



**Certified Information Security Expert (CISE L1 V3)
Detailed Course Module**



Certified Information Security Expert (CISE v3.0)

Innobuzz Knowledge Solutions Pvt Ltd is high quality-training provider for courses in the field of Information Security, Systems and Open-Source

The hands on security courses in the field of offensive security are built by the Innobuzz Knowledge Solutions Pvt Ltd members to ensure real world experience.

www.innobuzz.in



Chapter 1 – Introduction

- ✍ History of Hacking & Hackers
- ✍ What is Information Security?
- ✍ Problems faced by the Corporate World
- ✍ Why Corporate needs Information Security?
- ✍ The CIA Triad
- ✍ Hacking – Legal or Not?
- ✍ Type of Ethical Hackers
- ✍ Hackers vs. Crackers
- ✍ Classification of Hackers
- ✍ Phases of Hacking
- ✍ Basic Terminologies

Chapter 2 – Networking

- ✍ What is a Network?
- ✍ Network Topologies
- ✍ Networking Devices and Cables
- ✍ Concept of Ports and Services
- ✍ ISO - OSI Model
- ✍ TCP/IP Protocol Suite
- ✍ Client Server Relationship
- ✍ IP Address
- ✍ Anatomy of IP Addresses
- ✍ **Networking Protocols**
 - ✓ ARP
 - ✓ RARP
 - ✓ ICMP
 - ✓ FTP
 - ✓ Telnet
 - ✓ SMTP
 - ✓ SNMP



- ✓ HTTP
- ✓ POP
- ✎ **Virtualization**
 - ✓ Introduction to virtualization
 - ✓ Advantages of Virtualization
 - ✓ Virtual Box
 - ✓ Vmware Workstation
- ✎ **Linux**
 - ✓ Introduction
 - ✓ Installation
 - ✓ Basic Linux Commands
 - ✓ Installing Linux application

Chapter 3 – Footprinting/Reconnaissance

- ✎ Footprinting/Information Gathering
- ✎ Types of Footprinting
 - ✓ Active
 - ✓ Passive
- ✎ Information Gathering Principle
- ✎ Steps to Information Gathering
- ✎ Who.is and Domain Registry
- ✎ **Gathering Target Information**
 - ✓ Search for People and their Information
 - ✓ Search for Company's Information
 - ✓ Footprinting Through Search Engines
 - ✓ Tracking Target Location
 - ✓ Information gathering using social media
- ✎ Parallel Domain
- ✎ MX Entry
- ✎ Trace Route
- ✎ Archive Pages



- ✍ Crawling and Mirroring of Websites
- ✍ Banner Grabbing
- ✍ Prevention Techniques

Module 4: Google Hacking

- ✍ Introduction to Google
- ✍ Working of Google – Outline
- ✍ Working of Google – Crawling, Indexing & Searching
- ✍ Using Cache and Google as Proxy
- ✍ Directory Listing and Locating Directory Listings along with specific folders
- ✍ Google Hacking and what it is about
- ✍ The basics of Google Hacking: Advanced Search in Google
- ✍ Advance Search Operators: site:, filetype:, inurl:, intitle:, cache:, info:
- ✍ Wildcard and Quotes
- ✍ Understanding and Viewing Robots.txt for important Files
- ✍ **Prevention Techniques**
 - ✓ Robot.txt
 - ✓ Metatag and Google Official Remove
 - ✓ Hiding Detailed Error Messages
 - ✓ Disabling Directory Browsing
- ✍ **Tools**
 - ✓ Wikto
 - ✓ GoogleHacks

Module 5: Scanning

- ✍ Definition of Scanning
- ✍ Types of Scanning
- ✍ Difference between Port and Network Scanning
- ✍ Objectives and Benefits of Scanning
- ✍ TCP three way hands shake



- ✍ Classification of Scanning
- ✍ Fragments, UDP, ICMP, Reverse Ident, List & Idle, RPC, Window Scan, Ping Sweep
- ✍ Concept of War Dialer (History)
- ✍ OS Finger Printing and Types – Active & Passive
- ✍ Concealing file extensions
- ✍ Anonymizers
- ✍ **Scanning Tools**
 - ✓ T1Shopper.com
 - ✓ Yougetsignal
 - ✓ Advanced Port Scanner v1.3 (Radmin – Advanced Port Scanner)
 - ✓ Watsup Port Scanner
 - ✓ NetScanner
 - ✓ Mi-Tec Network Scanner

