Course Name: **Advanced Diploma on Information Security**

Course Duration: **1 Year**

Prerequisites: **Candidate should be HSC Pass & Basic Knowledge of Computer**

Courses Covered:

a. Linux essentials
b. Certificate in Information Security (CISE) Level 1
c. CISE Level 2 – Network Security
d. CISE Level 2 – Web Application Security
e. CISE Level 2 – Exploit Writing
f. CISE Level 2 – Cloud Security

Features:

a. 12 Months Diploma Certificate
b. 10+ Certifications
c. Up to 6 Months Industrial Training Certificate
d. 2 Projects & Assignments
e. International Validity of the Certifications & the Diploma
f. 1 Year after course support
g. 100% Placement Assistance
h. Case studies & Research Paper
I. Online & Offline Batches

Course Module

Linux Essentials & Lab Setup

- Accessing the Command Line
- Getting Help in Red Hat Enterprise Linux
- Managing Files from the command Line
- Managing Local Users and Groups
- Creating, Viewing & Editing Test Files
- Monitoring and Managing Linux Process
- Controlling Access to Files

- Controlling Services and Daemons
- Analyzing and Storing Logs
- Configuring and Securing SSH
- Archiving and Transferring Files
- Managing Networking
- Accessing Linux File System
- Installing and Updating Software Packages
- Analyzing Servers and Getting Support

Certified Information Security Expert Level 1 Modules:-

- Networking & Basics
- Foot printing
- Google Hacking
- Scanning
- Windows Hacking
- Linux Hacking
- Trojans & Backdoors
- Virus & Worms
- Proxy Server & Packet Filtering
- Denial of Service
- Sniffer
- Social Engineering
- Physical Security
- Steganography
- Cryptography
- Wireless Hacking
- Firewall & Honeypots
- IDS & IPS
- Vulnerability Assessment
- Penetration Testing
- Session Hijacking
- Hacking Web Servers
- SQL Injection
- Cross Site Scripting
- Exploit Writing
- Buffer Overflow
- Reverse Engineering
- Email Hacking
- Incident Handling & Response
- Mobile Phone Hacking
- Cloud Computing and Security
- IOT Hacking
- Vulnerabilities Analysis

Certified Information Security Expert WEB APP SECURITY Modules:-

- Web Architectures
- Web Application Introduction
- PHP-Basics
- Sessions & Cookies
- XSS Attacks
- Advanced SQLI
- Cross Site Request Forgery
- Session Hijacking
- Web based DDOS Attacks
- Cookie Poisoning
- PHP Injection
- Web Based Worms
- Flash based Web Attacks
- I-Frame based Web Attacks
- Clickjacking
- Attack frameworks: AttackAPI & BeEF
- Penetration testing on DVWA
- Honeytokens
- OWASP Top 10
- Metasploit and Web Application
- PHP Curl
- Automated Bots
- Phishing 2.0
- Brute forcing Web Applications
- Compliance Methodologies and Legalities
- Capture the Flag Exercise

Certified Information Security Expert NETWORK SECURITY Modules:-

- Network Topology
- Open Systems Interconnectivity Model
- TCP/IP In-depth
- WAP, NAT, DNS and ICMP
- Internet Routing
- Advanced Port Scanning
- Sniffing Attacks
- Masquerading Attacks
- Advanced DOS and DDOS
- Session Hijacking Attacks
- Network Operations Center - Security
- Network Traffic Analysis
- Network Vulnerability Assessment
- Network Penetration Testing
- Intrusion Detection System
- Snort 101

- OSSEC 102
- Intrusion Prevention System
- Firewalls (Installation, Configuration and Usage)
- OS Hardening for Networks - Linux and Windows
- Cryptography - Introduction
- Symmetric Key Encryption
- Asymmetric Key Encryption
- Hash functions
- Trust models
- VLAN - Security
- VPN - Security
- Wireless Networks - Introduction
- Radio Frequency Essentials
- Wireless Security - Basics
- Wireless Threats

- Attacking Wireless Hotspot and Security
- WEP Security
- WPA/WPA2 Security
- Secure Wireless Infrastructure Deployment
- DNS Tunneling
- Network Forensic Methodology
- Network Evidence Acquisition
- OS Logs and Splunk

<u>Certified Information Security Expert Exploit Writing Modules</u>:-

- Programming & Basics
- Assembly language
- Debugging
- Stack Based Buffer Overflow
- Understanding Windows Shellcode
- Fuzzers
- Heap Based Overflow
- Exploiting /GS Canary Protected Programs
- Exploiting SafeSEH Protected Programs
- Denial of Service
- Bypassing DEP & ASLR
- Advanced Shellcoding (Win32 Egghunting, Connect-back, Staged, Alphanumeric)
- Encoders & Writing Custom Encoders
- DLL Hijacking
- Client Side Exploits
- From Vulnerability to Exploit
- Metasploit Framework
- Binary payloads & Antivirus Evasion
- Exploit to Metasploit
- Capture The Flag Exercise

Certified Information Security Expert Level 2: Cloud Security Modules

- Introduction to Cloud Computing
- Features of Cloud Computing
- Basic Concepts
- Cloud Deployment Models
- Cloud Computing Services
- Cloud Computing Benefits
- Cloud Computing Threats or Risks
- Cloud Computing Attacks
- Cloud Security
- Cloud Security Controls
- Responsibilities in Cloud Security
- Cloud Service Provider
- Cloud Customer
- Responsibilities of a Cloud Customer
- Cloud Security Tools

Python Programming

- Python - An Introduction
- Comparisons of Python with other Language
- Python Variables & Data Types
- Operators
- Python Conditional Statements
- Python Looping Concept
- Control Statements
- Data Type Casting
- Python Number
- String
- Python
- Python Tuple
- Python Dictionary
- Python Array
- Python Date & Time
- File Handling (Input / Output)
- Multithreading
- Python Mail Sending Program
- Database Connection
- OOPs Concepts

Thank you for showing your interest in Innobuzz Learning Solutions LLP

You can visit us at www.innobuzz.in for further information.