MINISTERIO DE TRABAJO, MIGRACIONES Y SEGURIDAD SOCIAL

SERVICIO PÚBLICO DE EMPLEO ESTATAL SEPE

FONDO SOCIAL EUROPEO
El FSE invierte en tu futuro

PROGRAMA FORMATIVO

ESPECIALISTA EN SEGURIDAD EC COUNCIL

Diciembre 2019

DATOS GENERALES DE LA ESPECIALIDAD

1. Familia Profesional: INFORMÁTICA Y COMUNICACIONES

Área Profesional: SISTEMAS Y TELEMÁTICA

2. Denominación: ESPECIALISTA EN SEGURIDAD EC COUNCIL

3. Código: **IFCT66**

4. Nivel de cualificación: 3

5. Objetivo general:

Identificar amenazas e implementar controles que garanticen la seguridad de la información y las comunicaciones dentro de una red corporativa, utilizando las técnicas forenses adecuadas para investigar, resolver, reportar y prevenir futuros incidentes o ataques de seguridad.

6. Prescripción de los formadores:

6.1. Titulación requerida:

Titulación universitaria o Ciclo Formativo de Grado Superior, en su defecto, capacitación profesional equivalente en la especialización relacionada con el curso.

El formador deberá estar certificado por el fabricante como 'Certified EC Council Instructor' y contar con todas las certificaciones de la especialidad a impartir vigentes y actualizadas.

6.2. Experiencia profesional requerida:

Al menos doce meses de experiencia profesional en la especialidad objeto, excluyendo la experiencia docente

6.3. Competencia docente:

Será necesario tener experiencia metodológica o experiencia docente contrastada de 500 horas de formación en especialidades relacionadas con la especialidad a impartir.

7. Criterios de acceso del alumnado:

7.1. Nivel académico o de conocimientos generales:

- Título de FP Grado superior o Título de Bachillerato.
- Dominio de inglés a nivel de lectura.
- Conocimientos generales de informática y redes de ordenadores.

Cuando el aspirante al curso no posea el nivel académico indicado, demostrará conocimientos suficientes a través de una prueba de acceso.

8. Número de participantes:

Máximo 25 participantes para cursos presenciales.

9. Relación secuencial de módulos formativos:

- Módulo 1. Information Security and Network Fundamentals
- Módulo 2. Secure Network Protocols
- Módulo 3. Information Security Threats and Attacks

- Módulo 4. Social Engineering
- Módulo 5. Hacking Cycle (5 horas)
- Módulo 6. Identification, Authentication, and Authorization
- Módulo 7. Cryptography
- Módulo 8. Firewalls
- Módulo 9. Intrusion Detection System
- Módulo 10. Data Backup
- Módulo 11. Virtual Private Network
- Módulo 12. Wireless Network Security
- Módulo 13. Web Security
- Módulo 14. Ethical Hacking and Pen Testing
- Módulo 15. Incident Response
- Módulo 16. Computer Forensics Fundamentals
- Módulo 17. Digital Evidence
- Módulo 18. Understanding File Systems
- Módulo 19. Windows Forensics
- Módulo 20. Network Forensics and Investigating Network Traffic
- Módulo 21. Steganography
- Módulo 22. Analyzing Logs
- Módulo 23. E-mail Crime and Computer Forensics
- Módulo 24. Writing Investigation Report

Este curso deberá asegurar la formación requerida para preparar y presentarse a la siguiente certificación oficial de fabricante:

- ECSS EC-Council Certified Security Specialist.

10. Duración:

Horas totales: 120 horas.

Distribución horas:
- Presencial: 120 horas.

11. Requisitos mínimos de espacios, instalaciones y equipamiento

11.1. Espacio formativo:

- Aula de gestión de 3 m^2 por alumno

  Cada espacio estará equipado con mobiliario docente adecuado al número de alumnos, así mismo constará de las instalaciones y equipos de trabajo suficientes para el desarrollo del curso.

11.2. Equipamiento:

- Aula de gestión:
  - Mesa y silla para el formador
  - Mesas y sillas para el alumnado
  - Material de aula
  - Pizarra
  - PC instalado en red con posibilidad de impresión de documentos, cañon con proyector e internet para el formador
  - PCs instalados en red e internet con posibilidad de impresión para los alumnos

Los equipos tendrán unas características equivalentes a las enumeradas a continuación, consideradas siempre como mínimas:

Hardware:

- CPU: procesador Intel Core i5 de 6 generación o similar.

