MASTER EN SCIENCES INFORMATIQUES

Les outils d'audit
tests comparatifs

Vaca Toledo, Marco N.

Award date:
1999

FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX, NAMUR

INSTITUT D'INFORMATIQUE

RUE GRANDGAGNAGE, 21, B-5000 NAMUR (BELGIUM)

Année Académique 1998-1999

Les outils d'audit: Tests comparatifs

Marco N. Vaca Toledo

Mémoire présenté en vue de l'obtention du grade de

Maître en Informatique

Résumé

Les logiciels modernes tels que les systèmes d'exploitation, les browsers, etc... contiennent des vulnérabilités qui, lorsqu'elles sont découvertes, peuvent être exploitées par des personnes malveillantes dans le but de s'introduire dans un système informatique. Pour diminuer les risques d'intrusion, il existe des logiciels spécialement conçus pour détecter ces vulnérabilités. Nous comparons certains de ces programmes.

Abstract

The modern software like operating systems, browsers, etc... contain vulnerabilities which, if they are discovered, can be exploited by malevolent people who want to introduced themself into the informatic system. Some softwares are conceived to detect the vulnerabilities and decrease the intrusion risks. We compare some of these programs.

Avant-propos.

Tout d'abord, je remercie mon promoteur Jean Ramaekers qui m'a aidé en lisant et en commentant ce travail.

J'aimerais aussi adresser mes sincères remerciements aux membres de l'Internet Team de chez Siemens Nixdorf: Siegfried Delwiche, Guy Lambert, Isabelle Dehousse, Vincent Reidemeister, qui ont bien voulu m'accueillir parmi eux.

Je remercie aussi monsieur Bruno Delcourt pour m'avoir permis d'installer et de tester les logiciels nécessaires à la bonne réalisation de mon mémoire.

Un remerciement spécial à mon père et à Véronique qui m'ont donné la possibilité de réaliser les études en Belgique.

Je n'oublie pas les autres membres de ma famille qui ont eu confiance en moi et qui m'ont toujours encouragé. Ils m'ont appris que "rien ne tombe du ciel" et que pour atteindre un but il faut beaucoup travailler.

Finalement, je remercie aussi les personnes qui, de près ou de loin, ont contribué avec leurs conseils à corriger mes fautes monumentales d'orthographe.

Table de matières.

Table de matières.

Table de matières.

Introduction.

Les logiciels modernes tels que les systèmes d'exploitation, Browsers, etc. contiennent de plus en plus de lignes de code. Malheureusement, plus il y a de lignes de code, plus le risque d'introduire des vulnérabilités augmente.

Les réseaux connectés à Internet utilisent ces logiciels, ils ont donc besoin d'outils qui permettent de les rendre plus sûrs, des outils qui permettent de découvrir les vulnérabilités.

Ce document a pour objectif principal d'étudier plusieurs logiciels qui réalisent des audits de vulnérabilités. A la fin de l'étude, nous serons amenés à choisir le(s) logiciel(s) le(s) plus performant(s). Ce document est donc adressé aux personnes intéressées par la sécurité informatique comme les gestionnaires de réseaux et les responsables de la sécurité.

Ce travail fait suite à un stage réalisé par l'auteur chez Siemens Nixdorf, plus exactement au sein de l'Internet Team, l'équipe spécialisée dans la sécurité.

La sécurité informatique.

Dans le chapitre un, nous introduirons le problème complexe de la sécurité. Nous parlerons des attaques les plus connues et finalement nous citerons et expliquerons les moyens qui existent pour se protéger contre ces attaques.

Les organismes liés à la sécurité.

Dans le chapitre deux, nous donnerons une liste des différentes organisations spécialisées dans la sécurité. Nous parlerons aussi des plus importants New groups et Mailing lists qui traitent de la sécurité.

Les protocoles TCP/IP

Dans le chapitre trois, nous aborderons les protocoles TCP/IP, ce qui nous permettra de mieux comprendre le chapitre quatre.

Les audits de vulnérabilités et les logiciels d'audit.

Dans le chapitre quatre, nous traiterons des audits de vulnérabilités et de la façon de réaliser un audit de sécurité. Nous parlerons aussi des outils employés pour réaliser ces audits, son principe de fonctionnement, ses avantages et ses inconvénients.

Etude comparative des différents outils d'audit.

Dans le chapitre cinq, nous réaliserons une étude comparative des plusieurs outils qui réalisent des audits de vulnérabilités.

Chapitre Un : La sécurité informatique

1.1 Introduction.

Le **réseau informatique**[1] est devenu un outil de travail indispensable au sein des organisations. En plus des fonctionnalités locales, celui-ci assure également l'ouverture de ces organisations sur le monde entier grâce au réseau **Internet**[2].

A ce titre, il représente un maillon stratégique du système d'information de toute organisation.

Sa disponibilité, sa performance et sa sécurité, en sont des attributs sensibles auxquels une grande attention doit être attachée, afin d'aider à la constitution d'un capital "confiance" chez les utilisateurs et de maintenir une bonne image du service informatique et du réseau de l'établissement.

La sécurité informatique, tout particulièrement, mérite des efforts ciblés car tout le savoir, toute la stratégie, ou même toute la comptabilité d'une organisation peuvent reposer sur l'informatique.

---

[1] Un **réseau informatique** est un ensemble d'appareils (ordinateurs et périphériques) reliés entre eux dans le but de permettre à ses utilisateurs de transférer des informations électroniques (communiquer, partager des ressources matérielles et logicielles).[Réseaux]

[2] Un méta-réseau (réseau de réseaux) d'ordinateurs interconnectés capables de se transmettre des informations en utilisant un protocole de communication et un système d'adressage communs et ce, indépendamment de la distance qui sépare les composants [Internet - définition]

1.2 Définition de la sécurité informatique.

Il est difficile de donner une définition précise de la sécurité informatique, cependant, d'après [Ramaekers 99] *"La sécurité informatique, est la gestion des techniques physiques logiques et humaines destinées à protéger, contre les incidents, les erreurs et les composants malicieux qui confient certains de leurs valeurs à des systèmes informatiques fonctionnant dans un certain environement".*

1.2.1 Les objectifs de la sécurité informatique.

Une sécurité informatique efficace repose sur 3 éléments principaux : confidentialité, intégrité et disponibilité.[Ramaekers 99]

- ***La confidentialité.***

Le terme confidentialité est utilisé pour qualifier des données informatiques qui ne seraient accessibles et comprises que par des personnes autorisées. La confidentialité reste la notion de sécurité informatique la plus proche du monde réel et semble dès lors la plus claire.

- ***L'intégrité des données*** :

L'intégrité assure que l'information ne peut être modifiée que par les personnes autorisées ou seulement par les moyens autorisés.

- ***Disponibilité***

La disponibilité empêche les données d'être supprimées ou de devenir inaccessibles. Cela s'applique non seulement aux informations mais aussi aux machines en réseau ou à d'autres éléments de l'infrastructure technologique

Ce sont ces trois buts qui forment, ensemble, la sécurité informatique. Parfois, ils se chevauchent mais ils peuvent éventuellement être mutuellement exclusifs (ex. une confidentialité trop forte entraînant une perte de disponibilité).

1.3 Les problèmes liés à la sécurité : les types d'attaques possibles sur le réseau.

Il est difficile d'identifier les différents types d'attaques car nous sommes souvent en présence d'attaques mêlant plusieurs méthodes ou poursuivant

plusieurs buts. Nous pouvons cependant isoler cinq catégories de menaces qui nous permettront par la suite de mieux détailler les précautions à prendre.

1.3.1 Usurpation d'identité (IP-Spoofing)

Au niveau de la pile de protocoles TCP/IP[3] une machine est identifiée par son adresse IP . Cette adresse IP est très facilement configurable par le logiciel.

Le IP-spoofing est une méthode d'attaque active car l'attaquant modifie les paquets qui circulent sur le réseau. **Ce type d'attaque entraîne une perte d'intégrité et la confidentialité n'est plus assurée.** Cette méthode consiste à tromper le routeur (Anglais: router[4]) sur l'adresse d'origine des paquets transmis.En fait, les paquets émis contiennent l'adresse IP d'une machine interne au système que l'on désire pénétrer. Si le système emploie un service de défense simple comme celui d'un routeur, le stratagème a de bonnes chances de fonctionner.

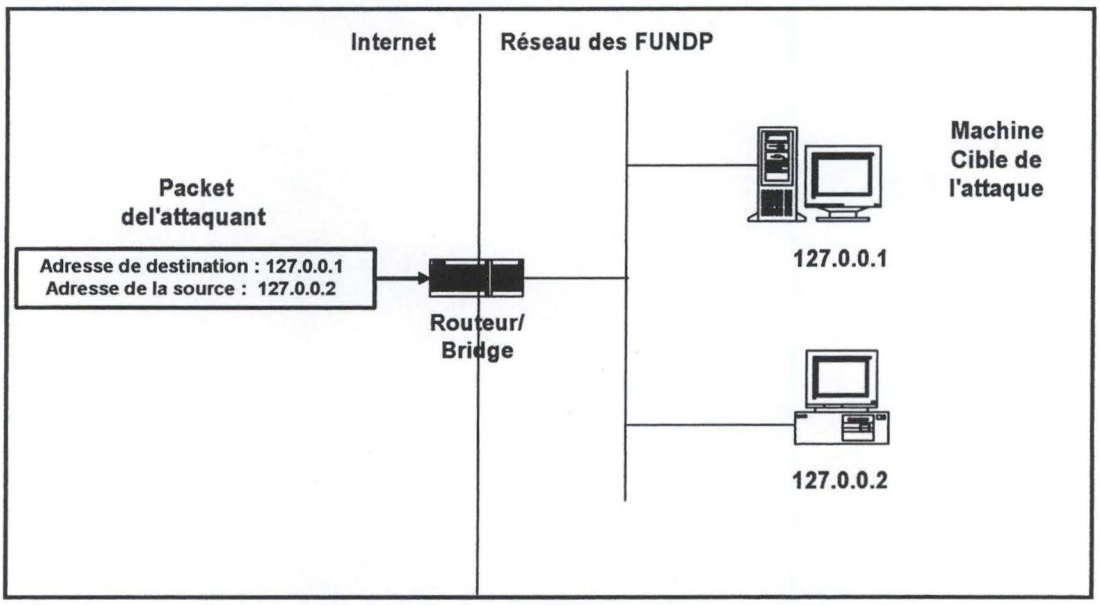

Figure 1-1 : Attaque IP-Spoofing

Le problème soulevé par l'usurpation d'identité est lié au fait que beaucoup de systèmes d'authentification ne se basent que sur l'adresse IP pour

[3] La pile de protocoles TCP/IP ainsi que les adresse IP serons expliques en détail au chapitre 3.

[4] A device that connects any number of LANs.
Routers use headers and a forwarding table to determine where packets go, and they use ICMP to communicate with each other and configure the best route between any two hosts. Very little filtering of data is done through routers. [Webopedia]

permettre à une machine d'accéder à tel ou tel service. Les commandes *rlogin, rsh* sont vulnérables à ce type d'attaque.

1.3.2 Ecoute des paquets (Sniffing)

Le sniffing est une méthode d'attaque passive, qui permet à une machine connectée au réseau de lire les paquets qui transitent par celui-ci. **Ce type d'attaque entraîne une perte de confidentialité**. On parle d'attaque passive car l'attaquant ne modifie pas l'information mais il réalise uniquement une copie pour une analyse ultérieure. De plus, il existe une grande quantité d'outils d'attaques disponibles et faciles d'accès. [ISS]

Les risques dus à ce type d'attaque sont très grands puisqu'on peut de cette manière reconstituer l'intégralité d'un transfert des données d'une connexion Telnet, lire le courrier d'une personne, connaître les pages Web qu'elle visite ou les News groups qu'elle fréquente.

L'obtention des mots de passe s'appuie beaucoup sur cette technique.

1.3.3 Cheval de Troie

Une attaque par Cheval de Troie se caractérise par le fait qu'une séquence d'instruction **visant à nuire à l'intégrité** du système est introduite par l'intermédiaire d'un programme tout à fait digne de confiance et remplissant normalement toutes les fonctionnalités que l'on attend de lui.
Il s'agit souvent d'un morceau de code rajouté dans un fichier source ou bien de quelques lignes supplémentaires insérées dans un fichier de commande.

1.3.4 Refus de Service (Denial of Service)

Le seul but de ce type d'attaque est de rendre indisponibles les services offerts par le réseau aux utilisateurs internes ou externes.

Une telle attaque peut prendre différentes formes. On peut par exemple saturer un disque par le courrier électronique ou via FTP. On peut aussi

envoyer des centaines de Mo vers une machine à l'aide de la commande *ping* par exemple [5].

1.3.5 Intrusion

On parle d'intrusion lorsqu'une personne arrive à exécuter des commandes ou lancer des programmes sur un ordinateur où elle n'a normalement pas accès. Le plus gros risque est qu'une personne mal intentionnée se serve d'une machine du réseau pour rebondir et aller s'introduire sur une autre machine afin de brouiller les pistes. Les moyens pour s'introduire sur une machine sont nombreux, on peut citer :

- L'obtention de mots de passe. Cela peut se faire par écoute sur le réseau, par essai des mots de passe les plus courants, par un œil indiscret sur le clavier, etc.

- L'exploitation de trous de sécurité dans le système.

- L'utilisation des accès de confiance. Il existe sur certains systèmes (Unix notamment), un mécanisme qui permet d'autoriser tel utilisateur de telle machine à se connecter sans avoir besoin de mot de passe sur un compte d'une autre machine. Ce mécanisme a été mis en place il y a bien longtemps, pour faciliter le travail de ceux qui possédaient des comptes sur plusieurs machines et qui ne voulaient pas passer leurs journées à taper des mots de passe. Celui-ci s'est depuis avéré très dangereux puisqu'il permet la propagation des attaques.

1.4 Problèmes des machines reliées au Réseau

Les machines reliées au réseau peuvent être vulnérables à deux niveaux: informatique (système d'exploitation et applications) et humain (utilisateurs).

1.4.1 Au niveau du Système Informatique et les applications.

Le problème principal au niveau du système informatique est l'existence de vulnérabilités ou trous de sécurité. Nous pouvons définir une vulnérabilité

[5] La commande ping sera expliquée en détail dans la chapitre 4.

comme *"anything about a computer system that will allow someone to either keep it from operating correctly, or that will let unauthorized people take it over. There are many types of vulnerabilities. They may be, a flaw in the programming of the service, or a misconfiguration in the setup of a service.*

Examples of errors in the programming of services are the large number of buffer overflow vulnerabilities in the programs that run services on port of Internet host computers. Many of these buffer overflow problems allow people to use the Internet to break into and take control of host computers.

An example of a setup misconfiguration is a incorrectly setting directory permissions on your FTP server so people can download the password file. In these cases, the vulnerability is not how the program was written, but with how the program is configured. Allowing file sharing on your Windows 95 or 98 computer when it is not necessary, or failing to put a password on file sharing, is another example". [Haching]:

Le problème est que tous les programmes ont des trous de sécurité, et n'oublions pas qu'un OS n'est qu'un programme. Dans le livre Firewalls et Sécurité Internet, Bellovin et Cheswich écrivent sur forme de "loi mathématique":

Axiome 1 (loi de Murphy) Tous le programmes ont des trous.

Théorème 1 (Lois de gros programmes) les gros programmes contiennent plus de trous que leur taille ne semble indiquer.

Corollaire 1.1 Un programme de sécurité contient des trous de sécurité.
(...) tout programme même s'il semble inoffensif peut contenir des failles de sécurité.

Ces trous de sécurité, lorsqu'ils sont découverts, peuvent être exploités, par des personnes malveillantes pour s'introduire dans le système.

Dans les premières versions de **sendmail** par exemple, il existait beaucoup de trous de sécurité qui permettaient à n'importe qui d'exécuter des

commandes avec des privilèges de **root.** Avec le temps, la plupart de trous (découverts) ont été corrigés, mais de nouveaux trous sont régulièrement découverts.

1.4.2 Au niveau des utilisateurs.

Au niveau des utilisateurs, il existe plusieurs problèmes:

- le mauvais choix des mots de passe (Ceci sera traité en détail au point 1.6.4.)
- la mauvaise utilisation des ressources informatiques, par exemple l'installation des programmes (qui pourrait contenir de virus, des trous de sécurité) sans l'autorisation de l'administrateur.
  le manque d'éducation à la sécurité informatique. Ce qui veux dire que la plupart des utilisateurs ignorent les problèmes de sécurité auxquels le réseau sur lequel ils travaillent est exposé. Ce qui peut provoquer des erreurs involontaires comme l'utilisation de disquettes avec des virus ou l'exécution de chevaux de Troie.

1.5 Les méthodes de défense.

Cette section explique d'une façon simple les différentes méthodes existantes actuellement pour protéger un réseau.

1.5.1 Les Firewalls

Un Firewall est un produit de sécurité, comportant une ou plusieurs composantes (routeurs, ordinateurs, software spécialisé), et qui offre un mécanisme de contrôle d'accès entre un réseau privé et un réseau publique comme par exemple Internet.

Le Firewall détermine :[3com]

- Quels sont les services internes qui peuvent être accédés à partir de l'extérieur.
- Quels éléments externes peuvent accéder aux services internes autorisés.
- Quels services externes peuvent être accédés par les éléments internes.

