CYBER™
SAVIOURS

WHEN CYBERCRIME STRIKES - CYBERSAVIOURS RESPOND

CS | CEH (Cybersaviours Certified Ethical Hacker)

Importance of CS | CEH

85% Career
Advancement

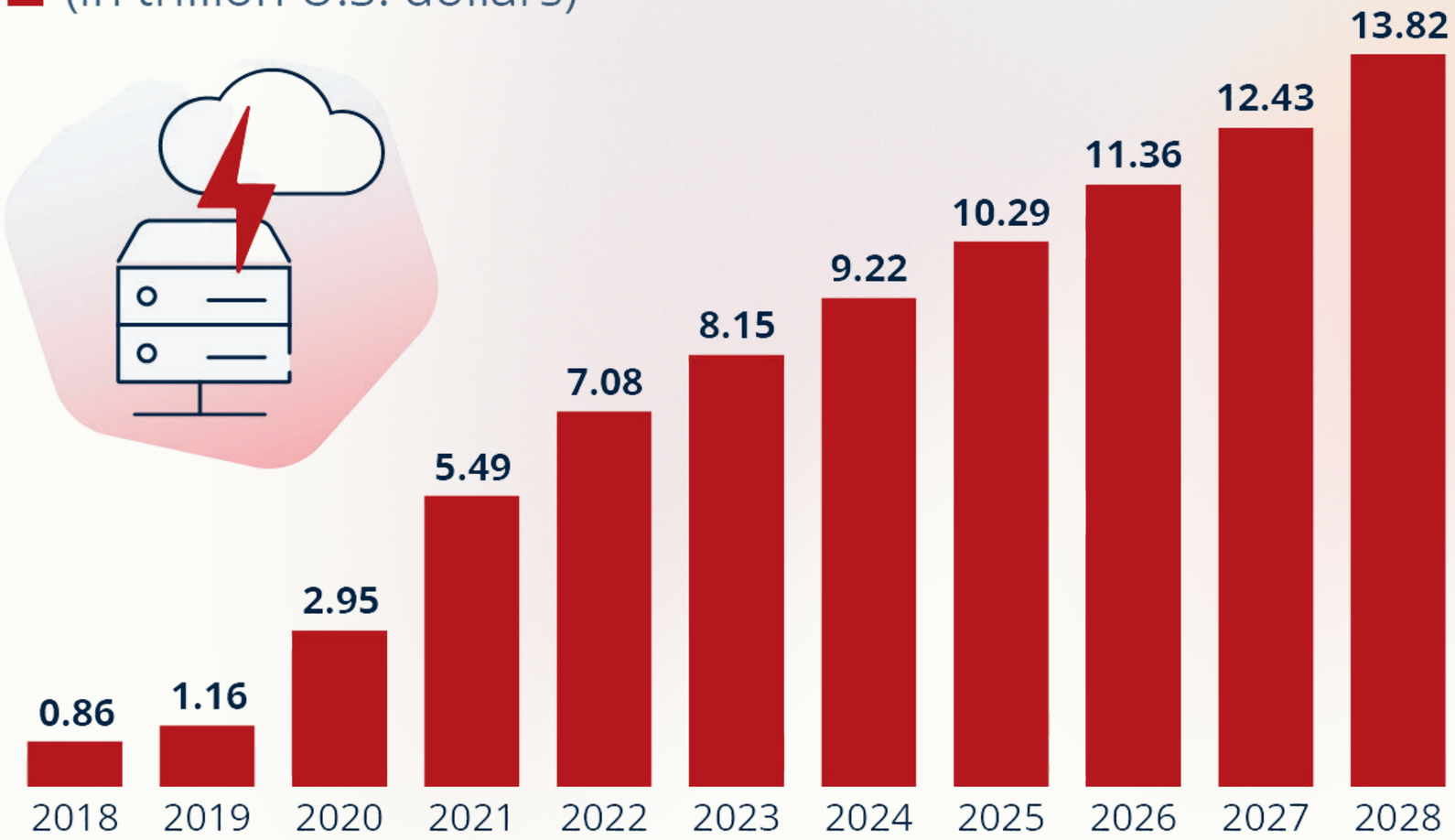
Higher Salary
Increased Potential

Latest Tools
Cutting-Edge Tech

Real-World
Attack Scenarios

Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide (in trillion U.S. dollars)



