CRAW
Security

Learn | Research | Innovate

1 YEAR MASTER DIPLOMA IN INFORMATION SECURITY

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

EC-Council CISCO CompTIA

RedHat python PECB

CERTNEXUS Beingcert Learn | CERTIFY | Grow

crawsec crawsec crawsec

www.craw.in

BASIC NETWORKING

LEVEL 1 : COURSE DURATION : 40 hrs

- 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

- ★ Weekend / Weekdays Classes
- ★ Classroom / Online Training
- ★ Internship Opportunity
- ★ 1 Year Membership
- ★ GNS/Packet Tracer
- ★ Video Nuggts
- ★ Audio Tutorial
- ★ Ebooks Tutorial

LINUX ESSENTIALS

LEVEL 2 : COURSE DURATION : 40 hrs

- Module 01 : Getting Started with Red Hat Enterprise Linux
- Module 02 : Accessing the Command Line
- Module 03 : Managing Files from the command Line
- Module 04 : Getting Help in Red Hat Enterprise Linux
- Module 05 : Creating, Viewing & Editing Test Files
- Module 06 : Managing Local Users and Groups
- Module 07 : Controlling Access to Files
- Module 08 : Monitoring and Managing Linux Process
- Module 09 : Controlling Services and Daemons
- Module 10 : Configuring and Securing SSH
- Module 11 : Analyzing and Storing Logs
- Module 12 : Managing Networking
- Module 13 : Archiving and Transferring Files
- Module 14 : Installing and Updating Software Packages
- Module 15 : Accessing Linux File System
- Module 16 : Analyzing Servers and Getting Support

PYTHON PROGRAMMING

LEVEL 3 : COURSE DURATION : 40 hrs

- 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

- ★ Weekend / Weekdays Classes
- ★ Classroom / Online Training
- ★ Internship Opportunity
- ★ 80% Practical 20% Theroetical

- 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

ETHICAL HACKING

LEVEL 4 : COURSE DURATION : 40 hrs

- 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

- ★ Weekend / Weekdays Classes
- ★ Classroom / Online Training
- ★ Internship Opportunity
- ★ 1 Year Membership
- ★ 80% Practical 20% Theroetical
- ★ 250 GB Toolkit
- ★ Extra Class / Backup Class
- ★ Course Certificate
- ★ Video Tutorial

- 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 5 : COURSE DURATION : 40 hrs

- Module 01 : Introduction
- Module 02 : In-Depth Scanning
- Module 03 : Exploitation
- Module 04 : Command Line Fun
- Module 05 : Getting Comfortable with Kali Linux
- Module 06 : Bash Scripting
- Module 07 : Practical Tools
- Module 08 : Active Information Gathering
- Module 09 : Passive Information Gathering
- Module 10 : Introduction to Buffer Overflows
- Module 11 : Buffer Overflows
- Module 12 : Fixing Exploits
- Module 13 : Locating Public Exploits
- Module 14 : Antivirus Evasion

- ★ Weekend / Weekdays Classes
- ★ Classroom / Online Training
- ★ Internship Opportunity
- ★ 80% Practical 20% Theroetical
- ★ Advanced Pentesting Class
- ★ Metasploit
- ★ VA/PT Tools

- Module 15 : File Transfers
- Module 16 : Windows Privilege Escalation
- Module 17 : Linux Privilege Escalation
- Module 18 : Password Attacks
- Module 19 : Port Redirection and Tunnelin
- Module 20 : Active Directory Attacks
- Module 21 : Power Shell Empire
- Module 22 : Trying Harder : The Labs
- Module 23 : Penetration Test Breakdown

CYBER FORENSICS INVESTIGATION

LEVEL 6 : COURSE DURATION : 60 hrs

- 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 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 Encase Tool
- Module 16 : Stenography and Image File Forensics
- Module 17 : Application Password Crackers

