République Algérienne Démocratique et Populaire

UNIVERSITE SAAD DAHLAB DE BLIDA

Département Informatique

MEMOIRE DE FIN D'ETUDES POUR L'OBTENTION DU DIPLOME

DE MASTER EN INFORMATIQUE

ETUDE ET DEVELOPPEMENT D'UN FIREWALL POUR LA SECURITE D'UN RESEAU INFORMATIQUE

Réalisé par :

M^elle^ LEMDANI Hanane.

M^elle^ KAABECHE Asma.

Promoteur :

M^r^ Mehdi Merouane

Encadreur:

M^r^HaferssasFouad

Président : Mr AMELD, AISSA

Année Universitaire 2009/2010

Remerciements

Durant ce stage, nous avons évolué dans un environnement très instructif et dont le cadre ouvert nous a permis d'obtenir tous les renseignements et toute l'aide dont nous avions besoin, pour cela nous tenons à remercier tout d'abord **Dieu** tout puissant.

Nos remerciements et notre gratitude se portent vers notre promoteur Monsieur MEHDI Merouane, Directeur du centre de calcul de l'Université Saad Dahlab de BLIDA et notre encadreur Monsieur HAFERSSAS Fouad, Ingénieur au sein de RMS-Algérie Télécom pour l'intérêt qu'ils ont porté à notre travail, pour leur disponibilité, pour leurs compétences et leur ouverture d'esprit.

Ensuite, nous remercions très sincèrement le membre de jury pour avoir accepté d'évaluer notre travail.

Nous adressons également nos remerciements, à tous nos enseignants qui nous ont donnés les bases de la science, pour leurs conseils prodigués.

Merci aussi à toutes les personnes ayant contribué de près ou de loin à l'achèvement de ce projet, directement ou indirectement, volontairement ou non.

Dédicaces

Je dédie ce modeste travail à :

Mes parents qui sont la source de ma réussite.

Mes chères sœurs et mes chers frères

Ma famille qui est la source de ma fierté.

Mes Ami(e)s qui sont la source de ma confiance.

Mes enseignants qui sont la source de mon savoir.

Et enfin à tous ceux qui m'ont soutenu de près ou de loin et qui ont contribué à l'achèvement de ce travail dans les meilleures conditions.

K.ASMA

Dédicaces

Je dédie ce modeste travail à :

Mes parents qui sont la source de ma réussite.

Ma chère sœur et mes chers frères

Ma tante Dalila et sa petite famille

Mon fiancé Mohamed ainsi que toute ma belle-famille.

Ma famille qui est la source de ma fierté.

Mes Ami(e)s qui sont la source de ma confiance.

Mes enseignants qui sont la source de mon savoir.

Et enfin à tous ceux qui m'ont soutenu de près ou de loin et qui ont contribué à l'achèvement de ce travail dans les meilleures conditions.

L. HANENE

ملخص

خلال العشرية الماضية، عرفت الانترنيت تطورا ملحوظا، بحيث أنها تمكّن تبادل كميات هائلة من المعلومات في ظرف زمني قصير جدا، مما ساهم في رفع إنتاج المؤسسات. غير أن توصيل شبكات هذه المؤسسات بالانترنيت يحتم وجود سياسة حماية و امن في مستواها، و استعمال أجهزة مصنعة أو برمجيات الحاسب و ذلك لاجتناب خطر التعرّض للقرصنة.

يهدف هذا المشروع إلى دراسة امن الحاسب بشكل عام و الجدران النارية بشكل خاص، و يتطرق أيضا إلى تصميم و انجاز جدار ناري.

كلمات المفاتيح : *امن الحاسب، جدار ناري، تصفية و تشريح الطرود، سنيفر، مسح الأبواب.*

Résumé

Durant la dernière décennie, le réseau informatique mondial Internet a connu une croissance exponentielle. En effet il permet d'échanger de très grande quantité d'informations dans des délais extrêmement cours, ce qui permet, notamment, d'augmenter la productivité des entreprises. Cependant, le raccordement de ces dernières au réseau mondial impose toute une politique de sécurité au niveau de l'entreprise qui s'y connecte, et des protections matérielles et logiciels suffisantes pour éviter tout risque de fuites ou piratages.

Ce projet a pour objectif d'étudier d'abord les concepts de la sécurité informatique en générale et les Firewalls en particulier, ensuite la conception et la mise en œuvre d'un Firewall.

Mots clés : *sécurité informatique, Firewall, filtrage des paquets, sniffer, scan des ports.*

Abstract

During the last decade, the Internet knew an exponential increase. In fact, it allows exchanging huge quantity of information within extremely small periods, which permits increasing the productivity of the companies. However, the connection of these last to the network imposes a whole security policy on the company level which is connected to, and sufficient material and software protections to avoid any risk of hackings.

The aims of this project are studying the concepts of the computer security in general and Firewalls in particular, then the design and the implementation of a Firewall.

Key words: *computer security, Firewall, packet filtering, sniffer, port scan.*

Table des matières

CHAPITRE 4 : Conception et mise en œuvre

CHAPITRE 5 : Tests par simulation d'attaque

Liste des figures

INTRODUCTION GENERALE

De nos jours, toute entreprise, institution, université et centre de recherche possédant un réseau local possèdent aussi un accès à Internet, afin d'accéder à la manne d'information disponible sur le réseau des réseaux, et de pouvoir communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable et dangereuse en même temps. S'ouvrir vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local et y accomplir des actions douteuses, parfois gratuites, de destruction, vol d'informations confidentielles, ... Les mobiles sont nombreux et dangereux.

Par conséquent, il faut adopter des politiques de sécurité et de mettre en œuvre des dispositifs de protection, les Firewalls constituent la base de toute architecture de sécurité. Ces derniers constituent aussi un point d'entrée au réseau afin de pouvoir recevoir et transmettre les données autorisées, et empêchent l'accès à des ressources réseau définies en créant une couche protectrice entre le réseau et le monde extérieur. L'objectif de notre projet est l'étude, la conception et la réalisation d'un Firewall pour contrôler l'accès à un réseau LAN en réalisant quatre (04) modules : un filtreur de paquets, un analyseur de réseau ainsi qu'un scanner et un mapper de ports en utilisant Windows XP comme plate forme et Visual C# 2008 comme langage de développement et on termine par établir une série de tests pour valider les fonctionnalités de notre Firewall et pour cela on a choisit d'utiliser un cheval de Troie qui est Back orifice 2000 « Bo2k ».

Ce qui concerne l'organisation, ce rapport est divisé en cinq (05) chapitres :

Dans le premier chapitre nous présenterons les vulnérabilités système et les attaques réseau les plus fréquentes.

Le chapitre deux (02) est réservée pour les généralités sur la sécurité informatique : ses objectifs, ses critères, ses outils et quelques protocoles de sécurité.

Le chapitre trois (03) est consacré à étudier un des outils de la sécurité informatique : le Firewall, notamment ses fonctionnalités, ses types, et sa place dans une architecture de sécurité.

A la suite de ce chapitre, on présentera la conception et l'implémentation de notre Firewall, en utilisant un langage de modélisation mondial l'UML. La solution présentée dans ce rapport est basée sur un filtreur de paquets, un Sniffer et un scanner de port. Et pour finir, une conclusion générale comme récapitulatif.

PRESENTATION DE L'ORGANISME D'ACCUEIL :

ALGERIE TELECOM :

ALGERIE TELECOM est leader sur le marché Algérien des télécommunications qui connait une forte croissance. Offrant une gamme complète de services de voix et de données aux clients résidentiels et professionnels.

Elle s'engage dans le monde des Technologies de l'Information et de la Communication avec trois objectifs:

- **Rentabilité**
- **Efficacité**
- **Qualité de service**

Son ambition est d'avoir un niveau élevé de performance technique, économique, et sociale pour se maintenir durablement leader dans son domaine, dans un environnement devenu concurrentiel.

Missions et objectifs :

L'activité majeure d'Algérie Télécom est de :

- Fournir des services de télécommunication permettant le transport et l'échange de la voix, de messages écrits, de données numériques, d'informations audiovisuelles, …
- Développer, exploiter et gérer les réseaux publics et privés de télécommunications ;
- Etablir, exploiter et gérer les interconnexions avec tous les opérateurs des réseaux.

RMS - Réseau Multiservices :

Le RMS est un réseau multiservices de nouvelle génération NGN, de type IP/MPLS et d'envergure nationale.

Pourquoi le NGN ?

- Simplifier les réseaux (l'architecture).
- Réduire les investissements.
- Réduire les coûts de fonctionnement.
- Proposer de nouveaux services.

Les avantages du RMS :

La solution de raccordement des sites sur notre Backbone RMS permet de garantir et d'offrir:

- Le débit
- La fiabilité
- La qualité de service QOS
- La sécurité
- La disponibilité
- L'extensibilité et la souplesse
- La Redondance (E1 ou DSL)
- De nouveau services (VOIP, Internet, vidéoconférence, ….)

Chapitre 1 :

Vulnérabilité et attaques réseau

1.1. Introduction :

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

Pour parer à ces problèmes il est nécessaire de connaître les différentes menaces existantes, ainsi que les vulnérabilités présentes sur un tel système, pour établir une stratégie de sécurité fiable contre ces attaques.

Donc dans ce premier chapitre on étudiera les différentes faiblesses du système, et les attaques exploitants ces failles. Cette investigation va nous permettre par la suite d'étudier les étapes nécessaires pour mener une stratégie de sécurité fiable.

1.2. Pourquoi les systèmes sont vulnérables ?

- La sécurité est chère et difficile. Les organisations n'ont pas de budget pour ça.
- La sécurité ne peut être sûre à 100%, elle est même souvent inefficace.
- La politique de sécurité est complexe et basée sur des jugements humains.
- Les organisations acceptent de courir le risque, la sécurité n'est pas une priorité.
- De nouvelles technologies (et donc vulnérabilités) émergent en permanence.
- Les systèmes de sécurité sont faits, gérés et configurés par des humains.

1.3. Attaques via Internet :

1.3.1. Quelques définitions :

➢ ***Vulnérabilité*** :

Peut-être matériel ou logique, c'est une faiblesse dans les procédures automatisées de sécurité de système, commandes administratives, disposition physique, commandes internes et ainsi de suit, qui pourraient être exploité par une menace pour gagner l'accès non autorisé à l'information ou perturber un traitement critique [1].

➢ ***Menace :***

Une menace est « une potentielle violation de la sécurité », elle cause vulnérabilités et faiblesses d'un système, une menace n'est pas dangereuse en soi, seulement quand une attaque est lancée on l'utilisant, elle comprend les éléments suivants :

- Destruction d'information et/ou d'autres ressources.
- Corruption ou modification d'informations.
- Vol, suppression ou perte d'informations et/ou d'autres ressources.
- Divulgation d'informations.
- Interruption de services.

Les menaces peuvent être classées en deux catégories.

- *Les menaces accidentelles* :

Elles sont celles qui existent sans qu'il y ait préméditation. Des exemples de menaces accidentelles qui se sont concrétisées sont : défaillance de système, bévues opérationnelles et bogue de logiciels. Un exemple concret de ce type de menaces serait l'envoi par un utilisateur d'un mail confidentiel à la mauvaise personne par erreur.

- *Les menaces intentionnelles (ou attaques) :*

Elles peuvent aller de l'examen fortuit, utilisant des outils de contrôle facilement disponibles, aux attaques sophistiquées, utilisant une connaissance spéciale du système. Une menace intentionnelle qui se concrétise peut être vue comme une « attaque ».

➢ ***Intrusion :***

C'est la pénétration par violence ou par ruse de personnes non autorisé dans une zone délimitée, avec intension de vol, de dommage ou d'abus [2].

➢ ***Hacking (piratage) :***

Le hacking est un ensemble de techniques informatiques, visant à attaquer un réseau, un site, … [3]

➢ ***Hacker (pirate) :***

Un hacker est une personne qui quelle que soit sa motivation, pénètre sans autorisation et de manière illégale, dans un système appartenant à tiers [3].

➢ ***Attaque :***

Une « attaque » est l'exploitation d'une faille d'un système informatique à des fins non connues par l'exploitant du système et généralement préjudiciables [4].

1.3.2. Motivation des attaques :

Comprendre les raisons pouvant motiver une attaque fournit parfois les indications sur les points de vulnérabilité d'un réseau et les actions qu'un intrus pourrait entreprendre. Parmi les motivations les plus courantes, on retrouve les suivantes [5] :

➢ ***Cupidité :***

L'intrus est payé par quelqu'un pour s'introduire sur un réseau d'entreprise afin d'y dérober ou endommager des informations relatives à l'échanges d'importantes somme d'argent.

- ***Curiosité :***

L'intrus est calé en informatique et curieux, et tente d'obtenir un accès aux sites qui lui semblent intéressants.

- ***Notoriété :***

L'intrus est très calé en informatique et tente de s'introduire sur des sites connus pour être difficiles à forcer pour prouver ses compétences. Une attaque réussie peut alors lui valoir le respect et la reconnaissance de ses pairs.

- ***Vengeance :***

L'intrus a été licencié, rétrogradé ou traité de façon déloyale par un employeur et entreprend une attaque dans le but de détruire des informations sensibles.

- ***Ignorance :***

L'intrus s'intéresse à l'informatique et aux réseaux et tombe par inadvertance sur une vulnérabilité, causant involontairement des préjudices en détruisant des données ou en réalisant une action illégale.

1.3.3. Etapes de réalisation d'une attaque :

Tous les pirates procèdent ces étapes pour réussir leurs attaques :

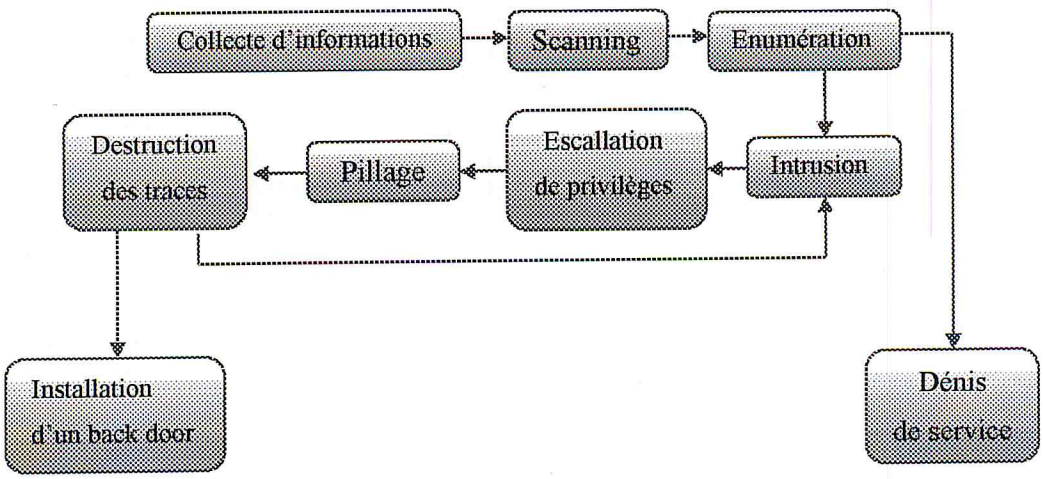


Figure 1.1 Etapes de piratage

- ***Collecte d'information (footprinting):***

Avant de pouvoir attaquer sa cible, le pirate doit faire une reconnaissance afin de découvrir ou se trouve les machines de la cible et par quels moyens elles sont atteignables. [6]

- ***Scan :***

Une fois que le pirate a identifié les réseaux appartenant à sa cible, il peut scanner la partie qui l'intéresse. A partir des réponses il peut trouver à quelle adresse il y a des machines qui répondent et quels sont les ports qui sont accessibles sur ces machines. En fonction des comportements exacts des machines il est aussi possible d'identifier le système d'exploitation de certaines machines. [6]

- ***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. [6]

- ***Intrusion :***

Le pirate doit trouver une vulnérabilité qui est connue mais qui n'est pas encore corrigée sur la cible. Un pirate doué pourra développer un exploit spécifique à sa cible. [6]

- ***Dénis de service :***

Le pirate peut lancer un déni de service (voir plus loin). Il est souvent plus facile de trouver une vulnérabilité qui permet l'exécution d'un déni de service qu'une vulnérabilité qui permet de s'introduire dans la cible. [6]

➢ ***Escalation des privilèges :***

Ayant obtenu l'accès au système, l'intrus utilise une autre vulnérabilité pour élever ses privilèges jusqu'à l'obtention des droits d'accès désirées. [6]

➢ ***Pillage :*** [6]

Le pirate peut maintenant voler des informations confidentielles (par exemple : n° carte de crédit) ou modifier des informations afin d'obtenir frauduleusement les services. Le pirate peut aussi utiliser ses privilèges pour trouver des mots de passes et des informations afin d'obtenir un accès à d'autres systèmes.

➢ ***Destruction des traces :***

Grace aux privilèges d'administrateur l'intrus peut effacer toute trace de son intrusion afin de ne pas éveiller des soupçons. Car par exemple les requêtes ayant provoqué un débordement (over flow) seront enregistré dans les logs de serveur ainsi que l'adresse IP à partir du quelle elles ont été lancées. Avec ces privilèges, le pirate peut réarranger tous les logs de sa cible pour masquer son intrusion. [6]

➢ ***Mise en place d'une porte d'accès dérobée :*** [6]

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

1.3.4. Typologie des attaques :

Il existe trois (03) classifications majeures d'attaques :

➢ ***Première classification :*** **[7]**

- *Attaque passive :*

Ne change pas les ressources du système, mais ont pour vocation de collecter l'information. Ce genre d'attaque est difficile à détecter.

