EC Council Certified Security Specialist (ECSS)

Course Duration: 5 Days

Course overview

EC-Council Certified Security Specialist (ECSS) is an entry level security program covering the fundamental concepts of information security, computer forensics, and network security. 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 information security, computer forensics, and network security. This program provides a solid fundamental knowledge required for a career in information security.

Target Audience

ECSS is designed for anyone who want to enhance their skills and make career in information security, network security, and computer forensics fields.

What you will learn

- Key issues plaguing the information security, network security, and computer forensics
- Fundamentals of networks and various components of the OSI and TCP/IP model
- Various types of information security threats and attacks, and their countermeasures
- Various network security protocols
- Social engineering techniques, identify theft, and social engineering countermeasures
- Different stages of hacking cycle
- Identification, authentication, and authorization concepts
- Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography
- attacks, and cryptanalysis tools
- Fundamentals of IDS and IDS evasion techniques
- Fundamentals of firewall, techniques for bypassing firewall, and firewall technologies
- such as Bastion Host, DMZ, Proxy Servers, Network Address Translation, Virtual Private
- Network, and Honeypot
- Fundamentals of IDS and IDS evasion techniques

- Data backup techniques and VPN security
- Wireless Encryption, wireless threats, wireless hacking tools, and Wi-Fi security
- Different types of web server and web application attacks, and countermeasures
- Fundamentals of ethical hacking and pen testing
- Incident handling and response process
- Cyber-crime and computer forensics investigation methodology
- Different types of digital evidence and digital evidence examination process
- Different type of file systems and their comparison (based on limit and features)
- Steganography and its techniques
- Different types of log capturing, time synchronization, and log capturing tools
- E-mails tracking and e-mail crimes investigation
- Writing investigation report

Course Outline

Module #	Module Topic
Module 01	Information Security Fundamentals
Module 02	Networking Fundamentals
Module 03	Secure Network Protocols
Module 04	Hacking Cycle
Module 05	Cryptography
Module 06	Firewalls
Module 07	Intrusion Detection System
Module 08	Data Backup
Module 09	Virtual Private Network
Module 10	Wireless Network Security
Module 11	Identification, Authentication, and

Module 12	Authorization
Module 13	Social Engineering
Module 14	Web Security
Module 15	Ethical Hacking and Pen Testing
Module 16	Incident Response
Module 17	Computer Forensics Fundamentals
Module 18	Digital Evidence
Module 19	Understanding File Systems
Module 20	Windows Forensics
Module 21	Steganography
Module 22	Analyzing Logs
Module 23	E-mail Crime and Computer Forensics
Module 24	Writing Investigative Report
Module 25	Network Forensics and Investigating

Exam Details:

Exam Details	ECCS (Exam)
Number of Questions	50
Test Duration	2 Hours
Test Format	Multiple Choice
Test Delivery	ECC Exam Portal
Passing Score	Score should be at least 70%