

Editions ENI

# **Sécurité informatique** **Ethical Hacking**

**Apprendre l'attaque  
pour mieux se défendre**

(5<sup>e</sup> édition)

Collection  
Epsilon

Table des matières

## Chapitre 1 Introduction et définitions

1. La sécurité informatique, pour quoi, pour qui ?	23
1.1 Hacking, piratage, sécurité informatique... Que met-on derrière ces termes ?	23
1.2 L'importance de la sécurité	25
1.2.1 Pour les particuliers	25
1.2.2 Pour les entreprises et les écoles	26
1.2.3 Pour un pays ou une nation	27
2. Le hacking se veut éthique	28
2.1 Le travail en coopération	28
2.2 Un esprit bidouilleur et passionné avant tout	29
2.3 Le hacker devient un expert recherché	29
2.4 Dans la peau de l'attaquant	30
2.5 Conseils et accompagnement vers la sécurisation	31
3. Connaître son ennemi pour s'en défendre	32
3.1 À chaque attaquant son chapeau.	32
3.1.1 Les hackers black hats	32
3.1.2 Les hackers grey hats	32
3.1.3 Les hackers white hats.	33
3.1.4 Les script kiddies	34
3.1.5 Les hackers universitaires	34
3.2 Et à chaque audit sa boîte à secrets	35
3.2.1 Les tests en black box	35
3.2.2 Les tests en grey box	36
3.2.3 Les tests en white box.	36

## Chapitre 2 Méthodologie d'une attaque

1. Préambule.	37
2. La discrétion avant tout	37
3. Cibler la victime.	39
3.1 Utiliser les bons outils	39
3.2 Repérer les domaines	40

# 2 \_\_\_\_\_ Sécurité informatique

Ethical Hacking

3.3	Google, cet ami si curieux . . . . .	41
3.4	Découvrir le réseau . . . . .	43
4.	L'attaque . . . . .	47
4.1	Profiter de la faille humaine . . . . .	47
4.2	Ouvrir les portes du réseau . . . . .	48
4.3	L'attaque par le Web . . . . .	50
4.4	La force au service de l'attaque . . . . .	51
5.	S'introduire dans le système et assurer son accès . . . . .	52
5.1	Rester discret . . . . .	52
5.2	S'assurer un accès . . . . .	54
5.3	Étendre son champ d'action . . . . .	55
6.	Bilan de l'intrusion et sécurisation . . . . .	55
6.1	Une politique de sécurité rigoureuse . . . . .	56
6.1.1	Les mots de passe . . . . .	56
6.1.2	La formation du personnel . . . . .	57
6.1.3	À chacun son rôle . . . . .	57
6.2	Chiffrer les informations essentielles . . . . .	58
6.3	Sécuriser les serveurs . . . . .	59
6.3.1	Effectuer les mises à jour de sécurité . . . . .	59
6.3.2	Emprisonner les services (chroot, jail) . . . . .	59
6.3.3	La sécurité côté noyau . . . . .	60
6.3.4	Empêcher les scans et les attaques . . . . .	60
6.3.5	Ne garder que l'essentiel . . . . .	61
6.3.6	Surveillance des activités . . . . .	61
6.4	Les tests d'intrusion . . . . .	62

## Chapitre 3 Éléments d'ingénierie sociale

1.	Généralités . . . . .	63
1.1	Introduction . . . . .	63
1.2	Systèmes d'information . . . . .	65
1.2.1	Précisions sur les systèmes d'information . . . . .	65
1.2.2	Faibles d'un système d'information . . . . .	66

1.3	Présentation de l'ingénierie sociale . . . . .	66
1.3.1	Définitions . . . . .	66
1.3.2	Caractéristiques et périmètre . . . . .	67
1.4	Problématique de la protection . . . . .	70
2.	Modes d'action de l'ingénierie sociale . . . . .	71
2.1	Les principes de l'attaque par ingénierie sociale . . . . .	71
2.2	Processus générique de l'ingénieur social . . . . .	72
2.2.1	Étude préalable . . . . .	73
2.2.2	Préparation . . . . .	76
2.2.3	Exploitation . . . . .	77
2.3	Compétences et outils de l'ingénieur social . . . . .	78
2.3.1	Comédies, ruses, subterfuges et tromperies . . . . .	79
2.3.2	Lecture de cible . . . . .	79
3.	Connaissance des organisations attaquées . . . . .	80
3.1	Typologies générales . . . . .	81
3.2	Typologies de valeurs et de croyances . . . . .	81
3.3	Modèles de maturité et certifications qualité . . . . .	84
3.4	Exploitation . . . . .	85
3.5	Exercices . . . . .	85
4.	Faillles humaines - Bases et modèles théoriques . . . . .	85
4.1	Bases biologiques et fonctionnalités du cerveau . . . . .	86
4.2	Biais cognitifs . . . . .	87
4.3	Méthodes hypnotiques . . . . .	88
4.4	Cohérence et recherche de « pattern » . . . . .	89
4.5	Conclusion . . . . .	90
4.6	Exercices . . . . .	90
4.6.1	Cas particulier du téléphone . . . . .	90
4.6.2	Camouflage final . . . . .	90
5.	Influence et manipulation . . . . .	90
5.1	Méthodes d'influence . . . . .	91
5.1.1	Influence . . . . .	91
5.1.2	Tentation, séduction et intimidation . . . . .	91
5.1.3	Manipulation . . . . .	92
5.2	Les grands ressorts de la manipulation . . . . .	92
5.2.1	La cohérence . . . . .	93
5.2.2	La réciprocité . . . . .	93

# 4 \_\_\_\_\_ Sécurité informatique

Ethical Hacking

5.2.3	Preuve sociale	94
5.2.4	Autorité	95
5.2.5	Sympathie	96
5.2.6	Rareté	96
6.	Les techniques de la manipulation	97
6.1	Les grandes techniques de manipulation	98
6.1.1	Les amorçages et les leurres	98
6.1.2	Le pied dans la porte	99
6.1.3	La porte au nez	99
6.2	Les petites techniques de manipulation	100
6.2.1	Pied dans la bouche, politesse, sympathie	100
6.2.2	Contact, touché, regard	100
6.2.3	Les pièges de la cohérence	100
6.2.4	Étiquetage	101
6.2.5	Déclaration de liberté	101
6.2.6	Quelques petites techniques à connaître	102
6.3	Exercices	103
6.3.1	Croiser grandes et petites techniques	103
6.3.2	Croiser techniques et ressorts	103
6.3.3	Script de camouflages final	103
7.	Savoir "patcher" les failles humaines	104
7.1	Volonté politique	104
7.2	Méthodologie	105
7.2.1	Professionalisme, qualité, procédures, maturité	105
7.2.2	Mesure : tests, audit, retest de détection	105
7.2.3	Optimisation et changement de paradigme	106
7.3	Actions concrètes à mener	106
7.3.1	Documenter une politique de classification de l'information	106
7.3.2	Contrôler les "Input/Output" (entrée/sortie d'information)	107
7.3.3	Instruire le personnel	108
7.3.4	Favoriser la remontée de l'information	108
7.4	Exercices	109
7.4.1	Manipuler les décideurs	109
7.4.2	Bloc-notes de réponse au téléphone	109
7.4.3	Remontée d'information	110
8.	Bibliographie	110

