CRAW
Security

Learn | Research | Innovate

6 MONTH DIPLOMA IN INFORMATION SECURITY

Craw Security Focus on Delivering Best **INDUSTRY CERTIFICATIONS**

EC-Council CISCO CompTIA

RedHat python PECB

CERTNEXUS Beingcert

crawsec crawsec crawsec

www.craw.in

ETHICAL HACKING
LEVEL 1

- Module 01 : Introduction to Basics of Ethical Hacking
- Module 02 : Foot-printing Active (Tool Based Practical)
- Module 03 : Foot-printing Passive (Passive Approach)
- Module 04 : In-depth Network Scanning
- Module 05 : Enumeration User Identification
- Module 06 : System Hacking Password Cracking & Bypassing
- Module 07 : Viruses and Worms
- Module 08 : Trojan and Back door
- Module 09 : Bots and Botnets
- Module 10 : Sniffers MITM with Kali
- Module 11 : Sniffers MITM with Windows
- Module 12 : Social Engineering Techniques Theoretical Approach
- Module 13 : Social Engineering Toolkit Practical Based Approach
- Module 14 : Denial of Service DOS & DDOS Attacks
- Module 15 : Web Session Hijacking
- Module 16 : SQL Injection Manual Testing
- Module 17 : SQL Injection Automated Tool Based Testing
- Module 18 : Basics of Web App Security
- Module 19 : Hacking Web servers Server Rooting
- Module 20 : Hacking Wireless Networks Manual CLI Based
- Module 21 : Hacking Wireless Network
- Module 22 : Evading IDS, Firewall
- Module 23 : Honey pots
- Module 24 : Buffer Overflow
- Module 25 : Cryptography
- Module 26 : Penetration Testing: Basics
- Module 27 : Mobile Hacking
- Module 28 : Internet of Things (IOT) Hacking
- Module 29 : Cloud Security and many more

ADVANCED PENETRATION TESTING
LEVEL 2

- Module 01 : Introduction
- Module 02 : In-Depth Scanning
- Module 03 : Exploitation
- Module 04 : Domain Domination
- Module 05 : Getting Comfortable with Kali Linux
- Module 06 : Command Line Fun
- Module 07 : Practical Tools
- Module 08 : Bash Scripting
- Module 09 : Passive Information Gathering
- Module 10 : Active Information Gathering
- Module 11 : Vulnerability Scanning
- Module 12 : Web Application Attacks
- Module 13 : Introduction to Buffer Overflows
- Module 14 : Windows Buffer Overflows
- Module 15 : Linux Buffer Overflows
- Module 16 : Client-Side Attacks
- Module 17 : Locating Public Exploits
- Module 18 : Fixing Exploits
- Module 19 : File Transfers
- Module 20 : Antivirus Evasion
- Module 21 : Privilege Escalation
- Module 22 : Password Attacks
- Module 23 : Port Redirection and Tunneling
- Module 24 : Active Directory Attacks
- Module 25 : Power Shell Empire
- Module 26 : Penetration Test Breakdown
- Module 27 : Trying Harder: The Labs

CYBER FORENSICS INVESTIGATION
LEVEL 3

- Module 01 : What is Computer Forensics
- Module 02 : Methods by which Computer gets Hacked
- Module 03 : Computer Forensics Investigation Process
- Module 04 : IDigital Evidence Gathering
- Module 05 : Computer Forensics Lab
- Module 06 : Setting up Forensics Lab
- Module 16 : Forensics Investigations Using Encase Tool
- Module 17 : Stenography and Image File Forensics
- Module 18 : Application Password Crackers
- Module 19 : Log Computing and Event Correlation
- Module 20 : Network Forensics Tools : Cellebrite Tool
- Module 21 : Investigating Tools

- Module 07 : Understanding Hard Disk
- Module 08 : File Systems Analysis : Linux/Window/mac
- Module 09 : Windows File Systems forensics
- Module 10 : Data Acquisition Tools and techniques
- Module 11 : Data Imaging Techniques and Tools
- Module 12 : Recovery Deleted Files and Folders
- Module 13 : Deleted Partitions Recovery Technique
- Module 14 : Forensics Investigations Using Forensics Toolkit (FTK)
- Module 15 : Forensics Investigations Using Forensics Toolkit (Oxygen)
- Module 22 : Investigating Network Traffic : Wireshark
- Module 23 : Investigating Wireless Attacks
- Module 24 : Investigating Web Application Attacks via Logs
- Module 25 : Tracking and Investigating Various Email Crimes
- Module 26 : Detailed Investiave Report

