

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	28
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 scripts 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. Les principales normes en cybersécurité	39
5. Conclusion	40

2 ————— Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

Chapitre 2

Éléments d'ingénierie sociale

1. Généralités	43
1.1 Introduction	43
1.2 Systèmes d'information	45
1.2.1 Précisions sur les systèmes d'information	45
1.2.2 Failles d'un système d'information	46
1.3 Présentation de l'ingénierie sociale	46
1.3.1 Définitions	46
1.3.2 Caractéristiques et périmètre	47
1.4 Problématique de la protection	49
2. Modes d'action de l'ingénierie sociale	51
2.1 Principes de l'attaque par ingénierie sociale	51
2.2 Processus générique de l'ingénieur social	52
2.2.1 Étude préalable	53
2.2.2 Préparation	56
2.2.3 Exploitation	57
2.3 Compétences et outils de l'ingénieur social	58
2.3.1 Comédie, ruse, subterfuge et tromperie	59
2.3.2 Lecture de cible	59
2.3.3 L'Humain : maillon faible ou première ligne de défense ?	60
3. Connaissance des organisations attaquées	70
3.1 Typologies générales	71
3.2 Typologies de valeurs et de croyances	71
3.3 Modèles de maturité et certifications qualité	74
3.4 Exploitation	74
3.5 Exercices	75
4. Failles humaines : bases et modèles théoriques	75
4.1 Bases biologiques et fonctionnalités du cerveau	76
4.2 Biais cognitifs	77
4.3 Méthodes hypnotiques	78
4.4 Cohérence et recherche de « pattern »	79
4.5 Conclusion	79
4.6 Exercices	80

5.	Influence et manipulation.	80
5.1	Méthodes d'influence	80
5.1.1	Influence.	80
5.1.2	Tentation, séduction et intimidation.	81
5.1.3	Manipulation.	82
5.2	Les grands ressorts de la manipulation	82
5.2.1	Cohérence.	82
5.2.2	Réciprocité	83
5.2.3	Preuve sociale.	84
5.2.4	Autorité	85
5.2.5	Sympathie	85
5.2.6	Rareté	86
6.	Les techniques de manipulation.	87
6.1	Les grandes techniques de manipulation	88
6.1.1	Les amorçages et les leurres.	88
6.1.2	Le pied dans la porte	88
6.1.3	La porte au nez.	89
6.2	Les petites techniques de manipulation	89
6.2.1	Pied dans la bouche, politesse, sympathie	90
6.2.2	Contact, touché, regard.	90
6.2.3	Pièges de la cohérence	90
6.2.4	Étiquetage.	91
6.2.5	Déclaration de liberté	91
6.2.6	Quelques petites techniques à connaître	92
6.3	Exercices	93
7.	Savoir « patcher » les failles humaines	93
7.1	Volonté politique	94
7.2	Méthodologie	95
7.2.1	Professionnalisme, qualité, procédures, maturité	95
7.2.2	Mesure : tests, audit, retex de détection	95
7.2.3	Optimisation et changement de paradigme	96
7.3	Actions concrètes à mener	96
7.3.1	Documenter une politique de classification de l'information.	96
7.3.2	Contrôler les « input/output » (entrée/sortie d'information)	96
7.3.3	Sensibiliser le personnel.	97
7.3.4	Favoriser la remontée de l'information.	98

4 _____ Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

7.4 Exercices	99
8. OSINT	99
9. Bibliographie	102

Chapitre 3 Black Market

1. Introduction	103
2. Deep Web, Dark Web, Darknet, Black Market	103
3. Black Market, entre le visible et l'invisible	105
4. Fonctionnement	106
5. Anonymat des boutiques	108
6. Mode d'emploi de Tor	109
6.1 Installation	109
6.2 Configuration de la sécurité	110
6.3 Vérification de l'adresse IP	111
6.4 Navigation	111
6.5 Changement d'adresse IP	112
6.6 Mise à jour	112
7. Le référencement du Black Market	112
8. Annuaire de sites en .onion	116
9. Vocabulaire	117
10. Les nouveaux risques : IA, arnaques émotionnelles et data leaks	118

Chapitre 4 La recherche d'informations

1. Préambule	119
2. Types et méthodologies des attaques	120
2.1 L'évolution de la cybercriminalité	120
2.2 Les motivations	120

2.3	Les différents types d'attaque	121
2.3.1	L'attaque de type destructif	121
2.3.2	Les attaques à motivation financière	121
2.3.3	Les attaques de type APT (Advanced Persistent Threat)	122
2.3.4	La cyber kill chain ou les différentes phases d'une attaque.	122
3.	L'analyse des risques	124
4.	Le test d'intrusion	124
4.1	Le pentester	124
4.2	Les types d'audit	125
4.3	Les stratégies d'audit	125
4.4	Scénarios d'audit appliqués	126
5.	Collecte d'informations ou prise d'empreinte	126
5.1	Recherche OSINT ou recherche dite « passive »	127
5.1.1	Avant de commencer sa recherche OSINT	127
5.1.2	Sécuriser son environnement	127
5.1.3	Anonymisation et protection	128
5.1.4	Exegol - Une alternative Docker aux VM traditionnelles	129
5.2	Méthodologie d'une recherche OSINT	131
5.2.1	Recherche basique	131
5.2.2	Recherche technique	131
5.2.3	Vérification et croisement des données	131
5.2.4	Organisation et analyse des données	132
5.2.5	Diffusion et stockage (si contractualisé)	132
5.3	Les différents types de recherche en mode OSINT	133
5.3.1	Service WHOIS	133
5.3.2	Renseignements sur la raison sociale de la cible	134
5.3.3	Actualités liées à la cible	135
5.3.4	Analyse du site web.	136
5.3.5	Agrégateurs d'informations spécialisés	139
5.3.6	Outils de recherche d'objets connectés sur internet	142
5.3.7	Réseaux sociaux et professionnels	158
5.3.8	Extensions navigateurs spécialisées en OSINT	165
5.3.9	Big Data, Google Hack et Google Dorks	168
5.3.10	Frameworks spécialisés	178
5.3.11	Outils d'énumération DNS.	191
5.3.12	Corrélation des données : une étape importante en OSINT	203

6 ————— Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

5.3.13 Outils graphiques (corrélation et investigation)	205
5.3.14 Ressources pour outils OSINT	211
5.4 OSINT et intelligence artificielle	211
5.4.1 Rôle de l'IA dans l'OSINT	211
5.4.2 Sources d'OSINT optimisées par l'IA	212
5.4.3 Applications en collecte active et analyse	212
5.4.4 Exemples d'utilisation de l'IA en OSINT	212
5.5 La reconnaissance de type active	215
5.5.1 Les scanners réseau.	215
5.5.2 Les failles informatiques et leur référencement	235
5.5.3 Les scanners de vulnérabilités	238
5.5.4 Le reporting	250
6. Conclusion	257

