Piratage éthique sur l'entreprise TSG

Nada Rizk

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

Centre régional associé du LIBAN

Institut des Sciences Appliquées et Économiques - Université Libanaise

---

MEMOIRE

présenté en vue d'obtenir

le DIPLOME D'INGENIEUR CNAM

SPECIALITE : Informatique

OPTION : Réseaux, Systèmes et Multimédia (IRSM)

par

RIZK Nada

Piratage Ethique sur l'entreprise TSG

Soutenu le 11 Avril 2011

JURY

PRESIDENT: ARNAUD Jean-Pierre

MEMBRES : FARES Pascal

IBRAHIM Abbas (Encadrant)

SOUEID Roland

Remerciements

Je désire exprimer mes vives reconnaissances à toutes les personnes qui m'ont aidé à réaliser ce projet et m'ont aidé et soutenu durant cette période.

Je souhaite tout d'abord remercier M. Abbas Ibrahim, mon superviseur, pour sa disponibilité, support et ses conseils tout le long de ce projet.

Ma gratitude va ensuite à la direction de l'ISAE – CNAM Liban, M. Elias El Hachem, directeur général et M. Pascal Fares, chef du département informatique, pour leur intérêt et support précieux pendant toutes les années au CNAM.

Je tiens à remercier particulièrement la direction de l'entreprise « TSG », M. Tony Salame, propriétaire et Président-Directeur Général, et M. Michel Salame, Directeur Opérationnel, qui m'ont permis de mener ma thèse dans de bonnes conditions et avec un degré de liberté précieux, M. Roland Soueid, chef du département informatique, qui m'a encadré avec patience durant la période du travail avec ses conseils et remarques qui m'ont été éminemment utiles et enfin tous les membres du département informatique qui m'ont aidé dans l'analyse et l'implémentation des études.

Je remercie spécialement les personnes à qui je dois d'avoir pu réaliser cette thèse : les professeurs qui ont contribué à me former au cours de ma scolarité et mes parents qui m'ont encouragé sur la voie des études.

Enfin, j'adresse mes remerciements aux membres du jury d'avoir la patience de lire et d'apprécier mon travail.

Merci Dieu...

Liste des abréviations

ARP	Address Resolution Protocol
DdoS	Distributed Denial of Service
DoS	Denial of service
DOS	Disk Operating System
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IM	Instant Messaging
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISA	Internet Security and Acceleration
ISO	International Organization for Standardization
ISP	Internet Service Provider
LDAP	Lightweight Directory Access Protocol
NTFS	New Technology File System
OCS	Office Communications Server
SMB	Server Message Block
SID	System ID
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure SHell
SSL	Secure Socket Layer
TCP/IP	Transmission Contrôle Protocol / Internet Protocol
UDP	User Datagramme Protocol
WEP	Wired Equivalent Privacy
WI-FI	Wireless Fidelity

Glossaire

Chiffrement	Opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas de clé permettant de le ramener à sa forme initiale.
Clé de cryptage	Séquence de symboles qui détermine le chiffrement des données, et qui sert également à leur déchiffrement dans un système cryptographique à clé secrète.
Commutateur	Equipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique.
FTP	Protocole TCP-IP permettant à des ordinateurs d'échanger n'importe quel type de fichiers.
HTTP	Protocole de la suite TCP/IP permettant la navigation dans des pages hypertexte, reliées par des liens. Ce protocole permet la construction du web.
HTTPS	Combinaison du protocole HTTP utilisant le protocole SSL pour chiffrer les communications.
Hypertexte	Caractéristique de fichiers textes dont certains mots ou groupes de mots sont reliés à d'autres documents par des liens permettant de passer de l'un à l'autre automatiquement.
Intranet	Réseau interne à l'entreprise, utilisant les mêmes outils et protocole qu'Internet.
IP	Protocole de communication par paquets à la base d'Internet.
IPSec	Ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP.
ISO	Producteur et éditeur mondial de Normes internationales.
ISP	Fournisseur d'accès à Internet.
Ligne louée	Connexion permanente louée d'un ISP.
Log File	Fichier contenant l'enregistrement séquentiel de tous les événements affectant un processus particulier.

Modem	Périphérique servant à communiquer avec des utilisateurs distants par l'intermédiaire d'une ligne téléphonique.
Pare-feu (Firewall)	Ensemble de composants (matériels et logiciels) qui bloquent la transmission de certaines classes de trafic.
Ping	Commande informatique permettant d'envoyer une requête ICMP d'une machine à une autre machine
Protocole	Séquence de règles à suivre dans les communications pour établir et entretenir des échanges entre des entités distantes.
Rejeu	Message répété intentionnellement en partie ou en totalité. C'est notamment le cas d'un message d'authentification d'échange prélevé et réémis par une autre entité afin de s'en approprier les droits.
Routeur	Machine chargée de gérer le réseau et servant de nœud d'interconnexion.
Sip	protocole standard ouvert de gestion de sessions souvent utilisé dans les télécommunications multimédia.
SMTP	Protocole de transmission de la messagerie Internet.
SNMP	Protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.
Spam	Messages à caractère commercial diffusés à un grand nombre de personnes, sans quelles en aient fait la demande au préalable.
Spoofing	Technique utilisée pour accéder à un ordinateur ou à une information électronique en usurpant l'identité d'un élément autorisé.
SQL	Langage standard d'accès aux bases de données.
SSL	Protocole de sécurisation des échanges sur Internet, devenu Transport Layer Security (TLS) en 2001, il intervient entre le protocole TCP-IP et les différents protocoles applicatifs tels SMTP ou HTTP.
SE	Ensemble de programmes central d'un appareil informatique qui sert d'interface entre le matériel et les logiciels applicatifs.
TCP/IP	Suite de protocole de contrôle pour gérer les échanges entre deux machines d'un réseau (sur Internet). IP est le protocole de communication par paquets à la base d'Internet, TCP étant un protocole assurant la

	validation du transport de paquets. La suite TCP/IP comprend de nombreux autres protocoles UDP, SMTP, HTTP, FTP…).
Telnet	Protocole d'émulation de terminal permettant d'obtenir à distance une ligne de commande sur un ordinateur. Telnet fait passer « en clair » l'ensemble des échanges, et n'est donc pas sécurisé.
UDP	Protocole de télécommunication utilisé pour la transmission des données en mode non-connecté sans garantie de livraison.
WEP	Protocole pour sécuriser les réseaux sans fil de type Wi-Fi.
Wi-Fi	Ensemble de protocoles de communication sans fil permet de relier sans fil plusieurs appareils informatiques au sein d'un réseau.

Table de Matières

Introduction

Les temps ont changé ainsi que les exigences et les contraintes qu'impose un marché en perpétuelle évolution, pour ne pas dire en pleine explosion. Afin de poursuivre les évolutions récentes et rapides de l'informatique et d'acquérir un marché national et international, les entreprises se trouvent désormais obligées d'ouvrir leur système d'information à leurs partenaires ou leurs fournisseurs. Elles doivent confronter le contrôle efficace de la confidentialité, de l'intégrité et de la disponibilité de ces informations. Il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

Par ailleurs, avec l'instabilité, consistant à permettre aux personnels de se connecter au système d'information à partir de n'importe quel endroit, les personnels sont amenés à « transporter » une partie du système d'information hors de l'infrastructure sécurisé de l'entreprise. Dès lors, la sécurité revêt une importance qui grandit avec le développement des réseaux de type *Internet Protocol* (IP). La complexité des technologies utilisées, la croissance des terminaux à protéger ainsi que l'augmentation des nouvelles menaces démontrent que la sécurité est, et sera plus encore demain un enjeu stratégique majeur. De nombreuses grandes entreprises ont déjà compris l'importance de ces enjeux et définissent un plan de sécurité proactif en ayant recours au piratage éthique qui est un élément essentiel de ce plan. Il est plus facile d'attaquer que de défendre, il ne suffit plus d'installer des anti-virus et pare-feux, il faut des méthodologies, des procédures, des outils et de l'expertise. La nécessité de former les professionnels de la sécurité des réseaux continue de croître. Il ne suffit pas de connaître les ennemis, il faut connaître leurs armes et leurs tactiques pour pouvoir se défendre. L'ennemi est très mobile et utilise l'effet de surprise. La veille et surveillance demandent trop de ressources.

Les grandes entreprises libanaises font face à ces enjeux, défis et problèmes mais peu sont celles qui motivent l'investissement sur un projet de piratage éthique. Dans le cadre de mon emploi actuel comme ingénieur des systèmes et réseaux dans le group TSG, afin de motiver mon entreprise pour un tel investissement, il m'a fallu ouvrir leurs yeux à l'existence de ces enjeux et leurs dangers inaperçus qui menacent silencieusement les ressources

matériels et intellectuels et proposer les solutions pour faire faces aux défis et éliminer les vulnérabilités existantes. Le travail a réalisé nécessite l'intervention des membres du département informatique qui vont m'aider à inciter la curiosité des responsables pour atteindre les résultats demandés.

Comme l'évolution est une qualité principale vécue continuellement dans l'organisation, en explorant les possibilités de mémoire et de tutorat avec les directeurs, j'ai reçu leur encouragement moral et matériel, ils ont même proposé quelques idées à explorer qui m'aideront à compléter mes connaissances et capacités ainsi qu'à aider à faire évoluer le travail de l'entreprise. L'objectif général de la thèse est d'exploiter les méthodes et outils du piratage éthique afin de mieux protéger les ressources de l'entreprise.

Ce document présente les travaux de piratage éthique réalisés, allant de la planification préliminaire du travail jusqu'à l'exécution des attaques, les résultats obtenus et les contres mesure suivies. Dans les pages suivantes, je commence par la phase préparatoire dans laquelle je fais l'étude du système existant, l'analyse de ses besoins et suite aux raisonnements effectués, la proposition d'un travail de piratage éthique. Dans la deuxième partie j'explique le piratage en général, en exposant les détails du piratage éthique, ces types, objectifs et commandements. La troisième partie couvre les outils et techniques de pénétration utilisés par les pirates éthiques et les testeurs de sécurité, leur application sur le système actuel et les résultats des tests qui dévoilent les vulnérabilités et enjeux existants. Après l'évaluation de ces problèmes j'enchaîne avec la proposition de recommandations et solutions pour remédier les failles existantes, renforcer la sécurité du système et protéger les données pertinentes contre d'éventuels pirates noirs. J'ai obtenue ensuite l'approbation de la direction sur les solutions proposées et poursuis avec l'implémentation effective des nouvelles politiques de sécurisation. La quatrième partie est dédiée pour le problème des utilisateurs privilégiés d'Oracle et l'élaborions d'une nouvelle norme de sauvegarde qui assure la limitation des privilèges et la sécurisation des bases de données Oracle de l'organisation. La dernière partie consiste à la gestion des systèmes après sécurisation, j'applique quelques outils de tests utilisés dans la deuxième partie pour évaluer le niveau de sécurité atteint et j'élabore ainsi un modèle de référence pour le futur et des listes de contrôle périodiques à vérifier par les membre du département informatique dans toutes les branches de l'organisation.

Chapitre 1

Phase préparatoire

1.1 Etude de l'existant

Le groupe *Toni Salame Group* (*TSG*) est Fondée en 1989 par *M. Tony Salame* qui gère une entreprise de gros par le biais de "*TSG*" et un commerce de détail par le biais de *AISHTI* pour des vêtements, accessoires, cosmétiques, meubles et produits architecturaux. Offrant des services à valeur ajoutée pour les marchés à échelle moyenne et supérieurs, le groupe emploie actuellement environ 600 personnels et exploite 14 points de vente et magasins franchisés au Liban et aux pays du Golfe.

L'entreprise a débuté par un seul magasin ensuite plusieurs branches ont été ouvertes dans divers régions libanaises : zalka, kaslik, verdun, achrafieh… Au début les branches n'étaient pas connectées, il n'y avait même pas un système informatisé pour la gestion et le contrôle du stock ou pour la facturation. Deux ans plus tard ils ont installé un système informatisé dans la branche centrale via lequel ils effectuaient uniquement le contrôle du stock. En 1994 l'entreprise a implémenté dans toutes ses branches un nouveau système informatisé basé sur le langage Dolphin. Afin de synchroniser les informations entre les branches, la compagnie a mis en fonction une connexion à travers les lignes téléphoniques par des modems pour transférer les données, ou, un employé emportait les données sur des disquettes d'une branche à une autre. En 2001 avec l'inauguration de 2 grandes branches et l'implémentation d'un nouveau système informatisé basé sur Oracle, on a connecté toutes les branches en utilisant plusieurs technologies suivant l'emplacement et la distance entre les branches, parmi les technologies utilisées : ligne louée, réseau micro-onde, réseau local….

Actuellement l'entreprise se divise en six grandes parties joignant leurs différentes tâches afin d'atteindre les normes de *l'Organisation Internationale de Normalisation* (*ISO*) 9001:2000 ainsi que les règles d'or de la société qui sont : le respect de tous, l'amélioration continue et l'excellent service clientèle.

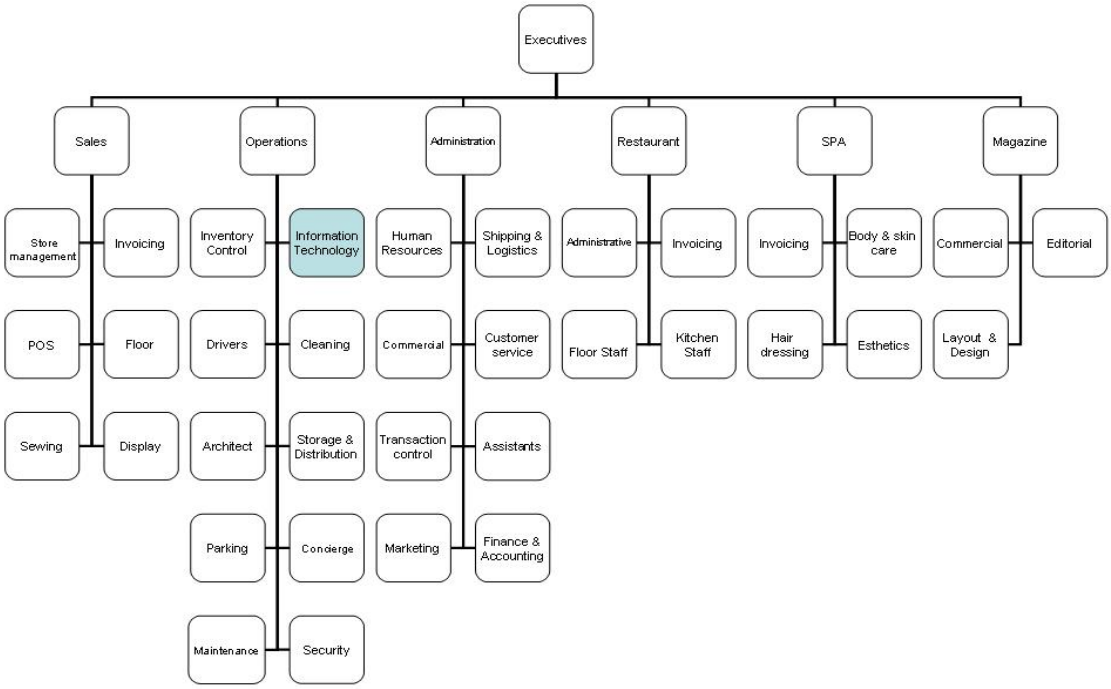


Figure 0.1 : Diagramme hiérarchique de l'organisation

Le département informatique dans l'entreprise forme un support opérationnel caché mais important par rapport aux utilisateurs et à la direction. Notre travail ne se limite pas au support des problèmes des utilisateurs, mais s'étend aussi à la planification des futurs besoins et l'amélioration continue de notre système tout en respectant la limite budgétaire imposée.

1.2 Analyse des besoins

Plus l'entreprise grandisse, plus les défis de conserver un haut niveau de sécurité deviennent difficiles. Avec l'inauguration de nouvelles branches au Liban et dans les pays du Golfe, et l'ouverture de notre système informatisé au marché international, les ressources informatiques de l'entreprise deviennent menacées par des attaques internes et externes nuisibles à l'entreprise entière.

Pourquoi maintenant a-t-on décidé de faire face à ces menaces ?!

Au début l'entreprise n'avait pas un système informatisé, ni des connections entre les branches, donc il y avait un contrôle manuel sur les ressources de l'entreprise. Lorsqu'on a installé le nouveau système et configuré la connexion temporaire à travers les lignes téléphoniques entre les branches, les exigences de sécurisation étaient minimes et faciles, d'abord parce que les outils d'attaques étaient restreints et difficiles, il faut beaucoup d'expertise pour trouver et utiliser les outils convenables, ensuite parce que la connexion était temporaire et le réseau utilisé était intégrer dans le réseau téléphoniques difficile à accéder.
Lorsque le nouveau système a été installé et avec l'implémentation d'une connexion permanente entre les branches et avec le réseau internet, les menaces commencent à apparaître. Mais les moyens de sécurisation utilisés à l'époque étaient suffisants. On a installé un pare-feu entre le réseau interne et externe et configurer les routeurs internes par des règles interdisant le passage des trafics non connus et cryptant le trafic permis.

L'ouverture de nouvelles branches au Liban et aux pays du Golfe était la première raison de dégradation du niveau de sécurité. Les règles et les matériels installés ne sont plus suffisants, les vulnérabilités augmentent, les outils d'attaques deviennent plus faciles à obtenir et à manipuler même par des non-experts, de même les intrusions menacent les ressources de l'entreprise. D'ici naît le premier besoin de reformulation de la sécurisation du réseau et des ressources qui sont la base de l'entreprise par rapport à la direction et au propriétaire.

La croissance de l'entreprise n'est pas la seule raison incitant le renforcement de la sécurité, l'obtention de la certification *ISO* 9001:2000 qui est renouvelée chaque 6 mois par un audit semestriel nous a ouvert l'esprit sur des obligations de sécurisation parfois négligées

antérieurement, comme les privilèges pour chaque type d'utilisateur, les anti-virus utilisés et leur mis à jour régulièrement, l'utilisation des cartes mémoires externes, l'accès physiques aux serveurs… Bien sur quelques points ont été déjà pris en considération, mais il faut aussi régler les nouvelles exigences signalés par les auditeurs de l'*ISO*.

1.3 Raisonnement et proposition

Afin de sécuriser les ressources informatiques des attaques internes ou externes, il faut penser comme les malveillants et essayer leurs façons d'attaque et leurs outils simples ou sophistiqués. Beaucoup d'entreprises ont recours à l'externalisation des spécialistes de sécurité ou plus récemment au piratage éthique pour résoudre les problèmes de sécurisation de leurs ressources… Mais ce que je pensais, c'est de proposer à ma direction que j'effectue ce travail moi-même.

J'ai présenté l'idée au directeur en exposant les arguments et les analyses mentionnés avant, qui synthétisent l'état actuel de notre système et consolident les raisons d'amélioration de la sécurité en ayant recours au piratage éthique. Je lui ai proposé d'effectuer cette tâche qui sera le thème de ma thèse pour l'obtention du degré d'Ingénieur, il a été convaincu par les arguments et analyses présentés et a encouragé l'idée d'effectuer moi-même le piratage éthique au lieu d'externaliser la tâche à quelqu'un d'étranger qui saisira les détails privés de l'entreprise et peut être sera lui-même une menace à ses ressources. Le directeur a accepté aussi de participer au tutorat et de poursuivre l'enchaînement du travail pendant toutes les phases du mémoire et même de participer au jury lors de la soutenance si cela est demandé.

Une fois l'idée a été admise, j'ai commencé méthodiquement à déterminer les phases préliminaires nécessaires pour la mise en œuvre effective du projet. Débutant par l'identification de ces ressources, leurs assigner des priorités, l'énumération des vulnérabilités possibles et la planification du travail à effectuer. Ces phases sont réalisées avec l'aide de tous les membres du département informatique afin de couvrir toutes les branches et ressources de l'entreprise.

Chapitre 2

Aperçu sur le piratage éthique

Avant d'entamer les phases pratiques du projet, il faut présenter un aperçu théorique sur le piratage éthique. Cette partie couvre les aspects fondamentaux du piratage éthique, débutant par une définition générale et puis détaillée du piratage informatique, ensuite une notion sur les types de piratage, l'objectif du piratage éthique, le profil de compétence du pirate éthique et enfin les commandements auxquels il doit obéir.

2.1 Définition du pirate informatique

La définition générale de « pirate » dans l'encyclopédie électronique *wikipedia* est un individu qui pratique de manière répétée le vol avec violence, plus précisément, un pirate informatique est une personne qui effectue des crimes dont l'objet ou l'arme est lié à l'informatique. Mais le terme englobe deux expressions antonymes majeures : Hacker et Cracker.

En sécurité informatique, un hacker est un spécialiste dans la maîtrise de la sécurité informatique, il utilise son savoir-faire dans un cadre légal, mais d'autres spécialistes utilisent ce savoir hors-la-loi, ces derniers sont appelés « crackers ».

La différence fondamentale est donnée par des auteurs de référence : *Eric Steven Raymond* et *Manuel Castells* :

« Les hackers construisent les choses, les crackers les démolissent »

2.1.1 Hacker

Le hacker est une personne passionnée en informatique, elle invente et innove pour le plaisir, elle veut comprendre le système informatique et tester ses connaissances et outils afin de découvrir les failles de sécurité et alerter ensuite les responsables. Tous les hackers n'ont pas les mêmes motivations, d'où la distinction de trois types de hackers définies dans plusieurs sources électroniques ou bibliothécaires:

2.1.1.1 Les chapeaux blancs ou *white hat*

Ils utilisent leurs connaissances pour tester la solidité des défenses des systèmes informatiques suite à la demande et permission du client. Ils utilisent les outils et techniques

de piratage mais d'une façon légale. Ils peuvent être consultants en sécurité, administrateurs des réseaux ou veiller sur la légitimité des produits informatiques et des droits de sécurité proclamés par les fournisseurs.

2.1.1.2 Les chapeaux noirs ou *black hat*

Ils utilisent leur savoir pour créer des outils nuisibles à la sécurité informatique comme les virus, vers, cheval de Troie… et effectuer des actes malveillants agissant hors-la-loi dans le but de nuire ou tirer profit de leurs actes. Leurs cibles peuvent être des ordinateurs individuels ou même un réseau d'une grande entreprise.

2.1.1.3 Les chapeaux gris ou *gray hat*

Ce genre de hacker est qualifié et expert, il pénètre légalement ou non dans un système mais il n'a pas un but nuisible. Il cherche plutôt l'exploit et faire preuve d'agilité. En terme simple c'est un hacker hybride entre les hackers *black hat* et *white hat.*

2.1.2 Cracker

Conçoit des programmes informatiques ou cracks pour modifier le comportement d'un logiciel, la plus part des temps, pour lever la protection ou restriction d'utilisation sans payement. Il utilise des débogueurs ou algorithmes pour trouver un code d'enregistrement valide ou des désassembleurs pour modifier directement le logiciel. L'intérêt du cracker est soit d'utiliser un certain logiciel gratuitement ou par exemple relever un défi.

2.1.3 Script-Kiddies

Des pirates débutants avec peu d'expertise technique, ils piratent pour le plaisir, en utilisant des programmes codés par les hackers, faciles à utiliser, préconfigurés et automatisés, sans comprendre comment ils fonctionnent. Ils veulent le pouvoir du hacker sans la discipline et la formation nécessaire, et dont le but est la destruction ou gain financier. Ils sont nombreux et forment une menace sur les systèmes informatiques.

2.2 Types de piratage

Les types de piratage passent d'un niveau simple, utilisé par la plus part des internautes à un niveau professionnel utilisé par les hackers. Ces types peuvent être groupés en 5 catégories principales :

- Communal : Besoin de contrôle, de l'acceptation
- Technologique : force le progrès
- Politique : A un message
- Economique : Gain économique personnel
- Gouvernementale : Terrorisme

Selon l'*Institut de sécurité informatique* (1999), les types de criminalité informatique sont :

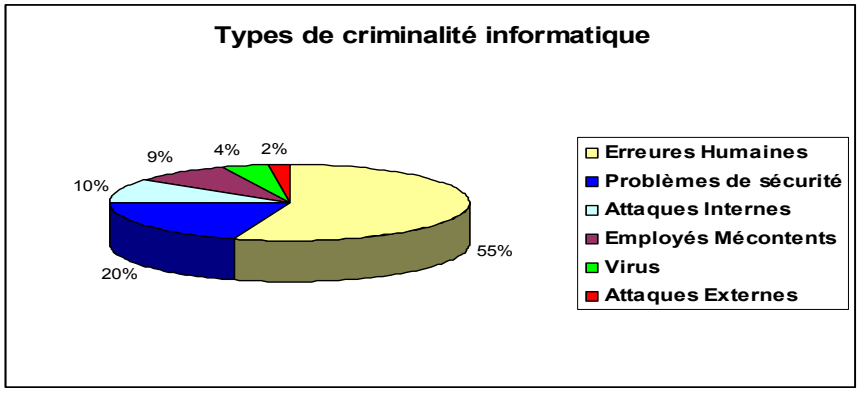


Figure 0.1 : Types de criminalité informatique

Selon une étude du *Computer Security Institute* publiée sur le site *http://znsoft.be*, plus de 40% des entreprises ont constaté au moins une tentative d'intrusion au cours de la dernière année. Laissant des serveurs piratés, des numéros de cartes bancaires volés, des sites défigurés… et résultant des pertes financières graves. Ces pertes sont schématisées grâce aux études de l'*Institut Computer Economics* (2006) dans le graphe suivant :

Financial impact of virus attacks 1995–2005

	Worldwide impact (US $)
2005	$14.2 Billion
2004	17.5 Billion
2003	13.0 Billion
2002	11.1 Billion
2001	13.2 Billion
2000	17.1 Billion
1999	13.0 Billion
1998	6.1 Billion
1997	3.3 Billion
1996	1.8 Billion
1995	500 Million

Source: Computer Economics, 2006

Figure 0.2 : Estimation des dégâts financiers des attaques informatiques 1995-2005

Malgré les efforts pour atténuer les dégâts, le graphe montre une fluctuation annuelle du montant des pertes dès l'an 2000.

2.3 Objectif piratage éthique

« Pour attraper un pirate, pensez comme un pirate. C'est la base du piratage éthique. » (Ankit Fadia – unofficial guide to ethical hacking)

Alors que la complexité des failles dans un système informatique ne cesse de croître, il devient indispensable de prendre des mesures défensives proactives pour contrer les attaques malveillantes. L'intention de piratage éthique est de découvrir les vulnérabilités à partir d'un point de vue du hacker afin de mieux sécuriser les systèmes. Le pirate attaque le système informatisé d'une entreprise, avec son consentement et à sa demande, afin de déceler d'éventuelles failles de ce système.

Comprendre les techniques de piratage est la première étape d'apprentissage des moyens de sécurisation des applications. Savoir ce que les pirates veulent aide à comprendre comment ils fonctionnent. Comprendre leur manière de travailler permet de regarder les systèmes d'information dans son ensemble d'une nouvelle manière.

Il faut donc utiliser le piratage éthique pour mettre en évidence les faiblesses dans les entreprises et choisir les contre-mesures nécessaires pour les annuler.

2.4 Profil de compétence:

Le hacker doit identifier les faiblesses du système informatisé d'une d'entreprise, exploiter de manière systématique les défenses internes et externes, élaborer des contre-mesures ainsi que réduire et limiter les risques encourus par une entreprise. Afin d'effectuer ces tâches, il doit se tenir à jour sur les diverses techniques, vulnérabilités et technologies. Pour se tenir à jour le pirate éthique doit s'informer de diverses sources et doit avoir un profile de haute compétence caractérisé par trais variés :

- Forte personnalité
- Discret
- Patient
- Loyal
- Certifié
- Qualifié

- Persévérant et méthodique
- Savant et pertinent
- Connaissance en programmation et réseaux
- Connaissance en installation et maintenance
- Connaissance en Gestion des systèmes

Malheureusement avec le temps les compétences nécessaires diminuent progressivement avec la présence de nouveaux outils et programmes sophistiqués et puissants à usage facile. Les études effectuées par *EC-Council* révèlent une proportion asymétrique entre les compétences demandées et la complexité et puissance des outils disponibles.

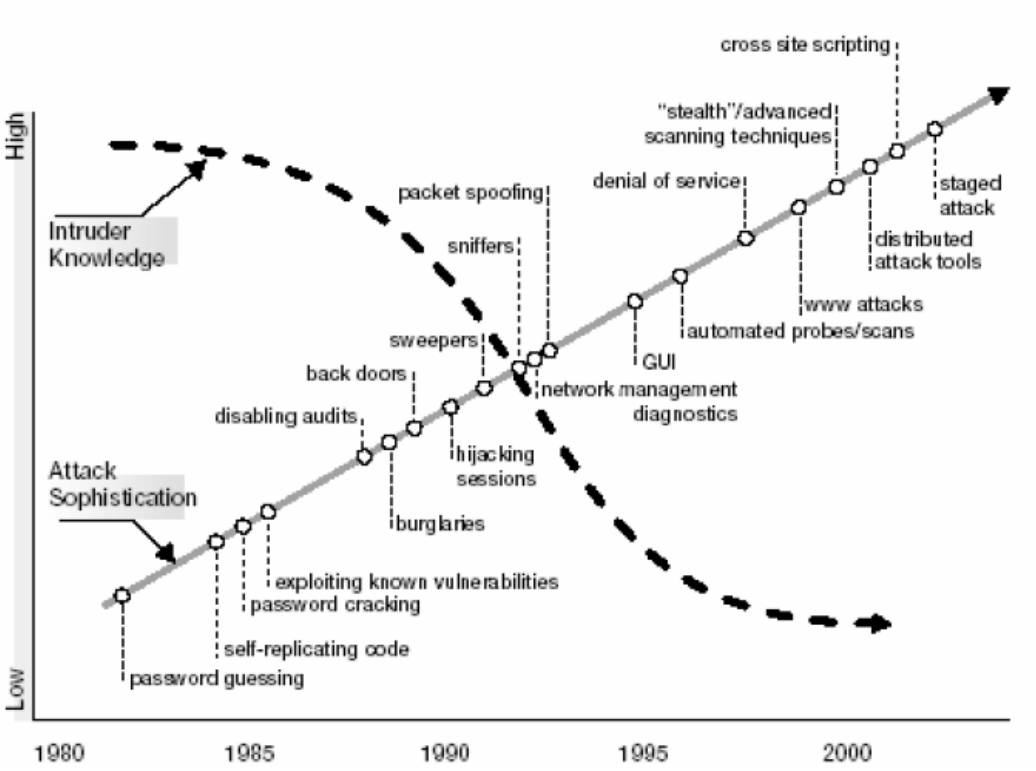


Figure 0.3 : Comparaison entre compétence des pirates et sophistication des outils
Référence: *CEH v5 Module 01 Introduction to Ethical Hacking*

2.5 Commandements du piratage éthique

Le pirate éthique doit respecter un nombre de commandements de piratage éthique. Ignorer ou oublier ces commandements lors de la planification ou l'exécution des tests de piratage mènent à des résultats néfastes. Les commandements se groupent selon trois catégories :

2.5.1 Travail Ethique

Le mot éthique dans ce contexte peut être défini comme étant le travail à haute moralité et principes professionnelles. Que ce soit des tests de piratage éthique sur son propre système ou sur celui d'une entreprise qui l'a embauché, le travail du pirate éthique doit être authentifié et doit soutenir les objectifs de l'entreprise.

2.5.2 Respect de l'intimité

Traiter les informations recueillies avec le plus grand respect. Toutes les informations obtenues lors des essaies doivent être gardées privées. Ne pas utiliser ces informations pour fureter dans les informations confidentielles de l'entreprise ou dans la vie privée. Si quelqu'un devrait savoir qu'il y a un problème, envisagé de partager cette information avec le gestionnaire. Impliquer d'autres personnes des processus de piratage utilisés. Il s'agit d'une "veille de la surveillance" du système qui peut renforcer la confiance et le support du projet de piratage éthique.

2.5.3 Garder le système opérationnel

Une des plus grandes erreurs rencontrées, quand les gens essaient de pirater leurs propres systèmes et le rendent inopérant. La principale raison est une faible planification. Les testeurs n'ont pas lu la documentation ou ont mal utilisé les outils et techniques d'attaque. On peut facilement créer des attaques de type Déni de Service (DoS) sur un système en phase de tests. Mais exploitant un grand nombre de tests sur un système provoque son blocage. Parfois les réseaux et les ordinateurs ne supportent pas les nombreuses attaques et outils utilisés lors des tests et finissent par s'épanouir. De nombreux outils d'évaluation de la sécurité permettent de contrôler le nombre de tests effectués simultanément sur un système. Ces outils sont particulièrement pratiques si on a besoin d'exécuter les essais sur les systèmes de production durant les heures de fonctionnement normal.

Chapitre 3

Attaques, Evaluation et Sécurisation

Comme pratiquement tous les projets informatiques ou de sécurité, le piratage éthique doit être planifié à l'avance. Cette deuxième partie couvre les étapes de cette planification, partant de la mentalité du pirate pour déterminer les processus stratégiques et tactique, y compris le repérage et l'identification des vulnérabilités et risques, le choix des outils d'attaques et la démarche de leur exécution, arrivant à l'évaluation des résultats et contre-mesure applicables.

3.1 Méthodologies d'attaque

3.1.1 Formulation du plan

La première phase dans la formulation du plan consiste à obtenir l'approbation de l'entreprise. Il faut informer les responsables de toutes les étapes à suivre et obtenir leur parrainage dès la première étape. Ca pourrait être un manager, un dirigeant, ou un client, il doit signer sur le plan élaboré par le pirate éthique, sinon les essais peuvent être annulés d'une façon inattendue si quelqu'un prétend ne jamais avoir autorisé la réalisation de ces tests.

Lorsqu'il est embauché par une organisation, le pirate éthique demande à l'organisation ce qu'elle tente de protéger, contre qui, et quelles ressources financières dispose-t-elle pour obtenir cette protection, à la suite, il élabore un plan détaillé du champ d'application des attaques comprenant les informations suivantes :

- Les systèmes à tester
- Les risques qui sont impliqués
- Le calendrier des tests
- Comment les essais sont effectués
- Informations nécessaires pour commencer les tests
- Que fait-on quand un problème est rencontré

Les résultats attendus dans plusieurs rapports sur :

- L'évaluation du niveau de sécurité
- Les vulnérabilités rencontrées
- Les contre-mesures applicables

Lors de la sélection du système à tester, il faut commencer par les plus critiques ou vulnérables avant de percer dans les systèmes les plus détaillés, et il faut avoir un plan d'urgence dans le cas où quelque chose passe mal.

3.1.2 Reconnaissance

La reconnaissance se réfère à la phase préparatoire du processus d'attaque, basé sur la prise d'empreinte et le recueil d'information, le hacker cherche à capter autant d'informations que possible sur la cible avant d'enchaîner son attaque. L'acquisition d'informations sur la cible est obligatoire pour pouvoir localiser les informations utiles et pertinentes ainsi que récupérer les données publiées et analyser les sites d'archive. On distingue deux genres de reconnaissance, active et passive :

3.1.2.1 Reconnaissance Active:

Acquérir les informations sans interaction directe avec la cible, par exemple la recherche des documents publics ou les communiqués de presse.

3.1.2.2 Reconnaissance Passive :

Interagir directement avec la cible par divers moyens, par exemple appeler le bureau d'assistance ou le département technique de l'entreprise.

Cette phase permettra donc au hacker de récupérer le maximum d'informations sur l'architecture du réseau, les Systèmes d'Exploitation (SE), les applications installées et les ressources pertinentes avec les méthodes d'authentification sur ces ressources.

3.1.3 Balayage et Identification des vulnérabilités

Une fois la topologie du réseau connue, le hacker effectue un balayage du système pour trouver les vulnérabilités et les exploits possibles à effectuer, le balayage peut être exécuté à l'aide de divers outils comme *NMAP* et *mappeur passif*. Lorsque le balayage du réseau est terminé, il suffit au pirate d'examiner le fichier journal ou *Log File* généré par l'outil utilisé pour déterminer les ports, services, applications et comptes sur les différentes

machines. Il utilise ensuite des logiciels spécialisés ou scanneurs de vulnérabilités qui soumettent le système à des tests d'intrusion pour examiner les failles ou vulnérabilités nuisibles à la sécurité du système, dans les protocoles, les SE les applications ou même le personnel de l'organisation.

3.1.4 Choix des outils d'attaques

Le pirate éthique doit choisir les outils convenables pour son travail ou l'accomplissement de sa tâche sera difficile. L'utilisation des meilleurs outils, n'implique pas nécessairement trouver toutes les vulnérabilités existantes. De nombreux outils d'évaluation de la sécurité génèrent des résultats manquants ou erronés car ils sont orientés vers des tests spécifiques, pour cela le hacker a besoin d'un ensemble d'outils variés et spécifiques pour tous genre d'attaques. Le choix de ces outils est lié aux résultats obtenus suite au balayage et identification des vulnérabilités pour pouvoir exploiter les failles trouvées. Lorsque le pirate choisit ses outils, il est préférable qu'il obtienne les conseils et commentaires des experts les ayant utilisés pour s'assurer de leur efficacité. Avant de les utilisés, il doit s'en familiarisé et comprendre leur capacité sinon les résultats de leur utilisation peuvent être erronée et par suite nuisibles par rapport au système étudié.

3.1.5 Exécution des attaques

Le piratage éthique peut prendre la persévérance du pirate, pour cela temps et patience sont importants. Le travail doit être effectué d'une façon privée et silencieuse surtout pendant la transmission et stockage des résultats, dont il est préférable de chiffrer ou protéger par des mots de passe. Durant cette phase il est nécessaire de planifier la démarche des tests afin d'éviter une faille possible du système. Ce plan doit inclure :

- Quand les tests sont performés
- Quels tests sont performés
- Comment et où les tests sont performés
- Quoi faire quand une vulnérabilité majeure est découverte

Lorsque le pirate a dressé son plan et l'inventaire des dispositifs du réseau, il est en mesure de préparer son intrusion. Pour pouvoir s'introduire dans le réseau, le pirate a besoin

d'accéder à des comptes valides sur les machines et cherche ensuite à augmenter ses privilèges en obtenant l'accès de l'administrateur du système pour étendre ses privilèges.

3.1.6 Résultats et contres mesure

Après l'exécution des tests, il est possible d'évaluer le niveau de sécurité suite aux résultats obtenus, et ainsi révéler les vulnérabilités rencontrées et proposer les contre-mesures applicables. Les taches à suivre durant cette phase seront :

3.1.6.1 Générer les rapports des résultats

Basé sur sa connaissance en tant que professionnel de la sécurité, et le classement des vulnérabilités trouvées par ses outils d'évaluation, le pirate éthique doit présenter à la direction de l'entreprise les rapports comprenant les résultats obtenus lors de ses tests, et les mesures à prendre afin d'atténuer les failles et risques rencontrés. Ces rapports montrent également que le temps, l'effort et l'argent sont utilisés à bon escient.

Durant la première phase, le pirate éthique rassemble les résultats dans une synthèse qui peut être organisée dans un tableau divisé par catégories pour être plus claire aux directeurs. Ci-dessous un exemple d'un tableau présenté :

Table 0-I : Vulnérabilités internes et externes

Vulnérabilités Internes	Vulnérabilités Externes
Employés ou utilisateurs	Clients publiques
Matériels : ordinateurs, serveurs, routeurs…	Connections avec réseaux de partenaires
Sécurité physique des matériels	Utilisateurs distants
Points d'accès sans fil	Mauvais pirates (*black hat*)

Une fois les résultats sont organisés, il faut prioriser les problèmes trouvés pour éviter de perdre le temps avec quelques vulnérabilités difficiles à éliminer à cause des raisons techniques ou financières. Cette priorité peut être évaluée suivant deux critères :

- Risques d'utilisation : Probabilité qu'un pirate malicieux prend avantage de cette vulnérabilité pour pénétrer dans le système
- Impacts d'exploitation : Evaluer la nuisibilité de la vulnérabilité par rapport aux systèmes existants.

Il est possible de classer les vulnérabilités suivant une tranche numérique de 1 à 5 ou suivant des critères comme grave, moyen et faible pour chacune des deux catégories comme dans le tableau ci-dessous :

Table 0-II : Rapport Risque / Impact des vulnérabilités

Risques / Impacts	Grave	Moyen	Faible
Grave	Point d'accès insécurisé	Manque de mot de passe	Messagerie en plein texte
Moyen	Access Internet aux utilisateurs	Access malicieux en absence de l'utilisateur	Cassettes de données sans mot de passe
Faible	Anti-virus non mis-a-jour	Pas de chiffrage	Personnel de nettoyage ayant accès

Une fois toutes les informations sont collectées et arrangées, elles doivent être organisées d'une façon aisée dans le rapport pour qu'elles soient compréhensibles par la direction de l'entreprise qui n'est pas experte en sécurité.

En résumé, le rapport doit contenir les informations suivantes :

- Tests performés
- Date des tests
- Vulnérabilités découvertes
- Liste par priorité de ces vulnérabilités
- Etapes de sécurisation
- Liste des recommandations pour améliorer la sécurité générale

Enfin il faut faire attention que ce rapport ne tombe pas dans les mains des pirates malicieux sinon des conséquences néfastes peuvent se produire. Pour prévenir tels incidents il est préférable de suivre quelques conseils :

- Le rapport et les documents annexes doivent rester confidentiels et sont livrés seulement aux personnes concernées.
- Effacer tous outils ou documents utilisés lors des tests comme les fichiers journal ou outils d'analyse des réseaux ou mots de passe.

3.1.6.2 Contres mesure applicables

Suite au compte-rendu des résultats des tests, le hacker crée un plan d'action pour débuter les opérations correctives et contres mesure défensives pour sécuriser le système. Pour décider par quelle vulnérabilité il faut commencer, il doit s'assurer qu'elle peut être fixée, si elle est critique au système et par suite si le système doit être arrêter pour la fixée et le coût d'achat des matériels et logiciels exigés pour effectuer le travail.

Les approches correctives sont divisées selon plusieurs niveaux : social, organisationnel, physique, humain… La variation de ces niveaux assure la sécurisation du système selon plusieurs angles, elle est indispensable au cas où l'une des mesures échoue.
On distingue quelques actions correctives communes dans la plupart des études :

- Démarrer l'audit sur tous les serveurs
- Enfermer les chambres des serveurs
- Renforcer la sécurité des systèmes en implémentant des recommandations de sécurité standardisées
- Utiliser les outils pour déchirer les papiers confidentiels
- Installer des pare-feux sur tous les ordinateurs et pour le réseau entier
- Implémenter des politiques de sécurisation
- Mis à jour régulière des logiciels des serveurs web

Une vision du système d'une perspective non technique aide le hacker à identifier des actions correctives complémentaires aux actions révélées par les outils de tests utilisés dans les phases ultérieures.

3.1.6.3 Gestion des systèmes après sécurisation

La procédure de sécurisation prend beaucoup d'effort et de temps au début, mais après l'établissement d'un seuil de sécurité, la poursuite de contrôle des nouveaux risques et vulnérabilités sera plus facile. La sécurisation est un processus permanent qui doit être géré avec succès pour rester efficace. Les tests de piratage éthique performés de temps en temps sont critiques pour prévenir de nouvelles failles possibles. Il faut considérer donc l'automatisation des tâches de contrôle en utilisant des outils pour effectuer des balayages et surveillance continue du système.

L'utilisation des automates est insuffisante et inefficace après une certaine période, d'où le recours de nouveau au piratage éthique et outils non automatisés. Mais le piratage éthique est lui-même insuffisant, donc il faut l'accompagner avec des logiciels d'évaluation des risques, des politiques de sécurisation, des plans d'action en cas d'incidents et des formations pour les utilisateurs pour les éveiller aux problèmes de sécurité.

3.2 Exécution des attaques et Evaluation

La mise en œuvre du projet à passé par plusieurs phases allant de l'identification des ressources, la planification du travail, la typologie des attaques, les outils concernés, l'exécution des attaques arrivant à l'évaluation des résultats obtenus. Je rentrerai dans la partie qui suit dans les détails de chaque phase afin de mieux présenter les tâches suivies et résultats obtenus.

3.2.1 Identification des ressources

La première question dans cette phase consiste à définir ce que l'entreprise veut protéger et contre qui…

Afin d'identifier les ressources de l'entreprise il faut d'abord comprendre son architecture et ses composants. L'entreprise comprend 14 branches reliées entre-elles par divers type de communication comme le montre le schéma ci-dessous :

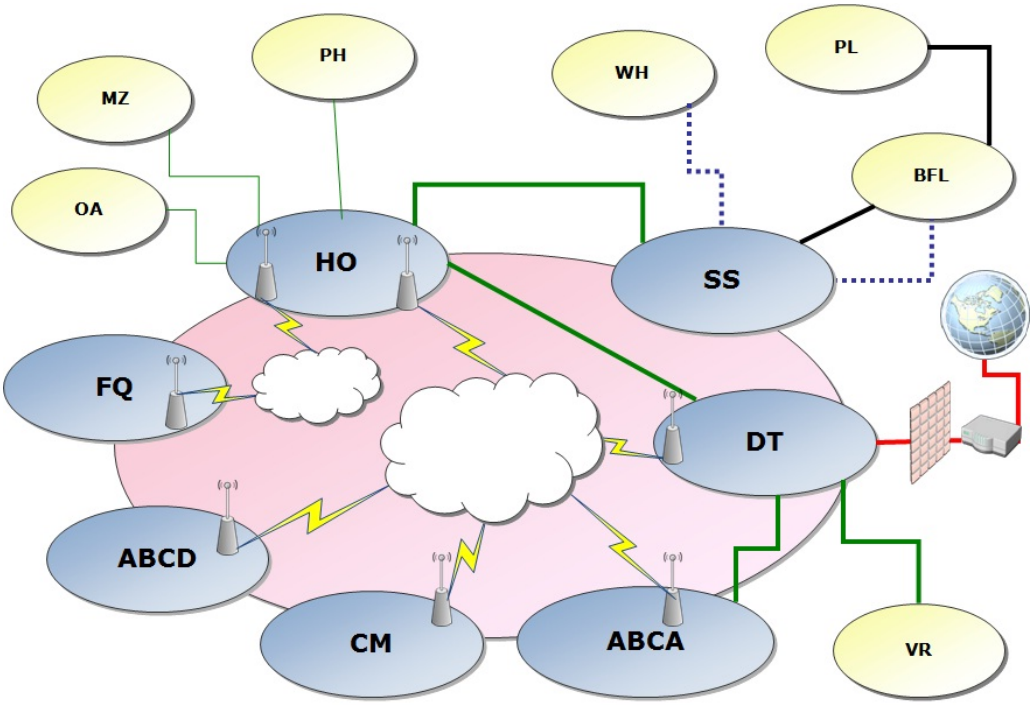


Figure 0.1 : Architecture globale de l'organisation

Les branches principales sont HO et DT, elles comprennent tous les départements administratifs qui gèrent le travail entier de l'organisation. Les autres branches sont des points de ventes localisés dans la capitale Libanaise et ses banlieues. Le système informatique de l'organisation est formé de plusieurs composants combinés ensemble pour assurer le fonctionnement correct des services nécessaires au déroulement du cycle de travail de l'entreprise. Les composants majeurs de ce système sont :

3.2.1.1 Système de gestion des identités et des accès

- **Service d'annuaire de Microsoft (Active Directory)**

  Active Directory (AD) renferme des informations relatives aux objets d'un réseau (utilisateurs, ordinateurs, politiques de groupe…) et met celles-ci à la disposition des utilisateurs et des administrateurs. AD permet aux utilisateurs d'accéder aux ressources autorisées partout sur le réseau à l'aide d'une simple procédure d'ouverture de session. Il fournit aux administrateurs réseau une vue hiérarchique intuitive du réseau et un point d'administration unique de l'ensemble des objets.

3.2.1.2 Services de messagerie

- **Microsoft Exchange Server**

  Plate-forme de messagerie qui intègre la messagerie, la planification et des outils pour des applications de collaboration et de service de messagerie personnalisées.
- **Office Communications Server (OCS)**

  Produit d'entreprise qui intègre les moyens de communication en temps réel avec la détection de la présence des utilisateurs, y compris la conférence Web

3.2.1.3 Outils de sécurisation

- **Internet Security and Acceleration Server (ISA Server)**

  Passerelle de haute sécurité qui protège le système informatique contre les menaces provenant de l'Internet, tout en offrant aux utilisateurs un accès à distance rapide et sécurisé aux données et aux applications.
- **Barracuda**

  Pare-feu qui forme une solution matérielle et logicielle intégrée pour assurer une protection complète du serveur de messagerie électronique. Il offre une solution à la fois puissante et simple à utiliser pour éliminer les courriers électronique indésirables.

- **Websense**

  Solution de sécurité Internet intégrée qui bloque les logiciels espions, les codes malicieux et autres menaces liées à Internet, de même que les communications entre les logiciels espions et autres enregistreurs de frappes de clavier vers leurs sites hôtes.

3.2.1.4 Systèmes de gestion des bases de données

- **Logiciel de base de données Oracle**

  Le logiciel actuellement employé dans l'organisation, est appelé MACC, il est basé sur la plateforme Oracle et développé par l'entreprise ***COMPUTEC***.

  MACC (Management Accounting and Cost Control) est formé de plusieurs modules d'application adaptée chacune pour répondre aux différents besoins du marché du travail. Les principaux modules utilisés sont :

  - Gestion des stocks
  - Système de point de vente : facturation, contrôle de stock, transfert des biens, clients…
  - Comptabilité générale
  - Budget et rapports financiers
  - Ressource Humaine : système de recrutement, données des employés, système de présence, système de rémunération

- **Logiciel de gestion des dispositifs informatiques « IT system »**

  J'ai développé ce logiciel sur la plateforme Visual Basic 6 avec une base de données sur la plateforme Microsoft SQL server, ce logiciel permet d'aménager les ressources informatiques, contrôler les dépenses et planifier les études budgétaires demandées. Il comprend plusieurs modules »

  - Gestion des dispositifs informatiques
  - Gestion des licences
  - Gestion de la consommation des articles jetable (CDs, DVDs, Encre…)
  - Gestion des routines de check up
  - Rapport pour la comparaison annuel des achats et consommations

3.2.1.5 Site Intranet

- **SharePoint Portal Server 2003**

  Série de logiciels pour applications web développée par Microsoft. Les fonctionnalités des produits SharePoint sont la gestion de contenu, les moteurs de recherche, la gestion électronique de documents, les forums, la possibilité de créer des formulaires.

  Le site interne de l'organisation appelé *AIWEB* permet aux employés d'accéder aux informations générales de l'entreprise, de partager leurs opinions sur des sujets précis, partager des images et d'être mis à jour avec les événements survenant.

Ces composants fournissent les activités majeures du système informatique de l'entreprise, l'étude des attaques les visera pour évaluer les vulnérabilités existantes et consolider le niveau de sécurité actuel.

3.2.2 Qu'est-ce que l'entreprise veut protéger ?

On peut diviser les ressources selon leurs types :

3.2.2.1 Serveurs et ordinateur

Les deux branches principales sont : HO et DT, elles comprennent les serveurs de base de données principale et ceux des services complémentaires : Exchange, ISA, OCS, Intranet… ainsi que les ordinateurs clients de tous les utilisateurs qui comprennent leurs information privées et relatives au travail. Dans les autres branches il existe un serveur de base de données et les ordinateurs de quelques employés administratifs. Les stations qui restent sont des points de vente qui ne contiennent pas d'information critiques.

3.2.2.2 Portables

Il existe dans l'entreprise 70 portables, certains utilisateurs les utilisent dans plusieurs branches et même à l'extérieur de l'entreprise, à leur maison ou dans les places publiques. Les portables et les données y existants sont menacés alors par des accès malins intentionnés ou accidentels

3.2.2.3 Dispositifs de réseaux

Il existe au moins dans chaque branche un commutateur, un routeur et un modem et parfois on trouve un point d'accès sans fil.

3.2.2.4 Réseaux externe

Afin de procurer un accès externe aux utilisateurs pour les services de messageries, il existe une zone intermédiaire entre le réseau interne el l'internet qui contient le pare-feu, le routeur externe, l'ISA et l'Exchange. Cette zone contient donc les ressources importantes pour l'entreprise et est menacées beaucoup plus que les autres ressources.

3.2.3 Contre qui l'entreprise veut protéger toutes ses ressources ?

3.2.3.1 Les employés

Ils forment des menaces directes ou indirectes sur les ressources existantes, par exemple un employé en colère cherchant la vengeance peut essayer d'accéder aux données privées et les détruire. Ou un employé qui prend des fichiers en dehors de l'entreprise et les utilisent sur des ordinateur publics qui peuvent par la suite être accédés par des malveillants. Un autre cas existe aussi, les employés qui communiquent des informations internes à l'entreprise oralement ou par écrit à des proches ou à des concurrents.

3.2.3.2 Les visiteurs ou clients

Ils accèdent les points de vente ou les bureaux administratifs. Ils peuvent être des clients, des agents de livraison, des représentants de nouveaux fournisseurs ou parfois des agents de support. Ces personnes peuvent accéder intentionnellement aux ressources qui ne sont pas bien sécurisées ou peuvent recueillir les informations à travers le passage parmi les employés.

3.2.3.3 Les Etrangers

Les malveillants sur l'internet forment des menaces périlleuses et multiples, ce genre de menace est le plus difficile à combattre et en prévenir. L'ouverture de notre système vers l'extérieur, notamment vers le monde de l'internet accroît ses vulnérabilités et failles.

3.2.4 Typologie d'attaque

Afin de protéger notre système contre ces menaces il est nécessaire d'élaborer un plan d'attaque basé sur une méthodologie élaborée d'un point de vue d'un pirate noir. Celle que j'ai choisie est basée sur l'hiérarchie des couches TCP/IP, débutant par les attaques au niveau de la couche physique arrivant à la couche application. Selon chaque niveau plusieurs outils et

logiciels seront utilisés pour attaquer toutes les ressources relatives à cette couche. Le schéma suivant montre les couches et protocoles à étudier.

