EC Council Certified Security Specialist (ECSS)

Length: 3 Days

Summary: 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 of the organizations.

Learning Objectives:

- Information security issues
- Symptoms and pinpoint the causes of those symptoms which reflect the security posture of the network
- Various hacking, investigation, and network security tools and techniques

COURSE CONTENT

1 - INFORMATION SECURITY FUNDAMENTALS

- Data Breach Statistics
- Data Loss Statistics
- The Global State of Information Security Survey 2016
- Information Security
- Need for Security
- Elements of Information Security
- The Security, Functionality, and Usability Triangle
- Security Challenges
- Information Security Attack Vectors
- Information Security Threat Categories
- Types of Attacks on a System
- Trends in Security
- Information Security Laws and Regulations

2 - NETWORKING FUNDAMENTALS

- Introduction
- Types of Networks
- OSI (Open Systems Interconnection) Reference Model
- OSI Reference Model: Diagram
- Application Layer
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer
- Data Link Layer
- Physical Layer
- OSI Layers and Device Mapping
- Protocols
- TCP/IP Model
- Comparing OSI and TCP/IP
- Network Security
- Essentials of Network Security
- Data Security Threats over a Network
- Basic Network Security Procedures
- Network Security Policies
- Types of Network Security Policies
- Data Policy: Example
- Computer Usage Policy: Example
- E-mail Policy

3 - SECURE NETWORK PROTOCOLS

- Introduction
- Terminology
- Secure Network Protocols
- E-mail Security Protocol – S/MIME
- E-mail Security Protocol – PGP
- Web Security Protocol – SSL
- Steps to Establish Connection Between Browser and Web server using SSL
- Web Security Protocol – SSH (Secure Shell)
- Web Security Protocol – HTTPS
- VPN Security Protocol – IPSec
- VPN Security Protocol – PPTP
- VPN Security Protocol – L2TP
- Wireless Security Protocol – WEP
- VoIP Security Protocol – H.323
- VoIP Security Protocol – SIP
- Public Key Infrastructure (PKI)

- Access Control List (ACL)
- Authentication, Authorization, and Accounting (AAA)
- RADIUS
- Kerberos
- Internet Key Exchange Protocol (IKE)

4 - INFORMATION SECURITY THREATS AND ATTACKS

- The Global State of Information Security Survey 2016
- Understanding Threat, Vulnerability and Exploit
- Internal Threats
- Sniffing
- Sniffing Countermeasures
- ARP Spoofing
- ARP Spoofing Diagram
- ARP Spoofing Countermeasures
- External Threats
- Malware Attacks
- Virus
- Introduction to Viruses
- Virus History
- Stages of Virus Life
- Indications of Virus Attack
- How does a Computer Get Infected by Viruses?
- Computer Worms
- How is a Worm Different from a Virus?
- Virus Detection Methods
- Virus and Worms Countermeasures
- Anti-Virus Tools
- Trojan
- What is a Trojan?
- Purpose of Trojans
- Indications of a Trojan Attack
- Different Ways a Trojan Can Get into a System
- How to Detect Trojans?
- Trojan Countermeasures
- Anti-Trojan Softwares
- Social Engineering
- Spamming
- Eavesdropping
- Eavesdropping Countermeasures
- Password Cracking
- Password Complexity
- Password Cracking Techniques
- Wire Sniffing
- Password Sniffing
- Man-in-the-Middle and Replay Attack
- Password Guessing
- Trojan/Spyware/Keylogger
- Non-Electronic Attacks
- Default Passwords
- Password Cracker
- L0phtCrack
- Ophcrack
- Cain & Abel
- RainbowCrack
- How to Defend against Password Cracking?
- Scanning
- Scanning Countermeasures
- Denial-of-Service (DoS)
- DoS Countermeasures
- Distributed DoS (DDoS)
- Distributed DoS Diagram
- Spoofing
- IP Spoofing
- IP Spoofing Diagram and Countermeasures
- Man-in-the-Middle Attack (MITM)
- TCP Session Hijacking
- Session Hijacking Countermeasures
- Corporate Espionage
- Accidental Security Breach
- Automated Computer Attack

5 - SOCIAL ENGINEERING

- What is Social Engineering?
- Behaviors Vulnerable to Attacks
- Why is Social Engineering Effective?
- Impact on the Organization
- Common Targets of Social Engineering
- Types of Social Engineering
- Technical Support Example
- Authority Support Example
- Human-based Social Engineering
- Eavesdropping
- Shoulder Surfing
- Dumpster Diving
- Tailgating
- In Person
- Third-Party Authorization
- Reverse Social Engineering
- Piggybacking
- Computer-based Social Engineering

- Computer-based Social Engineering: Phishing
- Social Engineering Through Impersonation on Social Networking Sites
- Identify Theft
- How to Steal an Identity?
- Social Engineering Countermeasures
- How to Detect Phishing Emails?
- Anti-Phishing Toolbar: Netcraft
- Identity Theft Countermeasures

6 - HACKING CYCLE

- What is Hacking?
- Who is a Hacker?
- Hacker Classes
- Hacktivism
- Stages of Hacking Cycle
- Phase 1 - Reconnaissance
- Phase 2 - Scanning
- Phase 3 – Gaining Access
- Phase 4 – Maintaining Access
- Phase 5 – Covering Tracks

7 - IDENTIFICATION, AUTHENTICATION, AND AUTHORIZATION

- Identification, Authentication and Authorization
- Identification
- Authentication
- Authorization
- Need for Identification, Authentication and Authorization
- Types of Authentication
- Basic Authentication
- Password Based Authentication
- Digest Authentication
- Form-based Authentication
- RSA SecurID Token
- Digital Certificates
- Certificate-based Authentication
- Biometrics Authentication
- Face Recognition
- Retina Scanning
- Fingerprint-based Identification
- Identification Based on Hand Geometry
- Factors of Authentication

8 - CRYPTOGRAPHY

- Terminology
- Cryptography
- Types of Cryptography
- Ciphers
- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)
- RC4, RC5, RC6 Algorithms
- The DSA and Related Signature Schemes
- RSA (Rivest Shamir Adleman)
- Example of RSA Algorithm
- The RSA Signature Scheme
- Message Digest Function: MD5
- Secure Hashing Algorithm (SHA)
- What is SSH (Secure Shell)?
- Public Key Infrastructure (PKI)
- Certification Authorities
- Digital Signature
- SSL (Secure Sockets Layer)
- Transport Layer Security (TLS)
- Disk Encryption
- Disk Encryption Tool: VeraCrypt

9 - FIREWALLS

- Firewall
- Features of Firewalls
- Firewall Architecture
- Types of Firewall
- Packet Filtering Firewall
- Circuit-Level Gateway Firewall
- Application-Level Firewall
- Stateful Multilayer Inspection Firewall
- Role of Firewalls in Network Security
- Advantages of Firewall
- Limitations of Firewalls
- Firewall Technologies
- Bastion Host
- Need for Bastion Host
- Positioning the Bastion Host
- Types of Bastion Hosts
- Basic Principles for Building a Bastion Host
- Setting Up Bastion Hosts
- Hardware Requirements for the Bastion Host
- Selecting the Operating System for the Bastion Host
- Auditing the Bastion Host
- Tool: IPSentry
- IPSentry: Automated Output Statistics HTML
- DMZ
- What is DMZ?
- Different Ways to Create a DMZ
- Proxy Servers

- What are Proxy Servers?
- Benefits of Proxy Server
- Functioning of a Proxy Server
- Proxy Server-to-Proxy Server Linking
- Proxy Servers vs Packet Filters
- Types of Proxy Servers
- Transparent Proxies
- Non-transparent Proxy
- Application Proxy
- SOCKS Proxy
- Anonymous Proxy
- Reverse Proxy
- How to Configure Proxy Server
- Steps to Configure Proxy Server on IE
- Ultrasurf
- Proxifier
- Limitations of Proxy Server
- List of Proxy Sites
- Network Address Translation
- Virtual Private Network
- Honeypot
- Types of Honeypots
- Honeypot Tool: KFSensor
- Honeypot Tool: SPECTER
- Bypassing Firewalls
- Firewall Identification
- Port Scanning
- Firewalking
- Banner Grabbing
- IP Address Spoofing
- Source Routing
- Bypass Blocked Sites Using IP Address in Place of URL
- Bypass Blocked Sites Using Anonymous Website Surfing Sites
- Bypass a Firewall Using Proxy Server

