EC-Council

E|CSS™
EC-Council Certified Security Specialist

EC-Council Certified
Security Specialist

START YOUR CYBERSECURITY TRAINING TODAY!

Learn the Fundamentals of 3 Core Domains of Cybersecurity

NETWORK DEFENSE | ETHICAL HACKING | DIGITAL FORENSICS

COURSE DESCRIPTION

EC-Council Certified Security Specialist (ECSS) is an entry level security program covering the fundamental concepts of Network Defense, Ethical Hacking, and Digital Forensics. It enables students to identify information security threats which reflect on the security posture of the organization and implement general security controls. This program will give a holistic overview of the key components of Network Defense, Ethical Hacking, and Digital Forensics. This program provides the solid fundamental knowledge required for a career in information security.

ECSS EMPOWERS INDIVIDUALS TO:

- Gain Foundational Knowledge in Cybersecurity
- Practice Essentials Skills such as how to defend networks and investigate them
- Challenge Industry recognized exams and earn cybersecurity credentials to build and further your career

WHY IS ECSS **IMPORTANT?**

It facilitates your entry into the world of Information Security.

It provides professional understanding about the concepts of Network Defense, Ethical Hacking, and Digital Forensics.

It provides best practices to improve organizational security posture.

It enhances your skills as a Security Specialist and increases your employability.

WHO IS IT **FOR?**

TARGET AUDIENCE

ECSS is designed for anyone who wants to enhance their skills and make a career in Network Defense, Ethical Hacking, Digital Forensics, and the Cybersecurity industry.

