MASTER EN HACKING ÉTICO



Máster Hacking Ético – Titulación Universitaria

1. Descripción:

IDO Business School (Iberoamericana de Desarrollo Organizacional), en colaboración con la **Universidad Internacional Isabel I de España**, han puesto en marcha para este periodo 2015/16 el ***Master Hacking Ético*** con la visión de brindar al estudiante los conocimientos teóricos-prácticos que conducen a desarrollar las competencias necesarias para ejecutar un proceso controlado de Hacking, a fin de conocer las vulnerabilidades y aplicar las medidas preventivas, así como también, usar de manera práctica las diferentes herramientas adecuadas para desarrollar un proceso de Ethical Hacking. De igual forma, el objetivo es mostrar cómo detectar y corregir vulnerabilidades de seguridad en una red, entender los conceptos y tecnologías utilizadas en la creación de páginas web, identificar las vulnerabilidades y proponer las mejoras, comprender los problemas de seguridad asociadas a las redes inalámbricas y cómo llevar a cabo pruebas de penetración para encontrar y atacar las vulnerabilidades, obtener conocimientos para analizar los códigos maliciosos con el fin de ampliar el alcance y la profundidad de la comprensión de las amenazas contra una organización, en la misma línea, ayudar a preparar los mecanismos de defensa y a la localización de amenazas, y definir el impacto que un incidente podría tener en el negocio de la compañía.

2. Requisitos de conocimientos para cursar el Master

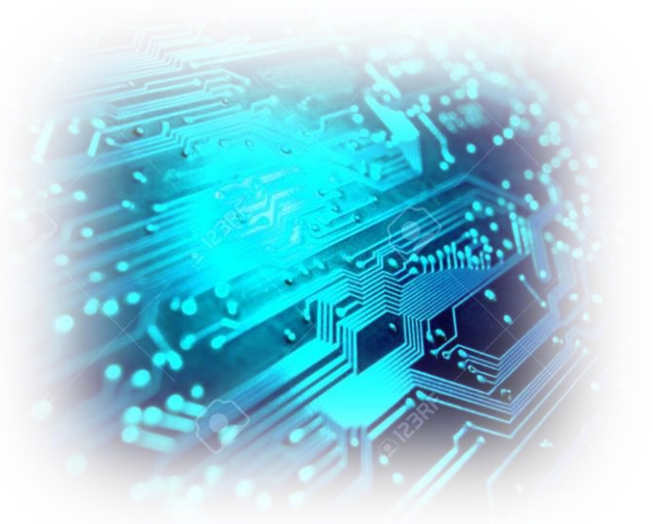


2.1. Obligatorios

1. Conocimientos básicos de administración de redes y sistemas operativos. (linux y windows).
2. Conocimientos básicos a nivel de Redes.
3. Conocimientos básicos de Servicios y Sistemas.
4. Manejo de máquinas virtuales. (Virtualbox o Vmware).
5. Conocimientos básicos de programación en cualquier lenguaje.
6. Conocimientos básicos de infraestructura Web.

2.2. Deseables

- Deseable conocimientos básicos de Lenguaje SQL, C, Java, Python., php .
- Deseable conocimiento básico de Ensamblador
- Deseable conocimiento básico de Android



3. Dirigido a

- Ingenieros de sistemas / TI.
- Ingenieros electrónicos.
- Ingenieros de telecomunicaciones.
- Profesionales con experiencia en seguridad de la información.
- Auditores de seguridad informática y sistemas.
- Personal de seguridad perimetral y administradores de red.

4. Temario:

Módulo 0. (Modulo Introductorio). Entorno web, Servidor Apache, lenguajes de implementación y bases de datos.

1. Teoría, Instalación y configuración de servidores Web (Apache)
1.1. Funcionamiento de Servidores Web
1.2. Arquitectura de Servidores Web
1.3. Tipos de Servidores Web
1.4. Seguridad y autentificación
1.5. Instalación y Configuración Servidor Web
1.5.1. Servidor HTTP Apache (Xampp)
1.5.2. Configuración del Servidor Web Apache
1.5.2.1. Directivas de Funcionamiento
1.5.2.2. Parámetros de Gestión de recursos
1.5.2.3. Directivas VirtualHost y NameVirtualHost
1.5.2.4. Directivas de Seguridad
1.5.3. Internet Información Services (IIS)



