

4<sup>ème</sup> édition

# Sécurité informatique

## Ethical Hacking

Apprendre l'attaque  
pour mieux se défendre

→ Informatique technique



€  
Collection

epsilon

ACISSI

 EPSILON  
Collection



2-005-881-1



4<sup>ème</sup> édition

# Sécurité informatique

## Ethical Hacking

Apprendre l'attaque  
pour mieux se défendre

## Chapitre 1

### Introduction et définitions

|   |    |
|---|----|
| 1. La sécurité informatique, pour quoi, pour qui ? .....                                  | 23 |
| 1.1 Hacking, piratage, sécurité informatique...<br>Que met-on derrière ces termes ? ..... | 23 |
| 1.2 L'importance de la sécurité .....   | 25 |
| 1.2.1 Pour les particuliers .....   | 26 |
| 1.2.2 Pour les entreprises et les écoles .....  | 27 |
| 1.2.3 Pour un pays ou une nation .....  | 28 |
| 2. Le hacking se veut éthique .....   | 30 |
| 2.1 Le travail en coopération .....   | 30 |
| 2.2 Un esprit bidouilleur et passionné avant tout .....                                   | 31 |
| 2.3 Le hacker devient un expert recherché .....   | 31 |
| 2.4 Dans la peau de l'attaquant .....   | 32 |
| 2.5 Conseils et accompagnement vers la sécurisation .....                                 | 33 |
| 3. Connaître son ennemi pour s'en défendre .....  | 34 |
| 3.1 À chaque attaquant son chapeau .....  | 34 |
| 3.1.1 Les hackers black hats .....  | 34 |
| 3.1.2 Les hackers grey hats .....   | 35 |
| 3.1.3 Les hackers white hats .....  | 36 |
| 3.1.4 Les script kiddies .....  | 37 |
| 3.1.5 Les hackers universitaires .....  | 38 |
| 3.2 Et à chaque audit sa boîte à secrets .....  | 38 |
| 3.2.1 Les tests en black box .....  | 39 |
| 3.2.2 Les tests en grey box .....   | 39 |
| 3.2.3 Les tests en white box .....  | 40 |

## Chapitre 2

### Méthodologie d'une attaque

|  |    |
|--|----|
| 1. Préambule .....   | 41 |
| 2. La discrétion avant tout .....                          | 41 |
| 3. Cibler la victime .....                                 | 43 |
| 3.1 Utiliser les bons outils .....                         | 43 |
| 3.2 Repérer les domaines .....                             | 45 |
| 3.3 Google, cet ami si curieux .....                       | 46 |
| 3.4 Découvrir le réseau .....                              | 48 |
| 4. L'attaque .....   | 53 |
| 4.1 Profiter de la faille humaine .....                    | 53 |
| 4.2 Ouvrir les portes du réseau .....                      | 54 |
| 4.3 L'attaque par le Web .....                             | 57 |
| 4.4 La force au service de l'attaque .....                 | 58 |
| 5. S'introduire dans le système et assurer son accès ..... | 59 |
| 5.1 Rester discret .....                                   | 59 |
| 5.2 S'assurer un accès .....                               | 61 |
| 5.3 Étendre son champ d'action .....                       | 63 |
| 6. Bilan de l'intrusion et sécurisation .....              | 63 |
| 6.1 Une politique de sécurité rigoureuse .....             | 64 |
| 6.1.1 Les mots de passe .....                              | 64 |
| 6.1.2 La formation du personnel .....                      | 65 |
| 6.1.3 À chacun son rôle .....                              | 66 |
| 6.2 Chiffrer les informations essentielles .....           | 67 |
| 6.3 Sécuriser les serveurs .....                           | 68 |
| 6.3.1 Effectuer les mises à jour de sécurité .....         | 68 |
| 6.3.2 Emprisonner les services (chroot, jail) .....        | 68 |
| 6.3.3 La sécurité côté noyau .....                         | 69 |
| 6.3.4 Empêcher les scans et les attaques .....             | 69 |
| 6.3.5 Ne garder que l'essentiel .....                      | 70 |
| 6.3.6 Surveillance des activités .....                     | 71 |
| 6.4 Les tests d'intrusion .....                            | 72 |

**Chapitre 3****Éléments d'ingénierie sociale**

|   |     |
|---|-----|
| 1. Généralités .....  | 73  |
| 1.1 Introduction .....                                      | 73  |
| 1.2 Systèmes d'information .....                            | 75  |
| 1.2.1 Précisions sur les systèmes d'information .....       | 75  |
| 1.2.2 Failles d'un système d'information .....              | 77  |
| 1.3 Présentation de l'ingénierie sociale .....              | 77  |
| 1.3.1 Définitions .....                                     | 77  |
| 1.3.2 Caractéristiques et périmètre .....                   | 78  |
| 1.4 Problématique de la protection .....                    | 82  |
| 2. Modes d'action de l'ingénierie sociale .....             | 83  |
| 2.1 Les principes de l'attaque par ingénierie sociale ..... | 83  |
| 2.2 Processus générique de l'ingénieur social .....         | 85  |
| 2.2.1 Étude préalable .....                                 | 86  |
| 2.2.2 Préparation .....                                     | 89  |
| 2.2.3 Exploitation .....                                    | 91  |
| 2.3 Compétences et outils de l'ingénieur social .....       | 93  |
| 2.3.1 Comédies, ruses, subterfuges et tromperies .....      | 93  |
| 2.3.2 Lecture de cible .....                                | 94  |
| 3. Connaissance des organisations attaquées .....           | 95  |
| 3.1 Typologies générales .....                              | 96  |
| 3.2 Typologies de valeurs et de croyances .....             | 97  |
| 3.3 Modèles de maturité et certifications qualité .....     | 100 |
| 3.4 Exploitation .....                                      | 101 |
| 3.5 Exercices .....   | 101 |
| 4. Failles humaines - Bases et modèles théoriques .....     | 101 |
| 4.1 Bases biologiques et fonctionnalités du cerveau .....   | 102 |
| 4.2 Biais cognitifs .....                                   | 104 |
| 4.3 Méthodes hypnotiques .....                              | 106 |
| 4.4 Cohérence et recherche de « pattern » .....             | 107 |
| 4.5 Conclusion .....  | 107 |

