

Avant-propos

Chapitre 1

Introduction et définitions

- 1. La sécurité informatique : pour quoi, pour qui ? . . . . . 25
  - 1.1 L'actualité cybercriminelle . . . . . 25
  - 1.2 Hacking, piratage, sécurité informatique, cyberdéfense...  
Que met-on derrière ces termes ? . . . . . 26
  - 1.3 L'importance de la sécurité . . . . . 27
    - 1.3.1 Pour les particuliers . . . . . 28
    - 1.3.2 Pour les entreprises et les écoles. . . . . 29
    - 1.3.3 Pour un pays ou une nation. . . . . 30
- 2. Le hacking se veut éthique . . . . . 31
  - 2.1 Le travail en coopération. . . . . 31
  - 2.2 Un esprit bidouilleur et passionné avant tout. . . . . 31
  - 2.3 Le hacker devient un expert recherché. . . . . 32
  - 2.4 Dans la peau de l'attaquant . . . . . 33
  - 2.5 Conseils et accompagnement vers la sécurisation. . . . . 34
- 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 . . . . . 35
    - 3.1.4 Les script kiddies. . . . . 36
    - 3.1.5 Les hackers universitaires. . . . . 37
  - 3.2 Et à chaque audit sa boîte à secrets . . . . . 38
    - 3.2.1 Les tests en black box. . . . . 38
    - 3.2.2 Les tests en grey box. . . . . 38
    - 3.2.3 Les tests en white box . . . . . 39
- 4. Conclusion . . . . . 39

# 2 Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

## Chapitre 2

### Éléments d'ingénierie sociale

1. Généralités . . . . .	41
1.1 Introduction . . . . .	41
1.2 Systèmes d'information . . . . .	43
1.2.1 Précisions sur les systèmes d'information . . . . .	43
1.2.2 Failles d'un système d'information . . . . .	44
1.3 Présentation de l'ingénierie sociale . . . . .	44
1.3.1 Définitions . . . . .	44
1.3.2 Caractéristiques et périmètre . . . . .	45
1.4 Problématique de la protection . . . . .	48
2. Modes d'action de l'ingénierie sociale . . . . .	49
2.1 Principes de l'attaque par ingénierie sociale . . . . .	49
2.2 Processus générique de l'ingénieur social . . . . .	50
2.2.1 Étude préalable . . . . .	51
2.2.2 Préparation . . . . .	54
2.2.3 Exploitation . . . . .	55
2.3 Compétences et outils de l'ingénieur social . . . . .	56
2.3.1 Comédie, ruse, subterfuge et tromperie . . . . .	57
2.3.2 Lecture de cible . . . . .	57
3. Connaissance des organisations attaquées . . . . .	58
3.1 Typologies générales . . . . .	59
3.2 Typologies de valeurs et de croyances . . . . .	59
3.3 Modèles de maturité et certifications qualité . . . . .	62
3.4 Exploitation . . . . .	63
3.5 Exercices . . . . .	63
4. Failles humaines : bases et modèles théoriques . . . . .	63
4.1 Bases biologiques et fonctionnalités du cerveau . . . . .	64
4.2 Biais cognitifs . . . . .	65
4.3 Méthodes hypnotiques . . . . .	66
4.4 Cohérence et recherche de « pattern » . . . . .	67
4.5 Conclusion . . . . .	68
4.6 Exercices . . . . .	68
4.6.1 Cas particulier du téléphone . . . . .	68
4.6.2 Camouflage final . . . . .	68

5.	Influence et manipulation. . . . .	68
5.1	Méthodes d'influence . . . . .	69
5.1.1	Influence . . . . .	69
5.1.2	Tentation, séduction et intimidation . . . . .	69
5.1.3	Manipulation . . . . .	70
5.2	Les grands ressorts de la manipulation. . . . .	70
5.2.1	Cohérence . . . . .	71
5.2.2	Réciprocité . . . . .	71
5.2.3	Preuve sociale . . . . .	72
5.2.4	Autorité . . . . .	73
5.2.5	Sympathie . . . . .	74
5.2.6	Rareté . . . . .	74
6.	Les techniques de manipulation . . . . .	75
6.1	Les grandes techniques de manipulation . . . . .	76
6.1.1	Les amorçages et les leurres . . . . .	76
6.1.2	Le pied dans la porte . . . . .	77
6.1.3	La porte au nez . . . . .	77
6.2	Les petites techniques de manipulation . . . . .	77
6.2.1	Pied dans la bouche, politesse, sympathie . . . . .	78
6.2.2	Contact, touché, regard . . . . .	78
6.2.3	Pièges de la cohérence . . . . .	78
6.2.4	Étiquetage . . . . .	79
6.2.5	Déclaration de liberté . . . . .	79
6.2.6	Quelques petites techniques à connaître . . . . .	80
6.3	Exercices . . . . .	81
6.3.1	Croiser grandes et petites techniques . . . . .	81
6.3.2	Croiser techniques et ressorts . . . . .	81
6.3.3	Script de camouflage final . . . . .	81
7.	Savoir "patcher" les failles humaines . . . . .	81
7.1	Volonté politique . . . . .	82
7.2	Méthodologie . . . . .	83
7.2.1	Professionnalisme, qualité, procédures, maturité . . . . .	83
7.2.2	Mesure : tests, audit, retest de détection . . . . .	83
7.2.3	Optimisation et changement de paradigme . . . . .	84
7.3	Actions concrètes à mener . . . . .	84
7.3.1	Documenter une politique de classification de l'information . . . . .	84
7.3.2	Contrôler les "input/output" (entrée/sortie d'information) . . . . .	85

# 4 Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

7.3.3	Sensibiliser le personnel	85
7.3.4	Favoriser la remontée de l'information	86
7.4	Exercices	87
7.4.1	Manipuler les décideurs	87
7.4.2	Bloc-notes de réponse au téléphone	87
7.4.3	Remontée d'information	87
8.	OSINT	87
9.	Bibliographie	90

## Chapitre 3 Black Market

1.	Introduction	91
2.	Deep Web, Dark Web, Darknet, Black Market	91
3.	Black Market, entre le visible et l'invisible	92
4.	Fonctionnement	94
5.	Anonymat des boutiques ?	95
6.	Mode d'emploi de Tor	97
6.1	Installation	97
6.2	Configuration de la sécurité	98
6.3	Vérification de l'adresse IP	98
6.4	Navigation	99
6.5	Changement d'adresse IP	99
6.6	Mise à jour	99
7.	Le référencement du Black Market	100
8.	Annuaire de sites en .onion	104
9.	Vocabulaire	104
10.	Liste des markets et autoshops	106