Module 6: System Hacking: Win7 and Linux

- ✍ **System Hacking**
 - ✓ Introduction to System Hacking
 - ✓ System Hacking Techniques
 - ✓ Steps to Crack Passwords
 - ✓ Password Attack Classification – Dictionary, Brute Force and Hybrid
 - ✓ LM Hash and Sam File
 - ✓ Password Recovery through Elcomsoft
 - ✓ SysKey
 - ✓ Hiding Files
 - ✓ Ophcrack
 - ✓ Hiren Boot
 - ✓ NTFS Stream Countermeasures
 - ✓ Password Cracking Countermeasures
 - ✓ Concept of Auditing, Logs, Covering Tracks
 - ✓ Concept of Application Isolation
- ✍ **Linux Hacking**
 - ✓ Why Linux is hacked?
 - ✓ Recent Linux Vulnerabilities



- ✓ Password cracking in Linux
- ✓ Introduction and explanation of IP Tables & IP Chains
- ✓ TCP wrappers
- ✓ Remote connection using SSH
- ✓ Log and Traffic Monitors in Linux
- ✓ Understanding Post Install Linux Security Auditing
- ✓ Understanding and using Backtrack

✎ **Keylogger**

- ✓ Categorization of Keystroke Loggers
- ✓ Acoustic/CAM Keyloggers
- ✓ Advanced Keylogger
- ✓ Keylogger: Spytech SpyAgent
- ✓ Keylogger: Perfect Keylogger
- ✓ Keylogger: Powered Keylogger
- ✓ Hardware Keylogger: KeyGhost

✎ **Rootkits**

- ✓ Types of Rootkits
- ✓ Rootkit Working Mechanism
- ✓ Rootkit: Fu
- ✓ Steps to detect Rootkits
- ✓ Shielding from Rootkit Attacks
- ✓ Anti Rootkit Tools: Rootkit Revealer and McAfee Rootkit Revealer

✎ **Cover Tracks**

- ✓ What are Covering Tracks?
- ✓ Techniques to clear Tracks
- ✓ Covering Track Tools

Module 7: Android & iPhone Hacking

✎ **Android Security**

- ✓ Introduction to Android Security
- ✓ Android Malwares
- ✓ Securing Your Android - Techniques
- ✓ APK File Package



- ✓ Investigating layout, manifest, permissions and binaries
- ✓ Analyzing file system access
- ✓ Investigating database & storage usage
- ✓ Memory analysis
- ✓ Memory dumps
- ✓ Patching & Binary modifications
- ✓ Traffic Manipulation
- ✓ Traffic interception
- ✓ Using proxies
- ✓ Exposing insecure traffic

iPhone Security

- ✓ iOS Security Basics
- ✓ iOS Hardware/Device Types
- ✓ Understanding the iOS Security Architecture
 - The Reduced Attack Surface
 - The Stripped-Down iOS
 - Privilege Separation
 - Code Signing
 - Data Execution Prevention
 - AddressSpace Layout Randomization
 - Sandboxing
- ✓ History of iOS Attack
 - Libtiff
 - Fun with SMS
 - Ilkee Worm
 - Jailbreakme

Module 8: Malwares

Trojans

- ✓ Introduction to Trojans
 - What is Trojan?
 - Identifying Overt & Covert Channels
 - Types of Trojans
 - Working of Trojans



- Purpose of Trojan inventor
- Detecting Trojan Attacks
- Ports used by Trojans
- ✓ Types of Trojans
 - Trojan Types
 - Remote Access Trojans
 - Beast - Demo
 - Remote Access Trojan: RAT DarkComet
- ✓ Trojan Detection
 - Trojan Detection
 - Suspicious Port Detection
 - Suspicious Process Scanning
 - Process Monitoring Tools
 - Examining the Registry Entries
 - Windows Startup Registry Entries
 - Startup Programs Monitoring Tools
 - Suspicious Files and Folders Detection
 - Reliability Check of Files & Folder
 - Network Activity Detection
- ✓ Backdoors
 - What is Backdoor?
 - Backdoor Installation Process
 - System Control through backdoor
- ✓ Prevention Techniques
 - Protection from Trojan Attacks
 - Protection from Backdoor Attacks
- ✍ **Virus**
 - ✓ Introduction to Virus
 - Working of Viruses: Infection Phase
 - Working of Viruses: Attack Phase
 - Purpose of Computer Viruses
 - Computer infection by Viruses
 - Signs of Virus Attack
 - Virus Hoaxes
 - Virus Analysis
 - ✓ Types of Virus
 - Characteristics, Symptoms of Viruses



