Brought to you by **iEnabler – THE IT ENABLING COMPANY**

Certified Ethical Hacker (CEH)

Course Objective :

C|EH is the world's most advanced ethical hacking course covering 20 of the most important security domains any individual will need when they are planning to beef-up the information security posture of their organization.

This course provides you with the tools and techniques used by hackers and information security professionals alike to break into any computer system. This course will immerse you into a "Hacker Mindset" in order to teach you how to think like a hacker and better defend against future attacks. It puts you in the driver's seat with a hands-on training environment employing a systematic ethical hacking process.

You will learn how to scan, test, hack and secure target systems. The course covers the Five Phases of Ethical Hacking, diving into Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

Prerequisite:

Participants should be familiar with :

- Basic computer literacy & Basic PC operating system navigation skills
- Basic Internet usage skills & Basic IP address knowledge
- Understanding of network fundamentals

Training Methodology & Materials:

- Practical hands-on sessions, 80% lab-based and 20% theory-based.
- Additional and well-designed labs handouts are given to enhance further enhance the courseware given.

Certificate Of Attendance :

Certificate Of Attendance will be awarded to participants completing the course achieving minimum 75% attendance.

Training Duration:

Full-Time : 5 Weekdays or 5 Sats
Time : 9am - 6pm

Certified Ethical Hacker Certification Exam

This course will help the participants to prepare for the **C|EH** Exam.

Exam Code : 312-50 (Pearson VUE).

Course Fee:

Normal Course Fee : S$2500
Regn Fee : S$50

* Course fee includes 1 CEH Exam voucher

All fees subject to prevailing GST.
Call us to check on latest promotion.

DETAILED COURSE OUTLINE

Module 01: Introduction to Ethical Hacking

1.1 Information Security Overview
1.2 Information Security Threats and Attack Vectors
1.3 Hacking Concepts
1.4 Ethical Hacking Concepts
1.5 Information Security Controls
1.6 Penetration Testing Concepts
1.7 Information Security Laws and Standards

Module 02 : Footprinting and Reconnaissance

2.1 Footprinting Concepts
2.2 Footprinting through Search Engines
2.3 Footprinting through Web Services
2.4 Footprinting through Social Networking Sites
2.5 Website Footprinting
2.6 Email Footprinting
2.7 Competitive Intelligence
2.8 Whis Footprinting
2.9 DNS Footprinting
2.10 Network Footprinting
2.11 Footprinting through Social Engineering
2.12 Footprinting Tools
2.13 Countermeasures
2.14 Footprinting Pen Testing

Module 03 : Scanning Networks

3.1 Network Scanning Concepts
3.2 Scanning Tools
3.3 Scanning Techniques
3.4 Scanning Beyond IDS and Firewall
3.5 Banner Grabbing
3.6 Draw Network Diagrams
3.7 Scanning Pen Testing

Module 04: Enumeration

4.1 Emumeration Concepts
4.2 NetBIOS Enumeration
4.3 SNMP Enumeration
4.4 LDAP Enumeration
4.5 NTP Enumeration
4.6 SMTP and DNS Enumeration
4.7 Other Enumeration Techniques
4.8 Enumeration Countermeasures
4.9 Enumeration Pen Testing

Module 05: Vulnerability Analysis

5.1 Vulnerability Assessment Concepts
5.2 Vulnerability Assessment Solutions
5.3 Vulnerability Scoring Systems
5.4 Vulnerability Assessment Tools
5.5 Vulnerability Assessment Reports

Module 06: System Hacking

6.1 System Hacking Concepts
6.2 Cracking Passwords
6.3 Escalating Privileges
6.4 Executing Applications
6.5 Hiding Files
6.6 Covering Tracks
6.7 Penetration Testing

Module 07: Malware Threats

7.1 Malware Concepts
7.2 Trojan Concepts
7.3 Virus and Worm Concepts
7.4 Malware Analysis
7.5 Countermeasures
7.6 Anti-Malware Software
7.7 Malware Penetration Testing