**Chapitre 4**  
**Prise d'empreinte ou Information Gathering**

- 1. Les attaques . . . . . 107
  - 1.1 Préambule. . . . . 107
  - 1.2 Types et méthodologies des attaques. . . . . 108
  - 1.3 L'évolution de la cybercriminalité. . . . . 108
  - 1.4 Les motivations . . . . . 108
  - 1.5 Les différents types d'attaques . . . . . 109
    - 1.5.1 L'attaque de type destructif . . . . . 109
    - 1.5.2 Les attaques à motivation financière . . . . . 110
    - 1.5.3 Les attaques de type APT. . . . . 110
  - 1.6 La cyber kill chain ou les différentes phases d'une attaque. . . . . 111
- 2. L'analyse des risques . . . . . 113
- 3. Le test d'intrusion . . . . . 114
  - 3.1 Les acteurs du hacking. . . . . 115
  - 3.2 Types et stratégies d'audit . . . . . 115
    - 3.2.1 Les types d'audit . . . . . 115
    - 3.2.2 Les stratégies d'audit. . . . . 116
- 4. Méthodologie d'une collecte d'informations ou prise d'empreinte . . . . . 116
- 5. Le service Whois . . . . . 117
  - 5.1 Présentation . . . . . 117
  - 5.2 La gestion des adresses IP dans le monde. . . . . 117
- 6. La recherche d'informations sur le Web . . . . . 119
  - 6.1 Les basiques . . . . . 120
  - 6.2 Recherche en ligne : les sites web spécialisés. . . . . 121
  - 6.3 Les réseaux sociaux et professionnels. . . . . 123
  - 6.4 Les agrégateurs d'informations spécialisés. . . . . 127
  - 6.5 Les add-ons navigateurs spécialisés . . . . . 131
- 7. Les moteurs de recherche de périphériques connectés . . . . . 134
  - 7.1 Shodan : la référence . . . . . 134
  - 7.2 Thingful : un moteur de recherche pour les IoT (Internet of Things) . . . . . 141
  - 7.3 Censys : tout sur les appareils connectés en IPv4 sur le Net . . . . . 142
  - 7.4 Zoomeye : l'alternative chinoise . . . . . 144

# 6 Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

8.	La recherche d'informations avec Google Hack	145
8.1	Le Big Data	145
8.2	Les techniques utilisées	145
8.3	Google : historique et clés de son succès	146
8.4	Google, un incontournable sur le Web	146
8.5	Définition du Google Hacking	146
8.6	Fonctionnement du moteur de recherche	147
8.7	Le référencement Google	148
8.8	Google Hack : les opérateurs basiques de Google	148
8.9	Les opérateurs avancés.	149
8.10	Les opérateurs spécifiques	150
8.11	Les Google Dorks	150
8.12	Une interface graphique pour Google Hack et Bing Hack	156
9.	Applications graphiques dédiées à la recherche d'informations	158
9.1	Maltego.	158
9.2	Foca Free.	161
10.	Les scripts de recherche d'informations	163
10.1	TheHarvester	163
10.2	CrossLinked	165
10.3	Emailfinder	166
10.4	Parsero.	167
10.5	Dirsearch.	168
11.	Énumération DNS : commandes et scripts	168
11.1	Nslookup	168
11.2	Host	169
11.3	Dig.	169
11.4	Dnsenum	170
11.5	Subwalker.	172
11.6	Dnsrecon.	172
11.7	Fierce.	173
11.8	Knockpy	174
11.9	SecLists	175
11.10	Bluto	176

12. Les scanners de ports . . . . .	176
12.1 Nmap . . . . .	176
12.1.1 Utilisation de nmap . . . . .	178
12.1.2 Services et protocoles . . . . .	179
12.1.3 Évasion de firewall . . . . .	180
12.1.4 Scan en Idle Scan . . . . .	183
12.1.5 Scans avancés : utilisation des scripts nmap (.nse) . . . . .	184
12.2 Le scanner de masse Masscan . . . . .	186
12.3 Le scanner web Httprint . . . . .	186
12.4 Dmitry (Deepmagic Information Gathering Tool) . . . . .	187
13. Frameworks et collecte d'informations . . . . .	188
13.1 Metasploit . . . . .	188
13.2 Recon-ng . . . . .	188
13.3 SpiderFoot . . . . .	190
14. Les scanners de vulnérabilités . . . . .	191
14.1 Nessus : scanner de réseaux . . . . .	191
14.2 OpenVAS : scanner de réseaux open source . . . . .	198
14.3 Nikto : scanner de vulnérabilités web . . . . .	202
15. Faraday : IPE (Integrated Penetration-Test Environment) . . . . .	203
16. TL-OSINT : une machine virtuelle pour l'OSINT . . . . .	208
17. Le protocole SNMP (Simple Network Management Protocol) . . . . .	209
17.1 Les requêtes SNMP . . . . .	210
17.2 Les réponses SNMP . . . . .	210
17.3 Les alertes SNMP (traps, notifications) . . . . .	210
17.4 La MIB . . . . .	211
17.5 Les outils SNMP . . . . .	211
17.6 SNMP et la sécurité . . . . .	212
17.7 L'outil snmpwalk . . . . .	212
17.8 L'outil snmpcheck . . . . .	213
17.9 Onesixtyone : recherche des communautés SNMP . . . . .	214
17.10 Quelques règles de sécurité . . . . .	214
18. Le reporting . . . . .	214
19. Sites indexant de nombreux outils et guides OSINT . . . . .	215
20. Pour conclure . . . . .	216

# 8 Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

## Chapitre 5

### Les failles système

1. Généralités . . . . .	217
2. Les failles physiques . . . . .	218
2.1 Introduction . . . . .	218
2.2 Lockpicking . . . . .	218
2.3 Accès physique direct à l'ordinateur . . . . .	219
2.3.1 Accès à un ordinateur éteint dont le BIOS est protégé . . . . .	219
2.3.2 Accès à un ordinateur allumé dont le BIOS est protégé . . . . .	220
2.3.3 Accès à un ordinateur éteint dont le BIOS n'est pas protégé . . . . .	222
2.3.4 Accès à un ordinateur allumé en mode session utilisateur courant . . . . .	225
3. Les mots de passe . . . . .	233
3.1 Introduction . . . . .	233
3.2 Complexité . . . . .	234
4. Chiffrement et cryptage . . . . .	235
4.1 Introduction . . . . .	235
4.2 Le chiffrement symétrique . . . . .	235
4.3 Le chiffrement asymétrique . . . . .	236
4.4 Les algorithmes One Way Digest . . . . .	236
4.5 Les tables arc-en-ciel (rainbow tables) . . . . .	236
4.5.1 Principe . . . . .	236
4.5.2 Générer ses tables arc-en-ciel . . . . .	238
4.6 Méthodes de détermination de mot de passe . . . . .	240
5. Les processus . . . . .	240
6. Le démarrage . . . . .	242
6.1 L'abus des modes de démarrage dégradés . . . . .	242
6.2 Les attaques de preboot . . . . .	243
6.3 L'hibernation . . . . .	243
6.4 Les sauvegardes . . . . .	244
7. Windows . . . . .	244
7.1 Gestion des utilisateurs . . . . .	244
7.2 Gestion des groupes . . . . .	245
7.3 Affectation des permissions . . . . .	246



7.4	Les mots de passe . . . . .	247
7.4.1	Changer son mot de passe en ligne de commande . . . . .	248
7.4.2	Stockage des mots de passe dans un groupe de travail . . . . .	248
7.4.3	Stockage des mots de passe dans un domaine . . . . .	249
7.4.4	Extraction des données d'une SAM . . . . .	250
7.4.5	Chiffrement LM (LAN Manager) . . . . .	253
7.4.6	Chiffrement NTLM (NT hash) NTLMv1 . . . . .	254
7.4.7	Chiffrement NTLM (NT hash) NTLMv2 . . . . .	255
7.4.8	Choix du niveau d'authentification . . . . .	256
7.5	Élévation des privilèges . . . . .	258
7.6	Le Planificateur de tâches . . . . .	263
7.7	Espionner des processus sous Windows . . . . .	263
7.8	Les appels de procédures distantes . . . . .	264
7.9	L'accès au registre à distance . . . . .	265
7.10	Les logs . . . . .	265
7.11	Les mises à jour . . . . .	266
7.12	Cas pratiques . . . . .	267
7.12.1	Révéler un mot de passe mémorisé par une application . . . . .	267
7.12.2	Utilisation de Hiren's BootCD . . . . .	272
7.12.3	Faible physique osk.exe . . . . .	273
7.12.4	Trouver les hashes en ligne . . . . .	274
7.12.5	Utilisation de John the Ripper . . . . .	275
7.12.6	Utilisation de Hashcat . . . . .	277
7.12.7	Récupération de condensat avec Responder . . . . .	281
7.12.8	Pass The Hash . . . . .	284
7.12.9	Récupération de condensat d'une machine locale et élévation de privilège avec Mimikatz . . . . .	286
7.12.10	Exploitation du krbtgt (Golden Ticket) . . . . .	289
8.	Linux . . . . .	295
8.1	Gestion des utilisateurs . . . . .	295
8.2	Gestion des groupes . . . . .	296
8.3	Affectation des permissions . . . . .	296
8.4	Les mots de passe . . . . .	297
8.5	Élévation des privilèges . . . . .	299
8.5.1	Activation du suid et du sgid . . . . .	300
8.5.2	Comment trouver les scripts suid root d'un système GNU/Linux . . . . .	300

# 10 \_\_\_\_\_ Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

8.6	Le changement de racine ou chrooting . . . . .	301
8.7	Les logs . . . . .	301
8.8	Les mises à jour . . . . .	301
8.9	Cas pratiques . . . . .	301
8.9.1	Utilisation de John the Ripper . . . . .	301
8.9.2	GRUB . . . . .	302
9.	macOS X . . . . .	304
9.1	Gestion des utilisateurs . . . . .	304
9.2	Les mots de passe . . . . .	306
9.3	Gestion des groupes . . . . .	307
9.4	Affectation des permissions . . . . .	307
9.5	Les logs . . . . .	308
9.6	Les mises à jour . . . . .	308
10.	Exploitation des vulnérabilités des systèmes d'exploitation . . . . .	308
10.1	Cas pratique . . . . .	315
11.	Big Data et confidentialité . . . . .	316
12.	Conclusion . . . . .	318

## Chapitre 6

### Les failles réseau

1.	Généralités . . . . .	319
2.	Rappel sur les réseaux TCP/IP . . . . .	319
2.1	Le modèle OSI . . . . .	319
2.2	Adresse MAC et adresse IP . . . . .	320
2.3	Notion de passerelle, de masque et de sous-réseau . . . . .	321
2.4	TCP et UDP . . . . .	323
2.5	Les services et les ports . . . . .	323
2.6	Les adresses IPv4 publiques et privées . . . . .	325
3.	Outils pratiques . . . . .	326
3.1	Des informations sur les sockets . . . . .	326
3.2	Des informations sur une adresse publique ou un nom de domaine . . . . .	328
3.3	Scanner de port TCP . . . . .	329
3.3.1	Scanner sa propre machine . . . . .	329
3.3.2	Scanner un sous-réseau . . . . .	330

3.3.3	Scanner un réseau sans communiquer directement avec la cible . . . . .	332
3.3.4	Scanner un réseau sans scanner les ports . . . . .	333
3.3.5	Scanner un réseau via "TCP SYN scan" (half open scan). . . . .	334
3.3.6	Scanner un réseau via "TCP XMAS scan" et "Maimon scan". . . . .	345
3.3.7	Scanner un réseau via "TCP FIN scan" . . . . .	346
3.3.8	Scanner un réseau via "TCP NULL scan" . . . . .	347
3.3.9	Scanner un réseau via "TCP IDLE scan" . . . . .	347
3.3.10	Scanner un réseau via "UDP scan" . . . . .	349
3.3.11	Scanner un réseau via "TCP-ACK scan" . . . . .	351
3.4	Gestion des sockets . . . . .	353
3.4.1	Comment prendre la main sur un hôte distant ? . . . . .	353
3.4.2	Transfert de fichiers entre deux machines . . . . .	354
3.4.3	Prise de contrôle d'un ordinateur sur un réseau privé . . . . .	355
3.5	SSH. . . . .	356
3.6	Tunnel SSH . . . . .	357
3.6.1	Contournement d'un pare-feu afin de joindre un hôte distant . . . . .	357
3.6.2	Autoriser un accès momentané depuis l'extérieur . . . . .	359
4.	DoS et DDoS . . . . .	361
5.	Sniffing. . . . .	362
5.1	Capturer des données avec Wireshark . . . . .	363
5.2	Les filtres . . . . .	365
6.	Man In The Middle dans un réseau local. . . . .	367
6.1	Empoisonnement du cache ARP (théorie) . . . . .	367
6.2	Empoisonnement du cache ARP (pratique). . . . .	372
6.2.1	Installation d'Ettercap . . . . .	372
6.2.2	Configuration d'Ettercap . . . . .	374
6.2.3	Les plugins sous Ettercap . . . . .	377
6.2.4	Création d'un filtre . . . . .	378
6.2.5	Caïn & Abel . . . . .	380
6.3	Empoisonnement du cache ARP (contre-mesures) . . . . .	380
6.4	Utilisation d'un serveur DHCPv4 clandestin (théorie). . . . .	382
6.5	Utilisation d'un serveur DHCPv4 clandestin (pratique). . . . .	383
6.6	Utilisation d'un serveur DHCPv4 clandestin (contre-mesures) . . . . .	384

# 12 \_\_\_\_\_ Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

7.	Vol de session TCP (hijacking) et spoofing d'IP	385
7.1	La faille : l'ACK/SEQ	385
7.2	Conséquence de l'attaque	386
7.3	Mise en pratique	386
7.4	Automatiser l'attaque	389
7.5	Spoofing d'adresse IP	389
8.	Failles Wi-Fi	392
8.1	Cracker un réseau WEP	392
8.1.1	Capturer des paquets	393
8.1.2	Générer du trafic	393
8.1.3	Trouver la clé	394
8.2	Cracker un réseau WPA2	396
8.3	Rogue AP	400
8.3.1	Introduction au Rogue AP	400
8.3.2	Mise en pratique d'un Rogue AP avec Karmetasloit	401
9.	IP over DNS	403
9.1	Principe	403
9.2	En pratique	403
9.3	Contre-mesures	404
10.	La téléphonie sur IP	405
10.1	Écoute de conversation	405
10.2	Usurpation de ligne	406
10.3	Autres attaques	408
11.	IPv6	408
11.1	Les logiciels	409
11.2	Le matériel	409
11.3	L'humain	409
11.4	THC-IPv6	410
11.5	Scanner les hôtes	410
11.5.1	Sur un réseau local	410
11.5.2	Sur Internet	410
11.6	Attaque Man In the Middle	411
12.	Conclusion	413

**Chapitre 7**

**La sécurité des communications sans fil**

- 1. Présentation . . . . . 415
- 2. Les objets connectés . . . . . 416
- 3. Les transmissions radio . . . . . 416
- 4. La radio logicielle . . . . . 419
- 5. Le matériel disponible . . . . . 420
  - 5.1 La clé RTL-SDR . . . . . 420
  - 5.2 Le HackRF One . . . . . 421
  - 5.3 Le bladeRF . . . . . 422
  - 5.4 Le PandwaRF . . . . . 423
  - 5.5 L'USRP . . . . . 424
- 6. Les protocoles . . . . . 425
  - 6.1 Le ZigBee . . . . . 425
  - 6.2 Le Z-Wave . . . . . 428
  - 6.3 Le Bluetooth . . . . . 430
- 7. La suite GNU Radio . . . . . 432
  - 7.1 Les bases de GNU Radio Companion . . . . . 433
  - 7.2 Module Python . . . . . 440
  - 7.3 Module écrit en CPP (C++) . . . . . 448
- 8. Exemples d'applications . . . . . 452
  - 8.1 Communication NRF24 . . . . . 453
  - 8.2 Communication ZigBee . . . . . 461
- 9. Conclusion . . . . . 466

