TG-36

الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي و البحث العلمي
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

جامعة سعد دحلب البليدة
UNIVERSITÉ SAAD DAHLAB DE BLIDA

DEPARTEMENT D'INFORMATIQUE

جامعة سعد دحلب البليدة
المكتبة
كلية العلوم

PROJET DE FIN D'ÉTUDES
POUR L'OBTENTION DU DIPLOME
D'INGENIORAT EN GENIE INFORMATIQUE

Option : SYSTEME D'INFORMATION

Thème

CONCEPTION ET MISE EN ŒUVRE D'UN FIREWALL POUR LE CONTROLE D'ACCES A UN RESEAU

Présenté par :
KEHILICHE OUIDED
MECHROUH FATIHA

Proposé par :
Mrs. MEHDI MEROUANE

BIG-04-36-1

2003-2004

MIG-004-36-1

REMERCIEMENTS

Nous tenons à adresser nos remerciements les plus sincères et toute nos reconnaissance à notre promoteur Mr.MEHDI MEROUANE, de nous avoir confier ce travail, pour sa disponibilité et pour ses conseils au cours de ce projet.

Toute nos reconnaissance aussi à Mr. BENELKAID ISMAIL, pour son aide inoubliable, ses encouragements et ses critiques au cours de ce projet.

Nous remercions Mr.Abdlah Elhaj Hichem et Mr.Hebal Aziz pour leur encouragements au cours de ce projet, leur relectures et leur critiques.

Nous remercions vivement le président ainsi que les membres du jury de nous avoir honoré par leur présence.

Nous exprimons notre profonde reconnaissance à tous ceux qui nous ont aidé, de prés ou de loin, matériellement ou moralement, et partager nos peines pour voir ce modeste ouvrage naître. A commencer par TOUIMER Nassim, et tous les étudiants de la promotion 2003/2004.

Kehiliche Ouided

Mechrouh Fatiha.

Conception et mise en œuvre d'un Firewall pour le contrôle d'accès à un réseau

Résumé

Depuis la mondialisation de l'Internet et bien avant, la sécurité informatique n'est plus le soucis des militaires, elle est devenue la préoccupation de tout individu utilisant l'outil informatique.

Cette thèse d'ingéniorat présente le concept de la sécurité informatique en générale et des Firewalls en particulier. Les Firewalls sont des dispositifs pour le contrôle d'accès à un réseau informatique.

L'objectif de ce projet de fin d'études est la conception et la réalisation d'un Firewall basé sur le filtrage statique de paquets IP, un snifer pour analyser le trafic réseau et un scan port.

Mots clés : *Sécurité informatique, Firewall, filtrage statique de paquets IP, snifer.*

Design and implementation of a Firewall to control the access to a network

Abstract

Nowadays, with the growing of the Internet, worldwide open ended business makes computer security becoming everyone's focus; it is not anymore a military research issue.

This work presents the computer security issues in general and the Firewall issues in particular. Firewall is a net access control mechanism.

The objective of this end studies project is the design and the implementation of Firewall based on the IP packets filtering and a snifer to analyze the traffic network and a scan port.

Key words: *Computer security, Firewall, mechanism, filtering of packages IP, snifer.*

SOMMAIRE

INTRODUCTION GENERALE.....1

CHAPITRE 1 : Vulnérabilités et attaques réseaux

1.1Introduction.....4

1.2 Définitions.....4

1.3 Différents types d'attaques.....5

1.3.1 Attaque passive.....5

1.3.2 Attaque active.....5

1.4 La méthode d'attaque.....6

1.5 Les principales vulnérabilités des systèmes 8

1.5.1 Les principales vulnérabilités de système Windows.....8

1.5.2 Attaques exploitant les vulnérabilités systèmes.....12

1.6 Vulnérabilités et attaques dans la suite de protocole TCP/IP.....12

1.6.1 Mots de passe envoyés en clair.....13

1.6.2 Buffer overflow.....13

1.6.3 Exploitation des failles IP.....13

1.6.4 Utilisation frauduleuse des commandes ICMP.....15

1.6.5 Exploitation des failles TCP.....15

1.6.6 Exploitation des failles UDP.....15

1.6.7 Les failles de protocole RIP.....16

1.7 Le sniffing des mots de passe et de paquets.....16

1.8 Attaque par déni de service DOS.....17

1.9 Les scanners.....18

1.10 Les chevaux de Troie.....18

1.11 Les vers.....18

1.12 Les virus.....19

1.13 Les trappes.....19

1.14 Les bombes logiques.....19

1.15Conclusion.....20

CHAPITRE 2 : La sécurité informatique

2.1 Introduction.....22

2.2 Terminologie de la sécurité informatique.....22

2.3 Les aspects de la sécurité.....23

2.3.1 La disponibilité de service.....23
2.3.2 Confidentialité 23
2.3.3 L'intégrité.....23
2.4 Les formes de sécurité.....23
2.4.1 Sécurité matérielle.....24
2.4.2 Sécurité de l'information 25
2.4.3 Sécurité organisationnelle.....25
2.5 Services de sécurité.....26
2.5.1 L'authentification.....26
2.5.2 Contrôle d'accès.....26
2.5.3 Confidentialité des données.....26
2.5.4 Intégrité des données.....27
2.5.5 Non-répudiation.....27
2.6 Mécanismes de sécurité.....27
2.6.1 Le chiffrement.....28
2.6.2 Authentification.....29
2.6.3 Mécanismes de contrôles d'accès.....29
2.7 Politique de sécurité.....30
2.8 La sécurité dans les couches de TCP/IP.....31
2.8.1 Protocole de sécurité de la couche Application.....31
2.8.2 Protocoles de sécurité de la couche Transport.....31
2.8.3 Protocole de sécurité de la couche Réseau.....32
2.9 Outils de sécurité.....34
2.9.1 Les VPN.....34
2.9.2 Les Pare-feu(Firewall).....34
2.9.3 Les IDS.....34
2.10 Conclusion.....35
CHAPITRE 3 : Les Firewalls
3.1 Introduction.....37
3.2 Définition d'un Firewall.....37
3.3 Fonction de sécurité de Firewall.....38
3.4 Fonction de sécurité de base d'un Firawall.....39
3.4.1 Algorithme de contrôle d'accès des paquets.....40
3.4.2 Les différents types de filtrage.....40

3.5 Architecture des Firewalls.....45
3.5.1 Architecture d'hôte à double réseau.....46
3.5.2 Architecture d'hôte à écran.....47
3.5.3 Architecture de réseau périphérique.....48
3.6 Récapitulatif.....50
3.7 Solution actuelles.....52
3.7.1 Solution matérielles.....52
3.7.2 Solution logicielles.....53
3.8 Points forts et points faibles d'un Firewall.....53
3.9 Conclusion.....55
CHAPITRE 4 : Conception et mise en œuvre
4.1 Introduction.....57
4.2 Méthode de développement.....57
4.3 Conception du Firewall.....59
4.3.1 L'approche utilisée.....59
4.3.2 Hypothèse.....59
4.3.3 Architecture de Firewall.....59
4.4 Implémentation des différents modules.....64
4.4.1 Outils de développement.....64
4.4.2 module de filtrage des paquets IP.....64
4.4.3 Module sniffer.....70
4.4.4 Module scan port.....74
4.4.5 Module Interface utilisateur.....75
4.5 Conclusion.....78
CHAPITRE 5 : Test par simulation d'attaque
5.1 Introduction.....80
5.2 Définition de SubSeven.....80
5.3 Composition de SubSeven.....80
5.4 Installation de SubSeven.....81
5.4.1 Installation de SubSeven serveur.....81
5.4.2 Configuration de serveur.....81
5.4.3 Installation de SubSeven client.....82
5.5 Conséquences.....83
5.6 Plates-formes des tests effectués.....84

5.7 Plan de test.....84

5.8 Conclusion.....90

CONCLUSION GENERALE.....91

ANNEXE A : Le Modèle TCP/IP.....94

ANNEXE B : Listes des ports utilisés par les chevaux de Troie.....114

BIBLIOGRAPHIE

LISTE DES FIGURES

Chapitre 1 : Vulnérabilités système et attaques
Figure1.1 : Méthode de piratage 6
Figure1.2: IP Spoofing 14
Figure1.3 : Attaque par petit fragment 14
Figure1.4 : TCP flooding 17
Chapitre 2 : La sécurité informatique
Figure2.1 : Aspects de la sécurité 23
Figure2.2 : Les formes de la sécurité 24
Figure2.3 : Le chiffrement à clé symétrique 28
Figure2.4 : Le chiffrement à clé asymétrique 29
Figure2.5 : Le rôle de la politique de sécurité 30
Figure2.6 : En-tête d'authentification 33
Figure2.7 : En-tête d'information de sécurité d'encapsulation 33
Chapitre 3 : Les Firewalls
Figure3.1 : Firewall séparant deux réseaux 37
Figure3.2 : Firewall séparant le réseau local et l'Internet 38
Figure3.3 : Passerelle d'application 44
Figure3.4 : Représentation de la zone DMZ 46
Figure3.5 : Firewall d'hote à double réseau 47
Figure3.6 : Firewall d'hote à écran 48
Figure3.7 : Firewall de réseau périphérique avec un seul bastion 49
Figure3.8 : Utilisation de plusieurs bastions 49
Chapitre4 : Conception et mise en œuvre
Figure4.1 : Phases de développement de projet 57
Figure4.2 : Architecture de Firewall 60
Figure4.3 : Schéma synoptique général de l'application 63
Figure4.4 : Niveau de filtrage 65
Figure4.5 : Les différentes classes de l'application 66
Figure4.6 : Niveau de fonctionnement de SocketView 70
Figure4.7: L'interface principale 75
Figure4.8: Le menu Firewall 76
Figure4.9 : L'interface d'ajout de règles de filtrage 76
Figure4.10 : L'interface d'analyse de trafic réseau 77
Figure4.11 : L'interface de scan port 77
Chapitre5 : Test par simulation d'attaque
Figure5.1 : L'interface de Edit 82
Figure5.2 : L'interface de SubSeven 83
Figure5.3 : Les ports ouverts dans la machine cible 85
Figure5.4 : Ouverture de port 1243 85
Figure5.5 : Etablissement de la connexion 86
Figure5.6 : Le Bureau de la machine victime 87
Figure5.7 : Disparition de la barre de tâche de la machine victime 87
Figure5.8 : Changement des couleurs 88
Figure5.9 : Installation de Firewall 88
Figure5.10 : Règle de filtrage 89

Liste des tableaux

Chapitre1 : Vulnérabilités et attaques réseaux
Tableau1.1 : Dégâts de propagation des vers et des virus 18
Chapitre3 : Les Firewalls
Tableau3.1 : Exemple de règles de filtrage 41
Tableau3.2 : Application des règles de filtrage 42
Tableau3.3 : Tableau récapitulatif des architectures de base de Firewalls 51
Chapitre4 : Conception et mise en œuvre
Tableau4.1 : Les relations entre les classes 67
Tableau4.2 : Propriétés et méthodes de SocketView 71

Liste des graphes

Chapitre1 : Vulnérabilités et attaques réseaux
Graphe1.1 : Ports les plus attaqués 4
Graphe1.2 : Les vulnérabilités systèmes 8
Graphe 1.3 : Sinistralité informatique 19

Liste des graphes

Chapitre1 : Vulnérabilités et attaques réseaux
Graphe1.1 : Ports les plus attaqués 4
Graphe1.2 : Les vulnérabilités systèmes 8
Graphe 1.3 : Sinistralité informatique 19

INTRODUCTION GENERALE

Avec le poids économique de plus en plus important de l'informatique dans l'industrie, et plus encore du fait de la dépendance grandissante envers les réseaux de communication, et étant donnée le nombre de plus grand des réseaux interconnectés, la sécurité des données informatiques est aujourd'hui un probléme crucial. Ce problème est aggravé avec l'existence des attaques surtout après l'apparition de l'Internet.

C'est pour cela que les entreprises, institutions, universités et centres de recherches doivent avant tout se prémunir de ces attaques grâce à la mise en place d'un dispositif de sécurité informatique tel qu'un Firewall. Ce dernier est capable d'intercepter et de bloquer tout type de tentative d'attaque. L'objectif de notre mémoire de fin d'études est 'la conception et la réalisation d'un Firewall pour le contrôle d'accés à un réseau'.

Aborder la sécurité informatique des systèmes d'information est souvent considérée comme une tâche technique difficile, généralement réservée à des spécialistes. Pour cette raison nous avons suivi les étapes suivantes :

Nous présenterons dans le premier chapitre les vulnérabilités systèmes et les attaques réseaux les plus fréquentes.

Dans le chapitre suivant nous aborderons la sécurité informatique, les différents services qu'un système de sécurisation doit prendre en compte, à savoir la disponibilité de service, l'authentification, l'intégrité et la confidentialité.

A la suite de ce chapitre nous présenterons en détails la solution du Firewall, les fonctions de filtrage, les architectures et quelques solutions actuelles.

Le quatrième chapitre sera consacré à la conception et la réalisation de notre Firewall, nous basons sur le développement de notre solution qui est un système de filtrage de paquets qui permettra à l'administrateur de contrôler l'accés, ainsi qu'un analyseur de trafic réseau et un scanneur de ports.

Dans le dernier chapitre, nous avons testé le fonctionnement de Firewall réalisé par la simulation d'une attaque à base de chevale de Troie.

Après la conclusion générale sur le travail réalisé, et dans l'éventualitè de la poursuite des travaux de notre projet et pour plus de détails, nous avons confectionné deux annexes, qui traiterons respectivement de :

-Modèle d'interconnexion (TCP/IP) ;
-Ports couramment utilisés par les chevaux de Troie (pouvant être bloqués grâce à notre application).

CHAPITRE I

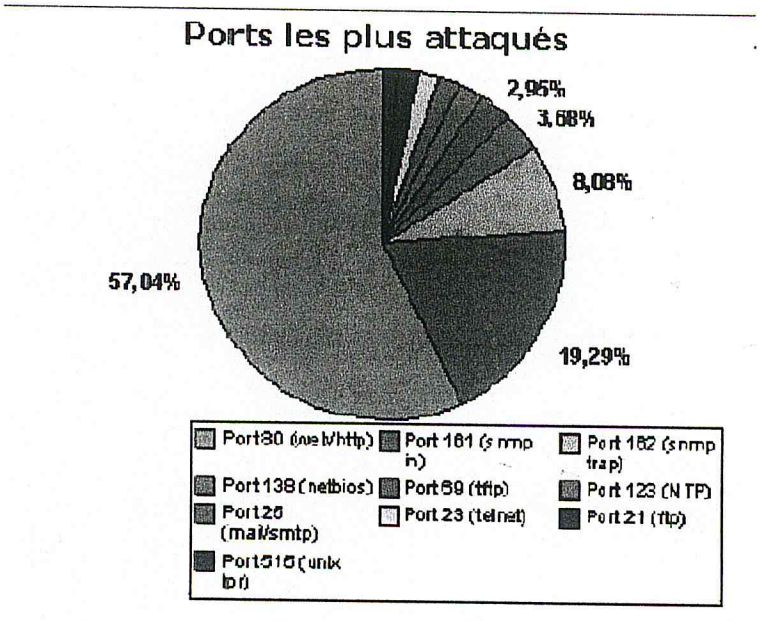
Les vulnérabilités système et les attaques réseaux

1.1 INTRODUCTION

L'Internet est devenue un outil de communication mondial, utilisait par des bons et des mauvais citoyens et toutes les déviances courantes y sont présentes. Cette connectivité totale était une aubaine pour les personnes mal intentionnées qui pouvaient essayer très facilement de pénétrer les mécanismes de sécurité d'un système distant pour voler ou détruire des informations stockées dans le système.

Deux exemples réels de ce type de pirates sont les espions capturés en Allemagne au milieu des années 1980 et le groupe de pirates « Global Hell (gh) » qui en Mai 1999 forçait la maison blanche et la police fédérale américaine (FBI) à fermer leur site Internet. Dans ce chapitre nous allons présenter les vulnérabilités des systèmes et les attaques exploitant les failles système de l'ordinateur.

Selon la société ISS (Internet Security System) les ports (voir Annexe A) les plus attaqués sont représentés par le graphique suivant :



Graphe1.1 : Ports les plus attaqués [CH 02].

S'approuve que la principale voie d'attaque est bien entendu le port Internet (80) sur les serveurs suivi de loin par le protocole d'administration SNMP.

1.2 DEFINITIONS

a. Pirates

Ce sont des personnes qui violent des systèmes à distance, détruisent des données, empêchent le fonctionnement des services.... [COM 03].

b. Intrusion

C'est la pénétration par violence ou par ruse de personnes non autorisées dans une zone délimitée, avec intention de vol, de dommage ou d'abus [ABD 01].

c. Vulnérabilité

C'est une faiblesse, une faille dans les mesures de protection ou encore dans l'absence de mesure de protection [CHA 01].

d. Attaque

C'est l'action entreprise par un individu pour modifier l'état d'un système. Une attaque peut réussir si elle exploite une vulnérabilité du système. Elle peut être direct auquel cas elle s'adresse à l'objet en question ou indirecte où elle obtient des informations d'un autre objet sans attaquer l'objet en question directement [CHA 01].

1.3 LES DIFFERENTS TYPES D'ATTAQUE

Les attaques sur le réseau sont des attaques passives ou des attaques actives :

1.3.1 Attaques passives

Les attaques passives sont basées sur l'écoute indiscrète ou surveillance de transmission afin d'obtenir les informations qui ont été transmise. Ces attaques ne produiraient aucune modification d'information contenue dans les systèmes et avec les quelles ni le fonctionnement ni l'état de système ne changent.

Les attaques passives sont :

a- Ecoute physique ou capture de contenu de message (une conversion téléphonique, un courrier électronique, un fichier transféré peuvent contenir une information sensible ou confidentielle).

b- Analyse de trafic : Afin de découvrir l'existence d'une communication entre deux machines (utilisation de sniffer).

Les attaques passives sont très difficiles à détecter car elles ne causent aucune altération des données et elles n'interagissent pas avec le fonctionnement normal du système. Donc pour ce type d'attaque l'accent est porté sur la prévention plutôt que sur la détection.

1.3.2 Attaques actives

Ces attaques impliquent certaines modifications du flux de données, l'altération des informations contenues dans ce système et modification de l'état ou de fonctionnement du système.

1.4 LA METHODE D'ATTAQUE

Tout les pirates procèdent ces étapes pour réussir leurs attaques.

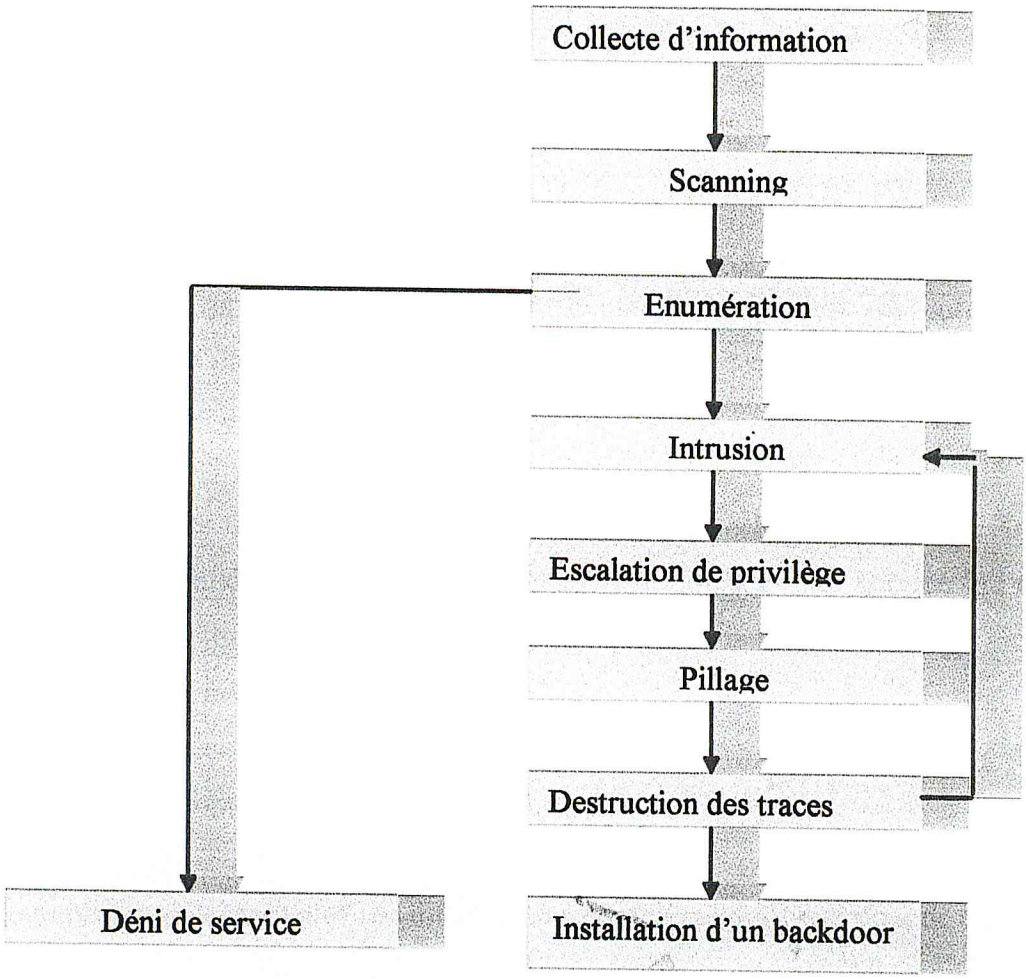


Figure 1.1 : Méthode de piratage .

1.4.1 Collecte d'information (Footprinting)

Avant de pouvoir attaquer sa cible, le pirate doit faire une reconnaissance afin de découvrir ou se trouvent les machines de la cible et par quels moyens elles sont atteignables. La premiére source d'information sont les registres de noms[PH 03].

1.4.2 Scan

Une fois que le pirate a identifié les réseaux appartenant à sa cible il peut en scanner la partie qui l'interesse. Pour ce faire il peut envoyer des ping (ICMP echo_request) ou des demandes de connexion TCP (Transmission control protocol), à toute les adresses du réseau. Apartir des réponses il peut trouver à quelles adresses il y à des machines qui répondent et quels sont les ports qui sont accessibles sur ces machines. En fonction de comportement exact des machines il est aussi possible d'identifier le système d'exploitation de certaines machines[PH 03].

1.4.3 Enumération

Dans cette étape le pirate peut essayer d'énumérer les services disponibles sur la cible. Il va essayer d'identifier la marque et la version des logiciels qui fournissent les services accessibles sur la cible. On peut dire que la recherche s'appuie sur les services vulnérables. Pour chaque service il va essayer d'énumérer les différents points d'entrée[PH 03].

1.4.4 Intrusion

Le pirate doit trouver une vulnérabilité qui est connue mais n'est pas encore été corrigée sur la cible. Un pirate doué pourra développer un exploit spécifique à sa cible [PH 03].

1.4.5 Déni de service

Le pirate peut lancer un déni de service (voir plus loin). Il est souvent plus facile de trouver une vulnérabilité qui permettre l'éxécution d'un déni de service qu'une vulnérabilité qui permettre de s'introduire dans la cible[PH 03].

1.4.6 Escalation des privilèges

Ayant obtenu l'accès au système, l'intrus utilise une autre vulnérabilité pour élever ses privilèges jusqu'au obtenir les droit d'accès désirés [PH 03].

1.4.7 Pillage

Le pirate peut maintenant voler des informations confidentielles (numéros de carte de crédits) ou modifier des informations afin d'obtenir frauduleusement des services. Le pirate peut aussi utiliser ces privilèges pour trouver des mots de passe et des informations afin d'obtenir un accès à d'autre systèmes[PH 03].

1.4.8 Déstruction des traces

Grâce aux privilèges d'administrateur l'intrus peut effacer toute trace de son intrusion afin de ne pas éveiller de soupçons. Car par exemple les requêtes ayant provoqué un débordement (overflow) seront enregistrées dans les logs de serveur ainsi que l'adresse IP à partir du laquelle elles ont été lancées. Avec ces privilèges, le pirate peut réarranger tous les logs de sa cible pour masquer son intrusion[PH 03].

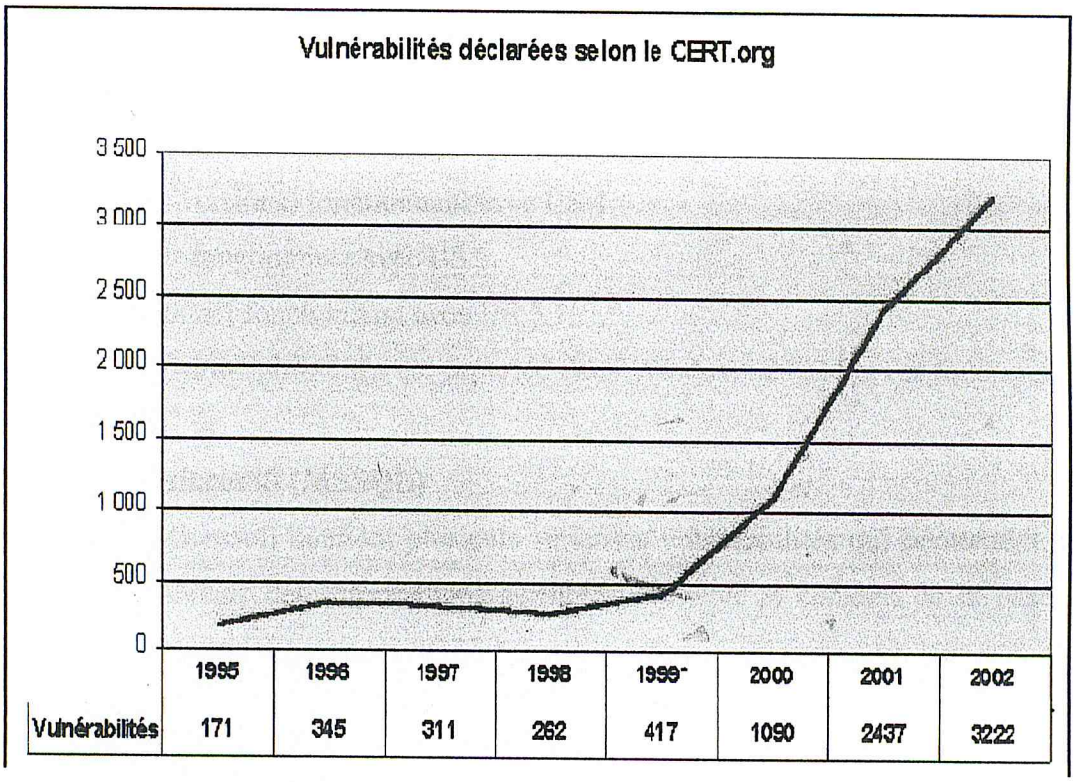
1.4.9 Mise en place d'une porte d'accés dérobée

Pour pouvoir reprendre possession de la machine même si le trou de sécurité qui a permis l'intrusion venait d'être fermé, le pirate peut installer un « backdoor »[PH 03].

1.5 LES PRINCIPALES VULNERABILITES DES SYSTEMES

La plus grande majorité des attaques réussies sont rendues possibles par des vulnérabilités inhérentes à un petit nombre de services communs dans les divers systèmes d'exploitation. Les attaquants prennent le chemin le plus facile et le plus commode et exploitent les vulnérabilités les mieux connues avec les outils d'attaque les plus efficaces et largement disponibles.

Selon CERT (Computer Emergency Response Team) les vulnérabilités des systèmes augmente chaque année



Graphe 1.2 : Les vulnérabilités systèmes [CERT 02].

Dans ce qui suit, nous allons décrit les principales vulnérabilités systèmes :

1.5.1 Principales vulnérabilités de système Windows

Selon l'Institut SANS (SysAdmin, Audit, Network, Security) [2003] les principales vulnérabilités de Windows sont :

- Internet Information Services (IIS).
- Serveur SQL Microsoft (MSSQL).
- Authentification Windows (AW).
- Internet Explorer (IE).
- Services d'Accès distant Windows.
- Composants Microsoft Data Access (MDAC).

- Windows Scripting Host (WSH).
- Microsoft Outlook et Outlook Express.
- Protocole SNMP (Simple Network Management Protocol).

1. Internet Information Service (IIS)

Les installations par défaut de IIS ont prouvé avec le temps leur vulnérabilité à un certain nombre d'attaques sérieuses. L'impact de ces vulnérabilités peut inclure :

• Le déni de Service.

• L'exposition ou compromission de fichiers sensibles ou de données.

• L'exécution de commandes arbitraires.

• La compromission complète du serveur [SANS 2003].

Systèmes d'Exploitation Affectés

Windows NT 4 (toutes versions) fonctionnant avec IIS 4.

Windows 2000 Serveur fonctionnant avec IIS 5.

Windows XP Professionnel fonctionnant avec IIS 5.1.

A ce moment, aucune vulnérabilité n'a été reportée dans Windows 2003 Server fonctionnant avec IIS 6 [SANS 03].

2. Serveur SQL Microsoft (MSSQL)

Le serveur SQL Microsoft contient plusieurs sérieuses vulnérabilités qui permettent aux attaquants distants d'obtenir des informations sensibles, d'altérer le contenu de la base de données, de compromettre les serveurs SQL (Structure Query Language), et dans certaines configurations, de compromettre les serveurs hôtes [SANS 03].

Systèmes d'Exploitation Affectés

Tout système Microsoft Windows avec le serveur Microsoft SQL/MSDE 7.0, le serveur Microsoft SQL/MSDE 2000 ou le Microsoft SQL/MSDE Desktop Engine installé, aussi bien que tout système qui utilise le moteur de MSDE séparément [SANS 2003]

3. Authentification Windows

Un accès correctement authentifié étant bien souvent non enregistré, un mot de passe compromis est une occasion d'explorer virtuellement sans détection un système de l'intérieur. Un attaquant aurait ainsi un accès complet à n'importe quelles ressources disponibles pour cet utilisateur, et serait significativement tout près d'avoir accès à d'autres comptes, à des machines proches, et peu être même à des privilèges administratifs. Les entreprises avec une bonne politique de mot de passe sont beaucoup trop rares.

Les vulnérabilités de mot de passe les plus communes sont:

• Comptes utilisateurs avec mots de passe faibles ou inexistants.

• Le système d'exploitation ou le logiciel additionnel créé des comptes administratifs avec des mots de passe faibles ou inexistants.

• Les algorithmes de hachage de mot de passe sont connus et les hashs sont souvent stockés de manière telle qu'ils sont visibles par n'importe qui [SANS 03].

Systèmes d'Exploitation Affectés

Tous les systèmes d'exploitation Microsoft Windows [SANS 2003].

4. Internet Explorer (IE)

Toutes les versions existantes d'Internet Explorer ont des vulnérabilités critiques, ces vulnérabilités peuvent être classées dans de multiples catégories incluant le « spoofing » (l'imitation) de pages web ou de l'interface Windows, des vulnérabilités de contrôle ActiveX, des vulnérabilités de script actifs, ainsi que des débordements de buffers. Les conséquences peuvent inclure la divulgation de cookies, de fichiers locaux ou de données, l'exécution de programmes locaux, le téléchargement et l'exécution de code arbitraire, ou la totale prise de contrôle du système vulnérable [SANS 2003].

Systèmes d'Exploitation Affectés

Ces vulnérabilités existent sur les systèmes Microsoft Windows fonctionnant avec n'importe quelle version de Microsoft Internet Explorer.

5. Services d'Accès distants Windows

La mauvaise configuration des partages réseau NETBIOS, les sessions nulles par connexions anonymes, l'accès distant à la Base de Registre et les appels de procédure distants constituent une grande part des exploits (i.e. exploitation des vulnérabilités) au niveau réseau sur Windows [SANS 03].

Systèmes d'Exploitation Affectés

Windows 95, Windows 98, Windows NT Workstation et Server, Windows Millennium, Windows XP Home et Professional, et Windows 2003 Server.

6. Composants Microsoft Data Access (MDAC) :

Des vulnérabilités plus récentes qui affectent beaucoup de versions de Windows ont aussi émergé, comme le débordement de buffer dans MDAC qui affecte la plupart des versions de Windows utilisées aujourd'hui. L'implémentation de MDAC dans Windows 2003 ne semble pas être vulnérable à cet exploit [SANS 03].

Systèmes d'Exploitation Affectés

La plupart des versions de Windows devraient être considérées comme vulnérables.

7. Windows Scripting Host (WSH) :

Cette fonction d'auto exécution de WSH (l'accès au shell Windows, au système de fichiers, à la base de registres) a été exploitée au printemps 2000 par le script Visual Basic du vers « The Love Bug » (connu aussi sous le nom de « ILOVEYOU »), causant des millions de dollars de dommages. Ce ver et d'autres qui l'ont suivi depuis, ont profité du fait que Windows Scripting Host (WSH) permet à n'importe quel fichier texte avec des extensions .vbs, .vbe, .js, .jse et .wsf d'être exécuté comme Script Visual Basic / JScript avec des privilèges de niveau applicatif ou système[SANS 03].

Systèmes d'Exploitation Affectés

Windows Scripting Host (WSH) peut être installé manuellement ou avec Internet Explorer 5 (ou plus récent) sur Windows 95 ou NT. Il est installé par défaut sur les versions Windows 98, ME, 2000 professionnel, XP professionnel et 2003 Server.

8. Microsoft Outlook et Outlook Express:

Un des buts de Microsoft a été de développer une messagerie électronique utilisable et intuitive ainsi qu'une solution de gestion de l'information. Malheureusement, les dispositifs inclus d'automatisation sont en contradiction avec les commandes de sécurité incorporées (souvent méconnues des utilisateurs finaux). Cela a été laissé à l'exploitation, augmentant l'expédition des virus par courrier électronique, des vers, de code malveillant pour compromettre le système local et beaucoup d'autres formes d'attaque [SANS 03].

Systèmes d'Exploitation Affectés

Les versions d'Outlook pour Microsoft Windows incluent:

- Outlook 95
- Outlook 97
- Outlook 2000, connu aussi sous le nom de Outlook 9
- Outlook XP, connu aussi sous le nom de Outlook 10 ou Outlook 2002

9. Protocole SNMP (Simple Network Management Protocol) :

Le Protocole de Gestion de Réseau Simple (SNMP, pour Simple Network Management Protocol) est considérablement utilisé pour contrôler et configurer à distance presque tous les types de systèmes modernes équipés de TCP/IP (voir plus loin dans l'Annexe A).

Les attaquants peuvent utiliser les vulnérabilités dans SNMP pour reconfigurer ou éteindre des dispositifs à distance. Un trafic SNMP « sniffé » peut révéler beaucoup d'information sur la structure de réseau aussi bien que sur les systèmes et dispositifs rattachés. Les intrus utilisent ce type d'information pour choisir les cibles et planifier des attaques [SANS 03].

Systèmes d'Exploitation Affectés

Presque toutes les versions des systèmes d'exploitation Windows fournissent SNMP comme option d'installation disponible.

1.5.2 ATTAQUES EXPLOITANT LES VULNERABILITES SYSTEME

Dans qui ce suit nous citons quelques fameux attaques exploitant les vulnérabilités systèmes

- **Accéder au fichier des mots de passe SAM (Security Account Manager)**

  Fichier SAM (Security Accounts Manager, Gestionnaire des comptes de sécurité) est l'un des principaux trésors de la base de registre NT. Il contient les noms des utilisateurs et les mots de passe cryptés de tous les utilisateurs de système local. Il se trouve dans \\WINNT\SYSTEM32\CONFIG\SAM.

- **Craquage de mot de passe par dictionnaire**

  La manière la plus classique par laquelle un Hacker va essayer d'obtenir un mot de passe est l'attaque par un dictionnaire. Dans ce genre d'attaque, le Hacker utilise un dictionnaire de mots et de noms propres, et il les essaie un par un pour vérifier si le mot de passe est valide. Ces attaques se font par des programmes qui peuvent deviner des milliers de mots de passe au second. Ce procédé est d'autant plus facile qu'il lui permette de tester des variations sur les mots : mots écrits à l'envers, majuscule et minuscule, ajout de chiffres à la fin du mot ... [DUP 02].

- **Craquage de Brute force**

  Ce procédé consiste à tester de façon exhaustive toutes les combinaisons possibles de caractères (alphanumérique + symboles), de manière à trouver au moin un mot de passe valide.

1.6 VULNERABILITES ET ATTAQUES DANS LA SUITE DE PROTOCOLES TCP/IP :

La suite de protocoles TCP/IP (voir annexe A), malgré sa popularité dans le monde Internet, n'est pas une suite de protocoles sûre à cent pour cent. TCP/IP était développée sous le parrainage du département de la défense Américaine pour des réseaux « amis » (Freindly Network) nommés ARPANET (Advanced Research Projects Agency), les développeurs voulaient que TCP/IP soit une suite ouverte et flexible. En dépit de ça, la suite TCP/IP a de nombreuses failles de sécurité qui peuvent être exploitées par des gens hostiles. Les principaux point faibles sont : [BEL 89]

1.6.1 Mots de passe envoyés en clair

Dans plusieurs applications TCP/IP, telle que Telnet, FTP (File Transfert Protocol), et POP (Post Office Protocol), les mots de passe sont envoyés sous une forme lisible (non chiffré) à travers le réseau local ou l'Internet. Un intrus peut facilement avoir les noms des utilisateurs et les mots de passe.

