CRAW ACADEMY

Learn | Research | Innovate

ONE YEAR CYBER SECURITY

DIPLOMA COURSE POWERED BY AI

TRAINING PARTNERS

OffSec The Path to a Secure Future™ · Red Hat · EC-Council · CISCO · PECB · CompTIA · python

OUR PRODUCTS

SHIELDXOR · ThreatFusionAI™ · CRACK THE LAB Gamified way of learning through challenge Labs · PhishNext

BASIC NETWORKING WITH AI

LEVEL 1 : COURSE DURATION : 60 hrs

- Module 01: Introduction to Networking and AI Integration
- Module 02: Network Fundamentals
- Module 03: Routing and Switching
- Module 04: Access Control and Security
- Module 05: IP Services and Automation
- Module 06: Advanced Routing Concepts
- Module 07: Network Monitoring and Troubleshooting
- Module 08: AI-Enhanced Lab Sessions
- Module 09: Final Project
- Module 10: Certification and Career Path

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

LINUX ESSENTIALS COURSE

LEVEL 2 : COURSE DURATION : 40 hrs

- Module 01: How to configure VMware?
- Module 02: How to Download RHEL 9.3 for Free?
- Module 03: Get Started with Red Hat Enterprise Linux
- Module 04: Access the Command Line
- Module 05: Manage Files from the Command Line
- Module 06: Get Help in Red Hat Enterprise Linux
- Module 07: Create, View, and Edit Text Files
- Module 08: Manage Local Users and Groups
- Module 09: Control Access to Files
- Module 10: Monitor and Manage Linux Processes
- Module 11: Control Services and Daemons
- Module 12: Configure and Secure SSH
- Module 13: Analyze and Store Logs
- Module 14: Manage Networking
- Module 15: Archive and Transfer Files
- Module 16: Install and Update Software Packages
- Module 17: Access Linux File Systems
- Module 18: Analyze Servers and Get Support
- Module 19: Test Papers For Linux

PYTHON PROGRAMMING COURSE

LEVEL 3 : COURSE DURATION : 60hrs

- Module 01: Python – An Introduction Special Elements Used in an OS Command
- Module 02: Comparisons of Python with Other Languages
- Module 03: Python Variables & Data Types
- Module 04: Operators
- Module 05: Python Conditional Statements
- Module 06: Python Looping Concept
- Module 07: Python Control Statements
- Module 08: Python Data Type Casting
- Module 09: Python Number
- Module 10: Python String
- Module 11: Python List

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

- 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

ETHICAL HACKING WITH AI

LEVEL 4: **COURSE DURATION : 60hrs**

- Module 01: Introduction to the Basics of Ethical Hacking
- Module 02: Introduction of AI in the world of Ethical Hacking (ShellGPT, TerminalGPT, ChatGPT)
- Module 03: Prompt Engineering for hacking Scripts and payloads.
- Module 04: Footprinting (Active) Using ShellGPT scripts.
- Module 05: Footprinting (Passive) Using ShellGPT scripts.
- Module 06: In-depth Network scanning and Advanced AI-driven Nmap Script Generation
- Module 07: Enumeration User Identification
- Module 08: System Hacking, Password Cracking & Bypassing
- Module 09: Developing Viruses and Worms Using AI
- Module 10: Developing Trojan and Back Door
- Module 11: Developing Bots and Botnets
- Module 12: Sniffers MITM with Kali
- Module 13: Sniffers MITM with Windows
- Module 14: Social Engineering Techniques Theoretical Approach
- Module 15: Social Engineering Toolkit Practical-Based Approach Using AI
- Module 16: Denial of Service (DoS) & DDOS Attacks
- Module 17: Web Session Hijacking
- Module 18: SQL Injection Manual Testing using AI scripts
- Module 19: SQL Injection Automated Tool-Based Testing
- Module 20: Basics of Web App Security
- Module 21: Hacking Web Servers Using TerminalGPT

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

- Module 22: Hacking Wireless Networks Manual CLI-Based
- Module 23: Hacking Wireless Networks
- Module 24: Evading IDS, Firewall using AI
- Module 25: Honey pots
- Module 26: Buffer Overflow
- Module 27: Cryptography using an AI tool.
- Module 28: Penetration Testing: Basics
- Module 29: Mobile Hacking Payloads Using AI.
- Module 30: Internet of Things (IoT) Hacking
- Module 31: Cloud Security and many more

