

Sommaire

Partie I – Introduction à la sécurité informatique

1. Les différents types de hackers
2. Motivations et objectifs des attaques
3. Méthodologie d'une attaque informatique
4. Politique de sécurité des systèmes d'information

Partie II – Ingénierie sociale (Social Engineering)

5. Manipulation psychologique
6. Techniques de collecte d'informations
7. Phishing et usurpation d'identité
8. Contre-mesures et sensibilisation

Partie III – Prise d'empreintes (Footprinting)

9. Recherche d'informations publiques
10. Cartographie des systèmes
11. Identification des services réseau
12. Analyse des vulnérabilités

Partie IV – Failles physiques

13. Sécurité des locaux
14. Intrusion physique
15. Vol et compromission de matériels
16. Protection des équipements

Partie V – Sécurité des réseaux

17. Protocoles réseau et vulnérabilités
18. Analyse du trafic
19. Attaques réseau courantes
20. Sécurisation des infrastructures

Partie VI – Sécurité Wi-Fi

21. Normes sans fil
22. Attaques sur les réseaux Wi-Fi
23. Chiffrement et authentification
24. Bonnes pratiques de sécurisation

Partie VII – Sécurité Web

25. Vulnérabilités des applications Web
26. Injection SQL
27. Cross-Site Scripting (XSS)
28. Authentification et gestion des sessions

29. Outils d'audit Web

Partie VIII – Sécurité des systèmes

- 30. Sécurité sous Windows
- 31. Sécurité sous Linux
- 32. Gestion des comptes et privilèges
- 33. Durcissement des systèmes

Partie IX – Sécurité applicative

- 34. Bases de la rétro-ingénierie
- 35. Introduction au langage assembleur
- 36. Dépassements de mémoire tampon
- 37. Analyse des applications

Partie X – Investigations numériques (Forensic)

- 38. Collecte des preuves numériques
- 39. Analyse des systèmes compromis
- 40. Chaîne de conservation des preuves

Partie XI – Sécurité des Box et équipements domestiques

- 41. Fonctionnement des Box Internet
- 42. Vulnérabilités courantes
- 43. Configuration sécurisée

Partie XII – Sécurité matérielle (Hardware Hacking)

- 44. Cartes à puce
- 45. RFID et systèmes embarqués
- 46. Attaques matérielles

Partie XIII – Cloud Computing

- 47. Concepts du Cloud
- 48. Risques de sécurité
- 49. Protection des données dans le Cloud

Partie XIV – Aspects juridiques

- 50. Législation sur la cybersécurité
- 51. Responsabilité des acteurs
- 52. Cadre légal des tests d'intrusion
- 53. Cybercriminalité et preuves numériques