Máster en Seguridad Informática y Hacking Ético + 60 Créditos ECTS

Elige aprender en la escuela
líder en formación online

ÍNDICE

inesem business school

SOMOS INESEM

INESEM es una **Business School online** especializada con un fuerte sentido transformacional. En un mundo cambiante donde la tecnología se desarrolla a un ritmo vertiginoso nosotros somos activos, evolucionamos y damos respuestas a estas situaciones.

Apostamos por **aplicar la innovación tecnológica a todos los niveles en los que se produce la transmisión de conocimiento.** Formamos a profesionales altamente capacitados para los trabajos más demandados en el mercado laboral; profesionales innovadores, emprendedores, analíticos, con habilidades directivas y con una capacidad de añadir valor, no solo a las empresas en las que estén trabajando, sino también a la sociedad. Y todo esto lo podemos realizar con una base sólida sostenida por nuestros objetivos y valores.

Más de **18** años de experiencia

Más de **300k** estudiantes formados

Más de un **90%** tasa de empleabilidad

Hasta un **100%** de financiación

Hasta un **50%** de los estudiantes repite

Hasta un **25%** de estudiantes internacionales

Leaders driving change

Elige Inesem

ALIANZA INESEM Y UTAMED

NESEM y **UTAMED** se unen para liderar la transformación de la educación superior online.

INESEM Business School destaca como business school de referencia en formación online para profesionales, con especial énfasis en áreas como empresa, marketing, recursos humanos, tecnología y gestión empresarial. Su modelo formativo combina accesibilidad, innovación y un fuerte enfoque en el desarrollo de competencias.

UTAMED, desde su origen digital y su mirada Atlántico-Mediterránea, comparte esa visión orientada al futuro. Como universidad 100% online, apuesta por programas actualizados, multidisciplinares y adaptados a las demandas de un mercado global.

Esta alianza refuerza el puente entre la formación profesional y la formación universitaria, creando itinerarios integrados que permiten a los estudiantes avanzar en sus carreras con titulaciones avaladas académicamente y conectadas con el entorno laboral.

Ambas instituciones coinciden en ofrecer una experiencia educativa ágil, práctica y con fuerte base tecnológica, gracias a la novedosa metodología EDUCA LXP.

UTAMED

inesem business school

RANKINGS DE INESEM

INESEM Business School ha obtenido reconocimiento tanto a nivel nacional como internacional debido a su firme compromiso con la innovación y el cambio.

Para evaluar su posición en estos rankings, se consideran diversos indicadores que incluyen la percepción online y offline, la excelencia de la institución, su compromiso social, su enfoque en la innovación educativa y el perfil de su personal académico.

QS STARS RATING SYSTEM
Online Learning

Financial Magazine
Actualidad Económica & Centros de Formación

Ranking Educativo Innovatec

LOS MEJORES MASTERS EN CIBERSEGURIDAD
CyberEOP

FSO RANKING

Webometrics
RANKING WEB OF UNIVERSITIES

NOSOLOMASTER
RANKING Y OPINIONES SOBRE MASTER

webempresa

EL MUNDO

ALIANZAS Y ACREDITACIONES

Relaciones institucionales

Relaciones internacionales

Acreditaciones y Certificaciones

BY EDUCA EDTECH

Inesem es una marca avalada por **EDUCA EDTECH Group,** que está compuesto por un conjunto de experimentadas y reconocidas **instituciones educativas de formación online.** Todas las entidades que lo forman comparten la misión de **democratizar el acceso a la educación** y apuestan por la transferencia de conocimiento, por el desarrollo tecnológico y por la investigación.

EDUCA EDTECH Group

ONLINE EDUCATION

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

inesem business school

INEAF BUSINESS SCHOOL

red educa.net

inesalud

EDU SPORT

EDUCA business school

ESIBE ESCUELA IBEROAMERICANA DE POSTGRADO

Educa.Pro

ceupe European Business School

UDAVINCI

CAPMAN testing solutions

Structuralia Engineering eLearning

UNIMIAMI International University of Miami

Educa PHAROS

METODOLOGÍA LXP

La metodología **EDUCA LXP** permite una experiencia mejorada de aprendizaje integrando la AI en los procesos de e-learning, a través de modelos predictivos altamente personalizados, derivados del estudio de necesidades detectadas en la interacción del alumnado con sus entornos virtuales.

