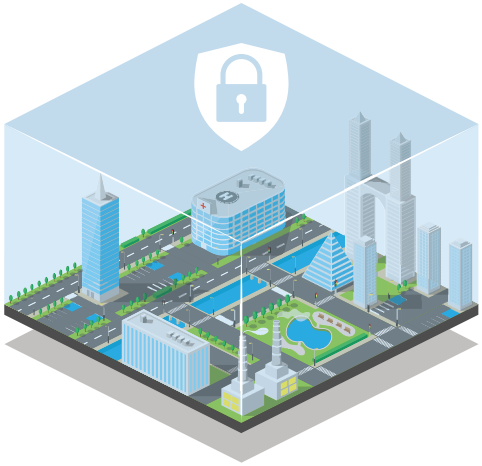
SCOPE GLOBAL SKILLS UNIVERSITY
CENTRAL INDIA'S 1st SKILLS UNIVERSITY

AISECT LEARN
Better Education. Better Careers.

BLENDED (LIVE + SELF PACED)

CERTIFIED IN ETHICAL HACKER



Call Now:
+91 7880100790

www.sgsuniversity.ac.in

COURSE OVERVIEW

The Course introduces you with the Cyber Security Fundamentals, footprinting and Reconnaissance, Scanning Networks, Enumeration, Vulnerability Analysis, System Hacking, Malware Threats, Sniffing, Social Engineering, Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks, Session Hijacking, Web Application Hacking, Wireless Network Security, Evading IDS, Firewalls, and Honeypots, and Cryptography. At the end, we have a hands-on live project where we will implement all the concepts learned.

COURSE OBJECTIVE

The goal of the CEH course is to give students the information and abilities they need to secure and ethically hack computer networks, systems, and applications. The ultimate objective is to provide experts with the knowledge and skills necessary to spot vulnerabilities and fix them before malevolent hackers can take advantage of them, improving cybersecurity generally.

WHAT YOU WILL LEARN

In this course, you will learn CIA Traid, OSI/TCP-IP Model, Transmission Medium, VAPT TTP, Network Monitoring and Analysis, Static and Dynamic Malware Analysis, Different Cyber Attacks and Mitigation.

COURSE SKILL SET

System Hacking
Malware analysis
Network Scanning
Vulnerability analysis
Social Engineering
DOS Attack
Firewall and Honeypots
Web Server Hacking
Web Application
SQL Injection

PROGRAM HIGHLIGHTS

Instructor- Mr. Aman Kumar Gupta | Cyber Security Trainer & Bug Hunter
Access - 1 Year
Duration - 100 hours
Eligibility- 10th pass
No. of Modules - 20 modules
Language - English
Shareable certificate - Yes
Webinar- Yes

PROGRAM SYLLABUS

Module 1 - Information Security Overview Information Security Threats and Attack Vectors Hacking Concepts Ethical Hacking Concepts Information Security Controls Penetration Testing Concepts Information Security Laws and Standards.

Module 2 - Learn how to use the latest techniques and tools to perform footprinting and reconnaissance, a critical pre-attack phase of the ethical hacking process.

Module 3 - Network Scanning Concepts Scanning Tools Scanning Techniques Scanning Beyond IDS and Firewall Banner Grabbing Scanning Pen Testing.

Module 4 - Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, and associated countermeasures.

Module 5 - Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools.

Module 6- Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.

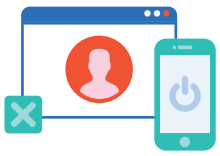
Module 7 - Learn different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures.

Module 10 - Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Module 11 - Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

Module 12 - Get introduced to firewall, intrusion detection system (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

Module 13 - Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.



Module 14 - Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

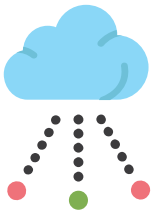
Module 15 - Learn about SQL injection attacks, evasion techniques, types of sql injection, and SQL injection countermeasures.

Module 16 - Understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi security tools, and countermeasures.

Module 17 - Learn Mobile platform attack vectors, android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

Module 18 - IoT Concepts IoT Attacks IoT Hacking Methodology IoT Hacking Tools Countermeasures

Module 19- Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodology, and cloud security techniques and tools.



Module 20- Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.