ADVANCED PENETRATION TESTING WITH AI

LEVEL 5 : **COURSE DURATION : 60 hrs**

- Module 01: Welcome to the World of Penetration Testing
- Module 02: Supercharged Scanning with AI
- Module 03: Exploitation Tactics Unleashed
- Module 04: Command Line Adventures with AI
- Module 05: Conquering Kali Linux Like a Pro
- Module 06: Master Bash Scripting with AI
- Module 07: AI-Powered Practical Tools

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

- Module 08: Active Information Gathering with AI
- Module 09: Passive Information Gathering with AI
- Module 10: Buffer Overflow Fundamentals
- Module 11: Advanced Buffer Overflow Attacks
- Module 12: Fixing Exploits with AI
- Module 13: Hunting Public Exploits with AI
- Module 14: Mastering Antivirus Evasion with AI
- Module 15: Seamless File Transfers with AI
- Module 16: Windows Privilege Escalation Demystified
- Module 17: Linux Privilege Escalation Tactics
- Module 18: Cracking Passwords with AI
- Module 19: Port Redirection and Tunneling with AI
- Module 20: Active Directory Attacks with AI
- Module 21: PowerShell Empire
- Module 22: The Labs - Real-World Challenges
- Module 23: Penetration Test Breakdown
- Module 24: Crafting Killer Penetration Test Reports

CYBER FORENSICS INVESTIGATION

LEVEL 6 : **COURSE DURATION : 60 hrs**

- Module 01: Computer Forensics in Today's World
- Module 02: Computer Forensics Investigation Process
- Module 03: Understanding Hard Disks and File Systems
- Module 04: Data Acquisition and Duplication
- Module 05: Defeating Anti-Forensics Techniques
- Module 06: Windows Forensics
- Module 07: Linux and Mac Forensics
- Module 08: Network Forensics
- Module 09 : Investigating Web Forensics
- Module 10 : Dark Web Forensics
- Module 11 : Cloud Forensics
- Module 12 : Investigating Email Crimes
- Module 13 : Malware Forensics
- Module 14 : Mobile Forensics
- Module 15 : IOT Forensics

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

WEB APPLICATION SECURITY WITH AI

LEVEL 7 : **COURSE DURATION : 40 hrs** OWASP TOP 10 & SANS 25

- Module 01: Introduction
- Module 02: OWASP Top 10
- Module 03: Recon for bug hunting With AI
- Module 04: Advanced SQL Injection
- Module 05: Command injection With AI
- Module 06: Session Management and Broken Authentication Vulnerability
- Module 07: Cross-Site Request Forgery (CSRF)
- Module 08: Server Site Request Forgery (SSRF)
- Module 09: Cross-Site Scripting (XSS) With AI
- Module 10: Insecure Direct Object Reference (IDOR)
- Module 11: Sensitive Data Exposure and Information Disclose With AI
- Module 12: Server Site Template Injection (SSTI) With AI
- Module 13: Multi-Factor Authentication Bypass

- ★ 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 14: HTTP Request Smuggling
- Module 15: External Control of File Name or Path
- Module 16: Local File Inclusion (LFI) and Remote File Inclusion (RFI)
- Module 17: Directory Path Traversal
- Module 18: HTML Injection
- Module 19: Host Header Injection
- Module 20: File Upload Vulnerability With AI
- Module 21: JWT Token Attack
- Module 22: Flood Attack on the Web With AI
- Module 23: API Testing With AI
- Module 24: Report Writing With AI