EDUCA LXP es fruto de la **Transferencia de Resultados de Investigación** de varios proyectos multidisciplinares de I+D+i, con participación de distintas Universidades Internacionales que apuestan por la transferencia de conocimientos, desarrollo tecnológico e investigación.

1. Flexibilidad

Aprendizaje 100% online y flexible, que permite al alumnado estudiar donde, cuando y como quiera.

2. Accesibilidad

Cercanía y comprensión. Democratizando el acceso a la educación trabajando para que todas las personas tengan la oportunidad de seguir formándose.

3. Personalización

Itinerarios formativos individualizados y adaptados a las necesidades de cada estudiante.

4. Acompañamiento / Seguimiento docente

Orientación académica por parte de un equipo docente especialista en su área de conocimiento, que aboga por la calidad educativa adaptando los procesos a las necesidades del mercado laboral.

5. Innovación

Desarrollos tecnológicos en permanente evolución impulsados por la AI mediante Learning Experience Platform.

6. Excelencia educativa

Enfoque didáctico orientado al trabajo por competencias, que favorece un aprendizaje práctico y significativo, garantizando el desarrollo profesional.

Programas

PROPIOS UNIVERSITARIOS OFICIALES

RAZONES POR LAS QUE ELEGIR INESEM

1. Nuestra Experiencia

- Más de **18 años de experiencia.**
- Más de **300.000 alumnos** ya se han formado en nuestras aulas virtuales
- Alumnos de los 5 continentes.
- **25%** de alumnos internacionales.
- **97%** de satisfacción
- **100% lo recomiendan.**
- Más de la mitad ha vuelto a estudiar en Inesem.

2. Nuestro Equipo

En la actualidad, Inesem cuenta con un equipo humano formado por más **400 profesionales.** Nuestro personal se encuentra sólidamente enmarcado en una estructura que facilita la mayor calidad en la atención al alumnado.

3. Nuestra Metodología

100% ONLINE

Estudia cuando y desde donde quieras. Accede al campus virtual desde cualquier dispositivo.

APRENDIZAJE

Pretendemos que los nuevos conocimientos se incorporen de forma sustantiva en la estructura cognitiva

EQUIPO DOCENTE

Inesem cuenta con un equipo de profesionales que harán de tu estudio una experiencia de alta calidad educativa.

NO ESTARÁS SOLO

Acompañamiento por parte del equipo de tutorización durante toda tu experiencia como estudiante

inesem
business school

4. Calidad AENOR

- Somos Agencia de Colaboración Nº99000000169 autorizada por el Ministerio de Empleo y Seguridad Social.
- Se llevan a cabo auditorías externas anuales que garantizan la máxima calidad AENOR.
- Nuestros procesos de enseñanza están certificados por **AENOR** por la ISO 9001.

5. Somos distribuidores de formación

Como parte de su infraestructura y como muestra de su constante expansión Euroinnova incluye dentro de su organización una **editorial y una imprenta digital industrial.**

FINANCIACIÓN Y BECAS

Financia tu cursos o máster y disfruta de las becas disponibles. ¡Contacta con nuestro equipo experto para saber cuál se adapta más a tu perfil!

25% Beca **ALUMNI**

20% Beca **DESEMPLEO**

15% Beca **EMPRENDE**

15% Beca **RECOMIENDA**

15% Beca **GRUPO**

20% Beca **FAMILIA NUMEROSA**

20% Beca **DIVERSIDAD FUNCIONAL**

MÉTODOS DE PAGO

Con la Garantía de:

innovapay

Fracciona el pago de tu curso en cómodos plazos de forma segura.

mastercard maestro VISA PayPal

bizum amazon pay Pay Pay

Nos adaptamos a todos los métodos de pago internacionales:

OXXO mercado pago DISCOVER efecty Diners Club INTERNATIONAL CMR Falabella

y muchos mas...