|   |     |
|---|-----|
| 4.6 Exercices .....                                   | 108 |
| 4.6.1 Cas particulier du téléphone.....               | 108 |
| 4.6.2 Camouflage final.....                           | 108 |
| 5. Influence et manipulation .....                    | 108 |
| 5.1 Méthodes d'influence.....                         | 108 |
| 5.1.1 Influence .....                                 | 108 |
| 5.1.2 Tentation, séduction et intimidation .....      | 109 |
| 5.1.3 Manipulation.....                               | 110 |
| 5.2 Les grands ressorts de la manipulation .....      | 110 |
| 5.2.1 La cohérence.....                               | 111 |
| 5.2.2 La réciprocité .....                            | 112 |
| 5.2.3 Preuve sociale.....                             | 112 |
| 5.2.4 Autorité .....                                  | 114 |
| 5.2.5 Sympathie .....                                 | 114 |
| 5.2.6 Rareté.....                                     | 115 |
| 6. Les techniques de la manipulation .....            | 117 |
| 6.1 Les grandes techniques de manipulation .....      | 117 |
| 6.1.1 Les amorçages et les leurres.....               | 117 |
| 6.1.2 Le pied dans la porte .....                     | 118 |
| 6.1.3 La porte au nez .....                           | 119 |
| 6.2 Les petites techniques de manipulation .....      | 119 |
| 6.2.1 Pied dans la bouche, politesse, sympathie ..... | 120 |
| 6.2.2 Contact, touché, regard, .....                  | 120 |
| 6.2.3 Les pièges de la cohérence.....                 | 120 |
| 6.2.4 Étiquetage .....                                | 121 |
| 6.2.5 Déclaration de liberté .....                    | 122 |
| 6.2.6 Quelques petites techniques à connaître.....    | 122 |
| 6.3 Exercices .....                                   | 124 |
| 6.3.1 Croiser grandes et petites techniques.....      | 124 |
| 6.3.2 Croiser techniques et ressorts.....             | 124 |
| 6.3.3 Script de camouflage final.....                 | 124 |

|       |  |     |
|-------|--|-----|
| 7.    | Savoir "patcher" les failles humaines .....                          | 124 |
| 7.1   | Volonté politique .....  | 125 |
| 7.2   | Méthodologie .....   | 126 |
| 7.2.1 | Professionalisme, qualité, procédures, maturité .....                | 126 |
| 7.2.2 | Mesure : tests, audit, retest de détection .....                     | 126 |
| 7.2.3 | Optimisation et changement de paradigme .....                        | 127 |
| 7.3   | Actions concrètes à mener .....                                      | 128 |
| 7.3.1 | Documenter une politique de classification<br>de l'information ..... | 128 |
| 7.3.2 | Contrôler les "Input/Output"<br>(entrée/sortie d'information) .....  | 128 |
| 7.3.3 | Instruire le personnel .....   | 129 |
| 7.3.4 | Favoriser la remontée de l'information .....                         | 130 |
| 7.4   | Exercices .....  | 131 |
| 7.4.1 | Manipuler les décideurs .....  | 131 |
| 7.4.2 | Bloc-notes de réponse au téléphone .....                             | 131 |
| 7.4.3 | Remontée d'information .....   | 132 |
| 8.    | Bibliographie .....  | 132 |

## Chapitre 4

### Les prises d'empreintes

|       |   |     |
|-------|---|-----|
| 1.    | Le hacking éthique .....                              | 133 |
| 1.1   | Définition .....                                      | 133 |
| 1.2   | Les différents profils de hackers .....               | 134 |
| 1.3   | Les différents types d'audit .....                    | 135 |
| 1.4   | Les stratégies d'audit .....                          | 135 |
| 1.5   | Méthodologies d'audit .....                           | 136 |
| 2.    | Collecte d'informations .....                         | 136 |
| 2.1   | Le footprinting .....                                 | 138 |
| 2.1.1 | Collecte d'informations via les réseaux sociaux ..... | 140 |
| 2.1.2 | Les outils web .....                                  | 150 |
| 2.1.3 | Les outils d'énumération .....                        | 152 |

|       |  |     |
|-------|--|-----|
| 2.2   | Le fingerprinting .....                  | 160 |
| 2.3   | Découverte de failles potentielles ..... | 178 |
| 2.3.1 | Nessus .....                             | 178 |
| 2.3.2 | OpenVAS .....                            | 180 |
| 2.3.3 | AutoScan Network .....                   | 182 |
| 2.3.4 | Trouver des exploits .....               | 184 |
| 2.4   | Le reporting .....                       | 185 |

