SEMINARIOS 0xWORD

unir LA UNIVERSIDAD EN INTERNET

SEMINARIOS 0xWORD

Estos cursos variados relacionados con la **Ciberseguridad e Inteligencia Artificial** han sido desarrollados por la editorial de 0xWord que lidera **Chema Alonso**. Desde UNIR México impulsamos la mejora formativa de la **Maestría en Seguridad Informática** 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 la Maestría en Seguridad Informática, se te ofrece un seminario gratis

BLOQUE 1

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

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 2

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 2

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

unir LA UNIVERSIDAD EN INTERNET

Av. Universidad 472, Colonia Vertiz Navarte
Benito Juárez CP: 03600 Ciudad de México

mexico.unir.net | inscripciones@unirmexico.mx | +52 (55) 3683 3800