**Chapitre 4**  
**Les failles physiques**

- 1. Généralités . . . . . 111
- 2. Lockpicking . . . . . 112
- 3. Accès physique direct à l'ordinateur . . . . . 112
  - 3.1 Accès à un ordinateur éteint dont le BIOS est protégé . . . . . 112
  - 3.2 Accès à un ordinateur éteint dont le BIOS n'est pas protégé . . . . . 116
    - 3.2.1 Utilisation de Offline NT Password et Registry Editor v110511 . . . . . 116
    - 3.2.2 Utilisation de Trinity Rescue Kit . . . . . 120
    - 3.2.3 Récupérer la base SAM avec Kali Linux (distribution qui succède à Backtrack5) . . . . . 122
    - 3.2.4 Windows Password Recovery Bootdisk . . . . . 127
    - 3.2.5 Les différents types d'algorithmes de cryptage . . . . . 128
    - 3.2.6 Les hashes de type LM et NTLM . . . . . 129
    - 3.2.7 Utiliser John the Ripper pour trouver les mots de passe . . . . . 131
    - 3.2.8 Hashcat . . . . . 134
    - 3.2.9 Utiliser la puissance de la carte graphique . . . . . 136
    - 3.2.10 Méthode des tables arc-en-ciel (rainbow tables) . . . . . 138
    - 3.2.11 Générer ses tables arc-en-ciel . . . . . 140
    - 3.2.12 Utiliser OPHCRACK . . . . . 141
    - 3.2.13 Utilisation du logiciel Cain & Abel . . . . . 144
    - 3.2.14 Utilisation du script Findmyhash . . . . . 148
    - 3.2.15 Bypass authentification Windows et Linux . . . . . 150
    - 3.2.16 Firewire-Inception-Bypass authentification . . . . . 152
    - 3.2.17 Utilitaires de récupération de mots de passe . . . . . 153
    - 3.2.18 Mimikatz - Manipulations en mémoire . . . . . 157
    - 3.2.19 Exemples d'élévation de privilèges via exploits sous Linux . . . . . 160
    - 3.2.20 Failles Windows Vista, Windows 7 et Windows 8.1 . . . . . 161
    - 3.2.21 Windows-privesc-check-Recherche de failles sous Windows . . . . . 163
  - 3.3 Accès à un ordinateur allumé en mode session utilisateur courant . . . . . 165
    - 3.3.1 Les clés USB . . . . . 165
    - 3.3.2 U3PWN . . . . . 165
    - 3.3.3 La clé Ducky . . . . . 167
    - 3.3.4 Les keyloggers matériels et logiciels . . . . . 169
    - 3.3.5 Contre-mesures aux keyloggers . . . . . 173

# 6 --- Sécurité informatique

Ethical Hacking

3.3.6	Récupération d'images mémoire . . . . .	176
3.3.7	Méthodes de récupération de la mémoire RAM . . . . .	178
3.3.8	Créer une clé bootable pour vider la mémoire . . . . .	182
3.3.9	Récupération de la mémoire via le port FireWire - Méthode Carsten Maartmann-Moe (Inception) . . . . .	187
3.3.10	Dump mémoire sous Linux . . . . .	188
3.3.11	Analyse des images mémoire . . . . .	191
3.4	Conclusion . . . . .	203

## Chapitre 5

### Prise d'empreinte ou Information Gathering

1.	Les attaques . . . . .	205
1.1	Préambule . . . . .	205
1.2	Introduction sur les différents types d'attaques . . . . .	205
1.3	L'attaque de type destructif . . . . .	206
1.4	L'attaque sur les moyens de communication . . . . .	206
1.5	Les attaques à but mercantile . . . . .	207
1.6	Les attaques de type APT . . . . .	207
1.7	Les différentes phases d'une attaque et d'un test d'intrusion . . . . .	208
2.	L'analyse des risques . . . . .	209
3.	Le test d'intrusion . . . . .	211
3.1	Les acteurs du hacking . . . . .	211
3.2	Types et stratégies d'audit . . . . .	212
3.2.1	Les types d'audit . . . . .	212
3.2.2	Les stratégies d'audit . . . . .	212
4.	Méthodologie d'une collecte d'informations également appelée "prise d'empreintes" . . . . .	213
5.	Le service Whois . . . . .	213
5.1	La gestion des adresses IP dans le monde . . . . .	214
5.2	Recherche d'informations sur le Web . . . . .	216
5.3	Les basiques . . . . .	216
5.4	Les sites web spécialisés . . . . .	217
5.5	Les réseaux sociaux et professionnels . . . . .	219
5.6	Les agrégateurs d'informations spécialisés . . . . .	221
5.7	Les add-ons navigateurs spécialisés . . . . .	223

- 5.8 Un navigateur dédié à la recherche OSINT : Oryon ..... 224
- 5.9 Application spécifique : Net Tools ..... 226
- 6. Moteurs de recherche de périphériques connectés ..... 226
  - 6.1 Shodan : la référence. .... 226
  - 6.2 ThingFul : un moteur de recherche pour les IoT (Internet of Things) ..... 233
  - 6.3 Censys : tout sur les appareils connectés en IPv4 sur le Net ..... 235
  - 6.4 Zoomeye : l'alternative chinoise ..... 237
- 7. Recherche d'informations avec Google Hack. .... 238
  - 7.1 Le Big Data ..... 238
  - 7.2 Les techniques utilisées ..... 238
  - 7.3 Google - Historique et clés de son succès ..... 239
  - 7.4 Google incontournable sur le Web. .... 239
  - 7.5 Définition du Google Hacking. .... 239
  - 7.6 Fonctionnement du moteur de recherche. .... 240
  - 7.7 Le référencement Google ..... 241
  - 7.8 Google Hack : les opérateurs basiques de Google ..... 241
  - 7.9 Les opérateurs avancés ..... 242
  - 7.10 Les opérateurs spécifiques ..... 243
  - 7.11 Les Google Dorks ..... 243
  - 7.12 Une interface graphique pour Google Hack et Bing Hack ..... 249
- 8. Applications graphiques dédiées à la recherche d'informations ..... 250
  - 8.1 Maltego ..... 250
  - 8.2 Foca Free ..... 252
  - 8.3 The Harvester ..... 254
  - 8.4 Uberharvest. .... 256
- 9. Énumération DNS - Commandes et scripts ..... 256
  - 9.1 Nslookup ..... 256
  - 9.2 Host ..... 257
  - 9.3 Dig ..... 258
  - 9.4 Dnsenum. .... 259
  - 9.5 Dnsbf ..... 260
    - 9.5.1 Fierce. .... 261
  - 9.6 Bluto ..... 261



