République algérienne démocratique et populaire Ministère de l'enseignement supérieur et de la recherche scientifique

Université Mouloud Mammeri de Tizi-Ouzou
Faculté de génie électrique et d'informatique
Département électronique

Mémoire

En vue de l'obtention d'un diplôme du master en télécommunication et réseaux

Thème :

Les techniques de sécurité des réseaux

Promoteur : **Mr. ATTAF**

réalisé par : **Mr. OUELHADJ Mohamed Amine**

Promotion : 2014/2015

Introduction

Dans la sécurité des systèmes informatiques constitue un enjeu crucial. Le contrôle de l'information traitée et partagée au sein de ces systèmes est un problème d'autant plus délicat que le nombre d'utilisateurs de ces systèmes est important. Relier ces systèmes entre eux au sein de réseaux informatiques,

Eux-mêmes interconnectés, complexifie donc la tâche des responsables sécurité.

La sécurité d'un système informatique repose en premier lieu sur la mise en place d'une politique de sécurité. Celle-ci peut être définie comme un ensemble de règles permettant d'assurer trois propriétés.

La confidentialité des données : seuls les utilisateurs autorisés peuvent consulter une information donnée .

l'intégrité des données : seuls les utilisateurs autorisés peuvent modifier une information donnée .

la disponibilité du système : le système doit être capable de rendre le service prévu en un temps borné.

Une fois la politique de sécurité définie, il convient de la mettre en œuvre au sein du système informatique. Deux approches non exclusives sont envisageables: la prévention des attaques et leur détection.

La première approche, en appliquant un contrôle a priori sur les actions effectuées au sein du système, s'assure que les utilisateurs ne pourront violer la politique. Cette approche évite que le système ne se trouve dans un état corrompu, nécessitant une analyse et une correction. De ce fait, des mécanismes de prévention sont présents sur les systèmes informatiques ; il s'agit souvent de contrôle d'accès. Cependant, de tels mécanismes possèdent leurs propres limitations, qui peuvent porter sur des aspects théoriques des modèles sous-jacents ou sur leur implémentation.

Ces limitations justifient le recours à des mécanismes de détection Intrusion Détection Systems (IDS)par exemple.

L'objectif de la détection d'intrusions est d'automatiser la tâche d'audit.

Il s'agit bien, théoriquement, de détecter de manière automatique les violations de politique de sécurité, qu'on appelle intrusions. Dans la pratique, les outils actuels ne sont cependant pas configurés directement par la politique. Aussi, s'ils détectent certaines intrusions, ils détectent aussi des tentatives d'intrusions infructueuses, ce qui peut être souhaité, ou non. En outre, la relative naïveté des algorithmes de détection conduit à un nombre élevé d'alertes, dont une part significative est en fait constituée de fausses alertes (faux positifs).

Enfin, certaines intrusions peuvent ne pas être détectées (faux négatifs).

Afin de qualifier un IDS, on s'intéresse à sa fiabilité, qui est sa capacité à émettre une alerte pour toute violation de la politique de sécurité, et à sa pertinence, qui est sa capacité à n'émettre une alerte qu'en cas de violation de la politique de sécurité.

Le premier chapitre est un chapitre descriptif pour le principe de sécurité.

Le second chapitre est consacré à présenter quelques techniques de sécurité.

Le dernier chapitre est consacre pentesting.

Chapitre I :

1. Préambule

La sécurité à priori, c'est le sentiment, à tort ou à raison,
D'être à l'abri de tout danger.

Cependant doit-on se limiter à cette Définition , Assurément non. Bien qu'elle présente un postulat de départ satisfaisant, il ne faut pas s'y arrêter. Une autre formulation plus adaptée au contexte des systèmes d'information pourrait être la suivante : protéger l'intégrité, assurer la disponibilité et garantir la confidentialité des biens.

La sécurité des réseaux a toujours été vue comme le parent pauvre du Domaine des technologies de l'information numérique.

Elle constitue Pour beaucoup une contrainte et un investissement en temps, ressources et argent.

Longtemps, les utilisateurs et administrateurs n'ont pas bien vu la nécessité d'entreprendre des actions de sécurisation et les décideurs n'ont pas eu d'idée concrète du retour sur investissement qu'elles impliquaient.

Aujourd'hui, les directeurs ont pris le tournant de la sécurité des systèmes d'information.

Elle est progressivement devenue une préoccupation majeure s'intégrant dans les définitions de politiques de gestion des risques, motivées par le sentiment latent d'insécurité.

2. Principes de Sécurité du système d'information

2.1. Premières notions de sécurité

Ce chapitre introduit les notions de base de la sécurité informatique : menace, risque, vulnérabilité ; il effectue un premier parcours de l'ensemble du domaine, de

ses aspects humains, techniques et organisationnels, sans en donner de description technique.

La Sécurité des Systèmes d'Information (SSI) est aujourd'hui un sujet important
Parce que le système d'information (SI) est pour beaucoup d'entreprises un élément Absolument vital : le lecteur a priori, devrait être déjà convaincu de cette évidence, mais il n'est peut-être pas inutile de lui donner quelques Menaces, risques,vulnérabilitésmunitions pour l'aider à en convaincre sa hiérarchie.

Il pourra par exemple à cet effet expliquant comment pour une entreprise comme Air-France le SI, qui comporte notamment Le système de réservation Amadeus, est un actif plus crucial que les avions.

En effet,Toutes les compagnies font voler des avions : mais la différence entre celles qui survivent et celles qui disparaissent (rappelons l'hécatombe récente : Panam, TWA,
Swissair, Sabena...) réside d'une part dans l'aptitude à optimiser l'emploi du temps des avions et des équipages, notamment par l'organisation de hubs, c'est-à-dire de Plates-formes où convergent des vols qui amènent des passagers qui repartiront par d'autres vols de la compagnie, d'autre part dans l'aptitude à remplir les avions de passagers qui auront payé leur billet le plus cher possible, grâce à la technique du yield management, qui consiste à calculer pour chaque candidat au voyage le prix à partir duquel il renoncerait à prendre l'avion, et à lui faire payer juste un peu moins.

Ce qui permet aux compagnies d'atteindre ces objectifs, et ainsi de l'emporter Sur leurs rivales, c'est bien leur SI, qui devient dès lors un outil précieux, irremplaçable, en un mot vital.

La même chose est déjà vraie depuis longtemps pour les banques, bien sûr. Puisque le SI est vital, tout ce qui le menace est potentiellement mortel. Conjurer Les menaces contre le SI est devenu impératif, et les lignes qui suivent sont une Brève description de ce qu'il faut faire pour cela.

Les menaces contre le système d'information entrent dans une des catégories suivantes : atteinte à la disponibilité des systèmes et des données, destruction de Données, corruption ou falsification de données, vol ou espionnage de données, Usage illicite d'un système ou d'un réseau, usage d'un système compromis pour Attaquer d'autres cibles.

Les menaces engendrent des risques et coûts humains et financiers : perte de confidentialité De données sensibles, indisponibilité des infrastructures et des données, dommages pour le patrimoine intellectuel et la notoriété. Les risques peuvent se réaliser si les systèmes menacés présentent des vulnérabilités.

Il est possible de préciser la notion de risque en la décrivant comme le produit d'un préjudice par une probabilité d'occurrence : risque = préjudice x probabilités d'occurrence
Cette formule exprime qu'un événement dont la probabilité est assez élevée, par exemple la défaillance d'un disque dur, mais dont il est possible de prévenir le préjudice qu'il peut causer, par des sauvegardes régulières, représente un risque acceptable ; il en va de même pour un événement à la gravité imparable, comme l'impact d'un météorite de grande taille, mais à la probabilité d'occurrence faible.

Il va de soi que, dans le premier cas, le risque ne devient acceptable que si les mesures de prévention contre le préjudice sont effectives et efficaces : cela irait sans dire, si l'oubli de cette condition n'était très fréquent.

Si la question de la sécurité des systèmes d'information a été radicalement bouleversée par l'évolution rapide de l'Internet, elle ne saurait s'y réduire ; il s'agit d'un vaste problème dont les aspects techniques ne sont qu'une partie. Les aspects juridiques, sociaux, ergonomiques, psychologiques et organisationnels sont aussi importants, sans oublier les aspects immobiliers, mais nous commencerons par les aspects techniques liés à l'informatique.

2.2. Aspects techniques de la sécurité

Les problèmes techniques actuels de sécurité informatique peuvent, au moins provisoirement, être classés en deux grandes catégories :

•ceux qui concernent la sécurité de l'ordinateur proprement dit, serveur ou poste de travail, de son système d'exploitation et des données qu'il abrite ;

•ceux qui découlent directement ou indirectement de l'essor des réseaux, qui multiplie la quantité et la gravité des menaces.

Si les problèmes de la première catégorie citée ici existent depuis la naissance de l'informatique, il est clair que l'essor des réseaux, puis de l'Internet, en a démultiplié l'impact potentiel en permettant leur combinaison avec ceux de la seconde catégorie.

La résorption des vulnérabilités repose sur un certain nombre de principes et de méthodes que nous allons énumérer dans la présente section avant de les décrire plus en détail.

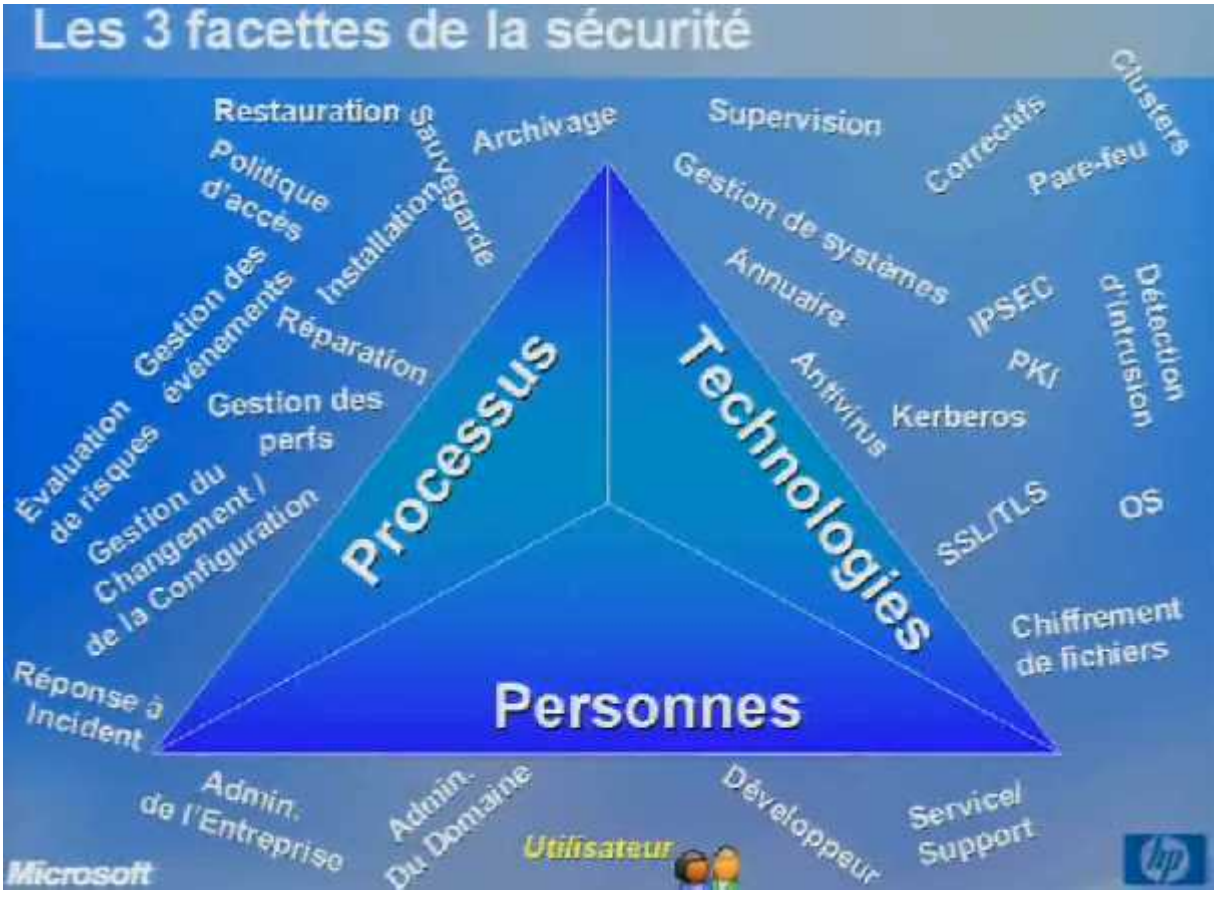

Fig.1.les 3 facettes de sécurité

3. Définir risques et objets à protéger

3.1. Périmètre de sécurité

Inutile de se préoccuper de sécurité sans avoir défini ce qui était à protéger : en d'autres termes toute organisation désireuse de protéger ses systèmes et ses réseaux doit déterminer son périmètre de sécurité. Le périmètre de sécurité, au sein de l'univers physique, délimite l'intérieur et l'extérieur, mais sa définition doit aussi englober (ou pas) les entités immatérielles qui peuplent les ordinateurs et les réseaux, essentiellement les logiciels et en particulier les systèmes d'exploitation.

Une fois fixé ce périmètre, il faut aussi élaborer une politique de sécurité, c'est a dire décider de ce qui est autorisé et de ce qui est interdit. À cette politique viennent bien sûr s'ajouter les lois et les règlements en vigueur, qui s'imposent à tous. Cela fait, il sera possible de mettre en place les solutions techniques appropriées à la défense du périmètre selon la politique choisie.

Mais déjà il est patent que les dispositifs techniques ne pourront pas résoudre tous les problèmes de sécurité, et, de surcroît, la notion même de périmètre de sécurité est aujourd'hui battue en brèche par des phénomènes comme la multiplication des ordinateurs portables qui, par définition, se déplacent de l'intérieur à l'extérieur et inversement, à quoi s'ajoute l'extraterritorialité de fait des activités sur l'Internet.

3.2. Périmètre et frontière

La notion de périmètre de sécurité, ainsi que le signalait déjà l'alinéa précédent,
Devient de plus en plus fragile au fur et à mesure que les frontières entre l'extérieur et l'intérieur de l'entreprise ainsi qu'entre les pays deviennent plus floues et plus poreuses.

Interviennent ici des considérations topographiques : les ordinateurs portables entrent et sortent des locaux et des réseaux internes pour aller se faire contaminer à l'extérieur ; mais aussi des considérations logiques : quelles sont les lois et les règles qui peuvent s'appliquer à un serveur hébergé aux États- Unis, qui appartient à une entreprise française et qui sert des clients brésiliens et canadiens ?

Par exemple la justice et les fournisseurs français d'accès à l'Internet (FAI) en ont fait l'expérienceun certain nombre d'organisations ont déposé devant les tribunaux français des plaintes destinées à faire cesser la propagation de pages Web à contenus négationnistes, effectivement attaquables en droit français.

Mais les sites négationnistes étaient installés aux États-Unis, pays dépourvu d'une législation anti négationniste, ce qui interdisait tout recours contre les auteurs et les éditeurs des pages en question.

Les plaignants se sont donc retournés contre les FAI français, par l'intermédiaire desquels les internautes pouvaient accéder aux pages délictueuses, mais ceux-ci n'en pouvaient mais aux résultats incertains, et en fin de compte vaine, car les éditeurs des pages en question disposent de nombreux moyens pour déjouer les mesures de prohibition.

Cette question du filtrage de contenu est traitée par le rapport Kahn-Brugidou [25] ; le site www.legalis.net [73] assure une veille juridique bien faite sur toutes les questions liées aux développements de l'informatique et de l'Internet ; les livres De SolveigGodeluck[59] et de Lawrence Lessig[74] replacent ces questions dans Un contexte plus général.

3.3. Ressources publiques, ressources privées

Les systèmes et les réseaux comportent des données et des programmes que nous considérerons comme des ressources. Certaines ressources sont d'accès public, ainsi certains serveurs Web, d'autres sont privées pour une personne, comme une boîte à lettres électronique, d'autres sont privées pour un groupe de personnes, comme l'annuaire téléphonique interne d'une entreprise.

Ce caractère plus ou moins public d'une ressource doit être traduit dans le système sous forme de droits d'accès, comme nous le verrons à la où cette notion est présentée.

4. Identifier et authentifier

Les personnes qui accèdent à une ressource non publique doivent être identifiées ; leur identité doit être authentifiée ; leurs droits d'accès doivent être vérifiés au regard des habilitations qui leur ont été attribuées : à ces trois actions correspond un premier domaine des techniques de sécurité, les méthodes d'authentification, de signature, de vérification de l'intégrité des données et d'attribution de droits (une habilitation donnée à un utilisateur et consignée dans une base de données adéquate est une liste de droits d'accès et de pouvoirs formulés de telle sorte qu'un système informatique puisse les vérifier automatiquement).

La sécurité des accès par le réseau à une ressource protégée n'est pas suffisamment garantie par la seule identification de leurs auteurs. Sur un réseau local de type
Ethernet où la circulation des données fonctionne selon le modèle de l'émission radiophonique que tout le monde peut capter (enfin, pas si facilement que cela, heureusement), il est possible à un tiers de la détourner.

Si la transmission a lieu à travers l'Internet, les données circulent de façon analogue à une carte postale, c'est à- dire qu'au moins le facteur et la concierge y ont accès. Dès lors que les données doivent être protégées, il faut faire appel aux techniques d'un autre domaine de la sécurité informatique : le chiffrement.

Authentification et chiffrement sont indissociables : chiffrer sans authentifier ne protège pas des usurpations d'identité (comme notamment l'attaque par interposition, dite en anglais attaque de type man in the middle, authentifier sans chiffrer laisse la porte ouverte au vol de données.

5. Empêcher les intrusions

Mais ces deux méthodes de sécurité ne suffisent pas, il faut en outre se prémuni contre les intrusions destinées à détruire ou corrompre les données, ou à en rendre l'accès impossible.

Les techniques classiques contre ce risque sont l'usage de pare-feu (firewalls) et le filtrage des communications réseaux, qui permettent de protéger la partie privée d'un réseau dont les stations pourront communiquer avec l'Internet sans en être « visibles » ; le terme visible est ici une métaphore qui exprime que nul système connecté à l'Internet ne peut de sa propre initiative accéder aux machines du réseau local (seules ces dernières peuvent établir un dialogue) et que le filtre interdit certains types de dialogues ou de services, ou certains correspondants (reconnus dangereux).