## Chapitre 5

### Les failles physiques

|        |  |     |
|--------|--|-----|
| 1.     | Généralités .....  | 187 |
| 2.     | Lockpicking .....  | 188 |
| 3.     | Accès physique direct à l'ordinateur .....   | 189 |
| 3.1    | Accès à un ordinateur éteint dont le BIOS est protégé .....                            | 189 |
| 3.2    | Accès à un ordinateur éteint dont le BIOS n'est pas protégé. .                         | 192 |
| 3.2.1  | Utilisation de Offline NT Password<br>et Registry Editor v110511 .....                 | 193 |
| 3.2.2  | Utilisation de Trinity Rescue Kit .....  | 198 |
| 3.2.3  | Récupérer la base SAM avec Kali Linux<br>(distribution qui succède à Backtrack5) ..... | 201 |
| 3.2.4  | Windows Password Recovery Bootdisk .....   | 205 |
| 3.2.5  | Les différents types d'algorithmes de cryptage .....                                   | 207 |
| 3.2.6  | Les hashes de type LM et NTLM .....  | 208 |
| 3.2.7  | Utiliser John the Ripper<br>pour trouver les mots de passe .....                       | 210 |
| 3.2.8  | Hashcat .....  | 213 |
| 3.2.9  | Utiliser la puissance de la carte graphique .....                                      | 216 |
| 3.2.10 | Utilisation des tables arc-en-ciel (rainbow tables) .....                              | 218 |
| 3.2.11 | Générer ses tables arc-en-ciel .....   | 220 |
| 3.2.12 | Utiliser OPHCRACK .....  | 223 |
| 3.2.13 | Utilisation du logiciel Cain & Abel .....  | 226 |
| 3.2.14 | Utilisation du script Findmyhash .....   | 231 |

|        |  |     |
|--------|--|-----|
| 3.2.15 | Bypass authentification Windows et Linux .....   | 233 |
| 3.2.16 | Contourner l'authentification Windows -<br>Méthode Adam Boileau.....                           | 235 |
| 3.2.17 | Adaptation de winlockpwn : Inception.....  | 240 |
| 3.2.18 | Exemples d'élévation de privilèges via exploits<br>sous Linux .....                            | 243 |
| 3.2.19 | Failles Windows Vista, Windows 7 et Windows 8.1 ..   | 245 |
| 3.3    | Accès à un ordinateur allumé<br>en mode session utilisateur courant .....                      | 247 |
| 3.3.1  | Récolter des informations.....   | 247 |
| 3.3.2  | La récolte d'informations automatisée.....   | 250 |
| 3.3.3  | La clé USB Microsoft COFEE .....   | 253 |
| 3.3.4  | Les clés USB U3 .....  | 257 |
| 3.3.5  | Le logiciel Gonzor-SwitchBlade .....   | 258 |
| 3.3.6  | Contre-mesures aux clés U3 piégées .....   | 262 |
| 3.3.7  | Clé Sandisk U3PWN .....  | 263 |
| 3.3.8  | La clé Ducky.....  | 265 |
| 3.3.9  | Les keyloggers matériels et logiciels .....  | 267 |
| 3.3.10 | Contre-mesures aux keyloggers .....  | 271 |
| 3.3.11 | Récupération d'images mémoire .....  | 276 |
| 3.3.12 | Méthodes de récupération de la mémoire RAM .....   | 277 |
| 3.3.13 | Créer une clé bootable pour vider la mémoire.....  | 284 |
| 3.3.14 | Récupération de la mémoire via le FireWire -<br>Méthode Adam Boileau.....                      | 289 |
| 3.3.15 | Récupération de la mémoire via le FireWire -<br>Méthode Carsten Maartmann-Moe (Inception)..... | 289 |
| 3.3.16 | Analyse des images mémoire .....   | 291 |
| 3.4    | Conclusion .....   | 304 |

## Chapitre 6

## Les failles réseau

|  |     |
|--|-----|
| 1. Généralités .....   | 305 |
| 2. Rappel sur les réseaux TCP/IP .....                                     | 305 |
| 2.1 Le modèle OSI .....  | 306 |
| 2.2 Adressage IPv4 .....   | 307 |
| 2.3 Notion de passerelle, de masque et de sous-réseau .....                | 309 |
| 2.4 TCP et UDP .....   | 310 |
| 2.5 Les services et les ports .....  | 311 |
| 2.6 Les adresses IP publiques et privées .....                             | 312 |
| 3. Outils pratiques .....  | 312 |
| 3.1 Des informations sur les sockets .....                                 | 312 |
| 3.2 Des informations sur une adresse publique<br>ou un nom de domaine      | 315 |
| 3.3 Scanner de ports TCP .....   | 319 |
| 3.4 Gestion des sockets .....  | 319 |
| 3.4.1 Comment prendre la main sur un hôte distant ? .....                  | 321 |
| 3.4.2 Transfert de fichier entre deux machines .....                       | 322 |
| 3.4.3 Prise de contrôle d'un ordinateur sur un réseau privé ..             | 322 |
| 3.5 SSH .....  | 322 |
| 3.6 Tunnel SSH .....   | 324 |
| 3.6.1 Contournement d'un pare-feu afin de joindre<br>un hôte distant ..... | 324 |
| 3.6.2 Autoriser un accès momentané depuis l'extérieur .....                | 327 |
| 4. DoS et DDoS .....   | 328 |
| 4.1 Établissement d'une session TCP .....                                  | 328 |
| 4.2 Principe de l'attaque .....  | 329 |
| 5. Sniffing .....  | 330 |
| 5.1 Capturer des données avec Wireshark .....                              | 332 |
| 5.2 Les filtres .....  | 333 |

