



SEMINARIOS

0xWORD

SEMINARIOS

OxWORD



Estos cursos variados relacionados con la **Ciberseguridad e Inteligencia Artificial** han sido desarrollados por la editorial de OxWord que lidera **Chema Alonso**. Desde UNIR, impulsamos la mejora formativa del máster en Ciberseguridad ofreciendo diferentes seminarios.

Duración

20 horas
(distribuidas en 1 mes)

Metodología

100% online.
Clases en directo

Créditos

1 ECTS

Precio

250€/seminario.
Si te matriculas en el Máster en Ciberseguridad, se te ofrece un seminario gratis.



BLOQUE 1

Inicio: Semana del 18 de abril de 2022

Fin: Semana del 18 de mayo de 2022

SEMINARIOS

Ciberinteligencia de analistas a través de técnicas OSINT + Singularity Hackers

Profesor Jezer Ferreira

La ciberinteligencia ha cobrado un lugar importante en la sociedad actual. Cada vez son más necesarios los analistas que puedan cubrir diferentes partes de la vigilancia digital y el entendimiento necesario para luchar contra las amenazas que pueden surgir de las fuentes abiertas de información. Cómo preparar una investigación, cómo enfocar una investigación en redes sociales, cómo trabajar en la Deep web, cómo se utiliza TOR, cómo aplicar una metodología, cómo presentar un informe.

- Introducción a la ciberinteligencia
- La disciplina de la inteligencia
- El ciclo de inteligencia
- Evaluación y catalogación de la información
- ¿Cómo preparar un entorno de investigación?
- OSINT
- Metodologías aplicadas
- Investigación en redes sociales
- DeepWeb & DarkNet
- Red TOR
- Técnicas aplicadas en un entorno real

Fortificación profesional de entornos de bases de datos

Profesor Rubén Alonso

- Introducción a las bases de datos y su arquitectura
- Buenas prácticas de seguridad en bases de datos
- Fortificación en profundidad del motor de base de datos
- Creación segura de tu base de datos
- Monitorización
- Logs
- Elementos activos en la seguridad



BLOQUE 1

Inicio: Semana del 18 de abril de 2022

Fin: Semana del 18 de mayo de 2022

SEMINARIOS

Docker para profesionales de la trifuerza

Profesor Fran Ramírez y Rafael Troncoso

Los contenedores y el papel que juegan en el despliegue de aplicaciones y servicios es algo tangible. El mundo del DevOps solicita cada vez más personas cualificadas y los contenedores y la tecnología Docker juega un papel amplio. En esta formación se detallará desde la base qué son los contenedores y cómo utilizar Docker, así como las buenas prácticas en seguridad. Todo ello con un enfoque totalmente práctico.

- Introducción a Docker
- Contenedores
- Imágenes
- Redes
- Volúmenes
- Docker-Compose
- Seguridad en Docker
- Aplicación de Docker en DevSecOps
- Introducción a Kubernetes
- Escenarios y ejemplos

Inteligencia Artificial y las técnicas ofensivas y defensivas

Profesor Fran Ramírez

La inteligencia artificial es un campo que se introduce en cualquier otro para facilitar las diferentes acciones: detección de anomalías en seguridad, toma de decisiones en los planes de negocio, ayudar a la publicidad dirigida. La inteligencia artificial aplicada al mundo de la ciberseguridad tiene un aporte fundamental de presente y futuro. El perfil dual entre experto en ciberseguridad y experto en inteligencia artificial será uno de los perfiles más demandados. En esta formación se introducirá la inteligencia artificial y se aplicará sobre escenarios de ciberseguridad.

- Introducción a la Inteligencia Artificial
- Tipos de aprendizaje
- Algoritmos de Machine Learning
- Uso de Python en ML
- Deep Learning
- Metodología de aplicación de la IA a diferentes campos
- Aplicando casos a la ciberseguridad
- Detección de anomalías
- Detección de phishing

BLOQUE 2

Inicio: Semana del 23 de mayo de 2022

Fin: Semana del 22 de junio de 2022

SEMINARIOS

Técnicas profesionales en hacking ético

Luis Eduardo Álvarez

El hacking ético se ha convertido en uno de los procesos más importantes y solicitados por las organizaciones para evaluar la seguridad de sus infraestructuras. El pentesting es una de las herramientas con valor para la evaluación y toma de decisiones en las inversiones en seguridad. Durante el curso puedes aprender lo necesario para llevar a cabo un pentest en sistemas con un enfoque práctico totalmente.

- Introducción al hacking ético
- Estándares, modelos y metodologías
- Fases pentesting
- Enumeración y recopilación de información
- Fuerza bruta directorios & Fuzzing
- Nmap & NSE
- Análisis vulnerabilidades
- Identificación y detección de vulnerabilidades
- Explotación sistemas Windows & Linux
- Tipos de exploits

Hardening profesional en entornos windows

Profesor Ángel Núñez

La fortificación de los entornos es fundamental en cualquier organización. Las organizaciones disponen de una gran cantidad de activos y es vital para la actividad de negocio que haya un alineamiento entre seguridad y productividad. En este curso podrás aprender sobre fortificación de entornos Microsoft Windows (cliente y servidor) y haciendo que el directorio activo sea un lugar más seguro.