La plupart des entreprises mettent en place des ordinateurs qu'elles souhaitent rendre accessibles aux visiteurs extérieurs, tels que leur serveur Web et leur relais de messagerie.

Entre le réseau privé et l'Internet, ces machines publiques seront placées sur un segment du réseau ouvert aux accès en provenance de l'extérieur, mais relativement isolé du réseau intérieur, afin qu'un visiteur étranger à l'entreprise ne puisse pas accéder aux machines à usage strictement privé.

Un tel segment de réseau est appelé zone démilitarisée (DMZ), en souvenir de la zone du même nom qui a été établie entre les belligérants à la fin de la guerre de Corée.

Les machines en DMZ, exposées donc au feu de l'Internet, seront appelées bastions.

Certains auteurs considèrent que ces techniques de sécurité par remparts, pont-levis et échauguettes sont dignes du Moyen-âge de l'informatique ; ils leur préfèrent les systèmes de détection d'intrusion (IDS), plus subtils, qui sont décrits et ses sous-sections.

La surenchère suivante proclame que si l'on a détecté une intrusion, autant la stopper, et les IDS sont devenus des IPS (systèmes de prévention d'intrusion). Et l'on verra plus loin que les IPS sont critiqués par les tenants des mandataires applicatifs, plus subtils encore.

Cela dit, dans un pays sage informatique où les micro-ordinateurs prolifèrent sans qu'il soit réaliste de prétendre vérifier la configuration de chacun, le filtrage et le pare-feu sont encore irremplaçables.

Pour couper court à toutes ces querelles autour des qualités respectives de telle ou telle méthode de sécurité, il suffit d'observer l'état actuel des menaces et des vulnérabilités.
Il y a encore une dizaine d'années, le paramétrage de filtres judicieux sur le routeur de sortie du réseau d'une entreprise vers l'Internet pouvait être considéré comme une mesure de sécurité bien suffisante à toutes fins pratiques.

Puis il a fallu déployer des antivirus sur les postes de travail.

Aujourd'hui, les CERT (Computer Emergency Réponse Teams, pour une description de ces centres de diffusion d'informations de sécurité informatique) publient une dizaine de vulnérabilités nouvelles par semaine, et l'idée de pouvoir se prémunir en flux tendu contre toutes est utopique.

La conception moderne de la protection des systèmes et des réseaux s'appuie sur la notion de défense en profondeur, par opposition à la défense frontale rigide, où l'on mise tout sur l'efficacité absolue d'un dispositif unique.

6. Défense en profondeur

La défense en profondeur —au sujet de laquelle on lira avec profit un article du
Général Bailey [12] qui évoque à son propos une véritable « révolution dans les affaires militaires » — consiste à envisager que l'ennemi puisse franchir une ligne de défense sans pour cela qu'il devienne impossible de l'arrêter ; cette conception s'impose dès lors que les moyens de frappe à distance et de déplacement rapide, ainsi que le combat dans les trois dimensions, amènent à relativiser la notion de ligne de front et à concevoir l'affrontement armé sur un territoire étendu.

Plus modestement, la multiplication des vulnérabilités, la généralisation des ordinateurs portables qui se déplacent hors du réseau de l'entreprise, l'usage de logiciels novateurs (code mobile, Peer to Peer, sites interactifs, téléphonie et visioconférence sur IP) et d'autres innovations ont anéanti la notion de « périmètre de sécurité » de l'entreprise, et obligent le responsable SSI à considérer que la menace est partout et peut se manifester n'importe où.

Il faut continuer à essayer d'empêcher les intrusions dans le SI de l'entreprise, mais le succès de la prévention ne peut plus être garanti, et il faut donc se préparer à limiter les conséquences d'une attaque réussie, qui se produira forcément un jour. Et ce d'autant plus que le SI contemporain n'est pas comme par le passé contenu par un « centre de données » monolithique hébergé dans un bunker, mais constitué de multiples éléments plus ou moins immatérielsqui vivent sur des ordinateurs multiples, dispersés dans toute l'entrepriseet au dehors ; et c'est cette nébuleuse qu'il faut protéger.

Nous allons au cours des chapitres suivants examiner un peu plus en détail certaines collections de techniques qui s'offrent au responsable SSI, en commençant par la cryptographie dont sont dérivées les techniques de l'authentification.

Fig.2. la défense en profondeur

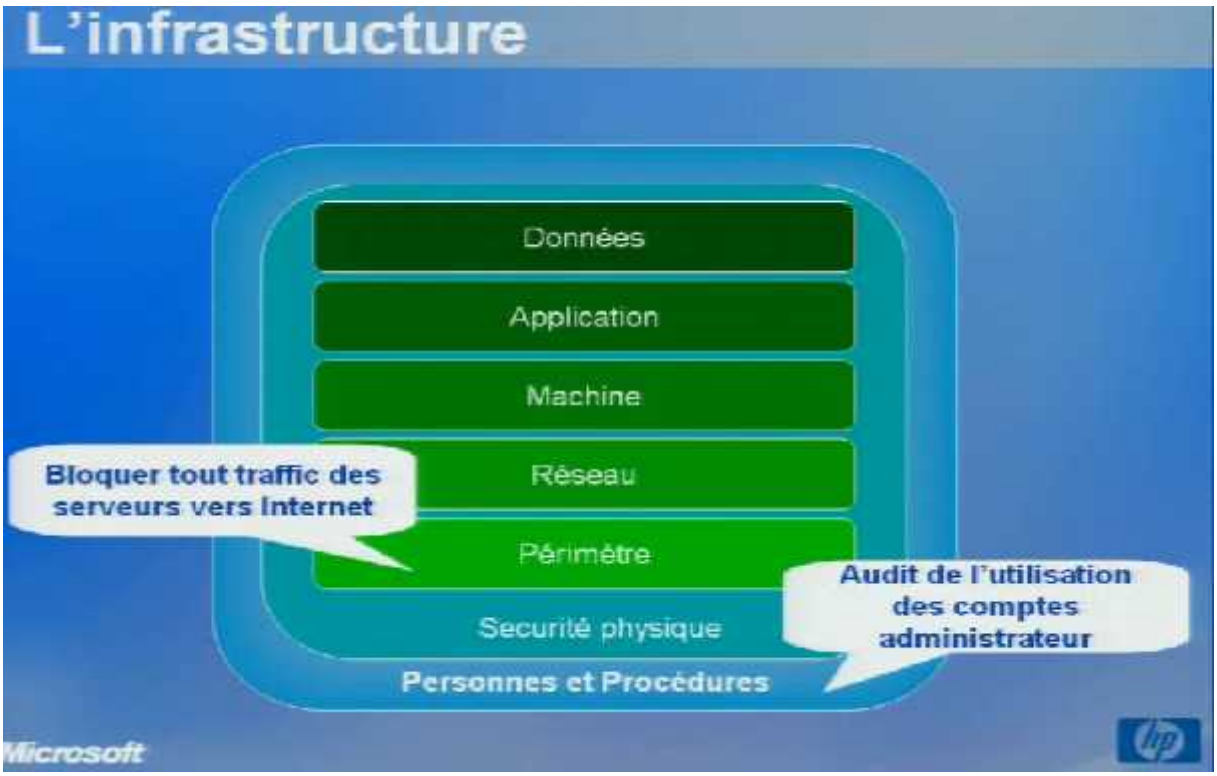

Fig.3. la défense en profondeur en infrastructure

La politique adapter en cas des réseaux applicative et serveur sql par exemple c est présent dans les figures suivantes :

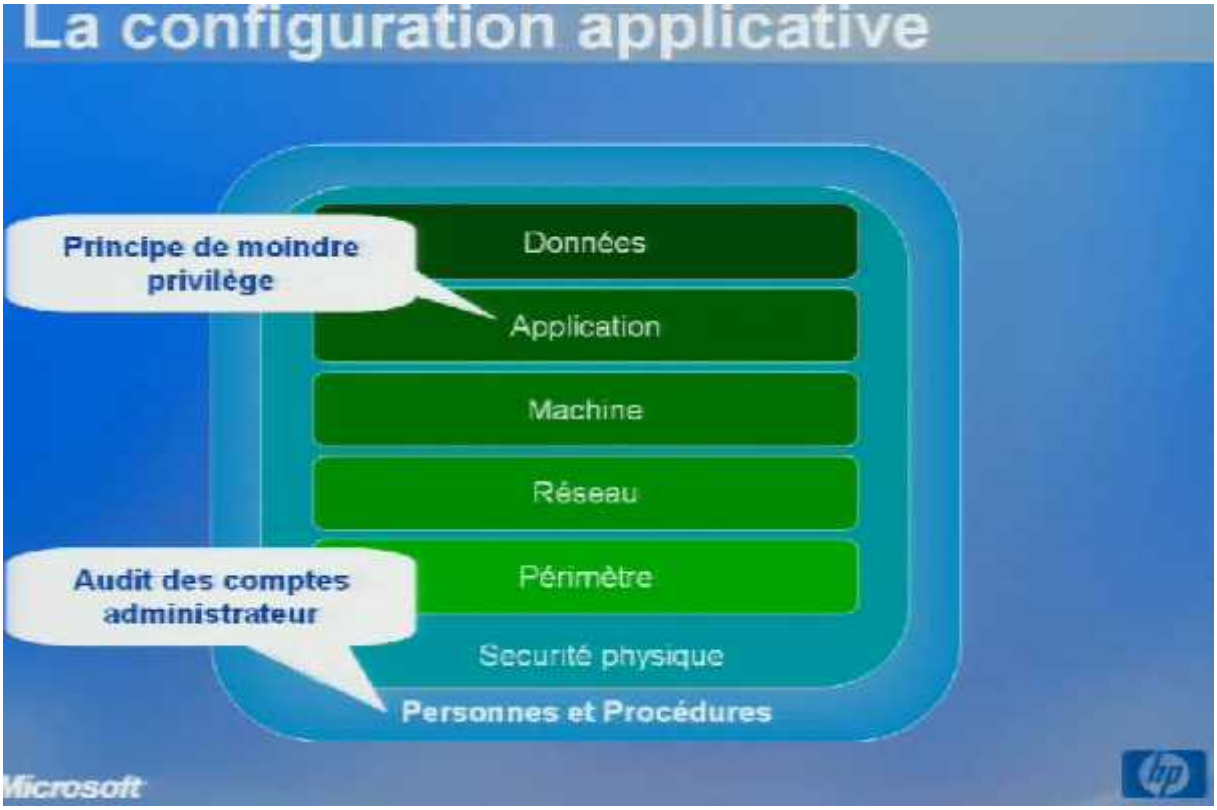

Fig.4.la défense en profondeur applicative.

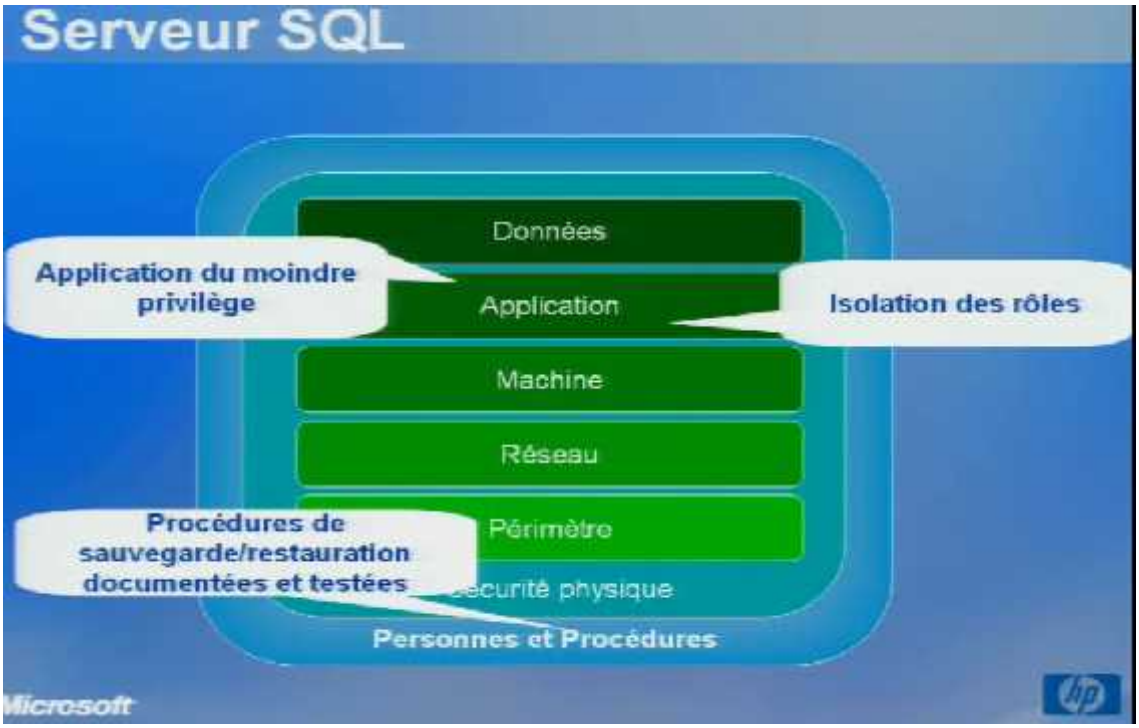

Fig.5.la défense en profondeur des serveurs

7. Sauvegarder données et documents

La sauvegarde régulière des données et de la documentation qui permet de les utiliser est bien sûr un élément indispensable de la sécurité du système d'information, elle constitue un sujet d'étude à elle seule, qui justifierait un livre entier.

Aussi ne ferons-nous, dans le cadre du présent ouvrage, que l'évoquer brièvement, sans aborder les aspects techniques. Mentionnons ici quelques règles de bon sens :

•Pour chaque ensemble de données il convient de déterminer la périodicité des opérations de sauvegarde en fonction des nécessités liées au fonctionnement de l'entreprise.

•Les supports de sauvegarde doivent être stockés de façon à être disponibles après un sinistre tel qu'incendie ou inondation : armoires ignifugées étanches ou site externe.

•Les techniques modernes de stockage des données, telles que Storage Area Network (SAN) ou Network Attached Storage (NAS), conjuguées à la disponibilitéde réseaux à haut débit, permettent la duplication de données à distance de plusieurs kilomètres (voire plus si l'obstacle financier n'est pas à considérer), et ce éventuellement en temps réel ou à intervalles très rapprochés ce type de solution est idéal pour un site de secours.

•De l'alinéa précédent, on déduit que, dans un système d'information moderne, toutes les données doivent être stockées sur des SAN ou des NAS, rien ne justifie l'usage des disques attachés directement aux serveurs, qui seront réservés aux systèmes d'exploitation et aux données de petit volume.

•Les dispositifs et les procédures de sauvegarde et, surtout, de restauration doivent être vérifiés régulièrement.

8. Vérifier les dispositifs de sécurité

Le dispositif de sécurité le mieux conçu ne remplit son rôle que s'il est opérationnel, et surtout si ceux qui doivent, en cas de sinistre par exemple, le mettre en œuvre, sont eux aussi opérationnels. Il convient donc de vérifier régulièrement les capacités des dispositifs matériels et organisationnels.

Les incidents graves de sécurité ne surviennent heureusement pas tous les jours : de ce fait, si l'on attend qu'un tel événement survienne pour tester les procédures palliatives, elles risquent fort de se révéler défaillantes. Elles devront donc être exécutées
« à blanc » périodiquement, par exemple en effectuant la restauration d'un ensemble de données à partir des sauvegardes tous les six mois, ou le redémarrage d'une application à partir du site de sauvegarde.

Outre ces vérifications régulières, l'organisation d'exercices qui simulent un événement de sécurité impromptu peut être très profitable. De tels exercices, inspirés des manœuvres militaires, révéleront des failles organisationnelles telles que rupture de la chaîne de commandement ou du circuit d'information. Un rythme bisannuel semble raisonnable pour ces opérations.

9. S'informer auprès des CERT

Les CERT (Computer Emergency Réponse Teams) centralisent, vérifient et publient les alertes relatives à la sécurité des ordinateurs, et notamment les annonces de vulnérabilités récemment découvertes. Les alertes peuvent émaner des auteurs du logiciel, ou d'utilisateurs qui ont détecté le problème. Détecter une vulnérabilité ne veut pas dire qu'elle soit exploitée, ni même exploitable, mais le risque existe.

Publication les failles de sécurité

Un débat s'est engagé sur le bien-fondé de certains avis, et sur la relation qu'il pourrait y avoir entre le nombre d'avis concernant un logiciel ou un système donné et sa qualité intrinsèque. Les détracteurs des logiciels libres ont mis en exergue le volume très important d'avis des CERT qui concernaient ceux-ci (par exemple Linux, le serveur Web Apache, Sendmail, etc.) pour en inférer leur fragilité.

Leurs défenseurs ont riposté en expliquant que les avis des CERT concernaient par définition des failles de sécurité
(1Du moins à en croire son auteur Robert Tappan Morris.
2Cf. http://www.certa.ssi.gouv.fr/

3Cf. http://www.renater.fr/rubrique.php3?id_rubrique=19
4Cf. http://www.cert-ist.com/)
découvertes et donc virtuellement corrigées, alorsque l'absence d'avis relatifs à tel système commercial pouvait simplement signifierque l'on passait sous silence ses défauts de sécurité en profitant de son opacité. Orl'expérience montre que tout dispositif de sécurité a des failles ; les attaquants neperdent pas leur temps à faire de la recherche fondamentale sur la factorisation desgrands nombres entiers, ils essaient de repérer les failles d'implémentation et ils lesexploitent.

Face à ce risque, la meilleure protection est une capacité de riposte rapide,qui consiste le plus souvent à commencer par désactiver le composant pris endéfaut en attendant la correction.

La communauté du logiciel libre excelle dans cetexercice, mais avec les logiciels commerciaux les utilisateurs n'ont souvent aucunmoyen d'agir : ils ne peuvent qu'attendre le bon vouloir de leur fournisseur.

Dansce contexte, la publication d'avis des CERT relatifs à des logiciels commerciauxest très bénéfique parce qu'elle incite les fournisseurs à corriger plus rapidementun défaut dont la notoriété risque de nuire à leur réputation.

Mais certains fournisseurscherchent à obtenir le silence des CERT en arguant du fait que leurs avisrisquent de donner aux pirates des indications précieuses... ce qui est fallacieux carles sites Web des pirates sont de toute façon très bien informés et mis à jour, eux,selon les principes du logiciel libre, ce qui indique bien où est l'efficacité maximale.

L'expérience tend à prouver qu'une faille de sécurité est d'autant plus vite comblée qu'elle est publiée tôt et largement. L'accès au code source du logiciel en défaut constitue bien sûr un atout.