|  |     |
|--|-----|
| 6. Man In The Middle (MITM).....                             | 336 |
| 6.1 Théorie .....  | 336 |
| 6.2 Pratique .....   | 338 |
| 6.2.1 Installation de Ettercap.....                          | 338 |
| 6.2.2 Configuration de Ettercap .....                        | 340 |
| 6.2.3 Les plug-ins sous Ettercap.....                        | 343 |
| 6.2.4 Création d'un filtre .....                             | 344 |
| 6.2.5 Cain & Abel .....                                      | 346 |
| 6.3 Contre-mesures.....                                      | 347 |
| 7. Vol de session TCP (hijacking) et spoofing d'IP.....      | 348 |
| 7.1 La faille : l'ACK/SEQ .....                              | 349 |
| 7.2 Conséquence de l'attaque.....                            | 350 |
| 7.3 Mise en pratique.....                                    | 350 |
| 7.4 Automatiser l'attaque .....                              | 353 |
| 7.5 Spoofing d'adresse IP .....                              | 353 |
| 8. Failles Wi-Fi.....  | 357 |
| 8.1 Cracker un réseau WEP .....                              | 358 |
| 8.1.1 Capturer des paquets.....                              | 358 |
| 8.1.2 Générer du trafic .....                                | 359 |
| 8.1.3 Trouver la clé.....                                    | 360 |
| 8.2 Cracker un réseau WPA .....                              | 362 |
| 8.3 Rogue AP.....  | 363 |
| 8.3.1 Introduction au Rogue AP .....                         | 363 |
| 8.3.2 Mise en pratique d'un Rogue AP avec Karmetasploit..... | 364 |
| 9. IP over DNS .....   | 367 |
| 9.1 Principe .....   | 367 |
| 9.2 Exploitation avec l'outil iodine .....                   | 367 |
| 9.3 Contre-mesures.....                                      | 368 |
| 10. La téléphonie sur IP .....                               | 369 |
| 10.1 Écoute de conversation avec VoIPong.....                | 369 |
| 10.2 Usurpation de ligne .....                               | 371 |
| 10.3 Autres attaques.....                                    | 372 |

|                                      |     |
|--------------------------------------|-----|
| 11. IPv6 .....                       | 373 |
| 11.1 Les logiciels .....             | 373 |
| 11.2 Le matériel .....               | 374 |
| 11.3 L'humain .....                  | 374 |
| 11.4 THC-IPv6 .....                  | 375 |
| 11.5 Scanner les hosts .....         | 375 |
| 11.5.1 Sur un réseau local .....     | 375 |
| 11.5.2 Sur Internet .....            | 375 |
| 11.6 Flooder .....                   | 376 |
| 11.7 Attaque Man In The Middle ..... | 377 |
| 12. Conclusion .....                 | 379 |

## Chapitre 7

### Cloud Computing : forces et faiblesses

|  |     |
|--|-----|
| 1. Présentation .....                            | 381 |
| 2. Introduction au Cloud Computing .....         | 382 |
| 2.1 Historique .....                             | 382 |
| 2.2 Concepts clés .....                          | 383 |
| 2.2.1 Facturation à l'usage .....                | 383 |
| 2.2.2 Élasticité et agilité des ressources ..... | 384 |
| 2.2.3 Mutualisation des ressources .....         | 384 |
| 2.2.4 Accès simple via le réseau .....           | 384 |
| 2.3 Les niveaux d'interaction .....              | 384 |
| 2.4 Cloud privé, public, hybride .....           | 386 |
| 2.4.1 Le Cloud public .....                      | 386 |
| 2.4.2 Le Cloud privé .....                       | 386 |
| 2.4.3 Le Cloud hybride .....                     | 387 |
| 2.5 La responsabilité des fournisseurs .....     | 387 |

|       |   |     |
|-------|---|-----|
| 3.    | Les risques liés aux données . . . . .                          | 389 |
| 3.1   | Responsabilité juridique du client et du prestataire . . . . .  | 389 |
| 3.1.1 | Droits et obligations . . . . .                                 | 389 |
| 3.1.2 | Le responsable des données . . . . .                            | 390 |
| 3.1.3 | Obligation d'information du fournisseur . . . . .               | 390 |
| 3.1.4 | Sécurité des données . . . . .                                  | 391 |
| 3.2   | Chiffrement des données . . . . .                               | 391 |
| 3.2.1 | La cryptographie symétrique . . . . .                           | 392 |
| 3.2.2 | La cryptographie asymétrique . . . . .                          | 392 |
| 3.3   | Accessibilité des données . . . . .                             | 393 |
| 3.4   | Disponibilité des données . . . . .                             | 394 |
| 3.5   | Localisation des données . . . . .                              | 395 |
| 3.6   | Protection et récupération des données . . . . .                | 396 |
| 4.    | La sécurité logique dans le Cloud Computing . . . . .           | 397 |
| 4.1   | Virtualisation : les nouveaux risques . . . . .                 | 397 |
| 4.2   | Solutions d'étanchéité logique . . . . .                        | 398 |
| 4.3   | Le facteur humain . . . . .                                     | 399 |
| 4.4   | Sécurité des accès : authentification et autorisation . . . . . | 400 |
| 4.5   | Audits réguliers . . . . .                                      | 401 |
| 5.    | La sécurité physique . . . . .                                  | 403 |
| 5.1   | Contrôle des accès . . . . .                                    | 404 |
| 5.2   | Catastrophes naturelles . . . . .                               | 405 |
| 5.3   | Redondance du matériel . . . . .                                | 406 |
| 5.4   | Normes à appliquer . . . . .                                    | 407 |
| 5.4.1 | TIA 942 . . . . .   | 407 |
| 5.4.2 | ISO 27001 . . . . .   | 407 |
| 5.5   | Audits réguliers . . . . .                                      | 409 |
| 6.    | Attaques via le Cloud Computing . . . . .                       | 410 |
| 6.1   | Description . . . . .   | 410 |
| 6.2   | Cassage de clés : exemple avec un hash SHA1 . . . . .           | 411 |
| 6.3   | Exemple d'une attaque DDoS . . . . .                            | 417 |
| 7.    | Conclusion . . . . .  | 420 |

