Escuela Superior de Ingeniería
Universidad de Cádiz

Avenida de la Universidad de Cádiz, nº 10
CP 11519, Puerto Real (Cádiz).

FICHA DE LA ASIGNATURA HACKING ÉTICO			
CARÁCTER:	**Prácticas Externas**	**LENGUA/S EN LA/S QUE SE IMPARTE:**	**Español**
ECTS:	**5**	**CUATRIMESTRE**	**2**
Asignatura de la MATERIA TECNOLOGÍAS EN SEGURIDAD			
PROFESORES QUE IMPARTEN LA ASIGNATURA			
Personal de la empresa Deloitte.			
COMPETENCIAS QUE SE ADQUIEREN: *(indicar código)*			
Comp. Básicas	**Comp. Generales**	**Comp. Específicas**	**Comp. Transversales**
CB6 CB7 CB8 CB9 CB10	**CG1 CG2 CG3 CG4 CG5**	**CE12 CE13**	

RESULTADOS DE APRENDIZAJE:
Identificar vulnerabilidades en redes, sistemas y aplicaciones, establecer los riesgos asociados a cada vulnerabilidad y definir las acciones correctivas que sean necesarias.
Realizar pruebas de penetración y auditorías de seguridad
Aplicar técnicas y herramientas para las pruebas de penetración en sistemas informáticos

CONTENIDOS:
1. Footprinting
– Introducción
– Entidades
– Buscadores
– El sitio web
– Otras fuentes
– Metadatos

2. Fingerprinting
– DNS
– ICMP
– Traceroute
– Ping
– Banner grabbing
– Nmap
– Zmap
– SMTP
– VoIP
– RPC
– SNMP
– Firewalls

3. Vulnerabilidades
– Publicaciones
– Problemática
– Categorías
– Acciones
– Gestión
– Introducción a las herramientas

4. Metasploit
– Introducción
– Herramientas
– msfconsole
– Conexión a BBDD
– Uso de BBDD
– Exploits para servidores
– Exploits para clientes
– Postexplotación
– Evasión de antivirus
– Automatización de tareas

5. Ataques a credenciales
– Introducción
– Consecuencias
– Escenarios de exposición
– Errores más comunes
– Credenciales seguras
– Almacenamiento
– Credenciales en GNU/Linux
– Credenciales en Windows
– Pass the Hash (PtH)
– Cisco
– Juniper

6. Malware
– Definición
– Tipos de malware
– Ejemplo: Zeus
– Clasificación de muestras
– Tipos de análisis
– Análisis automatizado
– Cuckoo sandbox
– Análisis online

7. Seguridad física de los equipos
– Introducción
– Protección del hardware
– Acceso físico
– Desastres naturales
– Alteraciones del entorno
– Protección física del entorno
– Soportes no electrónicos
– Gadgets

8. Seguridad en aplicaciones web
– Metodología OWASP 2013
– Inyecciones
– Autenticaciones y gestión de sesiones
– Cross Site Scripting (XSS)
– Referencias inseguras a objetos
– Configuraciones de seguridad incorrectas

– Exposición de datos sensibles
– Controles de acceso
– Cross-site Request Forgery (CSRF)
– Componentes con vulnerabilidades conocidas
– Redirecciones y encaminamientos no validados

OBSERVACIONES / REQUISITOS PREVIOS:
Algunas de las actividades podrán realizarse en inglés.

El sistema de evaluación consiste en un examen final de certificación que se realizará al final del curso. Dicho examen final será el examen de certificación DCEHA (Deloitte Certified Ethical Hacking Associate) en el que el alumno debe contestar correctamente a una batería de 50 preguntas de distinto tipo. En el examen se pueden encontrar preguntas de respuesta múltiple, única, verdadero/falso y desarrollo. Para aprobar la asignatura se necesitara un 50% de dicho examen final. Para obtener la certificación el alumno debe de obtener un 70% en dicho examen final. El certificado se emitirá, en su caso, junto al título del Máster.

	Id de la Actividad Formativa	Nº de horas	Presencialidad (%)
ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:	Clases de teórico-prácticas	25	100%
	Actividades académicas no presenciales	96	0%
	Evaluación	4	100%

METODOLOGÍAS DOCENTES:
Lección magistral expositiva
Resolución de problemas y casos prácticos
Prácticas de laboratorio

SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:

Denominación Sistema Evaluación	Ponderación Mínima	Ponderación Máxima
Prácticas de laboratorio	0%	70%
Pruebas escritas u orales	30%	100%

BIBLIOGRAFÍA RECOMENDADA:

a. Material teórico:
    i. Libro oficial de la certificación profesional D-CEHA 101 Hacking Ético