CONFIANZA ONLINE

Protección al Comprador

inesem business school

Máster en Seguridad Informática y Hacking Ético + 60 Créditos ECTS

DURACIÓN
1500 horas

MODALIDAD
ONLINE

ACOMPAÑAMIENTO
PERSONALIZADO

CREDITOS
60 ECTS

Titulación

Titulación de Máster de Formación Permanente en Seguridad Informática y Hacking Ético con 1500 horas y 60 ECTS expedida por UTAMED - Universidad Tecnológica Atlántico Mediterráneo.


UTAMED

inesem business school

INESEM BUSINESS SCHOOL
UNIVERSIDAD TECNOLÓGIC ALTÁNTICO - MEDITERRÁNEO

como centro acreditado para la impartición de acciones formativas
expide el presente título propio
NOMBRE DEL ALUMNO/A
con número de documento XXXXXXXXX ha superado los estudios correspondientes de
NOMBRE DEL CURSO
con una duración de XXX horas, perteneciente al Plan de Formación de UTAMED.
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX/XXXX-XXXX-XXXXXX.
Con una calificación XXXXXXXXXXXXXX.
Y para que conste expido la presente titulación en Granada, a (día) de (mes) del (año).

NOMBRE ALUMNO/A
Firma del Alumno/a

NOMBRE DE ÁREA MANAGER
La Dirección Académica

ISO ISO IQNET LTD

Con Estatuto Consultivo, Categoría Especial del Consejo Económico y Social de la UNESCO (Núm. Resolución 604/8)

inesem business school

Descripción

En la actualidad, la seguridad informática es una preocupación cada vez mayor debido al aumento de amenazas cibernéticas y ciberataques sofisticados. Los avances tecnológicos y la interconexión global han creado un entorno digital altamente vulnerable, donde los ciberdelincuentes aprovechan las brechas en la seguridad para acceder a sistemas, robar información confidencial y causar daños significativos a individuos y organizaciones. Ante este panorama, es fundamental contar con profesionales altamente capacitados en seguridad informática y hacking ético. El Master de Formación Permanente en Seguridad Informática y Hacking Ético se justifica por la necesidad de formar expertos que sean capaces de enfrentar los desafíos actuales y futuros en materia de ciberseguridad.

Objetivos

- Adquirir conocimientos avanzados en seguridad informática y hacking ético.
- Dominar técnicas y herramientas para el análisis de malware e ingeniería inversa.
- Desarrollar habilidades en pentesting y pruebas de vulnerabilidad.
- Aprender a proteger la privacidad y los datos en entornos digitales.
- Realizar análisis forenses en dispositivos y comunicaciones.
- Conocer los diferentes tipos de ciberdelitos y cómo prevenirlos.
- Utilizar herramientas especializadas para el peritaje informático

Para qué te prepara

Este Master de Formación Permanente en Seguridad Informática y Hacking Ético está dirigido a profesionales de la informática, ingenieros, administradores de sistemas y cualquier persona interesada en el campo de la ciberseguridad. También es adecuado para aquellos que deseen adquirir habilidades en hacking ético, análisis de malware, ingeniería inversa y análisis forense.

A quién va dirigido

Este Master de Formación Permanente en Seguridad Informática y Hacking Ético te prepara para enfrentar los desafíos actuales en seguridad informática. Adquirirás habilidades prácticas en el análisis de malware, la ingeniería inversa y el pentesting, lo que te permitirá identificar y mitigar los riesgos de ciberseguridad. Además, aprenderás a utilizar herramientas especializadas y a realizar análisis forenses en dispositivos y comunicaciones.

Salidas laborales

Al finalizar este Master de Formación Permanente en Seguridad Informática y Hacking Ético, podrás trabajar como analista de seguridad informática, consultor de ciberseguridad, especialista en hacking ético, investigador de malware, experto en análisis forense digital o perito informático. Podrás trabajar en empresas de seguridad, consultorías o compañías de tecnología.

