EHE – Ethical Hacking Essentials (e-Learning)

EC-Council

Com certificação

- **Nível:**
- **Duração:** 15h

Sobre o curso

Spring Deals: Cursos EC-Council com 5% de desconto até 30 de abril

Ethical Hacking Essentials is an Introductory cybersecurity course that covers ethical hacking and penetration testing fundamentals. It offers hands-on experience in computer and network security concepts such as threats, vulnerabilities, password cracking, web applications, and more. No IT/Cybersecurity experience required for this course.

Test your skills with CTF-based Capstone Project and validate these newly acquired skills in proctored exams. With 15 hours of premium learning, 11 labs, and 12 modules, the EHE provides a solid foundation and formal recognition to boost your resume and open doors for better opportunities.

Key Features:

- 15+ hours of premium self-paced video training
- 11 lab activities in a simulated lab environment
- 750+ pages of ecourseware
- Capstone Project
- Year-long access to courseware and labs
- Proctored exam voucher with 1-year validity
- Increase your value in the job market to advance your career
- Get globally recognized certification by the EC-Council

What Skills You'll Learn

- Key issues plaguing the information security world and information security laws and standards.
- Fundamentals of ethical hacking
- Information security threats and vulnerabilities
- Different types of malware
- Different types of password-cracking techniques and countermeasures

- Social engineering techniques, insider threats, identity theft, and countermeasures
- Network level attacks (sniffing, denial-of-service, and session hijacking) and countermeasures
- Application-level attacks (web-server attacks, web application attacks, and SQL injection) and countermeasures
- Wireless encryption, wireless threats, and countermeasures
- Mobile platform attack vector, mobile device management, mobile security guidelines, and security tools
- IoT and OT concepts, attacks, and countermeasures
- Cloud computing technologies, cloud computing threats, attacks, and security techniques
- Fundamentals of pen testing

Destinatários

Who is E|HE for?

- High School/ College/University students
- Teams and organizations
- Career Starters
- Working Professionals

Pré-requisitos

No prior cybersecurity knowledge or IT work experience required.

Metodologia

Exam Details:

- Exam Code: 112-52
- Number of Questions:
- Duration: 2 hours
- Test Format: Multiple Choice

Programa

- Information Security Fundamentals
- Ethical Hacking Fundamentals
- Information Security Threats and Vulnerability Assessment
- Password Cracking Techniques and Countermeasures
- Social Engineering Techniques and Countermeasures

- Network Level Attacks and Countermeasures
- Web Application Attacks and Countermeasures
- Wireless Attacks and Countermeasures
- Mobile Attacks and Countermeasures
- IoT and OT Attacks and Countermeasures
- Cloud Computing Threats and Countermeasures
- Penetration Testing Fundamentals

Information Security Fundamentals

- Information Security Fundamentals
- Information Security Laws and Regulations

Ethical Hacking Fundamentals

- Cyber Kill Chain Methodology
- Hacking Concepts and Hacker Classes
- Different Phases of Hacking Cycle
- Ethical Hacking Concepts, Scope, and Limitations
- Ethical Hacking Tools

Lab Exercise:

- Passive Footprinting to Gather Information About a Target
- Network Scanning to Identify Live Hosts, Open Ports and Services and Target OS in the Network
- Enumeration on a System or Network to Extract Usernames, Machine Names, Network Resources, Shares, etc

Information Security Threats and Vulnerability Assessment

- Threat and Threat Sources
- Malware and its Types
- Malware Countermeasures
- Vulnerabilities
- Vulnerability Assessment

Lab Exercise:

- Vulnerability Assessment to Identify Security Vulnerabilities in the Target System or Network

Password Cracking Techniques and Countermeasures

- Password Cracking Techniques
- Password Cracking Tools
- Password Cracking Countermeasures

Lab Exercise:

- Perform Active Online Attack to Crack the System’s Password
- Audit System Passwords

Social Engineering Techniques and Countermeasures

- Social Engineering Concepts and its Phases
- Social Engineering Techniques
- Insider Threats and Identity Theft
- Social Engineering Countermeasures

Lab Exercise:

- Social Engineering using Various Techniques to Sniff Users’ Credentials
- Detect a Phishing Attack

Network Level Attacks and Countermeasures

- Packet Sniffing Concepts
- Sniffing Techniques
- Sniffing Countermeasures
- DoS and DDoS Attacks
- DoS and DDoS Attack Countermeasures
- Session Hijacking Attacks
- Session Hijacking Attack Countermeasures

Lab Exercise:

- Perform MAC Flooding to Compromise the Security of Network Switches
- Perform ARP Poisoning to Divert all Communication between Two Machines
- Detect ARP Attacks using ARP Spoofing Detection Tools to Ensure Data Privacy
- Perform DoS and DDoS Attacks using Various Techniques on a Target Host to Prevents Access to System Resources for Legitimate Users
- Detect and Protect Against DDoS Attack
- Perform Session Hijacking to Seize Control of a Valid TCP Communication Session Between Two Computers
- Detect Session Hijacking Attempts using Manual Method

Web Application Attacks and Countermeasures

- Web Server Attacks
- Web Server Attack Countermeasures
- Web Application Architecture and Vulnerability Stack
- Web Application Threats and Attacks
- Web Application Attack Countermeasures
- SQL Injection Attacks
- SQL Injection Attack Countermeasures

Lab Exercise:

- Perform a Web Server Attack to Crack FTP Credentials
- Perform a Web Application Attack to Compromise the Security of Web Applications to Steal Sensitive Information
- Perform SQL Injection Attacks on a Target Web Application to Manipulate the Backend Database
- Detect SQL Injection Vulnerabilities using SQL Injection Detection Tools

Wireless Attacks and Countermeasures

- Wireless Terminology
- Wireless Encryption
- Wireless Network-Specific Attack Techniques
- Bluetooth Attacks
- Wireless Attack Countermeasures

Lab Exercise:

- Perform Wi-Fi Packet Analysis
- Perform Wireless Attacks to Crack Wireless Encryption

Mobile Attacks and Countermeasures

- Mobile Attack Anatomy
- Mobile Platform Attack Vectors and Vulnerabilities
- Mobile Device Management (MDM) Concept
- Mobile Attack Countermeasures

Lab Exercise:

- Hack an Android Device by Creating Binary Payloads
- Secure Android Devices using Various Android Security Tools

IoT and OT Attacks and Countermeasures

- IoT Concepts
- IoT Threats and Attacks
- IoT Attack Countermeasures
- OT Concepts
- OT Threats and Attacks
- OT Attack Countermeasures

Lab Exercise:

- Perform Footprinting using Various Footprinting Techniques
- Capture and Analyze IoT Device Traf

Cloud Computing Threats and Countermeasures

- Cloud Computing Concepts
- Container Technology
- Cloud Computing Threats
- Cloud Attack Countermeasures

Lab Exercise:

- Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools
- Exploit S3 Buckets

Penetration Testing Fundamentals

- Fundamentals of Penetration Testing and its Benefits
- Strategies and Phases of Penetration Testing
- Guidelines and Recommendations for Penetration Testing