# 8 \_\_\_\_\_ Sécurité informatique

Ethical Hacking

10. Les scanners de ports . . . . .	262
10.1 Nmap - Network Mapper . . . . .	262
10.1.1 Utilisation de nmap . . . . .	264
10.1.2 Services et protocoles . . . . .	265
10.1.3 Scan en Idle Scan . . . . .	268
10.1.4 Scans avancés - Utilisation des scripts nmap (.nse). . . . .	270
10.2 Le scanner de masse Masscan. . . . .	272
10.3 Le scanner web Httpprint . . . . .	273
10.4 Dmitry (Deepmagic Information Gathering Tool). . . . .	273
11. Frameworks et collecte d'informations . . . . .	274
11.1 Metasploit . . . . .	274
11.2 Recon-ng . . . . .	274
11.3 SpiderFoot . . . . .	276
12. Les scanners de vulnérabilités . . . . .	277
12.1 Nessus - Scanner de réseau . . . . .	277
12.2 OpenVAS - Scanner de réseau open source . . . . .	285
12.3 AutoScan Network - Scanner de vulnérabilités réseau. . . . .	289
12.4 Nikto - Scanner de vulnérabilités web. . . . .	291
13. Le protocole SNMP - Simple Network Management Protocol. . . . .	293
13.1 Les requêtes SNMP . . . . .	294
13.2 Les réponses SNMP . . . . .	294
13.3 Les alertes SNMP (traps, notifications). . . . .	294
13.4 La MIB . . . . .	294
13.5 Les outils SNMP . . . . .	295
13.6 SNMP et la sécurité. . . . .	295
13.7 L'outil snmpwalk. . . . .	296
13.8 L'outil snmpcheck . . . . .	297
13.9 Quelques règles de sécurité. . . . .	297
14. Le reporting . . . . .	298
15. Pour conclure . . . . .	299

**Chapitre 6**  
**La sécurité des communications sans fil**

- 1. Présentation . . . . . 301
- 2. Les objets connectés . . . . . 302
- 3. Les transmissions radio . . . . . 302
- 4. La radio logicielle . . . . . 305
- 5. Le matériel disponible . . . . . 306
  - 5.1 La clé RTL-SDR . . . . . 306
  - 5.2 Le HackRF One . . . . . 307
  - 5.3 Le bladeRF . . . . . 308
  - 5.4 Le PandwaRF . . . . . 309
  - 5.5 L'USRP . . . . . 311
- 6. Les protocoles . . . . . 312
  - 6.1 Le ZigBee . . . . . 312
  - 6.2 Le Zwave . . . . . 315
  - 6.3 Le Bluetooth . . . . . 317
- 7. La suite GNU-RADIO . . . . . 319
  - 7.1 Les bases de gnuradio-companion . . . . . 321
  - 7.2 Module Python . . . . . 328
  - 7.3 Module écrit en CPP (C plus plus) . . . . . 335
- 8. Exemples d'applications . . . . . 339
  - 8.1 Communication NRF24 . . . . . 340
  - 8.2 Communication ZigBee . . . . . 348
- 9. Conclusion . . . . . 354

**Chapitre 7**  
**Les failles réseau**

- 1. Généralités . . . . . 355
- 2. Rappel sur les réseaux TCP/IP . . . . . 355
  - 2.1 Le modèle OSI . . . . . 355
  - 2.2 Adressage IPv4 . . . . . 356
  - 2.3 Notion de passerelle, de masque et de sous-réseau . . . . . 357
  - 2.4 TCP et UDP . . . . . 359

2.5	Les services et les ports . . . . .	359
2.6	Les adresses IP publiques et privées . . . . .	360
3.	Outils pratiques . . . . .	361
3.1	Des informations sur les sockets . . . . .	361
3.2	Des informations sur une adresse publique ou un nom de domaine . . . . .	364
3.3	Scanner de ports TCP . . . . .	364
3.3.1	Scanner sa propre machine . . . . .	365
3.3.2	Scanner un sous-réseau . . . . .	365
3.3.3	Scanner un réseau sans communiquer directement avec la cible . . . . .	367
3.3.4	Scanner un réseau sans scanner les ports . . . . .	368
3.3.5	Scanner un réseau via TCP SYN scan (Half Open scan) . . . . .	370
3.3.6	Scanner un réseau via TCP XMAS scan et Maimon scan . . . . .	380
3.3.7	Scanner un réseau via TCP FIN scan . . . . .	382
3.3.8	Scanner un réseau via TCP NULL scan . . . . .	383
3.3.9	Scanner un réseau via TCP IDLE scan . . . . .	383
3.3.10	Scanner un réseau via UDP scan . . . . .	386
3.3.11	Scanner un réseau via TCP-ACK scan . . . . .	388
3.4	Gestion des sockets . . . . .	389
3.4.1	Comment prendre la main sur un hôte distant ? . . . . .	389
3.4.2	Transfert de fichier entre deux machines . . . . .	391
3.4.3	Prise de contrôle d'un ordinateur sur un réseau privé . . . . .	391
3.5	SSH . . . . .	392
3.6	Tunnel SSH . . . . .	394
3.6.1	Contournement d'un pare-feu afin de joindre un hôte distant . . . . .	394
3.6.2	Autoriser un accès momentané depuis l'extérieur . . . . .	396
4.	DoS et DDoS . . . . .	397
4.1	Établissement d'une session TCP . . . . .	397
4.2	Principe de l'attaque . . . . .	398
5.	Sniffing . . . . .	399
5.1	Capturer des données avec Wireshark . . . . .	400
5.2	Les filtres . . . . .	401
6.	Man In The Middle (MITM) . . . . .	404
6.1	Théorie . . . . .	404

- 6.2 Pratique . . . . . 406
  - 6.2.1 Installation de Ettercap . . . . . 406
  - 6.2.2 Configuration de Ettercap . . . . . 407
  - 6.2.3 Les plug-ins sous Ettercap . . . . . 410
  - 6.2.4 Création d'un filtre . . . . . 411
  - 6.2.5 Cain & Abel . . . . . 413
- 6.3 Contre-mesures . . . . . 414
- 7. Vol de session TCP (hijacking) et spoofing d'IP . . . . . 415
  - 7.1 La faille : l'ACK/SEQ . . . . . 415
  - 7.2 Conséquence de l'attaque . . . . . 416
  - 7.3 Mise en pratique . . . . . 416
  - 7.4 Automatiser l'attaque . . . . . 419
  - 7.5 Spoofing d'adresse IP . . . . . 419
- 8. Failles Wi-Fi . . . . . 423
  - 8.1 Cracker un réseau WEP . . . . . 423
    - 8.1.1 Capturer des paquets . . . . . 423
    - 8.1.2 Générer du trafic . . . . . 424
    - 8.1.3 Trouver la clé . . . . . 425
  - 8.2 Cracker un réseau WPA . . . . . 426
  - 8.3 Rogue AP . . . . . 428
    - 8.3.1 Introduction au Rogue AP . . . . . 428
    - 8.3.2 Mise en pratique d'un Rogue AP avec Karmetasploit . . . . . 428
- 9. IP over DNS . . . . . 430
  - 9.1 Principe . . . . . 430
  - 9.2 Exploitation avec l'outil iodine . . . . . 431
  - 9.3 Contre-mesures . . . . . 432
- 10. La téléphonie sur IP . . . . . 432
  - 10.1 Écoute de conversation avec VoIPong . . . . . 432
  - 10.2 Usurpation de ligne . . . . . 434
  - 10.3 Autres attaques . . . . . 435
- 11. IPv6 . . . . . 436
  - 11.1 Les logiciels . . . . . 436
  - 11.2 Le matériel . . . . . 436
  - 11.3 L'humain . . . . . 437
  - 11.4 THC-IPv6 . . . . . 437