68%

Increase in cyber attacks reported in 2023

4.1 Million

Global Cybersecurity Workforce Gap

32%

Increased from 2023 -24

Program Strategic Overview

Training Scope

In-depth training progressing from foundational cybersecurity concepts to advanced attack and defense techniques.

Practical Experience

Emphasizes hands-on practice with industry-standard tools and real-world scenarios to ensure practical skill development

Learning Objectives

- Develop comprehensive understanding of ethical hacking methodologies
- Master advanced network scanning and vulnerability assessment technique
- Gain proficiency in using cutting-edge cybersecurity tools

Course Modules

Module 1: Introduction to Ethical Hacking :

Objective: Build foundational knowledge in ethical hacking and understand cybersecurity threats, vulnerabilities.

- **Key Topics:**
  - Definition of Ethical Hacking and Penetration Testing
  - Cybersecurity Threat Landscape and Attack Vectors
  - Information Security Controls, Laws, and Compliance
  - Ethical Hacking Phases

- **Learning Outcome:** Understand the ethical hacking and the fundamentals of cybersecurity

Module 2: Footprinting and Reconnaissance

Objective: Master techniques for collecting information on a target network, including identifying vulnerabilities.

- **Key Topics:**
  - Footprinting Techniques: Active vs. Passive
  - Information Gathering: DNS, WHOIS, Network Mapping
  - Social Engineering and Physical Security Evasion
  - Countermeasures to Reconnaissance Techniques

- **Learning Outcome:** Practical experience in gathering and analyzing open-source information on targets.

- **Hands-on Lab:** Conducting footprinting to gather network details and identify potential entry points.

- **Tools:**
  - WHOIS
  - Shodan
  - theHarvester
  - Google Dorks
  - shodan.io
  - whois.net
  - Recon-ng
  - Maltego

Module 3: Scanning Networks

Objective: Develop skills in network scanning, open port identification, and network mapping.

- **Key Topics:**
  - Network Scanning Techniques: Ping Sweep, Port Scanning, Vulnerability Scanning
  - Identifying Live Systems, Open Ports, Service Version Detection
  - OS Fingerprinting and Network Topology Analysis

- **Learning Outcome:** Ability to accurately map network infrastructure and identify vulnerabilities.

- **Hands-on Lab:** Using network scanners to identify live hosts, open ports, and services.

- **Tools:**
  - Nmap
  - Angry IP Scanner
  - Netcat
  - Zenmap

Module 4: Enumeration

Objective: Enhance skills in gathering detailed information about networks, systems, and services.

- **Key Topics:**
  - Enumeration Techniques: User and Group, Network and Service
  - DNS, SNMP, and LDAP Enumeration

- **Learning Outcome:** Proficiency in extracting sensitive information via network services and protocols.

- **Hands-on Lab:** Conducting enumeration exercises to reveal details about user accounts and network services.

- **Tools:**
  - SNMP Enumeration Tool
  - Nessus
  - Enum4linux
  - Netcat
  - Metasploit
  - exploit-db.com

Module 5: Vulnerability Analysis

Objective: Equip participants with skills to assess vulnerabilities and prioritize security risks.

- **Key Topics:**
  - Vulnerability Assessment Lifecycle
  - Common Vulnerabilities and Exploits (CVEs)
  - Using Vulnerability Scanners

- **Learning Outcome:** Ability to identify, analyze, and report vulnerabilities in a network and website.