- *Attaque active :*

Sont plus facile à détecter par ce que souvent ce type d'attaque laisse des traces, la majorité des attaques de sécurité sont actives.

➢ ***Deuxième classification :*** [7]

- *Attaque directe :*

C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son ordinateur.

La plupart des pirates débutants utilisent cette technique. En effet, les programmes de hack qu'ils utilisent ne sont que faiblement paramétrable, et un grand nombre de ces logiciels envoient directement les paquets à la victime.

Figure 1.2 : Attaque directe

- *Attaque indirecte :*

✓ **Par rebond** :

Le principe en lui même, est simple : Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime. D'où le terme de rebond.

❖ Avantage :

- Masquer l'identité (l'adresse IP) du hacker ;
- Eventuellement, utiliser les ressources de l'ordinateur intermédiaire

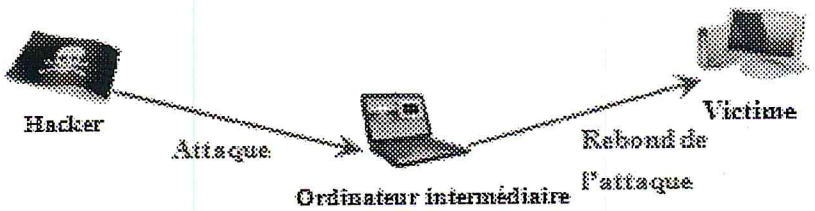


Figure 1.3 : Attaque indirecte par rebond

✓ **Par réponse :**

Cette attaque est une dérivée de l'attaque par rebond. Elle offre les mêmes avantages, du point de vue du hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.

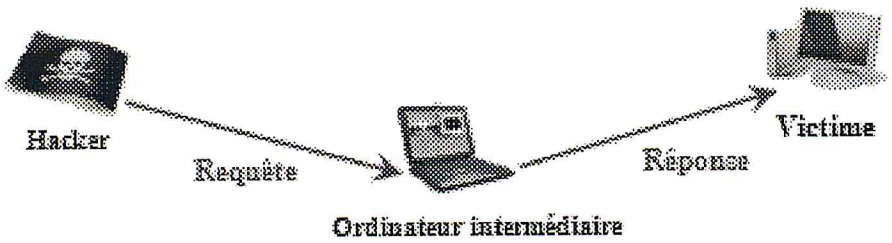


Figure 1.4 : Attaque indirecte par réponse

➢ ***Troisième classification :*** **[7]**

Selon la cible concernée par l'attaque, on peut différencier deux (02) types d'attaques :

- *Les attaques réseau :*

Leur but principal est d'empêcher les utilisateurs d'utiliser une connexion réseau, de rendre indisponible une machine ou un service et de surveiller le trafic réseau afin de l'analyser et d'en récupérer des informations pertinentes.

- *Les attaques système :*

Se sont des attaques qui portent atteinte au système comme par exemple effacer des fichiers critiques (tel que les fichiers password) ou modifier la page web d'un site dans le but de le discréditer ou simplement le ridiculiser.

1.3.5. Quelques techniques d'attaques :

De manière à pouvoir décrire précisément un certains nombre d'attaque, un recensement des grands types de menaces apparaît indispensable.

➢ ***Exemple de techniques en vue d'obtenir des informations :***

- *Social engenieering :*

Dans tout système informatisé, la première faille est toujours la composante humaine. Il est tellement plus facile de tromper un humain qu'une machine correctement sécurisée.

Elle consiste surtout à se faire passer pour quelqu'un que l'on n'est pas et de demander des informations personnelles (login, mot de passe, accès, numéro, données, ...) en inventant un quelconque motif (plantage de réseau, modification de celui-ci,...). Elle se fait soit au moyen d'une simple communication téléphonique soit par mail. [7]

- *Sniffing :*

Les sniffings sont des dispositifs, logiciels ou matériels, qui capturent les paquets qui circulent sur un réseau. Leurs objectifs principaux est d'analyser les données qui circulent dans le réseau et identifier les zones les moins sécurisées. [7]

- *Scaning :*

Le scaning est une technique utilisée pour rechercher les machines actives et déterminer les ports ouvert et fermés sur ces machines, et donc identifier les services qui écoutent sur ces ports. [7]

➢ ***Exemple de techniques en vue d'obtenir des droits :***

- *Spoofing:*

Le spoofing est une technique qui permet à une machine d'être authentifiée auprès d'une autre au moyen de paquets semblant émaner d'une adresse source approuvée. [7]

- *Perceurs de mots de passe (crackers):*

Un perceur de mot de passe est tout programme qui permet de violer une stratégie de sécurité en découvrant les mots de passes initialement cryptés. En général, ces programmes sont des moteurs agissants en force (Brut Force Engine), testant les mots de passe les uns après les autres à une grande vitesse. Ces programmes arrivent parfois à trouver les bons codes principalement en raison des négligences des utilisateurs dans le choix de leurs mots de passe. [7]

➢ ***Exemple de techniques visant à perturber ou détruire :***

- *Le déni de service (DoS) :*

Un déni de service DoS est une action qui empêche ou altère l'utilisation autorisée de réseau, des systèmes ou des applications en épuisant des ressources telles que les unités centrales de traitement (CPU), la mémoire, la largeur de bande et l'espace disque. [7]

1.4. Conclusion :

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

Dans le passé réaliser une attaque contre un système informatique était une tâche très difficile qui demande beaucoup d'expérience, mais avec l'avènement de l'Internet, des outils d'attaques sont devenus à la portée de tout le monde.

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

Chapitre 2 :

La sécurité informatique

2.1. Introduction :

La sécurité informatique est devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet.

La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place des réseaux informatiques. Ce chapitre a pour but de présenter globalement les principaux critères et outils de la sécurité qui vont nous permettre par la suite d'étudier les étapes nécessaires pour mener une stratégie de sécurité fiable.

2.2. Définition de la sécurité informatique :

La sécurité informatique est la capacité d'un système de protéger ses objets contre leur modification ou leur utilisation par des personnes non autorisées [8].

Le risque en termes de sécurité est généralement caractérisé par l'équation suivante :

$$Risque = \frac{Vulnérabilité \times Menace}{Contre - Mesure}$$

La sécurité informatique utilise un vocabulaire bien défini, il est nécessaire de définir certains termes :

- **La menace** « threat » **:** représente le type d'action susceptible de nuire dans l'absolu ;
- **La vulnérabilité:** représente le niveau d'exposition face à la menace dans un contexte particulier ;
- **La contre-mesure :** est l'ensemble des actions mises en œuvre en prévention de la menace.

2.3. Critères fondamentaux de la sécurité:

La sécurité informatique se base sur un certain nombre de services qui permettent de mettre en place une réponse appropriée à chaque menace :

2.3.1. Confidentialité : [9]

Elle assure la non divulgation des données à des personnes non autorisées.

2.3.2. Authentification :

Ce critère permet d'authentifier des entités qui communiquent entre elles, il a pour but de garantir l'identité des correspondants. **[9]**

2.3.3. Intégrité :

Contre les attaques actives en offrant une protection efficace qui pourrait être dérivée de l'observation des flux de données. **[9]**

2.3.4. Non répudiation :

La répudiation est la possibilité pour une des entités impliquée 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. **[9]**

2.3.5. Contrôle d'accès :

Est un critère de protection contre l'usage non autorisé des ressources accessibles par le réseau. Ce critère utilise le service authentification afin de s'assurer de l'identité des correspondants échangés lors de la phase d'initialisation des dialogues. **[9]**

2.3.6. Disponibilité :

L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources. **[9]**

2.4. Objectif de la sécurité informatique :

La sécurité informatique à plusieurs objectifs, bien sûr liés aux types de menaces ainsi qu'aux types de ressources, etc... Néanmoins, les points principaux sont les suivants [3]:

- empêcher la divulgation non-autorisée de données
- empêcher la modification non-autorisée de données
- empêcher l'utilisation non-autorisée de ressources réseau ou informatiques de façon générale

2.5. Politique de la sécurité :

La sécurité des systèmes d'information se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système, en mettant en place des mécanismes d'authentification et de contrôle. Ces mécanismes permettent d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leurs ont été octroyés.

La sécurité informatique doit toutefois être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance. C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, c'est-à-dire :

- élaborer des règles et des procédures, installer des outils techniques dans les différents services de l'organisation (autour de l'informatique) ;
- définir les actions à entreprendre et les personnes à contacter en cas de détection d'une intrusion ;
- sensibiliser les utilisateurs aux problèmes liés à la sécurité des systèmes d'informations ;
- préciser les rôles et responsabilités.

La politique de sécurité est donc l'ensemble des orientations suivies par une entité en termes de sécurité. À ce titre, elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.

2.6. Quelques protocoles de sécurité :

- ***SHTTP :*** (Secure HyperText Transport Protocol)

Il a été conçu pour sécuriser les messages qui utilisent le protocole HTTP. Il préserve les caractéristiques de HTTP tout en permettant aux messages de requête et de réponses d'être signés, authentifiés, cryptés, ou toute autre combinaison de ces fonctions. [5]

- ***SSL*** (Secure Socket Layer) *:*

Est un protocole ouvert développé par Netscape. Il fournit un mécanisme pour garantir la sécurité des données implémentée entre les protocoles de niveau application (http, Telnet…) et TCP/IP. Il assure le chiffrement des données, l'authentification de serveur, l'intégrité des messages et l'authentification optionnelle de clients pour une connexion TCP/IP. L'objectif principal de SSL est d'assurer la confidentialité et la fiabilité entre deux applications communiquant. [5]

- ***IPSec*** (IP Security)*:*

Est un protocole destiné à fournir différents services (critères) de sécurité. Il propose ainsi plusieurs choix et options qui lui permettent de répondre de façon adaptée aux besoins des entreprises, nomades, extranets, particuliers, etc... Néanmoins, son intérêt principal reste sans conteste son mode dit de tunneling, c'est-à-dire d'encapsulation d'IP qui lui permet entre autres choses de créer des réseaux privés virtuels.

IPsec est facultatif sur IPv4 mais est obligatoire sur IPv6. IPsec a d'autres avantages que la sécurisation du trafic, il permet par exemple d'économiser la bande passante grâce à la compression des en-têtes des paquets. IPsec est composé de plusieurs protocoles différents : AH, ESP, IPcomp et IKE. [5]

- *Le protocole AH :*

Le protocole AH (Authentification Header) permet de garantir l'authenticité des paquets échangés en leur inscrivant une somme de contrôle (de l'en-tête IP jusqu'à la fin du paquet) chiffrée. [5]

- *Le protocole ESP :*

Le protocole ESP (Encapsulating Security Payload) encrypte toutes les données du paquet garantissant leur confidentialité. [5]

- *Le protocole IPcomp :*

Le protocole IPcomp (IP payload compression) permet de compresser un paquet avant de le chiffrer avec ESP. [5]

- *Le protocole IKE :*

Le protocole IKE (Internet Key Exchange) est utilisé pour l'échange des clés utilisées pour l'encryptage. [5]

2.7. Outils de sécurité:

➢ **Système de détection d'intrusion :**

Mécanisme de sécurité permettant la détection d'intrusion en temps réel au niveau d'un réseau informatique.

➢ **Antivirus :**

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer les logiciels malveillants (dont les virus ne sont qu'un exemple) qui se basent sur l'exploitation de failles de sécurité.

- **Firewall :**

Un firewall (pare-feu) est un système, logiciel ou matériel, qui a pour fonction de contrôler le trafic et les flux d'applications entre différents réseaux.

- **Réseau privé virtuel (VPN) :**

Le VPN (pour Virtual Private Network) est une technologie qui permet à un ordinateur distant d'avoir, via Internet, un accès direct et totalement sécurisé à un autre ordinateur ou à un réseau local.

- **Biométrie :**

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques. Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu.

- **Cryptographie :**

La cryptographie est une science permettant de convertir des informations "en clair" en informations codées, c'est à dire non compréhensible, puis, à partir de ces informations codées, de restituer les informations originales.

2.8. Conclusion :

Il existe aujourd'hui très peu de systèmes sûrs en dehors de l'industrie militaire ou de quelques domaines spécialisés (multinationale investissant un grand budget pour la sécurité de leur installation informatique).

La sécurité joue un rôle très particulier par ce que la moindre défaillance peut compromettre le bon fonctionnement du système.

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

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 3 :

Les Firewalls

3.1. Introduction :

Chaque ordinateur connecté à internet (et d'une manière plus générale à n'importe quel réseau informatique) est susceptible d'être victime d'une attaque d'un pirate informatique. La méthodologie généralement employée par les pirates informatiques consiste à scruter le réseau (en envoyant des paquets de données de manière aléatoire) à la recherche d'une machine connectée, puis à chercher une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant.

Ainsi, il est nécessaire, autant pour les réseaux d'entreprises que pour les internautes possédant une connexion de type câble ou ADSL, de se protéger des intrusions réseaux en installant un dispositif de protection tel que le Firewall.

Dans ce chapitre on se concentrera à étudier les différentes fonctionnalités de ce dernier, ainsi que son positionnement dans une telle architecture, et on finira par étudier ses limites.

3.2. Définition d'un Firewall

Un Firewall (appelé aussi coupe-feu ou pare-feu en français) est indispensable. C'est un système qui permet de protéger un ordinateur ou un réseau des attaques qui proviennent d'un autre réseau, notamment Internet.

Le système Firewall est un système logiciel (parfois également matériel) constituant un intermédiaire entre le réseau local et le monde extérieur. Dans le cas où la zone protégée se limite à l'ordinateur sur lequel le Firewall est installé, on parle de Firewall personnel.

3.3. Fonctionnement d'un système Firewall :

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow)
- De bloquer la connexion (deny)
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- soit d'autoriser uniquement les communications ayant été explicitement autorisées.
- soit d'empêcher les échanges qui ont été explicitement interdits.

3.3.1. Fonctionnalité de filtrage :

➢ ***Le filtrage simple de paquet (Stateless) :***

C'est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI[1], elle consiste à accorder ou refuser le passage de paquets d'un réseau à un autre en se basant sur :

- L'adresse IP Source/Destination.
- Le numéro de port Source/Destination.
- Et bien sur le protocole des niveaux 3 ou 4.

Cette interprétation conditionnelle « si ce type de paquet est rencontré, faire cela **(soit l'accorder ou le refuser)**», sont appelées des *règles de filtrage.* Généralement, lorsqu'on installe un Firewall, on implémente des règles qui reflètent la politique d'accès de l'organisation. [10]

➢ ***Le filtrage de paquet avec état (Stateful) :***

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 DoS et une protection au courrier SMTP, ainsi que d'autre fonctionnalités de sécurité. [10]

[1] Voir l'annexe

➢ ***Le filtrage applicatif (ou pare-feu de type proxy ou proxying applicatif)***

Les Firewalls basés sur ce type de filtrage sont appelés Proxy Firewalls ou passerelle applicative. Lorsqu'un utilisateur distant contacte un réseau exécutant un Firewall proxy, celui-ci intercepte la connexion. Dans ce cas, les paquets IP ne sont pas transmis directement au réseau interne, mais subissent une sorte de traduction, le Firewall jouant le rôle de canal et d'intercepteur (**voir *figure 3.1***). [10]

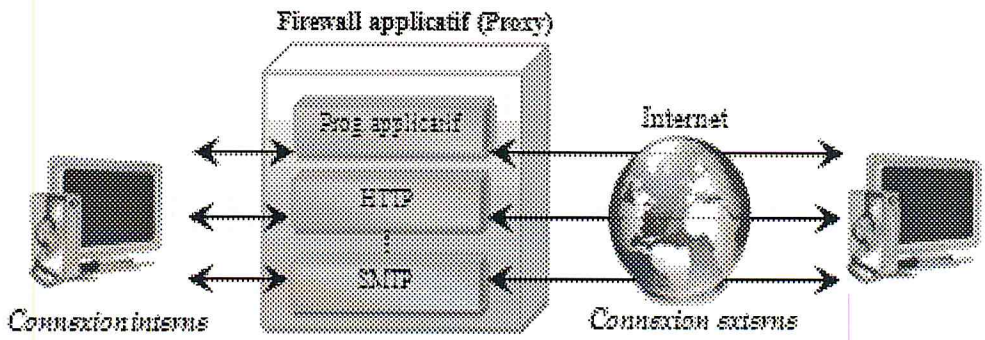


Figure 3.1 : Exemple de Firewall proxy

3.3.2. La traduction d'adresses réseau :

Le service « NAT: Network Address Translation » sert souvent à mettre en correspondance des blocs d'adresse illégaux ou réservés avec des blocs valides (par exemple, 10.0.100.3 avec 206.246.131.227). Même si la NAT n'est pas nécessairement une caractéristique de sécurité, les premiers dispositifs NAT qui apparaissent en entreprise sont souvent des produits Firewall.

3.3.3. L'équilibrage de charge

La plus générique de toutes, l'expression *équilibrage de charge,* est l'art de segmenter un trafic de façon répartie. Certains Firewalls permettent désormais d'orienter le trafic Web et FTP de cette façon.