**Chapitre 8**

**Les failles web**

- 1. Rappels sur le Web . . . . . 467
- 2. Composition et consultation d'un site web . . . . . 468
  - 2.1 Composition d'un site web . . . . . 468
  - 2.2 Consultation d'une page web . . . . . 468

# 14 \_\_\_\_\_ Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

3.	Les failles web	480
3.1	Définition et importances	480
3.2	Exposition et architecture d'un site web	480
3.3	Comment aborder la sécurité des sites web	483
3.3.1	Choisir son domaine d'étude	483
3.3.2	Les failles les plus répandues	485
3.4	Installation et configuration d'un serveur web complet	489
3.4.1	Installation et configuration du serveur de base	489
3.4.2	Installation et configuration du serveur de bases de données	495
3.4.3	Installation d'un langage côté serveur	498
3.5	Présentation de quelques failles web	503
3.5.1	Préambule	503
3.5.2	Les injections SQL classiques	503
3.5.3	Les injections SQL en aveugle	520
3.5.4	Les injections côté client	523
3.5.5	Passer les contrôles côté client	527
3.6	S'entraîner à l'audit et détecter les différentes failles web	529
3.6.1	Pour s'entraîner	529
3.6.2	Des outils pour auditer	530
4.	Contre-mesures et conseils de sécurisation	535
4.1	Filtrer toutes les données	535
4.1.1	Constat	535
4.1.2	Éviter les injections SQL	536
4.1.3	Filtrer les données	537
4.2	Utiliser des frameworks pour le développement	540
5.	Conclusion	541

## Chapitre 9

### Les failles applicatives

1.	Généralités	543
2.	Notions d'Assembleur	544
2.1	Introduction	544
2.2	Premiers pas	544
2.2.1	Apprenons à compter	544
2.2.2	Le binaire	544

- 2.2.3 L'hexadécimal . . . . . 545
- 2.3 Comment tester nos programmes ? . . . . . 547
  - 2.3.1 Squelette d'un programme en Assembleur . . . . . 547
  - 2.3.2 Notre premier programme . . . . . 548
- 2.4 Les instructions . . . . . 549
  - 2.4.1 La comparaison . . . . . 549
  - 2.4.2 L'instruction IF . . . . . 550
  - 2.4.3 La boucle FOR . . . . . 551
  - 2.4.4 La boucle WHILE . . . . . 552
  - 2.4.5 La boucle DO WHILE . . . . . 552
  - 2.4.6 La directive %define . . . . . 554
  - 2.4.7 Les directives de données . . . . . 554
  - 2.4.8 Les entrées-sorties . . . . . 554
- 2.5 Les interruptions . . . . . 555
- 2.6 Les sous-programmes . . . . . 557
- 2.7 Le tas et la pile . . . . . 558
  - 2.7.1 Le tas . . . . . 558
  - 2.7.2 La pile . . . . . 559
  - 2.7.3 Appel et retour de fonction : les notions fondamentales . . . . . 560
- 3. Bases des shellcodes . . . . . 562
  - 3.1 Exemple 1 : shellcode.py . . . . . 562
  - 3.2 Exemple 2 : execve() . . . . . 563
  - 3.3 Exemple 3 : Port Binding Shell . . . . . 565
- 4. Les buffer overflows . . . . . 566
  - 4.1 Quelques définitions . . . . . 566
  - 4.2 Notions essentielles . . . . . 567
  - 4.3 Stack overflow . . . . . 569
  - 4.4 Heap overflow . . . . . 576
  - 4.5 return-into-libc . . . . . 580
- 5. Les failles Windows . . . . . 584
  - 5.1 Introduction . . . . . 584
  - 5.2 Premiers pas . . . . . 584
    - 5.2.1 En mode console . . . . . 585
    - 5.2.2 Débogage . . . . . 586
    - 5.2.3 Problème d'un grand shellcode . . . . . 590
    - 5.2.4 Exécution d'une fonction non prévue . . . . . 593

# 16 \_\_\_\_\_ Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

5.2.5	Autres méthodes	594
5.3	La méthode du call [reg]	595
5.4	La méthode pop ret	595
5.5	La méthode du push return	596
5.6	La méthode du jmp [reg] + [offset]	596
5.7	La méthode du blind return	596
5.8	Que faire avec un petit shellcode ?	597
5.8.1	Principe	597
5.8.2	En pratique	597
5.9	Le SEH (Structured Exception Handling)	598
5.9.1	Les bases	598
5.9.2	SEH : les protections	600
5.9.3	XOR et Safe-SEH	600
5.10	Passer les protections	601
5.10.1	Stack cookie, protection /GS	601
5.10.2	Exemple : outrepasser le cookie	605
5.10.3	SafeSEH	608
6.	Cas concret : Ability Server	609
6.1	Fuzzing	609
6.2	Exploitation	611
7.	Cas concret : MediaCoder-0.7.5.4796	616
7.1	Crash du logiciel	616
7.2	Vérification des valeurs	621
7.3	Finalisation de l'exploit	621
8.	Cas concret : BlazeDVD 5.1 Professional	624
9.	Conclusion	627
10.	Références	628

## Chapitre 10 Forensic

1.	Introduction	629
1.1	Le cerveau	630
1.2	La mémoire	631
1.3	Les fichiers	633



- 2. Les méthodes . . . . . 634
  - 2.1 Préparation et environnement . . . . . 634
  - 2.2 Recherche et analyse de fichiers . . . . . 635
- 3. Les outils . . . . . 637
  - 3.1 Les outils d'analyse réseau . . . . . 638
    - 3.1.1 Wireshark . . . . . 638
    - 3.1.2 tcpdump . . . . . 638
    - 3.1.3 Scapy . . . . . 639
  - 3.2 Les outils d'analyse mémoire . . . . . 639
    - 3.2.1 Méthodes de récupération de la mémoire RAM . . . . . 641
    - 3.2.2 Dump mémoire sous Linux . . . . . 646
    - 3.2.3 Analyse des images mémoire . . . . . 647
    - 3.2.4 Le framework Volatility . . . . . 648
    - 3.2.5 Volatility et Linux . . . . . 660
    - 3.2.6 Introduction à Volatility 3 . . . . . 662
    - 3.2.7 Autres outils d'analyse mémoire . . . . . 663
  - 3.3 Les outils d'analyse binaire . . . . . 664
    - 3.3.1 Hexdump . . . . . 664
    - 3.3.2 Readelf . . . . . 665
    - 3.3.3 gdb . . . . . 665
  - 3.4 Les outils d'analyse système . . . . . 666
    - 3.4.1 The Coroner's Toolkit . . . . . 666
    - 3.4.2 Logstash . . . . . 666
- 4. Conclusion . . . . . 667

**Chapitre 11**

**Malwares : étude des codes malveillants**

- 1. Introduction . . . . . 669
- 2. Qu'est-ce qu'un malware ? . . . . . 670
- 3. La meilleure classification . . . . . 671
- 4. La détection par base de connaissance . . . . . 672
- 5. Correspondances partielles . . . . . 675
- 6. Structure d'un PE et imphash . . . . . 677
- 7. Entropie et packing . . . . . 679