Chapitre 5

Les failles système

1. Généralités	261
2. Les failles physiques.	262
2.1 Introduction	262
2.2 Lockpicking	262
2.3 Accès physique direct à l'ordinateur	263
2.3.1 Accès à un ordinateur éteint dont le BIOS/UEFI est protégé .	263
2.3.2 Accès à un ordinateur allumé dont le BIOS/UEFI est protégé	265
2.3.3 Accès à un ordinateur éteint dont le BIOS/UEFI n'est pas protégé.	265
2.3.4 Les attaques de preboot	268
3. Le démarrage	271
3.1 Faille des utilitaires d'accessibilité	271
3.2 Abus des modes de démarrage dégradés	272
3.3 Hibernation	274
3.4 Accès à la session de l'utilisateur	274
4. Les mots de passe.	279
4.1 Introduction	279
4.2 Complexité	279

4.3	Méthodes de détermination de mot de passe	280
4.3.1	Trouver les hashes en ligne	281
4.3.2	Outils de récupération de mots de passe	281
5.	Windows	286
5.1	Gestion des utilisateurs	286
5.2	Gestion des groupes	288
5.3	Affectation des permissions	289
5.4	Mots de passe	290
5.4.1	Changement du mot de passe en ligne de commande	290
5.4.2	Stockage des mots de passe dans un groupe de travail	291
5.4.3	Stockage des mots de passe dans un domaine	292
5.4.4	Extraction des données d'une SAM	292
5.4.5	Hash LM	294
5.4.6	Hash NT	295
5.4.7	NTLMv1	296
5.4.8	NTLMv2	297
5.4.9	Choix du niveau d'authentification	298
5.5	Élévation des privilèges	301
5.6	Runas	302
5.7	Planificateur de tâches	303
5.8	Services	304
5.9	Appels de procédures distantes	307
5.10	Potatoes	308
5.11	Pare-feu	313
5.12	Conclusion sur l'escalade de privilèges sous Windows	314
5.13	Cas pratiques	315
5.13.1	Utilisation d'outils de récupération de mots de passe	315
5.13.2	Pass The Hash	317
5.13.3	Récupération de condensat d'une machine locale et élévation de privilège avec Mimikatz	318
5.13.4	Exploitation du krbtgt (Golden Ticket)	321
5.14	Logs	326
5.15	Mises à jour	327
6.	Linux	328
6.1	Gestion des utilisateurs	328
6.2	Gestion des groupes	329

8 ————— Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

6.3	Affectation des permissions	329
6.3.1	Activation du suid et du sgid	333
6.3.2	Comment trouver les scripts suid root d'un système GNU/Linux	333
6.3.3	Mots de passe	334
6.4	Élévation des privilèges	336
6.5	Planificateur de tâches	338
6.6	Services	339
6.7	Kernel exploit	340
6.8	Pare-feu	342
6.9	Conclusion sur l'escalade de privilèges sous GNU/Linux	342
6.10	Logs	342
6.11	Mises à jour	343
7.	macOS	344
7.1	Gestion des utilisateurs	344
7.2	Gestion des groupes	346
7.3	Affectation des permissions	346
7.4	Les mots de passe	347
7.5	Élévation des privilèges	348
7.6	Logs	348
7.7	Mises à jour	349
8.	Exploitation des vulnérabilités des systèmes d'exploitation	349
9.	Big Data et confidentialité	360
10.	Conclusion	362

Chapitre 6

Les failles réseau

1.	Généralités	363
2.	Rappel sur les réseaux TCP/IP	363
2.1	Modèle OSI	363
2.2	Adresse MAC et adresse IP	364
2.3	Notion de passerelle, de masque et de sous-réseau	365
2.4	TCP et UDP	367
2.5	Services et ports	367
2.6	Adresses IPv4 publiques et privées	369

3.	Outils pratiques	370
3.1	Des informations sur les sockets	370
3.2	Des informations sur une adresse publique ou un nom de domaine	372
3.3	Scanner de port TCP	373
3.3.1	Scanner sa propre machine	373
3.3.2	Scanner un sous-réseau	373
3.3.3	Scanner un réseau sans communiquer directement avec la cible	375
3.3.4	Scanner un réseau sans scanner les ports	376
3.3.5	Scanner un réseau via "TCP SYN scan" (half open scan)	378
3.3.6	Scanner un réseau via "TCP XMAS scan" et "Maimon scan"	388
3.3.7	Scanner un réseau via "TCP FIN scan"	390
3.3.8	Scanner un réseau via "TCP NULL scan"	391
3.3.9	Scanner un réseau via "TCP IDLE scan"	391
3.3.10	Scanner un réseau via "UDP scan"	393
3.3.11	Scanner un réseau via "TCP-ACK scan"	395
3.4	Gestion des sockets	396
3.4.1	Comment prendre la main sur un hôte distant ?	396
3.4.2	Transfert de fichiers entre deux machines	398
3.4.3	Prise de contrôle d'un ordinateur sur un réseau privé	398
3.5	SSH	399
3.6	Tunnel SSH	400
3.6.1	Contournement d'un pare-feu afin de joindre un hôte distant	400
3.6.2	Autoriser un accès momentané depuis l'extérieur	402
4.	DoS et DDoS	404
5.	Sniffing	406
5.1	Capturer des données avec Wireshark	407
5.2	Les filtres	408
6.	Man In The Middle dans un réseau local	411
6.1	Empoisonnement du cache ARP (théorie)	411
6.2	Empoisonnement du cache ARP (pratique)	415
6.2.1	Installation d'Ettercap	415
6.2.2	Configuration d'Ettercap	416
6.2.3	Plugins sous Ettercap	419
6.2.4	Création d'un filtre	420