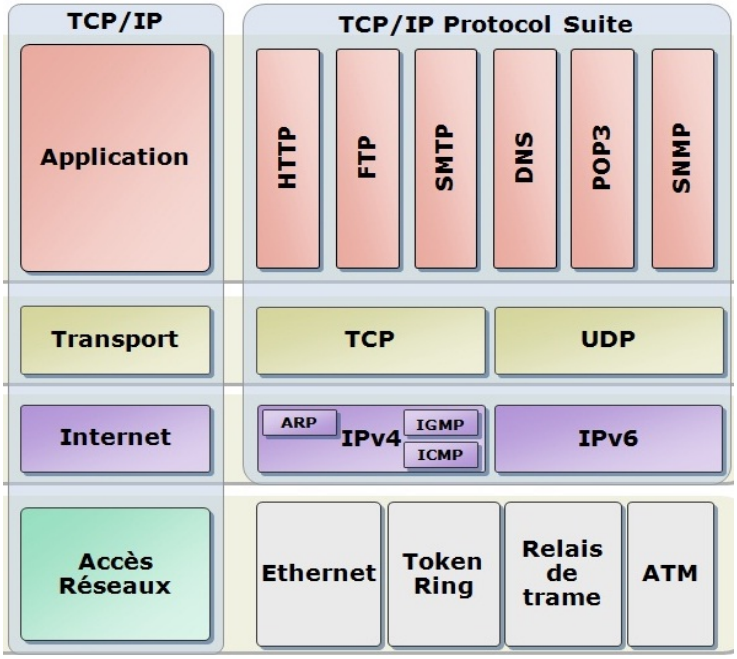


Figure 0.2 : Couches et protocoles de TCP/IP
Référence : *MCITP – cours 6420 – module 3*

Les ressources à tester suivant ce modèle peuvent être divisées comme suit :

3.2.4.1 Couche Accès Réseaux

- Accès physique aux serveurs, routeurs…
- Prises vides de réseaux dans les murs ou dans les commutateurs
- Supports de sauvegarde de données délaissés
- Chambres ou portes non-sécurisées
- Vol des ordinateurs portables

3.2.4.2 Couche Internet

- Balayage et analyse du réseau et trafic de données de l'organisation : *Omnipeek*, *GFI LanGuard* et *LanSpy*
- Pénétration des périphériques: *NMAP*, SolarWind Toolset (IP Network Browser), NetScanTools…
- Réseaux Wi-Fi : *Aircrack-ng*, *Cain* Abel…
- Attaques sur les modems ou War Dialing : ToneLoc
- Surcharge et blocage des ressources : *Ping* de mort, Inondation de SYN, Vol de session

3.2.4.3 Couche Transport

- Découverte des ports TCP et UPD ouverts : SuperScan, *NMAP*
- Attaque des ports communs
- Surpassement du SSL : *SSLstrip*

3.2.4.4 Couche Application

- Système d'exploitation : mots de passe, fichiers systèmes, extension de privilèges, maliciels
- Messageries : email, bannières, messages instantanés…
- Application web : serveur du courrier électronique, intranet
- Application client : Oracle, SQL…

3.2.5 Risques impliqués

Avant de débuter les tests il faut prendre en considération les risques et problèmes pouvant apparaitre lors des attaques pour cela les attaques risqués seront effectués dans un environnement de test répliquant la même architecture de n'importe quel endroit dans l'entreprise. Si des obstacles apparaissent ou des complications surviennent il faut avoir une procédure d'annulation et une solution alternative de récupération.

3.2.6 Exécution des attaques et résultats

3.2.6.1 Couche Accès réseaux

Plusieurs facteurs mènent à l'existence des vulnérabilités physiques, notamment la dimension de l'endroit, nombre de bâtiments, nombre d'employés, nombre des points d'accès et surtout l'emplacement des chambres informatiques. Dans la partie qui suit j'ai divisé les tests physiques selon l'emplacement et suivant deux scenarios : un employé dans l'entreprise à privilèges limités, et un étranger visitant l'entreprise.

a. Objectifs

- Rassembler les informations des branches
- Identifier les failles de sécurité physiques
- Accéder aux ressources non sécurisées

b. Détails d'évaluation

- **HO** : Branche principale déployée dans trois étages où résident les départements administratifs et les serveurs vitaux de l'organisation.
    - Comprend 4 points d'accès contrôlés par des systèmes de cartes d'accès et une réceptionniste à l'entrée.
    - Sept serveurs résident dans une chambre fermée à clé face au bureau de notre département
    - Dans chaque étage il y a un commutateur enfermé dans un rack sécurisé
    - Il y a un point d'accès sans fil dans le premier étage
    - Dans tous les étages il y a des cameras de surveillance dont les enregistrements sont disponibles pour un mois.
    - Dans le premier étage il y a un système de détection de mouvement branché à un système d'appel téléphonique automatisé.
    - Il existe environ 70 utilisateurs travaillant sur leurs propres stations et cinq employés divers

- **DT** : c'est la branche la plus grande parmi les points de ventes, elle comprend un grand magasin et 10 boutiques disséminées sur les bords d'une rue piétonne au center ville de Beirut. Dans cet endroit réside aussi un bâtiment pour les bureaux administratifs déployés sur 3 étages.
    - Le bâtiment administratif comprend 2 points d'accès dont un est contrôlé par une porte sécurisée et l'autre par un agent de sécurité. Chaque étage comprend un système de carte d'accès pour y accéder.
    - Le bâtiment Aishti comprend 3 points d'accès sécurisés par des agents de sécurité
    - Cinq serveurs sont dans une chambre fermée à clé ayant une fenêtre ouverte sur le bureau de notre département qui est sécurisé par un système de carte d'accès.
    - Les racks sont malheureusement dans une chambre ouverte non sécurisée
    - Il y a un point d'accès sans fil dans le restaurant « People » disponible à tous les clients
    - Tous les bureaux et les points de vente sont surveillé par des cameras dont les enregistrements sont disponibles pour un mois.

- Il existe environ 80 utilisateurs travaillant sur leurs propres stations et 200 employés divers

- **SS:** cet emplacement est formé par un bâtiment de 5 étages de points de vente et un bâtiment de bureaux administratifs
  - Le bâtiment administratif comprend 1 point d'accès contrôlé par des cameras de surveillance et système de cartes d'accès
  - Le bâtiment Aishti comprend 3 points d'accès sécurisés par des agents de sécurité
  - Le serveur et tous les appareils informatiques résident dans une chambre non sécurisée mais difficile à localisée par les étrangers
  - Tous les bureaux et les points de vente sont surveillé par des cameras dont les enregistrements sont disponibles pour un mois.
  - Il existe environ 20 utilisateurs travaillant sur leurs propres stations et 100 employés divers

- **WH** : Lieu principal de réception, stockage et distribution des marchandises. Lié par fibre optique au SS
  - Le bâtiment comprend 2 points d'accès surveillés par des cameras dont les enregistrements sont disponibles pour un mois et un agent de sécurité.
  - Serveur et rack situés dans un bureau non sécurisé pendant la journée
  - Il existe 7 utilisateurs travaillant sur leurs propres stations et 30 employés divers

- **CM, VR, ABC, FQ** : Ces branches suivent le même concept concernant l'emplacement des appareillages informatiques et leur sécurisation
  - Chaque branche est formée d'un ou deux étages, ayant 2 points d'accès contrôlés par des agents de sécurité
  - Le serveur et le rack sont situés dans la chambre de stockage
  - Le tout est surveillé par des cameras dont les enregistrements sont disponibles pour un mois.
  - Il existe environ 4 utilisateurs et une vingtaine d'employés dans chaque branche

- **PH,MZ,OA** : ces branches sont des petites boutiques qui ne sont pas liées directement avec le réseau de l'entreprise mais l'accèdent par une connexion sur modem.
    - Chacune des branche a un seul point d'accès non sécurisé par un agent permanent ou des cameras
    - Il n'y a pas un serveur dédié mais un ordinateur contenant la base de données auquel accède l'employé pour facturer

c. Résultats

Les résultats des tests de la couche accès physique obtenus ont dévoilé plusieurs vulnérabilités existantes dans certaines branches :

- Apparemment l'accès physique aux ressources est difficile dans la plus part des branches par rapport aux étrangers. Les ressources vitales sont situées dans des emplacements inaccoutumés, un client ne pourrait jamais deviner ces emplacements. Mais dans le cas d'un employé de l'entreprise ayant une carte d'accès et connu par les réceptionnistes ou les gardes de sécurité le contrôle est plus difficile. Ces employés peuvent accéder aux ressources non verrouillées et essayer d'ajouter des outils d'espionnage ou brancher leurs portables.
- Dans plusieurs branches j'ai pu brancher mon portable dans des prises vides et avoir une connexion avec le réseau
- J'ai trouvé les supports de données dans la branche HO mais conserver dans le bureau du département informatique et difficile à emporter par une personne étrangère.
- Plusieurs utilisateurs laissent leurs ordinateurs non verrouillés ce qui permet à un intrus d'y accéder.
- Des supports de données ont été délaissés sur tables ou dans les poubelles des utilisateurs.
- Dans les branches sur modems, les données ne sont pas sécurisées face aux utilisateurs ou employés, ils peuvent effacer ou détruire les données aisément.

La majorité des résultats dévoilent un environnement physique plutôt sécurisé, l'accès des employés aux ressources est plus aisé par rapport aux étrangers

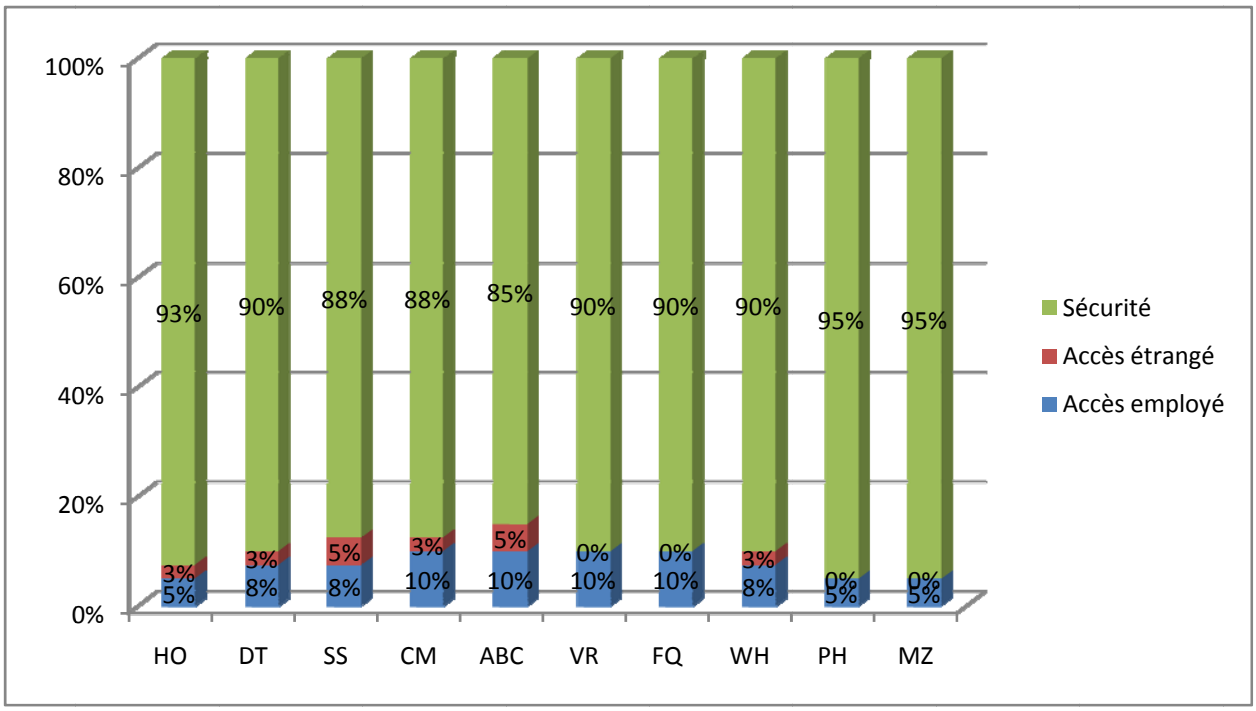


Figure 0.3 : Distribution de sécurisation dans les branches

d. Recommandations

La sécurité physique décrit les mesures qui empêchent ou dissuadent un attaquant d'accéder à un emplacement critique, aux ressources ou aux informations stockées sur des supports physiques. Afin de fortifier cette sécurité plusieurs recommandations sont présentées :

- Toutes les salles informatiques et les racks doivent être verrouillés et les clés réservés dans notre département
- Dans la branche DT il faut changer le positionnement des chambres des racks et des serveurs, ils doivent être sécurisés des dangers humains et naturels
- Il faut vérifier toutes les prises vides et les déconnectées des commutateurs.
- Si possible ajouter des verrous aux portables.
- Créer une interface limitée pour les utilisateurs des branches sur modem.
- Instruire les employés des recommandations de sécurité : verrouiller leurs ordinateurs, détruire les medias avant de les jetés, ne pas dévoiler des informations sur l'entreprise…

3.2.6.2 Couche Internet

Tout système informatique exige l'existence d'un système de communication fondamentale ou « réseau » pour fonctionner. Ce réseau est formé d'un ensemble de périphériques : routeurs, commutateurs, modems, pare-feu… Cette partie couvre les attaques permettant la découverte et pénétration de ce réseau et manipulation des ressources vitales.

a. Objectifs :

- Balayage et analyse du réseau
- Pénétration des périphériques du réseau
- Tests de surcharge et blocage des ressources

b. Détail d'évaluation

b.1 Balayage et analyse du réseau

La première phase consiste à découvrir l'architecture du réseau et l'emplacement des périphériques principaux de l'organisation. Il faut essayer plusieurs outils de balayage à partir d'un poste de client étranger à ce réseau ayant passé l'étape d'accès physique de l'intérieur de l'organisation ou de l'internet, ou d'un employé possédant un ordinateur branché et essayant d'accéder aux ressources vitales de l'entreprise.

Il existe trois genres de scanneurs : ports, réseaux et vulnérabilités, tous basés sur le principe d'envoie des requêtes spécifiques sur tous les adresses dans un réseau, ayant pour effet un comportement anormal et analysant ensuite les paquets réponses retournés.

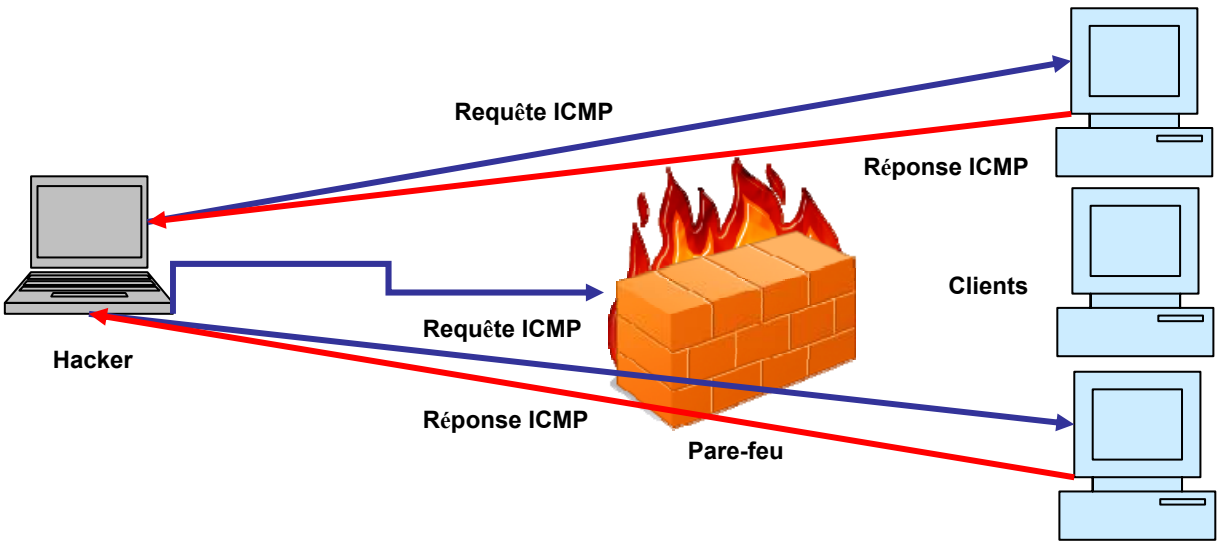
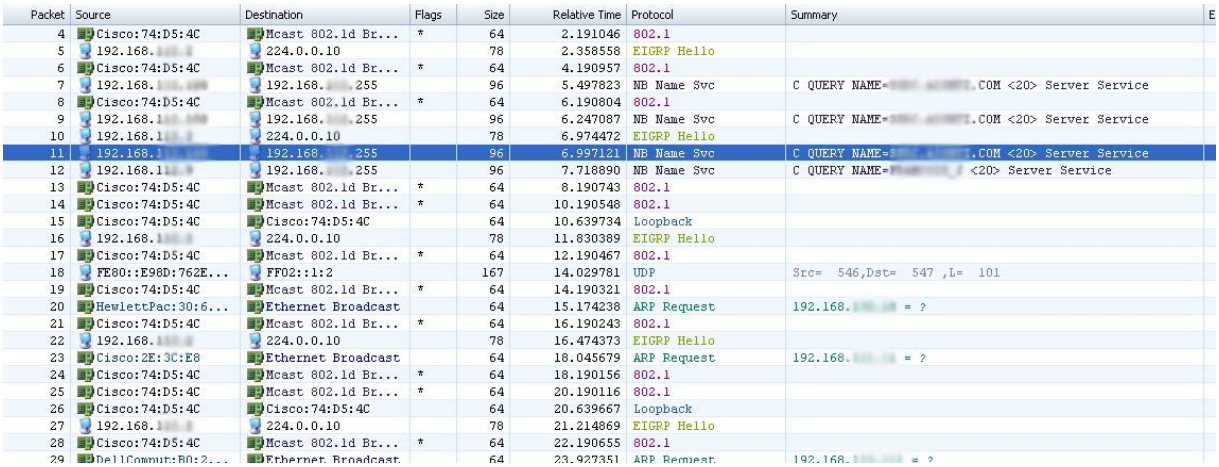


Figure 0.4 : Méthodologie générale des scanneurs

Dans cette étape j'ai effectué les tests à partir d'un portable étranger par rapport au réseau n'ayant ni adresse IP ni connecté au domaine de l'organisation. Les outils principaux utilisés sont *Omnipeek*, *GFI LanGuard* et *LanSpy*. Ces outils de captages recueillent tous les paquets passants sur le réseau et analysent leurs origines et leurs types. Comme le montre les schémas ci-dessous, les requêtes passantes sur le réseau dévoilent les rangées d'adresse IP utilisées, le routeur, le serveur et l'identité de quelques postes



Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary
4	Cisco:74:D5:4C	Mcast 802.1d Br...	*	64	2.191046	802.1	
5	192.168.	224.0.0.10		78	2.358558	EIGRP Hello	
6	Cisco:74:D5:4C	Mcast 802.1d Br...	*	64	4.190957	802.1	
7	192.168.	192.168. 255		96	5.497823	NB Name Svc	C QUERY NAME= .COM <20> Server Service
8	Cisco:74:D5:4C	Mcast 802.1d Br...	*	64	6.190804	802.1	
9	192.168.	192.168. 255		96	6.247087	NB Name Svc	C QUERY NAME= .COM <20> Server Service
10	192.168.	224.0.0.10		78	6.974472	EIGRP Hello	
11	192.168.	192.168. 255		96	6.997121	NB Name Svc	C QUERY NAME= .COM <20> Server Service
12	192.168.	192.168. 255		96	7.718890	NB Name Svc	C QUERY NAME= <20> Server Service
13	Cisco:74:D5:4C	Mcast 802.1d Br...	*	64	8.190743	802.1	
14	Cisco:74:D5:4C	Mcast 802.1d Br...	*	64	10.190548	802.1	
15	Cisco:74:D5:4C	Cisco:74:D5:4C		64	10.639734	Loopback	
16	192.168.	224.0.0.10		78	11.830389	EIGRP Hello	
17	Cisco:74:D5:4C	Mcast 802.1d Br...	*	64	12.190467	802.1	
18	FE80::E98D:762E...	FF02::1:2		167	14.029781	UDP	Src= 546,Dst= 547 ,L= 101
19	Cisco:74:D5:4C	Mcast 802.1d Br...	*	64	14.190321	802.1	
20	HewlettPac:30:6...	Ethernet Broadcast		64	15.174238	ARP Request	192.168. = ?
21	Cisco:74:D5:4C	Mcast 802.1d Br...	*	64	16.190243	802.1	
22	192.168.	224.0.0.10		78	16.474373	EIGRP Hello	
23	Cisco:2E:3C:E8	Ethernet Broadcast		64	18.045679	ARP Request	192.168. = ?
24	Cisco:74:D5:4C	Mcast 802.1d Br...	*	64	18.190156	802.1	
25	Cisco:74:D5:4C	Mcast 802.1d Br...	*	64	20.190116	802.1	
26	Cisco:74:D5:4C	Cisco:74:D5:4C		64	20.639667	Loopback	
27	192.168.	224.0.0.10		78	21.214869	EIGRP Hello	
28	Cisco:74:D5:4C	Mcast 802.1d Br...	*	64	22.190655	802.1	
29	DellComput:B0:2...	Ethernet Broadcast		64	23.927351	ARP Request	192.168. = ?

Figure 0.5 : Résultat du captage du trafic par *OmniPeek*

Une fois les rangés d'adresses IP ont été dévoilées j'ai donné au portable une adresse IP convenable dans les rangées trouvées dans chaque branche et effectué les tests de balayage détaillé du réseau.

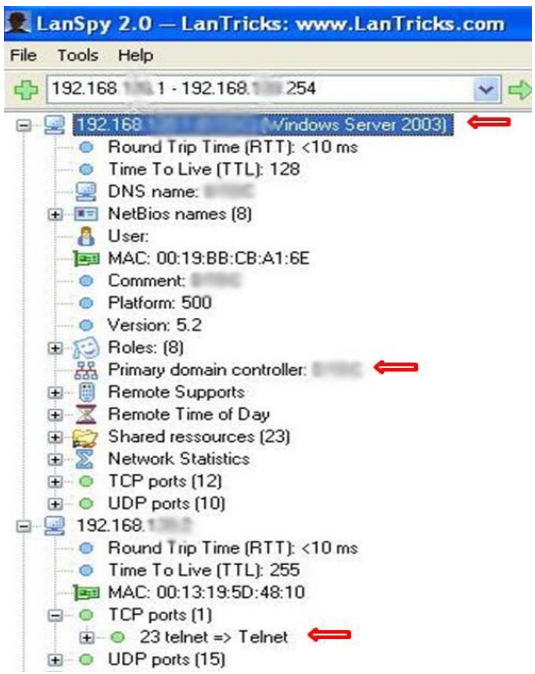


Figure 0.6 : Résultat du balayage d'une rangée d'adresse IP avec *LanSpy*

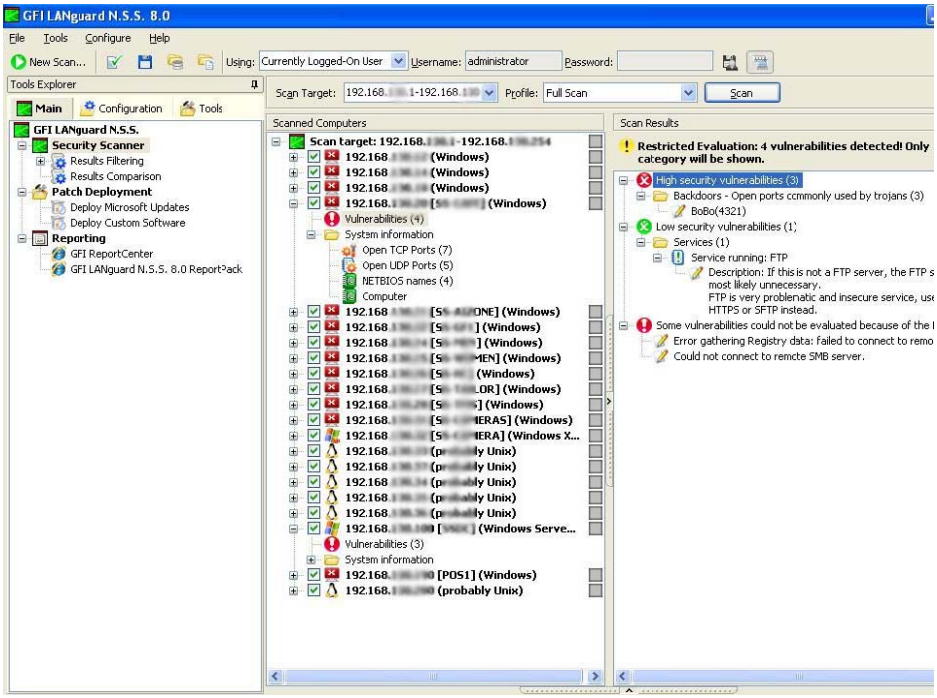


Figure 0.7 : Résultat du balayage d'une rangée d'adresse IP avec *GFI LanGuard*

L'exécution de ces outils dans différentes branche dévoile l'architecture complète du réseau :

- Rangées d'adresse IP utilisées
- Liste des utilisateurs
- Point d'accès Wi-Fi / Routeurs / commutateurs / pare-feu
- SE, services actives et vulnérabilités présentes

Les graphes suivants récapitulent les résultats des sévérités obtenues par branches :

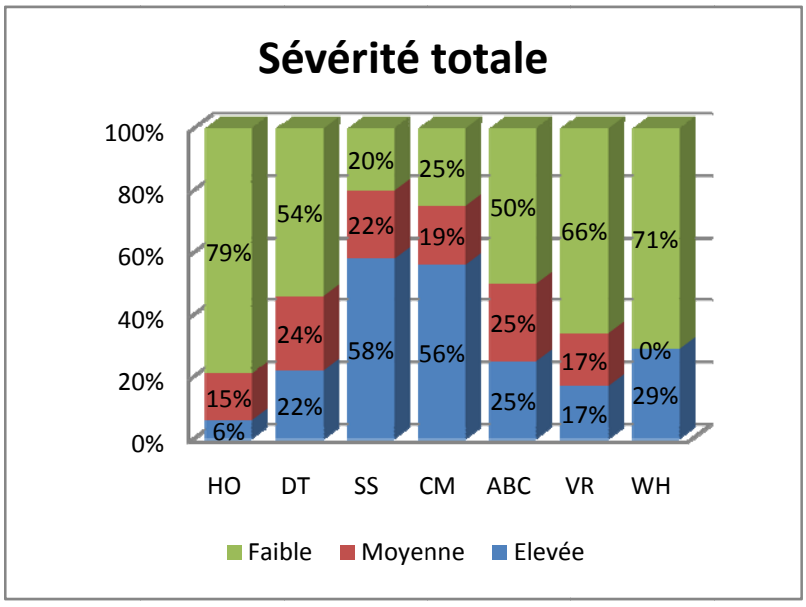


Figure 0.8 : Sévérité totale dans les branches principales

Les deux branches principales ont plutôt une sévérité totale faible, mais quelques branches présentent des vulnérabilités plutôt élevées dont il faut prendre en considération.

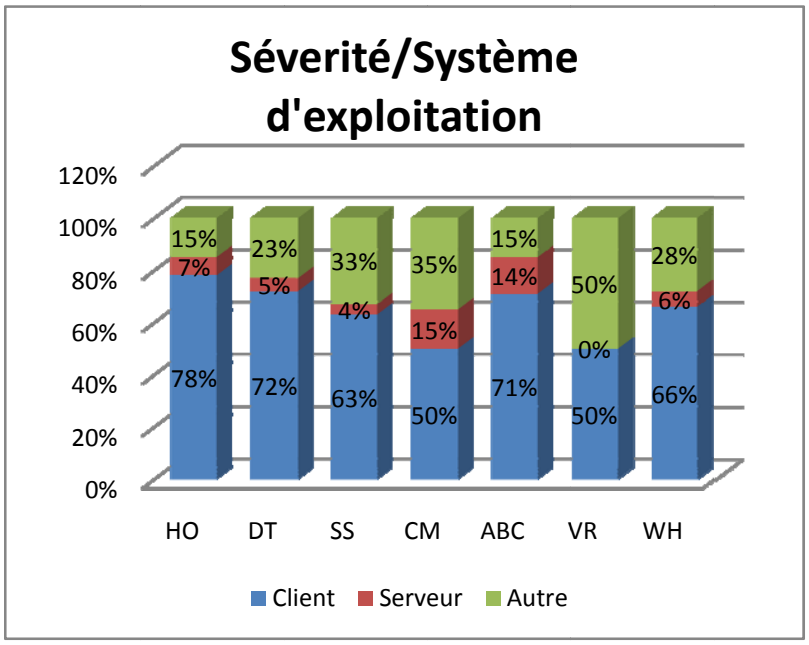


Figure 0.9 : Sévérité par SE

Les postes clients représentent la majorité des sévérités des SE, mais n'empêche l'importance des vulnérabilités existantes dans les serveurs comprenant les ressources importantes de l'organisation.

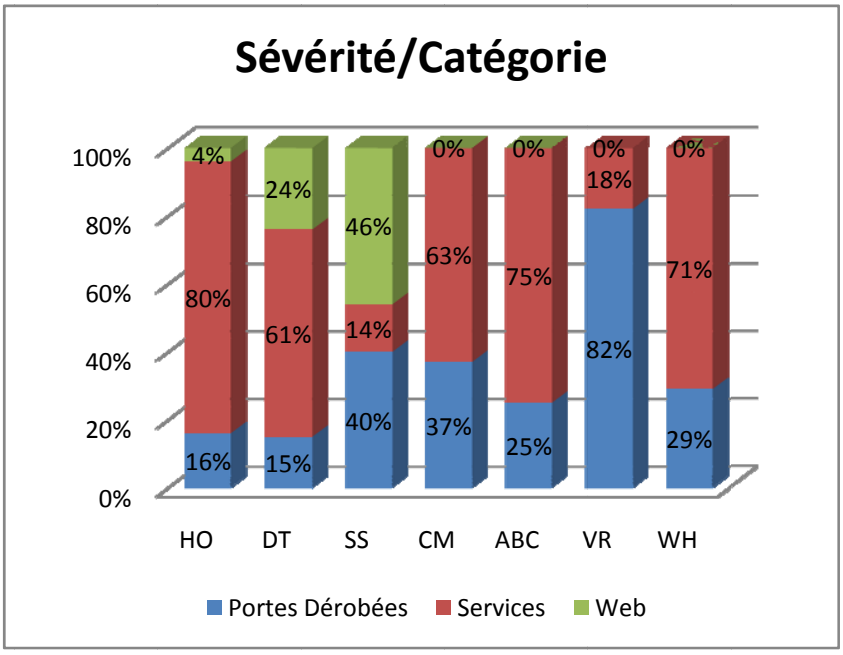


Figure 0.10 : Sévérité par catégorie de vulnérabilité

Les services fonctionnant dans les postes clients, serveurs ou sur les périphériques du réseau constituent la majorité des vulnérabilités existantes, il faut par la suite les contrôler pour minimiser leurs impacts.

Suite aux tests effectués les cibles de la couche internet à visées seront :

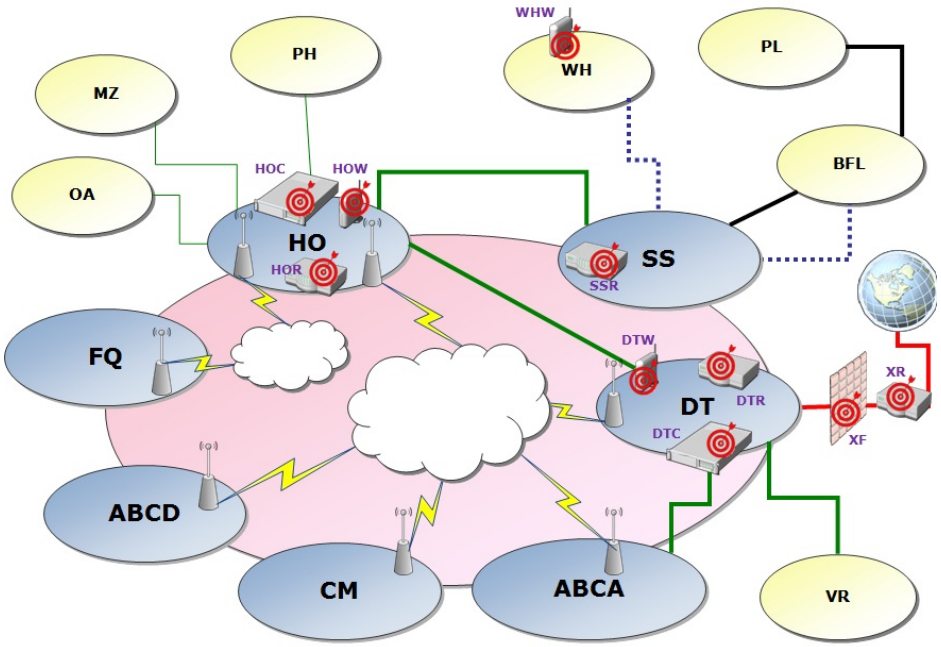


Figure 0.11 : Points d'attaque à visés dans le réseau

Table 0-III : Périphériques cibles de la couche internet

Branche	HO	DT	SS	WH	DMZ
Routeur	HOR	DTR	SSR		XR
Commutateur	HOC	DTC			
Point d'accès wifi	HOW	DTW		WHW	
Pare-feu					XF

b.2 Pénétration des périphériques du réseau

Cette deuxième phase consiste à pénétrer les périphériques du réseau et essayer d'élever les privilèges acquis afin de manipuler les configurations existantes. Les tests seront effectués d'un portable branché au réseau ayant une adresse IP des rangés d'adresses dévoilées dans la phase précédente, mais qui n'est pas membre du domaine et n'ayant aucun identifiant de ce domaine. Les tests effectués auparavant révèlent les informations nécessaires des cibles choisies :

Table 0-IV : Détails des cibles à attaquer

	Services	Ports TCP	Ports UDP
HOR	TELNET	23, 1720	67, 161, 162, 1985
HOC	HTTP, TELNET	23, 80	67, 161, 162, 1985
HOW	HTTP, HTTPS	80, 443	88, 123, 138, 3127…
DTR	TELNET	23, 1720	42, 53, 67, 88, 520, 4500
DTC	HTTP, TELNET	23, 80	42, 53, 67, 88, 520, 4500
DTW	HTTP, HTTPS	80, 443	161, 389, 520, 3127…
SSR	TELNET	23, 1720, 5060	161, 162, 1975, 2104, 5060
WHW	HTTP, HTTPS	80, 443	42, 53, 67, 88, 520, 4500
XR	212.98.X.X	22, 23	42, 53, 88, 389, 4500
XF	192.168.X.X	22	

- **SSR et HOR :**

Ces routeurs comprennent quelques ports TCP ouverts : 23 (Telnet), 1720 (H323. Hostcall) et 5060 (sip). J'ai essayé d'abord de connaitre le SE par l'outil *NMAP* sur un des ports ouverts 1720 et j'ai obtenu ainsi la version du SE.

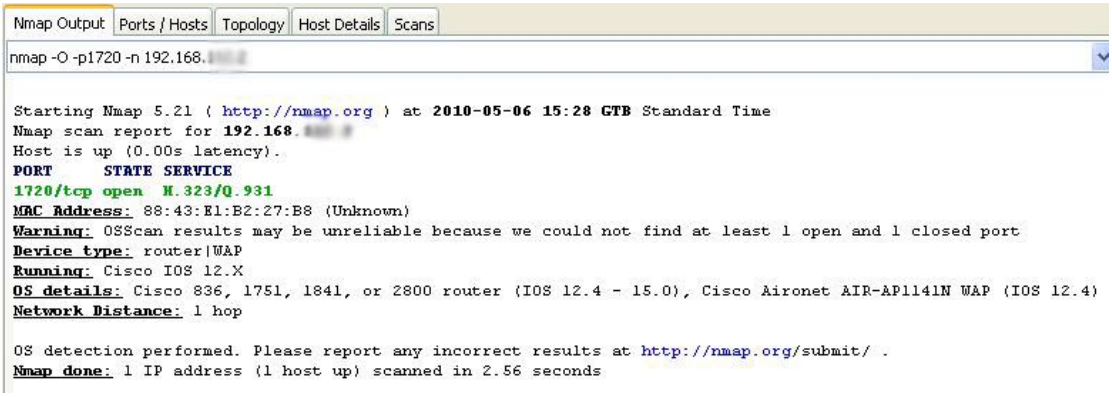


Figure 0.12 : Résultat *NMAP* sur SSR

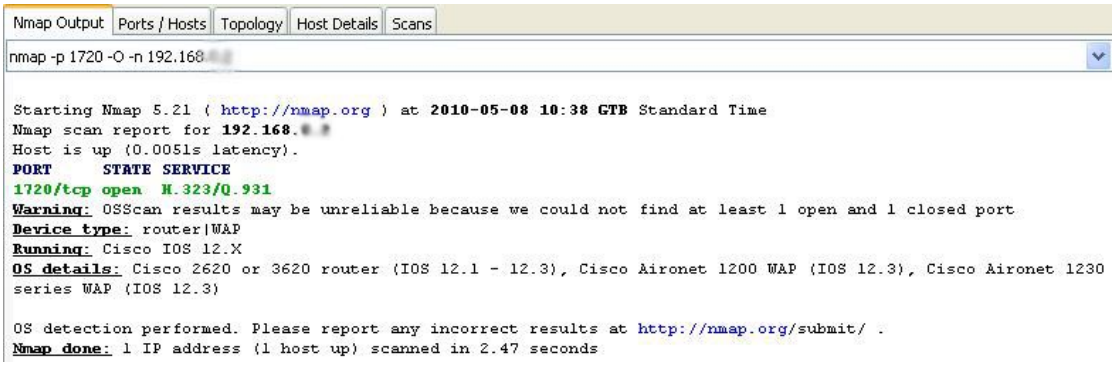


Figure 0.13 : Résultat *NMAP* sur HOR

J'ai essayé l'ouverture d'une session Telnet avec le mot de passe par default « cisco » est j'ai pu accéder avec des privilèges administratifs.

Résultat : Routeurs compromis, privilèges administratifs acquis.

- **DTR :**

Ce routeur comprend deux ports TCP ouverts : 23 (Telnet) et 1720 (H323. Hostcall). J'ai essayé d'abord de connaitre le SE par l'outil *NMAP* sur un des ports ouverts 1720 et j'ai obtenu ainsi la version du SE.

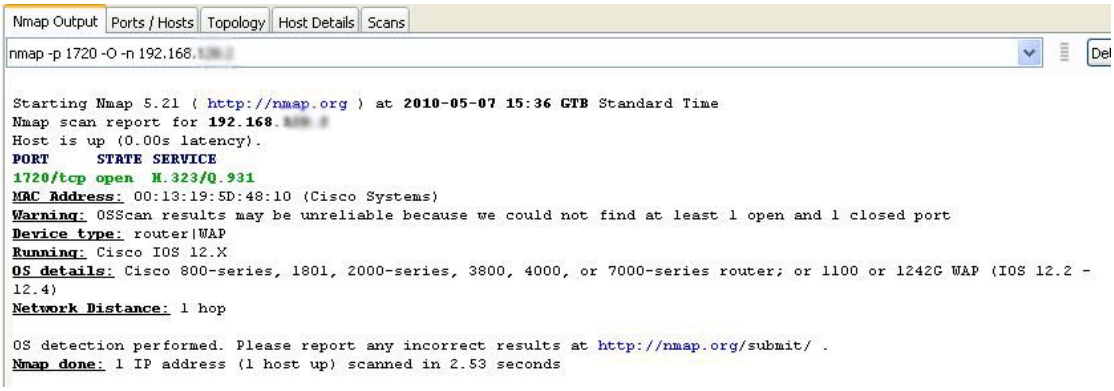


Figure 0.14 : Résultat *NMAP* sur DTR

Le but est d'avoir le mot de passe afin d'accéder au fichier de configuration. J'ai essayé Telnet avec le mot de passe par default « cisco » mais je n'ai pas pu accéder. Arrivant à ce point il existe deux options pour pouvoir pénétrer ce routeur :

- **HTTP :** Pour manipuler l'adresse URL

  Comme le port TCP 80 dédié pour les connexions HTTP est fermé, cette méthode ne marchera pas sur ce routeur.
- **SNMP** : Pour gérer le dispositif

  Pour ouvrir une connexion SNMP avec le routeur il faut savoir les *community string* (CS) existants, ils sont de deux type : Lire (Read Only), Lire/Ecrire (Read/Write). L'exécution de l'outil *SNMP Brute Force Attack* dévoile un CS « aiXXX » avec accès Lire. L'utilisation ensuite de l'outil *IP Network Browser* avec ce CS aperçoit une partie du fichier de configuration. Aucun CS avec accès Lire/Ecrire a été découvert.

Résultat : Routeur non compromis

- **XR :**

Ce routeur est le point d'accès externe de l'internet vers l'entreprise. Les tests seront effectués de l'extérieure à partir d'un portable lié directement à l'internet.

La première phase consiste à trouver l'adresse IP de ce routeur. Une recherche du domaine de l'entreprise sur internet retourne des informations sur un sous-domaine du serveur des messageries. C'est un bon point de départ pour suivre le chemin vers l'intérieur du réseau.

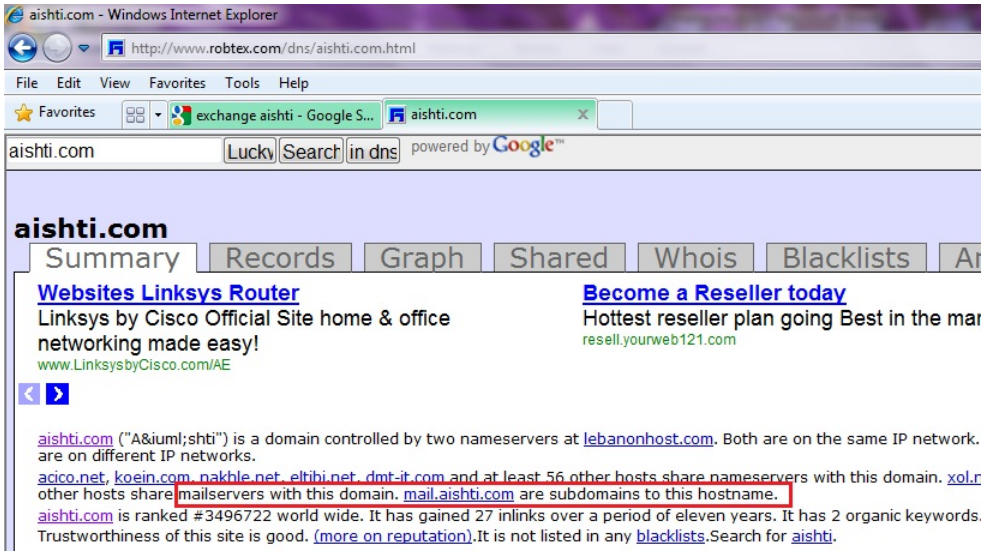


Figure 0.15 : Recherche du domaine sur internet

La deuxième phase consiste à suivre les traces aboutissant à : *mail.aishti.com* à l'aide de la commande *tracert*

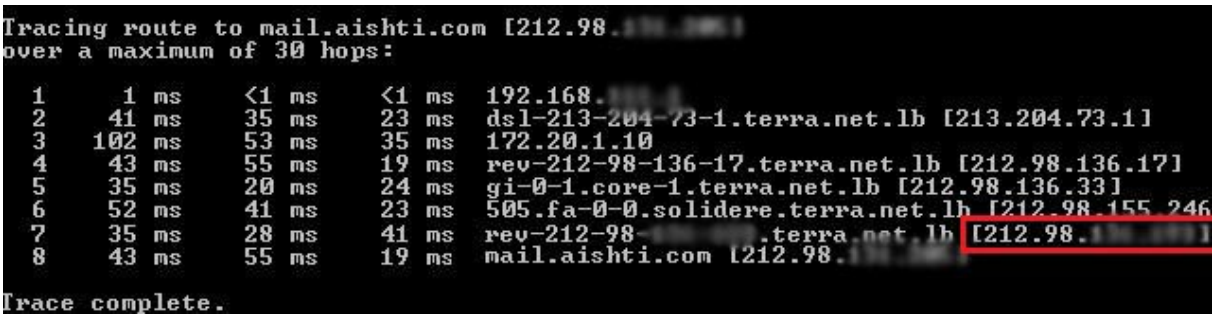


Figure 0.16 : Route de l'internet vers *mail.aishti.com*

Comme le montre la figure, l'adresse aboutissant au serveur recherché est probablement l'adresse du routeur externe de l'entreprise. Pour s'assurer j'ai utilisé *NMAP* pour découvrir le SE. Effectivement le résultat obtenu a confirmé que c'est un routeur *Cisco*.

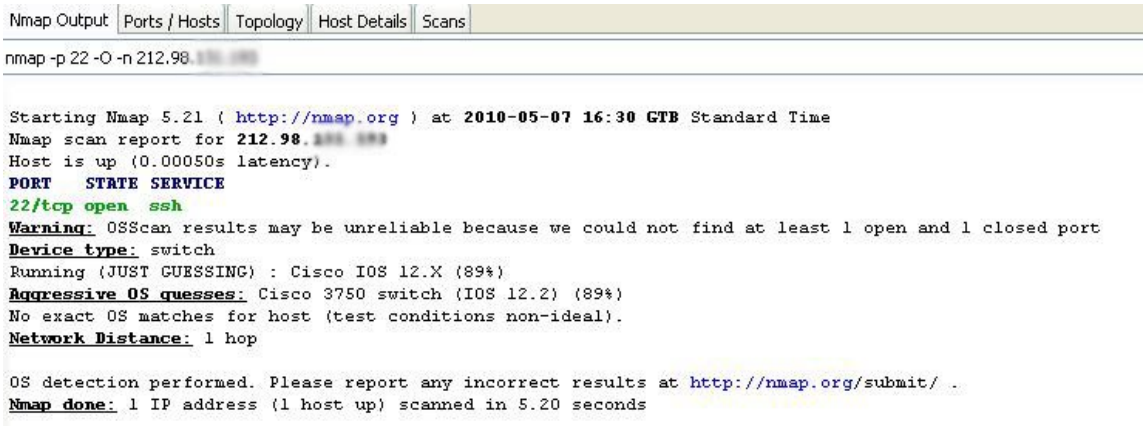


Figure 0.17 : Résultat *NMAP* sur XR

L'étape suivante est la découverte des ports accessible à travers l'outil *LanSpy*. Cet outil a dévoilé aussi l'existante d'une porte dérobée (3127) a but malicieux. Comme le port 23 est ouvert, j'ai essayé Telnet avec le mot de passe par default « cisco » est j'ai pu accéder avec des privilèges administratifs.

Figure 0.18 : Résultat *LanSpy* sur XR

Résultat : Routeur compromis, privilèges acquis pour changer les configurations du système

- **DTC :**

Ce commutateur comprend deux ports TCP ouverts : 23 (Telnet) et 80 (HTTP). J'ai essayé d'abord de connaitre le SE par l'outil *NMAP* sur un des ports ouverts 23 et j'ai obtenu ainsi la version du SE.

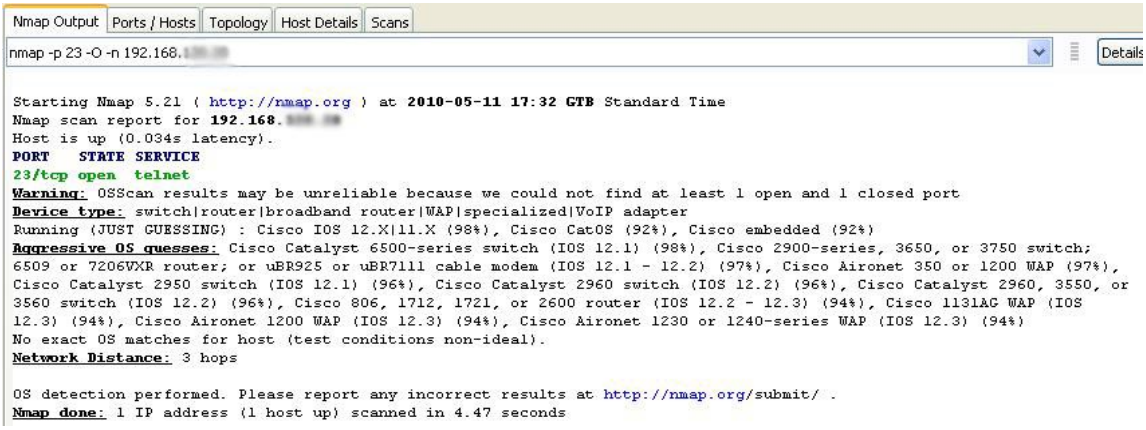


Figure 0.19 : Résultat *NMAP* sur DTC

Le but est d'accéder au fichier de configuration. Comme le port 23 est ouvert, j'ai essayé Telnet avec le mot de passe par default « cisco » est j'ai pu accéder avec des privilèges administratifs !

Résultat : Commutateur compromis, privilèges acquis pour changer les configurations du système

- **HOC:**

Ce commutateur comprend deux ports TCP ouverts : 23 (Telnet) et 1720 (H323. Hostcall). J'ai essayé d'abord de connaitre le SE par l'outil *NMAP* sur un des ports ouverts 23 et j'ai obtenu ainsi sa version.

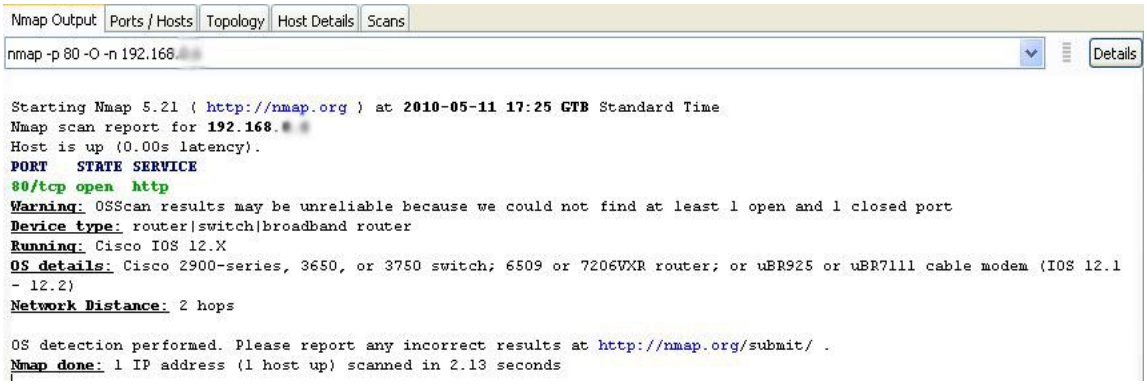


Figure 0.20 : Résultat *NMAP* sur HOC

Le but est d'avoir le mot de passe afin d'accéder au fichier de configuration. J'ai essayé Telnet avec le mot de passe par default « cisco » mais je n'ai pas pu accéder.

Arrivant à ce point il existe deux options pour pouvoir pénétrer ce routeur :

- **HTTP :** Pour manipuler l'adresse URL

  J'ai essayé d'abord l'accès à travers l'URL regulier sur le port 80 *http*://192.168.X.X mais j'ai eu le message d'identification dont je n'ai pas le nom ou mot de passe. J'ai alors manipulé l'adresse URL comme suit :

  http://192.168.X.X/level/99/exec/show/config

  Mais aussi le message d'identification apparu. Donc cette méthode est bien sécurisée

- **SNMP** : Pour gérer le dispositif

  Pour ouvrir une connexion SNMP avec le routeur il faut savoir les CS ou CS existants, ils sont de deux type : Lire (Read Only), Lire/Ecrire (Read/Write). L'exécution de l'outil *SNMP Brute Force Attack* dévoile un CS « dataXXX » avec accès Lire. L'utilisation ensuite de l'outil *IP Network Browser* avec ce CS aperçoit une partie du fichier de configuration. Aucun CS avec accès Lire/Ecrire a été découvert.

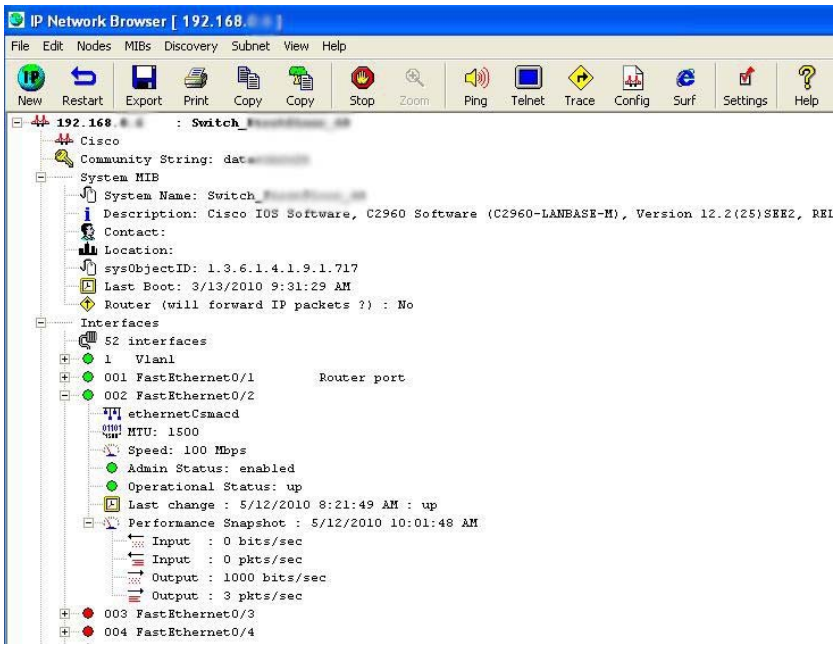


Figure 0.21 : Résultat *IP Network Browser* sur HOC

Résultat : Commutateur non compromis

- **DTW :**

Dans la branche DT, il existe un point d'accès sans fil installé pour les clients du restaurant. J'ai essayé de me connecter, aucun mot de passe ou clé WEP est demandée et j'ai obtenu une adresse IP de la rangée des adresses de cette branche.

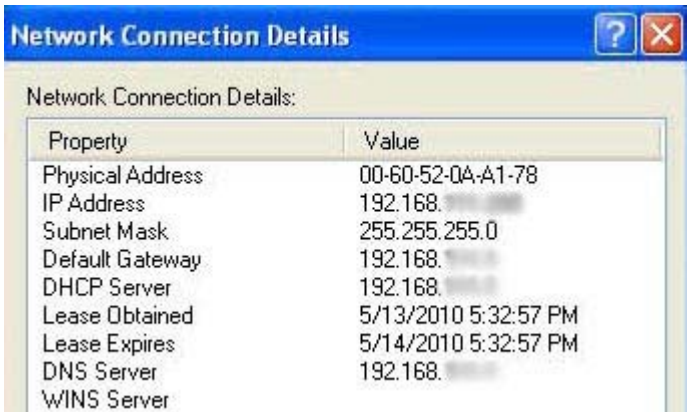


Figure 0.22 : Configuration automatique obtenu du point d'accès DTW

A ce point j'ai essayé d'accéder aux principaux équipements de cet endroit, mais je n'ai pu faire aucun contact avec l'une des adresses IP dans la rangée trouvée. J'ai essayé ensuite d'accéder au point d'accès à travers l'interface HTTP, mais les identifiants par default n'ont pas marché.