# 18 \_\_\_\_\_ Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

8. Analyses et outillage . . . . .	683
9. Simulations et profilage. . . . .	688
10. Sites de classifications et sandboxes. . . . .	691

## Chapitre 12

### Les appareils mobiles : failles et investigations

1. Généralités . . . . .	693
2. Les vecteurs d'attaque . . . . .	694
2.1 Introduction . . . . .	694
2.2 Anatomie des attaques mobiles . . . . .	694
2.3 Les données ciblées. . . . .	695
3. Top 10 des vulnérabilités des mobiles . . . . .	695
3.1 Utilisation incorrecte de la plateforme. . . . .	695
3.2 Stockage de données non sécurisé. . . . .	696
3.3 Communication non sécurisée . . . . .	696
3.4 Authentification non sécurisée . . . . .	696
3.5 Cryptographie insuffisante . . . . .	696
3.6 Autorisation non sécurisée . . . . .	697
3.7 Qualité du code faible . . . . .	697
3.8 Falsification de code. . . . .	697
3.9 Ingénierie inverse . . . . .	697
3.10 Fonctionnalité étrangère . . . . .	698
4. Réseau cellulaire. . . . .	698
4.1 Définitions . . . . .	698
4.2 IMSI-catcher. . . . .	699
4.3 Interception passive. . . . .	699
4.3.1 Installation . . . . .	700
4.3.2 Démonstration . . . . .	700
4.4 Conclusion . . . . .	702
5. Android. . . . .	703
5.1 Introduction. . . . .	703
5.2 Les différentes versions . . . . .	704
5.2.1 Introduction . . . . .	704
5.2.2 Problématique. . . . .	704

5.2.3	Solutions . . . . .	705
5.3	Les ROM Custom . . . . .	707
5.3.1	Processus de démarrage . . . . .	708
5.3.2	Bootloader . . . . .	708
5.3.3	Recovery . . . . .	710
5.3.4	Root . . . . .	712
5.4	L'architecture . . . . .	714
5.4.1	Linux Kernel . . . . .	715
5.4.2	Hardware Abstraction Layer . . . . .	715
5.4.3	Libraries . . . . .	715
5.4.4	Android Runtime . . . . .	716
5.4.5	Java API Framework . . . . .	717
5.4.6	System Apps . . . . .	717
5.5	Structure d'une application . . . . .	717
5.5.1	Activity . . . . .	718
5.5.2	View . . . . .	719
5.5.3	Service . . . . .	719
5.5.4	Intent . . . . .	720
5.5.5	BroadcastReceiver . . . . .	721
5.5.6	ContentProvider . . . . .	722
5.6	Android Package . . . . .	722
5.7	Système de fichiers . . . . .	723
5.7.1	Les partitions . . . . .	723
5.7.2	La hiérarchie . . . . .	724
5.8	Émulateurs . . . . .	727
5.8.1	Genymotion . . . . .	727
5.9	Forensic . . . . .	731
5.9.1	ADB . . . . .	731
5.9.2	Contourner l'écran de verrouillage . . . . .	734
5.9.3	Acquisition de données . . . . .	736
5.9.4	Analyse mémoire . . . . .	742
5.9.5	Solution tout en un . . . . .	743
5.10	Conclusion . . . . .	747
6.	Vulnérabilités des applications . . . . .	747
6.1	Distribution . . . . .	748
6.2	ADB . . . . .	748
6.3	Frameworks . . . . .	748

6.4	DIVA.....	749
6.5	Conclusion.....	768
7.	Conclusion.....	768

## Chapitre 13

### Les failles matérielles

1.	Introduction.....	769
2.	L'outillage de base.....	770
2.1	Lot de tournevis.....	770
2.2	Multimètre.....	771
2.3	Platine de test.....	771
2.4	Câbles Dupont.....	772
2.5	Fer à souder.....	772
2.6	Arduino.....	772
2.7	Matériel de récupération.....	773
3.	Utilisateur régulier.....	773
3.1	Adaptateur USB RS232 TTL.....	773
3.2	Sonde d'analyse logique.....	774
3.3	Interface JTAG.....	774
3.4	Bus pirate de Dangerous Prototypes.....	775
3.5	SDR low cost.....	775
4.	Utilisateur avancé.....	776
4.1	Logiciel de conception de PCB.....	776
4.2	Programmeur.....	777
4.3	Matériel d'électronicien.....	778
5.	Méthodologie du reverse engineering matériel.....	779
5.1	Attaque via sniffing I <sup>2</sup> C.....	781
5.2	Attaque via sniffing UART modem.....	783
6.	Étude autour des T2G et Arduino.....	784
6.1	Création d'un lecteur de cartes T2G.....	785
6.2	Émulateur partiel de carte T2G.....	793

## Chapitre 14

### La sécurité des box

1. Introduction . . . . .	797
2. Les fonctionnalités d'une box . . . . .	798
2.1 Routeur . . . . .	798
2.2 Switch . . . . .	798
2.3 Téléphonie . . . . .	798
2.4 TV . . . . .	799
2.5 Stockage multimédia . . . . .	799
2.6 Services domotiques . . . . .	799
3. Les différentes box . . . . .	800
3.1 Orange . . . . .	800
3.2 Free . . . . .	801
3.3 Bouygues . . . . .	802
3.4 SFR . . . . .	803
4. La configuration des box . . . . .	804
4.1 Le mode modem . . . . .	804
4.2 Le mode routeur . . . . .	804
4.3 Les fonctions téléphoniques . . . . .	806
5. La configuration par défaut, un danger . . . . .	806
5.1 L'interface d'administration web . . . . .	806
5.2 Le Wi-Fi . . . . .	807
5.3 Les services : SSH, Telnet, Samba, TR069 . . . . .	808
6. Installation d'un firmware alternatif . . . . .	809
6.1 Dans quel intérêt ? . . . . .	809
6.2 Connexion au port console . . . . .	810
7. La sécurité des firmwares officiels . . . . .	815
7.1 Les failles de ces dernières années . . . . .	815
7.2 Et actuellement ? . . . . .	816
8. Reverse engineering de la Neufbox 5 . . . . .	817
8.1 Introduction . . . . .	817
8.2 Caractéristiques techniques . . . . .	818
8.3 Recherche du port série . . . . .	818
8.4 Connexion au port série . . . . .	820
8.5 Création d'une image complète . . . . .	824

8.6	Flashage de l'image . . . . .	825
8.7	Utilisation de la box en tant que routeur . . . . .	829
8.8	Téléphonie SIP . . . . .	830
8.9	Installation d'un firmware libre OpenWRT . . . . .	834

## Chapitre 15

### Hacking du véhicule connecté

1.	Introduction : vers le véhicule autonome . . . . .	835
2.	Véhicule connecté et véhicule autonome . . . . .	836
3.	Services d'un véhicule connecté/autonome . . . . .	837
4.	Le véhicule connecté, une vaste surface d'attaque . . . . .	837
5.	Motivations du hacking du véhicule connecté . . . . .	839
6.	Les systèmes internes du véhicule connecté . . . . .	840
7.	Attaque physique de l'ECU : le chiptuning ou le remapping . . . . .	843
7.1	ECU et ports de communication du MCU . . . . .	843
7.2	Hacking mémoire : matériel, outils et logiciels utilisés . . . . .	847
7.3	Hacking de la mémoire morte : reprogrammation d'un "key immobilizer" de chez Toyota/Lexus . . . . .	849
8.	Attaque backdoor : l'injection dans le réseau CAN . . . . .	856
8.1	Présentation de l'OBD . . . . .	856
8.2	Présentation du bus CAN et de ses trames . . . . .	859
8.3	Hacking du CAN : conséquences et mises en garde . . . . .	862
8.4	Présentation des messages de diagnostic via l'OBD2 et via le protocole UDS . . . . .	863
8.5	Présentation du matériel utilisable pour l'injection . . . . .	869
8.5.1	ELM327 . . . . .	870
8.5.2	Arduino . . . . .	871
8.5.3	Raspberry Pi . . . . .	871
8.5.4	CANTACT . . . . .	872
8.6	Les outils de sniffing et d'injection pour le bus CAN . . . . .	873
8.6.1	SocketCAN et les utilitaires can-utils . . . . .	873
8.6.2	Kayak . . . . .	878
8.6.3	CANalyzat0r . . . . .	881
8.6.4	SavvyCAN . . . . .	882