10 ————— Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

6.3	Empoisonnement du cache ARP (contre-mesures)	422
6.4	Utilisation d'un serveur DHCPv4 clandestin (théorie)	424
6.5	Utilisation d'un serveur DHCPv4 clandestin (pratique)	424
6.6	Utilisation d'un serveur DHCPv4 clandestin (contre-mesures)	430
7.	Vol de session TCP (hijacking) et spoofing d'IP	432
7.1	La faille : l'ACK/SEQ	432
7.2	Conséquence de l'attaque	433
7.3	Mise en pratique	433
7.4	Spoofing d'adresse IP et inondation SYN	436
8.	Faillles Wi-Fi	439
8.1	Cracker un réseau WEP	440
8.1.1	Capturer des paquets	440
8.1.2	Générer du trafic	441
8.1.3	Trouver la clé	442
8.2	Cracker un réseau WPA2	443
8.3	Rogue AP	447
8.3.1	Introduction au Rogue AP	447
8.3.2	Mise en pratique d'un Rogue AP avec Karmetaspoit	448
9.	IP over DNS	450
9.1	Principe	450
9.2	En pratique	450
9.3	Contre-mesures	451
10.	La téléphonie sur IP	451
10.1	Écoute de conversation	452
10.2	Usurpation de ligne	453
10.3	Autres attaques	454
11.	IPv6	455
11.1	Les logiciels	455
11.2	Le matériel	455
11.3	L'humain	456
11.4	THC-IPv6	456
11.5	Scanner les hôtes	456
11.5.1	Sur un réseau local	456
11.5.2	Sur Internet	457
11.6	Attaque Man In the Middle	457
12.	Conclusion	459

Chapitre 7

Les objets connectés et embarqués

1. La communication sans fil	461
1.1 Présentation	461
1.2 Les objets connectés	462
1.3 Les transmissions radio	462
1.4 La radio logicielle	465
1.5 Le matériel disponible	466
1.5.1 La clé RTL-SDR	466
1.5.2 Le HackRF One	467
1.5.3 Le bladeRF	468
1.5.4 Le PandwaRF	469
1.5.5 L'USRP	470
1.6 Les protocoles	471
1.6.1 Le ZigBee	471
1.6.2 Le Z-Wave	474
1.6.3 Le Bluetooth	476
1.7 La suite GNU Radio	478
1.7.1 Les bases de GNU Radio Companion	479
1.7.2 Module Python	486
1.7.3 Module écrit en CPP (C++).	493
1.8 Exemples d'applications	497
1.8.1 Communication NRF24	498
1.8.2 Communication ZigBee	505
1.9 Conclusion	510
2. Les objets connectés et les failles matérielles	510
2.1 Introduction	510
2.2 L'outillage de base	511
2.2.1 Lot de tournevis	511
2.2.2 Multimètre	512
2.2.3 Platine de test	513
2.2.4 Câbles Dupont	513
2.2.5 Fer à souder	513
2.2.6 Arduino	514
2.2.7 Matériel de récupération	514

12 ————— Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

2.3	L'outillage pour un utilisateur régulier	515
2.3.1	Adaptateur USB RS232 TTL	515
2.3.2	Sonde d'analyse logique	515
2.3.3	Interface JTAG	516
2.3.4	Bus pirate de Dangerous Prototypes	516
2.3.5	SDR low cost	517
2.4	L'outillage pour un utilisateur avancé	518
2.4.1	Logiciel de conception de PCB	518
2.4.2	Programmeur	518
2.4.3	Matériel d'électronicien	520
2.5	Méthodologie du reverse engineering matériel	520
2.5.1	Attaque via sniffing I ² C	522
2.5.2	Attaque via sniffing UART modem	524
2.6	Étude autour des T2G et Arduino	525
2.6.1	Création d'un lecteur de cartes T2G	526
2.6.2	Émulateur partiel de carte T2G	534
3.	La sécurité des box	537
3.1	Introduction	537
3.2	Les fonctionnalités d'une box	537
3.2.1	Routeur	537
3.2.2	Switch	538
3.2.3	Téléphonie	538
3.2.4	TV	538
3.2.5	Stockage multimédia	539
3.2.6	Services « maison connectée »	539
3.2.7	Hyperviseur	539
3.3	Les différentes box	540
3.3.1	Orange	540
3.3.2	Free	541
3.3.3	Bouygues	542
3.3.4	SFR	543
3.4	Les différents modes d'une box	544
3.4.1	Le mode modem	544
3.4.2	Le mode routeur	544
3.4.3	Les fonctions téléphoniques	546

3.5	La configuration par défaut, un danger.	546
3.5.1	L'interface d'administration web	546
3.5.2	Le Wi-Fi	547
3.5.3	Les services : SSH, Telnet, Samba, TR069	548
3.6	Installation d'un firmware alternatif	549
3.6.1	Dans quel intérêt ?	549
3.6.2	Connexion au port console	550
3.7	La sécurité des firmwares officiels	554
3.7.1	Les failles de ces dernières années	554
3.7.2	Et actuellement ?	556
3.8	Le Reverse engineering de la Neufbox 5	556
3.8.1	Introduction	556
3.8.2	Caractéristiques techniques	557
3.8.3	Recherche du port série	557
3.8.4	Connexion au port série	559
3.8.5	Création d'une image complète	563
3.8.6	Flashage de l'image	564
3.8.7	Utilisation de la box en tant que routeur	568
3.8.8	Téléphonie SIP	569
3.9	Utiliser son accès Internet sans Box	573
3.9.1	Préambule	573
3.9.2	Étapes à suivre	573
3.9.3	Configuration avec une offre Bouygues	573
3.9.4	Configuration chez Orange	574
3.9.5	Configuration chez SFR	576
3.9.6	Configuration chez Free	577

Chapitre 8

Les failles web

1.	Rappels sur le Web	579
2.	Composition et consultation d'un site web	580
2.1	Composition d'un site web	580
2.2	Consultation d'une page web	581

14 Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

3.	Les failles web	589
3.1	Définition et importances	589
3.2	Exposition et architecture d'un site web	590
3.3	Comment aborder la sécurité des sites web	592
3.3.1	Choisir son domaine d'étude	592
3.3.2	Les failles les plus répandues	593
4.	OWASP WSTG : un guide inestimable	598
5.	Méthodologie de pentest	600
5.1	Préparation et accord contractuel	600
5.2	Reconnaissance et évaluation des fonctionnalités interactives	600
5.3	Scanning automatique et détection des vulnérabilités	600
5.4	Tests manuels approfondis	601
5.5	Exploitation et post-exploitation	603
5.6	Analyse des résultats et attribution de score CVSS	603
5.7	Rapport de vulnérabilités et recommandations de remédiation	603
5.8	Outils utiles	604
6.	Présentation de quelques failles web	607
6.1	Préambule	607
6.2	Mise en place du lab	607
6.3	Prise d'empreinte	608
6.4	SQLI Boolean Based Blind - /api/beneficiary/fetch	610
6.4.1	Repérage	610
6.4.2	Définition de la vulnérabilité	610
6.4.3	Exploitation	611
6.5	Local File Inclusion / Path Traversal - /api/show	613
6.5.1	Repérage	613
6.5.2	Définition de la vulnérabilité	614
6.5.3	Exploitation	614
6.6	RCE – PHP unsafe Deserialization - /api/loan/apply	616
6.6.1	Repérage	616
6.6.2	Définition de la vulnérabilité	617
6.6.3	Exploitation	619
6.7	Conclusion	620
7.	S'entraîner à l'audit et détecter les différentes failles web	621

