

ECSS

EC-Council

About The Course

EC-Council Certified Security Specialist (ECSS) allows students to enhance their skills in three different areas namely information security, network security, and computer forensics.

Information security plays a vital role in most organizations. Information security is where information, information processing, and communications are protected against the confidentiality, integrity, and availability of information and information processing.

About

The Course

In communications, information security also covers trustworthy authentication of messages that covers identification of verifying and recording the approval and authorization of information, non-alteration of data, and the non-repudiation of communication or stored data.



Duration: 40 hours / 5 days



Course Outline

Networking
Fundamentals

Secure
Network
Protocols

Information
Security Threats
and
Attacks

Social
Engineering

Hacking
Cycle

Identification,
Authentication,
and
Authorization

Cryptography

Information
Security
Fundamentals

Course Outline

Firewalls

Intrusion
Detection
System

Data Backup

Virtual Private
Network

Wireless Network
Security

Hacking
Cycle

Web Security

Ethical Hacking
and Pen Testing

Course Outline

Incident
Response

Computer
Forensics
Fundamentals

Digital Evidence

Understanding
File Systems

Windows
Forensics

Network
Forensics and
Investigating
Network Traffic

Steganography

Analyzing Logs

Course Outline

E-mail Crime
and Computer
Forensics

Writing I
nvestigative
Report

Course

Add Value

After ECSS the you will be able to



Key issues plaguing the information security, network security, and computer forensics



Social engineering techniques, identify theft, and social engineering countermeasures



Fundamentals of networks and various components of the OSI and TCP/IP model



Different stages of the hacking cycle



Various network security protocols




Identification, authentication, and authorization concepts




Various types of information security threats and attacks, and their countermeasures




Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography




Fundamentals of firewall, techniques for bypassing firewall, and firewall technologies.




Incident handling and response process




Fundamentals of IDS and IDS evasion techniques




Cyber-crime and computer forensics investigation methodology




Data backup techniques and VPN security




Different types of digital evidence and digital evidence examination process




Wireless Encryption, wireless threats, wireless hacking tools, and Wi-Fi security




Different types of file systems and their comparison (based on limit and features)




Different types of the web server and web application attacks, and countermeasures



Gathering volatile and non-volatile information from Windows and network.



Fundamentals of ethical hacking and pen testing



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.



GET IN TOUCH

www.iExperts.co

info@iExperts.co

Follow @iExperts10 on :