TEMARIO

MÓDULO 1. CIBERSEGURIDAD: NORMATIVA, POLÍTICA DE SEGURIDAD Y CIBERINTELIGENCIA

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 DE LA 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. POLÍTICA DE SEGURIDAD: ANÁLISIS Y GESTIÓN DE RIESGOS

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

UNIDAD DIDÁCTICA 4. INGENIERÍA SOCIAL, ATAQUES WEB Y PHISHING

1. Introducción a la Ingeniería Social
2. Recopilar información
3. Herramientas de ingeniería social
4. Técnicas de ataques
5. Prevención de ataques
6. Introducción a Phising
7. Phising
8. Man In The Middle

UNIDAD DIDÁCTICA 5. CIBERINTELIGENCIA Y CIBERSEGURIDAD

1. Ciberinteligencia
2. Herramientas y técnicas de ciberinteligencia
3. Diferencias entre ciberinteligencia y ciberseguridad
4. Amenazas de ciberseguridad

UNIDAD DIDÁCTICA 6. MÉTODOS DE INTELIGENCIA DE OBTENCIÓN DE INFORMACIÓN

1. Contextualización
2. OSINT
3. HUMINT
4. IMINT

5. Otros métodos de inteligencia para la obtención de información

UNIDAD DIDÁCTICA 7. CIBERINTELIGENCIA Y TECNOLOGÍAS EMERGENTES

1. Tecnologías emergentes
2. Desafíos y oportunidades de la ciberinteligencia en las tecnologías emergentes
3. Análisis de amenazas avanzado
4. Usos de las tecnologías emergentes en la ciberinteligencia

MÓDULO 2. HERRAMIENTAS DE CIBERSEGURIDAD OSINT

UNIDAD DIDÁCTICA 1. QUÉ SON LAS HERRAMIENTAS OSINT

1. Introducción

UNIDAD DIDÁCTICA 2. GOOGLE DORK

1. Qué es Google Dork
2. Uso y aplicación de Google Dork

UNIDAD DIDÁCTICA 3. SHODAN

1. Qué es Shodan
2. Uso y aplicación de Shodan

UNIDAD DIDÁCTICA 4. MALTEGO

1. Qué es Maltego
2. Uso y aplicación de Maltego

UNIDAD DIDÁCTICA 5. THE HARVESTER

1. Qué es The Harvester
2. Uso y aplicación de The Harvester

UNIDAD DIDÁCTICA 6. RECON-NG

1. Qué es Recon-ng
2. Uso y aplicación de Recon-ng

UNIDAD DIDÁCTICA 7. CREEPY

1. Qué es Creepy
2. Uso y aplicación de Creepy

UNIDAD DIDÁCTICA 8. FOCA

1. Qué es Foca
2. Uso y aplicación de Foca

MÓDULO 3. REDES INFORMÁTICAS: ARQUITECTURA, PROTOCOLOS Y CIBERSEGURIDAD

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LA RED

1. Elementos principales de una red
2. Tecnología de redes
3. Soporte para la continuidad de la actividad

UNIDAD DIDÁCTICA 2. ESTANDARIZACIÓN DE PROTOCOLOS

1. Modelo OSI
2. Enfoque pragmático del modelo de capas
3. Estándares y organismos

UNIDAD DIDÁCTICA 3. TRANSMISIÓN DE DATOS EN LA CAPA FÍSICA

1. Papel de una interfaz de red
2. Opciones y parámetros de configuración
3. Arranque desde la red
4. Codificación de los datos
5. Conversión de las señales
6. Soportes de transmisión

UNIDAD DIDÁCTICA 4. SOFTWARE DE COMUNICACIÓN

1. Configuración de la tarjeta de red
2. Instalación y configuración del controlador de la tarjeta de red
3. Pila de protocolos
4. Detección de un problema de red

UNIDAD DIDÁCTICA 5. ARQUITECTURA DE RED E INTERCONEXIÓN

1. Topologías
2. Elección de la topología de red adaptada
3. Gestión de la comunicación
4. Interconexión de redes

UNIDAD DIDÁCTICA 6. CAPAS BAJAS DE LAS REDES PERSONALES Y LOCALES

1. Capas bajas e IEEE
2. Ethernet e IEEE 802.3
3. Token Ring e IEEE 802.5
4. Wi-Fi e IEEE 802.11
5. Bluetooth e IEEE 802.15
6. Otras tecnologías