10 - INTRUSION DETECTION SYSTEM

- Terminologies
- Intrusion Detection System (IDS)
- Characteristics of IDS
- Importance of IDS
- IDS Vs Firewalls
- IDS Placement
- How IDS Works?
- Ways to Detect an Intrusion
- General Indications of System Intrusions
- General Indications of File System Intrusions
- General Indications of Network Intrusions
- Types of IDS
- IDS for an Organization
- Selecting an IDS
- Deploying the IDS
- Maintaining the IDS
- Limitations of Intrusion Detection System
- System Integrity Verifiers (SIV)
- Intrusion Detection Tools
- Snort
- Snort for Windows
- Running Snort on Windows
- Testing Snort
- Configuring Snort (snort.conf)
- Snort Rules
- SnortSam
- OSSEC (Open Source Security)
- Sguil
- Evading IDS
- Insertion Attack
- o Evasion
- o DoS Attack
- o Obfuscating
- o False Positive Generation
- o Session Splicing
- o Unicode Evasion Technique

11 - DATA BACKUP

- Introduction to Data Backup
- Identifying Critical Business Data
- Selecting Backup Media
- Backup Media
- Storage Area Network (SAN)
- o Advantages of SAN
- Network Attached Storage (NAS)
- Selecting Appropriate Backup Method
- Choosing the Right Location for Backup
- Backup Types
- Selecting Backup Types: Advantages and Disadvantages
- Choosing Right Backup Solution
- Data Backup Software: AOMEI Backupper
- Data Backup Tools

12 - VIRTUAL PRIVATE NETWORK

- What is a VPN?
- VPN Deployment

- Tunneling
- Types of Tunneling
- Popular VPN Tunneling Protocols
- VPN Security
- Authentication, Authorization and Accounting (AAA)
- VPN via SSH and PPP
- VPN via SSL and PPP
- VPN via Concentrator
- Other Methods
- VPN Registration and Passwords
- Introduction to IPSec
- IPSec Services
- Combining VPN and Firewalls
- VPN Vulnerabilities

13 - WIRELESS NETWORK SECURITY

- Wireless Networks
- Wireless Terminologies
- Types of Wireless Networks
- Wireless Standards
- Wireless Network Topology
- o Wireless Local Area Networks (WLANs)
- o Wireless Personal Area Networks (WPANs)
- o Wireless Metropolitan Area Network (WMANs)
- o Wireless Wide Area Network (WWANs)
- Antennas
- Service Set Identifier (SSID)
- Types of Wireless Encryption
- o WEP Encryption
- How WEP Works?
- Limitations of WEP Security
- Temporal Key Integration Protocol (TKIP) and Advanced Encryption Standard (AES)
- o What is WPA?
- How WPA Works?
- o What is WPA2?
- How WPA2 Works?
- o WEP vs. WPA vs. WPA2
- Wireless Threats
- o Effects of Wireless Attacks on Business
- o Wi-Fi Chalking
- o Access Control Attacks
- o Integrity Attacks
- o Confidentiality Attacks
- o Availability Attacks
- o Authentication Attacks
- o Rogue Access Point Attack
- o Denial of Service Attacks
- o Man-in-the-Middle Attack (MITM)
- o Locating Rogue Access Points
- Wi-Fi Discovery Tools
- o NetStumbler
- o inSSIDer
- o Aircrack-ng
- o Kismet
- Wireless Security
- o Wireless Transportation Layer Security (WTLS)
- o Extensible Authentication Protocol (EAP) Methods
- o Securing Wireless Networks
- o Maximum Security: Add VPN to Wireless LAN
- How to Defend Against Wireless Attacks?