- 8.6.5 Katy OBD ..... 883
- 8.7 Les simulateurs de trames du bus CAN ..... 884
  - 8.7.1 ICSim. .... 884
  - 8.7.2 UDS Server ..... 889
  - 8.7.3 ICSim de la conférence Barbhack 2020. .... 890
  - 8.7.4 VIC ..... 891
  - 8.7.5 UDSim. .... 892
  - 8.7.6 CANdevStudio ..... 893
- 8.8 Openpilot et la conduite autonome pour tous ..... 897
- 8.9 Une conséquence d'OpenPilot, l'interprétation standardisée des trames CAN via le format DBC ..... 899
- 8.10 Les injections à distance ..... 902
  - 8.10.1 Car Backdoor Maker et The Bicho ..... 902
  - 8.10.2 CANalyse et la messagerie Telegram ..... 904
- 9. Autres attaques du véhicule connecté ..... 905
  - 9.1 Application mal sécurisée : le cas Nissan Leaf de 2016 ..... 905
  - 9.2 Le hacking du TPMS ..... 909
    - 9.2.1 Matériel radio ..... 912
    - 9.2.2 Le logiciel RTL\_433 ..... 912
    - 9.2.3 Le simulateur de trames TPMS : TXTPMS ..... 913

**Chapitre 16**  
**Risques juridiques et solutions**

- 1. Préambule. .... 915
- 2. Atteintes à un système d'information ..... 917
  - 2.1 Accès et maintien dans un système d'information ..... 917
    - 2.1.1 Élément matériel. .... 920
    - 2.1.2 Élément moral. .... 922
  - 2.2 Atteinte au fonctionnement d'un système d'information ..... 924
  - 2.3 Atteinte aux données d'un système d'information. .... 926
  - 2.4 Diffusion d'un logiciel d'intrusion ..... 928
- 3. Atteintes aux traitements de données à caractère personnel ..... 929
  - 3.1 Notion de données à caractère personnel. .... 929
  - 3.2 Cas particulier de l'adresse IP ..... 931
  - 3.3 Collecte illicite de données à caractère personnel ..... 931

# 24 \_\_\_\_\_ Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

3.4	Divulgarion illicite de données à caractère personnel . . . . .	932
3.5	Sanctions administratives (CNIL) . . . . .	932
3.6	Obligation de sécurité du responsable de traitement . . . . .	933
3.7	Obligation de notification des failles de sécurité. . . . .	940
3.8	Contrôles en ligne de la CNIL. . . . .	942
3.9	Obligation de conservation des données de connexion. . . . .	944
3.10	Obligation de conservation des données relatives aux contenus . . .	945
3.11	Accès administratif aux données de connexion. . . . .	946
3.12	Les autres obligations spécifiques des FAI et hébergeurs. . . . .	949
4.	Infractions classiques applicables à l'informatique . . . . .	951
4.1	Escroquerie . . . . .	952
4.2	Usurpation d'identité . . . . .	952
4.3	Atteinte au secret des correspondances . . . . .	954
4.4	Dégradation physique d'un système . . . . .	957
4.5	Vol d'informations. . . . .	958
5.	Solutions et précautions . . . . .	958
5.1	Encadrement contractuel des tests d'intrusion . . . . .	959
5.1.1	Exonérations de responsabilité du prestataire. . . . .	959
5.1.2	Périmètre des tests d'intrusion. . . . .	960
5.1.3	Principes dégagés par la charte FPTI . . . . .	961
5.2	Hors cadre contractuel : la révélation publique de failles de sécurité . . . . .	962
5.2.1	Révélation d'une faille relative à un serveur . . . . .	962
5.2.2	Révélation d'une faille relative à un système d'exploitation .	965
5.2.3	Conseils quant à la divulgation de failles de sécurité . . . . .	966
6.	Conclusion . . . . .	968
7.	Références. . . . .	969



Les éléments à télécharger sont disponibles à l'adresse suivante :  
**<http://www.editions-eni.fr>**  
Saisissez la référence de l'ouvrage **EP4MAL** dans la zone de recherche  
et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

## Avant-propos

### Chapitre 1

#### Compréhension des malwares

1. Présentation des malwares par familles	13
1.1 Introduction	13
1.2 Backdoor	14
1.3 Ransomware et locker	15
1.4 Stealer	16
1.5 Miner	17
1.6 Banking trojan	17
1.7 Rootkit	17
2. Scénario d'infection	19
2.1 Introduction	19
2.2 Scénario 1 : exécution d'une pièce jointe	19
2.3 Scénario 2 : clic malencontreux	20
2.4 Scénario 3 : ouverture d'un document infecté	21
2.5 Scénario 4 : attaques informatiques	21
2.6 Scénario 5 : attaques physiques - infection par clé USB	22
2.7 Scénario 6 : attaques de type supply chain	22
3. Techniques de communication avec le C&C	23
3.1 Introduction	23
3.2 Mise à jour de la liste des noms de domaine	23
3.3 Communication via HTTP/HTTPS/FTP/IRC	24
3.4 Communication via un client e-mail	24
3.5 Communication via un réseau point à point	25

# 2 \_\_\_\_\_ Cybersécurité et Malwares

Détection, analyse et Threat Intelligence

3.6	Communication via des protocoles propriétaires . . . . .	25
3.7	Communication via le protocole DNS . . . . .	25
3.8	Communication passive . . . . .	26
3.9	Fast flux et DGA (Domain Generation Algorithms) . . . . .	26
3.10	Cibles sans accès internet . . . . .	27
4.	Mode opératoire en cas d'attaques ciblées persistantes (APT) . . . . .	28
4.1	Introduction . . . . .	28
4.2	Phase 1 : reconnaissance . . . . .	28
4.3	Phase 2 : intrusion . . . . .	29
4.4	Phase 3 : persistance . . . . .	30
4.5	Phase 4 : pivot . . . . .	30
4.6	Phase 5 : exfiltration . . . . .	31
4.7	Traces laissées par l'attaquant . . . . .	31
5.	Ressources sur Internet concernant les malwares . . . . .	32
5.1	Introduction . . . . .	32
5.2	Sites permettant des analyses en ligne . . . . .	32
5.3	Sites présentant des analyses techniques . . . . .	34
5.4	Sites permettant de télécharger des samples de malwares . . . . .	36
6.	Résumé . . . . .	37

## Chapitre 2

### Malwares ciblant les systèmes Microsoft Windows

1.	Introduction . . . . .	39
2.	Collecte d'informations . . . . .	40
2.1	Introduction . . . . .	40
2.2	Collecte et analyse de la base de registre . . . . .	40
2.3	Collecte et analyse des journaux d'événements . . . . .	42
2.4	Collecte et analyse des fichiers exécutés au démarrage . . . . .	43
2.5	Collecte et analyse du système de fichiers . . . . .	45
2.6	Gestion des fichiers bloqués par le système d'exploitation . . . . .	51
2.7	Outil DFIR ORC . . . . .	52