1.6.2 Buffer overflow

Plusieurs applications, telle que Finger (renvoie des informations sur un hôte ou un utilisateur distant), et HTTP (Hyper Text Transfer Protocol), n'assurent pas que les données envoyées par l'utilisateur ne dépassent pas la taille du buffer alloué par le programme. Il est possible dans certaines situations d'envoyer plus de données que le buffer supporte, si cette donnée est un code de programme substitué, l'attaquant peut avoir le contrôle du serveur.

1.6.3 Exploitation des failles IP (Internet Protocol)

Le protocole IP est considéré comme le protocole de base de TCP/IP, il existe plusieurs attaques visant ce protocole parmis les plus connus :

a. Trucage de la source (L'IP Spoofing)

L'agresseur change l'adresse IP de son ordinateur pour faire croire qu'il est un client certifié par le serveur.

Il va ensuite construire une route source jusqu'au serveur qui spécifiera le chemin de retour direct que les paquets IP devront prendre pour aller au serveur et qu'ils devront prendre pour retourner à l'ordinateur de l'agresseur en utilisant le client certifié comme dernière étape dans la route vers le serveur.

1-L'agresseur envoie une requête client au serveur en utilisant la route source.

2-Le serveur accepte la requête du client comme si elle provenait directemment du client certifié et retourne une réponse au client [CNA 01].

3-Le client, utilisant la route source, fait suivre le paquet à l'ordinateur de l'agresseur.

La figure suivante montre cette attaque

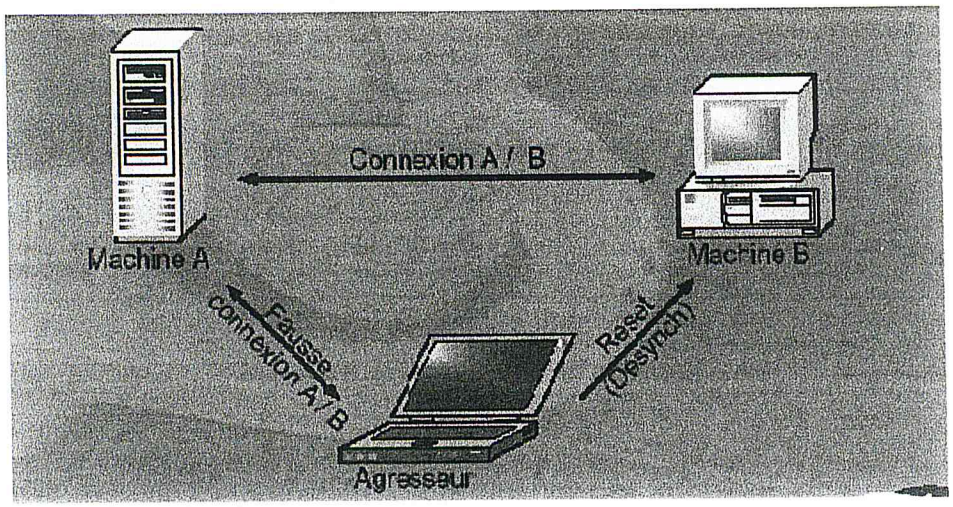


Figure 1.3: IP spoofing [Dup 01].

b. Petit fragment

Quand la taille d'un datagramme IP est plus grande que le MTU (Maximum Transfert Unit) d'un réseau il va être fragmenté pour qu'il puisse le traverser. Sachant que lors de la fragmentation seul le premier fragment IP contient les informations sur les couches supérieures (par exemple numéro de port TCP ou UDP). Plusieurs filtres de routeurs analysent seulement sur le premier fragment et ils ignorent le reste des fragments ; si le premier fragment est accepté le reste l'est aussi. Si un a attaquant envoie des datagrammes IP qui sont assez petit et ne contenant aucune information sur les couches supérieures, il peut passer à travers les filtres. La figure suivante présente cette attaque :

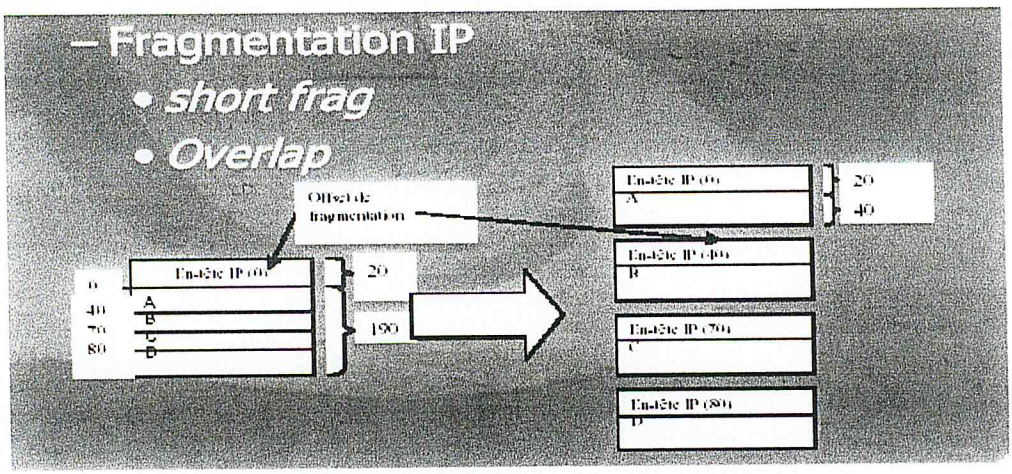


Figure1.4 : Attaque par petit fragment [Dup 01].

1.6.4 Utilisation frauduleuse des commandes ICMP (Internet Control MessageProtocol)

Il y a souvent des failles qui peuvent être exploiter, on cite parmi eux :

L'utilisation frauduleuse des commandes ICMP peut causer le blocage de machine victime, ralentissement de la connexion Internet, ... etc.

a. ICMP flooding

Cette attaque consiste à envoyer un nombre imporrtant de requête ping vers une cible. Cela provoque, des ralentissements ou un plantage de la machine cible

b. ICMP redirect

Il est utilisé par les passerelles pour donner des informations aux hôtes sur les chemins optimaux. Il est un peu similaire à RIP (Routing Information Protocol). La complication est qu'un message de redirection doit concerner une connexion existante. Quelques hôtes ne vérifient pas la validation de ces messages ; dans tel cas, il peut y avoir une attaque similaire à l'attaque basée sur RIP.

c. ICMP-destination unreachable

ICMP peut être aussi utilisé dans des attaques de déni de service (DoS). Plusieurs de ce message, tel que Destination Unreachable et Time to Live Exceeded, peuvent être utilisé pour fermer des connexions existantes par des intrus.

1.6.5 Exploitation des failles de TCP (Transmission Control Protocol)

Le TCP-Hijacking consiste pour l'agresseur à intercepter une connexion TCP/IP existante. Cette attaque peut être perpétrée lors de la session Telnet d'un administrateur, permettant ainsi à un attaquant de s'introduire dans une session telnet existante, sans se connecter à l'ordinnateur.

Cette attaque est réalisée en falsifiant l'adresse IP de l'expidéteur d'origine et en devinant le numéro correct de prochain paquet TCP [Mar 01].

1.6.6 Exploitation des failles UDP (User Datagramme Protocol)

De nombreuses attaques utilisent les failles UDP car le protocole UDP fonctionne en mode sans connexion et n'utilise pas de numéro de séquence, cette faille peut causer, soit la saturation de réseau ou une machine, soit autoriser l'accès à des fichiers distants NFS (Network File System).

De nombreuse applications, telles que DNS (Domain Name Service) et SNMP (Simple Network Management Protocol), utilisent UDP qui expose les utilisateurs au « déni de service ».

a. Attaque Bionk

Cette attaque vise les systèmes Win32. Elle consiste à envoyer des paquets UDP corrompus sur tous les ports ouverts. La machine cible ne peut pas gérer ces paquets et provoque un plantage [Ben 03].

b. Attaque Snork

Vise les systèmes WinNT. Elle consiste à envoyer une trame UDP provenant de port 7 (Echo), 19(Chargen) ou 135, et ayant pour destination le port 135, si les services sont lancés, cela a pour conséquence d'établir une communication de durée infinie, et génère des trames non nécessaire, cela réduit considérablement la bande passante et la puissance CPU [Ben 03].

1.6.7 Les failles de protocole RIP (Routing Information Protocol)

Le protocole RIP est utilisé pour propager les informations de routage dans un LAN (Local Area Network), essentiellement les media à diffusion. Typiquement les informations reçues ne sont pas vérifiées. Cela permet à un intrus d'envoyer de fausses informations de routage à un hôte spécifié, et à chaque passerelle le long du chemin, pour usurper l'identité d'un hôte particulier. L'attaque la plus probable est que l'intrus réclame un routage à un hôte particulier plutôt qu'à un réseau, tous les paquets vont être destinés à la machine de l'intrus. Une fois cela accomplie, les protocoles qui se basent sur l'authentification par adresse vont être compromis.

1.7 Le sniffing des mots de passe et des paquets

Cette méthode est devenue assez populaire. La plupart des réseaux utilisent la technologie de broadcast. En pratique tous les ordinateurs sauf le destinataire du message vont s'apercevoir que le message ne leur est pas destiné et vont donc l'ignorer. Mais par contre, beaucoup d'ordinateurs peuvent être programmés pour regarder chaque message qui traverse le réseau.

Il existe des programmes qui utilisent ce procédé et qui capturent tous les messages qui circulent sur le réseau en repérant les mots de passe. Les programmes de sniffing les plus

connu sont Sniff et TCPDump. Mais un sniffer est très bénéfique pour l'administrateur réseau pour détecter les failles de sécurité de réseau.

1.8 Attaque par déni de service (denial of service DOS):

Il existe divers types d'attaques par déni de services toutes les techniques existantes ont ceci de commun qu'elles visent à empêcher l'ordinateur ou le système d'exploitation visé de fonctionner normalement, ces attaques peuvent submerger le réseau de paquets inutiles corrompre ou saturent les ressources en mémoire ou exploitent une faille dans une application réseau, les techniques d'attaque par déni de services :

1. Attaque TCP SYN (TCP flooding).
2. Attaque ping of death.
3. Attaque Treadrop.
4. Attaque SMURF.

a. Attaque TCP SYN (TCP flooding) :

Cette attaque a pour principe d'ouvrir un très grand nombre de connexions TCP sur une machine cible afin de saturer ses ressources :

- Envoi d'un très grand nombre de paquets SYN (Synchronisation) vers la machine cible par la machine attaquante en cachant son adresse ;
- La machine cible renvoi les paquets SYN-ACK (Ackittement) en réponse ;
- La machine attaquante n'envoie jamais les paquets ACK ce qui laisse les connexions TCP en attente et consomme de la mémoire.

La figure suivante montre cette attaque :

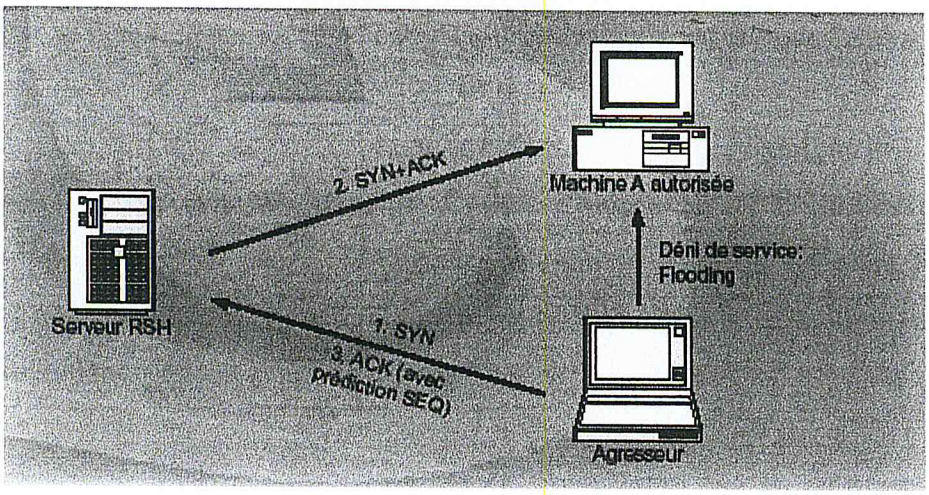


Figure1.5: TCP flooding [Dup 01].

b. Attaque de type ping of death

Cette attaque consiste à envoyer un ping de longueur supérieur à la taille maximale (65535), il est fragmenté en paquets plus petits. La machine cible recevant ces paquets commence alors à les reconstruire. Certains systèmes, tels que Win95, ne gèrent pas cette fragmentation et se plantent. Sur les systèmes Win2000 et WinXP, cette faille a été corrigée.

1.9 Les scanners

Un scanner est un programme qui permet de savoir quels ports sont ouverts sur une machine donnée. Les hackers utilisent les scanners pour savoir comment ils vont procéder pour attaquer une machine. Leur utilisation n'est heureusement pas seulement malsaine, car les scanners peuvent aussi permettre de prévenir une attaque.

Le plus connu des scanners réseau est ISS scanner, Retina, Realscure, Nessus [DUP 02].

1.10 Les chevaux de Troie

Un cheval de Troie est un programme qui semble effectuer une tâche par ailleurs une autre tâche. Un cheval de Troie peut modifier des bases de données, envoyer des messages ou même détruire des fichiers.il est très difficile de prévenir ou de détecter un cheval de Troie. Les chevaux de Troie les plus utilisés sont : Back Orifice 2000, Backdoor, Netbus, Subseven, Socket de Troie [WFI 99].

1.11 Les vers

Un ver est un programme capable de se propager et de s'autoreproduire sans l'utilisation d'un programme quelconque ni d'une action par une personne. Sur chaque ordinateur où il agit, le ver crée une nouvelle liste de machines distantes cibles.

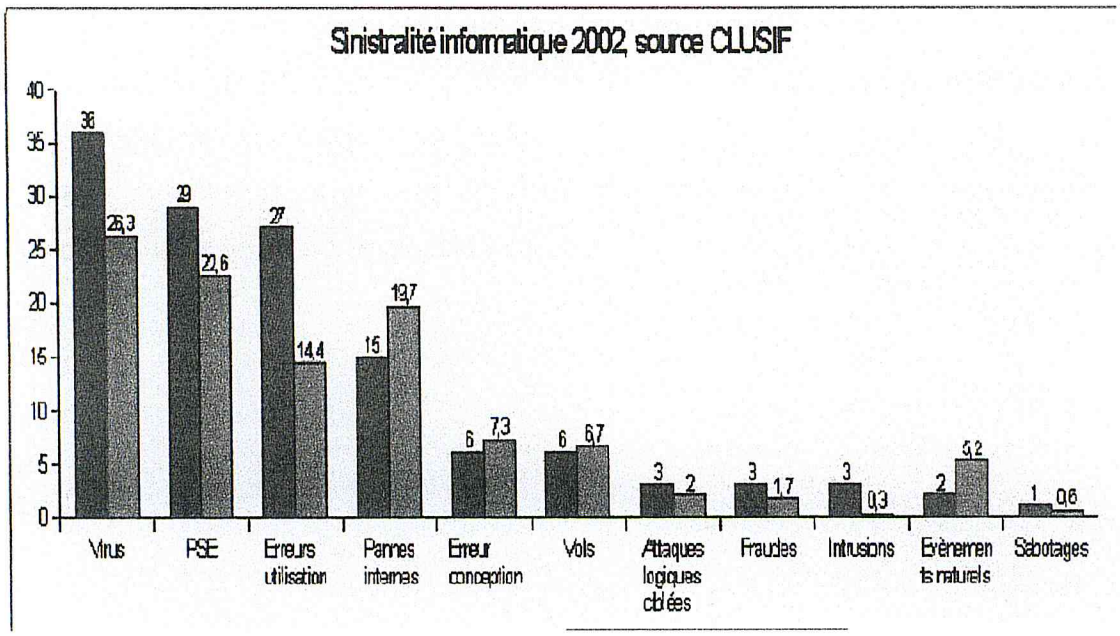
	Famille Cod Red	Famille NIMDA
Estimation de la vitesse de propagation	150 000 machines infectées en 14h	2.2 million de machine infectées en 24h
Impact économique mondiale estimé en 2001	2.62 milliards de Dollards	635 millions de Dollards

Tableau 1.1 : Dégâts de propagation des vers [CV 01].

1.12 Les virus

Un virus est une portion de code qui se recopie tout seule à l'intérieur d'un autre programme, et il ne peut s'executer que si celui-ci est actif ou si un événement est déclenché.

Selon CLUSIF (Club de la sécurité des systèmes d'Information Français), le principale risque externe se sont les virus.



Graphe 1.3 : Sinistralité informatique CLUSIF 2002 [CV 02].

1.13 Les trappes

Une trappe est un point d'entrée dans un système informatique qui passe au-dessus des mesures de sécurité normales. C'est généralement un programme caché ou un composant électronique rendant le système de protection inefficace. De plus, la trappe est souvent activée par un événement ou une action normale. Les trappes sont des programmes qui ne peuvent pas être détectés au niveau IP, mais au niveau application (signature).

1.14 Les bombes logiques

Ce sont des dispositifs programmés dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou m'importe quel appel au système.

1.15 CONCLUSION

Nous avons présenté dans ce chapitre les principales vulnérabilités de la sécurité, ainsi quelques attaques exploitant ces failles.

Dans le passé faire une attaque contre un système informatique était une tache très difficile qui demande beaucoup d'expérience, mais avec l'avènement de l'Internet des outils d'attaques sont devenus à la porté de tout le monde. Sachant que 99% des attaques proviennent des systèmes non « patchés ». Donc patché un système est considéré comme la première étape pour lutter telles attaques, mais cela reste insuffisant, autre mécanisme reste nécessaire pour renforcer la politique de sécurité.

Plusieurs mécanismes et services de sécurité ont été conçus pour lutter contre ces attaques, nous allons les voir dans le prochain chapitre.

CHAPITRE II

La sécurité Informatique

2.1 INTRODUCTION

La sécurité des systèmes informatiques comprend trois aspects majeurs qui sont : la confidentialités, l'intégrité, et la disponibilité de service. Pour assurer ces trois aspects, plusieurs mécanismes de sécurité ont été conçus et réalisés tels que les mécanismes d'authentification, de cryptage et de contrôle d'accès.

Dans ce chapitre, nous étudions la sécurité informatique et en particulier la sécurité dans les réseaux. D'abord, nous donnons une introduction très générale, puis nous étudions ses objectifs. Enfin, nous voyons les dispositifs possibles pour assurer la sécurité d'un système.

2.2 TERMINOLOGIE DE LA SECURITE INFORMATIQUE

Pour évaluer et choisir de nombreux produits et politique de sécurité il faut définir les exigences de la sécurité et caractériser les approches qui satisferont ces exigences. Une approche possible est de considérer trois aspects de la sécurité de l'information :

- Attaque.
- Service de sécurité.
- Mécanisme de sécurité.

2.2.1 Service de sécurité

C'est l'ensemble de contrôles physiques, des mécanismes et des procédures pour protéger le patrimoine informationnel et matériel des menaces de sécurité possibles [CHA 01].

2.2.2 Définition de la sécurité informatique

« La sécurité informatique est la capacité d'un système de protéger ses objets contre leur modification ou de leur utilisation par des personnes non autorisées » [OLO-92].

Un **objet** d'un système informatique est une entité passive qui contient ou reçoit de l'information (CPU, disque ou programme...). L'accès à un objet implique l'accès aux informations qu'il possède [DOD 85].

Un **sujet** d'un système informatique est une entité active, généralement sous la forme d'une personne, d'un processus ou d'un périphérique qui produit un flux d'information entre les objets ou qui change l'état du système. [DOD 85].

2.3 LES ASPECTS DE LA SECURITE :

Traditionnellement la sécurité a été divisée en trois différents aspects : la disponibilité du service, la confidentialité et l'intégrité.

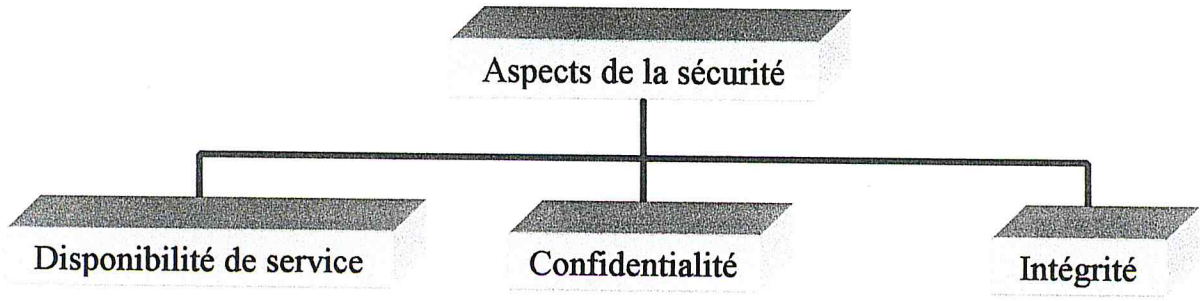


Figure 2.1 Aspects de la sécurité.

2.3.1 LA DISPONIBILITE DE SERVICE (AVAILABILITY) :

La disponibilité de service est la propriété d'être accessible et utilisable sur demande par une entité autorisée [ISO 89]. Une définition plus mathématique serais de définir la disponibilité de service comme étant la probabilité qu'un système soit opérationnel a un instant *t*, la perte de disponibilité est perçue comme étant un déni de service [OLO 92].

2.3.2 CONFIDENTIALITE (CONFIDENTIALITY) :

L'information contenue dans les objets ne doit être ni rendue accessible, ni divulguée, à un sujet non autorisé [NCS 87]. La confidentialité fait partie des propriétés à mettre en œuvre pour protéger les objets des diffusions non autorisées de l'information ou de l'utilisation non autorisée des ressources système tel que CPU, programmes et autres types d'équipement.

2.3.3 L'INTEGRITE (INTEGRITY)

L'information contenue dans les objets ne doit pas être altérée ou détruite de manière non autorisée (accidentelle ou maligne) [NCS 87]. Donc toute information n'est modifiée que par les personnes en ayant le droit.

2.4 LES FORMES DE SECURITE

Un attaquant peut trouver différents objets à attaquer dans un système dans le but d'obtenir une information spécifique : les composants logiciels d'un système peuvent être attaqués, l'installation physique des ordinateurs peut être attaquée, donc il est nécessaire de diviser la sécurité en différentes formes qui rassembleront les caractéristiques de la sécurité semblables ensemble.

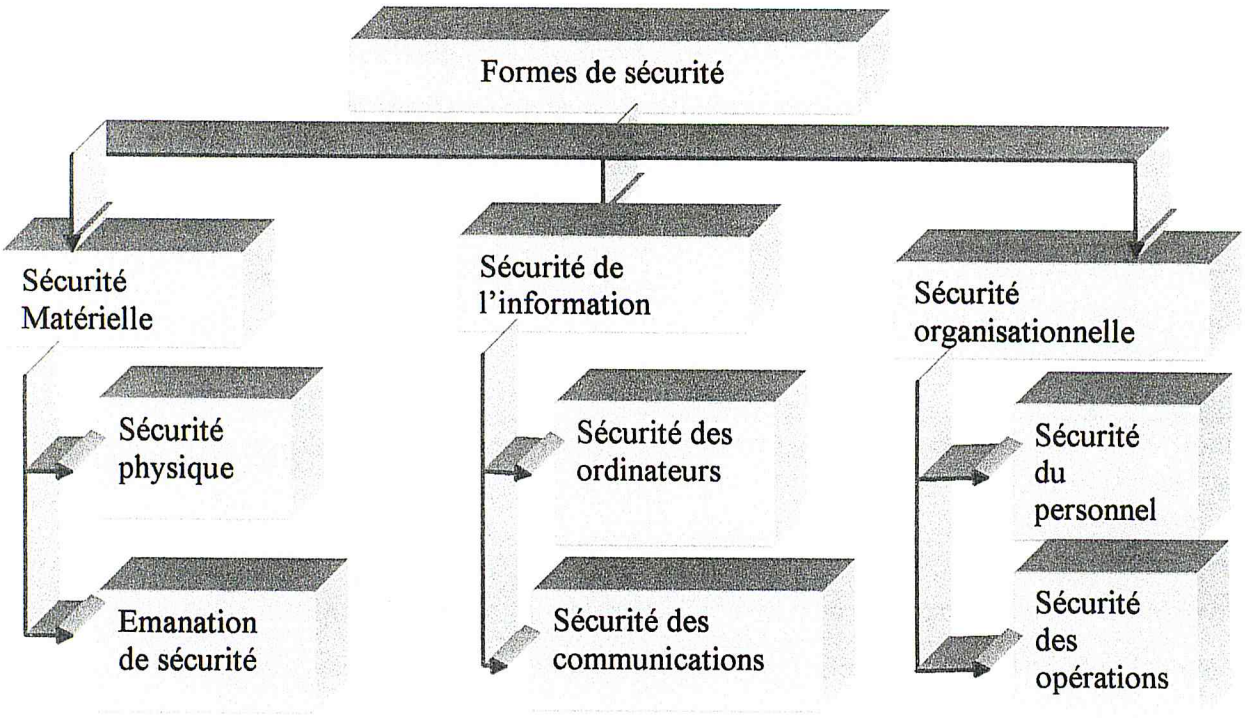


Figure2.2 : Les formes de la sécurité [ABD 01].

Cette structure est basée sur l'emplacement où on peut trouver des vulnérabilité du système : vulnérabilité dans le matériel, vulnérabilité dans l'information ou le logiciel et vulnérabilité dans l'organisation administrative du système comme le montre la figure2.2.

2.4.1 Sécurité matérielle

La sécurité matérielle traite la protection des objets contre les vulnérabilités présentés lors de la manipulation du matériel. Elle peut être divisée en deux parties :

- Sécurité physique.
- Sécurité d'émanation.

a. Sécurité physique

Concerne la protection du matériel du système des menaces physiques externes, tel que les intempéries, le vol, les tremblements de terre, les inondations, tous les équipements contenant des informations sensibles doivent être protégés. Ce problème peut être résolu en plaçant l'équipement dans un environnement assez sécurisé pour contenir les informations traitées par cet équipement. la sécurité physique traite la manière de créer et maintenir un tel environnement.

b. Sécurité d'émanation :

Traite la protection contre l'émission de signal (i.e. d'information) par le matériel du système, par exemple émission électromagnétique ou émission audio.

2.4.2 Sécurité de l'information

La sécurité de l'information est la protection des objets des vulnérabilités présentes dans l'architecture du système, c- à- d vulnérabilités dans le logiciel ou le matériel et dans la combinaison des deux, elle peut être divisée en :

- Sécurité des machines.
- Sécurité de communication.

a. Sécurité des machines

Elle concerne la protection des objets contre les expositions et les attaques qui font usage des vulnérabilités dans l'architecture du système.

b. Sécurité de communication

Elle traite la protection de l'information durant son transport. Lors du transport d'objets, entre les machines, une attaque active peut être entreprise dans le but d'interagir avec le processus de communication. Par exemple, pour modifier, retransmettre, réordonner ou détruire l'information.

2.4.3 Sécurité organisationnelle

La sécurité organisationnelle est la protection des objets contre les vulnérabilités causées par les utilisateurs (i.e les humains) et les menaces contre l'organisation de la sécurité des opérations, elle set divisée-en :

- Sécurité du personnel.
- Sécurité des opérations.

a. Sécurité du personnel

La sécurité du personnel est la protection des objets contre les attaques des utilisateurs légitimes. Les utilisateurs d'un système ont accès à différents objets, d'où la nécessité de mécanismes de protection contre les utilisateurs qui abusent de leurs privilèges.

En général, des utilisateurs autorisés constituent une plus grande menace, que les attaquants externes. Les statistiques montrent que seulement 10% des Crimes de piratage informatique sont causés par des attaques externes, 40% par des attaques de l'intérieur et 50% par d'anciens employés comme acte de vengeance. En clair, la sécurité du personnel doit avoir une grande influence sur les mécanismes de sécurité à implémenter dans le système.

b. Sécurité des opérations

Elle traite des moyens à mettre en œuvre pour renforcer les règles de sécurité établies dans la politique de sécurité, les actions à prendre quand une violation de la sécurité est détectée, ...etc. Il est important que les personnes responsables du maintien de la sécurité du système soient continuellement à jour, pour le renforcement des mécanismes de sécurité.

2.5 SERVICES DE SECURITE

L'ISO (International Standards Organization) à défini cinq catégories de services de sécurité. Sachant qu'un même mécanisme peut être utilisé pour réaliser plusieurs services.

- Service d'authentification.
- Service de contrôle d'accès.
- Service de confidentialité.
- Service d'intégrité.
- Service de non-répudiation.

2.5.1. L'authentification

Ce service permet d'authentifier les entités qui communiquent entre elles, il a pour but de garantir l'identité des correspondants, on peut distinguer deux types :

a. Authentification de l'entité homologue

Ce service est prévu pour être utilisé lors de l'établissement de la phase de transfert de données d'une connexion pour assurer que l'entité réceptrice et connectée est bien celle annoncée son objectif principal est la lutte contre le déguisement.

b. Authentification de l'origine des données

Ce service confirme la source d'une unité de données, le service n'assure pas de protection contre la duplication ou la modification des unités de données [ABD 01].

2.5.2 Contrôle d'accès

Le contrôle d'accès est un service de protection contre l'usage non autorisé des ressources accessibles par le réseau. Ce service utilise le service d'authentification afin de s'assurer l'identité des correspondants échangés lors de la phase d'initialisation des dialogues, par exemple : on peut demander à ce service d'attribuer des droits d'accès en lecture et écriture sur une ressource d'information ou de limiter l'utilisation d'une ressource de communication.

2.5.3 Confidentialité des données

Elle assure la non divulgation des données à des personnes non autorisée, on distingue plusieurs cas :

a. La confidentialité en mode orienté connexion

L'ensemble des données transmises sur une connexion donnée doit être protégé.

b. La confidentialité en mode sans connexion

Ce service assure la confidentialité de toutes les données de l'utilisateur (N) dans une unité de service (N) en mode sans connexion.

c. Confidentialité sélective par champ

Ce service assure la confidentialité de champ sélectionné dans les données de l'utilisateur (N) au cours d'une connexion (N).

d. Confidentialité du flux de données :

Ce service assure la protection des informations qui pourraient être dérivées de l'observation des flux de données [ABD 01].

2.5.4. Intégrité des données

Contre les attaques actives en offrant une protection efficace contre la modification, l'insertion et l'effacement des données et des flux entre émetteur et récepteur, on distingue cinq classes de services :

a. L'intégrité des données en mode connexion avec récupération

La vérification d'intégrité se fait sur l'ensemble des données transmises où le service relève les modifications, les insertions, les suppressions et les répétitions des données et assure la remise en état des données.

b. L'intégrité d'un champ spécifique

Ce service assure la détection de modification dans un champ de données sélectionnée.

c. L'intégrité des données en mode sans connexion

Ce service agit sur quelque données incluses dans une transmission (les modifications, suppression, insertions et répétitions sont détectées).

2.5.5 La non-répudiation

La répudiation est la possibilité pour une des entités impliquées dans une communication, de nier avoir participé aux échanges, totalement ou en partie. Le service de non répudiation doit assurer l'impossibilité de nier la participation à une communication [CHA 01].

2.6 MECANISMES DE SECURITE

Un mécanisme de sécurité est une méthode spécifique qui implémente une ou plusieurs fonctions de sécurité. L'ensemble des mécanismes de sécurité peut être divisé en trois sous ensemble :

- Ensemble des mécanismes garantissant la sécurité logicielle.

- Ensemble de mécanismes garantissant la sécurité matérielle.
- Ensemble de mécanismes garantissant la sécurité organisationnelle. [CHA 01]

Dans cette partie nous présentons les mécanismes les plus utilisés pour l'implémentation des différents services de sécurité.

2.6.1 Le chiffrement

Le chiffrement est l'opération qui consiste à transformer tout ou partie d'un texte dit clair en cryptogramme, message chiffré ou protégé. Si une ligne utilise des dispositifs de chiffrement, les données sont transmises sous une forme brouillée de manière qu'elles ne puissent être comprises par un intrus. Il existe deux classes d'algorithmes de chiffrement :

a. Chiffrement symétrique :

Les algorithmes de chiffrement symétrique (algorithme à clé secrète) utilisent la même clé pour le chiffrement et le déchiffrement comme par exemple DES (Data Encrypting Standard) [NBS 77]. Un autre exemple simple d'algorithme à clé secrète est le codage de César qui consiste à remplacer chaque lettre de message d'origine par une lettre de l'alphabet située n position plus loin. L'algorithme permute les lettres vers la droite ou vers la gauche, selon qu'il s'agit du processus de cryptage ou de décryptage.

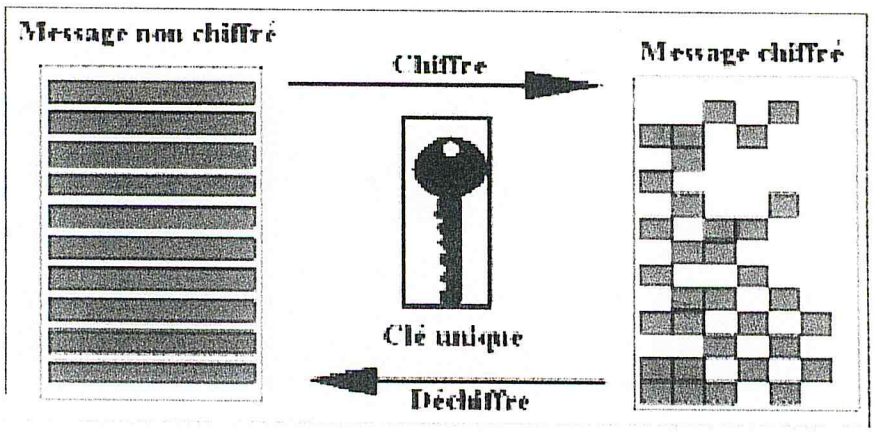


Figure 2.3 : Le chiffrement à clé symétriques.

b. Chiffrement asymétrique

Les algorithmes de chiffrement asymétrique utilisent deux valeurs de clés différentes : une clé pour le chiffrement qui est la clé publique (connue par tout le monde), la deuxième pour le déchiffrement qui est la clé privée (clé secrète) qui ne doit pas être divulguée par le récepteur.

Les algorithmes à clé publique sont surtout utilisés aux fins suivantes :

- Intégrité des données.
- Confidentialité des données.
- Non _ répudiation de l'émetteur.
- Authentification de l'émetteur.

Les algorithmes à clé publique les plus connus sont RSA, El Gamal.

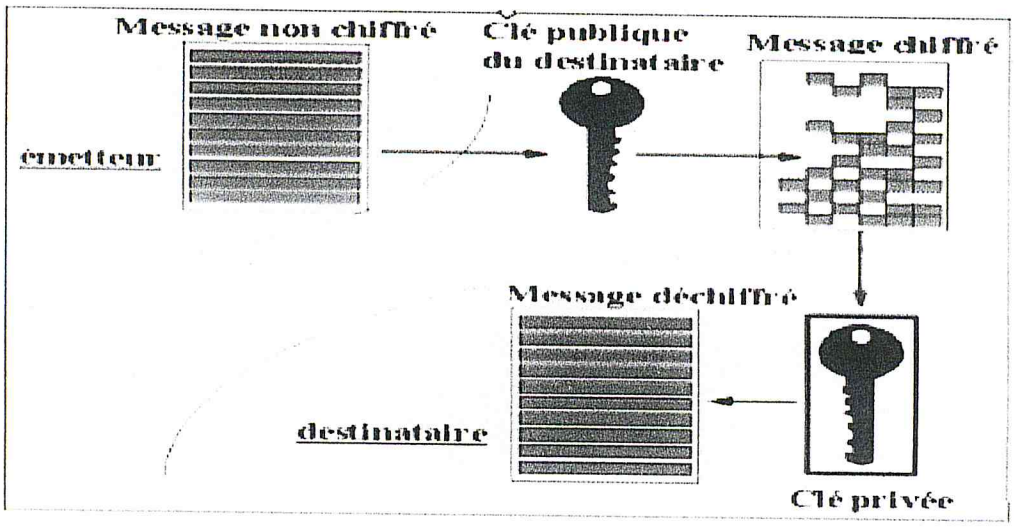


Figure 2.4 : Le chiffrement à clés asymétrique.

2.6.2 Authentification

Authentification est le processus qui permet de valider l'identité d'un utilisateur ou d'un équipement (client, serveur, dispositif pare _ feu ...), c'est un processus vital sur un réseau, car l'accès aux ressources est basé sur l'identité.

