Module Title : Certified Ethical Hacker v11

Duration : 5 days

Overview

The Certified Ethical Hacker (CEH) credential is the most trusted ethical hacking certification and accomplishment recommended by employers globally. It is the most desired information security certification and represents one of the fastest-growing cyber credentials required by critical infrastructure and essential service providers. Since the introduction of CEH in 2003, it is recognized as a standard within the information security community. CEH v11 continues to introduce the latest hacking techniques and the most advanced hacking tools and exploits used by hackers and information security professionals today. The Five Phases of Ethical Hacking and the original core mission of CEH remain valid and relevant today: "To beat a hacker, you need to think like a hacker."

CEH provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach you how hackers think and act maliciously so that you will be better positioned to set up your security infrastructure and defend future attacks. Understanding system weaknesses and vulnerabilities help organizations strengthen their system security controls to minimize the risk of an incident. CEH was built to incorporate a hands-on environment and systematic process across every ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to perform the job of an ethical hacker. You will be exposed to an entirely different posture towards the responsibilities and measures required to be secure. In its 11th version, CEH continues to evolve with the latest operating systems, tools, tactics, exploits, and technologies. Here are some critical updates of CEH v11:

- **Incorporating Parrot Security OS**
  - When compared to Kali Linux, Parrot Security OS offers better performance on lower-powered laptops and machines while offering an intuitive look and feel with a larger repository of general tools.
- **Re-Mapped to NIST/NICE Framework**
  - CEH v11 is mapped rigorously to important Specialty Areas under the NIST/NICE framework's Protect and Defend (PR) job role category overlapping with other job roles, including Analyze (AN) and Securely Provision (SP).
- **Enhanced Cloud Security, IoT, and OT Modules**
  - CEH v11 covers updated Cloud and IoT modules to incorporate CSP's Container Technologies (e.g., Docker, Kubernetes), Cloud Computing threats, and a number of IoT hacking tools (e.g. Shikra, Bus

Pirate, Facedancer21, and more). This is critical as the world moves towards broader and deeper cloud adoptions.

- **Cloud–Based Threats**
  - As the cloud industry is estimated to reach $354 billion by 2022, the businesses struggle to limit the frequency of data theft incidents due to misconfigured cloud environments. January to April 2020 alone saw a 630% spike in cloud-based attacks. Learn how to avoid, identify, and respond to cloud-based attacks with CEH v11.
- **IoT Threats**
  - Market reports anticipate that the worldwide IoT-connected devices are expected to reach 43 billion by 2023. To support this rapid expansion, the prominent players of the internet, including Amazon Web Services, Google, IBM, Microsoft, are swiftly shifting to private cloud services, creating complexities in IoT ecosystems. Learn to deal with IoTbased attacks with the CEH v11 course that covers the latest IoT hacking tools, such as Shikra, Bus Pirate, Facedancer21, and many others.
- **Operational Technology (OT} Attacks**
  - Last year, businesses experienced a 2,000% increase in OT based incidents. You can gain expertise in OT, IT, and IIoT (industrial IoT) to secure a critical enterprise OT/IoT deployments. To learn the advanced skills of OT, CEH covers concepts of OT, such as ICS, SCADA, and PLC, various challenges of OT, OT hacking methodology, tools, communication protocols of an OT network like Modbus, Profinet, HART-IP, SOAP, CANopen, DeviceNet, Zigbee, Profibus, etc., and gaining Remote Access using DNP3 protocol.
- **Modern Malware Analysis**
  - CEH v11 now includes the latest malware analysis tactics for ransomware, banking and financial malware, IoT botnets, OT malware analysis, Android malware, and more!
- **Covering the Latest Threats - Fileless Malware**
  - As the security community observed a rise in fileless attacks, it began to raise concerns about fileless malware attacks. As fileless malware is a relatively new form of malware attack, organizations find it difficult to detect with endpoint security solutions. With the CEH v11, you can now learn various fileless malware techniques with associated defensive strategies, as the course focuses on the taxonomy of fileless malware threats, fileless malware obfuscation techniques to bypass antivirus,

launching fileless malware through script-based injection, launching fileless malware through phishing, and more.