La réponse à la question posée par le titre de cette section est donc : oui, il faut publier les failles de sécurité, mais de façon organisée et responsable, c'est-à-dire de façon certifiée, sur le site d'un organisme accrédité, typiquement un CERT, et après avoir prévenu l'auteur ou l'éditeur du logiciel en défaut et lui avoir laissé un délai raisonnable pour au moins trouver un palliatif d'urgence.

Il faut savoir qu'il existe aujourd'hui un marché de la faille, qui parfois n'est pas loin de s'apparenter à du chantage.

10.Discussion

Dans ce chapitre, on a présenté les principales notions et concepts de la sécurité

des systèmes informatiques et des réseaux, dont on a décrit une politique de sécurité.

Ainsi différentes méthodes et mécanismes connus pour sécuriser les réseaux.

Chapitre II :

1. Préambule

Dans ce chapitre nous allons étudier quelques solutions de protection de sécurité quand on a un réseau important vise a vie sont capital et la situation social.

2. Chiffrement, tunnels et VPN

2.1. Chiffrement de documents

• Les documents importants doivent être chiffrés.

• Le chiffrement peut être matériel (ordinateur portable avec disque auto chiffrant, clé usb auto chiffrante, …)

• Le chiffrement peut être logiciel, beaucoup de logiciels existent.

– winrar (chiffrement symétrique)

-GnuPG (chiffrement asymétrique)

– Enigmail plugin de Thunderbird pour l'échange de courrier électronique chiffré/signé.

– Truecrypt: Chiffrement de disques, de partitions de disques,de clés USB.

2.2. Protocoles chiffrés

Les informations confidentielles doivent transiter sur le réseau par des protocoles chiffres

• Exemples:

– https plutôt que http

– pops plutôt que pop

– imaps plutôt que imap

– smtps plutôt que smtp

228

1.3.Session chiffrée

• ssh (Secure Shell) plutôt que Telnet ,login ,rsh,rcp

• Génération d'une paire de clef RSA (toutes les heures) par le serveur.

• Envoi de la clef publique au client qui se connecte.

• Le client génère une clef symétrique, la chiffre avec la clef du serveur et la renvoie au serveur.

• Le reste de la communication chiffrement symétrique.

3. Tunneling

• Un protocole de tunneling est utilisé pour créer un chemin privé (tunnel) à travers une infrastructure éventuellement publique.

• Les données peuvent être encapsulées et cryptées pour emprunter le tunnel.

• Solution intéressante pour relier deux entités distantes à moindre coût.

• Un flux tcp quelconque peut être redirigé dans un tunnel ssh:

client serveur

clientssh serveur ssh

Exemple tunneling s

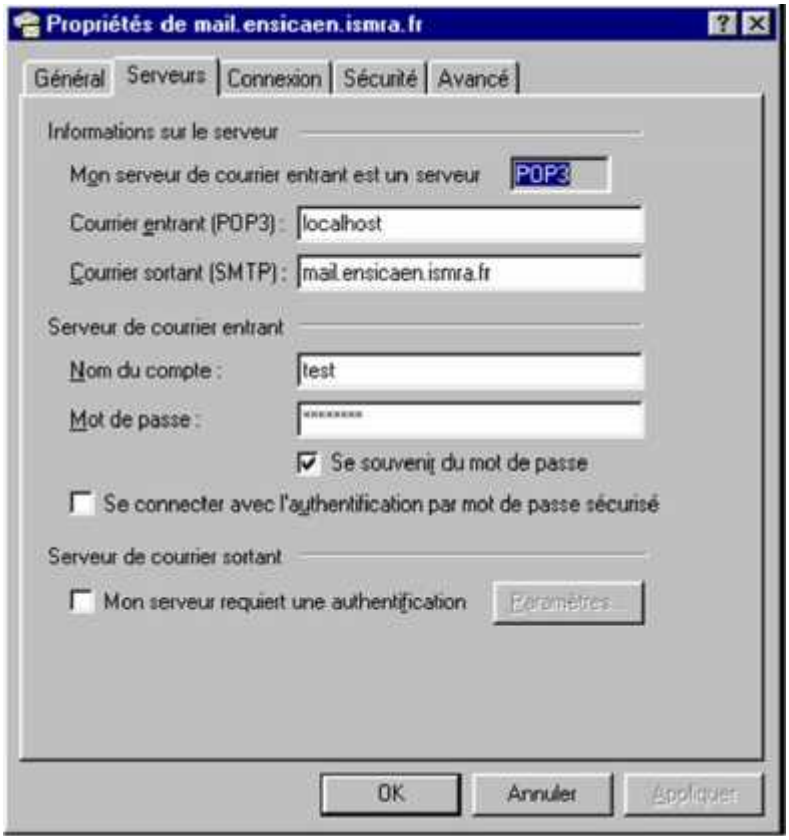

Fig.6. configuration du tunneling

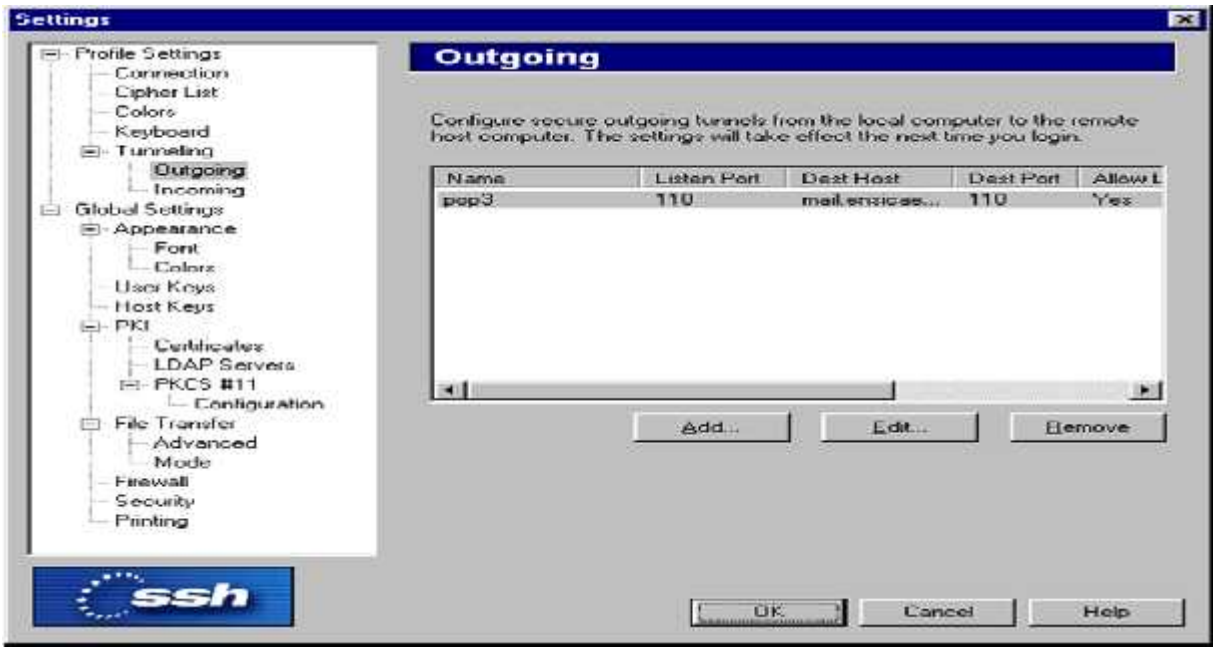

Fig.7.paramètres du tunneling.

Autre exemple de tunneling

• Autre logiciel de tunneling: stunnel utilisant SSL

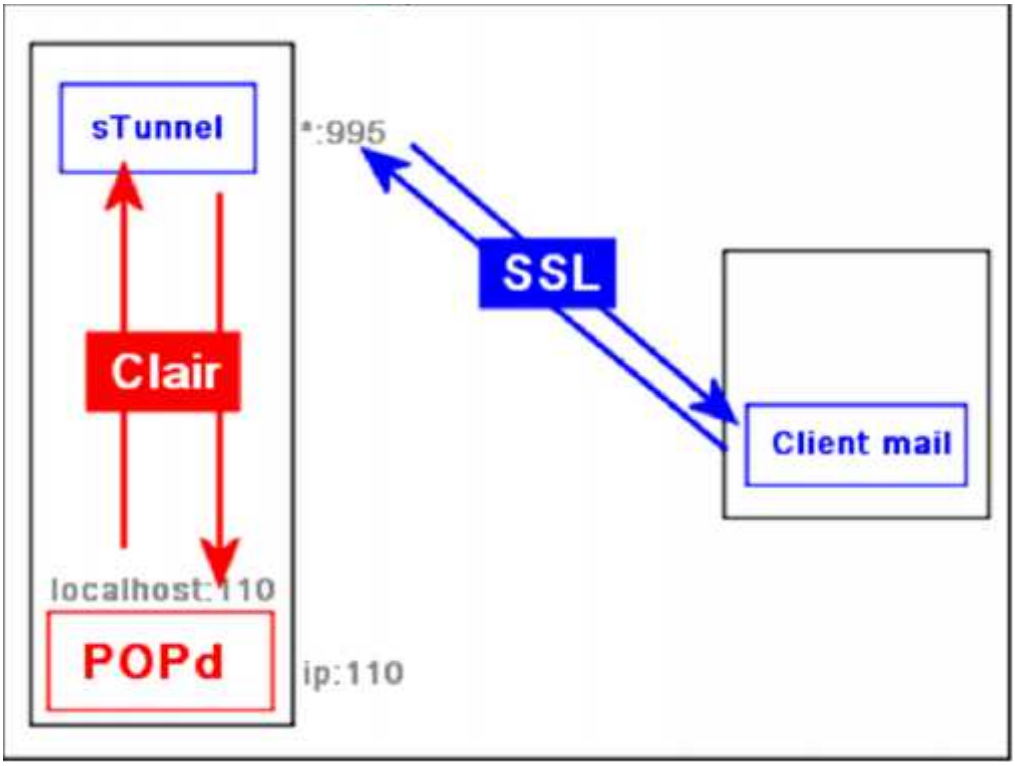

Fig.8.mécanisme du pop en tunneling.

4. Connexions TCP/IP sécurisées

4.1. SSL (Secure Sockets Layer)

– Se situe entre la couche application et la couche transport.

– Garantit l'authentification, l'intégrité et la confidentialité.

– Largement utilisé pour la sécurisation des sites www (https).

4.2. Fonctionnement SSL

1) Hello, version de SSL, protocole de chiffrement pris en charge, longueurs de clé, mécanisme d'échange de clé

2) Hello, examen des méthodes supportées par le client, envoi les méthodes et algorithmes de chiffrement, longueurs et mécanisme d'échanges de clé compatibles, envoi de la clé publique approuvée par client une autorité.

SSL serveur

SSL

3) Vérification du certificat envoyé par le serveur, envoi d'un message clé maître: liste de méthodologie de sécurité de sécurité employées par le client et clé de session cryptée avec la clé publique du serveur.

4) Message "client sécurisé" indiquant que les communications sont sûres.

4.3.1. IPSec

• IP SECurityprotocol issu d’une task force de l’IETF

• Quelques spécifications de l’IPSec:

– Authentification, confidentialité et intégrité (protection contre l'IPspoofing et le TCP session hijacking)

– Confidentialité (session chiffrée pour se protéger du sniffing)

– Sécurisation au niveau de la couche transport (protection L3).

• Algorithmes utilisés:

– Authentification pas signature DSS ou RSA

– Intégrité par fonction de condensation (HMAC-MD5, HMACSHA-1, …)

– Confidentialité par chiffrement DES, RC5, IDEA, CAST

4.3.2. Fonctionnement IP Sec

IPsec peut fonctionner:

– en mode transport; les machines source et destination sont les 2 extrémités de la connexion sécurisée.

– en mode tunnel: les extrémités de la connexion

Sécurisée sont des passerelles; les Communications hôte à hôte sont encapsulées

Dans les entêtes de protocole de tunnel IP Sec.

– en mode intermédiaire: tunnel entre une machine et une passerelle.

4.3.3. Services de sécurité IPSec

• IPSec utilise 2 protocoles pour implémenter la sécurité sur un réseau

IP:

– Entête d'authentification (AH) permettant d'authentifier les messages.

– Protocole de sécurité encapsulant (ESP) permettant d'authentifier et de crypter les messages.

IPSec: mode transport

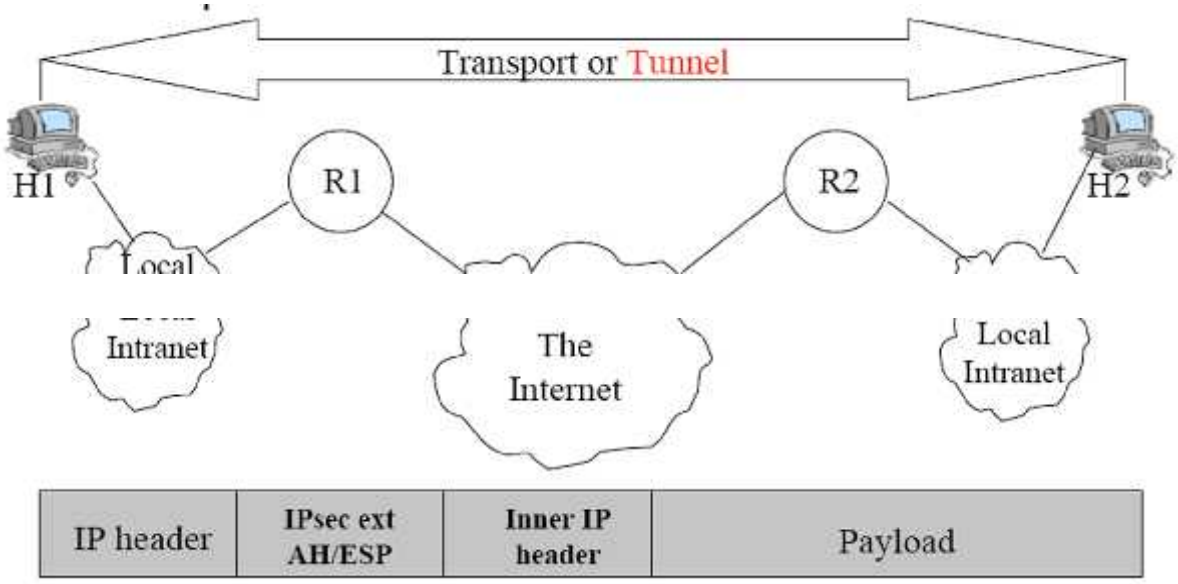

Fig.9. schéma du tunneling a travers internet entre 2 postes.

IPSec: mode tunnel

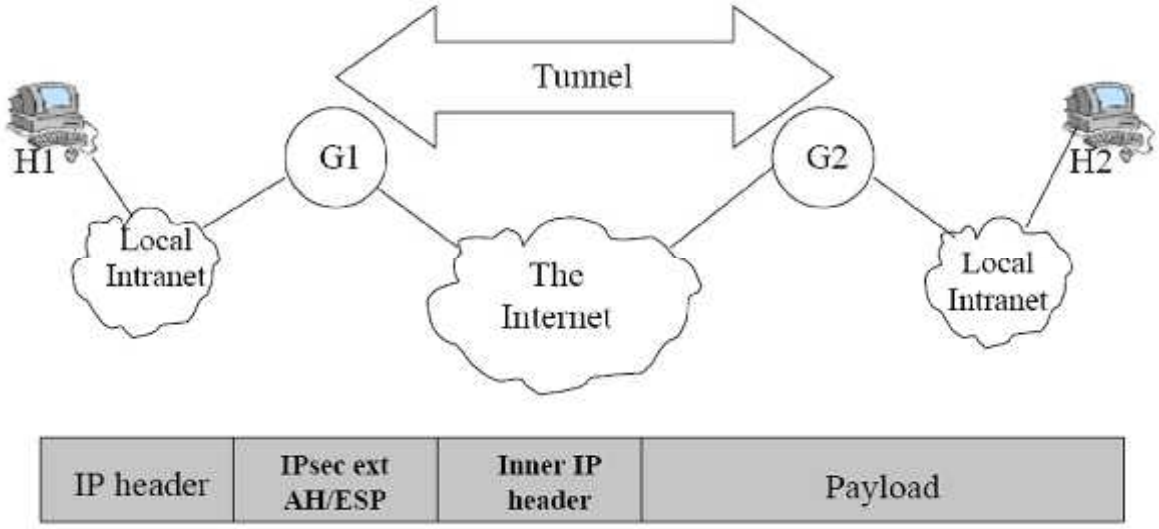

Fig.10.schéma entre 2 extrémités de connexion.

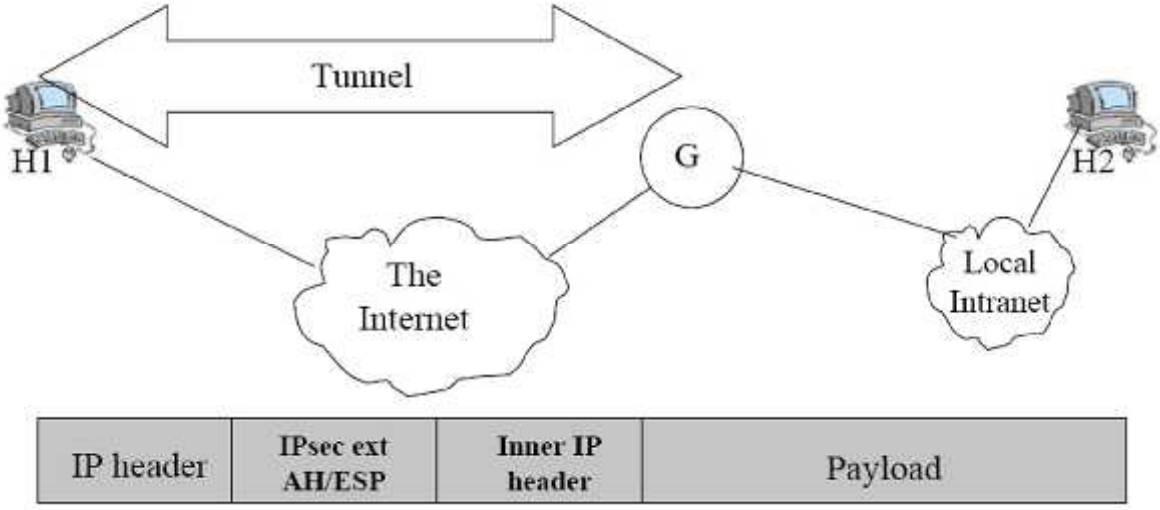

Fig.11.schéma entre un poste et une extrémité de connexion.