3.	Image mémoire	53
3.1	Présentation	53
3.2	Réalisation d'une image mémoire	54
3.3	Analyse d'une image mémoire	57
3.4	Analyse de l'image mémoire d'un processus	64
4.	Fonctionnalités des malwares	65
4.1	Techniques pour rester persistant	65
4.2	Techniques pour se cacher	67
4.3	Malware sans fichier	71
4.4	Contournement de l'UAC	72
5.	Création d'un laboratoire d'analyse	73
5.1	Introduction	73
5.2	VirtualBox	74
5.3	Machines virtuelles préconfigurées	80
5.4	Viper : l'outil de gestion d'échantillons de malwares	80
6.	Analyse du vecteur d'infection	88
6.1	Informations sur un fichier	88
6.1.1	Format d'un fichier	88
6.1.2	Chaînes de caractères présentes dans un fichier	89
6.2	Analyse dans le cas d'un fichier PDF	91
6.2.1	Introduction	91
6.2.2	Extraire le code JavaScript	92
6.2.3	Désobfusquer du code JavaScript	96
6.2.4	Conclusion	100
6.3	Analyse dans le cas d'un fichier Adobe Flash	100
6.3.1	Introduction	100
6.3.2	Extraire et analyser le code ActionScript	100
6.4	Analyse dans le cas d'un fichier JAR	101
6.4.1	Introduction	101
6.4.2	Récupération du code source depuis les classes	103

# 4 \_\_\_\_\_ Cybersécurité et Malwares

Détection, analyse et Threat Intelligence

6.5	Analyse dans le cas d'un fichier Microsoft Office . . . . .	104
6.5.1	Introduction . . . . .	104
6.5.2	Outils permettant l'analyse de fichiers Office . . . . .	104
6.5.3	Cas d'un malware utilisant des macros : Dridex . . . . .	105
6.5.4	Cas d'un malware utilisant une vulnérabilité . . . . .	107
6.6	Utilisation de PowerShell. . . . .	109
7.	Analyse dans le cas d'un binaire. . . . .	110
7.1	Analyse de binaires développés en AutoIt . . . . .	110
7.2	Analyse de binaires développés avec le framework .NET . . . . .	112
7.3	Analyse de scripts Python compilés . . . . .	113
7.4	Analyse de binaires développés en C ou C++ . . . . .	114
7.5	Analyse rapide des fonctionnalités d'un binaire. . . . .	114
7.6	Analyse de bootkits UEFI. . . . .	116
8.	Format PE . . . . .	117
8.1	Introduction . . . . .	117
8.2	Schéma du format PE . . . . .	117
8.2.1	En-tête MZ-DOS . . . . .	118
8.2.2	Segment DOS . . . . .	118
8.2.3	En-tête PE . . . . .	119
8.2.4	Table des sections. . . . .	122
8.2.5	Table des imports . . . . .	123
8.2.6	Table des exports . . . . .	124
8.2.7	Ressources . . . . .	125
8.3	Outils pour analyser un PE . . . . .	125
8.4	API d'analyse d'un PE . . . . .	128
9.	Suivre l'exécution d'un binaire. . . . .	132
9.1	Introduction . . . . .	132
9.2	Activité au niveau de la base de registre . . . . .	132
9.3	Activité au niveau du système de fichiers. . . . .	135
9.4	Activité réseau . . . . .	135
9.5	Activité réseau de type HTTP(S). . . . .	144

- 10. Utilisation de Cuckoo Sandbox . . . . . 145
  - 10.1 Introduction . . . . . 145
  - 10.2 Configuration . . . . . 145
  - 10.3 Utilisation . . . . . 147
  - 10.4 Limitations . . . . . 154
  - 10.5 Conclusion . . . . . 156
- 11. Résumé . . . . . 156

**Chapitre 3**  
**Reverse engineering**

- 1. Introduction . . . . . 157
  - 1.1 Présentation . . . . . 157
  - 1.2 Législation . . . . . 158
- 2. Qu'est-ce qu'un processus Windows ? . . . . . 159
  - 2.1 Introduction . . . . . 159
  - 2.2 Process Environment Block . . . . . 159
  - 2.3 Thread Environment Block . . . . . 161
- 3. Assembleur x86. . . . . 162
  - 3.1 Registres . . . . . 162
  - 3.2 Instructions et opérations . . . . . 167
  - 3.3 Gestion de la mémoire par la pile . . . . . 174
  - 3.4 Gestion de la mémoire par le tas . . . . . 177
  - 3.5 Optimisation du compilateur . . . . . 177
- 4. Assembleur x64. . . . . 179
  - 4.1 Registres . . . . . 179
  - 4.2 Paramètres des fonctions . . . . . 179
- 5. Analyse statique . . . . . 180
  - 5.1 Présentation . . . . . 180
  - 5.2 Ghidra . . . . . 180
    - 5.2.1 Présentation . . . . . 180

# 6 \_\_\_\_\_ Cybersécurité et Malwares

Détection, analyse et Threat Intelligence

5.3	Navigation	181
5.3.1	Renommages et commentaires	191
5.3.2	Extensions	193
5.3.3	Support de Python 3	195
5.4	Rizin	195
5.4.1	Présentation	195
5.4.2	Ligne de commande	195
5.4.3	Interface graphique : Cutter	197
5.5	Techniques d'analyse	201
5.5.1	Commencer une analyse	201
5.5.2	Sauts conditionnels	203
5.5.3	Boucles	204
5.6	API Windows	205
5.6.1	Introduction	205
5.6.2	API d'accès aux fichiers	206
5.6.3	API d'accès à la base de registre	209
5.6.4	API de communication réseau	215
5.6.5	API de gestion des services	220
5.6.6	API des objets COM	222
5.6.7	API restart manager	223
5.6.8	Exemples de l'utilisation de l'API	225
5.6.9	Conclusion	234
5.7	Comparaison entre binaires	234
5.7.1	Description	234
5.7.2	Outils	235
5.7.3	Exemple	235
5.8	Limites de l'analyse statique	241
6	Analyse dynamique	242
6.1	Présentation	242
6.2	x64dbg	242
6.2.1	Présentation	242
6.2.2	Contrôle de flux d'exécution	247
6.2.3	Points d'arrêt	251

- 6.2.4 Visualisation des valeurs en mémoire . . . . . 254
- 6.2.5 Copie de la mémoire . . . . . 255
- 6.3 WinDbg . . . . . 256
  - 6.3.1 Présentation . . . . . 256
  - 6.3.2 Interface . . . . . 257
  - 6.3.3 Commandes de base . . . . . 259
  - 6.3.4 Plug-in . . . . . 264
- 6.4 Analyse du noyau Windows . . . . . 265
  - 6.4.1 Présentation . . . . . 265
  - 6.4.2 Mise en place de l'environnement . . . . . 265
  - 6.4.3 Protections du noyau Windows . . . . . 266
- 6.5 Émulation et instrumentation . . . . . 267
- 6.6 Limites de l'analyse dynamique et conclusion . . . . . 268