Résultat : Point d'accès non compromis

- **WHW :**

Il existe dans cette branche un point d'accès pour les utilisateurs mobiles. Il comprend une clé WEP dont j'ai compromis avec l'outil *Aircrack-ng*.

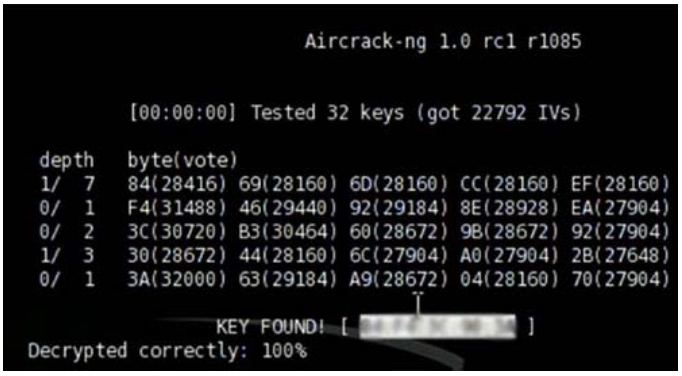


Figure 0.23 : WHW clé compromise

Une fois connectée j'ai obtenue une adresse appartenant au réseau et pu communiquer avec les périphériques. J'ai essayé ensuite d'accéder au point d'accès à travers l'interface HTTP, mais les identifiants par default sont incorrectes.

Résultat : Accès au réseau réussi, mais point d'accès non compromis

- **HOW :**

Dans la branche principale HO, il existe un point d'accès sécurisé, l'outil *Aircrack-ng* n'a pas réussi de compromettre la clé WEP, apparemment c'est une clé sur 128 bits et compliquée.

Résultat : Point d'accès non compromis

- **XF :**

XF représente le pare-feu externe de l'organisation, séparant le réseau internet du réseau interne de l'organisation. L'outil *NMAP* dévoile le port tcp 22 ouvert. L'essai d'accéder ce pare-feu par les protocoles FTP, HTTP et SNMP n'a pas réussi.

Les mêmes tests ont été effectués à partir du réseau interne et aucune communication avec le pare-feu n'a réussie.

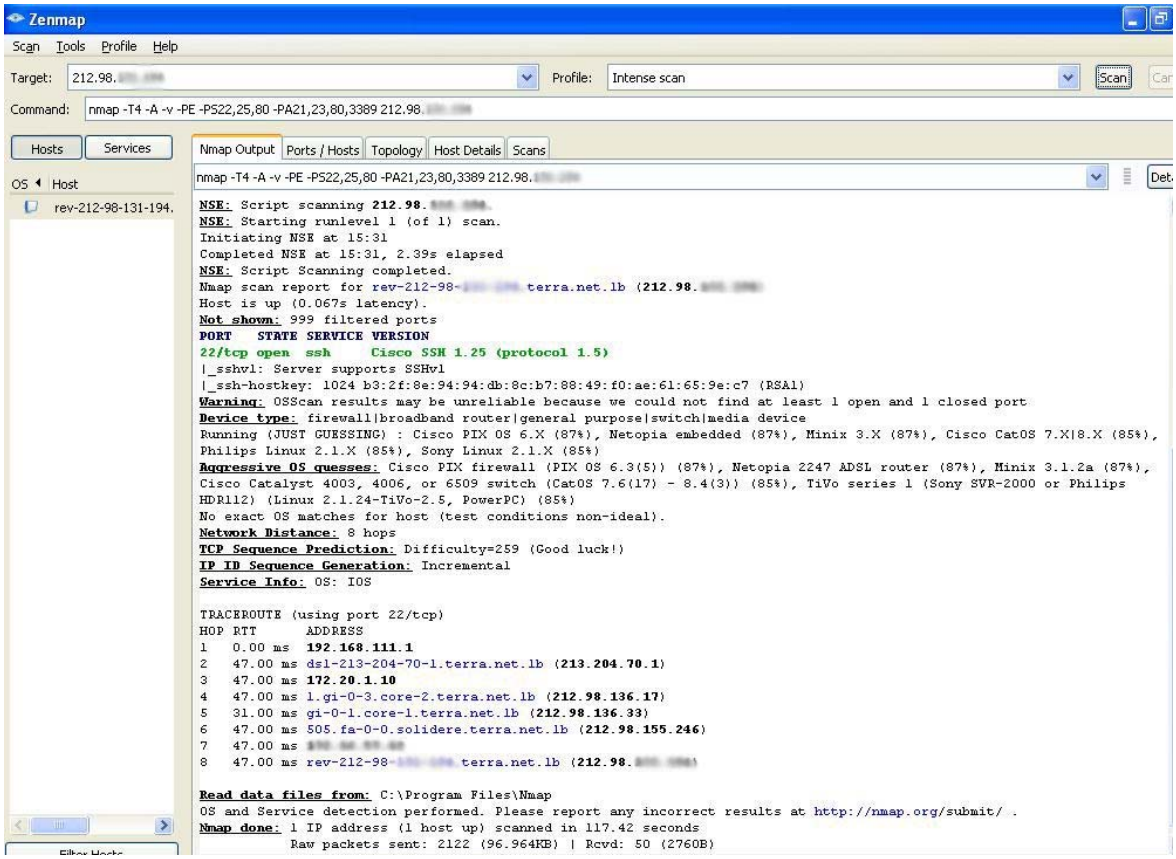


Figure 0.24 : Résultat *NMAP* sur XF

Résultat : Pare-Feu non compromis

- **Attaque sur les modems : War dialing**

La première étape de l'attaque sur les modems consiste à découvrir le numéro de téléphone lié au modem. L'outil *ToneLoc* effectue un balayage sur une liste de numéro et dévoile ceux qui sont connectés au modem.

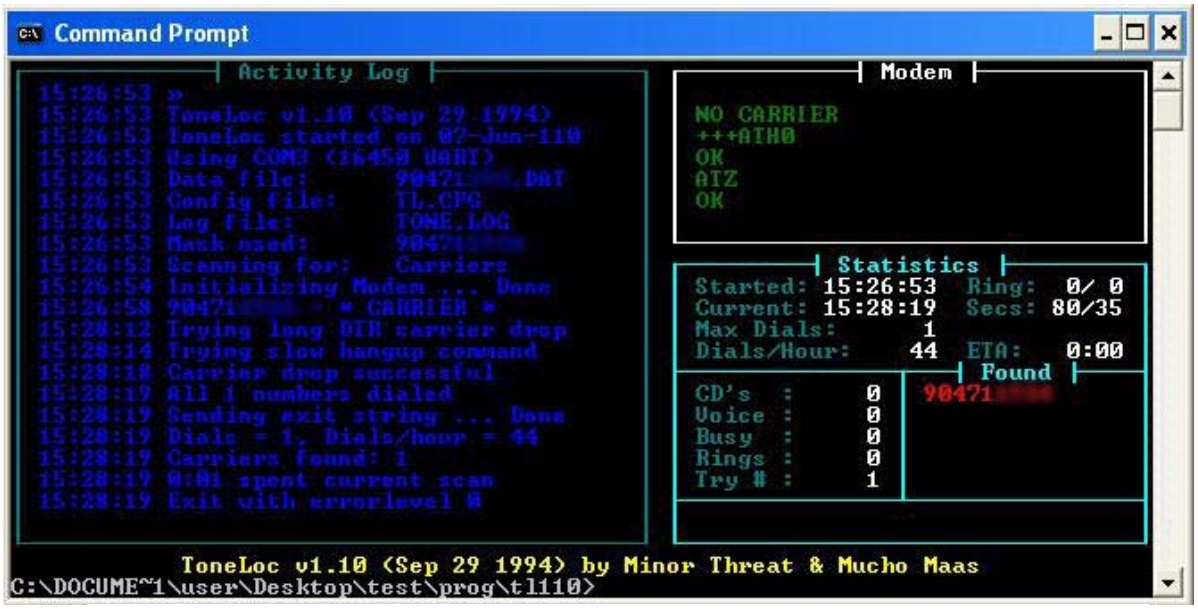


Figure 0.25 : Résultat *ToneLoc* sur le modem

La connexion de l'outil *hyper terminal* avec le modem utilisant le numéro découvert a réussi. Mais aucun transfert de données n'est passé d'un côté à l'autre. Une autre connexion directe pour accéder au réseau n'a pas réussi car il faut avoir les identificateurs corrects.

Résultats de pénétration des périphériques du réseau:

Les tests conduits dévoilent plusieurs risques et vulnérabilités menaçant les ressources pertinentes de l'organisation. Néanmoins on ne peut négliger les mesures de sécurité actuelles qui éliminent une partie majeure des risques possibles. Le tableau et le schéma ci-dessous récapitulent les résultats de ces tests :

Table 0-V : Résultats des tests sur les périphériques du réseau

	Date du test	Vulnérabilités / Etat	Risques / Impact	Résultat
HOR	8/5/2010	Ports TCP accessibles Mots de passe par default	Etat Critique Accessibilité facile	compromis
HOC	11-12/5/2010	Ports TCP accessibles Accès HTTP et SNMP sécurisé	Etat acceptable	Non compromis
HOW	19/5/2010	Diffusion de signal permis Clé WEP complexe sur 128bits	Accès au réseau interne	Non compromis
DTR	8/5/2010	Ports TCP accessibles Accès HTTP et SNMP sécurisé	Etat acceptable	Non compromis
DTC	8/5/2010	Ports TCP accessibles Mots de passe par default	Etat Critique Accessibilité facile	compromis
DTW	13/5/2010	Diffusion de signal permis Pas de clé WEP Attribution d'adresse IP (hors rangée privée)	Accès au réseau interne	Non compromis
SSR	6/5/2010	Ports TCP accessibles Mots de passe par default	Etat Critique Accessibilité facile	compromis
WHW	18/5/2010	Diffusion de signal permis Clé WEP non complexe	Accès au réseau interne effectué	Non compromis
XR	10/5/2010	Ports TCP accessibles Mots de passe par default	Accès critique majeur de l'internet vers l'intérieur	compromis
XF	2/6/2010	Un seul port 22 ouvert mais non accessible	Accès critique majeur de l'internet vers l'intérieur	Non compromis

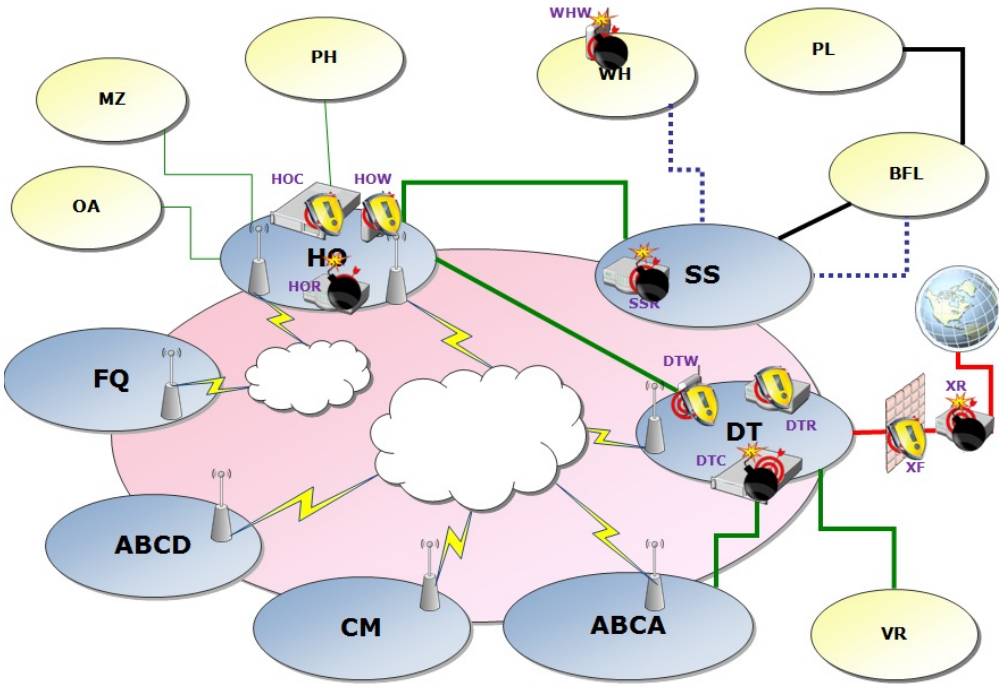


Figure 0.26 : Résultats schématisé des tests sur les périphériques du réseau

b.3 Surcharge et blocage des ressources

Pour tester la rigidité des périphériques il faut les attaquer suivant plusieurs stratégies et outils afin de surcharger et désactiver leurs services et par suite bloquer l'accès aux ressources pertinents. Les attaques suivantes ont été effectuées dans un environnement prototype de test similaire à l'environnement réel de l'organisation, comprenant un serveur de base de données, un ordinateur client, un routeur ayant la même configuration de SSR et enfin un portable étranger à partir duquel j'effectue les attaques.

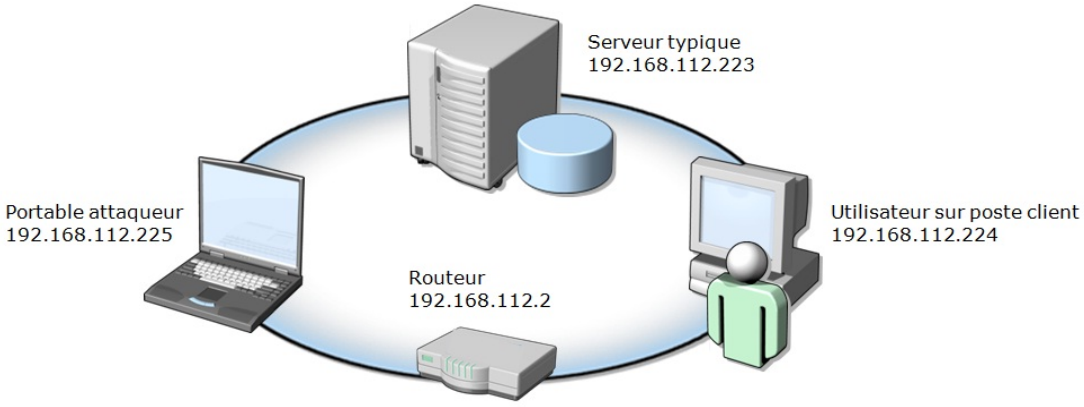


Figure 0.27 : Environnement test des attaques

- **Denis de Service (DoS) :**

Cette attaque vise à rendre un ordinateur, notamment un serveur, hors service en surchargeant ses ressources par un trafic inutile. Le but d'une telle attaque n'est pas de voler ou manipuler les données, mais de nuire au fonctionnement de l'entreprise victime et par suite offenser sa réputation dans le marché. L'attaque n'est pas compliquée, elle consiste à envoyer des paquets IP afin de provoquer une saturation ou un état instable des machines victimes, elle est valable sur différents SE car elle exploite les failles liées au protocole TCP.

L'attaque par dénis de service fonctionne suivant plusieurs façons :

- Inondation du réseau empêchant l'accès légitime du trafic sur le réseau
- Perturber la connexion entre deux machines empêchant l'accès aux services
- Empêche une personne particulière d'accéder à un certain service
- Perturber le service d'un système

Il existe deux types de dénis de service, la première par saturation, consiste à submerger une machine de requêtes afin qu'elle ne soit plus capable de répondre aux requêtes réelles, et la deuxième une variante de l'attaque par plusieurs dénis de service en parallèles appelée Denis de Service Distribué (DDoS) schématisée ci-dessous :

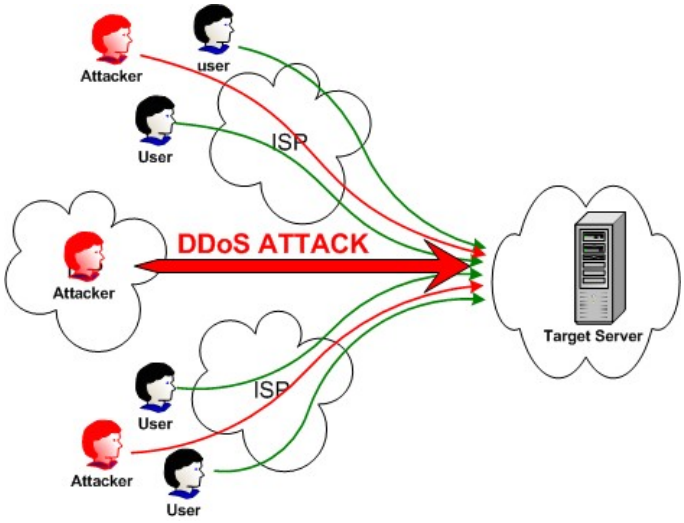


Figure 0.28 : Dénis de service distribué
Référence : *http://*nsl.cs.columbia.edu/projects/sos/

- **Inondation par Ping (Ping flood)**

C'est une attaque par saturation, elle consiste à utiliser la commande *ping* standard pour envoyer des paquets volumineux de type *Internet Contrôle Message Protocol* (ICMP). Cette action peut provoquer le blocage ou le plantage des systèmes qui sont incapables de gérer de telles anomalies.

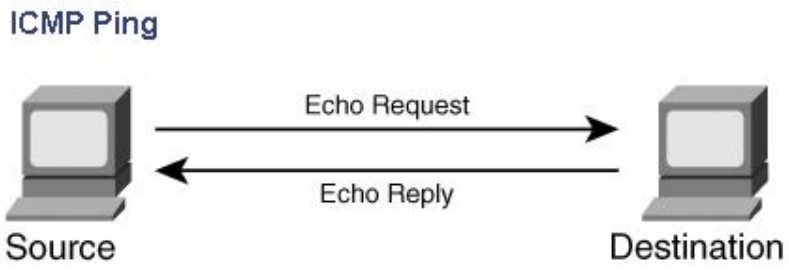


Figure 0.29 : Commande ping normale
Référence : *http://*swordfish.wordpress.com/2006/03/16/denial-of-service-attacks-dos

Application

La mise en pratique de cette attaque est effectuée par la commande suivant à partir du portable : **Ping 192.168.112.223 –t –l 65500**

Durant une heure et demi cette attaque a causé d'abord le ralentissement du réseau et enfin le blocage des ressources du serveur. Les images qui suivent montrent l'état de la carte réseau du serveur dans un intervalle de 30 min.

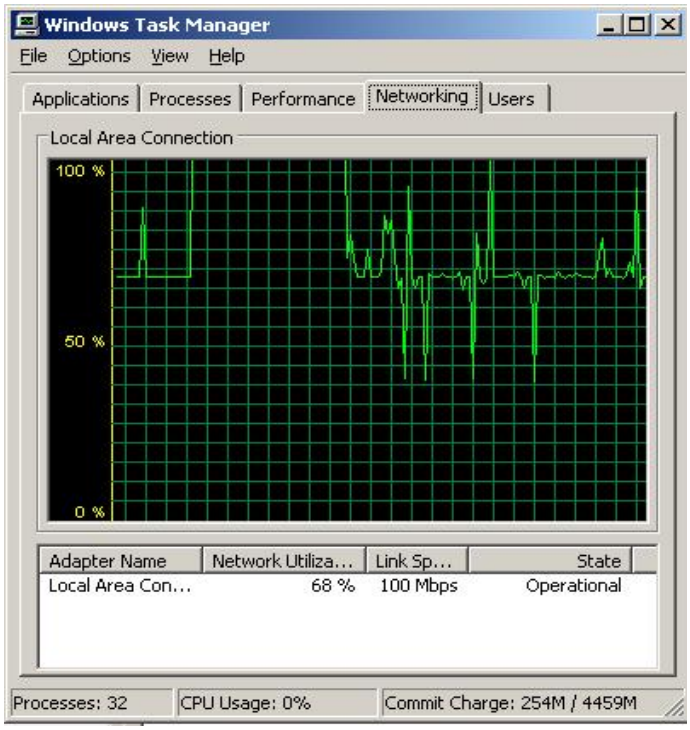


Figure 0.30 : Etat de la carte réseau après 30 min (65%chargé)

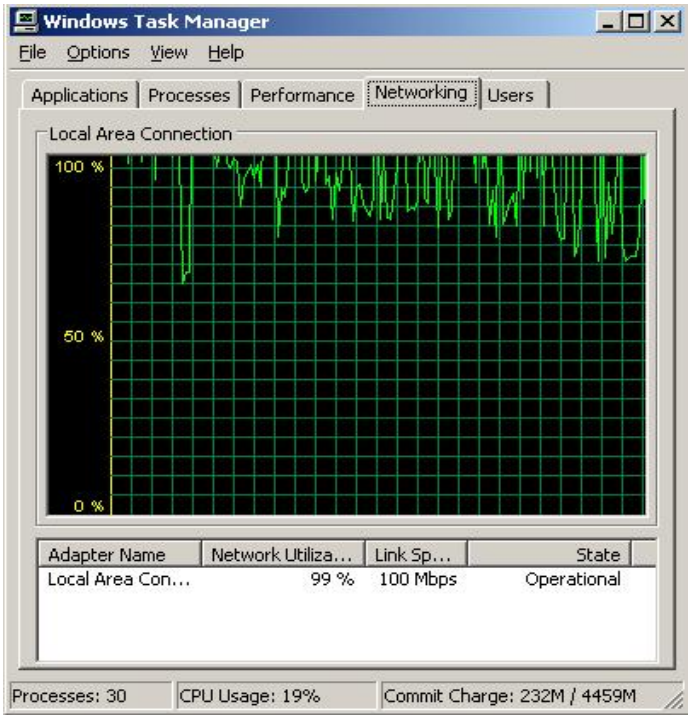


Figure 0.31 : Etat de la carte réseau après 60 min (85% chargé)

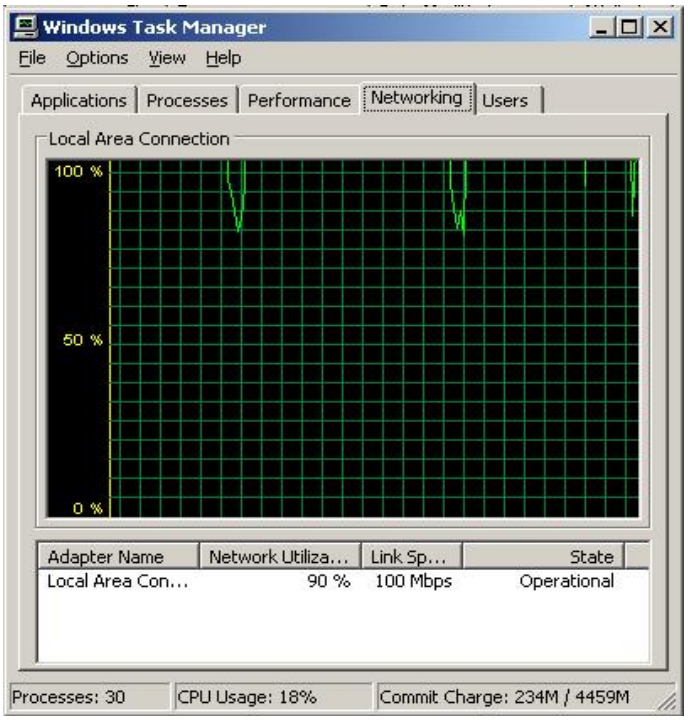


Figure 0.32 : Etat de la carte réseau après 90 min (>100% chargé)

- **Inondation par SYN (SYN Flood)**

Cette attaque consiste à envoyer plusieurs demandes de connexions TCP afin de capter les ressources d'un serveur. Elle exploite le mécanisme de poignée de main en trois (three-ways handshake) du protocole TCP utilisé pour initialiser une connexion fiable à l'Internet selon trois étapes SYN – ACK/SYN – ACK. L'attaque SYN consiste à envoyer un grand nombre de requêtes SYN avec une adresse IP source invalide sans le message ACK laissant ainsi la connexion semi-ouverte, ce qui cause une latence et consommation excessives des ressources du serveur.

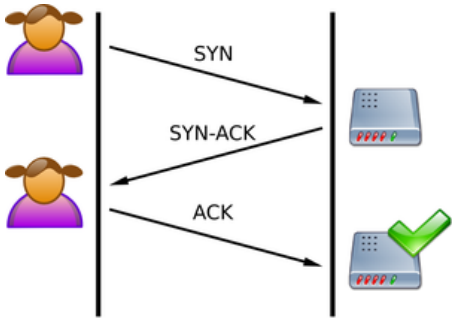


Figure 0.33 : Demande de connexion normale

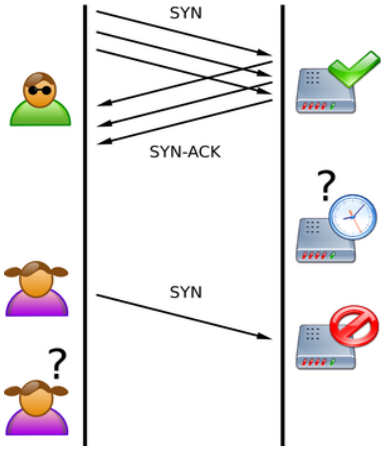


Figure 0.34 : Attaque SYN

Référence : *http://*fr.wikipedia.org/wiki/SYN_flood

Application

Afin d'effectuer l'attaque SYN j'ai utilisé l'outil *Sprut* qui envoi à la victime des milliers de requêtes SYN sans établir une connexion.

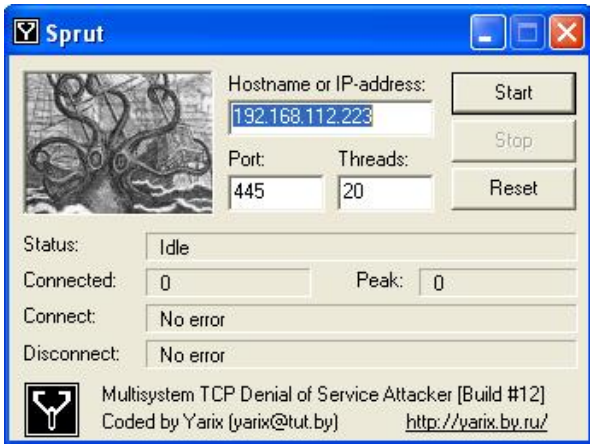


Figure 0.35 : Interface de l'outil *Sprut*

Le serveur ouvre des milliers de sessions et envoi des réponses SYN-ACK et reste en attente de réponses ACK ce qui rend ses ressources inaccessibles.

```
C:\Documents and Settings\Administrator.                >netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.112.223:80     192.168.112.225:15084  TIME_WAIT
  TCP    192.168.112.223:80     192.168.112.225:22688  TIME_WAIT
  TCP    192.168.112.223:80     192.168.112.225:22689  TIME_WAIT
  TCP    192.168.112.223:80     192.168.112.225:22753  TIME_WAIT
  TCP    192.168.112.223:80     192.168.112.225:22772  TIME_WAIT
  TCP    192.168.112.223:80     192.168.112.225:22782  TIME_WAIT
  TCP    192.168.112.223:135    192.168.112.225:15088  TIME_WAIT
  TCP    192.168.112.223:135    192.168.112.225:16175  TIME_WAIT
  TCP    192.168.112.223:139    192.168.112.225:15094  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.224:1883   TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14273  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14274  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14275  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14276  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14277  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14278  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14279  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14280  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14281  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14282  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14283  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14284  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14285  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14286  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14287  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14288  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14289  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14290  TIME_WAIT
  TCP    192.168.112.223:445    192.168.112.225:14291  TIME_WAIT
```

Figure 0.36 : Connexions ouvertes avec le serveur

- **Vol de session (Hijacking)**

Cette technique consiste à intercepter une session TCP initiée entre deux machines afin de la détourner. Le pirate contourne le processus d'authentification de la session et dialogue avec le serveur au lieu de la victime qui sera mis hors service par une attaque de dénis de service par exemple. Il se peut que le pirate seulement écoute et enregistre le trafic afin de recueillir des informations sensibles comme les mots de passe.

Pour établir une connexion entre deux machines, les échanges se font à l'aide de numéro de séquence, une machine accepte un segment lorsque le numéro de séquence de ce dernier est égal au numéro d'acquittement du dernier segment reçu. Ainsi si le pirate envoi au serveur un paquet semblant venir du client avec les numéros de séquence et d'acquittement corrects, ainsi le serveur mettra son numéro d'acquittement à jour et les données venant de ce client ne seront plus jamais acceptées. Lorsque le pirate termine son attaque, il pourra penser à resynchroniser la session TCP entre le client et le serveur.

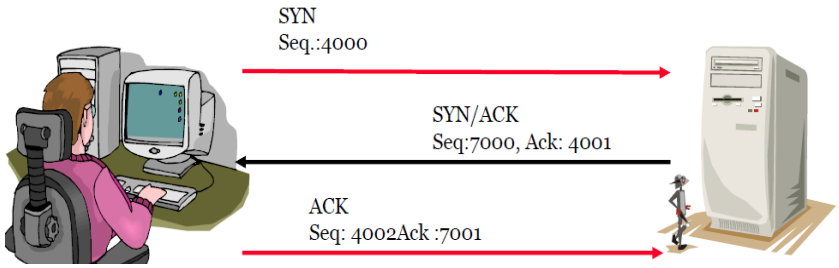


Figure 0.37 : Authentification TCP normale
Référence : ***CEH v5 Module 10 Session Hijacking***

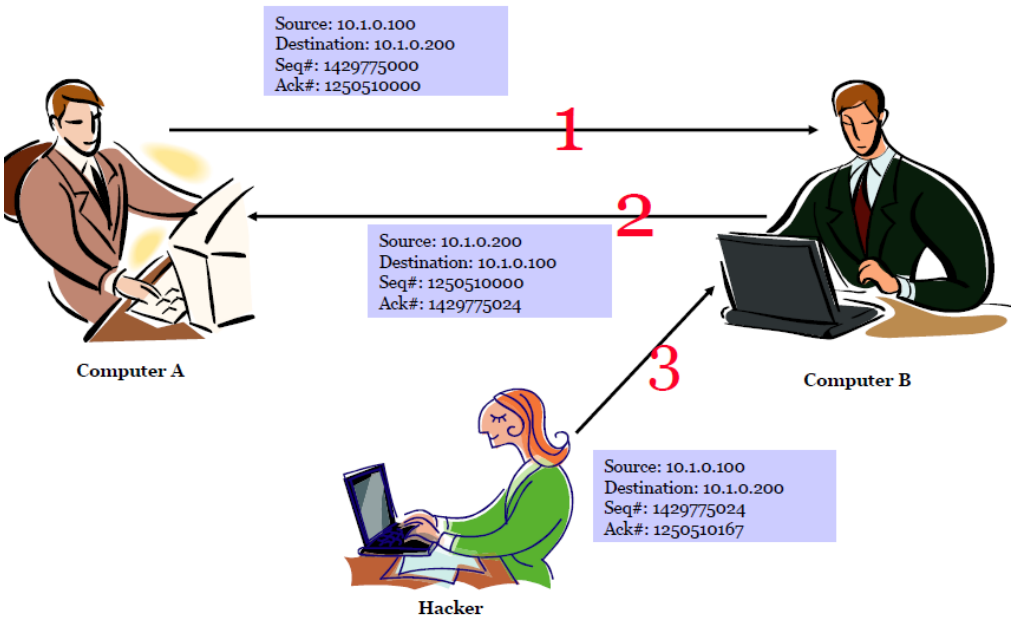


Figure 0.38 : Authentification interceptée par le pirate
Référence : ***CEH v5 Module 10 Session Hijacking***

Parmi les types de vol de session citons : attaque par rejeu, usurpation d'adresse IP, vol de session TCP ou UDP et l'homme au milieu.

Application

J'ai utilisé l'outil *Cain and Abel* qui emploie la technique de l'attaque de l'homme au milieu ou *Man In the Middle* (MITM), dans ce scenario on écoute la communication entre les deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties.

La première étape consiste à choisir la source et le destinataire desquels il faut voler la session, dans ce cas j'ai choisi le serveur et le routeur, ensuite il faut empoisonner le trafic par des requêtes *Address Resolution Protocol* (ARP) en manipulant les numéros de séquence SYN et ACK afin d'intercepter la session passante.

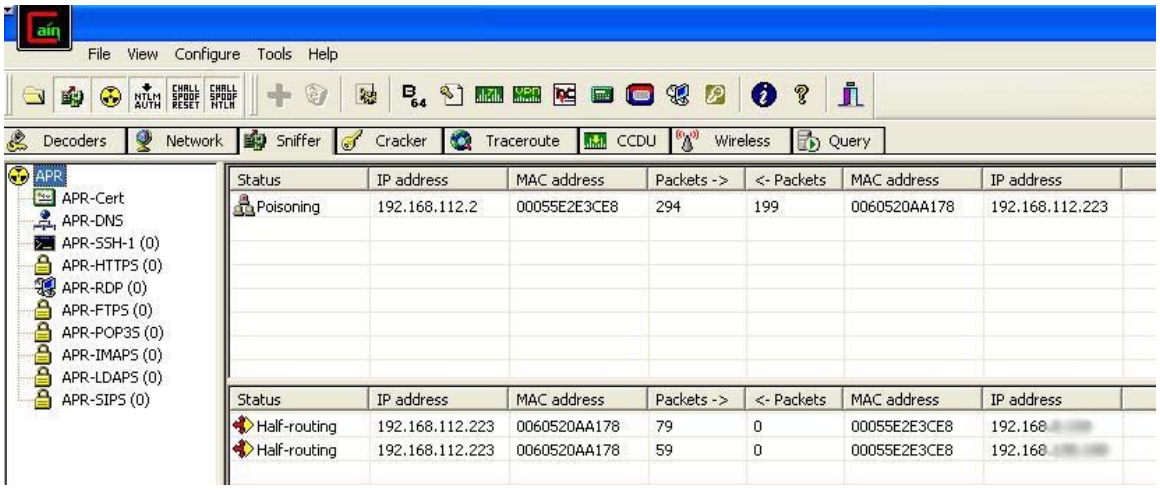


Figure 0.39 : Empoisonnement de la session TCP

Une fois l'interception est effectuée, on arrête l'empoisonnement et on obtient ainsi les données passantes durant la session. Dans ce cas les données obtenues sont une ouverture de session et communication avec le routeur. Le mot de passe et toute la configuration du routeur sont compromis.

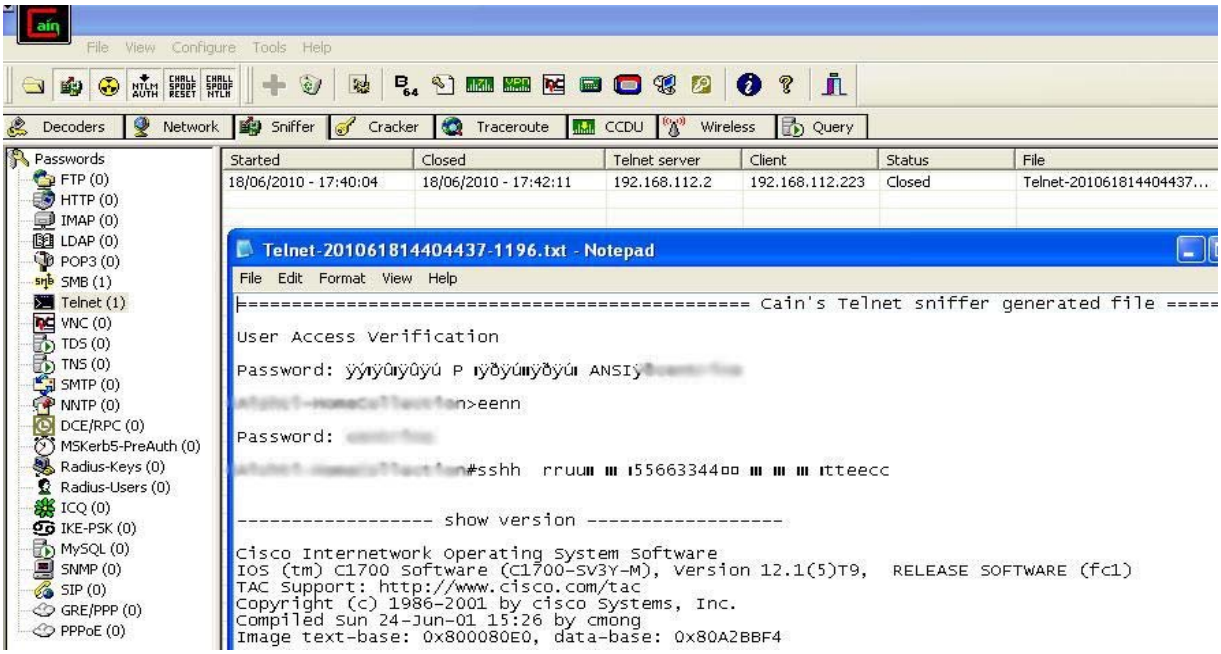


Figure 0.40 : Résultat de vol de session

Les trois attaques exécutées ont réussi de bloquer les matériels et interdire l'accès aux ressources.

c. Résultats

L'accès au niveau de la couche réseau a réussi plus ou moins dans chaque phase de l'attaque. L'exploitation à ce niveau forme une menace cruciale par rapport aux ressources physiques et intellectuelles de l'organisation.

Table 0-VI : Résultats des tests de la couche Internet

	Date des tests	Vulnérabilités / Etat	Risques / Impact	Résultat
Balayage et analyse du réseau	19/4/2010	Plusieurs ports ouverts Postes clients plus vulnérables que serveurs	Accessibilité possible sur plusieurs niveaux	Parfois compromis
Pénétration des périphériques du réseau	6/5/2010	Mots de passe par default Configuration initiale	Accessibilité possible sur plusieurs périphériques	Plutôt compromis
Surcharge et blocage des ressources	8/6/2010	Plusieurs ports ouverts facilitent les attaques	Accessibilité complexe	Parfois compromis

d. Recommandations

Les périphériques du réseau constituent les fondements de la couche internet, leurs rôles est critiques et primordial. Ils joignent tous les postes et périphériques dans chaque branche et toutes les branches entre elles et avec le réseau externe. La pénétration d'un d'eux menaces l'organisation entière.

Tous les types d'attaques constituent une grave menace et doivent être évités par des mesures de sécurisation afin d'atteindre un niveau de protection idéal. La démarche à suivre comprend les taches suivantes :

- Utiliser une authentification et un cryptage puissants chaque fois que cela est possible
- Ne pas étendre les relations d'approbation au-delà du pare-feu
- Maintenir les systèmes à jour avec les derniers correctifs de sécurité.
- Bloquer les paquets *ping* volumineux au niveau des commutateurs, des routeurs et du pare-feu
- Appliquer des filtres anti-usurpation sur le routeur, ce qui revient à bloquer les paquets entrants dont l'adresse source est identique à une adresse du réseau interne.
- Désactiver les ports et protocoles inutiles et services non utilisés sur les routeurs, commutateurs et pare-feu.
- Appliquer un filtrage approprié au niveau du routeur et du pare-feu.
- Utiliser le système de détection d'intrusion (IDS) pour détecter le trafic inhabituel et générer une alerte en cas de détection.
- Réduire la puissance de transmission des points d'accès et utiliser des clés WEP de 128 ou 192 bits.
- Changer les configurations initiales, identificateurs et bannières par default
- Désactiver le protocole SNMP pour empêcher le balayage et analyses des postes.
- Utiliser le service de sécurisation des ports dans les commutateurs pour éviter l'usurpation des requêtes ARP

3.2.6.3 Couche Transport

La Couche transport permet le transfert des données et contrôle l'état de la transmission. Elle gère 2 protocoles de transport des informations, indépendamment du type de réseau utilisé :

- Le protocole TCP fonctionne en mode connecté et assure un service fiable.
- Le protocole UDP assure un service de datagramme en mode non connecté sans aucune garantie de fiabilité.

Durant les tests de la couche Internet, plusieurs outils ont dévoilés les ports TCP et UDP ouverts qui m'ont aidé d'effectuer les attaques et pénétrer les périphériques. Mais dans cette partie, la concentration sera sur les types des ports ouverts, les services accessibles et les protocoles disponibles. Avant de commencer les tests, il faut prendre note des ports cibles qui peuvent être ouverts et accessibles dans la plus part des matériels connectés au réseau.

Table 0-VII : Ports TCP et UDP communs

	TCP	UDP
Routeurs	21 (FTP)	0 (tcpmux)
	23 (telnet)	49 (domain)
	79 (finger)	67 (bootps)
	80 (HTTP)	69 (TFTP)
	512 (exec)	123 (ntp)
	513 (login)	161 (SNMP)
	514 (shell)	
Commutateurs	23 (telnet)	0 (tcpmux)
	7161	123 (ntp)
		161 (SNMP)

Le balayage des ports effectué dans quelques branches montre l'accessibilité des ports cibles et leur taux qui est proportionnellement élevé dans les branches principales HO et DT par rapport au nombre total d'adresses IP existantes.

Table 0-VIII : Résultat du balayage des ports ouverts

	Nbre Total IP	TCP							UDP					Total
		FTP	ssh	telnet	dns	SMTP	HTTP	Total TCP	TFTP	SNMP	smb	ipsec	Total UDP	
		21	22	23	53	25	80		69	161	445	4500		
WH	16	0	0	1	0	1	3	47	0	2	10	8	80	127
SS	23	0	0	2	1	0	0	86	0	1	11	12	122	208
CM	11	0	0	1	1	0	0	25	0	0	0	0	0	25
ABCA	10	0	1	1	0	0	0	31	0	0	0	0	0	31
DT	78	1	1	5	3	1	64	662	2	20	45	38	683	1345
HO	104	1	10	7	9	2	22	391	1	21	54	66	1332	1723

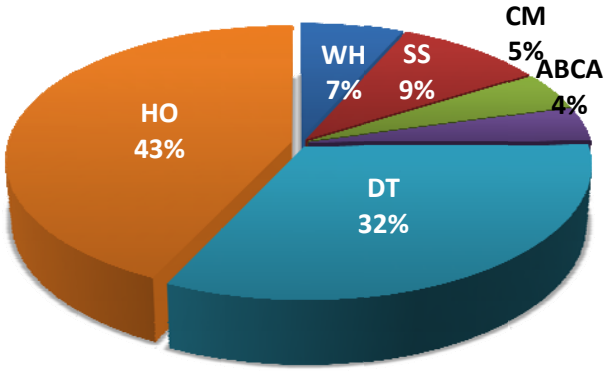


Figure 0.41 : Pourcentage des adresses IP par branche

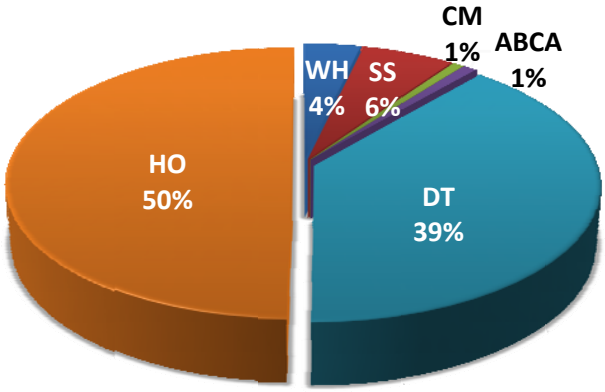


Figure 0.42 : Pourcentage des ports accessibles par branche

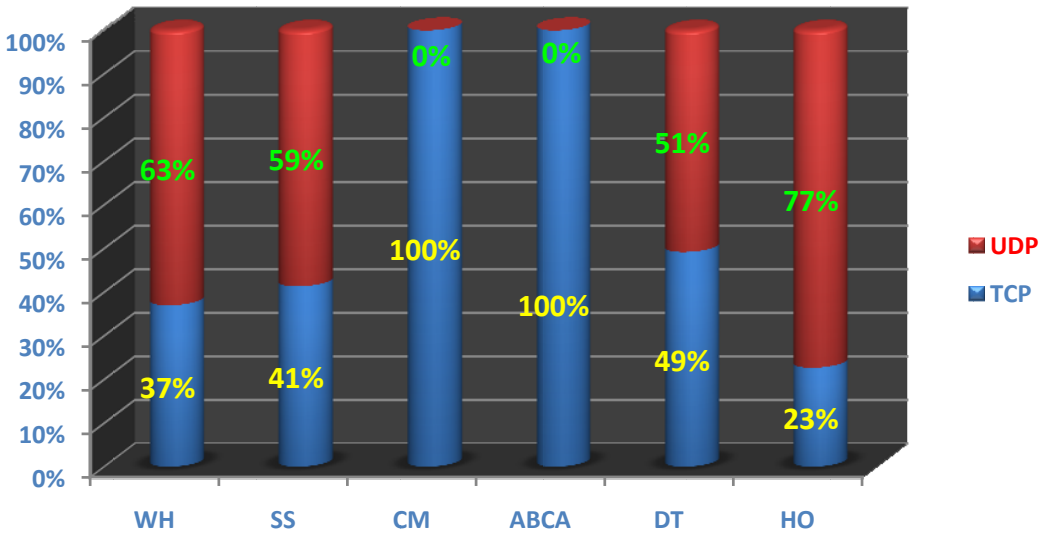


Figure 0.43 : Rapport entre le pourcentage des ports TCP et UDP accessible

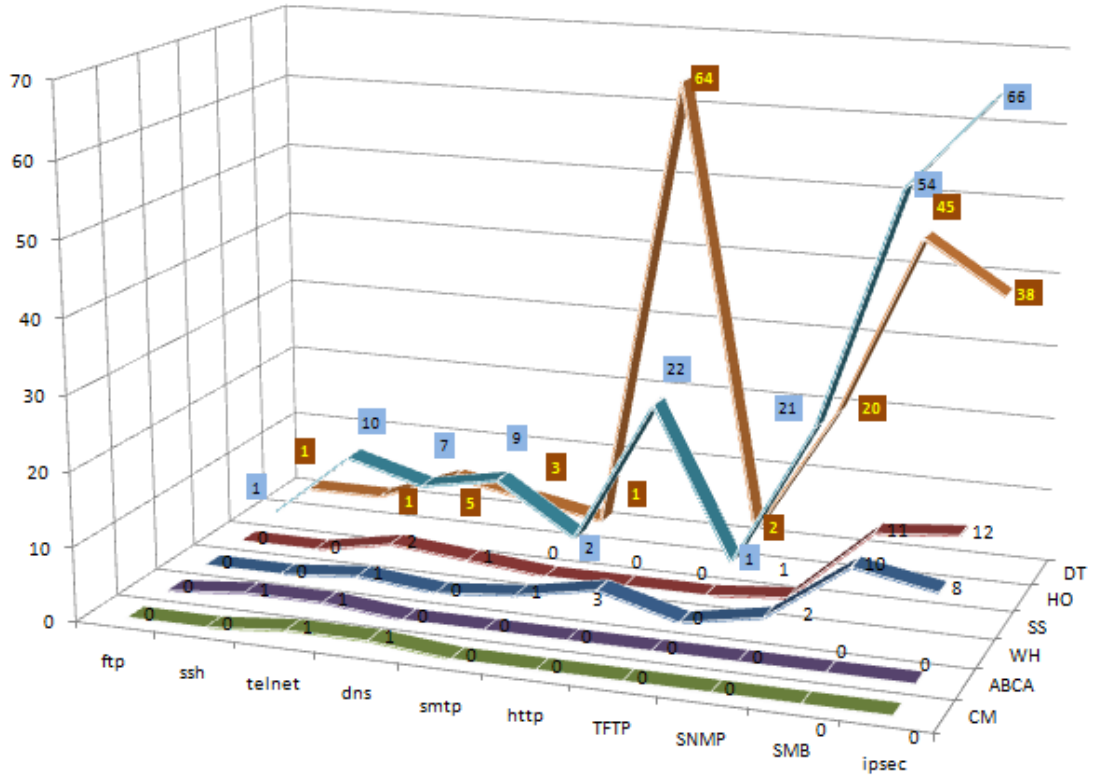


Figure 0.44 : Répartition totale des ports cibles accessibles

a. Objectifs

On remarque que le protocole TCP forme la majorité des ports et services cibles ouverts dans les branches, notamment le port 80 du service HTTP qui forme 65% des ports TCP cibles et 7% du nombre total de ports TCP ouverts. Les attaques vont être exécutées sur les ports cibles, non visés dans l'étude des couches restantes du protocole TCP, selon leurs disponibilités dans les branches étudiées.

b. Détails d'évaluation

b.1 TCP Port 21 FTP

L'ouverture d'une session FTP avec les adresses IP trouvées dans les branches HO et DT a réussi sans besoin d'identificateurs. Mais les machines accédés sont des imprimantes ne contenant aucune information nécessaire.

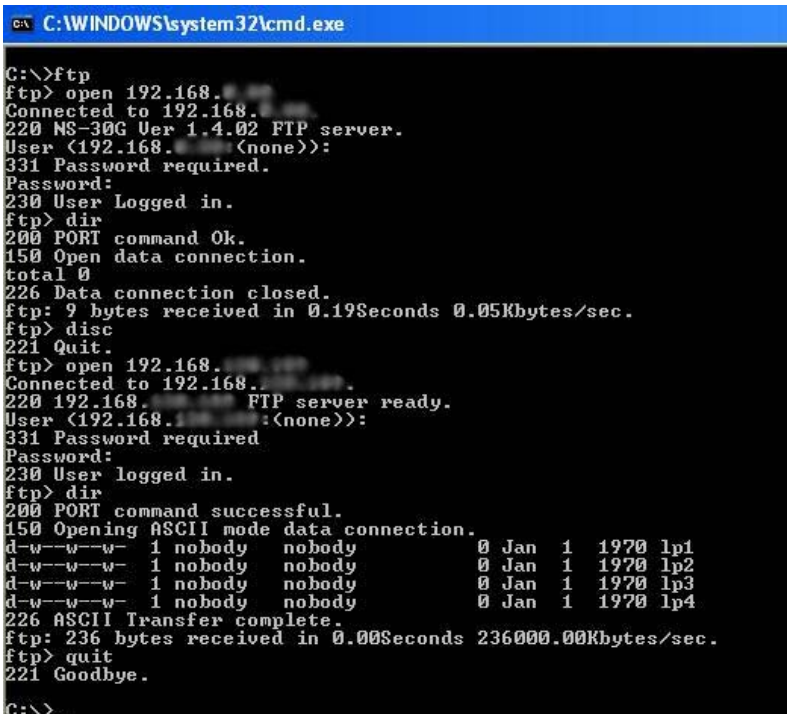


Figure 0.45 : Accès FTP dans HO et DT

b.2 TCP port 22 SSH

L'ouverture d'une session avec les adresses IP trouvées dans les branches HO et DT en utilisant l'outil *PuTTY* n'a pas réussie. Il faut avoir les identificateurs correctes et l'essai des identificateurs communs ou par default n'a pas réussi.

Figure 0.46 : Accès SSH dans HO

Afin de deviner les identificateurs corrects j'ai effectué une attaque par force brute en utilisant l'outil *Hydra* sur la plateforme linux. Comme le montre le schéma ci-dessous l'essai de 5000 combinaisons d'identificateurs n'a pas abouti à la bonne combinaison ce qui implique un niveau de complexité élevé pour les identificateurs.

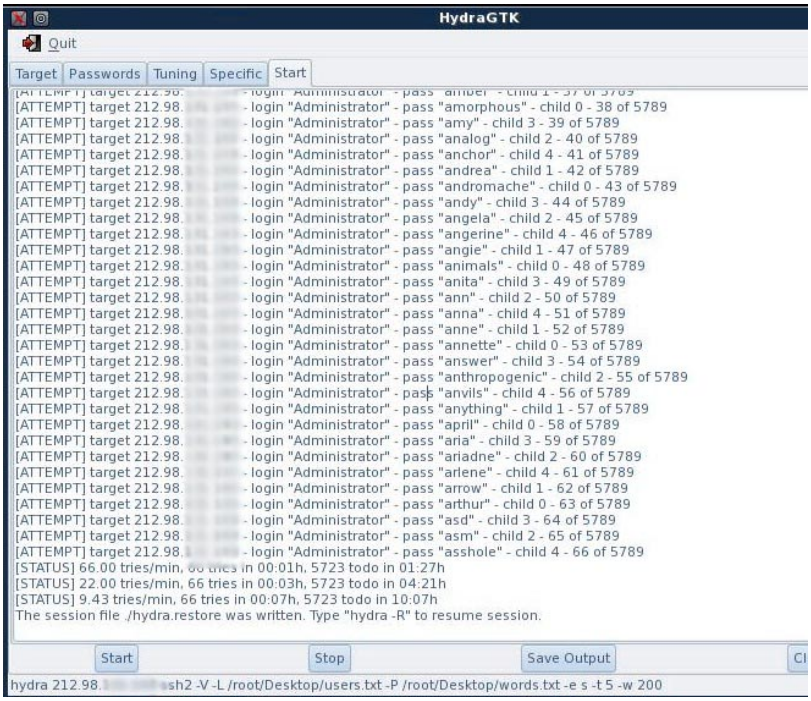


Figure 0.47 : Attaque SSH par force brute

Notons que l'exécution de la même attaque sur le pare-feu XF montre qu'il existe un IDS qui a arrêté l'attaque après quelques minutes. Le logiciel *Hydra* est alors obligé d'attendre un intervalle de temps de 3 à 6 heures pour continuer les essais.

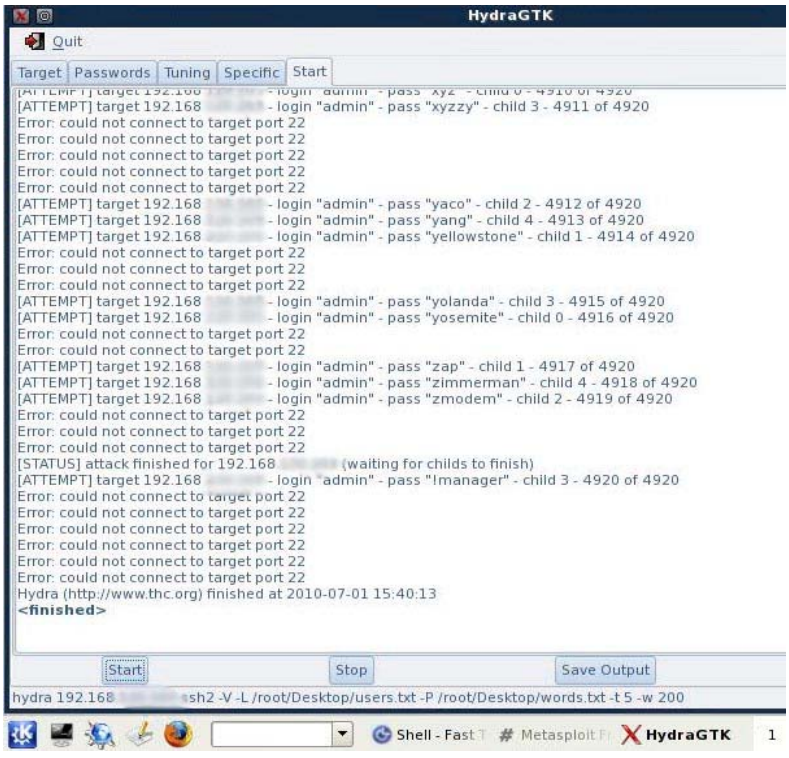


Figure 0.48 : Attaque SSH par force brute arrêtée par XF

b.3 UDP port 69 TFTP

L'ouverture d'une session avec les adresses IP trouvées dans les branches HO et DT en utilisant l'outil *TFTP32* n'a pas réussie. La connexion été refusée à cause des identificateurs incorrectes.

