# Ethical Hacking Essentials

**Course Duration: 16 Hrs.** **Course code: EHE**

## Course Overview

The Ethical Hacking Essentials (EHE) course is an introductory cybersecurity course that provides foundational knowledge and skills in ethical hacking and penetration testing, preparing learners for a career in cybersecurity. It covers concepts like threats, vulnerabilities, password cracking, web application attacks, and more, with hands-on labs and practical experience.

## What you'll learn?

- **Fundamentals of Information Security and Ethical Hacking:**
  Learn the basics of cybersecurity, ethical hacking methodologies, and the importance of protecting systems and data.
- **Threats and Vulnerabilities:**
  Understand common cybersecurity threats, vulnerabilities in systems and networks, and how to identify and mitigate them.
- **Malware and Vulnerability Assessments:**
  Learn about different types of malwares, their characteristics, and how to conduct vulnerability assessments.

## Target Audience

- **Cybersecurity Professionals:**
  This course is ideal for those who want to enter the cybersecurity field, including students, fresh graduates, and career switchers.



**Phone:** +91-999-911-1686 **Mail Us:** info@ssdntech.com

- **IT Professionals:**
  IT professionals looking to enhance their cybersecurity knowledge and skills, including network and system administrators, security analysts, and those responsible for data security.
- **Security Enthusiasts:**
  Individuals interested in learning about ethical hacking and cybersecurity fundamentals, including those with a general interest in technology and security.
- **Students:**
  Students in computer science, IT, or related fields who want to specialize in cybersecurity or gain a foundational understanding of ethical hacking.

## Pre-Requisites

- **Basic Computer Skills:**
  Familiarity with operating systems, file management, and general computer usage is essential.
- **Networking Fundamentals:**
  Understanding of network protocols, TCP/IP, IP addresses, and basic network concepts is crucial.
- **Cybersecurity Basics:**
  A foundational understanding of security concepts like threats, vulnerabilities, and security controls is helpful.
- **Programming Knowledge (Optional but Recommended):**
  While not always mandatory, some courses benefit from basic programming knowledge, especially in languages like Python.


**Phone:** +91-999-911-1686 **Mail Us:** info@ssdntech.com

## Course content

**Module 01: Information Security Fundamentals**

A. Information Security Fundamentals
B. Information Security Laws and Regulations

**Module 02: Ethical Hacking Fundamentals**

A. Cyber Kill Chain Methodology
B. Hacking Concepts and Hacker Classes
C. Different Phases of Hacking Cycle
D. Ethical Hacking Concepts, Scope, and Limitations
E. Ethical Hacking Tools

**Module 03: Information Security Threats and Vulnerability Assessment**

A. Threat and Threat Sources
B. Malware and its Types
C. Malware Countermeasures
D. Vulnerabilities
E. Vulnerability Assessment

**Module 04: Password Cracking Techniques and Countermeasures**

A. Password Cracking Techniques
B. Password Cracking Tools
C. Password Cracking Countermeasures

**Module 05: Social Engineering Techniques and Countermeasures**

A. Social Engineering Concepts and its Phases
B. Social Engineering Techniques
C. Insider Threats and Identity Theft
D. Social Engineering Countermeasures



**Phone:** +91-999-911-1686 **Mail Us:** info@ssdntech.com

**Module 06: Network Level Attacks and Countermeasures**

A. Packet Sniffing Concepts
B. Sniffing Techniques
C. Sniffing Countermeasures
D. DoS and DDoS Attacks
E. DoS and DDoS Attack Countermeasures
F. Session Hijacking Attacks
G. Session Hijacking Attack Countermeasures

**Module 07: Web Application Attacks and Countermeasures**

A. Web Server Attacks
B. Web Server Attack Countermeasures
C. Web Application Architecture and Vulnerability Stack
D. Web Application Threats and Attacks
E. Web Application Attack Countermeasures
F. SQL Injection Attacks
G. SQL Injection Attack Countermeasures

**Module 08: Wireless Attacks and Countermeasures**

A. Wireless Terminology
B. Wireless Encryption
C. Wireless Network-Specific Attack Techniques
D. Bluetooth Attacks
E. Wireless Attack Countermeasures

**Module 09: Mobile Attacks and Countermeasures**

A. Mobile Attack Anatomy
B. Mobile Platform Attack Vectors and Vulnerabilities
C. Mobile Device Management (MDM) Concept
D. Mobile Attack Countermeasures


**Phone:** +91-999-911-1686 **Mail Us:** info@ssdntech.com

**Module 10: IoT and OT Attacks and Countermeasures**

A. IoT Concepts
B. IoT Threats and Attacks
C. IoT Attack Countermeasures
D. OT Concepts
E. OT Threats and Attacks
F. OT Attack Countermeasures

**Module 11: Cloud Computing Threats and Countermeasures**

A. Cloud Computing Concepts
B. Container Technology
C. Cloud Computing Threats
D. Cloud Attack Countermeasures

**Module 12: Penetration Testing Fundamentals**

A. Fundamentals of Penetration Testing and its Benefits
B. Strategies and Phases of Penetration Testing
C. Guidelines and Recommendations for Penetration Testing

## Exam Preference

| | |
|---|---|
| Exam Code | 112-52 |
| Number Of Questions | 75 |
| Length Of Test | 120 Minutes |
| Test Format | MCQ. |


**Phone:** +91-999-911-1686 **Mail Us:** info@ssdntech.com