
ed-watch
Your online resource partner
New User ? Sign Up
Sign In
Login to LMS
LEARNING MANAGEMENT SYSTEM
Welcome to Ed-Watch
your online resource partner
- TECHNICAL TRAINING
- MENTAL STRENGTH PROGRAMS
- BUSINESS & ECONOMIC FORUM
ETHICAL HACKING

ed-watch
Your online resource partner

# Program Overview

This comprehensive program provides complete knowledge and skills in the field of ethical hacking. Discover the fascinating world of cybersecurity as you learn how to assess and secure computer systems, networks, and applications. Through hands-on exercises and real-world scenarios, you will gain practical experience in identifying vulnerabilities, performing penetration testing, and implementing effective security measures. Whether you are an aspiring cybersecurity professional or an IT enthusiast, this program will equip you with the tools and techniques needed to become an ethical hacker. Start your journey today and unlock the secrets of cybersecurity.

The course comprises 21 modules with multiple assignments and quiz at end of each module. After successfully completing the course, you will have strong grip over different hacking methods and techniques.

This program comprises:

- Project: System Hacking Project based on CTF
- Multiple Labs
- Final Course Assignment

ed-watch
Your online resource partner

## LEARNING MODULES:

- Module A – Introduction to Ethical Hacking

  Lesson 1: Fundamentals of ethical hacking
  Lesson 2: Types of hackers
  Lesson 3: Types of hacking
  Lesson 4: Cyber Kill Chain
  Lesson 5: Lab Setup for ethical hacking

- Module B – Foot printing & Reconnaissance

  Lesson 1: What is Foot printing?
  Lesson 2: Types of foot printing
  Lesson 3: Search engine & google hacking
  Lesson 4: Website Foot printing
  Lesson 5: WHOIS foot printing
  Lesson 6: DNS Foot printing
  Lesson 7: Email Foot printing
  Lesson 8: How to protect yourself from foot printing?
  Lesson 9: Hands on Lab

- Module C – Scanning networks

  Lesson 1: What is network scanning?
  Lesson 2: Introduction to Nmap and Zenmap
  Lesson 3: Port knocking & service discovery.

## LEARNING MODULES:…cont.1

Lesson 4: OS fingerprinting
Lesson 5: Scanning beyond IDS
Lesson 6: Understanding Network structure using Zenmap
Lesson 7: Hands on Lab

- Module D – Enumeration
  Lesson 1: What is enumeration?
  Lesson 2: SMTP and DNS Enumeration
  Lesson 3: SMB Enumeration
  Lesson 4: LDAP enumeration
  Lesson 5: Hands on Lab
  Lesson 6: Anti-Enumeration techniques

- Module E – Vulnerability Analysis
  Lesson 1: What is vulnerability analysis
  Lesson 2: Vulnerability analysis tools
  Lesson 3: Vulnerability scanning using mobile
  Lesson 4: Generating report

- Module F – System Hacking
  Lesson 1: What is system hacking?
  Lesson 2: Initial access
  Lesson 3: Execution
  Lesson 4: Defense evasion

ed-watch
Your online resource partner

## LEARNING MODULES:…cont. 2

Lesson 5: Escalate privilege
Lesson 6: Password cracking
Lesson 7: Deleting logs
Lesson 8: Hands on lab using Metasploit

- Module G – Malware Threats

Lesson 1: What is malware?
Lesson 2: Trojans
Lesson 3: Virus and worms
Lesson 4: Advanced persistent threats
Lesson 5: In-Memory (Fileless) Threats
Lesson 6: Static and dynamic analysis of malwares
Lesson 7: Anti-malware software
Lesson 8: Lab

- Module H – Sniffing

Lesson 1: What is sniffing?
Lesson 2: Sniffing tools
Lesson 3: DHCP attacks
Lesson 4: ARP poisoning
Lesson 5: Spoofing attacks
Lesson 6: DNS poisoning
Lesson 7: Lab

## LEARNING MODULES:…cont. 3

Lesson 8: How to protect from sniffing?

- Module I – Social engineering & password harvesting

Lesson 1: What is social engineering?
Lesson 2: Types of social engineering
Lesson 3: Different techniques used in social engineering
Lesson 4: What is website cloning & password harvesting?
Lesson 5: How to protect from social engineering attacks?
Lesson 6: Lab

- Module J – Denial of Service

Lesson 1: What is DOS?
Lesson 2: Methods and techniques used for DOS
Lesson 3: Available tools
Lesson 4: Case study
Lesson 5: Lab
Lesson 6: How to protect from DOS

- Module K – Session Hijacking

Lesson 1: What is session hijacking?

ed-watch
Your online resource partner

## LEARNING MODULES:…cont. 4

Lesson 2: App level session hijacking
Lesson 3: Network level
Lesson 4: Available tools
Lesson 5: How to protect from session hijacking?