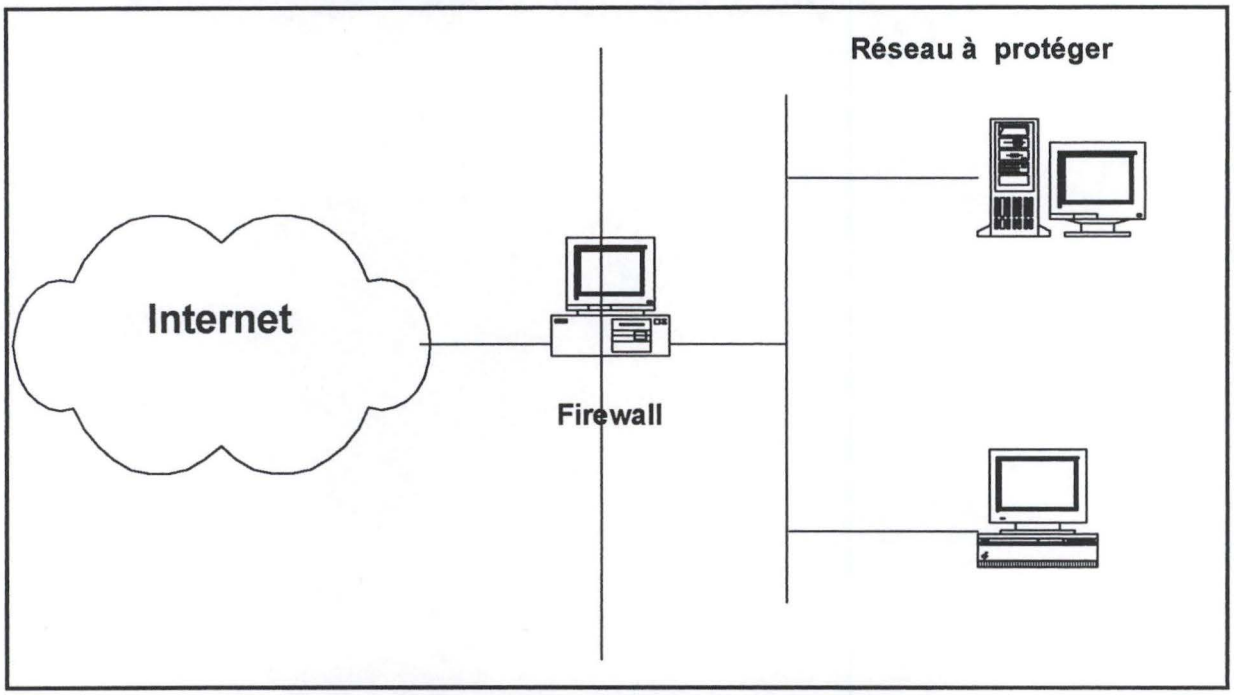

Figure 1-2 : Exemple d'un réseau protégé par un Firewall

Les buts d'un Firewall.

Plusieurs sont les raisons qui nous poussent à utiliser un firewall parmi lesquelles, on peut citer:

- Vouloir se protéger contre des attaques "externes".
- Interdire que des services potentiellement vulnérables entrent ou sortent du réseau.
- Avoir un point de passage obligé permettant de bien vérifier si les règles de sécurité telle que spécifiées dans la **politique de sécurité**[6] de l'établissement sont réellement celles qui sont appliquées. Contrôler le trafic entre le réseau interne et externe, d'auditer/tracer de façon "centrale" ce trafic, éventuellement avoir une vue sur la consommation d'Internet par différents utilisateurs/services.
- Le firewall simplifie la gestion de la sécurité par le fait que celle-ci est consolidée plutôt que distribuée sur chaque station hôte du réseau privé. L'administrateur peut dès lors définir un point de centralisation (check point) à partir duquel il pourra protéger le réseau privé dans son entièreté.

Les limitations du firewall

Nous pouvons relever 3 principales limitations au firewall :

[6] Enoncé général émanant de la direction d'une organisation, et indiquant la ligne de conduite adoptée relativement à la sécurité informatique, à sa mise en oeuvre et à sa gestion.

- Le firewall ne protège pas contre les traîtres auxquels doivent régulièrement faire face les responsables sécurité dans les organisations.

- Le firewall ne prévient pas contre le transfert de fichiers infectés par un virus. Parce qu'il y a une multitude de virus, de systèmes d'exploitation et de manières d'encoder et de compresser les fichiers différents, un firewall peut difficilement scanner chaque fichier dans l'espoir incertain d'en déceler un.

- Le firewall ne prévient pas contre les applications du type Cheval de Troie.

On le voit, l'implémentation d'un firewall soulève une série de questions dont la portée dépasse largement celle du firewall en lui-même et va dépendre essentiellement de la politique de l'entreprise comme de sa culture.

1.5.2 Le Chiffrement

Lorsqu'un intrus a réussi à capturer une information utilisant une des techniques vue en 1.2, il peut faire usage de ces informations. Supposons que l'information capturée est classée top-secret par un gouvernement. On imagine les conséquences que cela pourrait entraîner.

Dans ce cas, le chiffrement peut être utile pour améliorer la sécurité des données transitant sur le réseau.

Définition et vocabulaire.

Le chiffrement est un processus qui transforme un texte lisible, appelé message en claire, en une suite de caractères illisibles appelée message codé. Par un processus inverse appelé déchiffrement on peut retrouver le texte en claire. Pour chiffrer un message les spécialistes font souvent appelle à une clé de chiffrement, cette clé peut être un mot, un nombre ou une phrase, de cette façon le message chiffré dépendra du message en claire et de la clé.

Notation : Nous parleront de message en claire *(P)* et de message chiffré *(C)*. Nous noterons E un algorithme quelconque de chiffrement, D un algorithme de déchiffrement et K la clé.

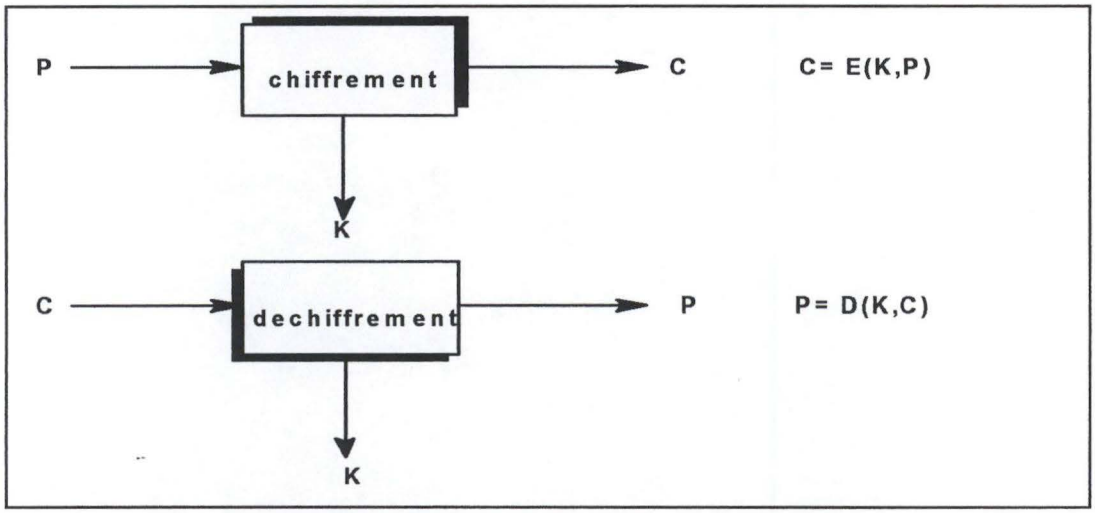

Figure 1-3 : Exemple schématique du chiffrement et du déchiffrement.

Les buts de la cryptographie

En chiffrant le message on évite la lecture ou la modification de celui-ci, mais aussi la fabrication d'un message fictif. La cryptographie protège la confidentialité d'une information.

Les organisations ont besoin de la cryptographie pour protéger :

- la confidentialité des transactions bancaires,
- la protection des systèmes informatiques contre les intrusions,
- les secrets industriels ou commerciaux,
- les sessions de télétravail,
- les secrets médicaux,
- la vie privée,
- les jeux, etc.

Les méthodes de chiffrement.

On peut diviser les méthodes de chiffrement en 2 catégories: le chiffrement par substitution et le chiffrement par transposition.

Les Algorithmes de chiffrement.

Un algorithme de chiffrement est une fonction mathématique utilisée pour le chiffrement et le déchiffrement d'un message. Il existe 2 types d'algorithmes, ceux à clé secrète et ceux à clé publique.

Les algorithmes à clé secrète

Ce sont des algorithmes connus de tous et dont la sécurité repose sur l'utilisation d'une clé secrète. Dans ce cas une même clé sert à chiffrer et décrypter. C'est pour cette raison qu'on les appelle algorithmes symétriques.

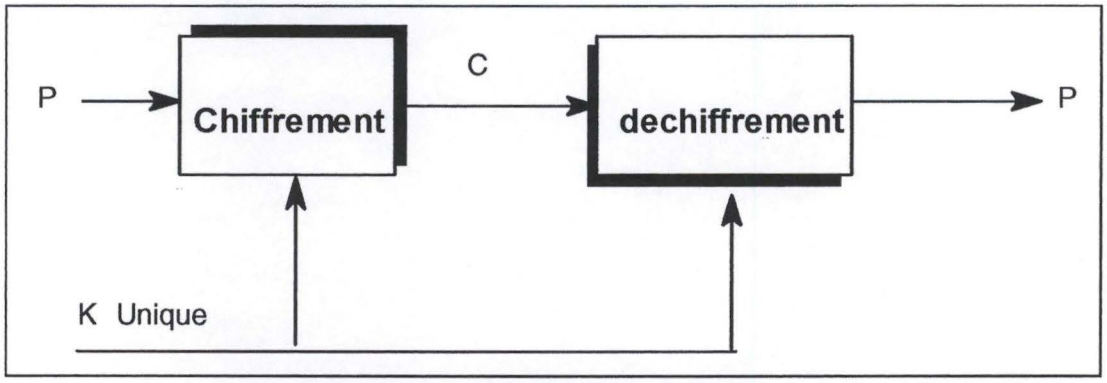

Figure 1-4 : Les algorithmes à clé secrète.

La sécurité de l'algorithme repose sur la clé ; si celle-ci est dévoilée, alors n'importe qui peut chiffrer ou déchiffrer des messages dans ce système car on supposera toujours que l'algorithme est connu par toute la communauté.

A titre d'information disons que les algorithmes de chiffrement les plus connus sont DES et IDEA.

Les algorithmes à clé publique.

Les algorithmes à clé publique utilisent 2 clés différentes, une pour chiffrer le message et une autre pour le déchiffrer. C'est pour cette raison qu'on les appelle algorithmes asymétriques.

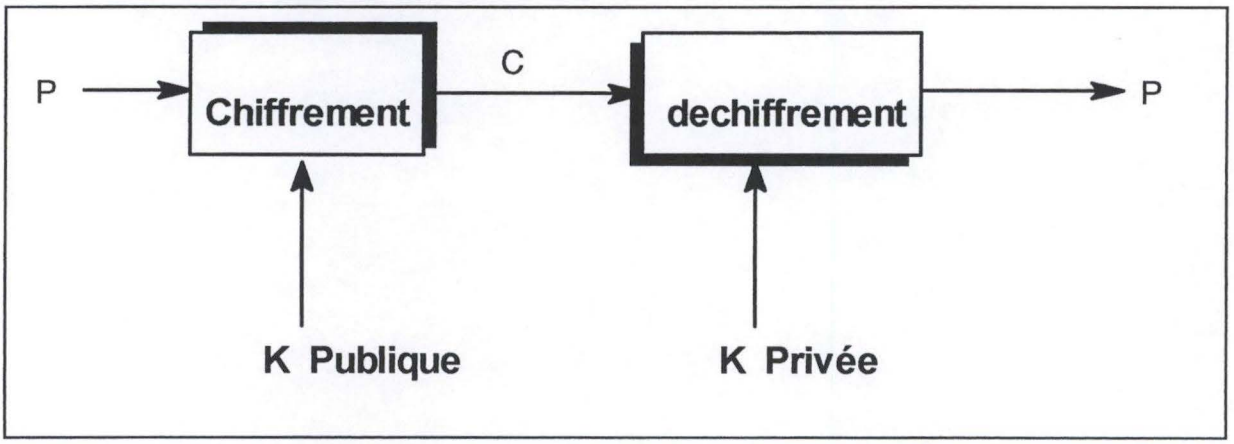

Figure 1-5 : Les algorithmes à clé publique.

L'une des clés est tenue secrète par son détenteur; c'est la clé secrète. L'autre clé peut être connue par tous, c'est la clé publique. Pour envoyer un message à quelqu'un, il suffit de le chiffrer avec la clé publique de la personne. Seul le destinataire pourra déchiffrer la message avec la clé secrète.

Le problème avec le chiffrement à clé publique est qu'il existe forcément une relation mathématique entre la clé publique et la clé privée, relation qui permet théoriquement de déterminer la seconde connaissant la première. Toute la difficulté consiste donc à trouver des algorithmes tels que cette relation ne soit pas exploitable avec un temps de calcul raisonnable.

A titre d'information, disons que un des algorithmes de chiffrement le plus connu est RSA.

Les applications du chiffrement.

Les applications du chiffrement sont très variées. Nous pouvons citer parmi les plus importantes:

- la protection de données,
- la signature électronique,
- les certificats.

La protection des données

Quelque soit le support utilisé pour communiquer (ligne téléphonique normale, ligne louée, réseau sans fil) il est possible de le mettre sur écoute. Le moyen le plus efficace contre ce danger potentiel est de chiffrer les donnés.

Le protection des données a pour but de transformer un message compréhensible par tous en un message seulement lisible par un ou plusieurs destinataires; cette application est d'autant plus importante que l'information circule sur un réseau non privé (comme Internet) ou est stockée sur des ordinateurs ne garantissant pas la confidentialité.

La signature électronique

"Il s'agit d'un code alphanumérique infalsifiable qui garantie qu'une personne déterminée a écrit ou a donné son accord au texte du document auquel la signature est attachée." [John Vacca]

Lorsque l'émetteur envoie un message, il peut éventuellement signer son envoi au moyen de sa propre clé privée. Cette signature pourra être vérifiée à la

réception au moyen de la clé publique de l'émetteur. Ceci permet d'authentifier le message puisque seul l'émetteur possède la clé privée correspondante permettant d'apposer sa signature électronique.

Les certificats

Puisque les personnes qui participent à un échange électronique ne se voient pas, il est dès lors très important de prévoir un mécanisme formel de confirmation de leur identité. C'est ce que l'on appelle ici la certification électronique d'identité.

"Un certificat est un document numérique qui garantie l'appartenance d'une clé publique à une entité, particulier, entreprise ou administration. Ce qui permet d'éviter qu'une personne puisse utiliser une clé pour se faire passer pour quelqu'un d'autre. " [John Vacca]

La certification est réalisée par un tiers certificateur digne de confiance. L'émission de certificats est une procédure simple. Une personne **A** envoi sa clé publique à un certificateur de son choix, ainsi que des preuves de son identité. Le certificateur va alors prendre toutes les mesures nécessaires pour vérifier la provenance de la clé. Il retourne alors un certificat qui atteste de la correspondance entre la clé et l'identité de **A.** Il retourne aussi une chaîne de certificats qui, eux, garantissent la clé publique du certificateur. A utilise alors cette chaîne pour témoigner de la légitimité de la clé publique.

1.5.3 Les Audits de sécurité.

Un audit de sécurité consiste à détecter tous les problèmes possibles dans le système (vulnérabilités) et qui pourraient permettre l'accès à des personnes non autorisées. Il permet aussi de tester si les moyens de prévention et de protection prévus ou en place sont suffisants ou efficaces pour garantir un niveau de risque acceptable. Les audits de sécurité seront expliqués en détail dans le chapitre 4.

1.5.4 Les tests d'intrusion.

Un test d'intrusion est une simulation de situations réelles, réalisé sous contrôle afin d' accéder aux ressources d'un réseau d'ordinateurs, que les responsables espèrent inaccessibles.

Les buts des tests d'intrusion :

- Se mettre dans la situation d'un pirate informatique pour identifier le plus grand nombre possible de problèmes.

En utilisant les vulnérabilités trouvées, le testeur va développer un scénario et essayer de s'introduire dans le système.

- Fournir, aux responsables, une liste exhaustive de tout ce qui a été constaté pour permettre des corrections.

Les résultats des tests d'intrusion permettent d'évaluer différents éléments qui concourrent à la sécurité globale :

- la robustesse des composants,
- la configuration du dispositif,
- la conception de l'architecture,
- ldes procédures d'exploitation et l'administration.

1.5.5 L'Education des utilisateurs.

Le problème principal avec les utilisateurs d'une machine reliée à un réseau est le mauvais choix des mots de passe.

"Un pourcentage élevé d'intrusions de système survient à cause de l'échec du système de mot de passe dans son entièreté.

