MINISTERIO DE TRABAJO, MIGRACIONES Y SEGURIDAD SOCIAL

SERVICIO PÚBLICO DE EMPLEO ESTATAL SEPE

FONDO SOCIAL EUROPEO
El FSE invierte en tu futuro

PROGRAMA FORMATIVO

ETHICAL HACKER EC COUNCIL

Diciembre 2019

DATOS GENERALES DE LA ESPECIALIDAD

1. Familia Profesional: INFORMÁTICA Y COMUNICACIONES

Área Profesional: SISTEMAS Y TELEMÁTICA

2. Denominación: ETHICAL HACKER EC COUNCIL

3. Código: **IFCT68**

4. Nivel de cualificación: 3

5. Objetivo general:

Utilizar las mismas herramientas y conocimientos que un hacker 'malicioso', de manera legítima y desde una perspectiva de fabricante neutral, para garantizar la seguridad en una red corporativa, planificando su protección, detectando y respondiendo a los ataques que se realizan sobre la misma.

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/experiencia en informática y redes de ordenadores.
- Certificación ECSS (EC Council Security Specialist) o certificado de profesionalidad de Seguridad Informática o experiencia profesional relacionada.

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. Network Defender Skills for Network Administrators: EC-COUNCIL Certified Network Defender

- Módulo 2. Mastering Hacking Technologies I: EC COUNCIL Certified Ethical Hacker
- Módulo 3. Mastering Hacking Technologies II: EC COUNCIL Certified Ethical Hacker Practical

Este curso deberá asegurar la formación requerida para preparar y presentarse a las siguientes certificaciones oficiales de fabricante:

- CND EC-Council Certified Network Defender.
- CEH EC-Council Certified Ethical Hacker.
- CEH EC-Council Certified Ethical Hacker Practical.

10. Duración:

Horas totales: 300 horas.

Distribución horas:
- Presencial: 300 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 están incluidos los siguientes exámenes de certificación oficial de EC-Council, o el que los sustituya actualizados al momento de su impartición:

- CND EC-Council Certified Network Defender.
- CEH EC-Council Certified Ethical Hacker.
- CEH EC-Council Certified Ethical Hacker Practical.

MÓDULOS FORMATIVOS

Módulo nº 1

Denominación: NETWORK DEFENDER SKILLS FOR NETWORK ADMINISTRATORS: EC-COUNCIL CERTIFIED NETWORK DEFENDER

Objetivo: Proteger, detectar y responder ante las amenazas de seguridad a las que está sometida una red corporativa, así como diseñar políticas de seguridad y programas de respuesta a incidentes que permitan anticipar y prevenir nuevas amenazas.

Duración: 105 horas

Contenidos teórico prácticos:

- Computer Network and Defense Fundamentals
- Network Security Threats, Vulnerabilities, and Attacks
- Network Security Controls, Protocols, and Devices
- Network Security Policy Design and Implementation
- Physical Security
- Host Security
- Secure Firewall Configuration and Management
- Secure IDS Configuration and Management
- Secure VPN Configuration and Management

- Wireless Network Defense
- Network Traffic Monitoring and Analysis
- Network Risk and Vulnerability Management
- Data Backup and Recovery
- Network Incident Response and Management

Módulo nº 2

Denominación: MASTERING HACKING TECHNOLOGIES I: EC COUNCIL CERTIFIED ETHICAL HACKER

Objetivo: Utilizar las herramientas y técnicas de piratería de manera legal y legítima para evaluar la situación de seguridad de uno o varios sistemas (sin importar su proveedor) e implementar mecanismos de protección ante futuros ataques.

Duración: 120 horas

Contenidos teórico prácticos:

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography

Módulo nº 3

Denominación: MASTERING HACKING TECHNOLOGIES II: EC COUNCIL CERTIFIED ETHICAL HACKER PRACTICAL.

Objetivo: Aplicar técnicas éticas de piratería, como identificación de vectores de amenazas, escaneo de redes, detección de SO, análisis de vulnerabilidad, piratería de sistemas, piratería de aplicaciones web, etc. para resolver los distintos desafíos que se plantean en una auditoría de seguridad utilizando un entorno de prácticas que replica casos de uso reales.

Duración: 75 horas

Contenidos teórico prácticos:

- Practical approach for the Mastery of Ethical Hacking Skills
- Security audit Challenges: Application of ethical hacking techniques such as threat vector identification, network scanning, OS detection, vulnerability analysis, system hacking, web app hacking, etc.
- Code of ethics
- Preparation for the CEH Practical Certification Exam