regularly updated to reflect latest developments in the domain, including new hacking techniques, exploits, automated programs as well as defensive recommendations as outlined by experts in the field.
- The CEH body of knowledge represents detailed contributions from security experts, academicians, industry practitioners and the security community at large.

Aftab Alam
CEHv9, CCNA, CNE, MCP

كلية المجتمع بجدة
Jeddah Community College

King Abdulaziz University

Benefits of Taking This Course:

- The ANSI accredited Ethical Hacking program is primarily targeted at security
- professionals who want to acquire a well rounded body of knowledge to have better opportunities in this field.
- Acquiring a CEH means the candidate has minimum baseline knowledge of security threats, risks and countermeasures.
- Organizations can rest assured that they have a candidate who is more than a systems administrator, a security auditor, a hacking tool analyst or a vulnerability tester.
- The candidate is assured of having both business and technical knowledge.

"Having this certification from EC Council has brought me great credibility. They have helped me gain a great foundation of knowledge that I can build on for the future."

Terry Cutler (CEH), Premium Services Engineer, Novell, Canada

Prerequisites:

You should have 2 years of work experience in security related field.

Follow-on Courses:

- EC-Council Certified Security Analyst (ECSA)
- Licensed Penetration Tester (LPT)

Course Materials:

Participants will receive the following as part of this course:

- 2 Courseware Books
- CDs
- Online Videos

Examination:

- Exam Format: Web-Based
- Questions: 125 multiple choice questions
- Passing Score: 70%
- Exam Duration: 240 minutes
- Proctoring: Physical proctoring

Aftab Alam
CEHv9, CCNA, CNE, MCP

كلية المجتمع بجدة
Jeddah Community College

King Abdulaziz University

Technical Requirements:

For eBooks:

- Internet for downloading the eBook
- Windows and Mac based systems
- Android, iOS, and Windows Phone based Tablet and SmartPhones
- Adobe Reader 10

For eLearning:

- Web Browser (IE, Mozilla, Chrome, or Safari)

Aftab Alam
CEHv9, CCNA, CNE, MCP

كلية المجتمع بجدة
Jeddah Community College

King Abdulaziz University

Agenda:

Day 1	Day 2	Day 3	Day 4	Day 5
Session hijacking techniques and countermeasures	Different types of web application attacks, web application hacking methodology, and countermeasures	Mobile platform attack vector, android vulnerabilities, jailbreaking iOS, windows phone 8 vulnerabilities, mobile security guidelines, and tools	Various cloud computing concepts, threats, attacks, and security techniques and tools	Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap and SQL injection attacks and injection detection tools etc
Different types of webserver attacks, attack methodology, and countermeasures	Wireless Encryption, wireless hacking methodology, wireless hacking tools, and wi- security tools	Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures	Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools	

Aftab Alam
CEHv9, CCNA, CNE, MCP

كلية المجتمع بجدة
Jeddah Community College

King Abdulaziz University

Course Outline:

Module 1: Session hijacking techniques and countermeasures

Module 2: Different types of webserver attacks, attack methodology, and countermeasures

Module 3: Different types of web application attacks, web application hacking methodology, and countermeasures

Module 4: Wireless Encryption, wireless hacking methodology, wireless hacking tools, and wi-security tools

Module 5: Mobile platform attack vector, android vulnerabilities, jailbreaking iOS, windows phone 8 vulnerabilities, mobile security guidelines, and tools

Module 6: Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures

Module 7: Various cloud computing concepts, threats, attacks, and security techniques and tools

Module 8: Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools

Module 9: Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap and SQL injection attacks and injection detection tools etc

For more information and enrolment to this course, kindly contact

Aftab Alam

205-Cisco Lab,2nd Floor,

CIT Dept , Jeddah Community College

King Abdulaziz University

Email: aabdussami@kau.edu.sa

Mobile: 056 11 77861