COLLECTION INFORMATIQUE

Sécurité informatique

concepts et outils

Ameur Salem Zaidoun

ISTE editions

Sécurité informatique

First published 2023 in Great Britain by ISTE Editions Ltd.

ISTE Editions Ltd
27-37 St George's Road
London SW19 4EU
UK

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN: 978-1-78405-907-1 (print)
ISBN: 978-1-78406-907-0 (e-book)

Printed and bound in Great Britain by CPI Group (UK) Ltd., Croydon, Surrey CR0 4YY, March 2023

Sécurité informatique

concepts et outils

Ameur Salem Zaidoun

iSTE editions

Collection dirigée par Jean-Charles Pomerol

À la mémoire de mes parents
À ma femme
À mes fils Mohamed Bairam et Iyed et à ma fille Elaa
À tous les partisans de la paix et la liberté du monde

Table des matières

Introduction 1

Chapitre 1. Mise en évidence de la sécurité 5

1.1. Introduction 5
1.2. Raisons d'être de la sécurité 6
1.2.1. Raisons techniques 6
1.2.2. Raisons sociales 8
1.3. Attaques de sécurité 9
1.3.1. Classification passive/active des attaques 10
1.3.2. Classification directe/indirecte des attaques 12
1.3.3. Exemples d'attaques 14
1.3.4. Quelques statistiques 16
1.4. Objectifs de la sécurité 17
1.4.1. Mise en place d'une culture 18
1.4.2. Mise en place des solutions techniques 18
1.5. Domaines de la sécurité 18
1.5.1. Sécurité énergétique 19
1.5.2. Sécurité organisationnelle et physique 19
1.5.3. Sécurité logique 21
1.6. Normalisation de la sécurité 23
1.6.1. Problématique et présentation générale 23
1.6.2. Norme ISO 7498-2 23

1.7. Services de sécurité 29
1.7.1. Authentification 30
1.7.2. Confidentialité 31
1.7.3. Intégrité 32
1.7.4. Non-répudiation 32
1.7.5. Traçabilité et contrôle d'accès 32
1.7.6. Disponibilité de service 32
1.8. Mécanismes de sécurité 32
1.8.1. Chiffrement. 33
1.8.2. Contrôle d'intégrité. 34
1.8.3. Contrôle d'accès 34
1.8.4. Signature numérique 35
1.8.5. Notarisation 35
1.9. Bonnes pratiques. 35
1.10. Conclusion. 36

Chapitre 2. Failles de sécurité. 39

2.1. Introduction 39
2.2. Failles au niveau de TCP/IP. 40
2.2.1. Arpanet, ancêtre d'Internet 40
2.2.2. Internet et problèmes de sécurité 40
2.2.3. Internet et facilité d'analyse 41
2.3. Failles dues aux *malwares* et outils d'intrusions 42
2.3.1. Virus 43
2.3.2. Ver (*worm*) 46
2.3.3. Spam 47
2.3.4. Bombe logique 48
2.3.5. Cheval de Troie 48
2.3.6. Espiogiciel (*spyware*) 50
2.3.7. *Keylogger* 51
2.3.8. *Adware* 51
2.3.9. Autres *malwares* 52
2.3.10. Comparaison entre quelques outils d'intrusion. 52
2.4. Conclusion 53

Chapitre 3. Techniques et outils d'authentification 55

3.1. Introduction 55
3.2. Concepts théoriques de l'authentification 56
3.2.1. Identification 56
3.2.2. Authentification 57
3.3. Différents types d'authentification 57
3.3.1. Authentification à un service local 57
3.3.2. Authentification à travers le réseau 58
3.4. Service AAA 62
3.4.1. AAA en local 63
3.4.2. AAA sur serveur 65
3.5. Conclusion 70

Chapitre 4. Techniques de contrôle d'accès, ACL et *firewall* . . 71

4.1. Introduction 71
4.2. Liste de contrôle d'accès 72
4.2.1. Classifications des ACL 72
4.2.2. Configuration des ACL sous Cisco 74
4.2.3. Configuration des ACL sous Huawei 80
4.3. *Firewall* 85
4.3.1. Fonctionnalité de filtrage 86
4.3.2. Fonctionnalités de traçage et NAT 88
4.3.3. Architecture d'un *firewall*. 89
4.3.4. Fonctionnement d'un *firewall* 91
4.3.5. Classifications des *firewalls* 92
4.3.6. *Firewall* à états 94
4.3.7. *Firewall* basé sur les zones 95
4.3.8. Exemples de *firewall*. 98
4.4. Notion de DMZ 100
4.4.1. Définition et utilité 100
4.4.2. Topologies de mise en œuvre 101
4.5. Conclusion 104

Chapitre 5. Techniques et outils de détection d'intrusions . . . 105

5.1. Introduction . . . 105
5.2. Antivirus . . . 105
5.2.1. Fonctionnalités d'un antivirus . . . 106
5.2.2. Méthodes de détection de virus . . . 106
5.2.3. Manipulations possibles pour un antivirus . . . 107
5.2.4. Composants d'un antivirus . . . 107
5.2.5. Comparaison entre antivirus et *firewall* . . . 108
5.3. Systèmes de détection d'intrusions . . . 109
5.3.1. Fonctionnalités d'un IDS . . . 109
5.3.2. Composants et fonctionnement d'un IDS . . . 109
5.3.3. Classifications des IDS . . . 111
5.3.4. Exemples d'IDS/IPS . . . 114
5.4. Conclusion . . . 115

Chapitre 6. Techniques et outils de chiffrement, IPSec et VPN . . . 117

6.1. Introduction . . . 117
6.2. Techniques de chiffrement . . . 118
6.2.1. Principes de base du chiffrement . . . 119
6.2.2. Cryptanalyse . . . 120
6.2.3. Évolution de la cryptographie . . . 121
6.2.4. Notion de certificat . . . 126
6.2.5. Comparaison entre les techniques de chiffrement . . . 127
6.3. IPSec . . . 128
6.3.1. AH . . . 128
6.3.2. ESP . . . 129
6.3.3. Différents modes IPSec . . . 129
6.3.4. Différentes implémentations de l'IPSec . . . 130
6.3.5. Différentes encapsulations IPSec . . . 131
6.3.6. Protocole IKE . . . 134
6.4. VPN . . . 135
6.4.1. Problématique et raisons d'être . . . 135
6.4.2. Principe du VPN . . . 135
6.4.3. Différents types de VPN . . . 136

6.4.4. Différents protocoles de tunnelisation 137
6.4.5. Configuration VPN IPSec *Site-to-Site* 137
6.5. Conclusion 140

Chapitre 7. Nouvelles tendances de sécurité pour SDN et IoT 143

7.1. Introduction 143
7.2. Sécurité du réseau SDN 144
7.2.1. Description générale du réseau SDN 144
7.2.2. Architecture du réseau SDN 145
7.2.3. Composants du réseau SDN 146
7.2.4. Problématiques de sécurité d'un réseau SDN 148
7.2.5. Solutions de sécurité d'un réseau SDN 149
7.3. Sécurité IoT/IoE 152
7.3.1. Réseaux de capteurs 152
7.3.2. Problématique de sécurité en IoT 153
7.3.3. *Blockchain*, solution de sécurité pour IoT 156
7.4. Conclusion 157

Chapitre 8. Management de la sécurité 159

8.1. Introduction 159
8.2. Audit sécurité 160
8.2.1. Objectifs 160
8.2.2. Diagramme d'action d'audit 161
8.2.3. Audit organisationnel et physique 162
8.2.4. Audit technique 163
8.2.5. Test intrusif 165
8.2.6. Méthodologies d'audit 165
8.3. Mise en évidence d'une politique de sécurité 167
8.3.1. Test et évaluation de sécurité 167
8.3.2. Développement d'une politique de sécurité 172
8.3.3. Composants d'une politique de sécurité 174
8.4. Normes, directives et procédures 175

8.4.1. Norme ISO 27000 176
8.4.2. Norme ISO/FDIS 31000 176
8.4.3. Norme ISO/IEC 38500 177
8.5. Conclusion 177

Liste des acronymes 179

Bibliographie 181

Index 183

Introduction

Depuis l'Antiquité, l'Homme cherche à se sécuriser, il confère à ce besoin une importance capitale. Une importance qui se justifie par la volonté de se protéger contre les facteurs externes.

Avec l'apparition de l'informatique et sa pleine expansion, le problème de sécurité s'impose, c'est un nouveau problème multiaxes qui touche à l'ensemble des activités, des intervenants, des équipements qui concernent le domaine de l'informatique.

La sécurité admet plusieurs axes :

– le premier axe concerne l'aspect énergétique, il consiste à assurer et maintenir l'énergie nécessaire pour le bon fonctionnement du système informatique ;

– le deuxième axe s'intéresse à l'aspect physique, il consiste à sécuriser physiquement les locaux et l'infrastructure matérielle du système informatique, en l'occurrence les systèmes de communication câblés et sans fil, les équipements intermédiaires d'interconnexion, de transmission et de sécurité (répéteurs, concentrateurs, commutateurs, routeurs, *firewalls*, etc.), des équipements terminaux de traitement aussi bien des stations de travail que des serveurs. La sécurité physique permet de sécuriser le système informatique contre les facteurs naturels tels que l'inondation, l'incendie, etc. et humains tels que le vol ;

– le troisième axe est un aspect propre à la sécurité informatique contrairement aux deux premiers qui s'appliquent dans n'importe quel domaine industriel nécessitant de l'énergie et admettant un patrimoine matériel critique. Cet axe a pour objectif de résoudre les problèmes spécifiques de la sécurité relatifs à la

technologie de l'informatique afin d'assurer un accès sûr et d'interdire l'accès non autorisé d'une part et de protéger le patrimoine logiciel et les données, contre toute utilisation non autorisée, d'autre part.

Bien qu'il n'existe pas une solution radicale de sécurité toute prête à appliquer, les solutions de sécurité ne cessent de se développer mais restent toujours insuffisantes pour résoudre les problèmes de sécurité. Nous assistons à une bataille continue entre les responsables de sécurité d'une part et les attaquants, les pirates et les intrus d'autre part.

Cette bataille se manifeste par les groupes de travail de chacune des deux parties, c'est le cas du groupe Anonymous et des organismes internationaux qui s'intéressent à la sécurité.

Les attaquants ne cessent de chercher et d'identifier les failles, concevoir les moyens d'attaques appropriés qui exploitent les vulnérabilités en question et surmonter les contre-mesures qui peuvent éventuellement être déployées.

Ce défi nécessite de l'autre côté un investissement qui permet de mobiliser des moyens humains et matériels pour faire face aux attaques et aux actions malveillantes diversifiées qui menacent la sécurité d'un système informatique. Divers moyens organisationnels, intellectuels, matériels et logiciels de sécurité ont vu le jour et ne cessent de se développer en quantité et en qualité dans les dernières années.

La sécurité, bien qu'elle soit négligée par ignorance dans la majorité des cas, constitue un défi très important. Lever ce défi n'est pas une tâche simple faute d'absence de solution radicale ou d'une feuille de route claire et exacte à appliquer. La seule façon de garantir un minimum de sécurité, c'est à travers l'alliance de plusieurs mesures sociales, culturelles et techniques. Cependant, ces mesures de sécurité restent dynamiques et dépendantes des circonstances, on assiste à la nécessité d'une veille technologique qui permet d'effectuer perpétuellement les modifications et les correctifs nécessaires sur la politique de sécurité en vigueur.

L'intervention d'experts et de personnes externes représente une action de valeur et un facteur d'importance capitale pour la définition et l'évolution de la politique de sécurité. Cette intervention peut se matérialiser par les missions

d'audit sécurité qui s'effectuent au niveau de l'entreprise ou par l'intervention directe d'experts lors d'actions de *consulting* pour les PME/PMI.

Plusieurs recommandations d'ordre général doivent être appliquées afin de garantir le minimum nécessaire en matière de sécurité.

D'abord, le service ou la cellule de sécurité doit forcément figurer au niveau de l'organigramme de l'entreprise tout en allouant au responsable de ce service ou de cette cellule, qui doit posséder un minimum de culture en matière de sécurité, le pouvoir et les facilités logistiques d'intervention nécessaires.

De plus, miser sur l'ignorance des agents et des utilisateurs n'a jamais été une mesure de sécurité. Il fallait instaurer une culture en matière de sécurité à travers des cycles de formations bien étudiés qui touchent à l'ensemble du personnel (cadres et agents) d'une part et prévoir des chartes et des affiches d'autre part.

Finalement, il fallait appliquer les mesures techniques de sécurité nécessaires et qui dépendent du patrimoine informatique de l'entreprise, et ce en déployant les équipements et les logiciels appropriés et en appliquant les mesures de sécurité. Reste à signaler que cette dernière recommandation, bien qu'elle soit incontournable, peut être mise en cause, et voire même sans intérêt, si on néglige pour une raison ou une autre les deux premières recommandations.

Le problème de sécurité n'est pas un souci purement professionnel qui concerne uniquement les entreprises et les institutions, il s'agit d'une question sociale en premier lieu et qui concerne la famille et la société d'une façon générale. En effet, l'utilisation de l'informatique et l'accès à Internet a envahi la société et pose plusieurs défis notamment pour les enfants qui peuvent accéder à n'importe quelle information et être stimulés par les réseaux sociaux avec l'incapacité des parents pour les contrôler. Pour lever ce défi qui présente une gravité non négligeable, deux mesures de base sont nécessaires, culturelle et technique, à travers des tâches de sensibilisation en famille, à l'école, dans les médias en plus du déploiement des logiciels appropriés de contrôle parental.

Cet ouvrage s'intéresse à plusieurs sujets en relation avec la sécurité :

1) la mise en évidence du sujet de la sécurité en identifiant la problématique, en précisant l'importance, les services et les mécanismes ;

2) l'identification des failles et problèmes de sécurité, et ce qu'ils soient d'ordres culturels et humains aussi bien que matériels et techniques ;

3) la mise au point des solutions de sécurité sur le plan technique et organisationnel en l'occurrence les antivirus, les *firewalls*, les IDS et les différentes techniques de contrôle d'accès, d'authentification et de chiffrement ;

4) la sécurité des réseaux SDN et des réseaux de capteurs IoT/IoE qui sera abordée moyennant la spécificité de ces technologies ;

5) le management de la sécurité, en l'occurrence l'audit sécurité et la mise en place de la politique de sécurité.

Chapitre 1

Mise en évidence de la sécurité

1.1. Introduction

L'évolution massive de nos jours dans le domaine de l'informatique et des technologies de communication présente quelques effets de bord, ce sont les problèmes de sécurité.

En effet, l'utilisation des réseaux facilite la communication et par la suite la propagation des outils d'attaques et la coordination entre les pirates. C'est exactement le cas du développement des réseaux routiers et des moyens de transport qui engendre des problèmes liés aux accidents et qui a nécessité un investissement dans le domaine de la sécurité routière.

De plus, l'expertise cumulée en matière de développement des logiciels a été utilisée dans le mauvais sens pour la création des programmes malveillants.

Les attaques en matière de sécurité peuvent être classées de deux façons. Une première classification concerne l'effet de l'attaque : on distingue les attaques passives ou encore les attaques de reconnaissance qui consistent à observer et divulguer l'information par une entité tierce et les attaques actives, appelées aussi attaques d'accès, qui se présentent par des actions malveillantes *via* la mise en cause de l'information, des intervenants ou des canaux de communication. La deuxième classification se rapporte à la façon même d'attaquer : l'attaque directe se définit par l'utilisation de ses propres ressources et de sa propre identité et l'attaque indirecte par l'utilisation de machines intermédiaires.

Plusieurs variantes d'attaques ne cessent d'apparaître périodiquement. D'ailleurs, les statistiques ont montré le volume du danger qui menace les systèmes informatiques et les dégâts matériels qui en résultent. Ce qui confère, sans aucun doute, à la sécurité une importance capitale et en fait un besoin indispensable.

Face aux problèmes déjà recensés, l'investissement en matière de la sécurité s'impose dans l'objectif d'instaurer une culture d'une part et de mettre en place des solutions techniques d'autre part. Elle vise principalement l'utilisateur de l'outil informatique indépendamment de son degré d'utilisation et de sa culture à travers des cours, des formations, des forums, des chartes et des annonces. De plus, elle s'intéresse au système informatique lui-même en mettant en place des mesures et des solutions techniques.

La sécurité d'un système informatique concerne plusieurs aspects à commencer par le maintien de l'énergie, en passant par le contrôle physique et en terminant par la gestion d'accès et des mesures de sécurité logicielles, qui concerne de près l'information et les entités qui la manipulent.

Ce dernier aspect, le plus important et dont généralement la sécurité se simplifie, doit satisfaire au moins quatre points pour être considéré comme sécurisé.

1.2. Raisons d'être de la sécurité

La sécurité informatique vient de s'imposer depuis plusieurs années à la suite de l'évolution massive de l'informatique et la socialisation de son utilisation. Les raisons qui ont favorisé l'apparition de la sécurité informatique en tant que sujet d'importance se classe en deux grandes parties, une première d'ordre technique liée aux services et aux technologies en soi et une deuxième d'ordre social liée à l'utilisation massive diversifiée et généralisée des outils informatiques.

1.2.1. *Raisons techniques*

Le développement de l'informatique, malgré ses avantages, était utilisé dans le mauvais sens pour mettre en cause la sécurité. Cette dernière a été négligée au début mais s'est imposée par la suite pour faire face aux problèmes qui viennent d'apparaître ou qui deviennent exploitables par les attaquants.

1.2.1.1. *Développement du génie logiciel*

L'ingénierie des logiciels a connu une évolution importante marquée par l'utilisation de plusieurs langages de programmation et plusieurs techniques de développement qui s'intègrent d'une façon ou d'une autre dans la majorité des progiciels ; on peut citer à titre d'exemple Microsoft Office qui permet à l'utilisateur de développer des macros (à l'origine du virus appelé macrovirus, c'est-à-dire virus à base de macro qui infecte les documents Office).

De plus, les utilisateurs acquièrent de plus en plus d'expertise en matière de programmation. Ce développement massif des moyens logiciels et de l'expertise a été mal utilisé dans certains cas, et ce pour créer des logiciels d'attaques (outils d'analyse, outils de scan) ou injecter des outils d'intrusion (virus, vers, etc.).

De nos jours, les outils d'attaques sont disponibles sur le net, ils sont à la portée des utilisateurs finaux et ne requièrent aucune qualification de leur part pour les exploiter. Ils prennent plusieurs formes (applications web, applications graphiques, etc.). De plus, un utilisateur non averti ne peut pas les distinguer des applications légitimes et il peut par ignorance ou par négligence les déployer en mettant en cause la sécurité de son propre système. Plusieurs mauvaises habitudes facilitent ce problème.

1.2.1.2. *Développement des réseaux*

On assiste à un développement important au niveau des réseaux, ce qui facilite la communication et le transfert de l'information. Cette qualité et ce service peuvent être mal utilisés par les intrus pour attaquer et pour échanger des informations suspectes.

Les failles dues aux réseaux prennent leurs effets de deux facteurs. Le premier est l'utilisation massive des réseaux dans plusieurs domaines, ce qui permet d'interconnecter tout le monde avec toutes leurs divergences. Le deuxième concerne la technologie réseau en soi qui est basée sur TCP/IP, un protocole qui, bien qu'il soit simple et efficace, présente plusieurs failles en mettant à la disposition des utilisateurs finaux une grande panoplie d'outils et de services.

1.2.1.2.1. Utilisation

Actuellement, c'est l'époque de la révolution de l'informatique et des techniques de télécommunication. L'information traverse le globe terrestre de bout à bout en quelques fractions de seconde et ceci grâce à la prolifération des réseaux

dans lesquels Internet joue le rôle le plus important. De ce fait, un ordinateur n'est pas isolé, il communique chaque jour avec des milliers d'ordinateurs et exécute explicitement ou implicitement des milliers de programmes qui peuvent être malveillants pour son fonctionnement. Ce danger est encore renforcé par l'utilisation des amovibles et notamment les disques détachables.

Les réseaux représentent des autoroutes d'informations utilisées par les pirates et les programmes d'attaques aussi bien que pour faciliter la communication. La vie dans une maison isolée est difficile, le fait de lui créer une route facilite la vie aussi bien que l'attaque par les voleurs.

1.2.1.2.2. Uniformité technologique (TCP/IP)

L'apparition et la prolifération d'Internet a favorisé l'utilisation de la famille de protocoles TCP/IP même en local (Intranet). Dans la mesure où les services et les protocoles TCP/IP sont connus par tout le monde, cela qui implique la possibilité de procéder à des attaques qui visent les failles enregistrées au niveau de TCP/IP. On assiste actuellement à une uniformité technologique. Bien qu'elle soit bénéfique pour le développement de l'informatique en général, elle présente une lacune utilisable par les intrus qui peuvent se pencher sur le développement des outils d'attaques spécifiques à TCP/IP et utilisables pour attaquer n'importe quel nœud du réseau.

TCP/IP a vu le jour au sein de la défense américaine (DoD) dans les circonstances de la guerre froide, l'objectif à l'époque était de déployer un système de communication robuste qui pouvait fonctionner même dans des circonstances critiques et même s'il était partiellement détérioré. La solution proposée était un système avec « intelligence aux bornes », ce qui est contradictoire avec le principe de sécurité puisqu'il met à la disposition des utilisateurs finaux une grande panoplie de fonctionnalités. Avec la prolifération d'Internet, le problème de sécurité est devenu de plus en plus prégnant sans aucune solution radicale possible.

1.2.2. *Raisons sociales*

La raison sociale est aussi importante que la raison technique puisque l'on assiste actuellement à l'émergence d'un monde virtuel avec toutes ses caractéristiques en parallèle avec le monde réel. Un nouveau jargon a vu le jour, en l'occurrence la cybercriminalité, la cyberintimidation, etc., des termes qui reflètent

des problèmes et des caractéristiques inhérents au monde virtuel qui se manifestent notamment par les réseaux sociaux.

On parle actuellement de la société d'information marquée par la prolifération de la culture informatique et l'utilisation massive des ordinateurs et des appareils mobiles qui représentent des outils banals accessibles à tout le monde, on assiste à un espace d'objets connectés (IoT et IoE). L'absence de règles de gestion et charte de sécurité au niveau des organisations facilitent la divulgation d'information, on parle de *social engineering*.

1.2.2.1. *Société de l'information*

Avec la prolifération et l'utilisation répandue des ordinateurs et d'Internet, on assiste actuellement à l'apparition d'une société d'information où personne ne peut être à l'extérieur. La société de l'information désigne une société dans laquelle les technologies de l'information jouent un rôle central.

1.2.2.2. Social engineering

Appelée ingénierie sociale, cette technique représente une façon d'extraire des informations confidentielles chez des responsables de sécurité et des administrateurs.

> « Le "social engineering", encore appelé en français "subversion psychologique" est une pratique consistant à abuser de la confiance d'une ou de plusieurs personnes, dans le but principal de récupérer des informations confidentielles. » Magali Jakusic[1]

Cette attaque peut se faire directement sur rencontre ou à travers les réseaux sociaux et les moyens de communication. Les victimes sont généralement les administrateurs des systèmes informatiques.

1.3. Attaques de sécurité

Il existe deux classifications possibles des attaques. La première se base sur la nature même de l'action (passive ou active) et la deuxième se base sur le procédé de l'attaque (directe ou indirecte).

1. Voir : www.securite.teamlog.com.

1.3.1. *Classification passive/active des attaques*

Les attaques qui permettent de mettre en cause la sécurité peuvent être classées en deux types : passives et actives, et ce, selon l'influence et le degré d'implication dans le processus de communication. On parle aussi d'attaques de reconnaissance et d'attaques d'accès.

1.3.1.1. *Attaque passive (attaque de reconnaissance)*

L'attaque passive, appelée aussi attaque de reconnaissance, consiste à observer passivement l'information ou ses caractéristiques qu'elle soit résidente sur une machine ou encore transférée à travers le réseau.

Cette attaque peut être menée à travers une famille de logiciels, ce sont les *sniffers* ou encore les observateurs réseaux ; ces logiciels sont très abondants sur Internet, ils permettent de faire le scan des caractéristiques et des configurations systèmes et réseaux en exploitant diverses failles et vulnérabilités systèmes et réseaux d'une part et d'analyser le trafic et extraire le flux d'information d'autre part.

L'attaque de reconnaissance peut être mise en œuvre à travers un ensemble d'actions élémentaires :

– requête initiale sur la cible ;

– *ping* de balayage du réseau cible ;

– scan de ports des adresses IP actives ;

– scan des failles ;

– exploitation des outils (*sniffers* et *malwares* appropriés).

On peut citer à titre d'exemple les *sniffers* suivants : Wireshark, WinPcap, WebSiteSniffer, SocketSniff, SmartSniff, Packetyzer, PacketViewer, Packet Mon, CommView et IP Sniffer.

On distingue plusieurs cas de figure :

– découverte des intervenants : c'est le fait d'arriver à découvrir les identités des intervenants d'une communication bien déterminée ;

– découverte de la durée d'intermessage : se manifeste par la découverte de la fréquence des messages, ce qui permet de connaître la nature de l'application (interactive, etc.) ;

– découverte de l'information même : c'est la découverte du contenu de l'information communiquée, elle représente l'attaque passive la plus grave.

1.3.1.2. *Attaque active (attaque d'accès)*

L'attaque active, appelée aussi attaque d'accès, consiste à agir sur l'information et/ou sur le processus de communication, elle est par la suite plus grave que l'attaque passive. Elle consiste à modifier les données ou les messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement système et réseau.

Les objectifs principaux relatifs à une attaque d'accès consistent à :

– récupérer les données ;

– gagner l'accès ;

– faire élever les privilèges d'accès.

On distingue différents cas de figure :

– connexion frauduleuse : c'est le fait d'arriver à se connecter à un serveur sans en avoir le droit. Cette attaque permet à celui qui en est l'auteur d'effectuer des manipulations comme s'il était le propriétaire de ce compte. Il peut effacer des documents, changer la configuration, etc. ;

– déni de service : c'est le fait d'empêcher une ou plusieurs entités autorisées à un service d'y accéder, elle consiste à attaquer le serveur et le rendre hors service, ce qui parallélise tout accès. Ce type d'attaque est connu sous le nom de DoS (*Denial of Service*). On parle aussi du DDoS (*Distributed DoS*), c'est un cas d'attaque qui se produit lorsqu'une machine principale arrive à prendre le contrôle de plusieurs machines et à les orienter pour attaquer la victime et la mettre hors service ;

– altération de messages : consiste à modifier l'ordre des messages en en capturant quelques-uns avant d'en réinjecter de nouveaux plus tard ;

– arrêt/retard de communication : se manifeste lorsqu'un pirate arrive à arrêter une connexion ou encore retarder l'accès et la transmission des messages ;

– modification/divulgation du contenu de message : c'est l'action la plus grave, elle consiste à modifier ou à diffuser le contenu des messages transférés ;

– *port redirection* : consiste à rediriger le trafic d'une façon générale ou rediriger une réponse, une action, une commande vers une machine tierce non autorisée ;

– *Man-in-the-Middle* : c'est une attaque permettant à une partie tierce de s'intercaler entre deux entités en communication sans que ces dernières arrivent à s'en rendre compte ;

– *Buffer Overflow* : cette attaque consiste à exploiter le dépassement mémoire, possible dans un langage faiblement typé tel que le langage C, pour arriver à placer un code bien choisi au sein de la mémoire et créer une faille système ou réseau ;

– IP, MAC, DHCP *Spoofing* : cette attaque permet d'exploiter l'identité d'une machine autorisée (adresse IP, MAC) pour attaquer ou rediriger les données ;

– perte de données : représente l'action la plus coûteuse vu que les données une fois perdues nécessitent un effort énorme de récupération et une remise à niveau qui n'est pas efficace dans la majorité des cas pouvant engendrer des répercutions financières très graves pour l'entreprise. Les axes et les vecteurs qui facilitent la perte de données sont :

- l'accès email/webmail non sécurisé ;
- périphériques non contrôlés ;
- les clouds de stockage ;
- les médias amovibles ;
- le contrôle d'accès inapproprié et non conforme à l'exigence minimale de sécurité.

1.3.2. *Classification directe/indirecte des attaques*

Sur Internet, une attaque peut viser directement la victime avec ses propres ressources et sa propre identité ou se cacher derrière un intermédiaire avec une utilisation éventuelle de son identité et/ou de ses ressources.

1.3.2.1. *Attaque directe*

C'est l'attaque la plus simple mais aussi la plus facile à détecter. Elle consiste à lancer une requête d'attaque sur une victime avec sa propre identité (adresse IP, adresse MAC) et en utilisant ses propres ressources (mémoire, CPU et disque) comme l'illustre la figure 1.1. Elle est devenue de plus en plus rare et les pirates les plus dangereux cherchent à se cacher et enrichir leurs capacités puisque les utilisateurs ont développé des moyens de détection des connexions d'attaque lancées directement.

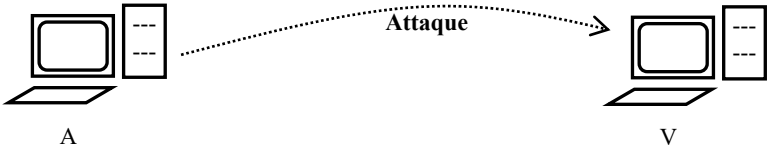

Figure 1.1. *Attaque directe*

1.3.2.2. *Attaque indirecte*

C'est l'attaque la plus complexe et la plus difficile à tracer, il en existe deux types :

– le premier est par rebond, le rebond est une machine intermédiaire qu'on utilise sous son identité et/ou ses ressources pour attaquer ;

– le deuxième est par réponse, il exploite un serveur comme machine intermédiaire pour attaquer une machine tierce.

1.3.2.2.1. Par rebond

Le pirate essaye de prendre le contrôle d'une machine intermédiaire ayant généralement des ressources importantes comme l'illustre la figure 1.2. Elle jouera le rôle de rebond : son identité et éventuellement ses ressources seront utilisées pour attaquer la machine victime qui ne peut en aucun cas connaître l'attaquant réel. On parle de deux attaques en cascade. De nouvelles variantes d'attaques de ce type se basent sur trois ou plusieurs attaques en cascade, on parle de deux ou plusieurs rebonds dans ce cas de figure. Le rebond est lui-même une victime bien qu'il soit à l'origine de l'attaque qui vise la victime finale.

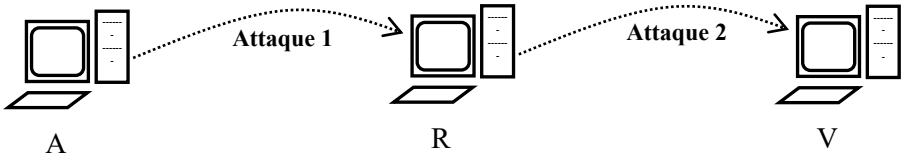

Figure 1.2. *Attaque indirecte par rebond*

C'est pour cette raison qu'il ne faut pas négliger de sécuriser une machine pour la simple raison qu'elle est sans utilité, une telle machine peut être utilisée comme rebond surtout dans le cas où elle présente des ressources importantes.

1.3.2.2.2. Par réponse

L'attaquant envoie une requête à un serveur de telle sorte qu'il redirige la réponse vers une machine tierce comme l'illustre la figure 1.3. L'attaque réside pour cette dernière dans le fait qu'elle reçoit une réponse qu'elle n'a pas sollicitée, qui peut l'induire en erreur, inhiber son fonctionnement, l'obliger à réagir à travers un mauvais comportement ou même la rendre hors service.

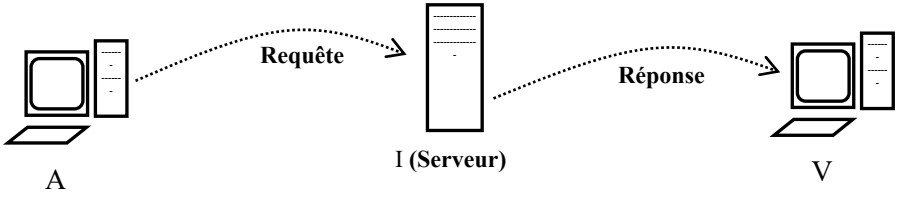

Figure 1.3. *Attaque indirecte par réponse*

L'attaque par réponse se fait forcément à travers un serveur qui ne sera pas lui-même attaqué alors que l'attaque par rebond se matérialise par deux attaques en cascade.

1.3.3. *Exemples d'attaques*

Les pirates ne cessent d'identifier ou de créer des failles au niveau des systèmes et des réseaux, on se contente d'en présenter quelques-unes.

1.3.3.1. *Injection SQL*

Elle permet à un utilisateur de se connecter sans avoir le mot de passe dans le cas où l'authentification se fait par la requête SQL suivante :

```
SELECT * FROM Utilisateurs WHERE login='le login' AND
password='le mot de passe'
```

Si l'utilisateur introduit comme *login* « `a' OR 1=1 #` » et n'importe quel *password*.

La requête devient :

```
SELECT * FROM Utilisateurs WHERE login='a' OR 1=1 #
password=azerty
```

Une requête toujours vraie, le # rend ce qui suit comme commentaire. C'est aussi l'utilisation de l'apostrophe (') pour casser l'authentification dans le cas de sites web développés avec Jomla.

1.3.3.2. *TCP SYN*

Une connexion TCP se fait en trois étapes (*three hand shake*), comme l'indique la figure 1.4. La machine qui initie la communication envoie une requête de demande de connexion SYN C, la machine qui reçoit la demande envoie un acquittement ACK SYN C+1 ainsi que le numéro de séquence SEQ S et déclenche un temporisateur (*time-out*) en attendant un acquittement de ce numéro de séquence ACK SEQ S+1.

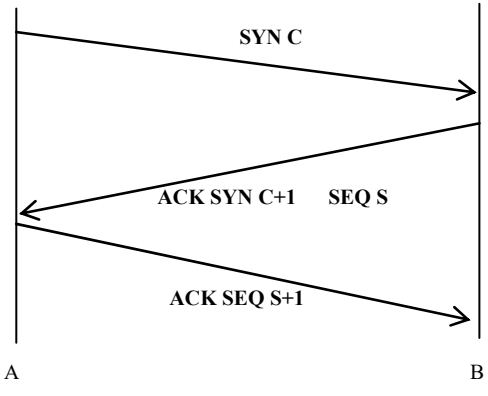

Figure 1.4. *Attaque TCP SYN*

Dans le cas où la machine qui initie la connexion n'envoie pas le dernier message (ACK SEQ S+1) et à l'épuisement du *time-out*, l'autre machine crée une structure de données volumineuse contenant les contextes des différentes connexions.

Si le nombre de connexions TCP incomplètes augmente, alors l'espace mémoire sera épuisé et la machine attaquée sera hors service. On parle dans ce cas de figure d'attaque TCP SYN.

1.3.3.3. Buffer Overflow

C'est une attaque très efficace mais énormément complexe. Elle vise à injecter un programme en écrivant dans un *buffer* plus de données que sa taille afin d'écraser le code et d'injecter des données utiles pour prendre le contrôle du programme à attaquer.

```
int buf[20] ;
strcpy(buf, "un code de taille important") ;
/*Dépassement de taille*/
```

L'erreur de dépassement d'espace mémoire n'apparaît pas lors de la compilation ni systématiquement lors de l'exécution. Il cause un crash dans le cas où l'espace mémoire qui suit l'espace réservé pour *buf* est utilisé par d'autres variables. L'espace mémoire utilisé peut correspondre même au système d'exploitation. Un choix du contenu de la chaîne peut permettre de prendre le contrôle de la machine par création d'une faille système.

1.3.3.4. Mail Bombing

Ce type d'attaque se produit s'il y a un bombardement d'un compte email par des messages divers qui peuvent dans certains cas de figure s'envoyer automatiquement vers les adresses email présentes dans le carnet d'adresses.

1.3.4. *Quelques statistiques*

On se limite dans ce paragraphe à donner quelques chiffres selon des statistiques menées par l'association CompTIA (*Computing Technology Industry*)[2] :

2. Voir : www.comptia.org.

– 52 % des dommages sont dus à des erreurs humaines (le facteur humain est le plus important, ce qui nécessite des travaux de sensibilisation) ;

– 80 % des attaques sont faites par les employés et surtout par les ex-employés soit par négligence soit par irresponsabilité (la prise en compte au niveau des contrats pour les employés des clauses de responsabilisation s'impose).

Les dégâts des attaques sont répartis comme suit :

– 44 % des dégâts représentent des pertes de temps ;

– 16 % des dégâts se manifestent par des dommages des logiciels ;

– 16 % des dégâts se manifestent par des pertes d'informations.

En ce qui concerne les intrusions, on peut citer à titre d'exemple :

– MyDoom a causé 38 millions $ de dégât en EUA en 2004 ;

– SirCam a causé des dégâts de 1,15 million $ en EUA ;

– CodeRed a causé des dégâts de 2,62 millions $ en EUA (250 000 de systèmes infectés en moins de 9 heures) ;

– Himda a causé des dégâts de 635 millions $ en EUA.

1.4. Objectifs de la sécurité

Les statistiques ont montré l'importance du facteur humain par sa négligence ou par son ignorance pour la génération et le renforcement des failles de sécurité ; c'est la même chose au niveau des accidents de la route. De ce fait, une grande partie de l'investissement en matière de sécurité s'adresse à l'utilisateur afin de le cultiver et le sensibiliser. De plus, il fallait mettre en place des solutions techniques de sécurité.

L'objectif de toute mesure de sécurité consiste à atténuer (*to mitigate*) les risques engendrés par les failles de sécurité afin de minimiser les attaques qui exploitent les failles de sécurité que les pirates ne cessent de découvrir au sein des réseaux, des systèmes et des applications.

Il n'existe plus de solution de sécurité radicale, il s'agit seulement d'une atténuation (*mitigation*).

1.4.1. *Mise en place d'une culture*

Le facteur humain doit toujours constituer l'axe de tout investissement. Pour la sécurité, il s'impose comme l'élément le plus important vu les failles qu'il peut engendrer.

L'instauration d'une culture en matière de sécurité consiste à sensibiliser et responsabiliser les intervenants à travers plusieurs mécanismes :

– effectuer des formations pour tous les utilisateurs de l'outil informatique et ne pas miser sur leur ignorance comme mesure de sécurité ;

– formuler et faire signer et suivre une charte d'utilisation et d'exploitation des ressources matérielles et logicielles ainsi que les données et les documents utilisés ;

– mettre en place au sein de l'entreprise une cellule pour gérer les problèmes de sécurité et sensibiliser le personnel à travers des affiches, des clauses à signer, des mesures de contrôle, etc.

1.4.2. *Mise en place des solutions techniques*

C'est la partie technique de la sécurité, elle consiste à apporter des solutions et mettre en place des équipements de sécurité matériels et logiciels appropriés. Elle consiste à empêcher :

– la divulgation non autorisée des données ;

– la modification non autorisée des données ;

– l'utilisation non autorisée des ressources.

Ces mesures de sécurité sont généralement le résultat d'une enquête effectuée par des experts de sécurité au sein de l'entreprise ; c'est la mission d'audit sécurité ou encore de *consulting* exigée par la loi.

1.5. Domaines de la sécurité

La sécurité informatique couvre plusieurs domaines complémentaires qui touchent les aspects : énergétique, physique, organisationnel, environnemental, etc. :

– l'évaluation des risques ;

– politique de sécurité ;

– organisation des informations de sécurité ;

– gestion du patrimoine (logicielle et données) ;

– sécurité des ressources humaines ;

– sécurité physique et environnementale ;

– management des communications et des opérations ;

– acquisition, développement et maintenance du système d'information ;

– contrôle d'accès ;

– management des incidents de sécurité de l'information ;

– gestion de la continuité des activités ;

– conformité.

La sécurité dans son sens le plus large peut concerner plusieurs éléments on ne peut plus variés. On distingue principalement trois domaines de sécurité, en l'occurrence la sécurité énergétique, physique et logique.