(...) le problème le plus classique est que les gens ont tendance à choisir de très mauvais mots de passe. Des études successives ont montré que l'on pouvait en toute vraisemblance deviner un mot de passe(...) tout le monde ne choisit pas un mot de passe faible; cependant suffisamment de personnes le font pour qu'une attaque par le biais d'un mot de passe deviné garde une probabilité de réussite. "[Bellovin, Cheswich 1994:12]

Nous comprenons donc que le choix d'un bon mot de passe est nécessaire pour éviter qu'une personne puisse le deviner et s'introduire dans le système.

Avec l'apparition de programmes qui automatisent les tests, deviner un mot de passe est encore plus facile. Le programme **Crack** par exemple qui partant

d'un dictionnaire de mots quelconques, va tester si l'un ou l'autre mot de celui-ci correspond au mot de passe qui donne accès au système. Ce programme va même jusqu'à contourner les astuces assez répandues comme:

- prendre comme mot de passe un mot courant et à le soumettre à des variations faciles à retenir. Par exemple '@', '0' ou 'l' à la place de 'a', 'o' ou 'i'.
- écrire à l'envers ou en alternant les majuscules et minuscules.

Pour réduire les chances d'intrusion du système à cause d'un mauvais mot de passe voici un ensemble de suggestions qui pourrait aider à prévenir ce genre de problèmes.

- Les mots courants, les prénoms, noms de lieux, de personnages littéraires, historiques, termes informatiques etc. ainsi que leurs variations sont absolument à proscrire comme mots de passe.
- Eviter également les chaînes formatées de caractères voisins sur le clavier, par exemple "azertyui", "qsdfghjk", "poiuytre", etc.
- Choisir des mot de passe avec une longueur adéquate.
- Toujours utiliser toute la gamme de caractères disponibles:
  - lettres majuscules et minuscules
  - chiffres
  - autres signes: ponctuation, parenthèses, signes arithmétiques, etc.
- Le programme Crack peut être très utile pour les administrateurs qui pourraient de cette manière tester si les mots de passe des utilisateurs sont fiables.
- Il ne faut jamais écrire le mot de passe sur un bout de papier, ou un post-it collé à l'ordinateur.
- Changer périodiquement les mots de passe.

1.5.6 Les autres.

Finalement, il existe une série d'organismes, de "news groups" et de "mailing lists", qui donne une quantité énorme d'information concernant les problèmes de sécurité informatique. Ces organismes seront traités plus en détail dans le chapitre suivant.

1.6 Conclusion.

La meilleure solution pour la protection sur Internet réside sans doute dans la combinaison de toutes les techniques mentionnées précédemment.

De nos jours, les entreprises veulent choisir des options de haute sécurité dont elles ont besoin pour communiquer, et elles sont donc amenées à utiliser toutes ces techniques de protection.

Comme il n'y a pas et il n'y aura sans doute jamais de réseaux sûrs à 100%, nous pouvons quand même nous protéger d'une majorité de problèmes associés à l'Internet en étant vigilants. Toutefois, Internet continue à grandir en popularité et les statistiques de fraudes et d'attaques risquent de continuer à augmenter si les utilisateurs ne prennent pas conscience que la sécurité est un enjeu capital pour Internet.

Chapitre deux:

Les organismes liés à la sécurité

2.1 Introduction

En dépit des mesures prises pour améliorer la sécurité sur Internet, les organisations auront encore des incidents à déplorer. Des incidents tels que des attaques, des erreurs, etc.

Pour combattre ces menaces, un nombre croissant d'organismes gouvernementaux et privés du secteur informatique ont établi une coalition pour échanger l'information et centraliser les réponses. Voici liste non exhaustive, ainsi qu'une petite description, des mécanismes d'alerte les plus importants:

2.2 CERT-CC (Computer Emergency Response Team - Coordination Center)

Le CERT Coordination Center est l'organisation qui s'est développée à partir de l'équipe de réaction aux urgences formée par DARPA. Ses objectifs sont :

- donner une assistance technique 24 heures sur 24 pour réagir à des incidents de sécurité,
- donner des alertes sur les vulnérabilités découvertes ainsi que des solutions possibles,
- fournir des documents et organiser des séminaires,
- mener des recherches destinées à améliorer la sécurité des systèmes existants,
- publier une variété d'alertes de sécurité.

La figure 2.1 donne un exemple d'alerte de sécurité publié par le CERT.

```
CERT® Advisory CA-99-07 IIS Buffer Overflow

Revised: June 18, 1999
Originally released: June 16, 1999
Source: CERT/CC

Systems Affected

Machines running Microsoft Internet Information Server 4.0

I. Description
Buffer overflow vulnerabilities affecting Microsoft Internet
Information Server 4.0 have been discovered in several libraries, including
libraries that handle .HTR, .STM, and .IDC files.

A tool to exploit at least one of the vulnerabilities has been
publicly released.

II. Impact
These vulnerabilities allow remote intruders to execute arbitrary
code with the privileges of the IIS server. Additionally, intruders can use
this vulnerability to crash vulnerable IIS processes.

III. Solution
Microsoft has released and updated Microsoft Security Bulletin MS99-
019, which points to a patch for these vulnerabilities. We encourage you to
read this bulletin, available from

http://www.microsoft.com/security/bulletins/ms99-019.asp

We will update this advisory as more information becomes available.
Please check the CERT/CC Web site for the most current revision.
```

Figure 2-1: Un exemple d'alerte de sécurité.

Nous devons noter que *"le Cert s'est fixé comme règle de ne pas poster de telles alertes avant d'avoir trouvé un antidote. Mais cela peut prendre de mois (...) "* [John Vacca]

De plus, le CERT fournit un serveur FTP anonyme: ftp://info.cert.org , où des documents relatifs à la sécurité, les précédents avis du CERT-CC et des outils y sont archivés. Les informations fournies par le CIAC sont disponibles à l'adresse suivante: http://www.cert.org. Ces informations sont gratuites.

2.3 CIAC (Computer Incident Advisory Capability)

Le CIAC a été créé en 1989. Il fournit l'assistance technique et l'information dans le domaine de la sécurité informatique aux employés et aux sociétés travaillant pour le département de l'énergie du Lawrence Livermore Laboratory des Etats-Unis. Le but du CIAC est de fournir:

- des formations,
- les dernières vulnérabilités découvertes ainsi que des solutions possibles. (Ces informations sont les mêmes que celles publiées par le CERT mais avec quelques mois de retard).
- la publication des canulars circulant sur Internet,
- un ensemble de documents sur une grande variété de sujets concernant la sécurité.
- De plus, le CIAC met à la disposition de tout intéressé un ensemble de logiciels de sécurité gratuits.

Les informations fournies par le CIAC sont disponibles à l'adresse suivante: http://ciac.llnl.gov. Ces informations sont gratuites.

2.4 COAST (Computer Operations, Audit and Security Technology)

Le COAST poursuit un ensemble de projets et d'enquêtes de recherche en sécurité informatique au Computer Science Department de l'Université de Purdue. Il est destiné à fonctionner en étroite liaison avec les chercheurs et les ingénieurs des grandes compagnies et des agences gouvernementales.
Les informations fournies par le COAST sont disponibles à l'adresse suivante: http://www.cs.purdue.edu/coast/coast.html. Ces informations sont gratuites.

2.5 FIRST (Forum of Incident Response and Security Team)

Le FIRST est constitué d'une soixantaine d'équipes intégrant des représentants de l'administration, de l'industrie, des constructeurs de matériel informatique et des universités américaines. Le FIRST est chargé de mettre en place des unités de riposte individuelle (individual response teams), chargées d'établir des procédures de traitement des incidents dans leurs champs de compétence. Elles doivent être en mesure de communiquer avec les autres services du FIRST.
Les informations fournies par le FIRST sont disponibles à l'adresse suivante: http://www.first.org. Ces informations sont gratuites.

2.6 NIST (National Institute of Standards and Technologies) Computer Security Ressource Clearinghouse

Le NIST *"est un organisme d'état qui dépend du ministère du Commerce des Etats-Unis, et qui propose des normes et des recommandations auxquelles se conforment les autorités fédérales et le secteur privé"*. [John Vacca]

En matière de sécurité sur Internet, le but principal du NIST est de publier des normes et des recommandations sur des nombreux aspects tels que:

- la sensibilisation des utilisateurs des systèmes informatiques au sujet de la sécurité informatique,
- les normes cryptographiques,
- l'utilisation de mots de passe,
- les normes de sécurité du commerce électronique,
- les virus, etc.

Toutes les informations concernant le FIRST sont disponibles à l'adresse suivante: http://csrc.ncsl.nist.gov. Ces informations sont gratuites.

2.7 Le site de la sécurité de Internet Security Systems (ISS).

Internet Security Systems est une société commerciale qui fournit des outils de gestion de la sécurité, comme la détection de vulnérabilités et la détection d'intrusions.

De plus, le ISS fournit un site appelé Xforce qui donne:

- une grande quantité d'informations concernant la sécurité,
- une liste des dernières vulnérabilités connues ainsi que des solutions possibles,
- un ensemble de mailing lists qui traitent de problèmes liés à la sécurité,
- un ensemble des liens vers de sites concernant la sécurité informatique,
- une base de données avec une grande quantité de vulnérabilités.

Les informations fournies par ISS sont disponibles à l'adresse suivante: http://xforce.iss.net/. Ces informations sont gratuites.

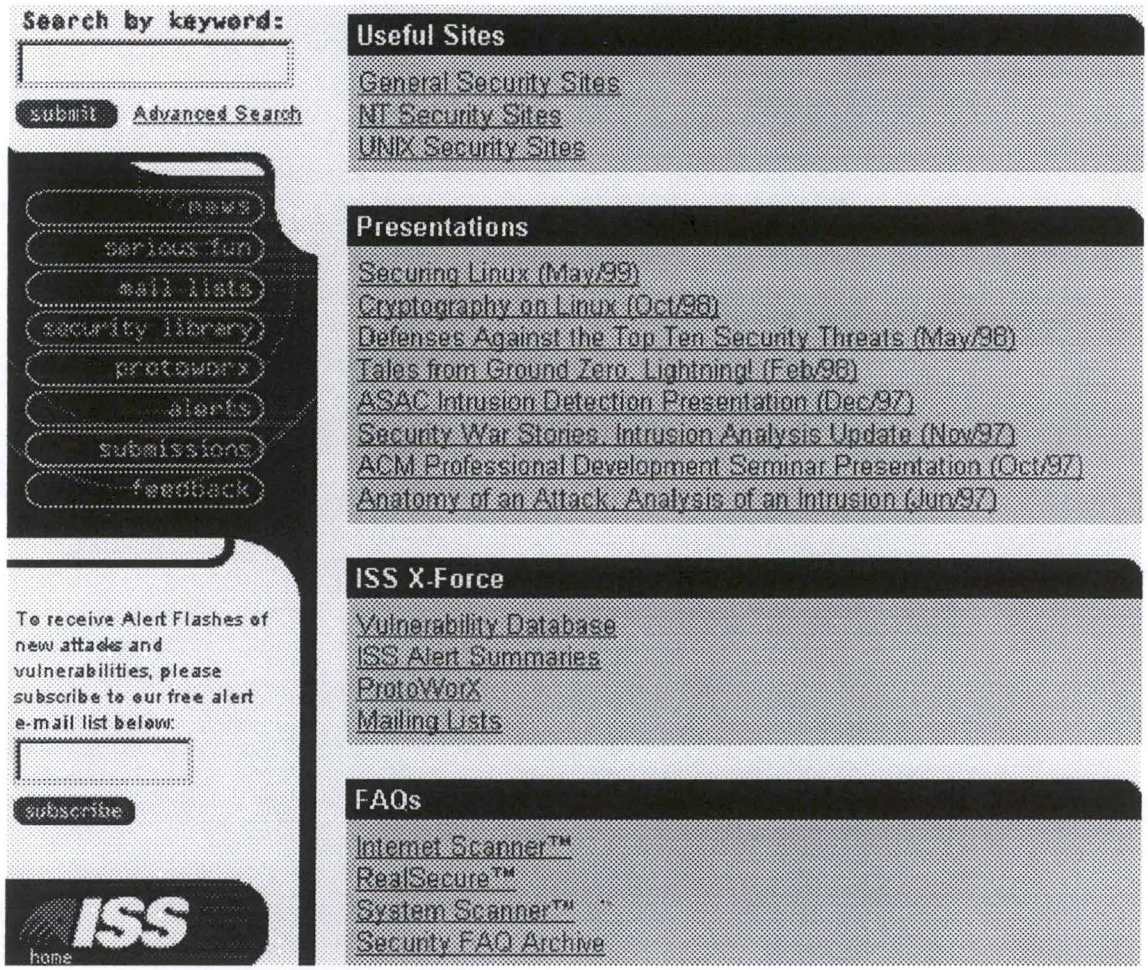

Figure 2-2 : Un exemple du site Xforce de ISS

2.8 Mailing Lists (ML)

Une Mailing list est une liste d'adresses de personnes qui sont intéressées par le sujet de discussion auquel est consacré celle-ci. Elle est en général gérée par un logiciel qui enregistre automatiquement les abonnements et les désabonnements à cette liste.

Le principe de fonctionnement est simple :

Il suffit de poster un message vers l'adresse e-mail de la ML. Celui-ci est alors automatiquement envoyé aux membres qui peuvent répondre et réagir en postant à leur tour.

Les Mailing Lists de la sécurité

ISS fournit un ensemble de mailing lists dont les plus importantes sont :

- **Alert**

Cette ML contient des informations sur les points suivants:

- les nouveaux produits de sécurité et sur les mise à jour.

- les nouvelles vulnérabilités qui ont été trouvées.
- les nouvelles FAQ's sur la sécurité
- les nouvelles techniques d'intrusion

- **NSA - Network Security Assessment**

Cette ML traite des sujets suivants:

- Comment faire une évaluation des serveurs, des réseaux, et des firewalls.
- Quels sont les contrôles de vulnérabilité qui devraient faire partie d'un audit.
- Comment évaluer l'état de sécurité des réseaux, des firewalls et des serveurs.
- Quel est l'écart entre la politique de sécurité « écrite » et la politique de sécurité « appliquée ».
- Discussions sur les dernières vulnérabilités apparues sur les réseaux
- Comment rédiger un rapport sur toutes les données à analyser.

- **SecTech - Security Technology**

Cette ML est destinée à tenir au courant sur les derniers progrès technologiques à propos de sécurité de réseau, incluant:

- les information sur les produits de sécurité commerciaux, de domaine publique et shareware.
- les informations sur les nouvelles mises à jour d'un produit de sécurité, et les patchs de sécurité.

Pour s'abonner à cette liste il suffit d'aller à l'adresse suivante :
http://xforce.iss.net/maillists/

La CERT Advisory Mailing List donne des informations sur les dernières vulnérabilités découvertes , informations telles qu' une description de la vulnérabilité, l'impact et les solutions. Pour s'abonner à cette liste il suffit d'aller à l'adresse suivante : http://www.cert.org/contact_cert/certmaillist.html

```
Date: Fri, 18 Jun 1999 18:00:54 -0400
From: CERT Advisory <cert-advisory@cert.org>
To: cert-advisory@coal.cert.org
Subject: CERT Advisory CA-99.07 - New Information regarding IIS
Reply-To: cert-advisory-request@cert.org
Organization: CERT(sm) Coordination Center -  +1 412-268-7090

-----BEGIN PGP SIGNED MESSAGE-----

CERT Advisory CA-99-07 IIS Buffer Overflow

   Revised: June 18, 1999
   Originally released: June 16, 1999
   Source: CERT/CC

Note: This re-distribution of CA-99-07 contains new information
regarding variations of the IIS vulnerability that was widely reported this
week. In particular, we encourage sites to obtain and install the patch
that is available from Microsoft which addresses all of the variations of
this vulnerability.

Systems Affected

* Machines running Microsoft Internet Information Server 4.0
I. Description

Buffer overflow vulnerabilities affecting Microsoft Internet Information
Server 4.0 have been discovered in several libraries, ncluding libraries
that handle .HTR, .STM, and .IDC files.

A tool to exploit at least one of the vulnerabilities has been    publicly
released.

II. Impact

These vulnerabilities allow remote intruders to execute arbitrary code with
the privileges of the IIS server. Additionally, intruders can use this
vulnerability to crash vulnerable IIS processes.

III. Solution

   Microsoft has released and updated Microsoft Security Bulletin    MS99-
019, which points to a patch for these vulnerabilities. We encourage you to
read this bulletin, available from
http://www.microsoft.com/security/bulletins/ms99-019.asp

   We will update this advisory as more information becomes available.
   Please check the CERT/CC Web site for the most current revision. (...)
```

Figure 2-3 : Un exemple de Mail envoyé par le CERT.

Il existe une grande quantité de ML qui n'ont pas été citée ici. Par exemple, tous les constructeurs de produits de sécurité ont leurs propres ML. Il existe aussi une ML appelée Netbugtraq qui traite des problèmes de sécurité liés à Windows NT et un grand nombre de ML qui traitent des virus.

2.9 Les News groups (NG)

Identifications des News groups les plus actifs

Le concept de News est né du regroupement de messages autour d'un pôle d'intérêt, où, pendant une durée de temps donnée, tous les courriers envoyés sont conservés. Ainsi, sur un forum réservé à Unix, les questions des uns sont envoyées par mail et quelques heures plus tard d'autres peuvent y répondre. Les News sont de formidables réservoirs d'informations vivants.