## Chapitre 8

### Les failles web

|  |     |
|--|-----|
| 1. Rappels sur les technologies du Web . . . . .                                   | 421 |
| 1.1 Préambule . . . . .  | 421 |
| 1.2 Le réseau Internet . . . . .   | 421 |
| 1.3 Qu'est-ce qu'un site web ? . . . . .   | 422 |
| 1.4 Consultation d'une page web,<br>anatomie des échanges client/serveur . . . . . | 422 |
| 1.5 Comment sont réalisées les pages web ? . . . . .                               | 427 |
| 2. Généralités sur la sécurité des sites web . . . . .                             | 430 |
| 3. Petite analyse d'un site web . . . . .  | 431 |
| 3.1 Cartographie des parties visibles d'un site web . . . . .                      | 431 |
| 3.1.1 Le site est-il statique ou dynamique ? . . . . .                             | 432 |
| 3.1.2 Quelles sont les variables utilisées ? . . . . .                             | 434 |
| 3.1.3 Y a-t-il des formulaires et quels champs utilisent-ils ? . . . . .           | 434 |
| 3.1.4 Le serveur envoie-t-il des cookies ? . . . . .                               | 435 |
| 3.1.5 Le site contient-il des médias ? . . . . .                                   | 436 |
| 3.1.6 Le site fait-il appel à des bases de données ? . . . . .                     | 437 |
| 3.1.7 Pouvons-nous accéder à certains dossiers ? . . . . .                         | 437 |
| 3.1.8 Le site fait-il appel à du JavaScript ? . . . . .                            | 438 |
| 3.1.9 Quel serveur est utilisé et quelle est sa version ? . . . . .                | 440 |
| 3.1.10 Des outils pour nous aider . . . . .  | 441 |
| 3.2 Découvrir la face cachée d'un site web . . . . .                               | 443 |
| 3.2.1 Utilisation de Burp Suite . . . . .  | 443 |
| 3.2.2 Utilisation de Wfuzz . . . . .   | 448 |
| 3.3 Analyser les informations récupérées . . . . .                                 | 457 |
| 4. Passer à l'attaque d'un site web . . . . .                                      | 458 |
| 4.1 Envoyer des données non attendues . . . . .                                    | 458 |
| 4.1.1 Principes et outils . . . . .  | 458 |
| 4.1.2 Utilisation de l'URL . . . . .   | 461 |
| 4.1.3 Utilisation des formulaires . . . . .  | 465 |
| 4.1.4 Utilisation de l'en-tête . . . . .   | 469 |
| 4.1.5 Utilisation des cookies . . . . .  | 470 |

|     |   |     |
|-----|---|-----|
| 4.2 | Le vol de session .....                             | 471 |
| 4.3 | Le dépôt de fichiers malicieux .....                | 474 |
| 5.  | Les injections SQL .....                            | 477 |
| 5.1 | Préambule .....                                     | 477 |
| 5.2 | Introduction aux bases de données .....             | 478 |
| 5.3 | Principe des injections SQL .....                   | 491 |
| 5.4 | Technique du Blind SQL .....                        | 502 |
| 5.5 | Des outils efficaces .....                          | 526 |
| 6.  | Passer les CAPTCHA .....                            | 530 |
| 6.1 | Présentation des différents CAPTCHA .....           | 530 |
| 6.2 | Passer les CAPTCHA de base .....                    | 531 |
| 6.3 | Passer les CAPTCHA images .....                     | 535 |
| 7.  | Les nouvelles menaces sur le Web .....              | 542 |
| 8.  | Contre-mesures et conseils de sécurisation .....    | 543 |
| 8.1 | Filtrer toutes les données .....                    | 543 |
| 8.2 | Renforcer l'identification du client .....          | 546 |
| 8.3 | Configurer judicieusement le serveur .....          | 547 |
| 9.  | Utiliser des frameworks pour le développement ..... | 548 |
| 10. | Conclusion .....                                    | 549 |

## Chapitre 9

### Les failles système

|       |  |     |
|-------|--|-----|
| 1.    | Généralités .....                                    | 551 |
| 2.    | Les mots de passe .....                              | 552 |
| 2.1   | Introduction .....                                   | 552 |
| 2.2   | Révéler un mot de passe sous Microsoft Windows ..... | 552 |
| 2.3   | Complexité .....                                     | 553 |
| 2.4   | Le stockage des mots de passe .....                  | 554 |
| 2.4.1 | Précisions sur le stockage des mots de passe .....   | 554 |
| 2.4.2 | Visualisation des empreintes LM et NTLMv1-2 .....    | 556 |

|       |   |     |
|-------|---|-----|
| 2.5   | Cas pratique : trouver les mots de passe sous Microsoft Windows ..... | 559 |
| 2.6   | Cas pratique : trouver les mots de passe sous GNU/Linux .....         | 560 |
| 2.7   | Cas pratique : trouver les mots de passe sous Mac OS X .....          | 561 |
| 2.8   | Changer son mot de passe en ligne de commande .....                   | 562 |
| 2.8.1 | Sous Windows .....  | 562 |
| 2.8.2 | Sous GNU/Linux .....  | 563 |
| 2.8.3 | Sous Mac OS X .....   | 563 |
| 3.    | Utilisateurs, groupes et permissions sur le système .....             | 564 |
| 3.1   | Gestion des utilisateurs .....  | 564 |
| 3.1.1 | Définition .....  | 564 |
| 3.1.2 | Sous GNU/Linux .....  | 565 |
| 3.1.3 | Sous Windows .....  | 566 |
| 3.1.4 | Sous Mac OS X .....   | 567 |
| 3.2   | Gestion des groupes .....   | 569 |
| 3.2.1 | Sous GNU/Linux .....  | 570 |
| 3.2.2 | Sous Windows .....  | 570 |
| 3.2.3 | Sous Mac OS X .....   | 570 |
| 3.3   | Affectation des permissions .....                                     | 570 |
| 3.3.1 | Sous GNU/Linux .....  | 570 |
| 3.3.2 | Sous Windows .....  | 572 |
| 3.3.3 | Sous Mac OS X .....   | 573 |
| 4.    | Élévation des privilèges .....  | 574 |
| 4.1   | Sous UNIX .....   | 574 |
| 4.1.1 | Activation du suid et du sgid .....                                   | 575 |
| 4.1.2 | Comment trouver les scripts suid root d'un système GNU/Linux .....    | 576 |
| 4.2   | Sous Windows .....  | 576 |
| 4.3   | Le Planificateur de tâches .....                                      | 581 |
| 5.    | Les processus .....   | 582 |
| 5.1   | Espionner des processus sous Windows .....                            | 583 |

|        |   |     |
|--------|---|-----|
| 5.2    | Le hooking et l'injection de processus .....                                | 584 |
| 5.2.1  | Exemple de hooking des événements<br>du clavier sous Windows .....          | 585 |
| 5.2.2  | Exemple de hooking des paquets réseau<br>via Netfilter sous GNU/Linux ..... | 589 |
| 5.2.3  | Exemple d'injection de code<br>dans un autre processus sous Mac OS X .....  | 591 |
| 5.3    | Les situations de concurrence (race conditions) .....                       | 592 |
| 6.     | Le démarrage .....  | 593 |
| 6.1    | L'abus des modes de démarrage dégradés .....                                | 594 |
| 6.2    | Les attaques de preboot .....   | 594 |
| 7.     | L'hibernation .....   | 595 |
| 8.     | Les appels de procédures distantes .....                                    | 595 |
| 8.1    | Principe .....  | 595 |
| 8.2    | L'accès au registre à distance .....  | 596 |
| 9.     | SELinux et AppArmor .....   | 596 |
| 10.    | La virtualisation .....   | 596 |
| 10.1   | L'isolation .....   | 597 |
| 10.2   | Le changement de racine ou chrooting .....                                  | 598 |
| 10.3   | Noyau en espace utilisateur .....   | 598 |
| 10.4   | La machine virtuelle .....  | 599 |
| 10.5   | La paravirtualisation .....   | 599 |
| 10.6   | Exemple de solution de paravirtualisation : Proxmox VE .....                | 600 |
| 10.7   | Détection et attaque d'une machine virtuelle .....                          | 601 |
| 11.    | Les logs, les mises à jour et la sauvegarde .....                           | 602 |
| 11.1   | Les logs .....  | 602 |
| 11.2   | Les mises à jour .....  | 603 |
| 11.2.1 | Mise en place des mises à jour automatiques<br>sous GNU/Linux .....         | 604 |
| 11.2.2 | Mise en place des mises à jour automatiques<br>sous Microsoft Windows ..... | 604 |

|  |     |
|--|-----|
| 11.2.3 Mise en place des mises à jour automatiques | 604 |
| sous Mac OS X .....                                | 604 |
| 11.3 Les sauvegardes .....                         | 605 |
| 12. Bilan .....                                    | 605 |

## Chapitre 10

### Les failles applicatives

|  |     |
|--|-----|
| 1. Généralités .....                               | 607 |
| 2. Notions d'Assembleur .....                      | 608 |
| 2.1 Introduction .....                             | 608 |
| 2.2 Premiers pas .....                             | 608 |
| 2.2.1 Apprenons à compter .....                    | 608 |
| 2.2.2 Le binaire .....                             | 608 |
| 2.2.3 L'hexadécimal .....                          | 610 |
| 2.3 Comment tester nos programmes ? .....          | 611 |
| 2.3.1 Squelette d'un programme en Assembleur ..... | 611 |
| 2.3.2 Notre premier programme .....                | 613 |
| 2.4 Les instructions .....                         | 614 |
| 2.4.1 La comparaison .....                         | 614 |
| 2.4.2 L'instruction IF .....                       | 615 |
| 2.4.3 La boucle FOR .....                          | 617 |
| 2.4.4 La boucle WHILE .....                        | 617 |
| 2.4.5 La boucle DO WHILE .....                     | 618 |
| 2.4.6 La directive %define .....                   | 619 |
| 2.4.7 Directives de données .....                  | 619 |
| 2.4.8 Entrées-sorties .....                        | 620 |
| 2.5 Les interruptions .....                        | 621 |
| 2.6 Les sous-programmes .....                      | 623 |
| 2.7 Le heap et la pile .....                       | 624 |
| 2.7.1 Le heap .....                                | 624 |
| 2.7.2 La pile .....                                | 625 |

