



Hacking Ético y Ciberseguridad

OBJETIVOS

Cuando hablamos de hacker a mucha gente le viene a la cabeza un personaje dedicado a causar estragos en sistemas informáticos con una gran habilidad para conseguir sus fines.

Veremos qué de cierto hay en esta percepción, así como los diferentes tipos de hackers existentes según sus características, motivaciones, conocimientos y vinculación con la seguridad.

DIRIGIDO A

Todas aquellas personas que tengan que deseen adquirir una base de conocimiento profundo en las amenazas y riesgos cibernéticos y cómo defenderse ante ellos desde el punto de vista empresarial

DURACIÓN, MODALIDAD Y PRECIO

60 Horas

Modalidad: elearning

Precio: 350 €

Ayudamos a tu empresa a **gestionar la bonificación** de este curso, contacte con nosotros 10 días antes del inicio del curso.

METODOLOGÍA

La modalidad de formación online es muy flexible ofreciendo al alumno la posibilidad de formación cuando y donde quiera, por lo que el ritmo de aprendizaje lo marca el alumno. Con acceso multiplataforma podrás asistir a clase desde cualquier dispositivo (Ordenador, Tablet, Móvil...)

A lo largo del curso se facilitará la documentación para el estudio, junto con ejercicios y actividades de evaluación continua.

Profesores y tutores: Un proceso de aprendizaje que estará tutorizado y guiado en todo momento por profesionales expertos en las diferentes áreas temáticas, que aportan una experiencia real y actualizada.

Desde la plataforma e-learning los alumnos podrán interactuar con profesores y alumnos, acceder a Ejercicios, casos prácticos y evaluación continua.

Foro, Chat, Video, tutorías, seguimiento, feedback...



PROGRAMA 1/2

1- Qué es un hacker, tipos de hackers:

- Introducción y objetivos.
- Concepto de hacker.
- Cómo actúa el hacker.
- Tipos de hacker.
- Daños que se pueden producir .
- Malware.

2- Técnicas y herramientas de intrusión utilizadas por los hackers:

- Introducción y objetivos.

INFORMACIÓN Y MATRÍCULA

formacion3@camarabadajoz.es



Contáctanos
924 23 46 00
Ext 4053



Hacking Ético y Ciberseguridad



PROGRAMA 2/2

- Laboratorio de pruebas .
- Herramientas de trabajo básico .
- Acciones iniciales.
- Escaneo de redes.
- Escaneo de puertos.
- Explotación de vulnerabilidades.

3- Hacking de sistemas, redes, web y dispositivos móviles:

- Introducción y objetivos.
- Sistemas y redes.
- Tecnologías WiFi.
- Servidores web.
- Tecnologías móviles.

4- Análisis y clasificación de vulnerabilidades:

- Introducción y objetivos.
- Conceptos previos.
- Causas de las vulnerabilidades.
- Clasificación de las vulnerabilidades.
- Análisis de las vulnerabilidades.

5- Hacking de sistemas y redes

- Introducción y objetivos.
- Tipos de ataques.
- Procedimientos de ataque.
- Resumen.



6- Hacking de redes inalámbricas: WiFi, WEP, WPS, WPA:

- Introducción y objetivos.
- Tecnologías WiFi.
- Laboratorio de pruebas.
- WEP.
- WPS.
- WPA.

7- Hacking de dispositivos móviles:

- Introducción y objetivos.
- Tecnologías móviles.
- Tipos de ataques.
- Herramientas.
- Medidas de seguridad.

8- Ingeniería social

- Introducción y objetivos.
- Fundamentos de la Ingeniería social.
- Tipos de ataques.
- Medidas de protección.

INFORMACIÓN Y MATRÍCULA
formacion3@camarabadajoz.es



Contáctanos
924 23 46 00
Ext 4053

www.camaramadrid.es

