EC-Council
Building A Culture Of Security

E|HE
Ethical Hacking Essentials

Ethical Hacking Essentials

Begin Your Cybersecurity Journey with Hands-On, Technical Foundational Skills in Ethical Hacking

No IT / Cybersecurity Experience Required

Video Lessons • Hands-on Labs • CTF Challenges • Proctored Exam

EC-COUNCIL ESSENTIALS SERIES

In response to the growing talent gap and the lack of skilled cybersecurity professionals, EC-Council, the inventor of the industry-leading Certified Ethical Hacker (C|EH) has launched the Essentials Series. It offers multi-domain, hands-on technical training to equip learners for entry-level cybersecurity positions. The aim is to create a robust workforce that is ready to step into entry-level cybersecurity roles, including systems analysts, cybersecurity analysts, incident analysts, and more, through instructor-led learning without compromising on affordability.

EC-Council's Essential Series is a hands-on, immersive program focused on **eight cybersecurity domains** - Ethical hacking, Network Defense, Digital Forensics, Cloud Security, IoT Security, SOC, Threat Intelligence, and DevSecOps. Designed for high school students, recent graduates, career switchers, beginners, and IT/Technology teams with minimum or no prior experience in IT/Cybersecurity, the Essentials Series empowers learners to choose their areas of specialization across essential domains.

Take the First Step Toward Your Cybersecurity Career Now!

What is EC-Council Ethical Hacking Essentials?

Ethical Hacking Essentials is an introductory cybersecurity course that covers ethical hacking and penetration testing fundamentals and prepares learners for a career in cybersecurity. This ethical hacking course will introduce learners to computer and network security concepts such as threats and vulnerabilities, password cracking, web application attacks, IoT and OT attacks, cloud computing, pentesting fundamentals, and more. EC-Council's ethical hacking essentials course provides hands-on practical experience to learners, thus giving them the skills necessary for a future in cybersecurity. Put your newly acquired abilities to the test with an exhilarating Capture the Flag (CTF) Exercise seamlessly integrated in our Capstone project. This CTF is seamlessly integrated by live virtual machines, genuine software, and real networks, all delivered within a secure and regulated sandbox environment. With these exclusive hands-on, human-versus-machine CTF challenges you will develop the hands-on proficiencies essential for success in your cyber professional role.

E|HE-certified learners have an assured means of formal recognition to add to their resumes and show off their expertise and skills to prospective employers. This improves their prospects for employment advancement, higher salaries, and greater job satisfaction.

If you are looking to learn advance ethical hacking click here: Ethical Hacking Certification (Certified Ethical Hacker **C|EH**)

Ethical Hacking Essentials Program Information

Course Outline

Module 01: Information Security Fundamentals

- Information Security Fundamentals
- Information Security Laws and Regulations

Module 02: 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.

Module 03: 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

Module 04: 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

Module 05: 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

Module 06: 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

Module 06: 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

Module 07: 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

Module 08: 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

Module 09: 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

Module 10: 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 Traffic

Module 11: 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

Module 12: Penetration Testing Fundamentals

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

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

Who Is It For

- School students, fresh graduates, Professionals, Career starters and switchers, IT / Technology / Cybersecurity teams with little or no work experience.
- Anyone who wants to start their cybersecurity career and master the fundamentals of security online.
- Anyone who wants to prepare for a cybersecurity career and aid their IT education.
- Professionals who want to get into the cybersecurity field but are unsure where to start their education journey.

Training and Exam

Training Details: Self-paced, in-demand lecture videos led by world-class instructors and hands-on labs.
Pre-requisite: No prior cybersecurity knowledge or IT work experience required.

Exam Details:

- Exam Code: 112-52
- Number of Questions: 75
- Duration: 2 hours
- Test Format: Multiple Choice
- 750+ pages of ecourseware

Key Features

- 15+ hours of premium self-paced video training
- 11 lab activities in a simulated lab environment
- 750+ pages of ecourseware
- Capstone Projects with Real-World CTF Challenges
- Year-long access to courseware and 6-month access to labs
- Proctored exam voucher with one-year validity
- Increase your value in the job market to advance your career.
- Get globally recognized certification by EC-Council.