La phase d'authentification de l'utilisateur consiste à associer à chaque utilisateur un unique identifiant qui est en général un nom connu par tout le monde, que personne ne peut changer ou créer.

Cette phase est décomposée en deux parties : l'identification, lors de la quelle l'utilisateur présente son identifiant, et l'authentification où l'utilisateur prouve son identité.

2.6.3 Mécanismes de contrôle d'accès

Dans un système les objets sont protégés par un mécanisme de contrôle d'accès qui contrôle les façons dont les entités les utilisent. Les composants de base d'un mécanisme de contrôle d'accès sont les entités, les objets et les droits d'accès. Les droits d'accès définissent les privilèges des entités et établissent les conditions d'accès des entités aux objets et sous

quelles conditions ces entités ont le droit d'accès aux objets. Le contrôle d'accès peut être soit discriminatoire, soit mandataire [ABD 01].

a. Contrôle d'accès discrétionnaire :

Le contrôle d'accès est dit discrétionnaire lorsque la technique de restriction d'accès aux objets est basée sur l'identité des sujets et/ou des groupes auxquels ils appartiennent. Le contrôle est discrétionnaire dans le sens où un sujet possédant un certain droit d'accès est capable de conférer ce droit à tout autre utilisateur [BID 95].

Pour le cas d'un contrôle d'accès discrétionnaire, la gestion des informations sensibles (informations confidentielles, informations intègres) est sous la responsabilité du propriétaire de ces informations. Par ailleurs, la politique de sécurité est individuelle, c'est à dire que chaque utilisateur construit sa propre politique de sécurité. Le modèle de sécurité consiste alors à vérifiés que le système informatique applique correctement les droits d'accès spécifiés par chaque utilisateur [BID 95]. Les systèmes qui réalisent une politique d'autorisation discrétionnaire sont particulièrement vulnérables aux attaques comme le cheval de Troie.

b. Contrôle d'accès mandataire

Dans le cas d'une politique d'autorisation d'accès mandataire, les interactions entre sujets et objets sont dirigés par des règles incontournables. Ces règles déterminent les droits d'accès qu'un sujet particulier peut posséder sur n'importe quel objet. Le contrôle d'accès mandataire est requis pour les systèmes à haut niveau de sécurité [DOD 83].

2.7 LA POLITIQUE DE SECURITÉ

La politique de sécurité d'un système est l'ensemble des lois, règles et pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique [ITS 91].

L'analyse des menaces est d'une aide importante lors de la définition de la politique de sécurité, l'analyse de menace est un processus où toutes les menaces possibles contre un système sont identifiées, une liste contenant ces menaces et leur gravité est crée, cette liste est ensuite utilisée comme une base pour la définition de la politique de sécurité.

La politique de sécurité ainsi définie pourra être utilisée pour décider quel mécanisme de sécurité devrait être sélectionné, par exemple un mécanisme de contrôle d'accès qui décide quels entités est allouée a accédé à un objet donné [OLO 92].

Analyse de menace ➔ politique de sécurité ➔ mécanismes de sécurité

Figure 2.5 : Le rôle de la politique de sécurité.

2.8. LA SECURITE DANS LES COUCHES TCP/IP

Il existe de nombreuses technologies offrant des services de sécurité aux diverses couches de la pile TCP/IP (voir ANNEXE A). La couche application et la couche transport utilisent des protocoles de bout en bout, les systèmes doivent assurer la sécurité aux deux extrémités.

2.8.1. Protocole de sécurité de la couche Application

Un protocole de sécurité spécifique a été développé pour sécuriser les transactions Web qui SHTTP (Secure HyperText Transport Protocol).

Protocole SHTTP

Secure http a été conçu pour sécuriser les messages qui utilisent le protocole http en permettant aux messages de requêtes et de réponse d'être signés, authentifiés, cryptés.

Il supporte plusieurs mécanismes de gestion de clés, y compris les secrets partagés par échange manuel de mot de passe et l'échange de clés publiques. Il peut vérifier l'intégrité des messages de l'authenticité de l'émetteur en calculant un code d'authentification de message.

Il s'accorde le client et le serveur sur les caractéristiques suivantes :

- Modes de transactions : déterminer ce qui doit être signé ou crypté, ou les deux.
- Algorithmes de chiffrement : déterminer les algorithmes qui doivent être utilisés pour la signature et le chiffrement.
- Sélection de certificat : déterminer les certificats qui doivent être utilisés [Mer 99].

2.8.2. Protocoles de sécurité de la couche Transport

Ces protocoles sécurisent la couche Transport et fournissent des méthodes assurant la confidentialité, l'authentification et l'intégrité.

a. Protocole SSL

SSL (Secur Sockets Layer) est un protocole ouvert développé par Netscape. Il fournit un mécanisme pour garantir la sécurité des donnés implémentée entre les protocoles de niveau application(http, Telnet, Ftp) et TCP/IP. Il assure le chiffrement des données, l'authentification de serveur, l'intégrité des messages et l'authentification optionnelle de client pour une connexion TCP/IP. L'objectif principal de SSL est d'assurer la confidentialité et la fiabilité entre deux applications communicantes [Mer 99].

b. Protocole SSH

SSH (Secure Shell) fournit une protection sur un réseau non sécurisé. Il offre une sécurité pour les connexions à distance, le transfert de fichiers et la transmission du trafic TCP/IP. Il peut automatiquement crypter, authentifier et compresser les données transmises. Il fournit un chiffrement fort, une authentification d'hôte cryptée et une protection de l'intégrité. [Mer 99]

c. Protocole SOCKS

SOCKS (Socket Security) est un protocole de proxy sécurisé basé sur la couche Transport. Il fournit un cadre pour les applications client-serveurs, à la fois avec TCP et UDP pour exploiter de façon pratique et sécurisée les services d'un pare-feu de réseau [Mer 99].

2.8.3 Protocoles de Sécurité de la couche Réseau

La sécurité de ce niveau est gérée par les services au niveau de la couche IP de la pile de protocoles TCP/IP, un ensemble de standards ont été produit pour définir comment sécuriser les services au niveau de la couche Réseau

Suite de protocoles IP Security

IPSec s'applique au niveau IP, il est utilisé pour sécuriser n'importe quel type de trafic sur IP. IPSec comprend un ensemble de standards qui fournissent des services de confidentialité et d'authentification pour la couche IP. L'ensemble des services de sécurité IPSec peut assurer le contrôle d'accès, l'intégrité en mode non connecter, l'authentification de l'origine des données, le rejet de paquets redondants, la confidentialité (chiffrement). [Mer 99]

IPSec utilisent deux protocoles pour assurer la sécurité du trafic, qui définissent chacun un nouvel ensemble d'en-têtes à ajouter aux datagrammes IP :

- **En-tête d'authentification (AH) :**

Il garantit l'intégrité et l'origine des données, en incluant les champs invariants de l'en-tête IP externe. Il est employé lorsque la confidentialité n'est pas requise. La figure suivante représente l'application de AH.

En-tête IP original	TCP	Données

Avant application de AH.

En-tête IP original	AH	TCP	Données

Après application de AH.

Figure2.6 : En-tête d'authentification. [Mer 99]

- **Information de sécurité d'encapsulation (ESP) :**

Lorsque cet en-tête est ajouté à un datagramme IP, il protège la confidentialité, l'intégrité et l'authentification de l'origine des données. La figure suivante décrite l'application de ESP.

En-tête IP original	TCP	Données

Avant application dc ESP.

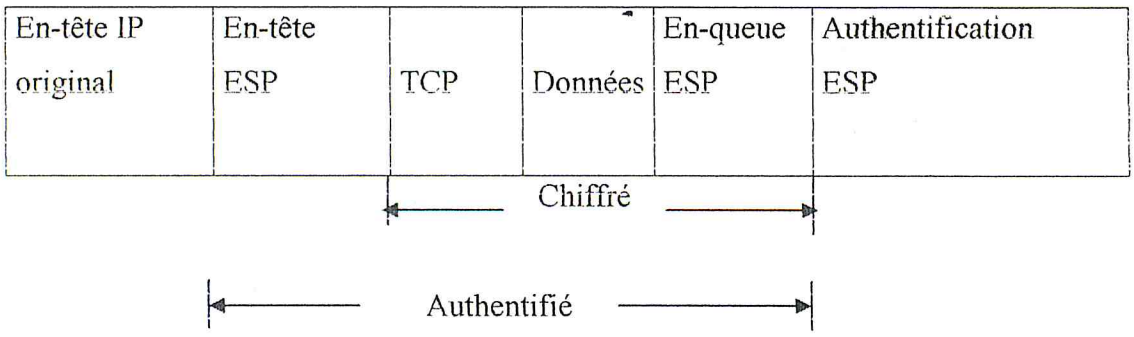


Figure2.7 : En-tête d'information de sécurité d'encapsulation. [Mer 99]

2.9 OUTILS DE SECURITE

Les trois principaux outils qui permettent d'assurer la sécurité des réseaux sont : les VPN (Virtual Private Network), les Firewalls et les systèmes de détection d'intrusion (IDS).

2.9.1 Les VPN :

Les réseaux privés virtuels permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Avec le développement d'Internet, il est intéressant de permettre ce processus de transfert de données sécurisé et fiable. Grâce à un principe de tunnel (tunnelling) dont chaque extrémité est identifiée, les données transitent après avoir été chiffrées. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'Internet. Le tunelling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

Il existe sur le marché quatre principaux protocoles [GUI 00] :

- PPTP (Point to Point Tunnelling Protocol) de Microsoft,
- L2F (Layer Two Forwarding) de Cisco,
- L2TP (Layer Two Tunnelling Protocol),
- IPSec (version protégée du protocole IP).

2.9.2 Les Pare-feu (Firewall)

Un Firewall, est un système physique ou logique servant d'interface entre un ou plusieurs réseaux afin de contrôler et éventuellement bloquer la circulation des paquets de données, en analysant les informations contenues dans les couches 3, 4 et 7 du modèle OSI (Open Systems Interconnection).

2.9.3 Les IDS

La détection d'intrusion est une technologie de sécurité complémentaire des autres mécanismes mis en œuvre dans le cadre d'une sécurité globale (authentification, chiffrement, outils de test de vulnérabilités, Firewall). Elle a pour objectif d'isoler les « intrusions » contre les systèmes informatiques, la mise en œuvre de cette fonctionnalité est réalisée par les outils de détection d'intrusion.

Les IDS (Intrusion Detection System) sont des systèmes qui collectent des informations de différents manières, soit à partir du système ou du réseau, sur les différentes activités se rapportent à ce même système pour les analyser à la recherche de signes d'une intrusion (attaques suspectes) et alerter dans le cas positif [BAC 00].

2.10 CONCLUSION

Il existe aujourd'hui très peu de systèmes sûrs en dehors de l'industrie militaire ou de quelques domaines spécialisés (multinationale investissant un gros budget pour la sécurité de leurs installations informatiques).

La sécurité joue un rôle très particulier, parce que la moindre défaillance peut compromettre le bon fonctionnement du système. Si l'algorithme d'ordonnancement marche dans 95% des cas, mais n'est pas équitable dans 5% des cas, le système continue à fonctionner. Si le système de sécurité ne marche que dans 95% des cas, les 5% restants peuvent être exploités par un adversaire et compromettre toute la sécurité du système.

Dans ce chapitre, nous avons identifié un certain nombre d'objectifs pour la sécurité et des menaces contre la sécurité des réseaux informatiques.

Les objectifs les plus importants sont :

- La confidentialité des informations stockées dans le système.
- L'intégrité de ces informations.
- La disponibilité des informations et des ressources du système.

Pour atteindre ces objectifs, le système doit mettre un certain nombre de dispositifs en place tel que le Firewall qui est l'objet d'étude du prochain chapitre.

CHAPITRE III

Les Firewalls

3.1 INTRODUCTION

Il existe plusieurs approches pour la prise en charge du problème de sécurité informatique d'un réseau d'entreprise connecté à un réseau externe [CHA 95].

L'approche la plus utilisée est la mise en place de mécanismes de sécurité au niveau des points d'accès au réseau. Ce point d'accès est appelé Firewall, il est composé d'une ou plusieurs fonctions de sécurité pour protéger le réseau contre les différentes attaques possibles.

3.2 DEFINITION D'UN FIREWALL

Le mot Firewall, posséde plusieurs traduction en français : « pare-feu » et « garde barrière », étant les deux les plus classiques. Nous préférons garder le mot en anglais, qui est le plus souvent utilisé.

Le terme Firewall est une métaphore pour désigner toute barrière qui protége un réseau informatique connecté à un réseau informatique pouvant présenter des risques de sécurité pour le réseau à protéger [BEL 94]. Le rôle du Firewall est de contrôler tous les accès aux ressources du système et de décider l'autorisation ou le refus de l'accès aux ressources demandées.

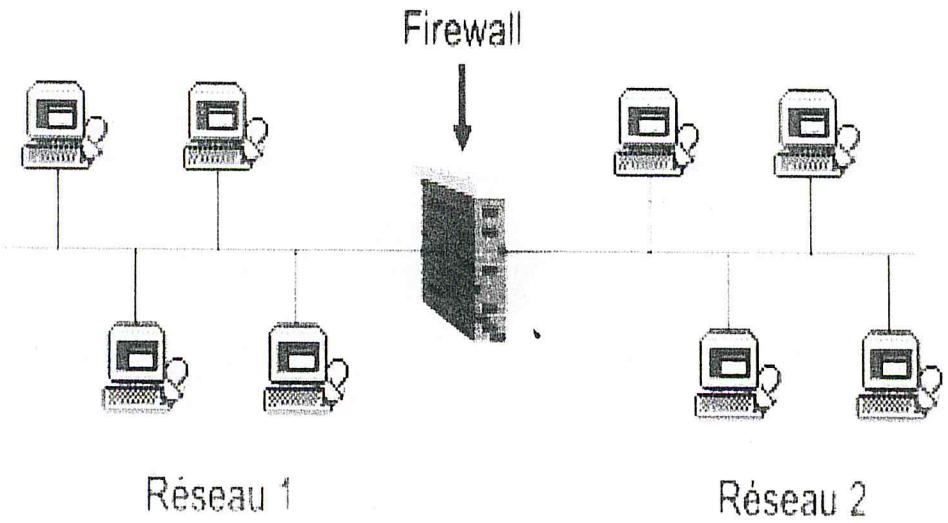


Figure3.1 : Firewall séparant 2 réseaux[SAU 03]

Souvent, on utilise un firewall pour protéger un réseau local du réseau Internet:

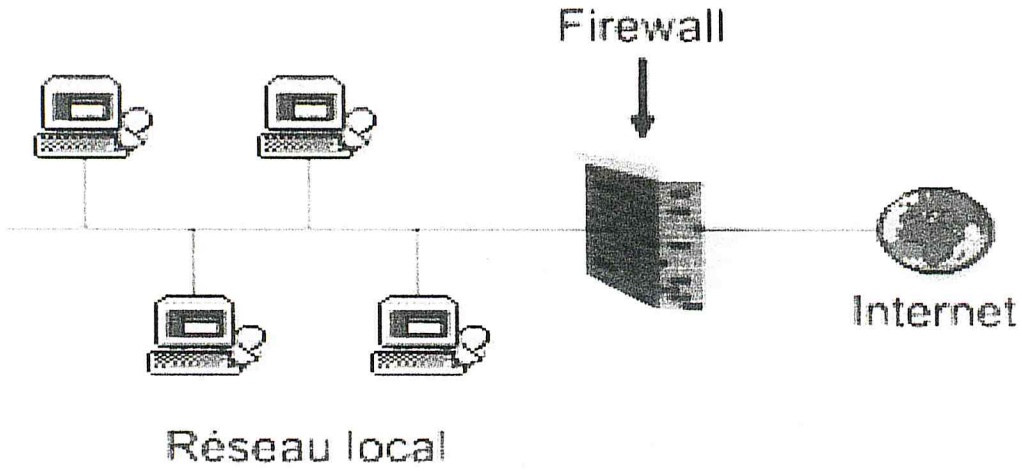


Figure3.2 : Firewall séparant le réseau local et l'Internet [SAU 03]

3.3 FONCTIONS DE SECURITE D'UN FIREWALL

Le firewall est un mécanisme de contrôle d'accès, il a pour vocation d'implémenter des fonctions de contrôle d'accès au niveau d'un réseau informatique.

Les différentes fonctions de contrôle d'accès implémentées par ce dernier sont [CHA 01] :

-La fonction d'authentification AF (Authentification function),

-La fonction d'intégrité IF(Integrity Function),

-La fonction de contrôle d'accès ACF (Access Control Function),

-La fonction d'audit Aud-f,

-La fonction de décision AEF (Access Enforcement Function).

- La fonction d'authentification **AF** vérifie l'identité d'une entité voulant accéder au réseau. L'AF est une composante nécessaire pour la fonction de contrôle d'accès ACF. Chaque entité voulant accéder au système doit être authentifiée à n'importe quel point de la connexion établie. Pour cela, des identificateurs sont attribués aux entités connues par la politique de sécurité.
- La fonction d'intégrité **IF** protège le trafic de données contre les modifications non autorisées telles que l'insertion, le remplacement, la suppression. Elle ne prévient pas l'occurrence de ces évènements mais elles les détectent.

- La fonction de contrôle d'accès **ACF** assure la réponse à la question : Quels sont les services ou les applications autorisés et ceux qui ne le sont pas? Dans le cas du trafic sortant, la fonction de contrôle d'accès prévient les connexions non autorisées aux sites externes ainsi que la diffusion d'informations sensible telles que le fichier des mots de passe. Dans le cas du trafic entrant, elle assure le contrôle de l'identité et les accès des entités externes voulant accéder au système.
- La fonction d'audit **Audf** permet de disposer d'un journal des événements touchants au système. Ce journal doit entre autre permettre de suivre la trace d'une éventuelle tentative d'intrusion et éventuellement l'utiliser comme pièce à conviction dans le cas ou le responsable de l'attaque est poursuivi en justice.
- Enfin, l'**AEF** ou « Access Enforcement Function » a pour objectif de conjuguer le résultat des fonctions de sécurité concentrées(AF, IF, ACF) et de vérifier que la décision d'autoriser ou de rejeter un paquet de données est bien cohérente au résultat de chaque fonction de sécurité.

3.4 FONCTIONS DE SECURITE DE BASE D'UN FIREWALL :

Le Firewall étant un mécanisme de sécurité, il implémente selon la politique de sécurité et selon certaines contraintes techniques les fonctions de contrôle d'accès adéquates [CHA-95]. Deux niveaux de contrôle d'accès sont possibles :

- Le contrôle d'accès des paquets échangés,
- Le contrôle d'accès des utilisateurs participant aux échanges de données.

Le contrôle d'accès des paquets doit considérer la nature du paquet, les machines sources et destination du paquet, ainsi que la direction du service demandé auquel appartient le paquet. En utilisant la terminologie du modèle client/serveur, on définit deux directions de service comme suit :

-Un service entrant « inbound service »; dans ce cas le client est à l'extérieur du réseau et le serveur offrant le service est à l'intérieur du réseau.

-Un service sortant « outbound service »; dans ce cas, le client est à l'intérieur du réseau et le serveur est à l'extérieur du réseau.

La politique de sécurité peut autoriser les services entrants à des utilisateurs connus. Ils doivent être authentifiés avant d'utiliser le service interne. Les services sortants sont très souvent autorisés par les politiques de sécurité car très souvent on fait confiance aux utilisateurs internes et non pas aux utilisateurs externes [CHA 01].

Selon que le service est entrant ou sortant, il implique des paquets entrants et sortants Le Firewall doit reconnaître si un paquet appartient à un service entrant ou sortant pour pouvoir lui appliquer le contrôle d'accès adéquat. Pour déterminer si un paquet donné appartient à un service entrant ou sortant et décider de l'accepter ou de le rejeter, les fonctions de filtrage du Firewall suivent le raisonnement exprimé par l'algorithme suivant :

3.4.1 Algorithme de contrôle d'accès des paquets [CHA 01]

Pour chaque paquet **Faire**

A. ***Si*** le paquet sortant est un paquet d'initialisation (SYN) de connexion venant des machines internes

Ou le paquet entrant est une réponse à une demande de connexion (SYN, ACK) lancée par un client interne vers un serveur externe

Alors

Le paquet appartient à un service sortant. Aller à C

B. ***Si*** le paquet entrant est une demande de connexion(SYN)

Alors le paquet appartient à un service entrant, Aller à C

C. ***Si*** la politique de sécurité autorise le service

Alors établir la connexion en prenant les mesures de sécurité nécessaires. Aller à D

D. ***Si*** le paquet appartient à la connexion autorisée

Alors Autoriser le paquet

Sinon rejeter le paquet

Fait.

3.4.2 Les différents types de filtrage [CHA 01]

Il existe trois fonctions de filtrage, qui sont :

1- Fonction de filtrage simple de paquet (Stateless Inspection),

2- Fonction de filtrage de paquet avec état (Stateful Inspection),

3- Fonction de filtrage applicatif (ou pare-feu de type proxy ou proxying applicatif).

a. Fonction de filtrage simple de paquet (filtrage statique)

Le filtrage statique est une des premières solutions firewalls a avoir été mis en oeuvre. Ce système inspecte les paquets *IP* (en-tête et données) des couches *réseau* et *transport* afin d'extraire l'adresse et le port source et l'adresse et le port de destination et le protocole utilisé, ces valeurs identifient la session en cours. Cette solution permet de définir si le paquet *IP* doit être accepté ou rejeté en fonction des règles définies.

a.1 Exemple

Nous supposons dans l'exemple qui suit que, pour chaque paquet, le systeme de filtrage examine les règles dans l'ordre à partir de la première. Il balaye jusqu'à trouver une règle qui correspondre au paquet, puis effectue l'action spécifiée.

Regle	Direction	Adresse source	Adresse destination	Protocole	Port destination	Action
A	Entrant	Externe	Interne	TCP	25	Permission
B	Sortant	Interne	Externe	TCP	>1023	Permission
C	Sortant	Interne	Externe	TCP	25	Permission
D	Entrant	Externe	Interne	TCP	>1023	Permission
E	Toutes	Toutes	Toutes	Tous	Tous	Refus

Tableau3.1 : Exemple de règles de filtrage.

Les règles A et B autorisent les connexions SMTP (Simple Mail Transfert Protocol) entrantes (courrier entrant).

Les règles C et D autorisent les connexions SMTP sortantes (courrier sortant).

La règle E est la règle par défaut qui s'applique si rien d'autre ne correspond.

Posons que l'adresse IP de notre hôte est 172.16.1.1, et que quelqu'un essaye de nous envoyer du courrier électronique depuis sa machine distante à l'adresse IP 192.168.3.5. Le client SMTP de l'expéditeur utilise le port 1234 pour parler à notre serveur SMTP qui se trouve sur le port 25.

Paquet	Direction	Adresse source	Adresse destination	Protocole	Port destination	Action (règle)
1	Entre	192.168.3.5	172.16.1.1	TCP	25	Permission (A)
2	Sort	172.16.1.1	192.168.3.5	TCP	1234	Permission (B)

Tableau3.2 : application des règles de filtrage.

a.2 Avantages et inconvénients des filtres à paquets

- C'est une solution non coûteuse, vu que les opérations de filtrage basées sur les adresses IP source et destination, le type de paquets, les numéros de port ...etc sont déjà intégrés dans les logiciels de configuration des routeurs standard.
- Les filtres à paquets sont flexibles, l'ajout d'un nouveau service sera pris en charge en ajoutant les règles de filtrage qui lui correspondent, il suffit pour cela de définir les numéros de port correspondant ainsi que le type de protocole du service.
- L'installation d'un filtre à paquet sur un réseau n'implique aucune modification sur le réseau des utilisateurs, ils sont transparents pour l'utilisateur.

Cependant, les filtres à paquets ont aussi des faiblesses qui sont :

- La fonction de filtrage ne peut pas filtrer efficacement les protocoles sans état tel que UDP.
- Ne peut pas filtrer les services utilisant le même port.

Exemple :

Si le service HTTP et FTP utilise le port 80. Un routeur filtre ne pourra pas autoriser le service http tout en interdisant le service FTP.

b. Fonction de filtrage de paquet avec état (filtrage dynamique)

Le filtrage dynamique reprend le principe de travail du filtrage statique au niveau de la couche réseau, ainsi que la transparence de sa mise en place. Or, de nombreux services (le *FTP* par exemple) initient une connexion sur un port statique, mais ouvrent dynamiquement

un port de manière aléatoire afin d'établir une session entre la machine faisant office de serveur et la machine cliente. Ainsi, il est impossible de prévoir les ports à laisser passer ou à interdire. Pour y remédier, l'entreprise CHECK POINT SOFTWARE TECHNOLOGIES a breveté un système de filtrage dynamique de paquets ou « stateful inspection » basée sur l'inspection des couches réseau et transport du modèle OSI. Cette technologie permet d'effectuer un suivi des transactions entre le client et le serveur et donc d'assurer la bonne circulation des données de la session en cours. Le filtrage dynamique tient donc à jour une table des connexions ouvertes par les clients pour certaines applications. C'est pour cette table gérée de manière dynamique qu'il porte son nom [PAU 03].

L'amélioration par rapport au filtrage simple, est la conservation de la trace des sessions et des connexions dans des tables d'états internes au Firewall. Le Firewall prend alors ses décisions en fonction des états de connexions, et peut réagir dans le cas de situations protocolaires anormales. Ce filtrage permet aussi de se protéger face à certains types d'attaques.

c. Fonction de filtrage d'application

La fonction de filtrage peut aussi être implémentée au niveau application du modèle TCP/IP et cela pour parer à certains limites posées par le filtrage au niveau inférieur. Cette fonction est nommée dans la terminologie des Firewalls «application proxy » ou « proxy service ».

Ainsi le Firewall pour contrôler le trafic de données peut implémenter des services proxy sur des machines, celles ci sont appelées application gateways ou passerelles d'application car elle achemine les paquets IP au niveau application du modèle OSI.

On peut représenter le service proxy par la fonction suivante :

P (paquet (en-tête IP, en-tête TCP, donnée)) **={accepter, refuser}**

P : la fonction de filtrage du niveau application, il s'agit du serveur proxy qui prend comme argument le **paquet** à analyser avec tous ses arguments entre autre les adresses sources et destination, les ports sources et destination ainsi que les informations liées à l'application ou le service.

Le filtrage réalisé à ce niveau peut être très fin puisque la fonction de filtrage a accès à tout le contenu du message.

Les applications Proxy gèrent le trafic sous le principe « Store and Forward » c'est à dire que les paquets sont stockés analysés puis acheminés vers leur destination ou encore rejetés.

La figure suivante schématise le passage du trafic de données à travers des passerelles d'application.

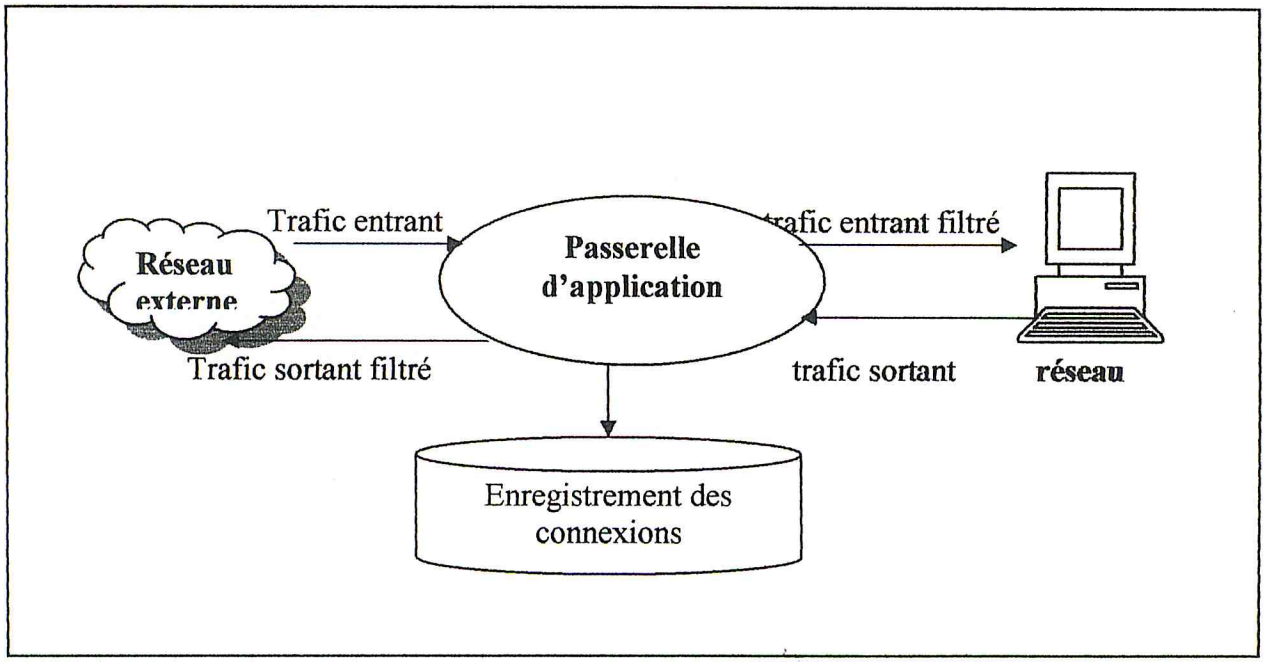


Figure3.3 : passerelle d'application.

L'utilisation des applications proxy nécessite le développement d'une application proxy pour chaque type de service ou application. Un paquet ne peut franchir la passerelle d'application que s'il existe sur celle ci une application proxy correspondant au service auquel il est destiné.

Concernant le fonctionnement de l'application proxy, celle ci se comporte comme serveur pour prendre en charge la requête du client interne, et comme client pour récupérer les réponses du serveur externe. Ainsi il n'y a pas de contacte direct entre le serveur externe et le client interne comme c'est illustré sur la figure3.3.

c.1 Avantages et inconvénients des applications proxy

-Le filtrage d'application permet de filtrer n'importe quel service, il suffit qu'il ait une application correspondante.

-L'un des avantages des applications proxy est le fait de garder le réseau interne inconnu de l'extérieur.

-De plus le fait de n'autoriser le passage qu'aux paquets ayant un proxy correspondant offre une forte sécurité. En effet, un nouveau service ne pourra pas traverser la passerelle d'application tant qu'on n'aura pas installé son application proxy.

-La programmation des applications proxy utilise des codes différents pour chaque service, ce qui apporte aussi un niveau de sécurité supplémentaire.

Les applications proxy présentent aussi certaines limites :

-Les applications proxy agissent au niveau le plus haut du modèle OSI, l'application proxy analyse entièrement le paquet de données ce qui rend le processus lent et limite le nombre de connexions simultanées au serveur proxy.

-l'utilisation des passerelles d'application n'est pas flexible.

3.5 ARCHITECTURE DES FIREWALLS

Il existe trois architectures de base pour un Firewall, chacune pouvant assurer un certain niveau de sécurité. Nous allons présenter les architectures de base des Firewalls en mettant en valeur leurs avantages et leurs inconvénients ainsi que leur champ d'action.

Avant de rentrer à proprement dit dans l'architecture des Firewalls, nous allons nous attarder sur quelques définitions nécessaires :

Hôte : un ordinateur rattaché au réseau

Bastion : le bastion est un ordinateur qui doit être le plus sécurisé possible car il est principalement exposé à l'Internet est le point de contacte avec les utilisateurs du réseau.

Hôte à double réseau (dual homed host) : ordinateur classique ayant au moins deux interfaces.

Réseau périphérique : c'est un réseau ajouté entre le réseau protégé et un réseau extérieur afin de fournir une couche de sécurité supplémentaire. Ce réseau est aussi appelé **DMZ** (De-Militarized Zone).

Les services ne pouvant pas être exécutés à l'intérieur du réseau sans causer des problèmes de sécurité sont transférés vers la zone DMZ où ils s'exécuteront soit sur des bastions ou des machines standard, ils sont éloignés du réseau interne et protégé du réseau externe.

Le Firewall peut contenir une ou plusieurs zones DMZ, elle est isolée entre deux dispositifs de sécurité comme c'est illustré dans la figure 3.4.

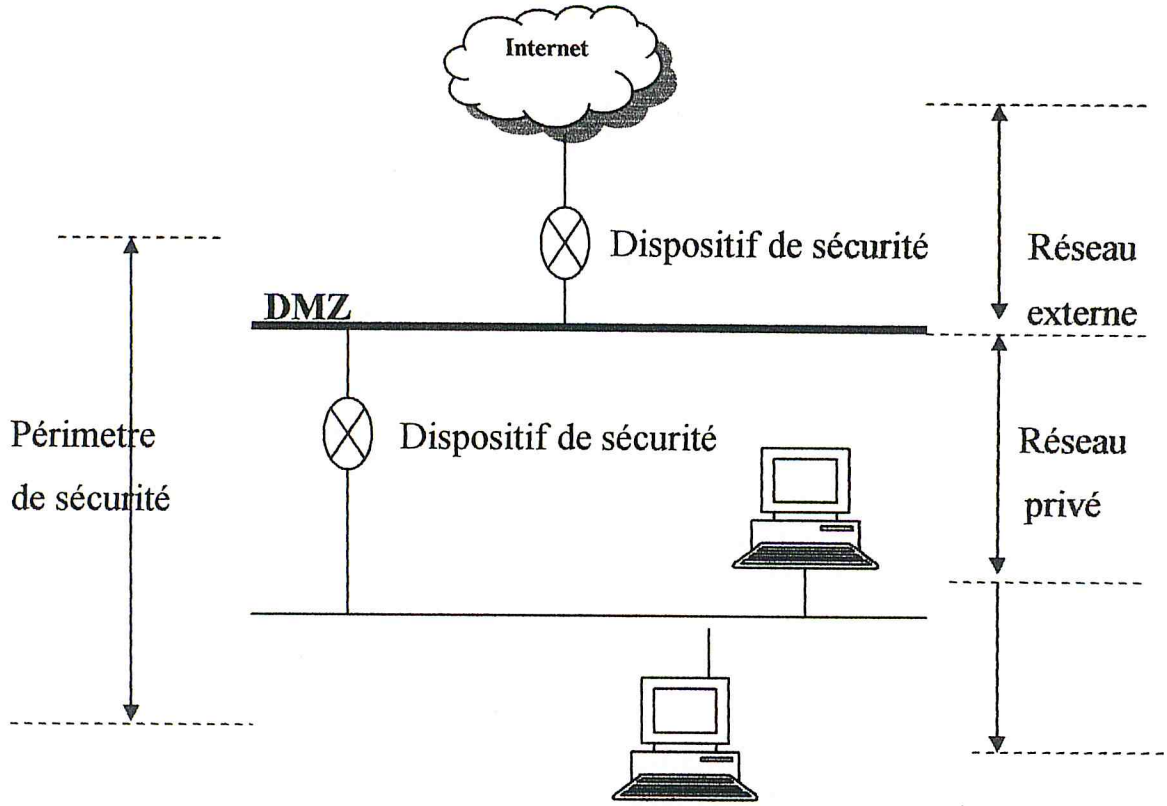


Figure3.4 : Représentation de la zone DMZ [CHA 01].

Les différentes architectures de base sont [CHA 01] :

3.5.1 Architecture d'hôte à double réseau (Dual homed host Firewall)

Dans ce cas le Firewall est composé par un hote à double réseau, Ce type de machine peut jouer le rôle de routeur entre les réseaux auxquels sont rattachées les interfaces, c'est à dire qu'il est capable d'acheminer les paquets IP. Il faut pourtant désactiver cette fonction de routage pour avoir une architecture d'hôte à double réseau. Ainsi, l'hôte à double réseau bloque complètement tout trafic IP entre le réseau interne et le réseau externe.

L'architecture réseau d'un hôte à double réseau est simple : la machine est située entre l'Internet et le réseau interne comme le montre la figure 3.5.

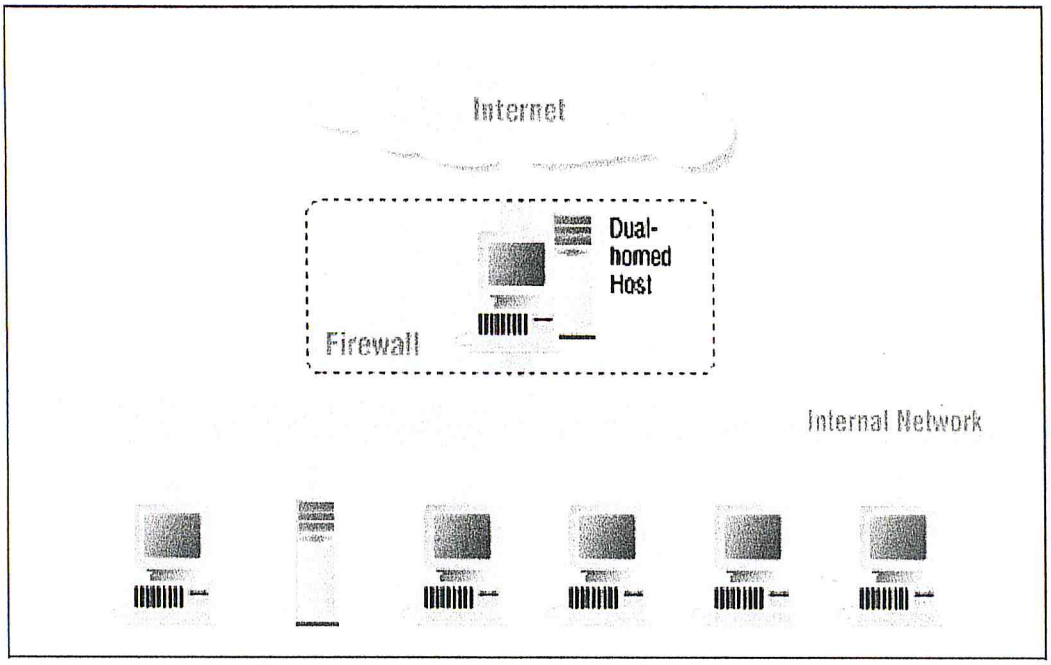


Figure3.5:Firewall d'hote à double réseau [CHA 95]

3.5.2 Architecture d'hôte à écran (Screened-host Firewall)

L'architecture d'hote à écran ou « screened host firewall » utilise un routeur filtre comme première ligne de défense et un bastion installé à l'intérieur du réseau ou s'exécutent des applications proxy. L'architecture d'hôte à écran est plus flexible que l'architecture d'hôte à double réseau. Cependant, cette flexibilité ne s'obtient pas sans perte de sécurité.
Le bastion ne laisse passer que les services qui possèdent un agent proxy associé. Le routeur filtre empêche les paquets dangereux d'atteindre le bastion et les machines du réseau interne. Il rejette ou accepte le trafic applicatif selon les règles suivantes :

1. Le trafic venant de l'Internet vers le bastion est routé,
2. Tout le trafic restant venant de l'Internet est rejeté,
3. Le routeur filtre rejette tout le trafic originaire du réseau interne sauf s'il vient du bastion.

Contrairement à l'architecture d'hôte à double réseau, l'architecture d'hôte à écran n'a besoin que d'une seule interface réseau et ne crée pas de sous-réseaux séparés entre le bastion et le routeur. Ceci permet à l'architecture firewall d'être plus flexible mais peut-être moins sûr

puisqu'il autorise le routeur à accepter les connexions aux services appartenant au domaine de confiance. Ces services appartenant au domaine de confiance peuvent correspondre aux services qui ne possèdent pas de service mandataire associé et qui présentent un niveau de risque acceptable suite à la phase d'analyse des risques au cours de l'élaboration de la politique de sécurité.

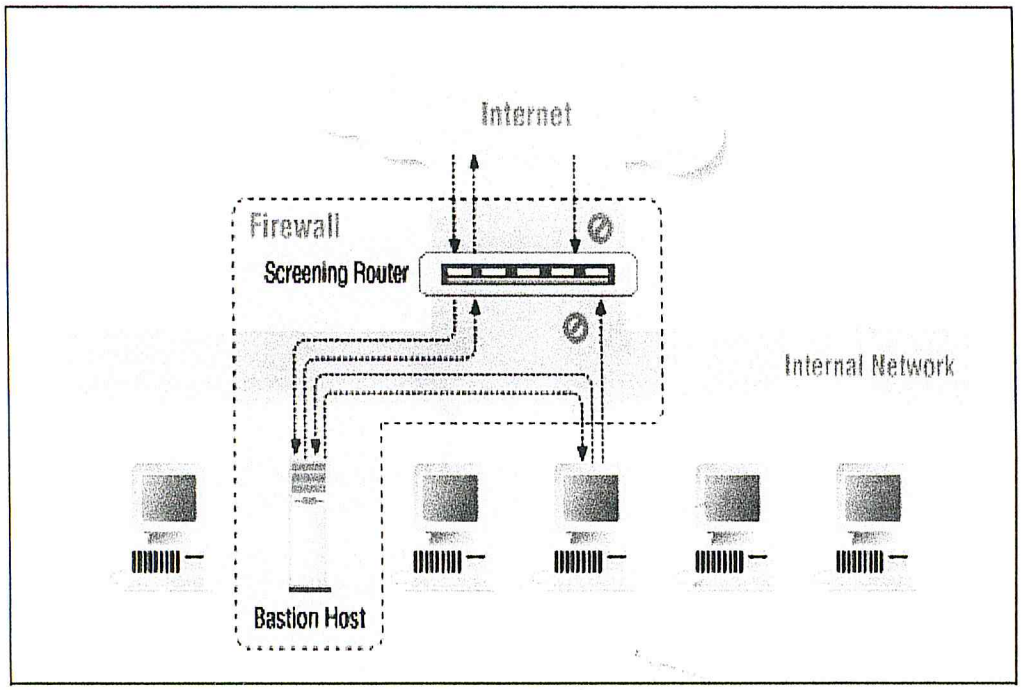


Figure3.6 : Firewall d'Hôte à écran[CHA 95]

D'une manière générale le routeur filtre est configuré de telle façon à diriger le trafic devant être filtré par les applications proxy vers le bastion et diriger certains services directement vers le réseau interne. Il faut être très prudent pour l'écriture des règles de filtrage.

3.5.3 Architecture de réseau périphérique (Sub-screened host firewall)

L'architecture de réseau périphérique ou DMZ *(Demilitarized Zone)* utilise comparativement à l'architecture d'hôte à écran un second routeur filtre. La zone qui se situe entre les deux routeurs s'appelle la zone démilitarisée *(DMZ)* ou le réseau périphérique car il s'agit, en fait, d'un réseau appartenant à la périphérie du réseau interne. De plus, le routeur filtre externe et le bastion représente la première ligne de défense après laquelle la probabilité d'intrusion est relativement faible. La seconde ligne de défense correspond au routeur filtre interne qui sert de sauvegarde au bastion pour protéger le réseau interne des machines

appartenant à la DMZ dans le cas où un agresseur serait parvenu à corrompre l'une d'entre elles.

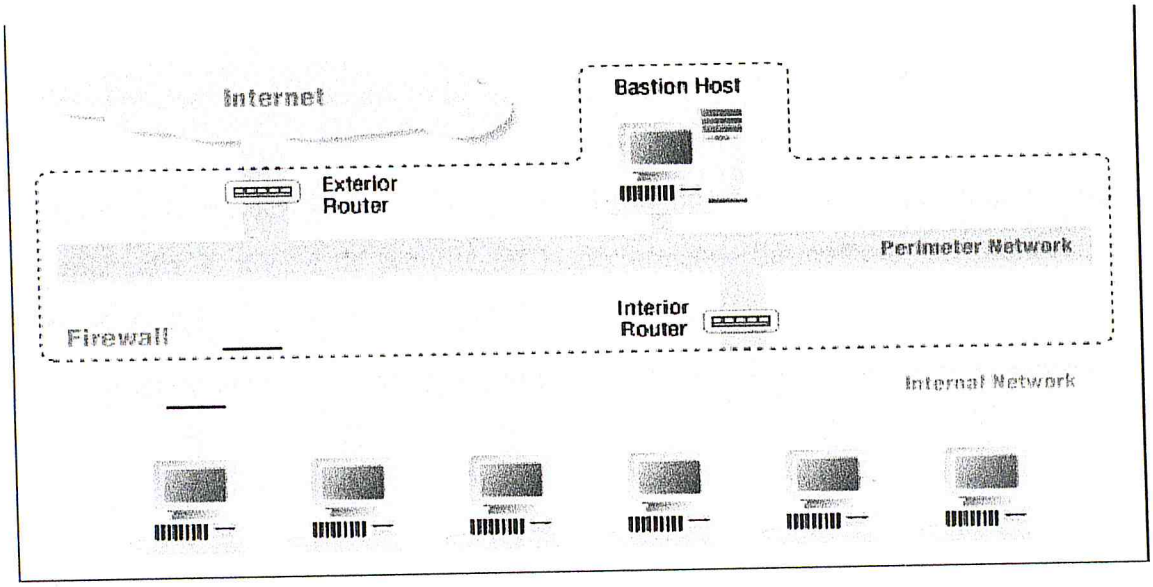


Figure3.7: Firewall de Réseau périphérique avec un seul bastion [CHA 95]

Pour des raisons de performances on peut utiliser plusieurs bastions pour exécuter sur chacun d'eux une application proxy comme le montre la figure suivante:

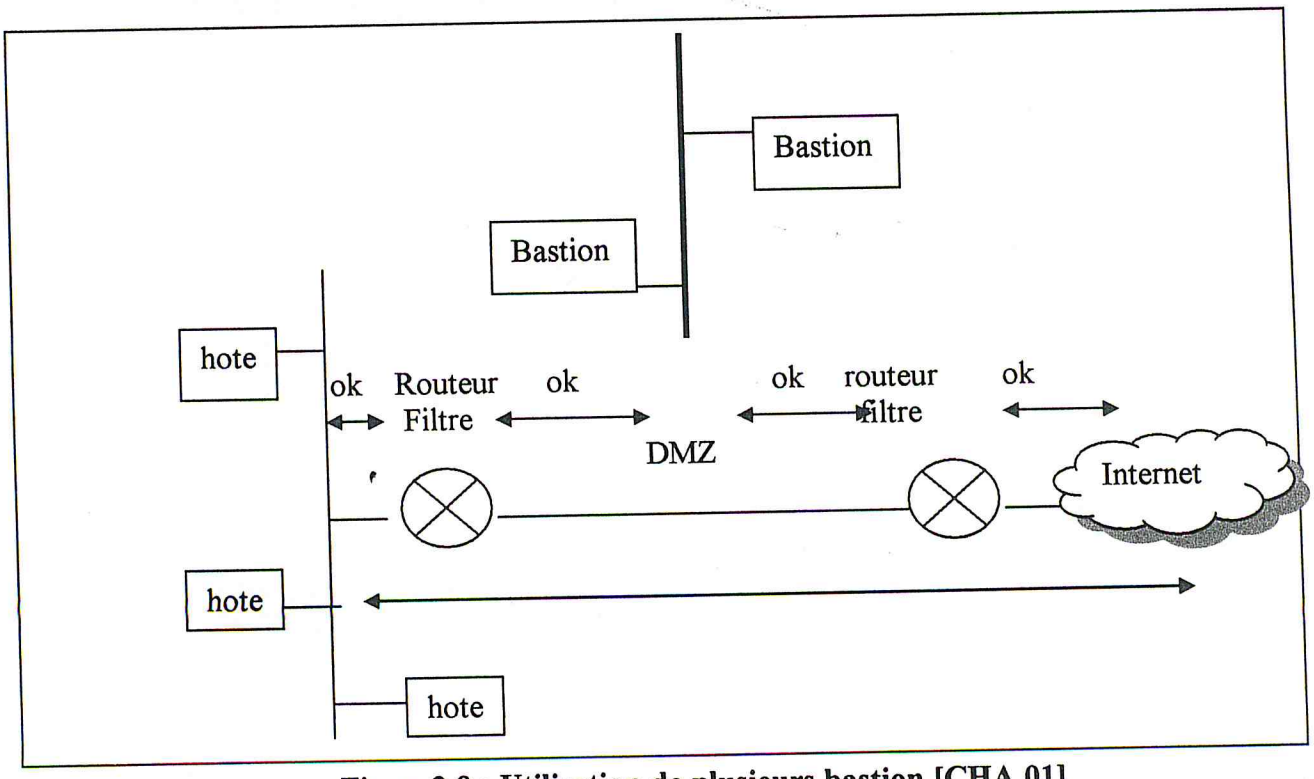
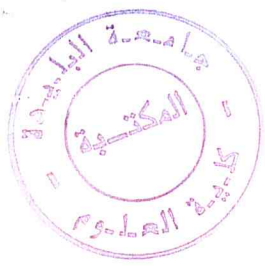


Figure3.8 : Utilisation de plusieurs bastion [CHA 01]

3.6 RECAPITULATIF

Le Firewall est un mécanisme de sécurité qui peut implémenter une ou plusieurs fonctions de sécurité selon les besoins en sécurité définis par la politique de sécurité. Notons qu'un Firewall est d'autant plus sécurisant que s'il est composé de plusieurs fonctions de sécurité [CHA-95]. Cependant l'installation de plusieurs fonctions de sécurité du Firewall sur le réseau diminue la vitesse du trafic traversant celui-ci, ce qui pose le problème de la dégradation des performances du réseau et par conséquent la dégradation du rendement des utilisateurs. Le choix des fonctions de filtrage et d'équipement correspondant doit assurer un compromis entre le niveau de sécurité et la performance du système sans oublier le coût qu'induit la solution de sécurité.

La règle générale de construction d'un Firewall est de disposer d'un maximum de lignes de défense pour diminuer les risques d'un intrus d'atteindre les ressources du réseau interne [CHA-95]. Le choix de l'architecture du Firewall dépend du niveau de sécurité requis par le réseau à protéger sans dégrader les performances de celui ci. De plus l'utilisation de certaines fonctions de sécurité impose l'utilisation d'un certain équipement et donc d'une architecture de Firewall. La fonction d'authentification par exemple ne peut être implémentée sur un routeur, elle pourra être implémenté sur une machine telle qu'un hote à double réseau ou sur un bastion. Dans le tableau suivant, nous avons représenté les architectures, leurs composants, leurs points forts et leurs points faibles.



Architecture	Composants	Utilisations	Faiblesse	Forces
Architecture d'hote à double réseau	Hote à double réseau	• Services Filtrables par adresse IP • Services Filtrables par proxy • Blocage de trafic	• Non flexible • Lent	• Bon Niveau de sécurité • Masque complètement la structure du réseau interne
Architecture d'hote à écran	Routeur filtre et bastion	• Services Filtrables par adresse IP • Services Filtrables par proxy	• Contourner son proxy et d'accéder directement au système.	• Flexible • Bon niveau de sécurité • Masque complètement la structure du réseau interne • Transparent aux utilisateurs finaux
Architecture de réseau périphérique	• routeurs filtre et/ou hote à double réseau et/ou bastion (DMZ)	• services filtrable par adresses • Services Filtrables par proxy	• architecture difficile à administrer • lent	• flexible • très bon niveau de sécurité • Masque complètement la structure du réseau interne

Tableau3.3 : Tableau récapitulatif des architectures de base des Firewalls.

3.7 SOLUTIONS ACTUELLES

De nombreuses solutions Firewalls existent sur le marché mais seul quelques solutions nous semblant être les plus répandues seront présentés ici. Il existe des Firewalls de deux types principaux :

- Les Firewalls matériels;
- Les Firewalls logiciels.

3.7.1 Solutions matérielles

Les Firewalls matériels vont du simple routeur qui assure, outre le routage, le filtrage de paquets. Ils présentent l'avantage d'etre particuliérement rapide, car le systeme d'exploitation mis en œuvre est optimisé de maniére à utiliser le minimum de ressources.

a. Cisco Secure PIX* Firewall

La gamme Cisco Secure PIX Firewall propose une réponse haute performance en matière de sécurité à tous les types d'applications sans impacter les performances du réseau. Depuis le pare-feu pour petites agences locales jusqu'au pare-feu pour grandes entreprises et fournisseurs de services, le PIX Firewall répond aux besoins des réseaux actuels à travers une sécurité, une fiabilité et des performances sans équivalent sur le marché[CIS 98].

b.Principales fonctionnalités

- Installation entre le réseau d'entreprise et le routeur d'accès à Internet,
- Nombreuses options de connexions LAN : Ethernet, Fast Ethernet, Token Ring ...
- Schéma de protection basé sur l'algorithme de sécurité adaptatif (ASA),
- Support de 250 000 connexions simultanées,
- Filtrage des URL,
- Interface utilisateur graphique pour l'administration et la configuration (logiciels PIX Firewall Manager et Setup Wizard),
- Notification d'alertes via e-mail [CIS 98],

* : Cisco Pix ne désigne pas un seul Firewall, mais une famille d'équipements. Différents modéles sont disponibles, selon la taille du réseau et les performances nécessaires.

3.7.2 Solutions logicielles

Les solutions logicielles sont généralement des programmes ou des services qui sont exécutés sur un serveur ou sur un poste de travail, en plus des autres programmes.

a. Zone Alarm pro

Zone Alarm est un utilitaire et un Firewall Internet de sécurité qui permet de détecter tout accès Internet d'un ordinateur et de controler les programmes qui ont accès à l'Internet. Zone Alarm inclut cinq services de sécurité qui fournissent la protection facile à utiliser et complète : un Firewall, une commande d'application des fonctions, capacité Internet de serrure, et une sécurité dynamiquement assignés des niveaux et zones [Lab 01].

b. BlackIce Pc Protection

Contrairement à Zone Alarm, BlackIce se concentre non pas sur les applications mais uniquement sur les paquets de données qui entrent dans le systeme.Lorsqu'un paquet suspect est détecté, il analyse son contenu et vérifie qu'il ne correspond pas à une intrusion répertoriée dans sa base de données qui en comporte plus de 400 [Net 04].

c. Norton Internet Security

Le succès de ce produit est essentiellement lié à son utilisation particuliérement simple avec des niveaux de sécurités prédéfinis, il est doté d'une fonction de Firewall par filtrage de paquets avec la possibilité d'établir des régles permettant de bloquer ou de transmettre les flux de données ICMP, TCP, et UDP [Sym 04].

De l'avis de nombreux spécialistes de la sécurité, les Firewalls matériels sont nettement plus sûr que leurs équivalents logiciels, pour les raisons suivantes :

- Les failles de sécurité du système d'exploitation rendent l'ordinateur vulnérable.
- Les programmes des Firewalls spécialisés comportent un nombre de lignes de code nettement faible, ce qui réduit le risque d'erreurs.

3.8 POINTS FORTS ET POINTS FAIBLES D'UN FIREWALL

Le firewall a pour vocation de contrôler l'accès au réseau qu'il protége en assurant le maximum de ces trois propriétés[BEL-94] :

- Tout le trafic entrant ou sortant doit passer par le Firewall.
- Le trafic autorisé tel que définit par la politique de sécurité locale est le seul qui peut passer.
- Le Firewall lui-même doit être impénétrable.

Les Firewalls différent par le fait qu'ils assurent la totalité ou une partie de ces propriétés. Les Firewalls présentent plusieurs avantages qu'on peut les résumer comme suit :

- Un Firewall est plus sécurisé qu'un simple hote, car il ne dispose que des services nécessaires à son fonctionnement, tous les autres services qui sont susceptibles de nuire à la sécurité du réseau sont désactivés.
- L'utilisation d'un Firewall concentre le problème de sécurité en un point unique ce qui est plus facile à gérer et à contrôler.
- Un Firewall permet de prévenir un certain nombre d'attaques dont les suivantes :
  - Tentative d'accès de l'extérieur du réseau au site interne non autorisée.
  - Authentification compromise: c'est l'utilisation de l'identité d'un utilisateur autorisé par un utilisateur non autorisé pour accéder au système.
  - Tentative d'accès de l'intérieur du réseau au site externe non autorisé.
  - le vol de session
  - Flooding (inondation)
- Un Firewall maintien un audit sur toutes les informations qui le traverse et permet ainsi de retrouver la trace d'une intrusion et de renforcer la sécurité au niveau des points représentant des failles.
- Lorsque le Firewall est bien configuré, il assure un bon niveau de sécurité.
- Possibilité de mettre en place un tunnel crypté pour l'échange des informations sensibles. Il s'agit du réseau privé virtuel (VPN : Virtual Private Network) Le trafic de données échangées entre les Firewalls est automatiquement crypté, ce qui assure la confidentialité et l'intégrité des données.

Le Firewall est un mécanisme de sécurité qui doit être intégré dans une solution de sécurité globale, car tout seul il ne peut pas prendre en charge certains problèmes de sécurité. Ainsi le Firewall présentent certaines limitations [CHA 01]:

- Le premier problème lié au fait que la configuration du Firewall est une opération très délicate qui pourrait être à l'origine de beaucoup de problèmes de sécurité. C'est le cas des filtres à paquets ou la simple erreur dans l'ordre des règles de filtrage pourrait être fatale pour la sécurité du réseau.

- Un Firewall ne protége pas des attaques au sein du réseau local. Si un pirate à l'interieur du réseau local veut attaquer une machine au sein du même réseau local, le Firewall (étant donné que le trafic n'y transite pas) ne sera d'aucune utilité.
- Un Firewall ne peut pas prévenir les attaques qu'il ignore ce qui signifie qu'il pourrait être victime à n'importe quel moment d'un nouveau type d'attaques d'un nouveau protocole.
- Un Firewall ne peut pas contrôler les connexions externes crées par les utilisateurs internes pour ne pas passer par le Firewall, citons l'utilisation d'une connexion directe vers l'extérieur par modem sans passer par le Firewall.
- Un Firewall ne peut pas se protéger contre les erreurs de programmation de son concepteur ou contre les erreurs de décisions liées à la politique de sécurité mise en œuvre par l'administrateur du réseau.

3.9 CONCLUSION

Dans ce chapitre nous avons identifié les différentes fonctions de contrôle d'accès qui pouvant être implémentées par un Firewall, notons que chaque fonction de contrôle d'accès a ses propres avantages et inconvénients. Nous avons présenté aussi les architectures de base d'un Firewall, chaque architecture répond à des besoins particuliers en sécurité définis par la politique de sécurité. Dans le prochain chapitre, nous allons voir en détail la conception et la mise en œuvre de notre Firewall.

CHAPITRE IV

Conception et mise en œuvre

4.1 INTRODUCTION

Dans le chapitre précédent, nous avons détaillé la technologie des Firewalls, car la réalisation d'un Firewall est le but de notre projet. Dans ce chapitre, nous allons fait l'étude de conception d'un Firewall qui servira à protéger une machine des dangers provenant de l'intérieur et l'extérieur (exemple Internet).

4.2 METHODES DE DEVELOPPEMENT

Dans la phase de développement de ce projet on a choisie une methode cascade. Ce modèle comporte sept phases ou activités principales que nous allons détailler brièvement dans la figure suivante :

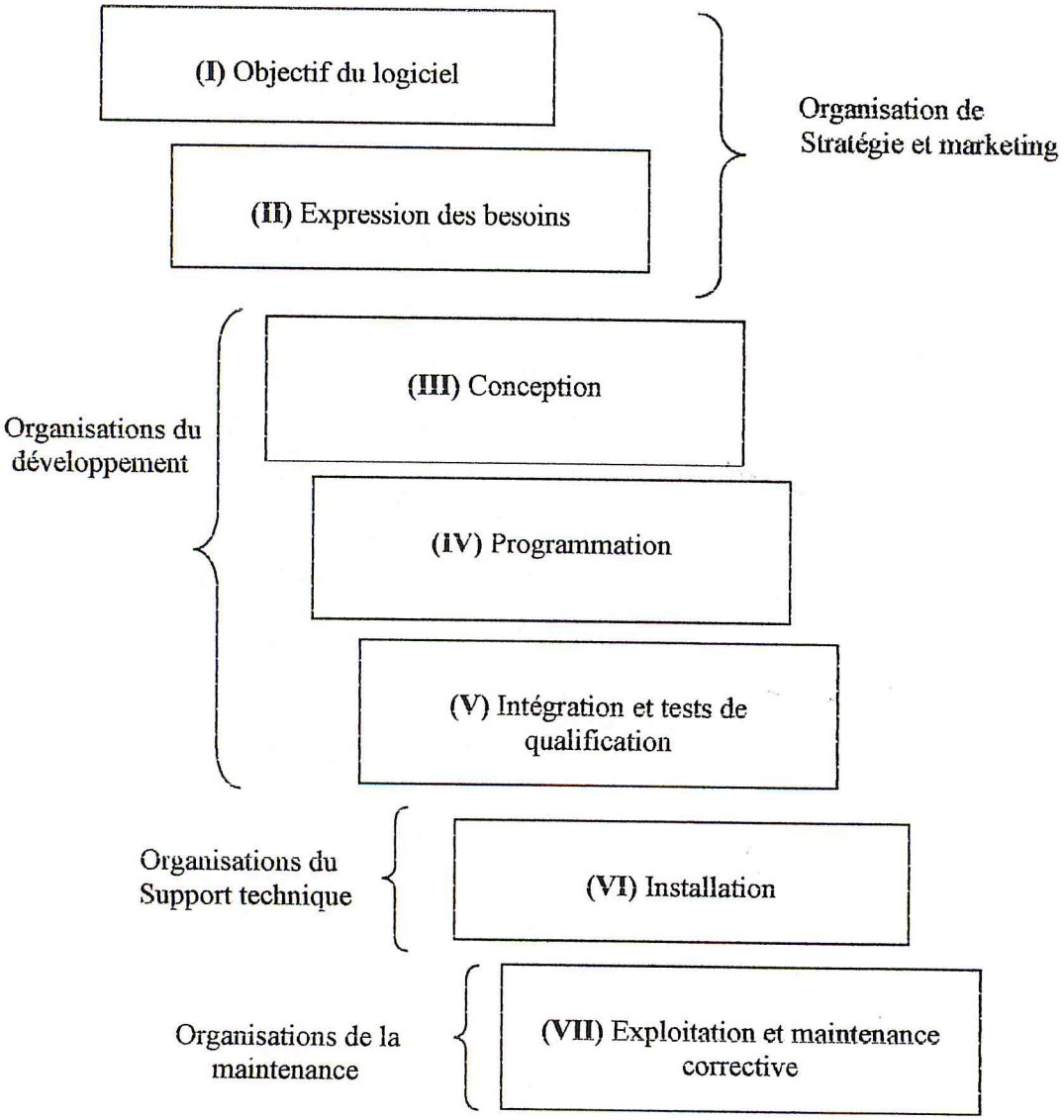


Figure4.1 : Phases de développement de projet.

4.2.1 Phase I Objectifs du logiciel

Cette phase initiale du développement de tout projet logiciel, notre objectif est la réalisation d'un Firewall pour le contrôle d'accès aux ressources d'une machine.

4.2.2 Phase II Expression des besoins

On décrit dans cette phase les fonctions que le logiciel doit effectuer :

- Filtrer les paquets IP ;
- Analyser le trafic ;
- Détecter les ports ouverts ;

4.2.3 Phase III Conception

La conception permet de définir de façon très précise les fonctions et l'architecture du logiciel, à partir des besoins exprimés en phase II, nous allons détailler cette phase par la suite.

4.2.4 Phase IV Programmation

Elle correspond à la programmation proprement dite des fonctions sur la base des informations précises venant de la phase de conception, on va détailler cette phase après la conception.

4.2.5 Phase V Intégration et tests de qualification

Cette phase correspond au regroupement progressif de tous les modules de façon à garantir la vérification et la validation progressive du logiciel, jusqu'à pouvoir le faire fonctionner dans son environnement réel.

4.2.6 Phase VI Installation

L'installation correspond à la mise en fonctionnement opérationnel du logiciel.

4.2.7 Phase VII Exploitation et maintenance

Elle à pour objectif de s'assurer que le logiciel installé fonctionne correctement.

4.3 LA CONCEPTION DU FIREWALL

4.3.1 L'APPROCHE UTILISEE

Parmis les fonctions de base de sécurité d'un Firewall citées dans le chapitre précédent, on a choisi la fonction de filtrage simple des paquets IP qui présente une bonne performance.

L'algorithme générique mise en œuvre pour le filtrage des paquets se décompose comme suit :

1- Les critères de filtrage doivent être définies, ils sont appelés les règles de filtrage de paquet ; (cible
2- Lorsque un paquet arrive sur un port, ses entêtes (IP, ICMP, IGMP, TCP, UDP) sont analysées ;
3- Les règles de filtrage de paquet sont appliquées dans un ordre précis ;
4- Si une règle bloque la transmission ou la réception d'un paquet, il est bloqué;
5- Si une règle autorise la transmission ou la réception d'un paquet, ou le paquet ne suit aucune règle, il passe.

4.3.2 HYPOTHESE

Le développement de notre Firewall repose sur deux suppositions :

- La première supposition concerne la technologie du réseau sur lequel notre Firewall doit opérer : il s'agit d'un réseau Ethernet. Cela semble être une supposition raisonnable vu qu'un grand pourcentage des réseaux reliés à Internet est de technologie Ethernet.
- La deuxième supposition suppose que le protocole utilisé par le réseau est TCP/IP, cela est motivé par le fait que d'une part : de plus en plus de réseaux sont connectés à Internet, donc utilisent le protocole TCP/IP, et d'autre part TCP/IP est aujourd'hui le protocole, de loin, le protocole le plus populaire.

4.3.3 ARCHITECTURE DE NOTRE FIREWALL :

Après avoir expliqué la fonction de base de sécurité de notre Firewall, nous présenterons dans ce qui suit les différents modules composant notre outil.

Ainsi notre Firewall est composé de cinq (5) modules. La figure suivante illustre l'architecture générale de Firewall.

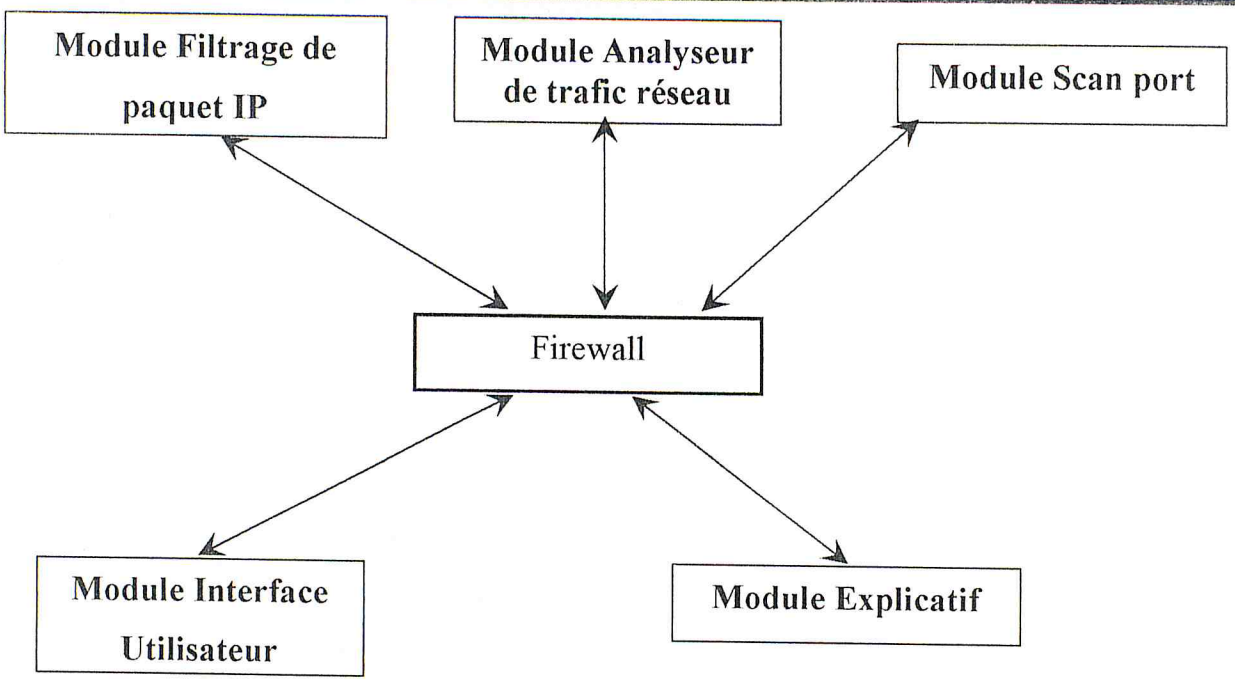


Figure 4.2 : Architecture de Firewall.

Les modules encadrés en bleu communiquent avec l'utilisateur, ceux qui sont encadrés en rouge communiquent avec le réseau.

Ainsi les différents modules de Firewall sont :

a. Module de filtrage des paquets IP

C'est le module de base de notre Firewall, il filtre les paquets IP selon les critères suivants :

- L'adresse IP source, IP destination (couche réseau) ;
- Port source, port destination (couche transport) ;
- Protocole utilisé (IP, ICMP, IGMP, TCP, UDP).

a.1 Type de connexions filtrées

Par le biais de ce module de filtrage on peut bien filtrer les connexions TCP, UDP, IP, ICMP et même les connexions IGMP. Le protocole ICMP se trouve au niveau de la couche IP, et si on bloque ce dernier nous sommes dans la possibilité de bloquer le ping venant d'hôtes internes ou externes.

a.2 Pourquoi bloquer les PING ?

Ping, qui veut dire Packet Internet Gopher, est une suite de paquets envoyés vers l'hôte distant pour le tester s'il est connecté au réseau ou non.Nous avons inclus dans ce module une partie pour le blocage de PING pour une sécurité optimale du serveur.

N'importe quel pirate ou Hacker averti commence toujours d'abord par voir si l'hôte qu'il veut attaquer est disponible sous le réseau ou connecté à Internet, pour qu'il puisse ensuite utiliser une méthode d'attaque. Nous savons cela à travers les discussions des pirates dans plusieurs forums de discussion sur le net.

Par conséquent, si on bloque les ping venant de l'exterieur du serveur, nous restons invisible d'une certaine maniere pour l'ensemble du réseau local et de l'Internet. Ainsi le pirate se dira peut-être qu'on n'est pas encore connecté à Internet, ce qui minimisera le risque d'attaque.

a.3 Invisibilité réseau

Pour améliorer l'invisibilité réseau, nous devons aussi de préférence bloquer le port du NetBios SMB et qui est le 139 en TCP, en plus du blocage du PING en ICMP, car c'est ce port qui est utilisé à mainte reprise dans le cas d'une recherche d'un hôte sur le réseau.

En appliquant ces deux méthodes, on est sûr que nous sommes invisible pour le reste du réseau entier, que ce soit pour ce qui est de l'interieur que de l'exterieur (Internet).

Cela réduira considérablement les attaques de hacker, car un hacker ne perdra jamais son temps à essayer de pirater une machine non connecté au réseau.

a.4 Bloquer tout le trafic réseau

Si la machine est soumise à un nombre important des attaques, l'administrateur doit bloquer immédiatement toutes les activités du réseau (trafic entrant et trafic sortant).

b. Module Analyseur de trafic réseau (sniffer)

C'est un analyseur réseau, il capte tout le trafic qui transite sur un réseau. Ce module fournit les informations suivantes :

- Le temps de réception ou d'émission de paquet ;
- L'adresse IP source ;
- L'adresse IP destination ;
- Port source ;
- Port destination ;
- Protocole.

Il fournit aussi la possibilité de filtrer le trafic dont le but d'indiquer seulement les caractéristiques des paquets contenant une donnée spécifique.

b.1 Types de connexions analysées

On peut analyser tout type de connexions (IP, ICMP, IGMP, GGP, TCP, UDP……).

c. Module Scan port

La communication entre les machines interconnectées ne peut dérouler qu'à travers les ports qui sont des portes logiques d'entrer à un ordinateur connecter au réseau.

On a conçu ce module dans le but de connaître quels sont les services ou bien les ports ouverts, ou bien autrement dit, savoir dans le cas d'attaque sur des ports non connus, quel port devrait-on vraiment verrouiller. En effet, grâce à ce module on peut à n'importe quel moment savoir quel sont les ports ouverts, dans le cas de protocole de communication TCP.

Etant donné que l'administrateur du serveur connaît les ports ou services étant autorisés à communiquer des données ou simplement des informations, grâce à ce module il aura la possibilité de savoir si un port ou un service a été ouvert illicitement par un utilisateur ou un hacker.

Le scan de ports ne concerne pas seulement la machine locale, on peut scanner les ports de n'importe quelle machine située dans le réseau.

c.1 La base de données de correspondance

Nous avons établi une base de données de correspondance qui fournit la liaison entre chaque numéro de ports et chaque nom de service.

En général chaque numéro de port correspond à un service bien particulier sur la machine, et ces ports concernent surtout les ports administrateur, c'est-à-dire de 0 à 1023.

Par conséquent, si on affiche qu'il y a ouverture d'un port, on sait directement quel est le service concerné qui est ouvert grâce à cette base de données.

c.2 Scan de tous les ports

Nous envisageons d'employer ce sous-module lors du premier démarrage de la machine. Cette opération nous permettra de savoir dès les premiers instants quels sont les ports à surveiller, ou bien à filtrer, autrement dit à verrouiller, en ayant connaissance sur des ports à laisser ouverts. Nous nous basons dans cette approche sur l'ouverture et le déclenchement d'interruption sur les sockets l'une après l'autre en commençant par le numéros de port 0 jusqu'à arriver à la socket concernant le port 65000.

c.3 Scan d'intervalle de ports

Nous avons conçu ce sous-module suivant un principe identique au module précédent. Mais cette fois ci, le travail à effectuer dans ce cas-la sera plus rapide et plus précis, car il y

aura un scan de juste une suite de ports bien définis basée sur une borne inférieure et une borne supérieure des ports, et non pas de 0 à 65000.

d. Module Interface utilisateur :

Il permet à l'utilisateur d'effectuer ses requêtes ainsi que les tests et saisir les informations nécessaires (adresses IP et ports à tester, ...) et d'afficher les résultats des tests.

e. Module explicatif

Il est chargé de fournir des explications à l'utilisateur concernant les tests et les méthodes utilisées pour le blocage et l'autorisation des paquets IP, ainsi que le fonctionnement du Firewall.

La figure suivante illustre l'intéraction entre les différents modules.

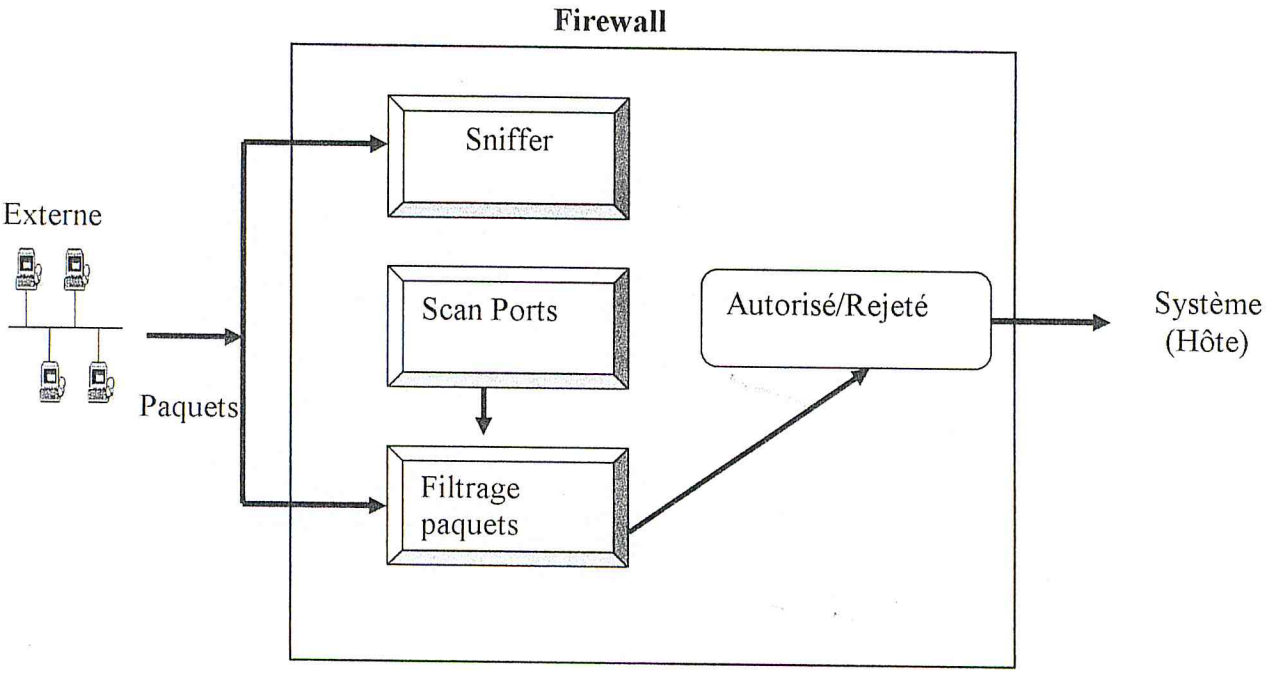


Figure4.3 : Schéma synoptique général de l'application.

4.4 IMPLEMENTATION DES DIFFERENTS MODULES

4.4.1 OUTILS DE DEVELOPEMENT :

Pour implémenter notre Firewall, on a opté pour l'environnement Windows (Windows NT4.0/2003 server.....) qui est largement répandu dans les administrations et les différentes organisations et même les librairies utilisées dans le filtrage de paquets et dans l'analyse du réseau ne supporte que la technologie NT (Network Technologie) qui fournit de nombreux moyen pour la gestion de réseau. Dans ce qui suit nous argumenterons le choix du langage Visual Studio.Net comme outils de développement.

CHOIX DU LANGUARE VISUAL STUDIO.NET

Le choix porté sur le langage Visual Studio.Net est dû aux avantages offerts par Visual Studio.Net:

- IDE (Integrated Development Environment ou environnement de développement intégré) commun à tous les langages et intégre directement les outils. Ainsi que l'on développe en C #, en J#, en VB.Net, l'environnement reste le meme.
- La vitesse et la convivialité d'un environnement de développement visuel.

Par la suite nous allons expliqué l'implémentation de chaque module définit précédemment.

4.4.2 Module Filtrage des paquets IP

Il filtre les paquets IP par l'analyse des en-tête (IP, ICMP, IGMP, TCP, UDP), la capture de ces paquets du réseau est une opération de bas niveau qui permet d'intercepter les paquets directement de la carte réseau, Le développement de ce module nécessite la programmation d'une DLL (Dynamic Link Library) COM (Component Object Model) qui est nommée **'PFE_FIREWALL_LIB'**.

a. Definition de PFE_FIREWALL_LIB

PFE_FIREWALL_LIB est une librairie de liaison dynamique, permet de filtrer le trafic réseau entrant et sortant selon les filtres définis par l'utilisateur.

b. Conditions système et logiciels pour utiliser 'PFE_FIREWALL_LIB'

- Tout système d'exploitation supporte la technologie NT.
- PFE_FIREWALL_LIB.dll installée sur la machine.

La figure suivante illustre le niveau de filtrage effectué par la DLL **'PFE_FIREWALL_LIB'** :

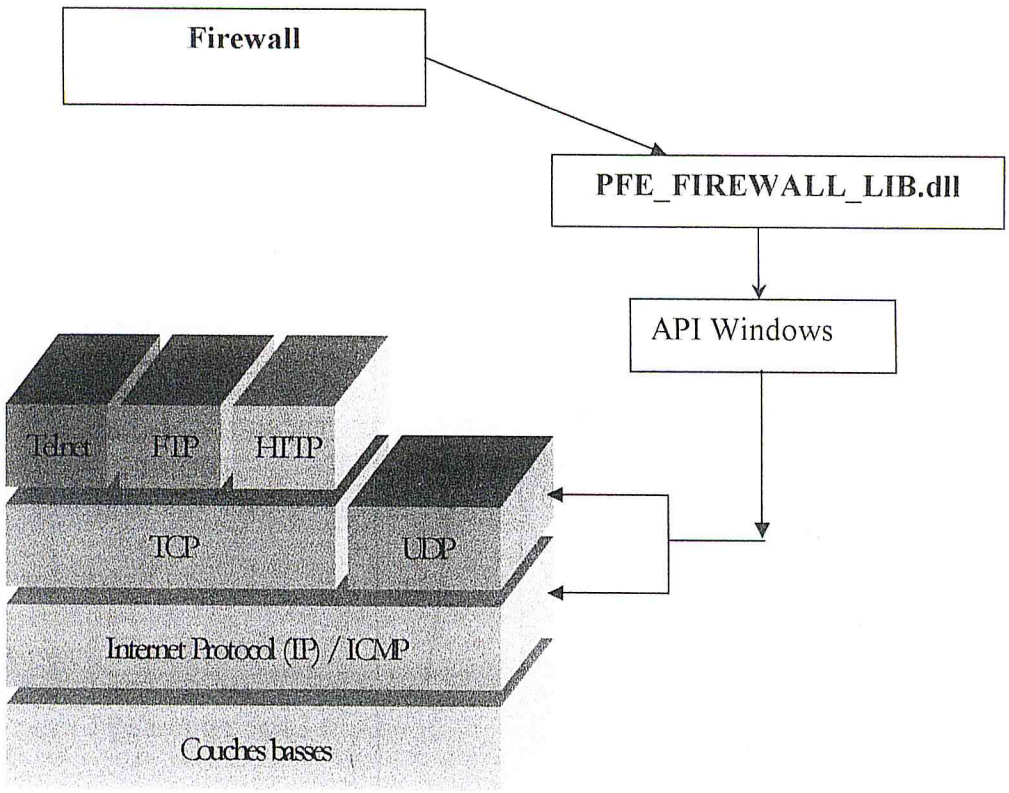


Figure4.4 : Niveau de filtrage

c. API (Interface de Programmation d'Application) Windows

Ensemble de routines qu'une application utilise pour demander et traiter des services de bas niveau effectués par le système d'exploitation d'un ordinateur. En règle générale, ces routines exécutent les tâches de maintenance, telles que la gestion des fichiers et l'affichage des informations.

d.Service Windows

Les services de Microsoft Windows, autrefois connus sous le nom de services de NT, permettent de créer des applications exécutables qui fonctionnent en leurs propres sessions de Windows. Ces services peuvent être automatiquement lancés lors de démarrage de la machine.

Dans notre application, il existe deux classes principales qui sont:

CFirewall : C'est une classe qui possède plusieurs fonctions et une donnée membres.

TDriver : C'est une classe secondaire qui contient un ensemble de fonctions membres utilisées par la classe CFirewall.

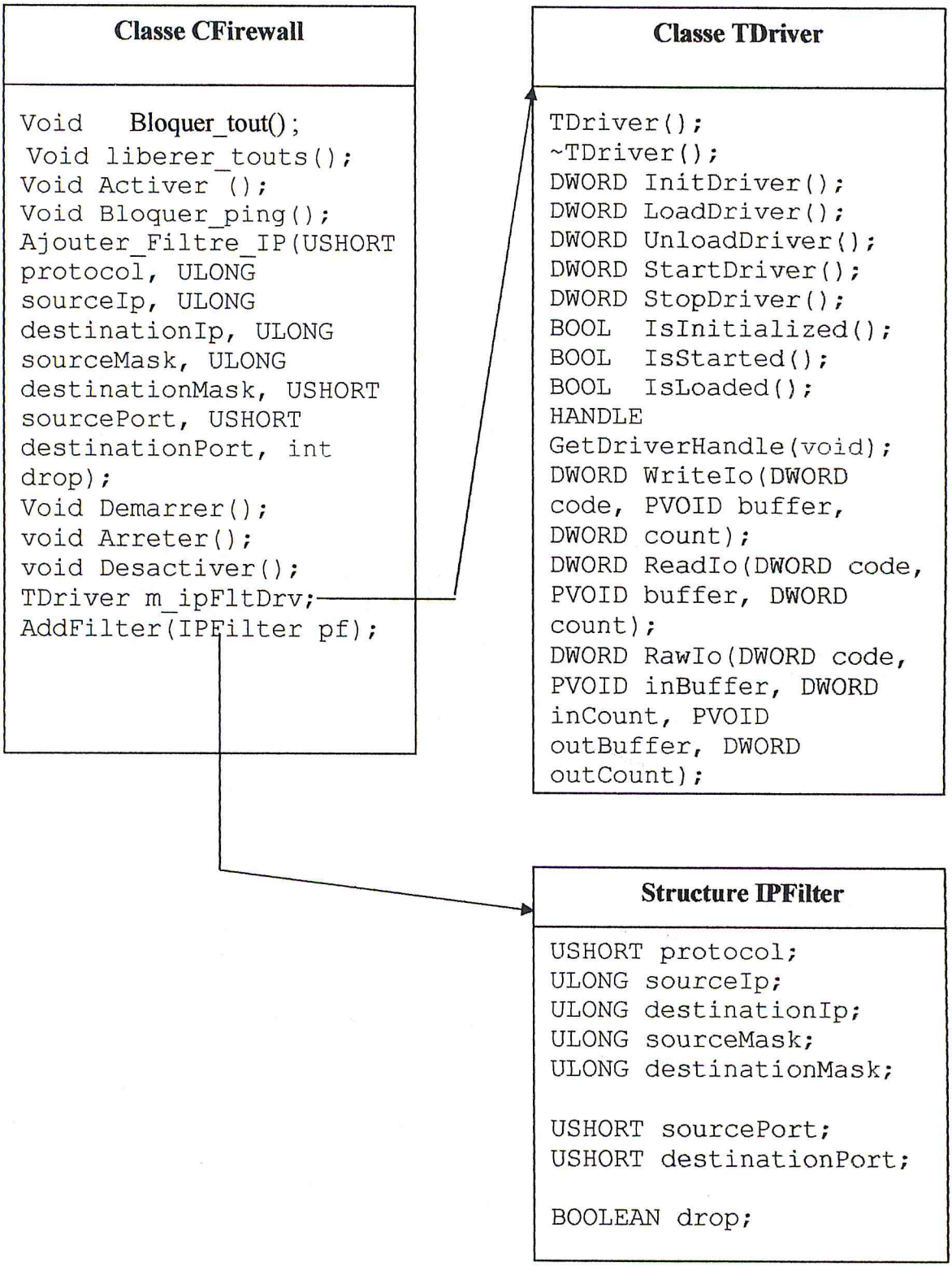


Figure 4.5 : Les différentes classes de application.

Le schéma suivant explique les liens entre les différentes classes décrites précédemment :

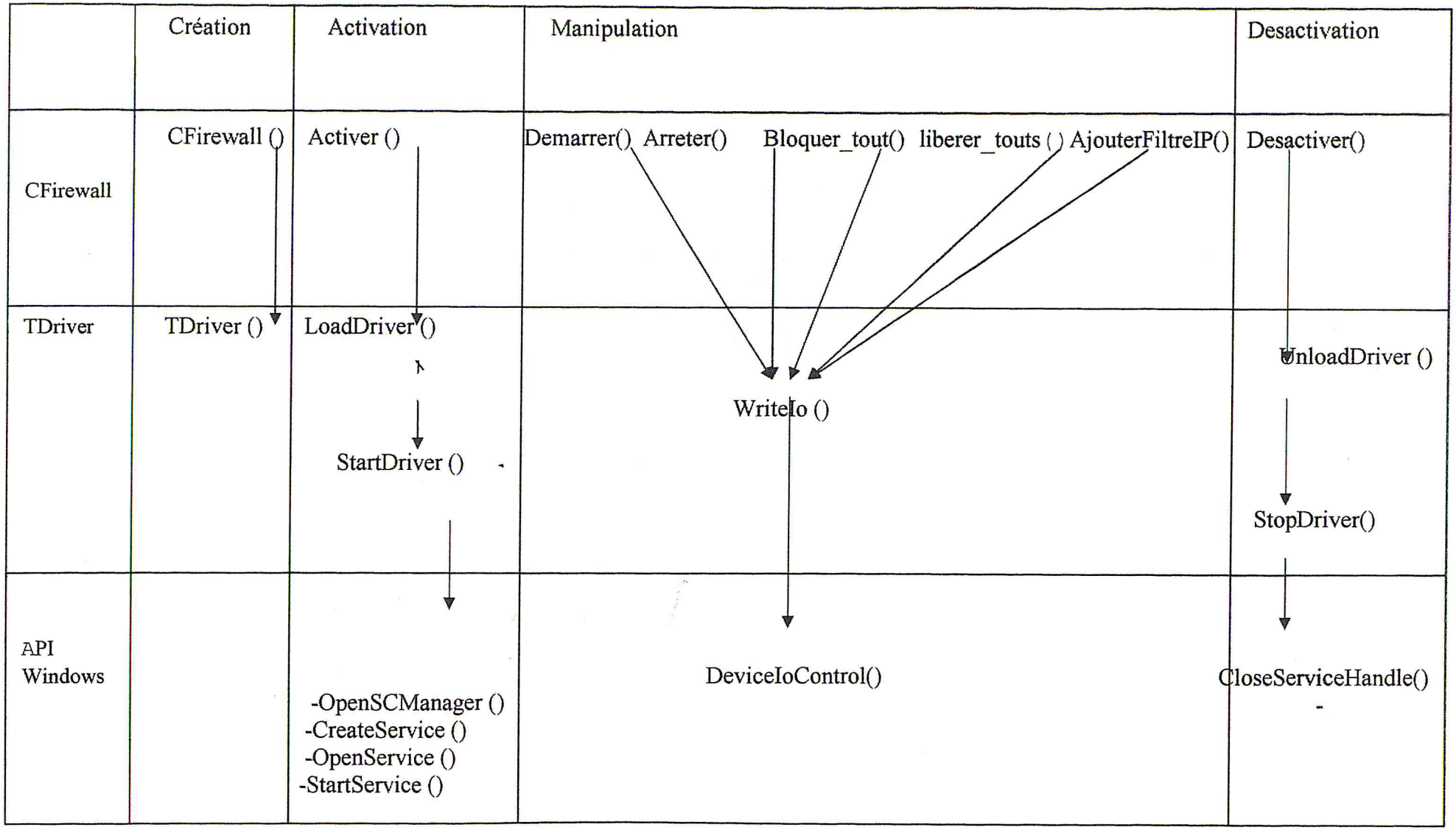


Tableau 4.1 : Les relations entre les classes.

e. Les Méthodes de CFirewall

Les méthodes sont :

1- La methode Activer () : elle permet de créer un service windows pour gérer le trafic réseau, ce service reste inactif jusqu'à l'appel de la méthode Demarrer (). Elle doit etre appelée avant n'importe quelle autre methode.

2- La methode Demarrer () : elle permet de lancer le fonctionnement du service créer.

3- La methode Arreter () : Elle permet de suspendre le fonctionnement de service.

4- La méthode Bloquer_tout () : elle permet d'informer le service pour bloquer tout le trafic réseau

5- La méthode Liberer_tout () : elle permet d'informer le service pour liberer tout le trafic réseau.

6- Ajouter_Filtre_IP () : elle permet d'ajouter une règle de filtrage.

7- Bloquer_Ping () : elle permet d'ajouter une regle de filtrage qui bloque le Ping.

8- Desactiver () : elle permet d'arreter le service.

f. Algorithme de la méthode créer ()

Etape1 : Créer un service en utilisant la methode créer () ;

Etape2 : Si la création du service est avec succés

Alors on peut appeler toutes les autres méthodes ;

Etape3 : activer le service pour que la méthode appelée soit fonctionnelle.

```
class  CFireWall :

{
public:
      CFireWall()
      {
      }



public:

      TDriver m_ipFltDrv;

      STDMETHOD(Bloquer_tout)(void);

      DWORD AddFilter(IPFilter  pf);

      STDMETHOD(Ajouter_Filtre_IP)(USHORT protocol,ULONG sourceIp,
......, USHORT destinationPort, int drop);
      .....
      STDMETHOD(Desactiver)(void);

}
```

g. Les Fonctions de la classe TDriver

1- LoadDriver () : Elle fait appel à des API Windows qui sont

1.1 OpenSCManager : Elle renvoie un pointeur sur la liste des services.

1.2 CreateService : Elle crée un service qui doit être relie avec son fichier pilote et ajouter le au gestionnaire de service.

1.3 OpenService : Obtenir un pointeur sur le service crée à partir de son nom.

1.4 StartService : Démarrer le service crée.

2- UnloadDriver () : Elle permet de détruire le service en utilisant l'API CloseServiceHandle.

3- WriteIo () : Chaque fonction (Demarrer(), Arreter(), ...) est représentée par une règle ajoutée au fichier pilote de service à l'aide de l'API Windows DeviceIoControl().

```
class TDriver

{
public:

      TDriver(void);          //constructeur
      ~TDriver(void);         //destructeur

      ..........................................................
      DWORD InitDriver(LPCTSTR name, LPCTSTR path, LPCTSTR .....);

      DWORD InitDriver(LPCTSTR path);
      ..........................................................
      DWORD LoadDriver(LPCTSTR path, BOOL start=TRUE);
      ..........................................................

      void SetRemovable(BOOL value);
      BOOL IsInitialized();
      HANDLE GetDriverHandle(void);

}
```

h. Structure IPFilter

Elle représente la règle de filtrage définie par l'utilisateur.

4.4.3 Module Sniffer

L'implémentation de ce module a imposé l'utilisation d'une dll de bas niveau qui est SocketView.dll.

a. Définition

SocketView est une dll qui permet à des développeurs de filtrer d'une manière transparente des paquets de n'importe quel centre serveur sur un réseau (pas seulement le centre serveur locale), avec l'impact minimal sur l'activité de réseau. Elle peut indiquer toutes les informations conçernant les paquets IP qui transitent le réseau (adresse IP source, adresse IP destination, port source, port destination, protocole utilisé, la donnée transportée).

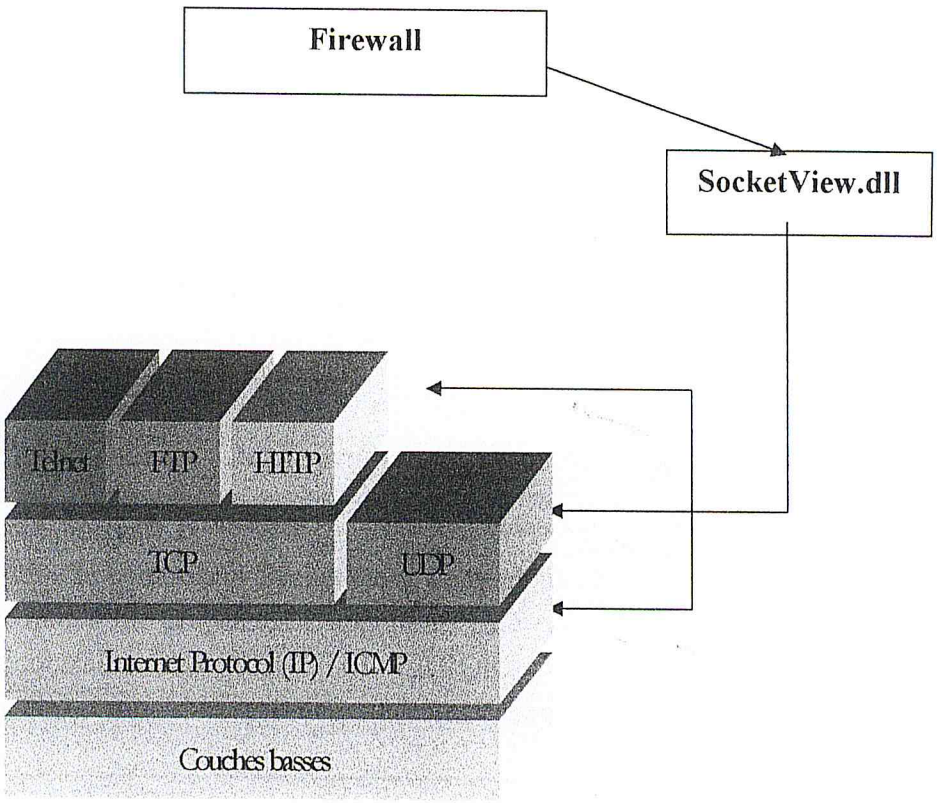


Figure 4.6: Niveau de fonctionnement de SocketView.

b. Conditions système et logiciels pour utiliser SocketView

Pour utiliser SocketView il faut avoir :

- Système d'exploitation Windows 2000, Windows XP, ... (Technologie NT) ;
- Au minimum WinSock2 correctement installé et configuré;
- L'utilisateur doit être un administrateur ;

- SockView.dll installée sur la machine.

c. Les classes

TSockView : c'est la classe principale qui fait l'instanciation et la liaison de SockView.dll.

d. Propriétés, événement et méthode de SocketView

Toutes les propriétés, les méthodes et événements sont énumérées dans le tableau suivant :

Propriétés	Evénements	Méthodes
• BufferItems • FilterMode • IsActive • IsSniffing • Port • IPAddress • LastSockErr • SniffType • IsAdmin • FilterRecCount • LocalHostIPAliases	• DataArrival	• Activate • StartSniff • StopSniff • GetErrorDescription • AddFilterRec • HostRangeClear • DeleteFilterRec • HostRangeSet

Tableau 4.2: propriétés et méthodes de SocketView.

d.1 La méthode Activate ()

Elle active le composant SocketView, cette méthode doit être appelée avant que toutes les autres méthodes ou propriétés s'appellent. Elle peut être échoué avec n'importe quel valeur de la constante SBK_GENERAL_ERRORS (échec d'allocation mémoire, système d'exploitation non compatible, privilèges administrateur).

Valeur	Constante
-2	SBK_ERROR_PLATFORME_VER
-3	SBK_ERROR_MEMALLOC_FAILURE
-6	SBK_ERROR_NO_ADMIN_PRIVILEGE

d.2 La propriété IsActive

Indique si la méthode de déclenchement s'est appelée avec succès.

Algorithme de la méthode Activate ()

Etape 1 : Activer le composant SocketView en utilisant la méthode Activate ;

Etape2 : *Si* la propriété IsActive égale à *true*

Alors autoriser l'utilisation de toutes les autres méthodes, propriétés et

Evènnement ;

Sinon une erreur est générée par la constante SBK_GENERAL_ERRORS.

d.3 La Méthode StartSniff ()

Cette méthode permet de démarrer le sniffing selon les critéres choisies.

d.4 La Méthode StopSniff

Elle permet d'arreter le sniffing et fournir les résultats.

d.5 La propriété Is Sniffing

Indique si la méthode de StartSniff s'est appelée avec succès.

d.6 La méthode AddFilterRec :

Elle permet d'enregistrer un filtre (donnée, adresse IP source, adresse IP destination, port source, port destination, protocole).

Algorithme de l'analyse

*S'*il n'existe aucun filtre;

Alors tout le trafic réseau est analysé;

Sinon seulement les paquets IP qui correspondent aux critères indiqués lors le 'enregistrement de filtre.

d.7 L'événement DataArrival

Elle est déclenchée dés que la donnée demandée dans n'importe quel filtre est trouvée.

Algorithme de l'évènement

Pour chaque paquet IP

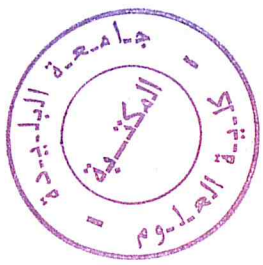
Faire

Analyser en-tete (IP, TCP, UDP) et donnée

*S'*il existe un filtre qui correspond aux caractéristiques du paquet

Alors l'évenement DataArrival est déclenchée

Fait;



```
Private  DataArrival( ref Object Data  ,  int TTL  ,int Proto,.....)
{
                string sData="" ;
                CPacket objPacket=new CPacket() ;

                ..........................................................
                if( gobjPackets.Count >= 40 )
                      {
                            gobjPackets.Remove(gobjPackets.Count);

                      //enregistrer les données
                      objPacket.DestIP = DestIP;
                      objPacket.DestPort = DestPort;
                      objPacket.Proto = Proto;
                      objPacket.SourceIP = SrcIP;
                      objPacket.SourcePort = SrcPort;
                      objPacket.TTL = TTL;

                      ..........................................................


}
```

Pour bien exploiter les methodes, évenementds et propriétés précédemment décrites, nous avons implémenté la classe **CPacket** qui représente les paquets à analyser.

```
class CPacket
      {
            public int TTL ;
            public int Proto ;
            ..........................
            ..........................

            private Byte[] mbytPacketData;

            public  Object  PacketData
            {
                  get
                  {
                        return Support.CopyArray(mbytPacketData);
                  }
                  ..........................................................
            }

            ..........................
      }
```

4.4.4 Module Scan Port

Ce module permet d'effectuer un scan sur une suite de ports bien définis basée sur une borne inférieure et une borne supérieur des ports de 0 à 65000. Le principe est d'envoyer une socket pour chaque port, si la socket est valide alors le port concerné est ouvert.

Pour implémenter ce module nous avons utilisé les classes suivantes :

a. IPAddress

Contient l'adresse IP d'un ordinateur sur un réseau, elle dispose d'un ensemble de méthodes et propriétés qui permettent de manipuler cette adresse.

b. IPEndPoint

Elle forme un point de raccordement à un service en combinant l'adresse IP et le numéro de port de service.

c. Socket

Elle fournit un ensemble riche de méthodes et de propriétés pour des communications de réseau. La classe Socket permet d'exécuter le transfert synchrone et asynchrone de données en utilisant n'importe lequel de protocole de communication.

```
bool connect;
                IPAddress ip=IPAddress.Parse(textBox1.Text);
                for(int i=min; i<= max;i++)
                {
                      IPEndPoint ipe = new IPEndPoint(ip, i);
                      Socket tmpS = new
                      ..........
                      connect=false;
                      try
                      {
                       .....
                      }
                      catch
                      {
                      .....
                      }
                      if(connect)
                      {
                            tmpS.Close();
                       }
                }
```

4.4.5 Module interface utilisateur

L'interface principale de Firewall réalisé représente la fonction de base de ce dernier qui est le contrôle d'accès en fonction des règles définies par l'utilisateur.

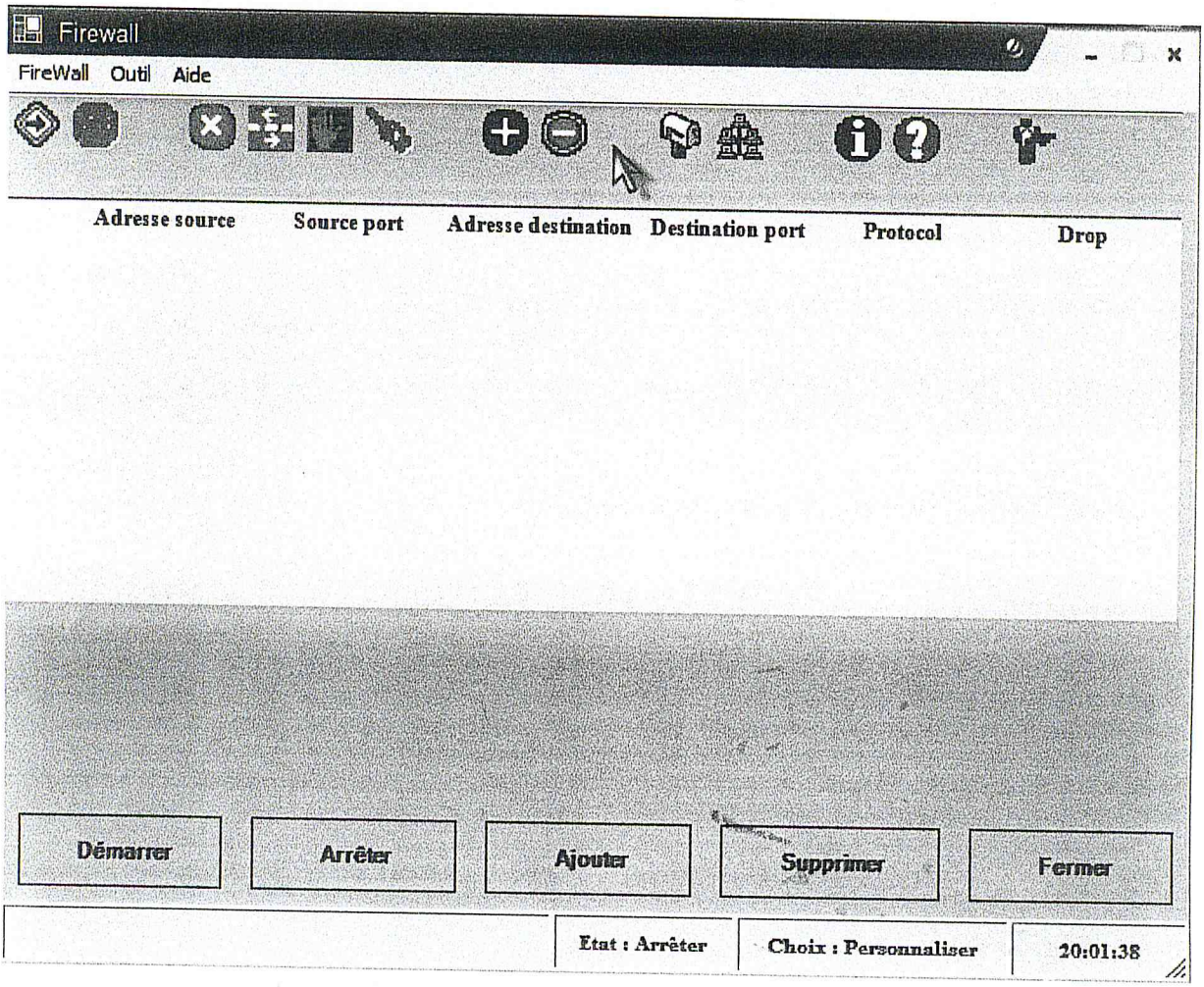


Figure 4.7 : L'interface principale

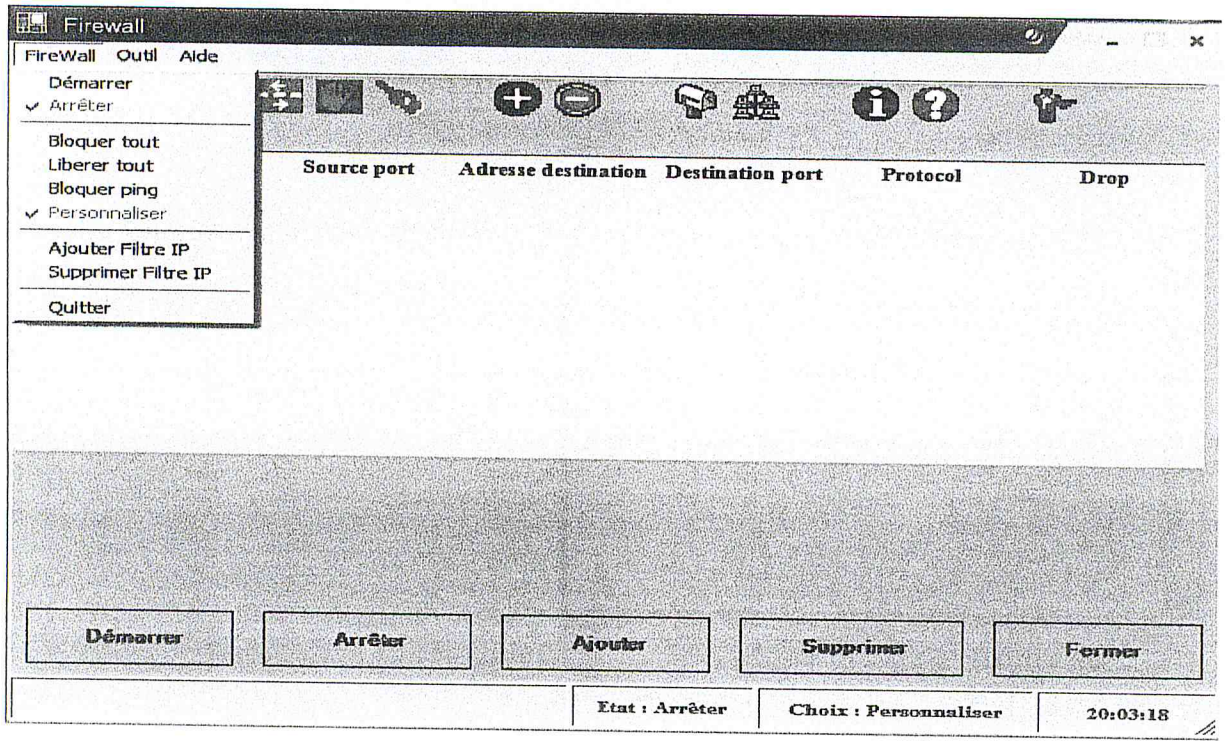


Figure 4.8 : Le menu Firewall.