3.3.4. La tolérance de pannes (Fail over) :

Certains Firewall parmi les plus aboutis, comme Cisco PIX et l'union Nokia/Checkpoint, supportent des fonctionnalités assez complexes. Souvent reconnues comme étant des dispositifs élevés, les fonctionnalités de tolérance de pannes sophistiquées permettent souvent d'exécuter les Firewall par paire, l'un des dispositifs fonctionnant comme une « réserve chaude » en cas de panne de l'autre.

3.4. Types de Firewalls :

3.4.1. Les Firewalls bridge

Ces derniers sont relativement répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de Firewall. Leurs interfaces ne possèdent pas d'adresse IP, et ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le Firewall est indétectable pour un hacker lambda. [10]

- ***Avantages***
  - ✓ Impossible de l'éviter (les paquets passeront par ses interfaces)
  - ✓ Peu coûteux

- ***Inconvénients***
  - ✓ Possibilité de le contourner (il suffit de passer outre ses règles)
  - ✓ Configuration souvent contraignante
  - ✓ Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless).

3.4.2. Les Firewalls matériels

Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco ou Nortel. Intégrés directement dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement difficile, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée de par leur présence sur le même équipement réseau. [10]

- ***Avantages***
  - ✓ Intégré au matériel réseau
  - ✓ Administration relativement simple
  - ✓ Bon niveau de sécurité

- ***Inconvénients***
  - ✓ Dépendant du constructeur pour les mises à jour
  - ✓ Souvent peu flexibles.

3.4.3. Les Firewalls logiciels

Présents à la fois dans les serveurs et les routeurs « faits maison », on peut les classer en plusieurs catégories : [10]

- ***Les Firewalls personnels***

Ils sont assez souvent commerciaux et ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs. Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés. En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que vers l'exhaustivité, afin de rester accessible à l'utilisateur final.

- ***Avantages***
  - ✓ Sécurité en bout de chaîne (le poste client)
  - ✓ Personnalisable assez facilement

- ***Inconvénients***
  - ✓ Facilement contournable
  - ✓ Difficiles à départager de par leur nombre énorme.

- ***Les Firewalls plus « sérieux »***

Tournant généralement sous linux, car ce SE offre une sécurité réseau plus élevée et un contrôle plus adéquat, ils ont généralement pour but d'avoir le même comportement que les Firewalls matériels des routeurs, à ceci prêt qu'ils sont configurables à la main. Le plus courant est iptables (anciennement ipchains), qui utilise directement le noyau linux.

- ***Avantages***
  - ✓ Personnalisables
  - ✓ Niveau de sécurité très bon
- ***Inconvénients***
  - ✓ Nécessite une administration système supplémentaire

3.5. Architecture d'un Firewall :

3.5.1. Hôte Bastion

Tout système exécutant un Firewall de niveau application dont le rôle est critique dans la sécurité du réseau est appelé machine bastion. Ce système est alors spécifiquement conçu pour être fortement protégé et résister au maximum d'attaques possible. Ainsi, la machine bastion exécute le plus souvent une version sécurisée de son système d'exploitation, spécifiquement protégée contre certaines vulnérabilités.

Il existe 4 configurations possibles, mais les architectures complexes (les 3 dernières) sont les plus utilisées. [9]

3.5.2. Firewall avec routeur de filtrage des paquets « Packet-Filtering Router Firewall »

La manière la plus simple et la plus commune de réaliser un Firewall consiste uniquement à relier son réseau privé à l'Internet par l'intermédiaire d'un routeur de filtrage des paquets (***Figure 3.2***). Celui-ci réalise donc les opérations de routages habituelles d'un routeur, plus des opérations de filtrage au niveau des paquets IP.

Figure 3.2 : L'architecture « Firewall avec routeur de filtrage de paquets »

3.5.3. Hôte à écran « Single-Homed Bastion Host » :

Dans cette architecture (***Figure3.3***), le Firewall consiste en deux systèmes : un routeur de filtrage de paquets et un hôte bastion. Généralement le routeur est configuré comme suit :

- Pour le trafic depuis l'internet, on *autorise* seulement *les paquets destinés à l'hôte bastion* ;
- Pour le trafic depuis le réseau interne, on *autorise* seulement *les paquets IP provenant de l'hôte bastion.*

Cette architecture procure une plus grande sécurité que celle définie par un routeur de filtrage de paquet ou une passerelle de niveau application, et cela est pour deux raisons : D'abord, cette architecture assure un filtrage au niveau paquet et applicative, permettant une flexibilité considérable dans la définition de la politique de sécurité. Deuxièmement, un intrus doit pénétrer deux systèmes distincts avant que la sécurité du réseau ne soit mise en danger.

Mais si le routeur ne remplit plus sa fonction, le trafic peut s'écouler directement par le routeur entre l'Internet et d'autres hôtes sur le réseau privé.

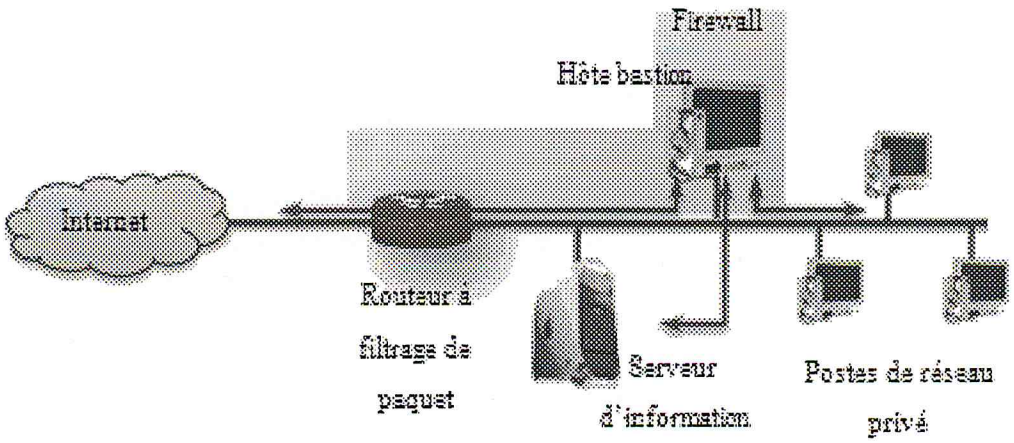


Figure 3.3 : L'architecture « Hôte à écran »

3.5.4. Hôte à double réseau « Dual-Homed Bastion Host »

Ce système fournit la solution au problème posé par l'hôte **à écran** : une machine bastion à deux interfaces relie le réseau privé au **routeur de filtrage des paquets** (***Figure3.4***). Non seulement elle ne peut plus être évitée par un client extérieur qui tenterait de se connecter au réseau protégé, mais cette architecture impose aussi aux utilisateurs internes de passer obligatoirement par la machine bastion [9]

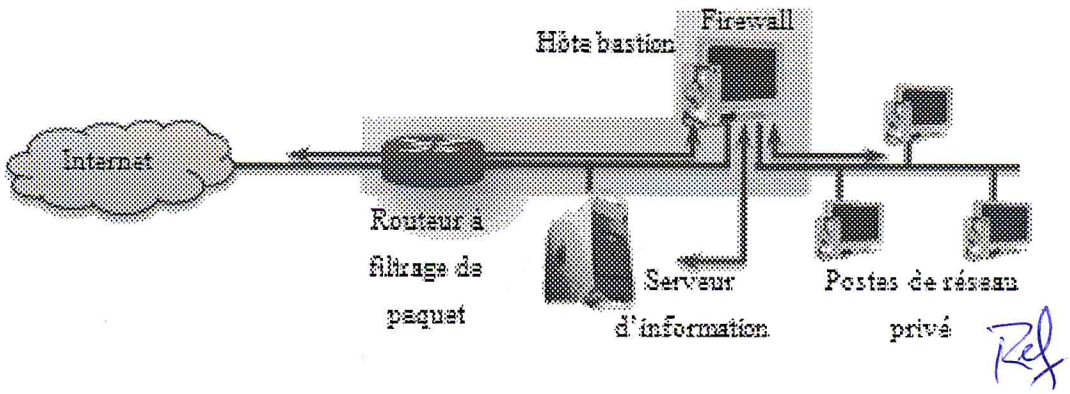


Figure 3.4 : L'architecture « Hôte à double réseaux »

3.5.5. Sous-réseau à écran « Screened-Subnet Firewall » :

L'architecture de la ***figure 3.5*** est la plus sûre de celles que nous avons considérées. Dans cette architecture, deux routeurs de filtrage des paquets sont employés, l'un entre l'hôte bastion et l'Internet et l'autre entre l'hôte bastion et le réseau interne. Cette architecture crée un sous réseau isolé, qui peut se limiter au seul bastion, mais peut aussi inclure un ou plusieurs serveurs d'information avec les modems associés, cette zone entre un intranet et l'Internet est appelée « zone démilitarisée ».

> **DMZ « DeMilitarized Zone »est une zone du réseau semi-protégée. Cette zone est normalement délimitée par des contrôles d'accès au réseau tels que des Firewalls ou des routeurs dont les filtres sont finement paramétrés. Généralement tous les systèmes auxquels un utilisateur externe peut accéder doivent être placés dans la DMZ** [9]

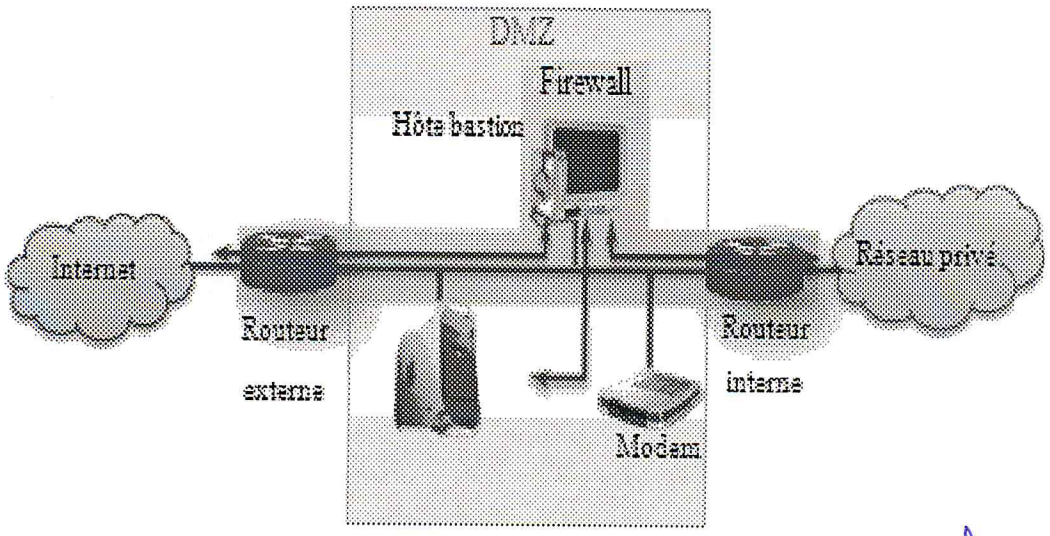


Figure 3.5 : L'architecture « Sous-réseau à écran »

3.6. Limites d'un Firewall :

Malgré qu'un Firewall permet de restreindre l'accès à un point unique, mais il reste incapable devant certains situations [11] :

- ***La protection contre la menace interne :***

Les utilisateurs internes ayant accès à une ressource non protégée peuvent voler ou détruire des données sans jamais approcher le Firewall.

- ***La protection contre des connexions ne passant pas par le Firewall :***

Un Firewall ne peut contrôler efficacement que le trafic qui passe par lui : il ne peut systématiquement rien faire contre les connexions qui lui échappe. Il est fréquent de constater que des utilisateurs « experts » ou administrateurs mettent en place leur propre « entrée de service » à l'intérieur du réseau.

- ***La protection contre les menaces nouvelles :***

Un Firewall est destiné à protéger le réseau de l'entreprise contre des menaces connues. La mise en place d'un Firewall doit impérativement s'accompagner d'une politique de mise à jour régulière.

➢ ***La protection contre les virus :***

L'examen des flux traversant un Firewall s'effectue surtout par examen des adresses source et destination ainsi que des numéros de port mais pas sur le détail des données. Même avec le filtrage de paquets sophistiqués la protection contre les virus à l'aide d'un Firewall est difficilement réalisable. C'est pour ça que la mise en place d'un Firewall doit s'accompagner de la mise en place d'un anti-virus.

➢ ***La fragmentation de paquet :***

On peut facilement échapper à un Firewall avec une simple fragmentation de paquets

3.7. Conclusion :

Comme on peut le constater, les Firewalls possèdent de multiples capacités qui peuvent différer en fonction de leurs types. Cette multitude de solutions impose donc une étude rigoureuse de la sécurité devant être mise en place.

Il est également nécessaire de préciser que le Firewall est seulement un composant de sécurité, il ne protégera donc pas à lui seul un réseau. Il est nécessaire de l'inclure dans une démarche qui prendra en compte d'autres paramètres.

Chapitre 4 :

Conception et mise en œuvre

4.1. Introduction

Il n'est pas facile de réaliser un processus proxy pour chaque protocole de la couche applicative, ni de conserver les traces des connexions, pour cela nous avons opté pour la fonctionnalité de filtrage qu'offre un système Firewall le type de *filtrage statique*.

Dans ce chapitre nous allons parler de l'analyse des besoins et la conception du Firewall, pour cela on a choisit d'utiliser UML (Unified Modeling Langage).

On va détailler les étapes suivies en mentionnant les méthodes et les outils utilisés pour réaliser nos objectifs.

4.2.Méthode de développement

4.2.1. Les étapes suivies :

Pour réaliser notre projet, nous avons suivi les étapes suivantes:

- Définition et analyse des besoins.
- Conception du système.
- Implémentation du système.
- Intégration des tests globaux.
- Installation.
- Maintenance.

4.2.2. Définition et analyse des besoins :

Dans cette étape on va déterminer les objectifs et les fonctionnalités attendues de notre système « Firewall ». Pour exprimer les besoins, on a utilisé les diagrammes ***USE CASE*** du langage UML.

Le but de notre projet est de réaliser les modules suivants :

- Un filtreur de paquets ;
- Un analyseur de réseau (Sniffer) ;
- Un analyseur de ports (port scanner) ;
- Un mappeur de ports (port mapper) ;

Les éléments importants d'un diagramme de cas d'utilisation sont :

L'*acteur* et le *cas d'utilisation*.

On distingue dans le cadre de ce projet un seul type d'acteur c'est l'***utilisateur*** direct du système, et les cas d'utilisations sont représentés à travers les diagrammes des ***figures 1, 2, 3*** et ***4***.

- *Diagramme de cas d'utilisation global :*

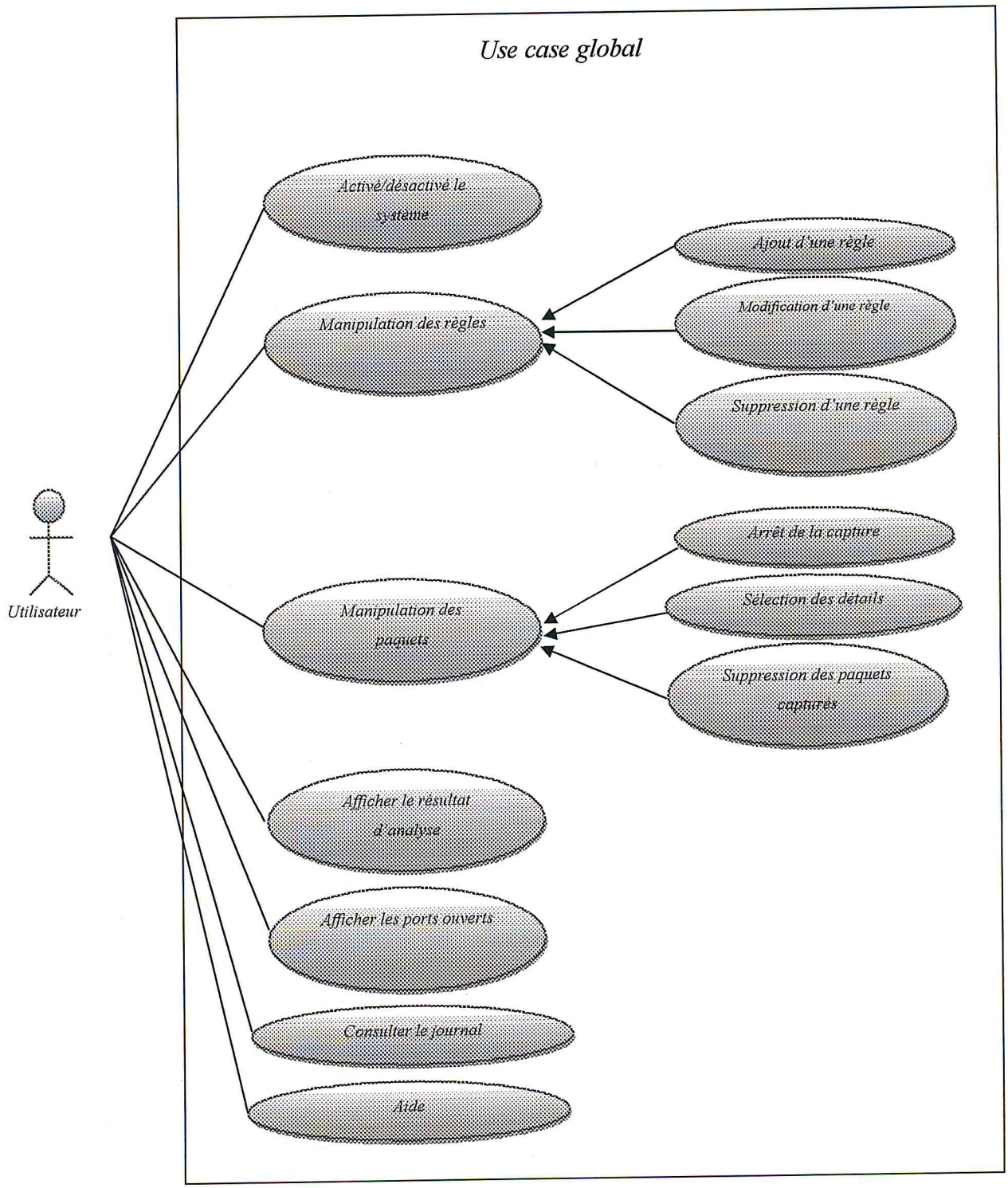


Figure 4.1 : Diagramme cas d'utilisation « global »

- *Filtreur de paquet :*

Ce module permet d'ajouter ou de supprimer des filtres (règle de filtrage).

