CRAW
ACADEMY

Hacker 667

The Ultimate Manual for Becoming an Ethical Hacker

Ethical Hacking

VERSION 2.0

+91 951 380 5401 training@craw.in https://www.craw.in

Table of **Content:**

Program **Overview:**

Our Ethical Hacking Course is designed to offer an immersive experience in the world of cybersecurity and ethical hacking. This program covers the fundamental skills and knowledge needed to protect organizations against cyber threats and vulnerabilities. Through a hands-on approach, participants will learn to think like hackers to defend against future attacks. This course is ideal for aspiring cybersecurity professionals seeking to enhance their skills in network security, system penetration testing, and ethical hacking.

Program **Features:**

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ Accredited by the FutureSkills Prime, Approved by the Government of India.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Learn from Industry-leading experts with extensive experience in ethical hacking fundamentals and security.
- ✓ Hands-on practical exercises to learn with real-time problem-solving scenarios.
- ✓ Cutting-edge curriculum to stay at the forefront of the ethical hacking sector.
- ✓ Join a community of cybersecurity enthusiasts and professionals for networking and support.
- ✓ Access course materials and live sessions through both online and offline modes to suit your learning preferences.

Delivery **Mode:**

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of **Ethical Hacking:**

- ✓ Basic understanding of networking concepts.
- ✓ Familiarity with operating systems, especially Windows and Linux.
- ✓ A keen interest in cybersecurity and ethical hacking.

Target **Audience:**

- ✓ IT professionals who are seeking to transition into cybersecurity roles.
- ✓ Network administrators and engineers.
- ✓ Security officers and practitioners.
- ✓ College students and recent graduates looking to enter the cybersecurity field, and
- ✓ Anyone who is willing to know more about the ethical hacking course.

Key Learning **Outcomes:**

This Ethical Hacking Course will help you:

- ✓ **Understanding of Ethical Hacking Fundamentals:** Gain a comprehensive understanding of what ethical hacking is, including the ethics and legality surrounding the practice. Learn about the role of an ethical hacker in strengthening the cybersecurity posture of organizations.
- ✓ **Proficiency in Identifying Vulnerabilities:** Develop the ability to perform thorough vulnerability assessments to identify potential security weaknesses in computer systems, networks, and applications.
- ✓ **Skills in Exploiting Vulnerabilities:** Learn how to exploit identified vulnerabilities in a controlled and safe environment. This includes gaining unauthorized access to systems in a manner that mimics the approach of malicious hackers, with the intent of finding and fixing the vulnerabilities.
- ✓ **Expertise in Penetration Testing:** Acquire the skills to conduct comprehensive penetration tests, simulating cyberattacks on an organization's network to evaluate the security of the system.
- ✓ **Knowledge of Countermeasures and Preventive Measures:** Understand and be able to implement countermeasures to protect against hacking attacks. Learn about various security practices and technologies that can be employed to secure systems and networks.
- ✓ **Familiarity with Various Hacking Tools and Techniques:** Gain hands-on experience with the latest hacking tools and techniques used in real-world cybersecurity assessments, including those for network scanning, password cracking, and encryption/decryption.
- ✓ **Insight into Emerging Cybersecurity Trends:** Stay abreast of the latest cybersecurity threats and trends, including those related to cloud computing, mobile platforms, and IoT devices. Learn how to adapt and apply ethical hacking techniques to new technologies.
- ✓ **Preparation for Industry-Recognized Certifications:** Prepare for various industry-recognized certifications such as Certified Ethical Hacker (CEH), CompTIA Security+, and Offensive Security Certified Professional (OSCP), enhancing career prospects and professional credibility.
- ✓ **Critical Thinking and Problem-Solving Skills:** Develop critical thinking and problem-solving skills essential for identifying and mitigating complex cybersecurity challenges.
- ✓ **Ethical Decision-Making and Professionalism:** Emphasize the importance of ethics and professionalism in the cybersecurity field. Understand the legal implications of hacking and ensure all activities are conducted within legal and ethical boundaries.

Certification **Alignment:**

Our Ethical Hacking Course is genuinely accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. Moreover, Craw Security is a proud partner of FutureSkills Prime.

Certification **Details & Criteria:**

Certification Details -
Upon successful completion of the course and passing the examination, participants will receive a certification from Craw Security. The examination assesses the participant's ability to apply ethical hacking best practices and techniques in a controlled environment. Specific criteria for certification include practical assessments and a theoretical exam.