11.5	Scanner les hosts . . . . .	438
11.5.1	Sur un réseau local . . . . .	438
11.5.2	Sur Internet . . . . .	438
11.6	Flooder . . . . .	438
11.7	Man in the middle Attack . . . . .	439
12.	Conclusion . . . . .	442

## **Chapitre 8** **Les failles web**

1.	Rappels sur les technologies du Web . . . . .	443
1.1	Préambule . . . . .	443
1.2	Le réseau Internet . . . . .	443
1.3	Qu'est-ce qu'un site web ? . . . . .	444
1.4	Consultation d'une page web, anatomie des échanges client/serveur . . . . .	444
1.5	Comment sont réalisées les pages web ? . . . . .	448
2.	Généralités sur la sécurité des sites web . . . . .	450
3.	Petite analyse d'un site web . . . . .	451
3.1	Cartographie des parties visibles d'un site web . . . . .	451
3.1.1	Le site est-il statique ou dynamique ? . . . . .	452
3.1.2	Quelles sont les variables utilisées ? . . . . .	454
3.1.3	Y a-t-il des formulaires et quels champs utilisent-ils ? . . . . .	454
3.1.4	Le serveur envoie-t-il des cookies ? . . . . .	455
3.1.5	Le site contient-il des médias ? . . . . .	456
3.1.6	Le site fait-il appel à des bases de données ? . . . . .	456
3.1.7	Pouvons-nous accéder à certains dossiers ? . . . . .	457
3.1.8	Le site fait-il appel à du JavaScript ? . . . . .	458
3.1.9	Quel serveur est utilisé et quelle est sa version ? . . . . .	459
3.1.10	Des outils pour nous aider . . . . .	460
3.2	Découvrir la face cachée d'un site web . . . . .	462
3.2.1	Utilisation de Burp Suite . . . . .	462
3.2.2	Utilisation de Wfuzz . . . . .	467
3.3	Analyser les informations récupérées . . . . .	475

- 4. Passer à l'attaque d'un site web . . . . . 476
  - 4.1 Envoyer des données non attendues . . . . . 476
    - 4.1.1 Principes et outils . . . . . 476
    - 4.1.2 Utilisation de l'URL . . . . . 478
    - 4.1.3 Utilisation des formulaires . . . . . 481
    - 4.1.4 Utilisation de l'en-tête . . . . . 485
    - 4.1.5 Utilisation des cookies . . . . . 487
  - 4.2 Le vol de session . . . . . 488
  - 4.3 Le dépôt de fichiers malicieux . . . . . 490
- 5. Les injections SQL . . . . . 493
  - 5.1 Préambule . . . . . 493
  - 5.2 Introduction aux bases de données . . . . . 493
  - 5.3 Principe des injections SQL . . . . . 505
  - 5.4 Technique du Blind SQL . . . . . 514
  - 5.5 Des outils efficaces . . . . . 536
- 6. Passer les CAPTCHA . . . . . 539
  - 6.1 Présentation des différents CAPTCHA . . . . . 539
  - 6.2 Passer les CAPTCHA de base . . . . . 540
  - 6.3 Passer les CAPTCHA images . . . . . 543
- 7. Les nouvelles menaces sur le Web . . . . . 550
- 8. Contre-mesures et conseils de sécurisation . . . . . 550
  - 8.1 Filtrer toutes les données . . . . . 550
  - 8.2 Renforcer l'identification du client . . . . . 553
  - 8.3 Configurer judicieusement le serveur . . . . . 554
- 9. Utiliser des frameworks pour le développement . . . . . 555
- 10. Conclusion . . . . . 556

**Chapitre 9**  
**Les failles système**

- 1. Généralités . . . . . 557
- 2. Les mots de passe . . . . . 558
  - 2.1 Introduction . . . . . 558
  - 2.2 Révéler un mot de passe sous Microsoft Windows . . . . . 558
  - 2.3 Complexité . . . . . 559

2.4	Le stockage des mots de passe . . . . .	559
2.4.1	Précisions sur le stockage des mots de passe . . . . .	559
2.4.2	Visualisation des empreintes LM et NTLMv1-2 . . . . .	561
2.5	Cas pratique : trouver les mots de passe sous Microsoft Windows .	563
2.5.1	Récupération des mots de passe avec Ophcrack liveCD . . . . .	563
2.5.2	Récupération de condensat avec Responder . . . . .	564
2.5.3	Récupération de condensat d'une machine locale avec SMBEXEC . . . . .	567
2.5.4	Récupération de condensat d'une machine locale et élévation de privilège avec Mimikatz . . . . .	569
2.5.5	Récupération des mots de passe d'un contrôleur de domaine Windows 2012 R2 . . . . .	576
2.6	Cas pratique : trouver les mots de passe sous GNU/Linux . . . . .	580
2.7	Cas pratique : trouver les mots de passe sous Mac OS X . . . . .	580
2.8	Changer son mot de passe en ligne de commande . . . . .	581
2.8.1	Sous Windows . . . . .	582
2.8.2	Sous GNU/Linux . . . . .	582
2.8.3	Sous Mac OS X . . . . .	582
3.	Utilisateurs, groupes et permissions sur le système . . . . .	583
3.1	Gestion des utilisateurs . . . . .	583
3.1.1	Définition . . . . .	583
3.1.2	Sous GNU/Linux . . . . .	584
3.1.3	Sous Windows . . . . .	585
3.1.4	Sous Mac OS X . . . . .	585
3.2	Gestion des groupes . . . . .	587
3.2.1	Sous GNU/Linux . . . . .	588
3.2.2	Sous Windows . . . . .	588
3.2.3	Sous Mac OS X . . . . .	588
3.3	Affectation des permissions . . . . .	588
3.3.1	Sous GNU/Linux . . . . .	588
3.3.2	Sous Windows . . . . .	589
3.3.3	Sous Mac OS X . . . . .	591
4.	Élévation des privilèges . . . . .	591
4.1	Sous UNIX . . . . .	592
4.1.1	Activation du suid et du sgid . . . . .	592
4.1.2	Comment trouver les scripts suid root d'un système GNU/Linux . . . . .	593