Hands-on Lab: Conducting vulnerability assessments with a focus on prioritizing findings

- **Tools:**
  - OpenVAS
  - Nessus
  - Nikto
  - cvedetails.com

Module 6: System Hacking

Objective: Learn to compromise systems and gain unauthorized access, while understanding defensive measures.

- **Key Topics:**
  - Gaining Access and Escalating Privileges
  - Password Cracking, Keylogging, and Privilege Escalation
  - Covering Tracks and Creating Backdoors

- **Learning Outcome:** Mastery in using tools for system hacking and understanding countermeasures.

- **Hands-on Lab:** Exploiting systems and covering tracks on compromised machines.

- **Tools:**
  - Metasploit
  - John the Ripper
  - Cain & Abel
  - Mimikatz
  - PowerShell Empire
  - exploit-db.com

Module 7: Malware Threats

Objective: Understand the techniques for creating and deploying malware and learn about mitigation.

- **Key Topics:**
  - Types of Malware: Viruses, Worms, Trojans, Ransomware
  - Malware Analysis and Creation
  - Countermeasures and Mitigations

- **Learning Outcome:** Ability to identify malware threats, analyze them, and understand their effects on systems.
- **Hands-on Lab:** Analysing malware samples and testing detection methods.

- **Tools:**
  - REMnux
  - Cuckoo Sandbox
  - Process Monitor
  - Wireshark
  - virustotal.com
  - malwarebytes.com

Module 8: Sniffing

Objective: Master techniques for intercepting and analyzing network traffic, while understanding counter-sniffing techniques.

- **Key Topics:**
  - Packet Sniffing Techniques: Passive vs. Active
  - Protocol Analysis and Password Sniffing
  - Countermeasures for Sniffing Attacks

- **Learning Outcome:** Proficiency in packet capturing, analyzing network traffic, and applying anti-sniffing techniques.

- **Hands-on Lab:** Using packet sniffers to capture and analyze network data.

- **Tools:**
  - Wireshark
  - Tcpdump
  - Snort
  - Ettercap

Module 9: Social Engineering

Objective: Understand social engineering techniques, including psychological manipulation and phishing tactics.

- **Key Topics:**
  - Types of Social Engineering Attacks: Phishing, Pretexting, Baiting
  - Techniques for Human Manipulation and Psychological Exploitation
  - Countermeasures and Employee Training

- **Learning Outcome:** Ability to recognize and prevent social engineering attacks.

- **Hands-on Lab:** Simulating phishing attacks and evaluating awareness measures.

- **Tools:**
  - SET (Social-Engineer Toolkit)
  - Gophish
  - Maltego
  - social-engineer.org

Module 10: Denial-of-Service (DoS) Attacks

Objective: Develop an understanding of DoS and DDoS attacks, as well as mitigation techniques.

- **Key Topics:**
  - DoS Attack Types: Flood Attacks, SYN Flood, Ping of Death
  - Distributed Denial-of-Service (DDoS) Mechanisms
  - Detection and Mitigation Techniques

- **Learning Outcome:** Proficiency in identifying and countering DoS attacks.

- **Hands-on Lab:** Conducting DoS simulations and implementing defensive measures.

- **Tools:**
  - LOIC (Low Orbit Ion Cannon)
  - Hping3
  - OWASP ZAP
  - cloudflare.com/ddos

Module 11: Session Hijacking

Objective: Learn techniques to intercept and hijack active sessions and apply counter-hijacking measures.

- **Key Topics:**
  - Session Hijacking Concepts: Cookie Hijacking, Sidejacking, Cross-Site Scripting (XSS)
  - Tools and Techniques for Interception
  - Preventive Measures and Secure Session Management

- **Learning Outcome:** Capability to conduct and prevent session hijacking.

- **Hands-on Lab:** Session hijacking exercises to identify and mitigate vulnerabilities.