- ★ Weekend / Weekdays Classes
- ★ Classroom / Online Training
- ★ Internship Opportunity
- ★ 80% Practical 20% Theroetical
- ★ Software Toolkit
- ★ Ebooks
- ★ Practise Forensics Labs
- ★ Certification

- Module 18 : Log Computing and Event Correlation
- Module 19 : Investigating Tools
- Module 20 : Investigating Network Traffic : Wireshark
- Module 21 : Investigating Wireless Attacks
- Module 22 : Investigating Web Application Attacks via Logs
- Module 23 : Tracking and Investigating Various Email Crimes
- Module 24 : Detailed Investiave Report

WEB APPLICATION SECURITY

LEVEL 7 : COURSE DURATION : 60 hrs OWASP TOP 10 & SANS 25

- Module 01 : Introduction
- Module 02 : Owasp Top 10
- Module 03 : Recon for Bug Hunting
- Module 04 : Advanced SQL Injection
- Module 05 : Command Injection
- Module 06 : Session Management and Broken Authentication Vulnerability
- Module 07 : CSRF - Cross Site Request Forgery
- Module 08 : SSRF - Server Site Request Forgery
- Module 09 : XSS - Cross Site Scritpting
- Module 10 : IDOR - Insecure Direct Object Reference

- ★ Weekend / Weekdays Classes
- ★ Classroom / Online Training
- ★ Internship Opportunity
- ★ 1 Year Membership
- ★ Top 10 OWASP Training
- ★ Burpsuit/Proxy Interception
- ★ DVWA / SAMURAI 3.0
- ★ Vulnerable Web App Exploit

- Module 11 : Sensitive Data Exposure and Information Disclose
- Module 12 : SSTI - Server Site Template Injection
- Module 13 : Multi Factor Authentication Bypass
- Module 14 : HTTP Request Smuggling
- Module 15 : XXE - XML External Entities
- Module 16 : LFI - Local File Inclusion and RFI Remote File Inclusion
- Module 17 : Source Code Disclousre
- Module 18 : Directory Path Traversal
- Module 19 : AWS Pentesting
- Module 20 : HTML Injection
- Module 21 : Host Header Injection
- Module 22 : SQL Authentication Bypass
- Module 23 : File Upload Vulnerability
- Module 24 : JWT Token Attack
- Module 25 : Security Misconfiguration
- Module 26 : URL Redirection
- Module 27 : Flood Attack on Web

MOBILE APPLICATION SECURITY

LEVEL 8 : COURSE DURATION : 40 hrs

- 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

INTERNET OF THINGS (IOT) PENTESTING

LEVEL 9 : COURSE DURATION : 40 hrs

- Module 01 : Overview of Why IoT is so important
- Module 02 : Introduction of IoT
- Module 03 : Introduction to Sensor Network & Wireless protocol
- Module 04 : Review of Electronics Platform, Production & Cost Projection
- Module 05 : Conceiving a new IoT product- Product Requirement document for IoT
- Module 06 : Introduction to Mobile app platform & Middleware for IoT
- Module 07 : Machine learning for intelligent IoT
- Module 08 : Analytic Engine for IoT
- Module 09 : Iaas/Paas/Saas-IoT data, platform and software as a service revenue model

END POINT SECURITY

LEVEL 10 : COURSE DURATION : 40 hrs

- Module 01 : Implementing Internet Security Anti Virus
- Module 02 : Two-Factor Authentication Implementation
- Module 03 : Mobile Device Management For Industry
- Module 04 : Data Loss Prevention Overview & Implementation
- Module 05 : Security Information and Event Management (SIEM)
- Module 06 : APT- Attack
- Module 07 : MITRE Framework
- Module 08 : EDR
- Module 09 : MDR
- Module 10 : Next Generation Firewall
- Module 11 : Unified Threat Management
- Module 12 : Physical Security
- Module 13 : ISO 27001 Lead Auditor Guidelines