- System or Boot Sector Viruses
- Life Cycle of Viruses
- Famous Virus Program
- Virus Detection Method
- Countermeasures

Worms

- ✓ Computer Worms
- ✓ Difference between Worm & Virus
- ✓ Worm Analysis

Spyware

- ✓ Spyware: Introduction
- ✓ What does a Spyware do?
- ✓ Types of Spywares
- ✓ Routes of Infection
- ✓ Internet and E-mail Spyware
- ✓ Effects & Behaviors
- ✓ Difference between Spyware and Adware

Prevention Methods

- ✓ Anti-Spyware Program
- ✓ Anti-Virus Program
- ✓ Defense against Worms

Module 9: SQL Injection

SQL Injection Concepts

- ✓ Basics of SQL
- ✓ Web Application Working
- ✓ Introduction to Server Side Technologies
- ✓ HTTP Methods
- ✓ HTTP POST Method Basics

Testing for SQL Injection

- ✓ Identifying SQL Injection via
 - Error Messages
 - Attack Characters



- ✓ Techniques to identify SQL Injection
- ✓ Pentesting methodologies for SQL Injection
- ✎ **Types of SQL Injection**
 - ✓ Types of SQL Injection
 - ✓ Simple SQL Injection Attack
 - ✓ Union SQL Injection Example
 - ✓ SQL Injection Error Based
- ✎ **Blind SQL Injection**
 - ✓ What is Blind SQL Injection?
 - ✓ Symptoms of Blind SQL Injection
 - ✓ Information extraction via Blind SQL injection
 - ✓ Exploitation techniques (MySQL)
- ✎ **Advanced SQL Injection**
 - ✓ Information Gathering
 - ✓ Features of different DBMSs
 - ✓ Extracting Information through error messages
 - ✓ Understanding parameters of an SQL Query
 - ✓ Evading website login pages
 - ✓ Master Data and Enumeration Tables
 - ✓ Creating Database Accounts for alternate access
 - ✓ Password Grabbing via Hash Extraction
 - ✓ Database Transfer
 - ✓ Interacting with the Victim System
- ✎ **SQL Injection Tools**
 - ✓ BSQL Hacker
 - ✓ Marathon Tool
 - ✓ SQL Power Injector
 - ✓ Havij
 - ✓ SQLPoizon
- ✎ **Preventive measures for SQL Injection**
 - ✓ Defensive measures for Web Applications
 - ✓ Tools for detection of SQL Injection



Module 10: Cross Site Scripting

- ✍ Introduction Cross Site Scripting
- ✍ Cross-Site Scripting
- ✍ Ways of Launching Cross-Site Scripting Attacks
- ✍ Working Process of Cross-Site Scripting Attacks
- ✍ When will be an attack successful?
- ✍ Programming Languages Utilized in XSS Attacks
- ✍ Types of XSS Attacks
- ✍ Steps of XSS Attack
- ✍ Not Fixing CSS/XSS Holes Compromises
- ✍ Methodology of XSS
- ✍ How to protect Against XSS

Module 11: Sniffing

- ✍ Sniffing Concepts
- ✍ Sniffing Threats in Network
- ✍ Working of Sniffers
- ✍ **Types of Sniffing**
 - ✓ Active Sniffing
 - ✓ Passive Sniffing
- ✍ Protocols Vulnerable for Sniffing
- ✍ **Sniffing Tools**
 - ✓ Wireshark
 - ✓ Tcpdump
 - ✓ Cain & able
 - ✓ NwInvestigator
- ✍ **Sniffing Prevention Techniques**
 - ✓ Wiretapping
 - ✓ Hardware Protocol Analyzers
 - ✓ Port mirroring
 - ✓ MAC Flooding