Alors que les courriers électroniques entre individus ou au travers de ML sont stockés dans les boîtes aux lettres de chacun des correspondants, les News ne sont pas envoyées à tous les utilisateurs. Mais tout intéressé peut les consulter.

Quels sont les News Groups (NG) les plus fréquentés ?
Après une recherche minutieuse sur l'ensemble de News Groups nous avons déterminer que les NG les plus actifs sont:

News groups liés à la sécurité sur Unix	
• comp.security.unix	Discussions sur la sécurité des systèmes Unix.
• comp.unix.admin	Administration du système UNIX et sa sécurité.
• comp.unix.questions	Les questions les plus souvent posées.
• comp.unix.solaris	Questions sur l'installation, les ressources et la sécurité.
• comp.sys.sun.admin	Discussions sur l'administration et la sécurité des machines Sun.
• comp.sys.sun.hardware	Discussions sur le hardware, les produits et sur les patchs de Sun.
• comp.unix.misc	Informations diverses sur Unix
• comp.unix.shell	Utilisation et programmation en Shell Unix
• comp.os.linux.misc	Informations diverses telles que la sécurité, la configuration et l'administration de Linux
• comp.os.linux.networking	Gestion de réseaux sous Linux.
• comp.os.linux.setup	Configuration et administration de Linux
News groups liés à la sécurité sur Windows NT et à la sécurité en général	
• comp.os.ms-windows.nt.admin.security	Discussions sur la sécurité de Windows NT
• alt.security	Discussions sur la sécurité en général.
• comp.security.firewalls	Informations sur les firewalls
• comp.security.misc	Divers aspects de la sécurité informatique et de réseau.
• fr.comp.securite	Discussions autour de la sécurité informatique, et les manières de corriger les points faibles des systèmes informatiques en matière de sécurité.

A titre d'information disons qu'il existe également des NG qui traitent des virus. Mais ces NG ne sont pas traités ici.

2.10 Conclusion

Le problème de la sécurité est toujours d'actualité, des dizaines de vulnérabilités sont trouvées tous les jours. Cependant il y a un grand nombre de moyens pour en être informé et des solutions possibles. Mais encore faut-il savoir qu'ils existent.

Chapitre 3 : Les protocoles TCP/IP

3.1 Introduction.

Le U.S. DoD (departement of Defense) a mis en oeuvre un ensemble de protocoles, qui permettent à des ordinateurs de partager des ressources à travers un réseau. Cet ensemble de protocoles est appelé TCP/IP (Transmision Control Protocol/Internet Protocole), du nom des deux protocoles majeurs le composant.
TCP/IP est une architecture en quatre couches [Van Bastelaer :4]

3.2 Architecture des protocoles TCP/IP

On distingue dans le monde DOD quatre niveaux de couches majeurs : [Van Bastelaer :4]

- **Couche Accès Réseau**

N'importe quel réseau physique peut-être a priori utilisé pour transporter le protocole TCP/IP. Les réseaux les plus souvent utilisés sont Token-Ring, Ethernet, FDDI, X25, ATM, FDDI etc.

- **Couche Internet (IP - Internet Protocol)**

La couche IP est une couche "sans connexion"[1]. Cette couche est chargée de l'acheminement des paquets de données (appelés datagrammes) au travers du réseau.

- **Couche Transport**

La couche Transport est responsable du transfert de bout-en-bout des données au travers le réseau.

Il existe deux protocoles de transport.

Le protocole TCP (Transmission Control Protocol) assure que toutes les données arrivent au destinataire sans erreurs et dans l'ordre d'émission. TCP offre un service en mode connecté.

Le deuxième protocole est UPD (User Data Protocol). ce protocole fonctionne en mode non connecté Il ne fait aucun contrôle d'erreur, ne vérifie pas la bonne réception des données, ni le respect dans l'ordre d'émission.

- **Couche Application**

Enfin, la couche application comporte un certain nombre d'applications standardisées qui s'appuient elles-mêmes sur TCP ou UDP. Elle comprend l'émulation de terminal (TELNET), le transfert de fichiers (FTP) et la messagerie (SMTP).

Chaque couche de la pile ajoute des informations de contrôle, de manière à garantir une transmission de données correcte.

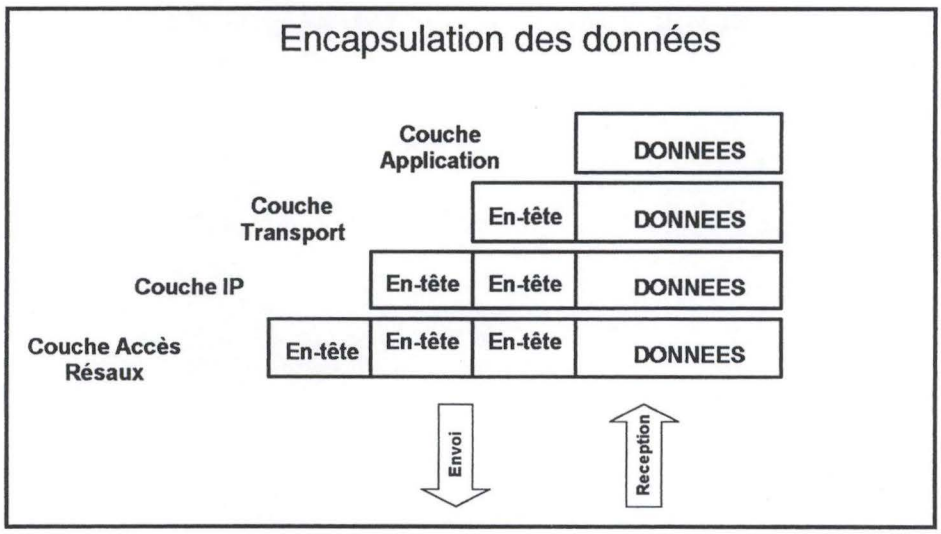

Figure 3-1:Encapsulation des données

[1] Le terme **sans connexion** signifie que IP ne maintient aucune information d'état concernant les datagrammes successifs. Chacun d'eux est géré indépendamment de tous les autres. Ceci signifie également que les datagrammes IP peuvent être délivrés en désordre.[TCP/IP]

3.2.1 Couche Accès Réseau

Les protocoles de cette couche fournissent au système les moyens nécessaires lui permettant de transmettre des données vers d'autres machines périphériques directement connectées sur le réseau. Elle définit l'utilisation de réseau afin de transmettre un datagramme IP.

Les fonctions qui sont exécutées à ce niveau comprennent l'encapsulation des datagrammes dans les trames transmises par le réseau et la mise en correspondance des adresses IP avec les adresses physiques qu'utilise le réseau. L'une des grandes forces de TCP/IP réside dans son plan d'adressage qui permet d'identifier précisément chaque machine-hôte connectée à Internet. Cette adresse IP doit être convertie en l'adresse appropriée du réseau physique sur lequel le datagramme est transmis.

3.2.2 Couche Internet

Le protocole Internet est l'élément du réseau Internet, ses fonctions incluent:

- La définition du datagramme, qui est l'unité de base des transmissions sur Internet.
- La définition du plan d'adressage Internet.
- La circulation de données entre la couche Accès Réseau et la couche Transport machine-hôte à machine-hôte.
- L'acheminement des datagrammes vers les ordinateurs à distance.
- La fragmentation et réassemblage des datagrammes.

Les adresses IP [Bellovin, Cheswich 1994]

Toutes les machines se trouvant dans un réseau possèdent une adresse IP. Cette adresse est codée sur 32 bits et partagée en deux parties: une partie qui permet d'identifier le **réseau** et une partie qui permet d'identifier la **machine**.

Ces adresses sont de la forme a.b.c.d dont a,b,c et d sont codé sur 8 bits. Un exemple d'adresse IP est 128 .40.0.12. Il a principalement cinq classes d'adresses IP.

Classe	Partie Machine	Partie Reseau	Bits de poids fort	Partie réseau	Partie machine	Nombre d'adresse possibles
A	**a**	**b.c.d**	**0**	**7**	**24**	**16 777 214**
B	**a.b**	**c.d**	**10**	**14**	**16**	**65 534**
C	**a.b.c**	**d**	**110**	**21**	**8**	**254**
D	**a.b.c**	**d**	**1110**	**adresses multidestinataires**		**268 435 456**
E	**a.b.c.d**		**1111**	**expérimentale**		

Figure 3-2 : Format des adresses.

On remarquera aussi que les adresses "tout à zéro" out "tout à un" sont réservées.

Les datagrammes

Les protocoles TCP/IP ont été développés pour transmettre des données sur ARPANET, qui était un réseau à commutation de paquets.
Le datagramme correspond au format d'un paquet défini par le protocole Internet.

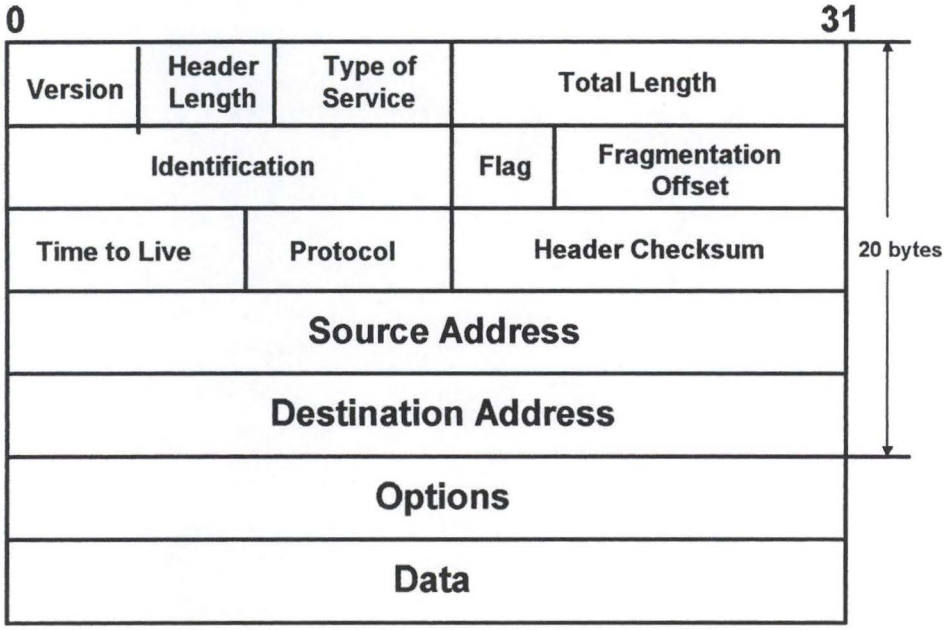

Figure 3-3: Le datagramme

Les 5 (6) premiers mots de 32 bits représentent les informations de contrôle appelées en-tête.

Puisque la longueur de l'en-tête est variable, elle induit un champ appelé longueur de l'en-tête en mots *"Header Length"*. L'en-tête contient toutes les informations nécessaires à la transmission du paquet.
Si l'adresse de destination correspond à l'adresse d'une machine-hôte connectée au réseau local, le paquet est transmis directement vers la destination. Dans le cas contraire, le paquet est transmis vers un routeur afin d'être transmis à la machine-hôte.

Acheminement des datagrammes

Il existe deux types de machines périphériques sur un réseau :

- Les routeurs qui transmettent les paquets entre réseaux.
- Les machines-hôtes (les ordinateurs qui appartiennent au réseau).

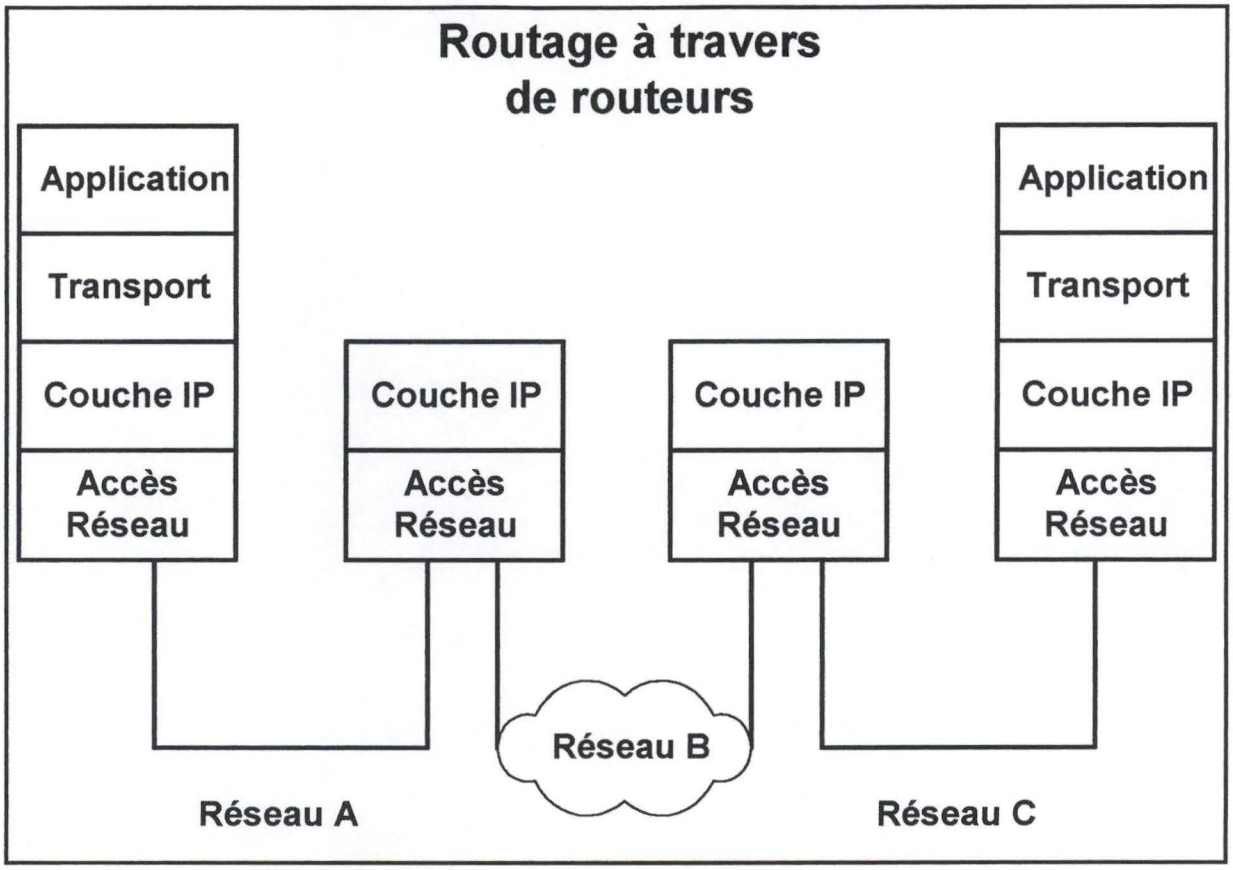

Figure 3-4 : Le routage à travers les passerelles ou routeurs.

Les machines-hôtes traitent les paquets à travers les 4 couches de protocole alors que les passerelles (intermédiaires) traitent les paquets jusqu'à la couche Internet au sein de laquelle la voie de routage des données est déterminée.

Le protocole ICMP Internet Control Message Protocol

Une partie du protocole IP Correspond au protocole ICMP défini dans le RFC 792. "Le fonctionnement d'Internet est piloté de façon interne, de proche en proche, par les routeurs . Lorsqu'un imprévu se produit, l'événement est rapporté par le protocole ICMP qui est également utilisé pour tester Internet.[Tanembaum]

Les messages ICMP sont transmis à l'intérieur des datagrammes IP comme le montre la figure 3-5.

Figure 3-5 : Message ICMP

Il existe environ une douzaine de messages. Ces messages sont de deux types:

- des messages d'information permettant par exemple de vérifier le bon fonctionnement d'un routeur,
- ou des messages d'erreur signalant par exemple que la machine de destination ou le réseau auquel appartient le machine n'existe pas, ou qu'un datagramme à été rejeté par un routeur.

3.2.3 Couche transport

Les deux protocoles les plus important de la couche transport sont :

- Le protocole de datagramme utilisateur (UDP: User Datagram protocol)

UDP offre un service de transmission de datagrammes sans connexion.

- Le protocole de contrôle de la transmission (TCP:Transmission Control Protocol)

TCP assure un service de transmission de données fiable avec une détection et une correction d'erreurs de bout en bout.

Les deux protocoles transmettent des données entre la couche application et la couche Internet.

Protocole UDP (User Datagram Protocol)

UDP est un protocole qui ne garantie pas la connexion de données ni le respect d'ordre d'émission. Avec ce protocole les applications peuvent encapsuler les datagrammes IP et les envoyer sans établir une connexion.