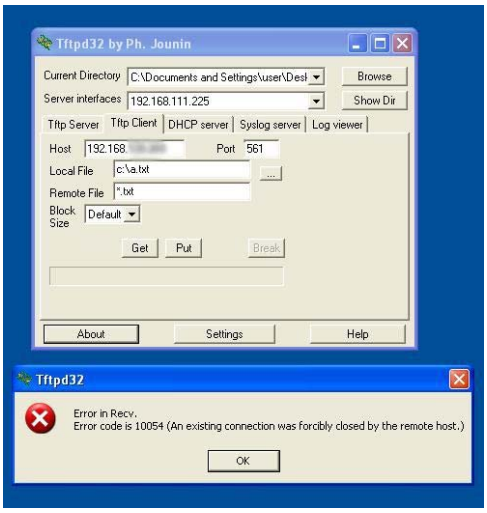


Figure 0.49 : Résultat de l'outil *TFTP32*

Afin de deviner les identificateurs corrects j'ai effectué une attaque par force brute en utilisant l'outil *Hydra* sur la plateforme Linux. Mais l'essai de 5000 combinaisons d'identificateurs n'a pas abouti à la bonne combinaison ce qui implique un niveau de complexité élevé pour les identificateurs.

b.4 UDP port 161 SNMP

Le protocole SNMP exige la connaissance d'un identificateur connu par CS qui est une chaîne de caractère qui définit la relation entre un système de serveur SNMP et les systèmes client. Cette chaîne se comporte comme un mot de passe pour contrôler l'accès des clients au serveur, elle est de deux types : Lire ou Lire/Ecrire. La première étape dans le test du port 161 consiste à scanner les adresses comprenant ce port ouvert afin de trouver les chaines. L'outil *SNMP Dictionnary attack* a dévoilé les chaînes de quelques périphériques ensuite à l'aide du logiciel *MIB walk* les informations essentielles sur chaque système sont révélées. Le test des privilèges des chaines obtenues à l'aide de l'outil *Remote TCP Session Reset*, qui liste les sessions existante et permet de les arrêter, n'a pas réussi d'arrêter les sessions car la plupart des chaines trouvées sont de type Lire.

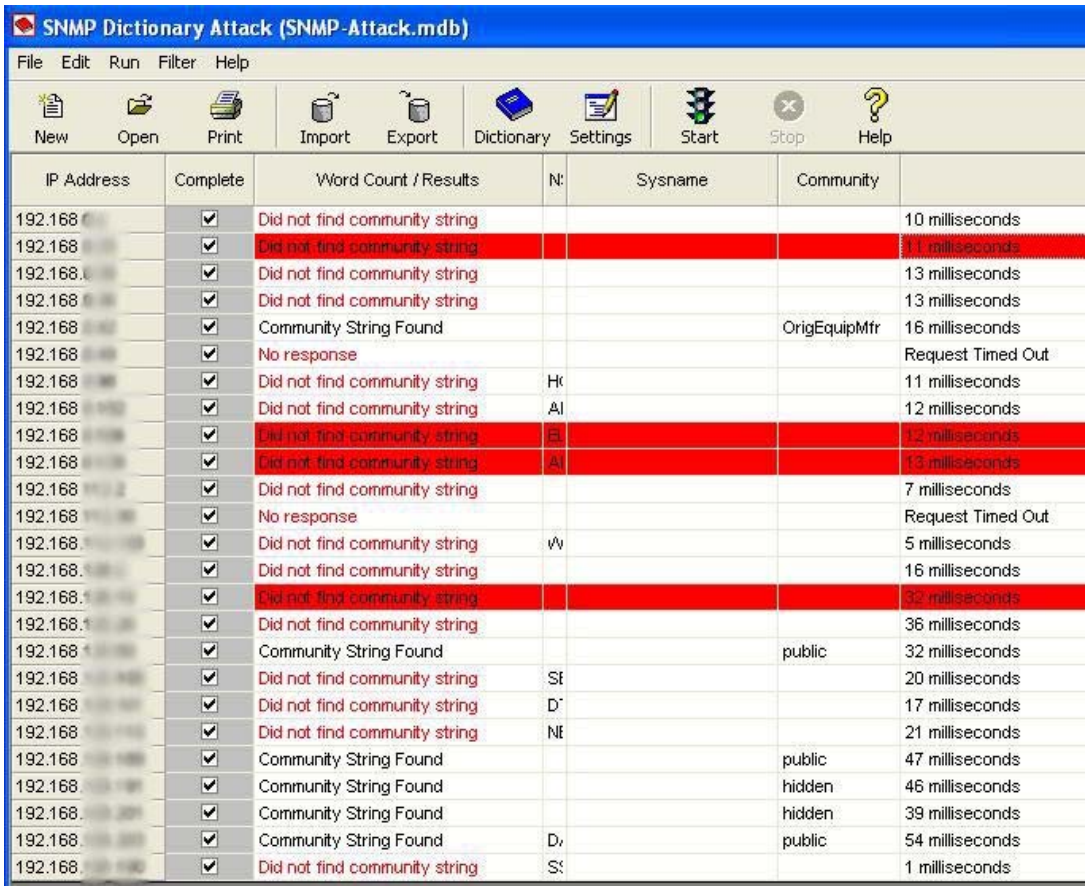


Figure 0.51 : Résultat de l'outil *SNMP Dictionnary Attack*

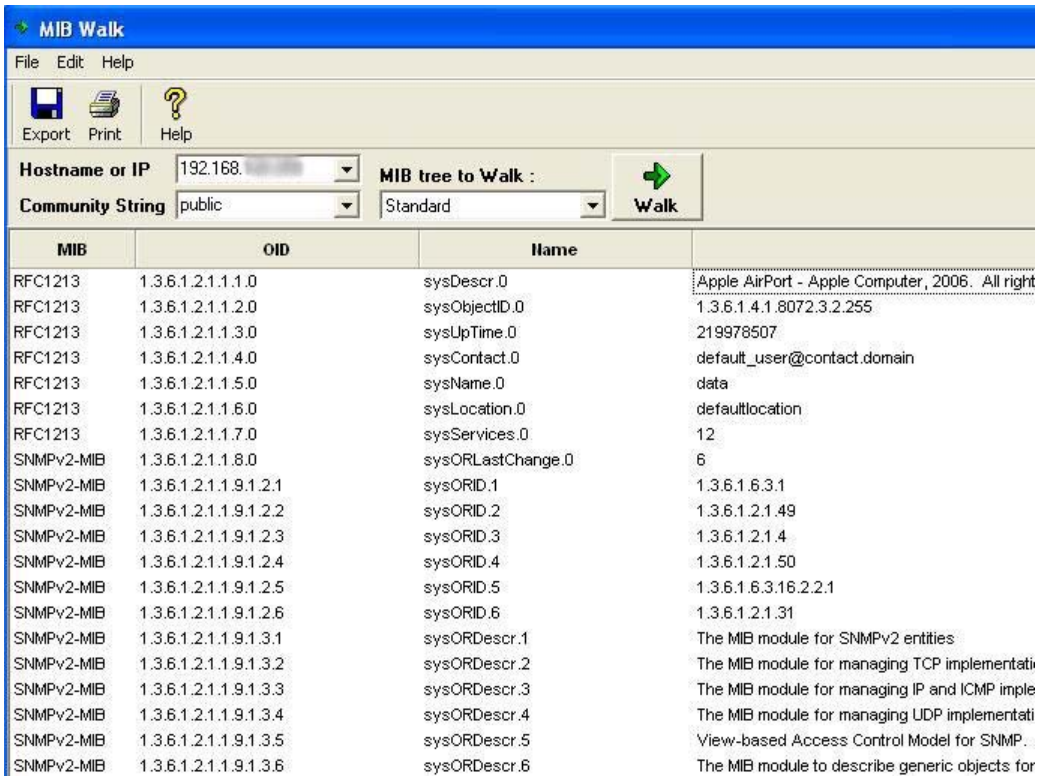


Figure 0.50 : Résultat *MIB Walk*

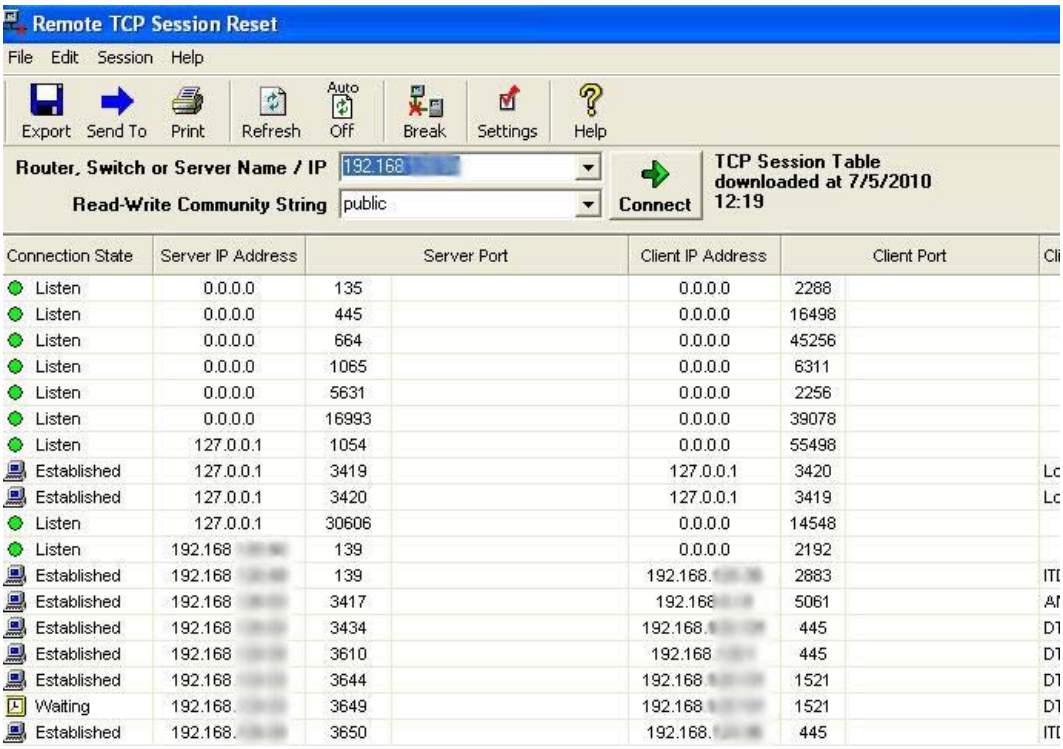


Figure 0.52 : Résultat *Remote TCP Session Reset*

b.5 UDP port 455 SMB

Ce port est utilisé pour le service de partage de fichier. Une fois exploité l'attaqueur aura accès aux fichiers systèmes de la victime. L'outil utilisé pour effectuer cette attaque est *Metasploit*. La première phase consiste à décider les paramètres de l'attaque : victime, port, exploit et charge, la deuxième phase est l'exécution de l'exploit et ouverture d'une session chez la victime si l'exploit réussi. Ce test a réussi sur plusieurs ordinateurs et m'a permis de créer un utilisateur à accès administratif qui sera bien sur utile pour l'attaque au niveau de la couche application.

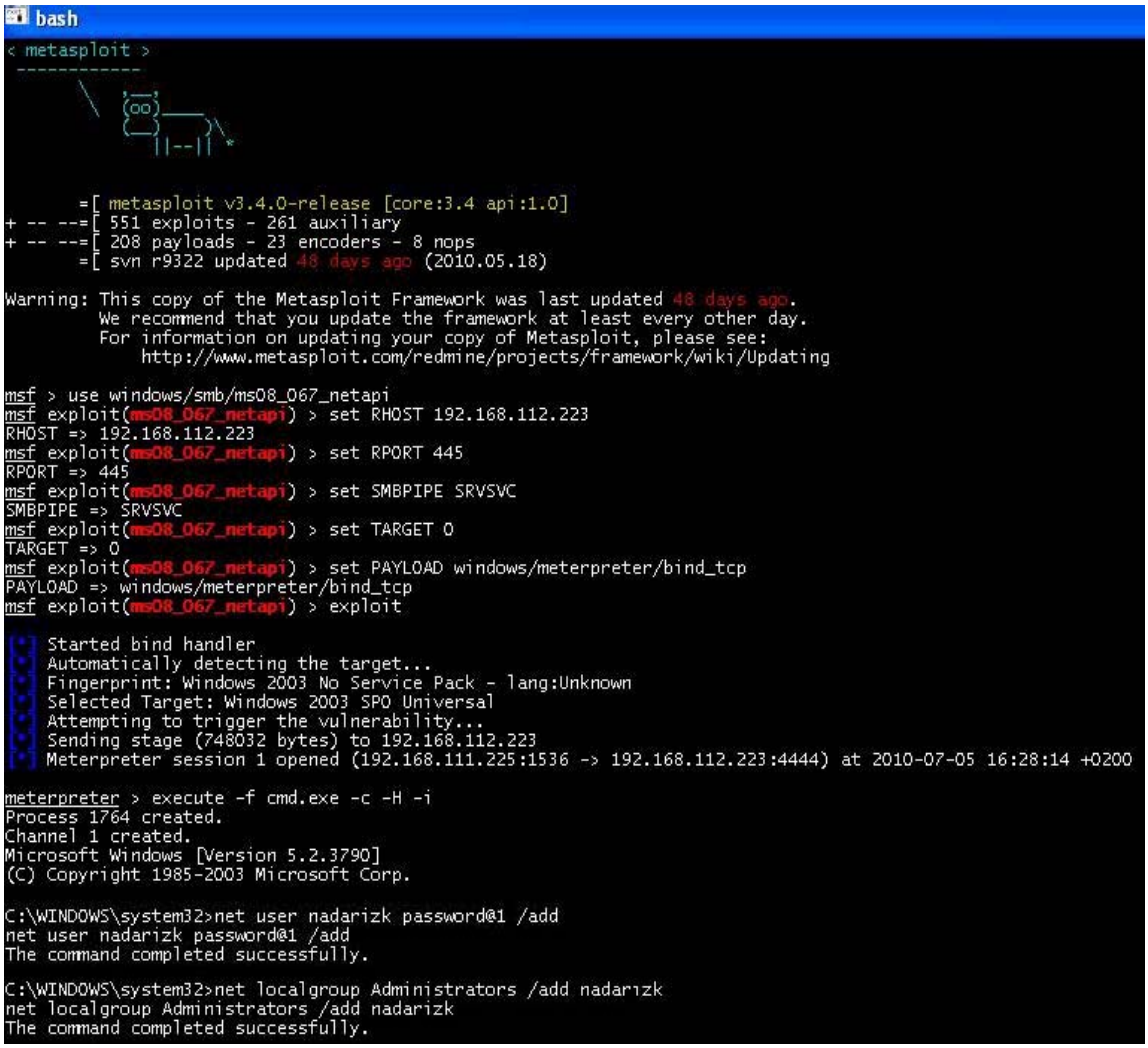


Figure 0.53 : Démarche de l'attaque *Metasploit*

b.6 TCP port 443 SSL

Ce port est utilisé pour ouvrir des sessions sécurisées. L'attaque consiste au surpassement de la session SSL à l'aide de l'outil *SSLstrip* en utilisant le mécanisme du *Man In The Middle* pour la redirection/transmission des paquets. Les commandes utilisées sont :

- Transfer des IP : ***echo 1 > /proc/sys/net/ipv4/ip_forward***
- Usurpation par des paquets ARP : ***arpspoof -i eth0 -t 192.168.111.224 192.168.111.1***
- Redirection de port : ***iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000***
- Démarrage du *SSLstrip* écoutant sur le port 10000 : ***SSLstrip –a***

Une fois la configuration terminée on attend l'ouverture d'une session SSL chez la victime et capte ainsi les données passantes comme nom d'utilisateur et mot de passe.

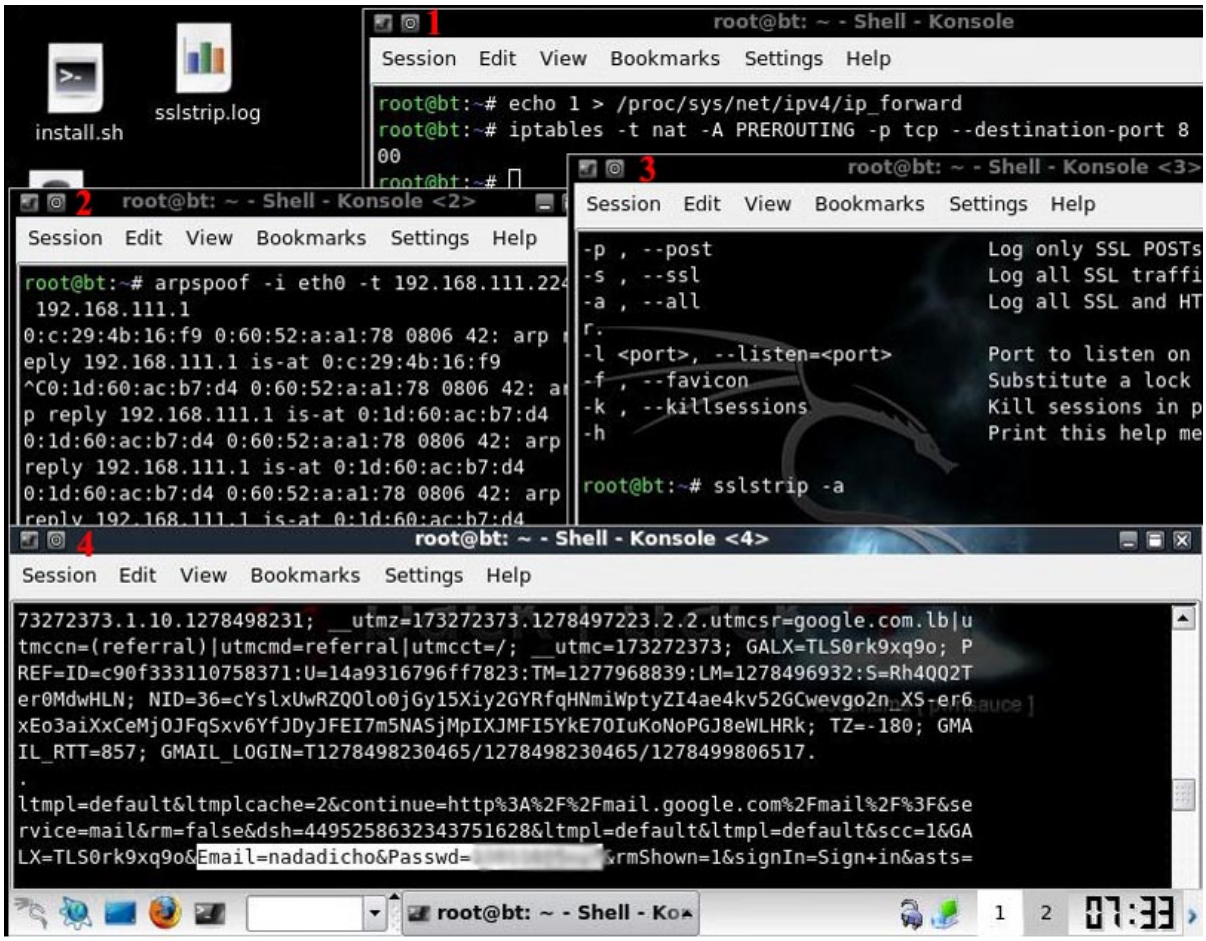


Figure 0.54 : Surpassement de session SSL

c. Résultats

50% des attaques effectuées au niveau de la couche transport ont réussies, les données révélées sont d'une grande importance et constituent une menace sur les ressources pertinentes de l'entreprise.

Table 0-IX : Résultats des tests de la couche Transport

	Date des tests	Vulnérabilités / Etat	Risques / Impact	Résultat
FTP	28/6/2010	Ports accessibles Pas de mots de passe	Accessibilité facile	compromis
SSH	1/7/2010	Ports ouverts sur machines pertinentes Accès difficile et sécurisé	Etat acceptable	Non compromis
TFTP	29/6/2010	Ports ouverts sur machines pertinentes Accès difficile et sécurisé	Etat acceptable	Non compromis
SNMP	30/6/2010	Ports accessibles Mots de passe parfois dévoilés	Accessibilité complexe	Parfois compromis
SMB	7/7/2010	Dangers sur tous les postes car ce port est ouvert par default	Etat Critique Accessibilité complexe	Parfois compromis

d. Recommandations

- Désactiver les ports et services inutiles surtout chez les postes serveurs
- Mise à jour régulière des SE et logiciels
- Activation des pare-feu pour bloquer les intrusions
- Audit régulier préférablement automatisé des accès et transactions
- Implémentation de logiciel de détection d'intrusion
- Désactiver les agents SNMP inutilisés
- Restreindre l'accès par FTP ou TFTP aux directoires systèmes
- Restreindre les routeurs de répondre aux paquets irréguliers

3.2.6.4 Couche Application

La couche application est la couche située au sommet des couches de protocoles TCP/IP. Elle contient les applications réseaux permettant de communiquer grâce aux couches inférieures. Les logiciels de cette couche communiquent donc grâce à un des deux protocoles de la couche inférieure (la couche transport) c'est-à-dire TCP ou UDP.

Les attaques sur cette couche sont de différents types dont chacun sera visé par des outils spécifiques au niveau de l'application choisi, quelques attaques risquées seront effectuées dans l'environnement virtuel des tests.

a. Objectifs

- Systèmes d'exploitation
- Maliciels
- Messagerie
- Application Web
- Injection de code SQL

b. Détail d'évaluation

b.1 Systèmes d'exploitation

La majorité des postes clients ont le SE *Windows XP* et les postes serveur *Windows server 2003*. Pour chaque système il existe bien sûr des failles exploitables qui aideront à effectuer les attaques tout en suivant un enchainement de plusieurs étapes :

- **Ouverture de session**

La première étape consiste à ouvrir une session avec un poste client afin d'obtenir la liste des utilisateurs et d'ajouter un utilisateur qui servira ultérieurement comme agent d'attaque. Dans cette phase l'utilisation de la méthode de l'attaque *Metasploit* vue précédemment dans la partie de l'attaque du port UDP 455 SMB servira pour ouvrir cette session. Cette méthode a échouée sur quelques postes n'ayant pas des utilisateurs sans mots de passe, mais sur d'autres postes a réussie et m'a permis de passer à la phase suivante.

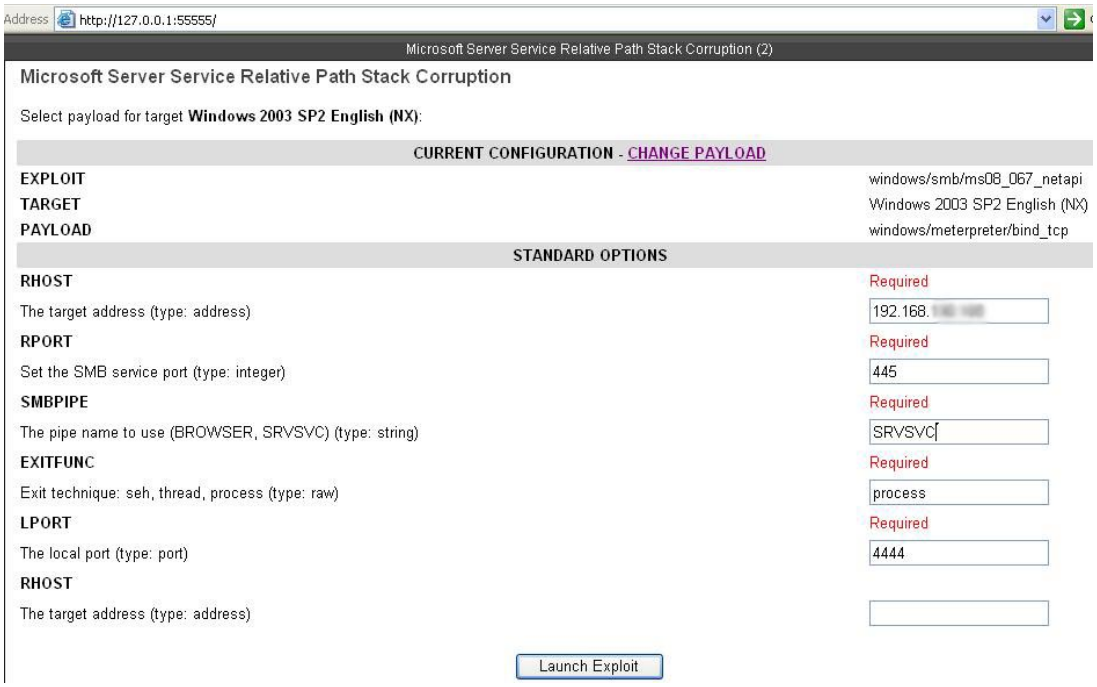


Figure 0.55 : Première étape de l'attaque *Metasploit*

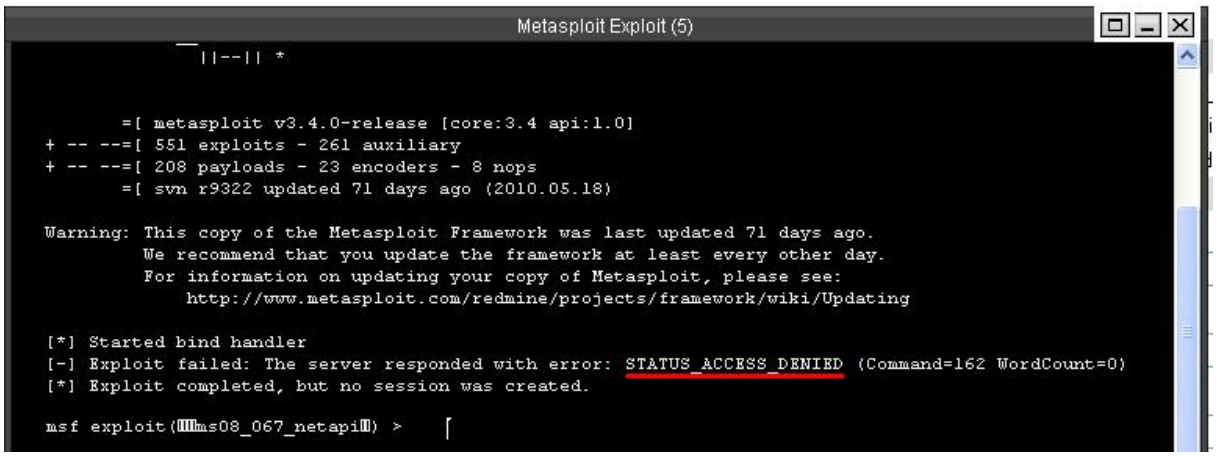


Figure 0.56 : Attaque échouée sur un poste serveur

En cas de réussite, j'ai créé un utilisateur et je l'ai ajouté au group administratif du client, ainsi j'ai ouvert une session et téléchargé les fichiers d'exécution pour voler les informations des comptes des utilisateurs. Une fois exécutées à partir de la session ouverte j'ai eu les fichiers nécessaires : SAM et SYSTEM.

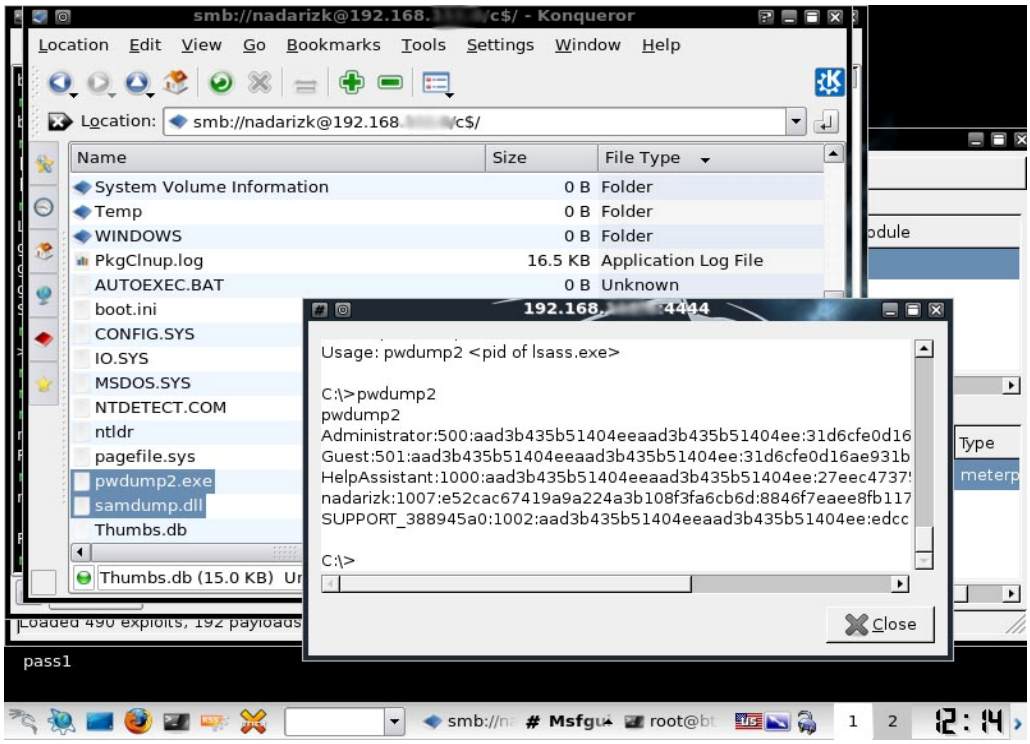


Figure 0.57 : Téléchargement des fichiers et exécution du logiciel chez la victime

- **Craquage des mots de passe**

Les mots de passe forment la première ligne de défense contre les attaques sur un système. Si le pirate parvient à connaître le mot de passe il pourra s'introduire en tant qu'administrateur dans le SE.

Les fichiers obtenus de la phase précédente sont importés dans le logiciel *CAIN* et on effectue une attaque par force brute afin de dévoiler les mots de passe des utilisateurs. Evidement si le mot de passe est complexe l'outil prendra beaucoup de temps et la plus part des fois ne pourra jamais le craquer.

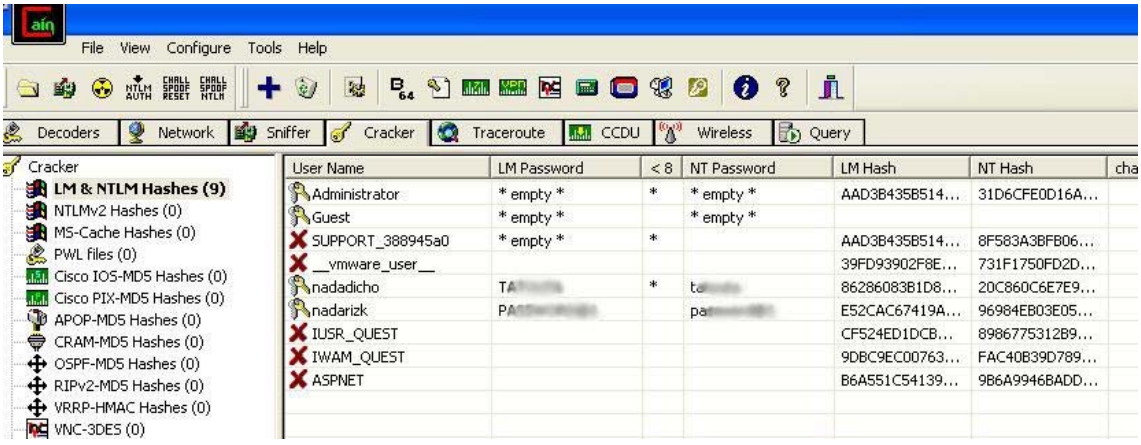


Figure 0.58 : Craquage des mots de passe

Cette méthode permet d'obtenir les utilisateurs locaux sur les postes client. Afin de craquer un utilisateur du domaine de l'organisation j'ai utilisé l'empoisonnement par paquets ARP de l'outil CAIN pour capter le trafic d'authentification des utilisateurs et craquer ensuite les mots de passe.

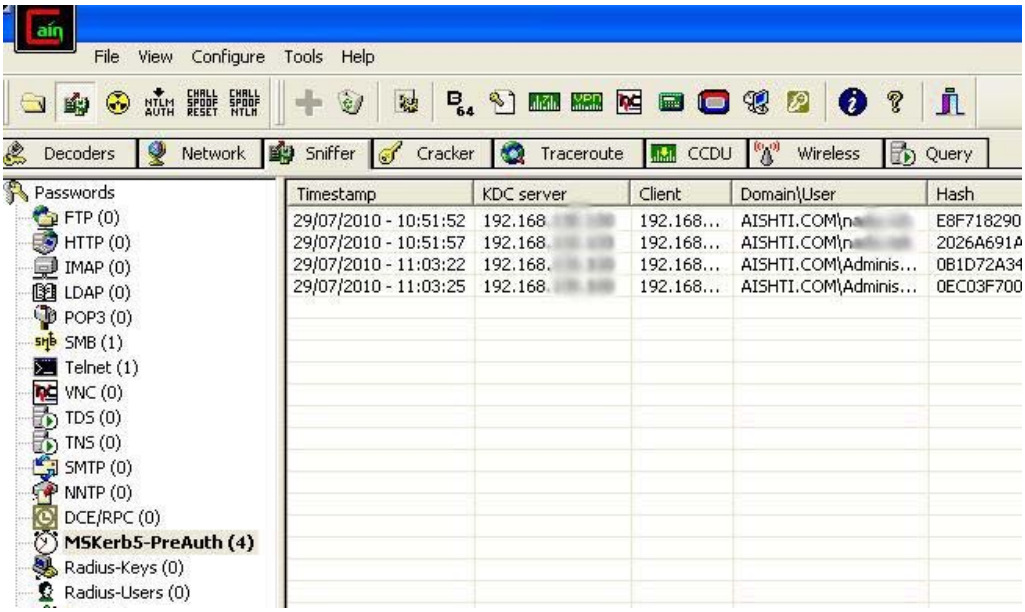


Figure 0.59 : Captage de session d'authentification

Une fois la session est captée, on utilise des méthodes de craquage du mot de passe par force brute ou par dictionnaire. Lorsque le mot de passe est complexe l'outil ne peut pas le craquer dans une limite de temps valable.

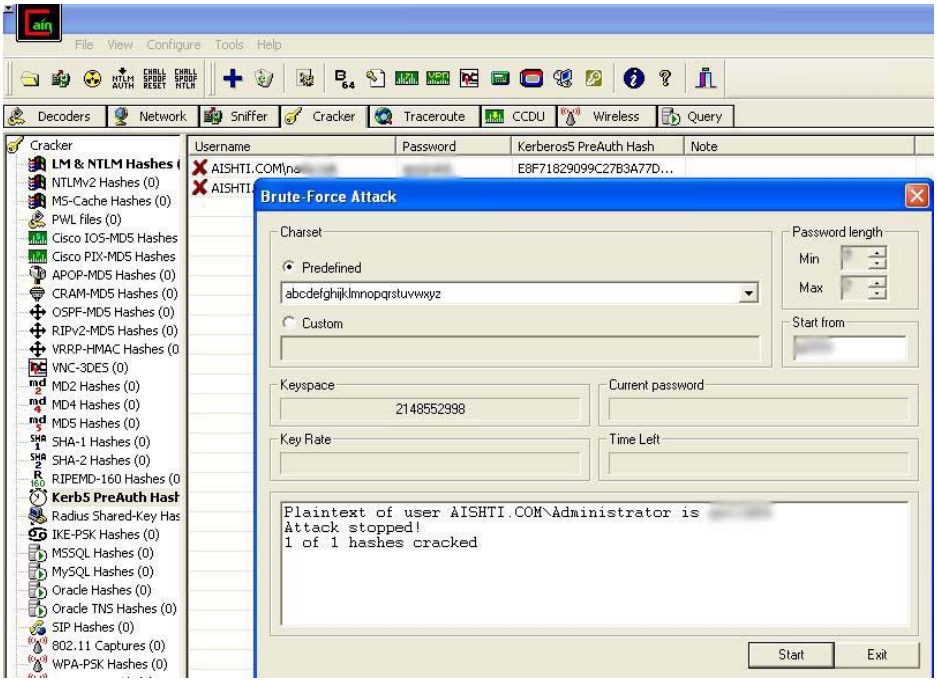


Figure 0.60 : Mot de passe craqué

- **Extension de privilèges**

Lorsque le pirate obtient un accès sur le réseau en utilisant des comptes peu protégés, il va chercher à augmenter ses privilèges en obtenant l'accès de l'administrateur. Pour obtenir cet accès il cherche à savoir le mot de passe de l'administrateur, la clé de cryptage du fichier SAM contenant les références des utilisateurs sur la machine ou changer ce mot de passe en utilisant des outils de craquage en mode *Disk Operating System* (DOS) ou il peut utiliser des outils qui créent des nouveaux utilisateurs avec des privilèges administratifs.

Dans les phases précédentes j'ai obtenu le fichier SAM et la clé de cryptage contenu dans le fichier SYSTEM et j'ai créé un nouveau utilisateur à privilèges administratifs. De même j'ai pu capter la session d'authentification de l'administrateur du domaine et craquer son mot de passe. Donc les privilèges administratifs sont déjà acquis.

Dans le cas d'accès physique directe la méthode la plus facile c'est le changement du mot de passe des utilisateurs, notamment celui de l'administrateur. Afin d'effectuer ce test j'ai utilisé la commande *chnptw* qui permet de changer le mot de passe en accédant le fichier SAM.

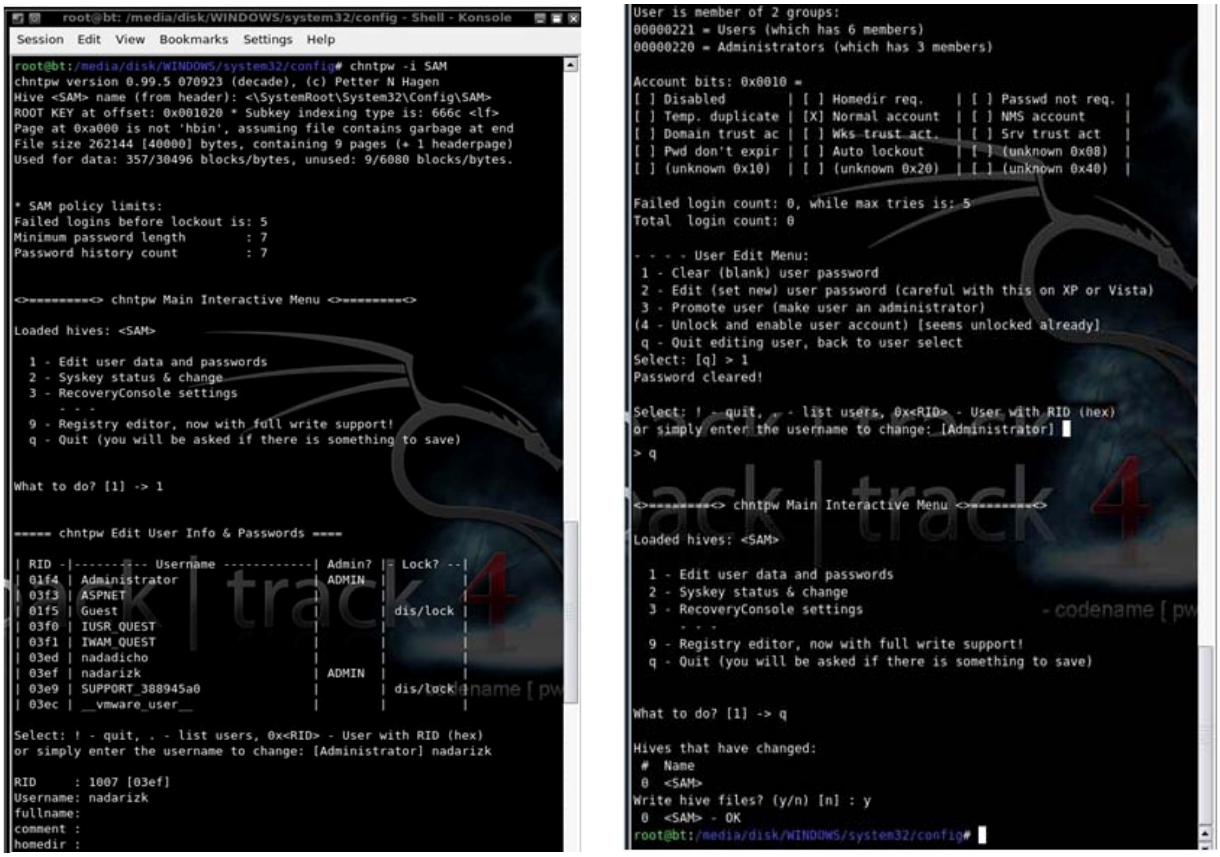


Figure 0.61 : Changement de mot de passe par la commande *chnptw*

- **Exécuter des applications malicieuses**

Une fois un accès administratif est obtenu sur le système, le pirate exécute des applications malicieuses en utilisant des outils qui lancent des commandes DOS à distance comme *psexec* et *remoexec*. Le but de ces application est d'obtenir toutes les informations possibles sur la machine cible. Le *spyware* ou logiciel espion est une de ces applications, ce logiciel enregistre les caractères insérés du clavier, les messages envoyés, les sessions de chat, les applications utilisées, les pages web visitées et des images de l'écran de temps en temps.

La première étape consiste à insérer les applications sur les postes cibles, cette tache peut être effectuée lors de l'ouverture de la session par *Metasploit* ou par l'utilisation de l'outil *psexec*. La deuxième étape consiste à lancer cette application à travers la session ouverte ou par lancement à distance. Ce travail sera effectué sur un serveur avec le service AD pour voler la base de données entière du domaine à partir de lancement à distance de l'application *ldp.exe* basée sur le protocole *Lightweight Directory Access Protocol* (LDAP), sachant le mot de passe de l'administrateur du domaine, l'ouverture de la session sur le port LDAP 389 est facile.

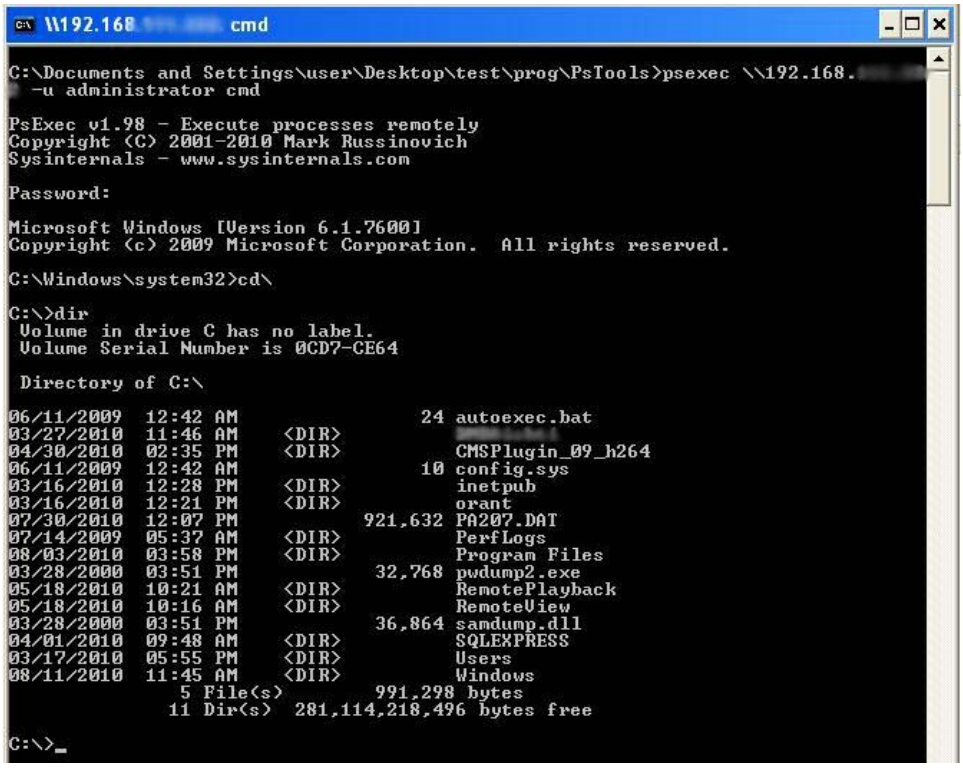


Figure 0.62 : Lancement commande par *psexec*

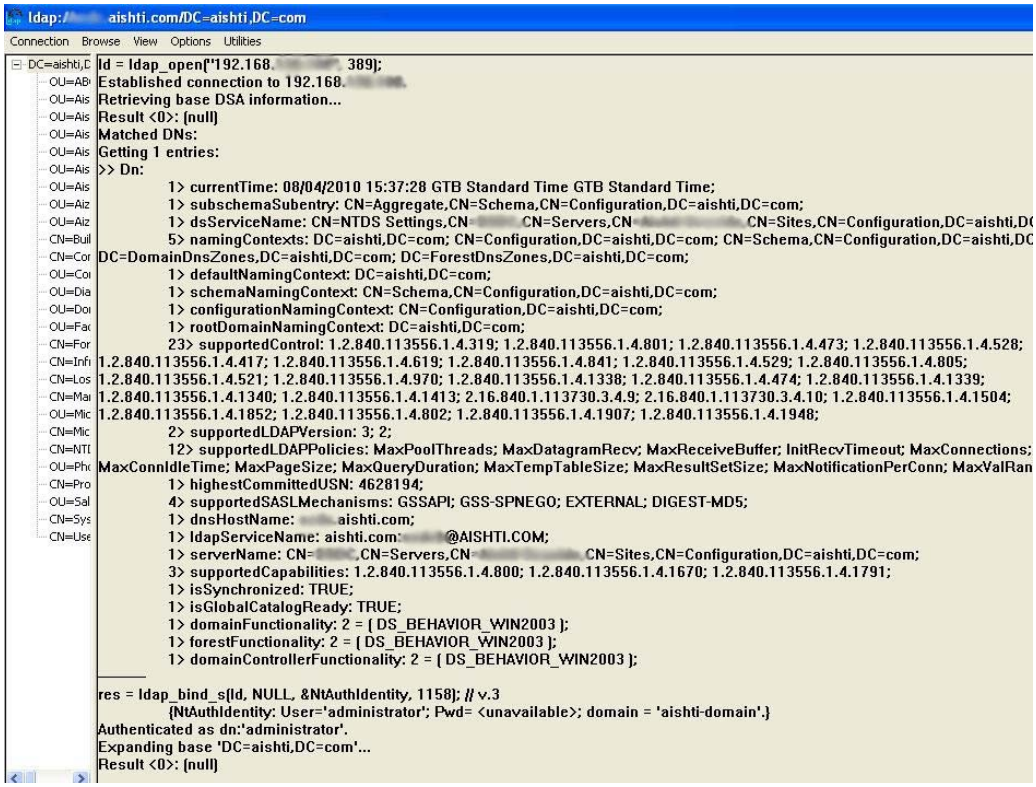


Figure 0.63 : Ouverture d'AD à travers LDAP

- **Cacher les fichiers**

Pour maintenir son accès privilégié, couvrir ses traces et éliminer les soupçons de l'administrateur du système, le pirate cache les fichiers utilisés en changeant l'attribut caché (Hidden) du fichier ou utilisant des fichiers de type *New Technology File System* (NTFS) à données alternées qui sont remplacées par des données falsifiées, il peut utiliser un logiciel comme *RootKit* qui a la capacité de se cacher et couvrir les traces des activités sur la machine.

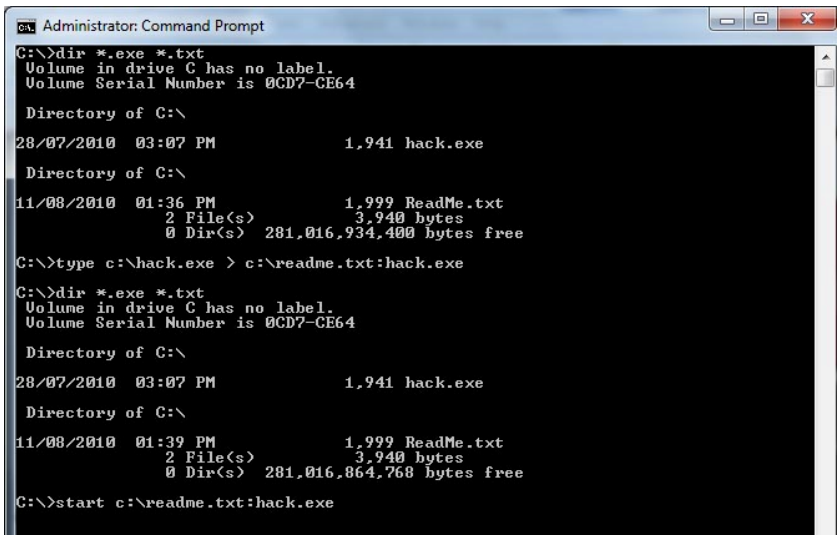


Figure 0.64 : Manipulation du flux NTFS

- **Nettoyer ou couvrir les traces**

Lorsque le pirate gagne l'accès administrateur et réussi à infiltrer le réseau, il essaye de supprimer la détection de sa présence en effaçant les fichiers qu'il a créé et en nettoyant les fichiers journaux des machines dans lesquelles il s'est introduit par la suppression des lignes relatifs à son activité sur le système.

Pour arrêter l'enregistrement dans les fichiers journaux:

C:\> auditpol /disable

Pour nettoyer les traces dans les fichiers journaux en utilisant l'outil *ELsave* :

C:\> elsave -s \\192.168.111.225 -l "Security" –C

Une fois terminé on démarre l'enregistrement de nouveau :

C:\> auditpol /enable

- **Installer une porte dérobée**

Quand le pirate termine son travail, il installe une porte dérobée ou trappe (*Backdoor*) qui est une faille de sécurité artificielle créée par une application pour obtenir un accès facile à l'avenir dans la machine victime. L'application utilisée est *netcat*. Le fichier exécutable *nc.exe* est d'abord copier chez la victime par l'ouverture d'une session par l'outil *Metasploit* et ensuite sera exécutée à distance à travers la session ouverte.

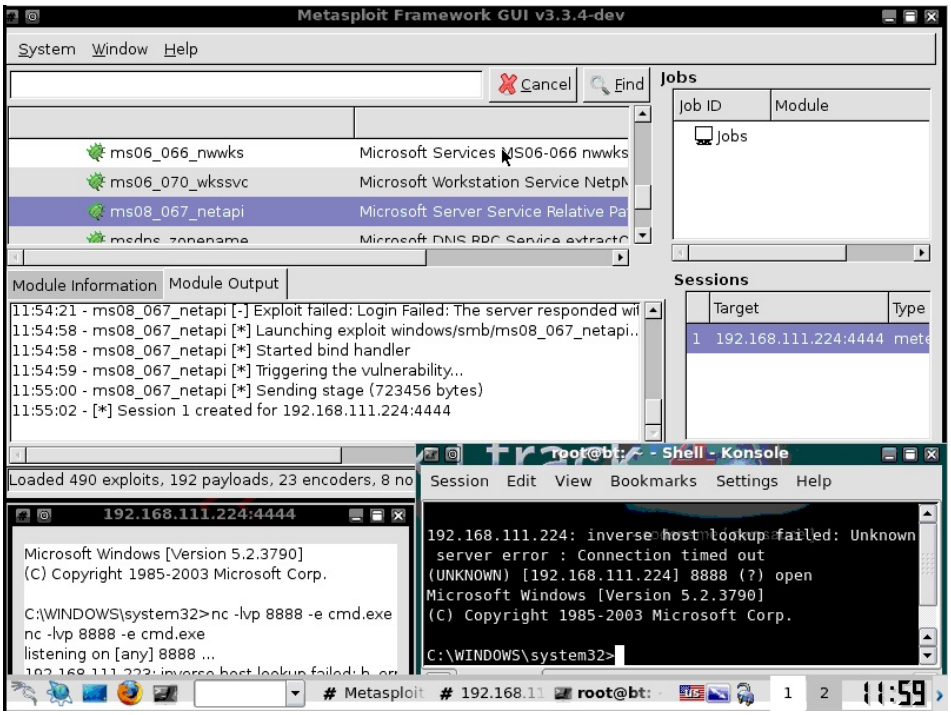


Figure 0.65 : Installation d'une porte dérobée

- **Recommandations**

Il est important d'implémenter des contre-mesures pour les outils que nous avons énumérés, afin d'éliminer les vulnérabilités de notre système. Voici quelques contre-mesures à prendre pour prévenir et remédier aux attaques déjà discuté :

- Définir des politiques de complexité des mots de passe
- Utiliser l'utilitaire *SYSKEY* pour stocker les clés cryptées sur le disque
- Surveiller les fichiers journaux du serveur générés par des attaques par force brute sur les comptes d'utilisateurs
- Surveiller les ouvertures de session échouées dans les fichiers journaux.
- L'utilisation des anti-virus et anti-spyware qui aident à identifier les trappes
- Blocage des ports et services inutilisés est essentiel pour éviter la création de portes dérobées.

b.2 Les maliciels (malware)

L'attaque des SE s'effectue non seulement directement par le pirate, mais à travers des logiciels malicieux élaborés par des pirates noirs pour nuire à ces systèmes. Le maliciel est un logiciel malveillant, développé dans le but de nuire à un système informatique. Les virus, vers et chevaux de Troie sont des exemples les plus connus :

- **Les virus**

Un virus informatique est un logiciel malicieux capable de se dupliquer à travers le réseau ou les moyens d'échange de données sur d'autres ordinateurs afin de nuire au fonctionnement du système et de la mémoire. Lorsqu'on l'exécute, il se charge en mémoire et accomplit des actions plus ou moins néfastes, allant de l'affichage d'un simple message à la perturbation grave du fonctionnement de l'ordinateur infecté et destructions de toutes les données. Les types de virus les plus rencontrés sont les chevaux de Troie et les vers.

- **Les vers :**

Logiciel autonome, utilise les connexions réseaux et les logiciels de messageries pour se propager, il consomme les ressources mémoire et la bande passante du réseau paralysant ainsi les ordinateurs.

- **Les chevaux de Troie :**

Programme exécutable mais caché dans un logiciel ordinaire gratuit ou commerciale, son but est de diffuser ou détruire les informations, ou ouvrir une porte dérobée pour son concepteur afin d'accéder et de prendre contrôle du système à distance.