14 - WEB SECURITY

- Introduction to Web Applications
- Web Application Components
- How Web Applications Work?
- Website Defacement
- Why Web Servers are Compromised?
- Impact of Webserver Attacks
- Web Application Threats
- Web Application Countermeasures
- How to Defend Against Web Server Attacks?

15 - ETHICAL HACKING AND PEN TESTING

- What is Ethical Hacking?
- o Why Ethical Hacking is Necessary
- o What Do Ethical Hackers Do?
- o Scope and Limitations of Ethical Hacking
- o Skills of an Ethical Hacker
- o Defense in Depth
- What is Penetration Testing?
- o Why Penetration Testing?

16 - INCIDENT RESPONSE

- Common Terminologies
- Data Classification
- Information as Business Asset
- Computer Security Incident
- o Types of Computer Security Incidents
- o Incident Response
- o Signs of an Incident

- o Incident Categories
- o Incident Reporting
- o Incident Reporting Organizations
- Incident Handling and Response Process
- o Step 1: Preparation for Incident Handling and Response
- o Step 2: Detection and Analysis
- o Step 3: Classification and Prioritization
- o Step 4: Notification and Planning
- o Step 5: Containment
- o Step 6: Forensic Investigation
- o Step 7: Eradication and Recovery
- o Step 8: Post-Incident Activities
- CSIRT Overview
- o Need for CSIRT
- o CSIRT Steps to Handle Cases
- o Best Practices for Creating a CSIRT
- CERT
- o World CERTs
- GFIRST
- FIRST

17 - COMPUTER FORENSICS FUNDAMENTALS

- Cyber Crime
- o Computer Facilitated Crimes
- o Modes of Attacks
- o Examples of Cyber Crime
- o Types of Computer Crimes
- o Investigating Computer Crime
- o Cyber Criminals
- o Cyber Crime Investigation
- o Forensics Science
- Computer Forensics
- o Aspects of Organizational Security
- o Evolution of Computer Forensics
- o Objective of Computer Forensics
- o Need for Computer Forensics
- o Why and When Do You Use Computer Forensics?
- o Goals of Forensics Readiness
- Benefits of Forensics Readiness
- o Computer Forensics Investigation Methodology
- o Key Steps in Forensics Investigation
- o Rules of Forensics Investigation
- o Role of Digital Evidence
- o Review Policies and Laws
- Forensics Laws
- Why you Should Report Cybercrime?
- Who to Contact at the Law Enforcement?
- Federal Local Agents Contact
- More Contacts

18 - DIGITAL EVIDENCE

- Definition of Digital Evidence
- o Increasing Awareness of Digital Evidence
- o Challenging Aspects of Digital Evidence
- o The Role of Digital Evidence
- o Characteristics of Digital Evidence
- o Fragility of Digital Evidence
- o Types of Digital Data
- o Rules of Evidence
- o Best Evidence Rule
- Electronic Devices: Types and Collecting Potential Evidence
- Digital Evidence Examination Process
- o Evidence Assessment
- o Evidence Acquisition
- o Handling Digital Evidence
- o Evidence Examination
- o Documenting the Evidence
- Evidence Examiner Report

19 - UNDERSTANDING FILE SYSTEMS

- Understanding File Systems
- Types of File Systems
- Understanding System Boot Sequence
- Windows File Systems
- o Exploring Microsoft File Structures
- o FAT vs. NTFS
- o Popular Windows File Systems
- FAT Structure
- NTFS Architecture
- o Encrypting File Systems (EFS)
- Components of EFS
- o Exploring Microsoft File Structures: Cluster
- o Gathering Evidence on Windows Systems
- Gathering Volatile Evidence on Windows
- Example: Checking Current Processes with Forensic Tool PsList
- Example: Checking Open Ports With Forensic Tool Fport
- Checking Registry Entries
- Forensic Tool: Registrar Registry Manager
- Linux File Systems
- o Linux Overview

- o Exploring Unix/Linux Disk Data Structures
- o Understanding Unix/Linux Boot Process
- o Understanding Linux Loader
- o Linux File System Architecture
- o Popular Linux File Systems
- Mac OS X File Systems
- o HFS vs. HFS Plus
- CD-ROM / DVD File Systems
- o Compact Disc File System (CDFS)
- Comparison of File Systems (Limits)
- Comparison of File Systems (Features)

