CRAW
Security
Learn | Research | Innovate

Hacker are here. **Where are you ?**

The Ultimate Ethical Hacking Certification

C|EH v11

Certified Ethical Hacker

COURSE MODULES

Introduction to Ethical Hacking

01 In this module we will learn about Information security, types of hackers, types of testing, CIA triat, Security Standards, Deep web and Dark web, and will finish up the lab setup for upcomming modules.

Footprinting and Reconnaissance

02 In this particular module we will collect Open/-public information about the target throuth Whois records, DNS Records, Google Dorks, Github tools, Maltego. We will be purly focused on Open Source Information Gathering techniques through OSINT (Opensource Inteligence) Tools.

Scanning Networks

03 In this module we will Collect information about Network like, active machines, active services, Operating Systems, and we cover tools like Nmap, Hping3, angryip-scanner, MSF, etc.

Enumeration

04 After collecting information about Active Machines in the network, we will test each and every service like FTP, SSH, Telnet, HTTP, VNC, etc. as per its security posture.

Vulnerability Analysis

05 In this module, we will use excellent Vulnerability scanners like Acunetix, Nessus, Qualys, Crashtest, Nikto, MSF-Pro, Nmap, etc. In this module we'll use these tools to test Network Services.

System Hacking

06 In this module, we will learn cracking Password techniques for windows as well as Linux, Buffer Overflow, Privilage Escalation techniques, and we will learn techniques to clear our footprints/logs from the system.

Malware Threats

07 In this module, we will learn about different types of malwares like Trojans, VIRUS, Worms, Malwares, Rootkits, RAT's, Ransomwares. and we learn how they are created and can be used to access Victim Device and how they can be used for Backdoors. We also learn techniques to prevent our system or network from these malwares.

Sniffing

08 In this module, we will cover-up attack for network services like ARP, DHCP, MAC Flooding, etc and how to Analyse network traffic to detect intrusions and how to Analyse to extract juicy information like Username/password using some Sniffing tools like Wireshark, Ettercap, Bettercap, Xerosploit, etc.

Social Engineering

09 In this module, we will cover techniqes different social engineering attacks like Phishing Emails, Smishing, Phishing web-pages, Mirroring websites, etc. we will also learn preventive measures for these Social Engineering Attacks.

Denial-of-Service

10 In this module, we will learn about DoS/DDoS, different types of Dos/DDoS, different tools & techniques used for Dos/DDos. we will also learn perventive measures for DoS/DDoS.

Course Description

C|EH is the world's most advanced certified Ethical Hacking Course that covers 20 Modules of the most current security domains any individual will ever want to know when they are planning to beef-up the information security posture of their organization.

The accredited course provides the advanced hacking tools and techniques used by hackers and information security professionals.

Sample Ethical Hacking Certification

Session Hijacking

11 In this module, we will coverup Attacks related to Authentication and Sessions created after Login like Cookie stealing, Cookie replay, IDOR, Session fixation, etc. and how these attacks can be fixed.

Hacking Web Servers

13 In this moudle, we will coverup direct attacks for web-server and what security an admin can apply to prevent direct attacks on web-server.

SQL Injection

15 This module covers different types of SQL Injection like Error Based, Union Based, Blind Based. we will test target website manually and then use automated tools like SQLmap, SQLNinja, etc.

Hacking Mobile Platforms

17 This module covers techniques used by attackers to gain access to android and IOS devices through malicious applications and Malwares. How to test mobile applications for authenticity and security.

Cloud Computing

19 This module covers attacks and Use case for different Cloud Computing services like EC2 instances, S3 Bucktes, IAM Policies and a lot more.

12 Evading IDS, Firewalls & Honeypots

In this module, we will learn about the working architecture of Firewall, IDS/IPS. What are the different types of Firewall and IDS/IPS, how they work, how attacks are able to bypass those security checks, how to write your own Firewall and IDS/IPS rules. Then we start with Honeypots which are used to trap Hackers.

14 Hacking Web Applications

This module covers attacks related to website like OWASP Top 10 2017, OWASP Top 10 2021 and SANS 25. We will be using best in industry tools like Burp-Suite Professional, OWASP Zap, etc.

16 Hacking Wireless Networks

This module covers different techniques used to attack wireless network authentication mechanisms used in WEP, WPA-1, WPA-2, and WPA-3 to gain access to any wireless network and a lot more.

18 IoT Hacking

This module covers attacks related to IOT (Internet of Things) and OT (Operational Technology) like your smart Watch, smart Televisions, Smart LED's, Smart Speakers, etc. This module covers firmware analysis techniques.

20 Cryptography

This module covers security algorithms used to maintain CIA with help of different Encryption Ciphers, Hashing Algorithms, Digital Certificates, etc. This module also helps us understand trust chain followed by our Operating Systems and software.

BECOME
CERTIFIED ETHICAL HACKER
UNDER THE GUIDANCE OF

Mr Mohit Yadav

Course Description

C|EH is the world's most advanced certified ethical hacking course that covers 20 modules of the most current security domains any individual will ever want to know when they are planning to beef-up the information security posture of their organization.

The accredited course provides the advanced hacking tools and techniques used by hackers and information security professionals.

Key Outcomes

- Thorough introduction to ethical hacking
- Exposure to threat vectors and countermeasures
- Addresses emerging areas of IoT, cloud and mobile hacking
- Prepares you to combat Trojans, malware, backdoors, and more
- Enables you to hack using mobile

Exam Information

- Exam Title: Certified Ethical Hacker (ANSI)
- Exam Code: 312-50 (ECC EXAM), 312-50 (VUE)
- Number of Questions: 125
- Duration: 4 hours
- Availability: ECC Exam Portal, VUE
- Test Format: Multiple Choice

Head Office Address

CRAW CYBER SECURITY PVT. LTD.

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

+91 951 380 5401 | 011 – 4039 4315

training@craw.in | info@craw.in

www.craw.in | www.crawsecurity.com

@crawsec