CYBER TECH ASSOCIATES

CERTIFED WHITE HAT HACKER

Build Your Carrer in Cyber Security

THE CERTIFIED WHITE HAT HACKER

Offering International Trainer for Cyber Security

Enhanced Career Opportunities

Increased Knowledge and Skills

Industry Recognition

Who is a Certified White Hat Hacker?

A Certified White Hat Hacker, also known as a Certified Ethical Hacker (CEH), is a cybersecurity professional skilled in identifying, understanding, and mitigating security threats. These experts are trained to use their hacking abilities for constructive purposes, helping organizations to enhance their security measures by identifying and addressing vulnerabilities before malicious hackers can exploit them. To earn the title of Certified White Hat Hacker, individuals typically undergo rigorous training and certification processes, such as the CEH certification offered by the EC-Council. This certification is a testament to their expertise in ethical hacking practices and their ability to simulate attacks to assess and improve an organization's security posture.

What is White Hat Hacking?

White hat hacking, also known as ethical hacking, involves the practice of intentionally testing and probing computer systems, networks, and software to identify and fix security vulnerabilities. Unlike malicious hackers, white hat hackers operate with permission and within legal boundaries, aiming to enhance cybersecurity rather than exploit weaknesses for personal gain. Their primary goal is to improve security by finding and addressing vulnerabilities before they can be exploited by malicious actors. White hat hackers conduct their activities with explicit authorization from system owners, ensuring their work is legal and ethical.

These professionals use a variety of techniques and tools, including penetration testing, vulnerability assessments, and security audits, to simulate cyberattacks and understand how systems respond under threat conditions. Many white hat hackers obtain certifications, such as the Certified Ethical Hacker (CEH), to validate their skills and knowledge. Their expertise allows them to identify potential weaknesses and recommend solutions to mitigate risks. By proactively addressing security issues, they help organizations safeguard their data, systems, and networks.

White hat hackers play a crucial role in the cybersecurity landscape, helping organizations develop robust security policies, implement effective defenses, and ensure compliance with industry standards. Their adherence to a strict code of ethics, guided by a commitment to security, transparency, and respect for privacy, builds trust with the organizations they assist and the broader cybersecurity community. In essence, white hat hacking is a vital component of modern cybersecurity efforts, contributing significantly to a safer and more secure digital environment.

What's New in the WHITE HAT HACKER ?

LEARN | CERTIFY | ENGAGE | COMPETE

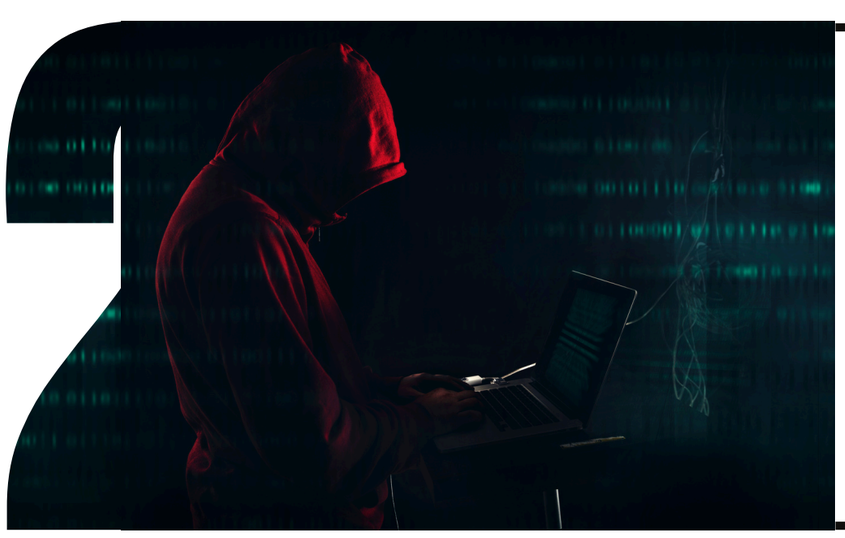
White hat hackers are essential as they proactively find and fix security vulnerabilities, reducing the risk of cyberattacks. Their expertise and ethical practices help organizations strengthen defenses, protect sensitive data, and maintain trust in digital environments.

Gain expertise in ethical hacking that goes beyond certification.

