Fundamentos de Ciberseguridad: un enfoque práctico
BID

Link: https://www.edx.org/es/learn/cybersecurity/inter-american-development-bank-fundamentos-de-ciberseguridad-un-enfoque-practico?utm_campaign=idbx&utm_medium=partner-marketing&utm_source=referral&utm_content=ciberseguridad_indes

Duración: 6 semanas. 5–7 horas por semana

Lo que aprenderás

- Los principales conceptos sobre amenazas, como son el cibercrimen o la ciberguerra.
- Técnicas y herramientas aplicadas en informática forense.
- Procesos y herramientas de ingeniería inversa.
- Conceptos y herramientas sobre la gestión de redes para ciberdefensa.
- Tipos y características de malware y amenazas persistentes avanzadas (APTs).
- Gestión de vulnerabilidades, junto con pruebas de penetración.

Plan de estudios

Lección 1. Ciberseguridad: una visión general
En esta lección se presenta el panorama actual del impacto de la ciberseguridad, así como tipos y ejemplos de ciberamenazas, ciberdelitos y ciberguerra.

Lección 2. Informática forense
En esta lección se aborda la informática forense, que es la técnica centrada en el análisis y la preservación de evidencias en un dispositivo informático, en particular después de un ataque. Se definen algunos de los rastros forenses más comunes, como son los rastros asociados de los archivos eliminados, datos ocultos y correos electrónicos falsos.

Lección 3. Ingeniería inversa
En esta lección se presentan los conceptos principales de la ingeniería inversa, es decir, la capacidad de estudiar un elemento ejecutable y tratar de descubrir su funcionamiento. Además, se muestran algunos ejemplos de decompilación y de desensamblado.

Lección 4. Ciberdefensa
Esta lección presenta los principales conceptos de ciberdefensa junto con algunas de las herramientas más comunes. Se abordarán los contrafuegos, los sistemas de detección de intrusiones, así como los sistemas de seguridad y gestión de eventos, que sirven para gestionar la ciberdefensa en múltiples niveles.

Lección 5. Malware y amenazas persistentes avanzadas (APT)
Esta lección explica los principales conceptos relacionados con los programas malignos, conocidos como malware, y las amenazas persistentes avanzadas (APT), junto casos reales y las técnicas principales para lograr su identificación.

Lección 6. Vulnerabilidades y exposiciones

En esta última lección se presentan ejemplos de múltiples vulnerabilidades a nivel software, red y web y cómo gestionarlas. También se muestran ejemplos de pruebas de penetración (pentesting) usando la herramienta de Metasploit.