EC-Council Certified Security Specialist

Duration 5 days

COURSE DESCRIPTION

EC-Council Certified Security Specialist (ElCSS) allows students to enhance their skills in three different areas namely Network Defense, Ethical Hacking, Digital Forensics and the cybersecurity industry. 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. 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.

COURSE OBJECTIVES

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 Countermeasure

- 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

COURSE AGENDA

Network Defense Essentials

- Network Security Fundamentals
- Identification, Authentication, and Authorization
- Network Security Controls: Administrative Controls
- Network Security Controls: Physical Controls
- Network Security Controls: Technical Controls
- Virtualization and Cloud Computing
- Wireless Network Security
- Mobile Device Security
- loT Device Security
- Cryptography and the Public Key Infrastructure
- Data Security
- Network Traffic Monitoring

Ethical Hacking Essentials

- Information Security Fundamentals
- Ethical Hacking Fundamentals
- Information Security Threats and Vulnerability Assessment
- Password Cracking Techniques and Countermeasures
- Social Engineering Techniques and Countermeasures
- Network Level Attacks and Countermeasures
- Web Application Attacks and Countermeasures
- Wireless Attacks and Countermeasures
- Mobile Attacks and Countermeasures
- IOT & OT Attacks and Countermeasures
- Cloud Computing Threats and Countermeasures
- Penetration Testing Fundamentals

Digital Forensics Essentials

- Computer Forensics Fundamentals
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems

- Data Acquisition and Duplication
- Defeating Anti-forensics Techniques
- Windows Forensics
- Linux and Mac Forensics
- Network Forensics
- Investigating Web Attacks
- Dark Web Forensics
- Investigating Email Crimes
- Malware Forensics

ABOUT THE EXAM

The ECSS exam will be conducted on the last day of training. Students need to pass the online EC-Council Exam to receive the ECSS certification.
Number of Questions: 100
Passing Score: 70%
Test Duration: 3 Hours
Test Format: Multiple Choice
Test Delivery: EC-Council Exam Portal

WHO SHOULD ATTEND

ECSS is designed for anyone who want to enhance their skills and make career in network defense, ethical hacking, and digital forensics fields.