Module Title : ECSS - EC-Council Certified Security Specialist
Duration : 3 days

Course Description

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.

Who should attend

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

What Will You 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 network security protocols
- Various types of information security threats and attacks, and their countermeasures
- 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 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)
- Gathering volatile and non-volatile information from Windows and network forensics analysis mechanism
- 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

- Information Security Fundamentals
- Networking Fundamentals
- Secure Network Protocols
- Information Security Threats and Attacks
- Social Engineering
- Hacking Cycle
- Identification, Authentication and Authorization
- Cryptography
- Firewalls
- Intrusion Detection System
- Data Backup
- Virtual Private Network
- Wireless Network Security
- Web Security
- Ethical Hacking and Pen Testing
- Incident Response
- Computer Forensics Fundamentals
- Digital Evidence
- Understanding File Systems
- Windows Forensics
- Network Forensics and Investigating Network Traffic
- Steganography
- Analyzing Logs
- E-mail Crime and Computer Forensics
- Writing Investigate Report