

Ethical Hacking and Countermeasures

Course Code: ECCEHv7 **Five days; Instructor-Led**

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 Certified Ethical Hacker exam 312-50

Audience

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

Duration

5 days (9:00 – 5:00)

AVANTUS TRAINING PTE LTD

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: enquiries@AvantusTraining.com

www.AvantusTraining.com

Credit towards Certification

The Certified Ethical Hacker exam 312-50 may be taken on the last day of the training (optional). Students need to pass the online Prometric exam to receive CEH certification.

Legal Agreement

Ethical Hacking and Countermeasures course mission is to educate, introduce and demonstrate hacking tools for penetration testing purposes only. Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system, and to indemnify EC-Council with respect to the use or misuse of these tools, regardless of intent.

Not anyone can be a student — the Accredited Training Centers (ATC) will make sure the applicants work for legitimate companies.

Skills Measured

The exam 312-50 tests CEH candidates on the following 19 domains.

1. Introduction to Ethical Hacking
2. Footprinting and Reconnaissance
3. Scanning Networks
4. Enumeration
5. System Hacking
6. Trojans and Backdoors
7. Viruses and Worms
8. Sniffers
9. Social Engineering
10. Denial of Service
11. Session Hijacking
12. Hacking Webservers
13. Hacking Web Applications
14. SQL Injection
15. Hacking Wireless Networks
16. Evading IDS, Firewalls, and Honeypots
17. Buffer Overflow
18. Cryptography
19. Penetration Testing

AVANTUS TRAINING PTE LTD

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: enquiries@AvantusTraining.com

www.AvantusTraining.com

Course Outline

Module 01: Introduction to Ethical Hacking

- Understand the issues plaguing the information security world
- Gain knowledge on various hacking terminologies
- Learn the basic elements of information security
- Understand the security, functionality and ease of use triangle
- Know the 5 stages of ethical hacking
- Understand the different types and implications of hacker attacks
- Understand hactivism and understand the classification of hackers
- Understand who is an ethical hacker
- Gain Information on how to become an ethical hacker
- Learn the profile of a typical ethical hacker
- Understand scope and limitations of ethical hacking
- Understand vulnerability research and list the various vulnerability research tools
- Learn the different ways an ethical hacker tests a target network
- Understand penetration testing and the various methodologies used

Module 02: Footprinting and Reconnaissance

- Understand the term Footprinting
- Learn the areas and information that hackers seek
- Gain knowledge on information gathering tools and methodology
- Understand the role of financial websites in footprinting
- Understand competitive intelligence and its need
- Understand DNS enumeration
- Understand Whois
- Learn different types of DNS records

AVANTUS TRAINING PTE LTD

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: enquiries@AvantusTraining.com

www.AvantusTraining.com

- Understand how traceroute is used in Footprinting
- Recognize the Role of search engines in footprinting
- Learn the website mirroring tools
- Understand how e-mail tracking works
- Understand Google hacking and its tools
- Learn the countermeasures to be taken in footprinting
- Understand pen testing

Module 03: Scanning Networks

- Understand the term port scanning, network scanning and vulnerability scanning
- Understand the objectives of scanning
- Learn the CEH scanning methodology
- Understand Ping Sweep techniques
- Understand the Firewalk tool
- Gain knowledge on Nmap command switches
- Understand the three way handshake
- Understand the following Scans:
 - SYN, Stealth, XMAS, NULL, IDLE, FIN, ICMP Echo, List, TCP Connect, Full Open, FTP Bounce, UDP, Reverse Ident, RPC, Window
- Learn TCP communication flag types
- Gain knowledge on War dialing techniques
- Understand banner grabbing using OS fingerprinting, Active Stack Fingerprinting, Passive Fingerprinting and other techniques and tools
- Learn vulnerability scanning using BidiBlah and other hacking tools
- Learn to draw network diagrams of vulnerable hosts using various tools

- Understand how proxy servers are used in launching an attack
- Gain insights on working of anonymizers
- Identify HTTP tunneling techniques
- Identify IP spoofing techniques
- Understand various scanning countermeasures

Module 04: Enumeration

- Learn the system hacking cycle
- Understand Enumeration and its techniques
- Understand null sessions and its countermeasures
- Understand SNMP enumeration and its countermeasures
- Describe the steps involved in performing enumeration

Module 05: System Hacking

- Understand the different types of passwords
- Identify the different types of password attacks
- Identify password cracking techniques
- Understand Microsoft Authentication mechanism
- Describe password sniffing
- Identifying various password cracking tools
- Identify various password cracking countermeasures
- Understand privilege escalation
- Gain insights on key loggers and other spyware technologies
- Learn how to defend against spyware
- Identify different ways to hide files
- Understanding rootkits

AVANTUS TRAINING PTE LTD

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: enquiries@AvantusTraining.com

www.AvantusTraining.com

- Learn how to identify rootkits and steps involved
- Understand Alternate Data Streams
- Understand Steganography technologies and tools used
- Understand covering tracks, tools used and erase evidences