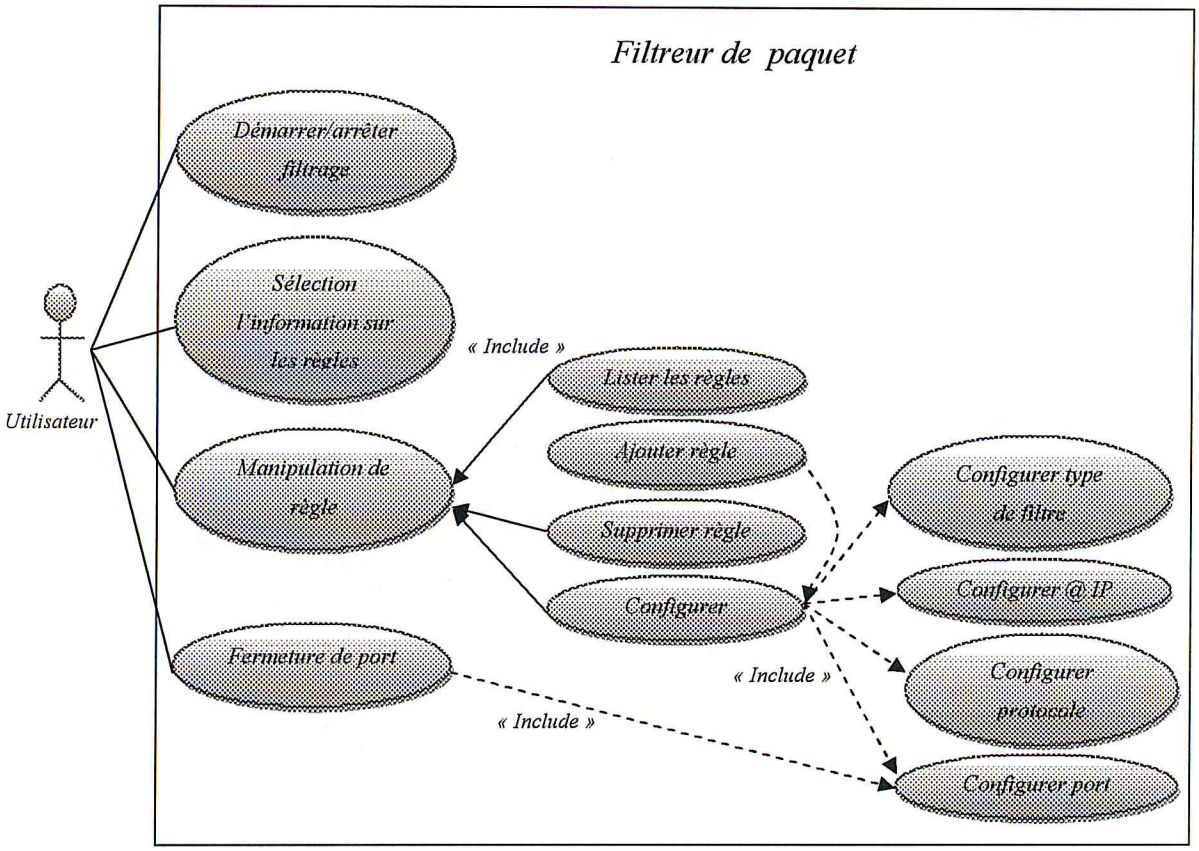


Figure 4.2: Diagramme cas d'utilisation « Filtreur de paquet »

- *Analyseur de trafic « Sniffer » :*

Ce module permet de lancer/arrêter la capture des paquets/datagrammes circulant dans le réseau local selon les configurations mises.

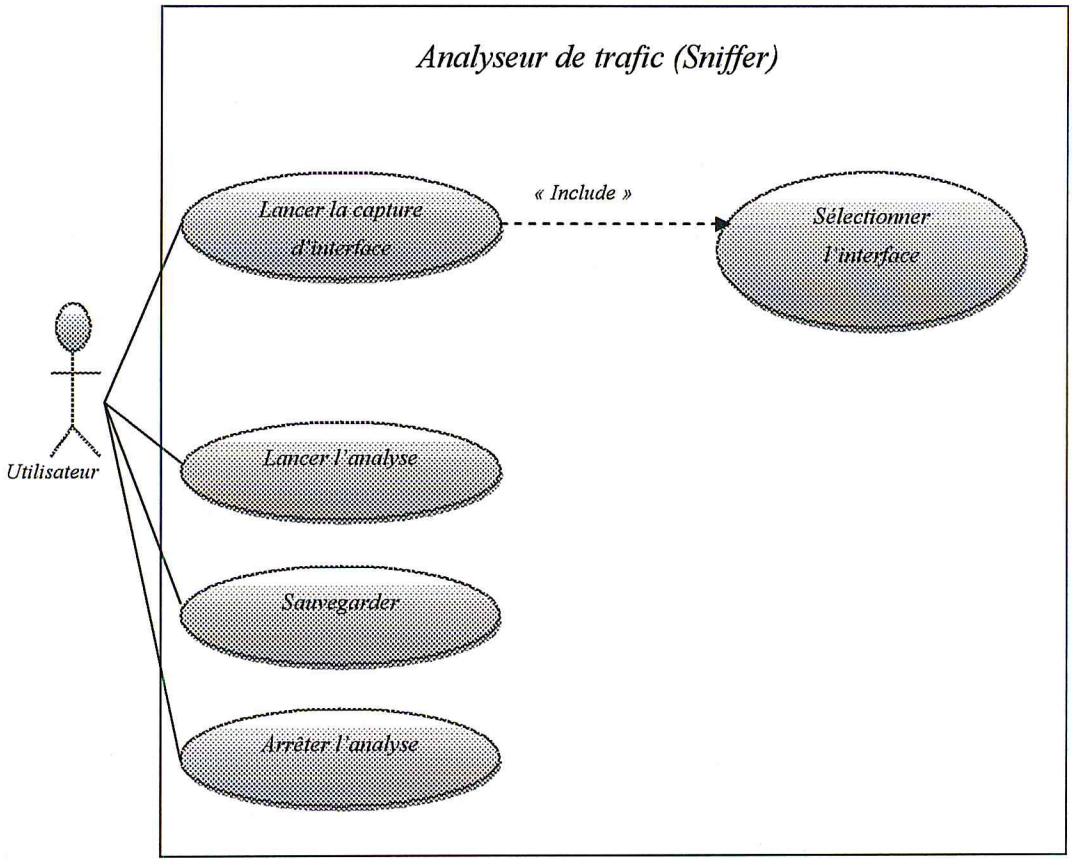


Figure 4.3: Diagramme cas d'utilisation « Analyseur de trafic »

- *Analyseur de ports (port scanner) :*

L'unique fonctionnalité de ce module est d'effectuer un balayage de ports ouverts sur une plage d'adresses IP.

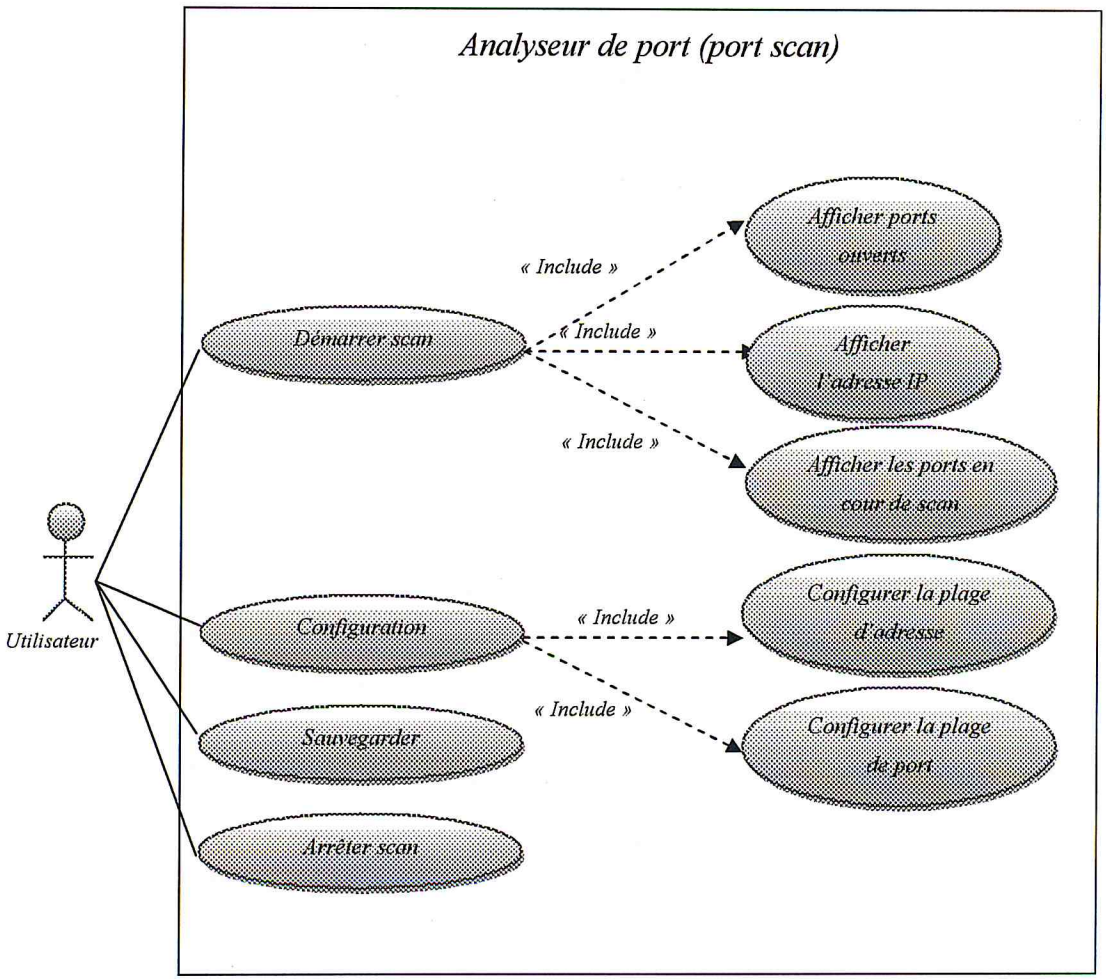


Figure 4.4: Diagramme cas d'utilisation « Analyseur de ports »

4.2.3. Conception

La conception consiste à définir chaque fonctionnalité du système de manière détaillée à partir des besoins exprimés dans la première phase, pour cette phase on a utilisé les diagrammes de SEQUENCE du langage UML.

Ces diagrammes livrent une spécification complète des besoins issus des cas d'utilisation en les structurant sous forme de scénarios qui facilitent la compréhension du futur système.

Dans ce qui suit nous détaillons quelques diagrammes de séquence décrivant des interactions du système.

- *Filtreur de paquets :*

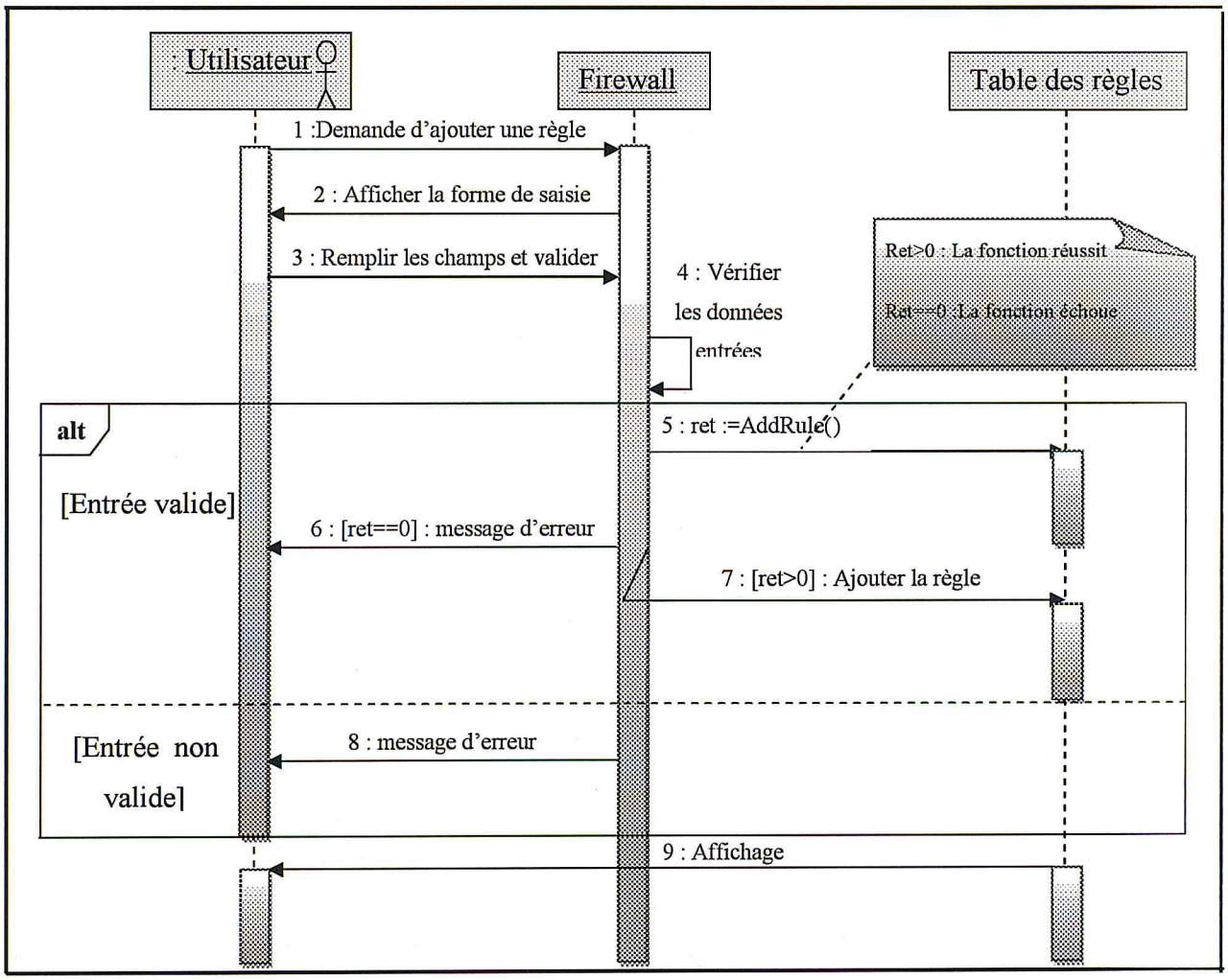


Figure 4.5 : Diagramme de séquence « Ajouter une règle ».