MOBILE APPLICATION SECURITY WITH AI

LEVEL 8 : **COURSE DURATION : 60 hrs**

- Module 01: Introduction to Mobile Penetration Testing
- Module 02: Lab Setup
- Module 03: Android Architecture
- Module 04: Apk File Structure
- Module 05: Reversing App with Apktool
- Module 06: Reversing App with MobSf
- Module 07: Static Analysis using AI
- Module 08: Scanning Vulnerability with Drozer
- Module 09: Improper Platform Usage
- Module 10: Insecure Data Storage
- Module 11: Insecure Communication
- Module 12: Insecure Authentication
- Module 13: Insufficient Cryptography
- Module 14: Insecure Authorization
- Module 15: Client Code Quality
- Module 16: Code Tampering
- Module 17: Reverse Engineering
- Module 18: Extraneous Functionality
- Module 19: SSL Pinning
- Module 20: Intercepting the Network Traffic
- Module 21: Dynamic Analysis
- Module 22: Report Preparation using AI
- Module 23: IOS Penetration: Basics
- Module 24: Report Writing

INTERNET OF THINGS (IOT) PENTESTING WITH AI

LEVEL 9 : **COURSE DURATION : 60 hrs**

- Module 01: Overview of IoT: Why IOT is so important?
- Module 02: IoT Pentesting through AI Tool, Use AI tools to automate vulnerability scanning in IoT devices by analyzing traffic patterns and identifying anomalies or weak points.
- Module 03: Introduction of IoT,
- Module 04: Introduction to Sensor Network,
- Module 05: Communication Models in IoT (Internet of Things),
- Module 06: Frequency,
- Module 07: Wireless Protocol,
- Module 08: Comparing Web and IOT Protocols,
- Module 09: SPI, UART, I2C,
- Module 10: IOT Architecture,
- Module 11: ARDUINO,
- Module 12: Raspberry,
- Module 13:Introduction to Mobile App Platform,
- Module 14: Flipper Zero,
- Module 15: Firmware,
- Module 16: Analysing IOT Hardware,
- Module 17: SDR (software-defined radio),
- Module 18: Conceiving a new IOT product- Product Requirement document for IoT,
- Module 19: Basic Intro Cloud Iaas Paas Saas-IoT data, platform, and software as a service revenue
- Module 20: Basic Introduction to ICS.

END POINT SECURITY WITH AI

LEVEL 10 **COURSE DURATION : 60 hrs**

- Module 01: Implementing Internet Security Antivirus
- Module 02: Multi-Factor Authentication
- Module 03: Mobile Device Management For Industry
- Module 04: Data Loss Prevention (DLP)
- Module 05: Security Information and Event Management with AI
- Module 06: APT Attack
- Module 07: Mitre Attack Framework
- Module 08: EDR and XDR with AI
- Module 09: Unified Threat Management
- Module 10: AI-Fortified Firewall
- Module 11: AI Enhanced ISO 27001

AWS ASSOCIATE WITH AI

LEVEL 11 : **COURSE DURATION : 60 hrs**

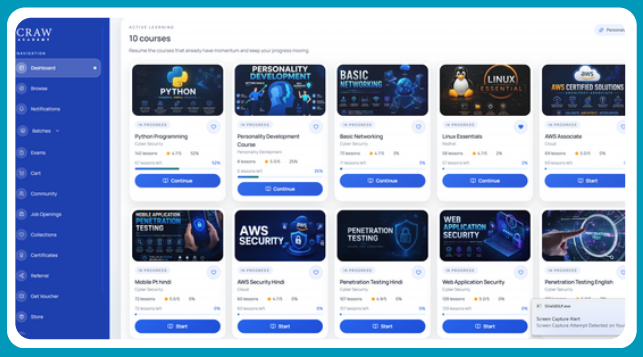
- Module 01 : Designing Highly Available, Cost-effective, Scalable Systems
  - (a) Planning and Design Using AI
  - (b) Monitoring and Logging
  - (c) Hybrid IT Architectures
  - (d) Elasticity and Scalability
- Module 02 : Implementation and Deployment
  - (a) Amazon EC2 implementation using AI
  - (b) Amazon S3 management using AI
  - (c) Amazon Web Service Cloud Formation
  - (d) Amazon Web Service VPS understanding with the help of AI
  - (e) Amazon Web Service IAM
- Module 03 : Data Security
  - (a) AWS IAM (Identity and Access Management) configuring using AI
  - (b) Amazon Web Service VPC and creating a log with AI
  - (c) Encryption Solutions
  - (d) Cloud watch logs analysis using AI
  - (e) Disaster Recovery
  - (f) Amazon Route 53
  - (g) AWS Storage Gateway
  - (h) Amazon Web Service Import/Export
- Module 04 : Troubleshooting