4.3.4. Etablissement d'une connexion IPSec

• 2 machines doivent s'accorder pour l'utilisation des algorithmes et protocoles à utiliser

• Une SA (Security Association) est établie pour chaque connexion.

• Une SA comprend:

– Un algorithme de chiffrement (DES, 3DES)

– Une clé de session via IKE (Internet KeyExchange)

– Un algorithme d'authentification (SHA1, MD5)

5. VirtualPrivate Network

• Permet de créer un tunnel chiffré sur une infrastructure publique entre 2 points.

• Les logiciels de VPN peuvent s'appuyer sur IP Sec ou SSL

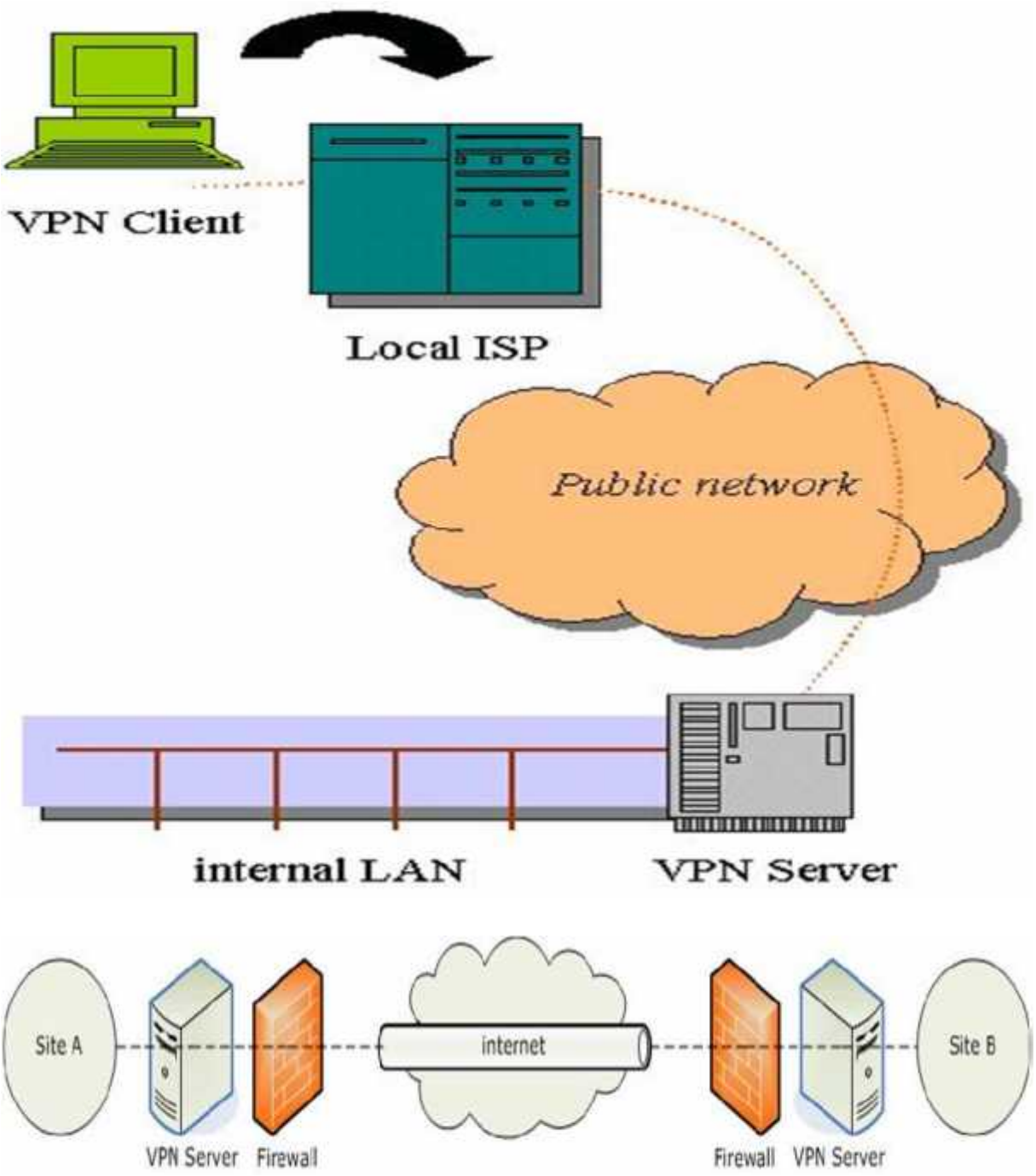

Fig.12.fonctionnement du VPN

6. Firewall

• Protéger son réseau du monde extérieur (Internet, autres services de l'entreprise).

• Maintenir des utilisateurs à l'intérieur du réseau

(Employé, enfant, …)

• Restreindre le nombre de machines à surveiller avec un maximum d'attention.

• Certaines machines doivent rester ouvertes (serveur www, DNS, etc).

C'est un outil souvent indispensable mais jamais suffisant:

– Pas de protection contre le monde intérieur

– Pas de protection contre les mots de passe faibles

6.1. Nécessite une politique de sécurité:

– Tout autoriser et interdire progressivement

– Tout interdire et ouvrir sélectivement

• Contrôler les accès entrant et sortant:

– par service

– par adresse IP

• Un firewall n'empêche pas:

– de bien protéger et administrer toutes ses machines.

– de bien structurer son réseau.

– d'éduquer et sensibiliser les utilisateurs.

– la signature de charte de bonne utilisation.

6.2. Différents types de firewall:

– filtres de paquets

– passerelles de circuits

– passerelles d'application

– Combinaison des 3 types précédents

Filtrage de paquets

• Paquets peuvent être triés en fonction des adresses

IP des ports sources et destination, du contenu.

• Pas de notion de contexte; la décision est prised'après le contenu du paquet en cours.

• Problème pour les fragments IP (pas de numéro deport dans la trame)

• Certains protocoles sont difficiles à filtrer (ftp, ...)

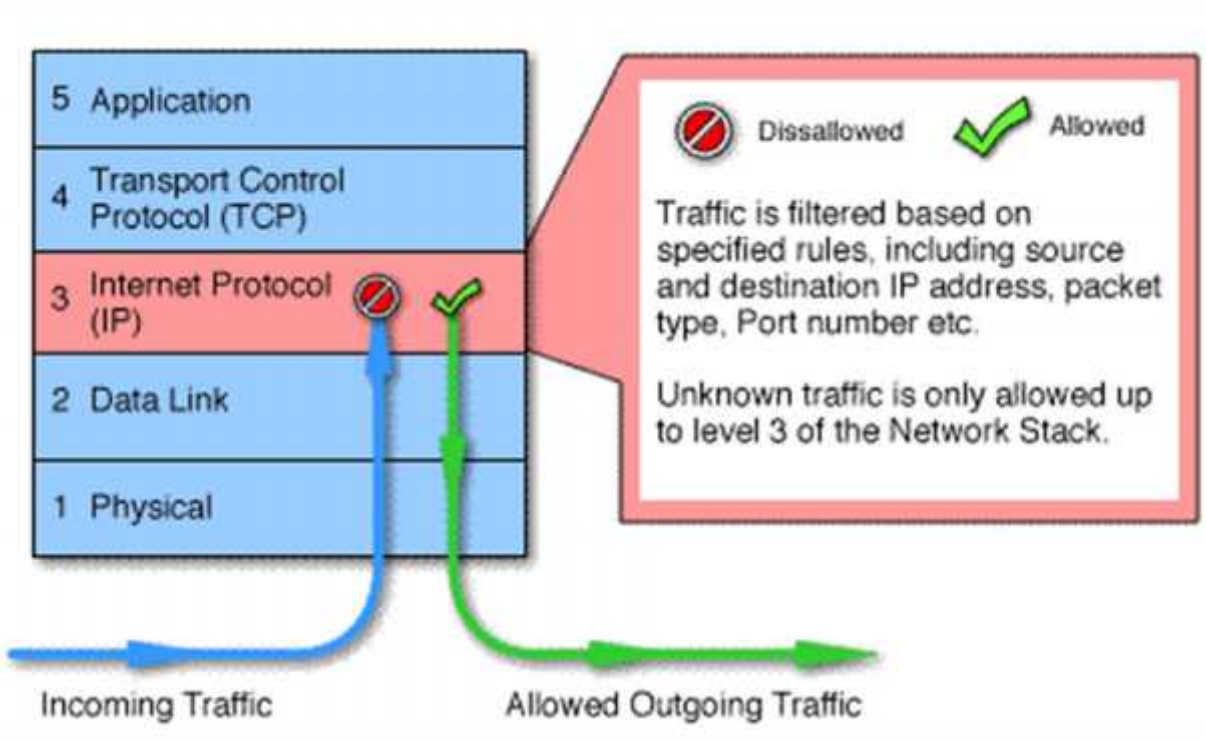

Fig.13.filtrage dans la couche 3.

6.3. Passerelles de circuits

• Les passerelles de circuits relaient les connexions TCP.

• L'appelant se connecte à un port TCP de la passerelle elle même connectée sur le port du service de la machine destination

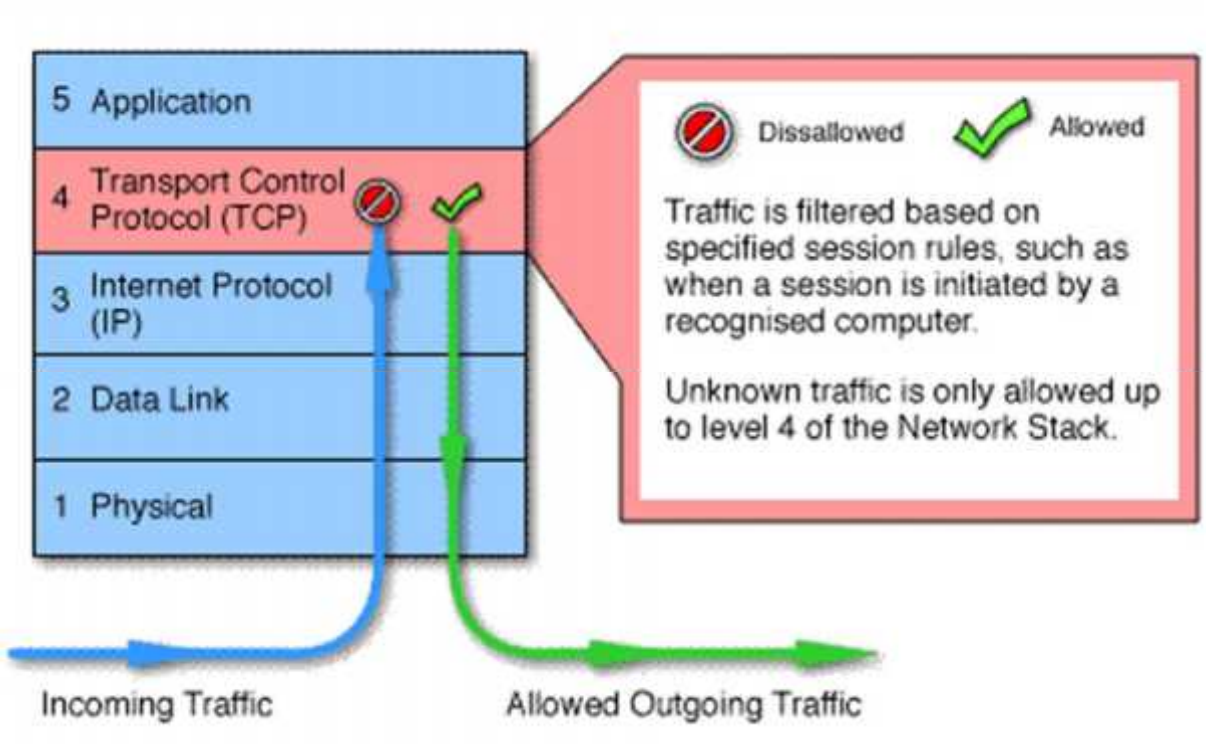

Fig.14.filtrage dans la couche 4.

6.4. Passerelles d'applications

• Un programme spécifique pour chaque application (exemples: relai de courrier, relai http, …).

• Permet de sectionner les flux.

• Plus complexes à mettre en œuvre.

Firewall "statefulmultilayer"

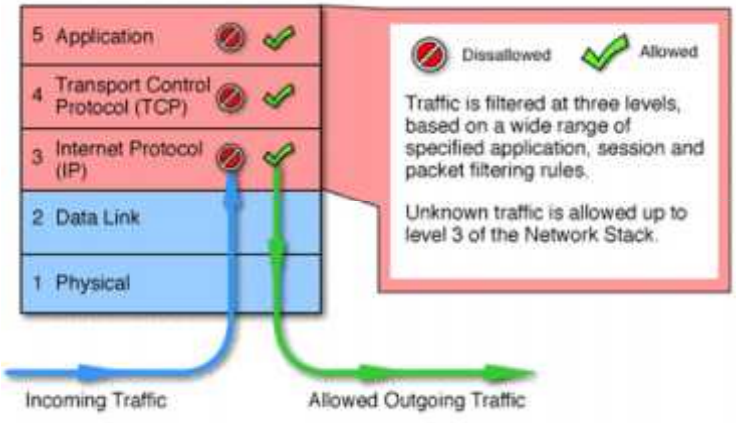

Fig.15.filtrage dans la couche application

6.5. Installation type d'un firewall

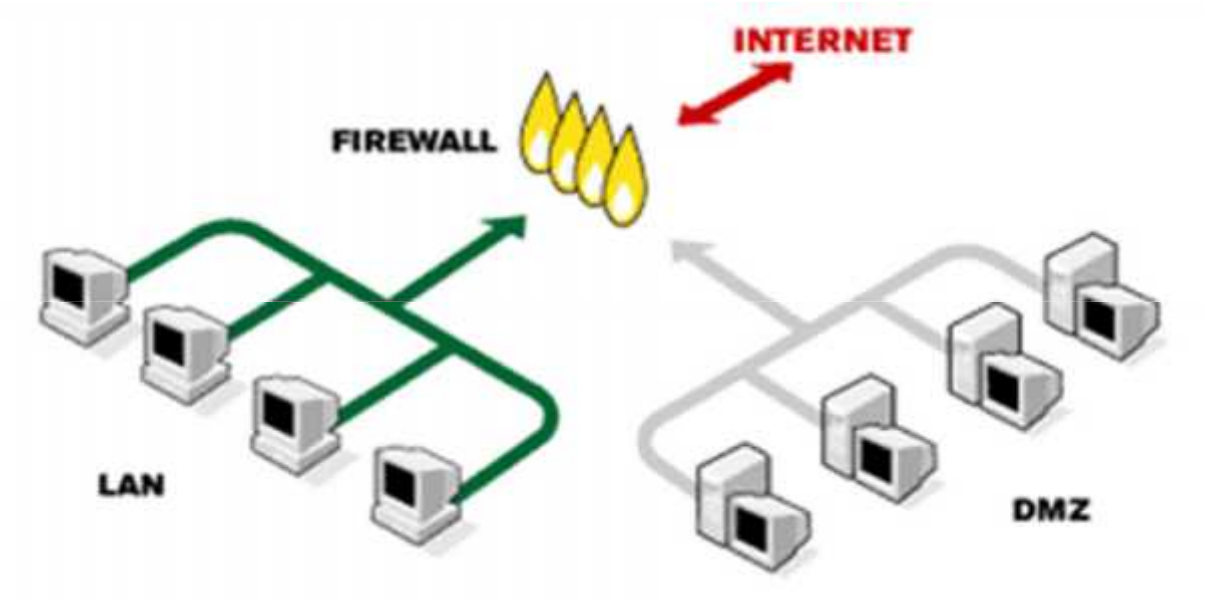

Fig.16.l'emplacement du pare-feu.

6.6. Fonctionnalités actuelles d'un Firewall

• Filtrage sur adresses IP/Protocole,

• Inspection stateful et applicative,

• Intelligence artificielle pour détecter le trafic anormal,

• Filtrage applicatif

– HTTP (restriction des URL accessibles),

– Anti Spam

– Antivirus, Anti-Logiciel malveillant

• Translation d'adresses,

• Tunnels IP Sec, PPTP, L2TP,

• Identification des connexions,

• Serveur Web pour offrir une interface de configuration agréable,

• Relai applicatif (proxy),

• Détection d'intrusion (IDS)

• Prévention d'intrusion (IPS).

7. Discussion

Les solutions proposées dans ce chapitre sont très fiable dans la sécurité des réseaux, quel nous que soit un réseau LAN, MAN ou WAN, la dernière figure nous montre par exemple la valeur de l’IDS.

Chapitre III :

1. Préambule

Dans ce chapitre, on va voir le niveau de sécurité des solutions proposer dans le chapitre précédent, et on appel cette méthode : pentesting.

L'outil utilise est : KALI LINUX.

2. Caractéristiques de Kali Linux

Kali est une reconstruction complète de BackTrack Linux, qui adhère aux standards de développement Debian. Une toute nouvelle infrastructure, tous les outils révisés et reconstruits.

- **Plus de 300 outils de tests d'intrusion:** Après une longue révisions des outils disponibles sur BackTrack, nous en avons éliminés plusieurs qui étaient soit non- fonctionnels, soit qui ont été remplacés par de nouveaux qui produisent des résultats similaires.
- **Gratuit pour toujours:** Kali Linux, comme son prédécesseur, sera entièrement gratuit et le sera toujours. Vous n'aurez jamais à débourser un cent pour Kali Linux.
- **Arborescence Git Open Source:** Promoteurs du mouvement Open Source, notrestructure de développement est disponible à tous. Téléchargement des codes sources pour que tout le monde puissent modifier et refaire les paquets selon ses abesoin.
- **Conforme au FHS:** Le développement de Kali adhère au standard FHS (FilesystemHierarchy Standard), ce qui permet aux utilisateurs de facilement naviguer le système et de rapidement trouver les fichiers de librairie, binaires, fichiers de support etc.
- **Vaste support pour appareils sans-fils:** Kali Linux est bâti pour supporter le plus d'appareils possible, lui permettant de fonctionner sans problèmes sur une grande variété de matériel, dispositifs USB et autres machins sans-fils.