AWS ASSOCIATE

LEVEL 11 : COURSE DURATION : 40 hrs

- Module 01 : Designing Highly Available, cost effective, scalable systems
  - (a) Planning and Design
  - (b) Monitoring and Logging
  - (c) Hybrid IT Architectures
  - (d) Elasticity and Scalability
- Module 02 : Implementation and Deployment
  - (a) Amazon EC2
  - (b) Amazon S3
  - (c) Amazon Web Service Cloud Formation
  - (d) Amazon Web Service VPS
  - (e) Amazon Web Service IAM
- Module 03 : Data Security
  - (a) AWS IAM (Identify and Access Management)
  - (b) Amazon Web Service VPC
  - (c) Encryption Solutions
  - (d) Cloud watch logs
  - (e) Disaster Recovery
  - (f) Amazon Route 53
  - (g) AWS Storage Gateway
  - (h) Amazon Web Service Import/Export
- Module 04 : Troubleshooting

AWS SECURITY

LEVEL 12 : COURSE DURATION : 40 hrs

- Module 01 : Given an AWS Abuse Notice, Evaluate a Suspected Compromised Instance or Exposed Access Key
- Module 02 : Verify that the Incident Response plan includes relevant AWS services
- Module 03 : Evaluate the Configuration of Automated Alerting and Execute Possible Remediation of Security-Related Incidents and Emerging Issues
- Module 04 : Design and implement security monitoring and alerting
- Module 05 : Troubleshoot security monitoring and alerting
- Module 06 : Design and Implement a Logging Solution
- Module 07 : Design Edge Security on AWS
- Module 08 : Troubleshoot Logging Solutions
- Module 09 : Design and implement a secure network infrastructure
- Module 10 : Troubleshoot a secure network infrastructure
- Module 11 : Design and implement host-based security
- Module 12 : Design and Implement a Scalable Authorization and Authentication System to Access AWS Resources
- Module 13 : Troubleshoot an Authorization and Authentication System to Access AWS Resources
- Module 14 : Design and implement key management and use
- Module 15 : Troubleshoot key management
- Module 16 : Design and implement a data encryption solution for data at rest and data in transit

OUR TRAINING **PARTNERS**

Craw Security Affiliate program, where you will promote our courses on your website or blog and start making money from it instantly without any special extra effort from your side. As we have 200+ certification and training programs, 70+ IT Professionals and certified instructors, and 30+ Authorizations, so you do not need to worry about any course training, and instructor for training purposes, we will simply take care of this.

We offer Registered and Authorized Certification from different Councils and Renowned Authorities, to our students from India and to the entire world as a Authorized Training Centre for

Training & Certification

EC-Council · Red Hat · CompTIA · python · cisco · CERTNEXUS · PECB · Beingcert Learn | CERTIFY | Grow

Head Office

Saket, New Delhi

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

Email ID : info@craw.in | training@craw.in
Tel : 011 - 4039 4315
Mobile Number : +91 951 380 5401
Website : www.craw.in

Laxmi Nagar, New Delhi

R31/ 32, 2nd floor , Jandu Tower, Vikas marg
Shakarpur, New Delhi - 110090

Email ID : info@craw.in | training@craw.in
Tel : 011 - 4504 0849
Mobile Number : +91 951 380 5401
Website : www.craw.in

CRAW Security
Learn | Research | Innovate

Payment Mode

1. One Shot Payment
2. Installment Availbale

Payment processing partner
Razorpay

Card, Wallets, UPI & Netbanking

VISA UPI Rupay

CRAW CYBER SECURITY PVT LTD

(Head Office | Saket, New Delhi)

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 : +91 951 380 5401

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

CRAW CYBER SECURITY

(Laxmi Nagar, New Delhi)

R31/ 32, 2nd floor , Jandu Tower
Vikas marg, Shakarpur
New Delhi - 110090

Office Landline : (011) 4504 0849
Mobile : +91 951 380 5401

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