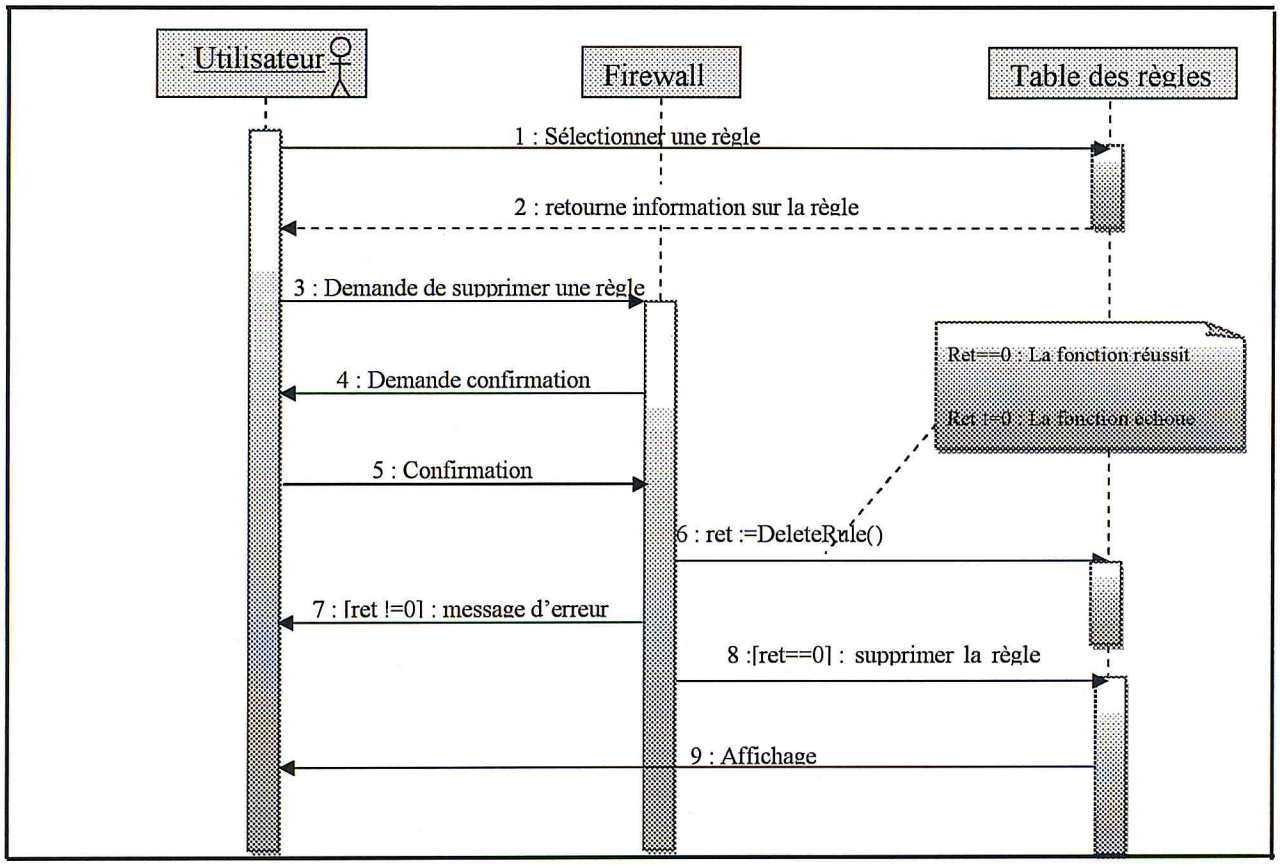


Figure 4.6 : Diagramme de séquence « Supprimer une règle ».

- *Analyseur de trafic (Sniffer) :*

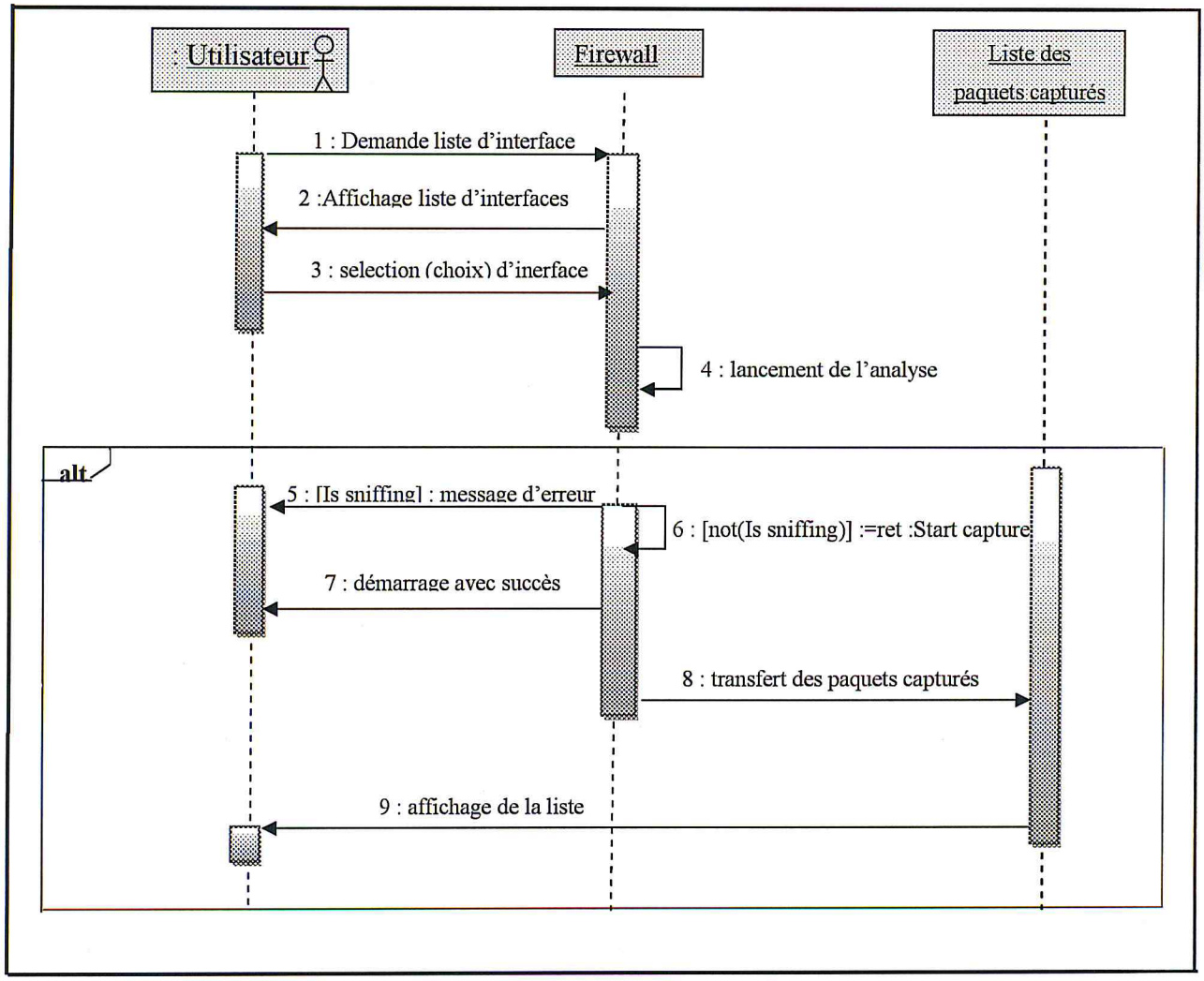


Figure 4.7 : Diagramme de séquence « Démarrer l'analyse ».

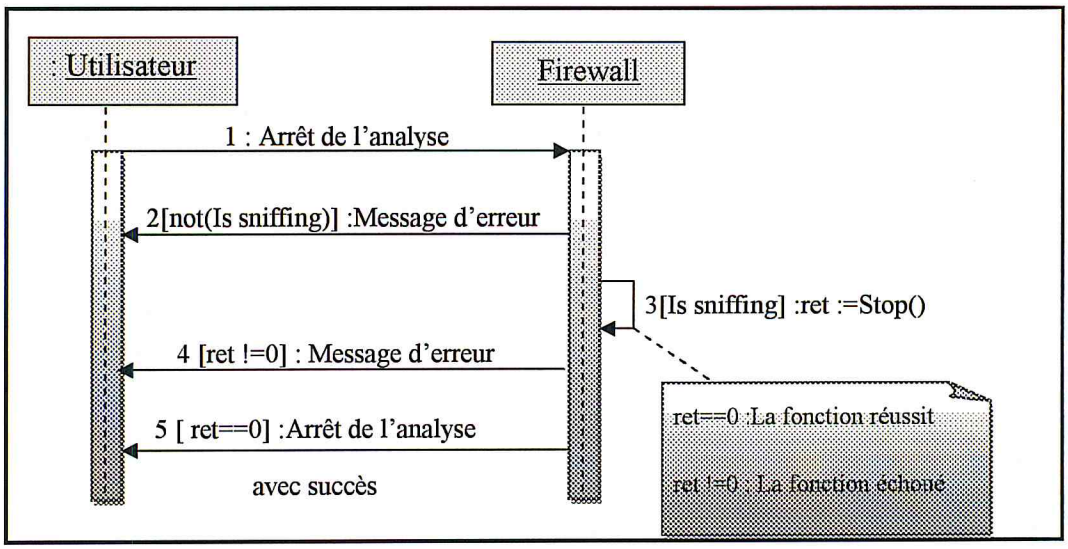


Figure 4.8 : Diagramme de séquence « Arrêter l'analyse ».

- *Analyseur de ports (scanneur de ports) :*

Le principe de ce module est de créer plusieurs sockets et de les connecter en parallèle, en suite analyser les réponses, s'il a eu une connexion donc le port est ouvert, sinon le port est fermé.

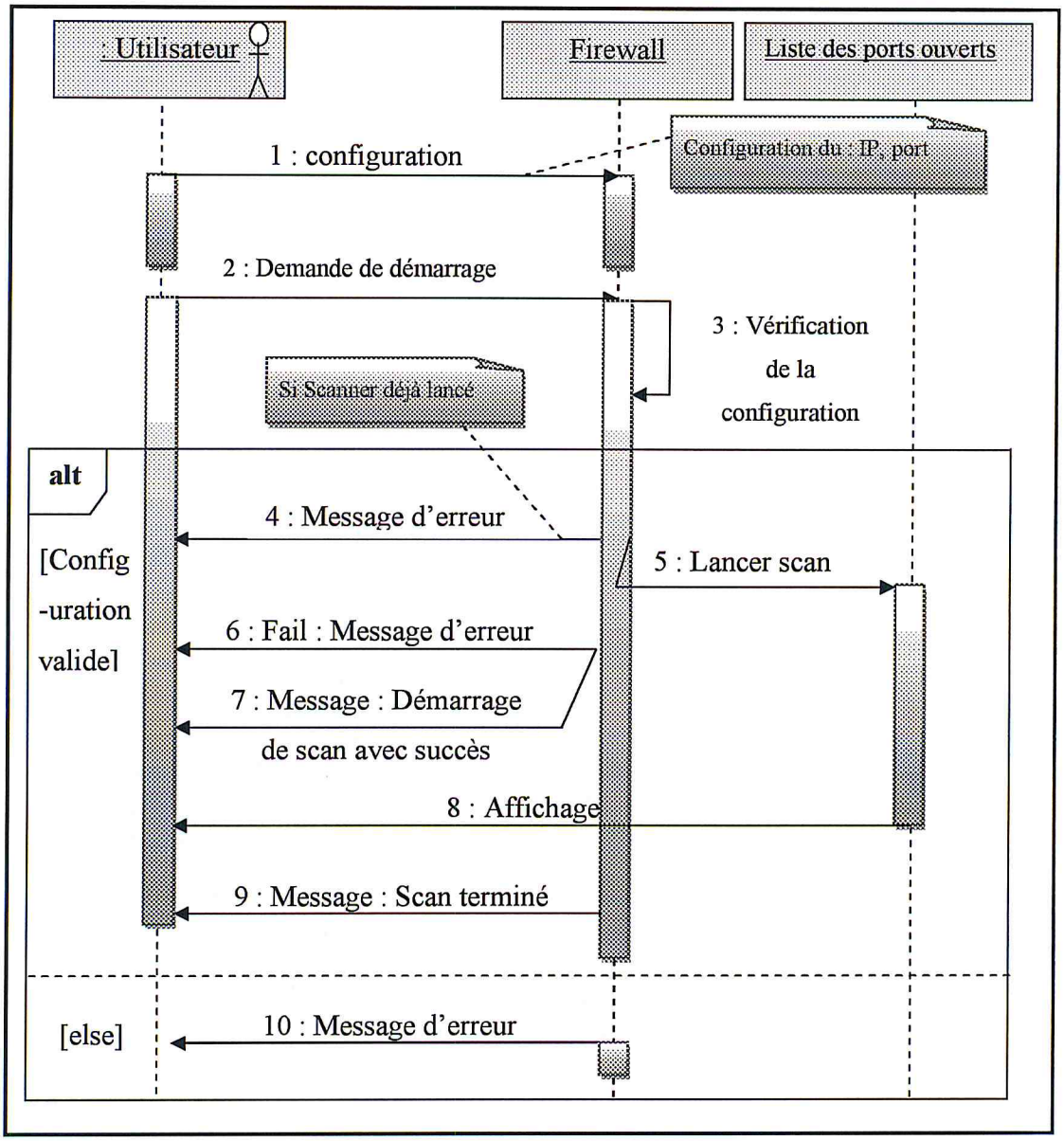


Figure 4.9 : Diagramme de séquence « Démarrer L'analyse de ports ».

4.2.4. Implémentation

a) Choix de la plate forme et du langage de programmation :

Le langage de programmation utilisé est le *Visuel C# 2008* et la plate forme est *Windows XP*.

Choix de la plate forme Windows :

Comme l'ensemble des machines utilisées par la plupart des utilisateurs tournent sous Windows, alors on a décidé que le développement sera sous système Windows.

Choix du Visuel C# 2008 :

Pour implémenter notre application, nous avons utilisé le langage de programmation Visuel C# 2008 qui est un environnement de programmation riche en outils comportant toutes les fonctionnalités nécessaires pour créer des projets C# de toute taille.

Microsoft Visual C# est un puissant langage orienté composant créé par Microsoft. C# joue un rôle essentiel dans l'architecture de Microsoft .NET Framework, et certaines personnes ont comparé son rôle à celui joué par C dans le développement d'UNIX. Sa syntaxe est très proche de celles des langages comme C, C++ ou Java.

Architecture de l'application :

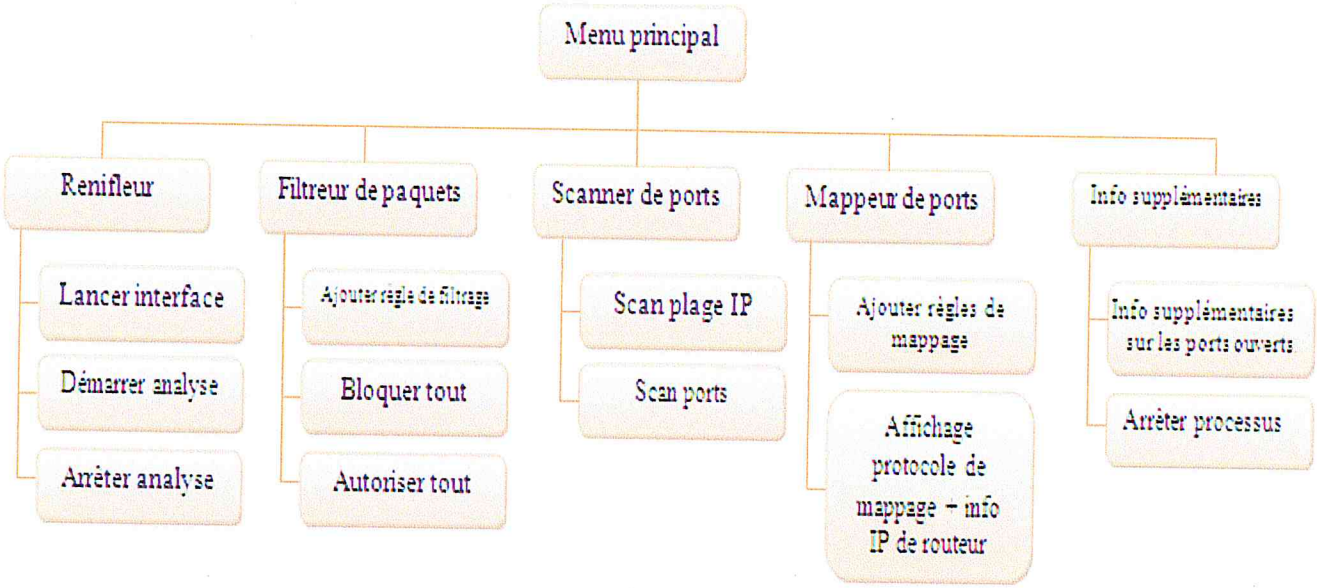


Figure 4.10 : Schéma générale de l'application

c) Module interface utilisateur :

Dans cette partie on présentera les modules étudiés précédemment par des captures d'écran.

Notre Firewall comporte une fenêtre principale donnant accès à tous ses composants :

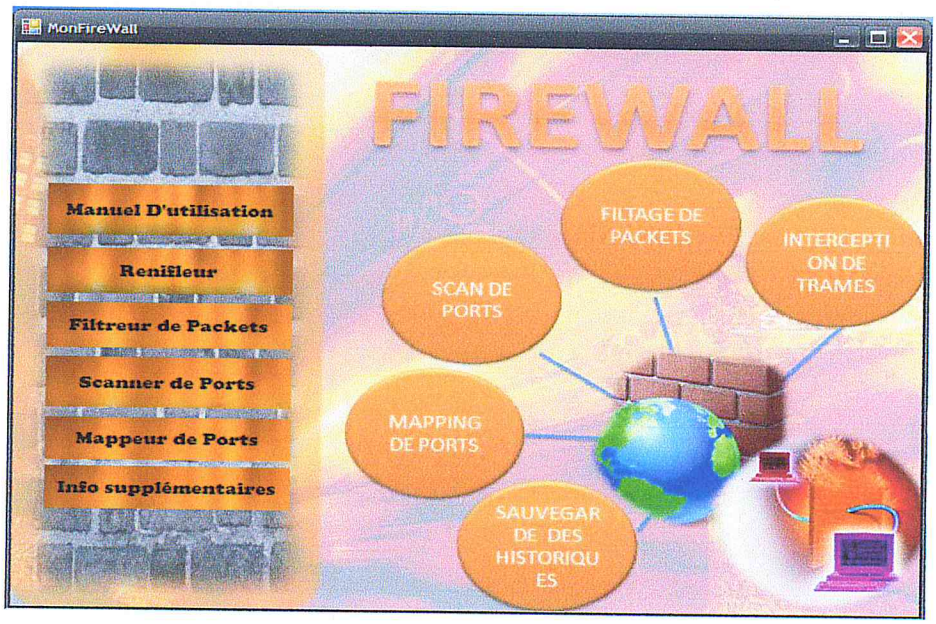


Figure 4.11 : capture d'écran «Accueil ».