- **Noyau patché pour injection:** Étant donné que les tests d'intrusions peuvent inclure aussi du réseau sans-fils, notre noyau est conçu et patché pour rendre la tâche possible.
- **Environnement de développement sécuritaire:** L'équipe de développement Kali est formé d'une petite équipe en confiance qui peut seulement interagir avec les répertoires de distribution via le biais de protocoles sécurisés.
- **Paquets signés GPG:** Tous les paquets Kali Linux sont signés par chaque auteur individuel quand ils sont construits et livrés à nos répertoires de distributions.
- **Multi-langues:** Tous les paquets Kali Linux sont signés par chaque auteur individuel quand ils sont construits et livrés à nos répertoires de distributions.
- **Personnalisation Complète:** Nous sommes au courant que tout le monde n'est pas d'accord avec nos conceptions. Les utilisateurs plus aventuriers peuvent personnaliser Kali Linux comme bon leur semble, jusqu'au noyau.
- **Support ARMEL et ARMHF:** Avec la popularité et la disponibilité des systèmes de base sur l'architecture ARM, nous savions que le support ARM pour Kali devait être aussi robuste que possible. Résultat, une version fonctionnelle de Kali sur les systèmesARMEL et ARMHF. Les répertoires de Kali Linux pour ARM sont intégrés aux autres distributions et les outils sont mis à jour en même temps que les autres outils. Kali est présentement disponible sur les systèmes suivants:
    - rk3306 mk/ss808
    - Raspberry Pi
    - ODROID U2/X2
    - Samsung Chromebook

Kali est spécifiquement conçu pour les tests d'intrusion et audit de sécurité, toutes documentation contenue sur se site suppose que le lecteur soit déjà familier avec le système d'exploitation Linux.

2.1. Metasploit :

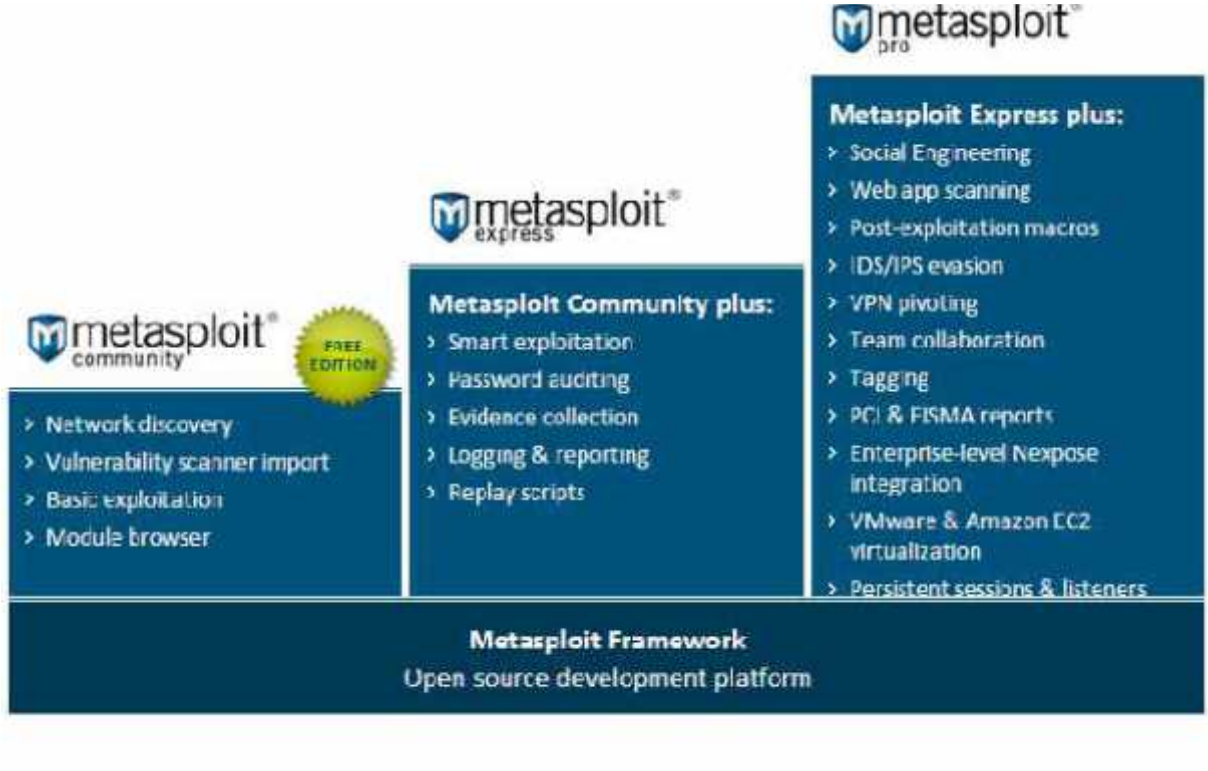

Fig.18. les versions du Metasploit.

Cette figure présente les différentes version du metsploit.

2.2.1. L’architecture interne

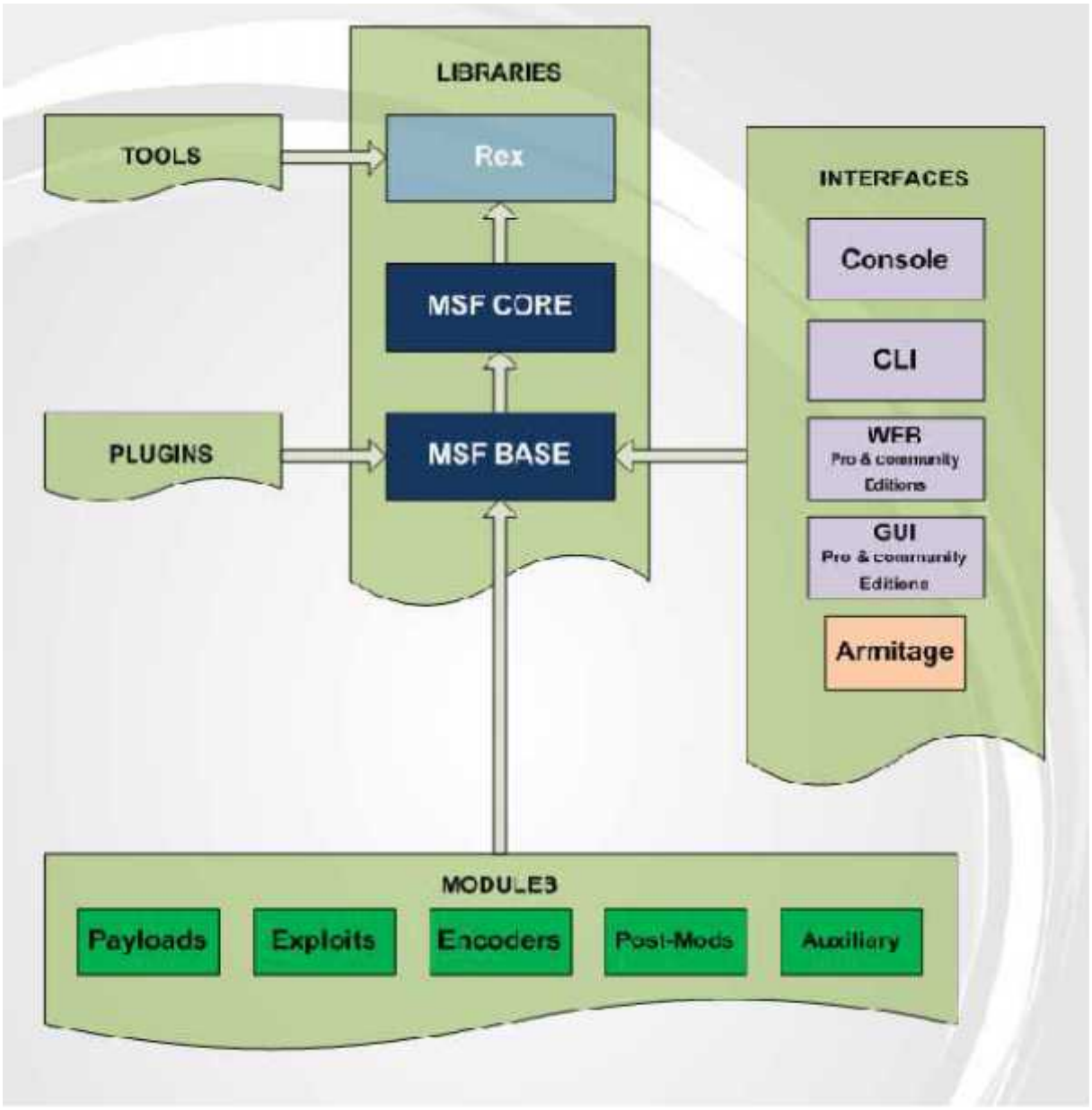

Fig.19. Architecture interne du Metasploit

Kali Linux - la distribution pour les geeks de sécurité critique

Quand il s'agit de piratage, de la sécurité, de la criminalistique chose comme ça, linux est le seul et l'outil préféré.Linux est très sympathique pirate à partir du sol. Mais il ya encore des distributions qui sont plus orientés vers l'assistance pirates. Pour n'en nommer que quelques-uns, backtrack, d'encastrement, etcblackbuntu.

Backtrack est la distribution la plus populaire quand il s'agit de tests de pénétration et des trucs de sécurité. Et maintenant, il a pris un nouvel avatar appelé Kali Linux . Kali Linux est le nouveau nom de backtrack (version 5 RC3 était la dernière version de backtrack).

2. Distribution complète basée sur Debian

Kali Linux a été amélioré sur Backtrack à bien des égards. Backtrack était une sorte de "outils de sécurité Ubuntu + placés dans le répertoire / pentest". Et de ce fait, d'exécuter un outil de sécurité d'abord l'utilisateur devait accéder au répertoire de

pentest. Ce fait les mises à jour trop difficile, car les outils ne sont pas de véritables installations qui pourraient être mises à jour à partir de synaptique.

Kali Linux est la nouvelle génération de tests de pénétration BackTrack Linux leader de l'industrie et de l'audit de sécurité distribution Linux. Kali Linux est une re-construction complète de BackTrack à partir du sol, en adhérant totalement aux normes de développement de Debian.

Kali linux a tout installé comme paquets qui peuvent être mis à jour à partir des référentiels. Kali Linux est basée sur Debian et est une distribution complète en elle-même. Pour exécuter n'importe quel outil il suffit de taper la commande à la borne et il irait.

Aussi, il n'est plus nécessaire de taper la commande startx au démarrage, comme dans backtrack.

Télécharger Kali Linux depuis l'adresse suivante

http://www.kali.org/downloads/

Il peut être facilement installé dans une de virtualisation comme VirtualBox. Enfait je l'utilise à l'intérieur virtualbox seulement. Kali linux a besoin pour fonctionner en tant que root, et donc sa très sûr de l'exécuter dans un environnement virtuel, ou d'un média en direct.

Au moment où écrire ce post, kali 1.0.4 était la dernière version.

Backtrack avait à la fois un gnome et kde version disponible en téléchargement.

Linux Cependant kali vient seulement dans le gnome basé construction. Cependant, d'autres postes de travail comme xfce, kde peuvent être facilement installés à partir synaptique.

Paquets par défaut

Kali linux par défaut livré avec beaucoup d'outils de sécurité, tout trouve dans le menu "Applications> Kali linux".En dehors de cela, il ya très peu de paquets. Les éléments suivants sont disponibles

Une. Navigateur - Iceweasel

2. Mysql

3. Serveur Apache

4. serveur ssh

D'autres outils de productivité tels que openoffice / libreoffice, gimpetc sont absents. Mais peut être facilement installé à partir de synaptic.

En outre, le bureau gnome de kali linux est gnome 3, mais il apparaît comme le classique bureau GNOME 2, parce que c'est une version piratée.

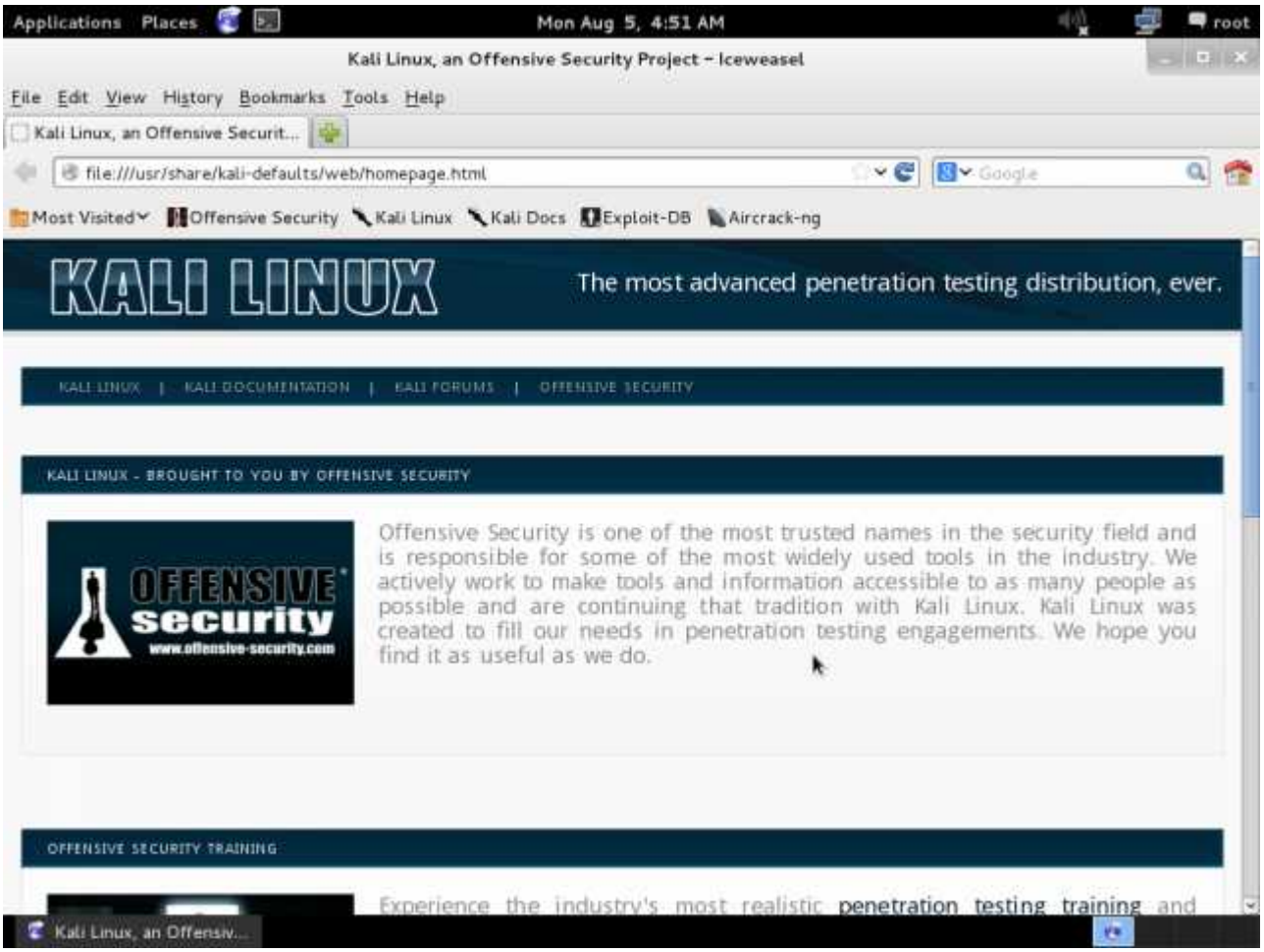

Fig.20.homepage du kali linux

Kali linux est configuré pour s'exécuter en tant que root. Même après l'installation sur le disque dur, il s'exécute en tant que root. Cela est nécessaire parce que de nombreux outils de sécurité comme Wireshark, nmap doivent fonctionner en tant que root.

Depuis kali linux est basée sur Debian, le menu de démarrage fournit des options pour un programme d'installation graphique ou basé sur du texte. Il suffit de choisir l'une et continuer. L'installateur graphique est plus facile si vous préférez.

Fig.21.l'interface du Boot du kali.

Pouvez soit vivre démarrage et l'utiliser. Ou de démarrer le programme d'installation pour l'installer. Démarrage direct est utile lorsqu'elle est utilisée avec un lecteur flash.

Pour installer il suffit de suivre les instructions à l'écran comme n'importe quelle autre distribution Linux et l'installation devrait fonctionner

parfaitement. Contrairement backtrack, bottes kali dans un gestionnaire d'affichage correct avec écran de connexion.

Kali Linux Top 10

Kali est emballé avec des centaines d'outils placés dans des catégories pertinentes, comme les tests d'applications web, l'injection SQL, l'exploitation de la mémoire tampon, la collecte d'informations, les empreintes digitales de serveur etc Cependant, il ya un menu séparé qui répertorie les 10 meilleurs outils.

Fig.22. Accès aux outils du kali.

Le menu "Applications> Kali Linux" comporte une liste séparée pour les 10 meilleurs outils de sécurité. Ce sont les outils les plus utiles, populaires et plus complet qui trouvent immense application dans divers types de tâches liées à la sécurité comme les tests de pénétration, analyse de la sécurité, les tests d'applications,

etc. La plupart de ces outils sont les meilleurs dans leurs domaines sans autre équivalent ou autre similaire.

aircrack-ng est la suite logicielle la plus populaire pour renifler le réseau sans fil et à la fissuration wep et wpa mots de passe réseau. Il est beaucoup utilisé dans le craquage de mots de passe de wifi et de voler la connectivité Internet.

Le site décrit comme.

Aircrack-ng est un WEP 802.11 et clés WPA-PSK programme qui peut récupérer les clés une fois les paquets de données suffisamment ont été capturés fissuration. Il met en œuvre l'attaque FMS standard avec quelques optimisations comme les attaques KoreK, ainsi que la toute nouvelle attaque PTW, rendant ainsi l'attaque beaucoup plus rapide par rapport à d'autres outils de craquage WEP.

En fait, Aircrack-ng est un ensemble d'outils pour l'audit des réseaux sans fil.

3. Outil de test d'applications Web - Burp Suite

Burp Suite est un outil de test d'applications Web très puissant et plus complet qui peut être utilisé pour un ping / applications web poussée / attaque dans un certain nombre de façons de découvrir les failles de sécurité comme l'injection SQL, XSS, CSRF, etc en eux. C'est un outil semi-automatique qui est très utile dans l'analyse des applications Web et de trouver des vulnérabilités.

