

cursos

extensión  
universitaria



2018

universidad  
de león

## HACKING ÉTICO

05/02/2018 - 23/11/2018

### Información y matrícula

Universidad de León  
Unidad de Extensión Universitaria y Relaciones Institucionales.  
Av. Facultad de Veterinaria, 25. 24004 · LEÓN.  
Tel. 987 291 961 y 987 293 372 · Fax 987 291 963.  
e-mail: ulesci@unileon.es  
<http://www.unileon.es/extensionuniversitaria>

## HACKING ÉTICO

### DIRECTOR:

Luis Panizo Alonso. Profesor titular. Escuela de Ingenierías Industrial, Informática y Aeronáutica. Universidad de León.

### LUGAR:

Escuela de Ingenierías Industrial, Informática y Aeroespacial

### FECHAS:

05/02/2018 - 23/11/2018

### HORARIO:

Formación ONLINE. Plataforma abierta 24 horas. Período máximo para completar la formación: 3 meses.

### NÚMERO DE ALUMNOS:

Mínimo: 0 y Máximo: 150

### TASAS:

- Ordinaria: 485 €
- Alumnos ULE: 425 €
- Alumnos de otras universidades: 425 €
- Desempleados: 385 €

### DESTINATARIOS:

Este curso va dirigido tanto a personal técnico de seguridad como a responsables de ciberseguridad que ejercen su labor dentro de una organización. También para todos aquellos que tengan interés por la seguridad de la información como parte de su formación en la TIC. No requiere conocimientos específicos previos.

### CRÉDITOS DE LIBRE CONFIGURACIÓN:

6 créditos LEC - 3 créditos ECTS

### OBJETIVOS:

Son numerosas las amenazas que atentan a los sistemas informáticos, tanto en Internet (virus, troyanos, spywares, hackers, etc.) como de dentro de la organización. Para poder hacer frente a ello se necesitan determinadas herramientas y conocimientos para poder realizar una prevención y análisis a conciencia y metódico. En este curso, aprenderemos las principales herramientas utilizadas así como la metodología para realizar un análisis de ciberseguridad ordenado y detallado.

### PROGRAMA:

El contenido del curso está repartido en 11 módulos de aprendizaje:

1. Introducción al Hacking Ético. Términos, elementos de la seguridad de la información,

amenazas y clases de hackers.

2. Seguimiento de huellas y reconocimiento. Objetivos, conceptos y herramientas para el seguimiento de huellas.

3. Escaneo de redes. Conceptos, tipos de escaneo, trazado del mapa de red y descubrimiento de vulnerabilidades.

4. Enumeración. La enumeración de dispositivos, técnicas y herramientas.

5. Hackeo del sistema. Técnicas para hackear sistemas, escalar privilegios y mantener un acceso permanente.

6. Ingeniería social. Conceptos, técnicas y contramedidas ante ataques de ingeniería social.

7. Sniffers. Conceptos, tipos y contramedidas aplicables.

8. Hackeo de servidores web. Técnicas y metodología para hackear servidores Web.

9. Criptografía. Conceptos, técnicas para cifrar mensajes y ataques.

10. Hackeo de redes WIFI. Técnicas para hackear redes WIFI y contramedidas.

11. El test de Intrusión. Tipos de test de intrusión, fases y metodología.

### PROFESORADO:

Julio César Miguel Pérez. Director General Grupo CFI.