- 16 GB de RAM
- Disco duro 500 GB
- Tarjeta de red 100/1000 Mbps
- Teclado multimedia USB
- Ratón sensor óptico USB de 2 botones y rueda de desplazamiento.
- Monitor color de 17” TFT

Software:

- Licencias del fabricante para la impartición de los cursos correctamente.
- Licencias del sistema operativo.
- Licencias de antivirus.
- Conexión a Internet con ancho de banda suficiente.

En todo caso los requisitos mínimos tanto HW como SW serán los que marque el fabricante en cada momento como recomendadas para las versiones actualizadas.

A los alumnos se le proporcionará la documentación oficial de EC-Council necesaria para el seguimiento del curso.

Las instalaciones y equipamientos deberán cumplir con la normativa industrial e higiénico sanitaria correspondiente y responderán a medidas de accesibilidad universal y seguridad de los participantes.

En el caso de que la formación se dirija a personas con discapacidad se realizarán las adaptaciones y los ajustes razonables para asegurar su participación en condiciones de igualdad.

12. Requisitos de los centros

Los centros impartidores de formación Oficial de EC-Council, deben cumplir los siguientes requisitos:

- Acreditación de encontrarse autorizado por el fabricante para impartir formación oficial.

13. Evaluación del aprendizaje

Se llevará a cabo una evaluación continua y sistemática durante el proceso de aprendizaje y al final del mismo para comprobar si los alumnos han alcanzado los objetivos establecidos en cada módulo y, por consiguiente, han realizado el curso con el aprovechamiento requerido.

14. Certificación oficial del fabricante

La ejecución y financiación del programa formativo incluye la presentación de los alumnos que han realizado el curso con aprovechamiento a los exámenes para obtener la certificación oficial del fabricante, que gestionará el centro y que en ningún caso supondrá coste alguno para el alumno.

En concreto, para esta acción formativa está incluido el siguiente examen de certificación oficial de EC-Council, o el que lo sustituya actualizado al momento de su impartición:

- ECSS EC-Council Certified Security Specialist.

MÓDULOS FORMATIVOS

Módulo nº 1

Denominación: INFORMATION SECURITY AND NETWORK FUNDAMENTALS

Objetivo: Identificar aspectos clave relacionados con la seguridad de la información, las comunicaciones dentro de una red corporativa, su infraestructura, componentes, protocolos y servicios.

Duración: 5 horas

Contenidos teórico prácticos:

- 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
- 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

Módulo nº 2

Denominación: SECURE NETWORK PROTOCOLS.

Objetivo: Identificar protocolos y servicios básicos que garantizan la seguridad en una red.

Duración: 5 horas

Contenidos teórico prácticos:

- 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 – HTTP
    - 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)

Módulo nº 3

Denominación: INFORMATION SECURITY THREATS AND ATTACKS.

Objetivo: Detectar amenazas y ataques de seguridad identificando las medidas adecuadas para contrarrestarlos.

Duración: 5 horas

Contenidos teórico prácticos:

- The Global State of Information Security Survey 2016
- Understanding Threat, Vulnerability and Exploit
- Internal Threats
    - Sniffing
    - ARP Spoofing
- External Threats
    - Malware Attacks
        - Virus
        - Trojan
    - Social Engineering
    - Spamming
    - Eavesdropping
        - Eavesdropping Countermeasures
    - Password Cracking
        - Password Complexity
        - Password Cracking Techniques
        - Password Cracker
        - How to Defend against Password Cracking?
    - Scanning
    - Denial-of-Service (DoS)
        - DoS Countermeasures
        - Distributed DoS Diagram
    - Spoofing
        - IP Spoofing
        - Man-in-the-Middle Attack (MITM)
    - TCP Session Hijacking
        - Session Hijacking Countermeasures
    - Corporate Espionage
    - Accidental Security Breach

- Automated Computer Attack

Módulo nº 4

Denominación: SOCIAL ENGINEERING.

Objetivo: Describir técnicas de ingeniería social, robo de identidad e identificar medidas de protección.

Duración: 5 horas

Contenidos teórico prácticos:

- 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

Módulo nº 5

Denominación: HACKING CYCLE.

Objetivo: Identificar las distintas fases del ciclo de hacking.

Duración: 5 horas

Contenidos teórico prácticos:

- 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.

Módulo nº 6

Denominación: IDENTIFICATION, AUTHENTICATION, AND AUTHORIZATION

Objetivo: Comprender la necesidad de los procesos de identificación, autenticación y autorización.

Duración: 5 horas

Contenidos teórico prácticos:

- Identification, Authentication and 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

Módulo nº 7

Denominación: CRYPTOGRAPHY

Objetivo: Usar de herramientas básicas de criptoanálisis.

