EC-Council

Building A Culture Of Security

N|D|E

Network Defense Essentials

Network Defense Essentials

Begin Your Cybersecurity Journey with Hands-On, Technical Foundational Skills in Network Security

No IT / Cybersecurity Experience Required

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

EC-COUNCIL ESSENTIALS SERIES

Cybersecurity is very complex and broad; it has many areas of specialty. And sometimes, determining your area of specialization and developing essential foundational skills becomes a significant challenge.

Essential series is a hands-on, immersive program to help learners gain solid technical foundational skills in various cybersecurity areas while ensuring the program is highly affordable. Designed and created to develop a new breed of technically abled professionals right at the start of their cybersecurity careers. Essential Series course methodology is designed for school students, fresh graduates, career switchers, starters, and IT / Technology teams with little or no experience in IT / Cybersecurity. This cybersecurity essentials certification enables students and IT teams to learn the different tenets of cybersecurity, allowing them to determine their area of interest/specialization for themselves, while developing diverse skill set in essential different domains. Gain skills for your first CTF competition with this Essentials Series Course. The final module of lab capstone project features a simulated CTF to test your skills in a controlled environment. Use live virtual machines, real software, and networks to solve real-world challenges as a hacker or defender.

EC-Council Essentials Series covers 8 essential skills like: Ethical hacking, Network defense, Digital Forensics, Cloud security, IoT Security, SOC, threat intelligence and DevSecOps.

What is EC-Council Network Defense Essentials?

Network Defense Essentials covers the fundamental concepts of information security and network defense. This introductory cybersecurity course is designed for today's entry-level information security or cybersecurity career professionals and is ideal for learners aspiring to pursue a career in cybersecurity.

The course gives a holistic overview of the key components of information security, which include identification, authentication, and authorization, virtualization and cloud computing, wireless networks, mobile and IoT devices, and data security. The interactive labs component ensures that learners receive the hands-on, practical experience required for a future in cybersecurity.

N|DE-certified learners have an assured means of formal recognition to add to their resumes and demonstrate their expertise and skills to prospective employers. 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.
The purpose of the N|DE certification is to recognize the competency and expertise of a professional in network defense and information security skills, thereby adding value to their workplace and employer. If you are looking to learn advanced network security skills, click here: Network Security Certification (Certified Network Defender C|ND).

Network Defense Essentials Program Information

Course Outline

Module 01: Network Security Fundamentals

Topics Covered:

- Fundamentals of Network Security
- Network Security Protocols

Module 02: Identification, Authentication and Authorization

Topics Covered:

- Access Control Principles, Terminologies, and Models
- Identity and Access Management (IAM) Concepts

Lab Exercise

- Implementing Access Controls in Windows Machine
- Managing Access Controls in Linux Machine
- Implementing Role-Based Access Control in Windows Admin Center (WAC)

Module 03: Network Security Controls - Administrative Controls

Topics Covered:

- Regulatory Frameworks, Laws, and Acts
- Design and Develop Security Policies
- Conduct Different Types of Security and Awareness Training

Lab Exercise

- Implementing Password Policies Using Windows Group Policy

Module 04: Network Security Controls - Physical Controls

Topics Covered:

- Importance of Physical Security
- Physical Security Controls
- Workplace Security
- Environmental Controls

Module 05: Network Security Controls - Technical Controls

Topics Covered:

- Types of Network Segmentation
- Types of Firewalls and their Role
- Types of IDS/IPS and their Role
- Types of Honeypots
- Types of Proxy Servers and their Benefits
- Fundamentals of VPN and its Importance in Network Security
- Security Incident and Event Management (SIEM)
- User Behavior Analytics (UBA)
- Antivirus/Anti-Malware Software

Lab Exercise

- Implementing Host-Based Firewall Protection with iptables
- Implementing Host-Based Firewall Functionality Using Windows Firewall
- Implementing Network-Based Firewall Functionality: Blocking Unwanted Website Access Using pfSense Firewall
- Implementing Network-Based Firewall Functionality: Blocking Insecure Ports Using pfSense Firewall
- Implementing Host-based IDS functionality Using Wazuh HIDS
- Implementing Network-Based IDS Functionality Using Suricata IDS
- Detect Malicious Network Traffic Using HoneyBOT
- Establishing a Virtual Private Network Connection Using SoftEther VPN

Module 06: Virtualization and Cloud Computing

Topics Covered:

- Virtualization Essential Concepts and OS
- Virtualization Security
- Cloud Computing Fundamentals
- Insights of Cloud Security and Best Practices

Lab Exercise

- Auditing Docker Host Security Using Docker-Bench-Security Tool
- Implementing AWS Identity and Access Management
- Securing Amazon Web Services Storage

Module 07: Wireless Network Security

Topics Covered:

- Wireless Network Fundamentals
- Wireless Network Encryption Mechanisms
- Types of Wireless Network Authentication Methods
- Implement Wireless Network Security Measures

Lab Exercise

- Configuring Security on a Wireless Router

Module 08: Mobile Device Security

Topics Covered:

- Mobile Device Connection Methods
- Mobile Device Management Concepts
- Common Mobile Usage Policies in Enterprises
- Security Risks and Guidelines Associated with Enterprises Mobile Usage Policies
- Implement Enterprise-level Mobile Security Management Solutions
- Implement General Security Guidelines and Best Practices on Mobile Platforms