- **Tools:**
  - Wireshark
  - Burp Suite
  - Firesheep
  - owasp.org

Module 12: Evading IDS, Firewalls, and Honeypots

Objective: Master evasion techniques to bypass detection systems such as IDS, firewalls, and honeypots.

- **Key Topics:**
  - Intrusion Detection and Prevention Systems (IDS/IPS)
  - Firewall and Honeypot Evasion Tactics
  - Countermeasures and Detection Techniques

- **Learning Outcome:** Capability to conduct and prevent session hijacking.

- **Hands-on Lab:** Skills in evading IDS and firewalls while understanding counter-evasion measures.

- **Tools:**
  - Nmap
  - Snort
  - Nikto
  - Metasploit

Module 13: Hacking Web Servers

Objective:Gain expertise in exploiting web server vulnerabilities and applying security measures..

- **Key Topics:**
  - Common Web Server Vulnerabilities: Directory Traversal, Misconfiguration, DDoS
  - Techniques for Exploiting Web Server Weaknesses
  - Defensive Strategies for Securing Web Servers

- **Learning Outcome:** Proficiency in identifying, exploiting, and securing web server vulnerabilities

- **Hands-on Lab:** Simulating attacks on web servers and applying security configurations.

- **Tools:**
  - Nikto
  - Metasploit
  - Nessus
  - securityheaders.com

Module 14: Hacking Web Applications

Objective: Understand web application vulnerabilities, exploit common weaknesses, and apply secure development practices

- **Key Topics:**
  - Web Application Vulnerabilities: XSS, CSRF, SQL Injection, LFI/RFI
  - Techniques for Exploiting and Securing Web Applications
  - OWASP Top 10 Security Risks

- **Learning Outcome:** Ability to detect and mitigate web application vulnerabilities.

- **Hands-on Lab:** Performing vulnerability assessments and exploiting web application flaws.

- **Tools:**
  - Burp Suite
  - OWASP ZAP
  - Acunetix
  - owasp.org

Module 15: SQL Injection

Objective: Master SQL injection techniques to compromise databases and implement secure coding practices.

- **Key Topics:**
  - SQL Injection Basics: Error-Based, Blind, Union-Based
  - Techniques for Database Exploitation and Data Exfiltration
  - Secure Coding and Mitigation Strategies

- **Learning Outcome:** Proficiency in detecting SQL vulnerabilities and applying countermeasures.

- **Hands-on Lab:** Conducting SQL injection attacks and practicing secure coding.

- **Tools:**
  - SQLmap
  - Havij
  - SQL Ninja
  - exploit-db.com

Module 16: Hacking Wireless Networks

Objective: Understand wireless network vulnerabilities and apply tools and techniques to exploit and secure wireless communications.

- **Key Topics:**
  - Wireless Network Protocols: WEP, WPA, WPA2
  - Common Attacks: Evil Twin, Deauthentication, MAC Spoofing
  - Wireless Security Standards and Best Practices

- **Learning Outcome:** Ability to assess and secure wireless networks against common threats.

- **Hands-on Lab:** Simulating attacks on wireless networks and implementing security measures.

- **Tools:**
  - Aircrack-ng
  - Wireshark
  - Kismet
  - Fern WiFi Cracker

Module 17: Hacking Mobile Platforms

Objective: Explore vulnerabilities in mobile platforms and understand methods for assessing and securing mobile applications and operating systems.

- **Key Topics:**
  - Mobile OS Vulnerabilities: Android, iOS
  - Mobile App Security Risks: Code Injection, Data Leakage
  - Security Measures for Mobile Devices and Applications

- **Learning Outcome:** Proficiency in identifying and securing mobile application vulnerabilities.

- **Hands-on Lab:** Performing vulnerability assessments on mobile applications and devices.

- **Tools:**
  - Drozer
  - MobSF (Mobile Security Framework)
  - APKTool
  - Burp Suite Mobile Assistant

Module 18: IoT and OT Hacking

Objective: Gain expertise in identifying vulnerabilities in Internet of Things (IoT) and Operational Technology (OT) environments.

