ESIBE ESCUELA IBEROAMERICANA DE POSTGRADO

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

FORMACIÓN ONLINE

Máster Hackers + Titulación Universitaria

ESIBE
Formación
Online

ESIBE se basa en una metodología completamente a la vanguardia educativa

SOBRE ESIBE

ESIBE nace del afán por crear un punto de encuentro entre Europa, en conc Latinoamérica.

A raíz de este reto, desarrollamos una nueva oferta formativa, marcada por en línea y unos contenidos de gran calidad que te permitirán obtener los cor necesitas para especializarte en tu campo.

Además, hemos diseñado para ti un campus con la última tecnología en sist que recoge todos los materiales que te serán útiles en tu adquisición de nue

Las Titulaciones acreditadas por ESIBE pueden certificarse con la Apostilla (Certificación Oficial de Carácter Internacional que le da validez a las Titulac en más de 160 países de todo el mundo).
Hemos reinventado la formación online, de manera que nuestro alumnado p superando de forma flexible cada una de las acciones formativas con las qu todas las áreas del saber y, con la garantía de aprender las habilidades y he realmente demandados en el mercado laboral.

Nuestro centro forma parte del grupo educativo Euroinnova, líder en el secto gracias a su contenido de calidad e innovadora metodología con 20 años de ESIBE cuenta con el respaldo de INESEM, reconocida escuela de negocios Euroinnova, centro formativo con más de 300.000 alumnos de los cinco con Además, ESIBE imparte formaciones avaladas por Universidades de prestig como Universidad Nebrija, Universidad Europea Miguel de Cervantes o Univ E-Campus.

No somos solo una escuela, somos el lugar ideal donde formarte.

Máster Hackers + Titulación Universitaria

DURACIÓN:
1.500 horas

MODALIDAD:
Online

PRECIO:
A consultar
(Sujeto a política de becas)

CRÉDITOS:
8 ECTS

CENTRO DE FORMACIÓN:

ESIBE
Escuela Iberoamericana de Postgrado

Titulación

Titulación Múltiple: - Titulación de Master Hackers 1500 horas expedida por EUROINNOVA INTERNATIONAL EDUCATION, miembro de la AEEN (Asociación Española de Escuelas de Negocios) y reconocido con la excelenc educación online por QS World University Rankings - Titulación Universitaria en Consultor en Seguridad Informát Hacking con 8 Créditos Universitarios ECTS. baremable en bolsas de trabajo y concursos oposición de la Administ Una vez finalizada la formación, el alumnado recibirá por parte de ESIBE vía correo postal, la titulación que acredit con éxito todas las pruebas de conocimientos propuestas.
Esta titulación incluirá el nombre del curso/máster, su duración, el nombre y DNI, el nivel de aprovechamiento que superación de las pruebas propuestas, las firmas del profesor y Director del centro, y los sellos de las instituciones q formación recibida (Euroinnova Formación, Instituto Europeo de Estudios Empresariales y Comisión Internacional a Distancia de la UNESCO)

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

EXPIDE LA SIGUIENTE TITULACIÓN

NOMBRE DEL ALUMNO/A

con D.N.I. XXXXXXXXX que presta sus servicios en la empresa LABORATORIO ELECTROTECNICO, S.C.C.L. con C.I.F. XXXXXXXXX ha cursado la acción formativa

Nombre de la Acción Formativa

perteneciente al Plan de Formación Continua impartido por EUROINNOVA con Nº Exp.XXXXXXXXX dentro del marco de la Fundación Estatal para la Formación en el empleo dirigido a trabajadores de todos los sectores en la convocatoria del 20XX
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX/XXXX-XXXX-XXXXXX

Con un nivel de aprovechamiento ALTO

Y para que conste expido la presente TITULACIÓN en
Granada, a (día) de (mes) del (año)

La Dirección General
JESÚS MORENO HIDALGO

Sello

Firma del Alumno/a
NOMBRE DEL ALUMNO

Descripción

Con el presente Master Hackers recibirá una formación especializada en el campo del hacking. El hacking es altame realizar auditorias de seguridad, comprometiendo y comprobando la seguridad de los sistemas informáticos, ya sean páginas webs o de redes de área local. Con el presente Master Hackers recibirá la formación necesaria para poder ab aspectos del hacking, ya sea mediante la búsqueda de exploit o usando herramientas especializadas para tal fin...