1

GAIN SKILLS

2

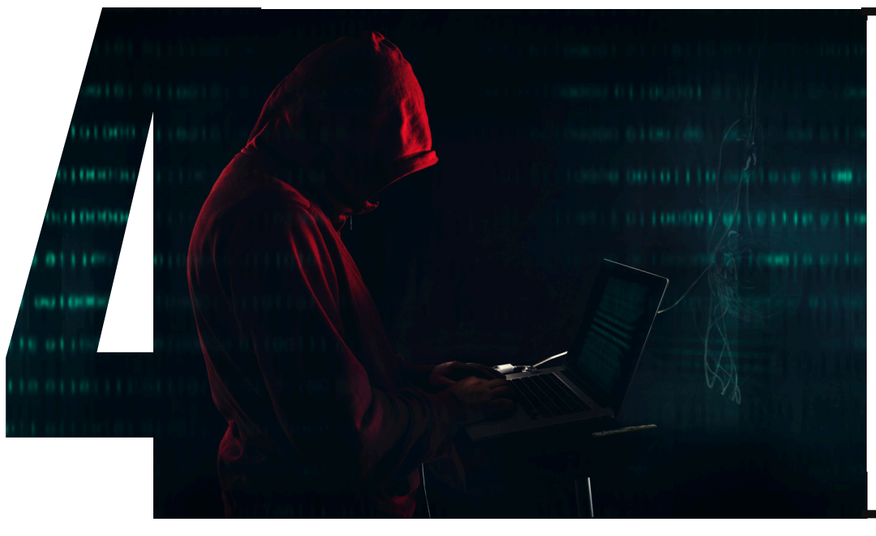


GAIN RECOGNITION

3

GAIN EXPERIENCE

4



GAIN RESPECT

CERTIFIED WHITE HAT HACKER PROGRAM

MODULE 1	**Introduction to Ethical Hacking** Examine the foundations of important topics in the field of information security, such as information security controls, ethical hacking, pertinent laws, and standard operating procedures.
MODULE 2	**Foot Printing and Reconnaissance** Discover how to carry out reconnaissance and foot printing using the newest methods and equipment. This is a crucial step before an ethical hack is launched.
MODULE 3	**Scanning Networks** Discover various network scanning methods and defences.
MODULE 4	**Enumeration** Discover a variety of enumeration techniques, including associated countermeasures and exploits for Network File Sharing (NFS) and Border Gateway Protocol (BGP).
MODULE 5	**Vulnerability Analysis** Discover how to locate security flaws in the end systems, communication infrastructure, and network of a target organisation. various forms of vulnerability assessments and the instruments used for them.
MODULE 6	**System Hacking** Discover the many techniques used by system hackers to find vulnerabilities in networks and systems, such as covering tracks, steganography, and steganalysis attacks.

MODULE 7	**Malware Threats** Learn about malware analysis techniques, malware countermeasures, APT and fileless malware, and various malware types (Trojan, viruses, worms, etc.).
MODULE 8	**Sniffing** Discover how to use packet-sniffing techniques to find network vulnerabilities and how to protect yourself from sniffing attacks by learning about countermeasures.
MODULE 9	**Social Engineering** Discover the principles and methods of social engineering, such as how to spot theft attempts, check for human-level weaknesses, and recommend countermeasures.
MODULE 10	**Denial-of-Service** Discover the various methods used to audit a target and create DoS and DDoS countermeasures and protections. You can also learn about Distributed DoS (DDoS) and Denial of Service (DoS) attack techniques.
MODULE 11	**Session Hijacking** Recognise the different methods of session hijacking that are employed to identify vulnerabilities in network-level session management, authentication, authorization, and cryptography, as well as the corresponding defences.
MODULE 12	**Evading IDS, Firewalls, and Honeypots** Learn about honeypot evasion, intrusion detection systems (IDS), firewall, and countermeasures. You will also learn about the tools used to audit a network perimeter for vulnerabilities.
MODULE 13	**Hacking Web Servers** Discover more about web server attacks, including an extensive attack methodology that is used to check for security holes in web server infrastructures and responses.

MODULE 14	**Hacking Web Applications** Discover web application attacks and how to audit web application vulnerabilities and countermeasures using a thorough web application hacking methodology.
MODULE 15	**SQL Injection** Study up on SQL injection countermeasures, evasion strategies, and attacks.
MODULE 16	**Hacking Wireless Networks** Recognise the many kinds of wireless technologies, such as encryption, security risks, hacking techniques, hacking instruments, Wi-Fi security tools, and defence strategies.
MODULE 17	**Hacking Mobile Platforms** Learn about mobile device management, mobile security guidelines, mobile attack vectors, and security tools for Android and iOS platforms.
MODULE 18	**IoT and OT Hacking** Discover the various IoT and OT attack types, hacking techniques, tools, and defences.
MODULE 19	**Cloud Computing** Discover the many cloud computing ideas, including serverless computing and container technologies, as well as the risks and attacks that affect cloud computing, hacking tactics, and cloud security solutions.
MODULE 20	**Cryptography** Discover more about public key infrastructure (PKI), encryption tools, email encryption, disc encryption, cryptography attacks, and cryptanalysis tools.

WHAT WE OFFER ?

Paid Internship in Cybersecurity: Gain hands-on experience and invaluable insights through a paid internship in cybersecurity, providing you with real-world exposure and enhancing your employability.

Placement Assistance: Benefit from personalized placement assistance by seasoned experts,ensuring you seamlessly transition into a rewarding cybersecurity career.

Complimentary Interview Preparation: Access exclusive interview preparation sessions conducted by multinational corporations (MNCs), helping you ace job interviews with confidence.

WHITE HAT HACKER EXAM INFORMATION

C | WH² THEORY

Exam Title:

THE CERTIFIED WHITE HAT HACKER (Theory)

Number of Questions:

150

Duration:

5 hours

Test Format:

Multiple Choice

C | WH² PRACTICAL

Exam Title:

THE CERTIFIED WHITE HAT HACKER (Practical)

Number of Practical Challenges:

25

Duration:

6 hours

Passing Score:

70%

TRAINING	MONTHS	DURATION
3 DAYS	6 MONTHS	145 HOURS