**Chapitre 4**  
**Techniques d'obfuscation**

- 1. Introduction . . . . . 269
- 2. Obfuscation des chaînes de caractères . . . . . 271
  - 2.1 Introduction . . . . . 271
  - 2.2 Utilisation de ROT13 . . . . . 271
  - 2.3 Utilisation de la fonction XOR avec une clé statique . . . . . 275
  - 2.4 Utilisation de la fonction XOR avec une clé dynamique . . . . . 280
  - 2.5 Utilisation de fonctions cryptographiques . . . . . 283
  - 2.6 Utilisation de fonctions personnalisées . . . . . 290
  - 2.7 Outils permettant de décoder les chaînes de caractères . . . . . 299
  - 2.8 Utilisation de Cyberchef . . . . . 300
  - 2.9 Utilisation de Malduck . . . . . 304
- 3. Obfuscation de l'utilisation de l'API Windows . . . . . 305
  - 3.1 Introduction . . . . . 305
  - 3.2 Étude du cas Duqu . . . . . 307
  - 3.3 Étude du cas EvilBunny . . . . . 311

# 8 \_\_\_\_\_ Cybersécurité et Malwares

Détection, analyse et Threat Intelligence

4. Packers . . . . .	313
4.1 Introduction . . . . .	313
4.2 Packers utilisant la pile . . . . .	315
4.3 Packers utilisant le tas . . . . .	327
4.4 Encodeur Metasploit . . . . .	334
4.5 Outils pour automatiser l'unpack . . . . .	336
5. Autres techniques . . . . .	337
5.1 Anti-VM . . . . .	337
5.2 Anti-reverse engineering et anti-débogage . . . . .	339
6. Résumé . . . . .	343

## Chapitre 5

### Malwares ciblant les systèmes Android

1. Introduction . . . . .	345
2. Système d'exploitation Android . . . . .	346
2.1 Historique . . . . .	346
2.2 Architecture . . . . .	347
2.3 Partitions et systèmes de fichiers . . . . .	351
2.4 Sécurité . . . . .	355
2.4.1 Sécurité au niveau système . . . . .	355
2.4.2 Sécurité au niveau Dalvik/ART . . . . .	357
2.4.3 Effet de bord des fonctionnalités de sécurité . . . . .	359
2.5 Application Android . . . . .	359
2.6 Malwares ciblant les téléphones Android . . . . .	364
3. Vecteurs d'infection . . . . .	366
3.1 Installation via Google Store . . . . .	366
3.2 Installation via des stores alternatifs . . . . .	367
3.3 Installation manuelle . . . . .	367
3.4 MDM (Mobile Device Management) . . . . .	368
3.5 Accès physique au terminal . . . . .	368



4. Création d'un laboratoire d'analyse .....	369
4.1 Machine virtuelle ou téléphone physique ? .....	369
4.2 Adb (Android Debug Bridge) .....	373
4.3 Accès administrateur (root) .....	375
4.4 Capture réseau .....	379
4.4.1 Capture réseau pure .....	379
4.4.2 Capture HTTP/HTTPS .....	379
5. Analyse statique et décompilation d'une application .....	382
5.1 Analyse d'un fichier APK .....	382
5.2 Code Java et décompilation : Bytecode Viewer .....	385
5.3 Anti-VM .....	388
5.4 Code natif .....	390
5.5 Techniques d'obfuscation .....	393
6. Analyse dynamique .....	397
6.1 Utilisation de Frida .....	397
6.2 Utilisation de gdb pour les binaires natifs .....	399
7. Résumé .....	400

## Chapitre 6

### Malwares ciblant les systèmes iOS

1. Introduction .....	401
2. Système d'exploitation iOS .....	402
2.1 Historique .....	402
2.2 Architecture .....	402
2.3 Partitions et systèmes de fichiers .....	406
2.4 Sécurité .....	408
2.5 Jailbreak .....	410
2.6 Application iOS .....	411
2.7 Malwares ciblant iOS .....	414

# 10 \_\_\_\_\_ Cybersécurité et Malwares

Détection, analyse et Threat Intelligence

3. Vecteurs d'infection . . . . .	415
3.1 Accès physique au terminal . . . . .	415
3.2 Liens vers un fichier .ipa . . . . .	415
3.3 Stores alternatifs . . . . .	415
3.4 MDM malveillant . . . . .	416
4. Création d'un laboratoire d'analyse . . . . .	416
4.1 Analyse réseau . . . . .	416
4.2 Jailbreak d'un terminal et déploiement d'une application . . . . .	417
5. Analyse statique d'une application . . . . .	420
5.1 Introduction . . . . .	420
5.2 Analyse avec Ghidra . . . . .	420
6. Analyse dynamique . . . . .	428
6.1 Utilisation de Frida . . . . .	428
6.2 Utilisation de lldb . . . . .	430
7. Technique utilisée par les malwares sous iOS . . . . .	431
7.1 Injection de bibliothèques . . . . .	431
7.2 Injection de JavaScript . . . . .	433
7.3 Keylogger sous iOS . . . . .	434
7.4 Terminal jailbreaké et injection de code . . . . .	435
8. Résumé . . . . .	436

## Chapitre 7

### Analyse de malware et Threat Intelligence

1. Introduction . . . . .	437
2. Indicateurs de compromission (IOC) . . . . .	439
2.1 Empreintes et signatures de fichiers . . . . .	439
2.1.1 Empreintes cryptographiques . . . . .	439
2.1.2 Empreintes par similarité : ssdeep et TLSH . . . . .	441
2.1.3 Empreintes des tables d'imports des exécutable Windows . . . . .	445

2.2	Indicateurs système	448
2.2.1	Clés de registre	449
2.2.2	Système de fichiers	454
2.2.3	Réseau	455
2.2.4	Exécutions	456
3.	Matrice du MITRE, TTPs et Threat Actors	457
3.1	Matrice du MITRE	457
3.1.1	Présentation	457
3.1.2	Exemples d'utilisation de la matrice ATT&CK	460
3.2	TTP et Threat Actors	462
3.2.1	Définition	462
3.2.2	TTP de TA505	463
3.2.3	Threat Actor et Intrusion Set	464
4.	Règles et détections	465
4.1	Introduction	465
4.2	Suricata	465
4.2.1	Suricata	465
4.2.2	Exemple de détection	467
4.3	YARA	470
4.3.1	Présentation	470
4.3.2	Syntaxe	470
4.3.3	Exemple de détection de webshells	472
4.3.4	Exemple de détection de Chinoxy via le module PE	472
4.3.5	Python et YARA	479
4.3.6	Outils open source utilisant YARA	479
5.	Sources de données	481
5.1	Présentation	481
5.2	Scanners	481
5.2.1	Définition	481
5.2.2	Shodan.io	482
5.2.3	Onyphe.io	486
5.2.4	Censys.io	490

# 12 \_\_\_\_\_ Cybersécurité et Malwares

Détection, analyse et Threat Intelligence

5.3	Passives DNS	494
5.3.1	Présentation	494
5.3.2	Passive DNS de VirusTotal	494
5.3.3	RiskIQ	496
5.4	Dépôts de malwares	499
5.4.1	Présentation	499
5.4.2	VirusTotal	499
5.4.3	MalwareBazaar	501
5.5	Sources multi-indicateurs	507
5.5.1	Présentation	507
5.5.2	OTX AlienVault	507
5.5.3	RiskIQ	511
6.	Plateformes de Threat Intelligence	515
6.1	Introduction	515
6.2	MISP	515
6.2.1	Généralités	515
6.2.2	Fonctionnalités	516
6.3	Yeti	522
6.3.1	Présentation	522
6.3.2	Fonctionnalités	522
7.	Résumé	528
	Index	529