Advanced Business Learning

Arizona Licensed Post-Secondary Vocational School

DoD Mandate 8570.1
Cyber Security Training

Catalog
with Program Syllabi and Pricing

2016

GSA – Advantage GS-02F-0109W

NAICS: 611430, 611420, 611691, 611710, 541618, 541613, 541612, 541611, 512240, 512191, 512110, 511210, 541519
MOBIS 874-4, 874-5
NASA SEWP
Seaport-e
First Source
Cage Code 5H7B8
DUNS 788489180
Teaming: AKNA, 8(a), HUBZone, EDWOSB, SDVOSB

www.advancedbusinesslearning.com

Advanced Business Learning, Inc.
DoD 8570 Certification Preparation Courses and Project Management 5-day Boot Camps

Advanced Business Learning is an Authorized Training Provider (ATP) representing CompTIA, EC-Council, ISACA, ISC2, GSEC and PMI.

All courses offered are approved industry standard in format and design and all instructors are licensed by the authorizing entity.

Supplemental course materials are provided to ensure learning application which include online practice tests and access to online labs (where applicable).

Instructors offer tutorials *at the end of every class day* for practice and individual assistance and coaching.

Please visit our Cyber Security website - www.ablcybertraining.com

Certified Ethical Hacker (CEH) Preparation Training - EC-Council

Credential to be awarded: Certificate of Completion

Total Hours: 40

Mode of delivery:
Instructor Led √ Live Webinar √ On-line √ Combination √

Tuition: $2,345
Fees, Itemized: Course book $850; Optional EC-Council Certification Voucher $600
Total tuition & fees: $3,795

Course Description

This certification preparation program is for individuals seeking the CEH certification. This program will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. The CEH, is the first part of a 3 part EC-Council Information Security Certification Focus Area which helps you master hacking technologies. You will become a hacker, but an ethical one!

Day 1: Introduction to Ethical Hacking, Foot printing and Reconnaissance, Scanning Networks, and Enumeration

Topic A: Information Security Overview
Topic B: Information Security Threats and Attack Vectors
Topic C: Hacking Concepts, Types, and Phases
Topic D: Ethical Hacking Concepts and Scope
Topic E: Information Security Controls
Topic F: Information Security Laws and Standards
Topic G: Foot printing Concepts
Topic H: Foot printing Methodology
Topic I: Foot printing Tools
Topic J: Foot printing Countermeasures
Topic K: Foot printing Penetration Testing
Topic L: Overview of Network Scanning
Topic M: CEH Scanning Methodology
Topic N: Scanning Pen Testing
Topic O: Enumeration Concepts
Topic P: NetBIOS Enumeration
Topic Q: SNMP Enumeration
Topic R: LDAP Enumeration
Topic S: NTP Enumeration
Topic T: SMTP Enumeration
Topic U: Enumeration Countermeasures
Topic V: SMB Enumeration Countermeasures
Topic W: Enumeration Pen Testing

Day 2: System Hacking, Malware Threats, and Sniffing

Topic A: CEH Hacking Methodology (CHM)
Topic B: CEH System Hacking Steps
Topic C: Hiding Files
Topic D: Covering Tracks
Topic E: Penetration Testing
Topic F: Introduction to Malware
Topic G: Types of Trojans
Topic H: Virus and Worms Concepts
Topic I: Malware Reverse Engineering
Topic J: Malware Detection
Topic K: Countermeasures
Topic L: Anti-Malware Software
Topic M: Penetration Testing
Topic N: Sniffing Concepts
Topic O: MAC Attacks
Topic P: DHCP Attacks
Topic Q: ARP Poisoning
Topic R: Spoofing Attack
Topic S: DNS Poisoning
Topic T: Sniffing Tools
Topic U: Sniffing Detection Techniques
Topic V: Sniffing Pen Testing

Day 3: Social Engineering, Denial-of-Service, Session Hijacking, and Hacking Webservers

Topic A: Social Engineering Concepts
Topic B: Social Engineering Techniques
Topic C: Impersonation on Social Networking Sites
Topic D: Identity Theft
Topic E: Social Engineering Countermeasures
Topic F: Penetration Testing
Topic G: DoS/DDoS Concepts
Topic H: DoS/DDoS Attack Techniques
Topic I: Botnets
Topic J: DDoS Case Study
Topic K: Counter-measures
Topic L: DoS/DDoS Protection Tools
Topic M: DoS/DDoS Attack Penetration Testing
Topic N: Session Hijacking Concepts
Topic O: Application Level Session Hijacking
Topic P: Network-level Session Hijacking
Topic Q: Session Hijacking Tools
Topic R: Session Hijacking Pen Testing
Topic S: Webserver Concepts
Topic T: Webserver Attacks
Topic U: Attack Methodology

