Compuserve Pvt Ltd.

Course Duration : 40 hrs

COMET CERTIFIED

ETHICAL HACKING AND PENETRATION TESTING

COURSE BROCHURE

www.cometcompuserve.com

Overview

Ethical Hacking and Penetration testing course provides the skills required for a candidate to become a Security Professional. The skills acquired through this course can make one to understand the essential concepts to perform penetration testing, uncover the vulnerability and solutions mitigate the risk of attack. In this course we will also discuss the scenarios with few advanced tools to identify, detect, and exploit any vulnerability uncovered in the target network environment. The interesting part of this course is that we will have more practical demos to understand the theoretical concepts.

Course Objective

In this course, you will learn to

- Overview of Information and Cyber Security
- Hacking and Ethical Hacking concepts
- Five Phases of Hacking
- Using tools for scanning and Vulnerability Assessment
- Malware based Attacks
- Man-in-the-Middle Attack
- VAPT of Web Servers and Web Application Servers
- Wireless Hacking

Audience Profile

This course is for Students/IT Professionals who is interested in becoming Information Security and Cyber Security professional.

Prerequisites

- For taking this course, knowledge about Networking Basics and Servers will be an essential.
- Good knowledge on TCP/IP, IP Address, Subnet, Ports and Protocols in Networking.
- Good Knowledge on Windows and Linux Servers including DNS, DHCP, Web Server, FTP Server and Active Directory.

Course Module

Module 1 : Introduction to Information Security **(2 Hrs)**

- Information Security Overview
- Hacking and Ethical Concepts
- Hacking Phases
- Information Security Controls
- Penetration Testing Overview

Module 02 : Footprinting **(2 Hrs)**

- Footprinting Concepts
- Footprinting through Search Engines
- Footprinting through Web Services
- Footprinting through Social Networking Sites

Module 03: Scanning Networks **(4 Hrs)**

- Understanding TCP Flags
- Network Scanning Concepts
- Scanning Techniques
- Scanning Devices

Module 04: Enumeration **(2 Hrs)**

- Enumeration Concepts
- Enumeration Methods and Tools

Module 05: Vulnerability Assessment **(4 Hrs)**

- Vulnerability Assessment Concepts
- Vulnerability Assessment Solutions
- Vulnerability Scoring Systems
- Vulnerability Assessment Tools
- Vulnerability Assessment Reports

Module 06: System Hacking **(4 Hrs)**

- System Hacking Concepts
- Cracking Passwords
- Escalating Privileges
- Executing Applications
- Hiding Files
- Covering Tracks

Module 07: Malware Threats **(4 Hrs)**

- Malware Concepts
- Trojan Concepts
- Virus and Worm Concepts
- Malware Analysis
- Countermeasures
- Anti-Malware Software

Module 08: Sniffing **(4 Hrs)**

- Sniffing Concepts
- Sniffing Technique: MAC Attacks
- Sniffing Technique: DHCP Attacks
- Sniffing Technique: ARP Poisoning
- Sniffing Technique: Spoofing Attacks
- Sniffing Technique: DNS Poisoning

Module 09: Web Servers/Application VAPT **(4 Hrs)**

- Web Server/Application Assessment Methodology
- Web Server/Application Assessment Tools
- Web Server/Application VAPT and Reporting

Module 10: Wireless Network VAPT **(4 Hrs)**

- Wi-Fi Authentication Modes
- Wireless Encryption Protocols
- Wireless Network VAPT and Reporting

Our Students Testimonials

CONTACT US

Mobile : +91 9940068251 / 58251

Mail : ramesh@cometcompuserve.com / ilanchezhian@cometcompuserve.com