8.	Contre-mesures et conseils de sécurisation	621
8.1	Durcissement serveur	622
8.2	Durcissement client	629
8.3	Conception de l'application	631
9.	Conclusion	633

Chapitre 9

Les failles applicatives

1.	Généralités	635
2.	Notions d'Assembleur	636
2.1	Introduction	636
2.2	Premiers pas	636
2.2.1	Apprenons à compter	636
2.2.2	Le binaire	636
2.2.3	L'hexadécimal	637
2.3	Comment tester nos programmes ?	639
2.3.1	Squelette d'un programme en Assembleur	639
2.3.2	Notre premier programme	640
2.4	Les instructions	641
2.4.1	La comparaison	641
2.4.2	L'instruction IF	642
2.4.3	La boucle FOR	643
2.4.4	La boucle WHILE	644
2.4.5	La boucle DO WHILE	644
2.4.6	La directive %define	646
2.4.7	Les directives de données	646
2.4.8	Les entrées-sorties	646
2.5	Les interruptions	647
2.6	Les sous-programmes	649
2.7	Le tas et la pile	650
2.7.1	Le tas	650
2.7.2	La pile	651
2.7.3	Appel et retour de fonction : les notions fondamentales	652

16 ————— Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

3.	Bases des shellcodes	654
3.1	Exemple 1 : shellcode.py	654
3.2	Exemple 2 : execve()	655
3.3	Exemple 3 : Port Binding Shell	657
4.	Les buffer overflows.	658
4.1	Quelques définitions.	658
4.2	Notions essentielles.	659
4.3	Stack overflow.	661
4.4	Heap overflow.	668
4.5	return-into-libc	671
5.	Les failles Windows	676
5.1	Introduction	676
5.2	Premiers pas.	676
5.2.1	En mode console.	677
5.2.2	Débogage	678
5.2.3	Problème d'un grand shellcode	682
5.2.4	Exécution d'une fonction non prévue.	685
5.2.5	Autres méthodes	686
5.3	La méthode du call [reg]	687
5.4	La méthode pop ret	687
5.5	La méthode du push return	688
5.6	La méthode du jmp [reg] + [offset].	688
5.7	La méthode du blind return	688
5.8	Que faire avec un petit shellcode ?	689
5.8.1	Principe	689
5.8.2	En pratique.	689
5.9	Le SEH (Structured Exception Handling)	690
5.9.1	Les bases	690
5.9.2	SEH : les protections	691
5.9.3	XOR et Safe-SEH	692
5.10	Passer les protections	693
5.10.1	Stack cookie, protection /GS.	693
5.10.2	Exemple : outrepasser le cookie.	696
5.10.3	SafeSEH	699

6. Cas concret : Ability Server.	700
6.1 Fuzzing	700
6.2 Exploitation.	702
7. Cas concret : MediaCoder-0.7.5.4796.	707
7.1 Crash du logiciel	707
7.2 Vérification des valeurs	712
7.3 Finalisation de l'exploit.	712
8. Cas concret : BlazeDVD 5.1 Professional.	715
9. Conclusion	718
10. Références	718

Chapitre 10 Forensic

1. Introduction.	719
2. Artefacts et méthodologie.	721
2.1 Artefacts Windows.	721
2.2 Bonnes pratiques et cadre légal	722
2.3 Stockage d'informations.	723
2.4 Les fichiers.	726
3. Analyses	727
3.1 Préparation et environnement	727
3.2 Recherche et analyse de fichiers.	728
3.3 Formats de logs	731
3.4 Étude de registres	732
3.5 Étude de la table de fichiers	733
3.6 Étude de la RAM.	734
4. Distributions et outils.	735
5. Conclusion	736

18 _____ Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

Chapitre 11

Malwares : étude des codes malveillants

1. Introduction	737
2. Qu'est-ce qu'un malware ?	738
3. La meilleure classification	739
4. La détection par base de connaissance	740
5. Correspondances partielles	743
6. Structure d'un PE et imphash	745
7. Entropie et packing	747
8. Analyses et outillage	751
9. Simulations et profilage	756
10. Astuces	759
11. Sites de classifications et sandboxes	759

Chapitre 12

Les appareils mobiles : failles et investigations

1. Généralités	761
2. Les vecteurs d'attaque	762
2.1 Introduction	762
2.2 Anatomie des attaques mobiles	762
2.3 Les données ciblées	763
3. Top 10 des vulnérabilités des mobiles	763
3.1 Utilisation incorrecte des identifiants	763
3.2 Sécurité inadéquate de la chaîne d'approvisionnement	764
3.3 Authentification/autorisation non sécurisée	764
3.4 Validation d'entrée/sortie insuffisante	764
3.5 Communication non sécurisée	764
3.6 Contrôles de confidentialité inadéquats	765
3.7 Protections binaires insuffisantes	765
3.8 Mauvaise configuration de la sécurité	765
3.9 Stockage de données non sécurisé	766
3.10 Cryptographie insuffisante	766

4.	Réseau cellulaire	766
4.1	Définitions	767
4.2	IMSI-catcher	768
4.3	Interception passive	768
4.3.1	Installation	768
4.3.2	Démonstration	769
4.4	Conclusion	771
5.	Android	771
5.1	Introduction	772
5.2	Les différentes versions	773
5.2.1	Introduction	773
5.2.2	Problématique	773
5.2.3	Solutions	774
5.3	Les ROM Custom	776
5.3.1	Processus de démarrage	777
5.3.2	Bootloader	777
5.3.3	Recovery	779
5.3.4	Root	782
5.4	L'architecture	783
5.4.1	Linux Kernel	785
5.4.2	Hardware Abstraction Layer (HAL)	785
5.4.3	Libraries	785
5.4.4	Android Runtime	786
5.4.5	Java API Framework	787
5.4.6	System Apps	787
5.5	Structure d'une application	788
5.5.1	Activity	788
5.5.2	View	789
5.5.3	Service	789
5.5.4	Intent	790
5.5.5	BroadcastReceiver	792
5.5.6	ContentProvider	792
5.6	Android Package	792
5.7	Système de fichiers	793
5.7.1	Les partitions	793
5.7.2	La hiérarchie	794
5.8	Émulateurs	797

