innobuzz KNOWLEDGE SOLUTIONS

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

Course Duration: **300 Hours; 12 Months (10 Months Training + 2 Months Project Work)**

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

Course Fee: **Rs.60,000**

Courses Covered:

a. Certificate in Information Security (CISE) Level 1 - Basic
b. CISE Level 2 – Network Security
c. CISE Level 2 – Web Application Security
d. CISE Level 2 – Exploit Writing
e. Cyber Forensics
f. Wi-fi Hacking

Features:

a. 12 Months Diploma Certificate
b. 4 Certifications
c. 6 Months Industrial Training Certificate
d. 2 Projects and their Certificates
e. International Validity of the Certifications & the Diploma
f. 12 Months Webinar Subscription Inclusive
g. 24X7 Student Support Desk
h. 100% Job Assistance

Course Module

Certified Information Security Expert Level 1 Modules:-

- Networking & Basics
- Footprinting
- 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
- Bluetooth Hacking
- Mobile Phone Hacking

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

Certified Information Security Expert EXPLOIT WRITING Modules:-

- 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

Cyber Forensics:-

- Memory Forensics
- Memory Acquisition
- Volatility for RAM Analysis
- File Carving
- Fuzzy Hashing
- Analysis of Extracted Malware Specimen
- Data Recovery

- Storage Fundamentals
- FAT32
- EXT2/EXT3
- Data Recovery Procedures
- Data Recovery (NTFS & FAT)
- Internet Fraud
- Application Threats
- Network Based Threats
- Identity Theft
- Friendly Fraud
- Internal Fraud
- Monitoring System
- Applicant Authentication
- Web system environment tracking
- False address tracking
- Various data checkpoints
- Controls for Online Banking Enrollment
- Tracking and Reporting Losses Associated with Online Banking
- Mobile Phone Cloning
- Security of GSM and CDMA
- Security of Phones
- Checking for cloning
- SIM Cloning
- SIM and carriers
- Formats
- Data
    - ICCID
    - International mobile subscriber identity (IMSI)
    - Authentication key (Ki)
    - Location area identity
    - SMS messages and contacts
- SIM Reader/Writer
- Worn Scan

Wi-Fi Hacking:-

- WEP / WPA
- Key Management
- Data Privacy & Integrity

- Sniffers
- Monitoring Traffic
- Injecting Packets
- Wireless Lab Setup
- Chipsets and Linux Drivers
- GPS on Operating Systems
- Vistumbler
- Deauth Attack
- Attacking a WPA Protected Network
- Cracking WPA-PSK on OS X
- Decrypting WPA-PSA Captures
- Bridging the Air Gap
- Gathering 802.11 Intel
- Managing OS X's Firewall
- Microsoft NetMon
- Cracking

Project Work:

Refer projects file