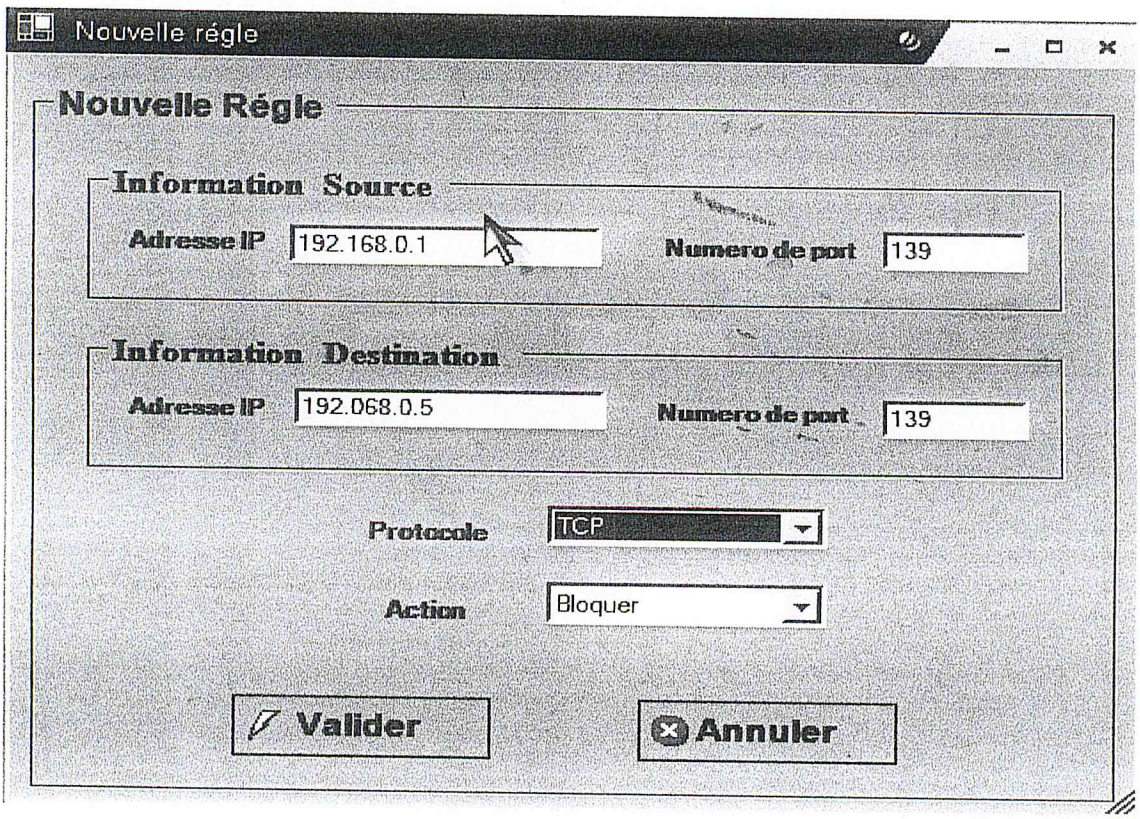


Figure 4.9 :l'interface d'ajout de regles de filtrage

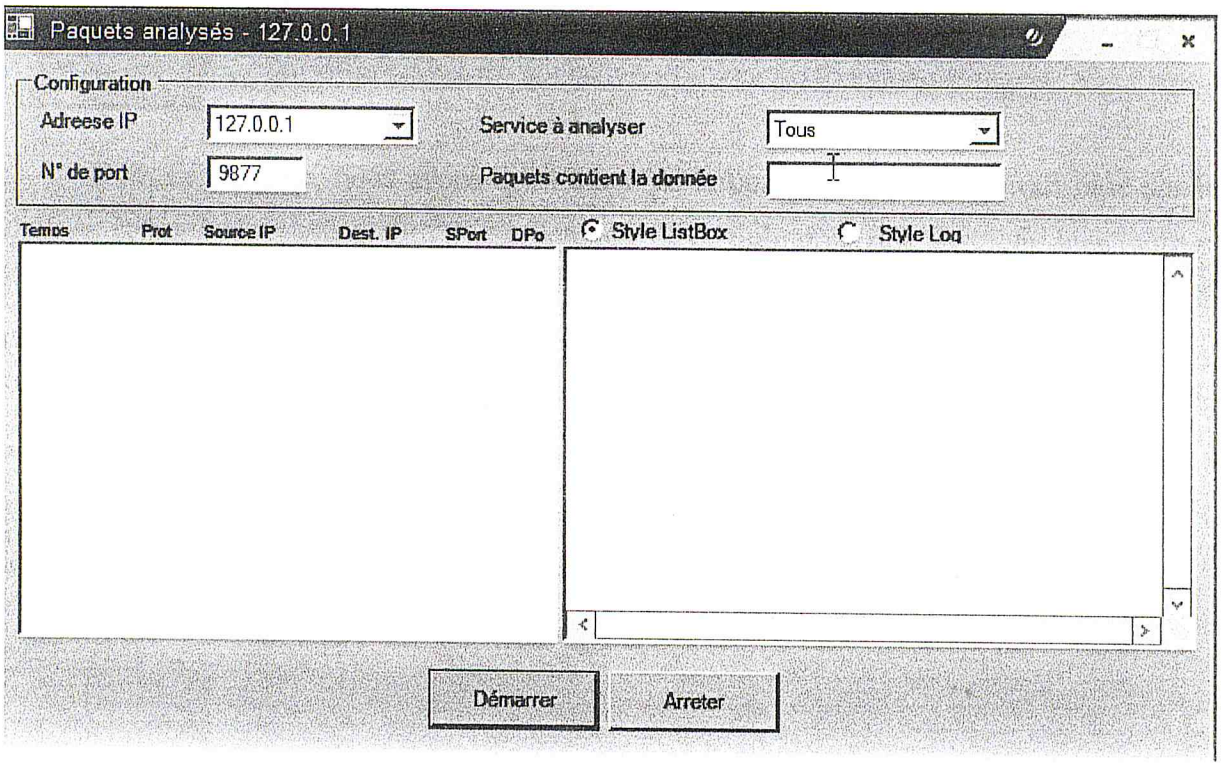


Figure 4.10 :L'interface d'analyseur de trafic réseau (snifer).

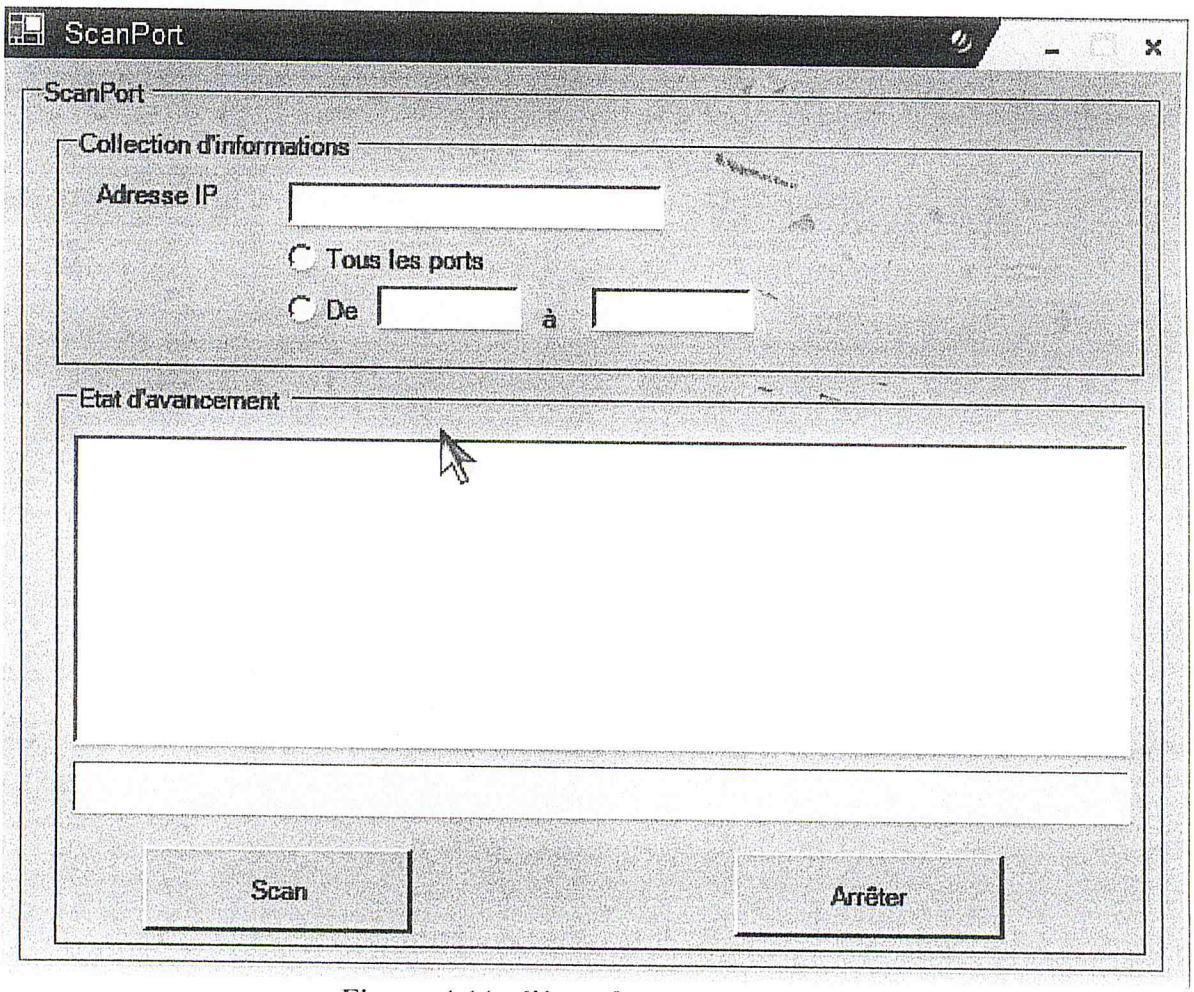


Figure 4.11 : l'interface de scan port.

4.5 Conclusion

Dans ce chapitre, nous avons fait l'étude de la conception d'un Firewall basé sur le filtrage statique de paquets IP. Il est doté de deux utilitaires qui sont : le scan port et l'analyseur de trafic réseau. Dans le prochain chapitre nous allons tester le fonctionnement de notre Firewall par la simulation d'une attaque à base de cheval de troie.

CHAPITRE V

Test par Simulation d'attaque

5. Introduction

Dans ce chapitre nous allons tester le Firewall réalisé en simulant une attaque de Cheval de Troie. Le choix porté sur ce type d'attaque est dû à son utilisation fréquente par les hackers. Les chevaux de Troie les plus connus sont :

- Back Orifice DLL Comm ;
- Back Door ;
- Spy Sender ;
- WinCrash ;
- Sockets de Trois v1 ;
- Sub Seven ;
- Sygate Back Door ;
- Back Orifice/ Bo-2K ;
- Back Orifice 2000.

Notre test sera effectué avec le cheval de Troie « Sub Seven1.9 ».

5.2 Définition de " Sub Seven "

" **Sub Seven** " est une **application client/serveur** qui permet au logiciel client de surveiller, administrer, et effectuer à distance n'importe quelle action (réseau, multimédia, redémarrage, fichiers,...) sur la machine exécutant le serveur.

5.3 Composition de Sub Seven

SUBSEVEN 1.9 est composé de 3 programmes : le client, le serveur et l'éditeur de server. Le client est celui que l'on utilise depuis la machine de pirate pour envoyer et recevoir les infos du serveur. Le serveur (server.exe) est le fichier qui ouvre le port (1243). L'éditeur de server (editserver.exe) permet de configurer le serveur selon les besoins de pirate.

5.4 Installation de Sub Seven

5.4.1 Installation de Sub Seven serveur

Il suffit d'exécuter le fichier exécutable SERVER.EXE. C'est ce programme qui va ouvrir un port (1243) sur la machine victime, il ouvre un port spécifique qui n'est pas le même avec tous les autres chevaux de Troie.

L'analyse approfondie du module exécutable *SERVER.EXE* a donné les résultats suivants :

Sub Seven fait appel à des **API très importantes** de Windows. Par exemple on dénote :

- accès et modification de la BDR (Base de Registre)
- gestion de processus
- gestion réseau
- terminaison de Windows

5.4.2 Configuration de serveur

Tout ce que vous pourrez faire (ou ne pas faire) dépend entièrement des caractéristiques affectées au serveur.

a.PORT

C'est le port que le serveur ouvrira pour permettre de connecter à la victime. Le port par defaut est 1243. Ce port fonctionne très bien. On peut choisir un autre entre 1 et 65536. Si on choisit un port déjà utilisé par une autre application, on crée un conflit et le serveur ne sera pas opérationnel.

b. Mot de passe (PASSWORD)

On choisit un mot de passe (cela évitera de faire piquer les victimes par d'autres personnes).

c. Le nom de la victime (VICTIM NAME)

Ce nom permet de rappeler qui est la victime.

d. Melt, Wait for Reboot, Server Name

" Melt server after installation " permet au serveur de s'installer dans Windows puis de s'effacer. Ainsi, le fichier téléchargé par la victime disparaît. Cette fonction est à proscrire. Elle crée un doute - un fichier qui disparaît,

" Wait for Reboot " est par contre très intéressant. Lorsque la victime clique sur le serveur, celui ci s'installe mais ne s'inscris pas dans la bas de registre .Donc, si la victime est méfiante, elle va vérifiée sa base de registre. Grâce à cette option, la victime ne verra pas les modifications effectuées par le serveur car elles se feront au prochain redémarrage de windows.

" Server name " est le nom du fichier qui se copiera dans C:/Windows/system.

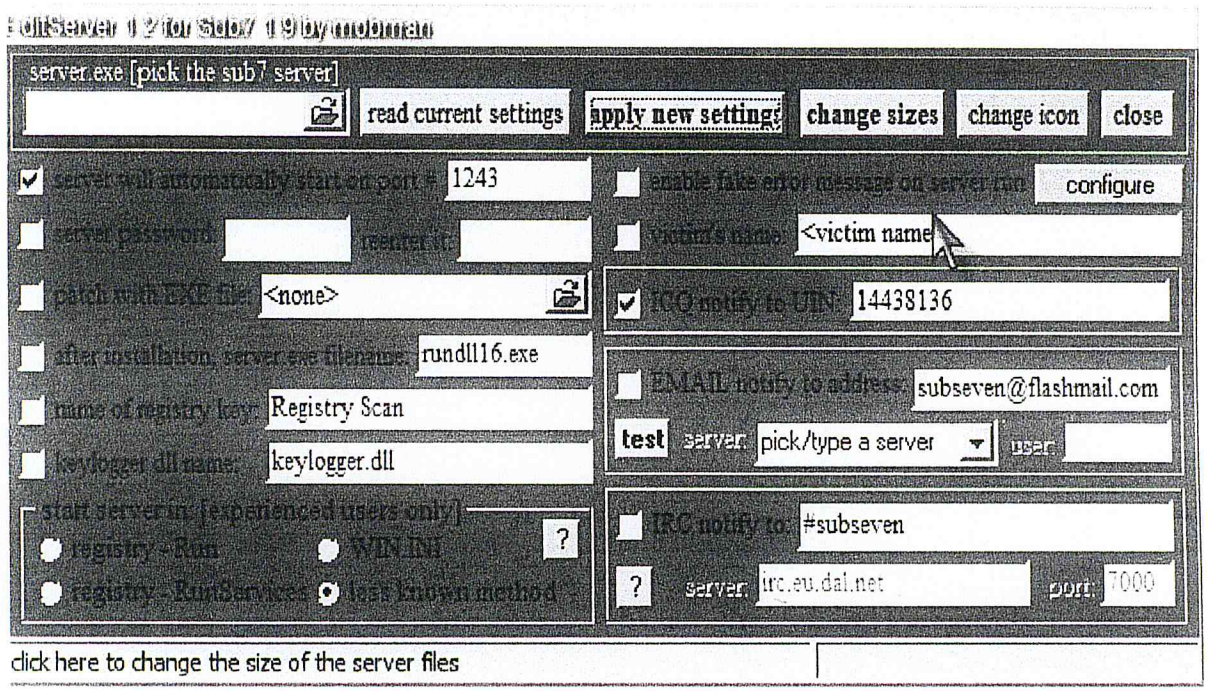


Figure 5.1 : L'interface de Editserver.

5.4.3 Installation de SUBSEVEN Client

Il suffit d'exécuter (sous Windows) le programme SUBSEVEN.*EXE*. Elle sert à se connectera l'ordinateur infecté. Elle se présente sous la forme de panneau de contrôle d'où l'on peut faire ce que l'on veut avec le pc cible comme démarrer des programmes, supprimer/ajouter des fichiers, afficher des images, rebooter la bécane contrôler la souris .....

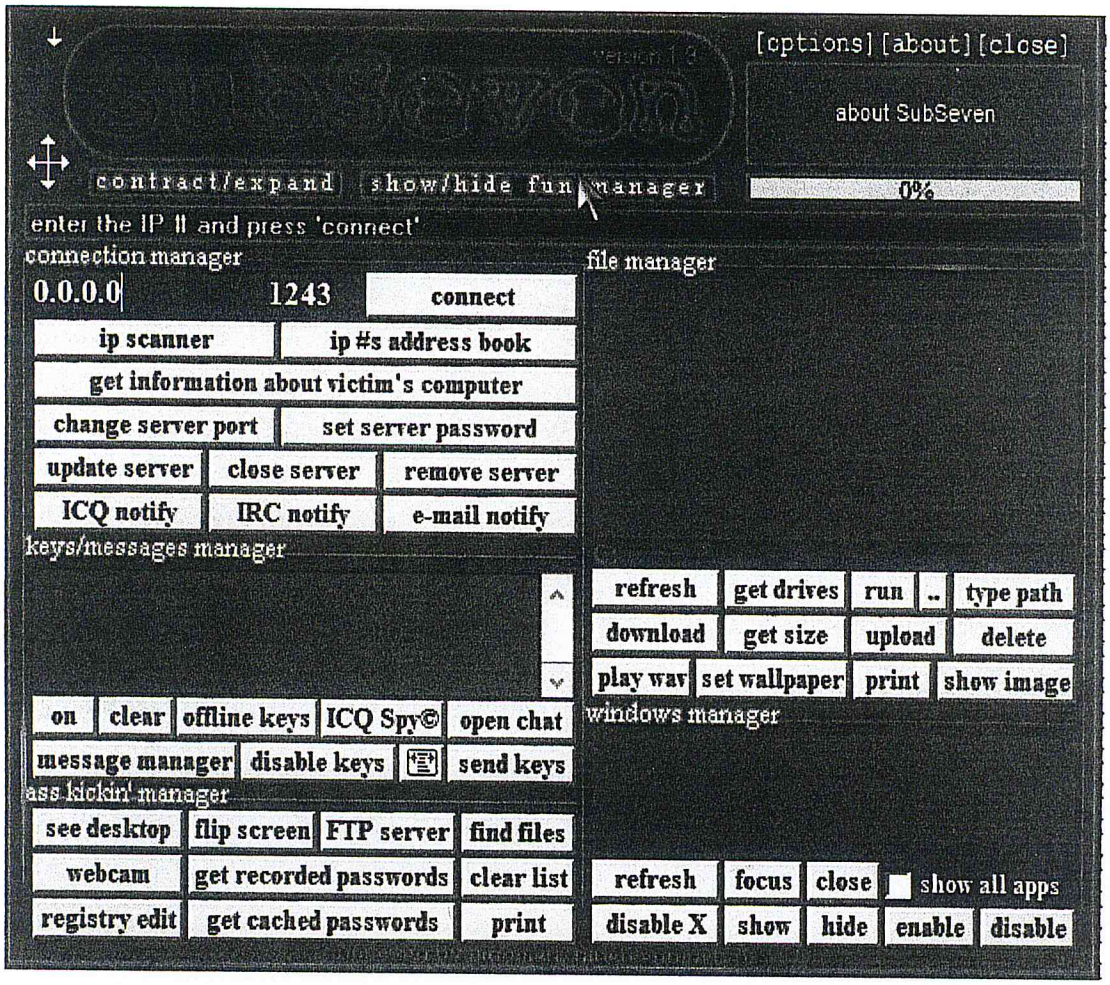


Figure 5.2 : L'interface de SubSeven1.9.

Les autres commandes existantes sont :

- transfert de fichiers via FTP
- arrêt puis redémarrage de Windows
- exécution d'un programme
- création / suppression de répertoires
- copie / suppression de fichiers
- compression / décompression de fichiers
- opérations "multimédia" (exécution d'un fichier son, clip vidéo,..)
- connexion / déconnexion réseau (montage / démontage de ressources)

5.5 Conséquences

Elles sont évidentes : Si le serveur SubSeven a été introduit sur une station Windows 95/98 ou Windows NT dans un but mal intentionné, toute station dotée du client SubSeven

pourra **TOUT** faire à distance sur cette machine (suppression de fichier, capture de mot de passe, exécution de n'importe quel programme,...). Donc les conséquences peuvent être **très graves**!

5.6 Plates-formes des tests effectués ici

Plate-forme cliente

PC sous Windows XP Professionnel (Pentium VI 1.8 GHZ, 128 Mo de RAM).

Plate-forme serveur

PC sous Windows XP Professionnel (Pentium VI 1.8 GHZ, 128 Mo de RAM).

5.7 Plan de Test

Dans notre test nous avons procédé comme suit :

1. Effectuer un Ping .
2. Scanner les ports de la machine cible.
3. Exécution de SubSeven Client.
4. Effectuer un deuxième scan.
5. Exploitation de l'attaque.
6. Lancer le Firewall réalisé.
7. Lancer l'attaque une autre fois.
8. Scan de nouveau la machine cible.

1. Ping

Nous avons effectué un Ping pour tester l'existence de la machine victime sur le réseau.

2. Scan Port

Dans cette étape, nous avons utilisé l'utilitaire SuperScan3.0 pour voir les ports ouvert avant le lancement de l'attaque.

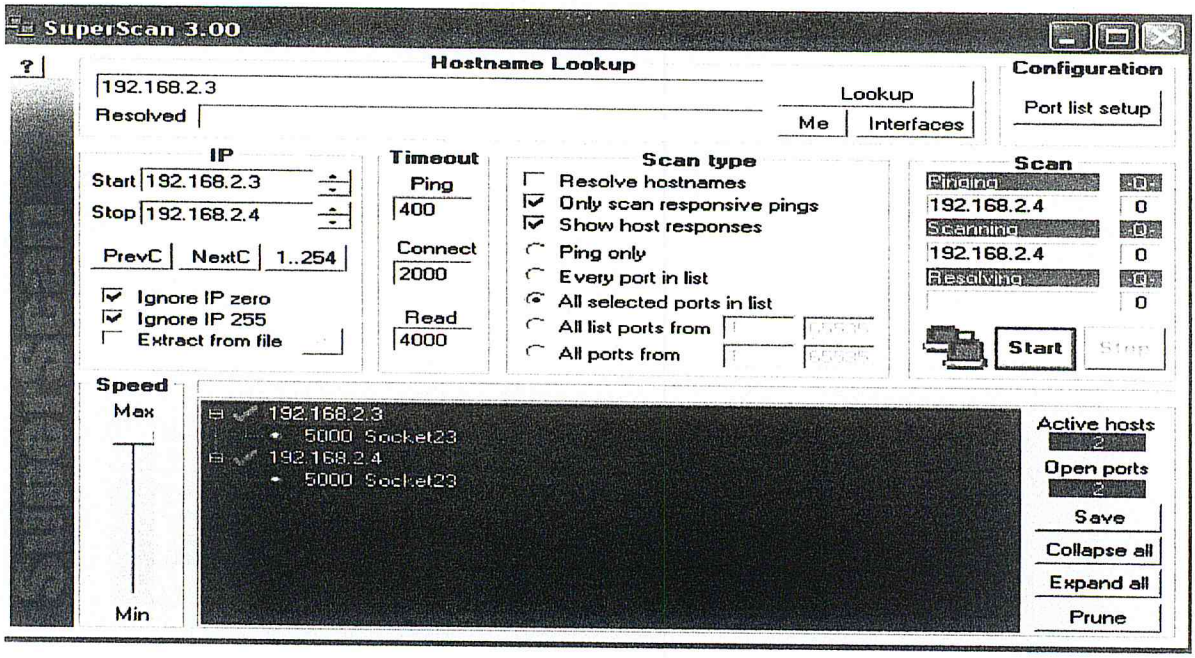


Figure 5.3: Les ports ouverts dans la machine cible.

3. Exécution de SubSeven Client

Dans cette étape, nous avons exécuté le fichier « SERVER.EXE » sur la machine victime.

4. Scan port

Lors de cette étape, nous avons effectué un deuxième Scan pour voir l'effet de « SERVER.EXE », il ouvre le port 1243 qui sera le point d'entrer dans la machine victime.

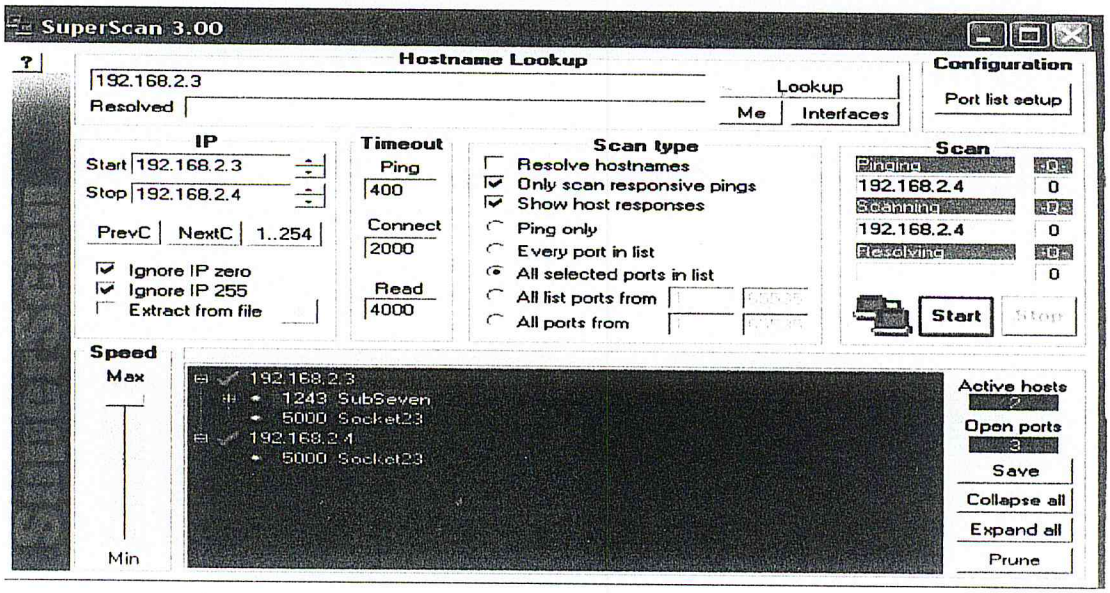


Figure 5.4: Ouverture de port 1243.

5. L'attaque

Dans cette etape, on execute le fichier « SubSeven.EXE ».

L'adresse IP de la machine victime Etablissement de connexion Port exploité

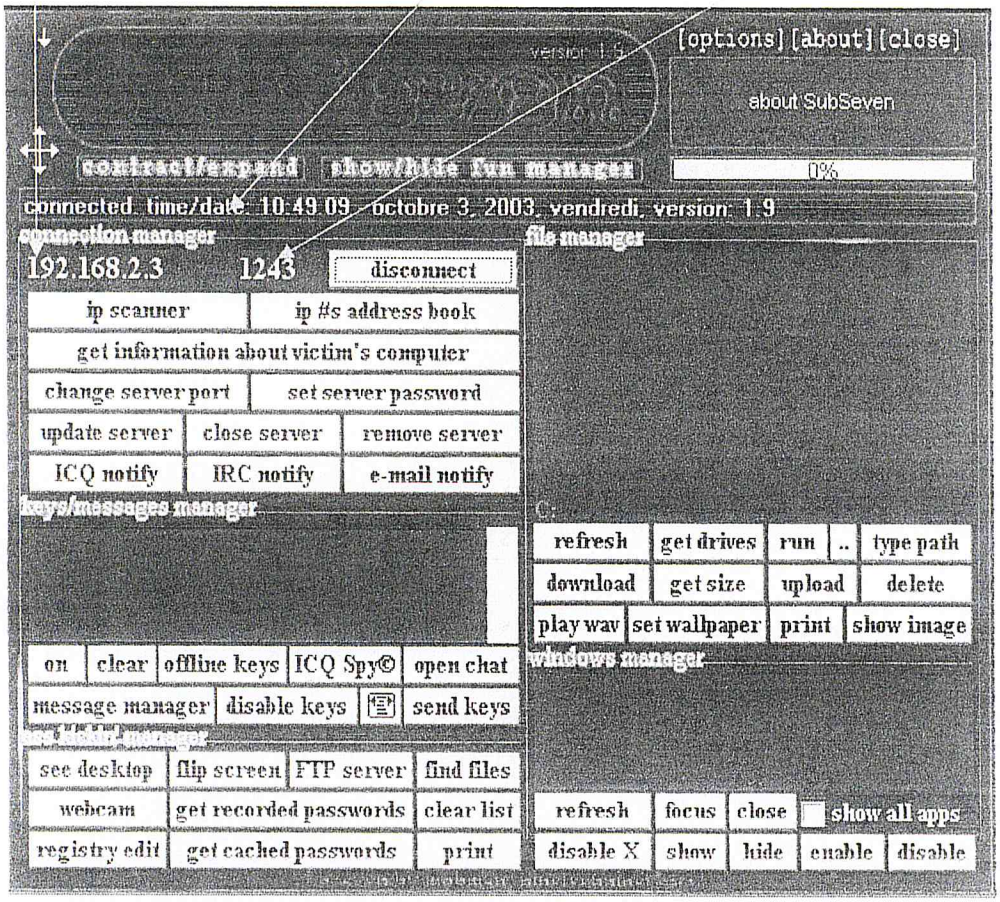


Figure 5.5: Etablissement de connexion.

Apres l'etablissement de connexion, nous avons lance quelques commandes a distance, par exemple :

1. Masquer/Afficher les icônes de Bureau comme c'est illustré dans la figure suivante

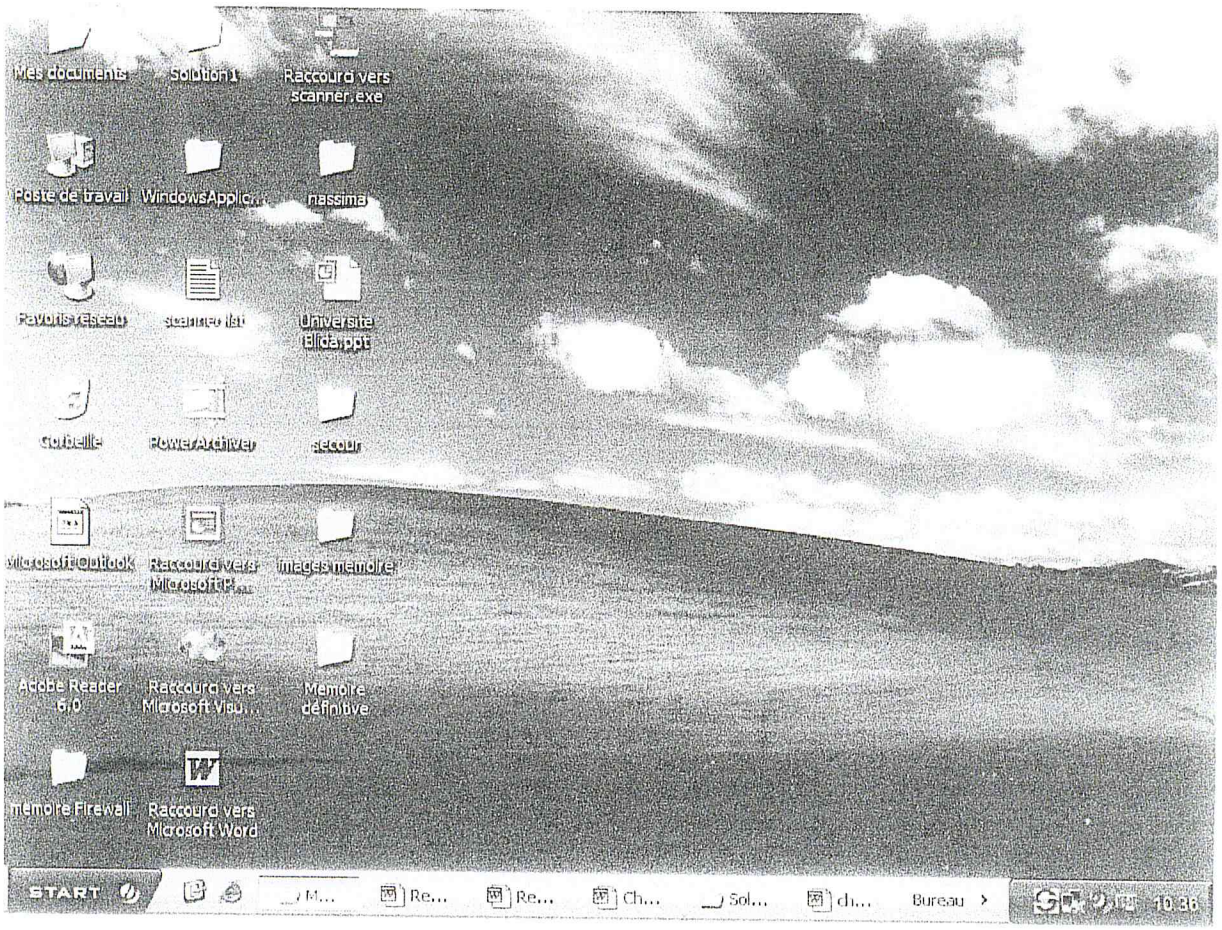


Figure 5.6 : Le bureau de la machine victime avant l'attaque.

Figure 5.7 : Disparition de bureau de la machine victime.

2. Changement /Restauration des couleurs de Windows.

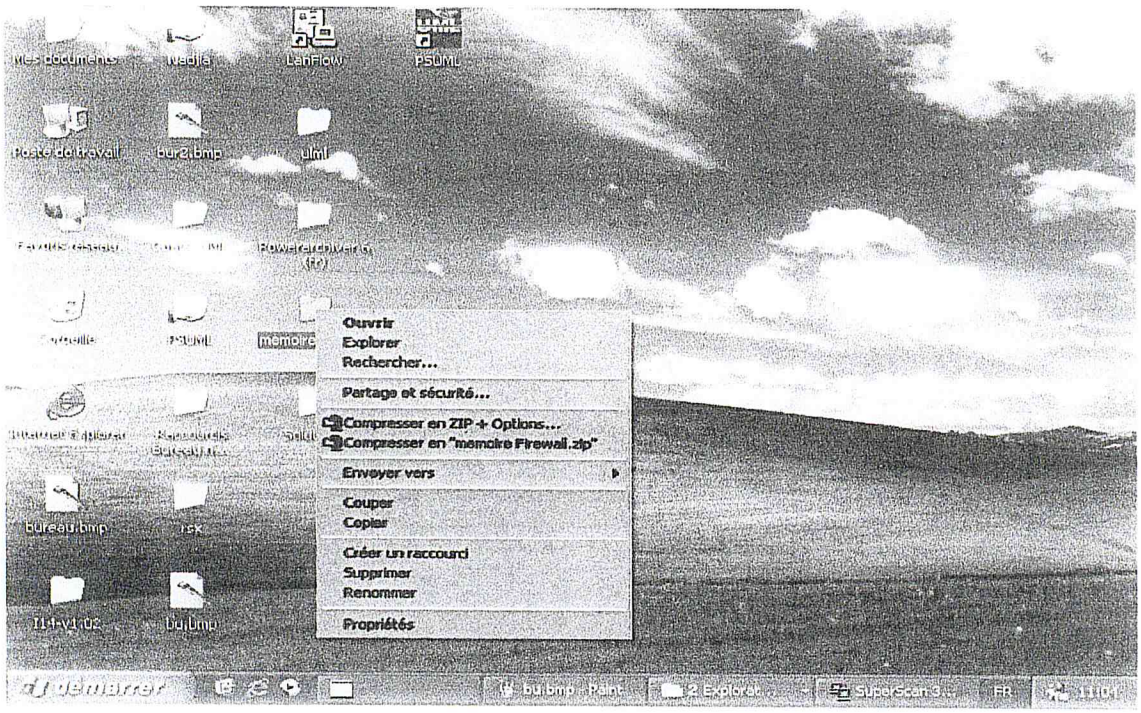


Figure 5.8: Changement des couleurs.

6. Installation de Firewall

Nous avons installé notre Firewall sur la machine victime, un pop menu apparaît dans la barre de tâche comme c'est illustré dans la figure suivante :

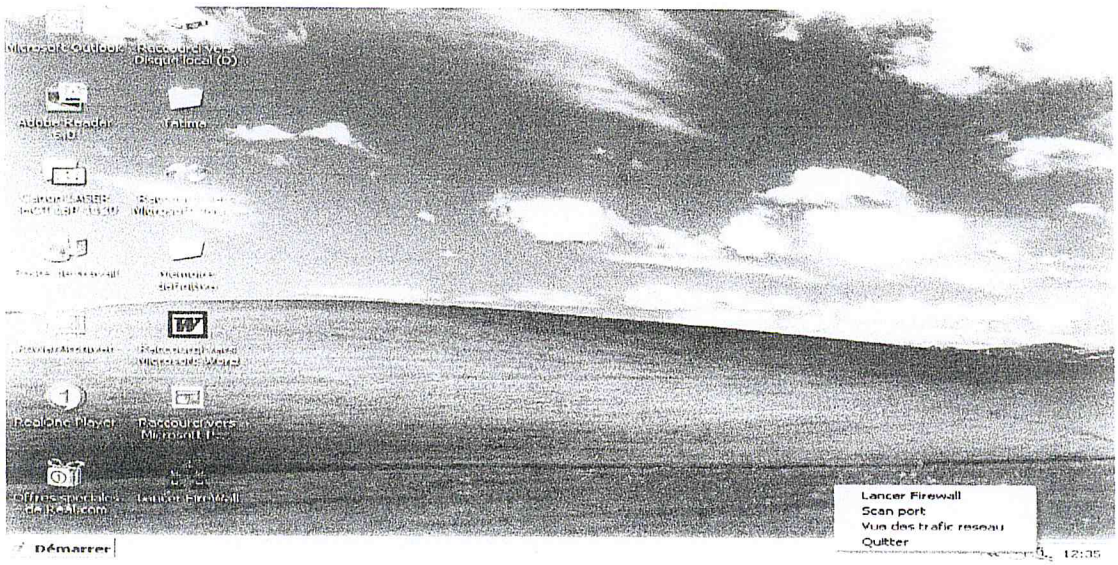


Figure 5.9 : Installation de Firewall.

Pour fermer le point d'entree dans la machine victime, nous avons bloque le port 1243 par la regle suivante :

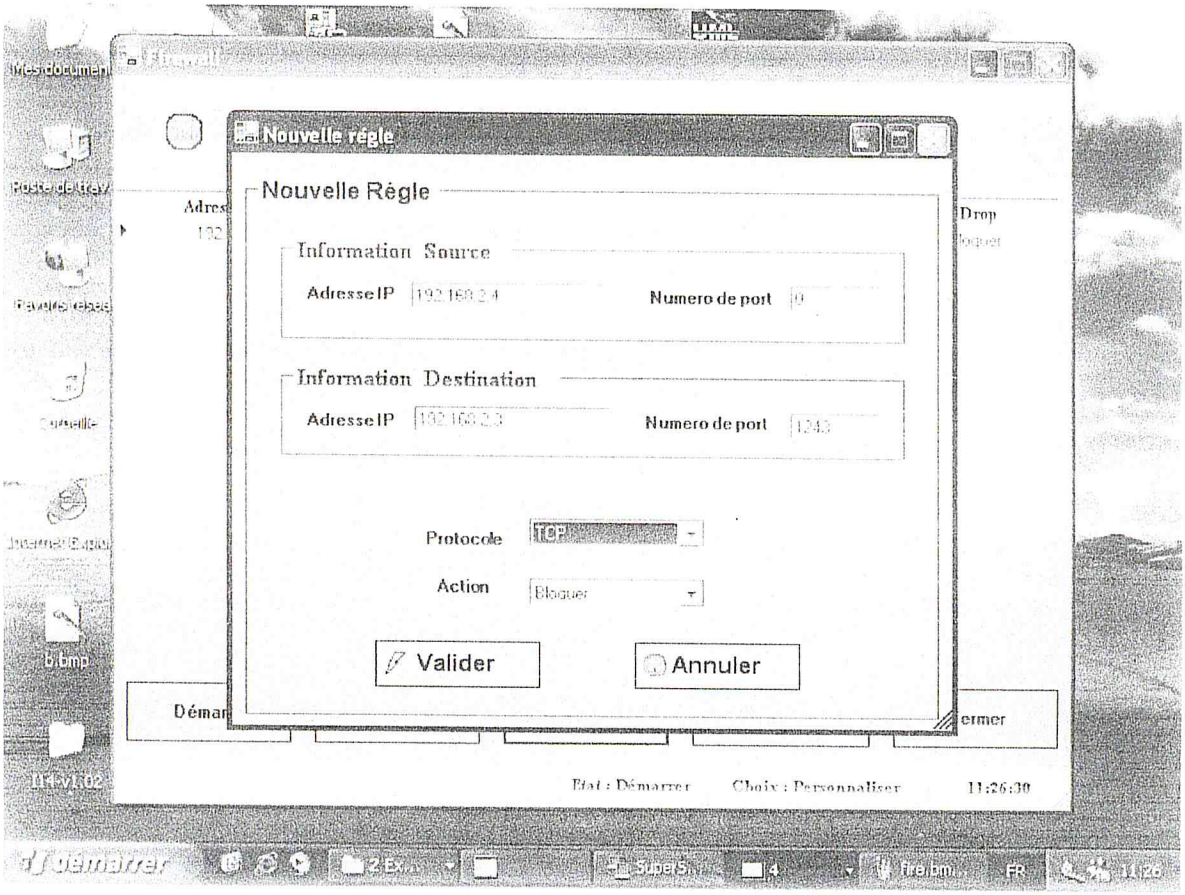


Figure 5.10 : Règle de filtrage.

7. Lancer l'attaque

Nous avons lance l'attaque en suivant les etapes precedemment decrites, mais cette fois ci on ne peut pas controler la machine victime.

8. Scan port

Nous avons scanner les ports de la machine victime à partir de la machine cliente. Nous avons trouve le port 1243 ferme.

5.8 Conclusion

La communication entre les machines interconnectées ne peut dérouler qu'à travers les ports qui sont des portes logiques d'entrer à un ordinateur connecter au réseau. L'ouverture de ces ports permet aux pirates de pénétrer le système, pour cela il faut que l'administrateur bloque certains ports dangereux (exemple : les ports utilisés par les chevaux de Troie) en utilisant un Firewall.

Après le test de notre Firewall, nous avons conclus que les chevaux de Troie ne peuvent pas ouvrir des ports bloqués par le Firewall, car ce dernier joue le rôle d'un mur entre le système d'exploitation et toute application externe.

Le Firewall ne bloque pas seulement les attaques à base de cheval de Troie, il peut aussi lutter contre certains types d'attaques comme :

- ICMP flooding ;
- Snork ;
- DoS (Denial of Service).

CONCLUSION GENERALE

Il est clair que la sécurité est l'un des problèmes les plus sérieux que connaissent les entreprises possédant des réseaux informatiques. Chaque entreprise doit donc savoir à quel point la sécurité est nécessaire, quoi qu'il en soit, il faut retenir qu'un réseau totalement sécurisé est une utopie. Un réseau totalement sécurisé est un réseau fermé, auquel personne n'a accès, que se soit par voie informatique ou par voie physique.

Alors il ne sera jamais possible de sécuriser totalement un système d'information. Il y aurra toujours des hackers génie pour découvrir des nouvelles failles dans les systèmes. Mais en peut toujours rendre une intrusion plus difficile, et si le pirate n'a pas d'interêt particulier à pénétrer cette entreprise plutôt qu'une autre, s'il éprouve trop de difficulté, il changera surement de cible, pour en trouver une plus facile.

C'est pour cette raison qu'actuellement plusieurs moyens de sécurité sont combinés pour répondre aux nouvelles exigences de sécurité, il s'agit des Firewalls, des VPN et des mécanismes de détection et de réaction aux intrusions (IDS) pour former ainsi ce qu'on appelle les CyberWalls. Les produits CyberWalls peuvent alors répondre aux exigences d'un centre de recherche. Mais le Firewall reste toujours la base de telle architecture de sécurité complexes.

De ce fait, nous avons réalisé un Firewall, qui est destiné à aider l'administrateur réseau pour contrôler l'accès aux ressources du système.

Notre application visait à atteindre les buts suivants :

- Filtrer les paquets IP ;
- Analyser le réseau ;
- Scanner les ports.

Ce projet nous a permet de découvrir la sécurité informatique, qui est une branche de l'informatique qui nous était totalement inconnue, et de nous familiariser avec de nouvelles techniques de réalisation de logiciels autres que celles déjà vus durant nos études. Nous avons aussi enrichi nos connaissances sur les réseaux.

L'outil réalisé n'étant pas une panacée pour les problèmes des réseaux interconnectés, il en reste toujours des améliorations à apporter. Pour cela, le prototype réalisé est ouvert aux modifications et à l'enrichissement, telle que l'ajout d'un proxy http, un système intelligent de détection d'intrusion et un antiVirus.

Annexe A

Le modèle TCP/IP

1. INTRODUCTION :

Ces quinze dernières années ont vu émerger de nouvelles techniques rendant possible l'interconnexion de réseaux différents (internet working) en les faisant apparaître comme un environnement unique de communication homogène. On désigne ce système d'interconnexion sous le nom d'Internet, sachant que réseau Internet et Internet désignent l'ensemble de ces réseaux dont le point commun est de fonctionner en suivant les protocoles TCP/IP (Transmission Control Protocol/Internet Protocol). [PAS 99]

Le nom TCP/IP se réfère à une suite complète de protocoles de communication de données. La suite tire son nom de deux protocoles en faisant partie : « Transmission Control Protocol » et « Internet Protocol ». Bien qu'il existe d'autres protocoles dans cette suite, TCP et IP en sont certainement les deux les plus importants.

Ils disposent de plusieurs caractéristiques : [CHA 95]

- Un protocole standard et ouvert, librement disponible et développé indépendamment de tout matériels informatiques et de tous systèmes d'exploitation.
- Une indépendance par rapport aux matériels réseaux spécifiques qui permet à TCP/IP d'intégrer différents types de réseaux.
- Un système d'adressage commun qui permet à tout système TCP/IP de s'adresser à n'importe quel autre système dans tout le réseau, même s'il est aussi étendu que l'Internet mondial.
- Des protocoles standardisés de haut niveau pour des services utilisateur cohérents et facilement disponibles.

2. ARCHITECTURE :

2.1 LES COUCHES DE LA PILE TCP/IP :

On admet que TCP/IP est structurés en quatre couches de protocoles qui s'appuient sur une couche matérielle comme illustré dans la figure 2.1 [STE 94] :

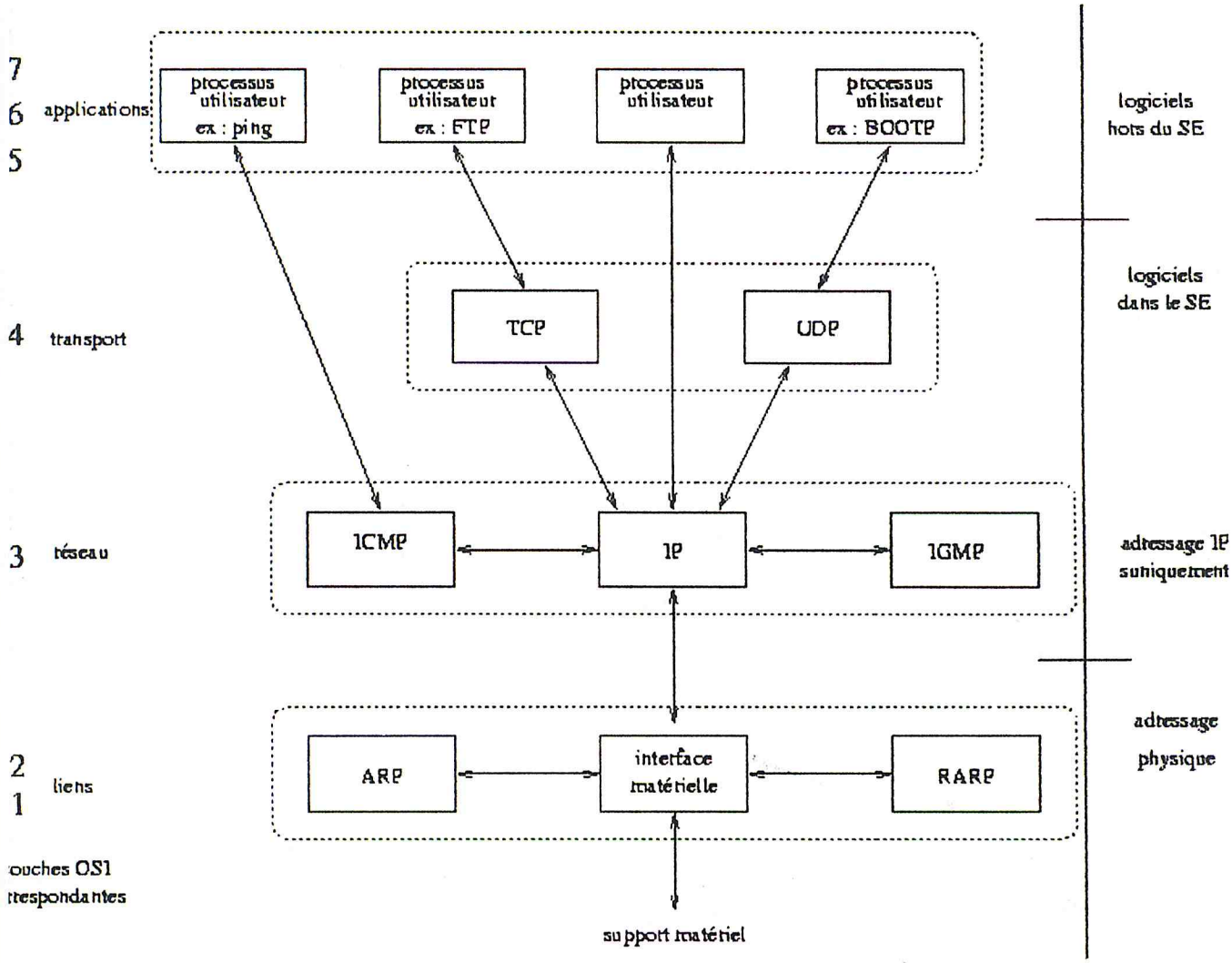


Figure 2.1 : Pile de protocole TCP/IP.

Chaque couche à une fonction différente :

- La couche liaison (Link layer) est l'interface avec le réseau, elle est constituée d'un driver du système d'exploitation et d'une carte d'interface de l'ordinateur avec le réseau.
- La couche réseau (Network layer) ou couche IP (Internet Protocol) gère la circulation des paquets à travers le réseau en assurant leur routage. Elle comprend aussi les protocoles ICMP (Internet Contrôle Message Protocol) et IGMP (Internet Groupe Management Protocol)

•La couche transport (Transport layer) assure tout d'abord une communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le destinataire. Elle s'occupe de réguler le flux de données et assure un transport fiable (données transmises sans erreur et reçues dans l'ordre de leur émission) dans le cas de TCP (Transmission Control Protocol) ou non fiable dans le cas de UDP (User Datagram Protocol). Pour UDP, il n'est pas garanti qu'un paquet (appelé dans ce cas datagramme) arrive à bon port, c'est à la couche application de s'en assurer.

•La couche application (Application layer) est celle des programmes utilisateurs comme Telnet (connexion à un ordinateur distant), FTP (File Transfert Protocol), SMTP (Simple Mail Transfert Protocol), etc. [PAS 99]

2.2 ENCAPSULATION DES DONNEES :

De même que pour le modèle OSI, les données sont passées vers la bas de la pile quand elles sont envoyées vers le réseau, et vers le haut quand elles sont reçues. Chacune des couches de la pile ajoute des informations de contrôle à fin d'assurer une livraison correcte. Ces informations de contrôle sont appelées un en-tête. [CHA 95]

La figure 2.2 [STE 94] montre ce processus.

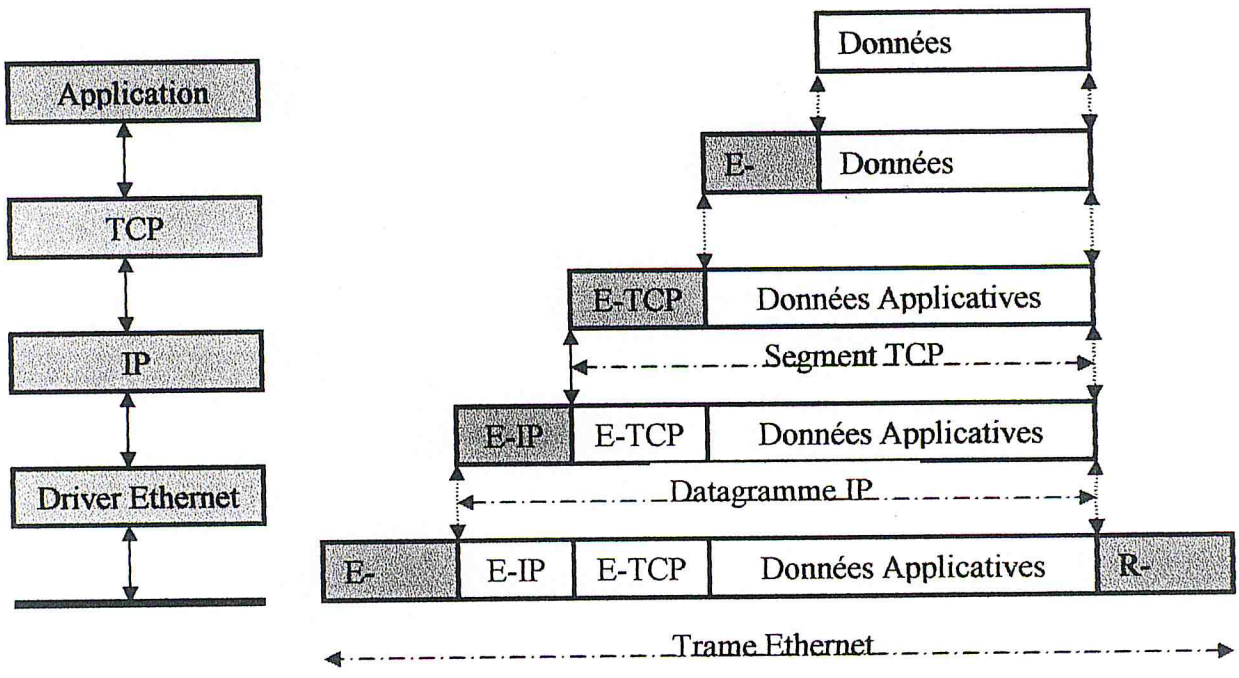


Figure A.2 : Encapsulation des données dans la pile de

3. ADRESSAGE IP :

3.1 STRUCTURE DE L'ADRESSE IP :

L'Internet a été conçu comme un réseau logique d'ordinateurs, dans lequel périphériques et logiciels sont connectés. Cette vision logique du réseau rend ce dernier indépendant de la technologie matérielle sous-jacente.

On a donc décider de structurer l'adresse IP de façon à ce qu'elle puisse refléter la distinction entre les différents réseaux logiques. Un certain nombre de bits dans l'adresse IP sont utiliser pour identifier le réseau individuel dans le réseau virtuel, et les bits suivants permettent d'identifier l'hôte au sein du réseau. [KAR 98]

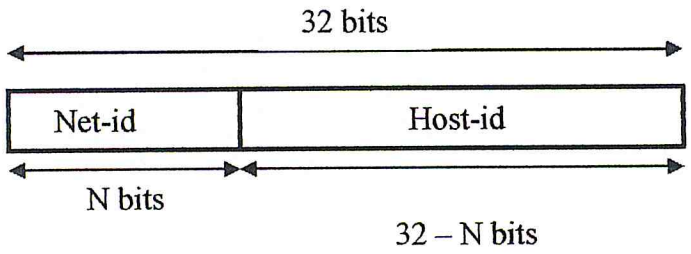


Figure 2.3 : L'adresse IP permet d'identifier le réseau et le hôte.

Le « netid » décrit chaque réseau connecté et le « hostid » identifie l'hôte au sein de ce réseau.

3.2 LES CLASSES D'ADRESSAGE :

chaque adresse IP appartient à une certaine classe (A, B, C, D ou E) selon la valeur de son premier octet, le tableau ci-après donne l'espace d'adresses possibles pour chaque classe.

Classe	Adresses
A	De **0**.0.0.0 à **127**.255.255.255
B	De **128**.0.0.0 à **191**.255.255.255
C	De **192**.0.0.0 à **223**.255.255.255
D	De **224**.0.0.0 à **239**.255.255.255
E	De **240**.0.0.0 à **247**.255.255.255

Figure 2.4 : Les cinq classe d'adresse IP.

3.3 ADRESSE PARTICULIERE :

En pratique, les adresses IP n'utilisent que peu de combinaisons de champ adresse « tout à zéro » ou « tout à un ». Parmis lesquelles on pourrait citer l'adresse de diffusion limité (les champ d'adresse sont tous à un), qui est utilisée pour envoyer àtous les nœuds du réseau, la source se trouvant dans le réseau lui même.

3.4 SOUS RESEAUX :

Le système des adresses IP permet également la définition d'adresses de sous-réseau en découpant la partie réservée à l'adresse des machines sur un réseau en deux parties dont la première sera un identificateur de sous-réseau. Ainsi un seul réseau de classe B, sur lequel on pourrait nommer 65 536 machines pourra être décomposées en 254 sous-réseaux de 254 machines, de la manière décrite ci-dessous. [KAR 98]

```
<Id de réseau, 16 bits>.<Id de sous-réseau, 8 bits>.<id de machine, 8 bits>
```

a) Masques de sous-réseau :

Le «masque » réseau est une adresse particulière, où tous les bits relatifs à la partie «Net-Id » sont à 1 et tous les bits relatifs à la partie «Host-Id » sont à 0.

Exemples :

Pour un réseau de classe C, Le netmask pourrait être = 255.255.255.0.

Ainsi on peut connaître l'adresse d'un réseau en réalisant l'opération « ET logique » entre l'adresse d'une machine et son masque réseau.

Exemple:

194.28.105.74 AND 255.255.255.0 = 194.28.105.0

On peut aussi connaître l'adresse de diffusion (Broadcast) en positionnant, dans l'adresse réseau, tous les bits de la partie « Host-Id » à un.

Ex: 194.28.105.255 est l'adresse de broadcast du réseau 194.28.105.

4. COUCHE LIAISON DE DONNEES :

Le but de la couche liaison de données de la pile TCP/IP est d'envoyer et recevoir des datagrammes IP pour la couche IP, d'envoyer des requêtes ARP (respt. RARP) et de recevoir des réponses pour le module ARP (respt. RARP).

TCP/TP supporte différent types de couche liaison, selon le type du matériel réseau utilisé : Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface)…

Nous examinons ici les caractéristiques des deux premières couches du modèle OSI (couches physique et de liens) dans le cas d'un réseau local Ethernet.

4.1 LE RESEAU ETHERNET :

Ethernet est le nom donné à une des technologies les plus utilisées pour les réseaux locaux utlisant TCP/IP. Elle a été inventée par Xerox au début des années 70 et normalisée par l'IEEE (Institute for Electrical and Electronics Engineers) vers 1980 sous la norme IEEE 802.

La méthode d'accès utilisée est la contention, tout le monde peut prendre la parole quand il le souhaite. Mais alors, il faut une règle pour le cas où deux stations se mettraient à " parler " au même moment. La principale méthode de contention en réseaux locaux est le **CSMA/CD** (Carrier Sense Multiple Access), avec détection de collision (CD). C'est celle d'Ethernet. Elle consiste pour une station, au moment où elle émet, à écouter si une autre station n'est pas aussi en train d'émettre. Si c'est le cas, la station cesse d'émettre et réémet son message au bout d'un délai fixe. Cette méthode est **aléatoire**, en ce sens qu'on ne peut prévoir le temps nécessaire à un message pour être émis, transmis et reçu.

4.1.1 Les différents types de réseaux Ethernet :

Les différents types de réseaux Ethernet sont [CAB 96] :

a) Thick Ethernet (IEEE 10Base5) : Aussi connu sous l'appellation « ThickNet », ce fût la forme originale des réseaux Ethernet. Le débit correspondant est de 10Mb/s. Les stations y sont reliées en « daisy chain » autour d'un bus.

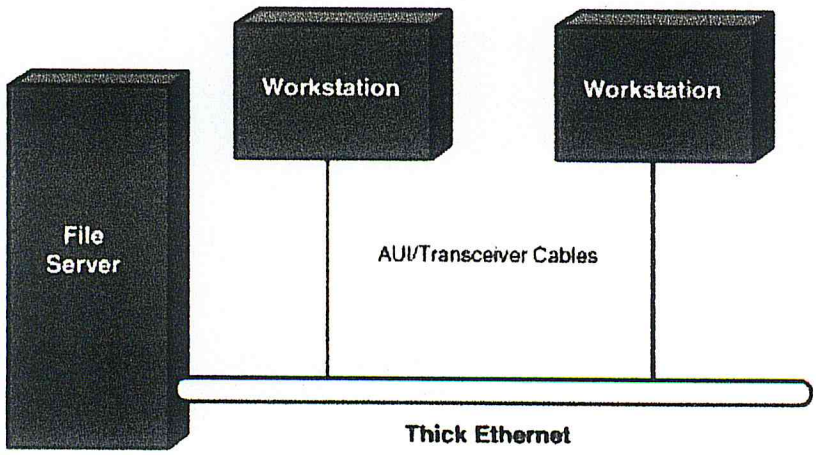


Figure 2.5 : Réseau 10Base5 élémentaire.

Câble utilisé : Le type de câble utilisé dans Ethernet 10Base5 est le coaxial épais (thick) d'impédance 50 Ohm. La longueur maximale d'un segment est de 500 m.

Composantes d'accès : Chaque station reliée au bus doit disposer d'une carte d'interface NIC (Network Interface Card) ainsi qu'un tranceiver ou MAU (Media Access Unit) greffé au bus. Le tranceiver est relié à la station (ou au NIC de la station) à l'aide du « Tranceiver Cable » ou AUI (Attachement Unit Interface).

b) Thin Ethernet (IEEE 10Base2) : C'est une variante de 10Base5 utilisant un câble coaxial fin (thin). Le débit est de 10Mb/s.

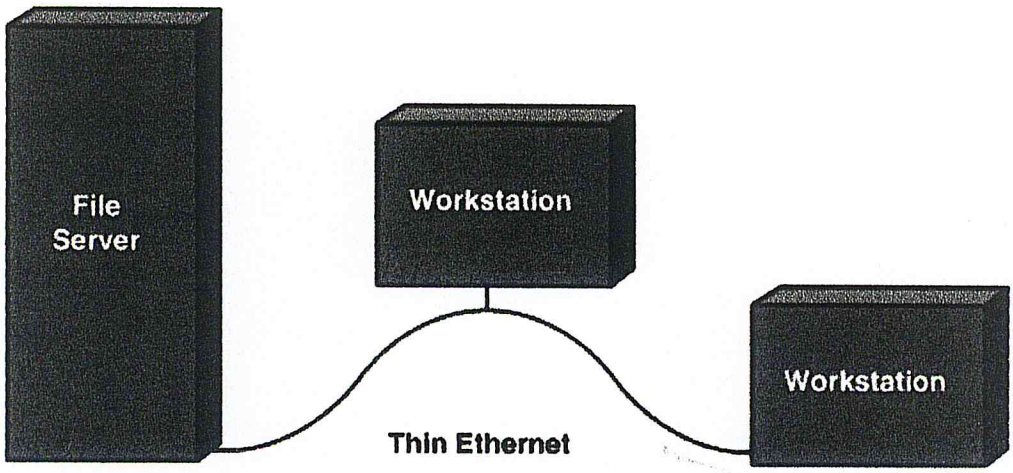


Figure 2.6 : Réseau 10Base2 élémentaire

La souplesse de la coaxiale fin lui permet d'être routé derrière chaque station, ainsi le MAU et le AUI se trouvent intégrés dans la carte d'interface.

c) 10BaseT et 100BaseT : Un réseau 10BaseT Ethernet est une adaptation des système de câbles téléphoniques existants pour une utilisation dans les LANs. 10BaseT est caractérisé par sa grande flexibilité et sa facilité d'installation ; ce qui fait que UTP (type de câble utilisé dans 10BaseT) est devenu le médium le plus utilisé dans Ethernet depuis sa standardisation en 1989. La topologie correspondante est l'étoile ce qui nécessite l'introduction d'une autre composante qui jouera le rôle de concentrateur. Le débit permit par 10BaseT est 10Mb/s tandis que dans 100BaseT il est de 100Mb/s.

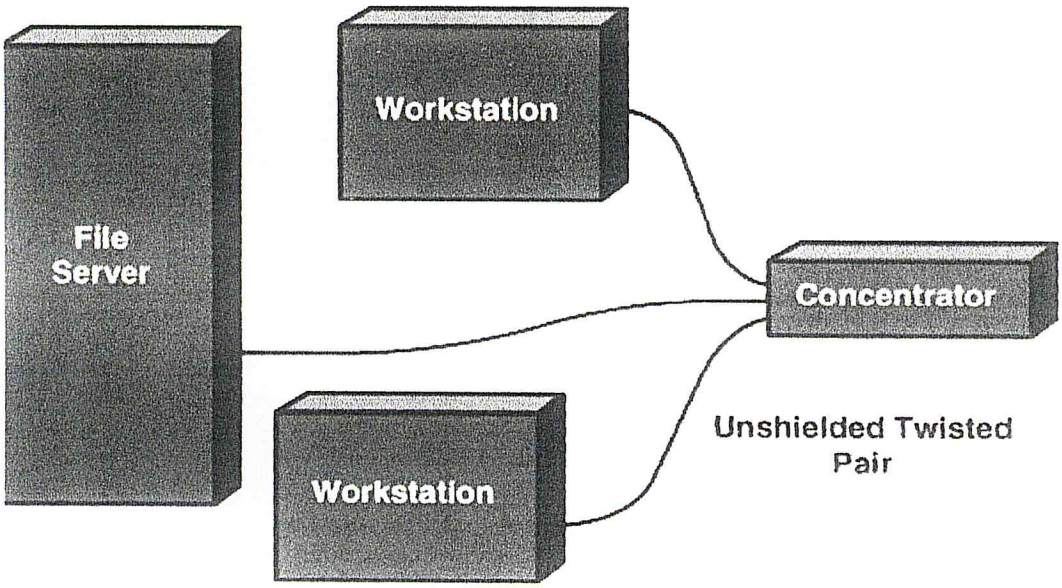


Figure 2.7: Réseau 10BaseT élémentaire.

4.1.2 L'adressage Ethernet :

Les adresses physiques Ethernet sont codées sur six octets (48 bits) et sont censées être uniques car les constructeurs et l'IEEE gèrent cet adressage de manière à ce que deux cartes réseau ne portent pas la même adresse. Elles sont de trois types :

- unicast dans le cas d'une adresse monodestinataire désignant une seule carte.
- broadcast dans le cas d'une adresse de diffusion générale (tous les bits à un) qui permet d'envoyer une trame à toutes les stations du réseau.
- multicast dans le cas d'une adresse multidestinataire qui permet d'adresser une même trame à un ensemble de stations qui ont convenu de faire partie du groupe que représente cette adresse multipoint.

4.1.3 La trame Ethernet :

Le format de la trame Ethernet tel que définit par le RFC 894 est :

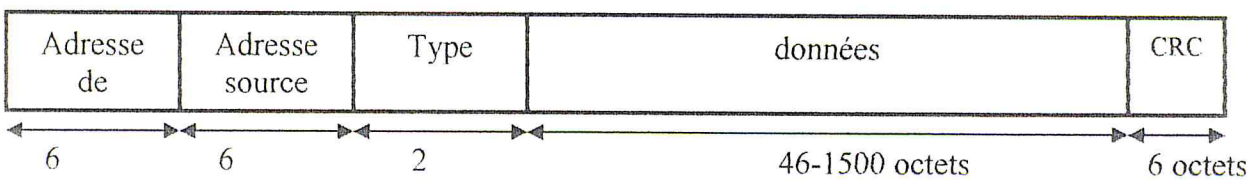


Figure 2.8 : Format de la trame

Le troisième champ contient le type de données transmises selon que c'est un datagramme IP, une requête ou réponse ARP ou RARP. Puis, viennent les données transmises qui peuvent avoir une taille allant de 46 à 1500 octets. Dans le cas de données trop petites, comme pour les requêtes et réponses ARP et RARP on complète avec des bits de bourrage ou padding.

4.2 LES PROTOCOLES ARP ET RARP :

Etant donné que le protocole IP, et ses adresses, peuvent être utilisés sur des architectures matérielles différentes (réseau Ethernet, Token-Ring, ...) possédant leurs propres adresses physiques, il y a nécessité d'établir les correspondances biunivoques entre adresses IP et adresses matérielles des ordinateurs d'un réseau. Ceci est l'objet des protocoles ARP (Address Resolution Protocol) et RARP (reverse Address Resolution Protocol). ARP fournit une correspondance dynamique entre une adresse IP connue et l'adresse matérielle lui correspondant, RARP faisant l'inverse. [PAS 99]

Un ordinateur utilise le protocole ARP pour déterminer l'adresse physique d'un autre ordinateur en diffusant une requête ARP (ARP Request). la requête contient l'adresse IP de l'ordinateur dont l'adresse physique est requise. Tous les ordinateurs d'un réseau reçoivent les demandes ARP : elles sont transmises en mode Broadcast. Un ordinateur sollicité répond à la requête qui montionne son adresse IP en envoyant une réponse (ARP Reply) qui contient son adresse physique, les réponses ARP sont directe, elles ne sont pas en mode diffusion.

Pour que ARP soit efficace, chaque ordinateur enregistre les associations adresse physique /adresse IP dans une mémoire cache (table cache ARP), qui permet d'éviter la plupart des diffusions de requêtes ARP.[KAR98] .

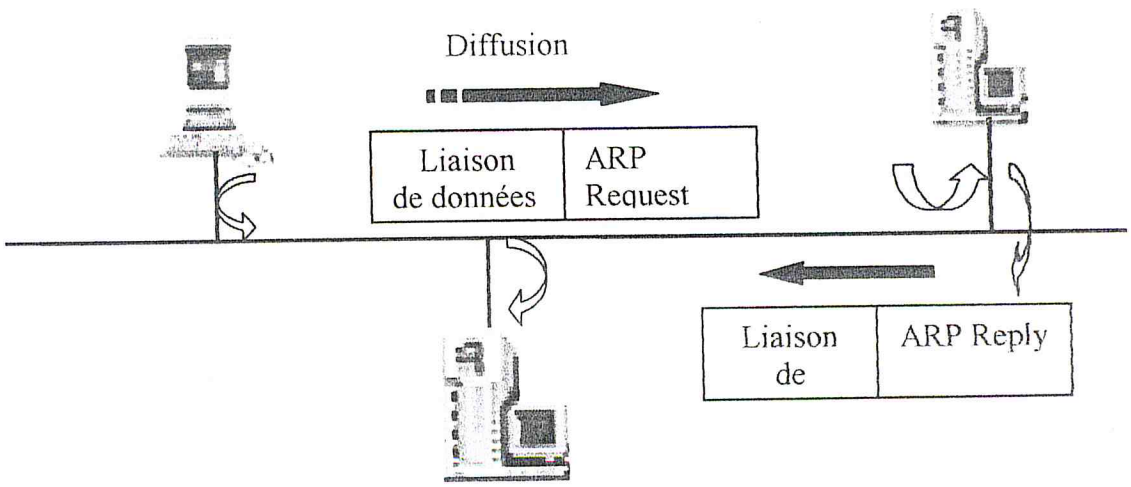


Figure 2.9 : Fonctionnement du protocole ARP.

Le format de la trame ARP et RARP est décrit dans la figure 2.10 : [PAS 99]

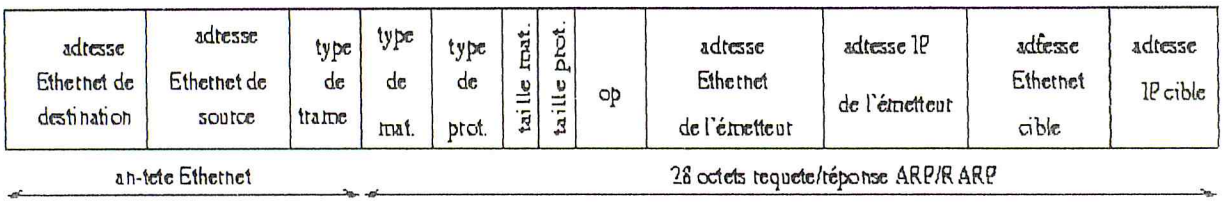


Figure 2.10 : Encapsulation de la trame APR et RARP

Le protocole RARP est utilisé par des stations pour découvrir leurs propres adresses IP. Les adresses IP sont stockées en un endroit central tel qu'un serveur. RARP est très souvent utilisé par les stations de travail sans disque. [KAR 98]

5. LE PROTOCOLE IP :

IP est la brique de base de l'Internet. Ces fonctions comprennent :

- La définition du datagramme, qui est l'unité de base de transmission de l'Internet.

La définition, du principe d'adressage de l'Internet.

- Le passage des données entre la couche d'accès réseau et la couche de transport Hôte a Hôte.
- Le routage des datagrammes vers les machines distantes.
- La fragmentation et le reassemblage des datagrammes. [CHA 95]

Il assure sans connexion un service non fiable de délivrance de datagrammes IP. Le service est non fiable car il n'existe aucune garantie pour que les datagrammes IP arrivent à destination. Certains peuvent être perdus, dupliqués, retardés, altérés ou remis dans le désordre. On parle de remise au mieux (best effort delivery) et ni l'émetteur ni le récepteur ne sont informés directement par IP des problèmes rencontrés. [STE 94]

Le mode de transmission est non connecté car IP traite chaque datagramme indépendamment de ceux qui le précèdent et le suivent. Ainsi en théorie, au moins, deux datagrammes IP issus de la même machine et ayant la même destination peuvent ne pas suivre obligatoirement le même chemin.