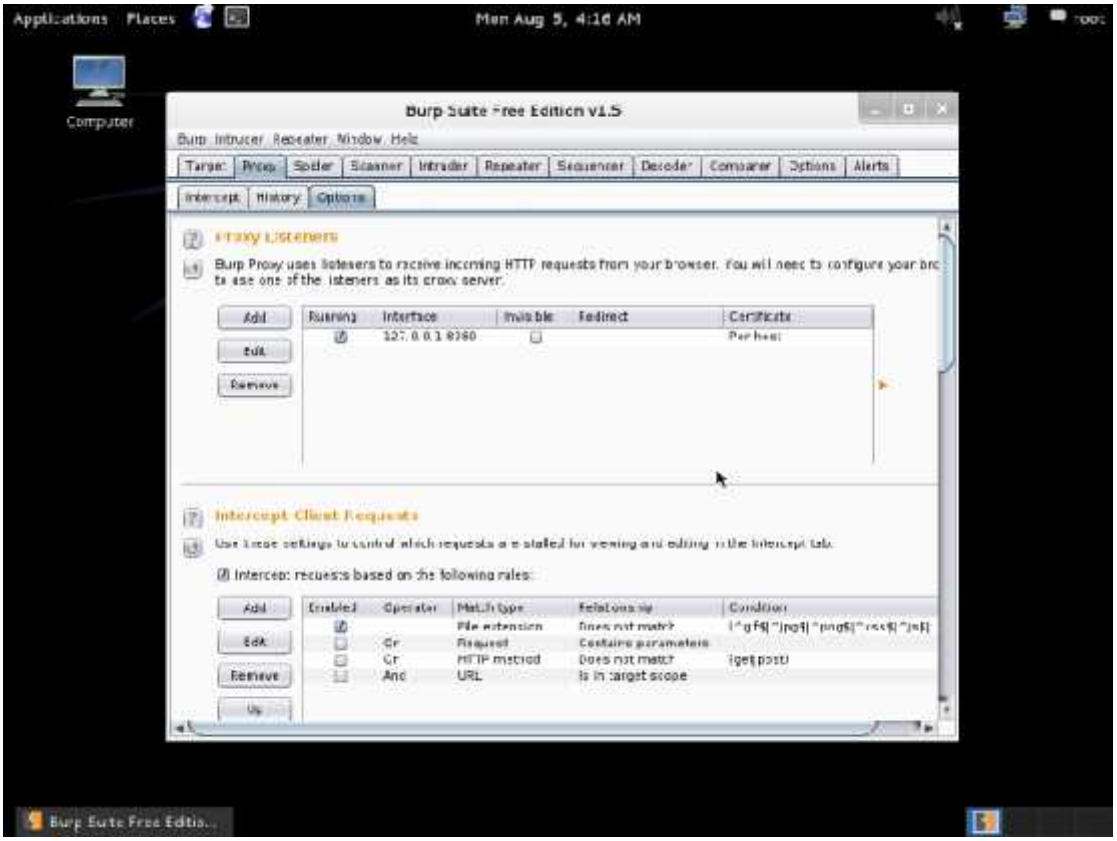

Fig.23.le Burp suite.

Écrit en Java et est multi-plateforme. Comprend des fonctionnalités telles que la modification des requêtes http, fuzzing paramètres http, spidering hôtes pour urls possibles, etc Il est livré en 2 versions, gratuite et pro. La version pro est payé et inclut des fonctionnalités puissantes telles que l'analyse automatisée des vulnérabilités, etc suite Burp a été utilisé pour trouver des vulnérabilités dans des sites comme Facebook.

Le site décrit comme

Burp Suite est une plate-forme intégrée pour la réalisation des tests de sécurité des applications Web. Ses divers outils fonctionnent parfaitement ensemble pour soutenir le processus de test, de la cartographie et l'analyse initiales de la surface d'attaque d'une application, par le biais de la recherche et de l'exploitation des failles de sécurité.

4. THC Hydra - Brute Force différents protocoles

Hydra est "Une connexion pirate de réseau très rapide qui supporte de nombreux services différents." Hydra est un outil simple brute force qui peut être utilisé pour casser le mot de passe d'un certain nombre de services comme ftp, http, vnc etc.

Les protocoles suivants sont pris en charge dans la version 7.4.2

Protocoles pris en charge: afp Cisco-permettre cvs ftp firebird FTPS http [s] - {tête | se} http [s] - {get |} après-forme http-proxy http-proxy-urlenumicqimap [s] irc LDAP2 [s] LDAP3 [- {cram | digérer} md5] [s] mssqlmysqlnntpncp oracle-auditeur PCNFS pcAnywhere oracle-sid pop3 [s] postgresrdprexecrloginrsh gorgée smbsmtp [s] smtp-énumération snmp socks5 sshsshkeysvnteamspeaktelnet [s] vmauthdvncxmpp

Utile dans de craquage de mots de passe de routeurs et autres périphériques qui sont principalement configurés avec leurs mots de passe par défaut.

Il dispose également d'une interface graphique appelée hydra-gtk/xHydra qui est également inclus dans Kali.Trouvez-le sur l'entrée de menu "Kali Linux> Mot de passe Attaque> Attaque en ligne>hydra-gtk".

4. John the Ripper - Crack les mots de passe

John the Ripper utilise des listes de mots / dictionnaire pour casser un hachage donné. Peut se fissurer beaucoup de différents types de tables de hachage dont md5, shaetc dispose d'une connexion ainsi que des listes de mots de passe payées disponible. Est multiplateforme.

John the Ripper est un cracker de mot de passe rapide, actuellement disponible pour de nombreuses saveurs d'Unix, Windows, DOS, BeOS, et OpenVMS. Son principal objectif est de détecter de faibles mots de passe Unix. Outre plusieurs

crypt(3) types de passe de hachage les plus couramment trouvés sur les différents systèmes Unix, soutenus hors de la boîte sont hashs LM de Windows, ainsi que beaucoup d'autres tables de hachage et de chiffrement dans la version améliorée de la communauté.

5. Maltego - La collecte d'informations

Fig.24.maltego.

Maltego une intelligence open source et l'application de la médecine légale. Il vous offrira minière timous et la collecte des informations ainsi que la représentation de ces informations dans un format facile à comprendre.

Maltego est essentiellement un outil de collecte d'informations, qui peut rechercher sur Internet des informations disponibles publiquement sur un site ou une organisation.

Cela aide à évaluer la quantité d'information qui a atteint le domaine public et si elle constitue une menace pour la sécurité. Par exemple, il peut chercher google, twitter et autres sources similaires pour les adresses électroniques, les noms de domaine liés à un site particulier, et même des noms et coordonnées des personnes.

L'idée de base est de trouver autant d'informations que possible sur une personne ou une organisation, à partir de sources gratuites sur Internet.

5. Metasploit - Développer, maintenir et lancer exploits

Metasploit est le grand outil de l'exploitation qui est largement utilisée dans les tests de pénétration. Metasploit est un cadre qui contribue à l'élaboration, la gestion et l'utilisation exploits. Exploits sont organisés en catégories telles que les modules individuels. Les utilisateurs peuvent ajouter leurs propres modules trop.

Écrit en Ruby et est multi-plateforme. Dispose d'une interface web et une interface graphique appelée armitage trop.

6. Scanner Port –Nmap

De facto le scanner de port de l'industrie. Nmap est un des plus anciens et l'outil de balayage de ports puissant là-bas. Bien qu'il a commencé comme un scanner de port, il est capable de faire beaucoup plus. Peut balayer les grands réseaux pour les hôtes vivants, scan de port les hôtes, obtenir les bannières de démon, obtenir des informations détaillées sur l'hôte y compris le système d'exploitation, etc.

Maintenant anmap une nouvelle fonctionnalité appelée **son nmap** qui permet aux développeurs de coder des scripts qui peuvent être utilisés avec nmap pour automatiser certains types de tâches de numérisation.

Nmap a une interface graphique appelée zenmap , qui peut être utilisé pour enregistrer les paramètres de numérisation que les profils et les utiliser plus

tard. Nmap inclut également un utilitaire de type netcat appelé NCAT qui est très featureful et est disponible pour Windows et Linux.

T Le site décrit comme

> Nmap ("Network Mapper") est un libre et open source (licence) utilitaire pour la découverte du réseau et l'audit de sécurité.
>
> De nombreux systèmes et les administrateurs réseau trouvent également utile pour des tâches telles que l'inventaire de réseau, les horaires de mise à niveau des services de gestion et de surveillance de l'hôte ou du service de disponibilité. Nmap utilise des paquets IP bruts dans de nouvelles façons de déterminer ce que les hôtes sont disponibles sur le réseau, quels services (nom de l'application et la version) ces hôtes offrent, quels systèmes d'exploitation (et les versions du système d'exploitation), ils sont en cours d'exécution, quel type de paquet filtres / pare-feu sont en cours d'utilisation, et des dizaines d'autres caractéristiques. Il a été conçu pour numériser rapidement de grands réseaux, mais fonctionne très bien contre de simples hôtes.
>
> Nmap fonctionne sur tous les principaux systèmes d'exploitation informatiques, et les paquets officiels binaires sont disponibles pour Linux, Windows et Mac OS X. En plus de la classique ligne de commande Nmap exécutable, la suite Nmap comprend une interface graphique avancée et les résultats spectateur (Zenmap), un transfert de données flexible, la redirection, et un outil de débogage (Ncat), un utilitaire pour comparer les résultats d'analyse (ndiff), et une génération de paquets et outil d'analyse de réponse (Nping).

8. OwaspZap - test des applications Web

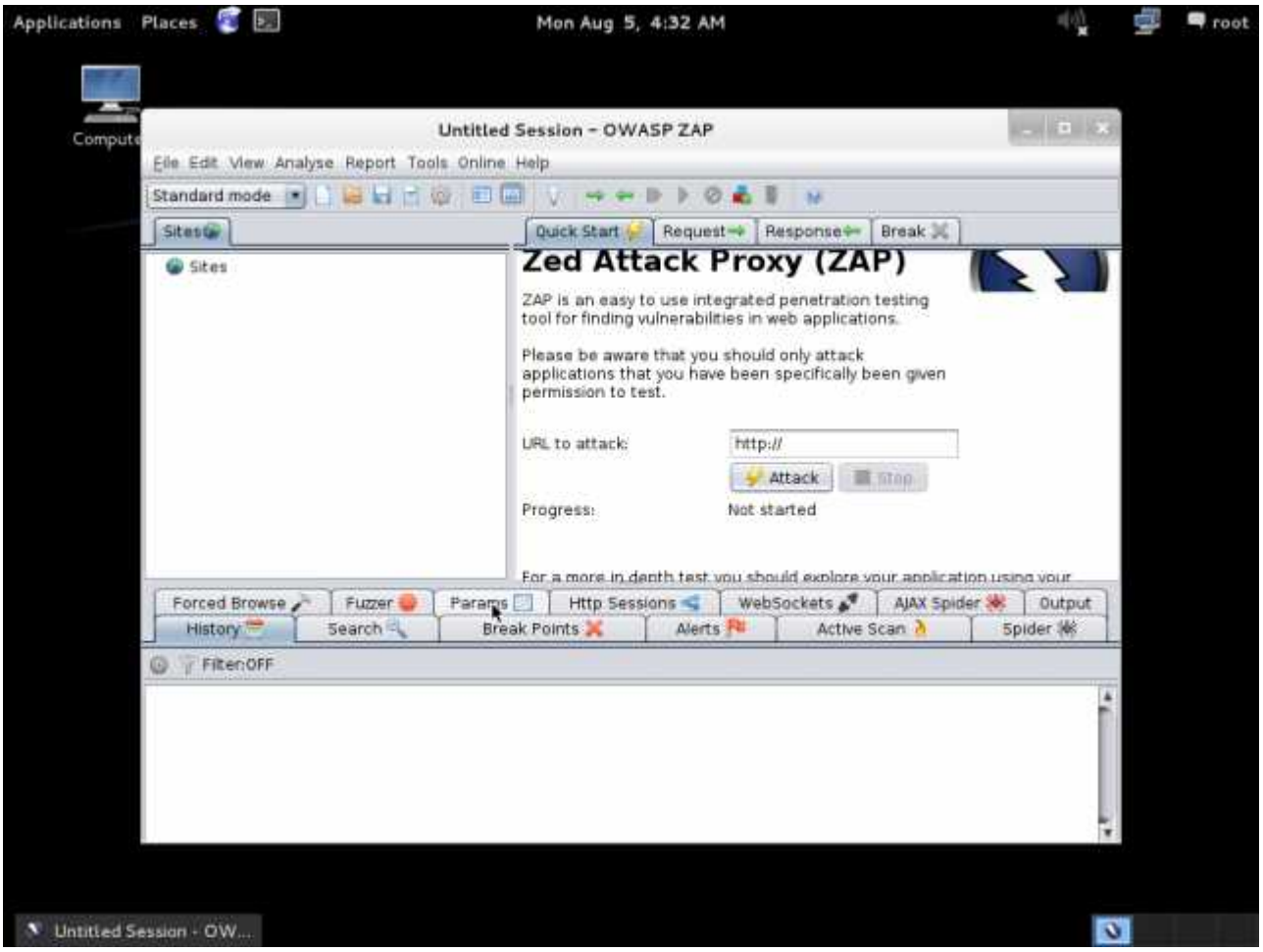

Fig.25. Zap (Attaque des applications Web).

Le Zed Attaque Proxy (ZAP) est un outil facile à utiliser de tests de pénétration intégrée pour trouver des vulnérabilités dans les applications web.

Owasp ZAP est un outil semblable à roter suite qui est utilisé pour tester des applications web. Contrairement suite rot, il est gratuit et open source et dirigée par owasp.

9. Sqlmap - sql injection automatique

Sqlmap est un outil de piratage le plus infâme du siècle qui permet à tout enfant de pirater et détruire tout site Web qui a oublié de se soustraire à ses requêtes sql correctement. C'est un outil d'exploitation entièrement automatisée des

vulnérabilités d'injection SQL. La plupart des sites étant piratés ont aujourd'hui cet outil derrière la scène.

Il met le pirate le contrôle complet de l'ensemble de la base de données d'une application web.

Sqlmap est le «Metasploit» d'injections SQL, et même mieux.

sqlmap est un outil de test de pénétration open source qui automatise le processus de détection et d'exploiter les failles de SQL injection et la prise en charge des serveurs de base de données.

Il est livré avec un puissant moteur de détection, de nombreuses fonctionnalités de niche pour le testeur de pénétration ultime et une large gamme de commutateurs d'une durée de base de données d'empreintes digitales, sur extraction de données à partir de la base de données, à l'accès au système de fichiers sous-jacent et l'exécution de commandes sur le système d'exploitation via out- les connexions de bande.

10. Wireshark - renifleur de paquets et analyseur de protocole

Wireshark est l'analyseur de réseau et analyseur de protocole le plus populaire et puissant là-bas. Disponible pour Windows et Linux. C'est une longue histoire de l'évolution et a trop de fonctionnalités. Utile dans les tests de pénétration pour analyser le réseau et de son trafic.

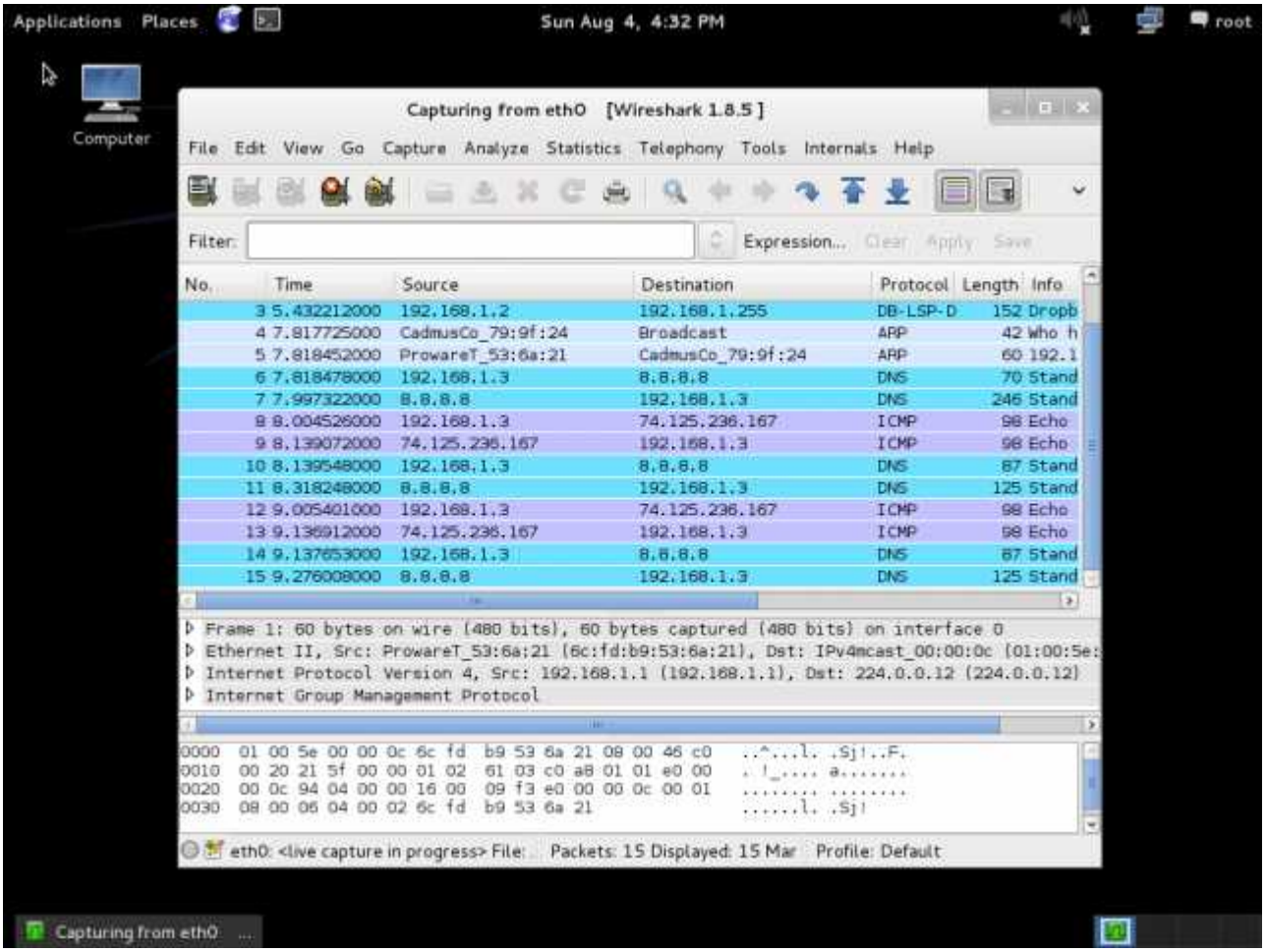

Fig.26. Wireshark.