Why EC-Council's Essentials Series is the Most Popular and Fastest Growing Beginner Level Training Program for Career Starters and Career Changers

213,000+ Learners Trust EC-Council's Essentials Series

150+ Countries

85+ Million Minutes Watched

4.95/5.0 Average Ratings

96.46% of Learners Gave a 5* Rating

Why Do Professionals, Students, Career Starters and Changers Worldwide Choose the EC-Council's Essentials Certification?

Gene (USA)

Strong Cybersecurity Foundation.

★★★★★

It has given me a solid foundation in the basics of cybersecurity. I now have a better understanding of the different types of cyberattacks, the tools and techniques that attackers use, and the ways to protect myself and my organization from these attacks.

Taylor Cooper (USA)

Career Advancement through Ethical Hacking.

★★★★★

This has helped me enhance my knowledge and skills in tech. I will be able to showcase my knowledge by certifying myself as an ethical hacker and adding it to my resume, which will give me an opportunity to advance in my career and opt for higher-paying roles.

Deeptankshu (USA)

Top Notched Cyber Investigation Skills.

★★★★★

It helped by teaching me how to collect data and evidence to solve crimes and prevent wrongdoers in the Cyber realm. As a Security and Intelligence major, I want to be well-versed in the Cyber realm as well as other realms.

Samuel Tetteh (USA)

Strong Foundation for Digital Forensics

★★★★★

After completing this course, I had the foundation I needed. It assisted me in completing my MS Cybersecurity course in digital forensics, which expanded my knowledge even further. This foundation is perfect for a start in Digital forensics.

Brian (USA)

Rebuilding Network Defense Knowledge.

★★★★★

This course helped rebuild my baseline knowledge of network defense, which I required before progressing toward more advanced studies in the field.

Nicolas Ntibaziyaremye (USA)
Practical Learning for Career Growth.
★★★★★

The course is project-based. This allows me to apply what I learn in the lectures to real-world problems. I have learned a lot from this course, and I am confident that it will help me in my career.

Learn Foundational Cybersecurity Skills with EC-Council's 8 Essential Series

E|HE
Ethical Hacking
Essentials

N|DE
Network Defense
Essentials

D|SE
DevSecOps
Essentials

I|SE
IoT Security
Essentials

D|FE
Digital Forensic
Essentials

C|SE
Cloud Security
Essentials

S|CE
SOC
Essentials

T|IE
Threat Intelligence
Essentials

About EC-Council

EC-Council's sole purpose is to build and refine the cybersecurity profession globally. We help individuals, organizations, educators, and governments address global workforce problems by developing and curating world-class cybersecurity education programs and their corresponding certifications. We also provide cybersecurity services to some of the largest businesses globally. Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the Department of Defence, Intelligence Community, NATO, and over 2,000 of the best Universities, Colleges, and Training Companies, our programs have proliferated through over 140 countries. They have set the bar in cybersecurity education. Best known for the Certified Ethical Hacker programs, we are dedicated to equipping over 2,30,000 information age soldiers with the knowledge, skills, and abilities required to fight and win against the black hat adversaries. EC-Council builds individual and team/organization cyber capabilities through the Certified Ethical Hacker Program, followed by a variety of other cyber programs, including Certified Secure Computer User, Computer Hacking Forensic Investigator, Certified Security Analyst, Certified Network Defender, Certified SOC Analyst, Certified Threat Intelligence Analyst, Certified Incident Handler, as well as the Certified Chief Information Security Officer.

We are an ANAB 17024 accredited organization and have earned recognition by the DoD under Directive 8140/8570 in the UK by the GCHQ, CREST, and various other authoritative bodies that influence the entire profession.

Founded in 2001, EC-Council employs over 400 individuals worldwide with ten global offices in the USA, UK, Malaysia, Singapore, India, and Indonesia. Its US offices are in Albuquerque, NM, and Tampa, FL.

Learn more at www.eccouncil.org

E | HE

Ethical | Hacking Essentials

Ethical Hacking Essentials

www.eccouncil.org