Objetivos

- Conocer el Ethical Hacking.
- Aprender a realizar hacking wifi.
- Aprender a desarrollar exploits y a buscar vulnerabilidades.
- Conocer el Phishing y como los hackers lo emplean.
- Conocer el sistema de información UNE-ISO/IEC 27001:2017.
- Conocer el Big Data.

A quién va dirigido

El presente máster está dirigido a todos los profesionales del mundo de la informática que quieran ampliar sus cono formarse en un mercado en continua evolución. Por lo que la formación adecuada y actualizada es indispensable pa mercado.

Para qué te prepara

El presente Master Hackers le proporcionará los conocimientos necesarios para destacar en el mundo de la informát especialmente en cuanto al hacking se refiere. Aprenderá y conocerá el ethical hacking, así como a realizar auditori a redes inalámbricas y conocer el desarrollo de exploits.

Salidas Laborales

Los conocimientos adquiridos en esta formación te permiten aplicar tu aprendizaje en consultorías, así como en dep informática de empresas de todos los sectores. Asimismo, te capacitan para desarrollar tu labor como jefe de proyec en las áreas de desarrollo y programación, ingeniería de software e ingeniería informática.

Materiales Didácticos

El alumn@ recibe un email con las Claves de Acceso al CAMPUS VIRTUAL en el que va a poder acced el contenido didáctico, así como las evaluaciones, vídeos explicativos, etc. así como a contactar con el t línea quien le va a ir resolviendo cualquier consulta o duda que le vaya surgiendo tanto por email, chat, telefono, etc.

Formas de Pago

- Tarjeta,
- Paypal

Otros: Otras formas de pago adaptadas a cada pais a traves de la plataforma de pago Ebanx.

Llama al teléfono (+34) 958 99 19 19 e infórmate de los pagos a plazos sin intereses que hay disponibles

Financiación

En ESIBE, tu aprendizaje es lo más importante. Por eso, hemos desarrollado contenidos, así como una innovadora en sistemas e-Learning con la que trabajarás para adquirir tus nuevos conocimientos con el nuestro claustro especializado en la materia. Te proporcionamos nociones imprescindibles para el desa actividad de tu ámbito.
Nuestro objetivo es convertirte en un profesional altamente cualificado, capaz de desempeñar las tarea puesto de responsabilidad en el sector.

Nuestra Metodología

En ESIBE, tu aprendizaje es lo más importante. Por eso, hemos desarrollado contenidos, así como una plataforma innovadora e sistemas e-Learning con la que trabajarás para adquirir tus nuevos conocimientos con el respaldo de nuestro claustro especializado en la materia. Te proporcionamos nociones imprescindibles para el desarrollo de la actividad de tu ámbito. Nuestro objetivo es convertirte en un profesional altamente cualificado, capaz de desempeñar las tareas propias de un pue de responsabilidad en el sector.

Redes Sociales

Síguenos en nuestras redes sociales y pasa a formar parte de nuest gran comunidad educativa, donde podrás participar en foros de opinión, acceder a contenido de interés, compartir material didácti e interactuar con otros/as alumnos/as, ex alumnos/as y profesores/ Además, te enterarás antes que nadie de todas las promociones y becas mediante nuestras publicaciones, así como también podrás contactar directamente para obtener información o resolver tus dudas.

Por qué estudiar en ESIBE

Formación en Linea

Organiza tu propio tiempo.

Apostilla de la Haya

Certifica tu titulación en países extranjeros.

Calidad Europea

Formacion especializada.

Contenido Actualizado

Revisamos de forma continua nuestro temario.

Campus Virtual

Plataforma con los últimos desarrollos del sector e-Learning.

Amplia Oferta Formativa

Encuentra la formación que se adapta a ti.

Valores ESIBE

Compromiso

En ESIBE, nuestros alumnos son lo más importante y, comiences tu formación con nosotros estaremos a tu la lograr tu máximo desarrollo profesional y personal.