AWS CLOUD SECURITY WITH AI

LEVEL 12 **COURSE DURATION : 60 hrs**

- Module 01: Overview of Security in AWS
- Module 02: AWS Identity and Access Management (Querying Logs for Authentication Activities using AI)
- Module 03: AWS Virtual Private Cloud (monitor, troubleshoot, and optimize your VPC network using AI)
- Module 04: Data Security in AWS
- Module 05: Securing Servers in AWS
- Module 06: Edge Security in AWS
- Module 07: Monitoring in AWS
- Module 08: Logging and Auditing in AWS

LMS PORTAL FOR STUDENTS AND VISITORS



We encourage students and visitors to sign up and log in to the LMS (Learning Management System) Portal for multipurpose usage, including free access to CrackTheLab Premium Subscription, enrolled course details, training videos, attendance records, examinations, physical and software hacking tools, training vouchers, job opportunities, certificates, and many more features.

To know more about the LMS Portal, please scan the QR code provided here.

INDUSTRY INTERNSHIP OPPORTUNITY

Gain practical industry exposure through a 6-month internship opportunity after completing the 1-Year Cyber Security Diploma, where students can work on real-world cybersecurity projects, enhance technical skills, and build professional experience for better career opportunities.

PD SESSIONS & GD SESSIONS

Get high-end Personality Development Sessions and know the details of enhancing your aura and charm to get fruitful results in making a lasting impression in face-to-face interactions and professional interviews.

RESUME BUILDING

Get expert guidance to create a strong, professional, and job-focused resume that highlights your skills and certifications. Our trainers help students present their cybersecurity knowledge, projects, and achievements effectively to recruiters.

ENGLISH COMMUNICATION CLASSES

Get expert guidance to create a strong, professional, and job-focused resume that highlights your skills and certifications.Our trainers help students present their cybersecurity knowledge, projects, and achievements effectively to recruiters.



MOCK INTERVIEW SESSIONS

Practice real interview scenarios with trainers and industry experts to understand common technical and HR interview questions.Mock interviews help students identify weak areas, improve answers, and gain confidence before facing actual recruiters.



PLACEMENT DRIVES

Craw Security conducts placement drives to connect trained students with hiring opportunities in reputed companies.Students get exposure to off-campus interviews as well as campus placement drives organized at our Saket branch.



Get trained with expert-led sessions including PD Sessions, Campus Placement Preparation, GD Sessions, Mock Interviews, English Communication Classes, Resume Building & more to become industry-ready.

Scan the QR Code to watch the video and explore how CRAW Security can help shape your future in Cyber Security & IT

INTERVIEW SESSIONS AT SAKET BRANCH – CAMPUS PLACEMENT DRIVE

Students are provided opportunities to attend interviews at various companies based on job openings and eligibility. These off-campus interview sessions help candidates gain real hiring exposure and industry-level interview experience.



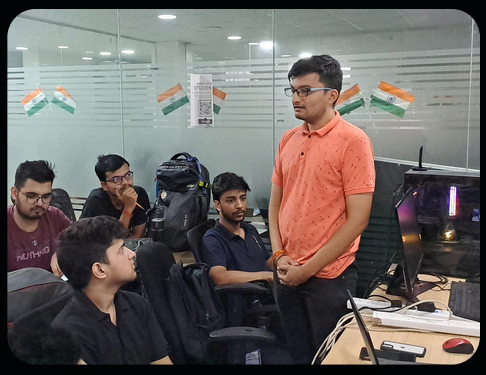
INDIVIDUAL COUNSELLING SESSIONS – IF REQUIRED

Personal counselling sessions are available for students who need career guidance, interview support, or learning direction. These one-to-one sessions help students choose the right career path and improve their preparation strategy



CONFIDENCE BUILDING CLASSES

Develop self-confidence, positive thinking, and a professional mindset through guided training and practical activities. These classes help students overcome hesitation and perform better in interviews, presentations, and workplace situations.