- 4.2 Sous Windows . . . . . 593
- 4.3 Le Planificateur de tâches . . . . . 598
- 5. Les processus . . . . . 598
  - 5.1 Espionner des processus sous Windows . . . . . 600
  - 5.2 Le hooking et l'injection de processus . . . . . 600
    - 5.2.1 Exemple de hooking des événements du clavier  
sous Windows . . . . . 601
    - 5.2.2 Exemple de hooking des paquets réseau  
via Netfilter sous GNU/Linux . . . . . 605
    - 5.2.3 Exemple d'injection de code  
dans un autre processus sous Mac OS X . . . . . 607
  - 5.3 Les situations de concurrence (race conditions) . . . . . 608
- 6. Le démarrage . . . . . 609
  - 6.1 L'abus des modes de démarrage dégradés . . . . . 609
  - 6.2 Les attaques de preboot . . . . . 609
- 7. L'hibernation . . . . . 610
- 8. Les appels de procédures distantes . . . . . 610
  - 8.1 Principe . . . . . 610
  - 8.2 L'accès au registre à distance . . . . . 610
- 9. SeLinux et AppArmor . . . . . 611
- 10. La virtualisation . . . . . 611
  - 10.1 L'isolation . . . . . 611
  - 10.2 Le changement de racine ou chrooting . . . . . 612
  - 10.3 Noyau en espace utilisateur . . . . . 612
  - 10.4 La machine virtuelle . . . . . 613
  - 10.5 La paravirtualisation . . . . . 613
  - 10.6 Exemple de solution de paravirtualisation : Proxmox VE . . . . . 614
  - 10.7 Détection et attaque d'une machine virtuelle . . . . . 614
- 11. Les logs, les mises à jour et la sauvegarde . . . . . 615
  - 11.1 Les logs . . . . . 615
  - 11.2 Les mises à jour . . . . . 616
    - 11.2.1 Mise en place des mises à jour automatiques  
sous GNU/Linux . . . . . 617
    - 11.2.2 Mise en place des mises à jour automatiques  
sous Microsoft Windows . . . . . 617
    - 11.2.3 Mise en place des mises à jour automatiques sous Mac OS X 617



11.3 Les sauvegardes . . . . .	617
12. Big Data et confidentialité . . . . .	618
13. Bilan . . . . .	620

## Chapitre 10 Les failles applicatives

1. Généralités . . . . .	621
2. Notions d'Assembleur . . . . .	622
2.1 Introduction . . . . .	622
2.2 Premiers pas . . . . .	622
2.2.1 Apprenons à compter . . . . .	622
2.2.2 Le binaire . . . . .	622
2.2.3 L'hexadécimal . . . . .	624
2.3 Comment tester nos programmes ? . . . . .	625
2.3.1 Squelette d'un programme en Assembleur . . . . .	625
2.3.2 Notre premier programme . . . . .	626
2.4 Les instructions . . . . .	627
2.4.1 La comparaison . . . . .	627
2.4.2 L'instruction IF . . . . .	628
2.4.3 La boucle FOR . . . . .	629
2.4.4 La boucle WHILE . . . . .	630
2.4.5 La boucle DO WHILE . . . . .	630
2.4.6 La directive %define . . . . .	632
2.4.7 Directives de données . . . . .	632
2.4.8 Entrées-sorties . . . . .	632
2.5 Les interruptions . . . . .	633
2.6 Les sous-programmes . . . . .	635
2.7 Le heap et la pile . . . . .	636
2.7.1 Le heap . . . . .	636
2.7.2 La pile . . . . .	637
2.7.3 Appel et retour de fonction : les notions fondamentales . . . . .	638
3. Bases des shellcodes . . . . .	640
3.1 Exemple 1 : shellcode.py . . . . .	640
3.2 Exemple 2 : execve() . . . . .	641
3.3 Exemple 3 : Port Binding Shell . . . . .	643

4.	Les buffer overflows	645
4.1	Quelques définitions	645
4.2	Notions essentielles	646
4.3	Stack overflow	647
4.4	Heap overflow	654
4.5	return-into-libc	658
5.	Les failles Windows	662
5.1	Introduction	662
5.2	Premiers pas	662
5.2.1	En mode console	663
5.2.2	Débogage	664
5.2.3	Problème d'un grand shellcode	669
5.2.4	Exécution d'une fonction non prévue	672
5.2.5	Autres méthodes	674
5.3	La méthode du call [reg]	674
5.4	La méthode pop ret	675
5.5	La méthode du push return	675
5.6	La méthode du jmp [reg] + [offset]	676
5.7	La méthode du blind return	676
5.8	Que faire avec un petit shellcode ?	676
5.8.1	Principe	676
5.8.2	En pratique	677
5.9	Le SEH (Structured Exception Handling)	677
5.9.1	Les bases	677
5.9.2	SEH, les protections	679
5.9.3	XOR et Safe-SEH	680
5.10	Passer les protections	681
5.10.1	Stack cookie, protection /GS	681
5.10.2	Exemple : outrepasser le cookie	685
5.10.3	SafeSEH	688
6.	Cas concret : Ability Server	689
6.1	Fuzzing	689
6.2	Exploitation	691
7.	Cas concret : MediaCoder-0.7.5.4796	697
7.1	Crash du logiciel	697
7.2	Vérification des valeurs	702

7.3	Finalisation de l'exploit . . . . .	703
8.	Cas concret : BlazeDVD 5.1 Professional . . . . .	705
9.	Conclusion . . . . .	709
10.	Références . . . . .	710

## Chapitre 11 Forensic

1.	Introduction . . . . .	711
1.1	Le cerveau . . . . .	712
1.2	La mémoire . . . . .	713
1.3	Les fichiers . . . . .	715
2.	Les méthodes . . . . .	716
2.1	Préparation et environnement . . . . .	716
2.2	Recherche et analyse de fichiers . . . . .	717
3.	Les outils . . . . .	719
3.1	Les outils d'analyse réseau . . . . .	720
3.1.1	Wireshark . . . . .	720
3.1.2	tcpdump . . . . .	721
3.1.3	Scapy . . . . .	721
3.2	Les outils d'analyse mémoire . . . . .	722
3.2.1	Volatility . . . . .	722
3.3	Les outils d'analyse binaire . . . . .	722
3.3.1	Hexdump . . . . .	722
3.3.2	Readelf . . . . .	723
3.3.3	Gdb . . . . .	723
3.4	Les outils d'analyse système . . . . .	724
3.4.1	The coroner's toolkit . . . . .	724
3.4.2	Logstash . . . . .	725
4.	Conclusion . . . . .	725

**Chapitre 12**  
**La sécurité des box**

- 1. Les fonctionnalités d'une box ..... 727
  - 1.1 Routeur ..... 727
  - 1.2 Switch ..... 727
  - 1.3 Téléphonie..... 728
  - 1.4 TV ..... 728
  - 1.5 Serveur multimédia ..... 728
- 2. Les différentes box..... 729
  - 2.1 Orange..... 729
  - 2.2 Free ..... 730
  - 2.3 Bouygues ..... 730
  - 2.4 SFR..... 731
- 3. La configuration des box..... 732
  - 3.1 Le mode modem ..... 732
  - 3.2 Le mode routeur ..... 733
  - 3.3 Les fonctions téléphoniques..... 734
- 4. La configuration par défaut, un danger ..... 734
  - 4.1 L'interface d'administration web ..... 734
  - 4.2 Le Wi-Fi ..... 736
  - 4.3 Les services : SSH, Telnet, Samba, TR069 ..... 736
- 5. Installation d'un firmware alternatif ..... 738
  - 5.1 Dans quel intérêt ? ..... 738
  - 5.2 Connexion au port console ..... 739
- 6. La sécurité des firmwares officiels ..... 744
  - 6.1 Les failles de ces dernières années ..... 744
  - 6.2 Et actuellement ? ..... 745
- 7. Reverse engineering ..... 746
  - 7.1 Neufbox 5 ..... 746
    - 7.1.1 Introduction..... 746
    - 7.1.2 Caractéristiques techniques ..... 746
    - 7.1.3 Recherche du port série ..... 747
    - 7.1.4 Connexion au port série ..... 748
    - 7.1.5 Création d'une image complète ..... 752
    - 7.1.6 Flashage de l'image..... 754