|  |     |
|--|-----|
| 2.7.3 Appel et retour de fonction :<br>les notions fondamentales ..... | 627 |
| 3. Bases des shellcodes .....  | 628 |
| 3.1 Exemple 1 : shellcode.py .....                                     | 629 |
| 3.2 Exemple 2 : execve() .....   | 630 |
| 3.3 Exemple 3 : Port Binding Shell .....                               | 632 |
| 4. Les buffer overflows .....  | 634 |
| 4.1 Quelques définitions .....   | 634 |
| 4.2 Notions essentielles .....   | 635 |
| 4.3 Stack overflow .....   | 637 |
| 4.4 Heap overflow .....  | 645 |
| 4.5 return-into-libc .....   | 648 |
| 5. Les failles Windows .....   | 653 |
| 5.1 Introduction .....   | 653 |
| 5.2 Premiers pas .....   | 654 |
| 5.2.1 En mode console .....  | 654 |
| 5.2.2 Débogage .....   | 656 |
| 5.2.3 Problème d'un grand shellcode .....                              | 662 |
| 5.2.4 Exécution d'une fonction non prévue .....                        | 665 |
| 5.2.5 Autres méthodes .....  | 667 |
| 5.3 La méthode du call [reg] .....                                     | 667 |
| 5.4 La méthode pop ret. ....   | 668 |
| 5.5 La méthode du push return .....                                    | 668 |
| 5.6 La méthode du jmp [reg] + [offset] .....                           | 669 |
| 5.7 La méthode du blind return .....                                   | 669 |
| 5.8 Que faire avec un petit shellcode ? .....                          | 670 |
| 5.8.1 Principe .....   | 670 |
| 5.8.2 En pratique .....  | 670 |
| 5.9 Le SEH (Structured Exception Handling) .....                       | 671 |
| 5.9.1 Les bases .....  | 671 |
| 5.9.2 SEH, les protections .....                                       | 673 |
| 5.9.3 XOR et Safe-SEH .....  | 673 |

|  |     |
|--|-----|
| 5.10 Passer les protections .....                | 675 |
| 5.10.1 Stack cookie, protection /GS .....        | 675 |
| 5.10.2 Exemple : outrepasser le cookie .....     | 679 |
| 5.10.3 SafeSEH .....                             | 682 |
| 6. Cas concret : Ability Server .....            | 683 |
| 6.1 Fuzzing .....                                | 683 |
| 6.2 Exploitation .....                           | 686 |
| 7. Cas concret : MediaCoder-0.7.5.4796 .....     | 692 |
| 7.1 Crash du logiciel .....                      | 692 |
| 7.2 Vérification des valeurs .....               | 697 |
| 7.3 Finalisation de l'exploit .....              | 698 |
| 8. Cas concret : BlazeDVD 5.1 Professional ..... | 701 |
| 9. Conclusion .....                              | 704 |
| 10. Références .....                             | 705 |

## Chapitre 11 Forensic

|  |     |
|--|-----|
| 1. Introduction .....                      | 707 |
| 1.1 Le cerveau .....                       | 709 |
| 1.2 La mémoire .....                       | 709 |
| 1.3 Les fichiers .....                     | 712 |
| 2. Les méthodes .....                      | 713 |
| 2.1 Préparation et environnement .....     | 713 |
| 2.2 Recherche et analyse de fichiers ..... | 714 |
| 3. Les outils .....                        | 717 |
| 3.1 Les outils d'analyse réseau .....      | 718 |
| 3.1.1 Wireshark .....                      | 718 |
| 3.1.2 tcpdump .....                        | 719 |
| 3.1.3 Scapy .....                          | 719 |

|       |                                    |     |
|-------|------------------------------------|-----|
| 3.2   | Les outils d'analyse mémoire ..... | 720 |
| 3.2.1 | Volatility .....                   | 720 |
| 3.3   | Les outils d'analyse binaire ..... | 720 |
| 3.3.1 | Hexdump .....                      | 720 |
| 3.3.2 | Readelf .....                      | 721 |
| 3.3.3 | Gdb .....                          | 722 |
| 3.4   | Les outils d'analyse système ..... | 723 |
| 3.4.1 | The coroner's toolkit .....        | 723 |
| 3.4.2 | Logstash .....                     | 723 |
| 4.    | Conclusion .....                   | 724 |

## Chapitre 12

### La sécurité des box

|     |  |     |
|-----|--|-----|
| 1.  | Les fonctionnalités d'une box .....          | 725 |
| 1.1 | Routeur .....                                | 725 |
| 1.2 | Switch .....                                 | 725 |
| 1.3 | Téléphonie .....                             | 726 |
| 1.4 | TV .....                                     | 726 |
| 1.5 | Serveur multimédia .....                     | 727 |
| 2.  | Les différentes box .....                    | 727 |
| 2.1 | Orange .....                                 | 727 |
| 2.2 | Free .....                                   | 728 |
| 2.3 | Bouygues .....                               | 729 |
| 2.4 | SFR .....                                    | 730 |
| 3.  | La configuration des box .....               | 731 |
| 3.1 | Le mode modem .....                          | 731 |
| 3.2 | Le mode routeur .....                        | 732 |
| 3.3 | Les fonctions téléphoniques .....            | 733 |
| 4.  | La configuration par défaut, un danger ..... | 734 |
| 4.1 | L'interface d'administration web .....       | 734 |
| 4.2 | Le Wi-Fi .....                               | 735 |

|     |   |     |
|-----|---|-----|
| 4.3 | Les services : SSH, Telnet, Samba .....       | 736 |
| 5.  | Détournement des fonctions initiales .....    | 738 |
| 5.1 | Dans quel intérêt ? .....                     | 738 |
| 5.2 | Personnalisation d'un firmware existant ..... | 739 |
| 6.  | La sécurité des firmwares officiels .....     | 746 |
| 6.1 | Les failles de ces dernières années .....     | 746 |
| 6.2 | Et actuellement ? .....                       | 747 |