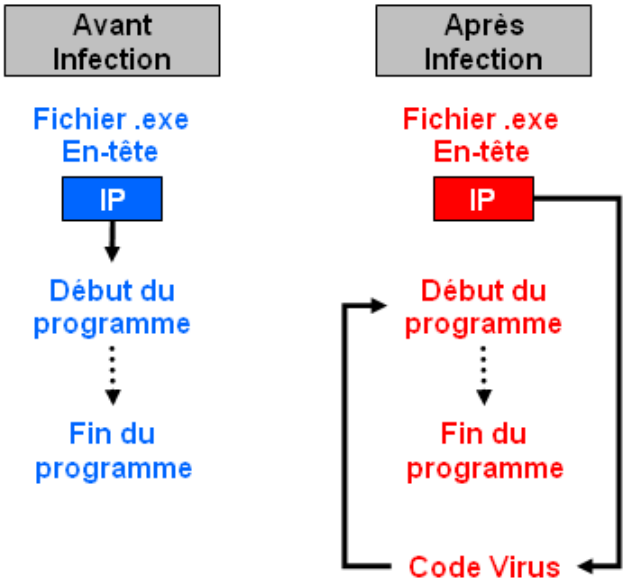


Figure 0.66 : Exécution d'un fichier avant et après infection par un maliciel
Figure : Référence: *CEH v5 Module 16 Virus and Worms*

L'injection des virus chez un poste client est une tache plus ou moins facile, la plus part des employés ont une curiosité innée qui leur pousse à ouvrir n'importe quel fichier reçu même s'il est d'un expéditeur étranger ou d'une forme soupçonneuse. Bien sur l'existence des antivirus complique cette tache, mais je prendrais le cas d'un utilisateur qui a reçu un message électronique contenant ce virus et l'a ouvert en dépassant l'anti-virus. Pour effectuer ce test, il faut d'abord choisir le virus ou l'application à injecter, dans ce cas j'ai choisi *netbus* dont l'exécutable s'appelle *patch.exe*, ensuite il faut lier cette application à un fichier régulier comme une image de type '*.jpg*' en utilisant l'outil *FileJoiner* une fois le poste est empoisonné j'ai utilisé l'outil *netbus* pour ouvrir une session à distance et contrôler totalement la victime.

Application

L'hors de l'exécution de ce test, l'antivirus a capté le virus *patch.exe* mais pour continuer le test j'ai désactivé l'antivirus pour poursuivre les étapes nécessaires

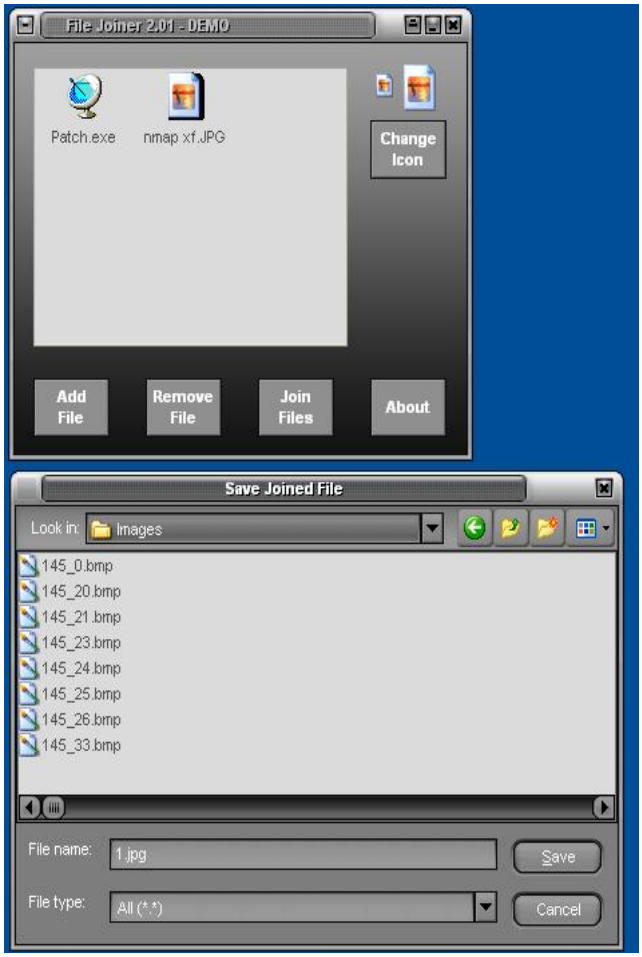


Figure 0.68 : Création de l'image contenant le virus

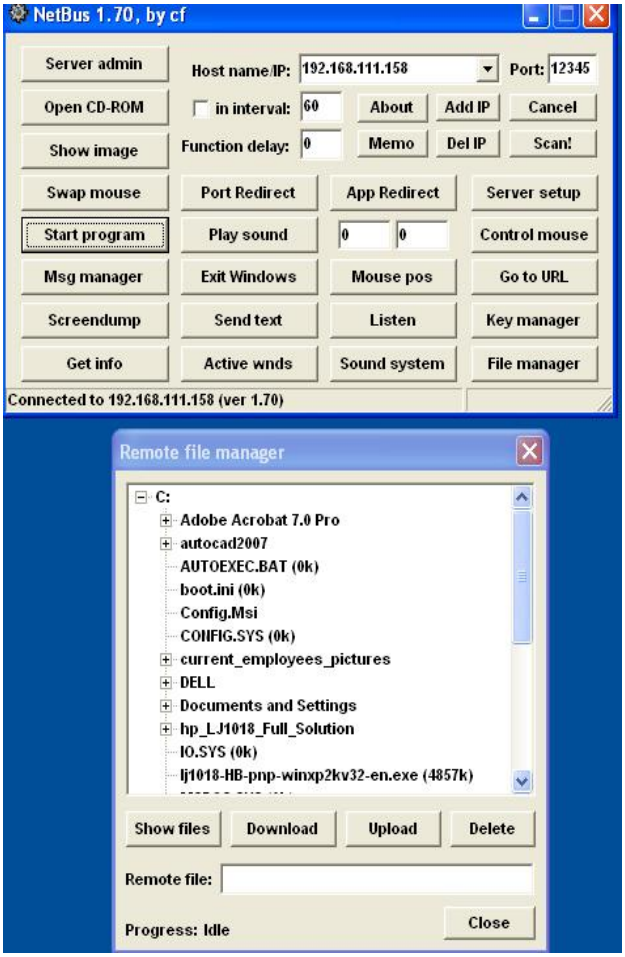


Figure 0.67 : Connexion à distance chez la victime

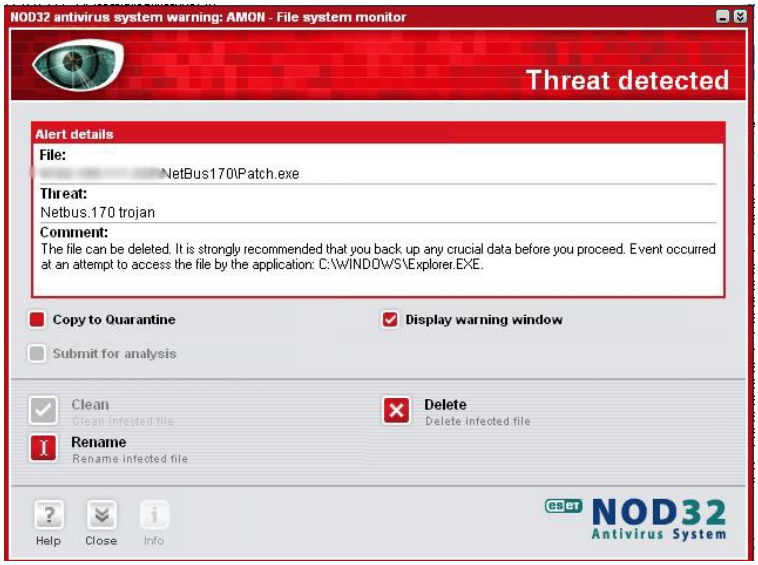


Figure 0.69 : Virus capté par l'antivirus

b.3 Les systèmes de messagerie

Les applications de messagerie constituent une menace à la sécurité car elles sont souvent négligées par les administrateurs qui pensent que les antivirus sont suffisants pour sécuriser les machines. En effet les courriers électroniques sont les plus ciblés par les pirates, ils peuvent transmettre des maliciels, arrêter les systèmes, obtenir un accès à distance, capter et modifier des informations confidentielles et connaître la configuration du réseau. Les attaques diffèrent selon les types des applications de messagerie :

- **Les messages électroniques (*email*)**

  - **Pièces jointes**

Le pirate envoi des milliers d'emails avec des larges pièces jointes qui paralysent le réseau et la mémoire de stockage de la machine. Pour éviter ce genre d'attaque, il faut limiter la taille de l'email ou des pièces jointes et allouer un espace mémoire fixe (*quota*) pour chaque utilisateur. Dans le cas de transfert de larges fichiers, il est préférable d'utiliser les services FTP ou http.

  - **Connexion**

Le pirate envoi des milliers d'emails simultanément à des adresses d'un même réseau causant une *attaque de connexion* ou *bombe de messages* où le serveur se bloque et arrête de travailler. Le pirate y prend avantage pour obtenir l'accès administratif sur le système. La limitation des ressources allouées et des requêtes sur le serveur de messagerie minimise l'occurrence d'une telle attaque ainsi qu'elle empêche une attaque par dénis de service.

  - **Réflexion**

Le pirate envoi des milliers d'emails de la part d'une adresse du réseau, ainsi tous les messages réponses retournerons vers la victime dont l'email sera bloqué ainsi que la bande passante et espace mémoire du serveur.

Application

D'abord pour avoir une liste des courriers électroniques des utilisateurs on utilise l'outil *ldap.exe* qui permet une connexion au service d'AD et obtention des informations de tous les utilisateurs. Cette liste sera importée dans un logiciel qui envoi des milliers de

courriers instantanément, utilisé d'habitude pour la distribution des bulletins électroniques *newsletter* dans lequel on ajoute plusieurs larges pièces jointes et on désigne l'adresse apparente de l'expéditeur qui est une adresse d'un utilisateur de l'organisation. Cette méthode permet donc de paralyser les ressources du serveur et plus tard abouti à mettre le domaine de l'entreprise dans la liste noire des expéditeurs.

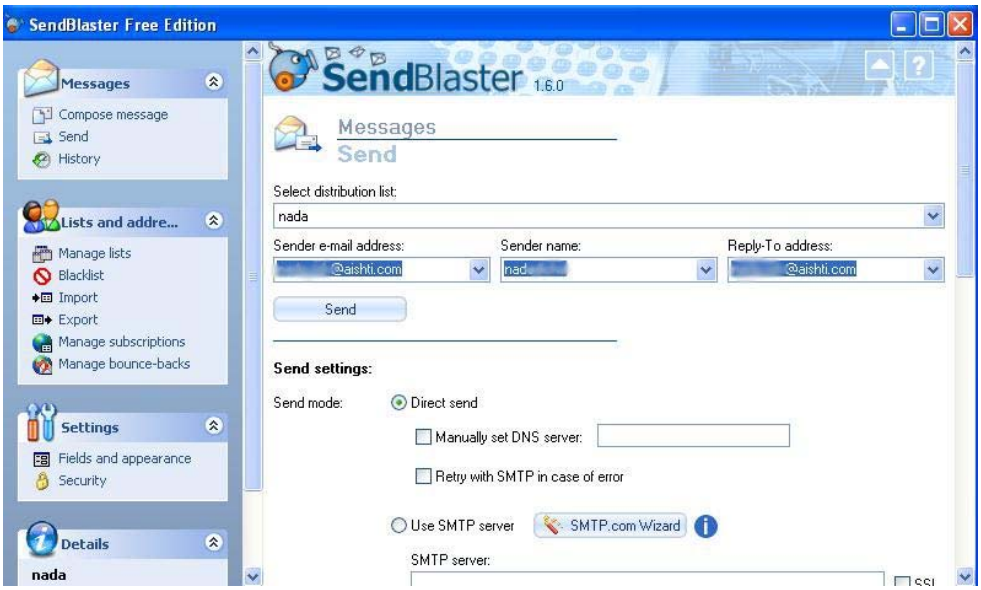


Figure 0.70 : Logiciel *SendBlaster* pour envoyer les courriers en masse

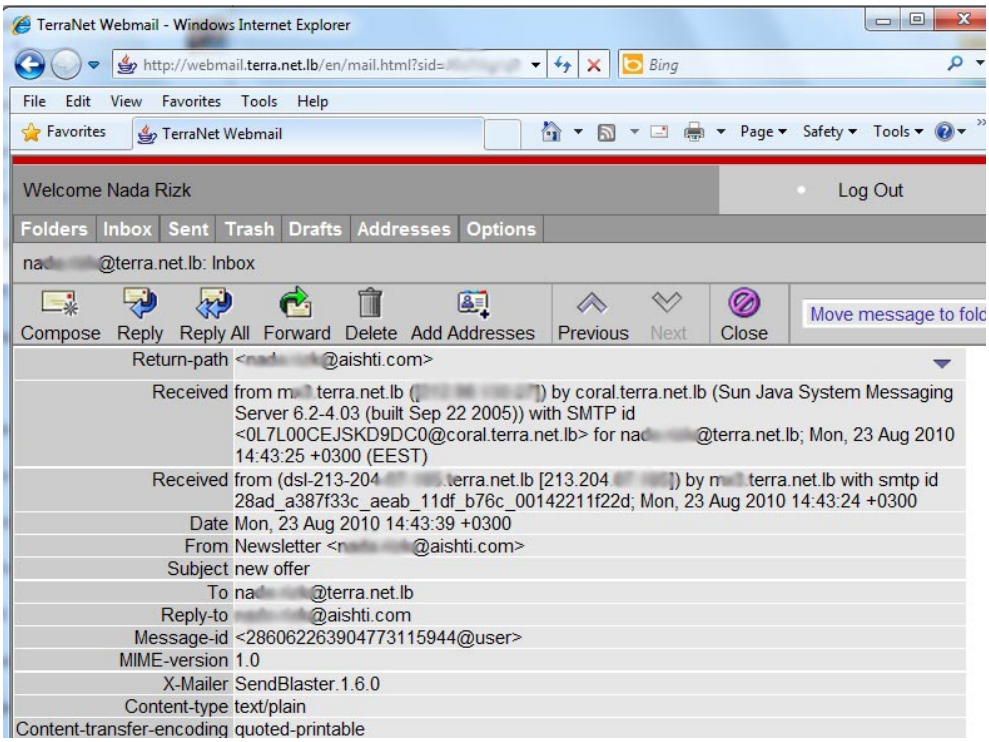


Figure 0.71 : Courrier livré apparent de la part d'un utilisateur de l'entreprise

Ce test n'a pas réussi à cause des systèmes de détection et de prévention d'intrusion (*IDP* ou *IPS*) qui ont détecté l'arrivée de plusieurs messages d'un même expéditeur simultanément et l'ont bloqué pour une période donnée, et un pare feu qui a filtré les messages à partir des critères prédéfinis par l'administrateur : sujet, contenu, expéditeur… Par contre on a pu envoyer les courriers de la part d'un utilisateur interne et causer le surpassement de la limite d'espace alloué à son compte.

- **Les bannières :**

La lecture des bannières affichées lors d'une connexion Telnet, par exemple, sur un serveur aide le pirate à connaître ces spécifications : logiciel, version, protocole, services… En connaissant les vulnérabilités du logiciel révélé, il choisira mieux les méthodes d'attaque. Pour éviter le dévoilement des données techniques et confidentielles résidents dans les serveurs, il est préférable de changer la bannière écrite par défaut et installer les derniers correctifs logiciels sur les serveurs. Le test des bannières est effectué sur tous les serveurs pertinents de l'entreprise, les résultats obtenus indiquent un échec de la connexion ou des bannières modifiées ne présentant aucune information sur le serveur ou sur ces spécifications.

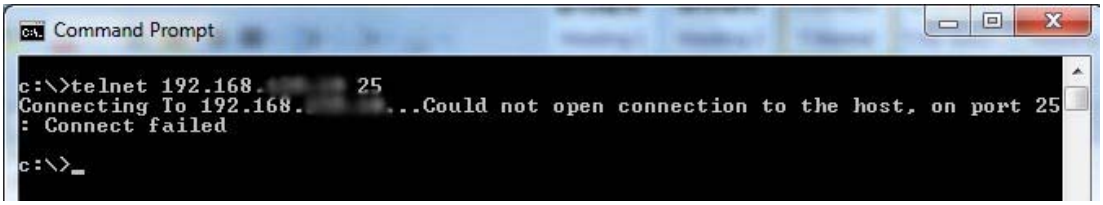


Figure 0.72 : Connexion échouée avec le pare-fu

Figure 0.73 : Bannière du pare-feu de messagerie modifiée

- **Les attaques Simple Mail Transfer Protocol (SMTP)**

Lorsque le pirate accède à un serveur par Telnet à travers le port 25 il peut utiliser quelques syntaxes communes comme VRFY ou EXPN pour révéler les utilisateurs existants et leur envoyer une attaque par bombe de messages. La meilleure solution contre ce type d'attaque dépend de l'administrateur, s'il n'utilise pas ces commandes, il doit les désactiver, sinon il peut limiter les personnes pouvant les exécuter sur le réseau.

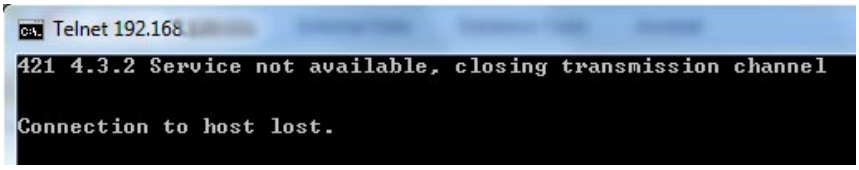


Figure 0.74 : Connexion SMTP échouée avec le serveur de messagerie à travers le port 25

L'utilisation des serveurs relais de messagerie (*Relay SMTP*) cause aussi des problèmes de sécurité car ils peuvent être utilisés par des pirates pour envoyer des messages spam au nom de la victime. La désactivation du service relais, s'il n'est pas utilisé, et l'imposition d'authentification sont les solutions pour ce genre d'attaque.

- **Les messages instantanés (*Instant Messaging - IM*)**

Cette technologie utilisée pour des raisons d'amusement ou de travail sérieux, présente aussi des vulnérabilités graves pour les systèmes informatiques :

- Usurpation des identités IM
- Lancement d'attaques de DoS
- Capturer les adresses IP
- Transfert des maliciels

La capacité de partage des fichiers qu'offrent les services IM crée une faille menaçante au réseau, elle ouvre un chemin d'accès et de contrôle à toutes les personnes connectées sur les ressources de la machine. La détection des vulnérabilités des services IM est difficile car c'est une application qui s'exécute localement chez les utilisateurs, mais il existe des outils de surveillance qui aident à détecter les trafics IM et les vulnérabilités résultantes. Bien sur dans ce cas aussi, l'utilisation de l'antivirus et l'application des correctifs logiciels aident à minimiser le danger de ce service.

Les services publiques des messages instantanés comme *MSN, GTALK, Yahoo*… sont bloqués chez la plus part des utilisateurs de l'organisation, diminuant ainsi les risques d'infection et de propagation des maliciels à travers les IM. Mais il existe un service de messagerie privé implémenté chez quelques employés appelé *Office Communication Server* (OCS) Le contrôle et filtrage du trafic peut être effectué sur le serveur comprenant ce service, interdisant tous les fichiers apparemment vulnérables.

J'ai effectué le test dans le cas de service public et privé et aucun fichier vulnérable n'a passé. La seule façon c'est de changer le type du fichier ou extension à *.txt* par exemple pour passer. Mais dans ce cas le destinataire doit rendre le type original pour exécuter le fichier ce qui est difficile à faire par rapport à un pirate.

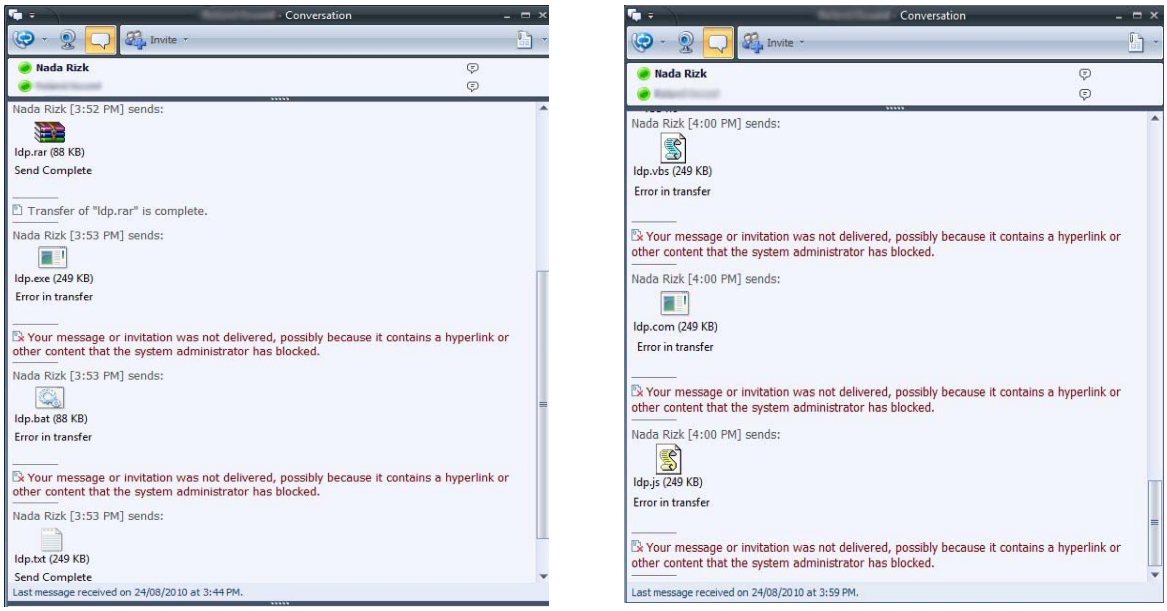


Figure 0.75 : Echec de transfert des fichiers vulnérables dans une communication IM privée

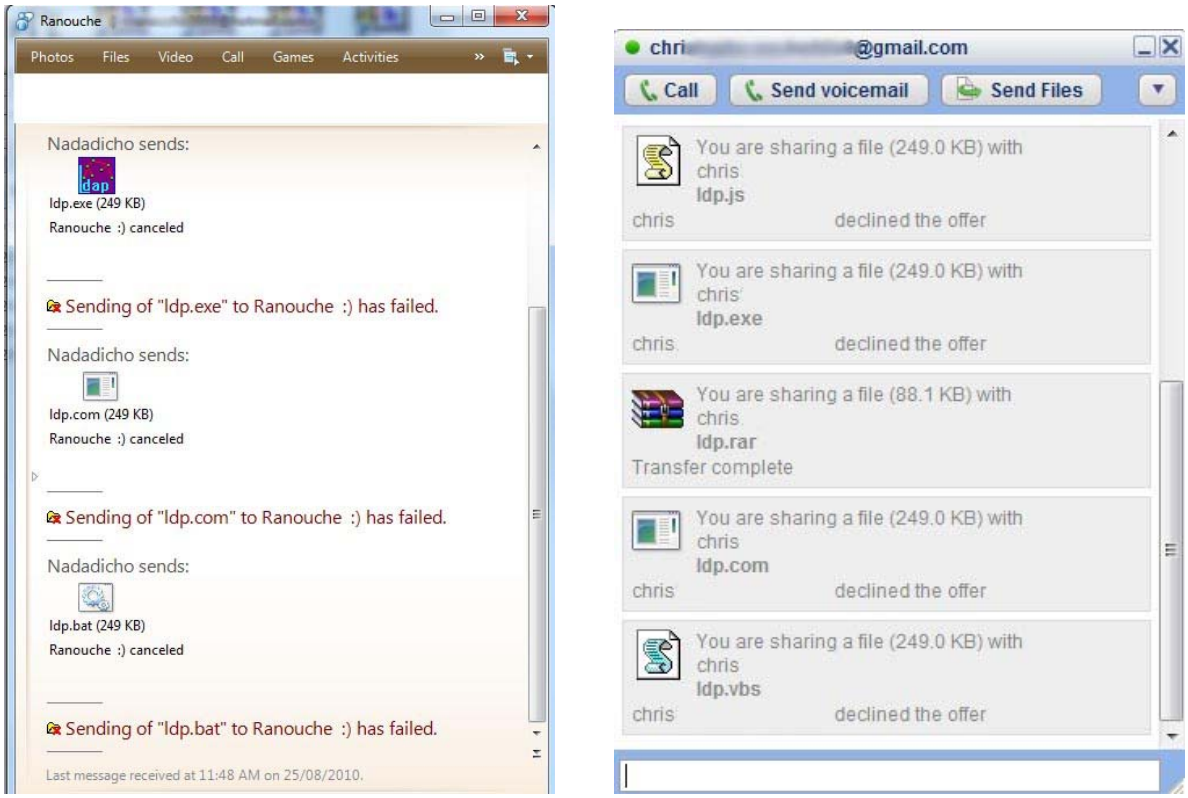


Figure 0.76 : Echec de transfert des fichiers vulnérables dans une communication IM publique

Comme le transfert des fichiers est contrôlé sévèrement, il reste une méthode d'infection à travers les adresses *URL*. Malheureusement l'utilisation de cette méthode est plus fréquente récemment car elle succède la plus part des fois. Ce genre d'attaque est contrôlé par la configuration des paramètres de l'application de messagerie ou par les pare-feux locaux ou des politiques de sécurité du domaine qui interdisent l'ouverture des adresses url soupçonnables.

b.4 Applications web

Les organismes publics et privés migrent leurs fonctions essentielles vers l'internet, ce qui incite et ouvre des possibilités aux pirates noirs d'accéder aux données pertinentes comme les informations sur l'entreprise, ses clients et ses employés à travers les applications web. Alors que la plupart des sites web sont fortement sécurisés au niveau du réseau avec des pares feu et des outils de chiffrement, ils autorisent l'accès des pirates aux données par la manipulation des applications web. Ces pirates attaquent les applications web en raisonnant comme les programmeurs, ainsi pour sécuriser ces applications il faut comprendre l'architecture des applications web, les techniques d'attaque utilisées par les pirates malveillants et les contres mesures de sécurisation.

- **Architecture des applications web**

Les applications web sont des entités à plusieurs niveaux de codes et de données formées par des parties publiques, accessibles directement ou indirectement de l'internet et d'autres parties privées, pour les employés à l'intérieur de l'entreprise. Une vulnérabilité dans n'importe quel niveau cause une faille de sécurité pour l'application web entière.

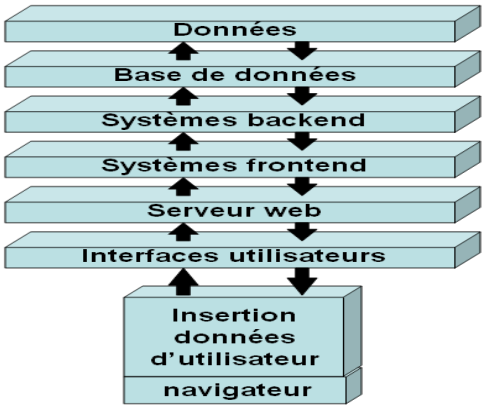


Figure 0.77 : Couches d'une application web
Référence: ***Auditing-and-Securing-Web-enabled-Applications***

- **Techniques d'attaque sur les applications web**

De nombreuses attaques contre les applications web sont de nuisances mineures et n'affectent pas les informations confidentielles ou la disponibilité du système. Cependant, certaines attaques causent des dégâts majeurs et arrêtent ces systèmes. Je discute ci-dessous quelques types d'attaques communs.

- **Processus d'identification insécurisés (login)**

La plupart des sites web exigent une identification des utilisateurs avant d'accéder à leurs ressources et services, ces mécanismes de connexion ne traitent pas généralement les identifiants et mots de passe d'utilisateur incorrects. Ils retournent souvent trop d'informations que les pirates utilisent pour recueillir les identifiants d'utilisateur et leurs mots de passe. Ces messages d'erreur de connexion précisent quel paramètre est erroné, mais d'un autre côté assurent aux pirates quel paramètre est correcte !

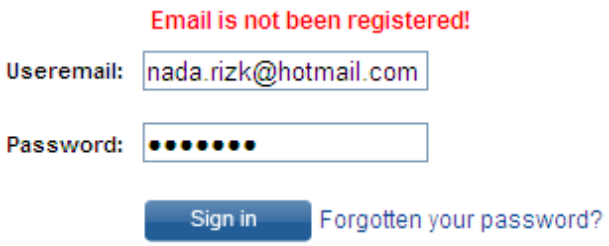


Figure 0.78 : Message de connexion erronée

Pour prévenir ce genre d'attaque, il faut unifier le message d'erreur pour être ambigu, par exemple : « *Identifiant ou mot de passe erroné* », et annuler les codes d'erreur retournés automatiquement par les serveurs

- **Manipulation des adresses URL**

Les pirates accèdent à des sites avec des ports différents que le port 80 usuel des pages web, si ces ports ne sont pas bloqués, ils peuvent accéder à des pages ou données confidentielles, ou utiliser les données retournées par les messages d'erreur pour obtenir des informations sur le site et serveur attaqué. Le blocage des ports inutilisés et changement du message d'erreur est essentiel pour arrêter ce type d'attaque.

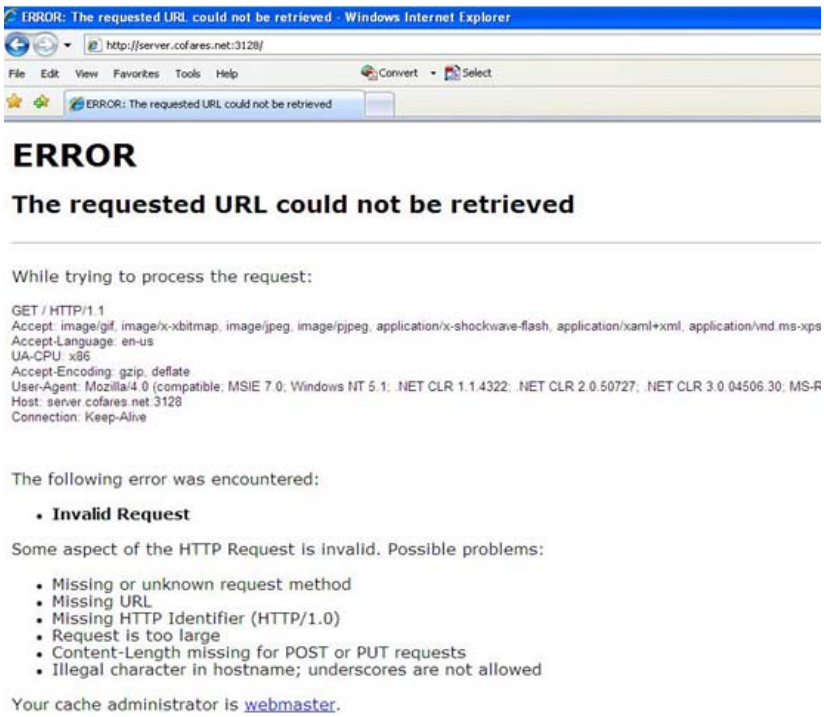


Figure 0.79 : Message d'erreur d'un site accédé par un port erroné

- **Balayage des directoires des serveurs web**

Les pirates utilisent des outils pour balayer les serveurs web et découvrir toutes les directoires et fichiers accessibles par le public et accèdent ainsi aux données confidentielles de l'entreprise. Les administrateurs de ces serveurs doivent éliminer tous les fichiers confidentiels des directoires principaux du serveur et s'assurer des permissions attribuées aux fichiers réservés aux employés, partenaires ou public.

- **Données mal formées en entrée**

Les applications web acceptent généralement tout type de données en entrée sans validation. Plusieurs attaques peuvent être lancées contre ces applications en insérant plusieurs données mal formées simultanément, ce qui peut engendrer une confusion, un accident ou dévoilement d'informations à l'attaquant.

Les pirates peuvent causer un débordement de tampon en manipulant la longueur du texte inséré, un DoS en registrant des milliers d'utilisateurs à la base de donnée du serveur ou injecter un code erroné en modifiant des paramètres dans les adresses url dans la barre d'adresse du navigateur.

La validation des données en entrée est la meilleur façon pour faire face aux attaques listées, le programmeur doit vérifier la longueur des données, le nombre et type des paramètres et

désactiver les *JavaScripts* pour arrêter les codes dynamiques. La manipulation de n'importe quel paramètre doit empêcher l'accès au serveur.

La plupart des vulnérabilités des applications web reposent sur la capacité d'insérer des données invalides ou un code malveillant dans l'application à l'aide de plusieurs techniques. Ils existent des outils capables d'effectuer automatiquement l'évaluation des vulnérabilités dans les applications web en essayant toutes les attaques de piratage possibles et générant des rapports sur les attaques réussis et gravité des vulnérabilités trouvées. Mais le procédé de sécurisation doit être effectué finalement par l'administrateur du système en appliquant toutes les contre mesures discutées, convenables à chaque type d'attaque.

- **Captage des sessions sécurisées**

Afin de sécurisées les pages web confidentielles de l'organisation, on a recours au protocole sécurisé *HTTPS* (port 443 TCP), de cette façon le trafic sur ce site sera crypté et difficile à être capté et déchiffré par un pirate connecté au réseau. Mais il ne faut pas oublier de vérifier la méthode d'authentification sur ce genre de sites. Ces méthodes peuvent envoyer les noms des utilisateurs et leur mots de passe en plein texte comme *Basic Authentication* ou cryptés comme *Integrated windows authentication.*

Application

Le site public de l'organisation est hébergé dans le serveur de l'entreprise qui l'a créé et responsable de sa maintenance. Mais il existe l'application web des messages électroniques qui existe à l'intérieur de l'organisation et est accessible de l'internet. Le premier test consiste à essayer le processus d'identification avec des données erronées :

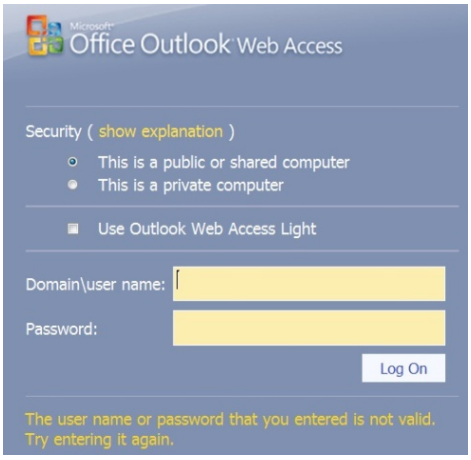


Figure 0.80 : Message d'erreur ambigu

L'essai de manipulation de l'adresse URL retourne un message d'erreur indéfini ou réoriente vers la page principale. L'essai d'outil de balayage ou d'accès retourne un message d'erreur indiquant un accès interdit.

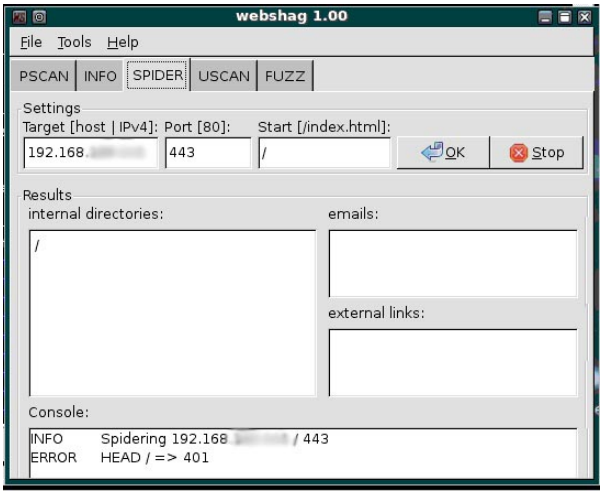


Figure 0.81 : Accès interdit sur le serveur

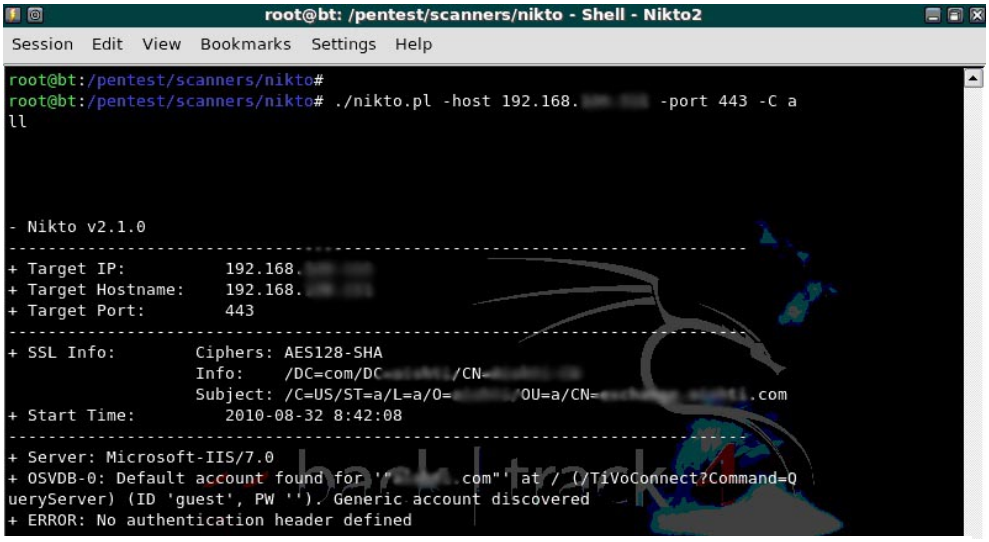


Figure 0.82 : Accès de balayage interdit sur le serveur

L'essai de captage d'une ouverture de session avec le serveur retourne le trafic contenant le nom de l'utilisateur et son mot de passe malgré l'utilisation du protocole sécurisé *HTTPS*, le problème réside donc dans la méthode d'authentification qui doit crypter les données confidentielle de l'utilisateur.

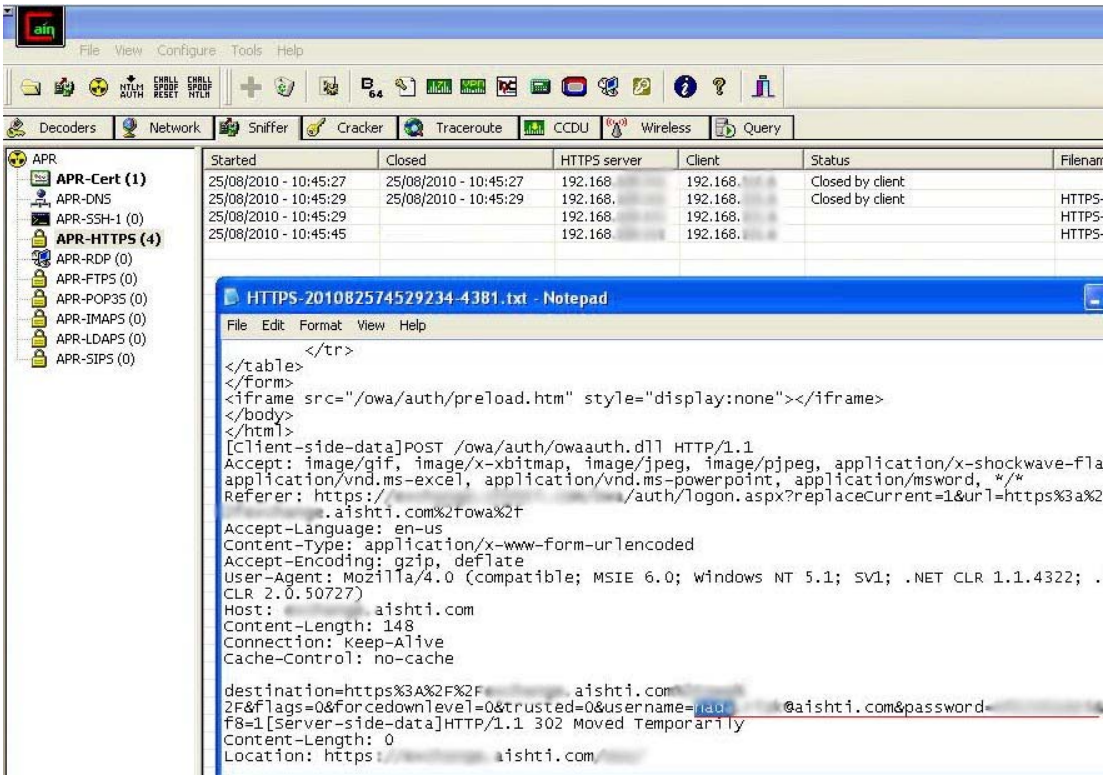


Figure 0.83 : Captage de session sécurisée HTTPS avec le serveur de messagerie

b.5 Injection de code SQL

C'est une attaque visant les applications interagissant avec des bases de données. Elle consiste à exploiter les fichiers système de la base de données et à injecter des commandes de type *Structured Query Language* (SQL) dans les requêtes qui passent les paramètres de l'application vers la base de donnée, ainsi si le concepteur n'effectue aucun contrôle sur les paramètres passés, il est possible à un pirate de modifier la requête et d'obtenir un accès aux ressources ou manipuler les données.

Les étapes d'attaque par injection SQL sur une base de données ORACLE sont :

- Balayage pour trouver le port du *TNS-Listener* qui contient les paramètres de connexion à la base de données
- Enumération du *TNS-Listener* pour obtenir des informations : version, IP, statut, nom du connecteur (System ID - SID)…
- Si *TNS-Listener* est sécurisé on utilise le system de recherche par force brute pour obtenir le SID
- Connexion avec la base de donnée par commande *sqlplus*
- Extension de privilèges par injection de code

- Scanner les identificateurs faibles
- Injection de code manipulant

Application

- **Trouver le TNS-Listener**

L'utilisation de la commande *NMAP* dévoile les ports accessibles chez le serveur victime, si le service *TNS-Listener* est présent on obtient le port 1521/TCP ouvert par Oracle. Ce test a réussi sur notre serveur de base de données oracle.

- **Enumération du TNS-Listener**

La commande *tnscmd* récupère les informations nécessaires du fichier *TNS-Listener* et permet d'injecter des codes SQL pour manipuler les paramètres de configuration de la base de données.

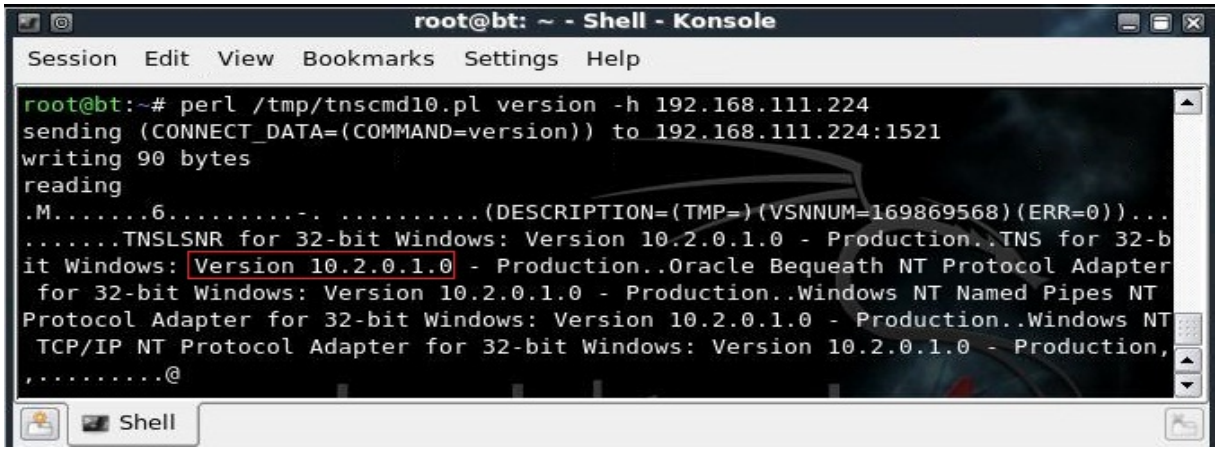


Figure 0.84 : Version de l'Oracle obtenue par *tnscmd*

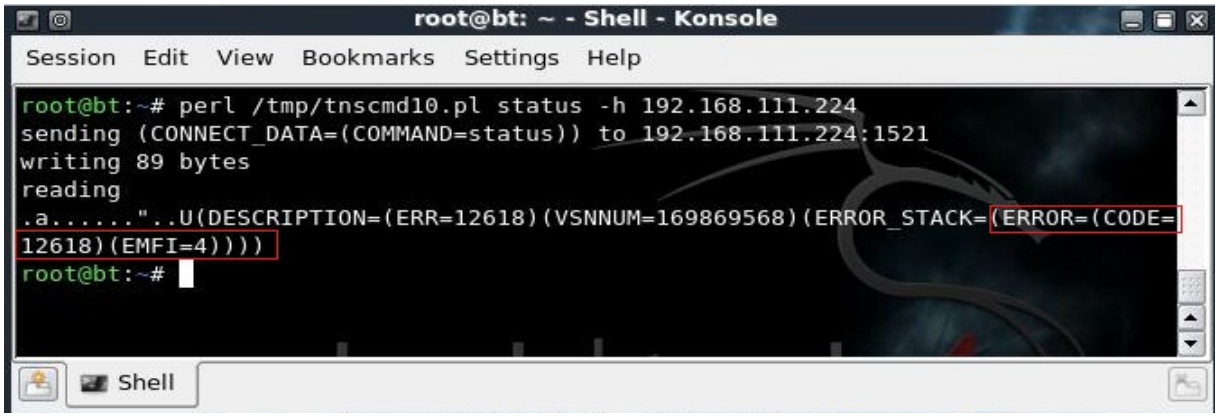


Figure 0.85 : Privilèges insuffisants pour obtenir le statut de la base de données oracle par *tnscmd*

La version d'oracle dévoilé est *10g*, le *TNS-Listener* est sécurisé donc on essai le moteur de recherche par force brute pour trouver les noms des connecteurs aux bases de données ou *SID* ou une méthode plus facile qui est l'accès par page web.

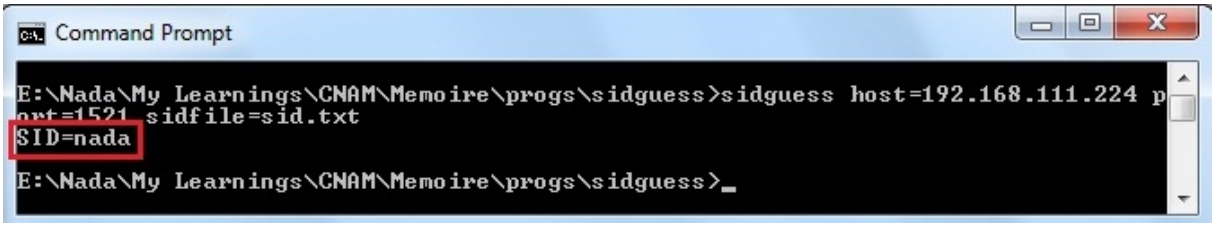


Figure 0.86 : Outil *sidguess* pour chercher les SID

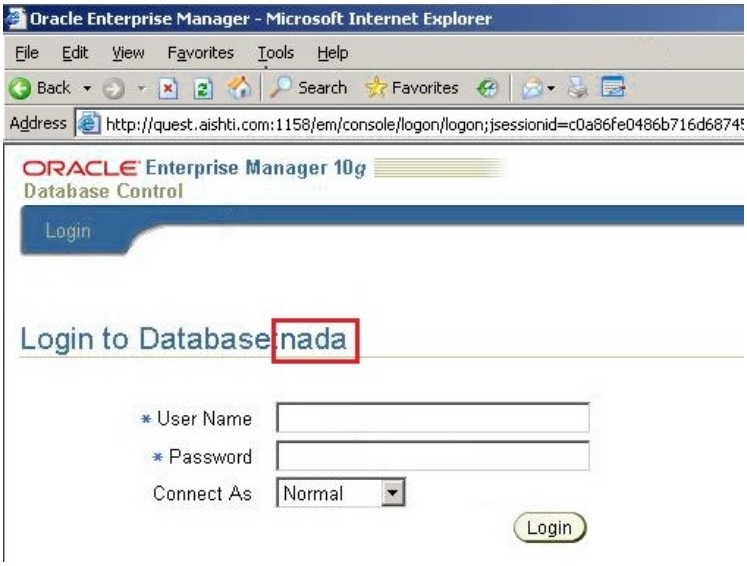


Figure 0.87 : Accès web sur le serveur de base de données

- **Connexion avec la base de donnée par commande *sqlplus***

La première étape consiste à accéder la base de donnée même si c'est avec un utilisateur à privilèges limités.

La deuxième étape est l'utilisation des quelques commandes sql pour obtenir plus d'informations, comme les tables existantes et leurs propriétaires, les rôles de sessions les objets de la base de données...

select * from v$version;
select * from all_users;
select * from session_roles;
select owner, table_name from all_tables;

Figure 0.88 : Connexion *sqlplus* avec utilisateur commun

Les commandes utilisées ont révélé les tables pertinentes de la base de données et j'ai pu manipuler ces tables et obtenir le mot de passe de l'administrateur du logiciel. La vulnérabilité découverte dans cette partie est d'une importance très élevée, n'importe quel utilisateur pourra détruire une base de données entière grâce aux privilèges qui lui sont assignés.

- **Extension de privilèges par injection de code**

Dans le cas ou l'utilisateur n'avais pas de privilèges on manipule le fichier de librairie oraclient10.dll en changeant une commande *ALTER SESSION SET NLS LANGUAGE* par *GRANT DBA TO PUBLIC*, à la prochaine ouverture de session le code sera exécuté et l'extension de privilèges sera acquise.

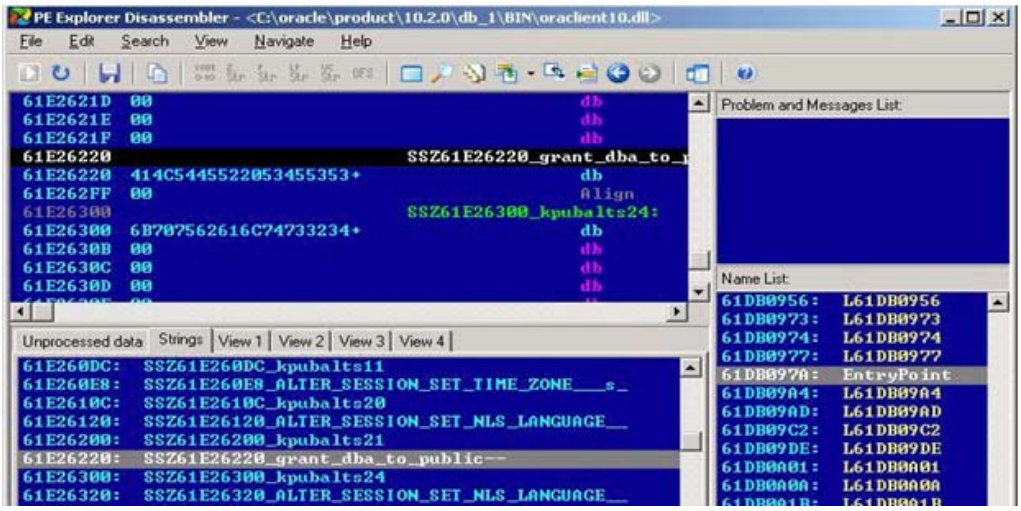


Figure 0.89 : Manipulation du fichier *oraclient10.dll*

Malgré l'obtention du rôle DBA cet utilisateur n'a pas pu accéder aux tables systèmes contenant les mots de passe des utilisateurs système car il faut obtenir les privilèges de SYS.

Figure 0.90 : Accès interdit aux tables systèmes

- **Scanner les identificateurs faibles**

On peut utiliser l'outil *checkpwd* pour scanner les utilisateurs existants dans la base de données afin de dévoiler les identifiants faibles. Ce test a repéré plusieurs identifiants dans notre base de données, mais la plus part sont expirés et fermés.

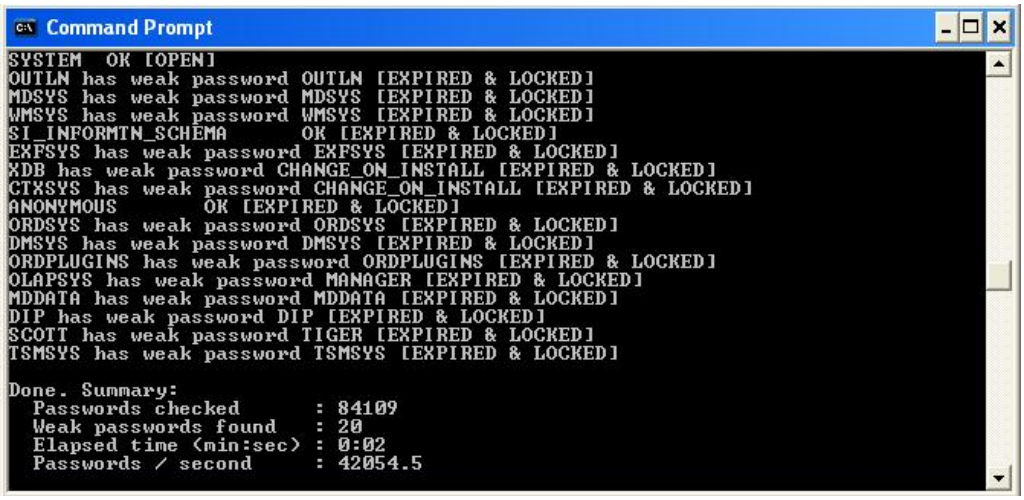


Figure 0.91 : Résultat de l'outil *checkpwd*

- **Injection de code manipulant**

Le pirate manipule la requête en insérant un type de caractères qui changent l'enchaînement de cette requête et exécute une autre commande. Un exemple de requête typique d'une session d'identification d'un utilisateur sur un site :

***SELECT * from** clients **where** nom= "$nom"*

Le pirate insert un nom tell « ***toto" OR 1=1 --*** » alors la requête devient :

SELECT * from** clients **where** nom= "toto" **OR** 1=1 **-- remarques

Cette requête sera toujours valide et retournera la liste de tous les utilisateurs.