20 - WINDOWS FORENSICS

- Volatile Information
- Non-Volatile Information
- o Registry Settings
- o Event Logs
- o Other Non-Volatile Information
- o Cache, Cookie, and History Analysis: Google Chrome
- o Cache, Cookie, and History Analysis: Microsoft Edge
- o Analysis Tools
- Message Digest Function: MD5
- o Why MD5 Calculation?
- o MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles
- Recycle Bin
- Metadata
- o Types of Metadata
- o Metadata Analysis Tool: Metashield Analyzer
- Understanding Events
- o Event Logon Types
- o Searching with Event Viewer
- Windows Forensics Tool: OS Forensics
- Windows Forensics Tool: X-Ways Forensics
- Windows Forensics Tools

21 - NETWORK FORENSICS AND INVESTIGATING NETWORK TRAFFIC

- Network Forensics
- Network Forensics Analysis Mechanism
- Network Addressing Schemes
- Overview of OSI Reference Model and Network Protocols
- TCP/IP Model
- Network Vulnerabilities
- Types of Network Attacks
- o IP Address Spoofing
- o Man-in-the-Middle Attack
- o Enumeration
- o Denial-of-Service Attack
- o Session Sniffing
- o Buffer Overflow
- o Trojan Horse
- Why Investigate Network Traffic?
- Evidence Gathering via Sniffing
- Capturing Live Data Packets Using Wireshark

22 - STEGANOGRAPHY

- What is Steganography?
- Steganography Vs. Cryptography
- How Steganography Works?
- Legal Use of Steganography
- Unethical Use of Steganography
- Steganography Techniques
- Application of Steganography
- Classification of Steganography
- o Technical Steganography
- Types of Steganography based on Cover Medium
- o Image Steganography
- Image Steganography Tool: QuickStego
- o Audio Steganography
- Audio Steganography Tool: DeepSound
- o Video Steganography
- Video SteganographyTool : OmniHide PRO
- o Document Steganography Tool: wbStego and SNOW
- Issues in Information Hiding

23 - ANALYZING LOGS

- Importance of Logs in Forensics
- Computer Security Logs
- Operating System Logs
- Application Logs
- Security Software Logs
- Examining Intrusion and Security Events
- Syslog
- o Syslog-ng OSE
- o Kiwi Log Viewer
- Windows Log File
- Configuring Windows Logging
- Why Synchronize Computer Times?
- Event Correlation
- o EventLog Analyzer

24 - E-MAIL CRIME AND COMPUTER FORENSICS

- Email Terminology
- Email System
- o Email Clients
- o Email Server
- SMTP Server
- POP3 and IMAP Servers
- o Email Message
- Importance of Electronic Records Management
- Email Crime
- o Email Spamming
- o Mail Bombing/Mail Storm
- o Phishing
- o Email Spoofing
- Example of Email Header
- List of Common Headers
- Why to Investigate Emails
- Investigating Email Crime and Violation
- o Obtain a Search Warrant and Seize the Computer and Email Account
- o Obtain a Bit-by-Bit Image of Email Information
- o Examine Email Headers
- Viewing Email Headers in Microsoft Outlook
- Viewing Email Headers in AOL
- Viewing Email Headers in Gmail
- Viewing Email Headers in Yahoo Mail
- Forging Headers
- o Analyzing Email Headers
- Email Header Fields
- Received Headers
- E-mail Forensics Tools
- o Recover My Email
- o Email Trace - Email Tracking
- o eMailTrackerPro
- o Forensic Toolkit (FTK)
- o Abuse.Net

25 - WRITING INVESTIGATION REPORT

- Computer Forensics Report
- o Salient Features of a Good Report
- o Aspects of a Good Report
- o Computer Forensics Report Template
- o Investigative Report Format
- o Case Report Writing and Documentation
- o Create a Report to Attach to the Media Analysis Worksheet
- Best Practices for Investigators
- Sample Forensics Report