Duración: 5 horas

Contenidos teórico prácticos:

- 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

Módulo nº 8

Denominación: FIREWALLS

Objetivo: Proteger redes corporativas configurando y combinando elementos y servicios como firewalls, proxy servers, DMZ, NAT, VPN y Honeypot.

Duración: 5 horas

Contenidos teórico prácticos:

- 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
    - 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
        - 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

Módulo nº 9

Denominación: INTRUSION DETECTION SYSTEM

Objetivo: Implementar técnicas de prevención y detección de intrusiones.

Duración: 5 horas

Contenidos teórico prácticos:

- 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

Módulo nº 10

Denominación: DATA BACKUP

Objetivo: Seleccionar e implementar los métodos y medios de backup más adecuados para las características de una red corporativa dada.

Duración: 5 horas

Contenidos teórico prácticos:

- 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

Módulo nº 11

Denominación: VIRTUAL PRIVATE NETWORK

Objetivo: Configurar el acceso seguro a una red privada a través de redes públicas.

Duración: 5 horas

Contenidos teórico prácticos:

- 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 Vulnerabilitiesl

Módulo nº 12

Denominación: WIRELESS NETWORK SECURITY

Objetivo: Implementar y configurar los servicios que garantizan la seguridad en una red inalámbrica.

Duración: 5 horas

Contenidos teórico prácticos:

- 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?

Módulo nº 13

Denominación: WEB SECURITY

Objetivo: Identificar las principales amenazas y ataques que se realizan contra los servidores web e implementar medidas que ayuden a contrarrestarlos y prevenirlos.

Duración: 5 horas

Contenidos teórico prácticos:

- 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?

Módulo nº 14

Denominación: ETHICAL HACKING AND PEN TESTING

Objetivo: Aplicar los fundamentos del hacking ético y pentesting.

Duración: 5 horas

Contenidos teórico prácticos:

- 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

Módulo nº 15

Denominación: INCIDENT RESPONSE

Objetivo: Gestionar los procesos de gestión y respuesta a incidentes relacionados con la seguridad.

Duración: 5 horas

Contenidos teórico prácticos:

- 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

Módulo nº 16

Denominación: COMPUTER FORENSICS FUNDAMENTALS

Objetivo: Identificar los pasos a seguir en la investigación forense de un ciberataque.

Duración: 5 horas

Contenidos teórico prácticos:

- 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

Módulo nº 17

Denominación: DIGITAL EVIDENCE

Objetivo: Evaluar diferentes tipos de evidencia en el proceso de evaluación de un incidente de seguridad.

Duración: 5 horas

Contenidos teórico prácticos:

- 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

Módulo nº 18

Denominación: UNDERSTANDING FILE SYSTEMS

Objetivo: Identificar las diferencias y limitaciones de los distintos tipos de sistemas de ficheros.

Duración: 5 horas

Contenidos teórico prácticos:

- 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)

Módulo nº 19

Denominación: WINDOWS FORENSICS

Objetivo: Obtener información volátil y no volátil de un sistema Windows.

Duración: 5 horas

Contenidos teórico prácticos:

- 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

Módulo nº 20

Denominación: NETWORK FORENSICS AND INVESTIGATING NETWORK TRAFFIC

Objetivo: Recopilar información relacionada con el tráfico de datos en una red para el análisis forense de distintos tipo de incidencias.

Duración: 5 horas

Contenidos teórico prácticos:

- 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 o Buffer Overflow
    - Trojan Horse
- Why Investigate Network Traffic?
- Evidence Gathering via Sniffing
- Capturing Live Data Packets Using Wireshark

Módulo nº 21

Denominación: STEGANOGRAPHY

Objetivo: Identificar las principales técnicas de la estenografía para el envío de mensajes ocultos.

Duración: 5 horas

Contenidos teórico prácticos:

- 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 Steganographyl
- 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

Módulo nº 22

Denominación: ANALYZING LOGS

Objetivo: Extraer información relevante de las capturas de logs de un sistema para la prevención y resolución de incidentes de seguridad.

Duración: 5 horas

Contenidos teórico prácticos:

- 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

Módulo nº 23

Denominación: E-MAIL CRIME AND COMPUTER FORENSICS

Objetivo: Investigar delitos relacionados con uso fraudulento del correo electrónico.

Duración: 5 horas

Contenidos teórico prácticos:

- 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

Módulo nº 24

Denominación: WRITING INVESTIGATION REPORT

Objetivo: Elaborar el informe forense resultado de la investigación de un ciberataque.

Duración: 5 horas

Contenidos teórico prácticos:

- 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