7.1.7	Utilisation de la box en tant que Routeur . . . . .	757
7.1.8	Téléphonie SIP . . . . .	759
7.1.9	Installation d'un firmware libre OpenWRT . . . . .	762

## Chapitre 13

### Les failles matérielles

1.	Introduction . . . . .	763
2.	La trousse à outils . . . . .	764
2.1	L'outillage de base . . . . .	764
2.1.1	Lot de tournevis . . . . .	764
2.1.2	Le multimètre . . . . .	765
2.1.3	Platine de test . . . . .	765
2.1.4	Les câbles Dupont . . . . .	766
2.1.5	Fer à souder . . . . .	766
2.1.6	Arduino . . . . .	767
2.1.7	Matériels de récupération . . . . .	767
2.2	Utilisateur régulier . . . . .	768
2.2.1	Adaptateur USB RS232 TTL . . . . .	768
2.2.2	Sonde d'analyse logique . . . . .	768
2.2.3	Interface JTAG . . . . .	769
2.2.4	Le bus pirate de chez Dangerous Prototypes . . . . .	769
2.2.5	SDR low cost . . . . .	770
2.3	Utilisateur avancé . . . . .	771
2.3.1	Logiciel de conception de PCB . . . . .	771
2.3.2	Programmeur . . . . .	771
2.3.3	Matériel d'électronicien . . . . .	773
2.4	Méthodologie du reverse engineering matériel . . . . .	773
2.4.1	Attaque via Sniffing I2C . . . . .	775
2.4.2	Attaque via Sniffing UART modem . . . . .	778
2.5	Étude et bidouille autour des T2G et Arduino . . . . .	778
2.5.1	Création d'un lecteur de cartes T2G . . . . .	779
2.5.2	Émulateur partiel de carte T2G . . . . .	787

**Chapitre 14**  
**Black Market**

- 1. Introduction . . . . . 791
- 2. Deep Web, Dark Web, darknet, Black Market . . . . . 791
- 3. Black Market, entre le visible et l’invisible . . . . . 792
- 4. Fonctionnement . . . . . 793
- 5. Anonymat des boutiques? . . . . . 795
- 6. Mode d’emploi de TOR . . . . . 796
  - 6.1 Installation . . . . . 796
  - 6.2 Configuration de la sécurité . . . . . 797
  - 6.3 Vérifier son IP . . . . . 797
  - 6.4 Surfez . . . . . 798
  - 6.5 Changer d’IP . . . . . 798
  - 6.6 Mise à jour . . . . . 798
- 7. Le référencement du Black Market . . . . . 799
- 8. Traducteur d’Onion . . . . . 803
- 9. Vocabulaire . . . . . 804
- 10. Liste des markets et autoshops . . . . . 805

**Chapitre 15**  
**Risques juridiques et solutions**

- 1. Préambule . . . . . 807
- 2. Atteintes à un système d’information . . . . . 809
  - 2.1 Accès et maintien dans un système d’information . . . . . 809
    - 2.1.1 Élément matériel . . . . . 811
    - 2.1.2 Élément moral . . . . . 814
  - 2.2 Atteinte au fonctionnement d’un système d’information . . . . . 816
  - 2.3 Atteinte aux données d’un système d’information . . . . . 818
  - 2.4 Diffusion d’un logiciel d’intrusion . . . . . 820
- 3. Atteintes aux traitements de données à caractère personnel . . . . . 820
  - 3.1 Notion de données à caractère personnel . . . . . 820
  - 3.2 Cas particulier de l’adresse IP . . . . . 823
  - 3.3 Collecte illicite de données à caractère personnel . . . . . 823

- 3.4 Divulgarion illicite de données à caractère personnel . . . . . 823
- 3.5 Sanctions administratives (CNIL) . . . . . 824
- 3.6 Obligation de sécurité du responsable de traitement . . . . . 824
- 3.7 Obligation de notification des failles de sécurité . . . . . 831
- 3.8 Contrôles en ligne de la CNIL . . . . . 834
- 3.9 Obligation de conservation des données de connexion . . . . . 835
- 3.10 Obligation de conservation des données relatives aux contenus . . . . . 836
- 3.11 Accès administratif aux données de connexion . . . . . 838
- 3.12 Les autres obligations spécifiques des FAI et hébergeurs . . . . . 841
- 4. Infractions classiques applicables à l’informatique . . . . . 842
  - 4.1 L’escroquerie . . . . . 843
  - 4.2 L’usurpation d’identité . . . . . 843
  - 4.3 Atteinte au secret des correspondances . . . . . 845
  - 4.4 La dégradation physique d’un système . . . . . 848
  - 4.5 Le vol d’informations ? . . . . . 849
- 5. Solutions et précautions . . . . . 850
  - 5.1 Encadrement contractuel des tests d’intrusion . . . . . 850
    - 5.1.1 Exonérations de responsabilité du prestataire . . . . . 851
    - 5.1.2 Périmètre des tests d’intrusion . . . . . 852
    - 5.1.3 Principes dégagés par la charte FPTI . . . . . 852
  - 5.2 Hors cadre contractuel : la révélation publique de failles de sécurité 853
    - 5.2.1 Révélation d’une faille relative à un serveur . . . . . 853
    - 5.2.2 Révélation d’une faille relative à un système d’exploitation . . . . . 856
    - 5.2.3 Conseils quant à la divulgation de failles de sécurité . . . . . 858
- 6. Conclusion . . . . . 860
- 7. Références . . . . . 860
  
- Index . . . . . 861

Editions ENI

# **Hacking et Forensic**

**Développez vos propres outils en Python**

(2<sup>e</sup> édition)

Collection  
Epsilon

Table des matières



Les éléments à télécharger sont disponibles à l'adresse suivante :  
**<http://www.editions-eni.fr>**  
Saisissez la référence de l'ouvrage **EP2HAFO** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

