Seguridad informática : Ethical Hacking: conocer el ataque para una mejor defensa /

ACISSI

Ediciones ENI,
2022

Monografía

Este libro sobre seguridad informática (y hacking ético) está dirigido a cualquier informático sensibilizado con el concepto de la seguridad informática, aunque sea novato o principiante en el dominio de la seguridad de los sistemas de información. Tiene como objetivo iniciar al lector en las técnicas de los atacantes para, así, aprender a defenderse. Esta nueva edición tiene en cuenta las novedades en el campo de la seguridad informática e incluye tres nuevos capítulos sobre la seguridad de los dispositivos móviles, los vehículos conectados y el estudio de malwares. El libro comienza sumergiéndose en el mundo de la ciberseguridad, para presentarle su funcionamiento, espíritu y los diferentes actores. Encontrará una definición precisa de los diferentes tipos de hackers y sus objetivos. El capítulo sobre Social Engineering o manipulación social, mostrará por qué las vulnerabilidades humanas representan más del 60 % de los ataques con éxito. Seguidamente, verá el Black Market, una plataforma real para la reventa de datos robados y soluciones maliciosas. El capítulo sobre la toma de datos, esencial para la preparación de una auditoría (y de un ataque), presentará la metodología de un ataque y la forma de búsqueda de información objetivo y vulnerabilidades explotables. Más adelante, llegamos al corazón del asunto, es decir, las vulnerabilidades de los sistemas en Windows o Linux con la aparición de sus nuevas versiones, así como las vulnerabilidades de la red y Wi-Fi, ilustradas con numerosas propuestas de contramedidas. También se trata la seguridad en la web y se identifican vulnerabilidades comunes, utilizando herramientas que el lector puede implementar fácilmente en sus propios sistemas. El objetivo siempre es identificar posibles vulnerabilidades e implementar la estrategia de protección adecuada. Posteriormente, se tratan las vulnerabilidades de la aplicación, introduciendo algunos elementos para familiarizarse con el lenguaje ensamblador y, de esta manera, entender mejor las posibilidades de ataque. Le siguen capítulos sobre Forensic o la búsqueda de pruebas comprometidas, así como una introducción al estudio del malware, la seguridad de los dispositivos móviles que forman parte de nuestro día a día, las vulnerabilidades de hardware (internet de las cosas), las Boxes, omnipresentes en nuestros hogares y la seguridad de los vehículos conectados, que también se ven afectados por ciberataques. Los autores de este libro son un equipo de personas con convicción, que se han propuesto hacer que la seguridad informática esté al alcance de todos: su lema es "Aprender a atacar para defenderse mejor". Hackers blancos de corazón, abren al lector las puertas del conocimiento underground. Todos son miembros de la asociación ACISSI (Auditoria, Consultoría, Instalación y Securización de Sistemas de Información), que es una asociación sin ánimo de lucro que asesora sobre los retos de la seguridad informática

Título: Seguridad informática Ethical Hacking: conocer el ataque para una mejor defensa ACISSI; Damien Bancal, Jacques Beirnaert-Huvelle,Joffrey Clarhaut, Robert Crocfer [y otros 8]; edición española, Angel Mª Sánchez Conejo

Edición: 5ª edición

Editorial: Barcelona Ediciones ENI 2022

Descripción física: 912 páxinas ilustracións 21 cm

Mención de serie: Epsilon

ISBN: 9782409039140

Materia: Seguridad informática $2UDCAM Delitos informáticos $2UDCAM

Autores: Bancal, Damien, autor Beirnaert-Huvelle, Jacques, autor Clarhaut, Joffrey, autor Crocfer, Robert, autor Sánchez Conejo, Angel M., editor literario

Punto acceso adicional serie-Título: Epsilon