UNIDAD DIDÁCTICA 7. REDES MAN Y WAN, PROTOCOLOS

1. Interconexión de la red local
2. Acceso remoto y redes privadas virtuales

UNIDAD DIDÁCTICA 8. PROTOCOLOS DE CAPAS MEDIAS Y ALTAS

1. Principales familias de protocolos
2. Protocolo IP versión 4
3. Protocolo IP versión 6
4. Otros protocolos de capa Internet
5. Voz sobre IP (VoIP)
6. Protocolos de transporte TCP y UDP
7. Capa de aplicación TCP/IP

UNIDAD DIDÁCTICA 9. PROTECCIÓN DE UNA RED

1. Comprensión de la necesidad de la seguridad
2. Herramientas y tipos de ataque
3. Conceptos de protección en la red local
4. Protección de la interconexión de redes

UNIDAD DIDÁCTICA 10. REPARACIÓN DE RED

1. Introducción a la reparación de red
2. Diagnóstico en capas bajas
3. Utilización de herramientas TCP/IP adaptadas
4. Herramientas de análisis de capas altas

UNIDAD DIDÁCTICA 11. COMUNICACIONES SEGURAS: SEGURIDAD POR NIVELES

1. Seguridad a Nivel Físico
2. Seguridad a Nivel de Enlace
3. Seguridad a Nivel de Red
4. Seguridad a Nivel de Transporte
5. Seguridad a Nivel de Aplicación

UNIDAD DIDÁCTICA 12. APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

1. Identificación de los componentes de una PKI y sus modelos de relaciones
2. Autoridad de certificación y sus elementos
3. Política de certificado y declaración de prácticas de certificación (CPS)
4. Lista de certificados revocados (CRL)
5. Funcionamiento de las solicitudes de firma de certificados (CSR)
6. Infraestructuras de gestión de privilegios (PMI)
7. Campos de certificados de atributos
8. Aplicaciones que se apoyan en la existencia de una PKI

UNIDAD DIDÁCTICA 13. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

1. Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
2. Identificación y caracterización de los datos de funcionamiento del sistema
3. Arquitecturas más frecuentes de los IDS
4. Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
5. Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

UNIDAD DIDÁCTICA 14. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS

1. Análisis previo
2. Definición de políticas de corte de intentos de intrusión en los IDS/IPS
3. Análisis de los eventos registrados por el IDS/IPS
4. Relación de los registros de auditoría del IDS/IPS
5. Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

UNIDAD DIDÁCTICA 15. INTRODUCCIÓN A LOS SISTEMAS SIEM

1. ¿Qué es un SIEM?
2. Evolución de los sistemas SIEM: SIM, SEM y SIEM
3. Arquitectura de un sistema SIEM

UNIDAD DIDÁCTICA 16. CAPACIDADES DE LOS SISTEMAS SIEM

1. Problemas a solventar
2. Administración de logs
3. Regulaciones IT
4. Correlación de eventos
5. Soluciones SIEM en el mercado

MÓDULO 4. CRIPTOGRAFÍA Y REDES PRIVADAS VIRTUALES (VPN)

UNIDAD DIDÁCTICA 1. HISTORIA Y EVOLUCIÓN DE LA CRIPTOGRAFÍA

1. La criptografía a lo largo de la historia
2. El nacimiento del criptoanálisis
3. La criptografía en nuestros tiempos
4. Criptografía en el futuro

UNIDAD DIDÁCTICA 2. SEGURIDAD INFORMÁTICA Y CRIPTOGRAFÍA

1. Seguridad Informática
2. Uso de seguridad informática y criptografía
3. Tipo de amenazas
4. Respuesta ante un ataque
5. Amenazas del futuro

UNIDAD DIDÁCTICA 3. CRIPTOGRAFÍA SIMÉTRICA Y CRIPTOGRAFÍA ASIMÉTRICA

1. Criptografía simétrica
2. Criptografía asimétrica
3. Criptografía híbrida
4. Criptografía y seguridad informática: El Ciclo de vida de las claves y contraseñas

UNIDAD DIDÁCTICA 4. CRIPTOGRAFÍA DE CLAVE PRIVADA

1. Cifrado de clave privada
2. Cifrado DES
3. Función F

UNIDAD DIDÁCTICA 5. CRIPTOGRAFÍA DE CLAVE PÚBLICA Y DIFERENTES APLICACIONES

1. Cifrado de clave pública
2. PKC como herramienta de cifrado
3. Uso en Generación de Firmas Digitales
4. Aplicaciones de la criptografía pública y privada
5. Certificado digital
6. DNI Electrónico
7. Bitcoin