Lab Exercise

- Implementing Enterprise Mobile Security Using Miradore MDM Solution

---

Module 09: IoT Device Security

Topics Covered:

- IoT Devices, Application Areas, and Communication Models
- Security in IoT-enabled Environments

Lab Exercise

- Securing IoT Device Communication Using TLS/SSL

Module 10: Cryptography and PKI

Topics Covered:

- Cryptographic Techniques
- Cryptographic Algorithms
- Cryptography Tools
- Public Key Infrastructure (PKI)

Lab Exercise

- Calculate One-way Hashes using HashCalc
- Calculate MD5 Hashes using HashMyFiles
- Create a Self-signed Certificate

Module 11: Data Security

Topics Covered:

- Data Security and its Importance
- Security Controls for Data Encryption 8
- Data Backup and Retention
- Data Loss Prevention Concepts

Lab Exercise

- Perform Disk Encryption using VeraCrypt
- File Recovery Using EaseUS Data Recovery Wizard
- Backing Up and Restoring Data in Windows

Module 12: Network Traffic Monitoring

Topics Covered:

- Need and Advantages of Network Traffic Monitoring
- Determine Baseline Traffic Signatures for Normal and Suspicious Network Traffic
- Perform Network Monitoring for Suspicious Traffic

Lab Exercise

- Capturing Network Traffic using Wireshark
- Applying Various Filters in Wireshark
- Analyzing and Examining Various Network Packet Headers in Linux using tcpdump

What Skills You'll Learn

- Key issues plaguing the network security
- Essential network security protocols
- Identification, authentication, and authorization concepts
- Network security controls
  - Administrative controls (Frameworks, laws, acts, and security policies)
  - Physical controls (Physical security controls, workplace security, and environmental controls)
  - Technical controls (Network segmentation, firewall, IDS/IPS, honeypot, proxy server, VPN, SIEM, UBA, and anti-malware)
- Fundamentals of virtualization, cloud computing, and cloud security
- Wireless network fundamentals, wireless encryption, and security measures
- Fundamentals of mobile and IoT devices and their security measures
- Cryptography and PKI Concepts
- Data security, data encryption, and data backup and data loss prevention techniques
- Network traffic monitoring for suspicious traffic

Who Is It For

- School students, graduates, professionals, career starters and changers, IT / Technology / Cybersecurity teams with little or no work experience.
- High-school students who aspire to get an early start on their cybersecurity career and master the fundamentals of security online.
- College or University students who are preparing for a cybersecurity career and aiding their IT education.
- Working professionals who are preparing to start with cybersecurity or switch to the field from another domain.

Training & Exam

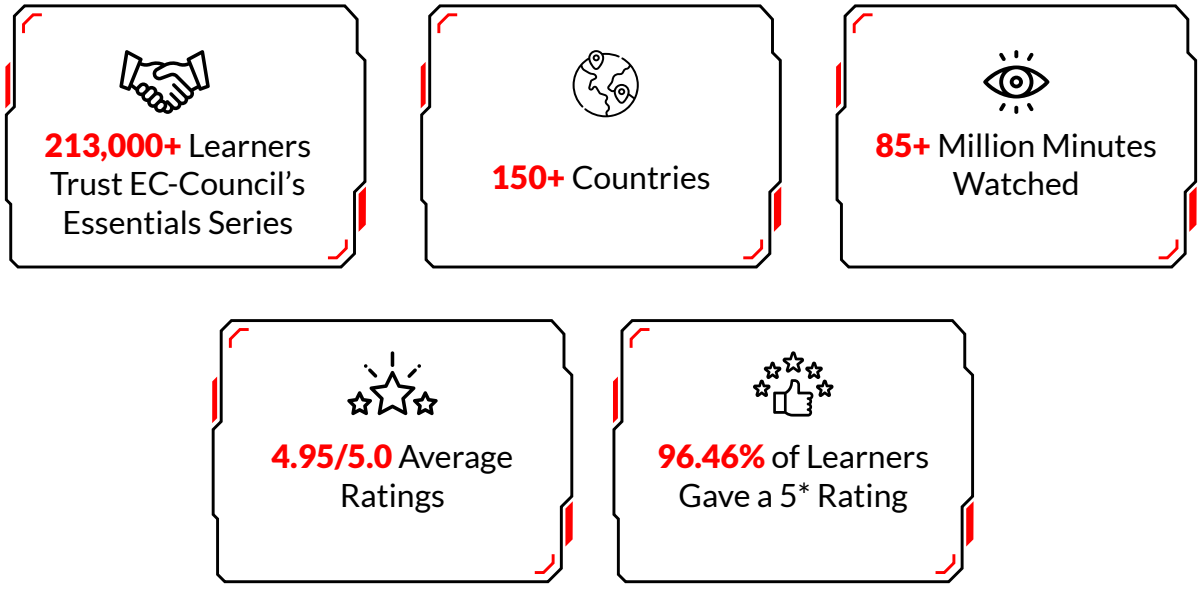
Training Details: Self-paced on-demand video led by world-class instructors along with hands-on labs.
Pre-requisite: No prior knowledge requirements.

Exam Details:
- Exam Code: 112-51
- Number of Questions: 75
- Duration: 2 hours
- Test Format: Multiple Choice

Key Features

- 14+ 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 1 year validity
- Increase your value in the job market to advance your career.
- Globally Recognized EC-Council's Certificate

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



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

Network Defense Essentials

www.eccouncil.org