Manuel D'utilisation : ce bouton permet d'accéder à un mini-manuel pour une utilisation optimale de l'application

Figure 4.12 : capture d'écran «Manuel d'utilisation ».

Renifleur : ou *packet sniffers,* permet de récupérer les données transitant par le biais d'un réseau local. Il offre un accès à tous les autres composants via une barre des menus dont la liste des interfaces pour pouvoir lancer l'analyse

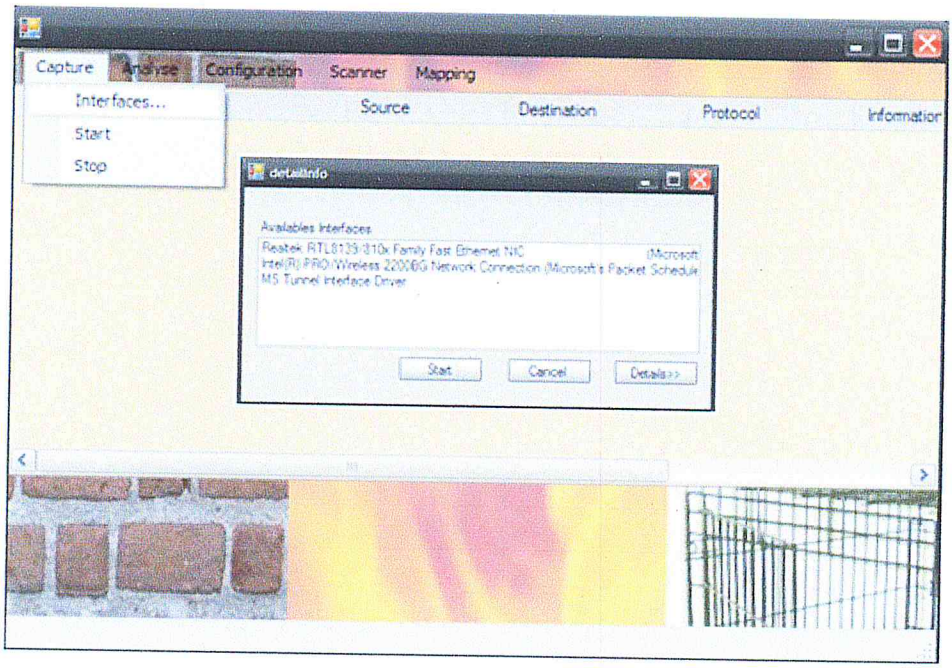


Figure 4.13 : capture d'écran «Liste d'interfaces ».

Détails info : permet d'avoir plus de détails sur l'interface sélectionnée.

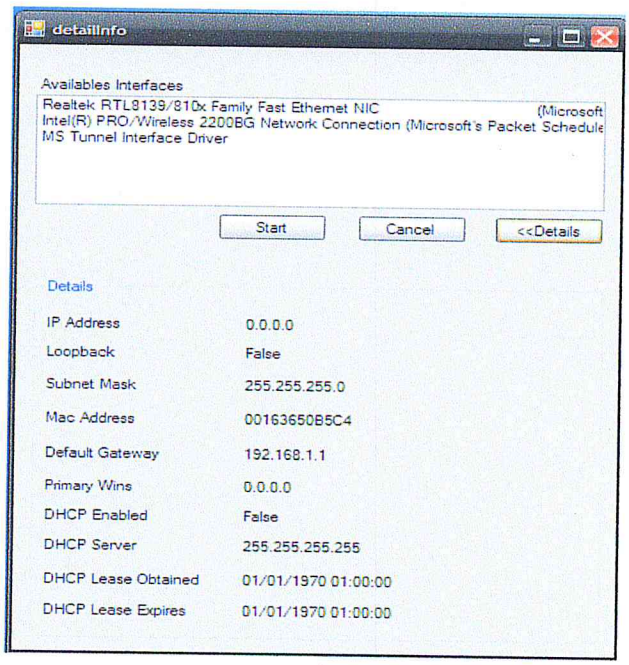


Figure 4.14 : capture d'écran «Détails info ».

Cette fenetre s'affiche lors du lancement de l'analyse du sniffer

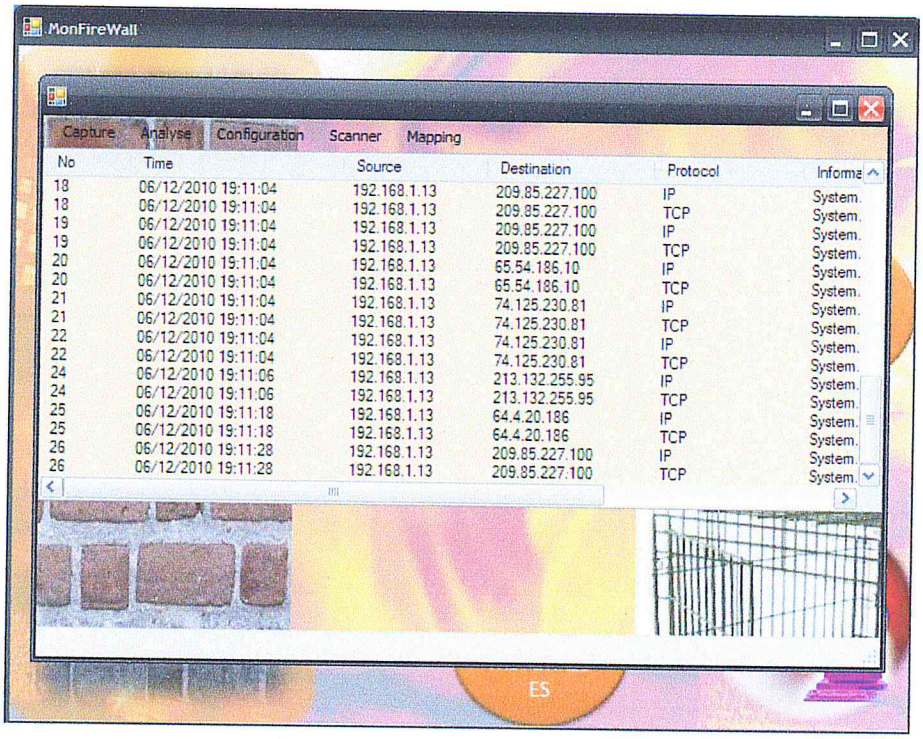


Figure 4.15 : capture d'écran «Lancer analyse ».

Filtreur de Paquets : il permet ou empêche le passage des paquets de données reçus, il examine tous les datagrammes afin de déterminer s'ils ne contiennent pas d'informations dérogeant aux règles de filtrage.

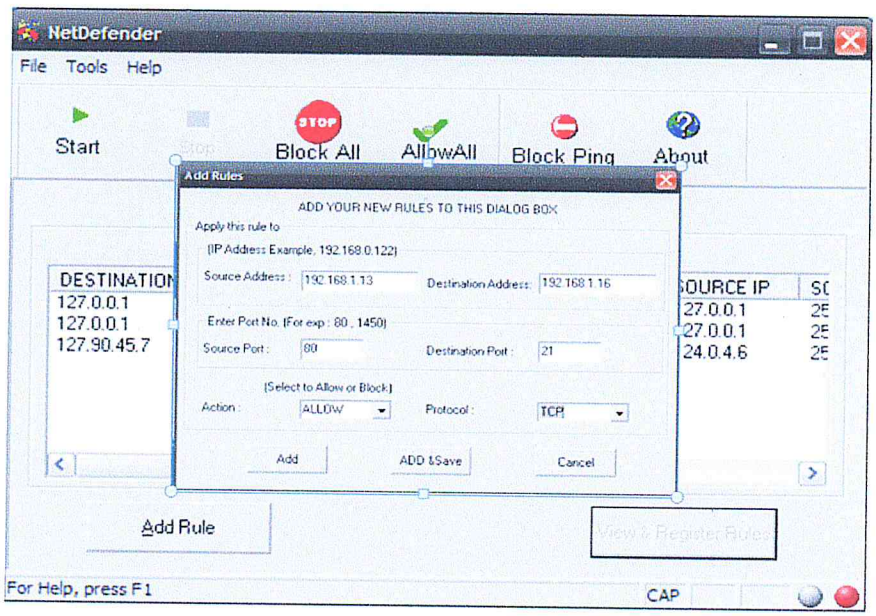


Figure 4.16 : capture d'écran «Filtreur de paquets ».

Scanner de Ports : permet le scan et le sondage des ports ouverts ou des plages IP utilisées.

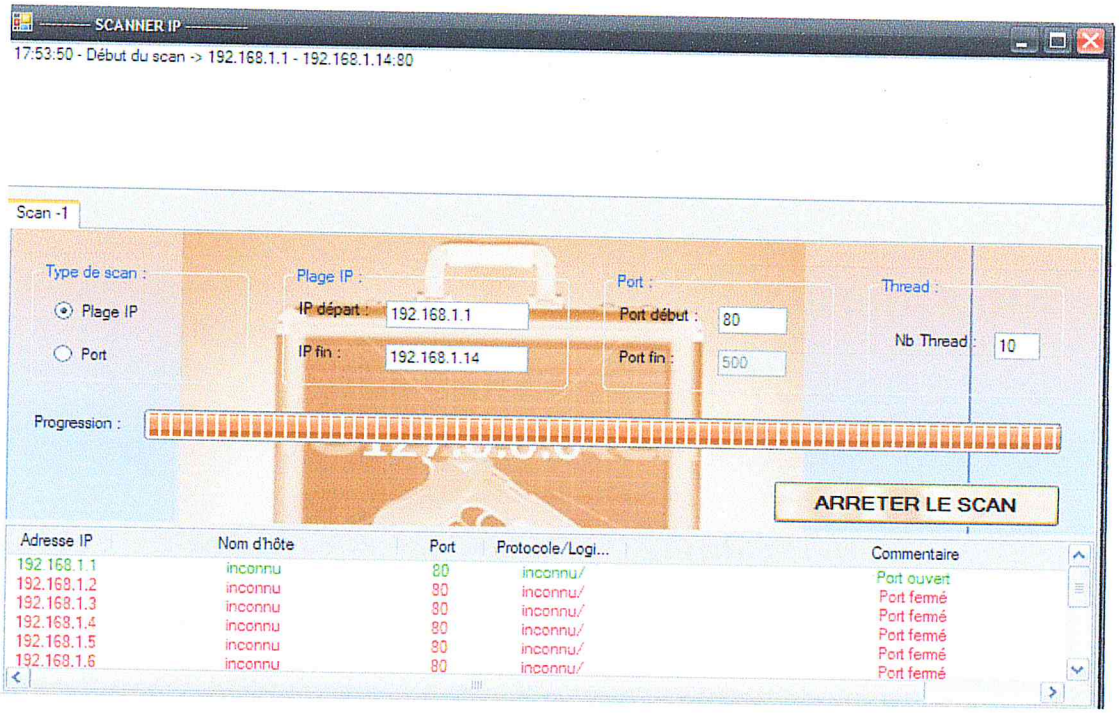


Figure 4.17 : capture d'écran «scan par plage IP ».

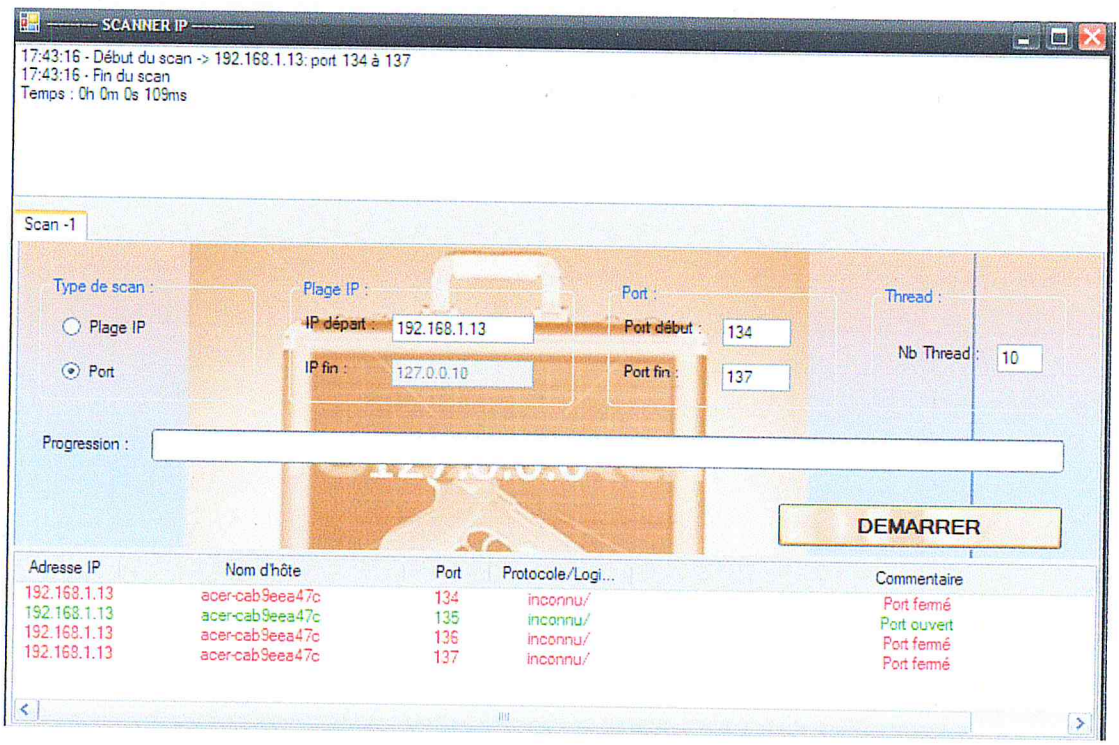


Figure 4.18 : capture d'écran «scan par port ».

Mappeur de Ports : la fenêtre du mappeur affiche le protocole de mappage utilisé ainsi que les informations IP du routeur.

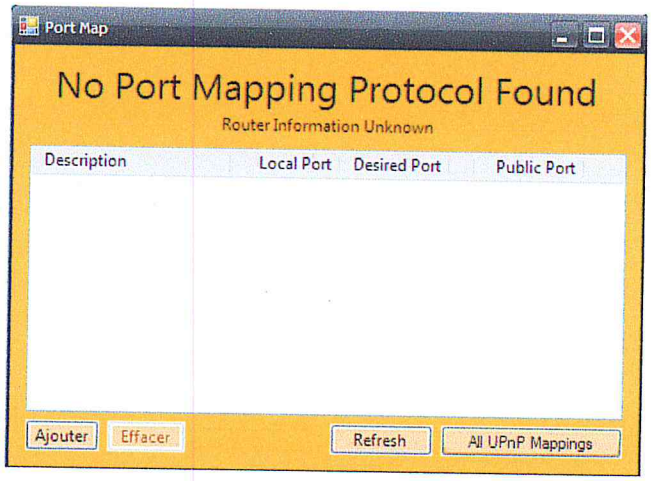


Figure 4.19: capture d'écran «port mapper ».

Cette fenêtre permet d'ajouter de nouvelles règles de mapping grâce au bouton ajouter, la règle comprend le port à mapper ainsi que son nouveau numéro, le Protocol suivi ainsi qu'une plage de description qui est optionnelle.

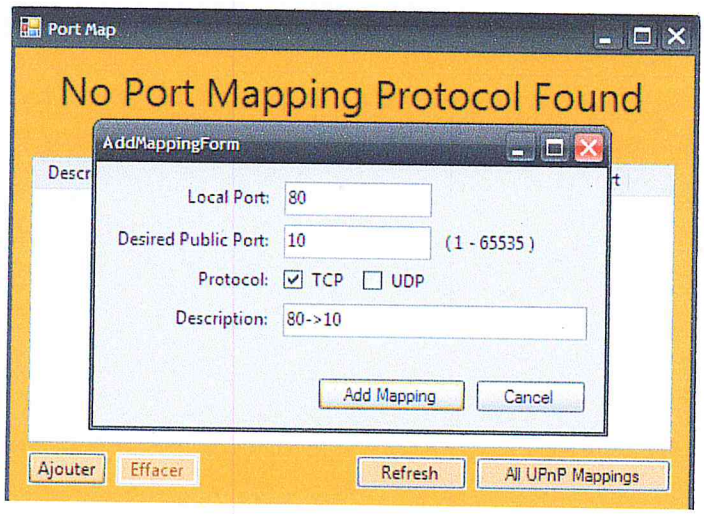


Figure 4.20 : capture d'écran «Ajouter règle de mappage ».