UNIDAD DIDÁCTICA 6. PROTOCOLOS CRIPTOGRÁFICOS Y FIRMAS DIGITALES

1. Protocolo criptográfico
2. Protocolo criptográfico avanzado
3. Firma segura hacia delante

UNIDAD DIDÁCTICA 7. APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

1. Identificación de los componentes de una PKI y sus modelos de relaciones
2. Autoridad de certificación y sus elementos
3. Política de certificado y declaración de prácticas de certificación (CPS)
4. Lista de certificados revocados (CRL)
5. Funcionamiento de las solicitudes de firma de certificados (CSR)
6. Infraestructuras de gestión de privilegios (PMI)
7. Campos de certificados de atributos
8. Aplicaciones que se apoyan en la existencia de una PKI

UNIDAD DIDÁCTICA 8. HASHING

UNIDAD DIDÁCTICA 9. TIPOS DE ALGORITMOS Y CIFRADOS CRIPTOGRÁFICOS

1. Métodos criptográficos históricos
2. Challenge Handshake Authentication Protocol (CHAP)
3. Federal Information Processing Standards (FIPS)
4. Private Communication Technology (PCT)
5. Secure Electronic Transaction (SET)
6. Secure Sockets Layer (SSL)
7. Simple Key Management for Internet Protocol (SKIP)
8. IP Security Protocol (IPSec)

UNIDAD DIDÁCTICA 10. HERRAMIENTAS CRIPTOGRÁFICAS Y EJEMPLOS DE USO

1. Herramientas Criptográficas de Microsoft
2. CrypTool-Online (CTO)
3. Java Cryptographic Architecture (JCA)
4. GNU Privacy Guard
5. Whisply
6. DiskCryptor
7. AES Crypt
8. Ejemplos criptográficos en Python

UNIDAD DIDÁCTICA 11. INTRODUCCIÓN A LAS REDES PRIVADAS VIRTUALES (VPN)

1. ¿Qué son las redes privadas virtuales o VPN?
2. Bloques de construcción de VPN
3. Tecnologías VPN, Topología y Protocolos
4. VPN vs IP móvil

UNIDAD DIDÁCTICA 12. ARQUITECTURAS VPN

1. Requisitos y arquitecturas VPN
2. Arquitecturas VPN basadas en seguridad y en capas
3. VPN de acceso remoto y extranet

UNIDAD DIDÁCTICA 13. PROTOCOLOS DE TUNELIZACIÓN VPN

1. PPTP
2. L2TP
3. L2F
4. IPSec
5. MPLS

UNIDAD DIDÁCTICA 14. AUTENTICACIÓN Y CONTROL DE ACCESO EN VPN

1. Autenticación PPP
2. RADIO y Kerberos
3. Autenticación de VPN
4. Control de acceso en VPN

UNIDAD DIDÁCTICA 15. GESTIÓN DE SERVICIOS Y REDES VPN

1. Protocolos y arquitectura de gestión de red
2. Gestión de servicios VPN
3. Centros de operaciones de red (NOC)
4. Redundancia y equilibrio de carga

MÓDULO 5. ANÁLISIS DE MALWARE, CRACKING E INGENIERÍA INVERSA

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN AL ANÁLISIS DE MALWARE

UNIDAD DIDÁCTICA 2. TÉCNICAS Y HERRAMIENTAS PARA ANÁLISIS DE MALWARE

UNIDAD DIDÁCTICA 3. CONTROL MALWARE

1. Sistemas de detección y contención de Malware
2. Herramientas de control de Malware
3. Criterios de seguridad para la configuración de las herramientas de protección frente a Malware
4. Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a Malware
5. Relación de los registros de auditoría de las herramientas de protección frente a Malware
6. Establecimiento de la monitorización y pruebas de las herramientas de protección frente a

Malware
7. Análisis de Malware mediante desensambladores y entornos de ejecución controlada