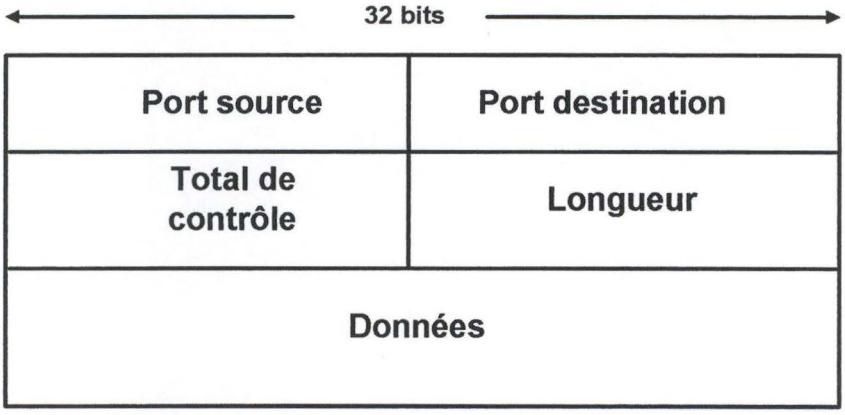

Figure 3-6 : Format du message UDP

UDP est utilisé pour transmettre de faibles quantités de données, où le coût de la création de connexions et le maintient de transmissions fiables s'avèrent probablement supérieurs au travail dû à la retransmission de la totalité des données.

Protocole TCP.

TCP fournie *"des circuits virtuels fiables aux processus utilisateurs. Les paquets endommagés ou perdus sont retransmis; les paquets qui arrivent sont réordonnés si cela est nécessaire pour retrouver l'ordre original de transmission".*

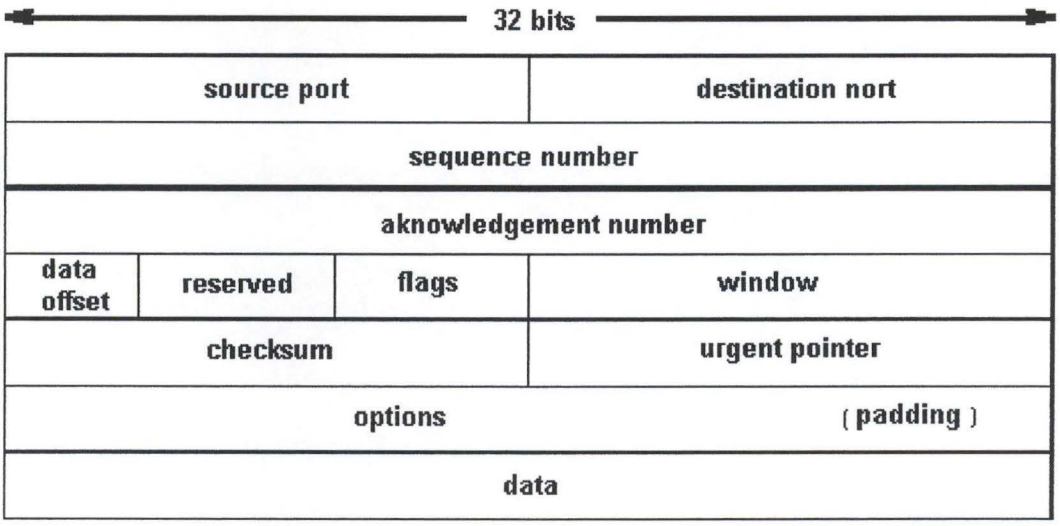

Figure 3-7 : Format d'un segment TCP

TCP est également responsable de la transmission des données provenant du protocole IP à l'application appropriée. Un numéro de 16 bits, appelé "numéro de port" permet d'identifier l'application destinatrice des données. Les numéros de "ports source" et "port destination" sont contenus dans le premier mot de l'en-tête du segment. La transmission correcte des données à destination et à partir de la couche **application** constitue une partie importante des activités que les services de la couche **transport** assurent.

3.2.4 Couche Application

La couche **application** constitue le sommet de l'architecture TCP/IP. Cette couche inclut tous les processus qui utilisent les protocoles de la couche **transport** pour transmettre des données. Il existe de nombreux protocoles d'application, la plupart assurent les services utilisateur qui sont toujours ajoutés au niveau de cette couche. Les protocoles d'applications les plus répandus sont:

TELNET (Network Terminal Protocol)

Le protocole de terminal de réseau, qui permet l'ouverture d'une session à distance sur un réseau. A l'aide d'un logiciel Telnet, un utilisateur se branche de son poste de travail sur un ordinateur étranger pour exploiter les programmes qui s'y trouvent, si, évidement, il en a la permission.

FTP (File Transfert Protocole)

Le protocole de transfert de fichiers, qui est utilisé pour le transfert de fichiers, et qui permet aux utilisateurs de télécharger des fichiers depuis un autre système informatique ou un réseau local relié à Internet. Il est également possible d'envoyer ses propres fichiers au système distant en utilisant FTP. Le protocole FTP réalise le transfert des fichiers en utilisant les services offerts par TCP.

SMTP (Simple Mail Transfert Protocole)

Le protocole de transfert de courrier, qui est utilisé pour le courrier électronique. Chaque utilisateur d'une machine hôte possède une boîte aux lettres sur sa machine. Avec le protocole SMTP, tout utilisateur à la possibilité d'envoyer un message à tout autre utilisateur, quelle que soit la machine hôte sur laquelle il travaille, a travers le réseau Internet. Le protocole SMTP utilise les services offerts par TCP.

Autre Applications

Le service DNS (Domain Name Service)

Il également appelé Name service. Cette application établit la correspondance entre les adresses IP et les noms attribués aux machines-périphériques du réseau.

Le protocole RIP (Routing Information Protocol)

Le routage est l'un des principaux éléments du fonctionnement de TCP/IP. Les systèmes en réseau utilisent RIP pour échanger des informations concernant le routage des données.

Le protocole NFS (Network File System)

Le " Network File System " (NFS) est un système développé depuis 1984 par Sun Microsystems. Il a pour but de fournir un accès transparent aux disques distants. Cela signifie que, grâce à NFS, l'utilisateur peut manipuler des fichiers distants de la même manière que des fichiers locaux, sans avoir besoin de se connecter à différents systèmes pour y avoir accès. Plutôt que de dupliquer des répertoires communs sur

chaque machine, NFS permet d'avoir une seule copie de ce répertoire qui est partagée par l'ensemble des systèmes du réseau.

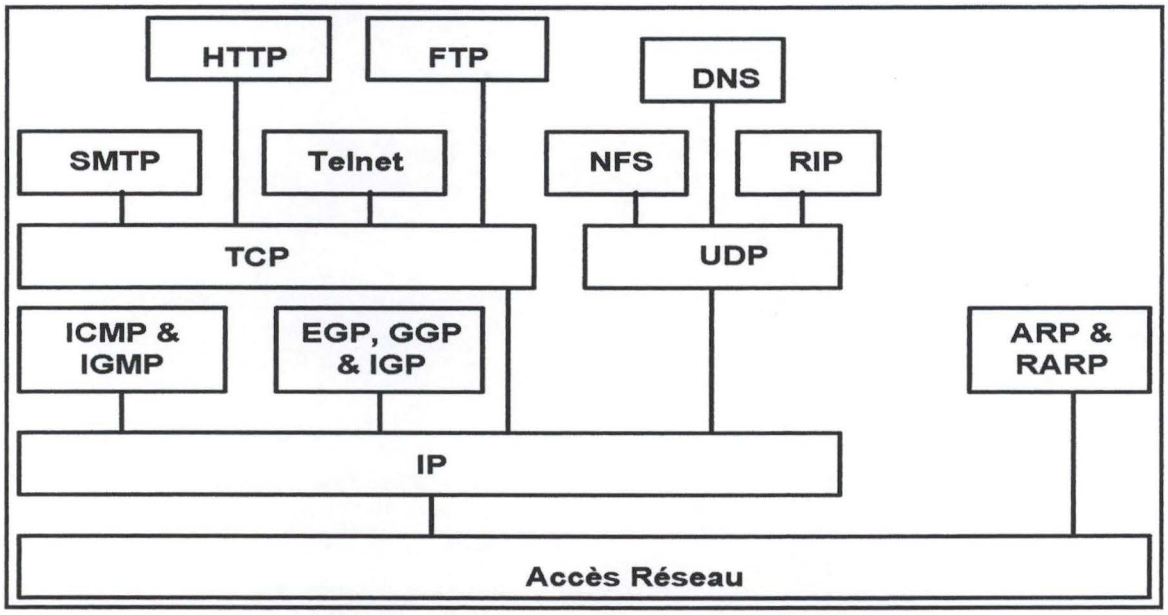

Figure 3-8 : Liens entre les différents protocoles.

Cette figure permet de mieux visualiser les liens qui existent entre les différents protocoles d'une machine-hôtes déterminée. Les protocoles d'applications tels que FTP et TELNET se trouvent dans la partie supérieure de la figure.

On peut constater que FTP, TELNET et SMTP dépendent de TCP, alors que NFS, DNS et RIP dépendent de UDP. Quelques protocoles de type application, tels que le protocole de passerelle externe (EGP), qui est un autre protocole d'acheminement, n'utilisent pas les services de couche transport; ils utilisent directement les services IP.

Chapitre Quatre: Les audits de vulnérabilités et les logiciels d'audit

4.1 Introduction

Auparavant, les administrateurs des réseaux et les responsables de la sécurité comptaient sur un mélange d'informations en provenance de l'industrie et sur leur propre expérience quand ils tentaient de résoudre des problèmes liés à la sécurité informatique.

A présent, il existe des outils automatiques conçus pour aider les administrateurs à identifier les vulnérabilités de leurs réseaux et y apporter des solutions appropriées. Ces outils seront appelés les *"Security Auditing Tools" (SAT)*.

En 1995, deux chercheurs diffusent SATAN, un *SAT*, qui a causé une panique générale parmi les administrateurs. Ils ont craint que des pirates même débutants allaient disposer d'un outil qui leur permettrait d'exploiter les vulnérabilités pour pénétrer dans le réseau.
Leur crainte ne s'est révélée que partiellement fondée. En effet, ces pirates disposaient déjà des moyens comme les mailing lists et les news groups. Simplement SATAN leur a permis d'exécuter de manière automatique ce qu'auparavant ils faisaient manuellement.

Les SAT existant maintenant peuvent identifier dans une machine ou dans des réseaux entiers une grande quantité de vulnérabilités. Les rapports détaillés que ces produits génèrent, permettent aux administrateurs de mieux se préparer pour les attaques.

4.2 Les audits de vulnérabilités

Un audit de vulnérabilités est un mécanisme qui consiste à détecter tous les problèmes possibles dans le système (vulnérabilités) et qui pourraient permettre l'accès à des personnes non autorisées. Il permet aussi de tester si les moyens de prévention et de protection prévus ou en place sont suffisants ou efficaces pour garantir un niveau de risque acceptable. Les audits de sécurité seront expliqués en détail dans le chapitre 4.

Nous distinguons deux types d'audit de vulnérabilités :

- Les audits de vulnérabilité externes.
- Les audits de vulnérabilités internes.

4.2.1 Les audits de vulnérabilité externes.

L'audit de vulnérabilités externe vise à déterminer l'état de sécurité d'un réseau utilisant le protocole TCP/IP.

Il doit être appliqué en différents endroits du réseau afin de déterminer les risques inhérents à chaque position.

Il permettra de constater les défaillances dans les systèmes de protections (Firewalls,...) ainsi que les systèmes d'exploitation qui les composent. Il permet également d'indiquer la présence de vulnérabilités sur les machines composant le réseau analysé.

A partir de ces constatations, une amélioration de la politique de sécurité interne pourra être construite afin de mieux préserver une entreprise contre des dangers de perte de disponibilité, d'intégrité, de confidentialité.

L'audit de sécurité révèle les vulnérabilités de sécurité au niveau des services proposés sur le réseau par les différentes machines qui le composent.

L'audit de sécurité externe ne perturbe pas les machines du réseau hormis potentiellement celle qui est en cours d'analyse.

L'audit de sécurité externe se pratique depuis une machine située sur un segment de réseau et balayera toutes les adresses réseaux qui lui auront été précisées.

L'audit externe produit un rapport de l'état de la sécurité qui, joint avec ceux d'autres analyses, permettra de déduire l'évolution de la sécurité du réseau de l'entreprise.

4.2.2 Les audits de vulnérabilités internes.

L'audit de sécurité interne vise à déterminer l'état de sécurité d'un système d'exploitation et de lui seul. Il doit être appliqué sur les machines d'un réseau local relié à un réseau public. Il peut également être appliqué dans un souci de sécurité interne de l'entreprise.

L'audit de sécurité interne permettra de constater les défaillances dans les configurations ainsi que les vulnérabilités internes des différents serveurs et stations analysés travaillant sur le réseau.

A partir de ces constatations, une amélioration de la politique de sécurité interne pourra être construite afin de mieux préserver l'entreprise contre des dangers de perte d'authenticité, d'intégrité, de confidentialité et de non-répudiation.

Dans la majorité des cas, les entreprises reliées à Internet pensent que leur dispositif de protection est suffisant. Il s'agit là de la "**vulnérabilité sécurité**" par excellence, puisque l'entreprise fait alors confiance à une machine qui représente elle-même un risque. Si ces dispositifs venaient à être outrepassés, ou que l'agresseur se situe à l'intérieur même de l'entreprise, la machine se trouverait à sa merci.

Le système d'exploitation présente généralement beaucoup de vulnérabilités sur un ordinateur. Il offre des services et peut donc être extrêmement vulnérable si sa configuration manque de rigueur.

Un audit de sécurité interne se fait avec un outil spécialisé qui sera installé au sein du système d'exploitation que l'on désire analyser. Il procédera à des analyses de la configuration selon les capacités de ce système d'exploitation.

Il pourra ainsi analyser :

- L'intégrité des comptes utilisateurs : afin d'éviter l'attribution de privilèges trop dangereux pour le système d'exploitation.
- L'intégrité des sauvegardes : afin de déterminer quels fichiers ne sont pas sauvegardés.

- Les permissions d'accès aux fichiers : afin de s'assurer que les permissions d'accès ne présentent pas de risques d'accès illégaux
- Les attributs de fichiers : afin de détecter quels fichiers ont été modifiés par rapport à leurs modèles originaux.
- Les éventuels virus dissimulés : afin d'éviter leur activation. (Avec un antivirus)
- Les paramètres de connexion : afin de ne pas laisser des possibilités d'attaques
par les points d'entrées.
- Les intégrités d'objets : les objets logiciels ou matériels selon le système d'exploitation et leurs protections.
- La force de résistance des mots de passe : une mauvaise politique à ce niveau permet la détection rapide des mots de passe des utilisateurs.
- Les procédures de démarrage : c'est l'endroit privilégié pour obtenir le droit de l'administrateur sur la majorité des systèmes d'exploitation.
- L'audit interne du système d'exploitation : un système d'exploitation dispose souvent de moyens d'audit internes qu'il faut savoir utiliser correctement
- Les services internes : selon les services présents et leurs configurations, des vulnérabilités supplémentaires peuvent apparaître
- Les vulnérabilités connues du constructeur : la perfection n'est pas de ce monde
- Les fichiers utilisateurs : ce sont souvent eux qui déposent un petit cadeau qui va empoisonner la vie de l'administrateur, volontairement ou par inadvertance.

L'audit interne enfin n'essaie pas de déchiffrer les données quel que soit l'algorithme utilisé.

Comme avec l'audit de sécurité externe, l'audit de sécurité interne produit un rapport de l'état de la sécurité.

4.3 Les *"security auditing tools" (S.A.T).*

Un SAT est un programme qui balaye automatiquement une machine ou une ensemble de machines, à la recherche de vulnérabilités. Nous distinguons 2 types de SAT:

- Les *"security auditing network"* SAN: ces programmes permettent de balayer un réseau entier à la recherche des vulnérabilités. Des programmes tels que SATAN,

ISS, WebTrend, CyberCop sont utilisés pour réaliser des audit de vulnérabilités externes.

- Les *"security auditing system"* SAS :ces programmes permettent de balayer uniquement la machine sur laquelle ils sont installés. Ils sont utilisés pour réaliser des audit de vulnérabilités internes.

  - le type d'OS installé sur machine,
  - l'existence de ports,
  - les services offerts.

Une fois que ces programmes ont fini de balayer les machines, ils génèrent des rapports avec des informations concernant les problèmes rencontrés.

4.3.1 Principe de fonctionnement.

Tous les programmes qui réalisent des balayage de sécurité sur un réseau doivent accomplir un certain nombre de tâches.
En effet ils doivent déterminer [SATAN]:

- Quelles sont les machines actives, pour pouvoir réaliser les tests.
- Quels sont les services offerts et finalement
- Quels sont les services qui présentent des vulnérabilités.

Comment déterminer les machines actives.

La façon la plus facile pour savoir si une machine est active sur un réseau est d'exécuter la commande *ping*[1] vers cette machine.

En questionnant toutes les machines d'un réseau avec *ping* on pourra avoir une liste complète des machines actives.

[1] Ping est l'acronyme de Paquet INternet Groper, qui envoie une demande d'écho ICMP à une autre station et attend une réponse. Cela permet de tester l'accessibilité d'une machine distante. Accessoirement, Ping informe aussi du nombre de millisecondes qu'il a fallu à ce paquet pour atteindre l'appareil distant.

Exemple:

```
Ping st22.info.fundp.ac.be
Pinging st22.info.fundp.ac.be [138.48.32.84] avec
32 octets de données :
Réponse de 138.48.32.84 : octets=32 temps<10ms
TTL=128
Réponse de 138.48.32.84 : octets=32 temps<10ms
TTL=128
Réponse de 138.48.32.84 : octets=32 temps<10ms
TTL=128
Réponse de 138.48.32.84 : octets=32 temps<10ms
TTL=128
```

Figure 4-1: exemple de la commande ping

Mais *ping* n'est pas une voie sûre pour trouver un ordinateur sur un réseau, un ordinateur pourrait ne pas avoir un itinéraire de retour vers la machine qui a réalisé le ping. Un autre problème serai qui les paquets ICMP (ou tout autre paquet d'ailleurs) pourrait être bloqués par un routeur ou n'importe quel autre dispositif.