- **Key Topics:**
  - IoT Protocols and Technologies: MQTT, CoAP
  - IoT and OT Security Challenges
  - Exploitation and Countermeasures for IoT/OT Environments

- **Learning Outcome:** Understanding of IoT/OT vulnerabilities and the ability to secure connected devices and industrial systems

- **Hands-on Lab:** Conducting security assessments on IoT and OT systems.

- **Tools:**
  - Shodan
  - IoT Inspector
  - Wireshark
  - Nmap

Module 19: Cloud Computing

Objective: Gain expertise in cloud security vulnerabilities and understand methods for securing cloud environments.

- **Key Topics:**
  - Cloud Security Architecture: Public, Private, Hybrid, and Community Clouds
  - Cloud-Specific Threats: Data Breaches, Account Hijacking, Misconfiguration
  - Compliance and Security Standards for Cloud Environments

- **Learning Outcome:** Ability to identify cloud vulnerabilities, apply security measures, and understand cloud compliance requirements.

- **Hands-on Lab:** Conducting cloud security assessments and implementing security configurations.

- **Tools:**
  - CloudSploit
  - ScoutSuite
  - AWS CloudTrail
  - Microsoft Azure Security Center

Module 20: Cryptography

Objective: Understand and apply cryptographic principles for secure data transmission and storage.

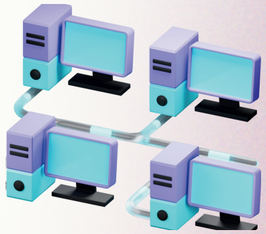
- **Key Topics:**
  - Cryptographic Algorithms: Symmetric, Asymmetric, Hash Functions
  - Digital Signatures, Certificates, and Public Key Infrastructure (PKI)
  - Encryption and Decryption Techniques for Data Protection

- **Learning Outcome:** Proficiency in encryption methods, cryptographic standards, and secure key management

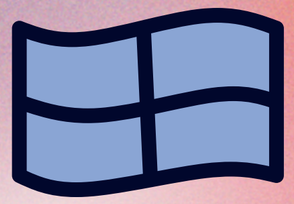
- **Hands-on Lab:** Implementing encryption and decryption processes and using digital certificates.

- **Tools:**
  - OpenSSL
  - HashCalc
  - GnuPG
  - Keyczar

Prerequisites



Networking Basics



Basics of Operating Systems (Windows,Linux)

Basics of Programming (Python,Bash,Javascript)

Pricings

Certification with Credits	₹34,999
LOR (Letter of Recomendation)	$499

Why Choose Cybersaviours

Advanced Curriculum

- Latest Techniques
- Emerging threat-Landscape
- Real world Hacking

Immersive Learning

- 70% Practicals
- 30% Theoritical
- Live Hacking - Demonstrations

- Expert Led Training
- Real World Penetration Testers

Job Opportunities in Reality

Penetration Tester	₹18k to 34k/month Excl : cuttings
Ethical Hacker	₹22k to 38k/month Excl : cuttings
SOC Analyst	₹ 20k to 36k/month Excl : cuttings

NOTE : Internship opportunities are free or 5k to 10k Stipend

About Us

CyberSaviours: Your Trusted Training Partner

Vision

• Transforming cybersecurity landscape

• Empowering organizations globally

• Creating resilient digital ecosystems

Mission

To provide exceptional cybersecurity, digital forensics, and governance solutions that protect businesses and strengthen their resilience.

- Integrity
- Excellence
- Innovation
- Client Centric Appraoch

Leadership

Obulesh
Ceo

MAnohar
Cto

Janani
coo

CONTACT US

Your Security- Our Responsibility

+919663081956

www.cybersaviours.com

info@cybersaviours.com

Bengaluru,Karnataka,India