Excelencia

Nuestros contenidos son de máxima calidad, ofreciénd oportunidad única de formación y crecimiento que te alcanzar puestos de gran responsabilidad en tu sector.

Unidad

Juntos, somos mucho más fuertes. Detrás de ESIBE ha equipo multidisciplinar que suma sus fuerzas para con sinergias que beneficien de forma directa a nuestros al

Adaptabilidad

Queremos facilitarte tu aprendizaje, por esto, tú marca propio ritmo.

Innovacion

ESIBE se sustenta en una cultura con un carácter innov diferenciado, promoviendo el desarrollo y uso de nuev tecnologías para el estudio y aprendizaje.

Flexibilidad

Tú tiempo es valioso para nosotros y, con el fin de que compaginar tu formación, te proporcionamos la flexibi necesitas, pudiendo realizar tu formación en cualquier del día.

Acreditaciones y Reconocimientos

Temario

PARTE 1. ETHICAL HACKING

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LOS ATAQUES Y AL HACKING ÉTICO

1.Introducción a la seguridad informática
2.El hacking ético
3.La importancia del conocimiento del enemigo
4.Seleccionar a la víctima
5.El ataque informático
6.Acceso a los sistemas y su seguridad
7.Análisis del ataque y seguridad

UNIDAD DIDÁCTICA 2. SOCIAL ENGINEERING

1.Introducción e historia del Social Engineering
2.La importancia de la Ingeniería social
3.Defensa ante la Ingeniería social

UNIDAD DIDÁCTICA 3. LOS FALLOS FÍSICOS EN EL ETHICAL HACKING Y LAS PRUEBAS DEL ATAQUE

1.Introducción
2.Ataque de Acceso físico directo al ordenador
3.El hacking ético
4.Lectura de logs de acceso y recopilación de información

UNIDAD DIDÁCTICA 4. LA SEGURIDAD EN LA RED INFORMÁTICA

1.Introducción a la seguridad en redes
2.Protocolo TCP/IP

3.IPv6
4.Herramientas prácticas para el análisis del tráfico en la red
5.Ataques Sniffing
6.Ataques DoS y DDoS
7.Ataques Robo de sesión TCP (HIJACKING) y Spoofing de IP
8.Ataques Man In The Middle (MITM).
9.Seguridad Wi-Fi
10.IP over DNS
11.La telefonía IP

UNIDAD DIDÁCTICA 5. LOS FALLOS EN LOS SISTEMAS OPERATIVOS Y WEB

1.Usuarios, grupos y permisos
2.Contraseñas
3.Virtualización de sistemas operativos
4.Procesos del sistema operativo
5.El arranque
6.Hibernación
7.Las RPC
8.Logs, actualizaciones y copias de seguridad
9.Tecnología WEB Cliente - Servidor
10.Seguridad WEB
11.SQL Injection
12.Seguridad CAPTCHA
13.Seguridad Akismet
14.Consejos de seguridad WEB

UNIDAD DIDÁCTICA 6. ASPECTOS INTRODUCTORIOS DEL CLOUD COMPUTING

1.Orígenes del cloud computing
2.Qué es cloud computing
1.- Definición de cloud computing
3.Características del cloud computing
4.La nube y los negocios
1.- Beneficios específicos
5.Modelos básicos en la nube

UNIDAD DIDÁCTICA 7. CONCEPTOS AVANZADOS Y ALTA SEGURIDAD DE CLOUD COMPUTING

1.Interoperabilidad en la nube
1.- Recomendaciones para garantizar la interoperabilidad en la nube
2.Centro de procesamiento de datos y operaciones
3.Cifrado y gestión de claves
4.Gestión de identidades

UNIDAD DIDÁCTICA 8. SEGURIDAD, AUDITORÍA Y CUMPLIMIENTO EN LA NUBE

1.Introducción
2.Gestión de riesgos en el negocio
1.- Recomendaciones para el gobierno
2.- Recomendaciones para una correcta gestión de riesgos
3.Cuestiones legales básicas. eDiscovery
4.Las auditorías de seguridad y calidad en cloud computing
5.El ciclo de vida de la información
1.- Recomendaciones sobre seguridad en el ciclo de vida de la información

UNIDAD DIDÁCTICA 9. CARACTERÍSTICAS DE SEGURIDAD EN LA PUBLICACIÓN DE PÁGINAS WEB

1.Seguridad en distintos sistemas de archivos.
1.- Sistema operativo Linux.
2.- Sistema operativo Windows.
3.- Otros sistemas operativos.
2.Permisos de acceso.
1.- Tipos de accesos
2.- Elección del tipo de acceso
3.- Implementación de accesos
3.Órdenes de creación, modificación y borrado.
1.- Descripción de órdenes en distintos sistemas
2.- Implementación y comprobación de las distintas órdenes.