5.9	Forensic	801
5.9.1	ADB.	801
5.9.2	Malwares	804
5.9.3	Contourner l'écran de verrouillage	807
5.9.4	Acquisition de données	810
5.9.5	Analyse mémoire	815
5.9.6	Solution tout en un	816
5.10	Conclusion.	820
6.	Vulnérabilités des applications	820
6.1	Distribution.	821
6.2	ADB	821
6.3	Frameworks.	821
6.4	Guide	822
6.5	DIVA	823
6.6	Conclusion.	842
7.	Conclusion du chapitre	842

Chapitre 13

Hacking du véhicule connecté

1.	Introduction : vers le véhicule autonome.	845
2.	Véhicule connecté et véhicule autonome.	846
3.	Services d'un véhicule connecté/autonome	847
4.	Le véhicule connecté, une vaste surface d'attaque.	847
5.	Motivations du hacking du véhicule connecté	849
6.	Les systèmes internes du véhicule connecté	850
7.	Attaque physique de l'ECU : le chiptuning ou le remapping	853
7.1	ECU et ports de communication du MCU	853
7.2	Hacking mémoire : matériel, outils et logiciels utilisés	857
7.3	Hacking de la mémoire morte : reprogrammation d'un "key immobilizer" de chez Toyota/Lexus	859
8.	Attaque backdoor : l'injection dans le réseau CAN	866
8.1	Présentation de l'OBD.	866
8.2	Présentation du bus CAN et de ses trames	869
8.3	La « Secure Gateway »	873

8.4	Hacking du CAN : conséquences et mises en garde	875
8.5	Présentation des messages de diagnostic via l'OBD2 et via le protocole UDS	876
8.6	Présentation du matériel utilisable pour l'injection	882
8.6.1	ELM327	883
8.6.2	Arduino.	884
8.6.3	Raspberry Pi	884
8.6.4	CANTACT.	885
8.7	Les outils de sniffing et d'injection pour le bus CAN.	886
8.7.1	SocketCAN et les utilitaires can-utils	886
8.7.2	CANalyzat0r	891
8.7.3	SavvyCAN	892
8.7.4	Katy OBD.	893
8.8	Les injections à distance.	894
8.8.1	Car Backdoor Maker et The Bicho	894
8.8.2	CANalyse et la messagerie Telegram	896
8.9	Les simulateurs de trames du bus CAN	897
8.9.1	VIC	897
8.9.2	ICSim	898
8.9.3	UDS Server.	903
8.9.4	ICSim de la conférence Barbhack 2020	903
8.9.5	UDSim	905
8.9.6	CANdevStudio.	906
8.10	Les bancs d'essai	910
8.10.1	Exemple de banc d'essai très simple	910
8.10.2	Le « Training ECU » et le « Connected Tiny ECU »	914
8.10.3	Les « Cars in boxes ».	916
8.11	Openpilot et la conduite autonome pour tous.	918
8.11.1	Présentation	918
8.11.2	Une conséquence d'OpenPilot, l'interprétation standardisée des trames CAN via le format DBC	920

Chapitre 14

Analyses de risques

1. Introduction à la notion de risques.	925
2. Pourquoi faire une analyse des risques ?	926
3. Comment faire une analyse des risques ?	927
3.1 Ce que disent les normes, les textes de référence et la loi	927
3.2 Les différentes méthodes d'analyse des risques.	930
3.2.1 Présentation des différentes méthodes	930
3.2.2 Comment choisir la bonne méthode	932
4. Mise en œuvre de la méthode EBIOS RM	936
4.1 Les avantages de la méthode EBIOS RM.	936
4.2 Présentation de la méthode	937
4.3 Première approche de la méthode	938
4.4 Mise en œuvre des cinq ateliers	939
4.4.1 Préambule	939
4.4.2 L'atelier 1	940
4.4.3 L'atelier 2	945
4.4.4 L'atelier 3	948
4.4.5 L'atelier 4	954
4.4.6 L'atelier 5	964
5. Conclusion et analyse critique	966

Chapitre 15

Risques juridiques et solutions

1. Préambule	967
2. Cadre légal de l'intrusion	968
2.1 L'élément fondamental : le Système de Traitement Automatisé de Données (STAD)	968
2.2 L'accès et le maintien frauduleux (Article 323-1 du Code pénal)	969
2.3 Les circonstances aggravantes	970
2.4 L'entrave au fonctionnement (Article 323-2 du Code pénal)	971

2.5	Introduction, suppression et modification frauduleuse de données (Article 323-3 du Code pénal).	971
2.6	La mise à disposition d'outils d'attaque (article 323-3-1 du Code pénal)	972
3.	Fondement de la protection	973
3.1	Jurisprudence liée à l'élément moral	974
3.2	Construction et signature du contrat de pentest	975
3.2.1	Identification des parties et compétences	975
3.2.2	Périmètre technique.	975
3.2.3	Méthodes et techniques autorisées.	976
3.2.4	Données personnelles et RGPD	976
3.2.5	Responsabilité et indemnisation.	976
3.2.6	Droit de rectification et divulgation.	977
3.2.7	Confidentialité bilatérale.	977
4.	Tiers et risque pénal étendu	978
4.1	Les prestataires cloud	978
4.2	Les risques de complicité et la responsabilité du client	978
5.	Données personnelles, RGPD et responsabilité accrue	979
5.1	Obligation de sécurité du responsable du traitement	979
5.2	Notification des violations.	979
5.3	Sanctions administratives (CNIL) et sanctions pénales.	980
6.	Architecture contractuelle avancée	980
6.1	Les clauses de sécurité partagée en environnement cloud	980
6.2	La problématique de la responsabilité solidaire et de la chaîne de contrats	981
6.3	L'assurance responsabilité civile professionnelle.	981
6.4	La limitation de portée temporelle et géographique.	982
7.	Nouveaux régimes de protection	982
7.1	Le statut de lanceur d'alerte	982
7.2	Les canaux de signalement protégés	983
7.3	La procédure ANSSI	983
8.	Bug bounty.	984
8.1	Plateforme et tiers de confiance.	984
8.2	Autoentrepreneur bug bounty.	984
8.3	Responsabilité civile et garantie de l'entreprise	985