Module 06: Trojans and Backdoors

- Define a Trojan
- Identify overt and covert channels
- Understand working of Trojans
- Identify the different types of Trojans
- What do Trojan creators look for
- Identify the different ways a Trojan can infect a system
- How to indicate a Trojan attack
- Identify the ports used by Trojan
- Identify listening ports using netstat
- Understand “wrapping”
- Understand Reverse Shell Trojan
- Understand ICMP tunneling
- Identify various classic Trojans
- Learn windows start up monitoring tools
- Understand the Trojan horse constructing kit
- Learn Trojan detection techniques
- Learn Trojan evading techniques
- Learn how to avoid a Trojan infection

Module 07: Viruses and Worms

- Understand virus and its history
- Characteristics of a virus
- Learn the working of a virus
- Understand the motive behind writing a virus
- Understand how does a computer get infected by viruses
- Gain insights on virus hoax
- Understand virus analysis
- Understand the difference between a virus and a worm
- Understand the life cycle of virus
- Identify the types of viruses
- Understand how a virus spreads and infects the system
- Understand the storage pattern of virus
- Identify various types of classic virus found in the wild
- Virus writing technique
- Virus construction kits
- Understand antivirus evasion techniques
- Understand Virus detection methods and countermeasures
- Understand worm analysis

Module 08: Sniffers

- Understand sniffing and protocols vulnerable to it
- Identify types of sniffing
- Understand Address Resolution Protocol (ARP)
- Understanding the process of ARP Spoofing
- Understand active and passive sniffing

- Understand ARP poisoning
- Understand MAC duplicating
- Learn ethereal capture and display filters
- Understand MAC flooding
- Understand DNS spoofing techniques
- Identify sniffing countermeasures
- Know various sniffing tools
- Identify sniffing detection and defensive techniques

Module 09: Social Engineering

- Understand Social Engineering
- Understand human weakness
- Identify the different types of social engineering
- Learn warning signs of an attack
- Understand Dumpster Diving
- Understand Human-based Social Engineering
- Understand Insider attacks and its countermeasures
- Gain insights on Social Engineering threats and defense
- Comprehend Identity Theft
- Understand Phishing Attacks
- Identify Online Scams
- Understand URL obfuscation
- Understand social engineering on social networking sites
- Identify Social Engineering countermeasures

Module 10: Denial of Service

- Understand a Denial of Service Attack
- Gain insights on Distributed Denial of Service Attacks
- Examine the working of Distributed Denial of Service Attacks
- Analyze Symptoms of a DoS Attack
- Understand Internet Chat Query (ICQ)
- Understand Internet Relay Chat (IRC)
- Assess DoS Attack Techniques
- Understand Botnets
- Assess DoS/DDoS Attack Tools
- Describe Detection Techniques
- Identify DoS/DDoS Countermeasure Strategies
- Analyze Post-Attack Forensics
- Identify DoS/DDoS Protection Tools
- Understand DoS/DDoS Penetration Testing

Module 11: Session Hijacking

- Understand what is Session Hijacking
- Identify Key Session Hijacking Techniques
- Understand Brute Forcing Attack
- Understand HTTP Referrer Attack
- Spoofing vs. Hijacking
- Understand Session Hijacking Process
- Identify types of Session Hijacking
- Analyze Session Hijacking in OSI Model
- Understand Application Level Session Hijacking

- Discuss Session Sniffing
- Describe Man-in-the-Middle Attack
- Understand Man-in-the-Browser Attack
- Examine Steps to Perform Man-in-the-Browser Attack
- Understand Client-side Attacks
- Understand Cross-site Script Attack
- Understand Session Fixation Attack
- Describe Network Level Session Hijacking
- Understand TCP/IP Hijacking
- Identify Session Hijacking Tools
- Identify Countermeasures of Session Hijacking
- Understand Session Hijacking Pen Testing

Module 12: Hacking Webservers

- Understand Open Source Webserver Architecture
- Examine IIS Webserver Architecture
- Understand Website Defacement
- Understand why Web Servers are compromised
- Analyze Impact of Webserver Attacks
- Examine Webserver Misconfiguration
- Understand Directory Traversal Attacks
- Learn regarding HTTP Response Splitting Attack
- Understand Web Cache Poisoning Attack
- Understand HTTP Response Hijacking
- Discuss SSH Bruteforce Attack
- Examine Man-in-the-Middle Attack

AVANTUS TRAINING PTE LTD

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: enquiries@AvantusTraining.com

www.AvantusTraining.com

- Learn Webserver Password Cracking Techniques
- Identify Web Application Attacks
- Understand Webserver Attack Methodology
- Identify Webserver Attack Tools
- Identify Counter-measures against Webserver Attacks
- Understand Patch Management
- Assess Webserver Security Tools
- Understand Webserver Pen Testing