UNIDAD DIDÁCTICA 10. PRUEBAS Y VERIFICACIÓN DE PÁGINAS WEB

1.Técnicas de verificación.
1.- Verificar en base a criterios de calidad.
2.- Verificar en base a criterios de usabilidad.
2.Herramientas de depuración para distintos navegadores.
1.- Herramientas para Mozilla.
2.- Herramientas para Internet Explorer.
3.- Herramientas para Opera.
4.- Creación y utilización de funciones de depuración.
5.- Otras herramientas.
3.Navegadores: tipos y «plug-ins».
1.- Descripción de complementos.
2.- Complementos para imágenes.
3.- Complementos para música.
4.- Complementos para vídeo.
5.- Complementos para contenidos.
6.- Máquinas virtuales.

UNIDAD DIDÁCTICA 11. LOS FALLOS DE APLICACIÓN

1.Introducción en los fallos de aplicación

2.Los conceptos de código ensamblador y su seguridad y estabilidad
3.La mejora y el concepto de shellcodes
4.Buffer overflow
5.Fallos de seguridad en Windows

PARTE 2. HACKING WIFI

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN: HACKING

1.Introducción
2.Historia del hacking
3.Tipos de hacking
4.Tipos de hacker

UNIDAD DIDÁCTICA 2. HARDWARE NECESARIO PREVIO AL HACK WIFI

1.Introducción
2.Hardware

UNIDAD DIDÁCTICA 3. TIPOS DE REDES WIFI Y CIFRADOS

1.Introducción
2.Estándares wifi
3.Cifrados wifi

UNIDAD DIDÁCTICA 4. DISTRIBUCIONES LINUX PARA EL HACK WIFI

1.Introducción
2.Sistemas operativos linux
3.Sistemas operativos utilizados en hacking wifi
1.- Kali linux
2.- Parrot
3.- Wifislax

UNIDAD DIDÁCTICA 5. SOFTWARE UTILIZADO PARA EL HACK WIFI

1.Introducción
2.Herramientas de wifislax
3.Aircrack
4.Cain & Abel

UNIDAD DIDÁCTICA 6. PROCESO PRÁCTICO DE HACKEO DE RED WIFI

1.Introducción al caso práctico
2.Desarrollo del caso práctico
3.Resultados del caso práctico

UNIDAD DIDÁCTICA 7. CONSEJOS DE SEGURIDAD

1.Introducción
2.Recomendaciones

UNIDAD DIDÁCTICA 8. LEGISLACIÓN

1.Introducción

2.Leyes anti piratería

PARTE 3. DESAROLLO DE EXPLOITS Y BÚSQUEDA VULNERABILIDADES

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN EXPLOITS

1.Historia de los exploits
2.Definición de exploit y cómo funciona
3.Tipología de exploits
4.Uso común de los exploits y medidas de protección

UNIDAD DIDÁCTICA 2. METAEXPLOIT Y CREACIÓN DE EXPLOIT

1.Introducción a metaexploit
2.Creando nuestro primer exploit
3.Post-Explotación
4.Meterpreter

UNIDAD DIDÁCTICA 3. TIPOS DE EXPLOITS

1.Code injection
2.Cross-site request forgery
3.Cross-site scripting
4.SQL injection
5.Buffer overflow
6.Heap overflow
7.Stack buffer overflow
8.Integer overflow
9.Return-to-libc attack
10.Format string attack

UNIDAD DIDÁCTICA 4. UTILIZANDO ARMITAGE

1.Introducción Armitage
2.Atacando con Armitage
3.Post-Explotación Armitage
4.Facilidades Armitage