Nous pourrions également réaliser un balayage systématique de chaque machine d'un réseau, sans réaliser de *ping*. Mais cela engendrerait une perte de temps, et si le réseau à balayer possède beaucoup de machines, le temps peut devenir extrêmement grand.

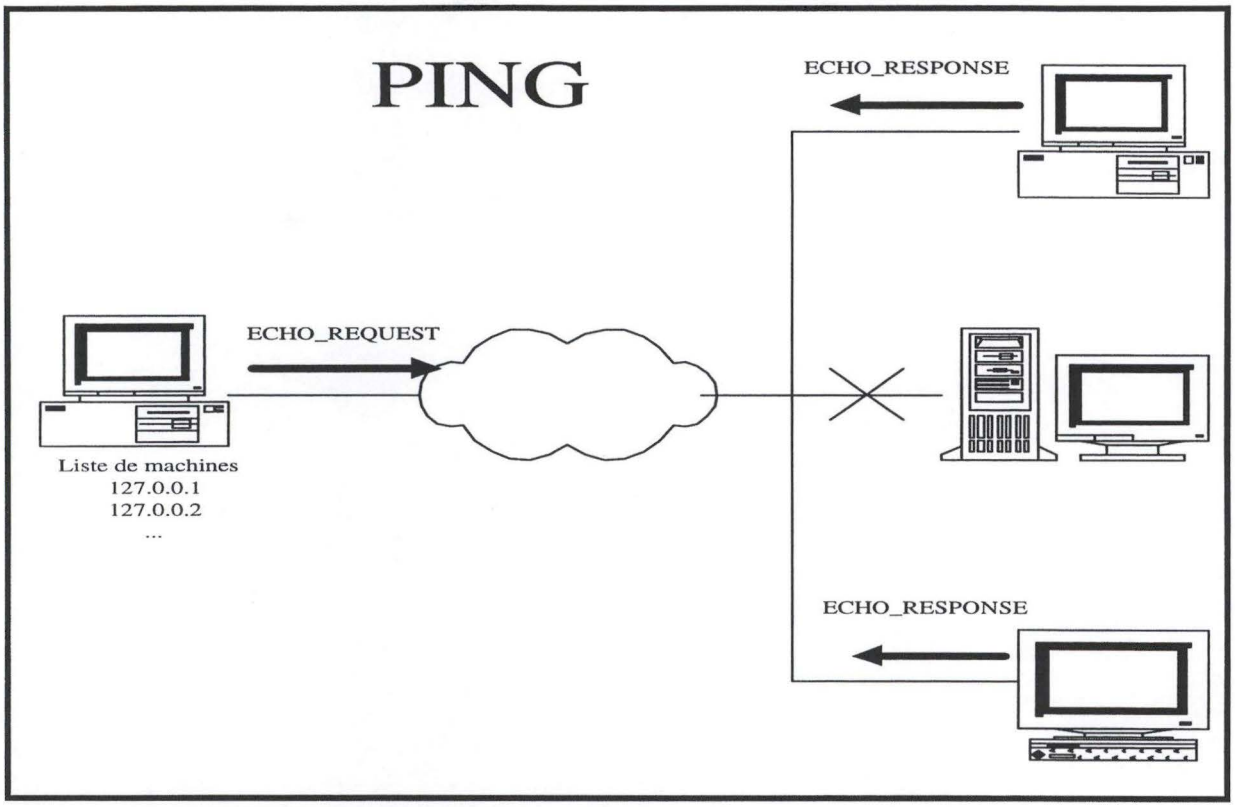

Figure 4-2: collecte de données avec ping

Quels sont les services offerts par le réseau.

Une fois que la liste d'adresses IP a été établie, il faut déterminer quels sont les services qui tournent sur ces machines.

Pour cela il nécessaire de vérifier les ports[2] qui sont liés à ces services. Ainsi les protocoles TCP et UDP utilisent différents numéros de ports pour différencier les services qui tournent sur un même ordinateur.

En balayant tous les 65536 ports disponibles il est possible d'avoir une image complète de tous les services qui tournent sur un ordinateur.

Si nous envoyons un paquet vers un numéro de port qui n'a pas été détecter par l'outil, nous recevrons une demande afin de terminer la connexion. Pour les services TCP. Un message d'erreur ICMP *"port unreachable"* pour les services UDP.

Après ceci, nous avons une liste des ports qui sont "ouverts" et une liste de messages de bienvenue, ou tout ce qui a été envoyé de chaque port.

Mais, le numéro de port tout seul ne suffit pas, nous avons besoin est des connaître les services tels que FTP, Telnet, WWW, etc.

[2] Un port TCP/IP est un numéro de service. Un port doit être vu comme un lieu de rendez-vous.

Heureusement, les services les plus utilisés peuvent être facilement identifiés parce qu'ils tournent sur des ports de "services standard"[3].
Les numéros de port inférieurs à 1024 sont réservés à des services standardisés d'Internet.

Ex: 80 -> HTTP, 25 -> SMTP, 21 -> FTP, etc.

Les services qui ne tournent pas sur des ports de "services standard", souvent peuvent être identifiés par les données qu'ils génèrent. Un Web serveur, par exemple, peut être identifié car il envoie les réponses en format HTML. De cette façon, en regardant les réponses envoyées, nous pouvons connaître non seulement les applications qui tournent sur chaque port, mais aussi le software utilisé pour cette application. La plupart des logiciels ont des caractéristiques propres. Par exemple **sendmail,** par défaut, envoi un en-tête qui détaille la version du logiciel, les web serveurs souvent incluent dans leurs codes d'erreur le nom, la version, etc.

Quels sont les services vulnérables ?

Beaucoup des services détectés peuvent être considérés directement comme vulnérables. D'autres services ont besoin de tests plus approfondis. Par exemple, si le port scanner et l'analyse des en-têtes montrent que **sendmail** dans une version particulière tourne sur une machine. Et nous savons que cette version présente des vulnérabilités ou des problèmes de configuration, alors l'audit de sécurité doit démarrer une subroutine qui essai d'exploiter le problème. Grâce au résultat de la subroutine nous saurons si les vulnérabilités sont présentes.

Les SAN généralement ont besoin d'une adresse IP ou d'un nom de domaine pour pouvoir travailler. A partir de là, ils vont réaliser (au moins) les 3 étapes décrites ci-dessous.

Quant aux SAS, leur fonctionnement est plus simple mais ils doivent être installés sur la machine qui va être testée.

Ces logiciels ont en général besoin d'avoir les droits *root* de cette façon il vont pouvoir tester tous les problèmes liés à la configuration du système.

[3]La RFC 1700 décrit les numéros des ports.

4.3.2 Les avantages d'un balayage automatique:

Les balayages automatiques donnent aux organisations un grand nombre de bénéfices parmi lesquels nous pouvons citer :

- Ils peuvent donner lieu à une utilisation active avec application de recommandations et de patchs[4] correcteurs, avec peu de risques sur le fonctionnement et la disponibilité du système.

- Puisque le scanner est automatique (moyennant la configuration du logiciel avant de l'exécuter), il permet aux administrateurs ou chargés de la sécurité d'allouer ressources et main d'œuvre vers d'autres tâches plus critiques et qui requièrent la surveillance ou l'intervention permanente de ceux-ci.

- Les outils utilisés pour réaliser les scanners automatiques sont bien connus des administrateurs et responsables de la sécurité.

- Renforcement de la politique de sécurité.

  Les scanners nous aident à connaître le réel niveau de sécurité d'un réseau, à être sûr des outils et procédures mis en place, à pouvoir prévenir aux éventuelles attaques. Lorsque toute cette information est réunie, l'organisation peut revoir la politique de sécurité et déterminer si elle est appropriée.

- Ces outils sont relativement faciles d'emploi et d'installation. Mais cela dépend de l'expérience de l'utilisateur et surtout de la capacité d'interprétation des résultats.

- Gestion centralisée

  Le scanner automatique permet de réaliser tous les tests du(es) réseau (x) à partir d'un seul point de contrôle (la machine de l'administrateur)

- En utilisant les scanners automatiques les organisations évitent de payer des éventuels examens et tests réalisés par des consultants externes, qui souvent coûtent très cher.

- Il sont relativement faciles à Installer et à utiliser.

4.3.3 Inconvénients :

Malheureusement il n'y a pas que des avantages avec les scanners automatiques, ils présentent aussi certains inconvénients, parmi les quels nous pouvons citer :

[4] Un patch est une correction d'un logiciel qui contient des vulnérabilités.

- Les actions des utilisateurs peuvent faire réapparaître très rapidement des vulnérabilités de sécurité. Par exemple si après un scanner un utilisateur installe un programme qui présente des vulnérabilités alors ces dernières ne serons pas détectées.

- Les balayages rassemblent la connaissance du moment. Si un SAT ne trouve pas des vulnérabilités dans le réseaux, cela ne veux pas dire qu'il aucun problème. Mais cela veux dire que peut être le logiciel ne fait pas tous les tests nécessaires, ou que il ignore des vulnérabilités qui ne sont pas (encore) documentées.

- On pourrait imaginer aussi que l'administrateur change la configuration d'un logiciel donné, après avoir exécuté le scanner, et ces changements vont permettre a toute personne d'exécuter des commandes en, mode super-utilisateur.

Ces 2 derniers points nous invitent à nous poser une question très essentielle:
Y a-t-il une voie de garantir que mon réseau ou système est sûr contre une attaque?

A ce propos en mars, 1998 le bulletin de l'institut CIO nous dit: *" (. . .) several smart organizations are running three automated vulnerability scans each year (. . .) They contract two of them out--one to a major company (a big accounting firm or system integrator) and one to a smaller, more specialized organization. The third they ask their own staff to perform. The combination of competition among the testing teams and continuous monitoring provides a very clear picture of what needs to be fixed."* [security consulting :FAQ]

4.3.4 Les dangers.

Les SAT sont des outils très pratiques et d'une grande utilité pour les administrateurs des systèmes, mais ils peuvent être très dangereux s'ils tombent entre les mains de personnes malveillantes.

En effet, ces outils peuvent scanner une machine (un réseau, un ensemble de réseaux) à distance et sans avoir besoin d'un mot de passe ni d'un "login name", mais uniquement grâce à une adresse IP. Les informations collectées par ces personnes malveillantes pourront donc être utilisées pour mieux préparer une attaque et s'introduire dans le réseau.

D'un autre côté, puisqu'à présent tout le monde a accès à Internet soit via les écoles, les universités ou à domicile ces outils sont facilement accessibles.

Des logiciels tels que SATAN , Saint, Cops, Tiger, etc. peuvent être téléchargés gratuitement via Internet. De même les logiciels commerciaux comme Iss, CyberCops, Web Tends existent en *"trial version"*[5] c'est-à-dire une version de test qui réalise un scanner complet sur un ensemble de machines.

Comme nous l'avons déjà dit, ces logiciels sont relativement faciles a installer. Une fois qu'ils sont installés, n'importe qui, même quelqu'un avec une connaissance de base en informatique peut exécuter ces logiciels et rassembler des informations concernant les machines balayées.

En effet ces logiciels, comme on l'a déjà dit, sont utilisés pour scanner les réseaux et collecter des informations concernant :

- Les types d'OS ;
- l'existence de ports,
- les services offerts,
- le vulnérabilités.

Exemples :

Detected Host		
Host	**Status**	**Platform**
192.168.0.31 (qa-sun-1.internal.webtrends.com)	Responded	Unix Server
192.168.0.225 (SUZANNEB.webtrends-nt.internal.wetrends.com)	Responded	Windows NT Workstation
Aruba (192.168.0.103)	Responded	Windows NT Server
Galapagos (192.168.0.145)	Responded	Windows NT Server
Haiti (192.168.0.102)	Responded	Windows NT Server
Palmyra (192.168.0.40)	Responded	Windows NT Server
QA-sun-2 (192.168.0.33)	Responded	Unix Server

Figure 4-3 : Extrait d'un raport généré par Web Trends

[5] Ces versions fonctionnent uniquement pendent une certaine période de temps, 14 jours, un moins, etc. Selon le constructeur .

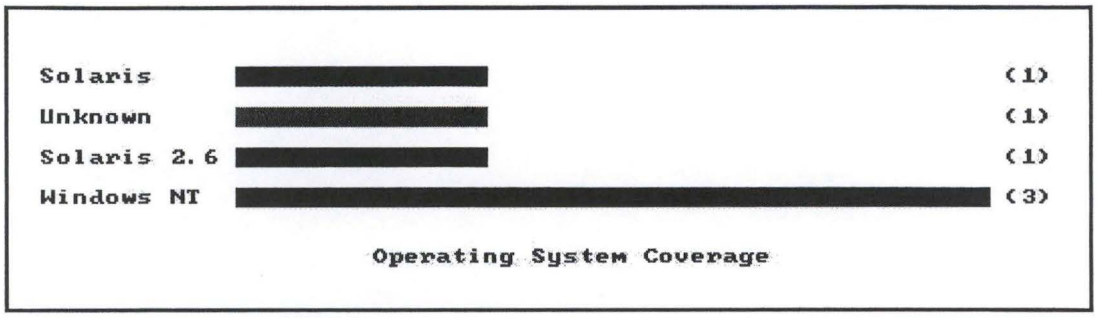

Figure 4-4 : Extrait d'un raport généré par Cyber Cops

Comme nous l'avons déjà dit, en balayant le réseau les SAT déterminent, les machines actives, ensuite les ports et les services disponibles et finalement les vulnérabilités liées à ces services. C'est à ce niveau que le problème se présente. En effet une fois le balayage terminé le programme nous informe sur:

- les vulnérabilités existantes,
- la façon de réparer les vulnérabilités trouvées,
- les types d'attaques auxquels les machines sont susceptibles,
- la façon de réaliser ces attaques, (même d'une façon indirecte)
- des URL vers des sites qui expliquent d'une façon précise le problème et parfois même le nom du programme qui exploite ces vulnérabilités .

Les figures 4-5 et 4-6 donnent un exemple des services rencontrés par Web Trends. La figure 4-7, nous explique la manière de télécharger la source ASP sur un certains serveurs IIS (Internet Information System).

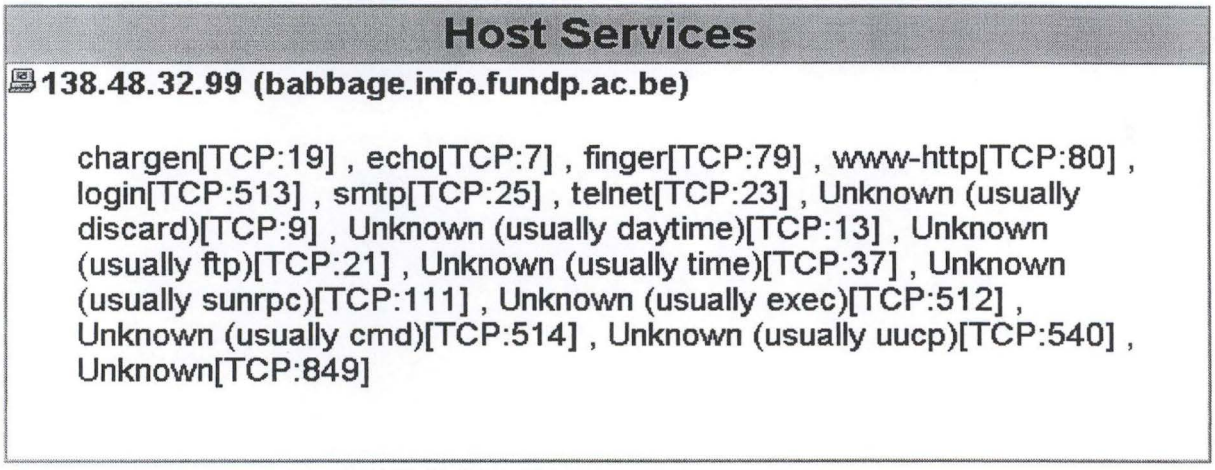

Figure 4-5 : Extrait d'un raport généré par Web Trends

Service Vulnerablilities	
Services	**Vulnerabilities**
smtp / TCP:25	Low - SMTP Service is Enabled
chargen / TCP:19	Low - CHARGEN Service is Enabled
echo / TCP:7	Low - Echo Service is Enabled
finger / TCP:79	Low - Finger Service is Enabled
login / TCP:513	Low - RLogin Service is Enabled
telnet / TCP:23	Low - Telnet Service is Enabled
www-http / TCP:80	Low - HTTP (Web) Service is Enabled

Figure 4-6 : Extrait d'un raport généré par Web Trends

High - Exploit $DATA hole

Under many IIS installations, an attacker can download the ASP Source by appending the string "::$DATA" to the URL. This can expose usernames and passwords that are hard coded within scripts. For example, the SQL administrator password is often hard coded in this way.
For more information, please see the Microsoft Security Advisory at:
http://www.microsoft.com/security/bulletins/ms98-003.asp
Additional information on this vulnerability is available at:
http://support.microsoft.com/support/kb/articles/q188/8/06.asp
and
http://www.rootshell.com/archive-j457nxiqi3gq59dv/199807/aspads.txt.html .