1.5.1. *Sécurité énergétique*

Dans le cas d'un système informatique complexe avec des services en temps réel, il est nécessaire d'avoir des serveurs en veille et des *back up* automatiques. De ce fait, une simple chute électrique peut causer des dégâts considérables. Dans ce cas de figure, il fallait déployer des groupes électrogénérateurs et/ou des onduleurs dans le but d'avoir une source d'énergie durable et indépendante du secteur qui peut présenter des coupures périodiques. On parle de sécurité énergétique.

1.5.2. *Sécurité organisationnelle et physique*

Le système informatique, aussi réduit qu'il soit, risque d'être physiquement touché par des moyens humains et/ou naturels ; on peut citer à titre d'exemple les incendies, les inondations, les vols, etc.

La sécurité physique consiste à prendre des mesures de contrôle et d'isolation physique du système. Il en existe deux types : la sécurité de haut niveau concerne la partie organisationnelle, elle gère les différentes stratégies de la sécurité physique. La sécurité des infrastructures s'intéresse à sécuriser physiquement les équipements informatiques.

1.5.2.1. *Sécurité de haut niveau*

La sécurité de haut niveau couvre plusieurs éléments, elle touche à :

– l'organisation ;

– la structure de sécurité ;

– le personnel ;

– la gestion des sauvegardes ;

– la gestion des incidents.

Il s'agit de la sécurité organisationnelle, elle s'intéresse à valider les structures et les organisations responsables de la sécurité telles que les cellules de veille technologiques, les administrateurs et les agents de sécurité. Elle permet de vérifier aussi les investissements en matière de sécurité au sein des entreprises comme les formations et les actions d'instauration de culture nécessaires *via* des chartes, des affichages, des règles de gestion. D'autres points entrent dans cet aspect de sécurité comme c'est le cas des politiques de sauvegardes et les actions de gestion des incidents qui peuvent arriver au sein de l'entreprise.

1.5.2.2. *Sécurité des infrastructures*

La sécurité des infrastructures couvre plusieurs éléments, elle concerne :

– le câblage ;

– les bureaux ;

– les locaux des serveurs ;

– les locaux d'archivage ;

– les locaux techniques ;

– les armoires serveurs ;

– le centre de calcul ;

– les sites de travail à domicile.

Cet aspect concerne la partie physique, il s'intéresse à sécuriser physiquement les équipements et les infrastructures informatiques ainsi que les locaux. En ce qui concerne les locaux, les politiques de sécurité dépendent de l'importance et du contenu de ses différents locaux. Les serveurs bénéficient d'une politique de sécurité spécifique vu leur importance dans tout système informatique. Les sites de travail à distance représentent une faiblesse et nécessitent des mesures de sécurité spécifiques à ne pas ignorer.

La sécurité physique couvre les aspects naturels et humains et sera assurée à travers :

– les détecteurs de fumée ;

– les détecteurs d'eau ;

– les détecteurs de mouvements ;

– les caméras de surveillance ;

– les systèmes de pointage (carte, empreinte, etc.).

1.5.3. *Sécurité logique*

La sécurité logique concerne le patrimoine logiciel et système qui doit être sécurisé à travers des mots de passe, des limitations d'accès, des classements électroniques des documents suivant l'importance et le degré de confidentialité. C'est l'aspect propre à la sécurité informatique à laquelle cette dernière peut se résumer, elle est gérée par la norme OSI 2 (ISO 7498-2).

La sécurité concerne tout système informatique (réseau, station de travail, serveur, etc.) ainsi que les systèmes d'exploitation et les applications.

1.5.3.1. *Sécurité des réseaux*

Les réseaux représentent un élément-clé au sein d'un parc informatique, de ce fait ils représentent une cible potentielle pour les attaquants, ce qui exige un investissement en matière de sécurité permettant de prendre les mesures nécessaires de filtrage, de contrôle d'accès, de protection des infrastructures, etc.

Différents équipements réseaux sont concernés par la sécurité :

– modem ;

– commutateurs (VLAN, sécurité par port) ;

– *firewall* ;

– routeur (ACL) ;

– point d'accès.

La sécurité des réseaux permet de limiter l'accès distant aux différents segments et équipements réseau.

1.5.3.2. *Sécurité des systèmes*

Les systèmes d'exploitation représentent l'élément de base de la partie logicielle au sein d'un système informatique, chaque système d'exploitation aussi récent qu'il soit admet des vulnérabilités qui peuvent être exploitées par les attaquants et plus particulièrement les systèmes Microsoft Windows qui représentent une cible très en vue en raison de son utilisation très répandue.

Cette partie de la sécurité vise aussi les standards téléphoniques et fax qui peuvent être utilisés comme chemin non autorisé pour nuire la sécurité.

1.5.3.3. *Sécurité des applications*

Les logiciels et les applications diverses ne sont pas au-dessus de toute critique et représentent des failles diverses que les attaquants ne cessent d'identifier malgré les patchs que les développeurs fournissent périodiquement afin d'apporter les correctives nécessaires. De plus les attaques menées sont spécifiques aux logiciels en question. De ce fait, des précautions et des préventions nécessaires de sécurité sont spécifiques aux différents logiciels. Les classes de logiciels qui représentent des cibles potentielles sont :

– les services web ;

– les services e-mail ;

– les services de bases de données, etc.

1.5.3.4. *Sécurité des données*

Bien que les logiciels soient d'importance capitale, la perte ou la mise en cause des données peuvent avoir des effets néfastes sur le système informatique. Il est donc nécessaire de prévoir les mesures de sécurité nécessaires afin de

protéger les données contre la divulgation et la modification non autorisées, et ce à travers un ensemble de mécanismes variés et complémentaires.

Les statistiques ont montré qu'une grande partie des dégâts relatifs aux attaques sont dus à la perte de données. La sécurité des données couvre plusieurs mesures :

– contrôle d'intégrité ;

– chiffrement ;

– redondance de serveurs de données ;

– sécurité des bases de données ;

– disponibilité des données.

1.6. Normalisation de la sécurité

La sécurité s'est imposée en tant que défi très important et afin d'éviter toute divergence, la normalisation se présente comme solution afin de définir la terminologie nécessaire ainsi que les différentes exigences et solutions.

1.6.1. *Problématique et présentation générale*

Pour remédier à la divergence et mener la sécurité sur une base solide et bien structurée, un standard vient d'apparaître, il s'agit de la norme ISO 7498-2:1989[3], qui représente la partie 2 du modèle OSI relative à l'architecture de sécurité. La norme internationale ISO 7498-2 a été élaborée par le comité technique ISO/TC 97.

L'Union internationale de la communication (ITU) a prévu la norme X.800 permettant de définir l'architecture de sécurité pour les systèmes ouverts.

1.6.2. *Norme ISO 7498-2*

Afin de couvrir les communications sûres entre systèmes ouverts, la deuxième partie de l'ISO 7498 publiée en 1989 :

3. Voir : http://www.iso.org.

1) donne une description générale des services de sécurité et des mécanismes associés qui peuvent être fournis par le modèle de référence ;

2) définit où, dans l'architecture OSI, les services et mécanismes peuvent être fournis.

Les services et les mécanismes de sécurité de base et leurs placements appropriés ont été identifiés pour toutes les couches du modèle de référence de base. En outre, les relations architecturales entre les services et les mécanismes de sécurité et le modèle de référence de base ont été identifiées. Des mesures supplémentaires de sécurité peuvent être nécessaires dans les systèmes extrémité, les installations et les organisations. Ces mesures s'appliquent dans différents contextes d'application. La définition des services de sécurité nécessaires à la prise en charge de ces mesures supplémentaires de sécurité est en dehors du champ d'application de la présente norme internationale.

Les fonctions de sécurité OSI ne concernent que les aspects visibles d'une voie de communication permettant aux systèmes d'extrémités de réaliser entre eux un transfert sûr d'informations. La sécurité OSI ne concerne pas des mesures de sécurité nécessaires dans les systèmes extrémité, installations et organisations, sauf lorsque ces mesures ont des effets sur le choix et le placement de services de sécurité visibles dans l'OSI. Ces derniers aspects de la sécurité peuvent être normalisés, mais pas le cadre des normes OSI.

La présente partie de I'ISO 7498 complète les concepts et principes définis dans I'ISO 7498-1 sans les modifier, l'ISO 7498 permet de définir les termes suivants applicables au domaine de sécurité :

– vulnérabilité : une faille ou une insuffisance système ou réseau qui peut être exploitée ou non ;

– attaque : une action malveillante permettant d'exploiter une faille ;

– contrôle d'accès : précaution prise contre l'utilisation non autorisée d'une ressource ; ceci comprend les précautions prises contre l'utilisation d'une ressource de façon non autorisée ;

– liste de contrôle d'accès : liste des entités autorisées à accéder à une ressource ; cette liste inclut les droits d'accès liés aux entités ;

– imputabilité : propriété qui garantit que les actions d'une entité ne peuvent être imputées qu'à cette entité ;

– menace active : menace de modification non autorisée et délibérée de l'état du système ;

– information d'authentification : information utilisée pour établir la validité d'une identité déclarée ;

– échange d'authentification : mécanisme destiné à garantir l'identité d'une entité par échange d'informations ;

– autorisation : attribution des droits, comprenant la permission d'accès sur la base de droits d'accès ;

– disponibilité : propriété d'être accessible et utilisable sur demande par une entité autorisée ;

– capacité : jeton utilisé comme identificateur d'une ressource de telle sorte que la possession du jeton confère les droits d'accès à cette ressource ;

– voie : chemin de transfert de l'information ;

– cryptogramme : données obtenues par l'utilisation du chiffrement. Le contenu sémantique des données résultantes n'est pas compréhensible.

Le cryptogramme peut lui-même être réinjecté dans un nouveau chiffrement pour produire un cryptogramme surchiffré :

– texte en clair : données intelligibles dont la sémantique est compréhensible ;

– confidentialité : propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés ;

– justificatif d'identité : données transférées pour établir l'identité déclarée d'une entité ;

– analyse cryptographique : analyse d'un système cryptographique, et/ou de ses entrées et sorties, pour en déduire des variables confidentielles et/ou des données sensibles (y compris un texte en clair) ;

– valeur de contrôle cryptographique : information obtenue en réalisant une transformation cryptographique (voir cryptographie) sur une unité de données.

La valeur de contrôle peut être obtenue en une ou plusieurs étapes et résulte d'une fonction mathématique utilisant la clé et une unité de données. Elle permet de vérifier l'intégrité d'une unité de données :

– cryptographie : discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée. La cryptographie détermine les méthodes de chiffrement et de déchiffrement. Une attaque portant sur les principes, moyens et méthodes de cryptographie est appelée une analyse cryptographique ;

– intégrité des données : propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée ;

– authentification de l'origine des données : confirmation que la source des données reçues est telle que déclarée ;

– déchiffrement/décryptage : opération inverse d'un chiffrement réversible ;

– déni de service : impossibilité d'accès à des ressources pour des utilisateurs autorisés ou introduction d'un retard pour le traitement d'opérations critiques ;

– signature numérique : données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple) ;

– chiffrement/cryptage : transformation cryptographique (voir cryptographie) de données produisant un cryptogramme. Le chiffrement peut être irréversible. Dans ce cas, le déchiffrement correspondant ne peut pas être effectué, c'est le cas des fonctions de hachage ;

– chiffrement de bout en bout : chiffrement de données à l'intérieur ou au niveau du système extrémité source, le déchiffrement correspondant ne se produisant qu'à l'intérieur, ou au niveau du système extrémité de destination ;

– politique de sécurité fondée sur l'identité : politique de sécurité fondée sur les identités et/ou les attributs des utilisateurs, d'un groupe d'utilisateurs ou d'entités agissant au nom d'utilisateurs et sur les identités et/ou attributs des ressources/objets auxquels on doit accéder ;

– clé : série de symboles commandant les opérations de chiffrement et de déchiffrement ;

– gestion de clés : production, stockage, distribution, suppression, archivage et application de clés conformément à la politique de sécurité ;

– chiffrement de liaison (liaison par liaison) : application particulière du chiffrement à chaque liaison du système. Le chiffrement liaison par liaison implique que les données soient du texte en clair dans les entités relais ;

– détection de modification : mécanisme utilisé pour détecter les modifications, accidentelles ou intentionnelles, d'une unité de données ;

– déguisement : prétention qu'a une entité d'en être une autre ;

– notarisation : enregistrement de données chez un tiers de confiance permettant de s'assurer ultérieurement de leur exactitude (contenu, origine, date, remise) ;

– menace passive : menace d'une divulgation non autorisée des informations, sans que l'état du système ne soit modifié ;

– mot de passe : information d'authentification confidentielle, habituellement composée d'une chaîne de caractères ;

– authentification de l'entité homologue : confirmation qu'une entité homologue d'une association est bien l'entité déclarée ;

– sécurité physique : mesures prises pour assurer la protection des ressources contre des menaces délibérées ou accidentelles ;

– respect de la vie privée : droit des individus de contrôler ou d'agir sur des informations les concernant, qui peuvent être collectées et stockées, et sur les personnes par lesquelles et auxquelles ces informations peuvent être divulguées. Ce terme étant lié au droit privé, il ne peut pas être très précis et son utilisation devrait être évitée sauf pour des besoins de sécurité ;

– répudiation : le fait, pour une des entités impliquées dans la communication, de nier avoir participé aux échanges, totalement ou en partie ;

– contrôle de routage : application de règles, au cours du processus de routage, afin de choisir ou d'éviter, des réseaux, liaisons ou relais spécifiques ;

– politique de sécurité fondée sur des règles : politique de sécurité fondée sur des règles globales imposées à tous les utilisateurs. Ces règles s'appuient généralement sur une comparaison de la sensibilité des ressources auxquelles on doit accéder avec les attributs correspondants d'utilisateurs, d'un groupe d'utilisateurs ou d'entités agissant au nom d'utilisateurs ;

– audit de sécurité : revue indépendante et examen des enregistrements et de l'activité du système afin de vérifier l'exactitude des contrôles du système pour s'assurer de leur concordance avec la politique de sécurité établie et les procédures d'exploitation, pour détecter les infractions à la sécurité et pour recommander les modifications appropriées des contrôles, du politique et des procédures ;

– journal d'audit de sécurité : données collectées et pouvant éventuellement être utilisées pour permettre un audit de sécurité ;

– étiquette de sécurité : marque liée à une ressource dénommant ou désignant les attributs de sécurité de cette ressource (cette ressource peut être une unité de données).

La marque et/ou l'association de la marque à la ressource peuvent être implicites ou explicites :

– politique de sécurité : ensemble des critères permettant de fournir des services de sécurité. Une politique de sécurité complète traite nécessairement des sujets qui sont hors du champ d'application de l'OSI ;

– service de sécurité : service, fourni par une couche de systèmes ouverts, garantissant une sécurité des systèmes et du transfert de données ;

– protection sélective des champs : protection de certains champs spécifiques dans un message à transmettre ;

– sensibilité : caractéristique d'une ressource relative à sa valeur ou à son importance et, éventuellement, à sa vulnérabilité ;

– menace : violation potentielle de la sécurité ;

– analyse du trafic : déduction d'informations à partir de l'observation des flux de données (présence, absence, quantité, direction, fréquence) ;

– confidentialité du flux de données : service de confidentialité fournissant une protection contre l'analyse du trafic ;

– bourrage : production d'instances de communication parasites, d'unités de données parasites et/ou de données parasites dans des unités de données ;

– fonctionnalité de confiance : fonctionnalité perçue comme correcte en ce qui concerne certains critères, tels que ceux définis par une politique de sécurité.

1.7. Services de sécurité

On désigne par service de sécurité : une exigence en matière de sécurité à satisfaire. Un système informatique est qualifié de « sécurisé » s'il satisfait les principales conditions appelées services de sécurité :

– authentification :
  - origine des données ;
  - entre entités ;

– confidentialité :
  - des données ;
  - du trafic ;

– intégrité :
  - des données ;
  - du trafic ;

– non-répudiation :
  - de l'origine ;
  - du destinataire ;

– contrôle d'accès ;

– disponibilité de service ;

– traçabilité.

L'authentification et l'intégrité peuvent être groupées par le terme authenticité.

Ces services s'appliquent aux entités systèmes et/ou à l'information stockée en local, en cours de traitement ou transmise à travers le réseau.

Assurer la sécurité informatique au sein d'une entreprise consiste forcément à assurer les différentes exigences mentionnées ci-dessus. Certains services se présentent plus critiques que d'autres selon la nature du trafic et des informations manipulées. Reste à l'administrateur système et réseau et plus principalement le responsable de sécurité de définir les priorités de satisfaction de différents services de sécurité, une priorité qui peut changer selon les circonstances.

Toute violation ou mise en cause d'un ou plusieurs services de sécurité entraîne forcément la mise en cause de la sécurité au niveau du système ou de l'instance concernée.

1.7.1. *Authentification*

À la différence de l'identification qui sert à marquer ou encore distinguer une entité parmi d'autres, l'authentification est une preuve d'identité, elle sert à assurer que l'entité en question est réellement l'entité qui vient de s'identifier.

Le fait de dire que « je suis X » est une identification qui doit être suivie par un moyen pour prouver qu'il est vraiment « X », c'est l'authentification.

Plusieurs moyens d'authentification de base en l'occurrence « je sais », « je possède » et « je suis » peuvent être envisagés. Ils peuvent être mis en place d'une façon individuelle ou couplée.

1.7.1.1. *« Je sais »*

C'est le moyen le plus simple et le plus connu. Il consiste à s'authentifier *via* une combinaison de caractères secrète : c'est le mot de passe associé à un *login*. Le *login* est unique, il sert pour l'identification. Le mot de passe est secret, il sert pour l'authentification.

Un mot de passe doit satisfaire un ensemble de règles afin d'éviter toute sorte de divulgation et faire face à toute tentative d'intrusion. En effet, un mot de passe doit satisfaire les règles suivantes :

– ne doit pas être trivial (abc, azerty, 123, etc.) ;

– ne doit pas être compliqué au point d'être difficile à apprendre ;

– ne doit jamais figurer sur un support physique (bout de papier, carnet, etc.) ou numérique (fichier, email, etc.) ;

– n'est pas issu du dictionnaire ;

– ne doit pas correspondre à une caractéristique propre (nom, prénom, matricule de voiture, etc.) ;

– n'est pas doublement utilisé (compte Facebook, compte email, etc.) ;

– doit comprendre une combinaison de majuscules, minuscules, chiffres et caractères spéciaux ;

– doit être modifié périodiquement afin de limiter sa durée d'exploitation.

Une bonne façon de choisir un mot de passe est de sélectionner un mot du dictionnaire ou issu d'une autre langue (arabe) et de le retranscrire en utilisant les lettres du français et éventuellement des chiffres (3a55alem@) tout en présentant explicitement des fautes d'orthographe (« aurtogaffe » au lieu de « orthographe ») ou en mélangeant ou inversant les syllabes (« phegrathoor »).

1.7.1.2. *« Je possède »*

L'authentification, dans ce cas de figure, est assurée par la possession d'un objet physique privé, c'est le cas de la carte à puce utilisée comme moyen de pointage du personnel.

Cette méthode est la plus primitive et la plus simple à utiliser, elle présente quelques lacunes liées à la possibilité de pouvoir céder l'objet en question.

C'est le cas de l'authentification d'accès à un local privé moyennant un badge visiteur pour les personnes étrangères à l'entreprise.

Pour le cas d'une carte bancaire, on assiste à deux moyens d'authentification en cascade : je possède (la carte) et je connais (le code).

1.7.1.3. *« Je suis »*

C'est le moyen d'authentification le plus fort, il est lié à des caractéristiques propres à une personne telles que l'empreinte digitale (on parle de l'authentification biométrique), les caractéristiques des yeux ou les caractéristiques de la main (forme, chaleur, etc.).

Une telle méthode est utilisable pour permettre de contrôler l'accès à des endroits ou des locaux critiques. Elle est aussi utilisable pour s'authentifier à une machine ou à un système.

1.7.2. *Confidentialité*

C'est le fait de s'assurer que l'information manipulée ne soit pas discrétisée par n'importe quelle entité tierce non autorisée. C'est une protection contre la

divulgation d'information critique, et ce en utilisant la technique de chiffrement afin de rendre l'information illisible et incompréhensible par les autres entités non concernées.

1.7.3. *Intégrité*

C'est une protection contre la modification de l'information manipulée, c'est un moyen permettant de détecter si un bloc d'information à subit une modification aussi simple qu'elle soit en utilisant les techniques de hachage qui consiste à générer un message représentatif, unique et dépendant de l'information en question.

1.7.4. *Non-répudiation*

C'est le fait de garantir pour une information transmise qu'aucun des correspondants (émetteur et récepteur) ne pourra nier une transaction.

1.7.5. *Traçabilité et contrôle d'accès*

La traçabilité consiste à pouvoir suivre les accès aux ressources informatiques sensibles (heure de connexion, suivi des actions, etc.). Le contrôle d'accès consiste à limiter l'accès aux différentes ressources partagées matérielles et logicielles.

1.7.6. *Disponibilité de service*

C'est le fait de maintenir un service en fonctionnement afin de pouvoir satisfaire les requêtes des utilisateurs autorisés dans tous les cas de figure. C'est une protection du serveur même à travers des mesures et des techniques de détection et de neutralisation des tentatives de mise hors service par des entités externes.

1.8. Mécanismes de sécurité

On désigne par mécanisme de sécurité une mesure ou une technique bien définie permettant d'assurer un ou plusieurs services de sécurité.

Les mécanismes de sécurité informatique représentent des moyens permettant d'assurer les services de sécurité. La norme ISO 7498-2 permet de spécifier :

– le chiffrement avec clé partagée ;

– le chiffrement avec clés privée/publique ;

– l'intégrité des données avec une fonction de hachage ;

– l'authentification ;

– le contrôle d'accès ;

– la signature numérique ;

– la notarisation.

1.8.1. *Chiffrement*

Le chiffrement, appelé aussi cryptage, est une technique utilisée depuis plusieurs siècles, elle permet de modifier un texte et le rendre indiscernable sauf par celui qui l'a généré. La branche de la mathématique qui s'intéresse à ce sujet s'appelle la cryptographie. Ce mécanisme permet d'assurer le service de confidentialité.

Le chiffrement se base sur deux techniques de base : c'est la substitution (un tableau de correspondance entre les lettres et les chiffres) et le décalage appelé aussi chiffrement de César qui permet de substituer les lettres d'une façon circulaire.

Depuis son apparition, ce mécanisme a vu plusieurs évolutions : d'abord les premières solutions étaient basées sur le choix d'un algorithme qui sera utilisé aussi bien pour le chiffrement que pour le déchiffrement. Ensuite, une nouvelle génération de solutions de chiffrement, c'est celle à clé symétrique (le pas dans le cas du chiffrement de César), cette clé sera utilisée à la fois pour le chiffrement et pour le déchiffrement. Finalement, le chiffrement à clés asymétriques a vu le jour, il présente une paire de clés utilisées pour le chiffrement et pour le déchiffrement dans l'objectif d'éviter le problème de partage qui représente une faille de sécurité au niveau des deux premières générations de techniques de chiffrement.

On peut citer à titre d'exemple les algorithmes de chiffrement : DES, 3DES, AES, RSA, BlowFish, etc.

Le chiffrement n'a jamais été une solution incontournable dans la mesure où n'importe quel cryptogramme peut être analysé afin d'obtenir le texte en clair correspondant. On parle de la cryptanalyse qui représente une technique qui se base sur les statistiques au niveau des langues. On peut citer à titre d'exemple les travaux de Turing lors de la Deuxième Guerre mondiale et qui ont permis de retrouver les textes en clair des messages militaires transmis par les gouverneurs de l'ennemi à leurs troupes, et ce à travers une solution de cryptanalyse appelée machine de Turing.

1.8.2. *Contrôle d'intégrité*

Le contrôle d'intégrité est un mécanisme basé sur le hachage et permettant d'assurer le service intégrité.

Un algorithme de hachage est une fonction non bijective permettant de générer une chaîne de taille fixe unique qui représente le *hashcode* à partir d'une chaîne de taille variable. Cette dernière peut correspondre à un paquet, à un message, à une page web, ou autre, c'est à l'entité d'assurer son intégrité.

Le *hashcode* représente la signature dans la mesure où tout changement au niveau du message original permet d'obtenir un *hashcode* différent, ce qui permet de détecter tout changement sur l'entité à sécuriser et par conséquent assurer l'intégrité. Plusieurs algorithmes de hachage sont disponibles dont les plus importants sont : MD5 (16 octets) et SHA1 (20 octets).

1.8.3. *Contrôle d'accès*

Le contrôle d'accès représente le mécanisme permettant d'assurer le service d'authentification. Les techniques d'authentification peuvent être classées en trois grandes familles liées à la possession, à la connaissance d'une entité ou à une caractéristique propre (biométrie, parole, etc.).

L'authentification est nécessaire pour assurer l'accès local ou distant à n'importe quel service, c'est le moyen convenable pour limiter les accès et identifier les responsabilités.

La technique d'authentification la plus utilisée est celle basée sur les mots de passe ; une telle technique exige des conditions sur le choix, la durée de vie et l'utilisation du mot de passe qui représente un élément-clé et une entité critique dans tout système informatique.

1.8.4. *Signature numérique*

La signature numérique (parfois appelée signature électronique) est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier. Un mécanisme de signature numérique doit présenter les propriétés suivantes :

– il doit permettre au lecteur d'un document d'identifier la personne ou l'organisme qui a déposé sa signature ;

– il doit garantir que le document n'a pas été altéré entre l'instant où l'auteur l'a signé et le moment où le lecteur le consulte.

1.8.5. *Notarisation*

La notarisation électronique est la certification des différentes étapes de l'évolution d'un document électronique en vue :

– de permettre lors d'un échange entre deux parties de garantir le contenu, l'origine, la date et la destination d'un message électronique ;

– d'archiver de façon sécurisée des documents numériques.

La notarisation électronique permet la vérification et l'archivage des preuves d'échanges et d'archivage électroniques par un tiers de confiance agréé (à la manière d'un notaire). Cette technique améliore la sécurité des échanges et de l'archivage électronique ; en effet, elle fournit différents mécanismes de suivi et d'archivage des transactions émises et reçues (l'intégrité, l'origine, la date et la destination des données).

1.9. Bonnes pratiques

La sécurité informatique peut être assurée à travers des bonnes pratiques permettant d'atténuer les risques de sécurité et rendre les attaques de plus en

plus difficiles. Les bonnes pratiques aussi bien d'ordre technique que comportemental consistent à :

– concevoir une politique écrite de sécurité ;

– former les employés concernant les risques de *social engineering* et développer des stratégies pour valider les identités à travers le téléphone, le mail ou encore des personnes ;

– contrôler d'accès physique aux systèmes ;

– utiliser des mots de passe forts et les changer régulièrement ;

– chiffrer les données sensibles et les protéger par mots de passe ;

– limiter la connexion en mode privilégié au niveau du système d'exploitation ;

– déployer le matériel et les logiciels la sécurité ;

– effectuer des sauvegardes et tester les fichiers sauvegardés régulièrement ;

– désactiver les services et les ports non utilisés ;

– garder les correctifs à jour en les installant chaque semaine ou tous les jours pour éviter les dépassements de mémoire tampon et les attaques par élévation de privilèges ;

– prévoir périodiquement des audits de sécurité pour tester le réseau et les systèmes et veiller à appliquer les recommandations qui en résultent.

1.10. Conclusion

La sécurité informatique s'impose actuellement comme solution aux problèmes déjà recensés comme l'illustrent les statistiques. En effet, les failles et les vulnérabilités sont multiples et diversifiées, elles couvrent tous les niveaux de l'informatique en passant du matériel au logiciel, des infrastructures et des structures aux intervenants (utilisateurs et administrateurs).

La sécurité informatique permet de couvrir plusieurs domaines et prévoit des solutions organisationnelles, culturelles et techniques afin de donner des éléments de solutions pour les diverses failles et vulnérabilités.

La sécurité, ayant pour objectif le maintien en fonctionnement du système informatique, touche plusieurs points externes et internes, physiques et logiques, matériaux et humains, etc.

La partie technique de la sécurité informatique à proprement parlé se résume par le mot magique ACID, acronyme des quatre points à satisfaire afin de garantir un fonctionnement normal. La vérification de ces points nécessite la connaissance des failles et des vulnérabilités.

Chapitre 2

Failles de sécurité

2.1. Introduction

TCP/IP est une norme de fait qui est apparue comme une normalisation de quelque chose qui existe déjà (ARPA-Net) sans aucune modification ni prise en considération de plusieurs points, en l'occurrence les mesures de sécurité.

De plus et vu sa simplicité et le développement exponentiel d'Internet, TCP/IP s'est imposé comme la norme la plus utilisée. En effet, il est rare, voire même impossible, qu'un informaticien rencontre une norme autre que TCP/IP.

L'historique de TCP/IP est celui d'Internet ou encore de son ancêtre Arpanet. Internet, par son historique et les circonstances de son apparition, est une solution distribuée ; on parle d'« intelligence aux bornes », c'est la raison principale derrière toutes les vulnérabilités enregistrées dans la mesure où des fonctionnalités avancées et complexes sont mises à la disposition de l'utilisateur final.

L'utilisation de TCP/IP en local (Intranet) présente les mêmes failles de sécurité, voire même plus graves, vu la taille restreinte et la facilité de divulgation de l'information.

L'évolution considérable dans le domaine du génie logiciel a facilité l'apparition des programmes malveillants : ce sont les *malwares* et les outils d'intrusion qui permettent de détruire les informations, de modifier les configurations, de mettre un système hors service, etc., et ce, soit directement soit indirectement en facilitant l'accès à une machine ou encore en épuisant ses ressources.

Les dégâts matériels et immatériels causés par les *malwares* ne cessent d'augmenter et présentent des répercutions sur les systèmes informatiques et engagent de plus en plus d'efforts et de temps pour remettre en fonctionnement le système à la suite de chaque attaque.

2.2. Failles au niveau de TCP/IP

TCP/IP largement utilisé, il représente par sa structure et vu son historique une famille de protocoles très vulnérable aux attaques.

2.2.1. *Arpanet, ancêtre d'Internet*

ARPANet est l'acronyme d'*Advanced Research Projects Agency Network*, c'est un réseau privé relatif à l'armée américaine.

Arpanet a vu le jour dans les circonstances de la guerre froide comme un moyen de communication privé pour la défense américaine. À l'époque, l'objectif qui a été fixé consiste à avoir un réseau qui peut fonctionner même s'il est partiellement détérioré par une attaque potentielle. Il fallait éliminer la centralisation comme dans le cas de certaines stratégies militaires.

Arpanet est d'une part un réseau de communication privé et par la suite sous le contrôle total de l'armée américaine et d'autre part une solution distribuée. La distribution concerne aussi bien les fonctionnalités que les outils. Il n'existe pas d'épine dorsale qui contrôle ; la seule garantie à l'époque est le caractère privé, ce qui n'est plus le cas aujourd'hui avec Internet qui est devenu un réseau de communication publique incontrôlable et dont l'accès ne peut pas être cerné ni limité par quiconque.

2.2.2. *Internet et problèmes de sécurité*

Le problème de sécurité est apparu avec la distribution mais il a été négligé par le fait que tous les nœuds du réseau Arpanet sont sous contrôle.

En 1974, le TCP/IP (*Transmission Control Protocol* et *Internet Protocol*) est créé pour uniformiser le réseau Arpanet ; le système est toujours utilisé jusqu'à nos jours.

En 1980, Arpanet s'est divisé en deux réseaux distincts, l'un militaire (Milnet : *Military Network*, qui deviendra le DDN : *Defense Data Network*) et l'autre, universitaire (NSFnet), que les militaires abandonnent au monde civil. La réflexion des constructeurs s'oriente vers une informatique décentralisée.

Le 1er janvier 1983, Arpanet adopte le TCP/IP qui sera la base d'Internet qui a connu des évolutions considérables avant de passer à l'industrie et le problème de sécurité devient de plus en plus pertinent.

L'université était la pépinière dans laquelle Internet s'est développé. Le problème de sécurité commence à apparaître mais, et vu que l'information transmise n'est pas critique, il n'a pas constitué un sujet de dialogue et de recherche.

Internet s'est développé considérablement, ce qui a incité les industriels à l'adopter comme moyen de communication et vu qu'on transmet des informations critiques et que les internautes deviennent de plus en plus nombreux, diversifiés et anonymes, le problème de sécurité apparaît sérieusement. À ce stade, il est devenu impossible de revenir en arrière, Internet est une nécessité inévitable, il fallait trouver des solutions de sécurité.

2.2.3. *Internet et facilité d'analyse*

Parmi les services de sécurité, on distingue la confidentialité. Cette dernière peut être mise en cause par simple espionnage couvrant aussi bien l'information que les entités. Cette action peut être suivie par une intervention afin de modifier les informations ou encore la configuration. L'espionnage et l'intervention se font à travers des logiciels appropriés.

2.2.3.1. *Outils de scan*

Les outils de scan sont des logiciels de surveillance système et réseau, ce sont des outils permettant d'identifier les entités au niveau d'un système informatique ou d'un réseau tel que les adresses physiques et logiques, les noms, les ports ouverts, les systèmes d'exploitation y compris les correctifs et failles, les applications, les bases de registres, les protocoles utilisés, les équipements interconnectés, les différentes configurations, etc.

Il existe une grande panoplie d'outils de scan sur Internet disponibles pour être facilement utilisés et exploités par les attaquants et les espions, ce qui rend la

tâche de scan banale et à la portée de tous. Une telle facilité permet de mettre en cause la sécurité des systèmes et des réseaux informatiques et rend l'accès plus facile, ce qui permet d'identifier les limites et les faiblesses système et réseau et par la suite de programmer et procéder à des attaques ciblées exploitant les vulnérabilités enregistrées.

Un système informatique exposé à des scans présentera une défaillance importante puisqu'il sera surveillé par les attaquants et les observateurs réseau qui peuvent passer à l'action et mettre en cause sa configuration système et/ou réseau.

2.2.3.2. *Outils d'analyse (*sniffers*)*

Ce sont des outils permettant de décortiquer et/ou de modifier les informations d'un système informatique. Les informations espionnées peuvent être soit résidentes sur les machines soit circulant à travers le réseau. On distingue deux familles d'analyseur, passive et active :

– un analyseur passif (de reconnaissance) se contente d'espionner les informations sans intervenir pour les modifier. C'est une attaque passive ;

– un analyseur actif (d'accès) met à jour les informations, ce qui permet d'induire en erreur, de changer la configuration, perdre l'information, etc.

Sur Internet, il existe une grande panoplie de logiciels d'analyse aussi bien passifs qu'actifs. Ce sont des outils exploitables facilement par les attaquants pour découvrir le trafic, les données enregistrées au niveau des nœuds et éventuellement les mettre en cause à travers des MAJ non autorisées. On peut citer à titre d'exemples quelques *sniffers* sur Internet : Wireshark, MSN Sniffer, ICQ Monitor Sniffer, Link Sniffer, EtherDetect, Jitbit Network, EffeTech http Sniffer, etc.

2.3. Failles dues aux *malwares* et outils d'intrusions

Un logiciel malveillant ou maliciel (en anglais : *malware*), appelé parfois logiciel nuisible, est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.

Actuellement, on assiste à une grande gamme de tels logiciels dont une grande partie se trouve sur Internet. Les maliciels englobent les virus, les vers, les

chevaux de Troie, ainsi que d'autres menaces ; en distingue les *spywares*, les *key loggers*, les *rootkits*, etc.

2.3.1. *Virus*

C'est un outil d'intrusion directe, il est le plus connu. Le véritable nom donné à ce type de programme est CPA (code autopropageable) mais par analogie avec le domaine médical, le nom virus lui a été affecté.

L'émission quotidienne des virus ne cesse d'augmenter progressivement. Le premier virus est apparu au Pakistan, il a été créé par les frères Amjed vers les années 1980.

Un virus admet des actions variées allant d'un message indésirable au formatage du disque, il peut arriver à mettre à jour les configurations systèmes et/ou réseaux, voire même mettre en cause les systèmes, les équipements de communication et le matériel.

2.3.1.1. *Définition*

C'est un bout de programme qui s'autoréplique (s'autocopie) pour en infecter d'autres et il est destructeur de l'information.

2.3.1.2. *Caractéristiques*

Un virus admet deux caractéristiques intrinsèques :

– l'autoréplication ;

– la destruction de l'information.

La première caractéristique reflète la capacité d'un virus à se copier d'un emplacement à un autre, de changer de répertoire, de disque, de machine, etc., sans aucune intervention ou assistance externe.

La deuxième caractéristique reflète la capacité de malveillance de ce bout de code, ce qui permet de mettre en cause les données, les programmes, les configurations, etc.

Un virus peut avoir d'autres caractéristiques s'il admet un comportement bien défini lui permettant d'acquérir des capacités supplémentaires afin d'être capable

de se cacher et de résister aux systèmes de protection, on distingue deux caractéristiques principales : la mutation et le polymorphisme.

2.3.1.2.1. Mutation

Un virus est dit mutant s'il admet plusieurs versions (on parle de variantes) qui diffèrent par leur comportement, en l'occurrence les messages affichés, les traces d'exécution. Un tel virus est difficile à vérifier puisqu'il change d'apparence sans changer ni de forme ni d'action, ce qui lui permet de garder sa signature.

2.3.1.2.2. Polymorphisme

Un virus est dit polymorphe s'il admet plusieurs formes, il se présente sous plusieurs formats de fichiers (.exe, .bat, .sys). C'est comme un caméléon, il prend la forme qui s'adapte au répertoire où il existe. Une telle caractéristique permet au virus de changer sa signature, ce qui rend la tâche de détection par les systèmes appropriés de plus en plus difficile.

2.3.1.3. *Différentes formes*

Il existe sept familles principales de virus :

1) blague : un tel type de virus fait apparaître des messages n'ayant aucun sens rien que pour déranger l'utilisateur ;

2) fausse alerte : dans ce cas de figure, le virus affiche des messages d'alerte pour annoncer des problèmes de sécurité ou des problèmes systèmes virtuels ;

3) test : ce type de virus permet d'espionner et de découvrir certaines informations critiques à travers des interrogations aux utilisateurs ;

4) macro : dans ce cas de figure, on parle de macrovirus, c'est-à-dire d'un virus à base de macro. C'est une forme de virus propre aux applications Microsoft (Office) si on crée une macro destructrice d'information et qui s'autoréplique ;

5) batch : ce sont des virus sous forme de fichiers batch (.bat) ;

6) exécutable : ce sont des virus sous forme de fichiers exécutables ou des bibliothèques dynamiques (.exe, .dll) ;

7) système : ce sont des virus sous forme de fichiers systèmes (.sys, .vxd).

2.3.1.4. *Exemples*

2.3.1.4.1. Klez

Apparu au début de l'année 2002, le virus Klez présente de nouvelles variantes du virus qui ne cessent d'apparaître (Klez.e, Klez.g, Klez.h, Klez.i, Klez.k, etc.). Il exploite également quatre autres modes de propagation :

– le web ;

– les répertoires partagés ;

– les failles de serveur Microsoft IIS ;

– les échanges de fichiers.

Il affecte particulièrement les utilisateurs de Microsoft Outlook sous les systèmes d'exploitation Windows 95, 98, Millenium, NT4, 2000 et XP ainsi que les utilisateurs de Microsoft Internet Explorer.

Le virus Klez récupère la liste des adresses présentes dans les carnets d'adresses de Microsoft Outlook, Eudora ainsi que des logiciels de messagerie instantanée (ICQ), puis il envoie à tous les destinataires un courrier à l'aide de son propre serveur SMTP.

Ainsi le virus Klez est capable de générer des courriers dont le corps est vide, dont le sujet est choisi aléatoirement parmi une gamme d'une centaine de thèmes prédéfinis et attache au courrier une pièce jointe exécutable contenant une variante du virus.

2.3.1.4.2. Magistr

Le virus Magistr est un ver polymorphe (c'est-à-dire un virus qui se propage à travers le réseau et dont la forme, ou plus exactement la signature, se modifie continuellement) se propageant à l'aide du courrier électronique. Il affecte particulièrement les utilisateurs de client de messagerie Microsoft Outlook, Eudora ou Netscape sous les systèmes d'exploitation Windows 95, 98, Millenium et 2000.

