

# Sommaire de l'ouvrage

- 1. Les menaces informatiques**  
Introduction aux attaques, pirates, méthodologie d'intrusion, écoute réseau, compromission, nettoyage des traces, types de menaces (physiques, réseau, social, rebond)
- 2. Les malwares**  
Virus, vers, chevaux de Troie, backdoors, et fonctionnement des botnets
- 3. Les techniques d'attaque**  
Ingénierie sociale, phishing, buffer overflow, scanning de ports, déni de service, etc.
- 4. La cryptographie**  
Concepts de base, chiffrement, échanges sécurisés, signatures numériques
- 5. Les protocoles sécurisés**  
TLS/SSL, DNSsec, VPN, HTTPS et autres mécanismes de sécurité réseau
- 6. Les dispositifs de protection**  
Pare-feu, antivirus, systèmes de détection d'intrusions (IDS), sandboxing, etc.
- 7. L'authentification**  
Gestion des mots de passe, biométrie, MFA, systèmes d'authentification émergents
- 8. La sûreté de fonctionnement**  
Continuité de service, redondance, tolérance aux pannes, mises à jour régulières
- 9. Sécurité des applications web**  
Vulnérabilités courantes telles que injection SQL, XSS, CSRF, sécurisation des API
- 10. Sécurité des réseaux sans fil**  
Risques liés au Wi-Fi, configurations sécurisées, chiffrement WPA3, attaques sur les réseaux mobiles
- 11. Sécurité des ordinateurs portables**  
Vol de matériel, chiffrement des disques, verrouillage, politiques de mobilité sécurisée
- 12. Sécurité des smartphones et tablettes**  
Risques sur plateformes mobiles, applications, IoT, QR-codes, NFC, cloaking
- 13. Sécurité et système d'information**  
Gouvernance IT, politique de sécurité, évaluation des risques, gestion de crise
- 14. La législation**  
Normes, réglementations françaises et internationales de cybersécurité
- 15. Structures et institutions de la sécurité informatique**  
Organisations publiques et privées, acteurs du cyber-défense
- 16. Les bonnes adresses de la sécurité**  
Répertoire commenté de sites web spécialisés, références et ressources utiles