CloudSystems Limited
Ka-57/1, Kazi Tower 3rd Floor,
Kuril Bus Stand, Dhaka-1229.
☎+880 1712900654

Certified Ethical Hacker (CEH) V9

Course Description:

The Certified Ethical Hacker (CEH) program is the core of the most desired information security training system any information security professional will ever want to be in. The CEH, is the first part of a 3 part EC-Council Information Security Track which helps you master hacking technologies. You will become a hacker, but an ethical one! As the security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment, this course was designed to provide you with the 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. It puts you in the driver's seat of a hands-on environment with a systematic ethical hacking process.

Duration:

5 Days (40 Hours)

Target Audience:

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of their network infrastructure.

Required Prerequisites:

It is Mandatory for student to record two years of information security related work experience and get the same endorsed by your employer. In case you do not process the same you can send us a request detailing your educational background and request for consideration on a case basis. The age requirement for attending the training or attempting the exam is restricted to any candidate that is at least 18 years old.

Certification:

The Certified Ethical Hacker exam 312-50 may be taken on the last day of the training (optional). Students need to pass the online exam to receive CEH certification.

Exam Details:

Exam Title: Certified Ethical Hacker v9 (ANSI)
Exam Code: 312-50 (ECC EXAM), 312-50 (VUE)
Number of Questions: 125
Duration: 4 hours
Availability: VUE / ECCEXAM
Test Format: Multiple Choice
Passing Score: 70%

Course Content:

CEHv9 consists of 20 core modules designed to facilitate a comprehensive ethical hacking and Penetration testing training.

1. Introduction to Ethical Hacking
2. Footprinting and Reconnaissance
3. Scanning Networks
4. Enumeration

Ka-57/1, Kazi Tower 3rd Floor,
Kuril Bus Stand, Dhaka-1229.
☎+880 1712900654

5. System Hacking
6. Malware Threats
7. Evading IDS, Firewalls and Honeypots
8. Sniffing
9. Social Engineering
10. Denial of Service
11. Session Hijacking
12. Hacking Web servers
13. Hacking Web Applications
14. SQL Injection
15. Hacking Wireless Networks
16. Hacking Mobile Platforms
17. Cloud Computing
18. Cryptography

What will you learn?

Students going through CEH training will learn:

1. Key issues plaguing the information security world, incident management process, and penetration testing
2. Various types of 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 covering tracks
6. Different types of Trojans, Trojan analysis, and Trojan countermeasures
7. Working of viruses, virus analysis, computer worms, malware analysis procedure, and 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. Different types of webserver attacks, attack methodology, and countermeasures
13. Different types of 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
16. Mobile platform attack vector, android vulnerabilities, jailbreaking iOS, windows phone 8 vulnerabilities, mobile security guidelines, and tools
17. Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures
18. Various cloud computing concepts, threats, attacks, and security techniques and tools
19. Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools
20. Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap