# Sécurité informatique

Type de contenu : Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : Sécurité informatique : ethical hacking : apprendre l'attaque pour mieux se défendre / [ACISSI]

A pour autre édition sur un support différent : Sécurité informatique ethical hacking apprendre l'attaque pour mieux se défendre [ACISSI] 7e édition 2026 St-Herblain Editions ENI Epsilon 978-2-4090-5340-5

Auteur(s) : Audit, conseil, installation et sécurisation des systèmes d'information

Mention d'édition : 7e édition [entièrement actualisée]

Publication : St Herblain : Éditions ENI

Date de copyright : C 2026

Description matérielle : 1 volume (1000 pages) : illustrations, couverture illustrée ; 22 cm

Collection : Epsilon

ISBN : 978-2-409-05339-9

EAN : 9782409053399

Appartient à la collection : Epsilon (Saint-Herblain) 1960-3444

Classification décimale Dewey : 364.168 2

Note sur la publication, la production, etc. : La graphie correcte du lieu d'édition est : Saint-Herblain

Note sur les bibliographies et les index : Bibliographie page 102. Liste de sites Internet page 718

Résumé ou extrait : "Ce livre sur la sécurité informatique et le Ethical Hacking s'adresse aux informaticiens sensibilisés aux enjeux de cybersécurité, mais débutants dans la protection des systèmes d'information. Son objectif est clair : comprendre les techniques d'attaque pour mieux se défendre. Cette nouvelle édition, entièrement actualisée, intègre un chapitre consacré à l'analyse des risques selon la méthode EBIOS, permettant d'identifier et de hiérarchiser les actifs d'un système d'information à protéger. Les chapitres sur les communications sans fil, les failles matérielles et la sécurité des box sont fusionnés en un ensemble cohérent dédié aux objets connectés et systèmes embarqués. L'ouvrage débute par une

immersion dans le monde de la cybersécurité, ses acteurs et ses pratiques. Il définit précisément les différents types de hackers, puis explore le Social Engineering, responsable de plus de 74 % des attaques réussies (rapport Mimecast 2024), avant d'aborder le Black Market, où s'échangent données volées et outils malveillants. Le lecteur découvre ensuite les méthodologies de recherche d'informations, essentielles en audit de sécurité. Le cœur du livre porte sur les failles système (Windows, Linux), les failles réseau et Wi-Fi, et la sécurité web, avec pour chaque thème des contre-mesures applicables. S'ajoutent les failles applicatives, une introduction au langage assembleur, ainsi que des chapitres dédiés au Forensic, aux malwares, à la sécurité des mobiles et des véhicules connectés. L'ouvrage s'achève sur les risques juridiques, incluant les exigences du RGPD."

Sujet - Nom commun : Systèmes informatiques -- Mesures de sûreté
Systèmes d'information -- Mesures de sûreté
Cyberdéfense
Pirates informatiques -- Lutte contre