24 ————— Sécurité informatique

Ethical Hacking : Apprendre l'attaque pour mieux se défendre

9. Gestion de crise post-découverte	985
9.1 La notification en cascade.	985
9.2 L'implication du pentesteur dans la procédure	986
9.3 La divulgation coordonnée de vulnérabilité	986
10. Pièges pénaux liés aux données personnelles	987
10.1 La collecte illicite de données personnelles	987
10.2 La divulgation non autorisée de données personnelles.	987
10.3 Le statut du pentesteur sous le RGPD.	988
10.4 L'obligation de destruction des données	988
11. Preuve numérique	989
11.1 La chaîne de preuve.	989
11.2 Les standards techniques	989
11.3 Les droits du pentesteur lors d'une perquisition	990
11.4 Documenter le pentest pour la justice.	990
12. Responsabilité étendue	991
12.1 Responsabilité directe envers les personnes concernées.	991
12.2 Responsabilité solidaire avec le client	991
12.3 Responsabilité envers les prestataires tiers	992
12.4 Cas spécifique du cabinet intermédiaire	992
13. Nouvelles réglementations	992
13.1 La Directive NIS 2.	993
13.2 DORA	993
13.3 Le Cyber Resilience Act (CRA)	994
14. Qualification PASSI.	994
14.1 Qu'est-ce que la qualification PASSI ?	994
14.2 Avantages et responsabilité accrue	994
14.3 Le chemin vers PASSI	995
15. Checklist de conformité 2026	995
15.1 Avant le pentest	995
15.2 Pendant le pentest.	996
15.3 Après le pentest.	997
16. Conclusion et perspective 2026	997

Les éléments à télécharger sont disponibles à l'adresse suivante :

<http://www.editions-eni.fr>

Saisissez la référence de l'ouvrage **EP5MAL** 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	17
1.1 Introduction	17
1.2 Backdoor	18
1.3 Ransomware et locker	19
1.4 Stealer	20
1.5 Miner	21
1.6 Banking trojan	21
1.7 Rootkit	21
2. Scénario d'infection	23
2.1 Introduction	23
2.2 Scénario 1 : exécution d'une pièce jointe	23
2.3 Scénario 2 : clic malencontreux	24
2.4 Scénario 3 : ouverture d'un document infecté	25
2.5 Scénario 4 : attaques informatiques	25
2.6 Scénario 5 : attaques physiques - infection par clé USB	26
2.7 Scénario 6 : attaques de type supply chain	26
3. Techniques de communication avec le C&C	27
3.1 Introduction	27
3.2 Mise à jour de la liste des noms de domaine	27
3.3 Communication via HTTP/HTTPS/FTP/IRC	28
3.4 Communication via un client e-mail	28
3.5 Communication via un réseau point à point	29

2 _____ Cybersécurité et Malwares

Détection, analyse et Threat Intelligence

3.6	Communication via des protocoles propriétaires.	29
3.7	Communication via le protocole DNS	29
3.8	Communication passive.	30
3.9	Fast flux et DGA (Domain Generation Algorithms)	30
3.10	Communication via un ORB.	31
3.11	Cibles sans accès internet.	32
4.	Mode opératoire en cas d'attaques ciblées persistantes (APT)	32
4.1	Introduction	32
4.2	Phase 1 : reconnaissance.	33
4.3	Phase 2 : intrusion	33
4.4	Phase 3 : persistance	34
4.5	Phase 4 : pivot.	34
4.6	Phase 5 : exfiltration.	35
4.7	Traces laissées par l'attaquant	35
5.	Ressources sur Internet concernant les malwares	36
5.1	Introduction	36
5.2	Sites permettant des analyses en ligne	36
5.3	Sites présentant des analyses techniques	38
5.4	Sites permettant de télécharger des échantillons de malwares.	40
5.5	Encyclopédie Malpedia.	41
6.	Résumé	42

Chapitre 2

Malwares ciblant les systèmes Microsoft Windows

1.	Introduction	43
2.	Collecte d'informations	44
2.1	Introduction	44
2.2	Collecte et analyse de la base de registre.	44
2.3	Collecte et analyse des journaux d'événements	46
2.4	Collecte et analyse des fichiers exécutés au démarrage	47
2.5	Collecte et analyse du système de fichiers	49

2.6	Gestion des fichiers bloqués par le système d'exploitation	55
2.7	Outil DFIR ORC	56
3.	Image mémoire	57
3.1	Présentation	57
3.2	Réalisation d'une image mémoire	58
3.3	Analyse d'une image mémoire	61
3.4	Analyse de l'image mémoire d'un processus	68
3.5	Utilisation de Volweb	69
4.	Fonctionnalités des malwares	82
4.1	Techniques pour rester persistant	82
4.2	Techniques pour se cacher	83
4.3	Malware sans fichier	88
4.4	Contournement de l'UAC	88
5.	Création d'un laboratoire d'analyse	89
5.1	Introduction	89
5.2	VirtualBox	90
5.3	Machines virtuelles préconfigurées	96
5.4	Viper : l'outil de gestion d'échantillons de malwares	96
6.	Analyse du vecteur d'infection	104
6.1	Informations sur un fichier	104
6.1.1	Format d'un fichier	104
6.1.2	Chaînes de caractères présentes dans un fichier	105
6.2	Analyse dans le cas d'un fichier PDF	107
6.2.1	Introduction	107
6.2.2	Extraire le code JavaScript	108
6.2.3	Désobfusquer du code JavaScript	112
6.2.4	Conclusion	116
6.3	Analyse dans le cas d'un fichier Adobe Flash	116
6.3.1	Introduction	116
6.3.2	Extraire et analyser le code ActionScript	116

4 **Cybersécurité et Malwares**

Détection, analyse et Threat Intelligence

6.4	Analyse dans le cas d'un fichier JAR	117
6.4.1	Introduction	117
6.4.2	Récupération du code source depuis les classes	119
6.5	Analyse dans le cas d'un fichier Microsoft Office	120
6.5.1	Introduction	120
6.5.2	Outils permettant l'analyse de fichiers Office	120
6.5.3	Cas d'un malware utilisant des macros : Dridex	121
6.5.4	Cas d'un malware utilisant une vulnérabilité	123
6.6	Utilisation de PowerShell	125
7.	Analyse dans le cas d'un binaire	126
7.1	Analyse de binaires développés en AutoIt	126
7.2	Analyse de binaires développés avec le framework .NET	128
7.3	Analyse de scripts Python compilés	129
7.4	Analyse de binaires développés en C ou C++	130
7.5	Analyse rapide des fonctionnalités d'un binaire	130
7.6	Analyse de bootkits UEFI	132
8.	Format PE	133
8.1	Introduction	133
8.2	Schéma du format PE	133
8.2.1	En-tête MZ-DOS	134
8.2.2	Segment DOS	134
8.2.3	En-tête PE	135
8.2.4	Table des sections	138
8.2.5	Table des imports	139
8.2.6	Table des exports	140
8.2.7	Ressources	141
8.3	Outils pour analyser un PE	141
8.4	API d'analyse d'un PE	144
9.	Suivre l'exécution d'un binaire	148
9.1	Introduction	148
9.2	Activité au niveau de la base de registre	148
9.3	Activité au niveau du système de fichiers	151