2. HTML
2.1. Hiperenlaces
2.2. Imágenes
2.3. Tablas
2.4. Formularios
2.5. Flash
2.6. Capas (DIV)
2.7. Lenguajes de Script
2.8. XML
2.9. HTML dinámico
3. Programación Web
4. BD MySQL
4.1. ¿Que es una BD.?
4.2. Objetos de la BD
4.3. Definiciones y Conceptos de BD
4.4. Cliente MySQL (sqlyog)
4.5. Creación de BD, Tablas y campos
5. Lenguaje SQL
5.1. Introducción
5.2. Clausulas
5.3. Operadores Lógicos
5.4. Operadores de comparación

5.5. Funciones de Agregado
5.6. Consultas de Selección
5.7. Criterios de Selección
5.8. Agrupamiento de Registros
5.9. Consultas de Acción
5.10. Consultas de Unión Internas
5.11. Consultas de Unión Externas

6. Php (introducción y acceso a bases de datos mediante SQL)

6.1. Introducción y conceptos básicos de programación.
6.1.1. ¿Que es un programa?
6.1.2. Tipos de datos
6.1.3. Variables
6.1.4. Constantes
6.1.5. Estructuras de Control
6.1.5.1. Estructura Condicional
6.1.5.2. Estructura Condicional Múltiple
6.1.5.3. Estructura de Repetición (Bucles)
6.1.5.4. Estructuras Anidadas
6.2. Lenguaje PHP
6.2.1. Bases de la sintaxis
6.2.2. Tipos de Datos
6.2.3. Variables
6.2.4. Constantes
6.2.5. Estructuras de Control Condicional
6.2.5.1. IF ELSE
6.2.5.2. SWITCH
6.2.6. Estructuras de Repetición (Bucles)
6.2.6.1. WHILE
6.2.6.2. DO WHILE
6.2.6.3. FOR
6.2.7. Funcniones
6.3. Acceso a bases de datos
6.3.1. Conexión a BD
6.3.2. Funciones de PHP y MYSQL
6.4. Ejemplos HTML + PHP + SQL



Teoría, Instalación y configuración de servidores Web (Apache)

La duración de este módulo es de 1 (un) mes y tiene la opción de acreditarse mediante la presentación de un examen.

Módulo 1. Introducción Hacking Ético

1. Introducción
    a. Definiciones y términos
2. Adopción de pautas de seguridad informática
3. Ataques y contramedidas en sistemas personales y servidores
4. Seguridad en la red corporativa + Servidores de Acceso remoto

Módulo 2. Hacking Web

1. Presentación general, Introducción y demostraciones reales
2. Detección y explotación de vulnerabilidades Web (Protocolo HTTP, XSS,CSRF, RFI, LFI, LFD, Path transversal, SQL Injection, etc…).
3. Software para evaluación y explotación de vulnerabilidades Web
4. Metodología
5. Practica final. Encontrar vulnerabilidades en aplicaciones web de un entorno controlado y explotarlas.

Módulo 3. Hacking a nivel de red

1. Introducción al hacking a nivel de red
    a. Definiciones y términos
    b. Tipos
    c. Limitaciones
    d. Informes
2. Reconocimiento
    a. Pasivo
    b. Activo
    c. Técnicas
    d. Herramientas
3. Escaneo
    a. Introducción
    b. Trazas de Red
    c. Escaneo de Puertos



    d. Detección de servicios y sistemas
    e. Generación de Paquetes
    f. Escaneo de Vulenrabilidades
    g. Herramientas
4. Explotación
    a. Introducción
    b. Categorías
    c. Framework Explotación
    d. Herramientas
    e. Post- Explotación
5. Practica final. Encontrar vulnerabilidades en servicios de un entorno controlado y explotarlas.



Módulo 4. Desarrollo de exploits y búsqueda de vulnerabilidades en software

1. Lenguaje Ensamblador.
2. Manejo de debuggers.
3. Buffer overflows.
4. SEH overflows.
5. Desarrollo de distintos tipos de exploits.
6. Soluciones a problemas en el desarrollo de exploits.
7. Fuzzing. Teoría.
8. Fuzzing de protocolos.
9. Fuzzing de file format.
10. Practica final. Encontrar vulnerabilidades en una aplicación y desarrollar el exploit.

Módulo 5. Análisis de vulnerabilidades en dispositivos móviles.

1. Introducción
    a. Infraestructura
2. Desempaquetado de la aplicación
3. Análisis Estático
    a. Técnicas y Herramientas
4. Análisis Dinámico
    a. Técnicas y Herramientas
5. Practica final. Analizar aplicación Android.

Módulo 6. Reversing malware



1. Introducción
2. Análisis Estático
    a. Técnicas y Herramientas
3. Análisis Dinámico
    a. Técnicas y Herramientas
4. Funcionalidades Malware
5. Anti Ingeniería Inversa
6. Practica final. Crear Prueba de concepto de Málware. Analizar Prueba de concepto Malware desarrollada.