- ✍ Spoofing Attack
- ✍ IP Spoofing
- ✍ MAC Spoofing
- ✍ MAC Spoofing Impact
- ✍ MAC Spoofing Tool
- ✍ Prevention measures form MAC Spoofing
- ✍ **DNS Poisoning**
 - ✓ DNS Poisoning Methodologies
 - ✓ Intranet DNS Spoofing
 - ✓ DNS Cache Poisoning
 - ✓ Prevention measures from DNS Spoofing

Module 12: Social Engineering

- ✍ **Introduction to Social Engineering**
 - ✓ What is Social Engineering?
 - ✓ Techniques of Social Engineering
 - ✓ Attempt Using Phone, E-mail, Traditional Mail, In person, Dumpster Diving, Insider Accomplice, Extortion and Blackmail, Websites, Shoulder surfing, Third Person Approach, Technical Support
 - ✓ Computer based Social Engineering
 - ✓ Social Networking Sites –Impersonation platform/medium
- ✍ **Social Engineering Prevention Methods**
 - ✓ Policies
 - ✓ Techniques to prevent Social Engineering Methods
 - ✓ Identifying Phishing Emails
 - ✓ Anti-Phishing Toolbar

Module 13: Identity Theft Fraud

- ✍ Introduction to Identity Theft
- ✍ Identity Theft Occurrence
- ✍ Impact of Identity Theft Fraud



- ✍ Types of Identity Theft
- ✍ Dumpster Diving
- ✍ Change of ID
- ✍ E-Mail Theft
- ✍ Smishing
- ✍ Vishing
- ✍ Data Breach
- ✍ Overlays
- ✍ ATM Schemers / Hand-held Skimmers
- ✍ Shoulder Surfing
- ✍ Prevention Techniques

Module 14: Denial of Service

- ✍ **DDOS Concepts**
 - ✓ Concept: Denial of Service
 - ✓ Introduction to Distributed Denial of Service Attacks?
 - ✓ Working of Distributed Denial of Service Attacks?
 - ✓ Symptoms of a DOS Attack
 - ✓ Impact DDOS/DOS Attack
 - ✓ Difference of DDOS & DOS
- ✍ **DoS/DDoS Attack Techniques**
 - ✓ Types of DOS Attack
 - ✓ Smurf Attack
 - ✓ Buffer Overflow Attack
 - ✓ Ping of Death Attack
 - ✓ Tear Drop Attack
 - ✓ SYN Attack
 - ✓ Concept of Reflected DOS
 - ✓ Permanent Denial of Service Attack
 - ✓ Mitigate the DDOS/DOS Attack



- ✍ **Botnets**
 - ✓ Introduction to Botnet
 - ✓ Botnet Propagation Technique
 - ✓ Detection Techniques
 - ✓ How to defend against Botnets

odule 15: Session Hijacking

- ✍ Session Hijacking Concepts
- ✍ What is Session Hijacking?
- ✍ **Types of Session Hijacking**
 - ✓ Active
 - ✓ Passive
- ✍ Success rate of Session Hijacking
- ✍ Techniques for Session Hijacking
- ✍ **Phases of Session Hijacking**
 - ✓ Tracking the session
 - ✓ Desynchronizing the connection
 - ✓ Session Sniffing
 - ✓ Predictable Session Token
- ✍ **Difference between Spoofing and Session Hijacking**
 - ✓ Man-in-the-Middle Attack
 - ✓ Man-in-the-Browser Attack
 - ✓ Steps to perform Man-in-the-Browser Attack
- ✍ **Session Hijacking Tools**
 - ✓ Greasemonkey with cookie injector
 - ✓ Paros
 - ✓ Burp Suite
 - ✓ Firesheep
- ✍ **Prevention Methods**
 - ✓ Browser protection
 - ✓ Methodologies to prevent Session Hijacking
 - ✓ IPSec
 - ✓ Modes of IPSec



- ✓ Architecture of IPSec
- ✓ IPSec Authentication and Confidentiality
- ✓ IPSec Components and Implementation

Module 16: Penetration Testing

✍ Pen Testing Concepts

- ✓ Security and Vulnerability Assessments
- ✓ Limitations of Vulnerability Assessments
- ✓ What is Penetration Testing?
- ✓ Why Penetration Testing is Necessary?

