CEH V10 CERTIFIED ETHICAL HACKER

BY THE GENEVA INSTITUTE OF TECHNOLOGY

"OUR CERTIFICATIONS ARE HERE TO STRENGHTEN YOUR CURRICULUM AND TO MAKE YOU GROW WITHIN TECHNOLOGY"

Quai du Seujet 10
1201 Genève
022 757 86 36

THE COURSE

The Certified Ethical Hacker program is the most desired information security training program any information security professional will ever want to be in. To master the hacking technologies, you will need to become one, but an ethical one! The accredited course provides the advanced hacking tools and techniques used by hackers and information security professionals alike to break into an organization. As we put it, **"To beat a hacker, you need to think like a hacker".**

This course will immerse you into the Hacker Mindset so that you will be able to defend against future attacks. The security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment.
This ethical hacking course puts you in the driver's seat of a hands-on environment with a systematic process. Here, you will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! You will scan, test, hack and secure your own systems. You will be taught the five phases of ethical hacking and the ways to approach your target and succeed at breaking in every time! The five phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

WHAT WILLL YOU LEARN?

- Key issues plaguing the information security world, incident management process, and penetration testing.
- Various types of footprinting, footprinting tools, and countermeasures.
- Network scanning techniques and scanning countermeasures.
- Enumeration techniques and enumeration countermeasures.
- System hacking methodology, steganography, steganalysis attacks, and covering tracks.
- Different types of Trojans, Trojan analysis, and Trojan countermeasures.
- Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures.
- Packet sniffing techniques and how to defend against sniffing.
- Social Engineering techniques, identify theft, and social engineering countermeasures.

DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures.

- Session hijacking techniques and countermeasures.
- Different types of webserver attacks, attack methodology, and countermeasures.
- Different types of web application attacks, web application hacking methodology, and countermeasures.
- SQL injection attacks and injection detection tools.
- Wireless Encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.
- Mobile platform attack vector, android vulnerabilities, mobile security guidelines, and tools.
- Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures.
- Various cloud computing concepts, threats, attacks, and security techniques and tools.
- Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.
- Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
- Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.
- Different threats to IoT platforms and learn how to defend IoT devices securely.

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**
- **SQL** Injection
- Hacking **Wireless Networks**
- Hacking **Mobile Platforms**
- **IoT** Hacking
- **Cloud Computing**
- **Cryptography**

AUDIENCE & PRE REQUISITES

- Ethical hackers
- System Administrators,
- Network Administrators and Engineers
- Webmanagers
- Auditors
- Security Professionals in general.

DURATION & PRICE

- **3 months** and **1 week**
- **13 sessions** that last **3.15 hours** each
- **CHF 5000.-** with examination voucher

ABOUT THE EXAM

- **Number of Questions:** 125
- **Test Duration:** 4 HoursTest
- **Format:** Multiple Choice
- **Test Delivery:** ECC EXAM, VUE