About the **Exam:**

- ✓ **Number of Questions:** 30-35 Questions
- ✓ **Exam Provider:** FutureSkills Prime
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security **Certification Criteria:**

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

100% Placement with **1 Year Cyber Security Course:**

There is a specialized set of Terms and Conditions for a 100% Placement Guarantee with **our 1 Year Cybersecurity Diploma** that needs to be fulfilled by each and every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take the advantage of 100% Placement Guarantee from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.
- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be 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 for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  1. Documentation
  2. Offer Letter
  3. Joining Date/ Timeline of Joining

What to Choose After this **Course:**

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India.

Course **Curriculum:**

Module 01: Introduction to Basics of Ethical Hacking

- ✓ Lesson 01: Intro To Ethical Hacking
- ✓ Lesson 02: Types of Attacks
- ✓ Lesson 03: Hacking Methodology
- ✓ Lesson 04: Cyber Kill Chain
- ✓ Lesson 05: Types of Attackers
- ✓ Lesson 06: CIA Traid
- ✓ Lesson 07: Risk Management
- ✓ Lesson 08: Cyber Laws

Module 02: Foot-printing Active (Tool-Based Practical)

- ✓ Lesson 01: What is Active Footprinting
- ✓ Lesson 02: Different kinds of information gathered in Footprinting
- ✓ Lesson 03: Tools for Active Footprinting = nmap, hping, masscan

Module 03: Foot-printing Passive (Passive Approach)

- ✓ Lesson 01: What is passive footprinting
- ✓ Lesson 02: Footprinting Through Whois
- ✓ Lesson 03: Footprinting Through Website / Web services
- ✓ Lesson 04: Footprinting Through search engine
- ✓ Lesson 05: Footprinting Through DNS
- ✓ Lesson 06: Footprinting Through Email
- ✓ Lesson 07: Footprinting Through Network
- ✓ Lesson 08: Footprinting Through Social Media
- ✓ Lesson 09: Tools for Passive Footprinting – Google dorks, shodan, netcraft

Module 04: In-depth Network Scanning

- ✓ Lesson 01: Overview of Network Scanning
- ✓ Lesson 02: Scanning Methodology
- ✓ Lesson 03: Host Discovery
- ✓ Lesson 04: Port Scanning Techniques
- ✓ Lesson 05: Scanning tools – nmap, netdiscover, arp-scan -1

Module 05: Enumeration User Identification

- ✓ Lesson 01: Enumeration Concepts
- ✓ Lesson 02: NetBIOS Enumeration
- ✓ Lesson 03: SNMP Enumeration
- ✓ Lesson 04: LDAP Enumeration
- ✓ Lesson 05: SMTP Enumeration
- ✓ Lesson 06: DNS Enumeration

Module 06: System Hacking Password Cracking & Bypassing

- ✓ Lesson 01: Authentication
- ✓ Lesson 02: Gaining Access
- ✓ Lesson 03: Password cracking
- ✓ Lesson 04: Password Cracking Techniques
- ✓ Lesson 05: Steganography

Module 07: Viruses and Worms

- ✓ Lesson 01: Introduction to Malware
- ✓ Lesson 02: Types of Viruses
- ✓ Lesson 03: Types of Worms

Module 08: Trojan and Back door

- ✓ Lesson 01: Types of Trojans
- ✓ Lesson 02: Components Of a Trojan

Module 09: Bots and Botnets

- ✓ Lesson 01: Introduction to Botnets
- ✓ Lesson 02: Characteristics of Botnets

Module 10: Sniffers MITM with Kali

- ✓ Lesson 01: Introduction to Ettercap and Bettercap

- ✓ Lesson 02: Practical on Ettercap
- ✓ Lesson 03: Practical on Bettercap

Module 11: Sniffers MITM with Windows

- ✓ Lesson 01: Introduction to Wireshark
- ✓ Lesson 02: Practical on Wireshark

Module 12: Social Engineering Techniques Theoretical Approach

- ✓ Lesson 01: Types of Social Engineering Attacks
- ✓ Lesson 02: Human Based Social Engineering Attacks
- ✓ Lesson 03: Computer Based Social Engineering Attacks
- ✓ Lesson 04: Mobile Based Social Engineering Attacks

Module 13: Social Engineering Toolkit Practical Based Approach

- ✓ Lesson 01: Practical on zphisher
- ✓ Lesson 02: Practical on Social Engineering Toolkit (SET)