UNIDAD DIDÁCTICA 4. FUNDAMENTOS DE LA INGENIERÍA INVERSA

1. Concepto de Ingeniería Inversa
2. Características de la Ingeniería Inversa
3. Ventajas del uso de Ingeniería Inversa

UNIDAD DIDÁCTICA 5. TIPOS DE INGENIERÍA INVERSA

1. Ingeniería inversa de datos
2. Ingeniería inversa de lógica o proceso
3. Ingeniería inversa de interfaces de usuario

UNIDAD DIDÁCTICA 6. HERRAMIENTAS DE INGENIERÍA INVERSA

1. Ghidra
2. IDA
3. Winhex
4. Hiew
5. x64dbg
6. Radare2
7. Cutter

UNIDAD DIDÁCTICA 7. INTRODUCCIÓN AL CRACKING

UNIDAD DIDÁCTICA 8. HERRAMIENTAS DE CRACKING

1. Depuradores
2. Desensambladores
3. Compiladores Inversos o Decompiladores

MÓDULO 6. PENTESTING Y HACKING TOOLS

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN AL HACKING ÉTICO

1. ¿Qué es el hacking ético?
2. Aspectos legales del hacking ético
3. Perfiles del hacker ético

UNIDAD DIDÁCTICA 2. FASES DEL HACKING ÉTICO EN LOS ATAQUES A SISTEMAS Y REDES

1. Tipos de ataques
2. Herramientas de hacking ético
3. Tests de vulnerabilidades

UNIDAD DIDÁCTICA 3. FASES DEL HACKING ÉTICO EN LOS ATAQUES A REDES WIFI

1. Tipos de ataques

2. Herramientas de hacking ético
3. Tipos de seguridad WiFi
4. Sniffing

UNIDAD DIDÁCTICA 4. FASES DEL HACKING ÉTICO EN LOS ATAQUES WEB

1. Tipos de ataques
2. Herramientas de hacking ético
3. Tipos de seguridad web
4. Tipo de test de seguridad en entornos web

UNIDAD DIDÁCTICA 5. KALI LINUX

UNIDAD DIDÁCTICA 6. NMAP

UNIDAD DIDÁCTICA 7. METASPLOIT

UNIDAD DIDÁCTICA 8. WIRESHARK

UNIDAD DIDÁCTICA 9. JOHN THE RIPPER

UNIDAD DIDÁCTICA 10. HASHCAT

UNIDAD DIDÁCTICA 11. HYDRA

UNIDAD DIDÁCTICA 12. BURP SUITE

UNIDAD DIDÁCTICA 13. ZED ATTACK PROXY

UNIDAD DIDÁCTICA 14. SQLMAP

UNIDAD DIDÁCTICA 15. AIRCRACK-NG

MÓDULO 7. HACKING TRAINING PLATFORMS

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A HACKING TRAINING PLATFORMS

1. ¿Qué es el hacking ético?
2. Máquinas virtuales
3. Plataformas para practicar hacking ético

UNIDAD DIDÁCTICA 2. HACK THE BOX (HTB)

1. Introducción a Hack The Box
2. Crear una cuenta
3. Tutoriales

UNIDAD DIDÁCTICA 3. TRYHACKME

1. ¿Qué es TryHackMe?
2. Crear una cuenta

3. Interfaz de TryHackMe
4. Introducción a la ciberseguridad
5. Seguridad ofensiva
6. Ciencia forense digital

UNIDAD DIDÁCTICA 4. HACKER101

1. ¿Qué es Hacker101?
2. Hacker101 CTF
3. Tutoriales

UNIDAD DIDÁCTICA 5. VULNHUB

1. ¿Qué es Vulnhub?
2. Interfaz de Vulnhub
3. Tutoriales

UNIDAD DIDÁCTICA 6. HACK THIS SITE

1. ¿Qué es Hack This Suite?
2. Desafíos Hack This Site

UNIDAD DIDÁCTICA 7. GOOGLE XSS GAME

1. ¿Qué es Google XSS Game?
2. Niveles de Google XSS game

UNIDAD DIDÁCTICA 8. HACKTHIS

1. ¿Qué es HackThis?
2. Tutorial HackThis
3. Basic+

MÓDULO 8. CIBERCRIMEN

UNIDAD DIDÁCTICA 1. ¿QUÉ SON LOS DELITOS INFORMÁTICOS?