Topic V: Webserver Attack Tools
Topic W: Patch Management
Topic X: Webserver Security Tools
Topic Y: Webserver Pen Testing

Day 4: Hacking Web Applications, SQL Injection, Hacking Wireless Networks, and Hacking Mobile Platforms

Topic A: Web App Concepts/Threats
Topic B: Web App Hacking Methodology
Topic C: Web Application Hacking Tools
Topic D: Security Tools
Topic E: Web App Pen Testing
Topic F: SQL Injection Concepts
Topic G: Types of SQL Injection
Topic H: SQL Injection Methodology
Topic I: SQL Injection Tools
Topic J: Evasion Techniques
Topic K: Counter-measures
Topic L: Wireless Concepts
Topic M: Wireless Encryption
Topic N: Wireless Threats
Topic O: Wireless Hacking Methodology
Topic P: Wireless Hacking Tools
Topic Q: Bluetooth Hacking
Topic R: Counter-measures
Topic S: Wireless Security Tools
Topic T: Wi-Fi Pen Testing

Day 5: Evading IDS, Firewalls, and Honeypots, Cloud Computing, and Cryptography

Topic A: Mobile Platform Attack Vectors
Topic B: Hacking Android OS
Topic C: Hacking iOS
Topic D: Hacking Windows Phone OS
Topic E: Hacking BlackBerry
Topic F: Mobile Device Management (MDM)
Topic G: Mobile Security Guidelines and Tools
Topic H: Mobile Pen Testing
Topic I: IDS, Firewall and Honeypot Concepts/System
Topic J: Evading IDS
Topic K: Evading Firewall
Topic L: IDS/Firewall Evading Tools
Topic M: Detecting Honeypots
Topic N: Penetration Testing
Topic O: Cloud Computing Threats/Attacks
Topic P: Cloud Security
Topic Q: Cloud Security Tools

Topic R: Cloud Penetration Testing
Topic S: Cryptography Concepts
Topic T: Encryption Algorithms
Topic U: Cryptography Tools
Topic V: Public Key Infrastructure(PKI)
Topic W: Email Encryption
Topic X: Disk Encryption
Topic Y: Cryptography Attacks
Topic Z: Cryptanalysis Tools

Recommendations and Prerequisites

EC-Council Organization Certification Recommendations/ Prerequisites	To be eligible for the CEH certification, you must attend an official training class (from an EC-Council Authorized Training Provider) OR have at least two years of Internet Security related experience. Students who complete an Advanced Business Learning EC-Council program are automatically eligible to sit for the certification exam due to their Authorized Training Provider status.
EC-Council Organization Certification Exam Requirements	To be certified, students must pass the certification exam with a minimum score of 70% or higher during the allotted 4-hour period to complete the 125-question exam.

Materials Provided

Official EC-Council CEH textbook

Supplemental Student Study Material Information

In addition to the official EC-Council CEH book, students receive 12 months of access to EC-Council's official iLabs which contain exercises with Scenario, Objectives, and individual step-by-step tasks to guide the user through completion of the exercise and become an ethical hacker. Students also receive the Boson ExSim-Max Practice Exam Simulator. ExSim-Max for CEH 2016 exam simulation software covers all of the concepts needed to pass the EC-Council CEH 312-50 exam. The CEH 312-50 practice exam includes well-written, technically accurate questions and answers, which are divided into four individual exam simulations. These practice exams simulate the difficulty and variety of question types on the real exam so closely that passing the ExSim-Max for CEH 312-50 simulations ensures passing the real exam.

Optional: ABL or Client provided

Figure #1 is a sample of the ABL certificate for Program Completion

Figure 1: Program Completion Certificate

Figure #2: is a sample of the industry certificate for the Program Certification

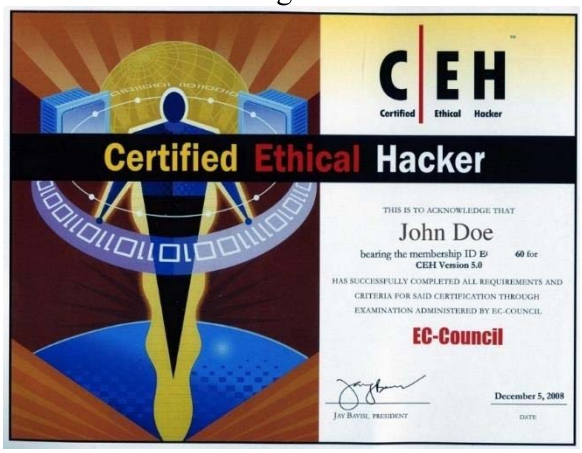

Figure 2: Program Certification Certificate