DURATION: 5 DAYS OR 40 HOURS

EXAM DETAILS

EXAM TITLE: EC-COUNCIL CERTIFIED SECURITY SPECIALIST

NUMBER OF QUESTIONS: 100

EXAM AVAILABILITY: EC-COUNCIL EXAM PORTAL

PASSING SCORE: 70%

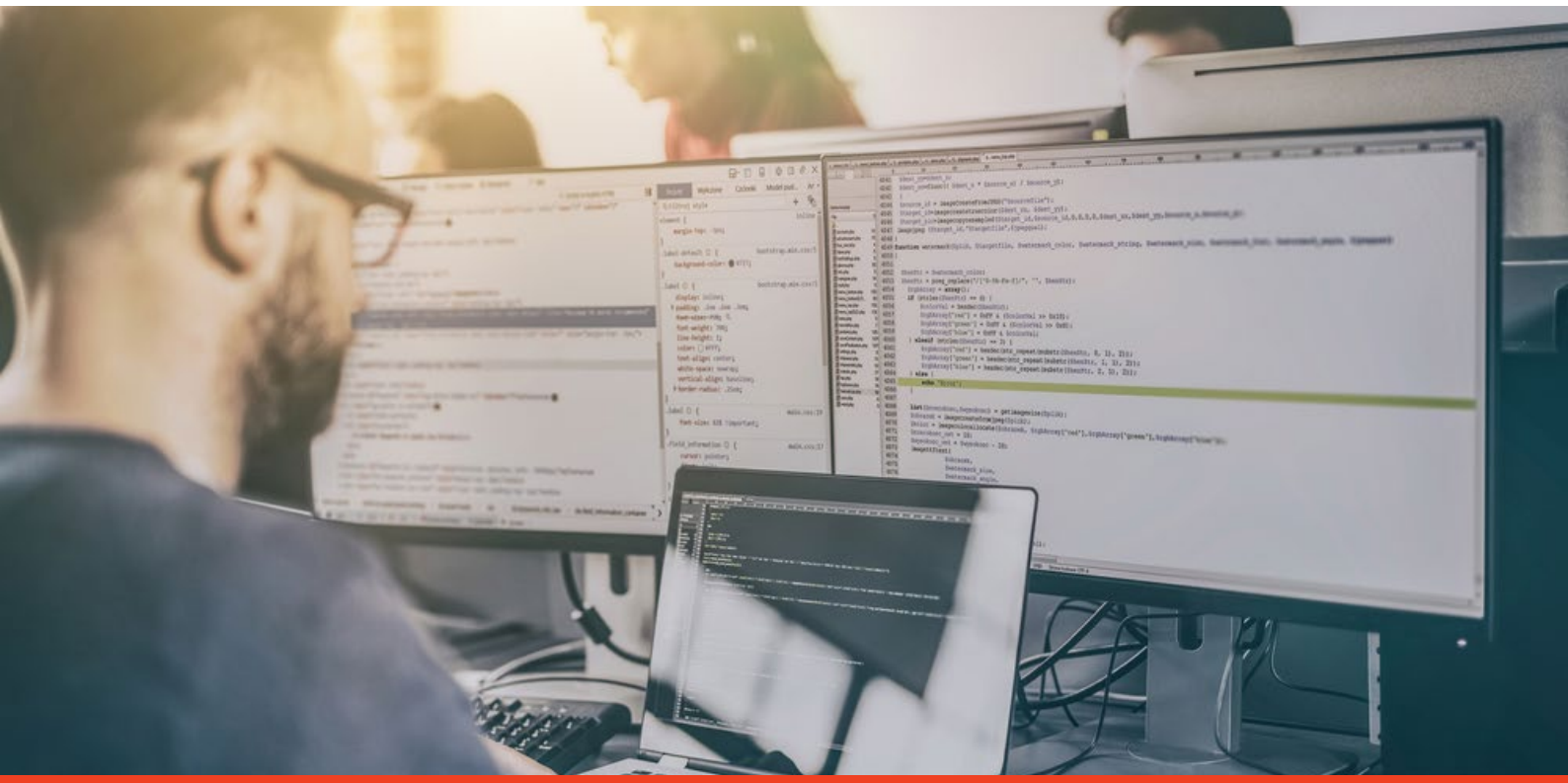
DURATION: 3 HOURS

TEST FORMAT: MULTIPLE CHOICE

COURSE OUTLINE

NETWORK DEFENSE ESSENTIALS

1. Network Security Fundamentals
2. Identification, Authentication, and Authorization
3. Network Security Controls: Administrative Controls
4. Network Security Controls: Physical Controls
5. Network Security Controls: Technical Controls
6. Virtualization and Cloud Computing
7. Wireless Network Security
8. Mobile Device Security
9. IoT Device Security
10. Cryptography and the Public Key Infrastructure
11. Data Security
12. Network Traffic Monitoring
13. Information Security Fundamentals



ETHICAL HACKING ESSENTIALS

14. Ethical Hacking Fundamentals
15. Information Security Threats and Vulnerability Assessment
16. Password Cracking Techniques and Countermeasures
17. Social Engineering Techniques and Countermeasures
18. Network Level Attacks and Countermeasures
19. Web Application Attacks and Countermeasures
20. Wireless Attacks and Countermeasures
21. Mobile Attacks and Countermeasures
22. IOT & OT Attacks and Countermeasures
23. Cloud Computing Threats and Countermeasures
24. Penetration Testing Fundamentals

DIGITAL FORENSICS ESSENTIALS

25. Computer Forensics Fundamentals
26. Computer Forensics Investigation Process
27. Understanding Hard Disks and File Systems
28. Data Acquisition and Duplication
29. Defeating Anti-forensics Techniques
30. Windows Forensics
31. Linux and Mac Forensics
32. Network Forensics
33. Investigating Web Attacks
34. Dark Web Forensics
35. Investigating Email Crimes
36. Malware Forensics

WHAT WILL YOU **LEARN?**

Students going through ECSS training will learn:

Network Security Fundamentals:	• Fundamentals of network security • Network security protocols that govern the flow of data
Identification, Authentication, and Authorization:	• Access control principles, terminologies, and models • Identity and access management (IAM)
Network Security Controls: Administrative Controls	• Regulatory frameworks, laws, and acts • Security policies, and how to conduct security and awareness training
Network Security Controls: Physical Controls	• Importance of physical security and physical security controls • Physical security policies and procedures • Best practices to strengthen workplace security • Environmental controls
Network Security Controls: Technical Controls	• Types of bastion hosts and their role in network security • IDS/IPS types and their role in network defense • Types of honeypots and virtual private networks (VPNs) • Security incident and event management (SIEM)

Virtualization and Cloud Computing	• Key concepts of virtualization and OS virtualization security • Cloud computing fundamentals and cloud deployment models • Cloud security best practices
Wireless Network Security	• Fundamentals of wireless networks and encryption mechanisms • Wireless network authentication methods • Implementing wireless network security measures
Mobile Device Security	• Mobile device connection methods and management • Mobile use approaches in enterprises • Security risks and guidelines associated with enterprise mobile usage policies • Implement various enterprise-level mobile security management solutions • Best practices on mobile platforms
IoT Device Security	• IoT devices, application areas, and communication models • How security works in IoT-enabled environments
Cryptography and PKI	• Cryptographic tools, security techniques, and algorithms • Public key infrastructure (PKI) to authenticate users and devices in the digital world
Data Security	• Data security and its importance • Security controls for data encryption • Perform data backup and retention • Implement data loss prevention concepts
Network Traffic Monitoring	• Network traffic monitoring concepts. • Traffic signatures for normal and suspicious network traffic. • Perform network monitoring to detect suspicious traffic
Information Security Fundamentals	• Information security fundamentals • Information security laws and regulations