PLACEMENT SUPPORT WITH LEADING COMPANIES

PRECISE Testing Solution · Cloud Infotech · Qualicentric · team COMPUTERS · Lucid Growth

SOPHOS · ProExcel · OrionSecure · cybroTech · NETRIKA

CYBER EVOLVE · LARSEN & TOUBRO · TechDefencelabs · maple CLOUD · eSOLUTIONS

CYBERSECURITY LIBRARY & LEARNING RESOURCES

CRAW Security provides dedicated library services and learning resources for students enrolled in one-year diploma programs. Our library support includes access to cybersecurity books, digital study materials, research content, technical documentation, and learning references designed to enhance practical and theoretical knowledge. These resources help students strengthen their understanding of ethical hacking, cyber security, digital forensics, and emerging technologies while supporting continuous learning and professional development.

DAILY CYBER SECURITY NEWS UPDATES

Stay informed with the latest cyber security news, hacking incidents, ransomware attacks, data breaches, and vulnerability disclosures from around the world with News4Hackers.com. Get real-time updates, expert insights, and breaking reports to stay ahead of emerging cyber threats, online scams, and digital security risks.

CYBERSECURITY COURSES, TOOLS , CTF PLATFORMS

We provide comprehensive cybersecurity training programs and courses available for organizations, businesses, and government institutions. we offer Capture The Flag (CTF) challenges, subscription-based cybersecurity learning programs, and specialized cybersecurity tools designed to support practical training, skill development, and advanced cyber defence capabilities.

CRACK THE LAB
Gamified way of learning through challenge Labs

HACKING TOOLS

Who Should Do This Course?

- Non-technical personnel are willing to learn about Information Security.
- Business & IT Managers who need healthy functional information on Cyber Security.
- Aspiring & Inexperienced IT Professionals from other trades.
- Students want to learn the terminology and nomenclature of computer security.
- Students who wish to build a shinier career in information security.
- College students preparing for certifications and cybersecurity job roles.
- Tech support and helpdesk professionals aiming to upgrade their security knowledge.
- Anyone passionate about building a strong foundation in Cyber Security and IT Security concepts.
- Ethical hacking enthusiasts who want to understand cybersecurity fundamentals.




Training & Certification

OffSec The Path to a Secure Future™ · EC-Council · CompTIA · python · CISCO · Red Hat · aws · Microsoft · CERTNEXUS · PECB

Terms & Conditions for 100% Placements

CRAW ACADEMY
Learn | Research | Innovate

- Attendance 75% is mandatory.
- Marks for internal exams should be 80% mandatory.
- Fees for the 1 Year Cybersecurity Diploma Course Powered by AI should be properly paid.
- Candidates can apply for a Job after completion of 6 modules.
- Candidates are eligible for taking Mock Interview sessions, PD Classes, Resume Making Sessions, Communication classes, and many more services from the Placement Cell right from the Day 1 after enrolling in the 1 Year Cybersecurity Diploma Course Powered by AI.
- Global certifications required, if needed by companies for a job.
- Candidates should be Graduate/Pursuing.
- One time job Assistance/ Placement will be provided, if candidate missed any interview, Craw Placement cell will not liable to re-arrange the interview and also Craw Academy will not be liable for any refund or future litigations or claims.
- Package as per candidate's skills or according to company norms.
- Ideal Candidates can apply in multiple jobs.
- Post Placement Process will be provided by Placement Cell which is as follows.
  - Documentation
  - Offer Letter
  - Joining Date/Timeline of Joining

Payment Mode

1. OneShotPayment
2. Installment Available

Card, Wallets, UPI & Netbanking
VISA UPI Rupay
Payment processing partner
Razorpay

Use UPI id : Craw@kotak

NOTE – * Terms & Conditions Apply only for 1 Year Diplomas.

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, Said-ul-ajab, New Delhi 110030

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

Office Landline : (+011) 4039 4315 Mobile : +91 951 380 5401

CRAW CYBER SECURITY PVT LTD

(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

CRAW CYBER SECURITY PTE LTD

(SINGAPORE OFFICE)

27 Paya Lebar Road, #13-05 Paya Lebar Residences, Singapore - 409042

Office Landline : +65 9797 6564

Email ID : info@crawsecurity.com Website : www.crawsecurity.com

CRAWSEC LLC USA

(USA Office)

30 N Gould St Ste R Sheridan, WY 82801

CRAW
Security
Learn | Research | Innovate