Fix - Apply $DATA Hotfix For IIS

Apply $DATA Hotfix For IIS

To download the hotfix for this vulnerability for IIS 3.0, go to:
ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/security/iis3-datafix/iis3fixi.exe
To download the hotfix for this vulnerability for IIS 4.0, go to:
ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/security/iis4-datafix/iis4fixi.exe
For more information, please see the Microsoft Security Advisory at:
http://www.microsoft.com/security/bulletins/ms98-003.asp

Figure 4-7 :Extrait d'un rapport généré par Web Trends

4.4 Conclusion

Nous l'avons vu tout au long de ces chapitres que la sécurité 100% n'existe pas.

Les OS et les applications existants possèdent tous de vulnérabilités qui peuvent entraîner des problèmes graves comme par exemple la perte pure et simple de données d'une entreprise. Mais grâces aux SAT et aux audits de vulnérabilités nous pouvons réduire les risques.

Nous devons également prendre garde à l'utilisation abusive des ces outils car les informations rassemblées peuvent être employées afin d'exploiter les vulnérabilités du réseau.

Chapitre cinq :

Comparaison des différents outils d'audit

5.1 Introduction

Les gestionnaires de réseau commencent à scanner leurs réseaux régulièrement. Cela veut dire qu'ils rajoutent à leurs moyens de défense des balayages automatiques.

Le problème est qu'il existe une grande quantité de SAT sur le marché, et les responsables de la sécurité se posent certaines questions telles que: quel scanner choisir ? quel est le meilleur ? quel scanner faut-il utiliser pour un type déterminé de société ?

Nous avons essayer de répondre à ces questions en testant 6 SAT parmi les plus connus. Parmi ces six SAT, quatre appartiennent au groupe des SAN et deux appartiennent au groupe de SAS.

Un des problèmes que nous avons rencontré, est que les versions ont été testées sur des "machines sûres" (ces machines étant les seules disponibles) c'est à dire des machines ayant déjà été contrôlées par les administrateurs ou les responsables de la sécurité. La probabilité de trouver des vulnérabilités ou des vulnérabilités graves dans ces machines diminue fortement. Cela ne veut pas dire que les machines ne contiennent plus de vulnérabilités car comme nous l'avons déjà dit, la sécurité 100% n'existe pas.

L'idéal aurait été d'avoir un ensemble de machines de tests avec un ensemble de vulnérabilités introduites intentionnellement à l'avance, ensuite de vérifier quels outils auraient trouvés quelles vulnérabilités.

Finalement les constructeurs donnent généralement 3 niveaux de dangers aux vulnérabilités trouvés à savoir: **High, medium et low.** Mais quels sont les critères qu'ils utilisent ? Est-ce que chaque constructeur utilise les même critères?

Les constructeurs donnent aussi un nom diffèrent à chaque test réalisé ce qui rend plus difficile les comparaisons.

Les logiciels qui ont été testés sont Internet Scanner, CyberCop, Web Trends, SAINT, Cops et Tiger. Les quatre premiers appartient au groupe de SAN el les deux derniers appartient au groupe de SAS.

Notre façon de travailler

Pour notre analyse nous avons classifié les vulnérabilités par groupes car il est impossible de détailler chaque vulnérabilité indépendamment.

En suite nous avons décrit, pour chaque outil, ses fonctionnalités, les vulnérabilités que ces produits peuvent tester classifiées par groupes, les systèmes d'exploitation sur lesquelles le logiciel tourne, la configuration minimum nécessaire et finalement ses points forts et ses points faibles.

La collection de ces informations ont été faites sur base des résultats obtenus lors des tests, et en grande partie grâce à la documentation de chaque produit.

5.2 ISS.

5.2.1 Description

"Internet Security Scanner" est un outil qui scanne une machine ou un réseau local ou distant à la recherche de problèmes de sécurité, les informations ressemblées sont ensuite présentées sous forme d'un fichier HTML, ou d'un fichier .DOC.

5.2.2 Fonctionnalités

Les fonctionnalités de ISS sont les suivantes:
a) Détection des machines et OS disponibles sur les machines. détection de réseaux.
b) Détection de services disponibles.
c) Tests réalisés:

Nous avons classifiés les tests en 23 groupes de vulnérabilités :

1. **Browser Checks.** Vulnérabilités dans Internet Explorer et Netscape Navigator web browsers.
2. **Brute ForceChecks.** Teste les utilisateurs par défaut.
3. **CGI-Bin Checks.** Teste la présence de scripts CGI vulnérables
4. **NIS+ Checks.** Teste les implémentations de Distributed Naming Service implementations à la recherche de vulnérabilités.
5. **Daemons Checks.** Teste la présence de plusieurs demons vulnérables
6. **DOS Checks.** Test de type Denial of Service.
7. **SMTP Checks.** Vulnérabilités dans Simple Mail Transfer Protocol (SMTP)
8. **Firewalls/Proxis Checks.** Teste certains Firewalls/Proxis à la recherche de vulnérabilités et de problèmes de configuration.
9. **IP-Spoofing Checks.** Essaye de prédire le numéro de séquence dans le protocole TCP.
10. **LDAP[1]Checks.**
11. **NFS Checks.** Teste les vulnérabilités dans le serveur NFS (Network File System) et le serveur X-Windows.
12. **NIS Checks.** Teste les implémentations de NIS (Network Information System implementations) à la recherche de vulnérabilités
13. **NT Groups/Networking Checks.** détermine des vulnérabilités propres à Windows NT.
14. **Rexec Checks.** Détermine le présence du service rexec sur Windows NT

[1] Short for Lightweight Directory Access Protocol, a set of protocols for accessing information directories. LDAP
is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Because it's a simpler version of X.500, LDAP is sometimes called X.500-lite. [Webopedia]

15.**Oracle Passwords Checks.**
16.**Sendmail Checks.** Vérifie les comptes des utilisateurs avec sendmail
17.**RPC Checks.** Teste les services RPC à la recherche de vulnérabilités
18.**Hardware Checks.** Teste les Router/Switch hardware à la recherche de vulnérabilités.
19.**SNMP Checks.** Teste les implémentations de SNMP (Simple Network Management Protocol) à la recherche de vulnérabilités.
20.**Security Zones Checks.**. Teste les zones de sécurité des URL d'après la classification de la machine ou le site.
21.**Shares/Dcom Checks.** Teste les permissions dans NetBIOS shares, DCOM Registry keys, et DCOM.
22.**Unauthorized access attempt Checks.** Vérifie les tentatives d'accès non autorisées.
23.**HTTP Server Checks.** Teste les serveurs HTTP à la recherche de vulnérabilités.

5.2.4 Systèmes d'exploitation:

La version testée est la 5.3.1 pour Linux.

5.2.5 Environnement Matériel.

- Space Disque: 10 Mb minimum.
- Mémoire: 32 Mb minimum

5.2.6 Caractéristiques

L'analyse du logiciel nous à permis de constater certaines points forts ainsi que certains points faibles.

LES POINTS FORTS:

+ Un nombre très élevé de tests réalisés
+ Très simple à installer. Sont interface est vraiment très simple ce qui rend sont utilisation très facile.
+ ISS offre plusieurs une trentaine de types de rapport, en format HTML, ASCII et CVS.
+ Les rapports contiennent une explication des problèmes rencontrés. Donnent les éléments pour y remédier et peuvent éventuellement donner des liens vers des sites pour y trouver plus d'information.
+ Il permet de personnaliser les scanners, c'est-à-dire que nous pouvons choisir les tests que nous voulons réaliser.
+ IS peut être exécuté en ligne de commandes ce qui permet d'écrire ses propres scripts par exemple en le shell script.

POINTS FAIBLES

- Contrairement aux autres scanners IS ne permet pas de rajouter ses propres tests.
- IS existe en 2 versions une spécialisée Windows NT et une spécialisée Unix. Si nous voulons obtenir un résultat optimal sur un réseau multi plate-forme il faut utiliser les deux. Il faut remarquer que si nous avons une des deux versions la deuxième est gratuite.[ISS FAQ's]

- Le licence du produit interdit de balayer n'importe quel réseau. Donc il existe un nombre limité de réseaux qui peuvent être scannés. Ceci est un grand obstacle pour les sociétés qui offrent des services de « tests de vulnérabilités », et dont les réseaux scannés ne sont jamais le mêmes.

5.3 Test de CyberCop Scanner (CSC).

5.3.1 Description.

CyberCop Scanner examine les systèmes informatiques et les dispositifs de réseaux à la recherche des plus de 450 vulnérabilités dans les systèmes d'exploitation (Windows NT et Unix) et les applications fonctionnant dans un environnement réseau.

5.3.2 Fonctionnalités

Les fonctionnalités de CyberCop sont les suivantes:

a) Détection des machines et de réseaux.
b) Détection de services disponibles.
c) Réalise des tests d'intrusion.
d) Vulnérabilités testées:

Nous avons classifiés les tests en 15 groupes de vulnérabilités :

1. **FTP Checks.** Problèmes de configuration et vulnérabilités dans certains
2. démons FTP.
3. **Port scanning Checks.** Détecte les ports présents dans le système.
4. **Device Checks.** Contrôles De Périphériques (bridges, routers,
5. printers, firewalls)
6. **DNS Checks.** Problèmes de configuration et vulnérabilités dans certains
7. démons DNS
8. **Backdoor Checks.** Détection de certains backdoors[2].
9. **NFS Checks.** Vulnérabilités dans le serveur NFS (Network File System)
10. **General Remote Services Checks.** Problèmes de configuration et vulnérabilités dans NNTP, Telnet, POP, UUCP, Kerberos
11. **DOS Checks.** Attaques de type Denial of Service
12. **Password Checks.** Les mots de passe faibles
13. **Checks.** Tests liés au Protocol Spoofing
14. **HTTP servers Checks.** Problèmes de configuration et vulnérabilités dans les Web Browsers et les scripts CGI
15. **RPC Checks.** Vulnérabilités dans le RPC
16. **General Network Security Checks.**
17. **NetBIOS /SMB Checks.** Problèmes de configuration dans NetBIOS /SMB
18. **Sendmail Checks.** Vulnérabilités dans Sendmail
19. **Network and Protocol Spoofing Checks.** Vulnérabilités inhérentes à TCP/IP.

[2] A backdoor is a program that is designed to hide itself on a target host. While all backdoor programs are different, generally they allow the installing user access to the target system at a later time without using normal authorization or vulnerability exploitation

20.**Windows NT Vulnérabilmities Checks.** Vulnérabilités propres à Windows-NT.

5.3.3 Systèmes d'exploitation:

La version testée est la 2.5 pour Linux.

5.3.4 Environnement Matériel nécessaire (minimum).

- Pentium 233 MHz
- 64 Mb de Ram
- 40 Mb disponibles dans le HD
- Serveur Xfree86 ou X11R6
- Browser capable de lire des images et qui supporte le frames.

5.3.5 Caractéristiques

L'analyse du logiciel nous à permis de constater certaines points forts ainsi que certains points faibles.

- **LES POINTS FORTS:**

+ CCS est très simple à installer et a utiliser, son interface est très intuitive ce qui permet d'y s'adapter facilement.
+ Réalise un nombre très élevé de tests. En autre il offre la possibilité de sélectionner parmi une liste de tests uniquement ce que nous voulons réaliser.
+ Les rapports peuvent être générés en format HTML, RTF, ASCII et CSV
+ Les rapports contiennent une explication des problèmes rencontrés. Donnent les éléments pour y remédier et peuvent éventuellement donner des liens vers des sites pour y trouver plus d'informations.
+ Il existe un utilitaire *"Auto Update"* qui permet de mettre a jour les dernières tests Update via Internet.
+ On peut créer ses propres scripts grâce a CASL (langage de script créé par Network associantes et qui permet facilement d'écrire des tests)
+ Il fournie une documentation complète sur l'utilisation du logiciel.
+ Il laisse des traces visibles de son passage ce qui permet de détecter si quelqu'un a scanner une machine sans autorisation.
+ Il n'y a pas de restriction sur la quantité d'adresses IP à scanner.

- **LES POINTS FAIBLES.**

- Les rapports générés donnent trop d'informations et
- ils ne sont pas très faciles à comprendre au début. Il existe cependant la possibilité de choisir les données qu'on veut générer, parmi un nombre limité d'options

5.4 Web Trends security Analyzer (WTSA).

5.4.1 Description.

"Web Trends security Analyzer" est un outil qui scanne une machine ou un réseau local ou distant à la recherche de vulnérabilités bien connues dans Windows 95/98/NT. Les informations ressemblées sont ensuite présentées sous forme d'un fichier HTML, ou d'un fichier .DOC. Lorsque WTSA détecte un OS diffèrent de Windows il peut scanner a la recherche des ports ouverts.

5.4.2 Fonctionnalités.

Les fonctionnalités de WTSA sont les suivantes:
a) Machines et de réseaux.
b) Les services disponibles, c'est-à-dire : les ports trouvés, les applications trouvées.
c) Vulnérabilités présentes dans le réseau:
cependant il est impossible de détailler tous les tests réalisés par WTSA, la version 2.1 pour Windows analyse plus de 501 vulnérabilités, mais on peut classifier ce tests par catégories.

1. **FTP Ckecks.** Problèmes de configuration et vulnérabilités dans les serveurs FTP.
2. **Game Servers Ckecks.** Teste l'existence des jeux tels que Hexen2 ou Quake et qui peuvent être vulnérables à des attaques de type denial of service.
3. **Mail Client Ckecks.** Problèmes de configuration et vulnérabilités dans les Mail Client
4. **Mail Server Ckecks.** Problèmes de configuration et vulnérabilités dans les Mail Server
5. **Other Servers Ckecks.** Problèmes de configuration et vulnérabilités dans certains serveurs tels que 3Comn, IMAIL 4.06, IIS, etc
6. **Proxy/Firewall Ckecks.** Problèmes de configuration et vulnérabilités dans les Proxy/Firewall
7. **Web Browsers Ckecks.** Problèmes de configuration et vulnérabilités dans les Web Browsers
8. **Web Server Ckecks.** Problèmes de configuration et vulnérabilités dans les Web Server.
9. **Password Ckecks.** Les mots de passe faibles dans Windows NT
10. **NT Privilege Ckecks.** Les permissions d'utilisateurs de Windows NT
11. **NT services Ckecks.** Problèmes de configuration et vulnérabilités dans certains services NT
12. **Workstation Hardening Ckecks.**. Contrôle si tous les patchs ont été installés. Et l'existence de certaines vulnérabilités.
13. **Registry Access Control.** Vulnérabilités dans la registy.

5.4.3 Environnement Logiciel nécessaire.

La version testée est la 2.1 Beta.

- Pour réaliser un scanner complet d'un réseau cette version doit être installée sur un machine Windows NT, avec les privilèges d'un administrateur. Mais elle peut aussi être installée sur une machine Windows 95 ou 98 pour scanner les machines locales.

- Netscape ou Explorer ou MS-word pour lire les rapports.

5.4.4 Environnement Matériel nécessaire (configuration minimum).

- 40 MB de HD disponible.
- 64 MB de RAM.

5.4.5 Caractéristiques

L'analyse du logiciel nous à permis de constater certains points forts ainsi que certains points faibles.

- **LES POINTS FORTS:**

+ WTSA réalise une grande quantité de tests (501). De plus, il est le seul à tester l'existence de jeux qui peuvent introduire de vulnérabilités.

+ WTSA possède un Kid de développement appelé Post SDK qui permet de créer ses propres tests en Perl ou en C.
+ Le Kit de développement possède des outils et des librairies qui permettent
+ d'intégrer facilement les tests écrits par un programmeur.
+ Permet de créer ses propres profils. L'utilisateur peut choisir parmi une liste uniquement les type de tests qu'il veux réaliser.

+ Possibilité de définir des scanners automatiques, l'utilisateur peut configurer le logiciel pour que celui-ci démarre à une heure bien précise, avec un profil bien précis et qu'il génère un type de rapport bien précis.

+ Il existe un utilitaire appelé *"AutoSync"* qui permet d'aller télécharger directement sur le site de WebTrends, les derniers tests disponibles.

+ WTSA permet de générer des rapports en format HTML ou DOC. En autre il existe la possibilité de choisir les informations qu'on veux voir uniquement.

+ Le générateur de rapports permet aussi d'envoyer le rapport généré a une personne via une adresse e-mail ou via FTP.

+ Les rapport générés donne une explication des vulnérabilités retrouvées, et une explication de ce qu'il fait faire pour réparer ces vulnérabilités.

+ Ils donnent éventuellement des liens ou trouver plus d'information, et ou trouver les derniers patchs.

+ WTSA est simple à installer et simple à utiliser en plus il possède une guide d'utilisation très complet

- **POINTS FAIBLES**

- Pour une même machine qui n'a pas changée de configuration lors d'un premier scanner WTSA a trouvé 305 vulnérabilités. Lors d'un deuxième scanner WTSA a trouvé 300 vulnérabilités.

- Ne laisse pas la possibilité de choisir un ensemble discontinu de machines. Supposons que nous voulons scanner la machine 127.0.0.1, 127.0.0.7,127.0.0.10 et 127.0.0.15. Il est impossible de scanner uniquement ces machines, nous devons donc choisir un ensemble continu de type 127.0.0.1-127.0.0.15.

