



ETHICAL HACKING AND Countermeasures Workshop

Course Introduction:

This course will immerse the participants 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. Participants 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.

Course Objectives:

- Explain accepted data warehouse terminology
- Explain the goals of data warehousing
- Identify the stages of the data warehousing lifecycle
- Apply the star schema model to a business case problem
- De-normalize relational tables into high level summary tables
- Design and Implement a multi-dimensional data cube using SQL Server Analysis Services

Who Should Attend?

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

Course Outline:

Introduction to Ethical Hacking

Internet is Integral Part of Business and Personal Life - What Happens Online in 60 Seconds

Information Security Overview

- Year of the Mega Breach
- Data Breach Statistics
- Malware Trends in 2014
- Essential Terminology
- Elements of Information Security
- The Security, Functionality, and Usability Triangle

Information Security Threats and Attack Vectors

- Motives, Goals, and Objectives of Information Security Attacks
- Top Information Security Attack Vectors
- Information Security Threat Categories
- Types of Attacks on a System
 - Operating System Attacks
 - Examples of OS Vulnerabilities
 - Misconfiguration Attacks
 - Application-Level Attacks
 - Examples of Application-Level Attacks
 - Shrink Wrap Code Attacks
 - Information Warfare

Hacking Concepts, Types, and Phases

- What is Hacking
- Who is a Hacker?
- Hacker Classes
- Hacking Phases
 - Reconnaissance
 - Scanning
 - Gaining Access
 - Maintaining Access
 - Clearing Tracks

Ethical Hacking Concepts and Scope

- What is Ethical Hacking?
- Why Ethical Hacking is Necessary
- Scope and Limitations of Ethical Hacking
- Skills of an Ethical Hacker

Information Security Controls

- Information Assurance (IA)
- Information Security Management Program
- Threat Modeling
- Enterprise Information Security Architecture (EISA)
- Network Security Zoning
- Defense in Depth
- Information Security Policies

Types of Security Policies

- Examples of Security Policies
- Privacy Policies at Workplace
- Steps to Create and Implement Security Policies
- HR/Legal Implications of Security Policy Enforcement

Physical Security

- Physical Security Controls

Incident Management

- Incident Management Process
- Responsibilities of an Incident Response Team

What is Vulnerability Assessment?

- Types of Vulnerability Assessment
- Network Vulnerability Assessment Methodology
- Vulnerability Research
- Vulnerability Research Websites

Penetration Testing

- Why Penetration Testing
- Comparing Security Audit, Vulnerability Assessment, and Penetration Testing
- Blue Teaming/Red Teaming
- Types of Penetration Testing
- Phases of Penetration Testing
- Security Testing Methodology
- Penetration Testing Methodology

Information Security Laws and Standards

- Payment Card Industry Data Security Standard (PCI-DSS)
- ISO/IEC 27001:2013
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes Oxley Act (SOX)
- The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)
- Cyber Law in Different Countries

Course Methodology:

A variety of methodologies will be used during the course that includes:

- (30%) Based on Case Studies
- (30%) Techniques
- (30%) Role Play
- (10%) Concepts
- Pre-test and Post-test
- Variety of Learning Methods
- Lectures
- Case Studies and Self Questionnaires
- Group Work
- Discussion
- Presentation

Course Fees:

To be advice as per course location. This rate includes participant's manual, Hands-Outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Certificate:

International Center for Training & Development (ICTD) will award an internationally recognized certificate(s) for each delegate on completion of training.

Course Timings:

Daily Course Timings:

08:00 - 08:20	Morning Coffee / Tea
08:20 - 10:00	First Session
10:00 - 10:20	Coffee / Tea / Snacks
10:20 - 12:20	Second Session
12:20 - 13:30	Lunch Break & Prayer Break
13:30 - 15:00	Last Session