- Introducción a la fortificación de entornos Windows
- Fortificación de sistemas Windows
- Administración de sistemas Windows
- Containers en Windows Server
- Objetos, directivas y directorio activo
- Gestión de identidades
- Windows Defender
- Device Guard
- EMET
- Firewall
- NAP
- otros roles y características de seguridad

BLOQUE 2

Inicio: Semana del 23 de mayo de 2022

Fin: Semana del 22 de junio de 2022

SEMINARIOS

Pentesting profesional a infraestructuras críticas y sistemas de control industrial

Profesor Jordi Ubach

Las infraestructuras críticas y los sistemas de control industrial se encuentran en nuestro día a día como sociedad. La seguridad en el mundo OT es algo de vital importancia y dónde existe una serie de necesidades. La conexión del mundo OT con el mundo IT abre un abanico de amenazas que pueden impactar sobre los activos del mundo industrial. En esta formación aprenderás las bases para llevar a cabo un pentesting sobre sistemas de control industrial.

- Introducción al mundo OT
- Dispositivos
- Ley PIC
- Sistemas de control industrial
- Consideraciones especiales en los sistemas industriales
- Protocolos Fases del pentesting
- Escaneo a redes industriales
- Uso de Moki
- Detección e identificación de debilidades y vulnerabilidades en entornos industriales
- Explotación de vulnerabilidades
- Escenarios y ejemplos
- Cómo fortificar los entornos industriales



BLOQUE 3

Inicio: Semana del 27 de junio de 2022

Fin: Semana del 27 de julio de 2022

SEMINARIOS

Técnicas profesionales de auditoría web + Singularity Hackers

Profesores Amador Aparicio y Pabel Abel

La auditoría y el pentesting web son algunos de los trabajos más solicitados dentro del mundo de la ciberseguridad. Durante esta formación se mostrarán diferentes técnicas que permitirán al alumno introducirse en la auditoría y pentesting web a nivel profesional. Se profundizará a través del uso de diferentes técnicas para llevar a cabo un pentest web profesional. La metodología de trabajo se mostrará desde un punto de vista totalmente práctico.

- Introducción a los sistemas web
- Pentesting web y sus fases
- Spidering & Crawling
- Fuzzing a tecnologías web
- Escaneos activos y pasivos
- Info Leaks
- OWASP
- Tipos de vulnerabilidades web
- Injections: SQL, LDAP, Blind, Command injection, XPathRFI
- Connection String Attacks
- NoSQLi
- Tipos de Cross-Site (XSS, CSRF...)
- Escenarios y ejemplos de pentesting web

Hardware Hacking profesional para Hackers & Makers

Álvaro Nuñez-Romero y Joel Serna Moreno

El mundo DIY (Do IT Yourself) ha cobrado gran importancia con el paso de los años. El hardware hacking dónde uno es capaz de implementar diferentes proyectos que pueden ayudarle en un pentest ha crecido. Las posibilidades son infinitas, no solo para la ciberseguridad. En esta formación aprenderás cómo trabajar con Arduino y con Raspberry para llevar a cabo proyectos de ciberseguridad de forma autónoma. Además, se verán ejemplos de cómo se implementan los diferentes proyectos.

- Introducción
- Lenguaje de programación de Arduino
- Conversión analógico a digital
- Serial
- Radiofrecuencia
- Proyectos Raspberry en ciberseguridad
- Montando RubberDucky con Arduino
- Radiofrecuencia en ciberseguridad con Arduino
- Herramientas de ciberseguridad con Arduino

BLOQUE 3

Inicio: Semana del 27 de junio de 2022

Fin: Semana del 27 de julio de 2022

SEMINARIOS

Técnicas profesionales para Red Team en entornos Windows

Profesores Carlos García García

El Red Team es parte fundamental de la seguridad en una organización. Un ejercicio de Red Team puede ayudar a mejorar drásticamente la seguridad de la organización y cómo funcionan los procesos internos de seguridad de la empresa. En esta formación podrás estudiar toda la parte de seguridad ofensiva sobre entornos Windows, siempre desde el punto de vista de detección de fallos, vulnerabilidades, seguridad en directorio activo, escalada de privilegios, persistencia. Todo lo necesario para afrontar un pentest dentro de un Red Team en un entorno Windows.

- Introducción al Red Team
- Autenticación y autorización en Windows
- Access Token & Incognito
- NTLM y el funcionamiento: pass-the-hash
- Pwdump
- Kerberos
- Ataques a Active Directory
- Golden Ticket, Silver Ticket, Pass-The-Ticket
- Mimikatz
- Escalada de privilegios





RECTORADO

Avenida de la Paz, 137
26004 Logroño
España
+34 941 210 211

DELEGACIÓN MADRID

C/ Almansa, 101
28040 Madrid
España
+34 915 674 391

DELEGACIÓN COLOMBIA

Calle 100 # 19 – 61
Edificio Centro Empresarial 100.
Oficina 801
+571 5169659

DELEGACIÓN MÉXICO

Av. Extremadura, 8.
Col Insurgentes Mixcoac. Del Benito
Juárez 03920, México D.F.
01800 681 5818

DELEGACIÓN ECUADOR

Av. República E7-123 y Martín
Carrión (esquina).
Edificio Pucará
(+593) 3931480

DELEGACIÓN PERÚ

Gabriel Chariarse, 415
San Antonio, Miraflores
Perú, Lima
(01) 496 – 8095

unir.net

