Certified Ethical Hacker- Course

Codevirus Security

CODEVIRUS SECURITY - 2022

Certified Ethical Hacker

MODULES

- Module 01 Introduction to Ethical Hacking
- Module 02 Footprinting and Reconnaissance
- Module 03 Scanning Networks
- Module 0 4 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

MODULES

- Module 11 Session Hijacking
- Module 12 Evading IDS, Firewalls, and Honeypots
- Module 13 Hacking Web Servers
- Module 14 Hacking Web Applications
- Module 15 SQLInjection
- Module 16 Hacking Wireless Networks
- Module 17 Hacking Mobile Platforms
- Module 18 IoT and OTHacking
- Module 19 Cloud Computing
- Module 20 Cryptography

What will you learn?

Key issues include plaguing the information security world, ethical hacking, information securitycontrols,laws, and standards.

Perform footprinting and reconnaissance using the latest footprinting techniques and tools as a critical pre-attack phase required in ethical hacking.

What will you learn?

Network scanning techniques and scanning counter measures.

Enumeration techniques and enumeration countermeasures.

Vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.

What will you learn?

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 counter measures.

Packet sniffing techniques to discover network vulnerabilities and counter measures to defend sniffing.

What will you learn?

Social engineering techniques and how to identify theft attacks to audit human-level vulnerabilities and suggest social engineering countermeasures.

DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS

Session hijacking techniques to discover Network-level session management, authentication/authorization, cryptographic weaknesses, and countermeasures.

What will you learn?

Web server attacks and a comprehensive attack methodology to audit vulnerabilities in web server infrastructure, and countermeasures.

Web application attacks and comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.

SQL injection attack techniques, injection detection tools to detect SQL injection attempts, and countermeasures.

What will you learn?

Wireless encryption, wireless hacking methodology, wireless hacking tools,and Wi-Fi security tools.

Mobile platformattack vector, android vulnerability exploitations, and mobile security guidelines and tools.

Firewall, IDS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.

What will you learn?

Cloud computing concepts(Container technology, serverless computing), various threats/attacks, and security techniques and tools.

Penetration testing, security audit, vulnerability assessment, and penetration testingroadmap.

Threats to IoT and OT platforms and learn how to defend IoT and OT devices securely.

Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysistools.