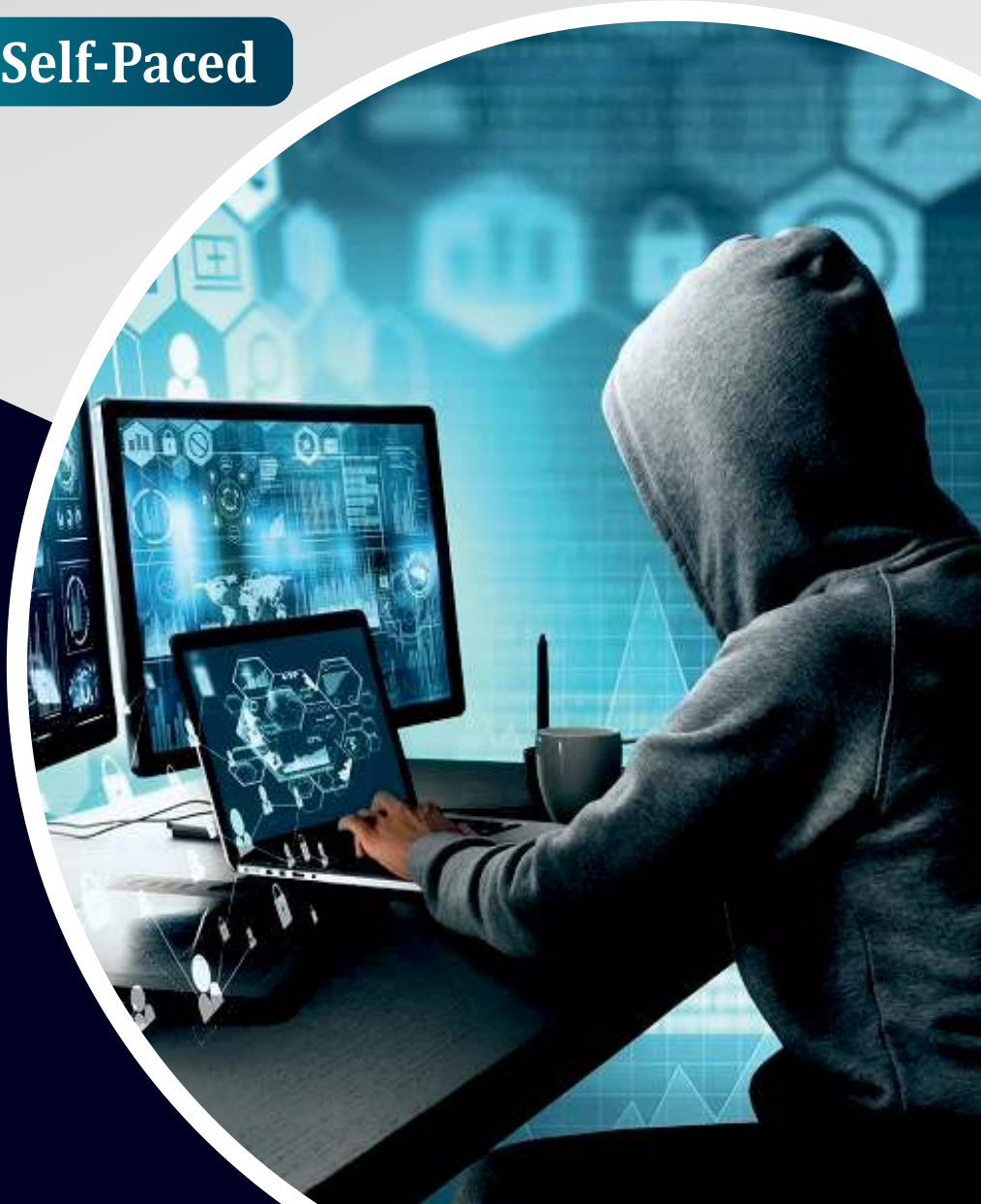
AISECT LEARN
Better Education. Better Careers.

Certified Ethical Hacking (CEH)

Live Lectures + Self-Paced



COURSE OVERVIEW

This Certified Ethical Hacking (CEH) course will enable you to master advanced network security skills. Through online training, you will gain expertise in network packet analysis and penetration testing, allowing you to effectively protect your network from potential hacking threats.

COURSE OBJECTIVE

This course will help learners develop a deeper understanding of modern information and system protection technology and methods. Skills you will learn Upon its completion, you'll be well-versed in cybersecurity fundamentals, enterprise architecture, and components, information system governance and risk assessment, and incident management.

WHAT YOU WILL LEARN

Upon its completion, you'll be well-versed in cybersecurity fundamentals, enterprise architecture, and components, information system governance and risk assessment and incident management.

COURSE SKILL SET

- "Cybersecurity fundamentals, Threat actors' attacks, Mitigation
- Security policies amp procedures,
- Secure architecture,
- Wireless networks,
- Network security controls,
- BYOD security testing,
- IS governance,
- Risk management,
- Incident management,
- Business continuity Disaster recovery"
- Instructor- Ajay Gautam | Cyber Security Expert
- Duration- 3 Months
- Eligibility- Any graduate with a Science Stream
- No. of Modules – 20 Modules
- Language - English
- Shareable certificate- Yes

PROGRAM SYLLABUS

Introduction to Cybersecurity

- Introduction
- Why Cyber Security is Important?
- Role of cyber security engineer
- CIA Triad The Hacking Methodology
- The WhoIS Query
- Social Engineering
- Brute Force Attacks
- Phishing
- Bots and Botnets
- DoS and DDoS
- Pings
- Man, in the Middle Attacks (MITM)

Cyber Security Building Blocks

- Malicious Codes and Terminologies
- Cybersecurity Breaches
- Penetration Testing and Methodologies
- Frameworks and Standards for Cybersecurity
- Hardware and Software Elements of Computer Systems
- Introduction to Networks and Reference Models
- OSI layers
- Network Protocol
- IP Address and Subnet Classes
- Network Devices

Security Basics

- Attacks & Threats
- Architecture & Design
- Implementation Operations & Incident Response
- Governance, Risk & Compliance

Python Scripting

- Introduction to Python
- Python execution and installation
- Identifiers, variables and Datatypes
- Operators
- Python-Flow Controls
- Functions
- Python Classes
- Inheritance, Files
- Python - File Handling, API programming
- Python - Important Modules
- Project 1 - Port Scanner
- Project 2 - Keylogger

Firewalls

- Firewalls – Host-based, network-based, and virtual
- Windows – Host-Based Firewalls - Windows Firewall

Application Security

- Introduction to Application Security
- Need for Application Security
- Why Application becomes vulnerable to Attacks
- The Three W's in Application Security (Why, When, What)
- SQL Injection Attacks
- Exercise for SQL Injection
- SQL Injection Hands-on
- Command Line Injection Hands-on
- Cross-Site Scripting (XSS) Attacks
- Brute Force using DVWA Hands-on
- Introduction to Android Application Testing
- Android Penetration Testing lab
- OWASP Mobile Top 10 Security

Blue Teaming & Cyber SOC

- Incident Management Process
- System Logs

Attacks, Threats and Vulnerabilities

- Compare and Contrast Information Security Roles
- Compare and Contrast Security Control and Framework Types
- Type of Threat Actors and Attack vectors
- Threat Intelligent Sources
- Assess Organizational Security with Network Reconnaissance Tools
- Security Concerns with General Vulnerability Types
- Vulnerability Scanning Techniques
- Penetration Testing Concepts
- Classify Contrast Social Engineering Techniques
- Indicators of Malware-Based Attacks

Cryptography

- Introduction to Cryptography
- Encryption Introduction
- Types of Encryption
- Practical Symmetric Encryption
- Asymmetric Encryption
- Hashing & Hashing Algorithms
- Cryptographic Protocols
- Public Key Infrastructure

Web Application Pen Testing

- Introduction to Web Applications
- Owasp Top 10
- Burpsuite Lab Setup
- DVWA Lab Setup
- Exploiting Injection Vulnerabilities
- SQL injection In-depth
- SQL injection with SQL map

Reconnaissance & Network Scanning

- Understanding Methodology
- Reconnaissance - Passive Methods
- Reconnaissance - Active Methods
- Introduction to Scanning & Scan Types
- Introduction To Nmap
- Port Scan & Syn Scan
- Tcp & UDP Scan
- Version Detection in NMAP
- OS detection in NMAP
- Nmap Scripting Engine
- Banner grabbing with Net cat
- Opensource recon with Malte go

Network Security

- ARP poisoning
- ARP Poisoning with AR spoof & Ettercap
- ARP Poisoning with Berrtercap
- Session Hijacking
- Introduction to DOS & DDOS Attacks

Malware Analysis

- Introduction to Malware
- Virus, Worms, Trojans
- Practical - Trojans in Action
- Adware and Spyware

Computer Forensics

- Computer Forensics investigation process
- Data Acquisition & Duplication
- Introduction to Windows Forensics
- Lab: Capturing Windows Memory
- Browser Forensics using Encase
- Lab: Web Historian
- Memory Forensics
- Lab: Analysing USB data
- Lab: Analysing Malware using Volatility
- Introduction to Indian Cyber Law

Virtual Private Network (VPN)

- Introduction
- Why VPN, Analogy, and tunnelling
- Bypassing Firewall Using VPN
- Which VPN protocol is best to use and why?
- VPN Weaknesses
- Setting up an OpenVPN client on Linux
- Choosing the right VPN provider

Wireless and Wi-Fi Security

- Wireless and Wi-Fi security- Introduction
- Wi-Fi Weaknesses - WEP, WPA, WPA2, TKIP, and CCMP
- Wi-Fi Weaknesses - Wi-Fi Protected Setup WPS, Evil Twin, and Rouge AP
- Wi-Fi Security Testing
- Wireless Security - Secure Configuration and Network Isolation
- Wireless security - RF Isolation and Reduction
- Wireless security - Who is on my Wi-Fi Network?

Testing Environment Using Virtual Machines

- Introduction to Setting up a Testing Environment Using Virtual Machines
- Vmware
- Creating virtual machines - [VirtualBox options]
- Ubuntu Linux - [Virtual system installation]
- Cloning virtual machines
- The basic configuration of a virtual satellite and its system - [VMs Snapshots]

- Virtual satellite network - [Ubuntu Linux network configuration]
- Basic firewall network configuration - [preparation for NAT]
- IP FORWARD and NAT - [iptables: MASQUERADE, POSTROUTING, save rules & restore]
- Telnet server setup - [2 rules from Troski behind us, Putty, Windows client]
- Kali Linux 2022

Security Incident Management

- Security Incident Management
- Incident Response Plan
- Incident Management Concepts and Practices
- Integration with DR and BCP
- Recovery Terms
- Incident Classification Methods
- Damage Containment
- Re-plan
- Roles and Responsibilities
- Incident Response Tools and Equipments
- Reliability of Evidence
- Validation of Evidence
- Incident Response Reporting and Procedures
- Root Cause Analysis
- Business Impact Analysis
- Detecting and Analyzing Security Events

Job Roles

- Analyst Analyst
- Application Security
- Engineer Trainee
- Penetration Tester
- Security Analyst
- Ethical Hacker

AISECT LEARN

Better Education. Better Careers.

Sign up for

Webinars, Free courses and Paid Courses

starting from ₹**499/-** onwards only

Contact Us

9111177800 | learn@aisectlearn.com | https://courses.aisectlearn.com