✍ Types of Pen Testing

- ✓ Penetration Testing Types
- ✓ External Penetration Testing
- ✓ Internal Security Assessment
- ✓ Black Box Penetration Testing
- ✓ Grey Box Penetration Testing
- ✓ White Box Penetration Testing

✍ Pen Testing Phases

- ✓ Phases of Penetration Testing
- ✓ Pre-Attack Phase
- ✓ Attack Phase
- ✓ Enumerating Devices
- ✓ Post Attack Phase
- ✓ Penetration Testing Deliverable Templates

✍ Pen Testing Methodology

- ✓ Terms Of Agreement
- ✓ Project Scope
- ✓ Application Security Assessment
- ✓ Web Application Testing
- ✓ Network Security Assessment



- ✓ Wireless/Remote Access Assessment
- ✓ Wireless Testing
- ✓ TeleSocial Engineering
- ✓ Denial of Service Assessment

✍ **Pen Testing Tools**

- ✓ Different types of Pentest Tools
- ✓ Application Security Assessment Tool: Webscarab
- ✓ Application Security Assessment Tool: Angry IP Scanner
- ✓ Application Security Assessment Tool: GFI LANguard
- ✓ Wireless/ Remote Access Assessment Tool: Kismet
- ✓ Telephony Security Assessment Tool: Omnippeek
- ✓ Testing Network- Filtering Device Tool: Traffic IQ Professional
- ✓ Metasploit Framework

✍ **Vulnerability Assessment**

- ✓ Concept of Vulnerability Assessment
- ✓ Purpose Types of Assessment
- ✓ Vulnerability Classification
- ✓ How to Conduct Vulnerability Assessment
- ✓ Vulnerability Analysis Stages
- ✓ Vulnerability Assessment Considerations
- ✓ Vulnerability Assessment Reports
- ✓ TimeLine and Penetration Attempts
- ✓ Vulnerability Assessment Tools

Module 17: Exploit Writing & Buffer Overflow

✍ **Exploit Writing**

- ✓ Concept of Exploit Writing
- ✓ Purpose of Exploit Writing
- ✓ Requirements of Exploits Writing & Shell Codes
- ✓ **Types of Exploits**
 - Stack Overflow Exploits



- Heap Corruption Exploit
- Format String Attack
- Integer Bug Exploits
- Race Condition
- TCP/IP Attack
- ✓ The Proof-of-Concept and Commercial Grade Exploit
- ✓ Converting a Proof of Concept Exploit to Commercial Grade Exploit
- ✓ Attack Methodologies
- ✓ Socket Binding Exploits
- ✓ Steps for Writing an Exploit
- ✓ Shellcodes
- ✓ Null Byte
- ✓ Types of Shellcode
- ✓ Steps for Writing a ShellCode
- ✓ Issues Involved With Shellcode Writing
- ✓ Buffer
- ✓ Static Vs Dynamic Variables
- ✓ Stack Buffers, Data Region and Memory Process Regions
- ✓ About the Stack
- ✓ Need of Stack, Stack Region, Stack frame, Stack pointer, Procedure Call (Procedure Prolog) , Return Address (RET), Word Size and Buffer Overflows
- ✓ Why do we get a segmentation violation and Segmentation Error
- ✓ Writing Windows Based Exploits
- ✓ EIP Register and ESP
- ✓ Metasploit Framework, msfconsole
- ✓ Development with Metasploit
- ✓ Need for Creating of Exploit
- ✓ Determining the Attack Vector
- ✓ Debugger
- ✓ Determine the offset & pattern create
- ✓ Where to place the Payload?