Module 14: Denial of Service DOS & DDOS Attacks

- ✓ Lesson 01: DoS/DDoS Concepts
- ✓ Lesson 02: DoS/DDoS Attack Techniques
- ✓ Lesson 03: DoS/DDoS Tools
- ✓ Lesson 04: DoS/DDoS Protection Tools and Techniques

Module 15: Web Session Hijacking

- ✓ Lesson 01: Session Hijacking Concepts
- ✓ Lesson 02: Session Hijacking Techniques
- ✓ Lesson 03: Session Hijacking Tools

Module 16: SQL Injection Manual Testing

- ✓ Lesson 01: SQL Injection Concept
- ✓ Lesson 02: Types of SQL Injection
- ✓ Lesson 03: Working Of SQL Injection
- ✓ Lesson 04: SQL Injection Methodology

Module 17: SQL Injection Automated Tool-Based Testing

- ✓ Lesson 01: Practical on sqlmap
- ✓ Lesson 02: Practical on Ghauri

Module 18: Basics of Web App Security

- ✓ Lesson 01: Fundamentals of Web Application Security
- ✓ Lesson 02: Common Vulnerabilities in Web Applications
- ✓ Lesson 03: Best Practices for Web App Security

Module 19: Hacking Web servers

- ✓ Lesson 01: Web Server Hacking Techniques
- ✓ Lesson 02: Server Rooting Methods
- ✓ Lesson 03: Securing Web servers

Module 20: Hacking Wireless Networks Manual CLI Based

- ✓ Lesson 01: Wireless Network Basics
- ✓ Lesson 02: Manual Hacking Techniques for Wi-Fi Networks
- ✓ Lesson 03: Command Line Tools for Wireless Hacking

Module 21: Hacking Wireless Network

- ✓ Lesson 01: Automated Wireless Hacking Tools
- ✓ Lesson 02: Wireless Network Exploitation Methods
- ✓ Lesson 03: Wireless Security Best Practices

Module 22: Evading IDS, Firewall

- ✓ Lesson 01: Intrusion Detection System (IDS) Evasion Techniques
- ✓ Lesson 02: Firewall Evasion Methods
- ✓ Lesson 03: Stealth and Evasion Tools

Module 23: Honey pots

- ✓ Lesson 01: Introduction on Honeypots
- ✓ Lesson 02: Types Of Honeypots
- ✓ Lesson 03: Install Of Honeypot (KF Sensor)

Module 24: Buffer Overflow

- ✓ Lesson 01: Introduction to Buffer Overflow

Module 25: Cryptography

- ✓ Lesson 01: What is cryptography, encryption, decryption
- ✓ Lesson 02: Types of cipher – substitution (Caesar) and Transposition (rail fence) techniques
- ✓ Lesson 03: Keys in cryptography – asymmetric and symmetric
- ✓ Lesson 04: What is encoding
- ✓ Lesson 05: Example of encoding
- ✓ Lesson 06: What is hashing
- ✓ Lesson 07: Example of hashes of a string

Module 26: Penetration Testing: Basics

- ✓ Lesson 01: Penetration Testing Overview
- ✓ Lesson 02: Phases of Penetration Testing
- ✓ Lesson 03: Reporting and Remediation

Module 27: Mobile Hacking

- ✓ Lesson 01: Mobile Security Threats
- ✓ Lesson 02: Exploiting Mobile Platforms
- ✓ Lesson 03: Theory of mobile and mobile attacks
- ✓ Lesson 04: Practical of Androrat

Module 28: Internet of Things (IoT) Hacking

- ✓ Lesson 01: IoT Concepts
- ✓ Lesson 02: IoT Hacking Methodology
- ✓ Lesson 03: IoT Hacking Tools
- ✓ Lesson 04: IoT Security Tools

Module 29: **Cloud Security and many more**

- ✓ Lesson 01: Cloud Computing Concepts
- ✓ Lesson 02: Cloud Computing Threats
- ✓ Lesson 03: Cloud Computing Attacks
- ✓ Lesson 04: Cloud Security Tools

About **us:**

Craw Security is India's leading cybersecurity training institute, dedicated to developing the next generation of cybersecurity professionals. With a focus on practical, hands-on training, we offer a wide range of courses tailored to all skill levels. Our mission is to enhance the cybersecurity posture of individuals and organizations worldwide.

For more information, please visit our course page website:
https://www.craw.in/ethical-hacking-course-in-delhi/

Contact **us:**

Craw Cyber Security Private Limited, India (Head Office)

1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,
Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel
Twitter: Join Twitter Channel