Module 13: Hacking Web Applications

- Understand Introduction to Web Applications
- Identify Web Application Components
- Understand working of Web Applications
- Examine Web Application Architecture
- Assess Parameter/Form Tampering
- Understand Injection Flaws
- Discuss Hidden Field Manipulation Attack
- Describe Cross-Site Scripting (XSS) Attacks
- Understand Web Services Attack
- Understand Web Application Hacking Methodology
- identify Web Application Hacking Tools
- Understand how to Defend Against Web Application Attacks
- Identify Web Application Security Tools
- Understand Web Application Firewalls
- Gain insights on Web Application Pen Testing

Module 14: SQL Injection

- Understand SQL Injection
- Examine SQL Injection Attacks
- Understand working of Web Applications
- Identify Server Side Technologies
- Understand SQL Injection Detection
- Discuss SQL Injection Black Box Pen Testing
- Types of SQL Injection
- Understand Blind SQL Injection
- Learn SQL Injection Methodology
- Understanding SQL Query
- Examine Advanced Enumeration
- Describe Password Grabbing
- Discuss Grabbing SQL Server Hashes
- Identify SQL Injection Tools
- Understand Evasion Techniques for SQL Injection
- Understand Defensive strategies Against SQL Injection Attacks
- Identify SQL Injection Detection Tools

Module 15: Hacking Wireless Networks

- Understand Wireless Networks
- Gain Insights on Wireless Networks
- Understand various types of Wireless Networks
- Understand Wi-Fi Authentication Modes
- Identify types of Wireless Encryption
- Understand WEP Encryption

- Understand WPA/WPA2
- Discuss Wireless Threats
- Understand Wireless Hacking Methodology
- Assess Wireless Hacking Tools
- Understand Bluetooth Hacking
- Understand how to Defend Against Bluetooth Hacking
- Understand how to Defend against Wireless Attacks
- Identify Wi-Fi Security Tools
- Examine Wireless Penetration Testing Framework

Module 16: Evading IDS, Firewalls, and Honeypots

- Understand Intrusion Detection Systems (IDS)
- Learn Ways to Detect an Intrusion
- Acquire knowledge on various types of Intrusion Detection Systems
- Understand what is a Firewall
- Types of Firewall
- Identify Firewall Identification Techniques
- Understand Honeypot
- Assess various types of Honeypot
- Understand how to Set up a Honeypot
- Understand IDS, Firewall and Honeypot System
- Examine Evading IDS
- Understand Evading Firewall
- Learn detecting Honeypots
- Identify Firewall Evading tools
- Identify Countermeasures

- Analyze Firewall and IDS Penetration Testing

Module 17: Buffer Overflow

- Understand Buffer Overflows (BoF)
- Understand Stack-Based Buffer Overflow
- Know Heap-Based Buffer Overflow
- Understand Stack Operations
- Identify Buffer Overflow Steps
- Analyze attacking a Real Program
- Examine Smashing the Stack
- Examples of Buffer Overflow
- Understand how to Mutate a Buffer Overflow Exploit
- Learn how to identify Buffer Overflows
- Testing for Heap Overflow Conditions: heap.exe
- Understand steps for Testing Stack Overflow in OllyDbg Debugger
- Identify Buffer Overflow Detection Tools
- Understand Defense Against Buffer Overflows
- Identify Buffer Overflow Countermeasures Tools
- Understand Buffer Overflow Pen Testing

Module 18 Cryptography

- Understand Cryptography
- Learn various types of Cryptography
- Understand Ciphers
- Gain insights on Advanced Encryption Standard (AES)
- Understand RC4, RC5, RC6 Algorithms

- Examine RSA (Rivest Shamir Adleman)
- Explain Message Digest Function: MD5
- Understand Secure Hashing Algorithm (SHA)
- Identify Cryptography Tools
- Understand Public Key Infrastructure (PKI)
- Understand Email Encryption
- Identify Digital Signature
- Describe SSL (Secure Sockets Layer)
- Examine Disk Encryption
- Identify Disk Encryption Tools
- Understand Cryptography Attacks
- Identify Cryptanalysis Tools

Module 19: Penetration Testing

- Understand Penetration Testing (PT)
- Identify Security Assessments
- Examine Risk Management
- Understand various types of Penetration Testing
- Understand Automated Testing
- Understand Manual Testing
- Understand Penetration Testing Techniques
- Know the Penetration Testing Phases
- Understand Enumerating Devices
- Understand Penetration Testing Roadmap
- Understand Denial of Service Emulation
- Outsourcing Pen Testing Services

AVANTUS TRAINING PTE LTD

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: enquiries@AvantusTraining.com

www.AvantusTraining.com

- Identify various Penetration testing tools

AVANTUS TRAINING PTE LTD

79 Robinson Road #15-04 CPF Building Singapore 068897

Sales Hotline: (65)64163078

Email: enquiries@AvantusTraining.com

www.AvantusTraining.com