Le virus Magistr recherche les fichiers de carnet d'adresses présents sur le système (respectivement d'extensions .WAB et .DBX/. MBX pour les clients Outlook et Eudora), afin de sélectionner les destinataires du message.

Le sujet et le corps du message envoyé par le ver Magistr sont choisis aléatoirement en prenant un extrait de fichier trouvé sur le disque de l'ordinateur infecté. Le virus Magistr adjoint au message une copie de lui-même dont le nom contient une extension (ou une double extension) du type .com, .bat, .pif, .exe ou .vbs. Il risque en outre de supprimer l'intégralité des informations contenues dans le CMOS, le Bios ou dans le disque dur.

Il peut ainsi gravement endommager le système et les informations s'y trouvant. De plus, il est capable de désactiver le *firewall* personnel ZoneAlarm à l'aide de la commande WM_QUIT.

2.3.2. *Ver (worm)*

Un ver, appelé en anglais *worm*, est un outil d'intrusion qui se propage à travers le réseau. C'est un virus réseau. C'est une caractéristique liée à la façon de propagation à travers le réseau.

2.3.2.1. *Effets*

Les vers actuels se propagent principalement grâce à la messagerie (et notamment par le client de messagerie Outlook) grâce à des fichiers attachés contenant des instructions permettant de récupérer l'ensemble des adresses de courrier contenues dans le carnet d'adresses et en envoyant des copies à tous ces destinataires.

Ces vers sont la plupart du temps des scripts (généralement VBScript) ou des fichiers exécutables envoyés en pièce jointe et se déclenchant lorsque l'utilisateur destinataire clique sur le fichier attaché.

2.3.2.2. *Moyens de prévention*

Il est simple de se protéger d'une infection par ver en se méfiant des pièces envoyées en tant que fichiers attachés.

Ainsi, tous les fichiers exécutables ou interprétables par le système d'exploitation peuvent potentiellement infecter votre ordinateur. Les fichiers comportant notamment les extensions suivantes sont potentiellement susceptibles d'être infectés : 386, ACE, ACM, ACV, ARC, ARJ, ASD, ASP, AVB, AX, BAT, BIN, BOO, BTM, CAB, CLA, CLASS, CDR, CHM, CMD, CNV, COM, CPL, CPT, CSC, CSS, DLL, DOC, DOT, DRV, DVB, DWG, EML, EXE, FON, GMS,

GVB, HLP, HTA, HTM, HTML, HTA, HTT, INF, INI, JS, JSE, LNK, MDB, MHT, MHTM, MHTML, MPD, MPP, MPT, MSG, MSI, MSO, NWS, OBD, OBJ, OBT, OBZ, OCX, OFT, OV?, PCI, PIF, PL, PPT, PWZ, POT, PRC, QPW, RAR, SCR, SBF, SH, SHB, SHS, SHTML, SHW, SMM, SYS, TAR.GZ, TD0, TGZ, TT6, TLB, TSK, TSP, VBE, VBS, VBX, VOM, VS?, VWP, VXE, VXD, WBK, WBT, WIZ, WK?, WPC, WPD, WML, WSH, WSC, XML, XLS, XLT, ZIP.

Sous Windows, il est conseillé de désactiver la fonction « masquer les extensions », car cette fonction peut tromper l'utilisateur sur la véritable extension d'un fichier. Ainsi un fichier dont l'extension est .jpg.vbs apparaîtra comme un fichier d'extension .jpg.

2.3.3. *Spam*

C'est un outil d'intrusion lié au mail, il se présente sous forme d'un massage indésirable.

Le spamming, 90 % du *traffic mail*, consiste à envoyer massivement des courriels généralement de type publicitaire (dit aussi *junk mail*), à un grand nombre de personnes n'ayant pas sollicité ce type d'envoi publicitaire, engorgeant ainsi les serveurs de messagerie et vos boîtes à lettres de messages publicitaires inutiles, non sollicités et généralement mensongers. Les emails « spammés » constituent actuellement la quasi-moitié des emails « circulant » à l'échelle planétaire.

Les récentes enquêtes réalisées depuis 2003 montrent que le pourcentage de propagation du spam représente la plus grande part de l'ensemble d'emails à l'échelle mondiale.

2.3.3.1. *Effets*

Un spam entraîne plusieurs effets :

– gaspillage de temps (et donc d'argent) des utilisateurs, qui doivent trier leur courrier et nettoyer leurs boîtes à lettres plus fréquemment ;

– risque d'ignorer un message important, « caché » entre les multiples messages de « spam » ;

– « corruption » des utilisateurs non avertis, avec des offres attirantes, et bien sûr fausses ;

– atteinte à la morale, *via* des messages de publicité sexuels, politiques ou religieux, etc. ;

– gaspillage de la bande réseau qu'il consomme inutilement, monopolisant « inutilement » une bonne partie de la bande passante.

2.3.3.2. *Moyens de prévention*

Les bonnes réactions à avoir pour contrer le spam :

– ne pas répondre aux messages de spam (même pour les menacer), car cela ne ferait qu'empirer les choses, puisque cela assurera aux spammeurs que vous recevez bien leurs emails et ainsi que vous êtes réceptif à ce genre de messages ;

– configurer votre client de messagerie. En effet, plusieurs logiciels de messagerie et certains services webmail permettent de bloquer l'accès aux expéditeurs indésirables. De plus, certains clients de messagerie suppriment systématiquement les emails en question ;

– ne pas donner votre adresse email sur des formulaires de sites douteux, car beaucoup de ces sites communiquent ces adresses aux spammeurs. Il serait même utile d'avoir deux ou plusieurs adresses email, une pour vous identifier sur le web, une autre pour les groupes de discussion.

2.3.4. *Bombe logique*

C'est un cas d'intrusion qui se cache et se déclenche tout d'un coup.

C'est un programme qui se déclenche suite à un événement système (démarrage, lancement d'un programme donné, etc.) ou encore selon un planning temporel préétabli. Une bonne illustration de ceci est l'outil d'attaque Tchernobyl qui se déclenche à la même date que la catastrophe nucléaire Tchernobyl.

2.3.5. *Cheval de Troie*

C'est un outil d'intrusion indirecte, il est plus complexe et plus grave qu'un virus. Son exploitation est liée au réseau.

2.3.5.1. *Définition*

C'est un programme qui se cache à l'intérieur d'un autre programme et ouvre des ports. Il permet de prendre le contrôle d'une machine, d'exécuter des programmes et de lancer des commandes à l'insu de l'utilisateur.

Un cheval de Troie n'effectue en soi aucune action malveillante mais il permet, à travers le réseau et en ouvrant des ports, à d'autres entités de divulguer l'information ou/et de la modifier.

2.3.5.2. *Symptômes*

L'infection par un cheval de Troie présente un certain nombre de symptômes, on peut citer :

– le mouvement incontrôlable de la souris ;

– l'ouverture/fermeture des fenêtres ;

– l'activité anormale du modem ou tout autre équipement de connexion qui reflète un trafic anormal sur le réseau ;

– la perte de contrôle de la machine.

Troyen	Port
TransScout	2002
TransScout	2003
TransScout	2004
TransScout	2005
Ripper	2023
Bugs	2115
HVL Rat5	2283
Striker	2565
SpySender	1807
Shockrave	1981
BackDoor	1999
TransScout	1999
TransScout	2000
TransScout	2001
Trojan Cow	2001

Tableau 2.1. *Exemples de troyens avec les ports concernés*

2.3.5.3. *Exemples*

Le tableau 2.1 présente des exemples connus de chevaux de Troie avec les ports appropriés qu'ils arrivent à ouvrir sans que l'utilisateur en soit conscient afin de créer des canaux cachés de communication.

2.3.6. *Espiogiciel (*spyware*)*

Un logiciel espion (aussi appelé mouchard ou espiogiciel ; en anglais *spyware*) est un logiciel malveillant qui s'installe dans un ordinateur ou un appareil mobile, dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est fortement associé à Internet qui lui sert de moyen de transmission de données.

Un *spyware* est un logiciel destiné à découvrir les habitudes de navigation d'un utilisateur. Installés en même temps qu'un petit logiciel gratuit téléchargé sur Internet ou reçu par email, les *spywares* se lancent généralement au démarrage du système et s'exécutent en tâche de fond, s'appropriant une partie des ressources du système. Sa fonction essentielle est de collecter un maximum d'informations sur les habitudes de navigation (voire les achats) de l'utilisateur de la machine afin d'en dresser un profil détaillé.

Certains espiogiciels utilisent les cookies afin de collecter les données relatives aux utilisateurs concernés dans le cas où les navigateurs permettent d'activer de telles options.

Les profils ainsi dressés, à l'insu des utilisateurs et donc sans autorisations préalables, sont ensuite utilisés pour envoyer de la publicité ciblée (modifications des pages affichées, ajouts de liens), voire sont revendus sous forme de fichiers de prospects qualifiés pour des campagnes d'emailing...

EXEMPLES. Adayairespy, AdwarePunisher, AdwareSheriff, AlphaCleaner, AVGold, BargainBuddy, BraveSentry, MalwareWipe, PestTrap, PSGuard, Quicknavigate.com, Security iGuard, Smitfraud, SpyAxe, SpyGuard, Spy Heal, SpySheriff, Spyware Soft Stop, Spyware Vanisher, SpywareQuake, SpywareSheriff, Startsearches.net, UpdateSearches.com, Virtual Maid, Win 32.puper, WinHound.

2.3.7. Keylogger

Un enregistreur de frappe (en anglais, *keylogger*) est un logiciel espion ou un périphérique qui espionne électroniquement l'utilisateur d'un ordinateur. Le but de cet outil est d'espionner l'intimité informatique de l'utilisateur.

Un *keylogger* est un dispositif chargé d'enregistrer les frappes de touches du clavier à l'insu de l'utilisateur.

Certains *keyloggers* sont capables d'enregistrer les URL visitées, les emails consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur.

Dans la mesure où les *keyloggers* enregistrent toutes les frappes de clavier, ils peuvent servir à des personnes malintentionnées pour récupérer les mots de passe des utilisateurs du poste de travail. Cela signifie donc qu'il faut être particulièrement vigilant lorsque vous utilisez un ordinateur en lequel vous ne pouvez pas avoir confiance (poste en libre accès dans une entreprise, une école ou un lieu public).

2.3.8. Adware

Un *adware* est un type de logiciel malveillant qui vous inonde de fenêtres publicitaires sans fin, potentiellement dangereuses pour votre appareil. Il permet à son éditeur de générer des revenus publicitaires et qui est le plus souvent installé à l'insu de l'internaute, lorsque celui-ci installe des logiciels de natures diverses librement disponibles en téléchargement.

EXEMPLES. 1ClickDownloader, 4-you.net Search, 7search, AnywhereMe Toolbar, Arcade Safari, Auto-Lyrics, AutoCompletePro Toolbar, BigSeek Pro Toolbar, Blekko Search, Boby Lyrics, Bomlabio, Bonanza, BrandPro files, Browse for the Cause, Browse to Save, BrowseBeyond, BrowseFox, BrowserSeek Search, Btosjs Info, Bubble Dock, Bueno Search, Buify, BuscaID Search, BuumpMe, Buzzdock, BuzzSearch, Certified Toolbar, ChatZum, Clickorati, Conduit Search, ContinueToSave, CoolLyrics, Coupon Alert Toolbar, Coupon Cactus, Coupon Caddy, Coupon Chaser, Coupon Companion, Coupon Genie, Coupon Locker, Coupon Matcher, Coupon Pigeon, Coupon Printer, Coupon Samurai, Coupon Server, Coupon Slider,

Findwide Search, First Address Bar, Gigantic Savings, Ginyas Companion, Glarysoft Toolbar, Glindorus, GlobaSearch, Goong Search, GoOnSearch, Govome Search, GreyGray, Guffins Toolbar, Hot Search Toolbar, Hotspot Shield, Ievbz Search, iLivid Search, Illoxum, iMesh Toolbar, IMinent Toolbar, Infomash Search, Kozaka, Lyrics Bot, Lyrics-Fan, LyricsSing, Nav-Links, Oyodomo.

2.3.9. *Autres* malwares

En plus des principaux *malwares* déjà présentés ci-dessus, il existe d'autres exemples de logiciels malveillants qui ne cessent de proliférer et de se renouveler sous de nouvelles formes.

– *Ransomware* : un rançongiciel est un logiciel rançonneur, logiciel de rançon ou encore logiciel d'extorsion, et un logiciel malveillant qui prend en otage des données personnelles et/ou le système. La libération de ces données/système est conditionnée par le paiement d'une somme d'argent (généralement *via* bitcoin) appelé rançon.

– *Scareware* : le *scareware* fait partie d'une classe de logiciels malveillants qui inclut les faux logiciels de sécurité, les logiciels de rançon et d'autres logiciels d'escroquerie qui suggère de payer pour télécharger de faux logiciels.

– *Phishing* : l'hameçonnage, *phishing* ou filoutage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de procéder à une usurpation d'identité.

– *Rootkits* : un *rootkit* appelé aussi « outil de dissimulation d'activité », « maliciel furtif » ou encore « trousse administrateur pirate » et parfois « kit », est un ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est d'obtenir et de prolonger un accès (généralement non autorisé) à un ordinateur de la manière la plus furtive possible.

2.3.10. *Comparaison entre quelques outils d'intrusion*

Les outils d'intrusion présentent des similitudes diverses, cependant ils admettent quelques différences qui peuvent être résumée à travers le tableau 2.2 qui permet d'identifier les caractéristiques intrinsèques, la nature de l'action malveillante en question et les symptômes de chaque outil.

Outil d'intrusion / Caractéristiques	Virus	Cheval de Troie	Ver	Bombe logique
Caractéristiques intrinsèques	Autoréplication Destruction d'information	Dissimulation dans un programme Ouverture de port	Propagation à travers le réseau	Déclenchement suite à un événement
Nature des actions (directe, indirecte)	Directe	Indirecte	Directe	Directe
Symptômes	Messages parasites Fichiers parasites	Mouvement de la souris Ouverture/fermeture des fenêtres Perte de contrôle de la machine Perturbation d'utilisation	Messages parasites Fichiers parasites	Aucun symptôme apparent jusqu'au déclenchement

Tableau 2.2. *Comparaison entre différents outils d'intrusion*

2.4. Conclusion

Bien qu'il soit simple à mettre en place, TCP/IP présente plusieurs failles de sécurité et vu son utilisation très répandue, il fallait investir en matière de sécurité afin d'éviter et de minimiser les problèmes ainsi présentés. TCP/IP est vulnérable aux outils de scan et d'analyse qui sont à la portée des utilisateurs finaux et qui offrent une très grande gamme sur Internet. Le déploiement d'un outil de scan ou d'analyse est une étape nécessaire avant de procéder à l'attaque.

De telles failles facilitent la propagation et l'attaque par les outils d'intrusion. Les outils d'intrusion et les *malwares* d'une façon générale sont des programmes d'attaque créés afin de perturber le fonctionnement d'un système. Quatre familles d'intrusion existent (virus, cheval de Troie, ver, bombe logique), cependant on peut avoir des outils d'intrusion hybrides, c'est-à-dire qui cochent les caractéristiques de plusieurs familles, ce sont des outils aux conséquences plus graves et plus complexes. Le développement du génie logiciel a aussi facilité la création des outils d'espionnage commandés par les intrus.

Chapitre 3

Techniques et outils d'authentification

3.1. Introduction

L'authentification constitue une caractéristique de base de la sécurité, elle permet de définir les droits d'accès et d'identifier les sources d'attaques en cas de problème. Elle permet de contrôler et limiter les accès aux différents services en local ou à distance. L'authentification est un mécanisme-clé de sécurité puisqu'elle constitue la première barrière de sécurité contre les attaques potentielles. Le défi le plus important pour un attaquant est de retrouver le mot de passe, ce qui lui permet de faire ce qu'il veut et de mettre en cause le système en question.

L'authentification s'effectue à travers trois techniques possibles :

– la première technique, appelée « je possède », est liée à la possession d'un objet qui représente une preuve d'identité, c'est le cas d'un badge, d'une carte. Cette technique est utilisée le plus souvent pour assurer la sécurité physique et contrôler l'accès aux locaux critiques ;

– la deuxième technique, appelée « je sais », est liée à la connaissance d'une combinaison secrète, c'est le mot de passe. Cette dernière est la plus utilisée pour assurer l'authentification au niveau du système informatique ;

– la troisième technique, appelée « je suis », est l'authentification la plus forte dans la mesure où elle est dépendante d'une caractéristique propre de la personne qui doit s'authentifier (empreinte, parole, etc.).

Dans certains cas de figure, plusieurs techniques peuvent être combinées pour une meilleure sécurité, c'est le cas de la carte bancaire (« je possède » la carte et « je sais » le code).

Le mot de passe doit admettre un certain nombre de critères afin d'empêcher sa divulgation qui représentera des effets néfastes sur le système ou l'entité à sécuriser, il doit d'autre part avoir une durée de vie limitée.

Afin d'assurer l'authentification d'une façon centralisée et contrôlée, le service AAA a vu le jour, il offre un certain nombre de fonctionnalités complémentaires qui assure aussi l'autorisation et le suivi des accès.

L'authentification en tant que service de sécurité peut se faire à un équipement réseau sans aucun besoin de serveur AAA, et ce *via* les protocoles Telnet et SSH. Ce type d'authentification admet des limites liées à la base de données des comptes utilisables pour assurer l'accès et la sécurité de la configuration elle-même. De ce fait, la configuration d'un serveur AAA permet de résoudre les insuffisances ci-dessus et assure de nouvelles fonctionnalités, en l'occurrence l'autorisation et la comptabilité.

Le service AAA peut utiliser une base de données locale utilisable seulement pour l'authentification ou une base de données distante utilisable pour assurer les trois fonctionnalités (authentification, autorisation et comptabilité). On distingue deux modes AAA possibles : en local et sur serveur.

3.2. Concepts théoriques de l'authentification

Afin d'éviter les confusions, on doit distinguer l'authentification de l'identification, deux termes ayant des significations différentes et représentant deux aspects complémentaires. Ces deux aspects peuvent être assurés d'une façon couplée ou séparément.

3.2.1. *Identification*

C'est le fait de s'identifier parmi d'autres en présentant son identité qui peut être sous forme de nom, adresse IP, adresse physique, adresse Mac. L'entité utilisée pour s'identifier doit être unique dans son contexte pour pouvoir la distinguer, c'est le cas du *login* ou tout autre identifiant de l'utilisateur.

3.2.2. *Authentification*

C'est une preuve d'identité à travers plusieurs techniques et moyens permettant d'assurer que l'entité ayant telle identité est réellement l'entité en question.

3.3. Différents types d'authentification

Selon l'entité à authentifier et son emplacement sur le réseau, il existe deux types d'authentification différents, en local et à distance.

3.3.1. *Authentification à un service local*

Pour accéder à un service local, le moyen d'authentification le plus utilisé est par *login* et mot de passe. Le *login* est unique pour s'identifier et le mot de passe est secret pour s'authentifier.

Un mot de passe doit respecter un certain nombre de caractéristiques :

– avoir une taille raisonnable qui dépend de l'importance de l'entité à sécuriser ;

– avoir un contenu diversifié (lettres majuscules et minuscules, chiffres et caractères spéciaux) ;

– éviter les mots de passe simples ;

– éviter les mots de passe issus du dictionnaire ;

– éviter les mots de passe trop complexes et difficiles à mémoriser sans être obligé de l'écrire sur un support physique ou magnétique ;

– modifier périodiquement le mot de passe, et ce suivant son importance et son utilisation ;

– éviter la double utilisation d'un mot de passe (le compte email et la carte de crédit).

Exemple de mot de passe réaliste : teurn@dior2(C)21 (un mot de passe issu du mot ordinateur avec inversement de syllabes et en remplaçant le chiffre « 0 » par la chaîne « (C) », ce qui engendre un mot de passe complexe mais facile à retenir sans besoin d'être transcrit sur support numérique ou physique).

Afin d'éviter toute connexion frauduleuse issue du tâtonnement, les systèmes de connexion exigent de saisir une clé (apparente sous forme d'image) pour s'assurer que le login et le mot de passe donnés ont été saisis manuellement.

Certains systèmes d'authentification peuvent être vulnérables ou subir des attaques de type injection SQL ; cette dernière permet de ne pas renseigner le mot de passe s'il contient un caractère spécial qui représente le caractère utilisé pour le commentaire (« # », « ' » ou autres).

3.3.2. *Authentification à travers le réseau*

Afin d'accéder à un service distant, chaque utilisateur doit s'authentifier, le mot de passe nécessaire à l'authentification ne doit jamais être transmis en clair sur le réseau. En effet, toute information qui circule à travers le réseau peut être capturée par un observateur (*sniffer*). C'est l'unique défi à relever lors de la manipulation.

3.3.2.1. *Problématique de l'authentification à distance*

Pour accéder à un service distant à travers le réseau, le moyen d'authentification le plus utilisé et le plus simple est d'envoyer son *login* et son mot de passe en clair sur le réseau comme le présente la figure 3.1.

Cette technique permet d'assurer à la fois l'identification et l'authentification. C'est le cas d'une grande panoplie de webmails jusqu'aux premières années du XXI^{e} siècle.

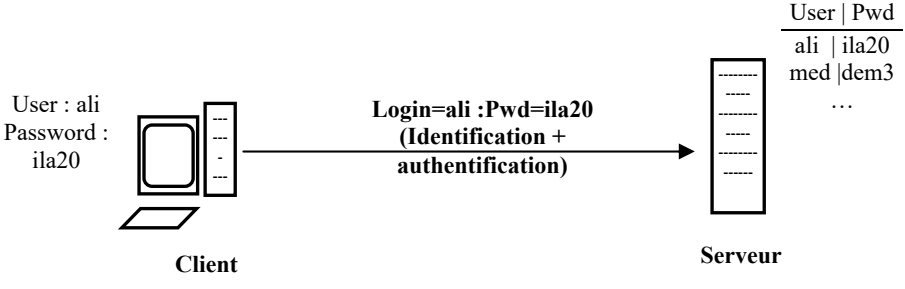

Figure 3.1. *Authentification par login et mot de passe en clair*

En utilisant un analyseur réseau, il devient facile de détecter le mot de passe, ce qui permet de mettre en cause la sécurité. Il fallait de ce fait éviter l'utilisation de cette technique.

Pour s'authentifier à travers le réseau d'une façon sécurisée, il fallait éviter d'envoyer son mot de passe en clair sur le réseau.

3.3.2.2. *Authentification à distance par message de défi*

L'authentification à distance consiste à s'identifier en premier lieu puis de s'authentifier en utilisant le résultat d'une fonction de hachage appliquée à une combinaison de *login*, de mot de passe et d'un message de défi aléatoire envoyé par le serveur lors de l'authentification. Elle se fait en plusieurs phases :

– le client envoie son *login* au serveur pour s'identifier ;

– le serveur vérifie la validité du *login* ;

– en cas d'identification correcte, le serveur génère aléatoirement un message de défi et l'envoie au client ;

– le client génère une chaîne de caractères en se basant sur les trois éléments : *login*, mot de passe et message de défi. Puis, il calcule *via* une fonction de hachage appropriée à partir de la chaîne ainsi générée une chaîne qui sera envoyée au serveur ;

– le serveur exécute à nouveau la tâche de calcul en utilisant la même fonction de hachage appliquée à la même combinaison (*login* identifié, mot de passe associé mémorisé au niveau du serveur et message de défi envoyé au client). Par la suite, il compare le résultat à celui envoyée par le client. En cas d'égalité, le client sera authentifié.

L'utilisation d'un message de défi différent d'une connexion à une autre permet d'éviter la réutilisation du *hashcode* dans une authentification frauduleuse par la suite.

Un hacker qui observe le réseau arrive à détecter le *login*, le defmesg et le *hashcode*. Ces paramètres ne sont pas suffisants pour pouvoir extraire le *password* même dans le cas où il connaît la formule de combinaison des différents éléments (*login*, *password* et defmesg) et la fonction de hachage utilisée.

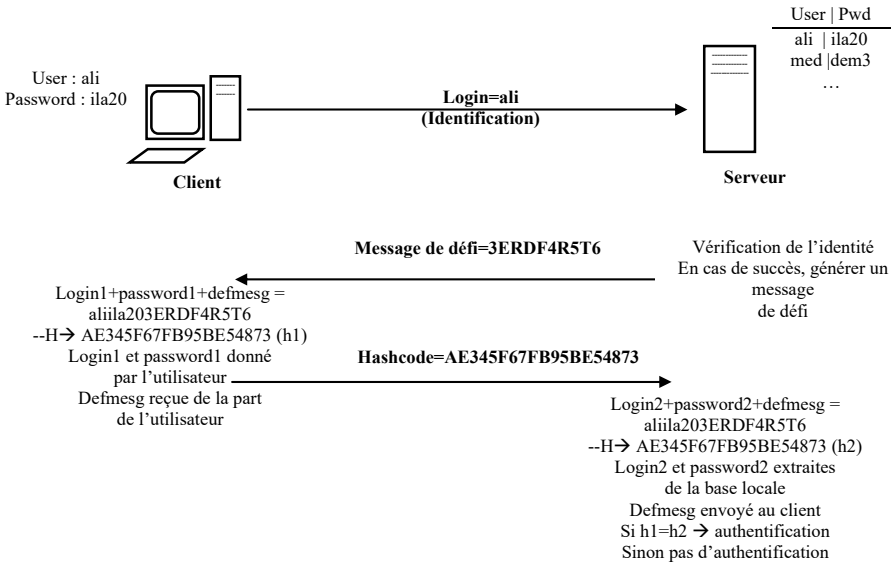

Figure 3.2. *Authentification par message de défi*

3.3.2.3. *Authentification à distance par mot de passe à utilisation unique*

Appelée en anglais *one-time used password*, cette technique se base aussi sur l'utilisation d'une fonction de hachage, elle consiste à changer de mot passe d'une connexion à une autre avec les conditions suivantes :

– les mots de passe sont générés à partir d'un mot de passe racine qui sera le dernier à avoir été utilisé ;

– un mot de passe déjà utilisé est extrait du mot de passe qui suit ;

– les mots de passe déjà utilisés ne peuvent en aucun cas permettre d'extraire un quelconque mot de passe de ceux qui seront utilisés ultérieurement.

Étant donné H une fonction de hachage et n un entier très grand, ce qui permet de s'authentifier n+1 fois en utilisant un seul mot de passe racine choisi :

– la première authentification s'effectue en utilisant un mot de passe par application de la fonction H n fois au mot de passe racine ;

– la deuxième authentification s'effectue en utilisant un mot de passe par application de la fonction H (n-1) fois au mot de passe racine ;

– la $n^{ième}$ authentification s'effectue en utilisant un mot de passe par application de la fonction H une seule fois au mot de passe racine ;

– la dernière authentification s'effectue en utilisant le mot de passe racine.

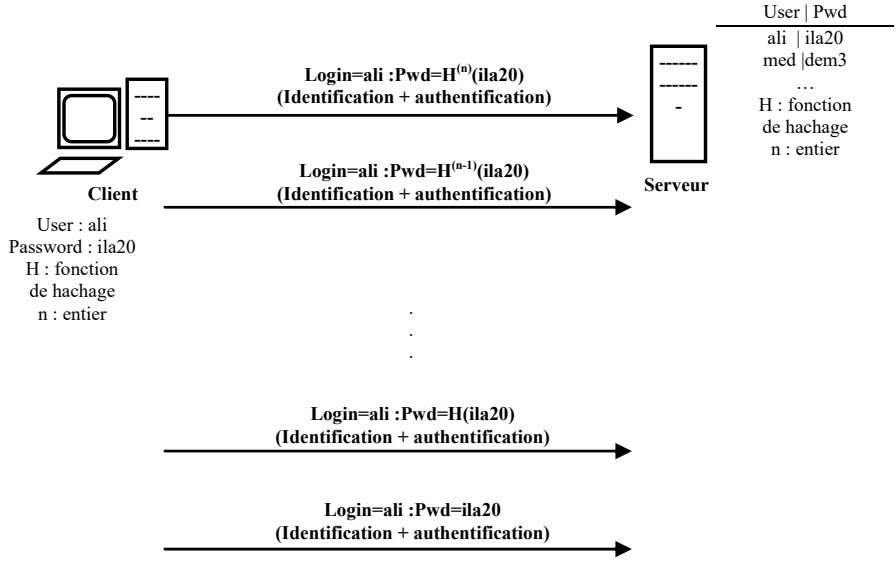

Figure 3.3. *Authentification par one-time used password*

Un observateur réseau et même s'il récupère tous les mots de passe déjà utilisés ne sera pas capable de les utiliser ni de récupérer à partir d'eux le mot de passe racine choisi par l'utilisateur.

3.3.2.4. *Telnet et SSH*

Telnet et SSH sont deux protocoles réseau qui sont utilisés pour accéder à un ordinateur distant en se connectant à ce système au sein d'un réseau, avec les émulateurs terminaux ou sur Internet, et ce pour contrôler ce système à l'aide de commandes à distance.

Telnet est un protocole d'accès distant à un serveur ou un équipement quelconque (routeur, switch, etc.) dont le mot de passe est transmis en clair à travers le réseau donnant la possibilité à un utilisateur du réseau et moyennant un simple *sniffer* de le capturer et de l'utiliser pour un éventuel accès frauduleux.

SSH, acronyme de *secure shell*, est un protocole similaire plus sécurisé dont la mesure ou le mot de passe ne peut plus être capturé à travers le réseau.

Sous un équipement Cisco, il est possible de limiter l'accès distant au protocole Telnet à travers la configuration suivante :

```
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#transport input telnet
```

ou de limiter l'accès distant au protocole SSH à travers la configuration suivante :

```
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#transport input ssh
```

Sous un équipement Huawei, il est possible de limiter l'accès distant au protocole Telnet à travers la configuration suivante :

```
[Huawei]user-interface vty 0 4
[Huawei-ui-vty0-4]protocol inbound telnet
```

ou de limiter l'accès distant au protocole SSH à travers la configuration suivante :

```
[Huawei]user-interface vty 0 4
[Huawei-ui-vty0-4]protocol inbound ssh
```

3.4. Service AAA

AAA est l'acronyme de *authentication*, *authorization*, *accounting*.

L'authentification (*authentication*) est une fonctionnalité permettant de valider l'identité dans l'objectif de limiter l'accès à un système bien défini. Elle répond à la question : « Qui êtes-vous ? »

L'autorisation (*authorization*) est une fonctionnalité permettant de déterminer les services auxquels une entité authentifiée peut accéder dans l'objectif de limiter les droits d'accès. Elle répond à la question : « Quels droits avez-vous ? »

La comptabilité ou encore l'enregistrement (*accounting*) est une fonctionnalité permettant d'enregistrer toutes les activités (accès et tâches effectuées) dans l'objectif d'assurer la traçabilité pour toute éventuelle analyse. Elle répond à la question : « Qu'est-ce que vous avez fait ? »

AAA peut être configurée en local ou en se basant sur des données d'authentification hébergées sur un serveur distant.

3.4.1. *AAA en local*

AAA en local admet une seule fonctionnalité, celle de de l'authentification.

L'authentification AAA en mode local se compose des étapes suivantes :

– l'utilisateur établit une connexion avec l'équipement ;

– l'équipement demande à l'utilisateur un nom d'utilisateur et un mot de passe, authentifiant l'utilisateur à l'aide d'une base de données locale.

L'authentification AAA locale doit être configurée pour les réseaux de taille réduite. Ce sont les réseaux admettant un ou deux routeurs qui donnent accès à un nombre limité d'utilisateurs.

Cette méthode utilise les noms d'utilisateur et mots de passe locaux stockés sur un routeur. L'administrateur système doit remplir la base de données de sécurité locale en spécifiant les profils de nom d'utilisateur et de mot de passe pour chaque utilisateur susceptible de se connecter.

La méthode d'authentification locale AAA est similaire à l'utilisation de la commande de connexion locale. AAA fournit également un moyen de configurer les méthodes de sauvegarde de l'authentification.

3.4.1.1. *Configuration authentification AAA en mode local*

Sur un routeur Cisco, la configuration de l'authentification AAA en mode local consiste à créer des utilisateurs, à activer le service AAA et à spécifier la base de données locale (sensible à la casse) comme méthode pour la liste par défaut pour l'authentification en *logins*.

```
Router(config)#username Bairam secret cisco
Router(config)#username Iyed password class
Router(config)#username Elaa password test
Router(config)#aaa new-model
Router(config)#aaa authentication login default local-
case
```

Il est aussi possible de créer une méthode d'authentification nommée utilisant la base de données locale plus le mot de passe *enable* et fixant le champ d'application de cette méthode (accès distant SSH).

```
Router(config)#aaa authentication login AUTH-SSH local
enable
Router(config)#line vty 0 4
Router(config)#login authentication AUTH-SSH
```

La syntaxe générale de la configuration d'une méthode d'authentification est :

```
Router(config)#aaa authentication login {default|NOM-
LISTE} méthode1 [méthode2] ...
```

Les méthodes locales possibles à appliquer sont :

– *enable* : consiste à utiliser le mot de passe *enable* pour s'authentifier ;

– *local* : consiste à utiliser la base de données locale des utilisateurs pour s'authentifier ;

– *local-case* : consiste à utiliser la base de données locale des utilisateurs (sensible à la casse) pour s'authentifier ;

– *none* : aucune authentification n'est utilisée.

Sur un routeur Huawei, la configuration de l'authentification AAA en mode local consiste à activer le service AAA, à créer des utilisateurs, à créer un schéma d'authentification et à spécifier le mode local pour cette dernière.

```
[Huawei]aaa
[Huawei-aaa]local-user Bairam password cipher huawei
[Huawei-aaa]local-user Iyed privilege level 12
password cipher haina
[Huawei-aaa]local-user Elaa password cipher test
[Huawei-aaa]authentication-scheme LISTE-AUTHEN
[Huawei-aaa-authen-LISTE-AUTHEN]authentication-mode
local
```

Cette méthode d'authentification peut être appliquée comme exemple pour l'accès distant à l'équipement à travers :

```
[Huawei]user-interface vty 0 4
[Huawei-ui-vty0-4]authentication-mode aaa
```

3.4.2. *AAA sur serveur*

L'authentification AAA sur serveur est composée des étapes suivantes :

1) l'utilisateur établit une connexion avec l'équipement ;

2) l'équipement demande à l'utilisateur un nom d'utilisateur et un mot de passe ;

3) l'équipement transmet le nom d'utilisateur et le mot de passe à un serveur ;

4) le serveur authentifie l'utilisateur selon la base de données hébergée.

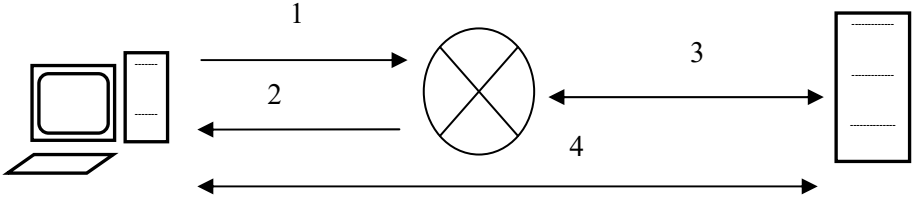

Figure 3.4. *Authentification AAA sur serveur*

La communication entre l'équipement réseau, en l'occurrence un routeur, et le serveur de sécurité AAA est gérée par l'un des protocoles :

– RADIUS : un protocole standard ;

– TACACS+/HWTACACS : un protocole propriétaire Cisco/un protocole propriétaire Huawei.

Une comparaison entre les protocoles est dressée dans le tableau 3.1.

	RADIUS	TACACS+/HWTACACS
Fonctionnalité	Combine l'authentification et l'autorisation mais sépare la comptabilité. Ce qui autorise moins de flexibilité	Sépare AAA selon son architecture. Assure la modularité de l'implémentation du serveur de sécurité
Standard	Ouvert (standard RFC)	Propriétaire Cisco/Huawei
Protocole de niveau transport	UDP	TCP
Authentification CHAP	Défi unidirectionnel et réponse du serveur de sécurité RADIUS au client RADIUS	Défi bidirectionnel
Protocoles supportés	ARA et NetBEUI non supportés	Tous les protocoles
Confidentialité	Chiffrement du mot de passe seulement	Chiffrement du paquet entier
Personnalisation	Aucune option d'autorisation des commandes du routeur par utilisateur ou par groupe	Autorise les commandes du routeur par utilisateur ou par groupe
Comptabilité	Étendue	Limitée

Tableau 3.1. *Comparaison RADIUS et TACACS+/HWTACACS*

On s'intéresse dans cette partie à la configuration des serveurs nécessaires et à l'activation des méthodes d'authentification appropriées, et ce respectivement sur un équipement Cisco et un équipement Huawei.

3.4.2.1. *Authentification AAA sur serveur sous Cisco*

La configuration de l'authentification AAA sur serveur avec CLI (*Command Line Interface*) s'effectue à travers les étapes suivantes :

1) activer AAA ;

2) spécifier l'adresse IP du serveur ACS ;

3) configurer la clé secrète ;

4) configurer l'authentification pour utiliser le serveur RADIUS ou TACACS +.

L'activation du service AAA s'effectue à travers :

```
Router(config)#aaa new-model
Router(config)#
```

La configuration du serveur TACACS+ et RADIUS consiste à :

```
Router(config)#tacacs server LE-SERVEUR-T
Router(config-server-tacacs)#address ipv4 192.168.1.10
Router(config-server-tacacs)#single-connection
Router(config-server-tacacs)#key TACACS-P@55w0rd
Router(config-server-tacacs)#exit
Router(config)#
Router(config)#radius server LE-SERVEUR-R
Router(config-radius-server)#address ipv4 192.168.1.11
auth-port 1812 acct-port 1813
Router(config-radius-server)#key RADIUS-P@55w0rd
Router(config-radius-server)#exit
Router(config)#
```

La création d'une méthode d'authentification par défaut permettant d'utiliser le protocole RADIUS se fait à travers la configuration :

```
Router(config)# aaa authentication login default group
radius
```

Pour TACACS+, on donne comme exemple la création d'une méthode d'authentification nommée à travers la commande suivante :

```
Router(config)# aaa authentication login AUTH-TACACS
group tacacs+
```

3.4.2.2. *Authentification AAA sur serveur sous Huawei*

La configuration du serveur RADIUS s'effectue avec les commandes suivantes :

```
[HUAWEI] radius-server template SERVER-R
[HUAWEI-radius-SERVER-R] radius-server authentication
10.7.66.66 1812 weight 80
[HUAWEI-radius- SERVER-R] radius-server accounting
10.7.66.66 1813 weight 80
[HUAWEI-radius-SERVER-R] radius-server shared-key
cipher Radius@2020
[HUAWEI-radius-SERVER-R] radius-server retransmit 2
[HUAWEI-radius-SERVER-R] undo radius-server user-name
domain-included
[HUAWEI-radius-SERVER-R] quit
```

L'activation de l'authentification RADIUS consiste à créer un schéma d'authentification nommé AUTH-R et configurer le schéma d'authentification pour utiliser l'authentification RADIUS comme mode d'authentification actif :

```
[HUAWEI]aaa
[HUAWEI-aaa] authentication-scheme AUTH-R
[HUAWEI-aaa-authen-AUTH-R] authentication-mode radius
[HUAWEI-aaa-authen-AUTH-R] quit
```

La configuration du serveur HWTACACS s'effectue avec les commandes suivantes :

```
[HUAWEI] hwtacacs-server template SERVER-T
[HUAWEI-hwtacacs-SERVER-R] hwtacacs-server
authentication 10.7.66.66 49
[HUAWEI-hwtacacs-SERVER-R] hwtacacs-server
authorization 10.7.66.66 49
[HUAWEI-hwtacacs-SERVER-R] hwtacacs-server accounting
10.7.66.66 49
[HUAWEI-hwtacacs-SERVER-R] hwtacacs-server shared-key
cipher Hwtacacs@2020
[HUAWEI-hwtacacs-SERVER-R] quit
```

L'activation de l'authentification HWTACACS consiste à créer un schéma d'authentification nommé AUTH-T et configurer le schéma d'authentification pour utiliser l'authentification HWTACACS comme mode d'authentification actif :

```
[HUAWEI]aaa
[HUAWEI-aaa] authentication-scheme AUTH-T
[HUAWEI-aaa-authen-AUTH-T] authentication-mode
hwtacacs
[HUAWEI-aaa-authen-AUTH-T] quit
```

3.4.2.3. *Configuration autorisation et comptabilité AAA sur serveur*

L'autorisation permet ou interdit l'accès des utilisateurs authentifiés à certaines zones et certains programmes du réseau par comparaison à l'authentification qui garantit qu'un appareil ou un utilisateur final est légitime.

TACACS+/HWTACACS permet de séparer l'authentification de l'autorisation, tandis que RADIUS ne sépare pas l'authentification de l'autorisation.

Sous Cisco, la syntaxe générale de la configuration d'une méthode d'autorisation est comme suit :

```
Router(config)#aaa authorization
{network|exec|commands level} {default|NOM-LISTE}
méthode1 [méthode2] ...
```

Et celle d'une méthode de comptabilité est comme suit :

```
Router(config)#aaa accounting
{network|exec|connection} {default|NOM-LISTE} {start-
stop|stop-only|none} [broadcast] méthode1 [méthode2]
...
```

Par exemple, la création d'une méthode d'autorisation et de comptabilité s'effectue à travers les commandes suivantes, et ce en utilisant respectivement le protocole RADIUS et TACACS+ :

```
Router(config)#aaa authorization exec default group
radius
```

```
Router(config)#aaa accounting exec ACCT-METH stat-stop
group tacacs+
```

Sous Huawei, la création d'un schéma d'autorisation nommé AUTHORIZ-T est suivie de la configuration du schéma d'autorisation utilisant l'autorisation HWTACACS comme mode d'autorisation :

```
[HUAWEI-aaa] authorization-scheme AUTHORIZ-T
[HUAWEI-aaa-author-AUTHORIZ-T] authorization-mode
hwtacacs
[HUAWEI-aaa-author-AUTHORIZ-T] quit
```

La création d'un schéma de comptabilité nommé ACCT-R est suivie de la configuration du schéma d'autorisation utilisant l'autorisation RADIUS comme mode d'autorisation :

```
[HUAWEI-aaa] authorization-scheme ACCT-R
[HUAWEI-aaa-author-ACCT-R] authorization-mode radius
[HUAWEI-aaa-author-ACCT-R] accounting start-fail
online
[HUAWEI-aaa-author-ACCT-R] quit
```

3.5. Conclusion

L'authentification, qu'elle soit en mode local ou à travers le réseau, doit se faire d'une façon sécurisée en choisissant un mot de passe réaliste et en utilisant des techniques évitant de transmettre le mot de passe en clair.

L'authentification est généralement couplée avec l'intégrité. On parle de l'authenticité, cette dernière permet de s'assurer à la fois de l'identité de l'émetteur ou du générateur d'une part et de la validité des données transmises ou générées d'autre part.

Le service AAA qu'on vient d'aborder dans le présent chapitre permet de gérer d'une façon méthodique et modulaire l'accès aux différents équipements et services et de tracer toutes ces activités. La configuration de ces services sur les différents équipements représente une mesure de sécurité très importante généralement négligée par les responsables au détriment de méthodes limitées et caduques d'authentification.

Chapitre 4

Techniques de contrôle d'accès, ACL et *firewall*

4.1. Introduction

Le trafic réseau ne cesse de croître d'une façon importante en rendant la charge des routeurs pour véhiculer les données de plus en plus difficile et la quantité des données de plus en plus volumineuse.

De plus, une grande partie de ces informations constitue des éléments parasites menés par les pirates et les entités non autorisées. La solution convenable à ceci consiste à filtrer le trafic et permettre seulement les entités légitimes à communiquer à travers le réseau, ce qui limite la quantité de données traitées d'une part et élimine les sources potentielles d'attaque. Ces filtres configurables sur les routeurs s'appellent des ACL.

Pour protéger un emplacement critique (labo, salle de contrôle) au niveau d'une organisation, il fallait isoler et suivre les accès à cet emplacement. En informatique, les mesures sont similaires pour sécuriser un système, et ce à travers un *firewall* qui permet de l'isoler et de suivre les accès. Le *firewall* représente l'outil de sécurité le plus important, c'est l'élément-clé dans toute mesure de sécurité.

De plus, le principe de *firewalling*, et plus précisément le filtrage, est présent au niveau de plusieurs outils de sécurité, en l'occurrence les équipements d'interconnexion réseau (routeur, commutateur de niveau 3) à travers les listes de contrôle d'accès (ACL).

4.2. Liste de contrôle d'accès

ACL est l'acronyme de *Access Control List*, ou encore liste de contrôle d'accès (LCA), il représente une liste ordonnée de filtres appelée *Access Control Entry* (ACE) qui s'applique à un trafic sortant ou entrant au niveau d'une interface LAN/WAN d'un routeur.

Les ACL permettent de filtrer des paquets suivant des critères définis par l'utilisateur. Il assure le filtrage des paquets entrant ou sortant d'une patte d'un routeur en fonction :

– de l'IP source ;

– de l'IP destination ;

– du port source ;

– du port destination ;

– du protocole : IP, TCP, UDP, ICMP, etc.

Une liste de contrôle d'accès est un script de configuration de routeur contrôlant l'autorisation ou le refus de passage des paquets ou éventuellement les trames, conformément aux critères stipulés dans leur en-tête. Elles servent également à sélectionner le type de trafic à analyser, transmettre ou traiter selon d'autres méthodes.

Au niveau d'un routeur, une seule ACL peut être définie par protocole, par interface et par direction :

– protocole (IPv4, IPv6) ;

– interface (GigabitEthernet0/0, etc.) ;

– direction (sens du trafic : entrant ou sortant).

4.2.1. *Classifications des ACL*

Il existe trois classifications possibles des ACL, et ce selon le sens de trafic concerné par l'ACL, selon le type même de l'ACL (sa structure et sa complexité) ou encore selon la façon dont est définie l'ACL (numérotée ou nommée).

4.2.1.1. *ACL entrante/sortante*

Les listes de contrôle d'accès peuvent s'appliquer au trafic entrant ou sortant :

– listes de contrôle d'accès entrantes : les paquets entrants sont traités avant d'être routés vers l'interface de sortie. Une liste de contrôle d'accès entrante est efficace car elle réduit la charge des recherches de routage en cas d'abandon du paquet. Si le paquet est autorisé à l'issue des tests, il est soumis au routage ;

– listes de contrôle d'accès sortantes : les paquets entrants sont routés vers l'interface de sortie puis traités par le biais de la liste de contrôle d'accès sortante.

4.2.1.2. *ACL standard/étendue*

Il existe deux types principaux d'ACL définies selon les critères utilisés pour assurer le routage, on distingue :

– les listes de contrôle d'accès standard : admettant des filtres basés uniquement sur les IP sources. On utilise l'appellation basique pour les équipements Huawei ;

– les listes de contrôle d'accès étendu : admettant des filtres basés sur quasiment tous les champs des en-têtes IP, TCP et UDP. On utilise l'appellation avancée pour les équipements Huawei.

Pour les routeurs Huawei, il est aussi possible de définir les ACL selon l'adresse Mac, il s'agit des ACL niveau 2 (*layer 2 ACL*).

4.2.1.3. *ACL numérotée/nommée*

Lors de la définition d'une ACL, on peut soit lui affecter un nom soit lui affecter un numéro, on distingue :

– ACL numérotée : l'ACL sera identifiée par un numéro choisi lors de sa définition :

- sous Cisco, le numéro permet d'identifier le type d'ACL comme ci-joint :
  - (1 à 99) et (1300 à 1999) : liste de contrôle d'accès IP standard ;
  - (100 à 199) et (2000 à 2699) : liste de contrôle d'accès IP étendue ;
- sous Huawei, le numéro permet d'identifier le type d'ACL comme ci-joint :

- 2000-2999 : liste de contrôle d'accès IP basique ;

- 3000-3999 : liste de contrôle d'accès IP avancée ;

- 4000-4999 : liste de contrôle d'accès IP de niveau 2 ;

– ACL nommée : l'ACL sera identifiée par un nom choisi lors de sa définition en indiquant son type (standard ou étendue) :

- les noms peuvent comporter des caractères alphanumériques ;

- il est recommandé d'écrire le nom en majuscules ;

- les noms ne peuvent pas contenir d'espaces ou de marques de ponctuation, ils doivent commencer par une lettre ;

- on peut ajouter ou supprimer des entrées dans la liste de contrôle d'accès.

4.2.2. *Configuration des ACL sous Cisco*

Une liste de contrôle d'accès est un ensemble séquentiel et ordonné d'instructions d'autorisation ou de refus, appelées entrées de contrôle d'accès (ACE).

Lorsque le trafic réseau traverse une interface configurée avec une liste de contrôle d'accès, le routeur compare les informations figurant dans le paquet à chaque règle de l'ACL, l'action spécifiée par la première ACE qui correspond sera appliquée au paquet en question.

4.2.2.1. *Masque générique*

Une entrée de contrôle d'accès IPv4 comprend l'utilisation d'un masque générique afin de filtrer les adresses IPv4.

Un masque générique prend la forme d'une adresse IPv4, les bits qui le constituent seront interprétés comme suit :

– un bit à 0 : permet d'établir une correspondance avec la valeur du bit de l'adresse IP correspondant ;

– un bit à 1 : permet d'ignorer la valeur du bit de l'adresse IP correspondant.

Comme exemples de masques génériques associés à l'adresse IP 192.168. 1.1, on distingue :

– 0.0.0.255 : permet d'ignorer le dernier octet, ce qui permet d'accepter toutes les adresses du réseau 192.168.1.0/24 ;

– 0.0.0.7 : permet d'ignorer les trois derniers bits, ce qui permet d'accepter toutes les adresses du réseau 192.168.0/29 ;

– 0.0.0.254 : permet d'ignorer les sept premiers bits du dernier octet, ce qui permet d'accepter toutes les adresses impaires du réseau 192.168.1.0/24 ;

– 0.0.0.0 : permet de vérifier la correspondance totale des bits (aucun bit à ignorer), ce qui permet d'accepter seulement l'adresse 192.168.1.1 ;

– 255.255.255.255 : permet d'ignorer tous les bits, ce qui permet d'accepter toutes les adresses IP.

La maque générique 0.0.0.0, permettant d'accepter une seule adresse, peut être remplacée par le mot host.

La maque générique 255.255.255.255, permettant d'accepter toutes les adresses, peut être remplacée par le mot any.

4.2.2.2. *Configuration des ACL numérotées*

Le numéro attribué à l'ACL permet d'indiquer le type de l'ACL :

– de 1 à 99 et 1300 à 1999 : concerne les ACL standards ;

– de 100 à 199 et de 2000 à 2699 : concerne les ACL étendues.

La syntaxe générale est :

```
R(config)#access-list NUM-ACL {permit|deny} ...
```

Comme exemples d'ACL standards :

```
R(config)#access-list 10 permit 192.168.1.0 0.0.0.255
R(config)#access-list 11 permit host 192.168.2.1
R(config)#access-list 11 permit host 192.168.3.254
R(config)#access-list 12 deny any
```

– l'ACL 10 autorise les paquets dont l'adresse source appartient au réseau 192.168.1.0/24 ;

– l'ACL 11 autorise seulement les paquets dont l'adresse source est soit 192.168.2.1 soit 192.168.3.254 ;

– l'ACL 12 interdit l'accès de tous les paquets indépendamment de leurs adresses sources.

Les ACL étendues assurent le filtrage selon le protocole (IP, TCP, UDP, ICMP, etc.), les adresses IP sources et destination et éventuellement des ports TCP ou UDP sources et destination. Une bonne illustration de ceci est :

```
R(config)#access-list 100 permit tcp 192.168.1.0
0.0.0.255 any eq 80
R(config)#access-list 101 deny ip any
R(config)#access-list 102 permit udp any host
192.168.4.100 eq 49
```

– l'ACL 100 permet d'autoriser les segments TCP dont l'adresse source appartenant au réseau 192.168.1.0/24 et qui représente le trafic web (relatif au port 80 qui peut être remplacé dans la configuration de l'ACL par www) ;

– l'ACL 101 permet d'interdire tout le trafic IP ;

– l'ACL 102 permet d'autoriser le trafic UDP (port 49 correspondant au service TACACS+) orienté vers la machine 192.168.4.100.

Une entrée implicite sera rajoutée à la fin de l'ACL pour interdire le reste du trafic.

Une fois l'ACL configurée, l'administrateur doit spécifier l'emplacement (interface ou ligne d'accès d'un routeur) afin de l'appliquer. Une ACL standard sera appliquée le plus près possible de la destination et une ACL étendue sera appliqué le plus près possible de la source.

On utilise la commande ip access-group pour appliquer une ACL au niveau d'une interface selon la syntaxe suivante :

```
R(config-if)#ip access-group NUM-ACL|NOM-ACL {in|out}
```

Comme exemple de ceci, l'ACL 101 peut être appliquée au trafic entrant de l'interface GigabitEthernet 0/0/0 du routeur R comme suit :

```
R(config)#interface GigabitEthernet 0/0/0
R(config-if)#ip access-group 101 in
```

On utilise la commande ip access-class pour appliquer une ACL au niveau d'une ligne d'accès selon la syntaxe suivante :

```
R(config-line)#ip access-class NOM-ACL {in|out}
```

Comme exemple de ceci, l'ACL ADMIN-PLAGE-IP peut être appliquée afin de filtrer les machines autorisées à accéder à distance au routeur R :

```
R(config)#ip access-list
R(config)#line vty 0 4
R(config-if)#ip access-class ADMIN-PLAGE-IP in
```

4.2.2.3. *Configuration des ACL nommées*

La configuration d'une ACL nommée (qui représente la seule possibilité de configuration pour IPv6) consiste à identifier les ACL par leurs noms tout en spécifiant qu'il s'agit d'une ACL standard ou étendue.

La syntaxe générale est :

```
R(config)#ip access-list {standard|extended} NOM-ACL
```

Pour une ACL standard, les règles de filtrage seront rajoutées en utilisant la commande selon la syntaxe suivante :

```
R(config-std-nacl)#deny|permit ADRESSE-IP MASQUE-
GENERIQUE
```

Un exemple de ceci est :

```
R(config)#ip access-list standard NO-ACCESS-HOST-1
R(config-std-nacl)#deny host 192.168.1.1
R(config-std-nacl)#permit any
R(config-std-nacl)#exit
R(config)#interface g0/0
R(config-if)#ip access_group NO-ACCESS-HOST-1 out
```

Les règles (ACE : *Access Control Entry*) sont organisées d'une façon ordonnée par des identifiants commençant par 10 et par addition de 10 comme suit : 10, 20, 30, etc., et manipulées comme suit :

– suppression d'une ACE (20 par exemple) :

```
R(config-std-nacl)#no 20
```

– redéfinition d'une ACE supprimée :

```
R(config-std-nacl)#20 deny host 192.168.1.20
```

– insertion d'une ACE en mentionnant son identifiant au début :

```
R(config-std-nacl)#15 deny host 192.168.1.3
```

– ajout d'une nouvelle ACE :

```
R(config-std-nacl)#permit any
```

Ce qui permet d'obtenir la liste des ACE suivantes :

```
10 deny host 192.168.1.1
15 deny host 192.168.1.3
20 deny host 192.168.1.20
30 permit any
```

Pour une ACL étendue, les règles de filtrage seront rajoutées en utilisant la commande selon la syntaxe suivante :

```
R(config-ext-nacl)#deny|permit {ip|icmp|udp|tcp}
{ADRESSE-IP-SRC MASQUE-GENERIQUE | any | host ADRESSE-
IP-SRC} [{eq|neq|gt|lt|range} PORT(S)-SRC] {ADRESSE-
IP-DEST MASQUE-GENERIQUE | any | host ADRESSE-IP-DEST}
[{eq|neq|gt|lt|range} PORT(S)-DEST]
```

Comme exemple d'ACL nommée étendue, on se propose de créer deux listes :

– une première sera appliquée au trafic entrant de l'interface GigabitEthernet 0/0 permettant d'autoriser les machines du réseau 192.168.10.0/24 à accéder seulement au trafic web : http (port 80) et https (port 443) ;

– la deuxième liste sera appliquée au trafic sortant de la même interface, permettant d'autoriser tous les paquets IP entrants qui font partie d'une connexion déjà établie.

```
R(config)#ip access-list extended SURFING
R(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255
any eq 80
R(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255
any eq 443
R(config-ext-nacl)#exit
R(config)#ip access-list extended BROWSING
R(config-ext-nacl)#permit tcp any 192.168.10.0
0.0.0.255 established
R(config-ext-nacl)#exit
R(config)#interface g0/0
R(config-if)#ip access-group SURFING in
R(config-if)#ip access-group BROWSING out
```

4.2.2.4. *ACL IPv6*

Les ACL IPv6 sont des listes nommées uniquement et fonctionnent comme des ACL IPv4 étendues.

La configuration d'une liste de contrôle d'accès IPv6 s'effectue en trois étapes :

– à partir du mode de configuration global, on utilise la commande pour créer une liste de contrôle d'accès IPv6 :

```
R(config)#ipv6 access-list NOM-LISTE
```

– en mode de configuration des listes de contrôle d'accès nommées, on utilise les instructions `permit` ou `deny` afin de spécifier une ou plusieurs conditions pour déterminer si un paquet est transféré ou abandonné.

```
R(config-ipv6-acl)#deny | permit {ipv6|icmp|udp|tcp}
{source-ipv6/préfixe | any | host source-ipv6}
[{eq|neq|lt|gt|range} Numéro(s)-de-port(s)-source]
{destination-ipv6/préfixe | any | host destination -ipv6}
```

```
[{eq|neq|lt|gt|range} Numéro(s)-de-port(s)-
destination]
```

Une ACL IPv6 sera appliquée au trafic entrant ou sortant d'une interface en utilisant la commande :

```
R(config-if)#ipv6 traffic-filter NOM-ACL in|out
```

Comme exemple d'une ACL IPv6 :

– la première instruction nomme la liste d'accès IPv6 par NO-R3-LAN-ACCESS ;

– la seconde instruction autorise la machine 2001:DB8:CAFE:30::1 à accéder à n'importe quel service web ;

– la troisième instruction refuse tous les paquets IPv6 de 2001:DB8:CAFE:30::/64 destinés à un réseau IPv6 ;

– la quatrième instruction autorise tous les autres paquets IPv6.

```
R(config)#ipv6 access-list NO-R3-LAN-ACCESS
R(config-ipv6-acl)#permit tcp host 2001:DB8:CAFE:30::1
any eq 80
R(config-ipv6-acl)#deny ipv6 2001:DB8:CAFE:30::/64 any
R(config-ipv6-acl)#permit ipv6 any any
```

L'ACL NO-R3-LAN-ACCESS sera appliquée au trafic entrant de l'interface GigabitEthernet 0/0 avec les commandes suivantes :

```
R(config)#interface g0/0
R(config-if)#ipv6 traffic-filter NO-R3-LAN-ACCESS in
```

4.2.3. *Configuration des ACL sous Huawei*

Avec un routeur Huawei, il est possible de configurer trois types d'ACL, et ce selon le tableau 4.1.

Vous pouvez créer une ACL basée sur le numéro ou le nom. Une ACL est composée de plusieurs listes de règles contenant des clauses d'autorisation ou de refus.

Types	Plage de valeurs	Paramètres
ACL basique	2000-2999	Adresse IP source
ACL avancées	3000-3999	Adresse IP source Adresse IP destination Protocole Port source Port destination
ACL niveau 2	4000-4999	Adresse Mac

Tableau 4.1. *Types d'ACL sous Huawei*

Pour créer une ACL, vous devez spécifier les paramètres suivants :

– lors de la création d'une ACL basée sur le numéro, vous devez spécifier le numéro ACL. Le numéro ACL spécifie le type d'une ACL. Par exemple, l'ACL avec le numéro allant de 2000 à 2999 est une ACL de base, et l'ACL avec le numéro allant de 3000 à 3999 est une ACL avancée ;

– lors de la création d'une ACL basée sur le nom, vous devez spécifier le nom de l'ACL. Vous pouvez spécifier le nombre ou le type d'une ACL nommée. Si le numéro d'une ACL nommée n'est pas spécifié, le système attribue automatiquement un numéro à l'ACL nommée.

La syntaxe générale permettant de créer une ACL se fait soit en utilisant le numéro de la plage appropriée et qui reflète le type de l'ACL, soit en choisissant un nom par l'administrateur et en spécifiant le type de l'ACL ou le numéro approprié.

La première façon est :

```
[R]acl [number] <Num-ACL>
[R-acl-<type>-<NumACL>]rule permit|deny …
```

La deuxième façon est :

```
[R]acl name <Nom-ACL> basic|advance|link|user|<Num-
ACL>
[R-acl-<type>-<NumACL>]rule [<rule-id>] permit|deny …
```

Avec la commande rule, les différentes règles de filtrages seront créées en utilisant les paramètres appropriés de chaque type d'ACL.

Les règles, une fois créées, seront numérotées 5, 10, 15, 20, etc., et elles seront testées dans cet ordre pour un paquet quelconque, la première règle qui fonctionne sera appliquée. Il est possible d'intégrer des règles avec des numéros bien choisis.

La valeur du pas par défaut est de 5. Il peut être modifié par la commande :

```
[R-acl-<type>-<NumACL>]step <valeur-pas>
```

Pour rétablir le pas par défaut, on utilise la commande :

```
[R-acl-<type>-<NumACL>]undo step
```

4.2.3.1. *ACL basique*

Une ACL basique, dont la valeur possible du numéro qui lui est affectée est dans la plage de 2000 à 2999, est une ACL dont les règles de filtrage sont basées seulement sur l'adresse IP source.

La syntaxe de configuration d'une ACL basique sous Huawei est :

```
[R]acl [number] <Num-ACL(de 2000 à 2999)>
[R-acl-basic-NumACL]rule [<rule-id>] permit|deny
source <Adresse-IP> <Masque-Inverse>
[R]interface <Type-Interface> <Num-Interface>
[R-InterfaceTypeInterfaceNum]traffic-filter
inbound|outbound acl <Num-ACL>
```

Une ACL peut aussi être définie autrement en lui associant un nom. Dans ce cas-là, on doit spécifier le type de l'ACL (*basic* dans ce cas) ou en lui associant un numéro dans la plage de valeurs de 2000 à 2999.

```
[Huawei]acl name <Nom-ACL> basic|<Num-ACL(de 2000 à
2999)>
```

4.2.3.2. *ACL avancée*

Une ACL avancée, dont la valeur possible du numéro qui lui est affectée est dans la plage de 3000 à 3999, est une ACL dont les règles de filtrage sont basées

sur plusieurs paramètres : protocole, adresse IP source, adresse IP destination, port source, port destination.

La syntaxe de configuration d'une ACL basique sous Huawei est :

```
[R]acl [number] <Num-ACL(de 3000 à 3999)>
[R-acl-advance-NumACL]rule [<rule-id>] permit|deny
<Protocol> …
[R]interface <Type-Interface> <Num-Interface>
[R-InterfaceTypeInterfaceNum]traffic-filter
inbound|outbound acl <Num-ACL>
```

Une ACL peut aussi être définie autrement en lui associant un nom. Dans ce cas-là, on doit spécifier le type de l'ACL (*advance* dans ce cas) ou en lui associant un numéro dans la plage de valeurs de 3000 à 3999.

```
[R]acl name <Nom-ACL> advance |<Num-ACL(de 3000 à
3999)>
```

Vous pouvez configurer des règles ACL avancées en fonction des protocoles portés par IP. Les paramètres varient selon le type de protocole.

Lorsque le type de protocole est ICMP, le format de la commande est :

```
[R-acl-advance-NumACL]rule [ rule-id ] { deny | permit
} { protocol-number | icmp } [ destination {
destination-address destination-wildcard | any } | { {
precedence precedence | tos tos } * | dscp dscp } | {
fragment | first-fragment } | logging | icmp-type {
icmp-name | icmp-type [ icmp-code ] } | source {
source-address source-wildcard | any } | time-range
time-name | ttl-expired | vpn-instance vpn-instance-
name ] *
```

Lorsque le type de protocole est TCP, le format de la commande est :

```
[R-acl-advance-NumACL]rule [ rule-id ] { deny | permit
} { protocol-number | tcp } [ destination {
destination-address destination-wildcard | any } |
destination-port { eq port | gt port | lt port | range
port-start port-end } | { { precedence precedence |
```

```
tos tos } * | dscp dscp } | { fragment | first-
fragment } | logging | source { source-address source-
wildcard | any } | source-port { eq port | gt port |
lt port | range port-start port-end } | tcp-flag { ack
| established | fin | psh | rst | syn | urg } * |
time-range time-name | ttl-expired | vpn-instance vpn-
instance-name ] *
```

Lorsque le type de protocole est UDP, le format de commande est :

```
[R-acl-advance-NumACL]rule [ rule-id ] { deny | permit
} { protocol-number | udp } [ destination {
destination-address destination-wildcard | any } |
destination-port { eq port | gt port | lt port | range
port-start port-end } | { { precedence precedence |
tos tos } * | dscp dscp } | { fragment | first-
fragment } | logging | source { source-address source-
wildcard | any } | source-port { eq port | gt port |
lt port | range port-start port-end } | time-range
time-name | ttl-expired | vpn-instance vpn-instance-
name ] *
```

Lorsque le type de protocole est GRE, IGMP, IP, IPINIP ou OSPF, le format de la commande est :

```
[R-acl-advance-NumACL]rule [ rule-id ] { deny | permit
} { protocol-number | gre | igmp | ip | ipinip | ospf
} [ destination { destination-address destination-
wildcard | any } | { { precedence precedence | tos tos
} * | dscp dscp } | { fragment | first-fragment } |
logging | source { source-address source-wildcard |
any } | time-range time-name | ttl-expired | vpn-
instance vpn-instance-name ] *
```

Comme exemple d'ACL nommée avancée, on se propose de créer une liste de contrôle d'accès qui sera appliquée au trafic entrant de l'interface Gigabit Ethernet 0/0 et permettant d'autoriser les machines du réseau 192.168.10.0/24 à accéder seulement au trafic web : http (port 80) et https (port 443).

```
[R]acl 3001
[R-acl-advance-3001]rule permit tcp
destination 192.168.10.0 0.0.0.255 destination-port
eq 80 eq 443 source any
```

```
[R] interface GigabitEthernet 0/0
[R- GigabitEthernet0/0]traffic-filter inbound acl 3001
```

4.2.3.3. *ACL couche 2*

Une ACL de couche 2, dont la valeur possible du numéro qui lui est affectée est dans la plage de 4000 à 4999, est une ACL dont les règles de filtrage sont basées sur des informations de la couche de liaison, y compris l'adresse Mac source, l'ID de VLAN source, le type de protocole de couche 2 et l'adresse Mac de destination.

La syntaxe de configuration d'une ACL de couche 2 sous Huawei est :

```
[R]acl [number] <Num-ACL(de 4000 à 4999)>
[R-acl-basic-NumACL] rule [ rule-id ] { permit | deny
} [ { ether-ii | 802.3 | snap } | l2-protocol type-
value [ type-mask ]]
[R]interface <Type-Interface> <Num-Interface>
[R-InterfaceTypeInterfaceNum]traffic-filter
inbound|outbound acl <Num-ACL>
```

Une ACL peut aussi être définie autrement en lui associant un nom. Dans ce cas-là, on doit spécifier le type de l'ACL (*link* dans ce cas) ou en lui associant un numéro dans la plage de valeurs de 4000 à 4999.

```
[Huawei]acl name <Nom-ACL> link|<Num-ACL(de 4000 à
4999)>
```

4.3. *Firewall*

Un *firewall* prend la forme d'une solution logicielle (au niveau d'un routeur ou d'un équipement terminal : PC, serveur, station de travail) ou d'un équipement matériel permettant de sécuriser une machine, un réseau ou un sous-réseau. Il est appelé aussi : pare-feu, mur de feu, coupe-feu, garde-barrière, barrière de sécurité.

Un *firewall* admet trois fonctionnalités principales : filtrage, traçage et dans certain cas la translation d'adresses NAT.

4.3.1. *Fonctionnalité de filtrage*

Cette fonctionnalité permet d'isoler l'entité à sécuriser, et ce en filtrant les entités qui y accèdent à travers l'adresse Mac, l'adresse IP, l'adresse web (URL), le numéro de port, le protocole, etc. Plusieurs politiques peuvent être appliquées :

– interdire quelques-uns et autoriser le reste (permettre l'accès par défaut), c'est une politique « optimiste » ;

– autoriser quelques-uns et interdire le reste (empêcher l'accès par défaut), c'est une politique « pessimiste » ;

– laisser le choix à l'utilisateur pour décider au fur et à mesure d'autoriser ou d'interdire une entité, c'est une politique interactive.

La politique de filtrage ainsi que les filtres doivent être choisis par l'administrateur et mis à jour périodiquement. L'importance d'un *firewall* dépend de la précision et de l'exactitude de sa configuration de filtrage.

Selon l'entité à filtrer, on assiste à deux modes de filtrage de bas ou de haut niveau.

On distingue aussi selon le processus même de fonctionnement, deux types de filtrages : sans et avec états.

4.3.1.1. *Filtrage de bas niveau*

Appelé aussi filtrage paquet, il permet de filtrer les paquets et éventuellement les trames selon leurs principaux paramètres :

– adresse Mac source/destination ;

– adresse IP source/destination ;

– protocole (IP, ICMP, UDP, TCP, etc.) ;

– port source/destination, etc.

4.3.1.2. *Filtrage de haut niveau*

Appelé aussi filtrage applicatif ou encore filtrage par contenu, il concerne les applications, les pages web. C'est un filtrage qui se base sur des paramètres de haut niveau :

– exécution, accès réseaux, accès base des registres pour les applications (*application filtring*) ;

– adresse URL (*url filtring*) ;

– liste de mots-clés présente dans la page web encore appelée filtrage par contenu (*content filtring*).

4.3.1.3. *Filtrage sans états*

Appelé en anglais *stateless filtring*, le filtrage sans états consiste à filtrer en se basant uniquement sur des informations concernant l'entité à filtrer indépendamment de son état et de son avancement. Bien qu'il soit superficiel, ce filtrage n'est pas gourmand en ressources CPU et mémoire.

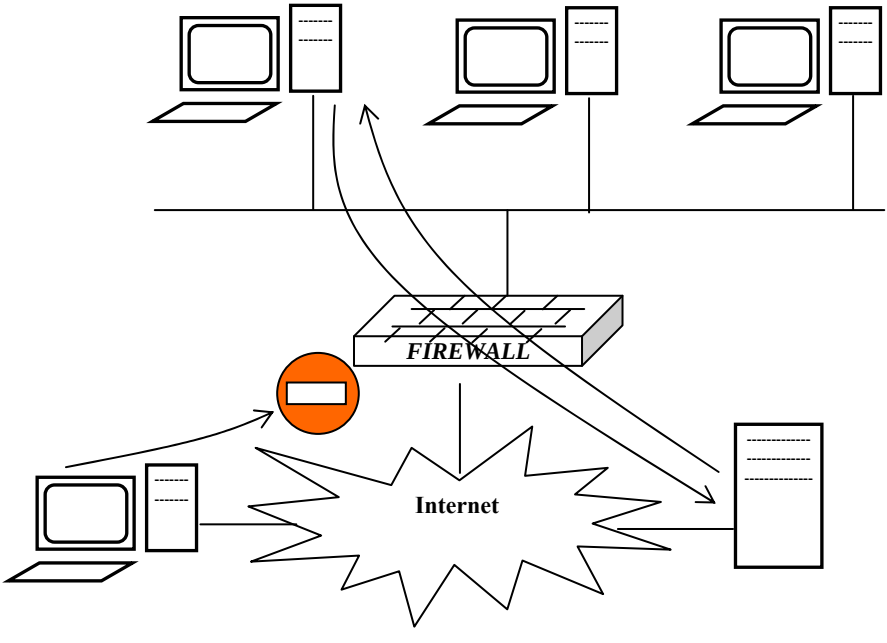

Figure 4.1. *Firewall supportant le filtrage à états (stateful)*

4.3.1.4. *Filtrage avec états*

Appelé en anglais *stateful filtring*, le filtrage avec états consiste à garder en mémoire les contextes des différentes sessions. Il est possible dans ce cas de

modifier dynamiquement les règles de filtrage. Une bonne illustration de ceci est l'autorisation en entrée des paquets qui sont des réponses à des connexions initialisées depuis l'intérieur du réseau et d'interdiction des paquets issus d'une tentative de connexion depuis l'extérieur comme l'illustre la figure 4.1.

4.3.2. *Fonctionnalités de traçage et NAT*

Afin d'identifier l'entité source d'attaque, il fallait enregistrer tous les accès et les tentatives d'accès. La base de données ainsi générée s'appelle LOG. L'administrateur doit consulter fréquemment le LOG pour identifier les sources d'attaque et analyser l'état des communications.

Cette journalisation des différentes activités est nécessaire pour l'administrateur qui peut les analyser manuellement ou en utilisant des outils appropriés afin de détecter tout accès non autorisé ou tentative d'accès.

NAT est l'acronyme de *Network Address Translation*, c'est une fonctionnalité qui existe au niveau d'un routeur ou d'un *firewall* et qui permet de sécuriser un réseau. Elle consiste à cacher les adresses IP locales (adresses privées) lors d'une communication externe (sur Internet) et à les remplacer par des adresses publiques dans l'objectif de protéger certaines machines inaccessibles depuis l'extérieur directement, économiser les adresses IP routables et faciliter la maintenance du réseau.

On assiste à deux modes de translation d'adresses statique et dynamique. La translation d'adresses statique (un pour un) représente une correspondance entre une adresse privée et une adresse publique. La translation d'adresses dynamique (N pour M avec M < N) consiste à attribuer des @ publiques (*pool* d'adresses) à la demande. On utilise aussi un *pool* de ports (PAT : *Port Address Translation*) afin d'identifier l'adresse interne concernée lorsqu'un paquet revient de l'extérieur puisqu'une adresse externe peut être allouée à plusieurs machines.

Le NAT est une technique plus évoluée que celle du proxy. Un proxy, comme l'illustre la figure 4.2, est un agent mandataire permettant de relayer une application (HTTP) vers ces utilisateurs. L'utilisation de l'application sera ouverte exclusivement au proxy et les postes de travail seront dans l'obligation de passer par le proxy.

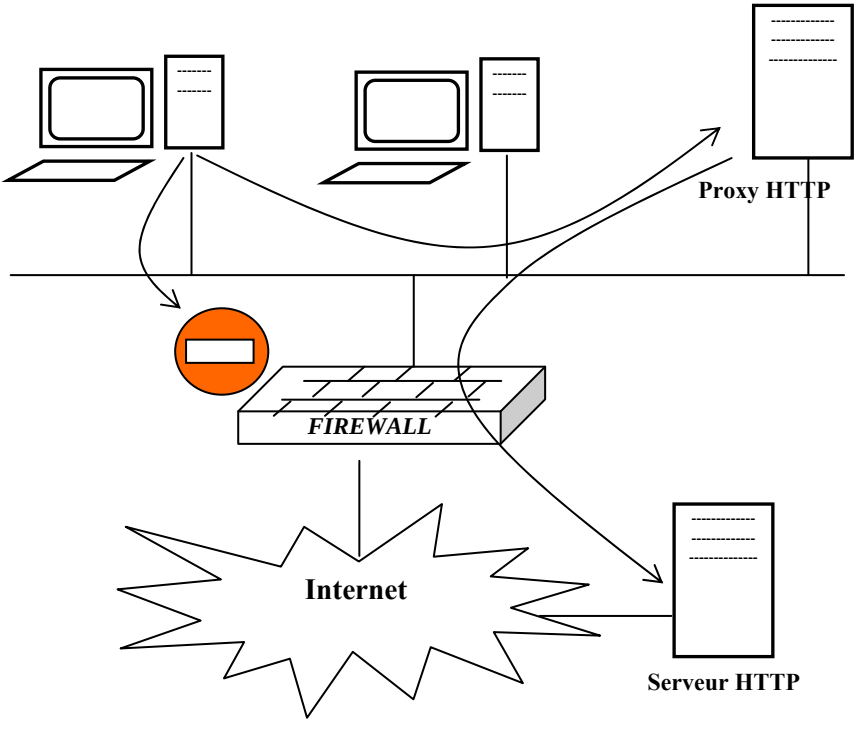

Figure 4.2. *Flux de données avec un Proxy*

4.3.3. *Architecture d'un* firewall

L'architecture générale d'un *firewall* est définie telle que représentée par la figure 4.3.

Cette solution de sécurité est composée de trois parties :

– le pilote d'interception ;

– le moteur ;

– l'interface de configuration.

Il permet de manipuler deux bases de données :

– la liste des filtres ;

– les journaux ou LOG.

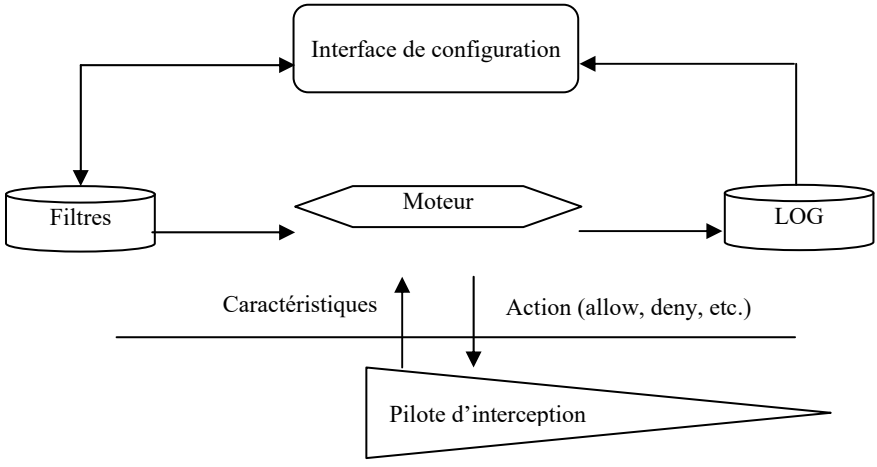

Figure 4.3. *Architecture d'un firewall*

4.3.3.1. *Pilote d'interception*

C'est un composant système de bas niveau permettant de capturer les paquets, les trames ou les entités et de leur appliquer les décisions. Ce composant est responsable de la détection et de l'application de l'action. Il se manifeste à travers un processus système qui doit avoir les privilèges nécessaires, ce qui lui permet d'agir au moment opportun et d'éviter tout échappement à l'action des entités concernées.

4.3.3.2. *Moteur*

C'est un composant de haut niveau qui permet de choisir la décision convenable à appliquer sur une entité moyennant ses caractéristiques par analyse de l'ensemble des filtres (génériques) mis en place par l'administrateur.

En effet, la configuration du *firewall* se présente à travers une liste de filtres diversifiés, complexes et complémentaires, ce qui fait que l'action convenable n'est pas intuitive et n'est plus évidente à identifier. Une telle caractéristique nécessite une analyse plus profonde afin de pouvoir résoudre la tâche de filtrage d'une entité bien définie, c'est le boulot principal du composant moteur.

4.3.3.3. *Interface de configuration*

Il permet à l'administrateur de choisir les filtres convenables. Il existe deux types d'interfaces soit en mode texte à travers une console d'administration (CLI : *Command Line Interface*) soit en mode graphique à travers une interface graphique conviviale (GUI : *Graphic User Interface*). La première nécessite une expertise de la part de l'administrateur.

4.3.3.4. *Base des filtres*

Il s'agit d'une base de données qui représente la configuration du *firewall*. Les filtres sont définis sous forme générique, c'est à la charge du moteur de définir l'ordre de priorité en passant du plus spécifique au plus général. L'action à appliquer sera déduite à partir des entités concernées et des circonstances et selon la politique générale adoptée par le *firewall*.

4.3.3.5. *LOG et journaux*

Il représente les traces d'accès et de tentatives d'accès enregistrées par le *firewall* ainsi que tout événement concernant le *firewall*. Les traces ainsi enregistrées sont historiées (selon la date et l'heure systèmes) afin d'être utilisées par l'administrateur pour identifier un problème bien défini.

4.3.4. *Fonctionnement d'un* firewall

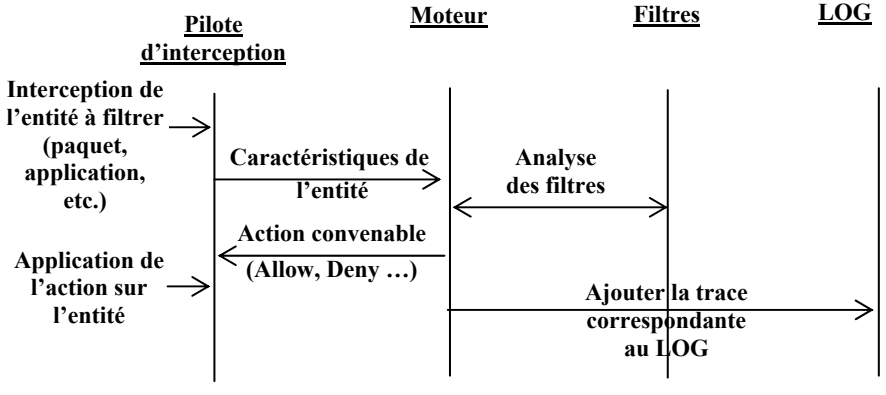

Figure 4.4. *Scénario de filtrage/traçage au niveau d'un firewall*

Le pilote d'interception capture l'entité (paquet, application), il envoie ces caractéristiques (source, destination, etc.) au moteur qui détermine l'action (autoriser, interdire, etc.) en cherchant le filtre qui s'applique à cette entité. L'ensemble des filtres applicables est choisi par l'administrateur lors de la configuration.

4.3.5. *Classifications des firewalls*

Il existe deux classifications possibles pour les *firewalls*. Le premier classement selon le niveau de filtrage par rapport à la pile TCP/IP et le second selon le champ d'action, c'est-à-dire la partie à sécuriser par le *firewall*.

4.3.5.1. *Par niveau d'action*

Ce classement répond à la question : à quel niveau se fait le filtrage ?

On parle de filtrage paquet ou encore de bas niveau dans un premier cas et de filtrage applicatif ou encore de haut niveau dans l'autre cas.

4.3.5.1.1. *Firewall* paquet

Dans cette classe de *firewalls*, l'entité concernée par le filtrage est le paquet et éventuellement la trame. Il intervient au niveau des couches 2, 3 et 4 du modèle OSI.

Le filtrage se fait par rapport aux :

– adresses physiques (@ Mac) source et destination ;

– adresses logiques (@ IP) source et destination ;

– protocoles utilisés (IP, ICMP, TCP, UDP, SLIP, PPP, etc.) ;

– numéros de ports source et destination, etc.

4.3.5.1.2. *Firewall* applicatif

Dans cette classe de *firewalls*, l'entité concernée par le filtrage est l'application. Il intervient au niveau 7 du modèle OSI.

Le filtrage se fait par rapport aux :

– flux web : URL, mots-clés, cookies, etc. ;

– droits des applications : exécution, accès réseau, accès bases des registres, accès disque, etc.

4.3.5.2. *Par champ d'action*

Ce classement répond à la question : que sécurise le *firewall* ?

Les premières générations de *firewalls* étaient conçues pour sécuriser un réseau (Intranet) contre l'extérieur (Internet) puisque ce dernier était considéré comme la source principale des attaques. Au fil du temps, les statistiques ont montré que 80 % des attaques sont issus de l'intérieur. Les *firewalls* qui sécurisent une machine sont apparus comme solution.

Afin d'éviter les difficultés de configurations relatives aux *firewalls* PC, des solutions *firewall* distribuées ont vu le jour admettant des agents et un serveur d'administration.

4.3.5.2.1. *Firewall* classique

On qualifie de *firewall* classique, tout *firewall* matériel qui sécurise un réseau. On parle aussi de *firewall* boîtier. C'est un équipement qui sera déployé entre le réseau local à protéger et le réseau externe (Internet), source potentielle d'attaque.

4.3.5.2.2. *Firewall* PC

C'est une solution logicielle permettant de sécuriser une machine et de se prémunir de cette machine. La raison d'être de cette nouvelle génération de *firewall* vient du fait que les statistiques ont montré que 80 % des attaques sont internes. Comme l'antivirus, le *firewall* PC est d'utilisation domestique et il existe plusieurs solutions à libre utilisation sur Internet.

4.3.5.2.3. *Firewall* distribué

C'est une solution réseau récente pour sécuriser les différentes machines avec configuration centralisée. On assiste à un agent de filtrage au niveau de chaque machine qui joue le rôle d'un *firewall* PC et dont la configuration est issue d'une machine centrale qui s'occupe aussi de la collecte du LOG. L'administrateur n'a pas besoin de passer machine par machine afin de reconfigurer et d'analyser le LOG ou de laisser cette tâche à l'utilisateur qui n'est pas forcément averti ou connaisseur.

4.3.6. Firewall *à états*

Un *firewall* à états (*statefull firewall*) est un *firewall* qui permet d'assurer le filtrage en se basant sur l'état de la connexion réseau. L'objectif est de sécuriser le réseau local contre toute tentative d'accès extérieur (à partir d'Internet). Cette fonctionnalité permet de distinguer un paquet qui fait partie d'une réponse à une requête interne (à autoriser) et un paquet qui fait partie d'une nouvelle connexion initiée depuis l'extérieur (à interdire). Pour cela, le *firewall* permet d'inspecter le trafic initié depuis le réseau local afin de savoir distinguer la réponse à une requête interne du reste du trafic entrant et d'appliquer l'action convenable.

Une implémentation possible à travers un routeur Cisco (IOS mis à jour pour supporter le *firewalling*) s'effectue en se basant sur les ACL, elle consiste à :

1) choisir les interfaces internes et externes :

– (GigabitEthernet 0/0 comme interface interne, Serial 0/0/0 comme interface externe) ;

2) configurer les ACL pour chaque interface :

– une ACL qui interdit le trafic entrant à toute interface externe :

```
R(config)#ip access-list extended OUTSIDE
R(config-ext-nacl)#deny ip any any
R(config)#interface Serial 0/0/0
R(config-if)#ip access-group OUTSIDE in
```

– une ACL qui permet de définir le trafic à autoriser parmi celui entrant à toute interface interne :

```
R(config)#ip access-list extended INSIDE
R(config-ext-nacl)#permit tcp any any eq 80
R(config-ext-nacl)#deny ip any any
R(config)#interface GigabitEthernet 0/0
R(config-if)#ip access-group INSIDE in
```

3) définir les règles d'inspection – créer une règle d'inspection :

```
R(config)#ip inspect name FWSF http
```

4) appliquer une règle d'inspection à une interface – appliquer la règle d'inspection au trafic entrant de toute interface interne :

```
R(config)#interface GigabitEthernet 0/0
R(config-if)#ip inspect FWSF in
```

4.3.7. Firewall *basé sur les zones*

Un *firewall* basé sur les zones (ZPF : *Zone-based Policy Firewall*) est un *firewall* qui permet de fournir une configuration souple indépendante des ACL et des interfaces physiques.

4.3.7.1. *Présentation générale et notion de zones*

Ce nouveau mode de configuration dans lequel les interfaces sont attribuées aux zones de sécurité et où la stratégie de pare-feu est appliquée au trafic circulant entre les zones consiste à :

– déterminer les zones ;

– établir des politiques entre les zones ;

– concevoir l'infrastructure physique ;

– identifier les sous-ensembles au sein des zones et fusionner les exigences de trafic.

Le Cisco IOS ZPF peut prendre en charge trois actions :

– *inspect* : permet d'effectuer une inspection des paquets avec état Cisco IOS ;

– *drop* : analogue à l'instruction *deny* dans une ACL, elle permet de supprimer un paquet. Une option de journalisation est disponible pour enregistrer les paquets rejetés ;

– *pass* : analogue à l'instruction *permit* dans une ACL, elle permet d'autoriser un paquet. L'action de réussite ne suit pas l'état des connexions ou des sessions dans le trafic.

Il est possible de créer deux ou plusieurs zones, une interface physique peut être affectée ou non à une zone ; une zone spécifique appelée *self-zone* représen-

te le routeur lui-même et comprend toutes les adresses IP attribuées à ces interfaces.

Une fois les zones de sécurité créées, l'administrateur peut créer des paires de zones et éventuellement prévoir des politiques de sécurité pour certains ou toutes ces paires de zones.

L'action (*pass*, *drop* ou *inspect*) à appliquer au trafic entres les interfaces sera présentée dans le tableau 4.2, et ce selon la source et la destination d'une part et la configuration du *firewall* ZPF d'autre part, en l'occurrence l'existence d'une paire de zones entre les zones mentionnées et éventuellement d'une politique de sécurité à appliquer sur la *zone-pair* en question.

Interface source membre dans une zone ?	Interface destination membre dans une zone ?	La zone-pair existe-t-elle ?	La politique existe-t-elle ?	Action
Non	Non	–	–	**Pass**
Oui	Non	–	–	**Drop**
Non	Oui	–	–	**Drop**
Oui (zone X)	Oui (zone X)	–	–	**Pass**
Oui (zone X)	Oui (zone Y)	Non	–	**Drop**
Oui (zone X)	Oui (zone Y)	Oui	Non	**Drop**
Oui (zone X)	Oui (zone Y)	Oui	Oui	**Inspect**
Oui (*self-zone*)	Oui (zone Y)	Non	–	**Pass**
Oui (*self-zone*)	Oui (zone Y)	Oui	Non	**Pass**
Oui (*self-zone*)	Oui (zone Y)	Oui	Oui	**Inspect**
Oui (zone X)	Oui (*self-zone*)	Non	–	**Pass**
Oui (zone X)	Oui (*self-zone*)	Oui	Non	**Pass**
Oui (zone X)	Oui (*self-zone*)	Oui	Oui	**Inspect**

Tableau 4.2. *Règles de filtrage relatives au trafic de transit entre les interfaces dans le cadre d'un firewall ZPF*

4.3.7.2. *Configuration et mise en place d'un* firewall *ZPF*

La configuration comporte cinq étapes :

1) création des zones en utilisant la commande `zone security <zone-sec-name>` :

```
R(config)#zone security PRIVATE
R(config-sec-zone)#exit
R(config)# zone security PUBLIC
```

2) identification du trafic en utilisant la commande `class-map type inspect`. La syntaxe générale est :

```
R(config)#class-map type inspect {match-all|match-any}
<class-map-name>
R(config-cmap)#match access-group {acl-name|acl-name}
R(config-cmap)#match protocol <protocol-name>
R(config-cmap)#match class-map <class-map-name>
```

L'option `match-all` exige pour un paquet de satisfaire tous les critères mentionnés tandis que l'option `match-any` se contente pour un paquet de satisfaire un seul critère parmi ceux mentionnés. Si on désire créer une *class-map* qui englobe tout le trafic web, on configure comme suit :

```
R(config)#class-map type inspect match-any WEB-TRAFFIC
R(config-cmap)#match protocol http
R(config-cmap)#match protocol https
R(config-cmap)#match protocol dns
```

3) définition d'une action en utilisant la commande `policy-map type inspect <policy-map-name>`. Cette commande permet de spécifier une *class-map* pour identifier le trafic concerné et choisir l'action à appliquer (*drop*, *pass* ou *inspect*) :

```
R(config)# policy-map type inspect PRIV-2-PUB-POLICY
R(config-pmap)#class type inspect WEB-TRAFFIC
R(config-pmap-c)#inspect
```

4) identifier la zone-pair avec la commande `zone-pair security <zone-pair-name> source <zone-sec-name> destination <zone-sec-name>` et l'affecter à la politique de sécurité avec la commande `service-policy type inspect <policy-map-name>` :

```
R(config)# zone-pair security PRIV-PUB source PRIVATE
destination PUBLIC
R(config-sec-zone-pair)# service-policy type inspect
PRIV-2-PUB-POLICY
```

5) affecter les interfaces physiques aux différentes zones en utilisant la commande `zone-member security <zone-sec-name>` :

```
R(config)#interface GigabitEthernet 0/0
R(config-if)# zone-member security PRIVATE
R(config-if)#exit
R(config)#interface Serial 0/0/0
R(config-if)# zone-member security PUBLIC
```

4.3.8. *Exemples de* firewall

On va présenter un exemple de *firewall* matériel et deux exemples de *firewalls* logiciels.

4.3.8.1. *Cisco PIX*

Cisco PIX (*Private Internet Exchange*) est le pare-feu boîtier de la société Cisco Systems.

La gamme Cisco PIX combine sur une plate-forme compacte et fiable des fonctions robustes de *firewall* et de VPN et des services réseau intelligents. Les Cisco PIX peuvent être configurés soit à travers un câble console soit moyennant un accès web ou accès Telnet à partir du réseau. Il est aussi possible d'intervenir à partir d'une ligne téléphonique en utilisant un modem.

4.3.8.2. *Iptables*

Iptables est un logiciel libre de l'espace utilisateur Linux grâce auquel l'administrateur système peut configurer les chaînes et règles dans le pare-feu en espace noyau (et qui est composé par des modules Netfilter).

Différents programmes sont utilisés selon le protocole employé : Iptables est utilisé pour le protocole IPv4, Ip6tables pour IPv6, Arptables pour ARP (*Address Resolution Protocol*) ou encore Ebtables, spécifique aux trames Ethernet.

Ce type de modifications doit être réservé à un administrateur du système. Par conséquent, son utilisation nécessite l'utilisation du compte root. L'utilisation du programme est refusée aux autres utilisateurs.

Sur la plupart des distributions Linux, Iptables est lancé par la commande /usr/sbin/iptables et documenté par sa page de manuel iptables1 et ip6tables2, laquelle peut être visualisée *via* la commande « man iptables ».

Iptables est également fréquemment utilisé pour faire référence aux composants de bas niveau (niveau kernel). X_tables est le nom du module noyau, plus générique, qui contient le code partagé pour les quatre protocoles. C'est aussi le module qui fournit l'API des extensions. Par conséquent, X_tables désigne usuellement le pare-feu complet (IPv4, IPv6, arp, eb).

4.3.8.3. *ZoneAlarm*

ZoneAlarm est un *firewall* en *freeware* (pour un usage personnel). C'est un *firewall* applicatif qui permet de protéger le PC des tentatives d'intrusions lors des connexions sur Internet. Il permet de limiter les accès web et présente notamment un module de contrôle parental nécessaire pour limiter et surveiller l'accès Internet pour les enfants. Ce dernier sujet est très important vu les effets néfastes d'Internet sur les enfants, on assiste à des problèmes de cyberintimidation ou cybercriminalité.

4.3.8.4. *ISA Server*

ISA Server (*Internet Security and Acceleration Server*) est un *firewall* Microsoft, c'est un serveur pare-feu d'entreprise et de cache extensible pour le Web. Il offre des fonctions de sécurité par stratégies, d'accélération et de gestion des interconnexions de réseaux. ISA Server présente deux modes étroitement intégrés : un serveur pare-feu multicouche et un serveur de cache pour le Web très performant.

Le pare-feu assure :

– le filtrage au niveau des couches de paquets, de circuits et d'applications ;

– l'examen des états pour examiner les données traversant le pare-feu ;

– le contrôle de la stratégie d'accès et le routage du trafic.

Le cache améliore la performance du réseau et l'expérience de l'utilisateur final en stockant le contenu du Web fréquemment demandé. Les services de

pare-feu et de cache peuvent être déployés séparément sur des serveurs dédiés ou intégrés sur un même ordinateur.

4.3.8.5. Firewall *ASA de Cisco*

Cisco *Adaptive Security Appliance* (ASA) fournit une solution de pare-feu complète et éprouvée. Il offre une évolutivité supérieure, une large gamme de solutions technologiques et une sécurité efficace et permanente, conçue pour répondre aux besoins d'une grande variété de déploiements.

ASA supporte plusieurs services (routage, AAA, etc.) en plus des fonctionnalités de *firewalling*. Il admet une syntaxe spécifique et différente de celle utilisée au niveau des autres équipements Cisco. De plus, les ACL sous ASA sont définies et appliquées en utilisant des commandes différentes des routeurs.

Cisco vient de commercialiser différents modèles de *firewall* Cisco, on cite à titre d'exemple : ASA 5505, ASA 5506-X, ASA 5512-X, ASA 5525-X, ASA 5555-X, etc., en plus du module ASA sous forme d'une carte qui peut être montée sur un autre équipement conforme.

ASA peut être déployé moyennant différents types d'architectures et il peut exploiter le service *Active Directory* de Microsoft. Il peut d'autre part être utilisé pour le montage d'une zone DMZ.

4.4. Notion de DMZ

Au niveau de tout réseau qui prévoit des services accessibles de l'extérieur, il fallait prévoir dans l'architecture correspondante une zone DMZ.

4.4.1. *Définition et utilité*

DMZ est l'acronyme de *Dimilitarised Zone* ou encore zone démilitarisée. C'est une partie du réseau local contenant des services accessibles de l'extérieur tel qu'un service web. C'est une zone surveillée sans qu'il y ait un filtrage fort par rapport au reste du réseau local plus sécurisé.

L'utilité de la zone DMZ est d'isoler les services visibles de l'extérieur du reste du réseau dans le but de définir une politique de filtrage différente avec un *firewall* à filtrage par états (*statefull*). En effet, tout trafic initié de l'extérieur sera

autorisé vers le DMZ et interdit vers le reste du réseau et dans le cas contraire, seulement, le trafic sortant issu de la partie sécurisée sera autorisé.

4.4.2. *Topologies de mise en œuvre*

Il existe deux façons possibles pour monter une topologie DMZ. La première se fait en montant la DMZ comme une branche associée à un *firewall*. La deuxième consiste à délimiter la zone DMZ entre deux *firewalls* (interne et externe).

4.4.2.1. *Topologie avec un seul* firewall

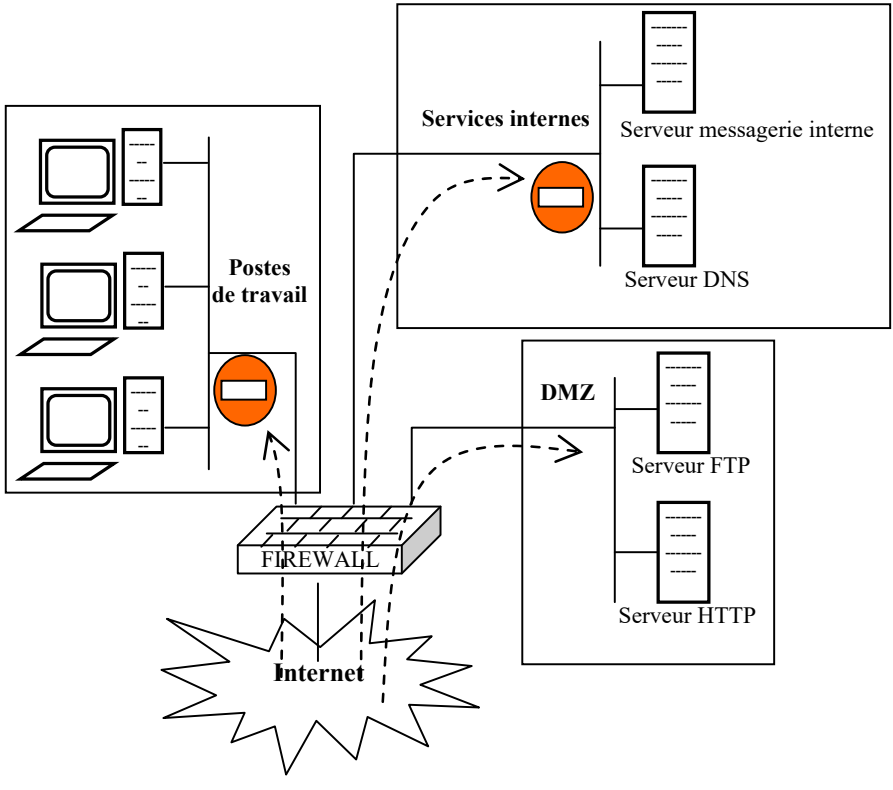

Figure 4.5. *Montage DMZ avec un seul firewall*

Le segment de la DMZ sera monté à une patte LAN indépendante du *firewall* (certains *firewalls* prévoient une patte réservée pour la DMZ).

Dans le cas où le *firewall* admet une entrée LAN unique, on opte pour la technologie de VLAN pour séparer la DMZ du reste du réseau local. On peut aussi séparer la partie sécurisée en plusieurs segments physiquement ou logiquement (VLAN) séparés dans l'objectif de définir des politiques de sécurité différentes. C'est le cas par exemple lorsque l'on sépare les services internes des postes de travail.

Dans le cas d'une seule patte LAN, on assiste à un segment physique unique qui contient tous les équipements internes. On opte pour la segmentation logique à travers les VLAN (*Virtual Local Area Network*). On assiste à trois technologies de VLAN.

La technologie de VLAN par port physique consiste à affecter chaque port d'un commutateur à un VLAN (identifié par son numéro). C'est la solution la plus simple mais la plus rigide dans la mesure où une machine risque de changer de segment logique en changeant de port de raccordement.

La technologie VLAN par adresse Mac consiste à assurer la sécurité par port et à associer à chaque port une adresse Mac figée ou encore par apprentissage et créer des segments logiques (DMZ, etc.), ce qui permet d'émuler la répartition physique des segments.

Le tableau 4.3 donne les politiques de filtrage générales appliquées au niveau du *firewall* entre les trois segments et Internet les uns par rapport aux autres.

De / À	Postes de travail	Services internes	DMZ	Internet
Postes de travail	–	Allow (accès possible de l'intérieur)	Allow (accès possible de l'intérieur)	Allow (accès Internet possible)
Services internes	Deny (aucun utilisateur)	–	Deny (aucun utilisateur)	Deny (aucun utilisateur)
DMZ	Deny (aucun utilisateur)	Deny (aucun utilisateur)	–	Deny (aucun utilisateur)
Internet	Deny (aucun service)	Deny (services internes)	Allow (services accessibles de l'extérieur)	–

Tableau 4.3. *Filtrage du trafic dans un montage DMZ avec un seul firewall*

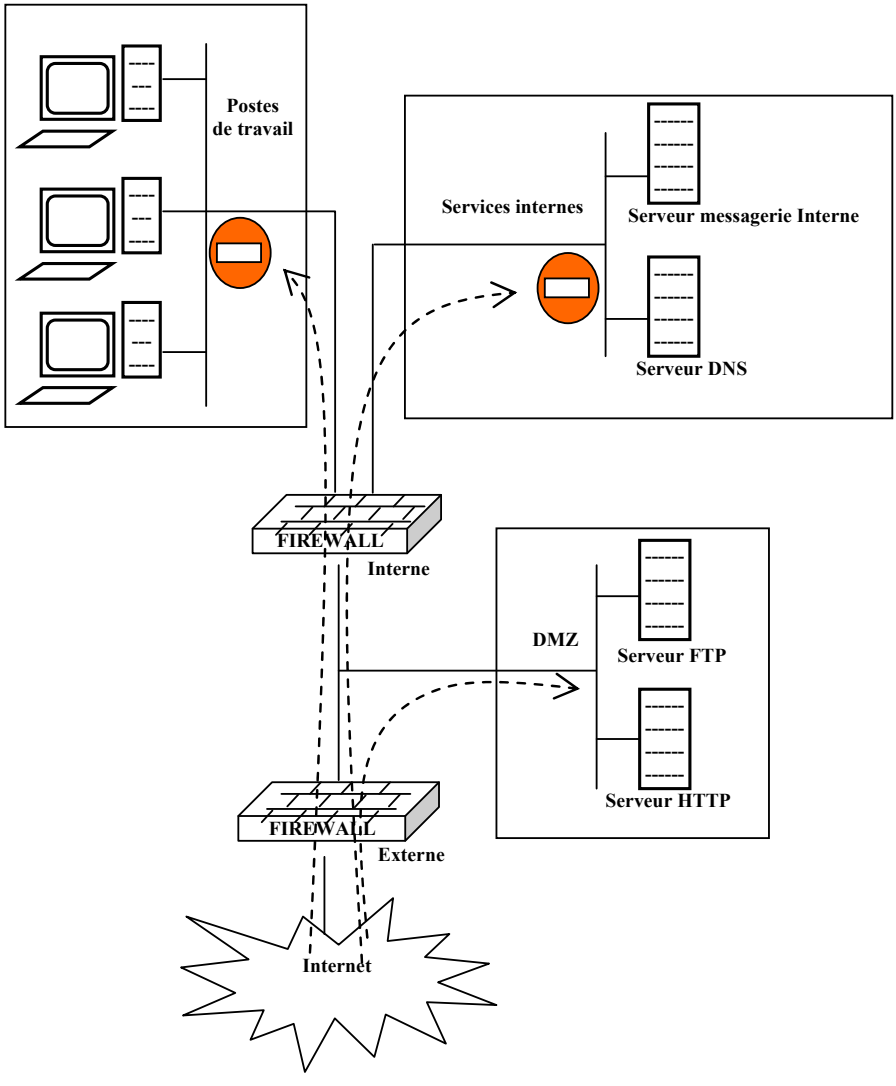

Figure 4.6. *Montage DMZ avec deux firewalls*

4.4.2.2. *Topologie à deux* firewalls

Le segment de la DMZ sera délimité entre deux *firewalls*, un *firewall* externe qui filtre le trafic entre Internet et le réseau local, un *firewall* interne qui filtre encore plus le trafic de la partie sécurisée, ce qui rend l'accès à cette partie encore plus difficile (passage par deux *firewalls*).

4.5. Conclusion

Le contrôle d'accès aussi bien physique que logique représente une mesure de sécurité nécessaire permettant de réduire les risques d'accès frauduleux de suivre toutes les connexions et les tentatives de connexions. Il est assuré, dans son volet logique, par les ACL et les *firewalls*.

Les ACL représentent une méthode primitive pour contrôler et limiter le trafic réseau permettant ainsi d'assurer un niveau de sécurité du patrimoine informatique aussi bien matériel que logiciel. Elle offre diverses fonctionnalités de filtrage statique et dynamique sur plusieurs niveaux. Bien qu'importante et efficace, une évolution de ce principe a vu le jour moyennant des équipements dédiés appelés *firewall*.

Les *firewalls* représentent une solution de sécurité incontournable au niveau de l'entreprise, le déploiement d'un *firewall* matériel est nécessaire pour sécuriser l'accès distant au niveau de l'entreprise d'une part et celui des *firewalls* logiciels pour sécuriser les différents serveurs et postes de travail reste aussi une mesure de sécurité qui s'impose pour sécuriser le patrimoine matériel et logiciel de l'entreprise. Mais le *firewall* ne peut en aucun cas résoudre le problème de sécurité sans être allié par d'autres solutions telles que des antivirus et les IDS.

Chapitre 5

Techniques et outils de détection d'intrusions

5.1. Introduction

Les virus représentent le moyen d'intrusion le plus grave, le plus répandu et le plus connu. On assiste à une production énorme de programmes malveillants et plus particulièrement de virus quotidiens. De ce fait, il fallait avoir un outil de protection efficace pour un tel problème. Dans ces circonstances, les antivirus sont apparus ; ils représentent une solution de sécurité spécifique.

Les *firewalls* représentent une solution générique de sécurité permettant de limiter la probabilité des attaques et les antivirus représentent une solution de sécurité spécifique ayant pour objectif de désinfecter les machines des virus. Ces deux solutions restent limitées pour garantir la sécurité d'un système informatique et le déploiement d'un système de détection d'intrusion est une action nécessaire afin de rassurer la sécurité, cette dernière solution permettant de résoudre les insuffisances aussi bien du *firewall* que de l'antivirus. C'est une solution plus complexe qui utilise des moyens divers afin de détecter et désinfecter les outils d'intrusion aussi complexes soient-ils.

5.2. Antivirus

C'est un logiciel permettant de détecter, d'isoler et de détruire les virus sur disques, amovibles ou encore chargés en mémoire.

5.2.1. *Fonctionnalités d'un antivirus*

Un antivirus comprend trois fonctionnalités : la détection, l'isolation et la destruction.

– Détection : un antivirus doit être capable de détecter les virus connus à travers l'analyse des fichiers et moyennant la signature. Il peut dans certains cas de figure détecter les virus inconnus à travers des heuristiques et moyennant leurs comportements.

– Isolation : l'isolation consiste à mettre en quarantaine un virus ou un programme infecté pour l'empêcher de se reproduire d'une part et de nuire au système informatique d'autre part.

– Destruction : c'est le fait de supprimer les fichiers relatifs à un virus pour limiter sa reproduction et sa propagation.

5.2.2. *Méthodes de détection de virus*

Les premières générations d'antivirus étaient limitées aux virus connus, et ce moyennant la base virale, mais les nouvelles générations deviennent de plus en plus intelligentes et peuvent détecter les virus même si leurs signatures n'existent pas dans la base virale, et ce en utilisant des techniques empruntées à l'intelligence industrielle.

5.2.2.1. *Détection des virus connus*

La détection des virus connus se fait à travers la signature, chaîne de caractères représentative du virus (le résultat d'une fonction de hachage). Ce qui implique une mise à jour périodique afin de prendre en compte les signatures des nouveaux virus et de pouvoir les détecter.

5.2.2.2. *Détection des virus inconnus*

La détection des virus inconnus est une tâche difficile et peu efficace, elle se base sur un ensemble de méthodes complémentaires :

– analyse comportementale : elle consiste à pouvoir détecter un comportement viral au niveau des programmes, c'est le cas d'apparition de fichiers parasites ou de perte de données ;

– contrôle d'intégrité : elle consiste à sauvegarder les signatures des différents programmes et applications au niveau d'un ordinateur et à contrôler périodiquement le changement qui peut être dû à un virus qui s'y est introduit ;

– détection générique multiniveaux : c'est une technique assez compliquée pour la détection des virus polymorphes dont la signature change par changement de forme.

5.2.3. *Manipulations possibles pour un antivirus*

Bien que le déploiement d'un antivirus n'exige pas d'expertise nécessaire, il nécessite quelques manipulations de base pour son bon fonctionnement.

– Analyse : l'utilisateur peut à tout moment demander explicitement l'analyse d'un disque, d'un amovible ou d'un fichier afin de pouvoir détecter avec précision s'il contient des virus.

– Mise à jour : l'utilisateur doit périodiquement effectuer des mises à jour pour prendre en considération les nouveaux virus. Un retard d'un jour vaut une absence de protection contre un nombre important de virus. Lors de l'installation d'un antivirus, il fallait faire la mise à jour car il ne prend en compte que les virus connus jusqu'à la date de sa mise sur le marché. En effet, s'il est apparu avant un an, il ne protège pas contre plusieurs milliers de virus.

5.2.4. *Composants d'un antivirus*

Un antivirus est composé de quatre parties : scanner, moniteur, base virale, LOG.

– Scanner : il permet d'analyser à la demande les fichiers au niveau d'un emplacement sur l'ordinateur. Il doit être assez efficace et vu sa complexité, il consomme beaucoup de ressources. Il s'agit d'une analyse exhaustive sur demande explicite de la part de l'utilisateur. Cette analyse couvre les fichiers, les enregistrements, les bases de registres et même dans certains cas, le contenu mémoire pour pouvoir détecter et supprimer les virus résidents en mémoire.

– Moniteur : il permet d'analyser à la volée les fichiers auxquels on accède. Il doit être assez rapide et exploite le minimum de ressources pour arriver à stop-

per immédiatement les virus sans encombrer la machine. Son action concerne quatre activités principales : le mail, le Web, le téléchargement et le système.

– Base virale : c'est une base de données composée de l'ensemble des signatures des différents virus connus. Il fallait effectuer périodiquement des mises à jour pour enrichir cette base par les nouveaux virus qui viennent d'être injectés. La mise à jour peut s'effectuer soit en ligne et nécessite une connexion Internet soit hors ligne en exécutant le patch convenable.

– LOG : il est composé des différents journaux utilisés pour enregistrer l'historique, les activités et les actions menées par l'antivirus.

5.2.5. *Comparaison entre antivirus et* firewall

Un antivirus, en tant que solution spécifique, peut être comparé avec le *firewall*, comme étant une solution générique, à travers le tableau 5.1.

Outil de sécurité / Caractéristique	Antivirus	*Firewall*
Nature	Spécifique	Générique
Forme	Logicielle	Logicielle ou matérielle
Degré d'expertise exigé	Minimum de connaissance	Expérience importante de la part de l'administrateur
Fonctionnalités	Détection, isolation et suppression des virus	Filtrage et traçage (réseau ou applications) ou encore NAT
Degré de complexité	Simple	Complexe
Actions périodiques nécessaires	Mise à jour périodique (de préférence automatique)	Configuration et analyse de LOG
Utilisation	Répandue, domestique	Modeste, professionnelle

Tableau 5.1. *Comparaison entre antivirus et firewall*

5.3. Systèmes de détection d'intrusions

Un système de détection d'intrusion (IDS : *Intrusion Detection System*) est un mécanisme destiné à repérer les activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance des intrusions réussies aussi bien que des tentatives échouées. Les IDS comportent plusieurs formes et peuvent agir sur plusieurs niveaux, ils ont connu de considérables évolutions.

5.3.1. *Fonctionnalités d'un IDS*

Un IDS permet d'assurer l'identification de tous les comportements intrusifs dans un environnement et la déclaration de ce comportement en temps opportun.

En effet, l'IDS est un système de surveillance qui se base sur des techniques diverses et complémentaires. Il doit annoncer toute action de détection qu'il assure afin de réagir dans le bon moment et trouver les remèdes ou les mesures de préventions nécessaires permettant d'éviter ou de désactiver l'attaque.

5.3.2. *Composants et fonctionnement d'un IDS*

Un IDS est composé de plusieurs éléments :

– la pile de production : consiste en un ensemble de modules TCP/IP intégré dans la majorité des opérations réseaux de la plate-forme système. Elle détecte les intrusions et les extrusions IPv4 et IPv6 ;

– la pile de service : consiste en un ensemble de modules intégrés dans le service et support de la plate-forme système. Elle détecte seulement les intrusions et les extrusions IPv4 et agit en premier lieu par rapport à la pile de production ;

– la tâche IDS : c'est le composant qui permet de traiter les événements générés par la pile de production et la pile de service ;

– l'interface graphique : permet de visualiser les événements à partir du journal d'audit ;

– la notification IDS : représente le composant d'alerte qui permet de transmettre les messages par mail ;

– le journal d'audit : permet de stocker le LOG.

Les composants de l'IDS ainsi que le scénario de son fonctionnement sont représentés par le schéma de la figure 5.1.

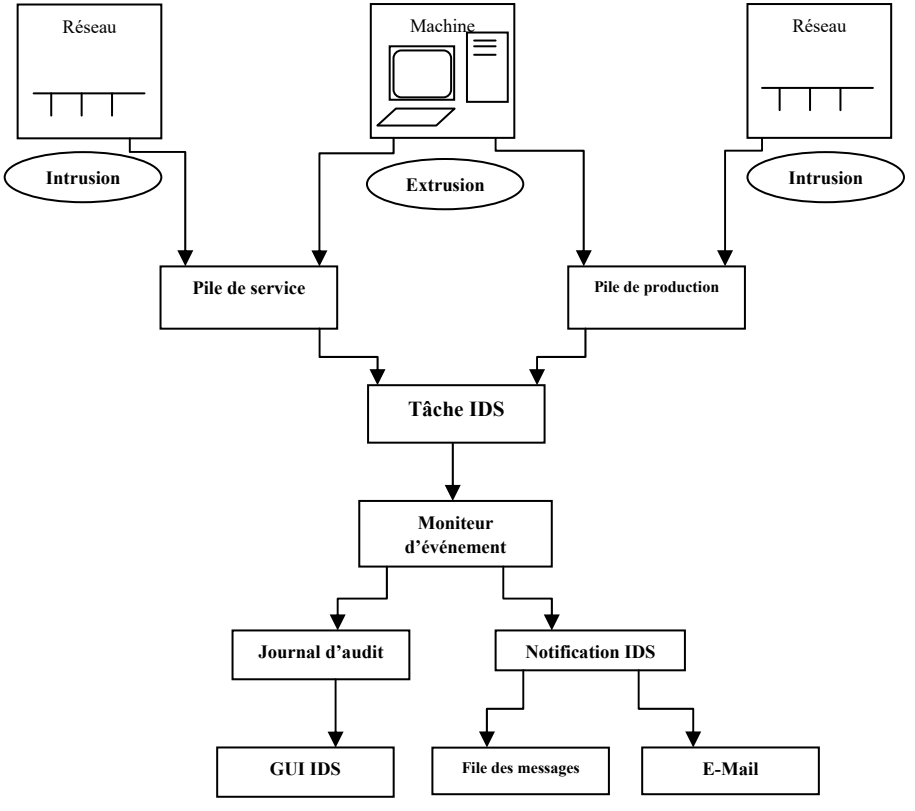

Figure 5.1. *Composants et fonctionnement d'un IDS*

L'IDS fonctionne de la façon suivante :

1) lorsque la pile de production ou de service détecte une intrusion avancée ou une extrusion, il envoie un événement à la tâche IDS ;

2) la tâche IDS prend les événements de la file un par un et assure la correspondance de chaque événement à une condition (à partir de la table de port). La tâche IDS détient également des statistiques sur les événements d'intrusion et d'extrusion ;

3) l'IDS signale des événements pour les intrusions et les extrusions qui dépassent les seuils fixés dans les fichiers de stratégie. Si un événement est signalé, l'enregistrement de surveillance d'intrusion est créé dans le journal d'audit ;

4) l'interface graphique IDS affiche les événements d'intrusion à partir des dossiers du journal d'audit ;

5) si vous avez configuré un email et un message de notification sur la page Propriétés IDS, la notification d'IDS envoie un email à l'adresse spécifiée et un message à une file de messages.

5.3.3. *Classifications des IDS*

Les IDS peuvent être classés selon le champ d'action (machine ou réseau) ou selon le niveau de protection (simple détection ou prévention).

5.3.3.1. *Classification selon le champ d'action*

Selon la cible à sécuriser qui peut être une machine ou un réseau, on distingue : HIDS (*Host based IDS*) et NIDS (*Network based IDS*).

5.3.3.1.1. HIDS

Les HIDS ou encore « système de détection d'intrusion machine » sont des IDS dédiés à la surveillance du matériel et des systèmes d'exploitation. Un HIDS récupère les informations qui lui sont données par le matériel ou le système d'exploitation. Il y a pour cela plusieurs approches : signatures, comportement.

Un HIDS se comporte comme un daemon ou un service standard sur un système hôte qui détecte une activité suspecte en s'appuyant sur une norme. Si les activités s'éloignent de la norme, une alerte est générée. La machine peut être surveillée sur plusieurs axes :

– activité de la machine : nombre et listes de processus ainsi que d'utilisateurs, ressources consommées, etc. ;

– activité de l'utilisateur : horaires et durée des connexions, commandes utilisées, messages envoyés, programmes activés, dépassement du périmètre défini, etc. ;

– activité malicieuse d'un ver, virus ou cheval de Troie.

Un autre type de HIDS cherche les intrusions dans le « noyau » (*kernel*) du système, et les modifications qui y sont apportées. Certains appellent cette technique « analyse protocolaire ». C'est une technique qui ne nécessite pas de recherche dans une base de signature.

5.3.3.1.2. NIDS

Les NIDS ou encore « système de détection d'intrusion réseau » sont des IDS dédiés à la surveillance de l'état de sécurité du réseau. L'analyse menée par un NIDS se découpe en trois grandes parties : la capture, les signatures et les alertes.

– Capture : la capture sert à la récupération en temps réel du trafic réseau. La plupart des NIDS utilisent la bibliothèque standard de capture de paquet libpcap, une bibliothèque présente sur la plupart des plates-formes.

– Signatures : il s'agit d'une bibliothèque de signatures d'attaques (approche par scénario) utilisables d'une façon similaire à l'antivirus. Ainsi, le NIDS est efficace s'il connaît l'attaque, mais inefficace dans le cas contraire. Les outils commerciaux ou libres ont évolué pour proposer une personnalisation de la signature afin de faire face à des attaques dont on ne connaît qu'une partie des éléments. Les outils à base de signatures requièrent des mises à jour très régulières.

– Alertes : les alertes sont généralement stockées sous forme de LOG. Il existe une norme qui permet d'en formaliser le contenu, afin de permettre à différents éléments de sécurité de les manipuler. Ce format s'appelle IDMEF (pour *Intrusion Detection Message Exchange Format*) décrit dans la RFC4765. IDMEF offre une infrastructure permettant aux IDS de ne pas avoir à s'occuper de l'envoi des alertes. Cela permet aux IDS de n'avoir qu'à décrire les informations qu'ils connaissent et sans se charger de les stocker pour permettre une visualisation humaine ultérieurement.

Les NIDS ont pour avantage d'être des systèmes temps réel et ont la possibilité de découvrir des attaques ciblant plusieurs machines à la fois. Leurs inconvénients sont le taux élevé de faux positifs qu'ils génèrent.

5.3.3.2. *Classification selon le niveau de protection*

Les systèmes de gestion des intrusions peuvent assurer la détection et/ou la prévention, on distingue trois familles de systèmes (IDS, IPS, IDS/IPS).

5.3.3.2.1. IDS

C'est la forme la plus simple dans la mesure où elle assure seulement la détection. Il admet un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte) et permet ainsi d'avoir une connaissance sur les tentatives d'intrusion d'une entreprise.

5.3.3.2.2. IPS

Le système de prévention des intrusions (IPS : *Intrusion Prevention System*) est un mécanisme destiné à protéger les systèmes contre les intrusions, c'est une évolution de l'IDS permettant d'assurer à la fois la détection et la prévention. Un IPS a le même rôle de détection qu'un IDS, sauf que ce système peut prendre des mesures afin de diminuer les risques d'impact d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement.

5.3.3.2.3. IDS/IPS

On assiste aussi à une nouvelle génération d'IDS/IPS, ce sont des solutions hybrides de détection/prévention des intrusions tant au niveau machine que des réseaux.

5.3.3.3. *Comparaison des différents types d'IDS/IPS*

Le tableau 5.2 permet de dresser une comparaison entre les H-IPS et les N-IPS en présentant les avantages et les inconvénients de chacun.

	Avantages	Inconvénients
Host-Based IPS	– Assure une protection spécifique pour machine. – Prévoit une protection de haut niveau pour le système d'exploitation et les applications. – Protège la machine après décryptage des messages.	– Dépendant du système d'exploitation. – Nécessite d'être installé sur toutes les machines.
Network-Based IPS	– Meilleur coût. – Indépendant du système d'exploitation.	– Incapable d'examiner un trafic chiffré. – Doit arrêter un trafic malicieux avant d'atteindre les machines.

Tableau 5.2. *Avantages et inconvénients des H-IPS/N-IPS*

5.3.4. *Exemples d'IDS/IPS*

Dans cette section, nous présenterons quelques exemples d'IDS ou d'IPS qui peuvent être une solution open source ou commerciale. Pour tout exemple présenté, ses avantages, ses faiblesses et ses classifications seront notés.

5.3.4.1. *Snort*

Snort est un IDS/IPS gratuit disponible sur www.snort.org. Il dispose de plusieurs modes de fonctionnement qui sont les suivants :

– mode « écoute » : ce mode permet de lancer Snort en mode *sniffer* et permet d'observer les paquets que l'IDS perçoit ;

– mode « LOG de paquets » : le LOG de paquet permet l'archivage des paquets circulant sur le réseau de l'IDS. Il permet grâce à ses arguments des opérations intéressantes permettant de limiter les logs à certains critères, comme une plage d'adresse ;

– mode « détection d'intrusion » : le mode IDS permet à Snort d'adopter un comportement particulier en cas de détection d'une (succession) de chaînes de caractères dans les paquets interceptés, et ce selon les règles définies dans les fichiers de configuration.

Les alertes émises par Snort peuvent être de différentes natures. Par exemple, on peut spécifier à Snort de rediriger l'intégralité des alarmes sur la sortie standard et ainsi observer l'évolution des attaques.

Snort est aussi capable d'adopter des comportements visant à interdire l'accès à certaines adresses IP, dans le cas où ces dernières auraient tenté de pénétrer le réseau. L'IDS peut alors interagir avec le *firewall* afin qu'il mette à jour ses règles d'accès pour empêcher tout contact avec l'éventuel pirate.

5.3.4.2. *Cisco IOS IPS*

La mise en place d'un tel IPS nécessite les étapes suivantes :

1) télécharger les fichiers IOS IPS. Rechercher un IPS convenable à partir du site officiel Cisco ;

2) créer un répertoire de configuration IOS IPS dans Flash :

```
R#mkdir IPSDIR
```

3) configurer une clé de chiffrement IOS IPS :

```
R#crypto key pubkey-chain rsa
```

4) activer IOS IPS :

```
R(config)#ip ips name IOSIPS
R(config)#ip ips name IOSIPS list <ACL-flux-concerné>
R(config)#ip ips config location flash:IPSDIR
R(config)#ip ips notify sdee
R(config)#ip ips notify LOG
R(config)#ip ips signature-category
R(config-ips-category)#category all
R(config-ips-category-action)#retired true
R(config-ips-category-action)#exit
R(config-ips-category)#category ios_ips basic |
advanced
R(config-ips-category-action)#retired false
R(config-ips-category-action)#end
R(config)#interface g0/0
R(config-if)#ip ips IOSIPS in | out
```

5) charger le package de signatures IOS IPS sur le routeur. Télécharger et copier le package des signatures à partir du serveur FTP approprié :

```
R#copy ftp://ftp-user:password@server_IP_adress/sign
_package idconf
```

5.4. Conclusion

Bien qu'ils représentent une solution spécifique, les antivirus sont des outils primordiaux pour sécuriser les systèmes informatiques. Actuellement les solutions modernes de sécurité permettent de grouper dans une même application plusieurs outils de sécurité, on parle des antivirus, des antispam, des *antispyware*, antimalware, etc. aussi bien que des fonctionnalités de *firewalling*, en l'occurrence le filtrage et le traçage.

Les IDS représentent une solution qui bien que complexe reste nécessaire pour assurer la sécurité d'un système informatique machine ou réseau. Assemblée avec d'autres outils, elle permet de diminuer l'effet des attaques.

Les IDS sont généralement négligés par les utilisateurs qui les confondent avec les antivirus bien qu'ils présentent des solutions complémentaires. Les IDS sont des solutions plus évoluées et plus complexes et leur déploiement au niveau des systèmes critiques représente un besoin inévitable mais reste optionnel pour l'utilisation domestique.

Chapitre 6

Techniques et outils de chiffrement, IPSec et VPN

6.1. Introduction

Le chiffrement est une technique très ancienne utilisée pour assurer la confidentialité des informations aussi bien en local qu'à travers le réseau. Elle a vu depuis son apparition plusieurs évolutions. Cependant, cette technique n'est pas au-dessus de toute possibilité de divulgation par les hackers. Son importance se mesure par le temps nécessaire pour casser cette technique.

Le chiffrement, une branche de la mathématique, n'est pas lié à l'informatique. Il existe depuis plusieurs siècles au cours desquels il a été scrupuleusement utilisé dans un contexte de guerre ou lors de la transmission d'informations critiques. Historiquement, plusieurs actions ont été menées et plusieurs plans ont été déjoués pour la simple raison que la partie tierce avait décodé le chiffrement comme c'est le cas de la Deuxième Guerre mondiale où des défaites ont été causées par la divulgation du mécanisme de chiffrement.

Actuellement, le chiffrement est devenu nécessaire et ne cesse d'envahir tous les domaines et toutes les activités, il est devenu une mesure nécessaire et inévitable dans le processus de sécurisation de n'importe quelle activité.

Plusieurs techniques de chiffrement ont vu le jour et touchent à plusieurs niveaux du modèle d'inférence TCP/IP. On peut citer à titre d'exemple le SSL au niveau applicatif et l'IPSec au niveau réseau et transport. Ces techniques permettent d'assurer l'authentification et/ou la confidentialité des paquets IP ou de leur contenu seulement.

Les VPN représentent une solution de communication très répandue puisqu'elle englobe deux avantages : coût limité et forte sécurité. Le déploiement des VPN ne cesse d'être de plus en plus répandu comme solution alternative pour les liaisons spécialisée et principalement pour les communications qui ne nécessitent pas un débit important. On peut citer à titre d'exemple l'interconnexion des différentes agences au sein d'une entreprise installée sur plusieurs sites distants, le télétravail ou tout autre accès à l'entreprise *via* Internet.

Les VPN représentent une application du mode tunnel de l'IPSec ou tout autre protocole de tunnelisation, ce qui permet de transmettre sur les infrastructures d'un réseau public des informations chiffrées qui ne peuvent pas être décortiquées par une tierce partie.

6.2. Techniques de chiffrement

Avec l'apparition de l'informatique et la prolifération de l'utilisation des réseaux marquée par l'accès facile à l'information qu'elle assure, il est, en effet, possible d'accéder sans aucun handicap à l'information aussi bien stockée sur les machines que transmise sur le réseau. La cryptographie a été utilisée depuis des siècles afin de transmettre des informations critiques principalement dans un contexte de guerre entre les dirigeants et les individus.

Le chiffrement, ou encore le cryptage, représente un mécanisme de sécurité d'importance capitale, il permet d'assurer le service de confidentialité et d'interdire l'attaque passive.

Il peut être résumé par le schéma 6.1.

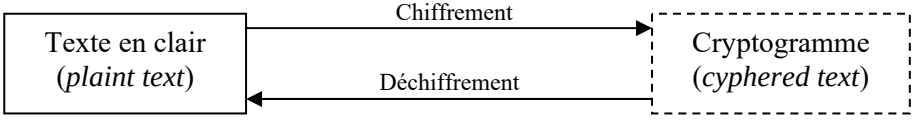

Figure 6.1. *Principe de chiffrement/déchiffrement*

Le chiffrement est le fait d'obtenir le texte chiffré (*ciphered text*) à partir d'un texte en clair (*plaint text*) en utilisant les outils nécessaires. C'est le fait de modifier un texte en clair et de le rendre incompréhensible par une entité tierce.

Le déchiffrement est l'opération inverse en utilisant les outils nécessaires.

6.2.1. *Principes de base du chiffrement*

Le chiffrement consiste à trouver des moyens permettant d'obtenir un cryptogramme à partir d'un texte qu'on se propose de sécuriser. Il s'agit d'une action réversible pour pouvoir obtenir le texte en clair correspondant lors de l'opération de déchiffrement.

Le chiffrement se base sur deux techniques complémentaires de base : substitution et décalage. Elles peuvent être appliquées plusieurs fois en cascade pour rendre le chiffrement plus fort.

6.2.1.1. *Substitution*

C'est une technique primitive de substitution mono-alphabétique manuelle, c'est le fait d'associer à chaque caractère un caractère différent. Les deux parties se mettent d'accord sur cette correspondance, ce qui nécessite d'être formulé et mémorisé par les deux parties.

EXEMPLE.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	A	W	X	S	Z	E	D	C	V	F	R	T	G	B	N	H	Y	U	J	K	I	O	L	M	P

"SECURITEINFOMRATIQUE" → "USWKYCJSCGZBYTQJCHKS"

6.2.1.2. *Décalage*

C'est le fait d'associer à un caractère le caractère correspondant selon un décalage d'un nombre choisi : c'est le pas. On parle du chiffrement de César, il s'agit d'une technique de chiffrement ancienne de substitution mono-alphabétique. Le pas représente une sorte de clé puisque la connaissance de ce nombre permet de déterminer complètement le cryptogramme lors du chiffrement, et inversement le texte en clair correspondant lors du déchiffrement.

EXEMPLE. Décalage de 2.

« SECURITEINFOMRATIQUE » → « UGEWTKVGKOHQTOCVKSWG »

En plus de ces deux techniques de base, d'autres techniques de substitution multi-alphabétique permettent de rendre le chiffrement encore plus fort. Le texte en clair peut subir des transformations diverses avant ou tout au long du processus de chiffrement.

6.2.2. *Cryptanalyse*

Le chiffrement, aussi fort qu'il soit, n'est pas au-dessus de toute critique dans la mesure où il peut être découvert et l'attaquant peut obtenir le texte en clair à partir d'un texte chiffré sans connaître quoi que ce soit sur la technique de chiffrement utilisée. L'effort de Turing lors de la Deuxième Guerre mondiale en représente une bonne illustration.

La cryptanalyse est une technique utilisée par les hackers afin de casser le chiffrement. Il consiste à analyser un texte chiffré dans le but d'obtenir le texte en clair correspondant.

6.2.2.1. *Mécanismes de la cryptanalyse*

La cryptanalyse utilise plusieurs mécanismes qui se basent sur des statistiques au niveau des langues (exemples : « ing » se trouve dans 4 % d'un texte anglais, « tion » dans 2 % d'un texte français, etc.) ou en se basant sur des phrases et expressions couramment utilisées au niveau des messages. Actuellement, avec la puissance des ordinateurs, on peut les utiliser pour des tâtonnements systématiques.

L'attaquant peut procéder de plusieurs façons :

– extraire des hypothèses sur un texte chiffré dont il possède le texte en clair correspondant pour casser le chiffrement d'un autre texte cible chiffré de la même façon ;

– chiffrer un texte bien choisi pour pouvoir déterminer certaines caractéristiques de la technique du chiffrement en question ;

– examiner les répétitions des lettres du cryptogramme afin d'obtenir la clé, c'est l'analyse fréquentielle, une attaque qui vise le chiffrement par substitution mono-alphabétique ;

– calculer la probabilité de répétitions des lettres du cryptogramme, c'est l'analyse par coïncidence ;

– tester tous les mots d'une liste comme clé, c'est l'analyse par dictionnaire ou encore attaque par force brute ;

– faire une approximation linéaire de la structure interne de la méthode de chiffrement, c'est la cryptanalyse linéaire ;

– modifier légèrement le texte en clair à chiffrer et faire des analyses statistiques dans la structure de la méthode de chiffrement, c'est la cryptanalyse différentielle ;

– combiner les deux dernières méthodes, c'est la cryptanalyse différentielle-linéaire.

6.2.2.2. *Mesure de robustesse d'une solution de chiffrement*

La cryptanalyse tente théoriquement dans tous les cas de trouver le texte en clair à partir d'un texte chiffré avec un coût matériel et temporel plus au moins important. N'importe quelle information possède une durée limitée de sa confidentialité. La robustesse d'un algorithme de chiffrement se mesure par le temps nécessaire à la cryptanalyse qui doit être nettement supérieur au temps de validité de l'information (temps pendant lequel l'information reste confidentielle).

Une information politique ou même militaire possède une durée de validité théorique, de ce fait, il fallait prévoir une technique de chiffrement dont la durée théorique nécessaire pour la cryptanalyse dépasse la durée de validité de l'information en question, ce qui rend sans intérêt toute divulgation d'un message chiffré.

6.2.3. *Évolution de la cryptographie*

L'évolution de l'informatique et des techniques de transmission a engendré un nouveau défi, c'est la confidentialité, et le chiffrement se présente comme solution à ce dernier défi. Le chiffrement a subi tout au long de son histoire plusieurs évolutions dont les plus importantes vont être abordées dans les sections suivantes.

6.2.3.1. *Algorithme partagé secret*

Cette génération représente les premières solutions de chiffrement ayant vu le jour. On peut l'illustrer par un tableau de correspondance entre les caractères et

leur remplacement. Ce tableau doit rester à l'abri de toute divulgation pour assurer la confidentialité.

6.2.3.1.1. Principe

Il consiste à choisir un algorithme, voir la figure 6.2, partagé entre deux ou plusieurs intervenants et qui reste secret entre les parties concernées. Cet algorithme sera utilisé aussi bien pour le déchiffrement que pour le chiffrement.

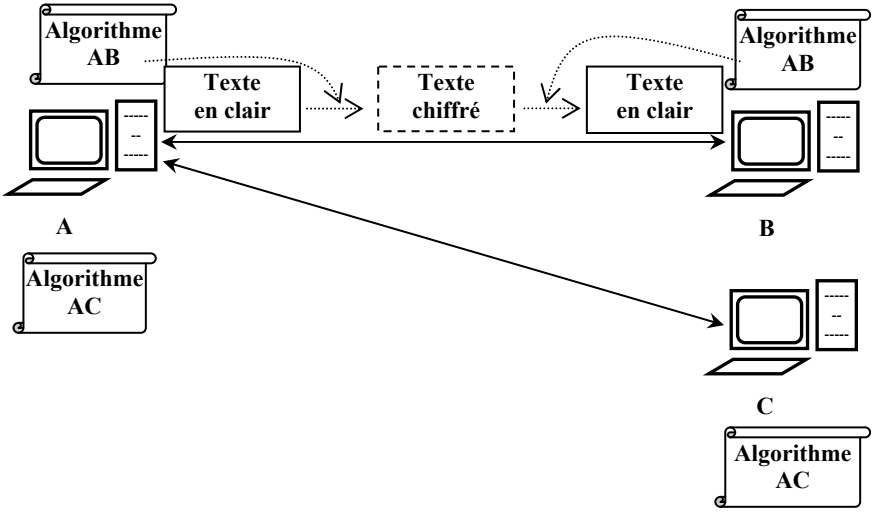

Figure 6.2. *Chiffrement à algorithme secret partagé*

6.2.3.1.2. Limites

Cette solution de chiffrement présente un certain nombre de lacunes :

– la difficulté du choix de l'algorithme et l'évaluation de sa robustesse ;

– le problème de partage de l'algorithme, quelque chose de complexe donc difficile à retenir et admettant une durée de vie importante, ce qui facilite sa divulgation.

6.2.3.2. *Algorithme à clé symétrique partagée*

Cette génération est apparue en réponse aux limites identifiées au niveau de la génération précédente. On assiste à l'apparition de la notion de clé qui représente généralement le *hashcode* associé à un mot de passe choisi par l'utilisateur. Cette

approche représente une révolution dans le domaine de la cryptographie. Plusieurs algorithmes de ce type ont vu le jour.

6.2.3.2.1. Principe

Les problèmes inhérents à l'utilisation de la méthode précédente ont favorisé la survenue de cette technique qui consiste à utiliser des algorithmes connus et judicieusement choisis et à associer à chaque utilisation de cet algorithme une clé qui sera secrète et partagée entre les deux intervenants (exemple : le pas dans le cas de l'algorithme de César). Elle sera utilisée à la fois pour le chiffrement et le déchiffrement (symétrie) comme présenté dans la figure 6.3. On peut citer à titre d'exemples les algorithmes suivants : DES, 3DES, Blowfish.

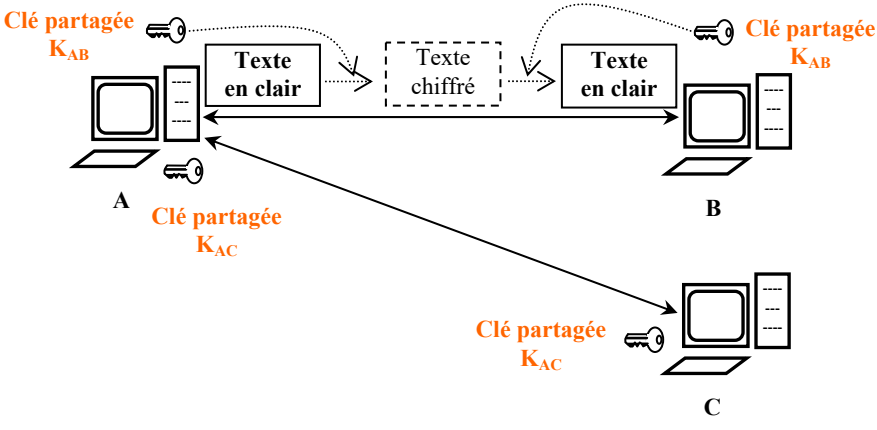

Figure 6.3. *Chiffrement à clé symétrique partagée*

EXEMPLES.

– DES : *Data Encryption Standard* depuis 1977, utilise une clé de 56 bits.

– 3DES : une variante du DES avec trois reprises avec trois clés différentes (A-B-C 168 bits) ou avec deux clés différentes (A-B-A 112 bits).

– RC2, RC4 et RC5 : ils utilisent des clés jusqu'à 1 024 bits.

– Blowfish.

– IDEA : *International Data Encryption Algorithm*.

– AES : *Advanced Encryption Standard* depuis 2001.

6.2.3.2.2. Limites

Cette technique admet aussi des limites moins intenses que celle de la première :

– problème de partage de clé, ce qui facilite sa divulgation et exige sa modification périodique ;

– autant de clés que de communication pour une entité donnée, ce qui engendre une tâche supplémentaire de gestion des clés.

6.2.3.3. *Algorithme à clés asymétriques*

Au niveau des deux générations précédentes, le problème majeur, c'est celui du partage (d'algorithme ou de clé). En effet, le partage de quelque chose de secret représente un scénario paradoxal, le partage facilite la divulgation ou encore il augmente l'incertitude des deux parties l'une vis-à-vis de l'autre. Il était nécessaire de trouver une solution qui élimine complètement le partage à travers des algorithmes dont l'utilisation est basée sur le choix d'une paire de clés et non plus d'une simple clé.

6.2.3.3.1. Principe

Cette technique a vu le jour pour résoudre le problème du partage identifié au niveau des techniques utilisées précédemment et par suite de l'apparition d'une nouvelle génération d'algorithmes. On peut associer à chaque utilisation une paire de clés (k1, k2) telles que si on en utilise une pour chiffrer, on ne peut déchiffrer que par l'autre et inversement ($D_{k1}(C_{k2}(X)) = X$ et $D_{k2}(C_{k1}(X)) = X$).

L'idée consiste à associer à chaque intervenant une paire de clés dont une sera désignée comme clé privée secrète et l'autre comme clé publique accessible à tout le monde comme l'illustre la figure 6.4.

EXEMPLES.

– RSA : *Rivest Shamir Adleman*. Cet algorithme a été décrit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman. Il est basé sur l'utilisation

d'une paire de clés composée d'une clé publique pour chiffrer (respectivement vérifier) et d'une clé privée pour déchiffrer (respectivement signer) des données confidentielles.

– DSA : *Digital Signature Algorithm*. C'est un algorithme de signature à clé publique. La clé privée est utilisée pour générer une valeur digitale appelée signature, la clé publique sert à vérifier cette signature.

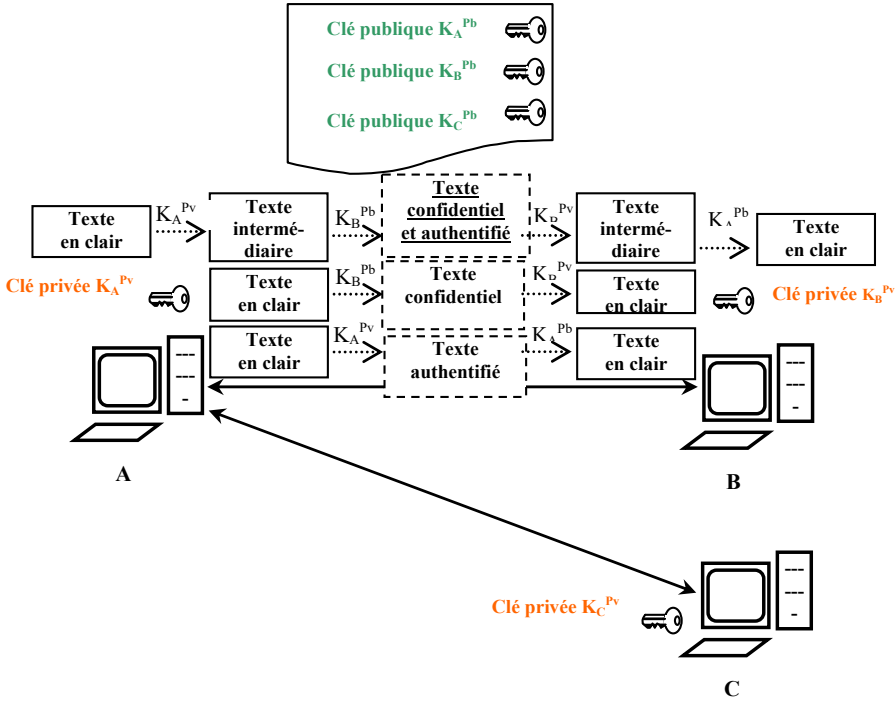

Figure 6.4. *Chiffrement à clés asymétriques*

6.2.3.3.2. Limites

Cette solution, bien qu'elle permette d'éviter le problème de partage, constitue une solution complexe. De plus, la question de la confiance quant à la clé publique se pose.

6.2.4. *Notion de certificat*

Les certificats permettent de résoudre le problème d'affectation des clés. Le certificat est un document numérique qui permet de s'assurer qu'une clé publique est associée à la personne ou l'entité concernée. Il comporte les informations suivantes :

– la clé publique ;

– le nom du propriétaire ;

– la date d'expiration de la clé ;

– le nom du responsable de certification ;

– le numéro de série du certificat.

L'ensemble de ces informations est signé par une autorité de confiance appelée autorité de certification puisqu'elle contient une empreinte (le *hashcode* relatif à l'ensemble des informations ci-dessus) chiffrée par la clé privée de l'autorité de certification comme le présente la figure 6.5. C'est le cas des certificats x509.

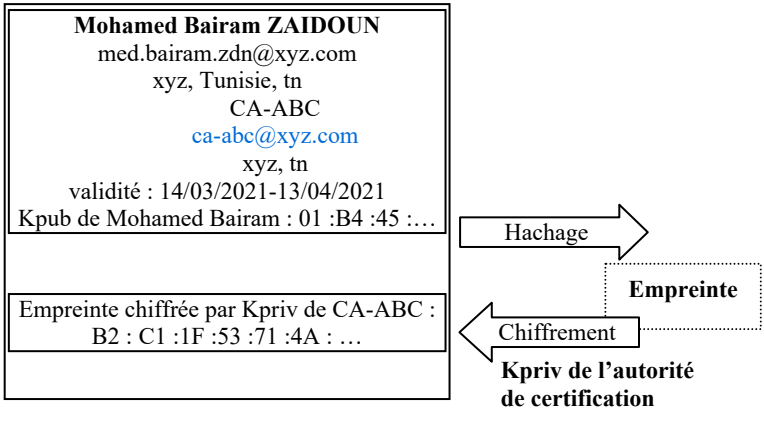

Figure 6.5. *Certificat x509 signé par l'autorité de certification*

La vérification selon la figure 6.6 se fait en comparant le *hashcode* des informations à la chaîne obtenue en déchiffrant l'empreinte par la clé publique de l'autorité de certification.

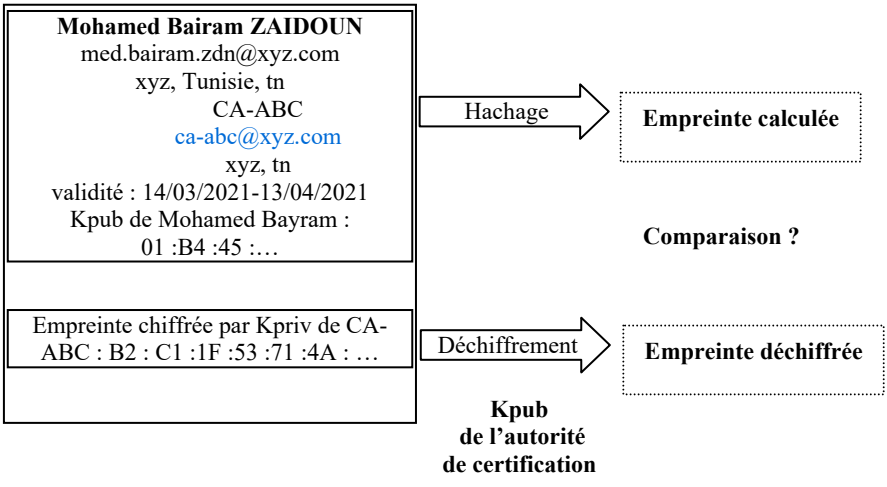

Figure 6.6. *Vérification de la validité du certificat x509*

6.2.5. *Comparaison entre les techniques de chiffrement*

Les trois générations de solutions de chiffrement présentent plusieurs points de rencontre et plusieurs points de différence en termes de principe, d'utilisation et de champs d'application. Une comparaison de ces techniques est présentée dans le tableau 6.1.

Technique de chiffrement / Caractéristique	À algorithme partagé	À clé partagée symétrique	À clés asymétriques
Définition des caractéristiques	Algorithme par communication	Clé par communication	Paire de clés par intervenant
Problème de partage	Oui (algorithme)	Oui (clé)	Non
Couplage authentification/confidentialité	Oui	Oui	Non
Gestion de clés	Pas de gestion	Gestion difficile (autant de clés que de communications)	Gestion simple (publication des clés publiques)
Complexité	Complexité de choix de l'algorithme et son évaluation	Complexité modérée	Complexité d'utilisation

Tableau 6.1. *Comparaison entre les différentes techniques de chiffrement*

6.3. IPSec

L'IPSec permet d'assurer l'authentification des paquets IP à travers le protocole AH et la confidentialité des données à travers le protocole ESP.

Le protocole IPSec est applicable selon deux modes, le mode transport et le mode tunnel. Le premier est le mode le plus simple, il concerne uniquement la partie données tandis que le second permet de sécuriser tout le paquet IP (en-tête et partie données). On parle d'encapsulation IP in IP. Le mode tunnel est utilisé, parmi d'autres, comme technique de base pour implémenter les VPN.

La famille de protocoles IPSec comporte deux techniques complémentaires AH et ESP. L'IPSec dispose aussi de l'implémentation de plusieurs algorithmes de chiffrement (DES, 3DES, Blowfish, RSA, etc.) et de hachage (MD5, SHA1, etc.). La configuration d'une communication IPSec détermine le choix convenable des algorithmes à utiliser. L'IPSec a été défini par l'IETF par une suite de 40 RFC permettant de spécifier tous les aspects de ce protocole. D'ailleurs, l'IPSec est intégré automatiquement au niveau de l'IPv6.

L'IPSec utilise la notion d'association de sécurité (*Security Association*) pour définir l'utilisation et le paramétrage de sécurité à appliquer par les différentes parties.

Une association de sécurité IPSec est une structure de données servant à stocker l'ensemble des paramètres de sécurité associés à une communication. Une SA étant unidirectionnelle, il faut deux SA pour protéger une communication dans les deux sens.

6.3.1. *AH*

AH (*Authentication Header*) est un protocole qui assure l'authentification et l'intégrité des paquets IP. Il est applicable en mode transport et en mode tunnel.

Le protocole AH fournit les services de sécurité suivants :

– intégrité en mode non connecté ;

– authentification des données ;

– anti-rejeu (optionnel).

6.3.2. *ESP*

ESP (*Encapsulating Security Payload*) est un protocole IPSec qui assure la confidentialité et peut assurer l'authentification, l'intégrité des données et l'anti-répudiation des sessions. Il est applicable en mode transport et en mode tunnel.

Le protocole ESP fournit les services de sécurité suivants :

– confidentialité ;

– protection contre l'analyse de trafic ;

– intégrité en mode non connecté (comme ah) ;

– authentification des données (comme ah) ;

– anti-rejeu (comme ah).

En effet, ESP couvre les services offerts par AH.

6.3.3. *Différents modes IPSec*

La sécurité peut concerner seulement la partie données d'un paquet IP comme elle peut s'appliquer à la totalité du paquet (en-tête et partie données). On distingue deux modes d'application de l'IPSec.

6.3.3.1. *Mode transport*

Il assure la sécurité de la partie de données d'un paquet IP. Le mode transport est le mode par défaut d'IPSec et est utilisé pour les communications de bout en bout (communications entre un client et un serveur). Lorsque le mode transport est utilisé, IPSec crypte uniquement la charge utile IP. Le mode transport assure la protection de la charge utile IP au moyen d'un en-tête AH ou ESP.

6.3.3.2. *Mode tunnel*

Il assure la sécurité d'un paquet IP (en-tête + données). Lorsque le mode tunnel IPSec est utilisé, IPSec crypte l'en-tête IP et la charge utile.

Le mode tunnel assure la protection de la totalité d'un paquet IP en le considérant comme une charge utile AH ou ESP. En mode tunnel, un paquet IP complet est encapsulé avec un en-tête AH ou ESP et un en-tête IP supplémentaire.

Les adresses IP de l'en-tête IP extérieur représentent les points d'arrêt du tunnel, alors que celles de l'en-tête IP encapsulé constituent les véritables adresses source et destination.

Le mode tunnel IPSec est utile pour protéger le trafic entre les différents réseaux lorsque le trafic doit passer par un réseau intermédiaire non approuvé. Il est principalement utilisé pour assurer l'interopérabilité avec les passerelles et systèmes terminaux qui ne prennent pas en charge les connexions IPSec.

On peut utiliser le mode tunnel dans les configurations suivantes :

– passerelle vers passerelle ;

– serveur vers passerelle ;

– serveur vers serveur.

6.3.4. *Différentes implémentations de l'IPSec*

Depuis son apparition, la famille de protocole IPSec a été implémentée à plusieurs reprises. On assiste à une divergence énorme, ce qui représente un handicap devant l'adaptation de telle solution vu l'incompatibilité.

D'un point de vue pratique, IPSec est un protocole relativement difficile à implémenter d'une part à cause de sa complexité intrinsèque (multiples sous-protocoles, etc.) et d'autre part à cause de ses interactions avec les processus réseau courants. De ce fait, il existe trois variantes d'implémentations :

– la modification de la pile IP du noyau : reste la méthode la plus directe et sans doute la plus compliquée. Cette méthode est applicable à tout type d'entités (hôtes ou passerelles) ;

– la « Bump-In-The-Stack » (BITS) : consiste à séparer les routines de traitement IPSec des routines habituelles de la pile IP (le code spécifique à IPSec vient en fait s'intercaler entre la couche réseau et la couche liaison/physique, d'où le nom de la méthode). Certains éléments restent tout de même à modifier dans cette pile, comme la fragmentation et le réassemblage des paquets. Néanmoins, le noyau reste intact dans ce type d'implémentation. Cette méthode est applicable à tout type d'entités (hôtes ou passerelles) ;

– la « Bump-In-The-Wire » (BITW) : consiste à écarter le traitement d'IPSec – et donc le code – dans un élément dédié placé en amont sur le réseau (d'où son nom), à l'extérieur de la machine. Un tel élément peut être soit une « boîte » dédiée, soit un *firewall*, un routeur, etc. Suivant son type, cette méthode ne s'appliquera pas à toute sorte d'hôtes.

6.3.5. *Différentes encapsulations IPSec*

Cette partie sera consacrée à la présentation des différentes transformations possibles sur le paquet IP lors de l'application de chacune des techniques (AH et ESP) de chacun des modes (transport et tunnel).

6.3.5.1. *AH en mode transport*

L'AH en mode transport consiste à authentifier la partie données du paquet IP. Cette tâche nécessite l'ajout d'un en-tête AH à la partie données du paquet résultat tout en gardant intact l'en-tête du paquet d'origine.

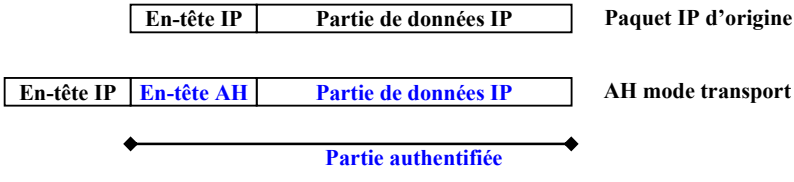

Figure 6.7. *Encapsulation AH en mode transport*

6.3.5.2. *ESP en mode transport*

L'ESP en mode transport consiste à chiffrer la partie données du paquet IP.

Cette tâche nécessite l'ajout d'un en-tête ESP et d'une queue ESP à la partie données du paquet résultat tout en gardant intact l'en-tête du paquet d'origine.

La partie données du paquet résultant, composée de l'en-tête ESP ajouté et de la partie données du paquet d'origine, sera authentifiée.

Le chiffrement et l'authentification concernent aussi une partie de la queue.

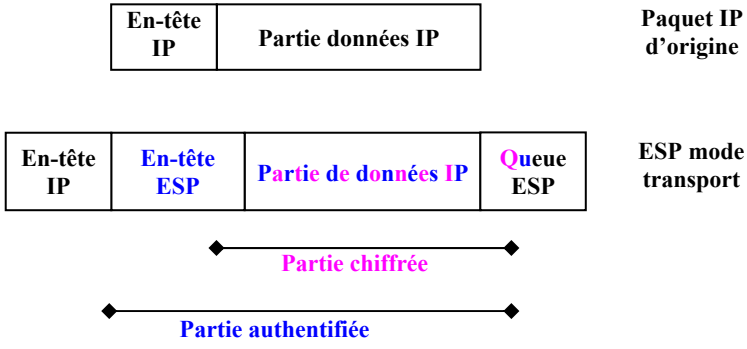

Figure 6.8. *Encapsulation ESP en mode transport*

6.3.5.3. *AH-ESP en mode transport*

L'AH-ESP en mode tunnel consiste à chiffrer la partie données du paquet IP en premier lieu en utilisant le protocole ESP avant d'appliquer le protocole AH pour remettre à la fin l'en-tête original du paquet IP.

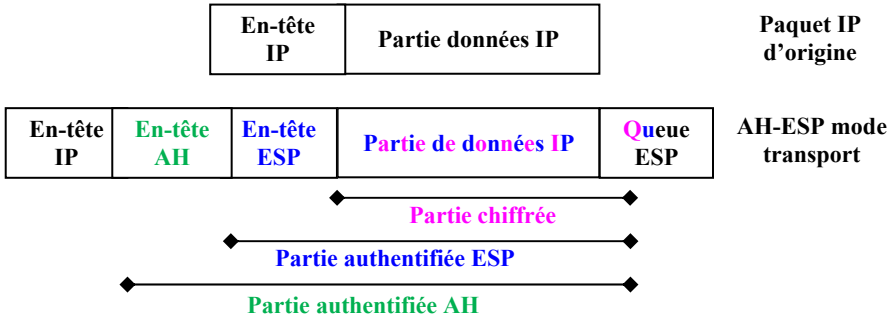

Figure 6.9. *Encapsulation AH-ESP en mode transport*

6.3.5.4. *AH en mode tunnel*

L'AH en mode tunnel consiste à authentifier la totalité du paquet IP (en-tête + partie données).

Cette tâche nécessite l'ajout d'un en-tête AH et d'un nouvel en-tête IP pour former un nouveau paquet avec des caractéristiques différentes.

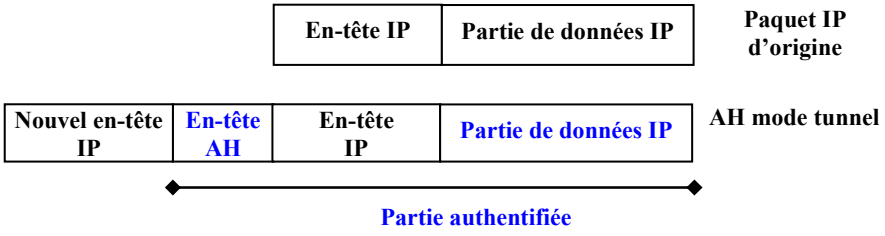

Figure 6.10. *Encapsulation AH en mode tunnel*

6.3.5.5. *ESP en mode tunnel*

L'ESP en mode tunnel consiste à chiffrer la totalité du paquet IP (en-tête + partie données). Cette tâche nécessite l'ajout d'un en-tête ESP et d'un nouvel en-tête IP pour former un nouveau paquet avec des caractéristiques différentes.

La partie données du paquet résultant, composée de l'en-tête ESP ajouté et de la totalité du paquet d'origine, sera authentifiée.

Le chiffrement et l'authentification concernent aussi une partie de la queue.

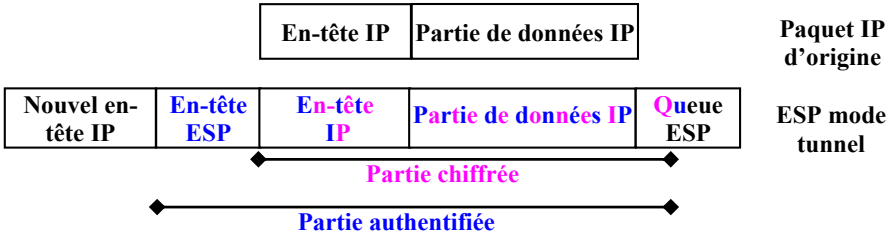

Figure 6.11. *Encapsulation ESP en mode tunnel*

6.3.5.6. *AH-ESP en mode tunnel*

L'AH-ESP en mode tunnel consiste à chiffrer la totalité du paquet IP (en-tête + partie données) en premier lieu en utilisant le protocole ESP avant d'appliquer le protocole AH pour générer à la fin un nouveau paquet IP.

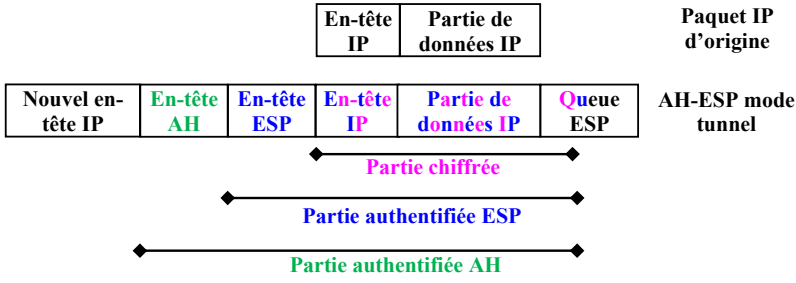

Figure 6.12. *Encapsulation AH-ESP en mode tunnel*

6.3.6. *Protocole IKE*

IKE est l'acronyme d'*Internet Key Exchange*. C'est un protocole d'échange de clés et de négociation des paramètres de sécurité. Il permet d'assurer la phase de mise en place des SA (*Security Association*) entre les partenaires, en l'occurrence les extrémités du tunnel.

SA représente un ensemble de paramètres de sécurité unidirectionnelle, il englobe les algorithmes à utiliser pour l'authentification, le chiffrement et le contrôle d'intégrité.

Les SA peuvent être négociées manuellement ou à travers le protocole ISAKMP. ISAKMP (*Internet Security Association and Key Management Protocol*) est utilisé pour la négociation, l'établissement, la modification et la suppression des SA et des paramètres associés. Il définit les procédures et les formats de paquets pour la création et la gestion d'authentification par les pairs des SA et les techniques de génération de clés.

IKE comporte deux phases :

– phase 1 : permet de négocier la politique ISAKMP pour la création du tunnel d'une part et l'échange de clés en utilisant le protocole DH (*Diffie-Hellman*) d'autre part avant de faire la vérification des identités ;

– phase 2 : consiste à négocier la politique IPSec pour transmettre le trafic d'une façon sécurisée à travers le tunnel.

6.4. VPN

VPN est l'acronyme de *Virtual Private Network* ou encore Réseau privé virtuel. C'est le fait de déployer des ressources publiques et de travailler d'une façon sécurisée en utilisant le chiffrement comme s'il s'agissait d'un réseau privé.

6.4.1. *Problématique et raisons d'être*

On se propose d'interconnecter des sites distants relatifs à une même entreprise (banque, assurance, etc.). Deux solutions sont envisageables : une solution publique et une solution privée.

La première solution consiste à utiliser Internet pour communiquer. C'est une solution non coûteuse mais aussi non sécurisée puisque l'on partage le même réseau avec des intervenants divers.

La deuxième solution consiste à déployer des liaisons spécialisées. Une infrastructure complètement privée, donc sécurisée, mais elle est très coûteuse.

Face à ce choix, le VPN s'impose comme solution d'interconnexion optimale sur le plan sécurité/coût.

6.4.2. *Principe du VPN*

La mise en place d'un VPN consiste à utiliser des tunnels pour communiquer *via* Internet au lieu de déployer les liaisons spécialisées.

Un tunnel permet de sécuriser aussi bien les données que l'identité des intervenants, on parle d'encapsulation IP in IP. Le nouveau paquet IP généré aura comme source et destination les adresses WAN des routeurs au niveau des deux réseaux locaux qui communiquent *via* Internet par le tunnel.

En effet, un VPN repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie.

Le terme tunnel est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN, les données sont chiffrées et donc normalement incompréhensibles pour

toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. De plus, créer un tunnel signifie encapsuler un protocole dans un protocole de même niveau que le modèle OSI (IP dans IPsec par exemple). Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer les données à l'entrée et serveur VPN (ou plus généralement serveur d'accès distant) l'élément déchiffrant les données en sortie. C'est le cas lorsqu'un système extérieur à un réseau privé (client nomade, agence ou travailleur à domicile) souhaite se connecter au réseau de son entreprise où :

– les paquets (qui contiennent les données) sont chiffrés par le client VPN (selon l'algorithme décidé par les deux interlocuteurs lors de l'établissement du tunnel VPN) et éventuellement signés ;

– ils sont transmis par le biais du réseau transporteur (Internet en général) ;

– ils sont reçus par le serveur VPN qui les déchiffre, les traite et regarde si les vérifications requises sont correctes.

6.4.3. *Différents types de VPN*

Selon les deux extrémités qui exploitent le VPN, on distingue deux types : VPN *Site-to-Site* et VPN d'accès distant.

6.4.3.1. *VPN* Site-to-Site

C'est un cas de figure qui permet d'interconnecter deux réseaux sur deux sites distants moyennant la configuration d'un VPN entre les routeurs qui représente l'interface avec laquelle s'effectue la connexion Internet de part et d'autre des deux sites. La bonne marche de ce dispositif réside dans l'interconnexion de deux ou plusieurs agences relevant d'une entreprise quelconque ou du site central. Un tel tunnel VPN peut être aussi utilisé pour interconnecter un fournisseur et un client. Ce type de VPN peut représenter une solution optimale à la fois sécurisée et peu coûteuse pour assurer l'interconnectivité totale d'une entreprise avec des sites distants.

6.4.3.2. *VPN d'accès distant*

Il s'agit d'une solution d'interconnectivité sécurisée *via* Internet d'un utilisateur nomade ou d'un bureau à domicile à un réseau distant. Cette technique

permet d'offrir une alternative pour faciliter le télétravail ou à un utilisateur isolé de se connecter à l'entreprise sans mettre en cause sa sécurité tout en se mettant à l'abri des attaques menées par les hackers et les pirates réseaux.

Ce type de VPN permet à l'entreprise d'interconnecter ses collaborateurs distants qui seront amenés à partager les services de l'entreprise pour un moindre coût et en toute sécurité.

6.4.4. *Différents protocoles de tunnelisation*

Les tunnels VPN peuvent être basés sur plusieurs protocoles :

– PPTP (*Point-to-Point Tunneling Protocol*) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics ;

– L2F (*Layer Two Forwarding*) est un protocole de niveau 2 développé par Cisco Systems, Nortel et Shiva ;

– L2TP (*Layer Two Tunneling Protocol*) est l'aboutissement des travaux de l'IETF (RFC 3931) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP ;

– IPSec (IP sécurisé) est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP ;

– SSL/TLS (*Secure Sockets Layer*/*Transport Layer Security*) offre une très bonne solution de tunnelisation. L'avantage de cette solution est d'utiliser un navigateur web comme client VPN ;

– SSH (*Secure Shell*) est initialement connu comme le remplacement sécurisé de telnet, il offre la possibilité de tunneliser des connexions de type TCP, permettant d'accéder ainsi de façon sûre à des services offerts sur un réseau protégé, sans créer un réseau privé virtuel.

6.4.5. *Configuration VPN IPSec* Site-to-Site

On se propose de configurer sous Cisco en mode CLI (*Command Line Interface*) un VPN IPSec *Site-to-Site* applicable à la configuration réseau de la figure 6.13.

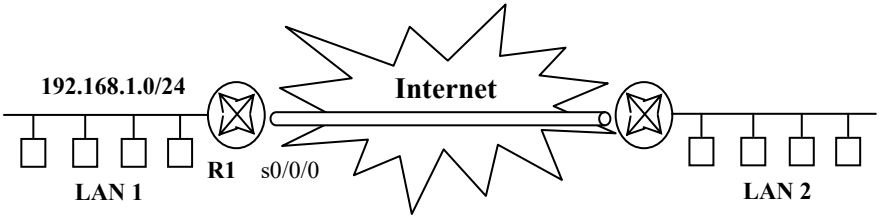

Figure 6.13. *Exemple de VPN IPSec Site-to-Site*

La configuration du tunnel est définie par le tableau 6.2.

Paramètres	R1	R2
Nom du *Transform Set*	VPN-SET	VPN-SET
Configuration de chiffrement ESP	esp-aes	esp-aes
Configuration d'authentification ESP	esp-sha-hmac	esp-sha-hmac
Adresses IP des extrémités du tunnel	10.2.2.2	10.1.1.2
Trafic chiffré	access-list 110 (source 192.168.1.0 dest 192.168.2.0)	access-list 110 (source 192.168.2.0 dest 192.168.1.0)
Nom *Crypto Map*	VPN-MAP	VPN-MAP
Moyen de génération de SA (*Security Association*)	ipsec-isakmp	ipsec-isakmp

Tableau 6.2. *Paramètres de configuration d'un tunnel IPSec*

La configuration comporte les étapes suivantes :

1) mettre à jour la licence des IOS des différents routeurs afin de supporter les nouvelles fonctionnalités de sécurité ;

```
R1(config)# license boot module c1900 technology-
package securityk9
```

```
R2(config)# license boot module c1900 technology-
package securityk9
```

2) accepter le contrat de licence de l'utilisateur final ;

3) enregistrer la configuration en cours d'exécution et recharger le routeur pour activer la licence de sécurité ;

4) vérifier que le package Security a été activé à l'aide de la commande `show version` ;

5) configurer les ACL pour identifier le trafic concerné par le tunnel sur les deux routeurs ;

```
R1(config)# access-list 110 permit ip 192.168.1.0
0.0.0.255 192.168.2.0 0.0.0.255
```

```
R2(config)# access-list 110 permit ip 192.168.2.0
0.0.0.255 192.168.1.0 0.0.0.255
```

6) configurer la politique de cryptage ISAKMP sur R1 et R2 avec la clé de cryptage partagée vpnpa55 ;

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2
```

```
R2(config)# crypto isakmp policy 10
R2(config-isakmp)# encryption aes 256
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 5
R2(config-isakmp)# exit
R2(config)# crypto isakmp key vpnpa55 address 10.1.1.2
```

7) configurer la politique IPSec IKE sur R1 et R2 à travers la création de la transform-set VPN-SET pour utiliser esp-aes et esp-sha-hmac et la création de la carte de chiffrement VPN-MAP qui permet de lier tous les paramètres de la phase 1 du protocole IKE ;

```
R1(config)# crypto ipsec transform-set VPN-SET esp-aes
esp-sha-hmac
```

```
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to
R2
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

```
R2(config)# crypto ipsec transform-set VPN-SET esp-aes
esp-sha-hmac
R2(config)# crypto map VPN-MAP 10 ipsec-isakmp
R2(config-crypto-map)# description VPN connection to
R1
R2(config-crypto-map)# set peer 10.1.1.2
R2(config-crypto-map)# set transform-set VPN-SET
R2(config-crypto-map)# match address 110
R2(config-crypto-map)# exit
```

8) lier le mappage de chiffrement VPN-MAP à l'interface série à chaque extrémité du tunnel de chaque routeur ;

```
R1(config)# interface s0/0/0
R1(config-if)# crypto map VPN-MAP
```

```
R2(config)# interface s0/0/1
R2(config-if)# crypto map VPN-MAP
```

9) vérifier le tunnel de part et d'autre sur les deux routeurs.

```
R1#show crypto ipsec sa
```

```
R2#show crypto ipsec sa
```

6.5. Conclusion

Le chiffrement est une technique très efficace afin de garantir la confidentialité et/ou l'authentification des informations locales ou des messages échangés par les applications réseaux. Une telle sécurisation reste insuffisante sans un chiffrement de bas niveau. C'est l'objet du protocole IPSec qui représente une

version de TCP/IP permettant d'assurer la confidentialité et/ou l'authentification au niveau paquet.

L'apparition de l'IPSec a été sans aucun doute une solution radicale afin de pallier les failles et les vulnérabilités de TCP/IP. Son utilisation reste timide vu la diversité et l'incompatibilité des implémentations.

L'IPSec représente l'application des techniques de chiffrement au niveau paquet pour créer une pile protocolaire sécurisée qui sera exploitée en haut niveau pour créer des VPN.

Les VPN utilisent un principe simple de tunnel, qui consiste en une encapsulation sécurisée par le chiffrement, basé sur une grande panoplie de technologies ouvertes ou propriétaires. Cette diversification représente une richesse et offre une large gamme de choix pour la mise en place des tunnels VPN. Elle offre une souplesse d'accès aux données de l'entreprise et permet d'élargir le champ d'action de la sécurité jusqu'au fournisseur, client, employé à domicile, etc. Cette technique couplée avec les techniques de virtualisation telles que le *cloud computing* permet de banaliser l'accès tout en assurant la sécurité.

Chapitre 7

Nouvelles tendances de sécurité pour SDN et IoT

7.1. Introduction

De nos jours, l'architecture classique des réseaux ne cesse de régresser au détriment de nouvelles technologies, parmi lesquelles on peut citer l'architecture SDN (*Software Defined Network*) ou encore l'architecture réseau définie par les logiciels. Cette nouvelle technologie comprend des caractéristiques et des architectures différentes permettant de causer des attaques différentes par rapport aux réseaux classiques et de représenter des défis spécifiques, ce qui exige des solutions appropriées de sécurité.

L'architecture réseau SDN a été développée à des fins de virtualisation du réseau. Elle permet de virtualiser le plan de contrôle en le déplaçant depuis chaque périphérique vers une entité centrale d'intelligence réseau et de génération de politiques, appelée « contrôleur SDN ».

D'autre part, les objets intelligents ne cessent d'envahir tous les domaines. Connectés entre eux à travers un réseau, ils se transforment de plus en plus vers l'intelligence et l'automatisation. Cette évolution considérable présente des défis aux enjeux de sécurité sur tous les plans. Ces défis, spécifiques et orientés, exigent des solutions de sécurité appropriées. En effets, ce type de réseau est cible potentielle d'intrusion dans la mesure où les objets connectés avec l'intelligence qu'ils intègrent et l'automatisation qu'ils offrent fournissent aux pirates des points de prise de contrôle et d'espionnage. Ces vulnérabilités font de la sécurité un enjeu capital en IoT/IoE.

7.2. Sécurité du réseau SDN

Les réseaux migrent progressivement vers l'automatisation et la virtualisation, ce qui ouvre la porte vers une nouvelle tendance de sécurité propre aux réseaux SDN.

7.2.1. *Description générale du réseau SDN*

SDN est l'acronyme de *Software Defined Network*, c'est une architecture réseau qui permet de séparer les données (trafic utile) du contrôle (trafic de gestion de réseau). L'architecture SDN est constituée de trois couches séparées par des interfaces par lesquelles des informations de contrôle et de gestion sont envoyées.

Le réseau SDN a des fonctionnalités spécifiques par rapport au réseau classique, il admet une architecture centralisée dans la mesure où la gestion du trafic réseau est effectuée par un équipement central appelé le contrôleur (SDN *Controller*). Il communique avec la couche d'infrastructure contenant les différents composants réseau à travers une interface de communication appelée *SouthBound* et il communique avec la couche de management contenant les équipements et les applications d'administration et de supervision à travers une interface de communication appelée *NorthBound*.

Le réseau SDN peut être géré par des scripts et des programmes écrits dans des langages de programmation de haut niveau tels que Java, Python, C, P4, etc.

Les deux fonctionnalités, centralisation et programmabilité, permettent de faire de SDN un réseau flexible dont la gestion est effectuée facilement à travers les mécanismes et les outils de virtualisation.

Ces fonctionnalités font que SDN déclenche différentes attaques, présente des vulnérabilités différentes et fournit différentes solutions de sécurité. Les défis de sécurité sont très différents des réseaux classiques.

Le réseau SDN peut être géré en collaboration avec une solution de *cloud computing* qui est utilisée pour stocker les règles et les politiques. Dans une sécurité basée sur le cloud, le contrôleur SDN récupère les actions de sécurité des services cloud afin de créer des règles de flux pour accomplir des actions de sécurité.

7.2.2. *Architecture du réseau SDN*

L'architecture d'un réseau SDN, représentée par la figure 7.1, est composée hiérarchiquement de trois couches.

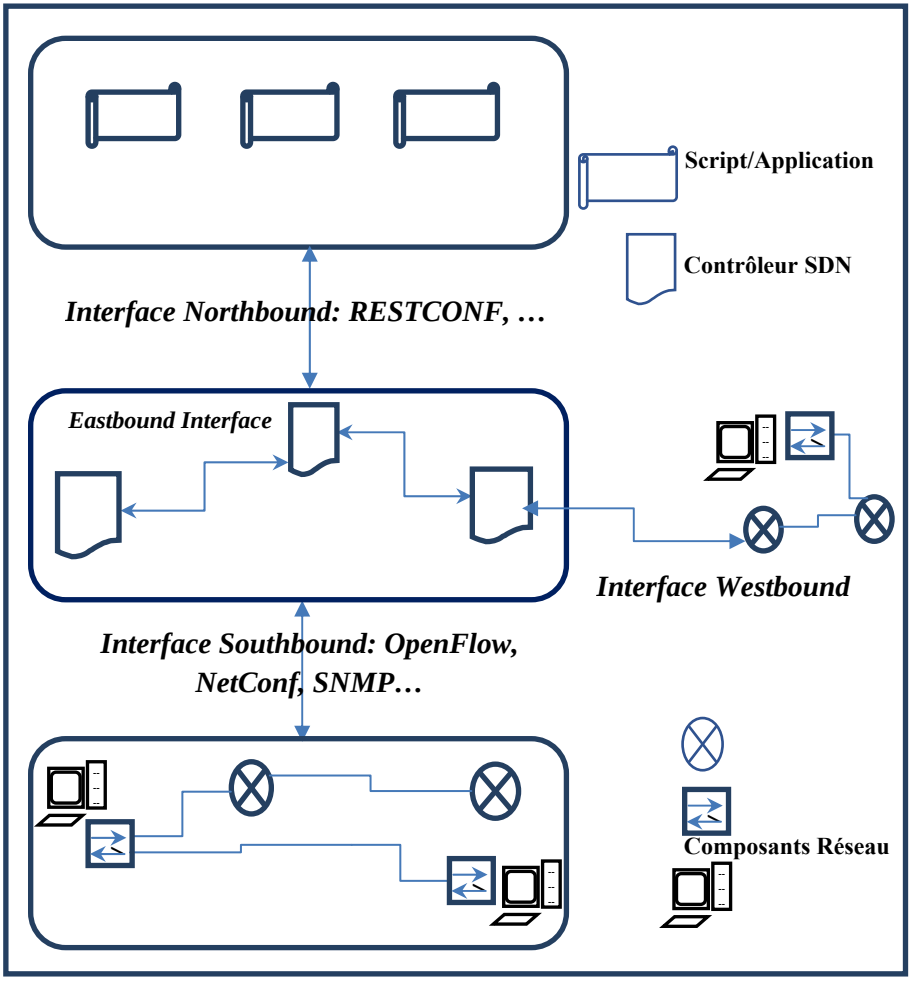

Figure 7.1. *Architecture d'un réseau SDN*

Les fonctionnalités et les composants des couches ou encore les plans qui définissent l'architecture d'un réseau SDN sont présentés comme suit :

1) couche d'infrastructure ou encore couche de données : c'est la couche basse, elle est composée des équipements et des nœuds réseaux tels que les switch/routeur, les stations de travail, les capteurs, etc. Également appelé plan de transmission ou plan de données, ce plan fait référence à la commutation qui relie les différents ports réseau sur un périphérique. Le plan de données de chaque périphérique permet de transmettre et d'acheminer le flux ;

2) couche de contrôle : c'est la couche intermédiaire, elle permet d'héberger le composant le plus important (le contrôleur SDN). Appelé aussi plan de contrôle, il est considéré comme le cerveau du système, le plan de contrôle permet de prendre les décisions de transmission. Les informations envoyées au plan de contrôle sont traitées par les nœuds du réseau ;

3) couche application : c'est la couche haute, elle est optionnelle, elle comporte les équipements de haut niveau faisant tourner des applications et des scripts de management et d'administration.

Cette architecture prévoit quatre types d'interfaces différentes :

1) *SouthBound* : utilisée par le contrôleur pour communiquer avec la couche de données ;

2) *NorthBound* : utilisée par le contrôleur pour communiquer avec la couche de gestion ou encore couche application ;

3) *EastBound* : utilisée par le contrôleur pour communiquer avec d'autres contrôleurs dans le même réseau SDN ;

4) *WestBound* : utilisée éventuellement par le contrôleur pour communiquer avec des équipements dans un réseau classique tiers.

Afin d'assurer la programmation et la virtualisation des réseaux, on utilise les protocoles OpenFlow, NETCONF, RESTCONF, etc., les langages de programmation C, C++, Java, etc., les langages de script Python, Lua, etc., le langage de modélisation des données Yang, le langage de balisage XML.

7.2.3. *Composants du réseau SDN*

Les composants d'un réseau SDN sont répartis sur les trois couches constituant son architecture.

Le composant le plus important est le contrôleur SDN figurant au niveau de la couche de contrôle. D'autres composants sont répartis sur les deux autres couches, en l'occurrence les nœuds sur la couche des données et les composants de haut niveau sur la couche application qui représente le plan de gestion.

7.2.3.1. *Nœuds réseau*

Ces composants assurent seulement la fonction de transmission des données sans aucun souci des fonctionnalités de routage et de contrôle virtualité par les contrôleurs SDN.

Les paquets sont transmis directement par le plan de données en fonction des informations contenues dans la FIB (*Forwarding Information Base*) et la table de contiguïté, sans avoir à faire appel directement au plan de contrôle qui se charge de mettre à jour la FIB en temps différé.

7.2.3.2. *Contrôleur SDN*

Il s'agit d'un appareil du plan de contrôle SDN qui joue le rôle d'un point programmable d'automatisation pour gérer, configurer et dépanner les infrastructures de réseau physiques et virtuelles. Il permet d'automatiser et de centraliser la configuration de l'infrastructure du réseau.

Ainsi le contrôleur centralisé gère le flux des données, renforce la sécurité et fournit d'autres services, et chaque nœud réseau peut se charger uniquement de la transmission des données.

Le contrôleur SDN, dans lequel est centralisée l'intelligence du réseau, représente le cerveau SDN. Un ou plusieurs contrôleurs peuvent être configurés. Avec un seul contrôleur, on parle de contrôle physiquement centralisé et avec plusieurs contrôleurs, il s'agit d'un contrôle physiquement distribué.

Dans ce dernier cas, les contrôleurs peuvent fonctionner ensemble (logiquement centralisés) ou indépendamment les uns des autres (logiquement distribués). Il est possible également de prévoir des contrôleurs SDN hybrides.

Le contrôleur SDN peut être configuré de différentes manières comme le mode web, le mode CLI (*Command Line Interface*) ou par l'utilisation d'un langage de programmation d'un haut niveau, par exemple Python.

7.2.3.3. *Composants de haut niveau*

Ces composants permettent d'exécuter des scripts et des programmes pour gérer le contrôleur SDN afin de mettre à jour la configuration et prévoir de nouvelles fonctionnalités de sécurité et d'optimisation.

7.2.4. *Problématiques de sécurité d'un réseau SDN*

SDN, ayant une architecture différente, exigera des défis de sécurité différents. Il admet de ce fait des attaques diversifiées et spécifiques.

7.2.4.1. *Attaques de sécurité d'un réseau SDN*

Le SDN peut être une cible de *sniffing* par des pirates qui exploiteront les informations recueillies pour lancer des attaques d'accès comme DoS, appelées attaques de trou noir, ou pour utiliser un code malveillant, appelé attaque de trou de ver. L'attaque Sybil est déclenchée en ajoutant des entrées pour influencer le trafic réseau.

D'autres attaques peuvent exister principalement dans les plates-formes IoT comme les attaques de brouillage causées par des interférences de fréquence et des attaques d'épuisement causées par la consommation excessive de l'énergie.

Dans d'autres situations, un attaquant peut prendre la forme d'un voisin frauduleux qui peut déclencher une action malveillante d'inondation Hello.

7.2.4.2. *Défis de sécurité d'un réseau SDN*

Vu que les problèmes de sécurité identifiés dans un réseau SDN sont différents du réseau classique, les défis de sécurité ne seront pas les mêmes.

Premièrement, au niveau du réseau SDN, le flux de données est plus important que le réseau classique. En effet, les données de contrôle sont envoyées par les contrôleurs SDN afin de gérer la communication. S'ils sont envoyés en clair sur le réseau, ils peuvent être capturés par les pirates. Cette vulnérabilité représente une menace importante et pose un défi sérieux.

Deuxièmement, il est nécessaire de fournir une solution de contrôle d'accès pour filtrer le flux de données qui transite à travers les différentes interfaces.

Troisièmement, les attaques DoS ou DDoS doivent être atténuées afin de garantir la disponibilité du SDN.

Quatrièmement, l'accès doit être limité à l'aide des règles de sécurité et des systèmes de contrôle d'accès appropriés.

Enfin, les contrôleurs SDN exigent des mesures de sécurité afin d'assurer l'évolutivité, la cohérence et la fiabilité, etc. Le placement et la synchronisation de ces derniers constituent un défi d'importance capitale.

7.2.5. *Solutions de sécurité d'un réseau SDN*

En raison de ce type de réseau défini par logiciel, les solutions de sécurité prennent principalement la forme logicielle, on parle de sécurité définie par logiciel (SDSec). Les solutions de sécurité doivent être principalement axées autour du contrôleur SDN, cerveau du dispositif qui doit être hautement sécurisé à travers des *firewalls*, des IDS/IPS afin d'atténuer les risques engendrés par les attaques DoS et DDoS. On distingue les systèmes de contrôle d'accès, les systèmes d'authentification, de chiffrement et de virtualisation des fonctions réseau MVF (*Network Function Virtualization*).

Dans le SDN, plusieurs stratégies de défense peuvent être déployées afin d'appliquer des solutions de sécurité et d'atténuer les attaques :

– la stratégie de défense basée sur des politiques est définie de manière dynamique et utilise les propriétés du système et les statistiques des réseaux ;

– la stratégie de défense par apprentissage automatique permet de détecter les attaques et de générer des règles de sécurité ;

– la stratégie de défense de mouvement de la cible est définie par analogie à la technique de pot de miel ou de DMZ dans la sécurité d'un réseau classique. Elle rend la surface d'attaque imprévisible pour les pirates ;

– la stratégie de défense collaborative/distribuée permet de partager les cybermenaces et prévoit une politique collaborative de défense appropriée.

7.2.5.1. *Exigences de sécurité SDN*

Dans les environnements SDN, la sécurité du réseau SDN doit être omniprésente. La sécurité SDN doit être intégrée à l'architecture, ainsi que fournie en tant

que service pour protéger la disponibilité, l'intégrité et la confidentialité de toutes les ressources et informations connectées.

Au sein de cette architecture, il est exigé de :

– protéger le contrôleur : si le contrôleur SDN tombe en panne (par exemple, en raison d'une attaque DDoS), le réseau disparaît également, ce qui signifie que la disponibilité du contrôleur SDN doit être maintenue ;

– mener des investigations et des remédiations : lorsqu'un incident se produit, vous devez être en mesure de déterminer de quoi il s'agit, de le récupérer, de le signaler éventuellement, puis de vous en protéger à l'avenir ;

– établir la confiance : il est essentiel de protéger les communications sur tout le réseau. Cela signifie que le contrôleur SDN, les applications qui y sont chargées et les périphériques qu'il gère sont tous des entités de confiance qui fonctionnent comme ils le devraient ;

– sécuriser l'accès au contrôleur : en tant que point de décision centralisé, l'accès au contrôleur SDN doit être étroitement contrôlé.

Les solutions de sécurité SDN à déployer auront pour objectifs l'un des défis ci-dessus.

7.2.5.2. Blockchain *: une solution de sécurité pour SDN*

La chaîne de bloc (*blockchain*) est une liste de transactions en constante augmentation sous forme de blocs. Ces blocs sont liés et sécurisés à l'aide de la cryptographie. Une blockchain utilise les éléments suivants :

– signatures numériques ;

– registre décentralisé ;

– algorithme pour parvenir à un consensus ;

– chaque bloc comprend le hachage du bloc précédent, formant une chaîne de blocs appelée *blockchain*.

Cette technique représente une solution efficace et fiable pour chiffrer la communication, principalement à travers l'interface *SouthBound* qui représente l'artère la plus importante du réseau SDN dans la mesure où elle permet de véhi-

culer les informations de contrôle générées par les SDN *Controllers* et de les appliquer *via* les nœuds de la couche d'infrastructure. De cette manière, il devient impossible pour les pirates de pouvoir capturer les informations de contrôle et par la suite soit de les altérer d'une façon frauduleuse, soit d'attaquer la source, en l'occurrence SDN *Controller*, qui représente le cerveau de cette technologie.

7.2.5.3. *Infrastructure Cisco axée sur les applications (ACI)*[1]

La sécurité dans un réseau SDN doit être intégrée à partir de la conception initiale et déployée dans le cadre de l'automatisation des différents services.

Dans la mesure où SDN peut fournir des services réseau fiables, plus rapides et plus faciles à concevoir, gérer et dépanner, l'objectif est de réduire l'échelle de temps menace/détection/réponse de jours/semaines en minutes/heures tout en maximisant habileté des outils de l'opérateur pour réagir et atténuer.

La solution Cisco ACI (*Application Centric Infrastructure*) est un *framework* dans lequel les applications guident le comportement du réseau.

Cisco ACI est la solution SDN qui fournit une automatisation basée sur des politiques, il étend l'automatisation des politiques à toutes les charges de travail, y compris les machines virtuelles, les serveurs physiques et les conteneurs.

Cisco adopte une approche opposée à celle du VMware : au lieu d'extraire l'intelligence du matériel, cette approche permet de rendre le matériel encore plus intelligent.

Cisco ACI permet à un administrateur réseau de créer un service de modèles de qualité et de les appliquer à des applications individuelles. Si une certaine application nécessite à tout moment une priorité de bande passante supérieure, comme un système vocal, un modèle peut être créé pour garantir cette priorité. Le même modèle peut ensuite être réutilisé pour toutes les autres applications avec les mêmes exigences.

Grâce à ce processus de création de modèles automatisés, Cisco ACI crée un environnement avec les mêmes avantages qu'un réseau défini par logiciel traditionnel, mais avec une stratégie complètement différente.

1. Voir : www.cisco.com, developer.cisco.com.

7.3. Sécurité IoT/IoE

Vu qu'ils représentent une partie importante et en perpétuelle évolution de tout système informatique, les IoT/IoE nécessitent d'être sécurisés dans l'objectif d'empêcher toute utilisation non autorisée et de neutraliser toute tentative pour s'infiltrer et attaquer les services, les applications et les infrastructures.

Toutes ces caractéristiques permettent de soulever plusieurs défis, et ce sur tous les plans, ce qui rend indispensable la sécurisation à travers plusieurs techniques aussi bien génériques que spécifiques.

7.3.1. *Réseaux de capteurs*

Dans un monde où tout est connecté, le nombre des objets connectés est de loin plus important, cinq ou six fois plus, que le nombre de personnes. Les réseaux de capteurs sont composés d'objets, qui, une fois convenablement programmés, seront capables d'automatiser l'évaluation des données (même en grande quantité) et de modifier les processus de traitements. Les villes intelligentes (*smart city*) en sont une bonne illustration. Elles tirent parti de l'intelligence des capteurs pour automatiser divers services municipaux liés au trafic, au stationnement, au contrôle de consommation de l'eau, de l'électricité et du gaz et de diverses installations et infrastructures. On peut aussi citer les véhicules autonomes dotés de divers capteurs spécifiques, caméras, GPS et services assistés par ordinateur.

7.3.1.1. *Caractéristiques et exigences d'un réseau de capteurs*

L'Internet des objets (IoT) désigne l'interconnexion de millions d'appareils et de capteurs intelligents connectés à Internet. Les réseaux de capteurs génèrent des données, automatisent des traitements et nécessitent d'être sécurisés.

Les données générées par les IoT sont très volumineuses. À titre d'exemple, une voiture autonome peut générer 4 000 giga-octets (Go) de données par jour, une « maison connectée » peut produire jusqu'à 1 giga-octet (Go) de données par semaine.

Ces données stockées et gérées sous forme de Big Data posent des problèmes en termes de gestion, de sécurité, de redondance, d'analyse et d'accès.

L'Internet des objets (IoT) ouvre tout un univers nouveau, où les tâches qui nécessitaient précédemment une intervention humaine peuvent être automatisées, principalement les tâches admettant des conditions dangereuses de fonctionnement ou un travail répétitif.

7.3.1.2. *Domaines d'application des IoT/IoE*

L'utilisation des IoT/IoE couvre plusieurs domaines d'application, on citera à titre d'exemples :

– les maisons intelligentes (*smart home*) ;

– les bâtiments intelligents (*smart building*) ;

– l'IoT industriel ;

– les usines intelligentes ;

– les villes intelligentes (*smart city*) ;

– les réseaux (routier, électrique, distribution d'eau, assainissement, communication, etc.) intelligents ;

– les voitures intelligentes ;

– la gestion des magasins et des services ;

– le diagnostic médical et chirurgical ;

– l'autopilotage et services de suivi et contrôle aérien et maritime.

7.3.2. *Problématique de sécurité en IoT*

Avec le développement de l'IoT/IoE dans le monde entier, de nouveaux et divers défis de sécurité sont apparus, qui se traduisent par des attaques spécifiques qui peuvent être lancées sur des environnements de ce type.

7.3.2.1. *Défis de sécurité en IoT*

Les réseaux de capteurs présentent des défis spécifiques en matière de protection des appareils connectés en IoT dus à :

– l'augmentation du nombre d'appareils : le nombre de capteurs et d'appareils intelligents interconnectés augmente de façon exponentielle, ce qui augmente les risques d'attaque ;

– la diversification des emplacements pour les appareils : certains appareils connectés à l'IoT peuvent interagir avec le monde physique ;

– des difficultés de mise à niveau : les appareils IoT dotés de capteurs peuvent se trouver dans des endroits éloignés et/ou inaccessibles, ce qui complique les interventions ou la configuration ;

– l'utilisation des systèmes de communication sans fil : cette technologie facilite l'accès, donc rend l'attaque des capteurs et des services IoT plus probable.

Les vulnérabilités des réseaux IoT varient d'une authentification faible ou inexistante, à des processus de serveurs intégrés non sécurisés et à des applications peu sécurisées permettant aux pirates de briser les limitations d'accès.

L'utilisateur peut déployer des clients web fonctionnant sur des appareils et des systèmes distants où encore sur le cloud pour accéder aux courriers et les lire au niveau des services et systèmes IoTs, ce qui les rend vulnérables aux mêmes attaques que n'importe quel ordinateur.

L'utilisation de nombreux appareils IoT sur une longue période, qui exécutent des systèmes d'exploitation anciens et obsolètes ou encore des dispositifs mal réglementés et souvent non conçus selon les normes de sécurité matérielle et logicielle, en fait des cibles vulnérables en cas d'attaques, ce qui constitue un défi majeur en matière de sécurité.

7.3.2.2. *Attaques de sécurité en IoT*

Les attaques en IoT peuvent être classées selon plusieurs niveaux :

– attaques de la couche de périphérique IoT : vulnérabilités matérielles, vulnérabilités physiques des dispositifs contraints, vulnérabilités des micrologiciels ;

– attaques de la couche de communication IoT : vulnérabilités IP, TCP, UDP, ICMP ;

– attaques de la couche d'application IoT : vulnérabilités des applications locales, vulnérabilités des applications web et cloud.

Les dispositifs contraints sont souvent placés dans des endroits éloignés où la sécurité physique peut être difficile à mettre en œuvre.

Les vulnérabilités matérielles potentielles pourraient inclure :

– le vol de l'appareil ;

– les dommages physiques à l'appareil ;

– la désactivation de l'appareil, la suppression de la source d'alimentation ;

– la désactivation de la communication, la déconnexion des câbles ou autres moyens de perturbation.

Les vulnérabilités du micrologiciel sont les suivantes :

– identifiants de connexion par défaut non mis à jour. En effet, il est important que les noms des utilisateurs et les mots de passe soient modifiés pour répondre à des critères stricts avant de connecter un appareil IoT à Internet ;

– attaques par déni de service distribué (DDoS) ;

– micrologiciel périmé non résolu avec un correctif ;

– attaques par débordement de tampon ;

– installation d'une porte détournée.

Les attaques TCP/IP les plus courantes sont :

– les attaques DoS : les acteurs de la menace tentent d'empêcher les utilisateurs légitimes d'accéder aux informations ou aux services ;

– les attaques DDoS : cette attaque est similaire à une attaque DoS, mais comporte une attaque simultanée et coordonnée à partir de plusieurs machines sources ;

– les attaques ICMP : les acteurs de la menace utilisent des paquets d'écho ICMP (*Internet Control Message Protocol*) pour découvrir les sous-réseaux et les hôtes sur un réseau protégé, pour générer des attaques par inondation DoS et pour modifier les tables de routage des hôtes ;

– les attaques d'usurpation d'adresse : l'acteur de la menace met l'adresse IP source dans un paquet pour se faire passer pour une source différente, trompant la destination en lui faisant croire que le paquet provenait d'une source légitime ;

– l'attaque de *Men-in-the-Middle* (MITM) : les acteurs de la menace se positionnent entre une source et une destination pour surveiller, capturer et contrôler la communication de manière transparente. Ils pourraient simplement espionner en inspectant les paquets capturés ou modifier les paquets et les transmettre à leur destination d'origine ;

– le détournement de session : les acteurs de la menace ont accès au réseau physique, puis utilisent une attaque MITM pour inspirer un jeton valide afin d'accéder à un serveur web.

7.3.3. Blockchain, *solution de sécurité pour IoT*

La technique de *blockchain*, présentée dans le chapitre précédent, est largement utilisée pour sécuriser les transactions et les communications entre les capteurs et les nœuds d'un réseau IoT. Parce que les capteurs sont des entités critiques et communiquent avec les moindres ressources en termes d'énergie et de configuration, ils ont besoin d'être sécurisés à travers une solution distribuée et autonome.

Cette technique peut être utilisée pour aider à résoudre de nombreux défis de sécurité et de confiance pour l'IoT :

– suivi des mesures des données des capteurs et prévention des données malveillantes ;

– fournir l'identification des appareils IoT, l'authentification et le transfert de données sécurisés ;

– permettre aux capteurs IoT d'échanger des données directement entre eux en toute sécurité, sans intermédiaire ;

– un registre distribué élimine une source unique de défaillance au sein de l'écosystème IoT ;

– le déploiement de l'IoT est simplifié et les coûts d'exploitation de l'IoT sont réduits car il n'y a pas d'intermédiaire ;

– les appareils IoT sont directement adressables avec la *blockchain*, fournissant un historique permanent.

7.4. Conclusion

Le réseau SDN, en tant que solution réseau basée sur la virtualisation, rend plus flexible sa gestion, son administration et éventuellement sa sécurisation, et ce *via* des solutions logicielles. Avec l'évolution des technologies de virtualisation et le *cloud computing*, le SDN favorisera de plus en plus l'automatisation des services et des tâches de contrôle et d'administration réseau qui englobent des fonctionnalités de surveillance et de filtrage en faveur d'une meilleure sécurisation.

