EC-Council Certified Security Specialist

Course Outline

(Version 9)

Module 01: 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

Module 02: 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

Module 03: 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)

Module 04: 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

Module 05: 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

Module 06: 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

Module 07: 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

Module 08: 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

Module 09: 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

Module 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
    - Evasion
    - DoS Attack
    - Obfuscating
    - False Positive Generation
    - Session Splicing
    - Unicode Evasion Technique

Module 11: Data Backup

- Introduction to Data Backup
- Identifying Critical Business Data
- Selecting Backup Media
- Backup Media
- Storage Area Network (SAN)
    - 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

Module 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

Module 13: Wireless Network Security

- Wireless Networks
- Wireless Terminologies
- Types of Wireless Networks
- Wireless Standards
- Wireless Network Topology
  - Wireless Local Area Networks (WLANs)
  - Wireless Personal Area Networks (WPANs)
  - Wireless Metropolitan Area Network (WMANs)
  - Wireless Wide Area Network (WWANs)
- Antennas
- Service Set Identifier (SSID)
- Types of Wireless Encryption

- WEP Encryption
  - How WEP Works?
  - Limitations of WEP Security
  - Temporal Key Integration Protocol (TKIP) and Advanced Encryption Standard (AES)
- What is WPA?
  - How WPA Works?
- What is WPA2?
  - How WPA2 Works?
- WEP vs. WPA vs. WPA2

- Wireless Threats
  - Effects of Wireless Attacks on Business
  - Wi-Fi Chalking
  - Access Control Attacks
  - Integrity Attacks
  - Confidentiality Attacks
  - Availability Attacks
  - Authentication Attacks
  - Rogue Access Point Attack
  - Denial of Service Attacks
  - Man-in-the-Middle Attack (MITM)
  - Locating Rogue Access Points
- Wi-Fi Discovery Tools
  - NetStumbler
  - inSSIDer
  - Aircrack-ng
  - Kismet
- Wireless Security
  - Wireless Transportation Layer Security (WTLS)
  - Extensible Authentication Protocol (EAP) Methods
  - Securing Wireless Networks

- Maximum Security: Add VPN to Wireless LAN
- How to Defend Against Wireless Attacks?

Module 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?

Module 15: Ethical Hacking and Pen Testing

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

Module 16: Incident Response

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

- Signs of an Incident
- Incident Categories
- Incident Reporting
- Incident Reporting Organizations

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

Module 17: Computer Forensics Fundamentals

- Cyber Crime
  - Computer Facilitated Crimes
  - Modes of Attacks
  - Examples of Cyber Crime
  - Types of Computer Crimes
  - Investigating Computer Crime
  - Cyber Criminals
  - Cyber Crime Investigation

- Forensics Science

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

Module 18: Digital Evidence

- Definition of Digital Evidence
  - Increasing Awareness of Digital Evidence
  - Challenging Aspects of Digital Evidence
  - The Role of Digital Evidence
  - Characteristics of Digital Evidence
  - Fragility of Digital Evidence
  - Types of Digital Data
  - Rules of Evidence
  - Best Evidence Rule
- Electronic Devices: Types and Collecting Potential Evidence

- Digital Evidence Examination Process
  - Evidence Assessment
  - Evidence Acquisition
  - Handling Digital Evidence
  - Evidence Examination
  - Documenting the Evidence
- Evidence Examiner Report

Module 19: Understanding File Systems

- Understanding File Systems
- Types of File Systems
- Understanding System Boot Sequence
- Windows File Systems
  - Exploring Microsoft File Structures
  - FAT vs. NTFS
  - Popular Windows File Systems
    - FAT Structure
    - NTFS Architecture
  - Encrypting File Systems (EFS)
    - Components of EFS
  - Exploring Microsoft File Structures: Cluster
  - 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
  - Linux Overview
  - Exploring Unix/Linux Disk Data Structures
  - Understanding Unix/Linux Boot Process

- Understanding Linux Loader
- Linux File System Architecture
- Popular Linux File Systems

- Mac OS X File Systems
  - HFS vs. HFS Plus
- CD-ROM / DVD File Systems
  - Compact Disc File System (CDFS)
- Comparison of File Systems (Limits)
- Comparison of File Systems (Features)

Module 20: Windows Forensics

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

- Windows Forensics Tools

Module 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
  - IP Address Spoofing
  - Man-in-the-Middle Attack
  - Enumeration
  - Denial-of-Service Attack
  - Session Sniffing
  - Buffer Overflow
  - Trojan Horse
- Why Investigate Network Traffic?
- Evidence Gathering via Sniffing
- Capturing Live Data Packets Using Wireshark

Module 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
  - Technical Steganography

- Types of Steganography based on Cover Medium
  - Image Steganography
    - Image Steganography Tool: QuickStego
  - Audio Steganography
    - Audio Steganography Tool: DeepSound
  - Video Steganography
    - Video SteganographyTool : OmniHide PRO
  - Document Steganography Tool: wbStego and SNOW
- Issues in Information Hiding

Module 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
  - Syslog-ng OSE
  - Kiwi Log Viewer
- Windows Log File
- Configuring Windows Logging
- Why Synchronize Computer Times?
- Event Correlation
  - EventLog Analyzer

Module 24: E-mail Crime and Computer Forensics

- Email Terminology
- Email System
  - Email Clients
  - Email Server

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

Module 25: Writing Investigation Report

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