- Il existe plusieurs versions pour un même produit : **Single System Edition**, (scanne uniquement la machine sur la quelle il est installé). **Professional Edition** (scanne 255 adresses IP maximum). Et l'**Enterprise Edition** (scanne un nombre illimité de machines). Pour chaque version il existe aussi la version plus qui fournit une assistance technique et permet de télécharger les dernières tests pendant un an.

- Les rapports générés contiennent trop d'informations redondantes.

5.5 SAINT.

5.5.1 Description.

"Security Administrator's Integrated Network Tool " est un outil qui rassemble des informations, telles que les services offerts ou des trous bien connus, sur des réseaux et des machines distantes ou locales. Ces informations sont ensuite présentées sur forme d'une page web.

5.5.2 Fonctionnalités.

Les fonctionnalités de SAINT sont les suivantes:

a) Détection des machines et de réseaux.
b) Détection de services disponibles.
c) Tests que SAINT réalise: la version 1.4 réalise presque 50 tests que nous avons essayé de les regrouper dans les catégories suivantes:

1. **Trojan Horse Checks.** Détecte la présence de NetBus et Back Oriffice.
2. **DOS Checks**. Attaques de type Denial of Service
3. **BIND Checks.** Vulnérabilités dans BIND[3].
4. **FINGER Checks.** Vulnérabilités dans FINGER[4]
5. **FTP Checks.** Vulnérabilités dans certains demons FTP
6. **HTTP Checks.** Vulnérabilités dans les serveurs HTTP
7. **IMAP/POP Checks.** Vulnérabilités des serveurs IMAP/POP
8. **INND Checks.** Vulnérabilités des serveurs INND[5]
9. **LP Checks.** Vulnérabilités dans lpd
10. **NetBIOS Checks.** Problèmes de configuration dans NetBIOS
11. **NFS/NIS Checks.** Vulnérabilités dans les serveurs NFS/NIS
12. **rlogin/rshell Checks.** Vulnérabilité de remote login/remote shell
13. **Denoms Checks.** Vulnérabilités des démons rexd, rexec, statd, rstat
14. **SSH Checks.** Vulnérabilités du programme SSH (Secure Shell)
15. **TFTP Checks.** Vulnérabilités dans TFTP (Trivial file transfer protocol)
16. **Tool Talk Checks.** Vulnérabilités du programme Tool Talk.

---

[3] The Berkeley Internet Name Daemon (BIND) is an implementation of the Domain Name Service (DNS) written primarily for UNIX Systems.

[4] A UNIX program that takes an e-mail address as input and returns information about the user who owns that e-mail address.

[5] InterNetNews is a complete Usenet system.

5.5.3 Environnement Logiciel nécessaire.

La version testée est la 1.4. Elle à été testé sur une machine Linux, distribution Red Hat 5.4. Pour exécuter Saint nous avons besoin aussi de :

- Perl 5.x
- Un compilateur C
- Navigateur WWW (Mosaic ou Netscape)

5.5.4 Environnement Matériel nécessaire (configuration minimum).

- SPACE DISQUE: Pour installer SATAN plus au moins 2 Mb de mémoire est requise
- MEMOIRE: La quantité de mémoire requise dépend du nombre de machines scannées. (d'après les auteurs....) Pour 1500 machines scannées il faut plus au moins 14 megabytes sur une machine SPARC 4/75 avec SunOS 4.1.3.

5.3.5 Caractéristiques

L'analyse du logiciel nous à permis de constater certains points forts ainsi que certains points faibles.

- **LES POINTS FORTS:**

+ SAINT, Perl , Netscape sont disponibles gratuitement.
+ Simple à utiliser grâce à l'utilisation d'un navigateur WWW[6].
+ Le résultat est présenté sous format HTML.
+ Il est récursif c'est-à-dire qu'à partir d'une machine il peut en découvrir des nouvelles et peut les analyser directement.
+ Les rapports générés donne une explication des vulnérabilités retrouvées, et une explication de ce qu'il faut faire pour réparer ces vulnérabilités.
+ Les rapports générés donnent beaucoup de URL[7] vers de sites qui donnent des informations sur les protocoles, les produits, ou même des articles qui parlent de la sécurité.
+ SAINT est extensible et adaptable. Dans les fichiers de configuration plusieurs valeurs par défaut peuvent être modifiées. Des nouveaux tests (programmes) peuvent être écrits et rajoutés.

---

[6] World Wide Web. A system of Internet servers that support specially formatted documents. The documents are formatted in a language called HTML (HyperText Markup Language) that supports links to other documents, as well as graphics, audio, and video files. This means you can jump from one document to another simply by clicking on hot spots. [webopedia]

[7] Abbreviation of Uniform Resource Locator, the global address of documents and other resources on the World Wide Web.

- **POINTS FAIBLES**
  - Le temps nécessaire pour scanner un réseau peut devenir très grand, cela dépend du nombre de machines.
  - Le nombres de vulnérabilités testées n'est pas grand (plus ou moins 50 tests)
  - La documentation est exactement la même que celle de SATAN. Ils ont simplement changé SATAN par SAINT.

5.6 COPS. Computer Oracle and Password System

5.6.1 Description.

COPS est un ensemble d'outils de sécurité conçus pour aider l'administrateur des systèmes UNIX, ou le consultant dans le domaine de la sécurité des réseaux, à trouver de problèmes de configuration ou des mots de passe faibles.

5.6.2 Fonctionnalités

Les fonctionnalités de Cops sont les suivantes:

1. permissions d'écriture dans tous les fichiers d'initialisation.
2. appartenance root des répertoires systèmes (/bin, /etc, ...)
3. positionnement de "umask" dans les fichiers /.login,/.cshrc, /.profile ...
4. droits d'accès en écriture dans chaque répertoire utilisateur.
5. permissions de points d'entrée dans /etc/fstab, /etc/exports et /etc/rc*.
6. permissions en écriture au niveau des commandes se trouvant dans les fichiers "cron".
7. Les mots de passe à partir de dictionnaires (mais Crack est plus performant).
8. La syntaxe des fichiers /etc/passwd et /etc/group
9. l'existence des utilisateurs ftp dans /etc/passwd.
10. le contenu du fichier /etc/ftpusers.
11. Le setup dans ftp anonyme.
12. permissions de tous les fichiers recensés dans "is_able.lst".
13. vérification des modifications des exécutables listés dans "crc_list" depuis leur dernière modification.

5.6.3 Environnement Logiciel nécessaire.

La version testée est la 1.4 qui tourne sur SunOs
Nous avons besoin d'un compilateur C.

5.6.4 Caractéristiques

L'analyse du logiciel nous à permis de constater certains points forts ainsi que certains points faibles.

- **LES POINTS FORTS**
  - \+ Peut être exécuté sans être root, mais si nous voulons que les tests soient réalisés d'une façon optimale il est conseillé de travailler en root.
  - \+ On peut : ajouter ses propres vérifications.
  - \+ Il est gratuit, donc on peut le télécharger facilement.

- **LES POINTS FAIBLES**
  - Cops ne peut pas être utilisé pour tester une machine distante, c'est-à-dire qu'il doit être installé dans la machine que nous voulons tester.
  - Cops fonctionne en mode commande uniquement.
  - Il commence à être dépassé
  - Les messages *"warnings"* n'ont pas beaucoup d'explications

Exemples

```
Security Report for Thu Mar 10 17:13:18 WET 1995 from host xxxx
**** root.chk ****
Warning!  "." (or current directory) is in roots path!
**** is_able.chk ****
Warning!  /usr/spool/mail is _World_ writable!
Warning!  /etc/aliases.dir is _World_ writable!
Warning!  /etc/aliases.pag is _World_ writable!
Warning!  /etc/motd is _World_ writable!
**** rc.chk ****
**** cron.chk ****
**** home.chk ****
Warning!  User uucp's home directory /var/spool/uucppublic is mode
03777!
**** passwd.chk ****
Warning!  Password file, line 10, no password:
        sync::1:1::/:/bin/sync
Warning!  Password file, line 11, user sysdiag has uid = 0 and is
not root
        sysdiag:*:0:1:Old System
**** user.chk ****
**** misc.chk ****
Warning! /bin/uudecode creates setuid files!
**** ftp.chk ****
Warning!  /etc/ftpusers should exist!
```

5.7 TIGER.

5.7.1 Description.

Tiger est un ensemble de programmes écrits en C et Shell script développe par l'université de Texas. Ces programmes exécutent une série de tests à la recherche de problèmes de sécurité. Une fois que les vérifications ont été réalisés Tiger génère un fichier avec toute l'information collecté.

5.7.2 Fonctionnalités.

Les fonctionnalités de Tiger sont les suivantes:

1. Vérifie les fichiers de configuration de l'utilisateur
2. Vérifie les permissions en écriture au niveau des commandes se trouvant dans les fichiers "cron".
3. Vérifie les alias de mail
4. Vérifie la configuration du serveur FTP anonyme
5. Vérifie la configuration du serveur NFS
6. Vérifie la configuration des fichiers /etc/inetd.conf at /etc/service
7. Vérification de la variable PATH[8], c'est à dire propriété et autorisations d'accès des exécutables dans le PATH.
8. Vérifie les fichiers .rhosts et .netrc
9. Vérification de la présence possible d'un intrus.
10. Vérification des permissions du fichier printcat
11. Vérification des fichiers « binaries » à l'aide des signatures digitales. ? ? ?

5.7.3 Environnement Logiciel nécessaire.

Le logiciel a été testé sur une machine Linux.

5.7.4 Caractéristiques

L'analyse du logiciel nous à permis de constater certaines points forts ainsi que certains points faibles.

- **LES POINTS FORTS:**
  - + Peut être exécuté sans être root, mais si nous voulons que les tests soient réalisés d'une façon optimale il est conseillé de travailler en root.
  - + On peut : ajouter ses propres vérifications.
  - + Il est gratuit, donc on peut le télécharger facilement.
  - + On peut sélectionner les tests qu'on peut réaliser.

[8] Il s'agit d'une variable d'environnement particulièrement cruciale pour l'utilisation d'un système Unix. Sa définition correcte conditionne la localisation des exécutables (programme binaire ou shell script) correspondants aux commandes. [Manuel Unix]

+ Tiger génère un fichier avec un ensemble d'informations, avec un numéro pour chaque information, exemple :

```
# Performing check of user accounts...
# Checking accounts from /etc/passwd.
--WARN-- [acc001w] Login ID mail  is disabled, but still has a valid
shell
         (/bin/sh).
--WARN-- [acc001w] Login ID news is disabled, but still has a valid
shell
         (/bin/sh).
--WARN-- [acc001w] Login ID uucp is disabled, but still has a valid
shell
         (/bin/sh).
--WARN-- [acc001w] Login ID operator is disabled, but still has a
valid shell
         (/bin/sh).
--WARN-- [acc001w] Login ID games is disabled, but still has a
valid shell
         (/bin/sh).
--WARN-- [grp002w] GID 1  exists multiple times in /etc/group
```

+ Il existe un script (tigexp) qui reçoit comme paramètre le numéro généré et qui renvoi une explication du problème. Exemple :
+ L'expression tigexp `[grp002w]` donne comme résultat :

```
The indicated group id (gid) exists multiple times in the same
group file.  This indicates a configuration problem which should be
corrected.
Failure to do so could allow unexpected access to resource
```

- **POINTS FAIBLES**

– Il est similaire a Cops (avec quelques tests en plus)
– Il commence à être dépassé, mais il existe une version commerciale appelée TARA[9] qui est le successeur de Tiger.

[9] Tiger Analytical Research Assistant

5.8 Conclusion

Il est évidant que face à des logiciels les logiciels comme SAINT "ne font pas les poids".

Un Logiciel d'audit moderne, doit offrit la possibilité de créer ses propres tests pour permettre aux utilisateurs de ne pas dépendre tout le temps des "Updates" du constructeur. **CyberCop Scanner** nous offre cette possibilité avec son langage de programmation CASL, de la même façon **WebTrends** avec son Kit de développement POST. **SAINT** est aussi écrit en Perl et C. **Cops** est écrit en shell et **Tiger** en C et shell ce qui permet, à un bon programmeur d'écrire ses propres tests.

D'un autre coté, si une société veux offrir un services d'**audit de vulnérabilités** à ses clients, elle doit pouvoir balayer n'importe quel réseau et ne pas être figé à un seul, par exemple celui de son entreprise. SAINT, WebTrends, CyberCop nous offrent cette possibilité.

De nos jours il n'existe plus des réseaux mono plate-forme (un seul type d'OS). Les plus connus étant Unix et Windows NT/95, il faut donc que les logiciels réalisent des tests sur au moins ces deux types de'OS. CyberCop et la combinaison de deux logiciels Internet Scanner remplissent cet objectif. Mais CyberCop réalise très peu de tests, alors que Internet Scanner for Windows réalise une grande quantité.

Tous les SAN testés réalisent uniquement des tests à la recherche de vulnérabilités. Sauf CyberCop qui intègre en un seul logiciel des tests de vulnérabilités et tests d'intrusion. Pour toutes ces raisons il me semble que le meilleur logiciel SAN est CyberCop suivie de très près par Internet Scanner.

	Crée ses propres Scripts?	Permet de scanner n'importe quel réseau à distance?	Multi plate-forme ?	Réalise des tests d'intrusion?
Internet Scanner	NON	NON	OUI	NON
SAINT	OUI	OUI	NON	NON
Web Trends	OUI	OUI	NON	NON
CyberCop	OUI	OUI	OUI	OUI

Quant au SAS, Cops est Tiger se ressemblent fortement, mais Tiger est plus récent et réalise plus de tests. En autre Tiger offre une aide en ligne sur chaque problème, alors que Cops pas. Nous pouvons dire que Tiger est plus performant que Cops.

5.9 Bibliographie.

[Bellovin, Cheswich]
William R Cheswich et al,
Firewalls et Securité Internet, Addison - Wesley profesional series,
USA, 1995.

[CERT]
Cornegie Mellon Software Engineering Institute,
CERT Coordination Center http://www.cert.org.(12/03/99)

[CIAC]
CIAC, CIAC
Security Website, http://ciac.llnl.gov (20/02/95)

[COAST]
Perdue University,
COAST, http://www.cs.purdue.edu/coast/coast.html (20/02/95)

[FIRST]
Forum of Incident Response and Security Teams,
http://www.first.org (12/03/99)

[Garde Barrière]
Jean-Paul Le Guigner, Garde Barrière,
http://www.cru.fr/securite/CRUGB/principe.html (12/03/99)

[Ghosh]
Anup K Ghosh, E-Commerce Security,
Wiley Computer Publishing, USA, 1998

[Hacking]
GUIDE TO (mostly) HARMLESS HACKING
http://d1o37.telia.com/~u34002171/hhd/gtmhh/gtmbeg7.html (12/03/99)

[Internet -définition]
Une définition d'Internet?,
http://www.cict.fr/ieutdm/TUTORIAL/1/FS1.HTM (20/07/99)

[ISS]
Internet Security Systems
http:// www.iss.net/vd/packcapt.htm (12/11/98)

[ISS FAQ's]
Internet Security Ssytems,
FAQ's, http://www.iss.net/prod/tpo/is_faq.php3 (13/08/99)

[ISS-Xforce]
Internet Security Ssytems,
xforce, http://xforce.iss.net/ (10/08/99)

[John Vacca]
John Vacca, Sécurité sur Interne, Sybex pour la version française
Paris, 1996.

[Le mot de passe]
Martin Ouwehand, Bien choisir son mot de passe
http://slwww.epfl.ch/SIC/SL/Securite/passwd.html (25/02/99)

[Manuel Unix]
Nicole Lhermitte, Manuel Unix,
http://lalinfo.in2p3.fr/SI/manuel-unix/node50.html (10/08/99)

[NIST]
NIST, Computer Security Resource Clearinghouse,
http://csrc.ncsl.nist.gov (12/08/99)

[Pujolle]
Guy Pujolle, Les Réseaux,
Cyrolles, Paris, 1995

[Ramaekers 99]
Jean Ramaekers, Cours de Sécurité Informatique,
Institut d'informatique 1999.

[Réseaux]
Laurent Delineau, Introduction aux réseaux informatiques
http://www.ac-idf.jussieu.fr/~infolyc/stage97/reseau/intro.htm, (25/04/99)

[SATAN]
Freiss, Martin, Protecting Networks with SATAN, O'Reilly & Associates Inc.,
[25/07/1998]

[Secure Unix]
Secure UNIX Programming FAQ
http://dread.orbitel.bg/xtern/sup/secure-faq.txt

[Spafford]
Spafford et al., Practical Unix an Internet Security,
O'Reilly & Associates Inc., USA, 1991

[Tanembaum]
Andrew Tanembaum, Réseaux,
Inter Edition pour la version française, Paris, 1997

[TCP/IP]
W Richard Stevens,TCP/IP illustré Les protocoles Volume 1,
Vuibert pour la version française, 1998

[Van Bastelaer]
Van Bastelaer ,Cours de téléinformatique, Institut d'informatique 1998.

[Webopedia]
Webopedia, http://www.pcwebopedia.com, (26/08/99)

[X-Cod]
X-Cod Technology
http://www.ntx-research.com/ntxipfr.htm#ref2, (23/05/99)