9.4	Activité réseau	151
9.5	Activité réseau de type HTTP(S)	160
10.	Utilisation de Cuckoo Sandbox	161
10.1	Introduction	161
10.2	Configuration	161
10.3	Utilisation	163
10.4	Limitations	170
10.5	Conclusion	172
11.	Résumé	172

Chapitre 3 Reverse engineering

1.	Introduction	173
1.1	Présentation	173
1.2	Législation	174
2.	Qu'est-ce qu'un processus Windows ?	175
2.1	Introduction	175
2.2	Process Environment Block	175
2.3	Thread Environment Block	177
3.	Assembleur x86	178
3.1	Registres	178
3.2	Instructions et opérations	183
3.3	Gestion de la mémoire par la pile	190
3.4	Gestion de la mémoire par le tas	193
3.5	Optimisation du compilateur	193
4.	Assembleur x64	195
4.1	Registres	195
4.2	Paramètres des fonctions	195
5.	Analyse statique	196
5.1	Présentation	196
5.2	Ghidra	196

6 **Cybersécurité et Malwares**

Détection, analyse et Threat Intelligence

5.3	Navigation	197
5.3.1	Renommages et commentaires	207
5.3.2	Extensions	209
5.3.3	Ghidra et CAPA	211
5.4	Rizin	216
5.4.1	Présentation	216
5.4.2	Ligne de commande	216
5.4.3	Interface graphique : Cutter	218
5.5	Techniques d'analyse	222
5.5.1	Commencer une analyse	222
5.5.2	Sauts conditionnels	224
5.5.3	Boucles	225
5.6	API Windows	226
5.6.1	Introduction	226
5.6.2	API d'accès aux fichiers	227
5.6.3	API d'accès à la base de registre	230
5.6.4	API de communication réseau	236
5.6.5	API de gestion des services	241
5.6.6	API des objets COM	243
5.6.7	API restart manager	244
5.6.8	Exemples de l'utilisation de l'API	246
5.6.9	Conclusion	254
5.7	Comparaison entre binaires	255
5.7.1	Description	255
5.7.2	Outils	255
5.7.3	Exemple	256
5.8	MCRIT	262
5.8.1	Présentation	262
5.8.2	Installation	263
5.8.3	Utilisation	265
5.8.4	Principe de comparaison	280
5.9	Limites de l'analyse statique	282

6. Analyse dynamique	282
6.1 Présentation	282
6.2 x64dbg	283
6.2.1 Présentation	283
6.2.2 Contrôle de flux d'exécution	287
6.2.3 Points d'arrêt	291
6.2.4 Visualisation des valeurs en mémoire	294
6.2.5 Copie de la mémoire	295
6.3 WinDbg	296
6.3.1 Présentation	296
6.3.2 Interface	297
6.3.3 Commandes de base	299
6.3.4 Plug-in	304
6.4 Analyse du noyau Windows	305
6.4.1 Présentation	305
6.4.2 Mise en place de l'environnement	305
6.4.3 Protections du noyau Windows	306
6.5 Émulation et instrumentation	307
6.6 Limites de l'analyse dynamique et conclusion	308

Chapitre 4

Techniques d'obfuscation

1. Introduction	309
2. Obfuscation des chaînes de caractères	311
2.1 Introduction	311
2.2 Utilisation de ROT13	311
2.3 Utilisation de la fonction XOR avec une clé statique	315
2.4 Utilisation de la fonction XOR avec une clé dynamique	320
2.5 Utilisation de fonctions cryptographiques	323
2.6 Utilisation de fonctions personnalisées	330
2.7 Outils permettant de décoder les chaînes de caractères	339
2.8 Utilisation de Cyberchef	340

8 _____ Cybersécurité et Malwares

Détection, analyse et Threat Intelligence

2.9	Utilisation de Malduck.	344
3.	Obfuscation de l'utilisation de l'API Windows.	345
3.1	Introduction	345
3.2	Étude du cas Duqu	347
3.3	Étude du cas EvilBunny	351
4.	Packers.	353
4.1	Introduction	353
4.2	Packers utilisant la pile.	355
4.3	Packers utilisant le tas	367
4.4	Encodeur Metasploit	374
4.5	Outils pour automatiser l'unpack	376
5.	Autres techniques.	377
5.1	Anti-VM	377
5.2	Anti-reverse engineering et anti-débogage	379
6.	Résumé	383

Chapitre 5

Malwares ciblant les systèmes macOS

1.	Introduction	385
2.	Système d'exploitation macOS	386
2.1	Historique	386
2.2	Architecture	387
2.3	Systèmes de fichiers	389
2.4	Mécanisme de sécurité	392
2.5	Application macOS	397
2.6	Format de fichier Mach-O	400
3.	Création d'un laboratoire d'analyse.	403
3.1	Contraintes matérielles	403
3.2	Configuration de VirtualBox.	404

4. Analyse d'un binaire Mach-O	408
4.1 Analyse statique avec Ghidra.	408
4.2 Langage C et C++	409
4.3 Langage Swift	410
4.4 Langage Objective-C.	413
4.5 Analyse dynamique avec LLDB.	416
4.6 Outils d'analyse Objective-See.	420
5. Cas d'étude CloudMensis.	427
5.1 Introduction	427
5.2 Persistance.	427
5.3 Configuration du malware.	431
5.4 Communication avec les serveurs de contrôle	432
5.5 Fonctionnalités	433
5.6 Contournement de TCC et SIP.	434
6. Résumé	437

Chapitre 6

Malwares ciblant les systèmes Linux

1. Introduction	439
2. Système d'exploitation Linux	440
2.1 Historique	440
2.2 Architecture	441
2.2.1 Spécificité des distributions Linux	441
2.2.2 Système de fichiers	442
2.2.3 Espace kernel et utilisateur	444
2.2.4 Services et systemd.	448
2.2.5 Processus sous Linux	450
2.2.6 Système de boot : LILO et GRUB	452
2.2.7 Cas des conteneurs Linux	452