## Avant-propos

### Chapitre 1

### Python : les fondamentaux

1. Introduction . . . . .	13
2. Historique . . . . .	15
3. Caractéristiques du langage . . . . .	15
4. Types de données . . . . .	19
4.1 Les nombres . . . . .	19
4.2 Les opérations arithmétiques . . . . .	23
4.3 Les chaînes de caractères . . . . .	24
4.4 Les tuples . . . . .	27
4.5 Les listes . . . . .	28
4.6 Les dictionnaires . . . . .	32
4.7 Supplément aux types de données . . . . .	34
5. Structures conditionnelles et répétitives . . . . .	36
5.1 Test if ... elif ... else . . . . .	36
5.2 Boucle while . . . . .	37
5.3 Boucle for . . . . .	38
5.4 Les listes en intention (comprehension list) . . . . .	39
6. Fonctions, modules et paquets . . . . .	41
6.1 Définition et appel de fonction . . . . .	41
6.2 Espaces de noms . . . . .	44
6.3 Fonctions particulières . . . . .	44
6.4 Modules . . . . .	45
6.5 Paquets . . . . .	46

# 2 --- Hacking et Forensic

Développez vos propres outils en Python

6.6	Instruction yield	47
7.	Les classes	48
7.1	Déclaration d'une classe	49
7.2	Surcharge des opérateurs	50
7.3	Propriétés, accesseurs et mutateurs	52
7.4	Héritage	53
7.5	Polymorphisme	54
8.	Manipulation de fichiers	55
9.	Les exceptions	58
10.	Modules utiles pour la suite du livre	61
10.1	Module sys	61
10.2	Module os	63
10.3	Module re	68
10.4	Modules pickle et shelve	73
10.5	Modules bases de données	74
10.5.1	MySQLdb	75
10.5.2	PostgreSQL	80
10.6	Module thread	86
10.6.1	Principe du module	86
10.6.2	Threading	87
10.6.3	Classe Lock()	88
11.	Conclusion	90

## Chapitre 2

### Le réseau

1.	Introduction	91
2.	Les sockets	92
2.1	Création d'un socket	92
2.2	Échange de données	93
2.3	Socket en UDP	94
2.4	Les erreurs	97

2.5	Socket et FTP	99
3.	Création d'un serveur	101
3.1	Introduction	101
3.2	Connexion cliente	103
3.3	Discussion avec le client	105
3.4	Création d'un trojan basique	106
3.5	Création d'un trojan plus complexe	109
4.	DNS : Domain Name Server	115
4.1	Introduction	115
4.1.1	Que signifie DNS ?	115
4.1.2	Principaux enregistrements DNS	116
4.2	nslookup basique	118
4.3	Reverse lookup	121
4.4	La librairie DNS	122
4.5	Demande à partir d'un serveur spécifié	123
4.6	Mise en forme des résultats obtenus	125
5.	FTP : File Transfer Protocol	128
5.1	Introduction	128
5.2	FTP anonyme	128
5.3	Téléchargement de fichiers ASCII	129
5.4	Téléchargement de fichiers binaires	131
5.5	Téléchargement avancé de fichiers binaires	132
5.6	Envoi de données	133
5.7	Les erreurs FTP	135
5.8	Lister le contenu des répertoires	135
5.9	Les autres commandes utiles	138
5.10	Télécharger récursivement des données	139
6.	Les expressions régulières	142
6.1	Introduction	142
6.2	Le module re	143

# 4 --- Hacking et Forensic

Développez vos propres outils en Python

6.3	Les méthodes utiles	144
6.3.1	Méthode search()	144
6.3.2	Méthode match()	145
6.3.3	Méthode sub()	146
6.3.4	Aller plus loin avec les groupes	147
6.4	Comment construire son pattern ou expression	147
7.	Le Web	149
7.1	Introduction	149
7.2	Récupération d'une page source	150
7.3	Méthodes GET et POST	151
7.3.1	Méthode GET	151
7.3.2	Méthode POST	153
7.4	Gestion des erreurs	154
7.4.1	Erreurs de connexion : urllib2.URLError	154
7.4.2	Erreur 404	154
7.5	Authentification	154
8.	Analyser les pages HTML et XHTML	156
8.1	Introduction	156
8.2	Première approche	157
8.3	Travail sur des pages « réelles »	159
8.3.1	Ampersand	159
8.3.2	Caractères spéciaux	161
8.4	BeautifulSoup	163
8.4.1	Introduction	163
8.4.2	Récupérer les liens	164
9.	Le XML	165
9.1	Introduction	165
9.2	Représentation du fichier XML	166
9.3	Python et XML	167
9.4	Lire un flux RSS	171

10. Les e-mails . . . . .	171
10.1 Introduction . . . . .	171
10.2 La bibliothèque smtplib . . . . .	173
10.2.1 Le corps du texte . . . . .	173
10.2.2 Mail avec pièce jointe . . . . .	175
10.3 Analyser des e-mails . . . . .	177
10.4 Analyser les dates . . . . .	180
10.5 Erreurs et débogage . . . . .	181
10.6 Mail et POP . . . . .	183
11. Le SSL en Python . . . . .	186
11.1 Introduction . . . . .	186
11.2 Utilisation d'OpenSSL . . . . .	187
11.3 Vérifier les certificats . . . . .	189
12. Utilisation de bases de données . . . . .	194
12.1 Introduction . . . . .	194
12.2 MySQLdb . . . . .	194
12.2.1 Rappel . . . . .	194
12.2.2 Utilisation . . . . .	195
12.3 PostgreSQL . . . . .	200
12.3.1 Introduction et première connexion . . . . .	200
12.3.2 Exécuter des commandes . . . . .	201
12.3.3 Cacher les changements . . . . .	203
12.3.4 Répéter des commandes . . . . .	204
12.3.5 Récupérer des données . . . . .	205
13. Conclusion . . . . .	207
14. Mise en pratique . . . . .	208
14.1 Cas 1 : Scan de ports . . . . .	208
14.2 Cas 2 : Envoi de mails . . . . .	210
14.3 Cas 3 : Fuzzing de FTP . . . . .	216
14.4 Cas 4 : Parsing de page web . . . . .	217
14.5 Cas 5 : Brute force MySQL . . . . .	219

# 6 **Hacking et Forensic**

Développez vos propres outils en Python

## **Chapitre 3**

### **Réseau : la bibliothèque Scapy**

1. Introduction . . . . .	221
2. Programmation réseau avec Scapy . . . . .	223
2.1 Liste des protocoles supportés . . . . .	223
2.2 Quelques notions sur les réseaux. . . . .	229
2.2.1 Topologie des réseaux . . . . .	229
2.2.2 Les différents types de réseaux . . . . .	230
2.2.3 Qu'est-ce qu'un protocole ? . . . . .	231
2.2.4 Adresse IP . . . . .	231
2.2.5 Les classes d'adresses . . . . .	232
2.2.6 Le masque de sous-réseau . . . . .	233
2.2.7 Le modèle OSI . . . . .	233
2.3 Manipulations basiques . . . . .	238
2.3.1 Commandes de base . . . . .	238
2.3.2 Fabrication de paquets . . . . .	241
2.3.3 Les entrées-sorties . . . . .	246
2.3.4 Entrons dans le détail . . . . .	250
2.4 Utilisation avancée : sécurité réseau . . . . .	259
2.4.1 traceroute . . . . .	259
2.4.2 Sniffing. . . . .	265
2.4.3 Scan TCP . . . . .	268
2.4.4 Tunneling . . . . .	269
2.5 Quelques exemples simples en « one-liner » . . . . .	270
2.5.1 Scan ACK . . . . .	270
2.5.2 Scan Xmas . . . . .	271
2.5.3 Scan IP . . . . .	273
2.5.4 Les différents ping . . . . .	273
2.5.5 Les attaques classiques . . . . .	273