Wireshark est avant tout analyseur de protocole réseau du monde. Il vous permet de capturer et interactive de parcourir le trafic fonctionnant sur un réseau informatique.

Il est de facto (et souvent de jure) la norme dans de nombreuses industries et les institutions éducatives.

3. Discussion

Si vous êtes fasciné par des termes tels que le piratage, les tests de pénétration et la sécurité du réseau puis vérifier Kali linux.

Peut être facilement installé à l'intérieur virtualbox comme n'importe quel distro basée sur Debian.

Conclusion

Le proverbe dit « mieux vaut prévenir que guérir » : au terme du parcours desdivers aspects de la sécurité des systèmes d'information, nous pourrions presquedire qu'en ce domaine prévenir est impératif, parce que guérir est impossible et detoute façon ne sert à rien.

Lorsqu'un accident ou un pirate a détruit les données del'entreprise et que celle-ci n'a ni sauvegarde ni site de secours, elle est condamnée,tout simplement : les personnels de ses usines ne savent plus quoi produire ni àquels clients livrer quoi, ses comptables ne peuvent plus encaisser les factures nipayer personnels et débiteurs, ses commerciaux n'ont plus de fichier de prospects.

Un accident moins grave aura sans doute des conséquences moins radicales, maisen règle générale les conséquences d'un incident de sécurité sont irréversibles siaucune prévention n'avait été organisée avant qu'il n'advienne.

Il est impossible de connaître à l'avance tous les types de menaces et de détectertoutes les vulnérabilités, puisque, ainsi que nous l'avons signalé et répété, il enapparaît de nouvelles chaque semaine, par dizaines. Par conséquent, l'analyse derisques se révèle vite une aporie si on lui accorde trop de confiance, si on la croitdéterministe ; il convient de s'y adonner, mais avec scepticisme.

L'analyste de risques sceptique sera un responsable de sécurité agnostique et pessimiste: il sait que son pare-feu sera franchi, que son antivirus ne sera pas à jour,que son système de détection d'intrusion ne le préviendra pas de l'attaque, queses copies de sauvegarde seront corrompues, que son site de secours sera inondéou détruit par un incendie, que son système redondant ne se déclenchera pasmais, éduqué dans la religion probabiliste, il sait que toutes ces catastrophes nesurviendront pas simultanément.

L'idée de défense en profondeur n'est pas sans parenté avec la démarche agnostiqueprobabiliste, mais elle s'en distingue : si la garnison de mon pare-feu est

finalementsubmergée par l’assaillant, elle en aura néanmoins réduit les effectifs avantde succomber, ce qui facilitera la mission des escadrons d’antivirus, et ainsi monsystème redondant risquera moins d’être saboté par un ver qui pourrait l’empêcherde se déclencher. Si au contraire je mise tout sur mon pare-feu ou sur mon réseauprivé virtuel et que derrière cette protection je commets des imprudences, je succombeau syndrome de la ligneMaginot, le jour où la défense est enfoncée tout estperdu.

Or, si une chose est sûre, c’est que la défense sera enfoncée.

Un jour Une autre certitude, c’est que le risque ne vient pas seulement de l’extérieur, lessources de danger prolifèrent aussi à l’intérieur du réseau, et d’ailleurs la frontièreentre l’intérieur et l’extérieur tend non pas à disparaître, mais à devenir poreuse etfloue, avec les systèmes mobiles en tout genre qui entrent et qui sortent, les tunnelsvers d’autres réseaux, les nouveaux protocoles infiltrables et furtifs. Les protocolesde téléphonie par Internet, de visioconférence et autres systèmes multimédia sonttous des failles béantes de sécurité, et la situation sur ce front ne s’améliorera pasavant des années.

Nous voyons que les menaces sont protéiformes, les vulnérabilités foisonnantes etle tout en transformation constante : c’est dire que le responsable de sécurité nechoisit pas le terrain sur lequel il va devoir manoeuvrer, il va lui falloir faire preuved’adaptabilité et de pragmatisme.

S’il ne veut pas se trouver condamné à réagir frénétiquementmais trop tard à des avalanches d’incidents mystérieux, il devra néanmoinsétablir un socle stable pour son activité, dont nous avons établi en principequ’elle sera essentiellement préventive. Pour cela il lui faudra principalement deuxchoses : une vraie compétence technique dans son domaine, suffisamment largeet profonde pour embrasser réseaux et systèmes, et, au sein de son entreprise, lepouvoir d’édicter les règles dans son domaine, et de les faire respecter : interdireles protocoles dangereux, imposer la mise à jour automatique des antivirus, mettreson veto à tel ou tel passe-droit dans le pare-feu.

Cela s’appelle une politique dne manque pas de méthodes qui laissent croire que la sécurité des systèmesd’information pourrait être assurée par des routines administratives : nous avonssignalé et expliqué leur vanité à la fin du premier chapitre de ce livre. Nous dironsque ces méthodes de sécurité sont procédurales, ou, plus crûment, qu’elles sontbureaucratiques.

Nous avons donc le choix entre ces méthodes bureaucratiques et celles que nousappellerons méthodes de sécurité négative, parce qu’elles proposent de colmaterles failles dès que celles-ci sont découvertes et d’interdire les malfaisances aprèsqu’elles se sont manifestées : ni celles-là ni celles-ci ne sont satisfaisantes, nousl’avons vu.

Nous préconiserons plutôt celles qui visent ce que nous appellerons lasécurité positive, parce qu’elles posent a priori ce qui est sûr, et qu’elles établissentla sécurité à la conception des systèmes, par la définition de ce qu’ils doivent faireet l’interdiction du reste selon une règle que nous énoncerons ainsi : « n’est permisque ce qui est explicitement permis, tout le reste est interdit ».

Par exemple, à l’heure où pratiquement toutes les applications informatiques sontfondées sur les techniques du Web, nous pensons, en suivant Marcus J. Ranum,qu’un outil de choix pour la sécurité positive est le mandataire applicatif (reverseproxy) : il s’agit d’un serveur Web spécialisé, qui reçoit les messages du protocoleHTTP, les filtre, rejette ce qui n’est pas autorisé et réécrit les requêtes avant de lestransmettre au « vrai » serveur, ce qui élimine tout imprévu, et notamment touteune famille d’attaques par injection de code.

Cette méthode revient à écrire sapropre version du protocole, adaptée exactement à ce que l’on veut faire.

De façon générale, l’évolution de l’informatique, de ses usages, et par conséquentdes systèmes d’information, est déterminée par l’offre de technologie plus quepar les demandes des utilisateurs, parce que celle-là évolue plus vite que celles-ci.

Pour des raisons évidentes, c’est encore plus vrai pour les questions de sécurité,parce que les utilisateurs ne « demandent » rien, et que l’« offre » est par définitiondestinée à surprendre ses « clients » par des attaques auxquelles ils ne s’attendentpas.

La lutte contre cette « offre » un peu spéciale ne peut donc reposer sur lesattentes du client, et la veille technologique « tous azimuts », si elle est nécessaire,ne saurait prétendre à l’efficacité totale. Ce qui renforce l’argument pour la sécurite.

Annexes

Les vulnérabilités

Tous les systèmes informatiques sont vulnérables. Peu importe le niveau de vulnérabilité de ceux ci. Une vulnérabilité est une faille ou une faiblesse pouvant être exploitée par une personne mal intentionnée pour nuire.

Les vulnérabilités des systèmes peuvent être classées en catégorie (humaine, technologique, organisationnelle, mise en œuvre).

a) Vulnérabilités humaines :

L'être humain de par sa nature est vulnérable.

La plupart des vulnérabilités humaines proviennent des erreurs (négligence, manque de compétences, surexploitation, etc.), car ne dit t-on pas souvent que l'erreur est humaine? Un SI étant composé des humains, il convient d'assurer leur sécurité si l'on veut garantir un maximum de sécurité dans le SI.

b) Vulnérabilités technologiques :

Avec la progression exponentielle des outils informatiques, les vulnérabilités technologiques sont découvertes tous les jours.

Ces vulnérabilités sont à la base dues à une négligence humaine lors de la conception et la réalisation. Pour être informé régulièrement des vulnérabilités technologiques découvertes, il suffit de s'inscrire sur une liste ou des listes de diffusion mises en place par les CERT(Computer Emergency Readiness ou Response Team).

c) Vulnérabilités organisationnelles :

Les vulnérabilités d'ordre organisationnel sont dues à l'absence des documents cadres et formels, des procédures (de travail, de validation) suffisamment détaillées pour faire face aux problèmes de sécurité du système.

Quand bien même ces documents et procédures existent, leur vérification et mises à jour ne sont pas toujours bien assurées.

d) Vulnérabilités mise en œuvre :

Les vulnérabilités au niveau mise en œuvre peuvent être dues à la non prise en compte des certains aspects lors de la réalisation d'un projet.

3 Menaces

On peut également classer les menaces en deux catégories selon qu'elles ne changent rien (menaces passives) ou qu'elles perturbent effectivement le réseau (menaces actives).

a) Les menaces passives :

consistent essentiellement à copier ou à écouterl'information sur le réseau, elles nuisent à la confidentialité des données.

Dans ce cas, celui qui prélève une copie n'altère pas l'information elle-même.

b) Les menaces actives : sont de nature à modifier l'état du réseau.

4 Risques

Les risques se mesurent en fonction de deux critères principaux : la vulnérabilité et la sensibilité.

La vulnérabilité désigne le degré d'exposition à des dangers.

Un des points de vulnérabilité d'un réseau est un point facile à approcher.

Un élément de ce réseau peut être très vulnérable tout en présentant un niveau de sensibilité très faible : le poste de travail de l'administrateur du réseau, par exemple, dans la mesure où celui-ci peut se connecter au système d'administration en tout point du réseau.

La sensibilité désigne le caractère stratégique d'un composant du réseau. Celui-ci peut être très sensible, vu son caractère stratégique mais quasi

invulnérable, grâce à toutes les mesures de protection qui ont été prises pour le prémunir contre la plupart des risques.

Les logiciels malveillants :

Un logiciel malveillant est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur infecté. Plusieurs types de logiciels malveillants ont été proposées nous citons les plus répandus :

1 Virus :

Un virus est un morceau de programme informatique malicieux, conçu et écrit pour qu'il se reproduise.

Cette capacité à se répliquer, peut toucher votre ordinateur, sans votre permission et sans que vous le sachiez. En termes plus techniques, le virus classique s'attachera à un de vos programmes exécutables et se copiera systématiquement sur tout autre exécutable que vous lancez.

Les virus peuvent s'avérer particulièrement dangereux et endommager plus ou moins gravement les machines infectées. Le virus peut se répandre à travers tout moyen d'échange de données numériques comme l'Internet, et notamment par l'intermédiaire des messages électroniques ou de leurs pièces attachées.

2. Vers :

Un ver (ou worm) est un type de virus particulier qui se propage par le réseau.

Le vers contrairement aux virus, une fois implantés et activés dans un ordinateur, sont des programmes capables de se propager d'un ordinateur à un autre via le réseau, sans intervention de l'utilisateur et sans exploiter le partage de fichiers.

3. Cheval de Troie :

Un cheval de Troie (Trojan horse) est un programme qui exécute des instructions sans l'autorisation de l'utilisateur. Ces instructions sont généralement nuisibles à l'utilisateur, et qui une fois installé sur un ordinateur y effectue des actions cachées et pernicieuses.

Le cheval de Troie contrairement au ver ne se réplique pas.

4 Logiciel Espion :

Un logiciel espion (ou spyware) est un programme, conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur, ou à un tiers via Internet ou tout autre réseau informatique, sans avoir obtenu au préalable une autorisation explicite et éclairée desdits utilisateurs.

Une variété particulièrement toxique de logiciel espion est le keylogger (espion dactylographique), qui enregistre fidèlement tout ce que l'utilisateur tape sur son clavier et le transmet à son honorable correspondant ; il capte ainsi notamment identifiants, mots de passe et codes secrets.

5 Spam :

Le spam est une vraie problématique. Il encombre les résultats de recherche ce qui gène l'utilisateur.

Un spam peut être définit comme étant un email anonyme, non sollicité, indésirable et envoyé en grand nombre de façon automatique sans l'accord de son destinataire.

6 Cookies :

Un cookie est un petit fichier très simple, en fait un texte, enregistré sur le disque dur de l'ordinateur d'un internaute à la demande du serveur gérant le site Web visité.

Il contient des informations sur la navigation effectuée sur les pages de ce site. L'idée originelle est de faciliter l'utilisation ultérieure du site par la même personne.

Un cookie n'étant pas exécutable, il ne peut contenir de virus.

7 Bombe logique :

Une Bombe logique est une partie d'un programme malveillant (virus, cheval de Troie, etc.) qui reste dormante dans le système hôte jusqu'à ce qu'un instant ou un événement survienne, ou encore que certaines conditions soient réunies, pour déclencher des effets dévastateurs en son sein.

Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise.

8 Porte dérobée :

C'est un moyen de contourner les mécanismes de contrôle d'accès.

Elle s'agit d'une faille du système de sécurité due à une faute de conception accidentelle ou intentionnelle.

Bibliographies:

[1] « MIT researchers uncover mountains of private data on discarded computers ». Massachusetts Institute of Technology, News Office, 15 janvier 2003. http://web. mit.edu/newsoffice/2003/diskdrives.html .

[2] « Site de l'Adullact ». Association des développeurs et des utilisateurs de logiciels libres pour l'administration et les collectivités territoriales, 2005. http://www.adullact. org/documents/comparatif_licences.html .

[3] « Site de l'OSSIR ». Observatoire de la sécurité des systèmes d'information et des réseaux,

2005. Cette association est aujourd'hui le meilleur cénacle francophone dans son domaine. http://www.ossir.org .

[4] « Site du journal MISC ». MISC, 2005. Revue francophone de sécurité informa- tique. http://www.miscmag.com .

[5] « Sécurité de Perl ». Site Perl de l'ENSTIMAC, 23 mars 2006. http://perl. enstimac.fr/DocFr/perlsec.html .

[6] Jean-François Abramatic. « Croissance et évolution de l'Internet ». Dans Université de tous les savoirs – Les Technologies, volume 7, Paris, 2002. Odile Jacob.

[7] Jean-Raymond Abrial. The B Book - Assigning Programs to Meanings. Cambridge University Press, Cambridge, 1996.

[8] Pascal Aubry, Julien Marchal, et Vincent Mathieu. « Single Sign-On Open Source avec CAS ». 2003. http://2003.jres.org/actes/paper.139.pdf .

[9] Autorité de régulation des communications électroniques et des postes (ARCEP). « Le cadre réglementaire des réseaux RLAN / Wi-Fi depuis le 25 juillet 2003 », 8 août 2003. http://www.art-telecom.fr/dossiers/rlan/schema-rlan. htm .

[10] Gildas Avoine, Pascal Junod, et Philippe Oechslin. Sécurité informatique – Exercices corrigés. Vuibert, Paris, 2004. Préface de Robert Longeon.248

Sécurité Informatique

[11] Daniel Azuelos. « Architecture des réseaux sans fil ». Dans JRES, editor, Actes du congrès JRES, 2005. http://2005.jres.org/tutoriel/Reseaux_sans_fil.
livre.pdf .

[12] Général de Brigade Bailey, MBE. « Le combat dans la profondeur 1914-1941 : la naissance d'un style de guerre moderne ». Les cahiers du Retex, (15), 17 mars 2005. http://www.cdef.terre.defense.gouv.fr//publications/
cahiers_drex/cahier_retex/retex15.pdf .

[13] Scott Barman. Writing Information Security Policies. New Riders, Indianapolis, USA, 2002.

[14] Salman A. Baset et Henning Schulzrinne. « An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol ». arXiv.org, 15 septembre 2004. http://arxiv.
org/ftp/cs/papers/0412/0412017.pdf .

[15] Didier Bert, Henri Habrias, et Véronique ViguiéDonzeau-Gouge (éd.). « Méthode B (numéro spécial) ». Technique et science informatique, 22, 1/2003.

[16] Philippe Biondi et Fabrice Desclaux. « Silver Needle in the Skype ».BlackHat Europe, 2-3 mars 2006. http://www.secdev.org/conf/skype_BHEU06.pdf .

[17] Laurent Bloch. Les systèmes d'exploitation des ordinateurs – Histoire, fonctionnement, enjeux. Vuibert, Paris, 2003. Texte intégral disponible ici : http://www.
laurent-bloch.org/article.php3?id_article=13 .

[18] Laurent Bloch. Systèmes de fichiers en réseau : NFS, SANs et NAS. 2005. Texte disponible ici : http://www.laurent-bloch.org/Livre-Systeme/livre008.
html .

[19] Laurent Bloch. Systèmes d'information, obstacles et succès – La pensée aux prises avec l'informatique. Vuibert, Paris, 2005. Extraits et documents complémentaires disponibles ici : http://www.laurent-bloch.org/rubrique.php3?id_
rubrique=5 .

[20] Laurent Bloch. « Théorie et pratique de la commande publique ». 2005. http:

//www.laurent-bloch.org/SI-Projets-extraits/livre005.html .

[21] Frédéric Bonnaud. « Signer et chiffrer avec GnuPG ». Lea-Linux.org, 2005.http: //lea-linux.org/cached/index/Reseau-secu-gpg-intro.html .

[22] Isabelle Boydens. Informatique, normes et temps. Bruylant, Bruxelles, 1999.

[23] Philippe Breton. La tribu informatique – Enquête sur une passion moderne. Métailié, Paris, 1991.

[24] Christophe Brocas et Jean-Michel Farin. « De la sécurité d'une architecture DNS d'entreprise ». MISC, (23), Janvier-février 2006.

[25] Antoine Brugidou et Gilles Kahn. « Étude des solutions de filtrage des échanges de musique sur Internet dans le domaine du peer-to-peer », 9 mars 2005. http: //www.recherche.gouv.fr/discours/2005/musiqueinternet.htm .

[26] Franck Cappello. « P2P : Développements récents et perspectives ». Dans 6 e jour-249 Bibliographie

nées réseau JRES, 2005. En ligne ici : http://2005.jres.org/slides/152.

pdf .

[27] Centre d'Expertise de Réponse et de Traitement des Attaques informatiques (Cert-RENATER). « Site du Cert-RENATER », 10 septembre 2006. http://www.

renater.fr/rubrique.php3?id_rubrique=19 .

[28] Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA). « Site du CERTA », 10 septembre 2006. http://www.

certa.ssi.gouv.fr/ .

