SULFMAN TRAININGS

COURSE:

CERTIFIED ETHICAL HACKER (CEHV12)

CERTIFIED ETHICAL HACKER (CEHV12)

OVERVIEW

C|EH v12 will teach you the latest commercial-grade hacking tools, techniques, and methodologies used by hackers and information security professionals to lawfully hack an organization. C|EH v12 has designed a new learning framework that uses a 4-phase methodology that includes: Learn, Certify, Engage and Compete. C|EH v12 is a renewed program that teaches you everything you need to know about ethical hacking with training, labs, assessment, a mock engagement(practice) and even a series of global hacking competitions

TARGET AUDIENCE

- **Target Audience:**
- **Mid-Level Information Security Auditor**
- **Cybersecurity Auditor**
- **Security Administrator**
- **IT Security Administrator**
- **Cyber Defense Analyst**
- **Vulnerability Assessment Analyst**
- **Warning Analyst**
- **Information Security Analyst 1**
- **Security Analyst L1**
- **Infosec Security Administrator**
- **Cybersecurity Analyst level 1, level 2, & level 3**
- **Network Security Engineer**
- **SOC Security Analyst**
- **Security Analyst**
- **Network Engineer**
- **Senior Security Consultant**
- **Information Security Manager**
- **Senior SOC Analyst**
- **Solution Architect**
- **Cybersecurity Consultant**

COURSE OUTCOMES

- Identify information security controls, laws, and standards
- Various types of footprinting, footprinting tools, and countermeasures
- Network scanning techniques and scanning countermeasures
- Enumeration techniques and enumeration countermeasures
- Vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems
- System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities
- System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities
- Different types of malware (Trojan, Virus, worms, etc.), system auditing for malware attacks, malware analysis, and countermeasures,