Business & IT Center
Tel: +961 (0)1 362 289
Mob: +961 (0)3 615 786

www.bitc-edu.com
info@bitc-edu.com

Course Outline: CEH Certified Ethical Hacker

Duration: 5 days/30 hours

Prerequisites:

Who should attend:

- Security officers
- Auditors
- Security professionals
- Site administrators
- Anyone who is concerned

Overview

This class will immerse the students into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When a student leaves this intensive 5 day class they will have hands on understanding and experience in Ethical Hacking. This course prepares you for EC-Council ANSI accredited Certified Ethical Hacker exam 312-50.

Outline:

Module 1: Introduction to Ethical Hacking

- Internet is Integral Part of Business and Personal Life - What Happens Online in 60 Seconds
- Information Security Overview
- Information Security Threats and Attack Vectors
- Hacking Concepts, Types, and Phases
- Ethical Hacking Concepts and Scope
- Information Security Controls
- Physical Security
- Incident Management
- What is Vulnerability Assessment?
- Penetration Testing
- Information Security Laws and Standards

Module 2: Footprinting and Reconnaissance

- Footprinting Concepts
- Footprinting Methodology
- Footprinting using Advanced Google Hacking Techniques
- Footprinting through Social Networking Sites
- Website Footprinting

Business & IT Center
Tel: +961 (0)1 362 289
Mob: +961 (0)3 615 786

www.bitc-edu.com
info@bitc-edu.com

- Email Footprinting
- Competitive Intelligence
- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting Tools
- Footprinting Countermeasures
- Footprinting Penetration Testing

Module 3: Scanning Networks

- Overview of Network Scanning
- CEH Scanning Methodology

Module 4: Enumeration

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP Enumeration
- Enumeration Countermeasures
- SMB Enumeration Countermeasures
- Enumeration Pen Testing

Module 5: System Hacking

- Information at Hand before System Hacking Stage
- System Hacking: Goals
- CEH Hacking Methodology (CHM)
- CEH System Hacking Steps
- Hiding Files
- Covering Tracks
- Penetration Testing

Module 6: Malware Threats

- Introduction to Malware
- Trojan Concepts
- Types of Trojans
- Virus and Worms Concepts
- Malware Reverse Engineering
- Malware Detection
- Countermeasures
- Anti-Malware Software
- Penetration Testing

Module 7: Sniffing

- Sniffing Concepts
- MAC Attacks
- DHCP Attacks
- ARP Poisoning Tool
- Spoofing Attack
- DNS Poisoning
- Sniffing Tools
- Sniffing Tool: Wireshark
- Follow TCP Stream in Wireshark
- Display Filters in Wireshark
- Additional Wireshark Filters
- Sniffing Tool
- Packet Sniffing Tool: Capsa Network Analyzer
- Network Packet Analyzer
- Counter measures
- Sniffing Detection Techniques
- Sniffing Pen Testing

Module 8: Social Engineering

- Social Engineering Concepts
- Social Engineering Techniques
- Impersonation on Social Networking Sites
- Identity Theft

Business & IT Center
Tel: +961 (0)1 362 289
Mob: +961 (0)3 615 786

www.bitc-edu.com
info@bitc-edu.com

- Social Engineering Countermeasures
- Penetration Testing

Module 9: Denial-of -Service

- DoS/DDoS Concepts
- DoS/DDoS Attack Techniques
- Botnets
- DDoS Case Study
- DoS/DDoS Attack Tools
- Counter-measures
- DoS/DDoS Protection Tools
- DoS/DDoS Attack Penetration Testing

Module 10: Session Hijacking

- Session Hijacking Concepts
- Application Level Session Hijacking
- Network-level Session Hijacking
- Session Hijacking Tools
- Counter-measures
- Session Hijacking Pen Testing

Module 11: Hacking Webservers

- Webserver Concepts
- Webserver Attacks
- Attack Methodology
- Webserver Attack Tools
- Counter-measures
- Patch Management
- Webserver Security Tools
- Webserver Pen Testing

Module 12: Hacking Web Applications

- Web App Concepts
- Web App Threats
- Web App Hacking Methodology
- Web Application Hacking Tools
- Countermeasures
- Security Tools

Module 13: SQL Injection

- SQL Injection Concepts
- Types of SQL Injection
- SQL Injection Methodology
- SQL Injection Tools
- Evasion Techniques
- Counter-measures

Module 14: Hacking Wireless Networks

- Wireless Concepts
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology
- Wireless Hacking Tools
- Bluetooth Hacking
- Counter-measures
- Wireless Security Tools
- Wi-Fi Pen Testing

Module 15: Hacking Mobile Platforms

- Mobile Platform Attack Vectors
- Hacking Android OS
- Hacking iOS
- Hacking Windows Phone OS
- Hacking BlackBerry

- Mobile Device Management (MDM)
- Mobile Security Guidelines and Tools
- Mobile Pen Testing

Module 16: Evading IDS, Firewalls, and Honeypots

- IDS, Firewall and Honeypot Concepts
- IDS, Firewall and Honeypot System
- Evading IDS
- Evading Firewalls

Module 17: Cloud Computing

- Introduction to Cloud Computing
- Cloud Computing Threats
- Cloud Computing Attacks
- Cloud Security
- Cloud Security Tools
- Cloud Penetration Testing

Module 18: Cryptography

- Cryptography Concepts
- Cryptography
- Types of Cryptography
- Cryptography Tools
- Public Key Infrastructure (PKI)
- Email Encryption
- Disk Encryption
- Cryptography Attacks
- Cryptanalysis Tools