J'ai essayé plusieurs types de manipulation de la requête est aucun n'a pus falsifier l'authentification du logiciel qui retourne un message ambigu ne précisant pas quel paramètre est erroné. Voila quelques genres de manipulation :

' or 1=1--

" or 1=1--

' or 'a'='a

" or "a"="a

') or ('a'='a)

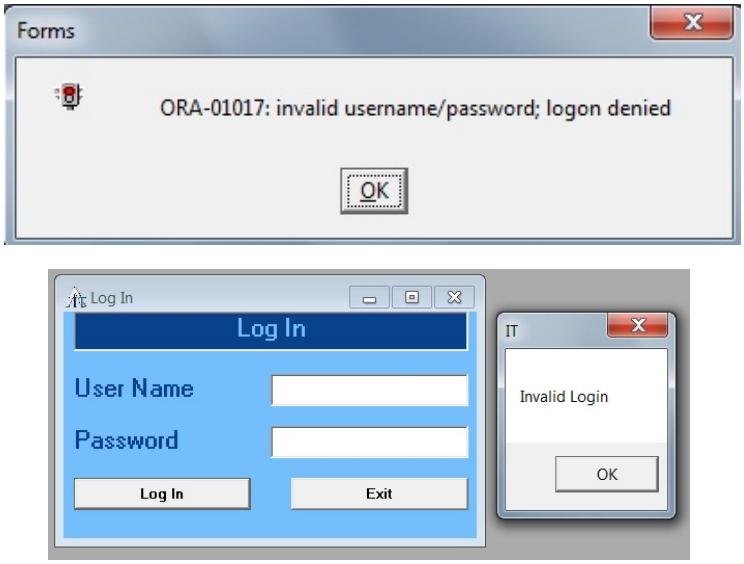


Figure 0.92 : Résultat d'authentification manipulée

Les tests d'injection par commande SQL ont permis d'identifier les vulnérabilités existantes dans notre système, les utilisateurs réguliers peuvent accéder et manipuler facilement les tables de l'administrateur mais on n'a pas pu avoir le mot de passe des utilisateurs système : SYS, SYSTEM… car les tables systèmes sont sécurise même pour ceux qui ont le rôle DBA. D'autre coté la manipulation du code dans une session d'authentification a aussi échoué ce qui indique un bon codage d'authentification.

Plusieurs méthodes permettent d'éviter les attaques par injection de commandes SQL :

- Vérification et validation des données en entrée
- Messages d'erreurs implicites
- Supprimer les comptes inutilisés
- Limiter l'accès aux comptes réguliers
- Remplacer le SQL dynamique par des procédures stockées

c. Résultats

Les résultats des attaques effectuées au niveau de la couche application sont variés, parfois une réussite d'accès totale comme dans l'attaque du SE, mais d'autre fois un échec total comme le cas des messageries ou manipulation du code sql d'authentification. Néanmoins, on peut considérer que les données révélées sont d'une grande importance et constituent une menace sur les ressources pertinentes de l'entreprise.

Table 0-X : Résultats des tests de la couche Application

	Date des tests	Vulnérabilités / Etat	Risques / Impact	Résultat
Systèmes d'exploitation	13/7/2010	Plusieurs postes sans mot de passe Mot de passe facile à craquer	Accessibilité parfois facile	compromis
Maliciels	10/8/2010	Quelques postes sans anti-virus Le reste totalement sécurisé	Etat acceptable	Non compromis
Messagerie	21/8/2010	Présence d'IDS et pare-feu Messagerie instantanée sécurisées Bannières ambigües Session d'authentification en plein texte	Accessibilité complexe	Non compromis
Application Web	25/8/2010	Message d'erreur ambigu Balayage sur serveur interdit Captage de session HTTPS à cause de méthode d'authentification en plein texte	Accessibilité parfois possible	Parfois compromis
Injection de code SQL	1/9/2010	Utilisateurs réguliers avec privilèges administratifs	Accessibilité aisée	compromis

3.2.6.5 Récapitulation des résultats obtenus

Les résultats des tests effectués ont été signalés à la fin de chaque partie, on peut récapituler ces résultats dans un tableau divisé par catégories pour indiquer à la direction le classement des risques trouvés.

Table 0-XI : Classification des vulnérabilités internes et externes

Vulnérabilité internes	Vulnérabilités externe
chambres insécurisées	clients des restaurants
points d'accès sans fil insécurisés	utilisateurs distants (messageries)
configuration par default	clients des magasins
administrateurs sans mot de passe	pirates sur internet
prises réseaux disponibles	
employés malveillants	
ordinateurs non verrouillés	
faible clé wep	
faible mots de passe	
utilisateurs avec accès privilégié	
ports communs ouverts	
faibles SID (Oracle)	

Il faut prioriser les problèmes trouvés pour éviter de perdre le temps avec quelques vulnérabilités difficiles à éliminer à cause des raisons techniques ou financières. Cette priorité peut être évaluée suivant deux critères : Risques d'utilisation et Impacts d'exploitation.

Table 0-XII : Rapport Risque / Impact des vulnérabilités

Risques / Impacts	Grave	Moyen	Faible
Grave	Points d'accès sans fil insécurisés Configuration par default	Manque de mot de passe Chambres insécurisées Utilisateurs avec accès privilégié	Messagerie en plein texte Clients
Moyen	Access Internet aux utilisateurs	Ordinateurs non verrouillés Partage de fichiers publics Employés malveillants Ports communs ouverts	Prises réseaux disponibles Faible clé WEP Faible mots de passe Pirates sur internet
Faible	Anti-virus non mis-à-jour Pare-feu désactivé	Pas de chiffrage Faibles SID (Oracle) Utilisateurs distants	Personnel de nettoyage ayant accès Ports non communs ouverts

3.3 Politique de sécurisation

Les approches correctives sont divisées selon les couches du protocole TCP/IP discutées dans les étapes précédentes, la variation de ces niveaux assure la sécurisation du système de différents angles au cas où l'une des mesures échoue. Le processus de sécurisation consiste à proposer les mesures correctives, obtenir l'approbation des directeurs et implémenter les propositions acceptées.

3.3.1 Propositions

Afin de planifier le travail à effectuer les propositions sont divisées dans un tableau selon les taches correctives dans chaque branche.

3.3.1.1 Couche Accès réseaux

Table 0-XIII : Solution de sécurisation au niveau de la couche Accès réseaux

Site	Solution	Arrêt système	Durée	Coût
HO	Ajout camera dans la chambre du serveur	Non	1h	400$
	Ajout point de détection de mouvement	Non	1h	50$
	Ajout détecteur de chaleur et humidité	Non	6 hrs	3150$
	Soulever plancher de la salle serveur	Oui	10 hrs (nuit)	1500$
	Changement du mur en glasses pour être rigide et opaque	Non	2 semaines	1500$
DT	Changement de l'emplacement de la chambre	Non	1 mois	10000$
	Equipement complet de la nouvelle chambre	Non	2 semaines	30000$
	Enregistreur + cameras			
	Détecteur de mouvement, chaleur et humidité + composeur automatique			
	System de contrôle d'accès			
	Soulever plancher de la salle serveur			
	Rack et nouveau câblage			
SS	Changement du rack	Oui	2 hrs	1000$
	Ajout détecteur de chaleur et humidité	Non	1 jour	3150$
	System de contrôle d'accès	Non	4 hrs	300$
WH	Isolation des appareillages dans une chambre fermée	Non	1 semaine	1000$
ABC CM VR SK	Isolation des appareillages dans une chambre fermée avec AC, camera, détecteur d'humidité et feu	Non	1 semaine	5000$ /site

Quelques propositions sont communes à toutes les branches, il faut vérifier toutes les prises vides et les débranchées du réseau et il faut sensibiliser les utilisateurs par des formations à base régulière.

3.3.1.2 Couche Internet

Table 0-XIV : Solution de sécurisation au niveau de la couche Internet

Vulnérabilité	Risque	Impact	Solution
Configuration par default	Grave	Grave	Personnalisation des configurations
Point d'accès sans fil insécurisé ou faible clé WEP	Grave	Grave	Sécurisation par clé WEP complexe
Large diffusion des signaux des points d'accès sans fil	Faible	Grave	Diminution ou élimination des diffusions
Faible mots de passe	Faible	Moyen	Mot de passe complexe
Ports commun ouverts	Moyen	Faible	Désactivation des ports et protocoles vulnérables
Écoute et empoisonnement du trafic sur le réseau	Moyen	Moyen	Authentification et cryptage des sessions
Surcharge et blocage des ressources	Moyen	Grave	Politiques de filtrage des paquets Utiliser un IDS Bloquer les paquets *ping* volumineux au niveau du routeur et du pare-feu.
Usurpation des requêtes passantes dans le réseau	Faible	Grave	Configuration de sécurisation des ports des commutateurs

Une durée de 2 semaines est prévue pour implémenter les solutions de cette couche dans toutes les branches. Aucun cout n'est requis pour les solutions de modification de configuration logicielle.

Il existe deux solutions pour l'implémentation d'un système IDS/IPS :

- Dispositif de Cisco ou HP coute environ 9000$
- Ajout d'un module *Cisco Advanced Inspection and Prevention Security Services Module (AIP-SSM)* au pare-feu coute 3500$

3.3.1.3 Couche Transport

Table 0-XV : Solution de sécurisation au niveau de la couche Transport

Vulnérabilité	Risque	Impact	Solution
Port et service FTP ouvert	Moyen	Moyen	Ajout d'identificateurs ou désactivation du service FTP
Identificateur du protocole SNMP commun (CS)	Moyen	Faible	CS complexe de type lire ou désactivation du service SNMP
Administrateur local sans mot de passe (attaque SMB)	Moyen	Grave	Ajout mot de passe complexe
Partage de fichier public	Moyen	Moyen	Annuler service de partage (SMB)
Surpassement du SSL	Moyen	Moyen	Activation des pare-feu pour bloquer les intrusions

Une durée de 2 semaines est prévue pour implémenter les solutions de cette couche dans toutes les branches. Aucun cout n'est requis pour cette tache.

3.3.1.4 Couche Application

Table 0-XVI : Solution de sécurisation au niveau de la couche Application

Vulnérabilité	Risque	Impact	Solution
Mots de passe faciles	Moyen	Moyen	Imposer la politique de complexité
Utilisateurs privilégiés	Moyen	Grave	Limitation des privilèges des utilisateurs réguliers
Anti-virus non mis-à-jour Pare-feu désactivé	Grave	Faible	Inspection de tous les postes pour activation et mis-à-jour des anti-virus
Accès internet aux utilisateurs	Grave	Moyen	Filtrage du trafic
Portes dérobées	Moyen	Grave	Surveillance des fichiers journaux
Messagerie en plein texte	Faible	Grave	Cryptage du trafic Sensibilisation des utilisateurs
Session d'authentification en plein texte	Moyen	Grave	Cryptage des sessions d'authentification
Utilisateurs d'e-mails distants	Moyen	Faible	Filtrage des messages (spam) Sensibilisation des utilisateurs
SID faciles	Moyen	Faible	SID complexe
Liste des utilisateurs non mis-à-jour	Moyen	Moyen	Supprimer les identifiants des utilisateurs éliminés
Circulation des données confidentielles dangereusement	Grave	Grave	System de protection et contrôle des données (right management service)

Une durée de 2 semaines est prévue pour implémenter les solutions de cette couche dans toutes les branches. Le seul coût requis pour cette couche est le prix des licences pour le

système de protection et contrôle des données (Right Management Service) qui est 30$ par utilisateur. En général on a besoin de 100 licences donc, un budget de 3000$.

La sensibilisation des utilisateurs est une tache corrective valable pour toutes les couches étudiées, une formation doit être dirigée suivant chaque catégorie d'employés, en générale elle doit englober les idées suivantes :

- Verrouiller les ordinateurs
- Mot de passe complexe
- Stockage des données confidentielles
- Partage des fichiers correctement
- Fuite de données confidentielles aux étrangers : conversations, e-mails, messagerie…
- Détruite des données avec des déchiqueteuses
- Confiance des expéditeurs avant d'ouvrir les e-mails et pièces jointes
- Téléchargement des fichiers vulnérables de l'internet

3.3.2 Approbation

La récapitulation des études suivis et résultats obtenus, avec la liste des politiques de sécurisation ont été présentés à la direction de l'entreprise afin d'obtenir l'approbation aux solutions proposées. Ces solutions ont été discutées avec la direction, quelques unes sont accordées et d'autre éliminées pour des raisons financières ou fonctionnelles. Les tableaux suivants synthétisent les réponses obtenues.

3.3.2.1 Couche Accès réseaux

Table 0-XVII : Approbation des solutions au niveau de la couche accès réseau

Site	Solutions	Coût	Statut	Raisons
HO	Ajout camera dans la chambre du serveur	400$	Accordée	
	Ajout point de détection de mouvement	50$	Pas besoin	Tous les points d'accès sont contrôlés par des détecteurs
	Ajout détecteur de chaleur et humidité	3150$	Ajournée	système d'alarme incendie suffisant pour le moment
	Soulever plancher de la salle serveur	1500$	Refusée	Câblage complexe, difficulté de changer l'aménagement
	Changement du mur en glasses pour être rigide et opaque	1500$	Refusé	Pour ne pas changer l'aspect décoratif de l'endroit
DT	Changement de l'emplacement de la chambre	10000$	Accordée	
	Equipement complet de la nouvelle chambre	30000$	Accordée	
SS	Changement du rack	1000$	Accordée	
	Ajout détecteur de chaleur et humidité	3150$	Refusée	système d'alarme incendie suffisant pour le moment
	System de contrôle d'accès	300$	Accordée	
WH	Isolation des appareillages dans une chambre fermée	1000$	Accordée	
ABC CM VR SK	Isolation des appareillages dans une chambre fermée avec AC, camera, détecteur d'humidité et feu	5000$ /site	Ajournée	L'aménagement existant est suffisant pour le moment. Possibilité d'exécution en cas de rénovation comme dans VR
Tous	Débrancher les prises inutilisées du réseau	0 $	Accordée	

Le coût total des corrections proposées au niveau de la couche accès réseau est : **57700$**

On remarque qu'une grande partie est réservée pour la branche DT qui est une des deux branches principales contenant les ressources informatiques vitales de l'organisation.

3.3.2.2 Couche Internet

Table 0-XVIII : Approbation des solutions au niveau de la couche Internet

Solutions	Statut	Raisons
Personnalisation des configurations	Accordée	
Sécurisation par clé WEP complexe	Accordée	Pas de clé pour les points d'accès publics, le réseau sera isolé
Diminution ou élimination des diffusions	Accordée	Pour les points d'accès internes
Mot de passe complexe	Accordée	
Désactivation des ports et protocoles vulnérables	Accordée	Quelques ports sont nécessaires pour des services secondaires
Authentification et cryptage des sessions	Pas besoin	Cause surcharge du trafic interne Déjà implémenter dans le trafic externe
Filtrage ou blocage des paquets Implémentation d'un IDS	Accordée	Ajout du module IDS/IPS au pare-feu cisco
Configuration de sécurisation des ports des commutateurs	Accordée	Risque de surcharge des commutateurs Mis-à-jour régulière des listes

Le coût total des corrections proposées au niveau de la couche internet est : **3500$**

3.3.2.3 Couche Transport

Table 0-XIX : Approbation des solutions au niveau de la couche Transport

Solutions	Statut	Raisons
Ajout d'identificateurs ou désactivation du service FTP	Accordée	
CS complexe de type lire ou désactivation du service SNMP	Refusée	Le service SNMP est nécessaire pour l'obtention régulière des informations des postes clients pour le contrôle journalier.
Ajout mot de passe complexe pour l'administrateur local	Accordée	Unification du mot de passe complexe chez tous les postes
Annuler service de partage(SMB)	Accordée	Contrôle par politique de domaine pour éviter l'attaque par session nulle
Activation des pare-feu pour bloquer les intrusions	Accordée	Il faut tester avant si les services nécessaires continuent à fonctionner régulièrement

Aucun coût n'est demandé à ce niveau.

3.3.2.4 Couche Application

Table 0-XX : Approbation des solutions au niveau de la couche Application

Solutions	Statut	Raisons
Imposer la politique de complexité	Accordée	Par les politiques de groupes (AD)
Limitation des privilèges des utilisateurs réguliers	Accordée	Pour les utilisateurs d'oracle une étude de cas détaillée sera suivie dans la partie suivante
Inspection de tous les postes pour activation et mis-à-jour des anti-virus	Accordée	Tache peut être automatisée par la console d'administration
Filtrage du trafic	Accordée	Quelques modifications au filtrage existant sur le pare-feu
Surveillance des fichiers journaux	Accordée	
Cryptage des sessions d'authentification	Accordée	
Filtrage des messages (spam)	Accordée	Quelques modifications au filtrage existant sur le pare-feu
SID complexe	Refusée	Complexité de changer tous les SID existants
Supprimer les identifiants des utilisateurs éliminés	Accordée	A base régulière
System de protection et contrôle des données (right management service)	Accordée	

Le coût total des mesures proposées pour les corrections au niveau de la couche application est : **3000$**

Les coûts varient suivant chaque couche, cette variation est due aux mesures de sécurisation déjà implémentées surtout au niveau de la couche transport. Les coûts élevés au niveau de la couche accès réseaux reviennent aux travaux de rénovation surtout dans les branches principaux.

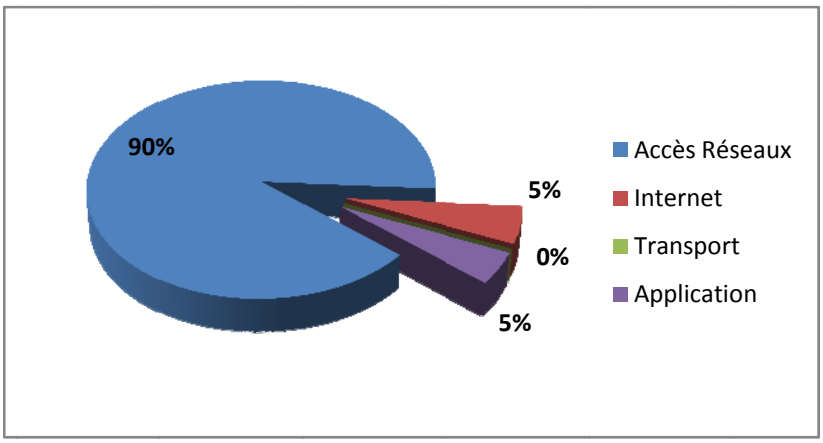


Figure 0.93 : Répartition du budget alloué aux mesures de corrections

3.3.3 Implémentation

Suite aux approbations accordées, un plan d'exécution détaillé est présenté aux membres du département informatique pour achever les taches nécessaires dans chaque branche. Ce plan est divisé selon les couches du protocole TCP et contient l'adresse de chaque poste nécessitant une intervention locale, et les configurations attribuées aux périphériques du réseau et serveurs de l'organisation. Les tableaux suivants récapitulent les travaux effectués, leurs durées et quelques informations à noter.

3.3.3.1 Couche Accès Réseaux

Table 0-XXI : Implémentation des solutions au niveau de la couche Accès réseaux

Site	Solutions	Durée	Statut	Notes
HO	Ajout camera dans la chambre du serveur	1 jour	Achevée	
DT	Changement de l'emplacement de la chambre	2 mois	En cours	
	Equipement complet de la nouvelle chambre			
SS	Changement du rack	1 jour	Achevée	
	System de contrôle d'accès	1 jour	Achevée	
WH	Isolation des appareillages dans une chambre fermée	15 jours	Achevée	
ABC CM VR SK	Isolation des appareillages dans une chambre fermée avec AC, camera, détecteur d'humidité et feu	15 jours	Achevée	VR, CM Bientôt dans : ABC
Tous	Débrancher les prises inutilisées du réseau	3 jours	Achevée	

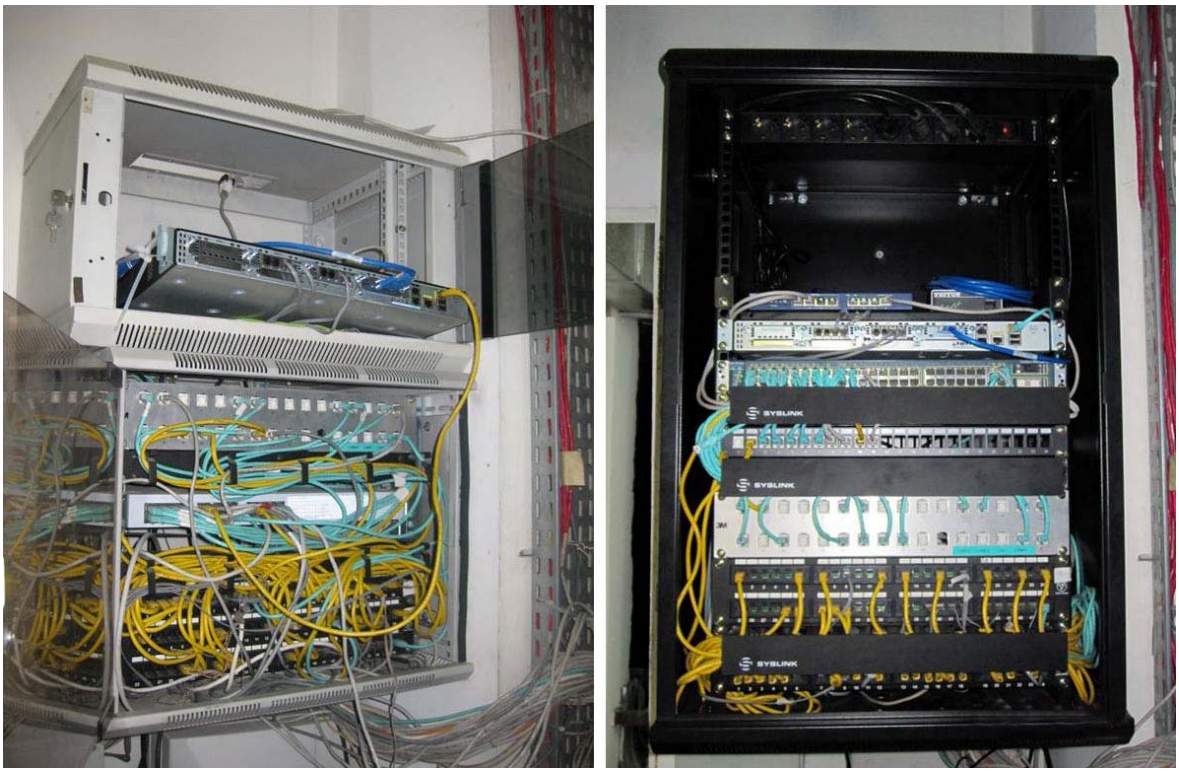


Figure 0.94 : Changement du rack dans SS

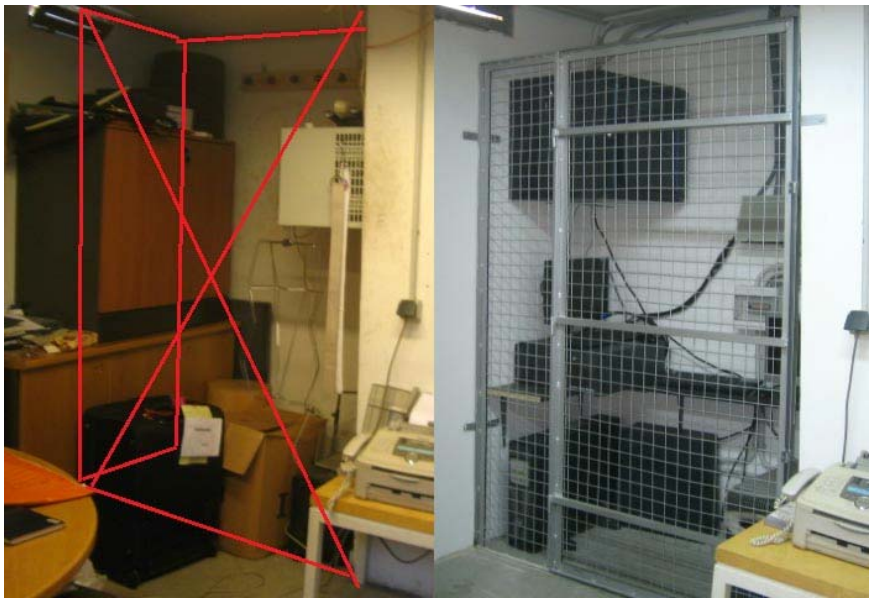


Figure 0.95 : Isolation des appareillages dans une chambre fermée dans WH

3.3.3.2 Couche Internet

Table 0-XXII : Implémentation des solutions au niveau de la couche Internet

Solutions	Durée	Statut	Notes
Personnalisation des configurations	15 jours	Achevée	
Sécurisation par clé WEP complexe		Achevée	
Diminution ou élimination des diffusions		Achevée	
Mot de passe complexe		Achevée	
Désactivation des ports et protocoles vulnérables		Achevée	
Filtrage ou blocage des paquets Implémentation d'un IDS		Achevée	Ajout du module IDS au nouveau pare feu
Configuration de sécurisation des ports des commutateurs		Achevée	

3.3.3.3 Couche Transport

Table 0-XXIII : Implémentation des solutions au niveau de la couche Transport

Solutions	Durée	Statut	Notes
Ajout d'identificateurs ou désactivation du service FTP	15 jours	Achevée	
Ajout mot de passe complexe pour l'administrateur local		Achevée	
Annuler service de partage(SMB)		Achevée	
Activation des pare-feu pour bloquer les intrusions		Achevée	Test des politiques de domaines dans un environnement virtuel avant l'application effective. Quelques problèmes rencontrés avec des applications clientes exceptionnelles : serveur oracle pour le restaurant, logiciel des portables des chauffeurs… L'ajout des exceptions dans les politiques a fixé ces problèmes

3.3.3.4 Couche Application

Table 0-XXIV : Implémentation des solutions au niveau de la couche Application

Solutions	Durée	Statut	Notes
Imposer la politique de complexité	1 jour	Achevée	
Limitation des privilèges des utilisateurs du domaine	15 jours	Achevée	
Inspection de tous les postes pour activation et mis-à-jour des anti-virus	15 jours	Achevée	
Filtrage du trafic	2 jours	Achevée	Ajout de règles de filtrage sur les routeurs
Surveillance des fichiers journaux	Quotidien	Achevée	
Cryptage des sessions d'authentification	1 heure	Achevée	
Filtrage des messages (spam)	2 jours	Achevée	Ajout de règles de filtrage sur le pare-feu
Supprimer les identifiants des utilisateurs éliminés	2 jours	Achevée	
System de protection et contrôle des données (right management service)	2 mois	En cours	Actuellement on est dans la phase d'acquisition du produit
Limitation des privilèges des utilisateurs d'oracle	15 jours	Achevée	Etude détaillée dans la partie suivante

Chapitre 4

Vulnérabilité d'oracle, élaboration d'une norme de sauvegarde

4.1 Problème des utilisateurs privilégiés d'oracle

L'étude effectuée dans la phase d'injection de code SQL à dévoilé une vulnérabilité grave au niveau des utilisateurs, on a découvert qu'un utilisateur régulier ayant un privilège limité à l'intérieur des interfaces du logiciel, a aussi un privilège élevé si jamais il se connecte par commande SQL. Cette vulnérabilité forme une menace élevée sur la base de donnée car cet utilisateur pourra manipuler toutes les données existantes puisqu'il a l'accès d'écrire sur cette base de donnée. Pour fixer ce problème on doit analyser l'état existant des méthodes utilisées pour la création des utilisateurs et sauvegarde des données et créer une nouvelle norme de création et sauvegarde des données.

4.1.1 Principe des bases de données d'Oracle

Une simple recherche sur le site d'Oracle nous donne une idée générale sur les principes de base de la plateforme *Oracle Database 10g* qui est utilisée actuellement dans l'organisation. Cette plateforme est un système de gestion de base de données d'Oracle, caractérisé par plusieurs trais principaux:

- Des grilles de bases de données rapides, fiables et évolutives
- Optimisation de la disponibilité et accélération de la performance par la compression des données vers des partitions de stockage peu coûteuses
- Protection de façon sécurisée les informations tout en permettant un suivi de conformité

Lorsque de nouveaux utilisateurs sont ajoutés dans Oracle, certains droits leurs sont assignés afin qu'ils puissent interagir directement ou par le biais des rôles sur la base de données. Chaque rôle est un ensemble de privilèges qui peuvent être accordées aux utilisateurs ou à d'autres rôles. Il existe deux types de privilèges accordés à un utilisateur:

- Privilèges système par lequel l'utilisateur peut gérer la performance des actions de la base de données et des objets système.

- Privilèges objets qui permettent d'accéder les objets, comme les tableaux, les colonnes des tableaux, les index, les synonymes, les procédures, etc

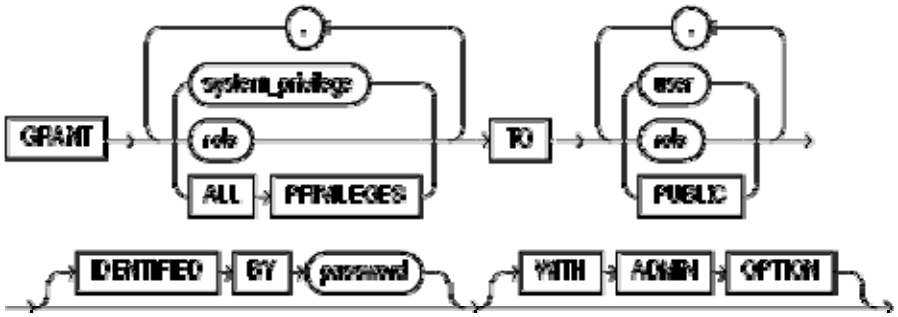


Figure 0.1 : Procédure d'assignation des privilèges système
Référence: *http*://oracle.developpez.com/guide/administration/adminrole/

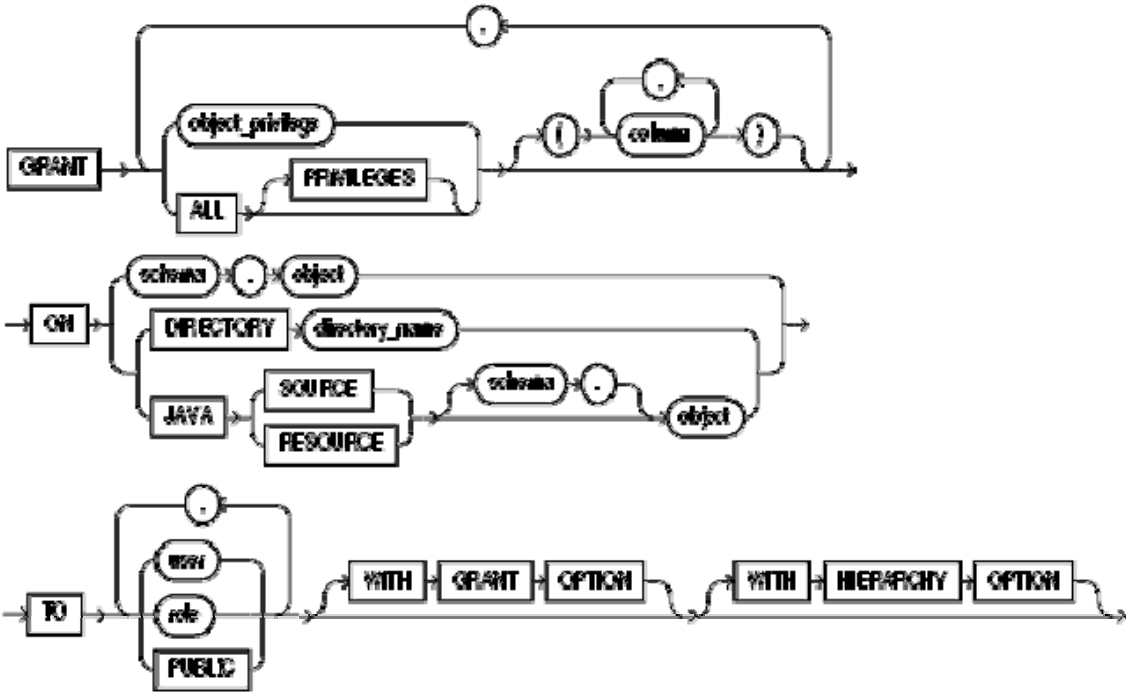


Figure 0.2 : Procédure d'assignation des privilèges objets
Référence: *http*://oracle.developpez.com/guide/administration/adminrole/

Un privilège est un droit pour exécuter un type particulier d'instructions SQL ou pour accéder les objets d'un autre utilisateur. Quelques exemples de privilèges comprennent le droit de :

- Connexion à la base de données
- Création des tables
- Sélectionner des lignes de la table d'un autre utilisateur
- Exécuter une procédure stockée d'un autre utilisateur

Les étapes à suivre pour créer un utilisateur et lui assigner ses privilèges seront :

4.1.1.1 Créer les rôles

CREATE ROLE rolename IDENTIFIED BY password;

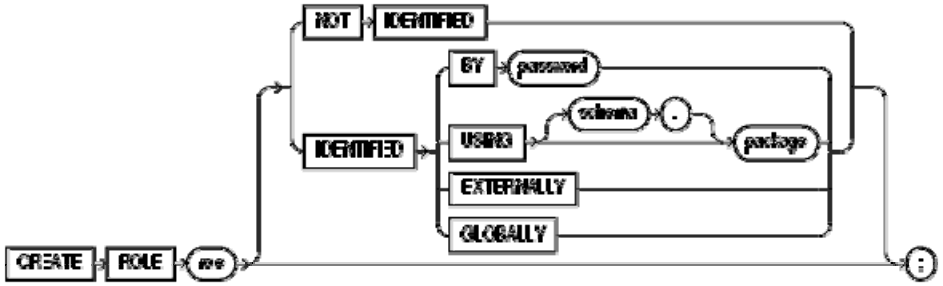


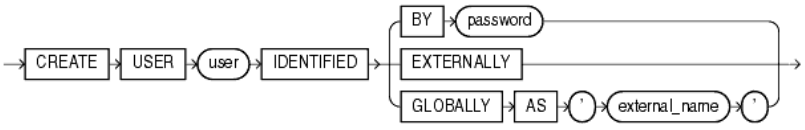
Figure 0.3 : Procédure de création d'un rôle
Référence: *http*://oracle.developpez.com/guide/administration/adminrole/

4.1.1.2 Assigner des privilèges sur des objets prédéfinis à ces rôles

GRANT SELECT ON tablename TO rolename

4.1.1.3 Créer les utilisateurs

CREATE USER username IDENTIFIED BY password



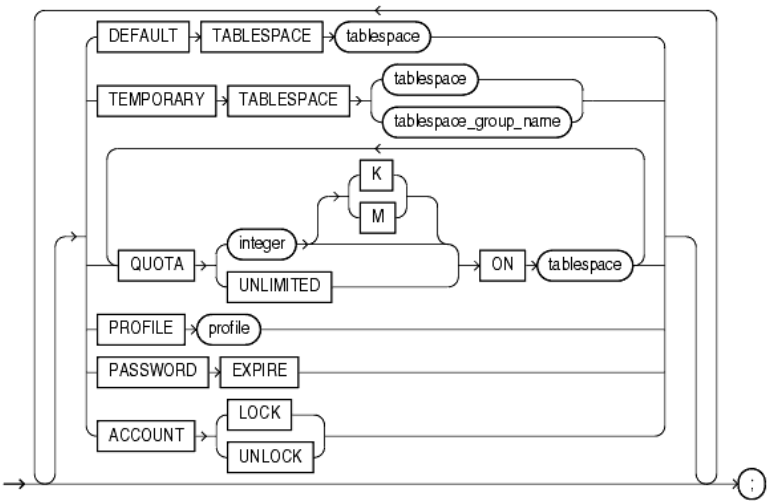


Figure 0.4 : Procédure de création d'un utilisateur
Référence:www.stanford.edu/dept/itss/docs/oracle/10g/server.101/b10759/statements_8003.htm

4.1.1.4 Assigner un ou plusieurs rôles à chaque utilisateur

GRANT rolename TO username

Cette notion de base sur le principe de fonctionnement des bases de données d'Oracle, notamment le processus de création d'un nouvel utilisateur et l'accordement des privilèges aidera par la suite la compréhension et l'analyse du codage existant.

4.1.2 Etat existant

Afin de comprendre le problème existant, il faut d'abord étudier le processus actuellement utilisé pour la création des utilisateurs. On va rentrer dans le codage existant et mettre en relief les points faibles causant les problèmes d'excès de privilèges.

4.1.2.1 Etapes de création d'une nouvelle base de données

- Créer une base de données initiale vide *bdd* à travers l'interface graphique de l'assistant de configuration et lui assigner un SID *bdd*
- Configurer les mots de passe des utilisateurs système : SYS, System…
- Connexion par l'utilisateur SYS sur SQL en insérant les paramètres suivants :

  SYS/password@bdd as SYSDBA
- Créer l'utilisateur ***super*** qui sera l'administrateur d'oracle ayant tous les privilèges du rôle ***dba*** et qui sera le propriétaire de toutes les tables

  CREATE USER super IDENTIFIED BY suppassword

  GRANT dba TO super
- Importer les tables de l'utilisateur ***super*** d'une base de données modèle temp.dmp
  - *> imp*
  - *> user: system@bdd*
  - *> pass: password*
  - *impfile> temp.dmp*
- Créer le rôle ***macc*** protégé par un mot de passe pour être accordé lors d'une connexion réussie

  CREATE ROLE macc IDENTIFIED BY maccpassword

  GRANT ALL ON '\|\|owner\|\|'.'\|\|table_name\|\|' TO macc;' FROM all_tables WHERE owner = 'SUPER';

- Créer le rôle ***macc2*** sans mot de passe assigné par default

CREATE ROLE macc2

GRANT create session TO macc2

GRANT ALL ON '||owner||'.'||table_name||' TO macc2;' FROM all_tables WHERE owner = 'SUPER';

- Exécuter la fonction pubfunc.sql pour créer les synonymes des tables de ***super*** et accorder les privilèges objet de ***super*** à l'utilisateur **PUBLIC**:

SPOOL ON

SELECT 'DROP PUBLIC SYNONYM '||SYNONYM_NAME ||';'

FROM ALL_SYNONYMS WHERE TABLE_OWNER ='super';

SPOOL OFF

@ON.LST

SPOOL ON

SELECT 'CREATE PUBLIC SYNONYM '||NAME||' FOR SUPER.'||NAME|| ';'

FROM SYS.OBJ$ WHERE TYPE# IN (7,8,2,4,6,5) AND OWNER# =

(SELECT USER# FROM SYS.USER$ WHERE NAME='super');

SPOOL OFF

@ON.LST

SPOOL ON

SELECT 'GRANT ALL ON '||NAME||' TO PUBLIC;'

FROM SYS.OBJ$ WHERE TYPE# IN (7,8,2,4,6,5) AND OWNER# =

(SELECT USER# FROM SYS.USER$ WHERE NAME='super');

SPOOL OFF

@ON.LST

4.1.2.2 Configuration de la base de données créée

Jusqu'à présent la base de données est prête à être utilisée on poursuit avec l'utilisateur ***super*** à travers l'interface graphique du logiciel en indiquant le code exécuté par chaque interface.

- Changement du rôle lors de l'ouverture d'une connexion avec le logiciel

PROCEDURE CHANGE_ROLES IS

TT EXEC_SQL.CONNTYPE;

```
TTC EXEC_SQL.CURSTYPE;
RET PLS_INTEGER;
BEGIN
:global.wrole := 'MACC/maccpassword';
   begin
      tt := exec_sql.curr_connection;
      ttc := exec_sql.open_cursor(tt);
      exec_sql.parse(tt, ttc , 'set role macc identified by maccpassword');
      ret := exec_sql.execute(tt, ttc);
      exec_sql.close_cursor(tt, ttc);
      exec_sql.close_connection(tt) ;
      exception  when exec_sql.package_error then dbg('error');
  end;
END;
```

- Créer un utilisateur régulier

```
PROCEDURE create_user (WXUSER VARCHAR2) IS
  wuser varchar2(15);
  wpwd  varchar2(15);
  wdb  varchar2(15);
  wcmd    varchar2(300);
begin
 wuser := upper(get_application_property(USERNAME));
 wpwd  := upper(get_application_property(PASSWORD));
 wdb   := upper(get_application_property(CONNECT_STRING));
 wcmd := 'grant connect , resource to '||wxuser||' identified by '||:wpassword;
 exec(wcmd);
wcmd := ' grant macc  to '||wxuser;
 exec(wcmd);
wcmd := ' grant macc2  to '||wxuser;
 exec(wcmd);
wcmd := 'alter user '||:wusername||' default role macc2
exec(wcmd);
        begin
```

```
update sys_user_profile
  set user_pwd = :wpassword ,
      full_name = :fullname
  where user_id = wxuser;
        if sql%notfound then
         begin
           insert into  sys_user_profile
                (USER_ID, USER_PWD , FULL_NAME )
           VALUES ( WXUSER , :WPASSWORD,  :FULLNAME );
         end;
       end if;
    end;
end;
```

- Attacher l'utilisateur à une branche

```
PROCEDURE att_user_branch IS
BEGIN
 first_record;
 while :systab.ot_code is not null loop
        begin
        insert into   sys_user_profile (USER_ID, USER_PWD, USER_LEVEL,
        FULL_NAME , SOCCODE, BRACODE, OUTLET, USER_FLAG )
       VALUES ( :USER_ID , :USER_PWD , nvl(:USER_LEVEL,10)  ,
          nvl(:systab.FULL_NAME , :systab.user_id )  , :systab.soccode,
          :systab.ot_branch , :systab.ot_code, :systab.user_flag );
        end;
        begin
        insert into systab (soccode,stappcode,stoffcode,stcode,
                    stlename,stsename,stsaname,stpoint,stvalue,stref )
        select :global.majorcc ,'MS','USR',:systab.user_id ,:systab.full_name,
             '' , :systab.soccode||:systab.ot_branch ,
             :systab.soccode||:systab.ot_branch , :user_level , :systab.ot_code
         from dual;
       end;
```

```
next_record;
end loop;
COMMIT_FORM;
END;
```

- Lui ouvrir les options utilisées dans le logiciel : facturation, recherche de stock…

```
PROCEDURE committo IS
BEGIN
        if :system.cursor_block = 'USR' then
          first_record;
          while :stcode is not null loop
            if :usr.accord = 'N' then
              begin
              delete from super.sysusr
              where usrnom = :usr.stcode
              and appniv = :lvl.wappniv
              and soccode = :wsoc;
              end;
            else
              if :savacc != 'Y' then
              insert into super.sysusr  values (:usr.stcode, :lvl.wappniv , :wsoc);
              end if;
            end if;
        next_record;
         end loop;
      end if;
END;
```

- Synchroniser les données entres plusieurs base de données.
  - Préparer le fichier des données mis à jour régulièrement de la branche actuelle

```
EXP %2/%2%3 file=%1
TABLES=(TRF_SYSTAB,TRF_FGART,TRF_FGARTDEP,TRF_FGFOU,TRF_
FGMVC,TRF_FGOUTLET,TRF_FGCLI,TRF_FGENT,TRF_FGCOUP,TRF_
```

ACCRAT,TRF_FGCONS,TRF_FGCLI_MRG,TRF_FGCHK,TRF_FGVAT,TRF_FGCLISWP,trf_fgdiscount) LOG=%1

- Importer le fichier des données mis à jour des autres branches préparé dans la branche principale

  IMP %3/%4%5 file=%1 FULL=Y IGNORE=Y LOG=%1 TOUSER=SUPER

  Les paramètres sont :

  %3 : nom de l'utilisateur

  %4 : mot de passe

  %5 : chemin vers le fichier à importer

4.2 Analyse et Nouvelle norme de sauvegarde

Signalons d'abord que la vulnérabilité initiale existante est la présence de l'interface SQL qui peut permettre à un utilisateur quelconque de se connecter à la base de données avec des privilèges élevés. Donc il faut annuler l'installation de cette interface au début de la configuration du logiciel chez les postes des utilisateurs et s'assurer que toutes les fonctionnalités du logiciel continuent à fonctionner normalement.

Les vulnérabilités existantes dans le codage d'oracle ont été mis en relief en rouge et gras dans les parties précédentes, analysons chacune en détail :

4.2.1 Excès de privilèges pour super et nouvelle norme de sauvegarde

GRANT dba TO super

Début des problèmes par cette commande, on assigne tous les privilèges système et objets à l'utilisateur ***super***. Ces privilèges ne doivent jamais être assignés à un utilisateur même si c'est l'administrateur du logiciel, Si jamais cet utilisateur est compromis toute la base de données est en danger. Ou si un administrateur du système l'utilise incorrectement il risque de manipuler les objets système de la base de données.

La solution consiste à éliminer l'assignation du rôle ***dba*** à ***super*** qui aura seulement des privilèges objets sur ses propres objets : tables, procédures. Dans le cas ou on aura besoin des privilèges système on utilise momentanément les privilèges de l'utilisateur **SYS** qui a par

default le rôle ***sysdba***. On ajoute par exemple dans le processus de création des utilisateurs dans lequel on doit accorder à l'utilisateur créé le privilège de connexion et les rôles ***macc*** et ***macc2*** appartenant au système, le code de connexion temporaire avec l'utilisateur *system*.

```
PROCEDURE create_user (WXUSER VARCHAR2) IS
 wuser varchar2(15);
 wpwd  varchar2(15);
 wdb  varchar2(15);
 wcmd    varchar2(300);
begin
 wuser := upper(get_application_property(USERNAME));
 wpwd  := upper(get_application_property(PASSWORD));
 wdb   := upper(get_application_property(CONNECT_STRING));
 LOGOUT;
 IF WDB IS NULL
 THEN logon ('system',:syspasswd) ;
 ELSE logon ('system',:syspasswd||'@'||wdb ) ;
 END IF;
 wcmd := 'grant connect , resource to '||wxuser||' identified by '||:wpassword;
 exec(wcmd);
wcmd := ' grant macc  to '||wxuser;
 exec(wcmd);
wcmd := ' grant macc2  to '||wxuser;
 exec(wcmd);
wcmd := 'alter user '||:wusername||' default role macc2
exec(wcmd);
LOGOUT;
IF WDB IS NULL
 THEN logon (wuser ,wpwd ) ;
 ELSE logon (wuser ,wpwd ||'@'||wdb ) ;
END IF;
begin
update sys_user_profile
 set user_pwd = :wpassword ,
```

```
 full_name = :fullname
 where user_id = wxuser;
 if sql%notfound then
 begin
    insert into  sys_user_profile
         (USER_ID, USER_PWD , FULL_NAME )
    VALUES ( WXUSER , :WPASSWORD,  :FULLNAME );
 end;
end if;
end;
end;
```

4.2.2 Excès de privilèges pour les rôles *macc* et *macc2*

GRANT ALL ON '||owner||'.'||table_name||' TO macc;' FROM all_tables WHERE owner = 'SUPER';
GRANT ALL ON '||owner||'.'||table_name||' TO macc2;' FROM all_tables WHERE owner = 'SUPER';

Ces deux commandes donne un accès complet sur toutes les tables de ***super*** parmi lesquelles citons : utilisateurs, clients, factures… il faut limiter l'accès sur quelques tables et interdire l'accès sur d'autres notamment les tables des utilisateurs et des privilèges.

Avant de manipuler les privilèges on doit d'abord révoquer les privilèges assignés aux deux rôles *macc* et *macc2*.

```
REVOKE ALL ON '||owner||'.'||table_name||' TO macc;' FROM all_tables
WHERE owner = 'SUPER';
REVOKE ALL ON '||owner||'.'||table_name||' TO macc2;' FROM all_tables
WHERE owner = 'SUPER';
```

Comme le rôle ***macc2*** est accordé par default à la création de l'utilisateur, ce rôle doit avoir strictement le privilège système de création de session.

CREATE ROLE macc2
GRANT create session TO macc2

Le rôle ***macc*** qui sera accordé lors de l'ouverture d'une connexion dans l'interface du logiciel doit avoir des privilèges personnalisés selon les exigences de chaque table :

GRANT select, update, insert, delete ON super.fgart TO macc;
GRANT select ON super.fgclient TO macc;
…

4.2.3 Excès de privilèges dans la fonction *pubfunc.sql*

SELECT 'GRANT ALL ON '||NAME||' TO PUBLIC;'
FROM SYS.OBJ$ WHERE TYPE# IN (7,8,2,4,6,5) AND OWNER# =
(SELECT USER# FROM SYS.USER$ WHERE NAME='super');

Cette commande est le problème majeur de défaillance de sécurité ou plutôt d'excès de privilège, on accorde des privilèges absolus sur tous les objets de ***super*** à PUBLIC ! Donc par transitivité ces privilèges seront disponible à n'importe quel utilisateur. Malgré toutes les restrictions dans le codage et l'assignation des rôles, les utilisateurs pourront manipuler librement les objets de ***super***.

Il faut révoquer tous les privilèges objet erronés assignés à **PUBLIC** par cette commande, et accorder des privilèges objets personnalisés sur les objets de ***super*** au rôle ***macc*** qui sera par la suite accordé aux utilisateurs.

SELECT 'REVOKE ALL ON '||NAME||' FROM PUBLIC;'
FROM SYS.OBJ$ WHERE TYPE# IN (7,8,2,4,6,5) AND OWNER# =
(SELECT USER# FROM SYS.USER$ WHERE NAME='super');

La fonction pubfunc.sql sera uniquement utilisé pour créer les synonymes pour les objets de super :

SPOOL ON
SELECT 'DROP PUBLIC SYNONYM '||SYNONYM_NAME ||';'

```
FROM  ALL_SYNONYMS WHERE TABLE_OWNER = 'super';
SPOOL OFF
@ON.LST
SPOOL ON
SELECT 'CREATE PUBLIC SYNONYM '||NAME||' FOR SUPER.'||NAME|| ';'
FROM SYS.OBJ$ WHERE TYPE# IN (7,8,2,4,6,5) AND OWNER# =
(SELECT USER# FROM SYS.USER$ WHERE NAME='super');
SPOOL OFF
@ON.LST
```

4.2.4 Excès de privilèges par le rôle *resource*

wcmd := 'grant connect , resource to '||wxuser||' identified by '||:wpassword;
exec(wcmd);

L'erreur dans cette commande est l'assignation du rôle ***resource*** à l'utilisateur créé, ce privilège lui accordera la permission de manipuler les objets systèmes de la base de données : CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE.

Un utilisateur régulier n'a pas besoin de tels privilèges, donc il suffit de lui accorder le rôle de connexion et modifier ainsi la commande pour devenir :

```
wcmd := 'grant connect  to '||wxuser||' identified by '||:wpassword;
exec(wcmd);
```

Dans le cas ou l'utilisateur à besoin de modifier une table dont il n'a pas d'accès, on utilise la même méthode de connexion instantanée vue précédemment avec l'utilisateur ***super***. Le code suivant sera ajouté lors de sauvegarde d'un fichier de client

```
LOGOUT;
 IF WDB IS NULL
 THEN logon ('super',:suppasswd) ;
```

```
 ELSE logon ('super',:suppasswd||'@'||wdb ) ;
 END IF;
...
LOGOUT;
IF WDB IS NULL
 THEN logon (wuser ,wpwd ) ;
 ELSE logon (wuser ,wpwd ||'@'||wdb ) ;
END IF;
```

4.3 Approbation et implémentation

La dernière phase dans l'étude des vulnérabilités d'Oracle consiste à obtenir l'approbation des directeurs sur les solutions proposées et l'implémentation des propositions acceptées.

4.3.1 Approbation

La nouvelle norme de sauvegarde, ainsi que la modification des rôles existants ont été discutées avec le directeur et les personnes responsables du codage du logiciel. Quelques idées on été acceptées alors que d'autres ont été modifiées pour mieux servir le logiciel.

- Supprimer l'interface SQL des postes clients : acceptée à condition de tester toutes les fonctionnalités des interfaces du logiciel
- Annuler le privilège ***dba*** à ***super*** : acceptée
- Connexion temporaire:
  - Acceptée pour l'utilisateur ***super*** pour ne pas lui accorder le privilège ***dba***
  - Modifiée pour les utilisateurs réguliers, cette méthode pourra surcharger le serveur par plusieurs demandes de connexion simultanées, on pourra l'utiliser dans le cas de modification de quelques tables importantes
- Changer les privilèges des rôles :
  - ***Macc2*** : acceptée pour avoir seulement le privilège d'ouverture de session
  - ***Macc*** : modifiée, il est préférable de lui accordé les privilèges SELECT, INSERT, UPDATE, DELETE sur toutes les tables primaire de ***super***, pour diminuer ainsi le processus de connexion temporaire pour les tables cruciales.
- Elimination des privilèges de PUBLIC sur les objets de ***super*** : acceptée
- Annuler l'assignation du rôle ***resource*** : acceptée

L'implémentation des modifications ont été effectuée au début dans un environnement virtuel similaire à la configuration existante dans chaque branche, pour tester la validité des nouvelles normes. Une fois validée elles seront implémentées dans les branches.

4.3.2 Implémentation

4.3.2.1 Supprimer l'interface SQL des postes clients

L'application a débuté chez les postes des caissiers de la branche SS, pendant une durée de 3 jours aucun problème n'est apparu. Ensuite chez les directeurs de la branche qui génèrent régulièrement des rapports de ventes pendant une durée d'une semaine et aucun problème n'est apparu. L'étape suivante est l'application chez les postes des utilisateurs des départements administratifs : stock, finance, relation humains… quelques problèmes dans certains rapports appelant SQL ont apparu, on les a fixé en manipulant le codage de certaines formes et rapport d'oracle pour annuler l'appel à l'interface SQL.
Cette tache a été implémentée avec succès dans toutes les branches

4.3.2.2 Annuler le privilège dba à super

L'application de cette tache a été effectuée d'abord dans un environnement virtuel de test, plusieurs problèmes ont apparus dont quelques un peuvent être fixés par codage.
Nous allons suivre les mêmes étapes utilisées lors de la création d'une nouvelle base de données et signaler les problèmes et solutions adoptées.

a. Créer une base de données initiale vide *bdd* à travers l'interface graphique de l'assistant de configuration et lui assigner un SID *bdd*
b. Configurer les mots de passe des utilisateurs système : SYS, System…
c. Connexion par l'utilisateur SYS sur SQL en insérant les paramètres suivants :
d. Créer l'utilisateur super qui sera l'administrateur d'oracle et le propriétaire de toutes les tables sans lui donner le privilège dba
e. Importer les tables de l'utilisateur super d'une base de données modèle temp.dmp

Le premier problème est apparu durant cette étape. L'utilisateur ***super*** n'ayant pas le privilège ***dba*** n'a pas pu importer la base de données entière, on est donc obligé de lui accorder temporairement le privilège ***dba***.

GRANT dba TO super

- *> imp*
- *> user: system@bdd*
- *> pass: password*
- *impfile> temp.dmp*

REVOKE dba FROM super

f. Créer le rôle macc protégé par un mot de passe pour être accordé lors d'une connexion réussie

g. Créer le rôle macc2 sans mot de passe assigné par default

h. Exécuter la fonction pubfunc.sql pour créer les synonymes des tables de super

i. Changement du rôle lors de l'ouverture d'une connexion avec le logiciel

j. Créer un utilisateur régulier

k. Attacher l'utilisateur à une branche

Deuxième problème apparu dans cette phase, ***super*** n'a pas le privilège d'accès à la table des branches et quelques tables systèmes nécessaires. On a trois solutions possibles :

- Ouvrir une connexion temporaire avec l'utilisateur SYTSEM
- Donner les privilèges nécessaires à super directement
- Créer un rôle dédié pour super et lui accorder les privilèges nécessaires.