10 _____ Cybersécurité et Malwares

Détection, analyse et Threat Intelligence

2.3	Mécanismes de sécurité	452
2.3.1	Gestions des utilisateurs	452
2.3.2	Étanchéité des processus	454
2.3.3	SELinux	454
2.3.4	Netfilter et iptables	455
2.3.5	Faiblesses comparées aux autres systèmes d'exploitation	456
3.	Vecteurs d'infection	457
3.1	Cas d'une compromission système	457
3.2	Cas d'une compromission web	457
4.	Format ELF	458
5.	Techniques utilisées par les malwares Linux	462
5.1	Persistance	462
5.2	Daemon Linux	463
5.3	LD_PRELOAD	465
5.4	Injection de bibliothèques	467
6.	Analyse de malware	469
6.1	Création du laboratoire d'analyse	469
6.2	Analyse statique	470
6.3	Analyse dynamique	471
6.3.1	Utilisation de strace	471
6.3.2	Utilisation de ltrace	473
6.3.3	Utilisation de gdb	476
7.	Cas d'étude d'un webshell	480
8.	Cas d'étude du malware Sysupdate	482
9.	Cas d'étude d'attaque de XZ Utils	486
10.	Résumé	487

Chapitre 7

Malwares ciblant les systèmes Android

1. Introduction	489
2. Système d'exploitation Android	490
2.1 Historique	490
2.2 Architecture	491
2.3 Partitions et systèmes de fichiers	495
2.4 Sécurité	499
2.4.1 Sécurité au niveau système	499
2.4.2 Sécurité au niveau Dalvik/ART	501
2.4.3 Effet de bord des fonctionnalités de sécurité	503
2.5 Application Android	503
2.6 Malwares ciblant les téléphones Android	508
3. Vecteurs d'infection	510
3.1 Installation via Google Store	510
3.2 Installation via des stores alternatifs	511
3.3 Installation manuelle	511
3.4 MDM (Mobile Device Management)	512
3.5 Accès physique au terminal	512
4. Création d'un laboratoire d'analyse	513
4.1 Machine virtuelle ou téléphone physique ?	513
4.2 ADB (Android Debug Bridge)	517
4.3 Accès administrateur (root)	519
4.4 Capture réseau	523
4.4.1 Capture réseau pure	523
4.4.2 Capture HTTP/HTTPS	523
5. Analyse statique et décompilation d'une application	526
5.1 Analyse d'un fichier APK	526
5.2 Code Java et décompilation : Bytecode Viewer	529
5.3 Anti-VM	532
5.4 Code natif	534
5.5 Techniques d'obfuscation	537

12 _____ Cybersécurité et Malwares

Détection, analyse et Threat Intelligence

6. Analyse dynamique	541
6.1 Utilisation de Frida	541
6.2 Utilisation de gdb pour les binaires natifs	543
7. Résumé	544

Chapitre 8

Malwares ciblant les systèmes iOS

1. Introduction	545
2. Système d'exploitation iOS	546
2.1 Historique	546
2.2 Architecture	546
2.3 Partitions et systèmes de fichiers	550
2.4 Sécurité	551
2.5 Jailbreak	553
2.6 Application iOS	554
2.7 Malwares ciblant iOS	557
3. Vecteurs d'infection	558
3.1 Accès physique au terminal	558
3.2 Liens vers un fichier .ipa	558
3.3 Stores alternatifs	558
3.4 MDM malveillant	559
4. Création d'un laboratoire d'analyse	559
4.1 Analyse réseau	559
4.2 Jailbreak d'un terminal et déploiement d'une application	560
5. Analyse statique d'une application	563
5.1 Introduction	563
5.2 Analyse avec Ghidra	563
6. Analyse dynamique	571
6.1 Utilisation de Frida	571
6.2 Utilisation de lldb	573

7. Technique utilisée par les malwares sous iOS	574
7.1 Injection de bibliothèques	574
7.2 Injection de JavaScript	576
7.3 Keylogger sous iOS	577
7.4 Terminal jailbreaké et injection de code	577
8. Résumé	578

Chapitre 9

Analyse de malwares et Threat Intelligence

1. Introduction	579
2. Indicateurs de compromission (IOC)	581
2.1 Empreintes et signatures de fichiers	581
2.1.1 Empreintes cryptographiques	581
2.1.2 Empreintes par similarité : ssdeep et TLSH	583
2.1.3 Empreintes des tables d'imports des exécutables Windows	587
2.2 Indicateurs système	590
2.2.1 Clés de registre	591
2.2.2 Système de fichiers	596
2.2.3 Réseau	597
2.2.4 Exécutions	598
3. Matrice du MITRE, TTPs et Threat Actors	599
3.1 Matrice du MITRE	599
3.1.1 Présentation	599
3.1.2 Exemples d'utilisation de la matrice ATT&CK	602
3.2 TTP et Threat Actors	604
3.2.1 Définition	604
3.2.2 TTP de TA505	605
3.2.3 Threat Actor et Intrusion Set	606

14_____Cybersécurité et Malwares

Détection, analyse et Threat Intelligence

4. Règles et détections	607
4.1 Introduction	607
4.2 Suricata	607
4.2.1 Suricata	607
4.2.2 Exemple de détection	609
4.3 YARA	612
4.3.1 Présentation	612
4.3.2 Syntaxe	612
4.3.3 Exemple de détection de webshells	614
4.3.4 Exemple de détection de Chinoxy via le module PE ...	614
4.3.5 Python et YARA	620
4.3.6 Outils open source utilisant YARA	621
5. Sources de données	622
5.1 Présentation	622
5.2 Scanners	623
5.2.1 Définition	623
5.2.2 Shodan.io	624
5.2.3 Onyphe.io	628
5.2.4 Censys.io	632
5.3 Passives DNS	636
5.3.1 Présentation	636
5.3.2 Passive DNS de VirusTotal	636
5.4 Dépôts de malwares	638
5.4.1 Présentation	638
5.4.2 VirusTotal	639
5.4.3 MalwareBazaar	641
5.5 Sources multi-indicateurs	647
5.5.1 Présentation	647
5.5.2 OTX AlienVault	647
5.5.3 RiskIQ	651

6. Plateformes de Threat Intelligence	655
6.1 Introduction	655
6.2 MISP	655
6.2.1 Généralités	655
6.2.2 Fonctionnalités	656
6.3 Yeti	662
6.3.1 Présentation	662
6.3.2 Concepts	662
6.3.3 Exemple d'utilisation	663
6.3.4 Conclusion	675
7. Résumé	675
 Index	 677