- **New Lab Designs and Operating Systems**
  - This latest iteration of CEH v11 includes new operating systems, including Windows Server 2019, Windows Server 2016, and Windows 10 configured with Domain Controller, firewalls, and vulnerable web applications for practicing and improving hacking skills.
- **Increased Lab Time and Hands–on Focus**
  - More than 50% of the CEH v11 course is dedicated to practical skills in live ranges via EC-Council labs. EC-Council leads in this aspect of the industry.
- **Industry's Most Comprehensive Tools Library**
  - The CEH v11 course includes a library of the latest tools required by security practitioners and pen testers across the world.

Target Audience

- Information Security Analyst / Administrator
- Information Assurance (IA) Security Officer
- Information Security Manager / Specialist
- Information Systems Security Engineer / Manager
- Information Security Professionals / Officers
- Information Security / IT Auditors
- Risk / Threat/Vulnerability Analyst
- System Administrators
- Network Administrators and Engineers

Certification

To be eligible to challenge the EC-Council CEH certification examination, the candidate has two options:

Attend Official Network Security Training by EC-Council:

If a candidate has completed an official EC-Council training at an Accredited Training Center, the candidate is eligible to challenge the relevant EC-Council exam without going through the application process.

Attempt the Exam without Official EC-Council Training:

In order to be considered for the EC-Council CEH exam without attending official network security training, the candidate must have at least 2 years of work experience in the Information Security domain. If the candidate has the required work experience, they can submit an eligibility application form along with a non-refundable fee

Course Outline

Module 01: Introduction to Ethical Hacking
Module 02: Footprinting and Reconnaissance
Module 03: Scanning Networks
Module 04: Enumeration
Module 05: Vulnerability Analysis
Module 06: System Hacking
Module 07: Malware Threats
Module 08: Sniffing
Module 09: Social Engineering
Module 10: Denial-of-Service
Module 11: Session Hijacking
Module 12: Evading IDS, Firewalls, and Honeypots
Module 13: Hacking Web Servers
Module 14: Hacking Web Applications
Module 15: SQL Injection
Module 16: Hacking Wireless Networks
Module 17: Hacking Mobile Platforms
Module 18: IoT and OT Hacking
Module 19: Cloud Computing
Module 20: Cryptography

What will you learn?

1. Key issues include plaguing the information security world, ethical hacking, information security controls, laws, and standards.
2. Perform footprinting and reconnaissance using the latest footprinting techniques and tools as a critical pre-attack phase required in ethical hacking.
3. Network scanning techniques and scanning countermeasures.
4. Enumeration techniques and enumeration countermeasures.
5. Vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.
6. System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities.

7. Different types of malware (Trojan, Virus, worms, etc.), system auditing for malware attacks, malware analysis, and countermeasures.
8. Packet sniffing techniques to discover network vulnerabilities and countermeasures to defend sniffing.
9. Social engineering techniques and how to identify theft attacks to audit human level vulnerabilities and suggest social engineering countermeasures.
10. DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS countermeasures.
11. Session hijacking techniques to discover network-level session management, authentication/authorization, cryptographic weaknesses, and countermeasures.
12. Web server attacks and a comprehensive attack methodology to audit vulnerabilities in web server infrastructure, and countermeasures.
13. Web application attacks and comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.
14. SQL injection attack techniques, injection detection tools to detect SQL injection attempts, and countermeasures.
15. Wireless encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.
16. Mobile platform attack vector, android vulnerability exploitations, and mobile security guidelines and tools.
17. Firewall, IDS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.
18. Cloud computing concepts (Container technology, serverless computing), various threats/attacks, and security techniques and tools.
19. Penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
20. Threats to IoT and OT platforms and learn how to defend IoT and OT devices securely.
21. Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.