Ces solutions ont été suivies selon chaque exigence, pour la table des branches par exemple, les privilèges nécessaires on été ajoutés et pour d'autre cas une connexion temporaire a été initiée.

l. Ouvrir les options utilisées dans le logiciel à l'utilisateur crée : facturation, recherche de stock…

m. Synchroniser les données entres plusieurs base de données :

- Préparer le fichier des données mis à jour régulièrement de la branche actuelle
- Importer le fichier des données mis à jour des autres branches préparé dans la branche principale

Nouveau problème apparu dans cette étape, ***super*** n'a pas le privilège d'importer les données dans les tables systèmes, on a obtenu alors l'erreur « privilèges insuffisants »

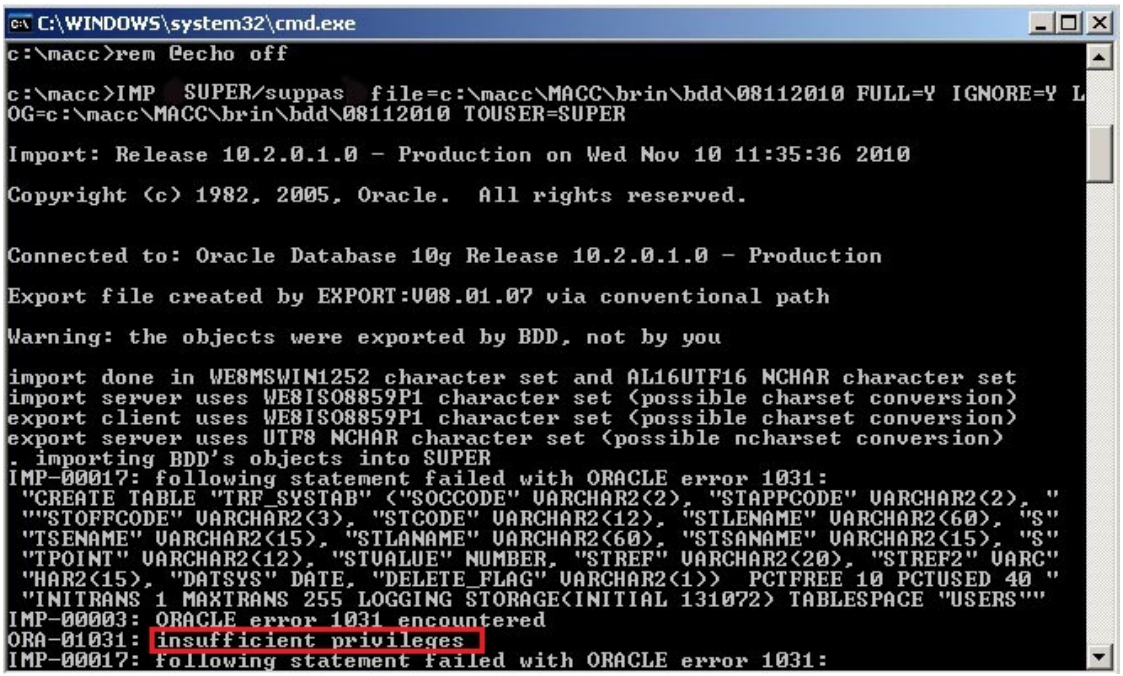


Figure 0.5 : Importer le fichier des données mis à jour des autres branches

Pour fixer ce problème en envoi en paramètre les données de l'utilisateur SYSTEM au lieu de ceux de ***super***

IMP %3/%4%5 file=%1 FULL=Y IGNORE=Y LOG=%1 TOUSER=SUPER

Les paramètres seront :

%3 : SYSTEM

%4 : SYSPASSWORD

%5 : chemin vers le fichier à importer

4.3.2.3 Connexion temporaire pour super

Pour accomplir cette tache, j'ai modifié le codage de la forme de création d'un utilisateur en ajoutant le code proposé précédemment :

```
LOGOUT;
 IF WDB IS NULL
 THEN logon ('system',:syspasswd) ;
 ELSE logon ('system',:syspasswd||'@'||wdb ) ;
 END IF;
```

```
…
LOGOUT;
 IF WDB IS NULL
 THEN logon (wuser ,wpwd ) ;
 ELSE logon (wuser ,wpwd ||'@'||wdb ) ;
END IF;
```

La nouvelle norme a été implémentée avec succès dans quelques formes principales de l'environnement virtuel et ensuite dans toutes les branches.
Afin d'implémenter ce codage dans toutes les formes nécessaire du logiciel il faudra beaucoup de temps, donc la démarche d'implémentation sera divisée sur plusieurs phases pendant ce temps le privilège ***dba*** restera assigné à ***super***

4.3.2.4 Connexion temporaire pour utilisateur régulier

Le même codage utilisé dans la partie précédente peut être utilisé dans cette étape. L'essai de cette méthode dans quelques formes a été implémenté avec succès dans l'environnement virtuel avec un nombre limité d'utilisateur. L'implémentation effective dans l'environnement réel risque de surcharger les serveurs par les requêtes de dizaine d'utilisateurs simultanément. La deuxième solution sera dans la personnalisation des privilèges des rôles ***macc*** et ***macc2*** dans la partie suivante.

4.3.2.5 Changer privilège du rôle *Macc*

Le rôle ***macc*** est assigné les privilèges objets uniquement sur les objets accédés fréquemment de ***super***. Ces privilèges sont de type : SELECT, INSERT, UPDATE, DELETE. Afin de tester cette tache, on a modifié les privilèges sur les tables utilisées par la forme de facturation uniquement et essayer de sauvegarder les factures. La sauvegarde des données a été effectuée avec succès. La poursuite de cette tache sera implémentée progressivement sur toutes les tables de la base de données.

4.3.2.6 Changer privilège du rôle *Macc2*

Les privilèges nécessaires pour chaque utilisateur ont été assignés au rôle Macc, ainsi le privilège de création de session est suffisant pour le rôle Macc2 qui est assigné par default aux utilisateurs.

4.3.2.7 Modifier la fonction *pubfunc.sql*

D'abord on a révoqué les privilèges assignés par excès à PUBLIC, et la fonction pubfunc.sql a été modifier pour assigner uniquement les privilèges sur le synonymes des objets de ***super***.

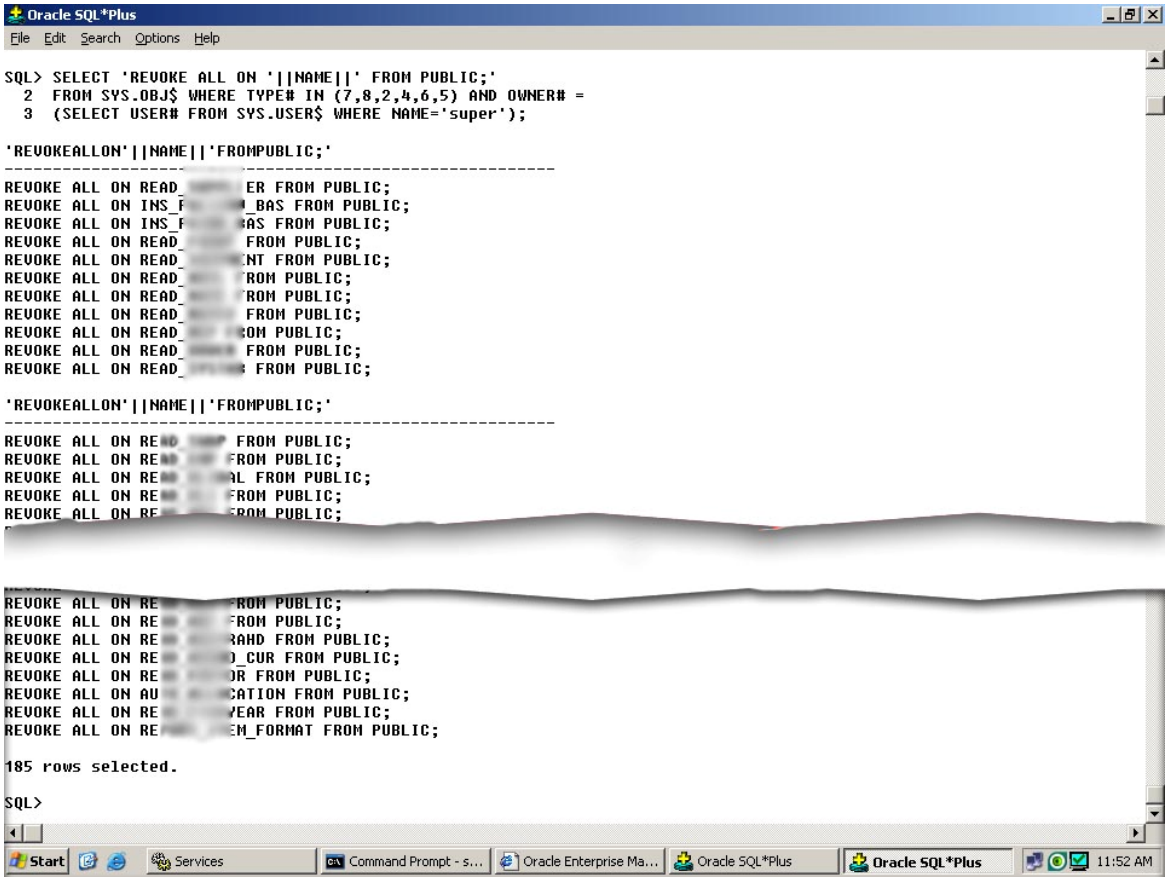


Figure 0.6 : Procédure d'élimination des privilèges de PUBLIC

4.3.2.8 Annuler l'assignation du rôle *resource*

Comme le rôle ressource donne un accès système inutiles par rapport aux utilisateurs réguliers, j'ai pu l'annuler et aucun problème n'est apparu chez les utilisateurs. Cette tache a été implémentée avec succès dans toutes les branches.

Les nouvelles normes proposées ont été testées d'abord dans l'environnement virtuel. La majorité était admissible et a été implémentée avec succès dans l'environnement réel. Ce qui reste jusqu'à présent est la personnalisation du rôle Macc selon les exigences des formes, tables et utilisateurs.

Chapitre 5

Gestion des systèmes après sécurisation

5.1 Le système après sécurisation

Arrivant à ce point, suite à l'effort et le travail effectués durant les mois passés, il est temps d'évaluer le système après sa sécurisation pour dévoiler le niveau de sécurité atteint. La méthodologie d'évaluation suivie sera l'hiérarchie des couches du protocole TCP.

5.1.1 Couche Accès physique

Une visite sur les différentes branches de l'organisation dévoile un niveau de sécurisation de la couche accès physique progressé : les chambres de contrôle sont totalement sécurisées, l'accès des étrangers est presque impossible à ces chambres, l'accès des employés est de même difficile à ces endroits grâce aux systèmes de contrôle d'accès implémentés. Néanmoins il reste 2 branches en cours de sécurisation car les travaux d'amélioration exigent une durée de 2 à 3 mois pour être achevés. Les photos qui suivent montrent quelques améliorations implémentées dans les branches.

Figure 0.1 : Système de control d'accès par carte préconfigurées

Figure 0.2 : Détecteur de mouvement

Figure 0.3 : Camera de surveillance

Figure 0.4 : Système de détection de feu et de mouvement avec composeur automatique

Figure 0.5 : Nouveau rack sécurisé

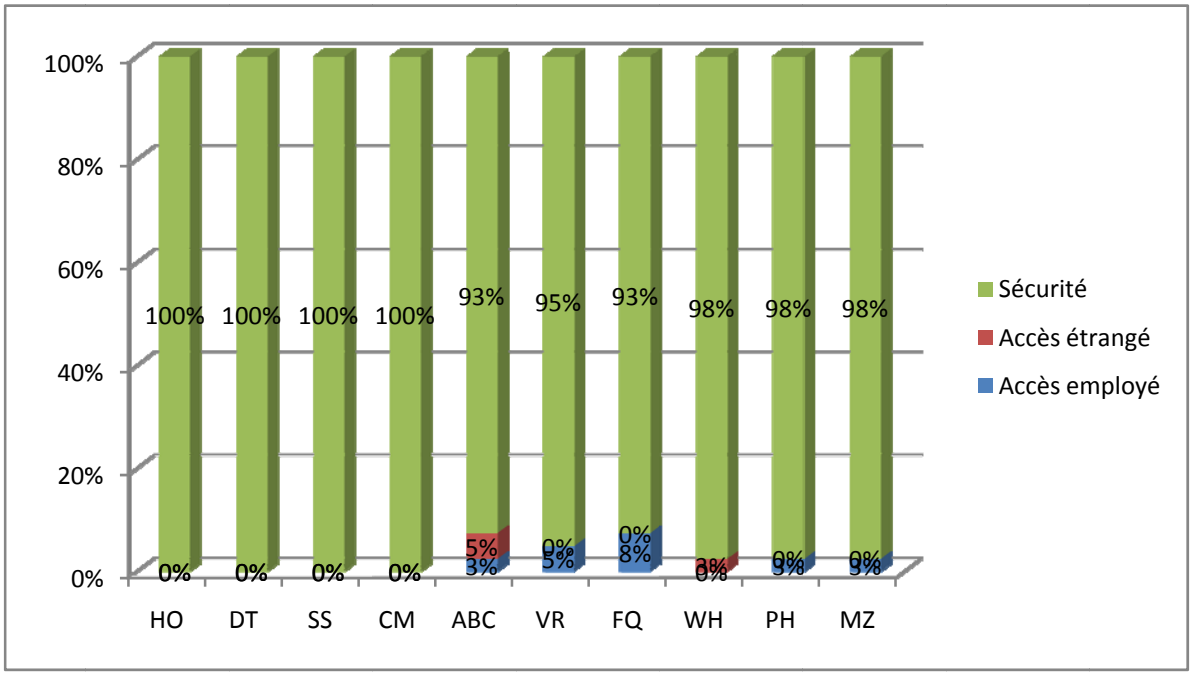


Figure 0.6 : Distribution de sécurisation dans les branches après amélioration

La majorité des branches est totalement sécurisée, ceux qui restent sont en voie de sécurisation.

5.1.2 Couche Internet

L'évaluation du système au niveau de la couche internet consiste à employer les mêmes outils utilisés dans l'étude de cette couche dans les phases d'attaques. Ainsi on peut comparer les résultats avant et après sécurisation.

5.1.2.1 Balayage et analyse du réseau

D'abord on essai de balayer tous les réseaux pour obtenir le niveau de vulnérabilité acquis.

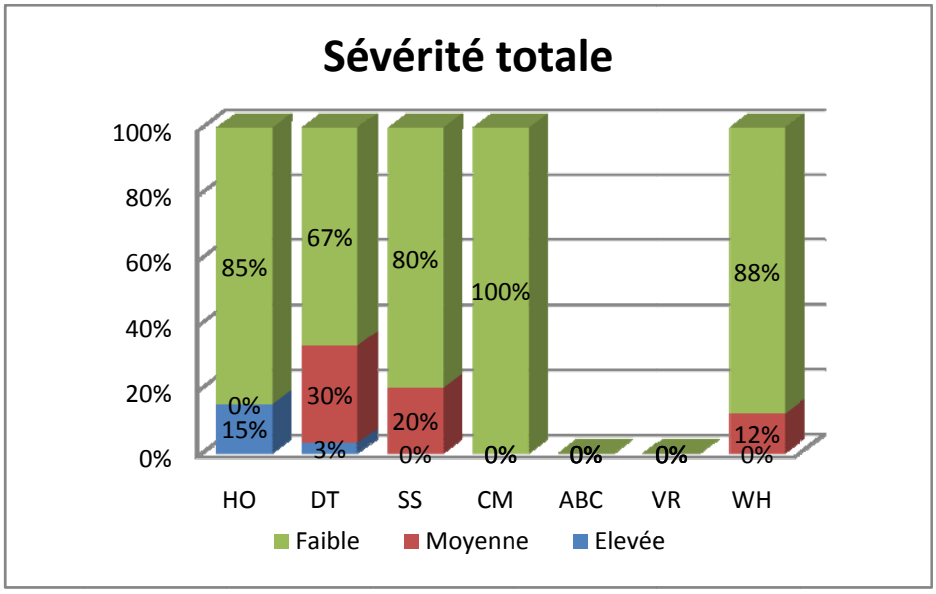


Figure 0.7 : Sévérité totale dans les branches principales

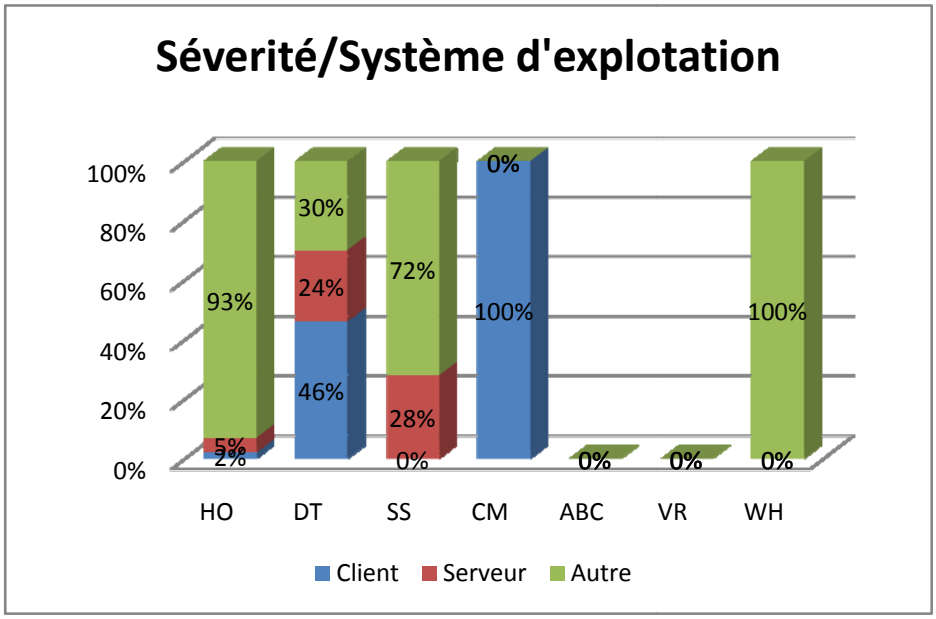


Figure 0.8 : Sévérité par SE

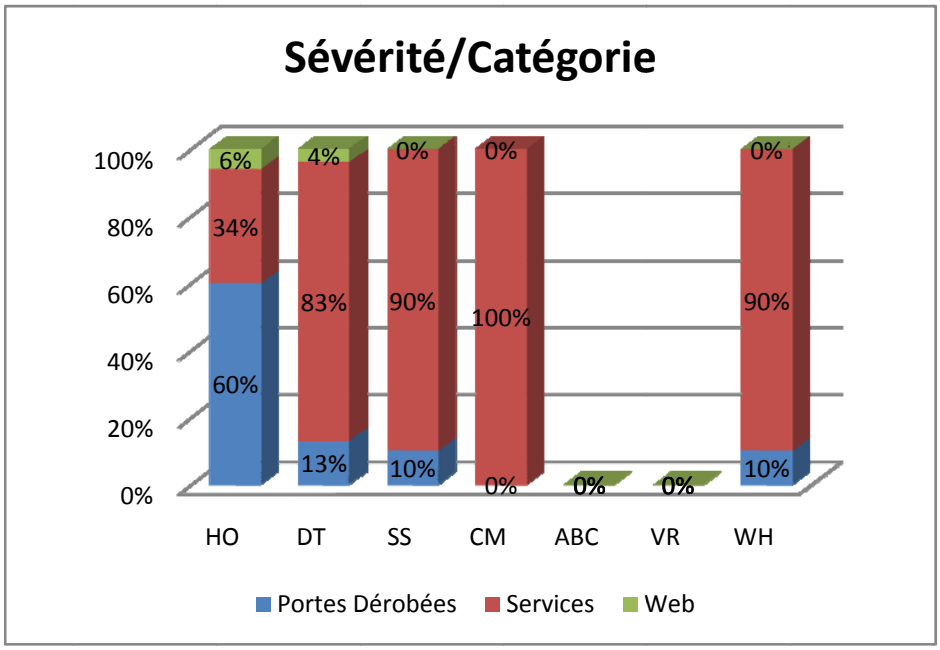


Figure 0.9 : Sévérité par catégorie de vulnérabilité

On remarque que le niveau de sécurité a considérablement évolué dans toutes les branches. Les vulnérabilités restantes sont d'une sévérité faible, ils persistent dans quelques postes secondaires, comme les unités d'enregistrement des cameras ou les commutateurs ayant quelques ports ouvert ou services additionnels pour leur gestion à distance.

5.1.2.2 Pénétration des périphériques du réseau

On poursuit avec les outils de pénétration pour évaluer les périphériques des réseaux étudiés auparavant. Comme le montre la partie suivante, la plus part des outils ont échoué d'obtenir les données critiques ou pénétrer les périphériques du réseau. Je présente ci-dessous les résultats de ces outils sur plusieurs dispositifs du réseau.

Le balayage par l'outil *LanSpy* retourne quelques information préliminaires sur l'un des périphériques, on remarque la plus part des ports TCP vulnérables sont fermés, et le pare-feu à bloquer l'accès à la liste des ports UDP.

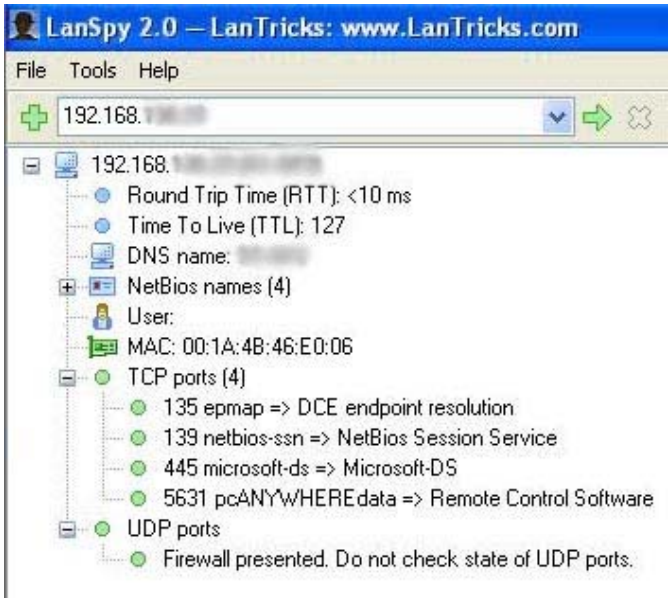


Figure 0.10 : Résultat de l'outil *LanSpy*

L'utilisation de l'outil *SNMP Brute Force Attack* à échoué d'obtenir le CS des périphériques après l'essai d'environ 200000 combinaisons pendant une durée de 2 jours.

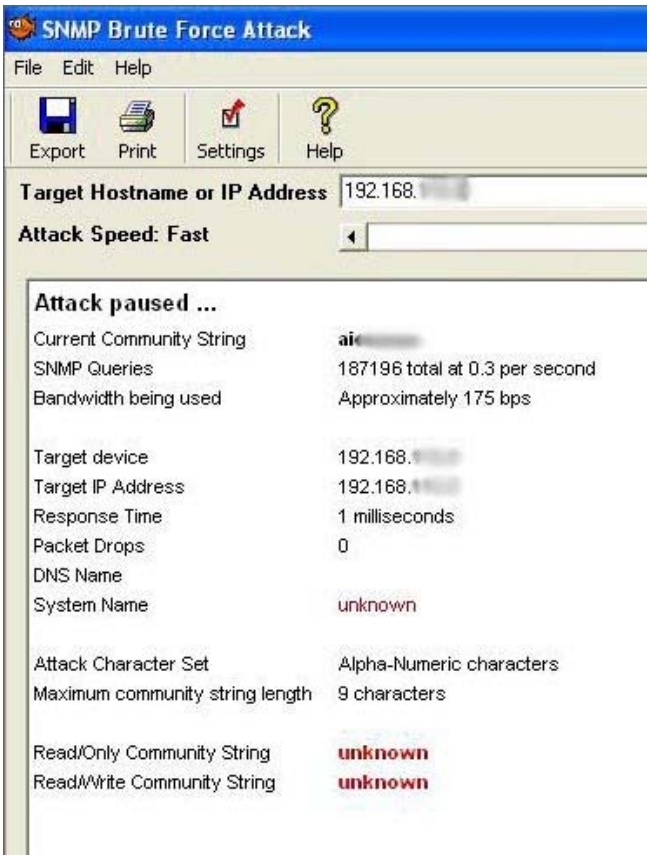


Figure 0.11 : Résultat de l'outil *SNMP Brute Force Attack*

Le balayage de tous les réseaux pour obtenir des CS possible a retourné une liste vide sauf quelques imprimantes-scanneurs nécessitant le CS « *public* »

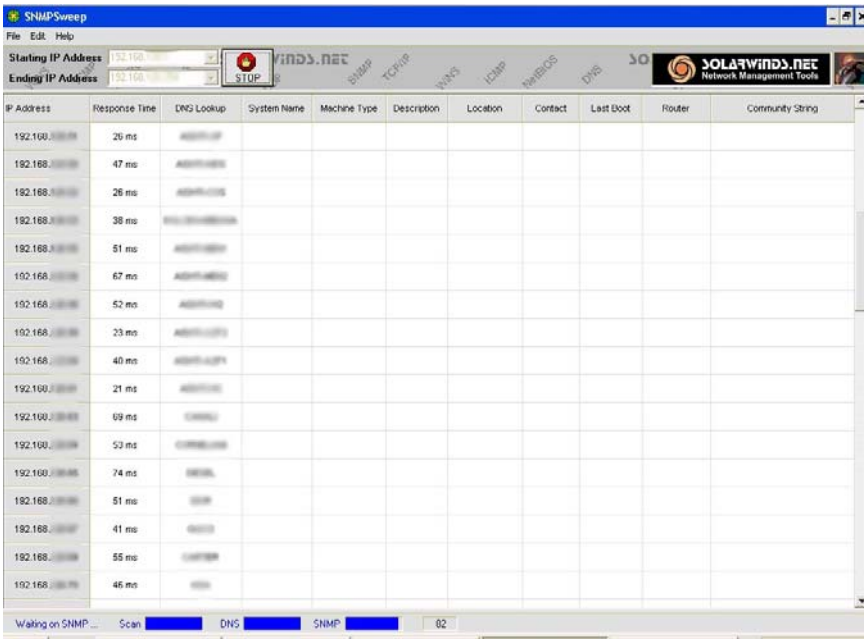


Figure 0.12 : Résultat de l'outil *SNMP Sweep*

L'essai de plusieurs mots de passe communs à échoué sur tous les périphériques internes et externes au réseau.

Le piratage au niveau de la couche internet a échoué, on a pu accéder au réseau internet par aucun moyen. Le niveau de sécurisation a considérablement évolué comme le montre la comparaison des résultats des balayages effectués durant les tests.

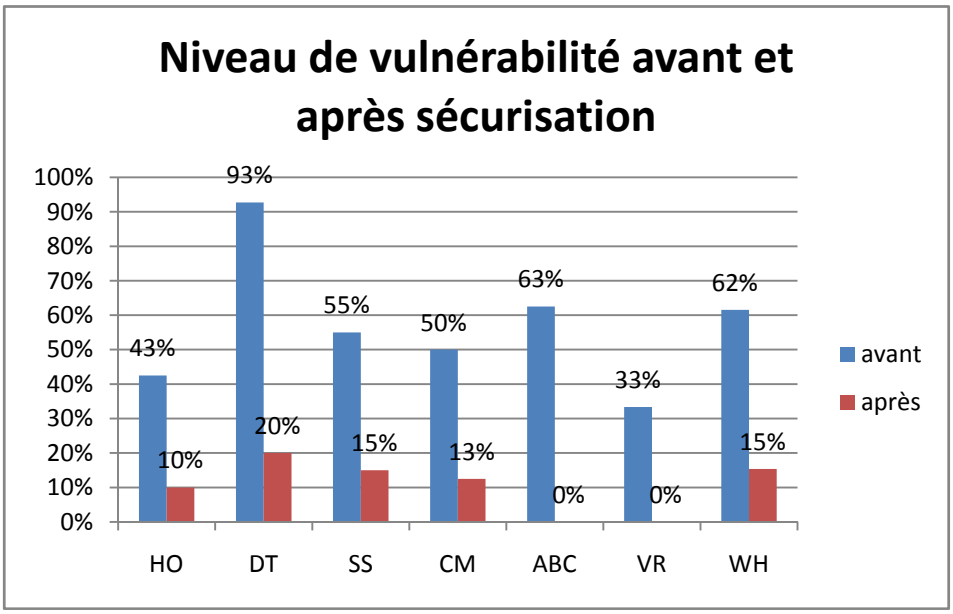


Figure 0.13 : Comparaison du niveau de vulnérabilité avant et après sécurisation

5.1.2.3 Surcharge et blocage des ressources

Avant de débuter les tests de surcharge et blocage des ressources, signalons la politique de domaine dans laquelle on active le pare-feu permettant l'accès d'une rangée d'adresse IP fixe à un nombre limité de ports et services qui sont strictement nécessaire.

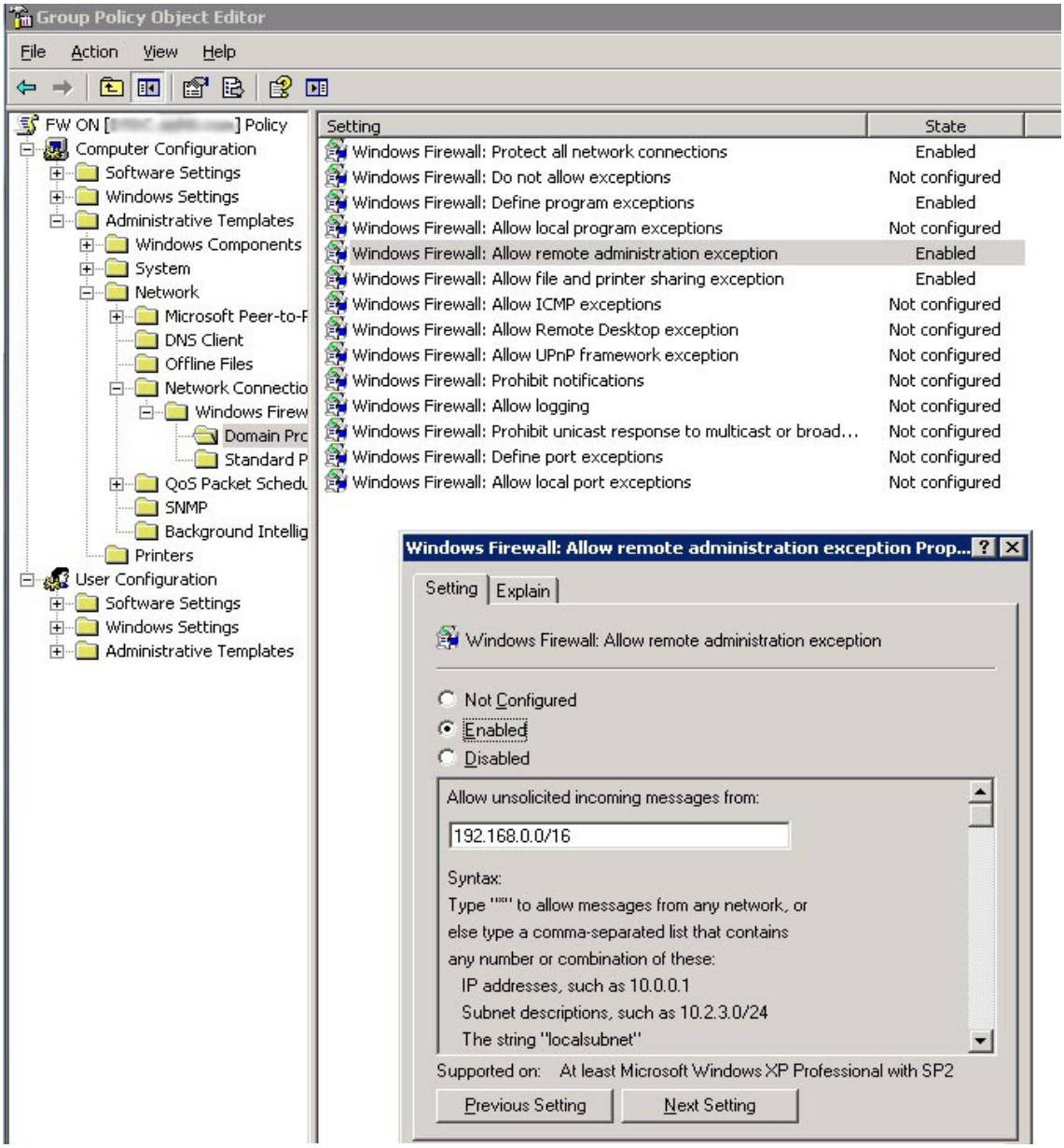


Figure 0.14 : Politique d'activation du pare-feu

Cette politique de groupe diminue considérablement les ports ouvert et accessibles, et les vulnérabilités d'attaque par dénis de service. L'ajout d'un nouveau pare-feu externe au réseau avec un IDS élimine tout danger externe (de l'internet) sur le réseau internet de l'organisation.

En effet on peut classer les contre-mesures aux attaques de dénis de service implémentées dans notre système selon la figure suivante :

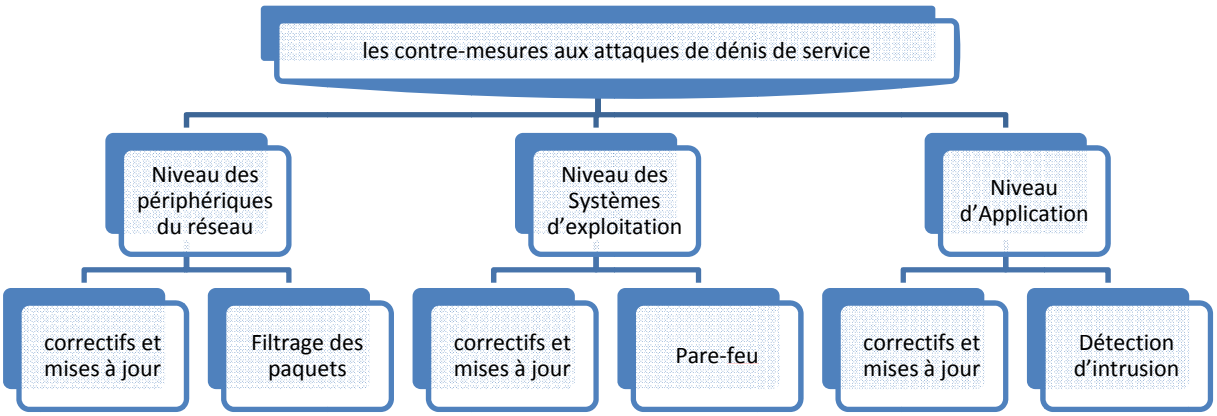


Figure 0.15 : Contremesures aux attaques de dénis de service

Suite à ces mesures correctives, l'essai des outils d'attaque de dénis de service à échoué sur plusieurs postes.

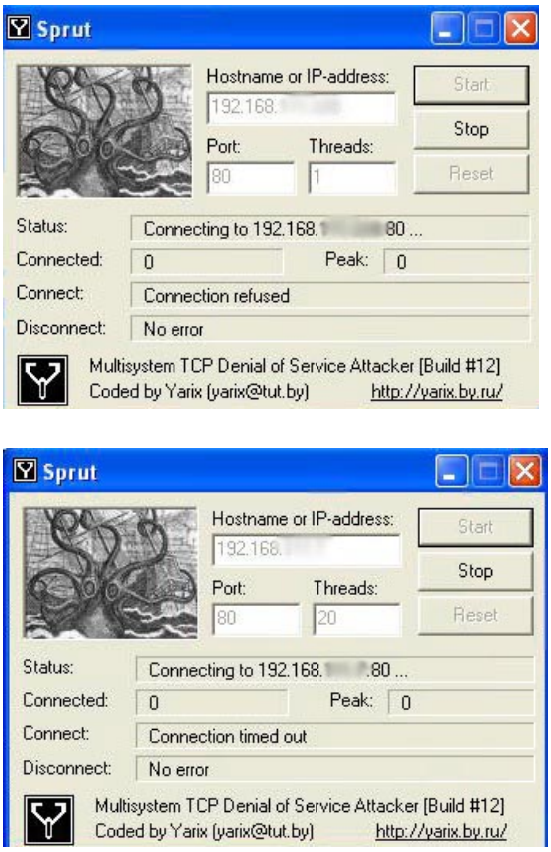


Figure 0.16 : Résultats de l'outil *Sprut* sur 2 postes sécurisés

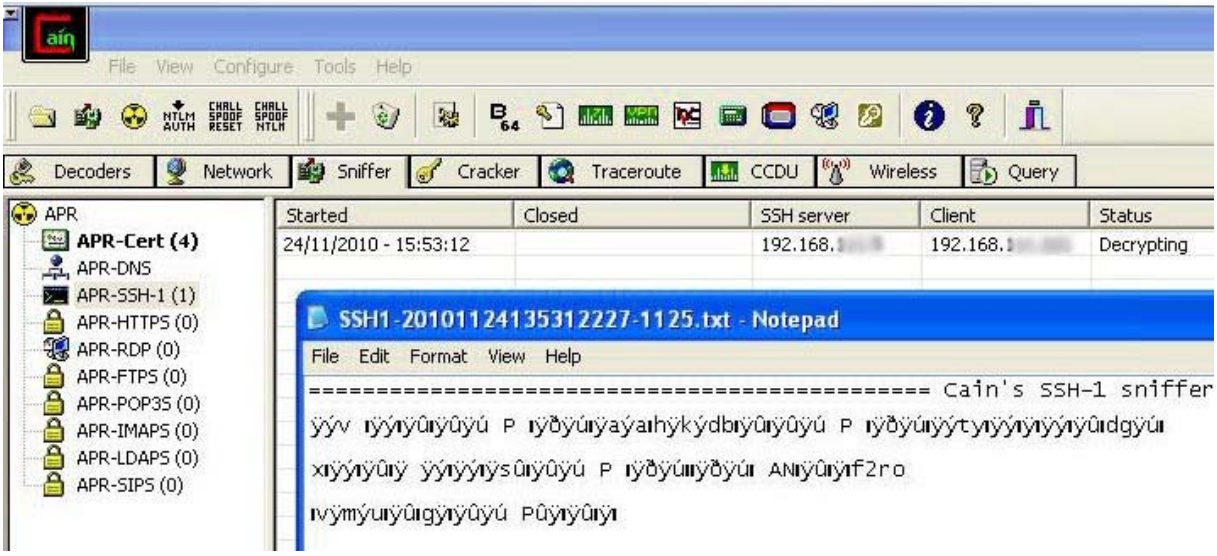


Figure 0.17 : Résultat de l'outil *Cain* pour un vol d'une session SSH

La majorité des tests de surcharge et blocage des ressources ont échoués au niveau de la couche Internet, mais par exemple l'attaque de *Ping* de mort a réussi de surcharger un client mais sans bloquer ses ressources. Ces vulnérabilités persistes car on est obliger de laisser des ports TCP primaires ouverts pour la gestion des postes à distance. Mais ces vulnérabilités sont uniquement au niveau des réseaux internes où le système est contrôlé au niveau des autres couches du protocole TCP.

Table 0-I : Résultats des tests de la couche Internet

	Date des tests	Vulnérabilités / Etat	Risques / Impact	Résultat
Balayage et analyse du réseau	15/11/2010	Majorités des ports fermés Vulnérabilités restantes faibles	Accessibilité difficile	Non compromis
Pénétration des périphériques du réseau	18/11/2010	Mots de passe complexes Configuration personnalisée	Accessibilité difficile	Non compromis
Tests de surcharge et blocage des ressources	23/11/2010	Pare-feu activé Cryptage du trafic Paquets ICMP non bloqués	Accessibilité difficile	Parfois compromis

5.1.3 Couche Transport

L'évaluation du système au niveau de la couche transport consiste à employer les mêmes outils utilisés dans l'étude de cette couche dans les phases d'attaques. Ainsi on peut comparer les résultats avant et après sécurisation.

Débutons par le résultat du balayage du système au niveau des ports TCP et UDP :

Table 0-II : Résultat du balayage des ports ouverts après sécurisation

	Nbre Total IP	TCP							UDP					Total
		FTP	ssh	telnet	dns	smtp	HTTP	Total	TFTP	*SNMP*	smb	ipsec	Total	
		21	22	23	53	25	80	TCP	69	161	445	4500	UDP	
WH	16	٠	١	١	٠	٠	٢	٤٩	٠	٣	١	١	18	67
SS	23	١	٢	٤	١	٠	٣	٩٣	١	٣	١	٣	41	134
CM	11	٠	٠	1	١	٠	٠	٤	٠	٠	٠	٠	0	4
ABCA	10	٠	٠	1	٠	٠	٠	٤	٠	٠	٠	٠	٠	4
DT	78	٠	٠	٤	١	١	٨	١٧٦	١	٢	٤	٤	185	361
HO	104	٠	٠	٣	١	١	٨	١٩٧	١	٥	٢	٧	105	302

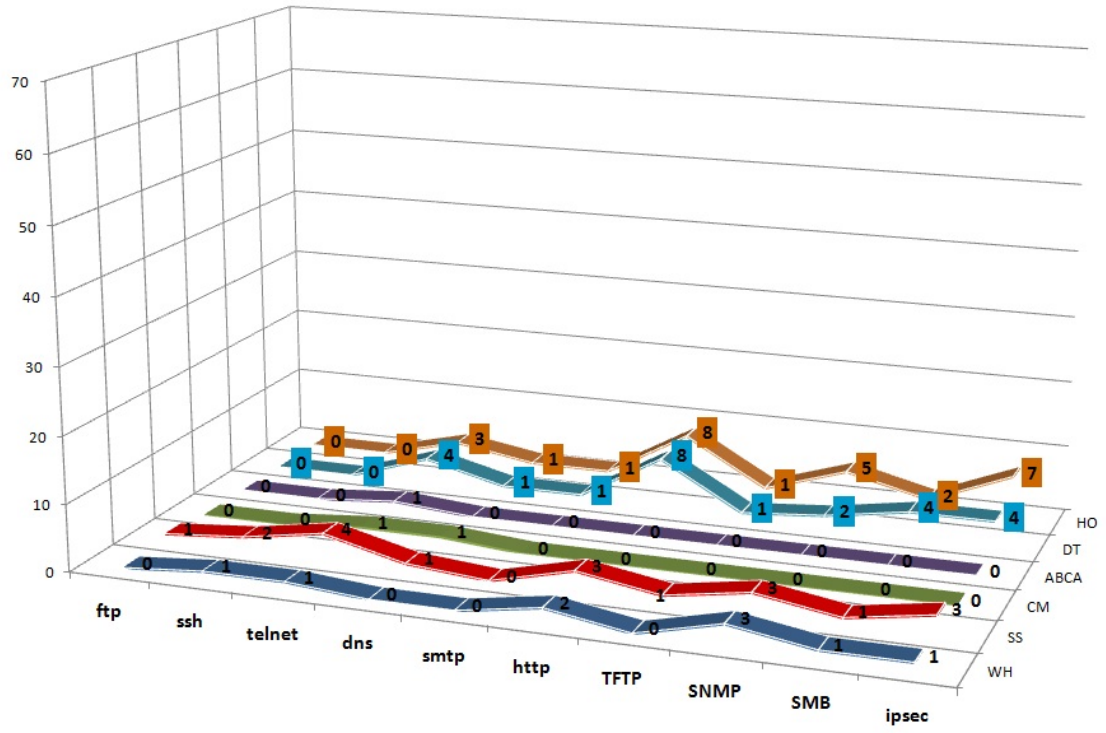


Figure 0.18 : Répartition totale des ports cibles accessibles après sécurisation

Le nombre des ports ouvert a diminué considérablement, ceux qui restent sont nécessaires pour les services des serveurs ou périphériques du réseau, et chez les postes clients pour leur gestion à distance. Les tableaux suivants montrent quelques comparaisons avant et après sécurisation.

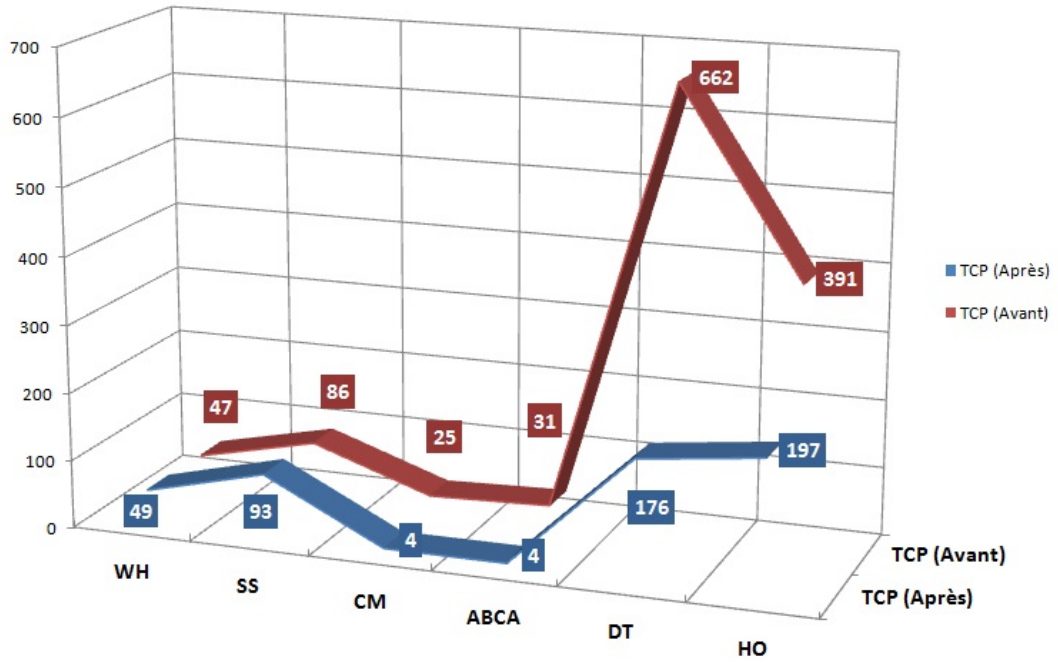


Figure 0.19 : Comparaison du nombre de port TCP ouverts

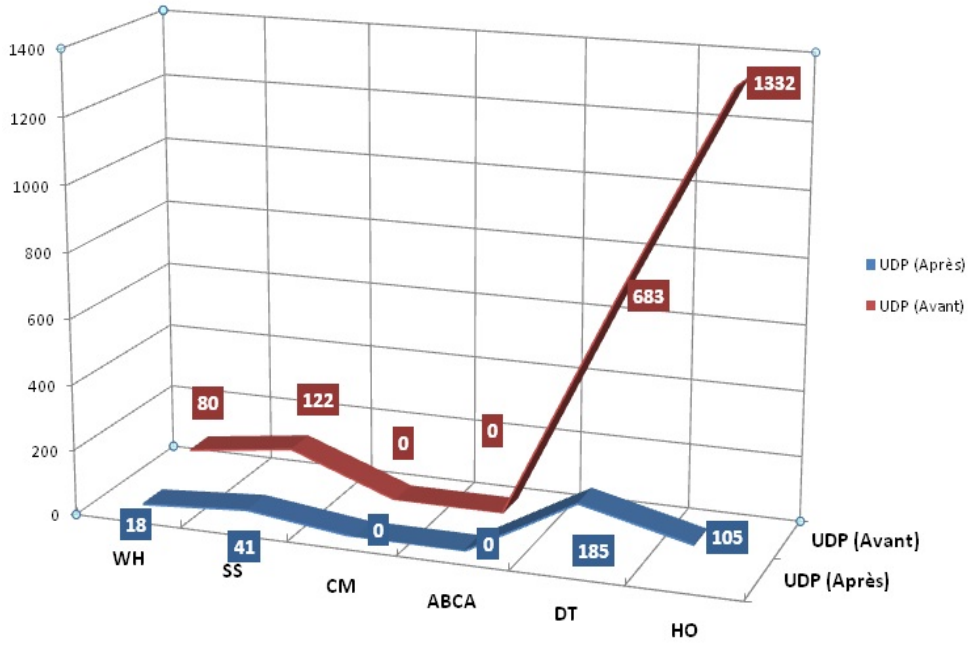


Figure 0.20 : Comparaison du nombre de port UDP ouverts

L'essai des mêmes outils d'attaques utilisés au niveau de la couche transport sur les ports restants ouvert a échoué de pénétrer aucun poste client ou serveur.

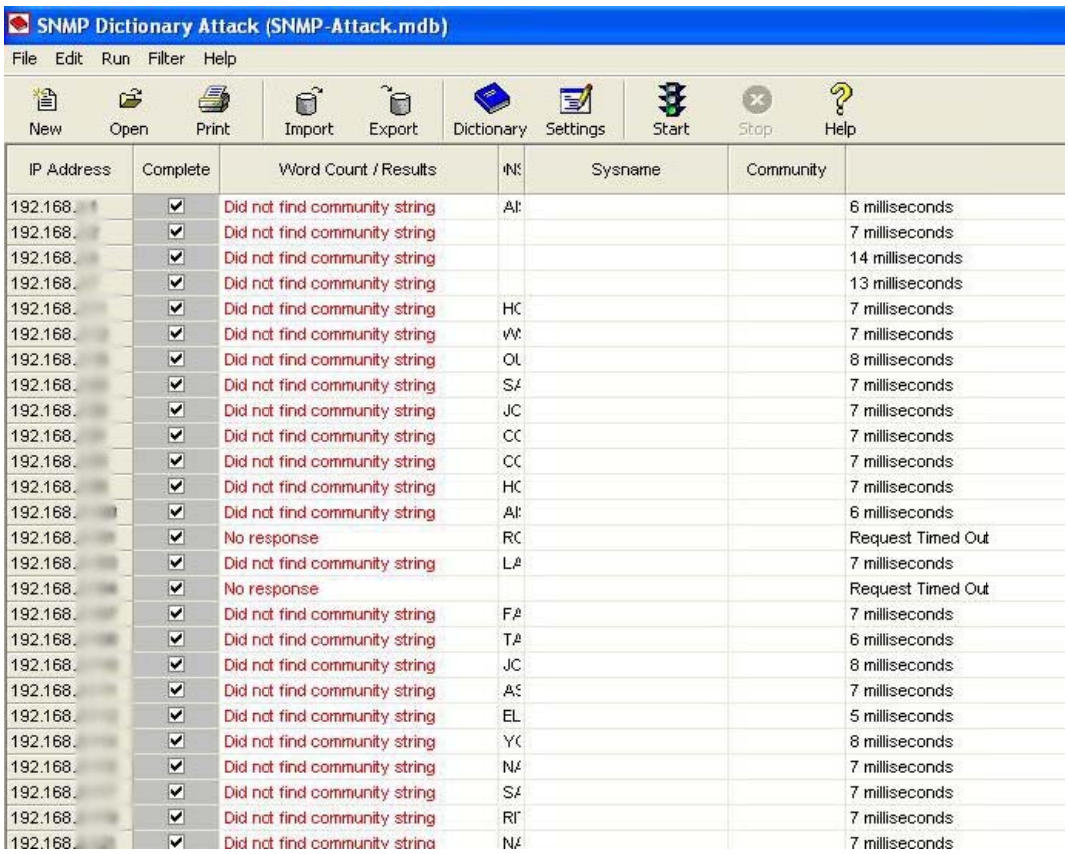


Figure 0.21 : Résultat de l'outil *SNMP Dictionnary Attack* après sécurisation

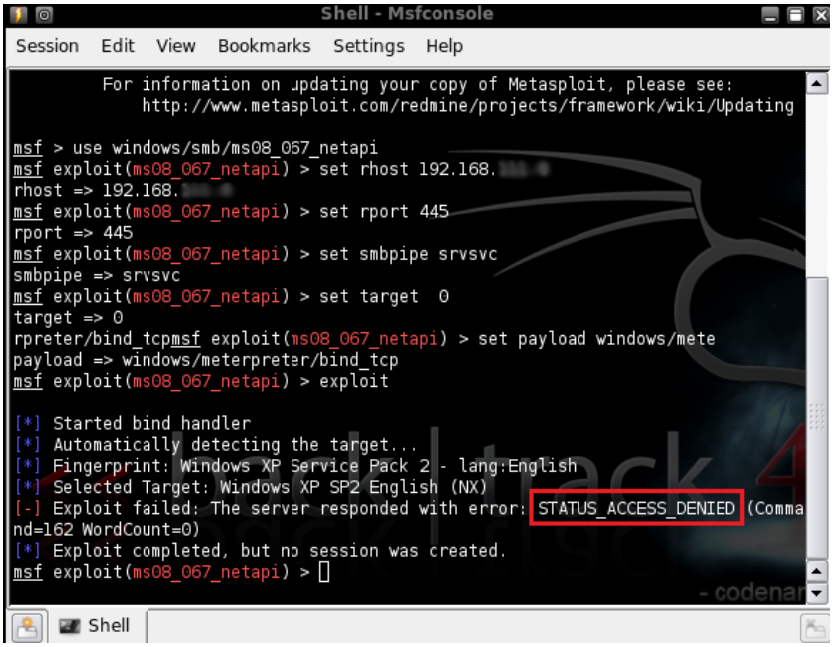


Figure 0.22 : Attaque *Metasploit* sur le port TCP 445

Quelques outils réussirent d'accéder aux données de quelques postes, comme *SSLStrip* qui a obtenue le mot de passe d'une session d'ouverture de messagerie comme Hotmail. Dans ce cas les postes importants ont été protégés par le cryptage à travers l'implémentation d'*IPSec* sur leur trafic. Mais on ne peut implémenter cette solution chez tous les postes car elle surcharge ces postes et le réseau.

