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 OFFENSIVE security

crawsec crawsec crawsec

www.crawpatna.in

ETHICAL HACKING

LEVEL 1 : DURATION : 40 Hour

- 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 : DURATION : 40 Hour

- 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
- 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 3 : DURATION : 40 Hour

- 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 13 : Deleted Partitions Recovery Technique
- Module 14 : Forensics Investigations Using Forensics Toolkit (FTK)
- Module 15 : Stenography and Image File Forensics
- Module 16 : Application Password Crackers
- Module 17 : Log Computing and Event Correlation

- 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 18 : Investigating Network Traffic : Wireshark
- Module 19 : Investigating Wireless Attacks
- Module 20 : Investigating Web Application Attacks via Logs
- Module 21 : Tracking and Investigating Various Email Crimes
- Module 22 : Detailed Investiave Report

IN-DEPTH NETWORKING

LEVEL 4 : DURATION : 40 Hour

- 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 : Network Address Translation
- Module 15 : Access Control List
- Module 16 : Dynamic Host Configuration Protocol
- Module 17 : Telnet & SSH
- Module 18 : Load Balancing Protocol
- Module 19 : Layers 2 Protocols
- Module 20 : Virtual Local Area Network
- Module 21 : Different Types of STP
- Module 22 : Ether Channel (L2)
- Module 23 : Port Security

WEB APPLICATION SECURITY

LEVEL 5 : DURATION : 40 Hour 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
- 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 : HTML Injection
- Module 20: Host Header Injection
- Module 21 : SQL Authentication Bypass
- Module 22 : File Upload Vulnerability
- Module 23 : JWT Token Attack
- Module 24 : Security Misconfiguration
- Module 25 : URL Redirection
- Module 26 : Flood Attack on Web

MOBILE APPLICATION SECURITY

LEVEL 6 : DURATION : 40 Hour

- 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 : DURATION : 40 Hour

- 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 Machine Learning
- Module 27 : Intro with Python Artificial Intelligence
- Module 28 : Functions

OFFENSIVE security · EC-Council · Red Hat · CompTIA · python · CISCO · aws · Microsoft · CERTNEXUS · PECB

CRAW Security

CRAW CYBER SECURITY PVT LTD

(Head Office)

(Head Office)

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

606 (6 Floor), Verma Centre, Boring Road Crossing
Patna, Bihar 800001

Mobile : +91 997 379 1666 | +91 997 378 1666

Email ID : training@crawpatna.in
Website : www.crawpatna.in

CRAW Security

Learn | Research | Innovate