Módulo 7. Redes Inhalámbricas

1. Introducción
2. Descubrimiento y esnifado de Redes
3. Crypto-ataques
4. Ataques a Cliente

Módulo 8. Legislación y normas sobre seguridad

1. Legalidad vigente e implicación en las implantaciones tecnológicas.
2. Legislación Nacional
3. Legislación Europea

4.1. Metodología E-learning

Presentación del Director del Master

1. Presentación general del módulo
2. E-book o temario)
3. Master Classes.
4. Topics Discussions
5. Análisis de casos prácticos
6. Virtual Conferences
7. Self- assessments
8. Exámenes



4.2. Horario: Modalidad Online

La duración del ***Máster Hacking Ético*** será de un total de 18 horas lectivas de clases virtuales repartidas en 9 módulos (9 meses) y 2 horas de tutoriales para proyecto fin de Master, de igual manera se contemplan 1480 horas de trabajo que hacen un total de 1500 horas y 60 créditos ECTS.

Las clases se impartirán **de manera virtual de acuerdo a la disponibilidad de los estudiantes y profesores** de forma que sean compatibles con otras ocupaciones como otros cursos o trabajos.

Posteriormente a la finalización del Master será necesaria la presentación de un Proyecto Final.

El curso dará comienzo en Octubre y tendrá matriculación continua mensual sujeta a disponibilidad de plazas, las gestiones operativas se desarrollaran desde nuestra sede c/ Manuel Tovar 25, 1º. 28034 – Madrid.



Distribución General del Plan de Estudios en Créditos ECTS y Horas de Trabajo- Modalidad Online

		Horas de clase	Horas de trabajo	Créditos ects
Entorno Web, Servidor Apache, Lenguajes de Implementación y Bases de Datos		**2**	**123**	**5**
Introducción Hacking Ético		**2**	**123**	**5**
Hacking Web		**2**	**148**	**6**
Hacking a Nivel de Red		**2**	**149**	**6**
Desarrollo de Exploits y Búsqueda de Vulnerabilidades en Software		**2**	**149**	**6**
Análisis de Vulnerabilidades en Dispositivos Móviles		**2**	**123**	**5**
Reversing Malware		**2**	**123**	**5**
Redes Inhalámbricas		**2**	**123**	**5**
Legislación y Normas sobre Seguridad		**2**	**123**	**5**
Proyecto Fin de Master		**2**	**296**	**12**
1 crédito ects= 25 horas	**Total**	**20**	**1480**	**60**

1.500 horas Totales

- **Coste:**

- Precio: 4.000 €

2.2. Horario: Modalidad Semipresencial

La duración del ***Máster Hacking Ético*** será de un total de 76 horas lectivas de clases presenciales repartidas en 09 módulos (9 meses) y 4 horas de tutoriales para proyecto fin de Master, de igual manera se contemplan 1420 horas de trabajo que hacen un total de 1.500 horas y 60 créditos ECTS.

Las clases se impartirán los sábados (uno al mes) de **10:00h a 14:00h y de 15:00h a 17:00h** de forma que sean compatibles con otras ocupaciones como otros cursos o trabajos.

Posteriormente a la finalización de la especialización será necesaria la presentación de un Proyecto Final.

El curso dará comienzo en Noviembre y tendrá matriculación continua mensual sujeta a disponibilidad de plazas, se realizará en la Sede Central de IDO Business School ubicada en c/ Manuel Tovar 25, 1º. 28034 – Madrid.



Distribución General del Plan de Estudios en Créditos ECTS y Horas de Trabajo- Modalidad Semipresencial o Blended

		Horas de clase	Horas de trabajo	Créditos ects
Entorno Web, Servidor Apache, Lenguajes de Implementación y Bases de Datos		**8**	**117**	**5**
Introducción Hacking Ético		**8**	**117**	**5**
Hacking Web		**8**	**142**	**6**
Hacking a Nivel de Red		**8**	**143**	**6**
Desarrollo de Exploits y Búsqueda de Vulnerabilidades en Software		**8**	**143**	**6**
Análisis de Vulnerabilidades en Dispositivos Móviles		**8**	**117**	**5**
Reversing Malware		**8**	**117**	**5**
Redes Inhalámbricas		**8**	**117**	**5**
Legislación y Normas sobre Seguridad		**8**	**117**	**5**
Proyecto Fin de Master		**4**	**294**	**12**
1 crédito ects= 25 horas	**Total**	**80**	**1420**	**60**

1.500 horas Totales

- **Coste:**

- Precio base: 5.500 €