CRAW
Security

Learn | Research | Innovate

6 MONTHS INFORMATION SECURITY

DIPLOMA COURSE

Include 7 Courses **

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

EC-Council CISCO CompTIA

RedHat python PECB

CERTNEXUS OFFENSIVE security

crawsec crawsec crawsec crawsecurity

www.craw.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 : Computer Forensics in today's World
- Module 02 : Computer Forensics Investigation Process
- Module 03 : Hard-Disk and File-System
- Module 04 : Data-Acquisition and Duplication
- Module 05 : Defeating Anti-Forensics Techniques
- Module 06 : Windows Forensics

- Module 07 : Linux Forensics
- Module 08 : Network Forensics
- Module 09 : Web-Forensics
- Module 10 : Dark web–Forensics
- Module 11 : Cloud forensics
- Module 12 : Email-Forensics
- Module 13 : Malware Forensics
- Module 14 : Mobile forensics
- Module 15 : IOT forensics

BASIC NETWORKING

LEVEL 4 : DURATION : 40 Hour

- Module 01 : Computer Networking
- Module 02 : Introduction to Networking
- Module 03 : IPV4 and IPV6
- Module 04 : Subnet Mask, CIDR and Subnetting
- Module 05 : VLSM, Wild Card, Summarization
- Module 06 : OSI MODEL
- Module 07 : TCP / IP MODEL
- Module 08 : Network Devices, Cabling & Packet Tracer
- Module 09 : ARP and ICMP
- Module 10 : Packet Flow
- Module 11 : Routing - Static and Dynamic
- Module 12 : Static Routing - Next HOP IP & Exit Interface
- Module 13 : Dynamic - RIP
- Module 14 : EIGRP
- Module 15 : OSPF
- Module 16 : Redistribution
- Module 17 : Remote Services (Telnet and SSH)
- Module 18 : DHCP
- Module 19 : ACL
- Module 20 : Switching
- Module 21 : L2 Protocols - CDP, VLAN, STP, DTP, VTP
- Module 22 : Ether - Channel
- 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 PTE LTD
(Singapore)

27 Paya Lebar Road,
#13-05 Paya Lebar Residences,
Singapore - 409042
Contact us : +65 9351 5400

Craw Cyber Security Pvt Ltd (Saket , New Delhi)
1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate
Westend Marg, Behind Saket Metro Station
Saidulajab, New Delhi - 110030

Craw Cyber Security Pvt Ltd (Laxmi Nagar, New Delhi)
R31/ 32, 2nd floor , Jandu Tower, Vikas marg
Shakarpur, New Delhi 110090

Mobile : +91 951 380 5401

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

CRAW Security
Learn | Research | Innovate