[29] Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA). « Sécurité des réseaux sans fil (Wi-Fi) », 26 octobre 2004.

http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002/ .

[30] D. Brent Chapman et Elizabeth D. Zwicky. Firewalls – La sécurité sur l'Internet.

O'Reilly, Sebastopol, Californie (Paris pour la traduction), 1995. Traduction de

Jean Zundel.

[31] Société ClearSy. « Atelier B ». juin 2004. http://www.atelierb.societe.com/ .

[32] Commission Nationale Informatique et Libertés. « Norme simplifiée n o 46 », 13 janvier 2005. http://www.cnil.fr/index.php?id=1231 .

[33] Computer Emergency Response Team - Coordination center. « Site du Cert-CC », 10 septembre 2006. http://www.cert.org/ .

[34] Computer Emergency Response Team - Industrie, Services et Tertiaire (Cert-IST). « Site du Cert-IST », 10 septembre 2006. http://www.cert-ist.com/ .

[35] Thomas Cormen, Charles Leiserson, Ronald Rivest, et Clifford Stein. Introduction à l'algorithmique. Dunod (pour la traduction française), Paris, 2002. Une somme d'une complétude impressionnante ; si les exposés mathématiques des algorithmes sont d'une grande clarté, le passage à la programmation (en pseudo-code) est souventdifficile.

[36] Alan Cox et EddDumbill. « The Next 50 Years of Computer Security : An Interview with Alan Cox ». O'Reilly Network, 12 septembre 2005. http://www.oreillynet.com/pub/a/network/2005/09/12/alan-cox.html .

[37] CROCUS (collectif). Systèmes d'exploitation des ordinateurs. Dunod, Paris, 1975. Ce manuel, quoique assez ancien, conserve un intérêt certain par sa rigueur dans l'introduction des concepts et du vocabulaire, et en a acquis un nouveau, de caractère historique, par la description de systèmes aujourd'hui disparus.

[38] Cunningham et Cunningham. « Cee Language and Buffer Overflows ».Cunningham and Cunningham, Inc., 16 août 2005. http://c2.com/cgi/wiki?CeeLanguageAndBufferOverflows .

[39] FabriceDesclaux. « Skype uncovered – Security study of Skype ». OSSIR – Groupe sécurité Windows, 7 novembre 2005. http://www.ossir.org/windows/250 Sécurité Informatique supports/2005/2005-11-07/EADS-CCR_Fabrice_Skype.pdf .

[40] WhitfieldDiffie et Martin E. Hellman. « New Directions in Cryptography ». IEEE Transactions on Information Theory, vol. IT-22, nov. 1976. http://citeseer.ist.psu.edu/340126.html .

[41] EdsgerWybeDijkstra. « The structure of the THE multiprogramming system ». Communications of the ACM (CACM), vol. 11 n o 5, mai 1968. http://www.acm.org/classics/mar96/ .

[42] Direction centrale de la sécurité des systèmes d'information. « Expression des Besoins et Identification des Objectifs de Sécurité », 2003. http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html .

[43] Gilles Dubertret. Initiation à la cryptographie. Vuibert, Paris, 2002.

[44] Albert Ducrocq et André Warusfel. Les mathématiques – Plaisir et nécessité. Vuibert, Paris, 2000. Plaidoyer pour une discipline malmenée, au moyen de nombreux exemples historiques et modernes auxquels l'érudition des auteurs et leur talent de vulgarisateurs confèrent un rythme trépidant et passionnant.

[45] Jean-Pierre Dupuy. Pour un catastrophisme éclairé – Quand l'impossible est certain. Éditions du Seuil, Paris, 2002.

[46] KjeldBorchEgevang et Paul Francis. « RFC 1631 – The IP Network Address Translator (NAT) », mai 1994. http://www.ietf.org/rfc/rfc1631.txt .

[47] Carl Ellison et Bruce Schneier. « Ten Risks of PKI : What You're Not Being Told About Public Key Infrastructure ».Computer Security Journal, vol. 16, n o 1, 2000. http://www.schneier.com/paper-pki.html .

[48] David Evans. « What Biology Can (and Can't) Teach Us About Security ». USENIX Security Symposium, 12 août 2004. http://www.cs.virginia.edu/~evans/usenix04/usenix.pdf .

[49] Edward W. Felten. « DRM and Public Policy ». Communications of the ACM (CACM), (vol. 48, n o 7), juillet 2005. http://www.csl.sri.com/users/neumann/insiderisks05.html#181 .

[50] Richard P. Feynman. « Personal observations on the reliability of the Shuttle ». 1986. http://science.ksc.nasa.gov/shuttle/missions/51-l/docs/rogers-commission/Appendix-F.txt .

[51] Éric Filiol. Les virus informatiques : théorie, pratique et applications. Collection IRIS. Springer Verlag, Paris, 2003.

[52] Éric Filiol. « Le danger des virus blindés ». La lettre – Techniques de l'ingénieur – Sécurité des systèmes d'information, (6), novembre-décembre 2005.

[53] Éric Filiol. « Évaluation des logiciels antiviraux : quand le marketing s'oppose à la technique ». MISC, (21), octobre 2005. Dans un excellent numéro consacré aux Limites de la sécurité.

[54] Nicolas Fischbach. « Sécurité de la VoIP chez un opérateur ». 2006. http://www.251 Bibliographie ossir.org/jssi/jssi2006/supports/1B.pdf .

[55] Gustave Flaubert. Bouvard et Pécuchet. Le Seuil, Paris, 1857. Comme il s'agit, en fin de compte, d'un livre sur la bêtise, sa lecture sera utile à quiconque se préoccupe de sécurité, puisque souvent les failles de sécurité ne sont pas sans lien avec la bêtise.

[56] Laurence Freyt-Caffin. « L'administrateur réseau, un voltigeur sans filet ». Dans 5 e journées réseau JRES, 2003. En ligne ici : http://2003.jres.org/actes/paper.130.pdf .

[57] Simson Garfinkel. PGP – Pretty Good Privacy.O'Reilly, Sebastopol, Californie (Paris), 1995. Traduction de Nat Makarévitch.

[58] Simson L. Garfinkel. « VoIP and Skype Security ». Tactical Technology Collective, 12 mars 2005. http://www.tacticaltech.org/skype_security .

[59] SolveigGodeluck. La géopolitique d'Internet. La Découverte, Paris, 2002. 247 pages.

[60] Katie Hafner et Matthew Lyon. Where Wizards Stay Up Late – The Origins of the Internet. Pocket Books, Londres, 1996.

[61] John L. Hennessy et David A. Patterson. Computer Architecture : a Quantitative Approach. Morgan Kaufman Publishers (Vuibert pour la traduction française), San Mateo, Calif., USA, 1996-2001. Ce livre donne à la description de l'architecture des ordinateurs une ampleur intellectuelle que peu soupçonnaient. En annexe, une bonne introduction à la représentation des nombres (norme IEEE 754 notamment). La traduction française est recommandable.

[62] Andrew Hodges. Alan Turing : the Enigma (Alan Turing : l'Énigme de l'intelligence). Simon and Schuster (Payot, Paris pour la traduction), New-York, USA, 1983.

[63] Michael Howard et David LeBlanc. Écrire du code sécurisé. Microsoft, Redmond, USA, 2003. Traduction de Marc Israël.

[64] G. Dan Hutcheson. « The World Has Changed ». VLSI Research, 13 avril 2005. https://www.vlsiresearch.com/public/600203v1.0.pdf .

[65] ISO/IEC. « Information technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM R
) ». Norme internationale n o 21827, 2002.

[66] ISO/IEC. « Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental ». Norme internationale n o 19011, 2002.

[67] ISO/IEC. « Common Criteria for Information Technology Security Evaluation ». Norme internationale n o 15408, 2005.

[68] ISO/IEC. « Information Security Management Systems – Requirements ».Norme internationale n o 27001, 2005.

[69] ISO/IEC. « Information technology. Code of practice for information security management ». Norme internationale n o 17799, 2005.

[70] KevinKrewell. « A Look Ahead To 2006 ».Microprocessor Report, vol. 20 n o 1,252 Sécurité Informatique
janvier 2006. La revue mensuelle avec édition hebdomadaire sur le Web : http:// www.mpronline.com/mpr/index.html du microprocesseur et de ses évolutions

techniques et industrielles. Informée, compétente, beaucoup de détail technique exposé avec clarté.

[71] Benjamin A. Kuperman, Carla E. Brodley, Hilmi Ozdoganoglu, T.N. Vijaykumar, etAnkitJalote. « Detection and Prevention of Stack Buffer Overflow Attacks ». Communications of the ACM (CACM), vol. 48 n o 11, novembre 2005.

[72] Sophie Le Pallec. « La convergence des identifiants numériques ». Dans Actes du congrès JRES, 2005. http://www.jres.org/paper/70.pdf .

[73] Legalis.net. « Legalis.net ».2 août 2006. http://www.legalis.net .

[74] LawrenceLessig. The future of ideas – The fate of the commons in a connected world. Random House, New York, 2001. 352 pages.

[75] Steven Levy. Hackers : Heroes of the Computer Revolution. Doubleday, USA, 1984.

[76] Cédric Llorens, Laurent Levier, et Denis Valois. Tableaux de bord de la sécurité réseau. Eyrolles, Paris, 2006.

[77] Robert Longeon et Jean-Luc Archimbaud. Guide de la sécurité des systèmes d'information – à l'usage des directeurs. Centre National de la Recherche Scientifique (CNRS), Paris, 1999.

[78] Michael W. Lucas. PGP & GPG - Assurer la confidentialité de ses e-mails et de ses fichiers. Eyrolles (traduit par Daniel Garance), Paris, 2006.

[79] Alfred J. Menezes, Paul C. van Oorschot, et Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, Boca Raton, Floride, États-Unis, 1997. Une introduction complète au sujet, disponible en consultation sur le Web : http: //www.cacr.math.uwaterloo.ca/hac/ .

[80] Multicians. « Multics », 10 septembre 2006. http://www.multicians.org/ .

[81] Stéphane Natkin. Les protocoles de Sécurité d'Internet. Dunod, Paris, 2002.

[82] Stephen Northcutt et Judy Novak. Détection d'intrusion de réseau. Vuibert, Paris, 2002 (2004 pour la traduction). Traduction de Raymond Debonne.

[83] Michael J. O'Donnell. « Separate Handles from Names on the Internet ». Com-

munications of the ACM, vol. 48, n o 12, pp. 79-83, décembre 2005.

[84] Loïc Pasquiet. « Déploiement d'une solution de téléphonie sur IP dans un campus ». 2006. http://www.ossir.org/jssi/jssi2006/supports/2A.pdf .

[85] Jacky Pierson et Robert Longeon. « La biométrie (suite) ». Sécurité Informatique, avril 2004. Suite de l'article du bulletin de sécurité informatique du CNRS qui expose clairement les limites de la biométrie : http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/num48.pdf .

[86] W. Curtis Preston. SANs and NAS.O'Reilly, Sebastopol, California, 2002.

[87] Christian Queinnec. « le Filtrage : une application de (et pour) Lisp ». 1995. http://www-spi.lip6.fr/~queinnec/Books/LeFiltrage.ps.gz .253

Bibliographie

[88] Marcus J. Ranum. « The Six Dumbest Ideas in Computer Security ».http://www.certifiedsecuritypro.com/, 1er septembre 2005. http://www.ranum.com/security/computer_security/editorials/dumb/ .

[89] Marcus J. Ranum. « What is Deep Inspection ? ». Site de Marcus J. Ranum, 6 mai 2005. http://www.ranum.com/security/computer_security/editorials/deepinspect/ .

[90] YakovRekhter, Robert G. Moskowitz, Daniel Karrenberg, Geert Jan de Groot, et Eliot Lear. « RFC 1918 – Address Allocation for PrivateInternets) », février 1996. Cette RFC remplace les 1597 et 1627 de 1994 ; http://www.ietf.org/rfc/rfc1918.txt .

[91] RonaldRivest, Adi Shamir, et Leonard Adleman. « A Method for Obtaining Digital Signatures and Public-Key Cryptosystems ». CACM, 21(2), février 1978. L'article fondateur, accessible en ligne ici : http://theory.lcs.mit.edu/~rivest/rsapaper.pdf .

[92] Mark E. Russinovich. Windows Internals : Windows 2000, Windows XP & Windows Server 2003.Microsoft Press, Redmond, État de Washington, 2005.

[93] Mark E. Russinovich. « Sony, Rootkits and Digital Rights Management Gone Too Far ».Sysinternals, octobre 2005. http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html .

[94] Alfred Rényi. Calcul des probabilités. Jacques Gabay [pour la traduction], Budapest [Paris], 1966. Ce livre qui a fait date dans son domaine contient un exposé particulièrement incisif et élégant de l'algèbre de Boole.

[95] Emmanuel Saint-James. La Programmation applicative (de Lisp à la machine en passant par le λ-calcul). Hermès, Paris, 1993. Avec une préface de Jacques Arsac. Une étude riche et originale avec des aperçus saisissants sur la programmation.

[96] OlivierSalaün. « Introduction aux architectures Web de Single-Sign On ». 2003. http://2003.jres.org/actes/paper.116.pdf .

[97] Cliff Saran. « BP turns its back on traditional IT security with Internet access to company systems ». Computer Weekly, 3 septembre 2004.

[98] Hervé Schauer. « Site d'Hervé Schauer Consultants ». Hervé Schauer Consultants, 16 octobre 2005. http://www.hsc.fr/index.html.fr .

[99] Hervé Schauer. « VoIP et sécurité – Retour d'expérience d'audits de sécurité ». 2006. http://www.hsc.fr/ressources/presentations/tenor06-voip-sec/ .

[100] Bruce Schneier. Secrets et mensonges – Sécurité numérique dans un monde en réseau.

John Wiley& Sons (Vuibert pour la traduction française), New York (Paris), 2000 (2001). Traduction de Gabriel Otman et Jean-Jacques Quisquater.

[101] Security Focus. « Site de Security Focus ». Security Focus, 16 octobre 2005.http://www.securityfocus.org/ .254

Sécurité Informatique

[102] AviSilberschatz, Peter Galvin, et Greg Gagne. Principes appliqués des systèmes d'exploitation. Vuibert (pour la traduction française), Paris, 2001.

[103] Simon Singh. The Code Book (Histoire des codes secrets). J.-C. Lattès (pour la tra-

duction française), Paris, 1999. Un ouvrage de vulgarisation passionnant.

[104] Sophos. « Rapport Sophos 2005 sur la gestion des menaces à la sécurité », 2005.

[105] Pyda Srisuresh et Kjeld Borch Egevang. « RFC 3022 – Traditional IP Network Address Translator (Traditional NAT) », janvier 2001. http://www.ietf.org/rfc/rfc3022.txt .

[106] Richard M. Stallman. « Pouvez-vous faire confiance à votre ordinateur ? ». Logiciel libre, société libre : articles choisis de Richard M. Stallman, 2002. http://www.gnu.org/philosophy/can-you-trust.fr.html .

[107] Michael Szydlo. « SHA-1 Collisions can be Found in 2 63 Operations ». RSA Laboratories, 19 août 2005. http://www.rsasecurity.com/rsalabs/node.asp?id=2927 .

[108] Andrew S. Tanenbaum. Réseaux. Pearson Education (pour la traduction française), Paris, 2003.

[109] Robert Bruce Thompson et Barbara Fritchman Thompson. PC Hardware in a Nutshell. O'Reilly, Sebastopol, Calif., USA, 2003. Un ouvrage pratique indispensable. Vous comprendrez rétrospectivement la cause de tous vos ennuis avec la gravure de CD-Roms, la géométrie des disques durs... ou la sécurité.

[110] Isabelle N. Tisserand. Hacking à cœur – Les enfants du numérique. Éditions e/dite, Paris, 2002.

[111] Roland Topor. Le sacré livre de Prouto. Syros, Paris, 1990.

[112] Vernor Vinge. True Names. Tor Books, USA, 1981.

[113] Michel Volle. « Histoire d'un tableau de bord ». 20 novembre 2002. http://www.volle.com/travaux/tdb.htm .

[114] Michel Volle. e-conomie. Economica, Paris, 2000. Une analyse économique informée et pénétrante des nouvelles technologies par un maître de l'économétrie et de la statistique, disponible en ligne ici : http://www.volle.com/ouvrages/e-conomie/table.htm .

[115] Michel Volle. De l'informatique. Economica, Paris, 2006.

[116] Michel Volle. « Histoire d'un datawarehouse ». 21 mars 2003. http://www.volle.com/travaux/dwh.htm .

[117] Xiaoyun Wang, Andrew Yao, et Frances Yao. « New Collision search for SHA-1 ». Dans Crypto'05, 2005.

[118] Xiaoyun Wang, Yiqun Lisa Yin, et HongboYu. « Finding Collisions in the Full SHA-1 ».Dans Advances in Cryptology – Crypto'05, 2005. http://www.infosec.sdu.edu.cn/paper/sha1-crypto-auth-new-2-yao.pdf .

[119] Gerald M. Weinberg. The Psychology of Computer Programming.Van NostrandReinhold, New York, 1971.

[120] Wikipédia. « Débordement de tampon ». Wikipédia, 14 octobre 2005. http://fr.wikipedia.org/wiki/Buffer_overflow .

[121] Wikipédia. « Poste à poste ». Wikipédia, 15 novembre 2005. http://fr.wikipedia.org/wiki/Poste-à-poste .

[122] Wikipédia. « SHA-1 ». Wikipédia, 15 novembre 2005. http://fr.wikipedia.org/wiki/SHA-1 .

[123] Wikipédia. « Network address translation ». Wikipédia, 19 décembre 2005. http://fr.wikipedia.org/wiki/NAT .

[124] Philippe Wolf. « De l'authentification biométrique ». Sécurité Informatique, octobre 2003. Cet article du bulletin de sécurité informatique du CNRS expose clairement les limites de la biométrie : http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/num46.pdf .

Résumé :

Ce mémoire consiste a présenter quelque technique de sécurité des réseaux, quel que soit informatique ou électronique.

Les technique ici site c'est : les vpn, tunneling et les pare feu.

Au troisième chapitre on parle de pentesting et l outils utilities c'est le kali linux.

Le kali linux est un outil de teste les niveaux de sécurités des réseaux site.

Soit on trouve ont des hauts niveaux de sécurité ou moyen ou faible.

L utilisation de cet outil demande beaucoup de connaissance on linux et unix, et même le développement.

Mots-Clés

1-le pentesting
2-sécurité des réseaux
3-solution de sécurités des réseaux
4-méthode de test de réseau
5-politique de sécurité.