1. Concepto de delincuencia informática y cibercriminalidad
2. ¿Qué es el cibercrimen?
3. Tipos de cibercrimen

UNIDAD DIDÁCTICA 2. CLASIFICACIÓN ATENDIENDO A LA INCIDENCIA DE LAS TIC

1. Ciberataques puros
2. Ciberataques réplica
3. Ciberataques de contenido

UNIDAD DIDÁCTICA 3. CLASIFICACIÓN ATENDIENDO AL MÓVIL CRIMINOLÓGICO

1. Cibercrimen económico

2. Cibercrimen social
3. Cibercrimen político

UNIDAD DIDÁCTICA 4. ¿QUÉ ES EL CIBERESPACIO?

1. Arquitectura del ciberespacio
2. Teoría criminológica y cibercrimen

UNIDAD DIDÁCTICA 5. CIBERVÍCTIMA

1. La importancia de la víctima en el cibercrimen
2. Prevención del cibercrimen
3. Multiplicidad de cibervíctimas
4. Victimización en el ciberespacio

UNIDAD DIDÁCTICA 6. CIBERDELINCUENTE

1. ¿Cuál es el perfil común de un ciberdelincuente?
2. Especialidades de ciberdelincuente

UNIDAD DIDÁCTICA 7. EL CIBERCRIMEN COMO PROBLEMA INTERNACIONAL

1. Seguridad cibernética
2. Deep web
3. Cooperación Internacional en asuntos de seguridad cibernética
4. Prevención del delito cibernético

MÓDULO 9. CIBERDELITOS

UNIDAD DIDÁCTICA 1. PRIVACIDAD Y PROTECCIÓN DE DATOS

1. ¿Por qué es importante la privacidad?
2. Privacidad y Seguridad
3. Ciberdelitos que comprometen la privacidad
4. Normativa sobre privacidad y protección de datos

UNIDAD DIDÁCTICA 2. PROPIEDAD INTELECTUAL

1. ¿Qué es la propiedad intelectual?
2. Tipos de propiedad intelectual
3. Teorías criminológicas en delitos contra la propiedad intelectual por medios cibernéticos

UNIDAD DIDÁCTICA 3. DELINCUENCIA ORGANIZADA

1. Delincuencia cibernética organizada y actores que intervienen
2. Perfil de los grupos delictivos
3. Actividades de los ciberdelitos organizados
4. Prevención de este tipo de ciberdelitos

UNIDAD DIDÁCTICA 4. TRATA DE PERSONAS Y TRÁFICO ILÍCITO DE INMIGRANTES

1. ¿La tecnología facilita este tipo de delitos?
2. Trata de personas y tráfico ilícito de inmigrantes como ciberdelito organizado

UNIDAD DIDÁCTICA 5. CIBERDELITOS CONTRA LAS PERSONAS

1. Explotación y abuso sexual infantil
2. Hostigamiento
3. Acoso
4. Violencia de género

UNIDAD DIDÁCTICA 6. CIBERTERRORISMO

1. Hacktivismo
2. Ciberespionaje
3. Ciberterrorismo
4. Guerra cibernética
5. La guerra de la información, la desinformación y el fraude electoral

MÓDULO 10. ANÁLISIS FORENSE Y HERRAMIENTAS PARA PERITAJE INFORMÁTICO

UNIDAD DIDÁCTICA 1. ANÁLISIS FORENSE DE DISPOSITIVOS FÍSICOS INFORMÁTICOS

UNIDAD DIDÁCTICA 2. ANÁLISIS FORENSE EN WINDOWS

UNIDAD DIDÁCTICA 3. ANÁLISIS FORENSE EN GNU/LINUX

UNIDAD DIDÁCTICA 4. ANÁLISIS FORENSE EN MAC OS

UNIDAD DIDÁCTICA 5. ANÁLISIS FORENSE EN ANDROID

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE EN IOS

UNIDAD DIDÁCTICA 7. ANÁLISIS FORENSE DE EMAILS, WHATSAPP Y OTRAS COMUNICACIONES

UNIDAD DIDÁCTICA 8. INFORME PERICIAL

MÓDULO 11. PROYECTO FIN DE MASTER (PFM)

inesem
business school

By
EDUCA EDTECH
Group