## **Chapitre 13**

### **Les failles matérielles**

|       |  |     |
|-------|--|-----|
| 1.    | Introduction .....                               | 749 |
| 2.    | La trousse à outils .....                        | 750 |
| 2.1   | L'outillage de base .....                        | 750 |
| 2.1.1 | Lot de tournevis .....                           | 750 |
| 2.1.2 | Le multimètre .....                              | 751 |
| 2.1.3 | Platine de test .....                            | 752 |
| 2.1.4 | Les câbles Dupont .....                          | 752 |
| 2.1.5 | Fer à souder .....                               | 753 |
| 2.1.6 | Arduino .....                                    | 753 |
| 2.1.7 | Matériels de récupération .....                  | 754 |
| 2.2   | Utilisateur régulier .....                       | 754 |
| 2.2.1 | Adaptateur USB RS232 TTL .....                   | 754 |
| 2.2.2 | Sonde d'analyse logique .....                    | 755 |
| 2.2.3 | Interface JTAG .....                             | 755 |
| 2.2.4 | Le bus pirate de chez Dangerous Prototypes ..... | 756 |
| 2.2.5 | SDR low cost .....                               | 756 |
| 2.3   | Utilisateur avancé .....                         | 758 |
| 2.3.1 | Logiciel de conception de PCB .....              | 758 |
| 2.3.2 | Programmeur .....                                | 758 |
| 2.3.3 | Matériel d'électronicien .....                   | 760 |

|       |  |     |
|-------|--|-----|
| 2.4   | Méthodologie du reverse engineering matériel . . . . . | 760 |
| 2.4.1 | Attaque via Sniffing I2C . . . . .                     | 763 |
| 2.4.2 | Attaque via Sniffing UART modem . . . . .              | 766 |
| 2.5   | Étude et bidouille autour des T2G et Arduino . . . . . | 768 |
| 2.5.1 | Création d'un lecteur de cartes T2G . . . . .          | 769 |
| 2.5.2 | Émulateur partiel de carte T2G . . . . .               | 777 |

## Chapitre 14

### Risques juridiques et solutions

|       |  |     |
|-------|--|-----|
| 1.    | Préambule . . . . .  | 781 |
| 2.    | Atteintes à un système d'information . . . . .                             | 783 |
| 2.1   | Accès et maintien dans un système d'information . . . . .                  | 783 |
| 2.1.1 | Élément matériel . . . . .   | 786 |
| 2.1.2 | Élément moral . . . . .  | 788 |
| 2.2   | Atteinte au fonctionnement d'un système d'information . . . . .            | 790 |
| 2.3   | Atteinte aux données d'un système d'information . . . . .                  | 793 |
| 2.4   | Diffusion d'un logiciel d'intrusion . . . . .                              | 795 |
| 3.    | Atteintes aux traitements de données à caractère personnel . . . . .       | 797 |
| 3.1   | Notion de données à caractère personnel . . . . .                          | 797 |
| 3.2   | Cas particulier de l'adresse IP . . . . .                                  | 799 |
| 3.3   | Proposition de règlement européen . . . . .                                | 801 |
| 3.4   | Collecte illicite de données à caractère personnel . . . . .               | 805 |
| 3.5   | Divulgence illicite de données à caractère personnel . . . . .             | 806 |
| 3.6   | Obligation de sécurité du responsable de traitement . . . . .              | 807 |
| 3.7   | Obligation de notification des failles de sécurité . . . . .               | 815 |
| 3.8   | Contrôles en ligne de la CNIL . . . . .                                    | 818 |
| 3.9   | Obligation de conservation des données de connexion . . . . .              | 819 |
| 3.10  | Obligation de conservation des données<br>relatives aux contenus . . . . . | 820 |
| 3.11  | Accès administratif aux données de connexion . . . . .                     | 822 |
| 3.12  | Les autres obligations spécifiques des FAI et hébergeurs . . . . .         | 823 |

|   |     |
|---|-----|
| 4. Infractions classiques applicables à l'informatique .....                        | 826 |
| 4.1 L'escroquerie .....   | 826 |
| 4.2 L'usurpation d'identité .....   | 827 |
| 4.3 Atteinte au secret des correspondances .....                                    | 829 |
| 4.4 La dégradation physique d'un système .....                                      | 833 |
| 4.5 Le vol d'informations ? .....   | 834 |
| 5. Solutions et précautions .....   | 835 |
| 5.1 Encadrement contractuel des tests d'intrusion .....                             | 836 |
| 5.1.1 Exonérations de responsabilité du prestataire .....                           | 836 |
| 5.1.2 Périmètre des tests d'intrusion .....   | 840 |
| 5.1.3 Principes dégagés par la Charte FPTI .....                                    | 840 |
| 5.2 Hors cadre contractuel : la révélation publique<br>de failles de sécurité ..... | 841 |
| 5.2.1 Révélation d'une faille relative à un serveur .....                           | 842 |
| 5.2.2 Révélation d'une faille relative<br>à un système d'exploitation .....         | 845 |
| 5.2.3 Conseils quant à la divulgation de failles de sécurité ..                     | 847 |
| 6. Conclusion .....   | 850 |
| 7. Références .....   | 851 |
| <br>  |     |
| Index .....   | 853 |