Module 08: Sniffing

8.1 Sniffing Concepts
8.2 Sniffing Technique: MAC Attacks
8.3 Sniffing Technique: DHCP Attacks
8.4 Sniffing Technique: ARP Poisoning
8.5 Sniffing Technique: Spoofing Attacks
8.6 Sniffing Technique: DNS Poisoning
8.7 Sniffing Tools
8.8 Countermeasures
8.9 Sniffing Detection Techniques
8.10 Sniffing Pen Testing

Module 09: Social Engineering

9.1 Social Engineering Concepts
9.2 Social Engineering Techniques
9.3 Insider Threats
9.4 Impersonation on Social Networking Sites
9.5 Identify Theft
9.6 Countermeasures
9.7 Social Engineering Pen Testing

Module 10: Denial-of-Service

10.1 DoS/DDoS Concepts
10.2 DoS/DDoS Attack Techniques
10.3 Botnets
10.4 DDoS Case Study
10.5 DoS/DDoS Attack Tools
10.6 Countermeasures
10.7 DoS/DDoS Protection Tools
10.8 DoS/DDoS Penetration Testing

Module 11: Session Hijacking

11.1 Session Hijacking Concepts
11.2 Application Level Session Hijacking
11.3 Network Level Session Hijacking
11.4 Session Hijacking Tools
11.5 Countermeasures
11.6 Penetration Testing

Module 12: Evading IDS, Firewalls and Honeypots

12.1 IDS, Firewall and Honeypot Concepts
12.2 IDS, Firewall and Honeypot Solutions
12.3 Evading IDS
12.4 Evading Firewalls
12.5 IDS/Firewall Evading Tools
12.6 Detecting Honeypots
12.7 IDS/Firewall Evasion Countermeasures
12.8 Penetration Testing

Module 13: Hacking Web Servers

13.1 Web Server Concepts
13.2 Web Server Attacks
13.3 Web Server Attack Methodology
13.4 Web Server Attack Tools
13.5 Countermeasures
13.6 Patch Management
13.7 Web Server Security Tools
13.8 Web Server Pen Testing

Module 14: Hacking Web Applications

14.1 Web App Concepts
14.2 Web App Threats
14.3 Hacking Methodology
14.4 Web App Hacking Tools
14.5 Countermeasures
14.6 Web App Security Testing Tools
14.7 Web App Pen Testing

Module 15: SQL Injection

15.1 SQL Injection Concepts
15.2 Types of SQL Injection
15.3 SQL Injection Methodology
15.4 SQL Injection Tools
15.5 Evasion Techniques
15.6 Countermeasures

Module 16: Hacking Wireless Networks

16.1 Wireless Concepts
16.2 Wireless Encryption
16.3 Wireless Threats
16.4 Wireless Hacking Methodology
16.5 Wireless Hacking Tools
16.6 Bluetooth Hacking
16.7 Countermeasures
16.8 Wireless Security Tools
16.9 Wireless Pen Testing

Module 17: Hacking Mobile Platforms

17.1 Mobile Platform Attack Vectors
17.2 Hacking Android OS
17.3 Hacking IOS
17.4 Mobile Spyware
17.5 Mobile Device Management
17.6 Mobile Security Guidelines and Tools
17.7 Mobile Pen Testing

Module 18: IoT Hacking

18.1 IoT Concepts
18.2 IoT Attacks
18.3 IoT Hacking Methodology
18.4 IoT Hacking Tools
18.5 Countermeasures
18.6 IoT Pen Testing

Module 19: Cloud Computing

19.1 Cloud Computing Concepts
19.2 Cloud Computing Threats
19.3 Cloud Computing Attacks
19.4 Cloud Security
19.5 Cloud Security Tools
19.6 Cloud Penetration Testing

Module 20: Cryptography

20.1 Cryptography Concepts
20.2 Encryption Algorithms
20.3 Cryptography Tools
20.4 Public Key Infrastructure (PKI)
20.5 Email Encryption
20.6 Disk Encryption
20.7 Cryptanalysis
20.8 Countermeasures

IT Enabler Consultancy Pte Ltd
(Co Reg No. 200211025Z)
35 Selegie Road #09-06 Parklane Shopping Mall Singapore188307 | Tel: 6333 4843 | Fax: 6333 4883 | www.ienabler.com.sg