5.1 LE DATAGRAMME IP :

Le datagramme IP contient un entête IP (IP Header) suivi dés données IP provenant des protocole des couches supérieures. L'entête IP est conçue pour s'accommoder des particularités de la couche IP. [KAR 98]

L'entête IP a une longueur minimale de 20 octets, si des options sont spécifiées dans le datagramme cette langueur peut être plus grande, la figure 2.11 montre la structure générale de l'entête IP [HUN 97]

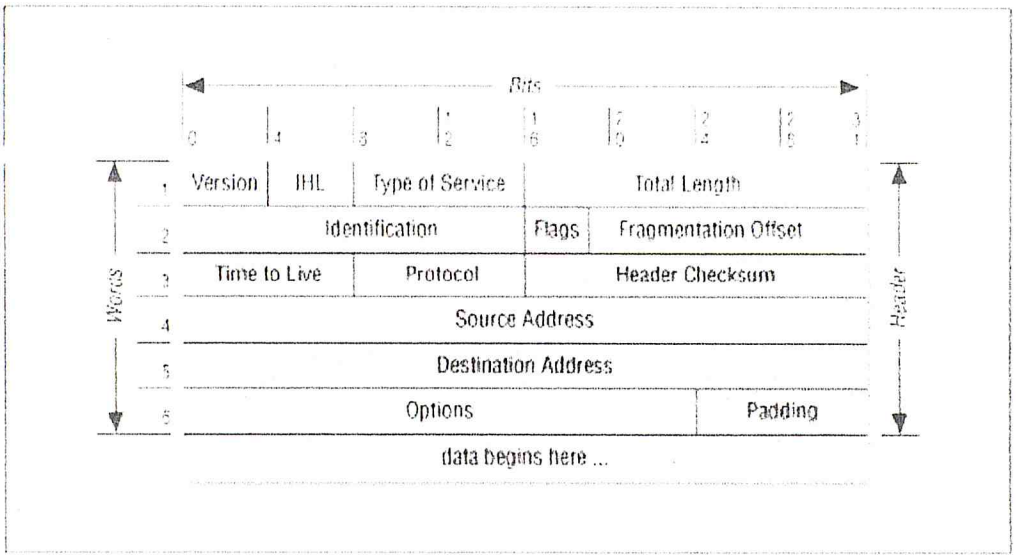


Figure 2.11 : Entête IP

La description des champs d'en-tête est : [STE 94]

- La version code sur quatre bits (4) le numéro de version du protocole IP utilisé (la version courante est la 4, d'où son nom d'IPv4.
- La longueur d'en-tête (IHL)représente sur quatre bits (4) la longueur, en nombre de mots de 32 bits, de l'en-tête du datagramme.
- Le type de services (TOS) est codé sur 8 bits, indique la manière dont doit être géré le datagramme et se décompose en six sous-champs.
- La longueur totale contient la taille totale en octets du datagramme (inférieure à 65535 octets)

- Les champs identification, drapeaux et déplacement de fragment interviennent dans le processus de fragmentation des datagrammes IP.
- La durée de vie (TTL – Time To Live -) indique le nombre maximal de routeurs que peut traverser le datagramme.
- Le champ « protocol » permet de coder quel protocole de plus haut niveau a servi a créé ce datagramme. Les valeurs codées sur 8 bits sont 1 pour ICMP, 2 pour IGMP, 6 pour TCP et 17 pour UDP.
- Les champs source adress IP et destination adress contiennent sur 32 bits les adresses de la machine émettrice et du destinataire finale du datagramme.
- Le champ options est une liste de longueur variable, mais toujours complétée par des bits de bourrage. Ces options sont très peu utilisées car peu de machines sont aptes à les gérer. Parmi elles, on trouve des options de sécurité et de gestion (domaine militaire)...

5.2 FRAGMENTATION DES DATAGRAMME :

Quand un datagramme est routé à travers différents réseaux, le module IP d'une passerelle peut se voir forcer de le diviser en partie plus petite. Un datagramme provenant d'un réseau peut se révéler trop grand pour être transmis d'un seul bloc sur un réseau différent. Cette condition ne se produit que quand une passerelle interconnecte des réseaux physiquement différents.

Chaque type de réseau comporte une unité de transmission maximale (Maximum Transmission Unit, MTU) qui est la taille du plus grand paquet transmissible. Si le datagramme d'un réseau est plus grand que la MTU de l'autre, il devient nécessaire de le diviser en fragments plus petits. Ce processus est appelé fragmentation.

6. LA GESTION DES ERREURS (LE PROTOCOLE ICMP) :

ICMP défini par le [RFC 792], fait partie intégrante de IP. Ce protocole appartient à la Couche Internet et emploie la fonctionnalité de livraison de datagramme IP afin d'envoyer ses messages. ICMP envoi des message qui se chargent des fonctions suivantes pour TCP/IP: [CHA 95]

- Contrôle de flux (Source Quench Message).
- Détection de destinations inaccessibles (Destination Unreachable).
- Redirection des routes (ICMP Redirect).
- Vérification des hôtes distants (ICMP Echo).

Le but d'ICMP n'est pas de fiabiliser le protocole IP, mais de fournir à une autre couche IP ou à une couche supérieure de protocole (TCP ou UDP), le compte-rendu d'une erreur détectée dans un routeur. Un message ICMP étant acheminé à l'intérieur d'un datagramme comme illustré dans la figure 2.12 [STE 94].

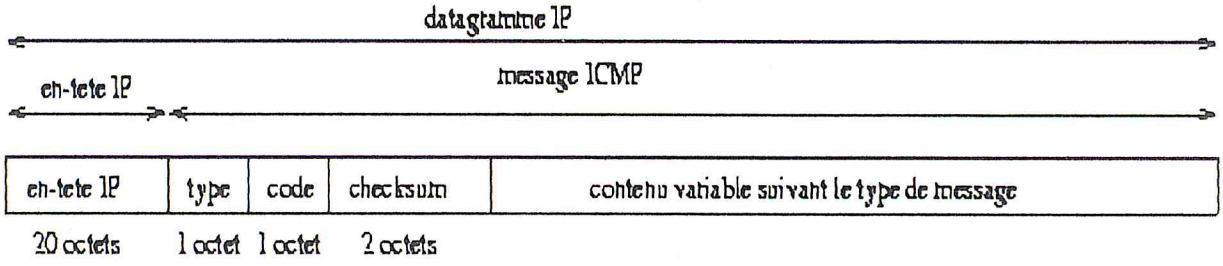


Figure 2.12 : Encapsulation d'un message ICMP.

a) Type ICMP 0 et 8 Echo/PING :

Les messages ICMP les plus utilisés sont sans doute les types Echo 0 et 8. Ces messages sont utilisés pour le diagnostic par l'utilitaire PING (Packet Internet Groper) qui est disponible sur la plupart des systèmes TCP/IP. PING permet de vérifier qu'un nœud IP est "vivant" et accessible, il envoie un message ICMP de type Requête d'écho (8) à un nœud IP. A la réception de ce message, le nœud IP renvoie un message ICMP de d'écho (0). Le message de réponse d'écho contient une copie des données envoyées dans le message de requête d'écho. La réception d'un message de réponse d'écho confirme que la couche IP (et les couches inférieures) du système de transport fonctionne bien entre la source et la destination. Si des routeurs intermédiaire sont rencontrés entre la source et la destination, le message de réponse d'écho indique aussi que les routeurs sont en mesure de transmettre des datagrammes entre la source et la destination.

7. LES PROTOCOLES DE TRANSFERT :

Les deux principaux protocoles de la couche transport d'Internet sont les protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol). Tous les deux utilisent IP comme couche réseau, mais TCP procure une couche de transport fiable (alors

même que IP ne l'est pas), tandis que UDP ne fait que transporter de manière non fiable des datagrammes.

7.1 PROTOCOLE UDP :

Le protocole UDP [RFC 768] assure un service de remise non fiable en mode non connecte qui utilise IP pour envoyer des datagrammes d'un programme d'application a un autre. C'est un outil orienté commande/réponse dont les commandes et les réponses peuvent tenir dans un seul datagramme. [KAR 98]

UDP n'utilise pas d'accusé de réception et ne peut donc pas garantir que les données ont bien été reçues. C'est donc à l'application qui utilise UDP de gérer les problèmes de perte de messages, duplications, retards, déséquencement....

Cependant, UDP fournit un service supplémentaire par rapport à IP, il permet de distinguer plusieurs applications destinatrices sur la même machine par l'intermédiaire des ports. Un **port** est une destination abstraite sur une machine identifiée par un numéro qui sert d'interface à l'application pour recevoir et émettre des données.[COM97, PAS00].

7.1.2 Format de l'entête UDP :

Chaque datagramme émis par UDP est encapsulé dans un datagramme IP en y fixant à 17 la valeur du protocole. Le format détaillé d'un datagramme UDP est donné dans la figure 2.13 : [HUN 97]

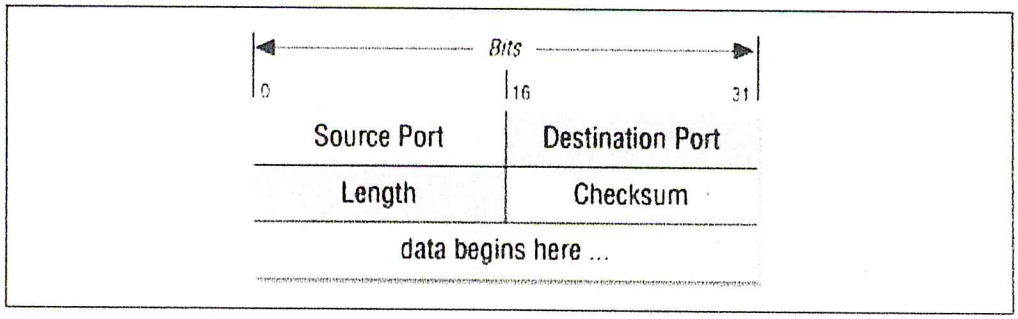


Figure 2.13 : En-tête UDP.

e champ longueur (Length) contient sur deux octets la taille de l'en-tête et des données transmises.

7.1.2 Applications utilisant UDP :

Les principaux services d'application utilisant UDP sont :

NFS (Network File System) : Montage de système de fichiers distant.

DNS (Domain Name Service) : La résolution de noms et d 'adresses IP.

BOOTP : (Boot Protocol) : Amorçage de stations sans disque

TFTP (Trivial File Transfert Protocol) : Transfert de fichier Simplifié.

SNMP (Simple Network Management Protocol) : Contrôle et gestion de réseaux à distance.

7.2 LE PROTOCOLE TCP :

TCP est un protocole orienté connexion, fiable à flux d'octets. Les données transmises par TCP sont encapsulées dans des datagrammes IP en y fixant la valeur du protocole à six (6). [RFC 792]

7.2.1 Caractéristique du protocole TCP :

Le protocole est caractérisé par :

a) **Orienté connexion :** signifie que les applications dialoguant à travers TCP sont considérées l'une comme un serveur, l'autre comme un client, et qu'elles doivent établir une connexion avant de pouvoir dialoguer. [STE 94].Une connexion est un circuit virtuel reliant deux programmes d'application, elle s'établit entre deux extrémités pour TCP : une extrémité de connexion est une paire de valeurs (adresse ip, port) [COM 97]. Une fois que tous les détails ont été précisés, les applications sont informées qu'une connexion a été établie et qu'elles peuvent commencer leurs échanges d'informations. Cette connexion est full duplex, et composé de deux flots de données indépendants et de sens contraire. [STE 94].

b) Tout au long de la connexion, TCP échange un **flux** continu d'octets et non pas des paquets indépendants [CHA 95].

c) **La fiabilité** : elle consiste à remettre des datagrammes, sans perte, ni duplication. Elle provient d'un mécanisme appelé positive acknowledgment with retransmission (PAR), Un système utilisant PAR renvoi les données à moins qu'il n'apprenne du système distant que les données sont bien arrivées [CHA 95]. TCP implantante ce mécanisme a l'aide de la technique général de l'accusé de réception (ACK). [KAR 98]

Chaque segment est émis avec un numéro qui va servir au récepteur pour envoyer un accusé de réception. Ainsi l'émetteur sait si l'information qu'il voulait transmettre est bien parvenue à destination. [KAR 98]

7.2.2 Entête TCP :

La figure 2.13 illustre l'entête TCP [HUN 97].

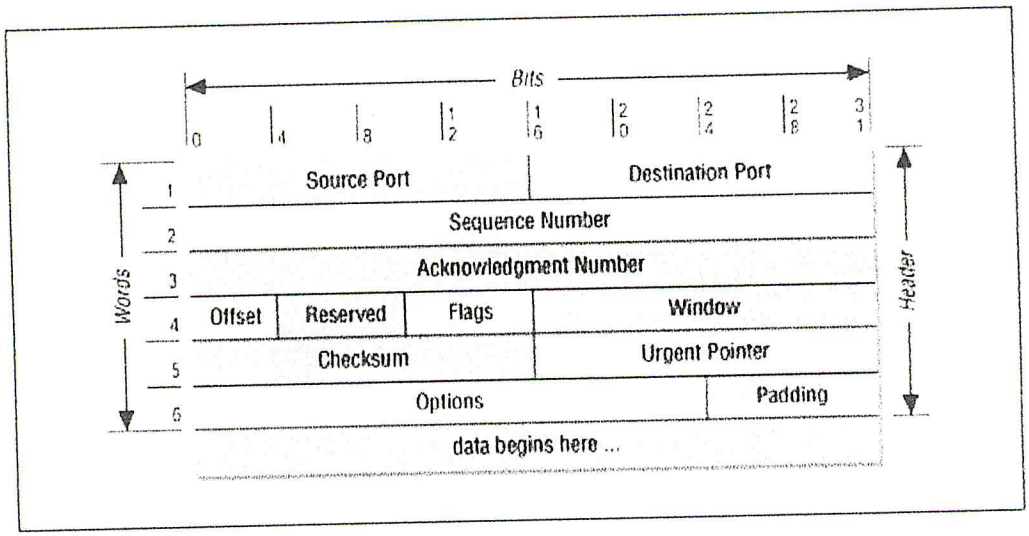


Figure 2.13 : Entête TCP

L'en-tête, sans option, d'un segment TCP (figure 1.13) a une taille totale de 20 octets et se compose des champs suivants :

- Le port source et le port destination identifient les applications émettrice et réceptrice.
- Le numéro de séquence (Sequence Number) donne la position du segment dans le flux de données envoyées par l'émetteur;.
- Le numéro d'accusé de réception (ACK) contient le numéro de séquence suivant que le récepteur s'attend à recevoir; c'est-à-dire le numéro de séquence du dernier octet reçu avec succès plus un. [KAR 98]
- La longueur d'en-tête (offset) contient sur quatre bits la taille de l'en-tête, y compris les options présentes, codée en multiple de quatre octets.
- Les six champs flags qui suivent le champ réservé permettent de spécifier le rôle et le contenu du segment TCP pour pouvoir interpréter correctement certains champs de l'en-tête. La signification de chaque bit, quand il est fixé à un est la suivante :

URG , le pointeur de données urgentes est valide.

ACK, le champ d'accusé de réception est valide.

PSH, ce segment requiert un push.

RST, réinitialiser la connexion.

- SYN, synchroniser les numéros de séquence pour initialiser une connexion.

- FIN , l'émetteur a atteint la fin de son flot de données

•La taille de fenêtre (Window) indique le nombre d'octets (moins de 65535) que le récepteur est prêt à accepter.

•Le pointeur d'urgence est un offset positif qui, ajouté au numéro de séquence du segment, indique le numéro du dernier octet de donnée urgente. Il faut également que le bit URG soit positionné à un pour indiquer des données urgentes que le récepteur TCP doit passer le plus rapidement possible à l'application associée à la connexion.

•L'option la plus couramment utilisée est celle de la taille maximale du segment TCP qu'une extrémité de la connexion souhaite recevoir.[PAS 99] .

7.2.3 Etablissement et fermeture d'une connexion TCP :

La connexion est établie entre les deux extrémités à l'aide d'un mécanisme de négociation a trois temps (three-way handshake) :

A : SYN =1 et ACK=0 paquet d'ouverture de connexion

B : SYN =1 et ACK=1 acquittement d'ouverture de la connexion

C : SYN =0 et ACK=1 paquet de données ou paquet ACK .

Une connexion TCP est libérée en un processus dit "trois temps modifié" [COM 97].

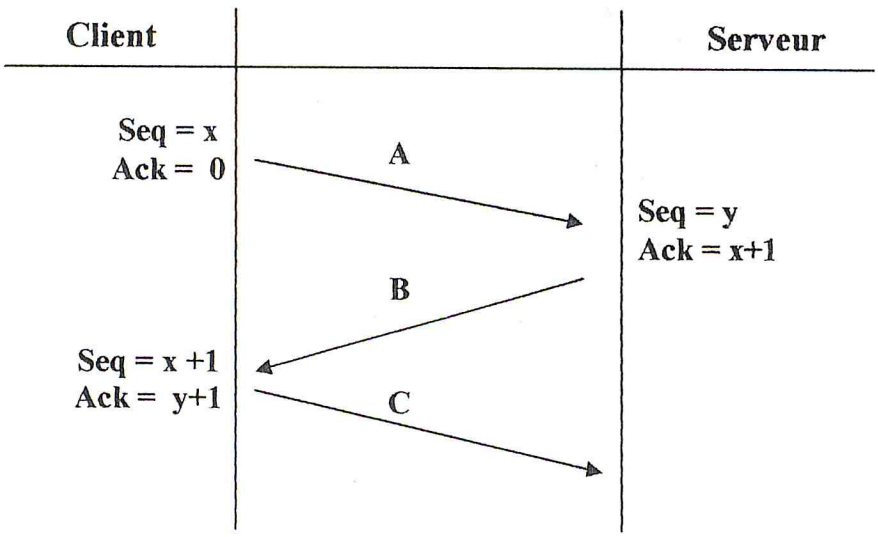


Figure 2.14: Le *Three-way Handshake.*

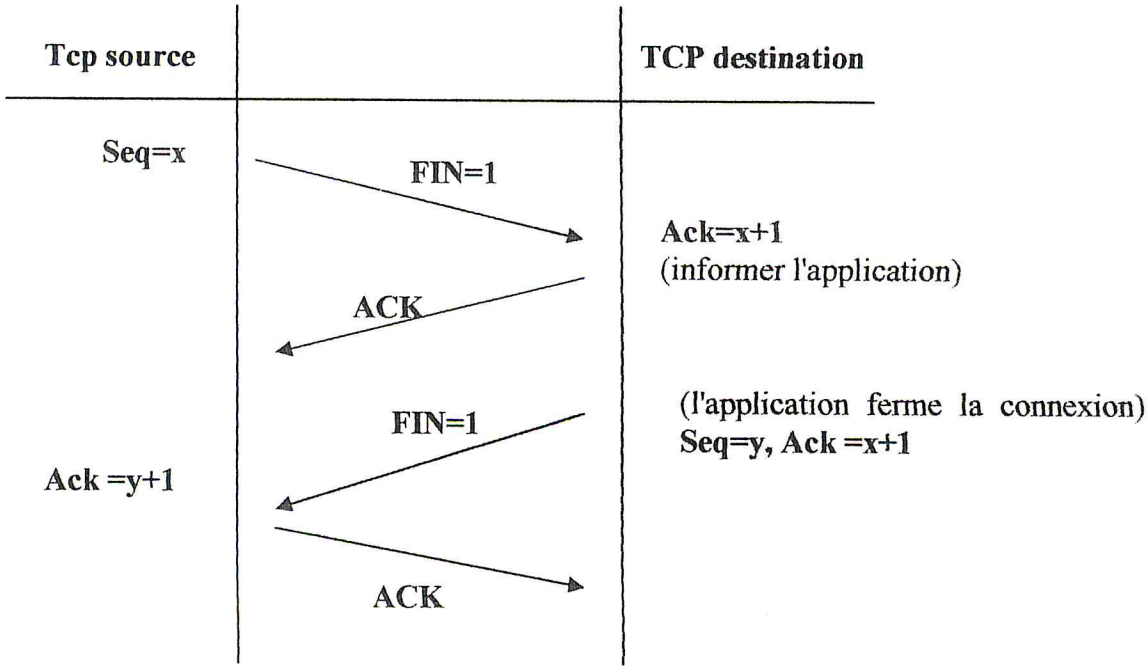


Figure 2.15: Le *tree-way Handshake* modifié.

Signalons le fait qu'il existe un autre moyen pour fermer une connexion TCP, qui consiste en l'envoi d'un message RST. A la réception du message RST le récepteur doit immédiatement terminer la connexion. Le message RST n'est pas la voie de fermeture normale d'une connexion TCP. [KAR 98]

7.2.4 Applications utilisant TCP:

Les principaux services d'application utilisant TCP sont :

- FTP (File Transfert Protocol) : Permet de transférer des fichiers d'une machine à une autre.
- Telnet et Rlogin : Deux applications qui permettent à un utilisateur de se connecter à distance sur un ordinateur.
- SMTP (Simple Mail Transfer Protocol) : Permet d'échanger des messages entre un expéditeur et un (ou plusieurs) destinataire.
- NNTP (Network News Transfert Protocol) : Le protocole d'échange des news ou forums de discussions à travers Usenet.
- HTTP (HyperText Transfer Protocol) : le protocole de communication du web, permettant d'échanger des documents hypertextes contenant des données sous la forme de texte, d'images fixes ou animées et de sons.

8. CONCLUSION :

TCP/IP est désormais reconnu unanimement comme le protocole de communication prédominant pour interconnecter différents systèmes informatiques. Cependant Les vulnérabilités décrits ci-dessus sont, en fait, des points faibles qui sont entrain d'être fixés (dans certain cas, il le sont déjà). Mais certaines d'entre elles font partie de la philosophie de design de TCP/IP.

Annexe B
Listes des ports utilisés par les chevaux de Troie

Listes des ports utilisés par les chevaux de Troie :

Voici une liste des chevaux de Troie les plus courant ainsi que des ports sur lesquels ils se mettent habituellement à l'écoute.
Bien sûr, elle n'est pas exhaustive puisque de nouveaux chevaux de Troie sont créés tous les jours.

PORT	PROTOCOLE	CHEVAL DE TROIE
8	ICMP	Ping A
9	UDP	Chargen
19	UDP	Chargen
21	TCP	FTP service
23	TCP	TELNET Service
25	TCP	Plusieurs troyens utilisent ce port
31	TCP	Agent 31
41	TCP	Deep Throat
53	TCP	DNS service
58	TCP	DM Setup
79	TCP	Firehotcker
80	TCP	Executor
99	TCP	Hidden Port 2.0
110	TCP	ProMail Trojan
113	TCP	Kazimas
121	TCP	Jammer Killah
129	TCP	Password Generator Protocol
135	TCP UDP	Netbios Remote procedure call
137	TCP UDP	Netbios name (DoS attacks)
138	TCP UDP	Netbios datagram
139	TCP UDP	Netbios session (DoS attacks)
146	TCP	Infector 1.3
421	TCP	Tcp Wrappers
456	TCP	Hacker's Paradise
531	TCP	Rasmin
555	TCP	Stealth Spy
666	TCP	Attack FTP
911	TCP	Dark Shadow
999	TCP	DeepThroat
9400	TCP	In Command
1000	TCP	Der Spaeher
1001	TCP	Silencer
1001	TCP	WebEx
1011	TCP	Doly Trojan
1012	TCP	Doly Trojan
1015	TCP	Doly Trojan

1015	TCP	Doly Trojan
1024	TCP	NetSpy
1025	UDP	Maverick's Matrix
1027	TCP	ICQ
1029	TCP	ICQ
1032	TCP	ICQ
1033	TCP	ICQ Trojan
1033	TCP	Exploit Descent Manager Module
1042	TCP	Rasmin
1045	TCP	Rasmin
1080	TCP	Socks/Wingate
1090	TCP	Xtreme
1170	TCP	Voice Streaming Audio
1207	TCP	SoftWar
1234	TCP	Ultors Trojan
1243	TCP	Sub Seven
1245	TCP	VooDoo Doll
1257	TCP	Sub Seven 2.1
1269	TCP	Maverick's Matrix
1492	TCP	Ftp 99CMP Trojan
1349	UDP	BackOrifice DLL Comm
1394	TCP	Gofriller
1394	TCP	BackDoor
1492	TCP	FTP99CMP
1509	TCP	Psyber Streaming Server
1600	TCP	Shivka-Burka
1807	TCP	SpySender
1981	TCP	Shockrave Trojan
1999	TCP	BackDoor Trojan
2000	TCP	Remote Explorer
2000	UDP	Remote Explorer/CallBook
2001	TCP	Trojan Cow
2023	TCP	Unknown Trojan
2086	TCP	Netscape/Corba exploit
2023	TCP	Ripper
2115	TCP	Bugs
2140	TCP	Deep Throat
2140	UDP	Deep Throat
2283	TCP	Troyen inconnu
2583	UDP	Troyen inconnu
2565	TCP	Striker
2583	TCP	WinCrash
2716	TCP	The Prayer 1.2 - 1.3

2721	TCP	Phase Zero
2801	TCP	Phineas Phucker
2989	UDP	Rat
3024	TCP	WinCrash
3129	TCP	Master's Paradise
3150	TCP	Deep Throat
3150	UDP	Deep Throat
3587	UDP	Sh*tHead Trojan
3587	TCP	Sh*tHead Trojan
3700	TCP	Portal of Doom
4092	TCP	WinCrash
4321	TCP	SchoolBus
4567	TCP	File Nail
4590	TCP	ICQ Trojan
4950	TCP	Troyen inconnu
5000	TCP	Sokets de Trois v1.
5001	TCP	Sokets de Trois v1.
5011	TCP	OOTLT
5031	TCP	Net Metropolitan
5032	TCP	Net Metropolitan
5321	TCP	Firehotcker
5400	TCP	Blade Runner
5401	TCP	Blade Runner
5402	TCP	Blade Runner
5501	UDP	Unknown
5521	TCP	Illusion Mailer
5550	TCP	X-Tcp Trojan
5555	TCP	ServeMe
5556	TCP	BO Facil
5557	TCP	BO Facil
5569	TCP	Robo-Hack
5666	TCP	PC Crasher
5742	TCP	WinCrash
6400	TCP	The Thing
6667	TCP	Sub-7 2.1
6670	TCP	Deep Throat
6711	TCP	Sub Seven
6712	TCP	Sub Seven
6713	TCP	Sub Seven
6723	TCP	MStream
6771	TCP	Deep Throat
6776	TCP	Sub Seven
6838	UDP	MStream

6939	TCP	Indoctrination
6969	TCP	Gate Crasher
6969	TCP	Priority
6970	TCP	Gate Crasher
7000	TCP	Remote Grab
7028	TCP	Troyen inconnu
7028	UDP	Troyen inconnu
7300	TCP	Net Monitor
7301	TCP	Net Monitor
7302	TCP	Net Monitor
7303	TCP	Net Monitor
7304	TCP	Net Monitor
7305	TCP	Net Monitor
7306	TCP	Net Monitor
7307	TCP	Net Monitor
7308	TCP	Net Monitor
7309	TCP	Net Monitor
7323	TCP	Sygate Backdoor
7323	UDP	Sygate Backdoor
7597	TCP	QaZ Trojan Communications
7789	TCP	ICKiller
7983	UDP	MStream
8783	TCP	Troyen inconnu
9325	UDP	MStream
9872	TCP	Portal of Doom
9873	TCP	Portal of Doom
9874	TCP	Portal of Doom
9875	TCP	Portal of Doom
9989	TCP	iNi-Killer
10067	TCP	Portal of Doom
10067	UDP	Portal of Doom
10167	TCP	Portal of Doom
10167	UDP	Portal of Doom
10498	UDP	Handler to Agent
10520	TCP	Acid Shivers
10607	TCP	Coma
10666	UDP	Ambush
11000	TCP	Senna Spy
11223	TCP	Progenic Trojan
12076	TCP	GJamer
12223	TCP	Hack'99
12361	TCP	TCP Whack-a-mole
12362	TCP	TCP Whack-a-mole

12345	TCP	Netbus
12345	TCP	Ultor's Trojan
12346	TCP	Netbus
12361	TCP	TCP Whack-a-mole
12362	TCP	TCP Whack-a-mole
12456	TCP	NetBus
12631	TCP	WhackJob
12701	TCP	Eclipse 2000
12754	TCP	MStream
13000	TCP	Senna Spy
13700	TCP	Troyen inconnu
15104	TCP	MStream
16660	TCP	Stacheldraht
16969	TCP	Priority
18753	TCP	shaft Handler to agent(s)
20000	TCP	Millennium
20001	TCP	Millennium
20034	TCP	NetBus 2 Pro
20432	TCP	shaft Client to handler
20433	UDP	shaft Agent to handler
21544	TCP	Troyen inconnu
21554	TCP	GirlFriend
22222	TCP	Prosiak
20203	TCP	"Logged"
20331	TCP	Troyen inconnu
23456	TCP	EvilFTP
24680	TCP	Troyen inconnu
24680	UDP	Troyen inconnu
26274	TCP	Delta Source
26274	UDP	Delta Source
27665	TCP	Trin00/TFN2K
27374	UDP	Sub-7 2.1
27374	TCP	Sub-7 2.1
27444	UDP	Trin00/TFN2K
27573	UDP	Sub-7 2.1
27573	TCP	Sub-7 2.1
27665	TCP	Trin00 DoS Attack
29891	TCP	The Unexplained
30029	TCP	AOL Trojan
30999	TCP	Kuang2 Trojan
30100	TCP	NetSphere
30101	TCP	NetSphere
30102	TCP	NetSphere

30303	TCP	Sockets de Troie
31335	UDP	Trin00 DoS Attack
31337	UDP	Backorifice/BO-2K
31337	TCP	Netpatch
31338	TCP	NetSpy DK
31338	UDP	Deep BO
31339	TCP	NetSpy DK
31666	TCP	BOWhack
31785	TCP	Hack'a'Tack
31789	UDP	Hack'a'Tack
31790	UDP	Hack`a'Tack
31791	UDP	Hack'a'Tack
32418	TCP	Acid Battery
33333	TCP	Prosiak
33390	UDP	Troyen inconnu
34324	TCP	BigGluck
34324	TCP	TN
34555	UDP	Trin00 Ping/Pong Response
33911	UDP	Trojan Spirit 2001
40421	TCP	Master's Paradise Trojan
40412	TCP	The Spy
40422	TCP	Master's Paradise
40423	TCP	Master's Paradise
40425	TCP	Master's Paradise
40426	TCP	Master's Paradise
47252	TCP	Delta Source
47262	UDP	Delta Source
49301	UDP	Online KeyLogger
50505	TCP	Sokets de Trois v2.
50766	TCP	Fore 1.0 Trojan
50776	TCP	Fore
53001	TCP	Remote Windows Shutdown
54320	TCP	Back Orifice 2000
54320	UDP	Back Orifice
54321	TCP	School Bus
54321	TCP	Back Orifice
54321	UDP	Back Orifice 2000
57341	UDP	Net Raider Trojan
57341	TCP	Net Raider Trojan
60000	TCP	Deep Throat
61603	TCP	Bunker-Hill Trojan
61348	TCP	Bunker-HillTrojan
61466	TCP	Telecommando

63485	TCP	Bunker-Hill Trojan
65000	TCP	Devil
65000	TCP	Stacheldraht

Bibliographie

BIBLIOGRAPHIE

Livres et Thèses

[ABD 01] Abdelleh El Haj .H
Korthobi .M,
« Réalisation d'un outil détecteur de SNIFFER : système de détection d'intrusion »,
Thèse d'ingéniorat 2000/2001. USTHB

[BEL 02] Amirouche Belkhiri, Slimane Reda,
«Conception et mise en oeuvre d'un Firewall»,
Thèse d'ingéniorat, option SI, Institut National d'Informatique, 2001-2002.

[BEL 94] Mark BELL,
« Protecting Networks With and Without Firewalls :
Part 1 – The Sniffer Attack »,
Technical Entrepises, Inc, 1997

[BEN 03] Benchibane Mohamed, Brahmi Abdelkader,
« Conception et Réalisation d'un scanner de sécurité»,
Thèse D'ingéniorat, Université de Blida, Département d'informatique 2003/2004.

[BID 95] C.Bidan et V.Issarny,
« Un aperçu des problèmes de sécurité dans les systèmes informatiques »,
Institut de Recherche en Système Aléatoires –IRISA-, Octobre 1995.

[BEL 89] S.M. Bellovin,
« Security Problems in the TCP/IP Protocol Suite »
AT&T Bell Laboratories Murray Hill, New Jersey, 1989.

[CAB 96] « Cabletron Systems : Cabling Guide »,
Cabletron Systems, INC, US, Décembre 1996.

[CHA 95] D.Brent Chapman, Elizabeth D.Zwicky,
« Building Internet Firewalls »,
First Edition O'Reilly, Novembre 1995.

[CHA 01] Chaouchi Hakima,
« Conception et realisation d'un outil intelligent d'aide au choix de Firewalls pour la protection d'un reseau informatique »,
Thèse Magistère, Institut National d'Informatique, 2000-2001.

[CLO 93] Bryan Glough,
« La délinquance assistée par ordinateur »,
Dunod Tech, 1993.

[CNA 01] Cnam-Cedric, F-Y.Villemin,
« Architecture d'un site Internet »,
www. 2000-2001.

[DOD 83] Department of Defence Standard.
« Trusted Computer System Evaluation Criteria »,
Orange book, CSC-STD-001-83.

[DOD 85] Departement of Defense Standard.
« Trusted Computer System Evaluation Criteria »,
Rapport technique n° DoD 5200.28-STD, décembre 1985.

[HUN 97] Craig Hunt,
« TCP/IP Network Administration »,
Second Edition, December 1997

[KAR 98] Karanjit S. Siyan
« TCP/IP »,
Simon & Schuster Macmilan, ISBN 2-7440-0391-3. 1998.

[PAS 99] Pascal Nicolas,
« Cours réseaux de l'université d'Angers », 1999.

[ITS 91] Commission of the European Communities - ITSEC -
« Information Technology Security Evaluation Criteria »,
European Comunities, v1.2 édition, juin 1991.

[ISO 89] Norme Internationale ISO 7498-2,
« Système de traitement de l'information Interconnexion des systèmes ouverts »,
Modèle de référence de base. Partie 2 : Architecture de sécurité.

[MER 99] Merike Kaeo,
« Sécurité des réseaux, un guide pratique pour créer une infrastructure de réseau sécurisé »,
CompusPress France 1999.

[NBS 77] N. B. of Standards,
« Data Encryption Standard »,
Number 46 in NBS, FIPS PUB, U. S. Department of Commerce,
Janvier 1977.

[NCS 87] National Computer Security Center,
« Trusted Network Interpretation of the TCSEC »,
Rapport technique, NCSC-TG-005, juillet 1987.

[OLO 92] Tomas Olovsson,
« A Structured Approach to Computer Security »,
Department of Computer Engineering Chalmers University of Technology S-412 96 Gothenburg SWEDEN, Technical Report n°122.
1992.

[GUI 00] Guillaume Desgeorge,
« La sécurité des réseaux. »,
http://www.guill.net , 2000.

[Lab 01] http://www.zonelabs.com, 2001.

[Net 04] http://www.networkice.com/products/index.html , 2004.

[PH 03] PH. Oechslin,
« La sécurité des réseaux, Chapitre 2 : les menaces »,
http://www.securityfocus.com .

[SANS 03] SANS Institut,
« Les vingt vulnérabilités de sécurité les plus critiques d'Internet »,
www.sans.org Octobre 2003.

[SAU 03] Sébastien Sauvage,
« C'est quoi un Firewall ? »,
http://www.sebsauvage.net, 2003.

[Sym 04] http://www.symantec.com , 2004.

[RFC xx] Request for comments,
Les RFC peuvent être obtenue via le site www.ds.internic.net.

[WFI 99] www.firewall.com.

Sites Web

[BAC 00] Rebecca BACE,
«An introduction to Intrusion Detection & Assesment.",
ICSA http://www.icsa.net , 2000.

[CERT 02] http://www.cert.org 2002.

[CH 02] N.Chazot,
« Statistique des risques »,
ISS http://www.iss.net, 2002-2004.

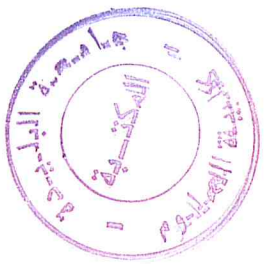
[CIS 98] CISCO Systems,
« Internet Working Technology Overview »,
http://www.cisco.com , 1998.

[COM 03] http://www.commentçamarche.com

[CV 01] Cyril Vision,
« Microsoft et sécurité »,
http://www.microsoft.com/france/securite/evenements/

[DUP 01] Nicolas Dubée,
« Actions offensives sur Internet »,
http://www.secway.com Septembre 2001.

[DUP 02] Dupont Sébastien,
« Administration et sécurisation des systèmes Linux et BSD »,
http://www.epita.fr. 28 Octobre 2002.



[PAU 03] Paul Grégory,
« Ecriture d'un Firewall en JAVA », 2003
Université de Paris, 30 Mars 2003.

[PRI 98] Jacques Printz
« Génie Logiciel»
Techniques d'ingénieur; 1998.

[STE 88] J. G. Steiner, B. C. Neuman, et J. I. Schiller,
« Kerberos: Authentification Service for Open Network Systems »,
In USENIX Conference Proceedings, Février 1988.

[STU 03] Stuart McClure, Joel Scambray, George Kurtz,
« Halte aux Hackers » Compusspress 2003.