✎ **Buffer Overflow**

- ✓ Why Applications are Vulnerable
- ✓ Buffer Overflow Attack
- ✓ Reasons of Buffer Overflow
- ✓ Knowledge for Buffer Overflow



- ✓ Understanding Stacks
- ✓ Understanding Heaps
- ✓ Types of Buffer Overflow Attack
- ✓ Stack Based
- ✓ Heap Based
- 👍 Heap Memory Buffer Overflow Bug
- 👍 Understanding Assembly Language
- 👍 Intro of Shell Code
- 👍 Detection of Buffer Overflows in a Program
- 👍 Attacking a Real Program
- 👍 Once the Stack is Smashed
- 👍 NOPS
- 👍 Mutate a Buffer Overflow Exploit
- 👍 Comparing Functions of libc and libsafe

Module 18: Cryptography & Steganography

- 👍 **Cryptography**
 - ✓ Concept of Cryptography
 - ✓ Advantages and uses of Cryptography
 - ✓ PKI (Public Key Infrastructure)
 - ✓ Algorithm's of encryption – RSA, MD5, SHA, SSL, PGP, SSH, GAK
 - ✓ Concept of Digital Signature
 - ✓ Encryption Cracking Techniques
 - ✓ Disk Encryption
 - ✓ Cracking S/MIME encryption using idle CPU time
 - ✓ Concept of Command Line Scriptor and Crypto Heaven, Cyphercalc
 - ✓ CA (Certificate Authority)
- 👍 **Steganography**
 - ✓ What is Steganography?
 - ✓ History
 - ✓ Steganography Today
 - ✓ Steganography Tools



- ✓ Steganalysis
 - What is Steganalysis?
 - Types of Analysis
 - Identification of Steganographic Files
- ✎ **Steganalysis meets Cryptanalysis**
 - ✓ Password Guessing
 - ✓ Cracking Steganography Programs
- ✎ **Conclusions**
 - ✓ What's in the Future?
 - ✓ Other tools in the wild

Module 19: Firewalls & Honeypots

- ✎ **Firewall**
 - ✓ What Does a Firewall Do?
 - ✓ What a Firewall cannot do
 - ✓ How does a Firewall work?
 - ✓ Types of Firewall
 - ✓ Working of Firewall
 - ✓ Advantages and Disadvantages of Firewall
 - ✓ Firewalls Implementing for Authentication Process
 - ✓ Types of Authentication Process
 - ✓ **Steps for Conducting Firewall Penetration Testing**
 - Locate the Firewall
 - Traceroute to identify the network range
 - Port scan the router
 - Grab the banner
 - Create custom packet and look for firewall responses
 - Test access control Enumeration
 - Test to indentify firewall architecture
 - Test firewall using firewalking tool
 - Test for port redirection
 - Test Convert channels
 - Test HTTP Tunneling
 - Test firewall specific vulnerabilities



- ✍ How to Bypassing the Firewall
- ✍ **Honeypots**
 - ✓ Concept of Honeypots
 - ✓ Purpose and working of Honeypots
 - ✓ Advantages and Disadvantages of Honeypots
 - ✓ Types of Honeypots
 - ✓ Uses of Honeypots
 - ✓ Detecting Honeypot
 - ✓ Honeynets
 - ✓ Architecture of Honeynet
 - ✓ Working process of Honeynet
 - ✓ Types of Honeynet
 - ✓ Honeywall CDROM

Module 20: IDS & IPS

- ✍ Concept of IDS (Intrusion Detection System)
- ✍ History and Characteristics of IDS
- ✍ Importance of IDS
- ✍ Deployment of IDS
- ✍ Intro, Advantages and Components of Distributed IDS
- ✍ Aggregate Analysis with IDS
- ✍ **Types and Architecture of IDS**
 - ✓ Network Based IDS
 - ✓ Host Based IDS
- ✍ Diff. Between Network Base IDS and Host Base IDS
- ✍ Methods to Detect IDS
- ✍ Signatures
- ✍ **Types of Signature**
 - ✓ Network Signatures
 - ✓ Host-based Signatures
 - ✓ Compound Signatures



- ✍ Methods to Detect Signature
- ✍ Prelude of IDS
- ✍ Concept of IPS (Intrusion Prevention System)
- ✍ Diff. Between IDS and IPS
- ✍ Network Antivirus Software