La fenêtre permet aussi de voir les informations du mappage UPnP en cas de présence d'un routeur et de visualiser son adresse IP courante, et cela à travers le bouton All UPnP Mappings :

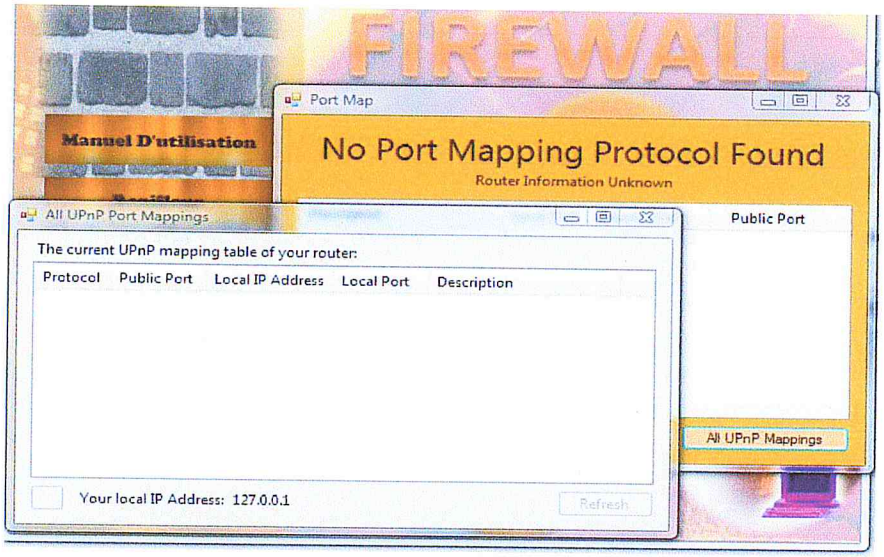


Figure 4.21 : capture d'écran «Information du mappage UPnP».

Info supplémentaires : Permet d'afficher la liste des ports (TCP/UDP) courants ouverts sur la machine locale, pour chaque port de la liste, des informations sur le processus associé (le processus qui a ouvert le port) sont également affichées, y compris le nom du processus, son chemin complet ainsi le nom de l'utilisateur qui l'a crée et terminer un processus.

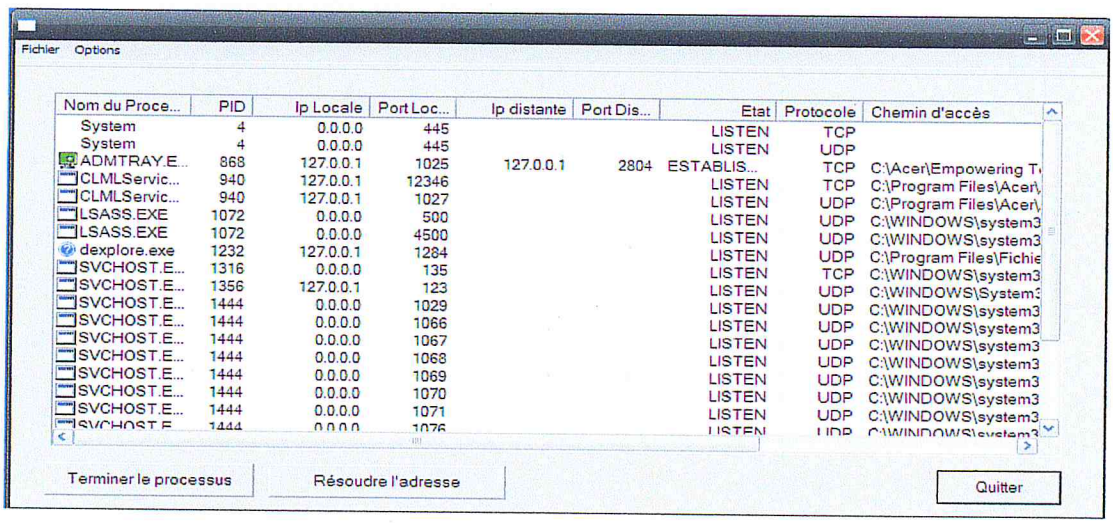


Figure 4.22: capture d'écran «Information supplémentaires».

4.2.5. Intégration et tests globaux

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. Installation

Cette phase correspond à la mise en fonctionnement opérationnel du logiciel.

4.2.7. Maintenance

Elle a pour objectif d'assurer que le logiciel installé fonctionne correctement. Cette phase ne sera pas traitée, car on est dans le cadre d'un projet fin d'étude.

4.3.Conclusion

Dans ce chapitre nous avons étudié et analysé d'abord les besoins et les objectifs du notre système, ce qui nous a mené par la suite à tracer les grands lignes à suivre pour concevoir et implémenter notre application, en utilisant l'approche **UML**.

Chapitre 5 :

Test par simulation d'attaque

5.1. Introduction

On a vu dans le chapitre précédant la conception et la réalisation de notre Firewall, et comme tout autre logiciel de sécurité, on doit valider ses fonctionnalités en établissant une série de tests, pour cela on a choisit d'utiliser un cheval de Troie, car ce malware est très répondu dans le monde des hackers.

Il existe plusieurs chevaux de Troie, parmi eux on cite : Prorat, Back orifice, SubSeven, Netbus…, dans ce chapitre on va tester notre Firewall en utilisant Back orifice 2000 « Bo2k », car ce dernier offre beaucoup de fonctionnalités configurables.

5.2. Définition de « Back orifice/ Bo2k »

Back Orifice est un outil d'administration à distance disponible sur les environnements de Microsoft. Il s'agit d'une application client/serveur qui permet au logiciel client de surveiller, d'administrer, et d'effectuer à distance n'importe quelle action (réseau, multimédia, redémarrage, …) sur la machine exécutant le serveur.

Le serveur de Back Orifice 2000, la version que nous avons utilisée, peut s'exécuter sous Windows 95/98 et également sous Windows NT. Par contre, il existe plusieurs versions du client, que ce soit sur Unix ou sur les systèmes de Microsoft.

5.3. Origine et buts

Cette application a été originellement développée en 1998 par un groupe de "hackers" nommé « **Cult of the Dead Cow** » (cDc) et diffusée sur Internet très rapidement, dans le but (d'après leurs auteurs) d'améliorer les capacités d'administration à distance des systèmes Windows et de mettre en évidence les trous de sécurité existants. L'intention « anti-MicroSoft » est clairement affichée, comme en témoigne le nom même de « Back **Orifice** », évoquant la suite bureautique de « Microsoft **Office** ».

5.4. Composition de Bo2k

Back Orifice est composé de:

Nom	Taille	Implantation	Interface	Rôle
BO2K.EXE	112 Ko	Serveur	aucune	application lancée en tache de fond sur la station cible.
BO2KCFG.EXE	192 Ko	Client	graphique	module de configuration du serveur.
BO2KGUI.EXE	424 Ko	Client	graphique	application cliente permettant d'envoyer des commandes vers le serveur.

5.5. Installation de Bo2k

5.5.1 Le serveur

Il suffit d'exécuter le fichier exécutable BO2K.EXE. Lors de sa première exécution, BO2K.EXE va procéder aux 2 opérations suivantes :

- ***Auto-renommage de "BO2K.EXE" en " .EXE" :*** Le nom du fichier se réduit à un espace, suivi de l'extension habituelle « exe » des exécutables!, ce qui le rend invisible dans le gestionnaire de tâches. En effet, une commande DOS telle que « dir *.exe » va afficher le nom court de ce fichier, qui est alors « exe~1 » (sans extension).
- ***Modification de la clef suivante de la base de registres :***
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
  La valeur par défaut de cette clef est vide en temps normal, affecter la chaîne « .exe» si le serveur BO2K est lancé.

Les fonctionnalités de Back Orifice serveur peuvent être enrichies par l'adjonction de plugins downloadables ou programmables en utilisant BO2KCFG.EXE, la **figure 5.1** montre que BO2KCFG est composé de 3 zones principales : la première où l'on spécifie le fichier du serveur qu'on va configurer, la seconde où on définisse les extensions qu'on va utiliser plus tard (qui seront rajoutées à l'exécutable). La dernière zone concerne les paramètres de chaque fonctionnalité, y compris les extensions qu'on vient d'ajouter. Ici on peut voir que l'option de connexion par TCP a été choisie et que le port à utiliser est le 54320.

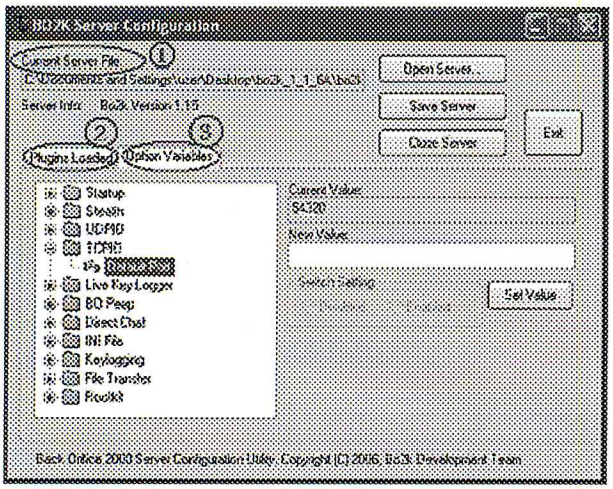


Figure 5.1 : Capture d'écran « BO2KCFG ».

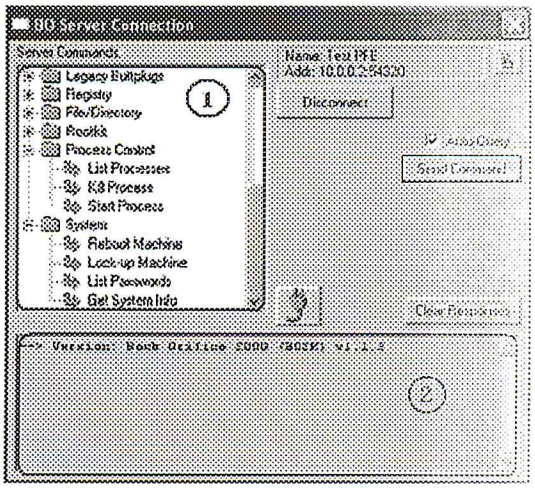


Figure 5.2 : Capture d'écran « BO2KGUI ».

Pour le moment, il existe beaucoup de plugins, par exemple :

- BOpeep.dll : Permet d'avoir accès en streaming (vidéo temps réel) à l'écran hôte ;
- Botool.dll : Permet de télécharger, ajouter, modifier ou supprimer les données ;
- Serpent.dll : Permet de crypter de façon sécurisée la communication entre l'ordinateur hôte et l'ordinateur client.

5.5.2. Le Client

Il suffit d'exécuter BO2KGUI.EXE et de configurer le client avec les mêmes paramètres que le serveur.

L'interface du BO2KGUI (**Figure 5.2.**) est composée de 2 zones importantes : dans la première zone on trouve la liste des plugins chargés, qui sont représentés par des nœuds, chaque nœud contient plusieurs commandes, et on utilise le bouton « send command » pour envoyer la commande sélectionnée, et le résultat sera affiché dans la deuxième zone.

Les fonctionnalités de Bo2k disponibles (de base) comprennent :

- Commandes d'administration : reboot, lockup, gestion de processus, registres… ;
- Récupération d'informations système ;
- Résolution de noms DNS ;
- Enregistrement des frappes clavier ;
- Récupération d'informations : fichiers, mots de passe,… ;
- Gestion de fichiers : copie, effacement, … ;
- Supporte HTTP pour navigation dans le système de fichiers (chargements possibles) ;
- Redirection de connections TCP/IP ;
- Affichage de message à l'écran ;
- Mises à jour à distance, ainsi que installation/désinstallation ;
- Journalisation de sessions ;
- Connections serveurs multiples (concurrentes possibles) et
- Connections de plusieurs clients possibles ;
- Support multimédia, capture audio/vidéo, lecture audio ;

5.6. Tests

5.6.1. Plates-formes des tests effectués

Plate-forme cliente :

PC sous Windows XP Professionnel SP2 (Pentium IV 3.00 GHz).

Plate-forme serveur :

PC sous Windows XP Professionnel SP2 (Pentium IV 3.00 GHz).

5.6.2. Plan du test

Dans notre test nous avons procédé comme suit :

1. Effectuer un Ping ;
2. Scanner les ports de la machine victime ;
3. Exécution du serveur (BO2K.EXE) ;
4. Effectuer un deuxième scan de la machine victime ;
5. Réalisation des attaques ;

6. Exécuter le Firewall réalisé ;
7. Essai d'établissement d'une connexion avec le serveur BO2K.EXE.

5.7. Conclusion

Back orifice est sans doute un logiciel remarquable par ses fonctionnalités, malgré ça la fermeture du port que le serveur utilise a empêché la communication avec son client, donc l'ouverture des ports constitue une faille de sécurité qu'il faut la gérée et surveillée afin de contrôler les communications qui déroulent entre les systèmes, le Firewall est le meilleur outil pour réaliser cet objectif. Donc les Firewalls couvrent une brèche importante de la sécurité informatique.

CONCLUSION GENERALE

En cette ère de communication électronique universelle, celle des virus, hackers, écoutes et fraudes électroniques, la sécurité des réseaux a pris une importance croissante. Cela a conduit à une conscience accrue du besoin de protéger données et ressources des divulgations, de garantir authenticité de ces données et message et de prémunir les systèmes contre des attaques menées depuis les réseaux.

Pour obtenir un niveau de sécurité suffisant afin de prévenir les risques et se protéger contre les attaques et les hackers, il faut définir une stratégie de sécurité comprenant un ensemble des dispositifs matérielles ou logicielles. Le Firewall qui est l'objet de notre projet est l'un de ces dispositifs, qui permet de renforcer la politique de la sécurité établie.

En fait, ce projet nous a permis de :

- Découvrir la sécurité informatique ;
- Bien comprendre et mettre en œuvre le déroulement d'un cycle de vie d'un logiciel ;
- Perfectionner en améliorant nos connaissances en programmation réseau et système en C#, et le design des interfaces en C#, en maitrisant des nouveaux outils ;
- Améliorer nos connaissances en modélisation UML.

Pour terminer, restant pragmatique, il ne faut pas perdre de vue qu'aucun Firewall n'est infaillible et que tout Firewall n'est efficace que si bien configuré. De plus, un Firewall n'apporte pas une sécurité maximale et n'est pas une fin en soi. Il n'est qu'un outil pour sécuriser et ne peut en aucun cas être le seul instrument de sécurisation d'un réseau, d'autres fonctionnalités peuvent être rajouté tel que : l'IDS, l'Antivirus…etc.

Toutes ces technologies sont et seront en pleine évolution, car la base même de tout cela est de jouer au chat et à la souris entre les hackers et les programmeurs de Firewall ainsi que les administrateurs. Une grande bataille d'imagination qui n'aura certainement jamais de fin.

Bibliographie :

[1]. Solange Ghernaouti-hélie « Sécurité informatique et réseau » Edition DUNOD 2006.

[2]. Abdallah El Hadj.H / Korthobi. M «Réalisation d'un outil détecteur de sniffer :système de détection d'intrusion», thèse d'ingéniorat, USTHB, 2000/2001

[3]. « Le grand livre de sécuritéinfo.com », 2004.

[4]. Jean-François Pillou, « Tout sur la sécurité informatique », édition DUNOD, 2005

[5]. MerikeKaeo, « Sécurité des réseaux : un guide pratique pour créer une infrastructure de réseau sécurisé », édition CampusPress, 2000.

[6]. PH. Oechslin, « La sécurité des réseaux » www.securityfocus.com

[7]. ZEBBARI.T / DJEDDI.M «La contribution à la sécurité informatique avec la mise en place d'un système de détection d'intrusion», thèse d'ingéniorat, USDB, 2004/2005

[8]. Tomas olovsson, « A strucured Approach to Computer security », thèsed'ingéniorat, University of Technology S-421 96 Gothenbuurg SWEDEN,1992

[9]. William Stallings « Sécurité des réseaux : applications et standards » Edition Vuibert 2002.

[10]. Alban Jacquemin et Adrien Mercier, « Les Firewalls » www.frameip.com/firewall/

[11]. DRIOUCHE Abdelhalim, KHITER Belkacem, « Etude et mise en œuvre d'un système de détection d'intrusion », thèse d'ingéniorat, USDB, 2004/2005.

ANNEXE

Le modèle OSI :

Le modèle OSI est fondé sur un principe énoncé par Jules César : *Diviser pour mieux régner*.

Le principe de base est la description des réseaux sous forme d'un ensemble de couches superposées les unes aux autres.

L'étude du tout est réduite à celle de ses parties, l'ensemble devient plus facile à manipuler.

Le nombre de couche, leurs noms et leurs fonctions varient selon les réseaux. L'objet de chaque couche est d'offrir certains services aux couches plus autres. Le modèle de référence OSI comporte sept couches numérotées, chacune illustrant une fonction réseau précise. Cette répartition des fonctions réseau est appelée organisation en couches.

Les couches du modèle OSI :

- ***la couche application :***

La couche application fournit des services réseau aux applications de l'utilisateur.

- ***La couche présentation :***

La couche de présentation s'assure que l'information envoyée par la couche application d'un système est lisible par la couche application d'un autre système. Au besoin, la couche de présentation traduit différents formats de représentation des données en utilisant un format commun.

- ***La couche session:***

La couche session ouvre, gère et ferme les sessions entre les applications.

➢ ***La couche transport :***

La couche de transport segmente et rassemble les données en un flot. Elle tente de fournir un service de transport des données qui protège les couches supérieures des détails d'implantation du transport. En fournissant un service fiable, la couche de transport procure des mécanismes permettant l'établissement, la maintenance et la terminaison ordonnée des circuits virtuels, la détection et la reprise sur incident ainsi que le contrôle du flux d'information, afin d'empêcher qu'un système n'en surcharge un autre de données.