IN-DEPTH NETWORKING

LEVEL 4

- Module 01 : Introduction to Networking
- Module 02 : OSI Model
- Module 03 : TCP/IP Model
- Module 04 : Subnetting / Summarisation
- Module 05 : Packet Flow in Same & Different Network
- Module 06 : Information About Networking Device
- Module 07 : IP / ICMP
- Module 08 : APIPA
- Module 09 : Address Resolution Protocol
- Module 10 : Routing Protocols (Static & Dynamic)
- Module 11 : Static - Next Hop / Exit Interface
- Module 12 : Dynamic - RIP / EIGRP / OSPF & BGP
- Module 13 : Wan Technologies
- Module 14 : NAT
- Module 15 : ACL
- Module 16 : Dynamic Host Configuration Protocol
- Module 17 : Telnet & SSH
- Module 18 : Load Balancing Protocol
- Module 19 : Layers 2 Protocols
- Module 20 : VLAN
- Module 21 : Different Types of STP
- Module 22 : Ether Channel (L2)
- Module 23 : Port Security

WEB APPLICATION SECURITY

LEVEL 5 OWASP TOP 10 & SANS 25

- Module 01 : Improper Neutralization of Special Elements used in an OS Command (‘OS Command Injection’)
- Module 02 : SQL Injection
- Module 03 : Code Injection
- Module 04 : Unrestricted Upload of File with Dangerous Type
- Module 05 : Download of Code Without Integrity Check
- Module 06 : Inclusion of Functionality from Untrusted Control Spher
- Module 07 : Missing Authentication for Critical Function
- Module 08 : Improper Restriction of Excessive Authentication Attempts
- Module 09 : Use of Hard-coded Credentials
- Module 10 : Reliance on Untrusted Inputs in a Security Decision
- Module 11 : Missing Authorization
- Module 12 : Incorrect Authorization
- Module 13 : Missing Encryption of Sensitive Data
- Module 14 : Cleartext Transmission of Sensitive Information
- Module 15 : XML External Entities
- Module 16 : External Control of File Name or Path
- Module 17 : Improper Authorization
- Module 18 : Execution with Unnecessary Privileges
- Module 19 : Use of Potentially Dangerous Function
- Module 20 : Incorrect Permission Assignment for Critical Resource
- Module 21 : Improper Neutralization of Input During web page Generation (Cross-Site Scripting)
- Module 22 : Use of Externally-Controlled Format String
- Module 23 : Integer Overflow or Wraparound
- Module 24 : Use of a Broken or Risky Cryptographic Algorithm
- Module 25 : Use of a One-way Hash Without a Salt
- Module 26 : Insufficient Logging and Monitoring

MOBILE APPLICATION SECURITY

LEVEL 6

- Module 01 : Improper Platform Usage
- Module 02 : Insecure Data Storage
- Module 03 : Insecure Communication
- Module 04 : Insecure Authentication
- Module 05 : Insufficient Cryptography
- Module 06 : Insecure Authorization
- Module 07 : Client Code Quality
- Module 08 : Code Tampering
- Module 09 : Reverse Engineering
- Module 10 : Extraneous Functionality

PYTHON PROGRAMMING

LEVEL 7

- Module 01 : Python - An Introduction
- Module 02 : Comparisons of Python with other Language
- Module 03 : Python Variables & Data Types
- Module 04 : Operators
- Module 05 : Python Conditional Statements
- Module 06 : Python Looping Concept
- Module 07 : Control Statements
- Module 08 : Data Type Casting
- Module 09 : Python Number
- Module 10 : String
- Module 11 : Python List
- Module 12 : Python Tuple
- Module 13 : Python Dictionary
- Module 14 : Python Array
- Module 15 : Python Date & Time
- Module 16 : File Handling (Input / Output)
- Module 17 : Multithreading
- Module 18 : Python Mail Sending Program
- Module 19 : Database Connection
- Module 20 : OOPs Concepts
- Module 21 : Interacting with Networks
- Module 22 : Graphical User Interface
- Module 23 : Python Web Scraping
- Module 24 : Python for Image Processing
- Module 25 : Python Data Science
- Module 26 : Intro with Python Matching Learning
- Module 27 : Intro with Python Artificial Intelligence
- Module 28 : Functions

EC-Council Red Hat CompTIA python
CISCO CERTNEXUS PECB Beingcert

CRAW Security

CRAW CYBER SECURITY PVT LTD
(Head Office)

1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate
Westend Marg, Behind Saket Metro Station
Saidulajab, New Delhi - 110030

Office Landline : (011) 4039 4315
Mobile : +91 964 364 8668 | 742 810 6667
+91 964 363 8668 | 965 020 2445

Email ID : info@craw.in
Website : www.craw.in

CRAW Security
Learn | Research | Innovate