Module 21: Hacking Web Server

- ✍ **Web Servers**
 - ✓ Working process of Web Server
 - ✓ Loopholes of Web Server
 - ✓ Introduction of Popular Web Server and Common Security Threats
 - ✓ Apache Vulnerability
 - ✓ Attacks against IIS
 - ✓ Components of IIS
 - ✓ IIS Directory Traversal
 - ✓ Unicode and Unicode Directory Traversal Vulnerability
 - ✓ Unspecified Executable Path Vulnerability
 - ✓ File System Traversal Counter measures
 - ✓ WebDAV / ntdll.dll Vulnerability
 - ✓ RPC DCOM Vulnerability
 - ✓ ASN Exploits
 - ✓ IIS Logs
 - ✓ Escalating Privileges on IIS
 - ✓ Hot Fixes and Patches
 - ✓ Countermeasures of Web Server

Module 22: Wireless Hacking

- ✍ Wireless Technology
- ✍ Introduction to wireless networking
- ✍ Basics & Terminologies
- ✍ Advantages of Wireless Technology



- ✍ Components of Wireless Network
- ✍ Types of Wireless Network
- ✍ Setting and detecting a Wireless Network
- ✍ Advantages and Disadvantages of Wireless Network
- ✍ Antennas, SSID, Access Point Positioning and Rogue Access Point
- ✍ Concept of Wired Equivalent Privacy (WEP)
- ✍ MAC Sniffing & AP Spoofing
- ✍ Terminology of Wi-Fi Access
- ✍ Denial-of-Service and MITM Attack in Wi-Fi
- ✍ Wireless Intrusion Detection System
- ✍ Tips to Secure Wireless Network

Module 23: Physical Security

- ✍ Physical Security
- ✍ Current Statistics
- ✍ Accountability and Need of Physical Security
- ✍ Factors Affecting Physical Security
- ✍ Physical Security Checklist
 - ✓ Company Surroundings
 - ✓ Premises
 - ✓ Reception
 - ✓ Server
 - ✓ Workstation Area
 - ✓ Wireless Access Points
 - ✓ Other Equipments such as fax, removable media etc
 - ✓ Access Control
 - ✓ Computer Equipment Maintenance
 - ✓ Wiretapping
 - ✓ Remote Access
 - ✓ Locks
 - ✓ Spyware



Module 24: Reverse Engineering

- ✍ Concept of Reverse Engineering
- ✍ Positive Application of Reverse Engineering
- ✍ Ethical Reverse Engineering
- ✍ DMCA ACT
- ✍ Disassembler
- ✍ Decompilers
- ✍ Program Obfuscation
- ✍ Why do you need to decompile?
- ✍ NET Obfuscator and NET Obfuscation
- ✍ Java Byte Code Decompilers
- ✍ How does OllyDbg Work?

Module 25: Email Hacking

- ✍ Concept of Email
- ✍ Spam and Spam Laws
- ✍ E-Mail Tracking By Header
- ✍ Concept of Fake E-mails
- ✍ Various Steps to send Fake mails
- ✍ Trace IP by PHP Script

Module 26: Security Compliance and Auditing

- ✍ Security Compliance and Auditing
- ✍ What is Compliance?
- ✍ Need for Security Compliance
- ✍ **Standards for Security Compliance**
 - ✓ ISO 27001
 - ✓ PCI DSS



- ✍ Introduction to IT Auditing
- ✍ What is Security Auditing?
- ✍ What is the need for Security Auditing?
- ✍ Relevance of Compliance Standards in Auditing
- ✍ Importance of Risk Management

Module 27: Incident Handling & Computer forensics

- ✍ Understanding Incidents
- ✍ Exploring the Incident Paradigm: Classifications and Meaning
- ✍ Incidents: Types and Functionality
- ✍ Controlling Incidents
- ✍ Incident Response: A Brief Overview
- ✍ Incident Response: Structural Design
- ✍ Incident Handling
- ✍ Computer Security Incident Response Team (CSIRT)?
- ✍ Define Computer Forensics
- ✍ Key Rules for Computer Forensics
- ✍ Computer Forensic Procedure
- ✍ Identification of Evidence
- ✍ Acquisition
- ✍ Preservation of Evidence
- ✍ Analysis of Evidence
- ✍ Documentation
- ✍ File Recovery, Data Analysis, Screen Capture
- ✍ Mail Password Viewer, Network Password Viewer
- ✍ IE History Viewer
- ✍ Mozilla Cookie Viewer
- ✍ Chain of Custody
- ✍ Introduction of Memory Forensics