UNIDAD DIDÁCTICA 5. INTRODUCCIÓN VULNERABILIDADES

1.Qué es una vulnerabilidad
2.Vulnerabilidad vs Amenaza
3.Análisis de vulnerabilidades
4.Evitar vulnerabilidades

UNIDAD DIDÁCTICA 6. TIPOS DE VULNERABILIDADES

1.Gravedad de las vulnerabilidades
2.Vulnerabilidades del sistema

3.Vulnerabilidades web

UNIDAD DIDÁCTICA 7. DESCUBRIR VULNERABILIDADES

1.Utilizar metasploit para descubrir vulnerabilidades
2.Prueba de penetración
3.Herramientas para escanear vulnerabilidades

UNIDAD DIDÁCTICA 8. UTILIZANDO VULNERABILIDADES JUNTO A EXPLOITS

1.Vulnerabilidades en Linux
2.Vulnerabilidades en Windows
3.Vulnerabilidades en Android

UNIDAD DIDÁCTICA 9. RECOMENDACIONES FRENTE A EXPLOITS Y VULNERABILIDADES

1.Recomendaciones de seguridad frente a exploits
2.Recomendaciones de seguridad frente a vulnerabilidades
3.Herramientas de seguridad

UNIDAD DIDÁCTICA 10. CASO PRÁCTICO

1.Introducción
2.Objetivos
3.Realización

PARTE 4. INGENIERIA SOCIAL, PHISHING Y HACK

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LA INGENIERÍA SOCIAL

1.Definición ingeniería social
2.Como evitar la ingeniería
3.Formación de empleados
4.Victimas mas frecuentes de los ataques

UNIDAD DIDÁCTICA 2. RECOPILAR INFORMACIÓN

1.OSINT
2.Doxing
3.Metadatos
4.Buscar información en la web

UNIDAD DIDÁCTICA 3. HERRAMIENTAS INGENIERÍA SOCIAL

1.FOCA
2.MALTEGO
3.GOOGLE HACKING
4.THEHARVESTER
5.SET

UNIDAD DIDÁCTICA 4. TECNICAS DE ATAQUES

1.Clasificación de ataques
2.Scareware
3.Utilizar dominios con erratas

4.USB olvidado y Piggyback
5.Caso practico

UNIDAD DIDÁCTICA 5. PREVENCION DE ATAQUES

1.Informar de los ataque comunes
2.Comprobar la seguridad antes ataques
3.Planear un sistema de contigencia
4.Lo que nunca te van a pedir
5.Pensar antes de actuar

UNIDAD DIDÁCTICA 6. INTRODUCCION PHISHING

1.¿Que es el phishing?
2.Historia del phishing
3.Técnicas de phishing
4.Identificar un email falso y que hacer con el

UNIDAD DIDÁCTICA 7. PHISHING

1.Como funciona el phishing
2.Anti-phishing
3.Objetivos del phishing
4.Casos prácticos ataques

UNIDAD DIDÁCTICA 8. MAN IN THE MIDDLE

1.Introduccion Man In The Middle
2.Protegernos de ataques Man In The Middle
3.Lugares comunes ataques Man In The Middle
4.Caso practico

UNIDAD DIDÁCTICA 9. HACKING WEB

1.Descubriendo subdominios
2.Escaneando servidores web
3.Escaneando huella digital servidor web
4.Hackeando un sitio Wordpress con WPScan
5.Securizar nuestro sitio web

PARTE 5. SISTEMA DE GESTIÓN DE SEGURIDAD DI INFORMACIÓN UNE-ISO/IEC 27001:2017

UNIDAD DIDÁCTICA 1. CIBERSEGURIDAD Y SOCIEDAD DE LA INFORMACIÓN

1.¿Qué es la ciberseguridad?
2.La sociedad de la información
3.Diseño, desarrollo e implantación
4.Factores de éxito en la seguridad de la información
5.Soluciones de Ciberseguridad y Ciberinteligencia CCN-CERT

UNIDAD DIDÁCTICA 2. NORMATIVA ESENCIAL SOBRE EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DI INFORMACIÓN (SGSI)