➢ ***La couche réseau :***

La couche réseau est une couche complexe qui assure la connectivité et la sélection du trajet entre deux systèmes d'extrémité pouvant être situés dans des réseaux géographiquement dispersés.

➢ ***La couche liaison de données :***

La couche liaison de données assure un transit fiable des données sur une liaison physique. Ce faisant, la couche liaison de données se rapporte à l'adressage physique, à la topologie de réseau, à la gestion de ligne à la signalisation des erreurs, à la livraison ordonnée des trames et au contrôle de flux.

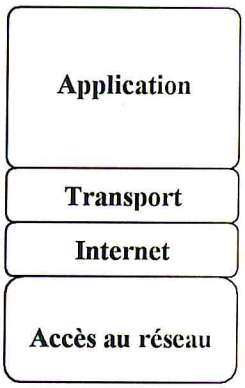
➢ ***La couche physique :***

La couche physique précise les caractéristiques physiques et électriques des connexions qui composent le réseau.

Le modèle TCP/IP :

TCP/IP «*Transmission Control Protocol/Internet Protocol*» est une suite de protocoles permettant de transférer des informations d'une unité de réseau à une autre, il représente d'une certaine façon l'ensemble des règles de communication sur internet et se base sur la notion d'adressage IP.TCP/IP a été décomposé en plusieurs modules (04) effectuant chacun une tâche précise. De plus, ces modules effectuent ces tâches les unes après les autres dans un ordre précis, on a donc un système stratifié, c'est la raison pour laquelle on parle de modèle en couches.

Les couches du modèle TCP/IP :



- **La couche d'Accès au réseau (Network access layer) :**

Sert au transport de l'information, elle regroupe le standard physique et la normalisation des signaux électriques.

On retrouve les réseaux Ethernet, TokenRing,FrameR elay, ATM, Fibre optique,…

- **La couche Internet (Internet layer) :**

Fournit les paquets de données, elle définit des datagrammes et gère le processus de mise en paquets, adressage et routage des informations vers les destinations réseau. Différents protocoles sont utilisés à ce niveau comme ARP, IP, RARP, ICMP ou IGMP.

- **La couche transport (Transport layer) :**

La couche transport permet à des applications tournant sur des machines distantes de communiquer, elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission. Deux protocoles sont utilisés : TCP et UDP.

➢ **La couche Application (Application layer) :**

Englobe les logiciels, elle se base sur des ports TCP ou UDP pour envoyer ou recevoir les données sur le réseau, on retrouve les applications courantes sur Internet comme l'HTTP, le FTP, le DNS, les applications de messagerie de type POP3 ou SMTP (Simple Mail Transfert Protocol), NNTP (Network News Transfert Protocol) ou Telnet.

L'encapsulation

Au cours de son passage par chacune des couches, des informations relatives à chacune d'entre elles sont ajoutées pour lui permettre d'effectuer la tâche qui lui incombe, on appelle cela l'en-tête. Cela permet d'avoir un certain nombre d'informations nécessaires à chaque couche pour effectuer son travail, et que ces informations circulent avec le message à transmettre.

couche 7 | Info à transmettre |

couche 6 | en-tête couche 6 | Info à transmettre |

couche 5 | en-tête couche 5 | en-tête couche 6 | Info à transmettre |

... et ainsi de suite ... jusqu'au paquet final

Couche 1 | en-tête couche 1 | ...| en-tête couche 5 | en-tête couche 6 | Info à transmettre |

Chaque couche ajoute donc son propre en-tête à l'information d'origine. Ce procédé s'appelle l'encapsulation.

L'adressage :

Les adresses IP sont composées de 4 octets. Par convention, on note ces adresses sous forme de 4 nombres décimaux de 0 à 255 séparés par des points.

L'originalité de ce format d'adressage réside dans l'association de l'identification du réseau avec l'identification de l'hôte.

• La partie réseau est commune à l'ensemble des hôtes d'un même réseau,

• La partie hôte est unique à l'intérieur d'un même réseau.

Adresses particulières :

Il existe différentes adresses IP particulières :

- La partie machine toute à 0 : adresse du réseau.
- La partie machine toute à 1 : adresse de diffusion.
- 127.0.0.1 : " cette machine"

Les adresses suivantes sont normalement réservées à des usages privés et ne devraient pas être diffusées sur Internet.

- 10.0.0.0-10.255.255.255 (10.0.0.0/8)
- 172.16.0.0-172.31.255.255 (172.16.0.0./12)
- 192.168.0.0-192.168.255.255 (192.168.0.0/16)

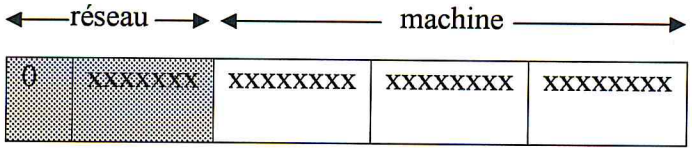
Les adresses suivantes sont normalement réservées comme adresse de configuration automatique et ne devrait pas être diffusées au delà d'un même segment.

- 169.254.0.0-169.254.255.255 (169.254.0.0/16)

Les classes d'adresses :

À l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser le cheminement (ou le routage) des paquets entre les différents réseaux. Ces groupes ont été baptisés classes d'adresses IP. Ces classes correspondent àdes regroupements en réseaux de même taille. Les réseaux de la même classe ont le même nombre d'hôtes maximum.

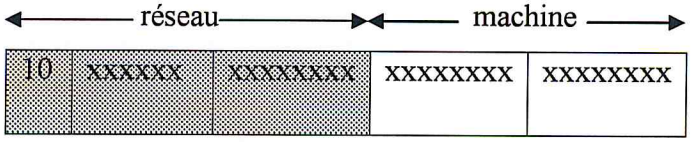
➢ ***Classe A***



Le premier octet a une valeur comprise entre 1 et 126 ; soit un bit de poids fort égal à 0. Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte.

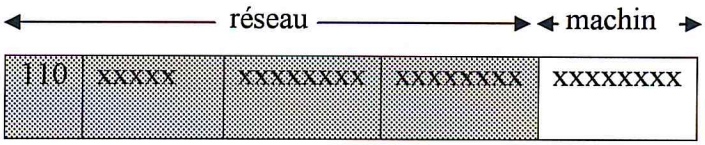
L'adresse réseau 127.0.0.0 est réservée pour les communications en boucle locale.

➢ ***Classe B***

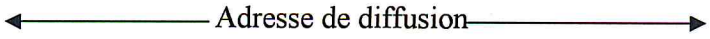


Le premier octet a une valeur comprise entre 128 et 191 ; soit 2 bits de poids fort égaux à 10. Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte.

➢ ***Classe C***



Le premier octet a une valeur comprise entre 192 et 223 ; soit 3 bits de poids fort égaux à 110. Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte.



➢ ***Classe D***

1110	xxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx

Le premier octet a une valeur comprise entre 224 et 239 ; soit 3 bits de poids fort égaux à 111. Il s'agit d'une zone d'adresses dédiées aux services de multi-diffusion vers des groupes d'hôtes (host groups).

➢ ***Classe E***

Le premier octet a une valeur comprise entre 240 et 255. Il s'agit d'une zone d'adresses réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

Le masque de réseau :

Le masque de réseau sert à séparer les parties réseau et hôte d'une adresse. On retrouve l'adresse du réseau en effectuant un ET logique bit à bit entre une adresse complète et le masque de réseau.

Prenons un exemple d'adresse IP pour en identifier les différentes parties :

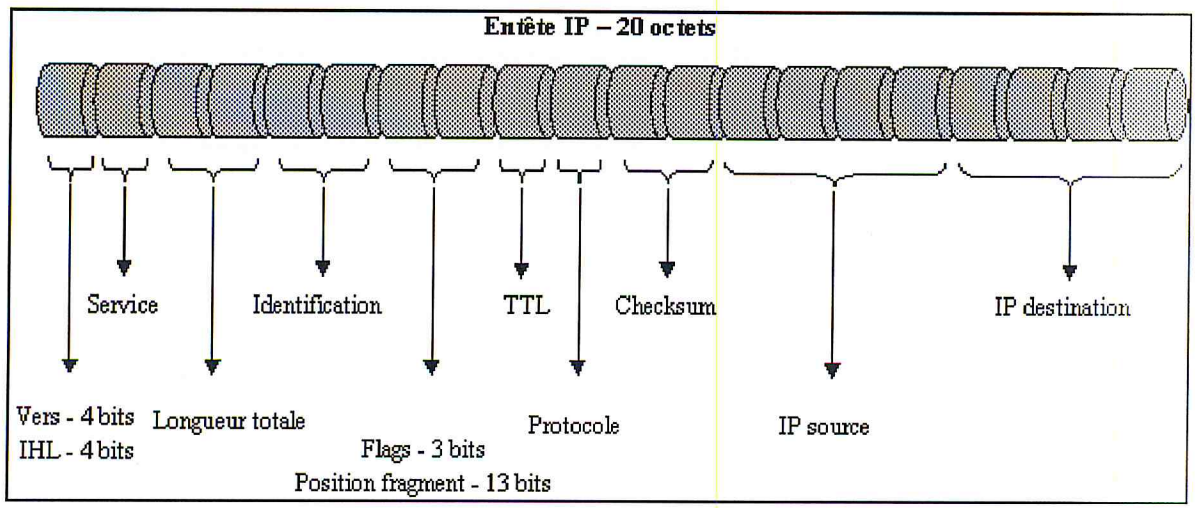
Adresse complète	192.168. 1 .1
Masque de réseau	255.255.255.0
Partie réseau	192.168.1.
Partie hôte	.1
Adresse réseau	192.168. 1 .0
Adresse de diffusion	192.168. 1 .255

Quelques protocoles:

- ***Le protocole IP:***

IP signifie "Internet Protocol", protocole Internet. Il représente le protocole réseau le plus répandu. Il permet de découper l'information à transmettre en paquets, de les adresser, de les transporter indépendamment les uns des autres et de recomposer le message initial à l'arrivée. Ce protocole utilise ainsi une technique dite de commutation de paquets. Il apportel'adressage en couche 3 qui permet, par exemple, la fonction principale de routage.

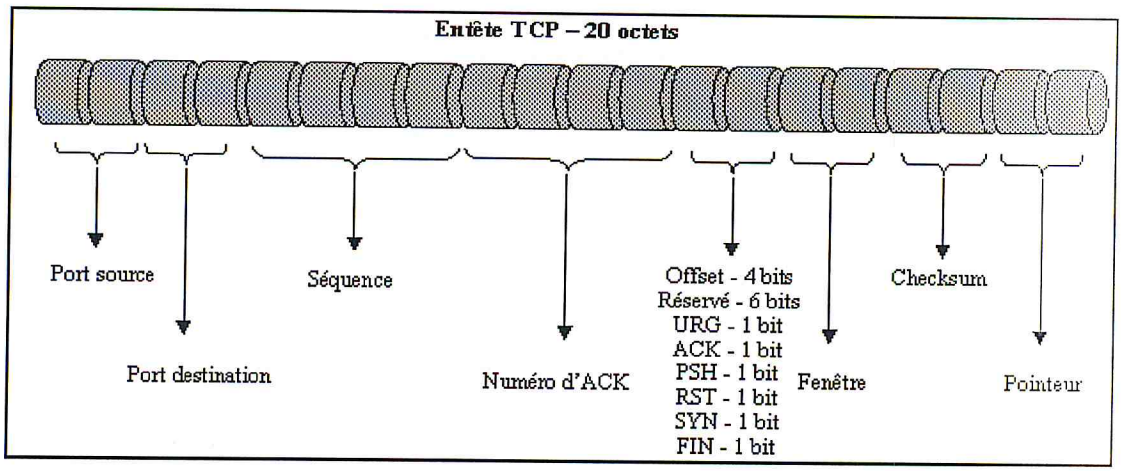
Structure de l'en-tête :



➢ ***Le protocole TCP:***

Le protocole TCP est basé en couche 4. Il ouvre une session et effectue lui-même le control d'erreur. Il est alors appelé "mode connecté".

Structure de l'entête

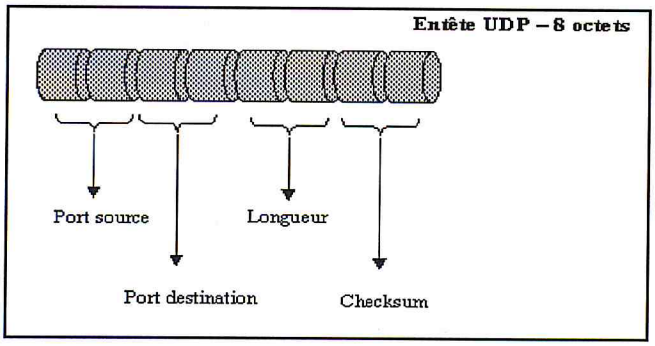


➢ ***Le protocole UDP:***

Le protocole UDP est basé en couche 4. Il n'ouvre pas de session et n'effectue pas de control d'erreur. Il est alors appelé "mode non connecté". Il est donc peut fiable, cependant, il permet aux applications d'accéder directement à un service de transmission de Datagrammes rapide.

UDP est utilisé pour transmettre de faibles quantités de données où le coût de la création de connexions et du maintient de transmissions fiables s'avèrent supérieur aux données à émettre. UDP peut également être utilisé pour les applications satisfaisant à un modèle de type "interrogation réponse". La réponse étant utilisée comme un accusé de réception à l'interrogation.

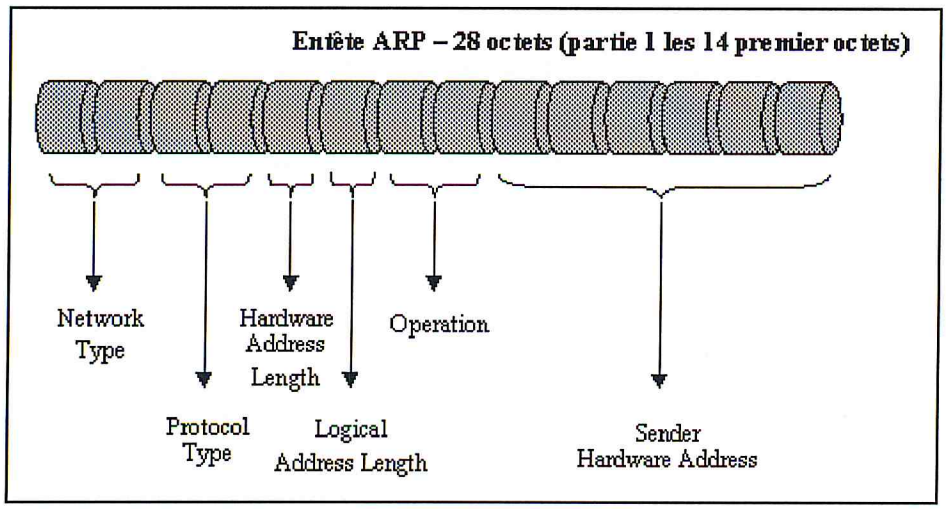
Structure de l'entête :

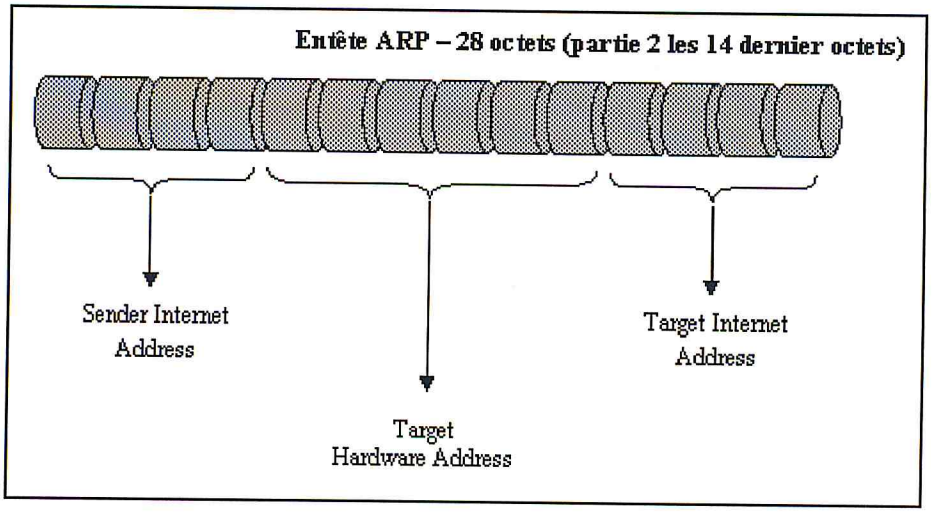


- ***Le protocole ARP:***

Le protocole Arp, signifiant AddressResolution Protocol, fonctionne en couche Internet du modèle TCP/IP correspondant à la couche 3 du modèle Osi. L'objectif de Arp est de permettre la résolution d'une adresse physique par l'intermédiaire de l'adresse IP correspondante d'un host distant. Le protocole Arp apporte un mécanisme de « translation » pour résoudre ce besoin.

Structure de l'entête :





- ***Le protocole ICMP:***

Le protocole ICMP (Internet Control Message Protocol) permet de gérer les informations relatives aux erreurs du protocole IP. Il ne permet pas de corriger ces erreurs, mais d'en informer les différents émetteurs des Datagrammes en erreurs. Chaque pile IP, que ce soit des routeurs ou des stations de travail, gèrent ICMP par défaut.

Structure de l'entête :