- Module L – Evading IDS, firewalls & honeypots

  Lesson 1: What is evading?
  Lesson 2: How it works?
  Lesson 3: Available tools
  Lesson 4: Bypassing IDS
  Lesson 5: Bypassing firewall
  Lesson 6: What is honeypot and how to detect honeypots

- Module M – Hacking webservers
  Lesson 1: What is web server hacking?
  Lesson 2: Web server attacks & methods
  Lesson 3: Available tools
  Lesson 4: Lab (webserver hacking demo)
  Lesson 5: How to secure web servers?

- Module N – Hacking web applications
  Lesson 1: What is web app hacking?

## LEARNING MODULES:…cont. 5

Lesson 2: Methods & techniques of web app hacking
Lesson 3: Web API, hooks and web shells
Lesson 4: How to secure web application?

- Module O – SQL Injection
  Lesson 1: What is SQL Injection & types of it?
  Lesson 2: Tools used for SQL injection.
  Lesson 3: Methodology for SQL injection
  Lesson 4: LAB (Demonstration)
  Lesson 5: How to protect from SQL injection?

- Module P – Hacking wireless networks
  Lesson 1: Fundamentals of wireless hacking
  Lesson 2: Wireless threats
  Lesson 3: Tool used for wireless hacking
  Lesson 4: WIFI hacking methodology
  Lesson 5: How to secure wireless networks?

- Module Q – Building malware
  Lesson 1: What is Malware?
  Lesson 2: Tools required
  Lesson 3: Customizing process injection
  Lesson 4: Compiling your first malware
  Lesson 5: Lab

ed-watch
Your online resource partner

## LEARNING MODULES:…cont. 6

- Module R – Antivirus evasion

  Lesson 1: What is antivirus evasion?
  Lesson 2: Approach for customizing Remote Access Trojan for evasion
  Lesson 3: Encryption
  Lesson 4: Packing Trojan & available tools
- Module S – APT attacks & TTPs
  Lesson 1: Introduction to APT's and MITRE ATT&CK Framework
  Lesson 2: How APT works
  Lesson 3: Getting Started with MITRE ATT&CK
- Module T – Cryptography
  Lesson 1: Fundamental s of cryptography
  Lesson 2: Encryption Algorithms
  Lesson 3: Available tools
  Lesson 4: Disk Encryption
  Lesson 5: Cryptanalysis
- Module U – Responsibilities as Ethical hacker
  Lesson 1: Your ethical responsibility in society as an ethical hacker
- Project: System Hacking Project based on CTF - Lab
- Final Course Assignment

**PARTICIPANTS:**

- IT professionals
- Security Analysts/ penetration testers
- Auditors & compliance professionals

**DELIVERY:**

- E-Learning – Self-paced
- Course duration: 25 Hours
- Virtual Classes 1 hour once a month
- 24/7 Support
- 60% passing criterion
- Quizzes & Assignments

**PAYMENT:**

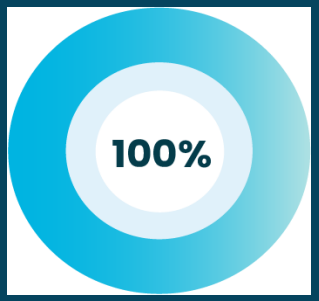
- US$ 1,100 Pay now
- Group discounts & installments available (contact@ed-watch.org)

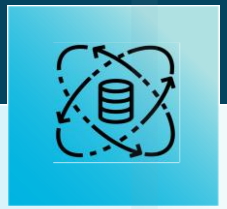
Scan to pay

ed-watch
Your online resource partner

# Training Programs by Ed-Watch

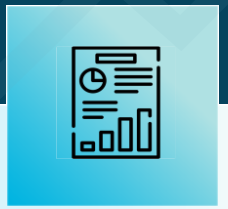
EXPERT



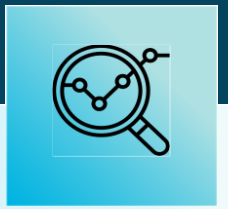
DATA LITERACY

DATA SECURITY



FINANCE & ESG REPORTING

TECHNOLOGY & AUTOMATION



ADVANCE ANALYTICS

BEGINNER

# REACH OUT TO US

ed-watch
Your online resource partn

**Sales & admin support**

jane@ed-watch.org contact@ed-watch.org

**USA OFFICE**

+1 (903)-424-6912
Ed-Watch LLC, 20 Hallo Street, Edison NJ 08837, USA

**UAE OFFICE**

+971 5 0565 3520
Smart Links Business Management Services; Office P3, Empire Heights Business Bay, Dubai, UAE