Ethical Hacking Fundamentals	• Cyber Kill Chain methodology • Hacking concepts, hacking cycle, and different hacker classes • Ethical hacking concepts, scope, and limitations
Information Security Threats and Vulnerabilities	• Detect various threat sources and vulnerabilities in a network or system • Different types of malwares
Password Cracking Techniques and Countermeasures	•Types of password cracking techniques
Social Engineering Techniques and Countermeasures	• Social engineering concepts and techniques • Insider threats and identity theft concepts
Network-Level Attacks and Countermeasures	• Packet sniffing concepts and types • Sniffing techniques and countermeasures • DoS and DDoS attacks under sniffing attacks
Web Application Attacks and Countermeasures	• Web Server Attacks • Web Application Attacks • Web Application Architecture and Vulnerability Stack Web Application Threats and Attacks • SQL Injection Attacks • Types of SQL Injection Attacks
Wireless Attacks and Countermeasures	• Wireless Terminology • Types of Wireless Encryption • Wireless Network-specific Attack Techniques Bluetooth Attacks • Wireless Attack Countermeasures
Mobile Attacks and Countermeasures	• Mobile Attack Anatomy • Mobile Attack Vectors and Mobile Platform Vulnerabilities

IoT and OT Attacks and Countermeasures	**IoT Attacks** • IoT Devices, their need and Application Areas • IoT Threats and Attacks	**OT Attacks** • Understand OT Concepts • OT Challenges and Attacks • OT Attacks Countermeasures
Cloud Computing Threats and Countermeasures	• Cloud Computing Concepts • Container Technology • Cloud Computing Threats • Cloud Computing Countermeasures	
Penetration Testing Fundamentals	• Fundamentals of Penetration Testing and its Benefits • Various Types and Phases of Penetration Testing • Guidelines and Recommendations for Penetration Testing	
Computer Forensics Fundamentals	• Fundamentals of computer forensics and digital evidence • Objectives of forensic readiness to reduce the cost of investigation • Roles and responsibilities of a forensic investigator. • Legal compliance in computer forensics	
Computer Forensics Investigation Process	• Forensic investigation process and its importance • Forensic investigation phases	
Understanding Hard Disks and File Systems	• Types of disk drives and their characteristics • Booting process of Windows, Linux, and Mac operating systems • Examine file system records during an investigation	
Data Acquisition and Duplication	• Data acquisition fundamentals, methodologies, and their different types • Determine the data acquisition format	
Defeating Anti-forensics Techniques	• Anti-forensics techniques and their countermeasures	

Windows Forensics	• How to gather volatile and non-volatile information • Perform Windows memory and registry analysis • Analyze the cache, cookie, and history recorded in web browsers • Examine Windows files and metadata
Linux and Mac Forensics	• Volatile and non-volatile data in Linux • Analyze filesystem images using the sleuth kit • Demonstrate memory forensics • Mac forensics concepts
Network Forensics	• Network forensics fundamentals • Event correlation concepts and types • Identify indicators of compromise (IoCs) from network logs • Investigate network traffic for suspicious activity
Investigating Web Attacks	• Web application forensics and web attacks • Understand IIS and Apache web server logs • Detect and investigate various attacks on web applications
Dark Web Forensics	• Dark web forensics investigation and how it works. • Tor browser forensics
Investigating Email Crime	• Email basics and how it can be used as evidence • Techniques and steps used in email crime investigation
Malware Forensics	• Malware, its components, and distribution methods • Malware forensics fundamentals and types of malware analysis • Perform static malware analysis and dynamic malware analysis • Conduct system and network behavior analysis

LEGAL AGREEMENT

EC-Council Certified Security Specialist (ECSS) course mission is to educate, introduce, and demonstrate fundamentals of Network Defense, Ethical Hacking, and Digital Forensics. Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system, and to indemnify EC-Council with respect to the use or misuse of these tools, regardless of intent. The age requirement for attending the training or attempting the exam is restricted to any candidate that is at least 18 years old. If the candidate is under the age of 18, they are not eligible to attend the official training or eligible to attempt the certification exam unless they provide the Accredited Training Center (ATC) or EC-Council a written consent of their parent or their legal guardian and a supporting letter from their institution of higher learning. Only applicants from nationally accredited institutions of higher learning shall be considered.

EC-COUNCIL CERTIFIED SECURITY SPECIALIST

www.eccouncil.org

EC-Council

www.eccouncil.org