1.Estándares y Normas Internacionales sobre los SGSI. ISO 27001 e ISO 27002
2.Legislación: Leyes aplicables a los SGSI

UNIDAD DIDÁCTICA 3. INTRODUCCIÓN A LA NIS2

1.Historia y evolución de la NIS2
2.Objetivos y alcance de la NIS2
3.Diferencias entre NIS1 y NIS2
4.Sectores críticos afectados por la NIS2

UNIDAD DIDÁCTICA 4. POLÍTICA DE SEGURIDAD: ANÁLISIS Y GESTIÓN DE RIESGOS

1.Plan de implantación del SGSI
2.Análisis de riesgos
3.Gestión de riesgos

UNIDAD DIDÁCTICA 5. IMPLANTACIÓN DEL SISTEMA DE SEGURIDAD EN LA ORGANIZACIÓN

1.Contexto
2.Liderazgo
3.Planificación
4.Soporte 213

UNIDAD DIDÁCTICA 6. SEGUIMIENTO DE LA IMPLANTACIÓN DEL SISTEMA

1.Operación
2.Evaluación del desempeño
3.Mejora

UNIDAD DIDÁCTICA 7. AUDITORÍA DEL SISTEMA DE GESTIÓN DE LA INFORMACIÓN POR LA DIRECCI

1.El porqué de la auditoría
2.La auditoría interna
3.El proceso de certificación

UNIDAD DIDÁCTICA 8. REVISIÓN POR LA DIRECCIÓN Y MEJORA DEL SISTEMA DE GESTIÓN DE LA IN

1.Revisión del sistema de gestión de la información por la dirección
2.Mejora del sistema de gestión de la seguridad de la información

UNIDAD DIDÁCTICA 9. GUÍAS DE SEGURIDAD: NORMATIVAS Y BUENAS PRÁCTICAS

1.Introducción a las guías de seguridad CCN-STIC
2.CCN-STIC-800 Glosario de términos y abreviaturas del ENS
3.CCN-STIC-801 Responsabilidades y funciones en el ENS
4.CCN-STIC-802 Auditoría del ENS
5.CCN-STIC-803 Valoración de Sistemas en el ENS
6.CCN-STIC-804 Medidas de implantación del ENS
7.CCN-STIC-805 Política de seguridad de la información
8.CCN-STIC-806 Plan de adecuación al ENS
9.CCN-STIC-807 Criptología de empleo en el ENS

10.CCN-STIC-808 Verificación del cumplimiento del ENS

PARTE 6. BIG DATA

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN AL BIG DATA

1.¿Qué es Big Data?
2.La era de las grandes cantidades de información: historia del big data
3.La importancia de almacenar y extraer información
4.Big Data enfocado a los negocios
5.Open Data
6.Información pública
7.IoT (Internet of Things-Internet de las cosas)

UNIDAD DIDÁCTICA 2. FASES DE UN PROYECTO DE BIG DATA

1.Diagnóstico inicial
2.Diseño del proyecto
3.Proceso de implementación
4.Monitorización y control del proyecto
5.Responsable y recursos disponibles
6.Calendarización
7.Alcance y valoración económica del proyecto

UNIDAD DIDÁCTICA 3. BIG DATA Y MARKETING

1.Apoyo del Big Data en el proceso de toma de decisiones
2.Toma de decisiones operativas
3.Marketing estratégico y Big Data
4.Nuevas tendencias en management

UNIDAD DIDÁCTICA 4. INTELIGENCIA DE NEGOCIO Y HERRAMIENTAS DE ANALÍTICA

1.Tipo de herramientas BI
2.Productos comerciales para BI
3.Productos Open Source para BI
4.Beneficios de las herramientas de BI

UNIDAD DIDÁCTICA 5. PRINCIPALES PRODUCTOS DE BUSINESS INTELLIGENCE

1.Cuadros de Mando Integrales (CMI)
2.Sistemas de Soporte a la Decisión (DSS)
3.Sistemas de Información Ejecutiva (EIS)

UNIDAD DIDÁCTICA 6: DEL BIG DATA AL LINKED OPEN DATA

1.Concepto de web semántica
2.Linked Data Vs Big Data
3.Lenguaje de consulta SPARQL