Le contrôle d'accès s'effectue à travers des scripts et des programmes utilisant une large panoplie de langages de programmation. Le chiffrement et le contrôle d'intégrité peuvent être assurés par l'utilisation de la *blockchain*.

Étant donné que le monde devient de plus en plus connecté, un nombre important de nouvelles personnes et environ cinq fois plus d'objets se connectent entre eux chaque jour et participent à générer des quantités énormes de données.

Les capteurs présentent des limites et des défis en termes de sécurité, aussi bien physique qu'énergétique, ainsi qu'au niveau des micrologiciels et des applications.

La sécurité peut être rassurée à travers un ensemble de mesures de sécurité physiques, d'autonomie énergétique et de contrôle d'accès par l'utilisation de *blockchain* en plus des techniques de filtrage et de sécurisation classiques.

Chapitre 8

Management de la sécurité

8.1. Introduction

La sécurité informatique est devenue un sujet majeur aussi bien pour les entreprises et les institutions que pour les individus. De ce fait, plusieurs textes juridiques ont été promulgués dans la plupart des pays du monde afin de structurer ce domaine et définir les solutions et les mesures à prendre en considération pour sécuriser les systèmes informatiques qui constituent une épine dorsale et un patrimoine de valeur pour l'individu et l'entreprise.

L'audit sécurité constitue, pour les entreprises, une exigence juridique et économique nécessaire pour la survie et l'existence de l'entreprise aussi bien que pour sa réputation et son rayonnement. C'est une mission périodique faite par des experts de sécurité pour dégager les vulnérabilités et les failles de sécurité et donner les solutions et les recommandations convenables. Un nouveau métier a vu le jour, c'est le métier de consultant ou auditeur en matière de sécurité.

Une mission d'audit passe par trois étapes nécessaires. La première concerne l'aspect organisationnel et physique, elle permet d'identifier les vulnérabilités d'ordre structurel et physique. La deuxième étape est consacrée à l'aspect technique, elle consiste à découvrir les failles de sécurité sur plusieurs niveaux et donner les solutions nécessaires pour telle faille. Enfin, le test intrusif doit être mené, qui consiste à bombarder son propre système par une série d'attaques pour évaluer sa robustesse.

Aussi bien à l'échelle domestique qu'au niveau d'une entreprise, il est nécessaire de prévoir une politique de sécurité dans l'objectif de limiter les risques,

atténuer les attaques et augmenter l'efficacité des solutions de sécurité. Une politique de sécurité touche plusieurs axes, intervient à plusieurs niveaux et fait appel à différents acteurs pour qu'elle soit convenablement appliquée.

Afin de développer une politique de sécurité, il faut en premier lieu procéder à un état des lieux et évaluer le niveau de sécurité existante.

Le développement et le suivi de l'application et l'évolution de la politique de sécurité seront à la charge d'un comité de pilotage animé par un responsable de sécurité. Une fois la politique développée selon les normes et les standards existants et les interlocuteurs identifiés, l'application de cette dernière exige la définition des directives et des procédures permettant de faciliter sa mise en évidence et son efficacité.

8.2. Audit sécurité

L'audit sécurité, exigée par les lois, est nécessaire pour une entreprise afin de lever un défi très important concernant les attaques et les failles de sécurité.

8.2.1. *Objectifs*

La sécurité représente un créneau très spécifique et très pointu qui a trait à un domaine qui ne peut en aucun cas être résolu en interne et par le personnel, dont l'expertise limitée peut être un frein à l'identification et à la résolution du problème. Une mission d'audit doit avertir les utilisateurs d'une part et, après l'identification des failles, doit apporter des solutions et des mesures pour y faire face d'autre part sous forme de recommandations.

8.2.1.1. *Instauration d'une culture de sécurité*

La sécurité est une culture avant tout, le personnel de l'entreprise doit en acquérir un minimum pour être averti, pouvoir se sécuriser et bien se comporter face aux attaques potentielles.

Une mission d'audit doit se concentrer sur la sécurité et faire en sorte que les responsables, les agents et les clients soient sensibilisés à la problématique de la sécurité en identifiant les mauvais comportements. Cette culture peut se manifester à travers des structures, des affiches, des chartes et des mesures d'isolation et de contrôle d'accès physique et logique.

8.2.1.2. *Mise en place de solutions techniques de sécurité*

Après avoir identifié les failles de sécurité, l'équipe d'audit doit essayer de trouver des solutions pour chaque problème. Les solutions doivent couvrir plusieurs aspects :

– topologie et interconnexions du réseau local ;

– connexion internet ;

– systèmes d'exploitation ;

– applications utilisées ;

– moyens d'authentification en vigueur.

8.2.2. *Diagramme d'action d'audit*

Le digramme d'action lors d'une mission d'audit se résume par le schéma de la figure 8.1.

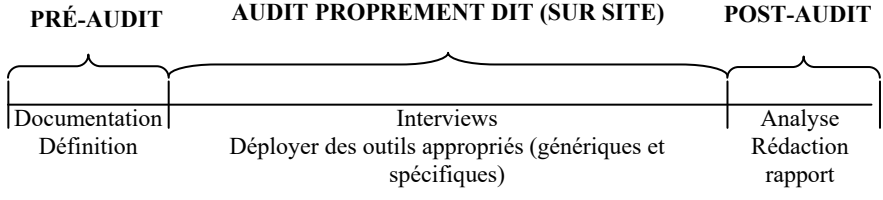

Figure 8.1. *Diagramme d'action d'une mission d'audit*

La première phase sera consacrée à un travail de documentation et de préparation de la mission avec une définition précise et claire des intervenants, des interlocuteurs, des circonstances, des limites et des obligations.

La deuxième phase représente la mission d'audit proprement dite, c'est l'intervention sur site en utilisant des outils appropriés génériques et spécifiques aussi bien techniques ou autres.

Finalement, lors de la troisième phase, l'équipe d'audit se penche sur l'analyse des résultats et la rédaction du rapport.

Les entreprises ne doivent pas se limiter à faire des missions d'audit et laisser de côté le rapport présenté. Il faut veiller à appliquer les recommandations demandées sachant que le rapport est validé éventuellement par les autorités autorisées.

8.2.2.1. *Structuration du service informatique et/ou de sécurité*

La majorité des entreprises négligent l'informatique et la sécurité dans la mesure où il s'agit d'un outil qui facilite le travail et ne constitue pas en soi une unité productive. Les mesures prises en matière d'informatique sont le fait de plusieurs intervenants qui ne sont pas des spécialistes du domaine.

C'est pour cette raison qu'il fallait à la suite de toute mission de *consulting* créer, restructurer, enrichir, assurer l'indépendance du service informatique et/ou de la cellule de sécurité.

8.2.2.2. *Formation continue*

Dans le but de cultiver le personnel, des activités de formation continue sont nécessaires. La mission d'audit doit donner un indicateur sur les connaissances de sécurité au sein de l'entreprise ; l'investissement en matière de formation continue doit se baser sur cet indicateur.

8.2.2.3. *Mise en place de solutions de sécurité*

C'est la partie technique à effectuer par suite d'une mission de *consulting* en sécurité. Elle couvre plusieurs aspects :

– la connexion internet ;

– la solution d'antivirus ;

– la solution de *firewalling* ;

– le chiffrement ;

– les moyens d'authentification.

8.2.3. *Audit organisationnel et physique*

Appelé aussi audit de haut niveau, il permet d'estimer les risques *via* l'analyse des vulnérabilités d'ordre organisationnel et physique.

8.2.3.1. *Objectifs*

C'est une étape préliminaire permettant de critiquer en premier lieu les organisations et de dégager les mauvaises structurations et les mauvaises répartitions de tâches et d'affectation des responsabilités pour les intervenants.

La deuxième partie s'intéresse à la sécurité physique en critiquant les accès physiques aux locaux des systèmes informatiques.

8.2.3.2. *Utilitaires et démarche de mise en œuvre*

La découverte des vulnérabilités d'ordre organisationnel et physique se fait à travers des questionnaires appropriés pour les responsables, les agents et les clients et couvrent plusieurs aspects.

On peut aussi se baser sur des modèles connus et qui offrent une base de données de questionnaires couvrant plusieurs aspects. Pouvant être paramétrés suivant le contexte de l'organisation auditée, ils donnent en sortie des statistiques et des indicateurs sur la sécurité.

On assiste à deux approches possibles : ascendante et descendante :

– approche descendante : c'est une approche systémique complète mais admettant une durée de mise en œuvre importante ;

– approche ascendante : c'est une approche intuitive dont la mise en œuvre est rapide mais qui présente des lacunes de précision et n'est pas complète.

8.2.4. *Audit technique*

Appelé aussi audit de bas niveau, il permet d'identifier les vulnérabilités d'ordre technique (systèmes et réseaux). Cette partie nécessite une expertise de la part des auditeurs et couvre des connaissances multiples. On distingue plusieurs aspects à auditer :

– audit de la topologie réseau ;

– audit de la résistance du système ;

– audit des serveurs ;

– audit des équipements d'interconnexion ;

– audit des applications réseau ;

– audit des bases de données et des SGBD ;

– audit des systèmes de messagerie ;

– audit des applications spécifiques.

8.2.4.1. *Objectifs*

C'est la partie la plus importante, elle permet d'auditer les systèmes et les applications informatiques en dégageant les vulnérabilités et les failles d'ordre technique d'une part et en formulant les recommandations convenables d'ordre technique.

L'audit technique nécessite un minimum d'expertise de la part des auditeurs qui vont s'entretenir dans ce cadre avec les administrateurs et les responsables de sécurité à travers des questionnaires et des discussions aussi bien que par l'utilisation des utilitaires appropriés visant les systèmes, les services et les applications.

Les outils et les utilitaires utilisés varient selon le contexte et l'importance du service informatique et son contenu en termes d'équipements et de solutions déployées, des flux de données échangées et des services et fonctionnalités assurés.

8.2.4.2. *Utilitaires*

Plusieurs outils logiciels peuvent être utilisés au niveau de l'audit technique. Les outils qui conviennent le mieux sont les logiciels libres, ceux-là mêmes utilisés par les hackers et les attaquants.

On peut citer à titre d'exemples les outils suivants :

– Nessus : un outil permettant de découvrir les failles de sécurité au niveau d'un réseau ou d'un segment de réseau ;

– NMAP : un outil permettant d'identifier les ports ouverts au niveau d'un réseau, d'un sous-réseau ou encore d'une machine ;

– LANguard : il permet de détecter les patchs, les partages, les ports ouverts, les comptes utilisateurs inutilisés et les services packs manquants.

8.2.5. *Test intrusif*

C'est une simulation d'attaques qui permet de tester la robustesse d'un système informatique et sa réponse vis-à-vis aux attaques. Il consiste à utiliser des outils d'attaques et observer la réaction du système. Le test intrusif doit être programmé dans les règles de l'art afin d'éviter une perturbation potentielle du fonctionnement.

8.2.6. *Méthodologies d'audit*

On assiste à plusieurs méthodologies d'audit qui peuvent être adaptées parmi d'autres plans lors d'une mission d'audit.

8.2.6.1. *ISO 17799*[1]

Issue de la norme britannique BS 7799, la norme ISO 17799 donne des lignes directrices et des recommandations pour le management de la sécurité.

La norme ISO 17799 fournit ainsi un modèle permettant d'identifier et de mettre en œuvre des solutions pour les risques suivants :

– politique de sécurité (*security policy*) : rédiger et faire connaître la politique de l'entreprise en matière de sécurité ;

– organisation de la sécurité (*security organisation*) : définition des rôles et des responsabilités. Mise sous contrôle des partenaires et de l'activité externalisée ;

– classification des biens et contrôle (*asset classification and control*) : état des lieux et des biens de l'entreprise et définition de leur criticité et du risque associé ;

– sécurité du personnel (*personnel security*) : embauche, formation et sensibilisation à la sécurité ;

– sécurité physique et environnementale (*physical and environmental security*) : périmètre de sécurité, état des lieux des équipements de sécurité ;

– management des communications et des opérations (*communication operation management*) : procédures en cas d'accident, plan de reprise, définition des niveaux de service et des temps de reprise ;

1. Voir : www.iso.org.

– contrôle d'accès (*access control*) : mise en place de contrôles d'accès à différents niveaux (systèmes, réseaux, bâtiments, etc.) ;

– développement et maintenance des systèmes (*system development and maintenance*) : prise en compte des notions de sécurité dans les systèmes de la conception à la maintenance ;

– planification de la continuité de l'entreprise (*business continuity planning*) : définitions des besoins en matière de disponibilité, des temps de reprise et mise en place d'exercices de secours ;

– conformité (*compliance*) : respect des droits d'auteur, de la législation et de la politique réglementaire de l'entreprise.

8.2.6.2. *Marion*

La méthode Marion (Méthodologie d'analyse de risques informatiques orientée par niveaux) est une méthodologie d'audit, qui, comme son nom l'indique, permet d'évaluer le niveau de sécurité d'une entreprise (les risques) au travers de questionnaires pondérés donnant des indicateurs sous la forme de notes dans différents thèmes concourant à la sécurité.

Le niveau de sécurité est évalué suivant 27 indicateurs répartis en six grands thèmes, chacun d'eux se voyant attribuer une note de 0 à 4, le niveau 3 étant le niveau à atteindre pour assurer une sécurité jugée correcte. La méthode est basée sur des questionnaires portant sur des domaines précis. Les questionnaires doivent permettre d'évaluer les vulnérabilités propres à l'entreprise dans tous les domaines de la sécurité.

L'ensemble des indicateurs est évalué par le biais de plusieurs centaines de questions dont les réponses sont pondérées (ces pondérations évoluent suivant les mises à jour de la méthode).

Les thèmes sont les suivants :

– sécurité organisationnelle ;

– sécurité physique ;

– continuité ;

– organisation informatique ;

– sécurité logique et exploitation ;

– sécurité des applications.

8.2.6.3. *Mehari*

Mehari (Méthode harmonisée d'analyse de risques) est dérivée de deux autres méthodes d'analyse des risques (Marion et Melisa). Cette méthode est développée et maintenue en France par le Clusif (Club de la sécurité des systèmes d'information français). Mehari demeure une des méthodes d'analyse des risques les plus utilisées actuellement. Cette méthode se présente comme une véritable boîte à outils de la sécurité des systèmes informatiques, permettant d'identifier les risques de différentes manières au sein d'une organisation. Cette boîte à outils est composée de plusieurs modules qui, indépendamment de la démarche sécurité choisie, permettent notamment :

– d'analyser les enjeux de la sécurité (en décrivant les types de dysfonctionnements redoutés) et de classifier les ressources et les informations selon les trois critères de sécurité de base (confidentialité, intégrité, disponibilité) ;

– d'auditer les services de sécurité, de manière à prendre en compte l'efficacité de chacun, son contrôle, et de synthétiser les vulnérabilités ;

– d'analyser les situations de risques, permettant d'évaluer les potentialités et les impacts intrinsèques, ainsi que les facteurs d'atténuation de risque, puis, enfin, de déduire un indicateur de gravité de risque.

8.3. Mise en évidence d'une politique de sécurité

Une politique de sécurité, écrite et publiée, doit être mise en place au sein de toute organisation présentant un système informatique de taille importante ou moyenne. Elle nécessite une phase de test afin de valider et mesurer les exigences et les niveaux de sécurité existants.

8.3.1. *Test et évaluation de sécurité*

Les tests et les évaluations constituent une étape préalable nécessaire avant de procéder à la formulation de la politique de sécurité. Les tests de sécurité prennent plusieurs formes et utilisent des outils divers et ciblés.

8.3.1.1. *Types de tests de sécurité*

Les tests de sécurité permettent de vérifier la robustesse d'un système informatique et d'identifier les faiblesses et les limites. On distingue les types de tests suivant :

– tests de pénétration ;

– analyse réseau ;

– analyse des vulnérabilités ;

– *cracking* de mot de passe ;

– examen du journal ;

– contrôles d'intégrité ;

– détection de virus.

Ces types de tests permettent de couvrir les différents domaines de sécurité et leurs résultats constituent un état des lieux du système informatique qui représentera un point de départ pour définir et formuler la politique de sécurité.

8.3.1.2. *Outils de test de sécurité*

Pour mener une évaluation efficace, il est conseillé d'utiliser les logiciels libres bien diversifiés, ce sont les mêmes outils qu'utilisent les pirates et les attaquants.

Parmi les plus utilisés, on trouve les outils suivants :

1) Nmap/Zenmap ;

2) SuperScan ;

3) SIEM ;

4) GFI LANguard ;

5) Tripwire ;

6) Nessus ;

7) L0phtCrack ;

8) Metasploit.

8.3.1.2.1. Nmap/Zenmap[2]

Nmap (*Network Mapper*) est un utilitaire gratuit et open source utilisé pour la découverte de réseau et l'audit de sécurité. De nombreux administrateurs système et réseau le trouvent également utile pour des tâches telles que l'inventaire du réseau, la gestion des calendriers de mise à niveau des services et la surveillance de la disponibilité de l'hôte ou du service. Nmap utilise les paquets IP bruts de manière innovante pour déterminer quels hôtes sont disponibles sur le réseau, quels services (nom et version de l'application) ces hôtes proposent, quels systèmes d'exploitation (et versions de système d'exploitation) ils exécutent, quel type de filtres de paquets/pare-feu sont en cours d'utilisation, et des dizaines d'autres caractéristiques. Il a été conçu pour analyser rapidement les grands réseaux, mais fonctionne très bien avec des hôtes uniques. Nmap fonctionne sur tous les principaux systèmes d'exploitation informatiques et des packages binaires officiels sont disponibles pour Linux, Windows et Mac OS X. En plus de l'exécutable classique en ligne de commande Nmap, la suite Nmap comprend une interface graphique avancée et une visionneuse de résultats (Zenmap), un outil flexible de transfert de données, de redirection et de débogage (Ncat), un utilitaire de comparaison des résultats d'analyse (Ndiff) et un outil de génération de paquets et d'analyse de réponse (Nping).

Nmap présente les caractéristiques suivantes :

– flexible : prend en charge des dizaines de techniques avancées pour cartographier les réseaux remplis de filtres IP, de pare-feu, de routeurs et d'autres obstacles. Cela inclut de nombreux mécanismes d'analyse des ports (TCP et UDP), la détection du système d'exploitation, la détection de version, les balayages ping, etc. ;

– puissant : Nmap a été utilisé pour analyser d'énormes réseaux de centaines de milliers de machines ;

– portable : la plupart des systèmes d'exploitation sont pris en charge, notamment Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, etc. ;

– facile : les versions traditionnelles de ligne de commande sont disponibles en plus de versions graphiques (GUI) utilisant des binaires pour ceux qui ne souhaitent pas compiler Nmap à partir des sources ;

2. Voir : Nmap.org.

– gratuit : les principaux objectifs du projet Nmap sont de contribuer à rendre Internet un peu plus sécurisé et de fournir aux administrateurs/auditeurs/hackers un outil avancé pour explorer leurs réseaux. Nmap est disponible en téléchargement gratuit, et est également livré avec le code source complet que vous pouvez modifier et redistribuer selon les termes de la licence.

Zenmap est l'interface graphique officielle du scanner de sécurité Nmap. C'est une application gratuite et open source multiplateformes (Linux, Windows, Mac OS X, BSD, etc.) qui vise à rendre Nmap facile à utiliser pour les débutants tout en fournissant des fonctionnalités avancées pour les utilisateurs expérimentés de Nmap. Les analyses fréquemment utilisées peuvent être enregistrées en tant que profils pour faciliter leur exécution répétée. Les résultats de l'analyse peuvent être enregistrés et affichés plus tard. Les résultats d'analyse enregistrés peuvent être comparés les uns aux autres pour voir en quoi ils diffèrent.

8.3.1.2.2. GFI LANguard[3]

GFI LANguard est le logiciel récompensé d'analyse de réseau et de sécurité utilisé par plus de 20 000 clients. GFI LANguard analyse votre réseau et les ports dans le but de détecter, d'écrire et de réparer les vulnérabilités avec une gestion minimale.

Tout administrateur réseau doit gérer individuellement des problèmes de vulnérabilité, de gestion des correctifs et d'audit, avec parfois plusieurs produits. Avec GFI LANguard, la gestion de ces trois pierres angulaires de la vulnérabilité peut être effectuée avec un seul progiciel.

GFI LANguard vous donne une image complète de votre réseau d'installation et vous aide à maintenir un réseau sécurisé plus facilement et plus efficacement.

8.3.1.2.3. Tripwire[4]

Tripwire est un logiciel de contrôle d'intégrité, permettant de s'assurer que les fichiers sensibles sur un ordinateur ne sont pas modifiés sans que cela déclenche une alerte. Pour ce faire, le logiciel crée une base de données (ou une table de référence pour les cas les plus simples) contenant la signature numérique

3. Voir : www.zdnet.fr.

4. Voir : www.tripwire.com.

(hash) des fichiers que l'administrateur souhaite surveiller. Lors de la phase de contrôle d'intégrité, Tripwire recalcule la signature numérique de chacun des fichiers à surveiller et vérifie que cette signature correspond bien à celle calculée lors de la création de la base de données. Si les deux signatures ne correspondent pas, Tripwire émet alors une alerte.

Les fichiers à surveiller peuvent être classés selon différents degrés de criticité. Tripwire peut être assez complexe à configurer car les fichiers de configuration sont chiffrés. Les éventuelles alertes à la suite de modifications de fichiers peuvent être transmises par courriel.

8.3.1.2.4. Nessus[5]

Nessus est un outil de sécurité informatique. Il signale les faiblesses potentielles ou avérées sur les machines testées. Ceci inclut, entre autres : les services vulnérables à des attaques permettant la prise de contrôle de la machine, l'accès à des informations sensibles, des dénis de service.

Nessus fonctionne sous Unix et Windows, sa dernière version est 8.4.0 publiée le 14 mai 2019.

Il est très largement utilisé par les utilisateurs et les administrateurs des systèmes informatiques. Il est également utilisé par les responsables de sécurité et les auditeurs.

Nessus détecte les machines vivantes sur un réseau, balaie les ports ouverts, identifie les services actifs, leur version, puis tente diverses attaques.

Nessus se divise en deux parties : Nessusd qui est un *daemon* (service) exécutant les requêtes ainsi que la communication avec la cible, et Nessus, une application cliente qui récupère les données et affiche le résultat.

Ce découpage est classique, le *daemon* tournant avec des privilèges élevés (*root*) alors que l'interface graphique, plus complexe et donc vulnérable, tourne sous l'identité d'un utilisateur non privilégié. Les tests sont joués par des *plugins* ; quelques-uns sont en C compilé, mais la majorité sont écrits dans le langage de script NASL (*Nessus Attack Scripting Language*).

5. Voir : Nesssus.org.

Nessus est un scanner de sécurité réseau capable de détecter les failles exploitables localement aussi bien que les failles exploitables à distance :

– soit en identifiant un numéro de version dans une bannière, mais ce procédé est limité à une classe de failles particulière : les failles de services réseau exploitables seulement localement ;

– soit en récupérant la liste des logiciels ou paquets installés sur la machine testée et en les comparant aux patchs publiés par les éditeurs.

8.3.2. *Développement d'une politique de sécurité*

Une politique de sécurité qui se manifeste par un plan d'action bien défini composé par un ensemble de mesures permettant de garantir un niveau minimal de sécurité. Cette politique couvre tous les aspects et fait appel à plusieurs interlocuteurs sur plusieurs niveaux. Elle doit prévoir les actions à entreprendre, les personnes à alerter en cas de détection d'une défiance organisationnelle ou d'une intrusion technique.

L'objectif principal, en l'occurrence maintenir le niveau de sécurité, se manifeste à travers l'instauration d'une culture en termes de sécurité et la mise en place de solutions techniques de sécurité.

Le premier sous-objectif sera garanti *via* des actions de formation, des chartes, des affiches, des sports, des alertes, etc.

Le deuxième sous-objectif couvre les politiques de sauvegarde, de surveillance, d'analyse, de filtrage, de mise à jour, d'alertes, etc.

Une fois définie, la politique de sécurité doit être formulée et écrite avant qu'elle soit distribuée et appliquée.

8.3.2.1. *Interlocuteurs de politique de sécurité*

Pour le développement et la mise en place d'une politique de sécurité, plusieurs intervenants peuvent être impliqués :

– le responsable de sécurité : chargé du développement et de la mise à jour de la politique de sécurité ;

– le comité de collaborateurs : une équipe de spécialistes diversifiés au sein de l'entreprise permettant d'aider le responsable de sécurité à développer, appliquer, suivre et mettre à jour la politique de sécurité ;

– les utilisateurs : il s'agit du personnel qui exploite et accède au service informatique ;

– les intervenants externes : composés des consultants et des auditeurs de sécurité ayant participé aux missions d'audit menées au sein de l'entreprise ou éventuellement intervenant dans la résolution d'un problème précis de sécurité ou de tout autre collaborateur externe dans le domaine de l'informatique.

8.3.2.2. *Étapes d'une politique de sécurité*

La mise en place et l'application d'une politique de sécurité passent par plusieurs étapes définies comme suit :

1) désigner un responsable de sécurité informatique, qui sera chargé de l'élaboration, de l'application et de la mise à jour de cette politique de sécurité ;

2) définir le périmètre et les objectifs de la politique de sécurité informatique afin de délimiter le champ d'action de cette politique et pouvoir évaluer ses effets et ses influences pour une meilleure efficience ;

3) effectuer une analyse de l'existant, matérielle et logicielle, et tenir à jour un registre de l'ensemble des éléments qui composent le système d'information. Ce registre est important lors des modifications des composants de la configuration informatique. En cas d'incident, il peut permettre aux équipes IT de trouver l'origine du problème et d'identifier les responsabilités ;

4) effectuer une analyse des risques informatiques, au regard du dommage possible et de la probabilité d'occurrence de l'incident ;

5) déterminer les moyens nécessaires pour la réduction des risques et la prise en charge des incidents, qu'il s'agisse de moyens matériels ou humains ;

6) définir les procédures adaptées, notamment en matière de gestion des incidents, ou de gestion de la continuité d'activité ;

7) rédiger une charte informatique, à l'attention des collaborateurs ;

8) communiquer la politique de sécurité informatique avec tous ses détails et ses procédures auprès de l'ensemble des intervenants au niveau de l'entreprise.

8.3.3. *Composants d'une politique de sécurité*

La politique de sécurité, dans l'objectif d'être efficace et applicable, doit être composée de plusieurs éléments complémentaires qui couvrent les différents niveaux hiérarchiques de l'entreprise.

8.3.3.1. *Politique de gouvernance*

L'importance de la sécurité informatique exige une intervention de haut niveau au sein de l'entreprise dans l'objectif d'une meilleure efficacité de prise de décision et d'action.

Pour satisfaire cette exigence, il faut prévoir un responsable de sécurité et un comité de sécurité.

Le responsable de sécurité sera rattaché à la direction des services informatiques admettant les tâches et les capacités suivantes :

– il est capable de faire remonter les alertes jusqu'à la direction générale ;

– il dispose des moyens logistiques et financiers et de l'autorité nécessaire pour accomplir ses tâches ;

– il est capable de définir et d'appliquer la politique de sécurité en étroite collaboration avec les membres du comité de sécurité ;

– il doit formuler périodiquement un rapport présentant l'état des lieux en termes de sécurité.

Le comité de sécurité implique et regroupe les acteurs pertinents de l'entreprise (dirigeant, DAF, DSI, RSSI, DO, DRH, DJ, etc.). Elle est animée par le responsable de la sécurité et permet d'assurer la veille technologique et d'instaurer une culture en matière de cybersécurité.

8.3.3.2. *Politique technique*

Le volet technique de la politique de sécurité couvre les domaines techniques, il varie selon le patrimoine matériel et logiciel installé et du degré de criticité des informations manipulées.

La politique de sécurité technique est composée par un ensemble de mesures et de solutions techniques de sauvegarde, de filtrage, de surveillance et de suivi. On distingue :

– la mise en place de logiciels antimalware tels que les antivirus, les anti-spams, les *antispywares*, etc., avec les mises à jour et les correctifs nécessaires ;

– le déploiement des solutions de filtrage utilisant les routeurs et les *firewalls* ;

– déploiement et application d'une politique de sauvegarde ;

– déploiement de solutions spécifiques à appliquer selon les services installés.

8.3.3.3. *Politique des utilisateurs finaux*

Le volet culture en matière de sécurité est d'importance capitale, il doit s'adresser à tout le personnel sans négliger aucun des utilisateurs finaux. L'utilisateur final et toute personne ayant accès au système informatique représentent un maillon important dans la chaîne de sécurité informatique et la politique à mettre en place.

L'utilisateur doit être sensibilisé et averti à travers des affiches, des chartes, des actions de formation ciblées et auxquelles il doit adhérer.

8.4. Normes, directives et procédures[6]

Pour mener à bien une mission d'audit ou suivre ses résultats et impacts, et conduire la mise en place d'une politique de sécurité informatique, plusieurs normes et standards peuvent être utilisés :

– famille des normes ISO 20000 : les normes ISO 20000-1 et ISO 20000-2 sont des standards décrivant des processus de gestion pour la livraison efficace des services informatiques à l'entreprise et à ses clients. Elles respectent les exigences ITIL ;

– famille des normes ISO 27000/ISMS ou SGSI : les normes de la famille 27000 servent à la mise en place, l'utilisation, la tenue à jour et la gestion d'une politique de sécurité informatique, de sécurité des systèmes d'information ou SGSI (ISMS) : système de gestion de la sécurité de l'information ;

– norme ISO/FDIS 31000 : gestion des risques ;

– norme ISO/IEC 38500 : gouvernance de la sécurité informatique ;

6. Voir : www.iso.org.

– normes du British Standards Institution BS 25999-1 : BCM, codes de pratique ;

– normes du British Standards Institution BS 25999-2 : BCM, spécifications.

8.4.1. *Norme ISO 27000*

La série de normes ISO 27000 a été spécifiquement réservée par l'ISO aux questions de sécurité de l'information. La série 27000 comprendra une gamme de normes et de documents individuels. Un certain nombre d'entre eux sont déjà publiés.

– ISO 27001 : il s'agit de la spécification d'un système de gestion de la sécurité de l'information (un SMSI) qui a remplacé l'ancienne norme BS7799-2.

– ISO 27002 : il s'agit du numéro standard de la série 27000 qui était à l'origine la norme ISO 17799 (elle-même anciennement connue sous le nom de BS7799-1).

– ISO 27003 : ce sera le numéro officiel d'une nouvelle norme destinée à offrir des conseils pour la mise en œuvre d'un ISMS (*IS Management System*).

– ISO 27004 : cette norme couvre les mesures et les métriques de gestion des systèmes de sécurité de l'information, y compris les contrôles suggérés alignés ISO27002.

– ISO 27005 : il s'agit de la norme ISO indépendante de la méthodologie pour la gestion des risques liés à la sécurité de l'information.

– ISO 27006 : cette norme fournit des lignes directrices pour l'accréditation des organisations offrant la certification SMSI.

8.4.2. *Norme ISO/FDIS 31000*

ISO 31000 désigne une famille de normes de gestion des risques codifiés par l'organisation internationale de normalisation. Le but de la norme ISO 31000 est de fournir des principes et des lignes directrices du management des risques ainsi que les processus de mise en œuvre au niveau stratégique et opérationnel. Elle ne vise pas à promouvoir l'uniformisation du management du risque au sein des

organismes, mais plutôt à harmoniser la multitude d'approches, de standards et de méthodologies existantes en matière de management des risques.

Actuellement, la famille ISO 31000 comprend :

– ISO 31000:2018 – Management du risque – Principes et lignes directrices ;

– ISO/CEI 31010:2009 – Gestion des risques – Techniques d'évaluation des risques ;

– ISO Guide 73:2009 – Management du risque – Vocabulaire.

8.4.3. *Norme ISO/IEC 38500*

ISO/IEC 38500 est la norme internationale concernant la gouvernance des technologies de l'information par l'entreprise. Elle est la première norme officielle relative à la gouvernance informatique.

Cette norme concerne la gouvernance des processus de gestion relatifs aux services d'information et de communication utilisés par une organisation. Ces processus peuvent être contrôlés par des spécialistes informatiques au sein d'une organisation ou par des fournisseurs de services externes.

8.5. Conclusion

L'audit sécurité est nécessaire pour sécuriser un système informatique mais il reste insuffisant. Il faut qu'il soit complété et valorisé par une veille technologique au niveau de l'entreprise afin d'assurer un suivi quotidien de l'état de sécurité à travers des outils d'audit et de surveillance et par une relation de coopération étroite avec les organismes appropriés.

L'audit de sécurité constitue une étape importante pour la survie d'une entreprise, il permet une critique constructive externe par des experts du domaine. Cette mission exigée par la loi est bénéfique pour l'entreprise afin de protéger son patrimoine informatique.

La politique de sécurité, bien définie et correctement appliquée, permet de couronner les mesures et les activités menées par tous les intervenants en termes

de sécurité. Elle couvre les aspects organisationnel et technique et permet d'instaurer une culture qui met l'entreprise à l'abri des risques et des menaces.

La sécurité informatique ne cesse de s'imposer au détriment de plusieurs autres facteurs, elle tire son importance et sa pertinence des circonstances et des états des lieux qui gardent en mémoire le volume des dégâts matériels et autres survenus aux dépens des individus, des entreprises, des sociétés et des États.

Liste des acronymes

ACL	*Access Control List*
AES	*Advanced Encryption Standard*
AH	*Authentication Header*
CA	*Certification Authority*
DES	*Data Encryption Standard*
DMZ	*DiMilitarised Zone*
CLI	*Command Line Interface*
DoS	*Denial of Service*
DSA	*Digital Signature Algorithm*
ESP	*Encapsulating Security Payload*
HIDS	*Host based IDS*
IDEA	*International Data Encryption Algorithm*
IDS	*Intrusion Detection System*
IKE	*Internet Key Exchange*

IoT/IoE	*Internet of Things/Internet of Everythings*
IPS	*Intrusion Prevention System*
ISAKMP	*Internet Security Association and Key Management Protocol*
L2F	*Layer Two Forwarding*
L2TP	*Layer Two Tunneling Protocol*
MARION	Méthodologie d'analyse de risques informatiques orientée par niveaux
MD5	*Message Digest 5*
MEHARI	Méthode harmonisée d'analyse de risques
NAT	*Network Address Translation*
NIDS	*Network Based IDS*
PAT	*Port Address Translation*
PPTP	*Point-to-Point Tunneling Protocol*
RSA	*Rivest Shamir Adleman*
SA	*Security Association*
SDN	*Software Defined Network*
SHA1	*Secure Hash Algorithm 1*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
TLS	*Transport Layer Security*
VPN	*Virtual Private Network*

Bibliographie

Boutherin, B., Delaunay, B. (2003). *Sécuriser un réseau Linux*. Eyrolles, Paris.

Cisco (2021). Cisco platform [En ligne]. Disponible aux adresses : cisco.netacad.net et developer.cisco.com.

Huawei (2021). Huawei platform [En ligne]. Disponible à l'adresse : e.huawei.com et support.huawei.com.

Sites Internet

CompTIA (n.d.) : https://www.comptia.org.

ISO (2021) : www.iso.org.

Jakusic, M. (2021) : www.securite.teamlog.com.

Nessus (2022) : https://www.nessus.org.

Sécurité Info (2021) : www.securiteinfo.com.

Snort (2022) : https://www.snort.org.

The Virus Encyclopedia (n.d.) ; http://virus.wikidot.com.

Tripwire (n.d.) : https://www.tripwire.com.

Index

A, B

AAA, 56, 62-70
accounting, 62, 63, 68-70
ACE, 72, 74, 78
ACI (*Application Based Cisco Infrastructure*), 151
ACL (*Access Control List*), 71-85, 94, 95, 100, 104
  étendue, 75, 76, 78
  standard, 73, 75-77
adware, 51
AH (*Authentication Header*), 128, 129, 131-134
antivirus, 105-108, 112, 115
attaque, 5, 8-14, 16, 24, 26
  d'accès, 11
  de reconnaissance, 10
  directe, 5
  indirecte, 5
atténuation (*mitigation*), 17
audit
  de sécurité, 169, 177
  technique, 164
authentication, 62-65, 67-69
authentification, 15, 25-27, 29-31, 33-35
authorization, 62, 63, 68-70
base virale, 106, 107

C

chaîne de bloc (*blockchain*), 150
CHAP, 66
cheval de Troie, 49, 53
chiffrement, 117-123, 127, 128, 131, 133-135, 138, 140, 141
clé symétrique partagée, 122, 123
confidentialité, 21, 25, 28, 29, 33
connexion frauduleuse, 11
contrôleur SDN, 143, 144, 146-150
couche
  d'application, 154
  d'infrastructure, 144, 146, 151
  de contrôle, 146, 147
cryptanalyse, 120, 121

D

déchiffrement, 118, 119, 122, 123
déni de service (DoS *Denial of Service*), 11, 26

deny, 75-85, 94, 95
DMZ (*DeMilitarized Zone*), 100-104

E, F, H

ESP (*Encapsulating Security Payload*), 129, 131-134
filtrage, 71, 72, 76-78, 82, 85-88, 90-94, 96, 99, 100, 102, 104
firewall, 85, 87, 89, 92-95, 100
  paquet, 92
  PC, 93
HWTACACS, 66, 68-70

I, J

identification, 56, 58, 59
IDS (*Intrusion Detection System*), 108-115
IKE, 134, 140
intégrité, 23, 25, 26, 29, 33-35
IoE (*Internet of Everything*), 152, 153
IoT (*Internet of Things*), 148, 152-156
IPS (*Intrusion Protection System*), 113-115
IPSec, 117, 118, 128-131, 134, 137, 138, 140, 141
ISAKMP, 134, 139
ISO 17799, 165, 176
journal d'audit, 109, 110

K, L, M

keylogger, 51
LANguard, 164, 168, 170
malware, 42
Marion, 166, 167
masque générique, 74
méthodologies d'audit, 165
mode
  transport, 128, 129, 131, 132
  tunnel, 118, 128-130, 132-134

N

NAT, 85, 88
Nessus, 164, 168, 171, 172
Nmap, 168-170

P

phishing, 52
pile de production, 109, 110
politique de sécurité, 159, 160, 165, 167, 168, 172-175, 177

R

RADIUS, 66-70
rebond, 13, 14
réseaux de capteurs, 152, 153
rootkit, 52

S

scareware, 52
SDN (*Software Defined Network*), 143-151, 157
service de sécurité, 28, 29
signature, 106, 107, 111, 112, 115
Snort, 114
social engineering, 9, 36
spam, 47, 48
spyware, 50
SSL, 117, 137

T

TACACS+, 66, 67, 69
TCP SYN, 15, 16
test intrusif, 159, 165

V, Z

ver, 45, 46, 53
virus, 42-46, 48, 53
VPN (*Virtual Private Network*)
    d'accès distant, 136, 137
    Site-to-Site, 136
vulnérabilité, 24, 28
ZPF, 95, 96

Les attaques informatiques se multiplient, chaque utilisateur se doit d'avoir un minimum de connaissances en termes de sécurité informatique pour lui permettre d'atténuer les menaces qu'il pourrait subir. Cette expertise exigée chez les individus et les organisations permettrait de garantir un minimum de sécurité à l'échelle de la famille, de l'école, du monde du travail et plus généralement de la société.

Sécurité informatique est un guide complet permettant aux utilisateurs de développer leurs connaissances concernant les attaques, les failles et les solutions de sécurité, et ainsi les inciter à se comporter de façon plus méfiante lors de l'utilisation quotidiennes des différents outils informatiques. Pour la personne plus qualifiée, il offre également une grande quantité d'outils pour sécuriser son patrimoine matériel et logiciel.

L'auteur

Titulaire du diplôme national d'ingénieur en informatique de l'ENSI, Ameur Salem Zaidoun est enseignant universitaire à l'ISET de Siliana (Tunisie). Ex-développeur et consultant en sécurité, il est certifié Cisco (CCNA-R&S, DevNet et CCNA-Security) et certifié Huawei HCNA R&S.

iSTE editions

9 781784 059071