- 3. Scapy et IPv6. . . . . 274
  - 3.1 Notion d'IPv6 . . . . . 274
    - 3.1.1 Généralités . . . . . 274
    - 3.1.2 IPv6 : RFC 2373 . . . . . 275
  - 3.2 Application . . . . . 277
    - 3.2.1 Requête ICMP IPv6 . . . . . 277
    - 3.2.2 Routage de paquets IPv6 . . . . . 277
    - 3.2.3 Exemple de routage de header . . . . . 278
    - 3.2.4 traceroute . . . . . 278
    - 3.2.5 IPv6 NA . . . . . 278
    - 3.2.6 Avertissement de daemon tués . . . . . 279
    - 3.2.7 Exemple . . . . . 279
- 4. Quelques autres exemples . . . . . 280
- 5. Conclusion . . . . . 281
- 6. Mise en pratique . . . . . 282
  - 6.1 Canal caché IP . . . . . 282
  - 6.2 Détection de Rogue AP . . . . . 283
  - 6.3 IP Spoofing . . . . . 284
  - 6.4 Spoofing IPv6 des voisins . . . . . 285

**Chapitre 4**  
**Débogage sous Windows**

- 1. Introduction . . . . . 287
- 2. Le module ctypes de Python . . . . . 288
- 3. Première approche . . . . . 290
- 4. État des registres . . . . . 304
  - 4.1 Énumération des threads . . . . . 304
  - 4.2 Récupération des valeurs des registres . . . . . 305
- 5. Les événements du debugger . . . . . 308

# 8 **Hacking et Forensic**

Développez vos propres outils en Python

6. Les points d'arrêt (breakpoints).....	318
6.1 Points d'arrêt logiciel .....	318
6.2 Points d'arrêt matériel .....	320
6.3 Point d'arrêt mémoire.....	322
7. La bibliothèque PyDbg .....	323
7.1 Violation d'accès des en-têtes (handlers) .....	325
7.2 Process snapshot .....	329
8. Mise en pratique : Hooking .....	334

## **Chapitre 5** **Le fuzzing**

1. Introduction .....	339
2. Fuzzing FTP .....	340
3. Fuzzing avec Scapy.....	345
4. Fuzzing avec PyDbg : format string .....	347
4.1 Introduction .....	347
4.2 Fuzzer de fichiers .....	348
5. Sulley.....	353
5.1 Introduction .....	353
5.2 Installation .....	354
5.2.1 Installation normale .....	354
5.2.2 Installation non standard .....	356
5.3 Utilisation.....	365
5.3.1 Structure du répertoire de Sulley .....	366
5.3.2 Représentation de données .....	368
5.3.3 Primitives statiques et aléatoires .....	368
5.3.4 Les entiers.....	369
5.3.5 Chaînes de caractères et délimiteurs .....	370
5.3.6 Les extensions Fuzz Library .....	371
5.3.7 Blocks .....	372
5.3.8 Groupes .....	373



- 5.3.9 Encodeur . . . . . 374
- 5.3.10 Dépendances . . . . . 374
- 5.3.11 Block helpers . . . . . 375
- 5.3.12 Legos . . . . . 377
- 6. Mise en pratique . . . . . 378
  - 6.1 Fuzzing 1 : HTTP . . . . . 378
  - 6.2 Fuzzing 2 : FTP . . . . . 381

**Chapitre 6**  
**Traitement d'images**

- 1. Introduction . . . . . 385
- 2. Utilisation . . . . . 386
  - 2.1 La classe Image . . . . . 386
  - 2.2 Lire et écrire . . . . . 387
  - 2.3 Couper, coller et fusionner . . . . . 390
  - 2.4 Transformations géométriques . . . . . 391
  - 2.5 Transformation des couleurs . . . . . 392
  - 2.6 Amélioration d'images . . . . . 392
    - 2.6.1 Filtres . . . . . 392
    - 2.6.2 Opérations sur les points . . . . . 392
    - 2.6.3 Améliorations . . . . . 393
- 3. Exemples d'utilisation . . . . . 394
  - 3.1 Création d'un captcha . . . . . 394
  - 3.2 Capture d'image et transformation . . . . . 395
  - 3.3 Lecture de captcha . . . . . 397

## Chapitre 7

### Un peu plus sur le Web

1. Introduction . . . . .	401
2. Reprenons les basiques . . . . .	401
3. Mapping de site web . . . . .	403
4. Brute force de répertoires ou d'emplacement de fichiers . . . . .	405
5. Brute force authentification HTML . . . . .	408
6. Selenium . . . . .	411
6.1 Introduction . . . . .	411
6.2 Installation . . . . .	412
6.3 Premier test . . . . .	412
6.4 Copie d'écran avec Selenium . . . . .	413
7. Connexion sur un site web et navigation . . . . .	414
8. Conclusion . . . . .	419

## Chapitre 8

### Forensic

1. Introduction . . . . .	421
2. Cryptographie et autres . . . . .	422
2.1 ROT13 . . . . .	422
2.2 Base 64 . . . . .	424
2.3 Hash . . . . .	427
3. Extraction des métadonnées dans les fichiers . . . . .	429
3.1 Métadonnées MP3 . . . . .	429
3.2 Métadonnées des images . . . . .	430
3.3 Métadonnées PDF . . . . .	431
3.4 Métadonnées OLE2 . . . . .	432
3.5 Cas concret . . . . .	433

- 4. Fichiers ZIP ..... 434
  - 4.1 Lire dans un fichier ZIP ..... 434
  - 4.2 Attaque brute force de mots de passe ..... 434
- 5. Lire dans un fichier OpenOffice ou Word ..... 435
  - 5.1 Parcourir une arborescence ..... 435
  - 5.2 Rechercher dans un document OpenOffice ..... 436
  - 5.3 Rechercher dans un document Word ..... 437
- 6. E-mail ..... 438
  - 6.1 Retrouver des e-mails dans des fichiers ..... 438
  - 6.2 Rechercher dans la boîte mail ..... 439
- 7. Stéganographie ..... 440
  - 7.1 Rechercher des informations dans une image ..... 440
  - 7.2 Cacher un message dans une image ..... 441
  - 7.3 Lecture du message ..... 443
- 8. Volatility ..... 443
  - 8.1 Informations sur l'image ..... 444
  - 8.2 Processus et DLL ..... 445
  - 8.3 Capture de mots de passe hachés ..... 446
  - 8.4 Exemple de programme ..... 448
- 9. Analyse des points d'accès sans fil dans la base de registre ..... 456
- 10. Retrouver les éléments supprimés (dans la corbeille) ..... 458
- 11. Mise en pratique ..... 461
  - 11.1 Décryptage ..... 461
  - 11.2 OCR ..... 462
  - 11.3 ZIP ..... 462
  - 11.4 Scapy et géolocalisation ..... 463
  
- Bibliographie ..... 465
- Index ..... 467