CERTIFIED ETHICAL HACKING

v.11

R-TECH TECHINCAL INSTITUTE

Course Description

The Certified Ethical Hacker program is a trusted and respected ethical hacking training Program that any information security professional will need.

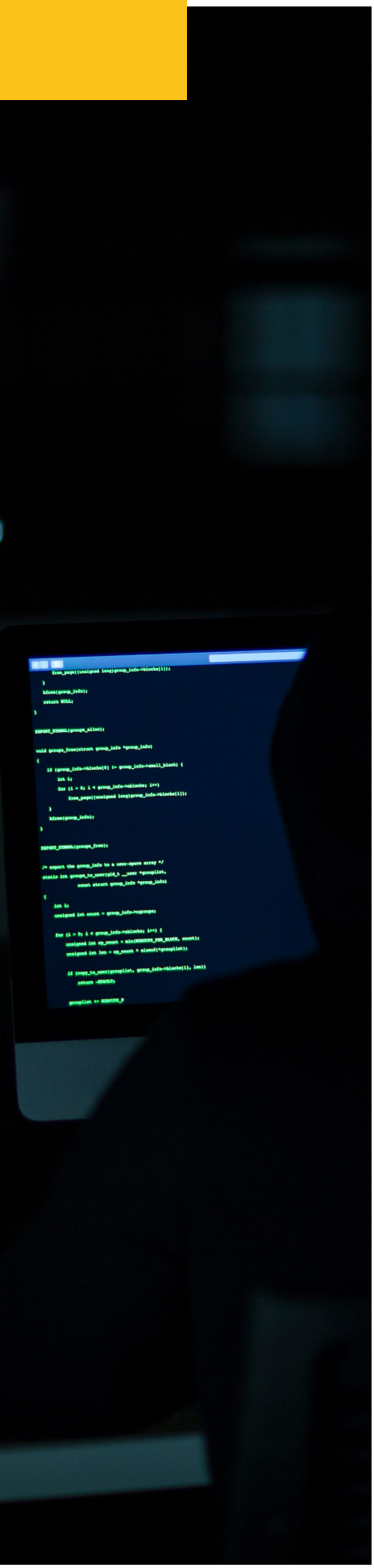
Since its inception in 2003, the Certified Ethical Hacker has been the absolute choice of the industry globally. It is a respected certification in the industry and is listed as a baseline certification on the United States Department of Defense Directive 8570. In fact, the C|EH exam is ANSI 17024 compliant adding credibility and value to credential members.

C|EH is used as a hiring standard and is a sought after certification by many of the Fortune 500 organizations, governments, cybersecurity practices, and a cyber staple in education across many of the most prominent degree programs in top Universities around the globe.

This course will immerse you into a "Hacker Mindset" in order to teach you how to think like a hacker and better defend against future attacks. It puts you in the driver's seat with a hands-on training environment employing a systematic ethical hacking process.

You are trained on creative hacking techniques to achieve optimal information security posture in any target organization! You will learn how to scan, test, hack and secure target systems. The course covers the Five Phases of Ethical Hacking, diving into Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

The tools and techniques in each of these five phases are provided in detail in an encyclopaedic approach and absolutely no other program offers you the breadth of learning resources, labs, tools and techniques than the C|EH program.



Course Outline

- *Introduction to Ethical Hacking*
- *Footprinting and Reconnaissance*
- *Scanning Networks*
- *Enumeration*
- *Vulnerability Analysis*
- *System Hacking*
- *Malware Threats*
- *Sniffing*
- *Social Engineering*
- *Denial-of-Service*
- *Session Hijacking*
- *Evading IDS, Firewalls, and Honeypots*
- *Hacking Web Servers*
- *Hacking Web Applications*
- *Hacking Wireless Networks*
- *Hacking Mobile Platforms*
- *SQL Injection*
- *IoT Hacking*
- *Cloud Computing*
- *Cryptography*

What will you learn?

1. *Key issues plaguing the information security world, incident management processes, and penetration testing*
2. *Footprinting, footprinting tools, and countermeasures*
3. *Network scanning techniques and scanning countermeasures*
4. *Enumeration techniques and enumeration countermeasures*
5. *System hacking methodology, steganography, steganalysis attacks, and the processes involved in covering tracks*
6. *Trojans, Trojan analysis, and Trojan countermeasures*
7. *Working of viruses, virus analysis, computer worms, malware analysis procedure, an countermeasures*
8. *Packet sniffing techniques and how to defend against sniffing*
9. *Social engineering techniques, identify theft, and social engineering countermeasures*
10. *DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures*
11. *Session hijacking techniques and countermeasures*
12. *Webserver attacks, attack methodology, and countermeasures*
13. *Web application attacks, web application hacking methodology, and countermeasures*
14. *SQL injection attacks and injection detection tools*
15. *Wireless encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools*

Thank You

www.rtnss.in

+91 9324805066