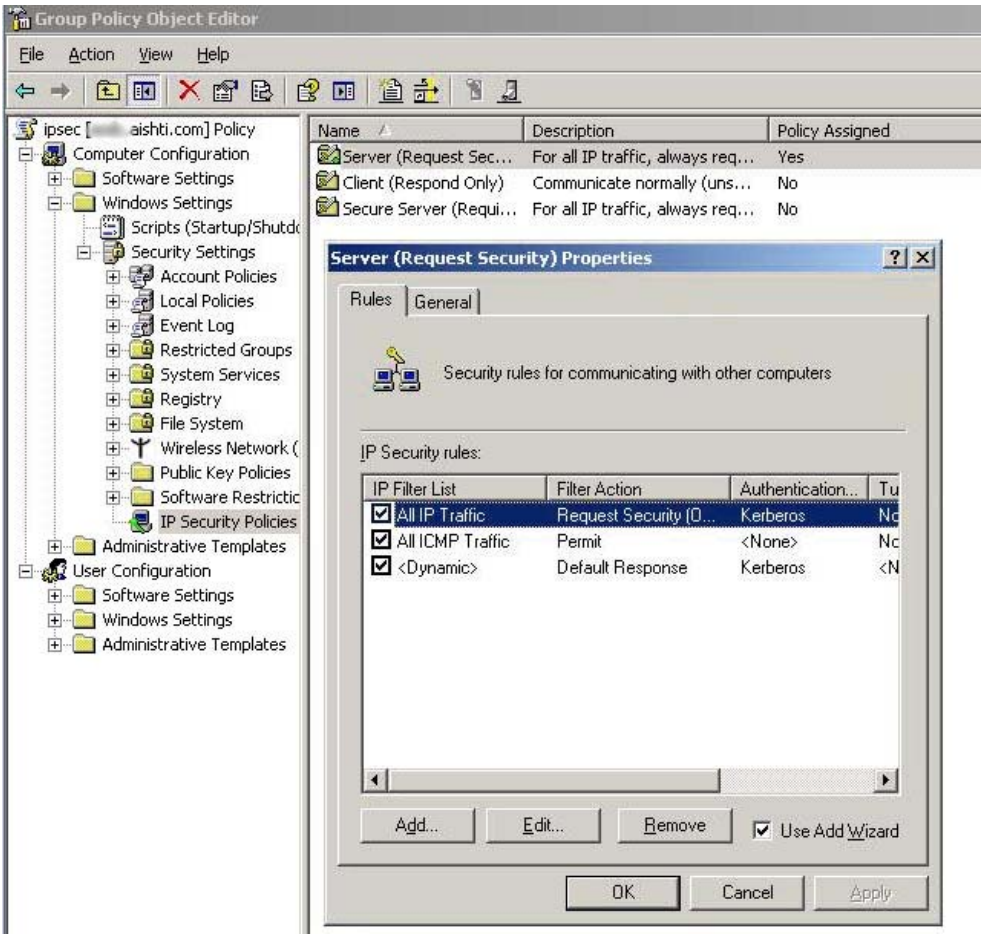


Figure 0.23 : Politique implémentant l'IPSec

La majorité des tests d'attaques au niveau de la couche transport ont échoués de pénétrer les systèmes ou d'obtenir des données pertinentes. Les postes clients n'ont plus des vulnérabilités de ports TCP ou UDP ouverts.

Table 0-III : Résultats des tests de la couche Transport

	Date des tests	Vulnérabilités / Etat	Risques / Impact	Résultat
FTP	24/112010	Ports inaccessibles mots de passe complexes	Accessibilité difficile	Non compromis
SSH	24/112010	Ports ouverts sur machines pertinentes Accès difficile et sécurisé	Etat acceptable	Non compromis
TFTP	25/112010	Ports ouverts sur machines pertinentes Accès difficile et sécurisé	Etat acceptable	Non compromis
SNMP	25/112010	Ports inaccessibles chez clients et serveur à cause du pare-feu	Etat acceptable	Non compromis
SMB	25/112010	Ports inaccessibles chez clients et serveur à cause du pare-feu	Etat acceptable	Non compromis

5.1.4 Couche Application

L'évaluation du système au niveau de la couche Application consiste à employer les mêmes outils utilisés dans l'étude de cette couche dans les phases d'attaques. Ainsi on peut comparer les résultats avant et après sécurisation. L'enchainement des tests suivra les mêmes objectifs étudiés avant :

5.1.4.1 Systèmes d'exploitation

L'ouverture d'une session chez plusieurs postes clients ou serveurs à travers l'outil *Metasploit* sur les ports ouverts restants a échoué, tous les postes sont sécurisés par des mots de passe pour l'administrateur local, l'utilisateur *Guest* est désactivé, aucun utilisateur local n'existe et aucun utilisateur du domaine n'est membre du groupe administratif local.

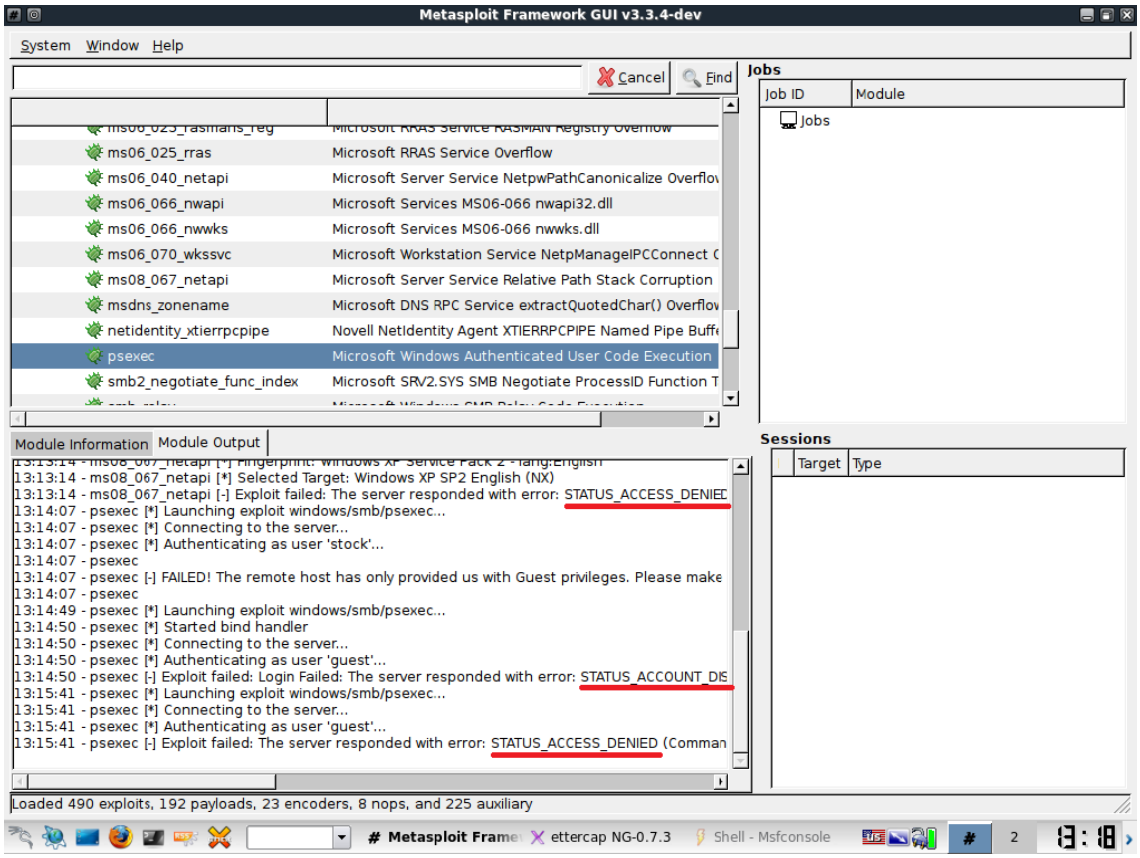


Figure 0.24 : Résultat d'exploitations échouées par *Metasploit*

L'essai de captage du trafic d'authentification par l'outil *Ettercap* a capté uniquement le trafic des postes hors du domaine malgré plusieurs essais d'authentification sur plusieurs postes du domaine afin de pouvoir capter le trafic. Cet outil n'a pas pu interférer le trafic protégé du domaine par cryptage et pare-feu.

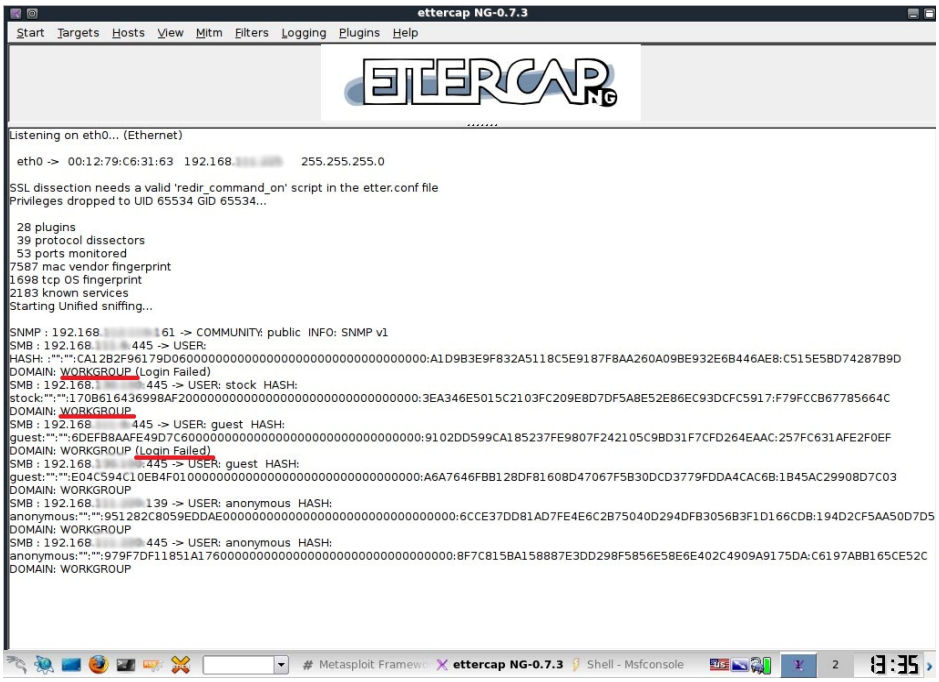


Figure 0.25 : Trafic capté par l'outil *Ettercap*

L'outil *ldp.exe* n'a pas pu accéder aux données d'AD car on n'a pas obtenu le mot de passe correcte de l'administrateur du domaine ou de n'importe quel utilisateur qui est membre des groupes administratifs.

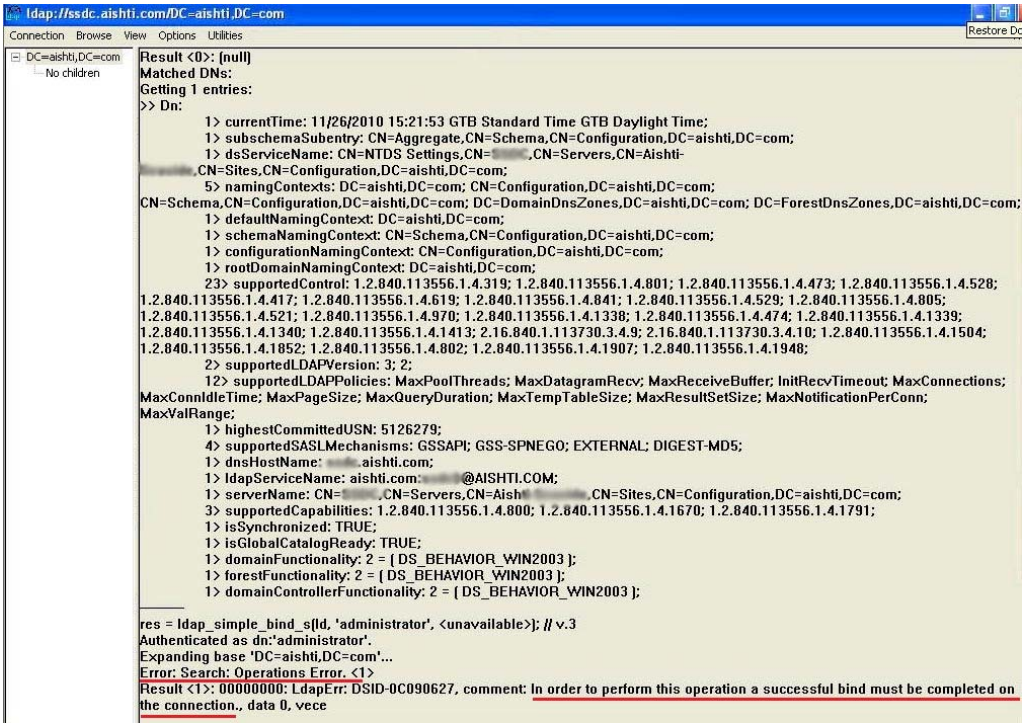


Figure 0.26 : Ouverture de session infructueuse avec *ldp.exe* sur AD

5.1.4.2 Les maliciels

L'infection par les maliciels est basée principalement sur la curiosité et l'ignorance des utilisateurs : Ouverture des pièces jointes de n'importe quel expéditeur, accès aux adresses *URL* étrangers malicieux, utilisation de medias infectées, téléchargement des fichiers soupçonneux…

Tous ces problèmes ont été réglés par plusieurs solutions :

- Sessions de sensibilisation pour tous les employés
- Interdire l'utilisation des medias externes
- Installation et mis à jour de l'anti-virus chez tous les postes
- Filtrage des pages web accessibles par les utilisateurs

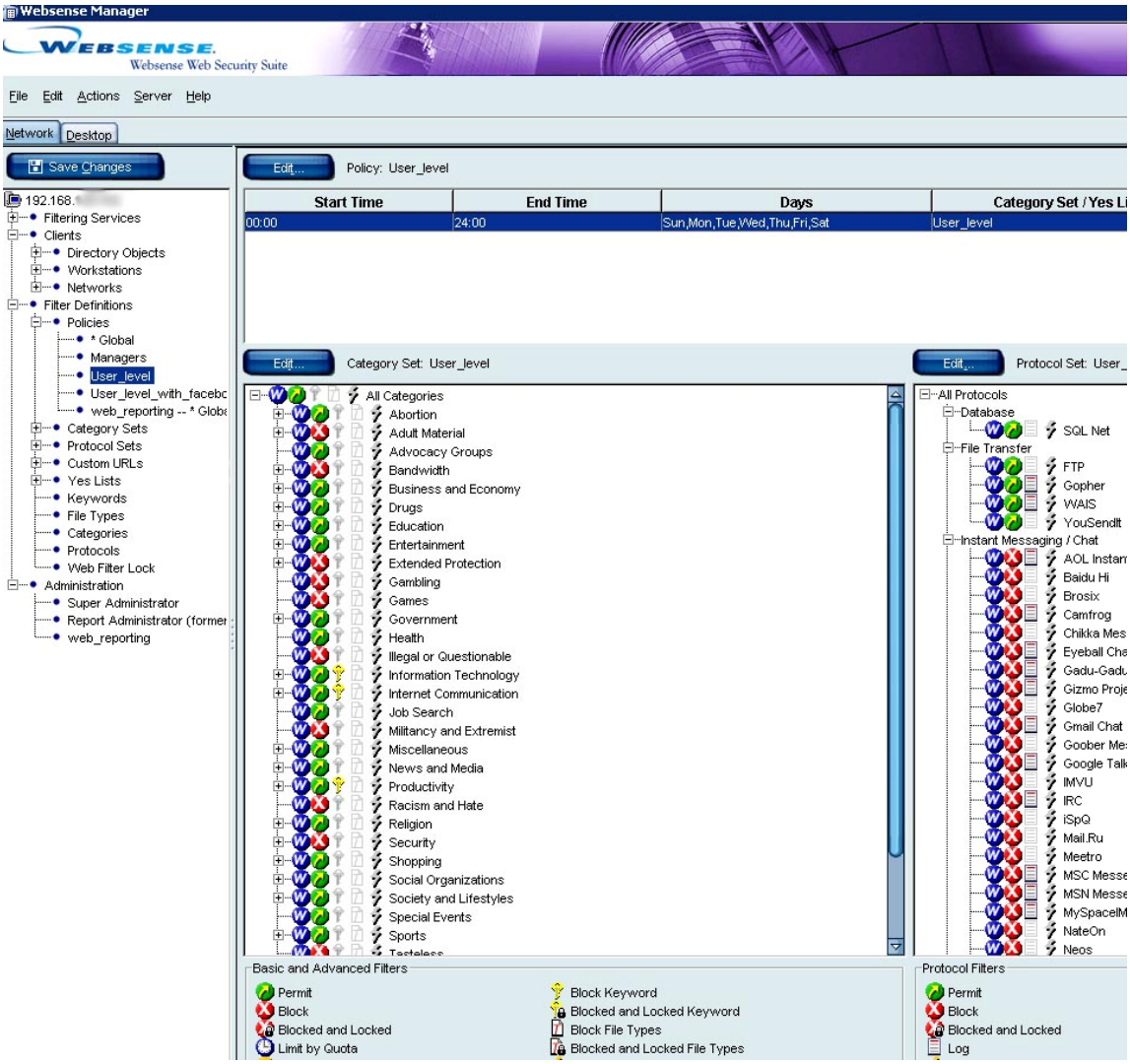


Figure 0.27 : Filtrages des pages web par l'outil Websense

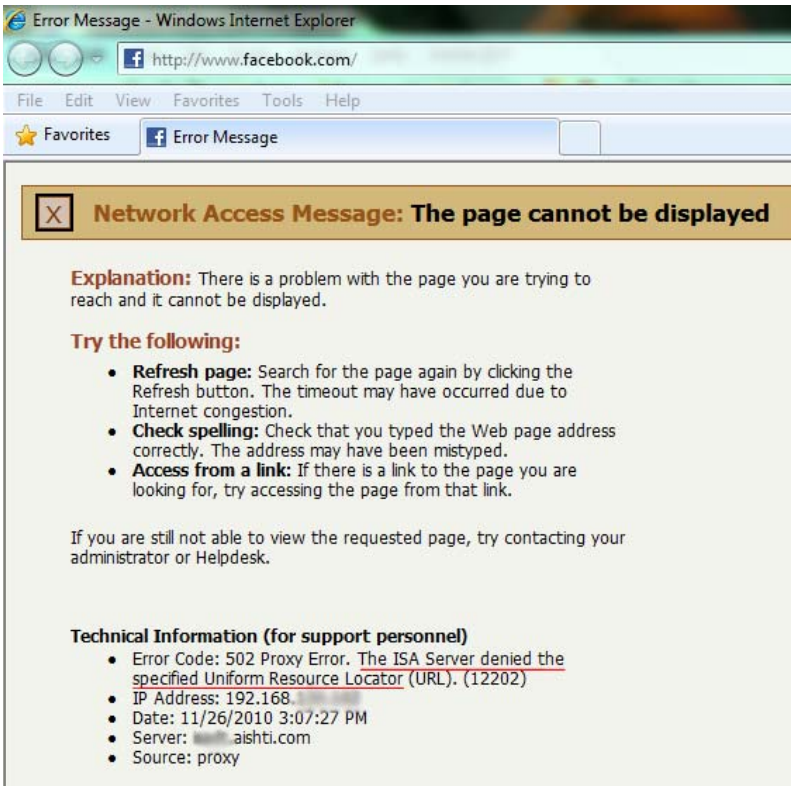


Figure 0.28 : Filtrages des pages web par l'outil ISA Server de Microsoft

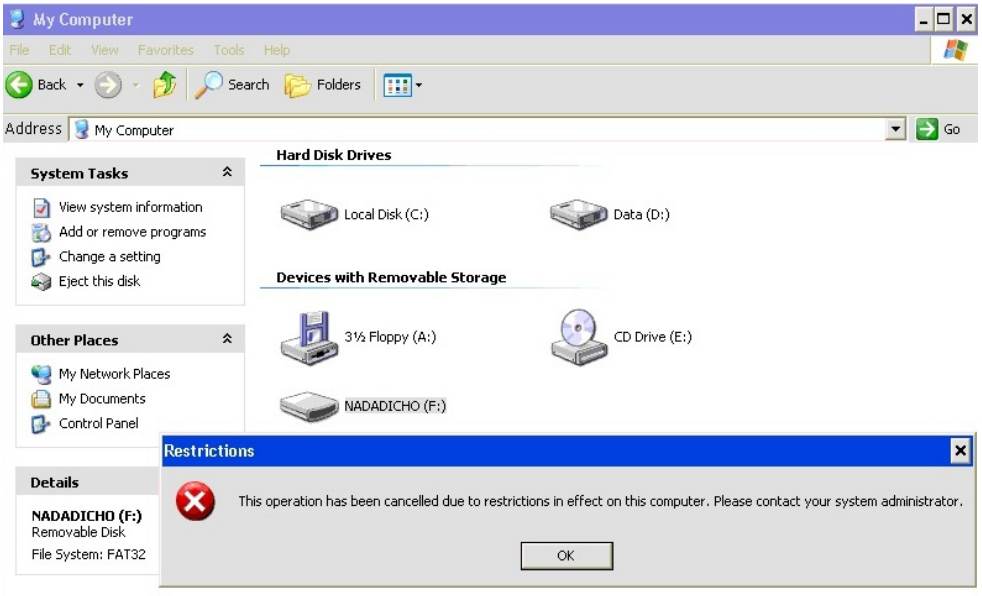


Figure 0.29 : Medias externe inaccessibles par les utilisateurs

5.1.4.3 Les messageries

La sécurisation des systèmes des messageries est réalisée grâce à plusieurs outils de filtrages des messageries électroniques et instantanées. Ces outils ont été implémentés depuis deux ans, à travers le pare-feu Barracuda, mais quelques modifications mineures ont été ajoutées aux règles existantes :

- Filtrage des pièces jointes des messages électroniques
- Filtrage des expéditeurs et destinataires autorisés

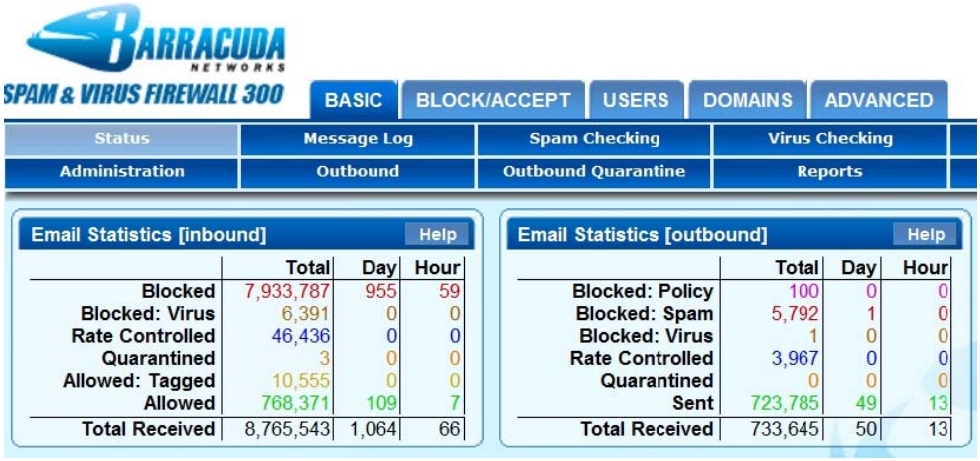


Figure 0.31 : Statistiques de filtrage des messages électroniques de l'outil Barracuda

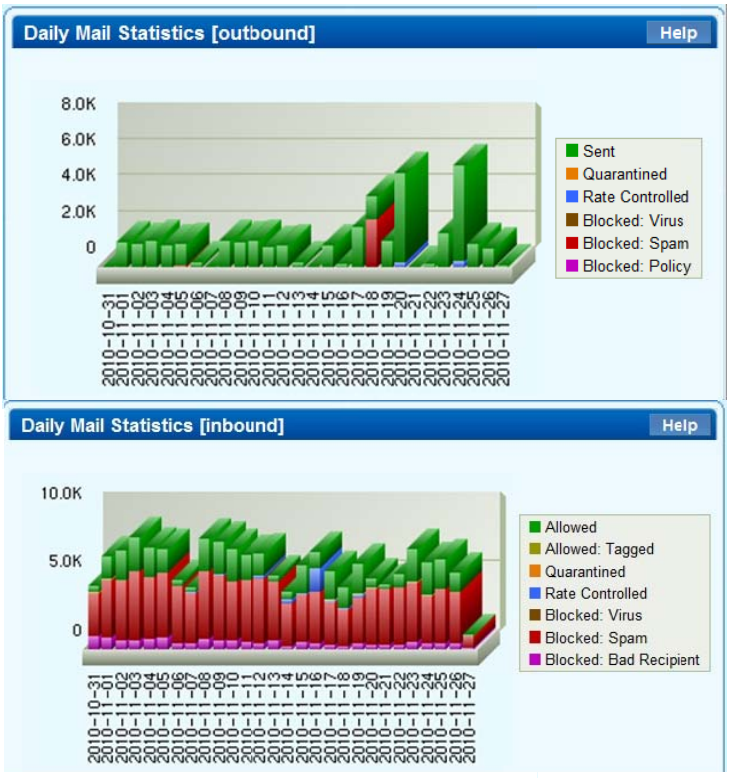


Figure 0.30 : Statistiques de filtrage journalières des messages électroniques de l'outil Barracuda

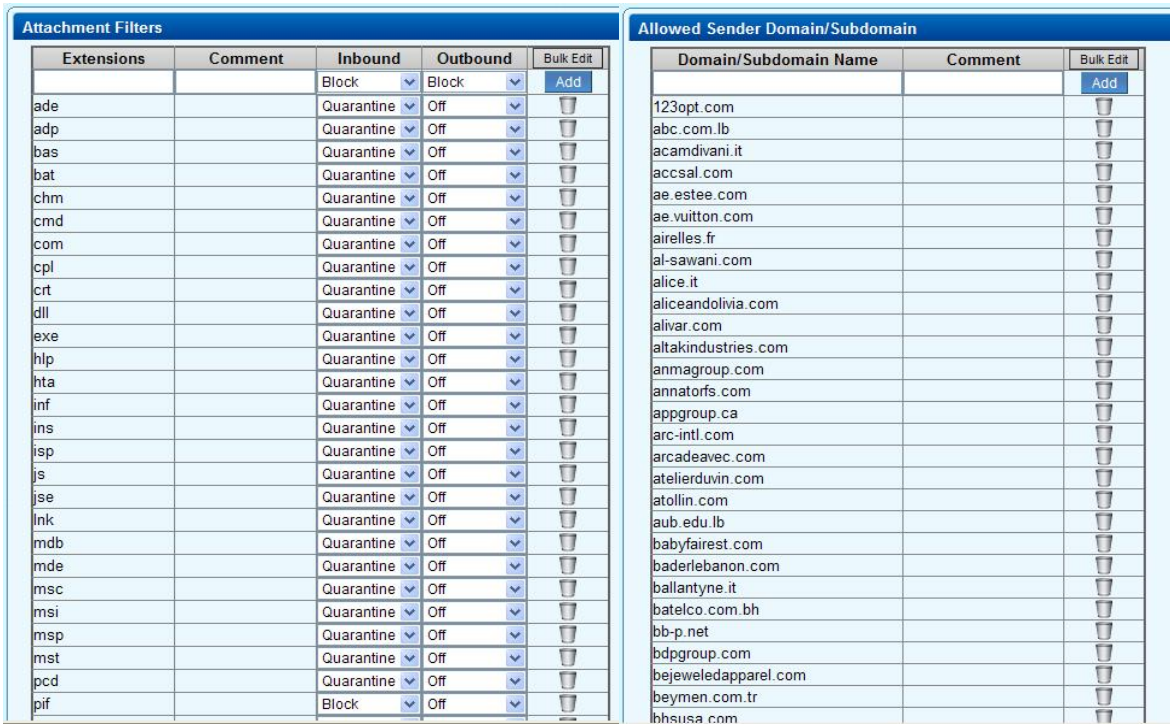


Figure 0.32 : Règles de filtrages des messageries électroniques

La sécurisation d'une session d'authentification avec le serveur de messagerie a été accomplie à travers le changement de la méthode d'authentification pour être *Integrated Windows Authentication* au lieu de *Form Based Authentication* qui envoi les données en plein texte.

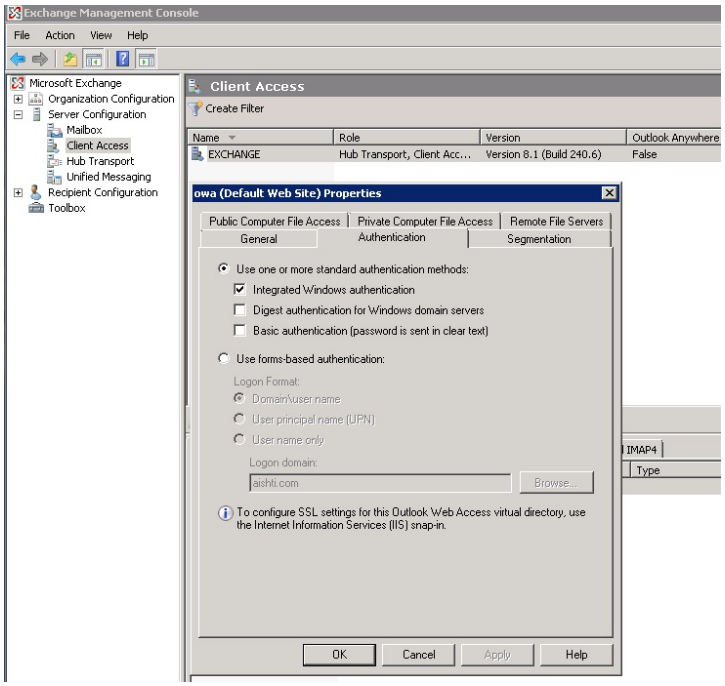


Figure 0.33 : Méthode d'authentification avec le serveur de messagerie

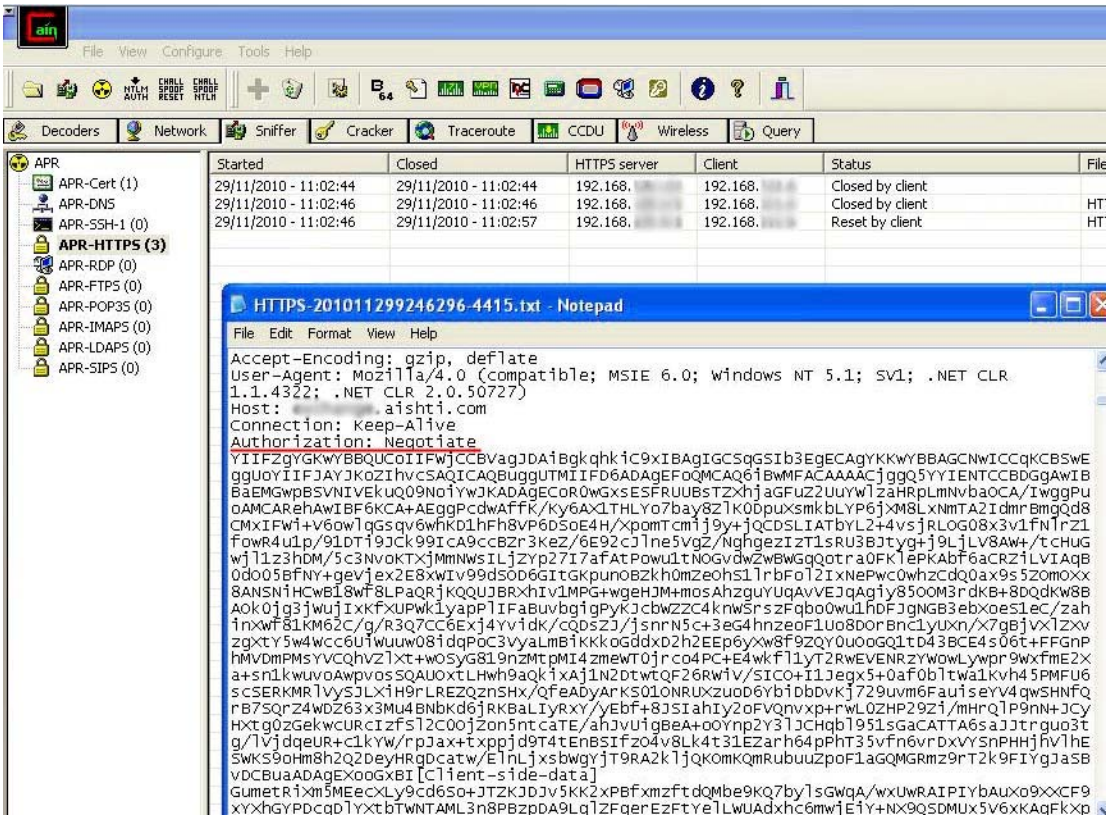


Figure 0.34 : Captage de session d'authentification crypté après sécurisation

L'essai d'envoyer un message de la part d'un utilisateur de l'organisation échoue suivant les règles du serveur destinataire. Ci celui-ci est bien configuré il s'assure de l'adresse IP du serveur du domaine reçu sinon il recevra de quiconque.

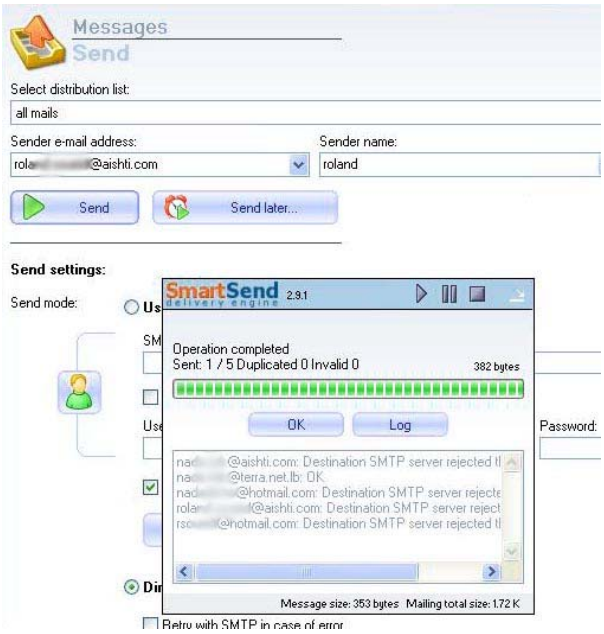


Figure 0.35 : Résultat de livraison d'un courrier envoyé de la part d'un utilisateur interne

5.1.4.4 Injection de code SQL

Le problème majeur d'Oracle rencontré dans les parties précédentes était l'excès de privilèges des utilisateurs réguliers. Après la révocation des privilèges excédés, les essais d'accéder aux ressources par un utilisateur régulier à travers l'interface SQL, la commande *sqlplus* ou les interfaces du logiciel MACC, ainsi qu'avec l'outil *checkpwd* pour balayer les utilisateurs existants ont échoué à cause de manque de privilèges.

La vulnérabilité dans l'extension de privilèges par injection de code dans le fichier de libraire *oraclient10.dll* a été fixée par le contrôle d'accès sur le répertoire contenant tous les fichiers système d'Oracle.

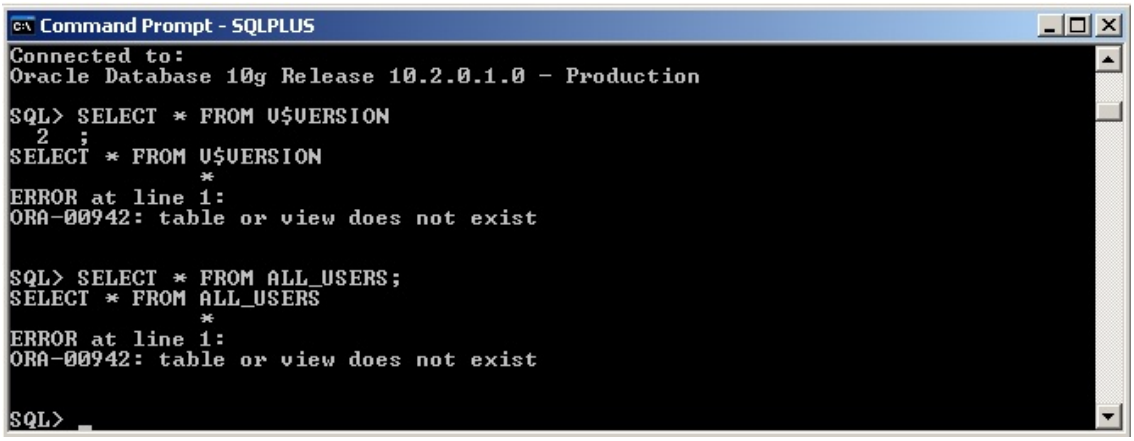


Figure 0.36 : Accès aux ressources systèmes par un utilisateur régulier échoué

Figure 0.37 : Résultat négatif de l'outil *checkpwd*

La majorité des tests d'attaques au niveau de la couche Application ont échoués de pénétrer les systèmes ou d'obtenir des données pertinentes. Le système est totalement sécurisé au niveau du SE, attaques des maliciels, attaques par messageries ou par injection de code SQL.

Table 0-IV : Résultats des tests de la couche Application

	Date des tests	Vulnérabilités / Etat	Risques / Impact	Résultat
Systèmes d'exploitation	26/11/2010	Tous les postes sécurisés par mot de passe complexe	Accessibilité difficile	Non compromis
Maliciels	26/11/2010	Tous les postes avec anti-virus totalement sécurisé	Accessibilité difficile	Non compromis
Messagerie	27/11/2010	Session d'authentification cryptée Messagerie instantanée sécurisées	Accessibilité complexe	Non compromis
Injection de code SQL	30/11/2010	Eliminer les privilèges administratifs des utilisateurs réguliers	Accessibilité complexe	Non compromis

5.2 Modèle de référence

Un système informatique sécurisé efficacement exige une approche intégrée de défense en profondeur. La première couche d'une approche de défense en profondeur est la mise en œuvre des éléments fondamentaux de la sécurité. Ces éléments constituent un modèle de référence solide sur lequel des méthodes et techniques avancées peuvent ensuite être construit.

Le développement et le déploiement d'un modèle de référence peut toutefois être difficile en raison de la vaste gamme de fonctions disponibles. Pour accomplir cette tâche on se base sur les éléments clés de sécurité qui devraient être abordées dans la première phase de mise en œuvre de la défense en profondeur.

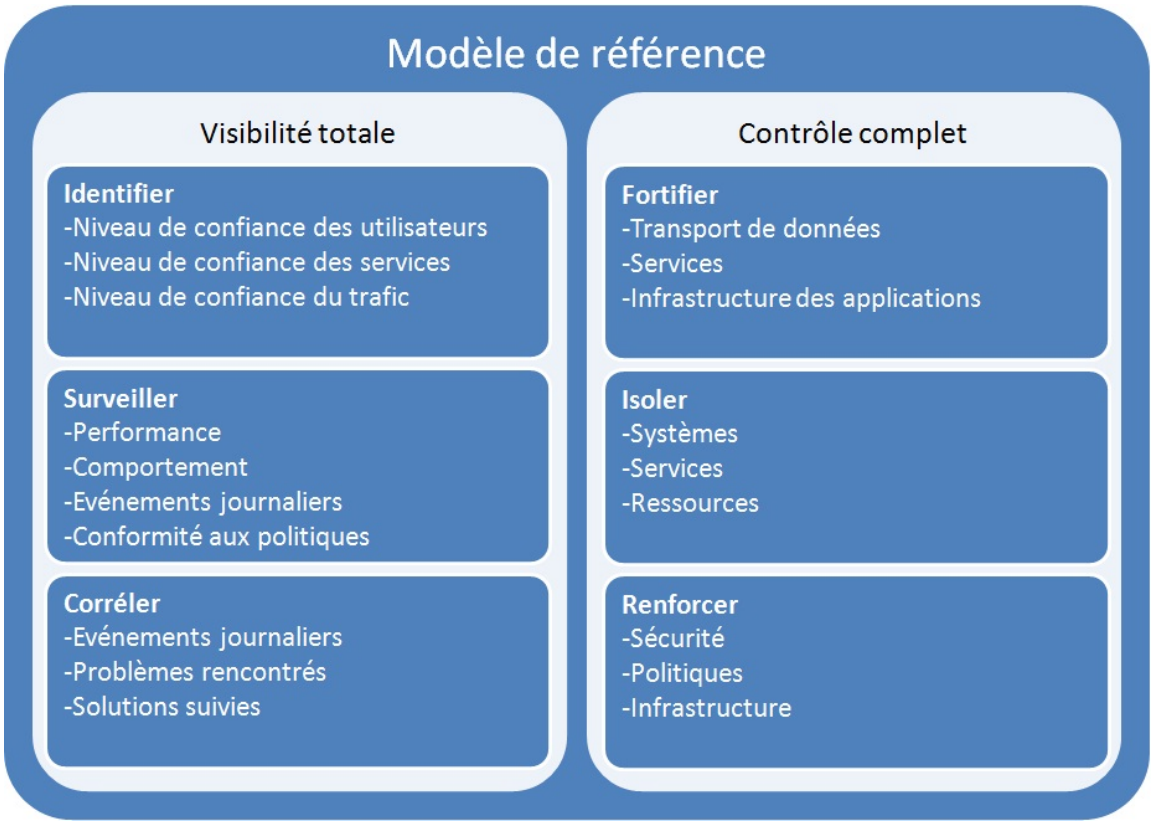


Figure 0.38 : Eléments clés d'un modèle de référence
Référence : ***Network Security Baseline – chapter 1 – Introduction (Cisco)***

Le modèle de référence doit joindre deux fonctions majeures : la visibilité totale du système et son environnement et le contrôle complet des activités et fonctions de ce système dans cet environnement. Les éléments du modèle de référence ont été catégorisés suivant les éléments majeurs d'un système informatisé.

5.2.1 Utilisateurs

- Mis à jour des comptes des utilisateurs
- Privilèges nécessaires et limités
- Contrôle et mis à jour des cartes d'accès
- Mis à jour des listes d'accès aux ressources (ACL)
- Grouper les utilisateurs à configuration commune
- Sensibilisation au système et dangers
- délai de session

5.2.2 Serveur et clients

- Anti-virus activé et mis à jour

- UPS et ventilation
- Verrouiller poste après certain temps d'inactivité
- Supprimer les utilisateurs locaux
- Mot de passe complexe pour l'administrateur local
- Horaire de scan quotidien par l'antivirus
- Mis à jour de l'inventaire des dispositifs informatiques

5.2.3 Périphériques du réseau

- Noms catégoriques et clairs
- Mots de passes complexes
- Eliminer configuration par default
- Bannière de notification : ACCÈS INTERDIT AUX PERSONNES NON AUTORISÉES
- Désactiver les services inutiles
- Fermer les ports inutiles
- Cryptage du trafic wi-fi
- Supprimer les CS inutilisés
- Sécurisation dans des racks verrouillés

5.2.4 Politiques de groupe

- Désactiver les medias externes (cd, usb, bluetooth…)
- Activé le Pare-feu
- Mis à jour régulière des SE
- Complexité des mots de passe
- Profile limité pour les caissiers
- Paramètre des journaux d'événements

5.2.5 Salles informatiques

- Système de contrôle d'accès
- Système de détection d'humidité, chaleur et feu
- Câblage sécurisé et annoté
- Plancher surélevé
- Cameras de surveillance
- Système de détection de mouvement lié à un composeur automatique

5.2.6 Documentation

- Inventaire des dispositifs informatiques et leurs propriétaires
- Problèmes survenus sur chaque dispositif
- Solutions suivies pour chaque problème
- Licences des SE et logiciels procurés
- Contrats de maintenance et rapports de visites correctives
- Incidents et actions correctives

5.2.7 Politiques de prévention

- Définir les éléments indispensables pour maintenir l'activité de l'entreprise : base de données, serveurs, commutateurs, emails…
- Backup des données hors sites : base de données, fichiers des utilisateurs, configurations des périphériques…
- Redondance des dispositifs : chargeurs électriques, disques durs, serveur…
- Planification de la capacité : alarme déclenché sur le seuil 80%
- Familiarisation avec le processus de récupération après incident
- Vérification de l'efficacité de la documentation de récupération
- Vérification de l'efficacité du site de récupération
- Vérification si les objectifs de récupération sont réalisables
- Tester le processus entier de récupération

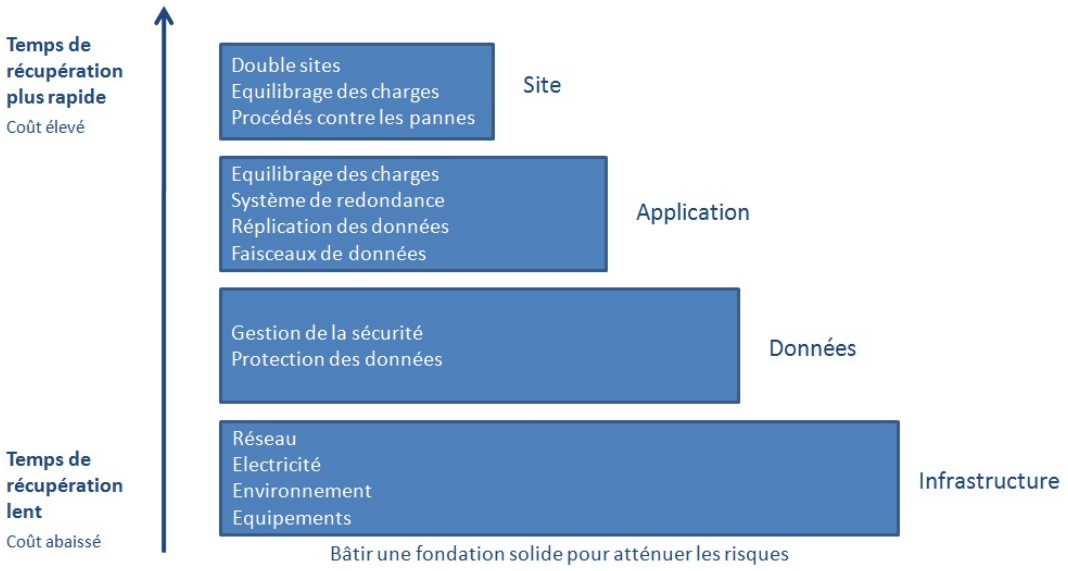


Figure 0.39 : Diagramme des éléments fondamentaux du système
Référence : *http*://eolastechnologies.com/what-we-do/it-management/disaster-recovery

5.2.8 La planification en cas d'incident

- Estimation temps de reprise après panne
- Suivre les procédures de récupération
- Identifier les améliorations et dispositifs nécessaires
- Utilisation des dispositifs secondaires

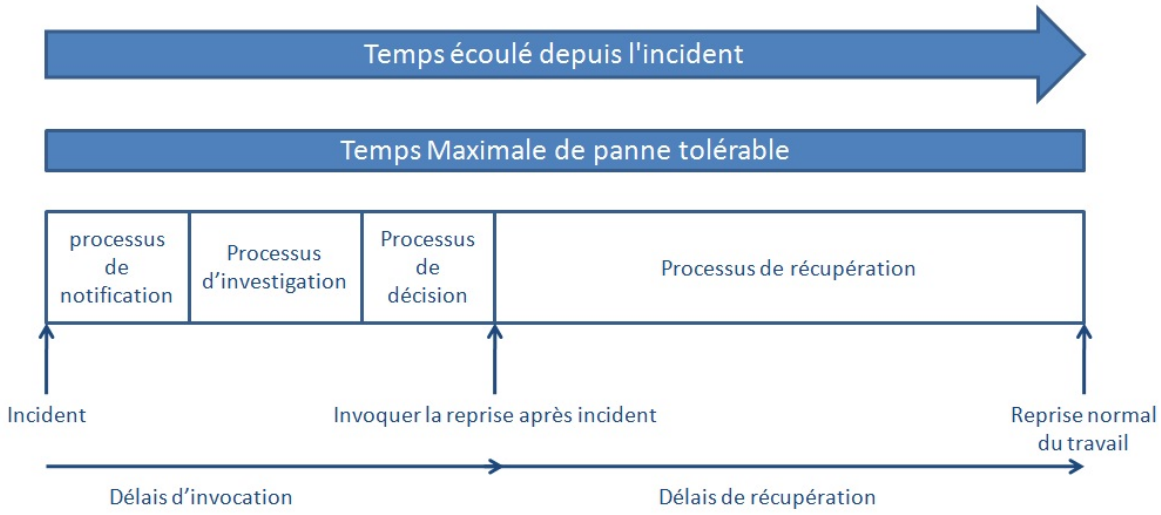


Figure 0.40 : Flux d'activités en cas d'incident
Référence : *http:*//www.continuitycentral.com/feature0524.htm

Ce modèle de référence peut être utilisé au cours de l'évaluation initiale d'un système informatique et durant les phases d'analyse des lacunes. Il donne les exigences minimales de contrôle et gestion de sécurisation de ce système. Dans le futur, les forces et faiblesses du système peuvent être identifiés en les comparants à ce modèle de référence.

5.3 Listes de contrôle

L'étude effectuée tout au long de ce projet, ainsi que les améliorations implémentées ont fortifié considérablement le niveau de sécurité des infrastructures informatiques de l'organisation. Mais ces travaux doivent être complémentés par des taches de contrôle à base quotidienne, hebdomadaire, mensuelle, annuelle et occasionnelle.

5.3.1 Quotidienne

- **Systèmes de contrôle**
  - Enregistrement des cameras continu

- Etat des cameras acceptable : vision, cadre…
- Système de détection de mouvement, feu et humidité fonctionnel
- Lumière ou message d'erreur sur les dispositifs
- Composeur automatique fonctionnel
- Mis à jour des nouveaux dispositifs dans le logiciel IT
- Mis à jour des cartes d'accès

- **Backup**
  - Base de données de Macc
  - Base de données des messageries électroniques et instantanées
  - Base de données du logiciel IT
  - Fichiers des utilisateurs

5.3.2 Hebdomadaire

- Vérification des fichiers journaux et de l'observateur d'événements (Event Viewer)
- Les adresses IP allouées par les modems d'internet
- Contrôle des anti-virus : versions, signatures, quarantaine, notifications…
- Redémarrage des serveurs
- Etat des UPS : surcharge, décharge…
- Suivre / surveiller la performance et l'activité du système
- Redémarrages des serveurs

5.3.3 Mensuelle

- **Mis à jour**
  - Utilisateurs et objets d'AD
  - Utilisateurs locaux des SE
  - Utilisateurs de MACC
  - Listes d'accès sur les ressources
  - Listes des adresses emails des utilisateurs des scanneurs
  - Listes d'accès sur les portes sécurisés
  - Correctifs logiciels

- **Contrôle**
    - Chambres informatiques : ventilation, fuite d'eau, câblage…
    - Niveau des vulnérabilités par branche
    - Espace disque restant
    - Fichiers journaux de l'AD
    - Fichiers journaux de MACC
    - Fichiers journaux des portes d'accès
    - Statistiques du trafic du réseau
    - Stock des consommables : CD, DVD, encre…
    - Stock des dispositifs informatiques : ordinateur, écrans, clavier, souris…

- **Backup**
    - Base de données de l'AD
    - Configuration des systèmes des messageries
    - Configurations des périphériques du réseau
    - Configurations des centrales téléphoniques (PBX)
    - Fichiers systèmes de Macc
    - Site interne de l'organisation

5.3.4 Occasionnelle

- Récupérer à partir des fichiers de sauvegarde (backup)
- Contrôle des licences des logiciels
- Contrats de maintenance

Conclusion

Le groupe « TSG » est en voie continue d'expansion géographique, humaine et technologique. Son système informatique s'est développé proportionnellement avec ses expansions, mais les mesures de sécurisation prises auparavant sont désormais insuffisantes pour faire face aux nouveaux risques et attaques informatiques. Les motivations des pirates performants ces attaques peuvent être un simple défi d'accès, un vol d'information ou l'arrêt total du système piraté. C'est en raisonnant comme un pirate qu'on peut protéger au mieux le système d'information de l'entreprise. Il faut comprendre les types de piratages auxquels on fait face et les objectifs des pirates attaquants, d'où le recours au piratage éthique pour évaluer les risques et vulnérabilités existantes et appliquer les contres mesure nécessaires.

Le système informatique est formé de plusieurs composants humains, matériels et logiciels. Afin de viser tous ces composants, la méthodologie d'attaque suivie est basée sur l'hiérarchie des couches du protocole TCP : Accès physique, Internet, Transport, Application. Sur chaque niveau plusieurs tests ont été conduits et le taux de réussite des attaques variaient entre 40% et 60% selon les vulnérabilités existantes dans chaque couche.

La majorité des vulnérabilités rencontrées résident dans les périphériques non sécurisés physiquement, ayant des configurations ou mots de passe par default et contenant des services ou ports inutile mais accessibles. Les solutions des vulnérabilités découvertes consistent à l'amélioration de la sécurisation et le contrôle des chambres informatiques, en ajoutant des systèmes de détection de chaleur, d'humidité et de mouvement, verrouillant les racks et implémentant des systèmes de contrôle d'accès avec des cameras de surveillance, personnalisation des configurations initiales avec des identifiants complexes et l'arrêtage des services et ports inutilisés.

Un problème majeur d'excès de privilèges est rencontré dans la base de données Oracle. Ce problème menace non seulement les données pertinentes de l'entreprise mais son cycle de travail entier. L'implémentation de nouvelles normes de sauvegarde à travers une connexion privilégiée temporaire et l'amélioration de la distribution des privilèges suivant les rôles a éliminé les risques existants.

L'étude des vulnérabilités des systèmes après sécurisation à partir des mêmes tests utilisées précédemment dévoile un taux de vulnérabilités inferieur à 5%, donc une réduction importante par rapport à l'état initial. Le piratage éthique est donc un moyen efficace de défense contre les mauvais pirates, il ne garantie pas la sécurité idéale du système mais il est un bon point de départ. Afin de maintenir ou même réduire le taux obtenu, il faut implémenter un programme de sécurisation basé sur le modèle de référence proposé et suivant les listes de contrôle périodiques.

Le travail de piratage éthique effectué dans ce projet a consolidé considérablement la sécurité du système informatique de l'organisation. Désormais les composants de ce système sont protégés de tout genre de pirates malveillants, que ce soit un employé, un client ou un étranger sur internet, ils ne pourront pas pénétrer le système et tout essai d'attaque sera capté et analysé par les membres du département informatiques.

Toute entreprise a un système informatisé ouvert aux utilisateurs internes et au réseau externe à travers l'internet. Les méthodes de sécurisations implémentées doivent être mise à jour régulièrement pour faire face aux nouvelles technologies d'attaques disponibles à tous genres de pirates. Le recours au piratage éthique est un bon point de départ pour toutes les entreprises, il aidera à évaluer le niveau de sécurité actuel et identifier les vulnérabilités existantes dans leur système. Il est important après l'évaluation d'élaborer un modèle de référence qui servira de base pour toute expansion future, et des listes de contrôle périodiques permettant aux administrateurs des systèmes de contrôler les activités survenant.

Les pirates éthiques œuvrent à une amélioration permanente des systèmes de sécurité des entreprises. Ils se mettent dans la peau d'un hacker pour mesurer la vulnérabilité des entreprises aux attaques. A mesure que l'Internet se développe et les outils d'infiltrations augmentent exigeant moins de compétence, le besoin de sécurité augmente.

La majorité des entreprises n'ont pas des spécialistes de sécurité informatique, ils ont recours alors à l'externalisation de service de piratage éthique. Le département informatique confronte alors plusieurs interrogations :

Serait-il toujours impliqué des activités effectuées ?

Est-ce une bonne idée de céder les rênes à un tiers pour tester la sécurité sans faire de suivi et rester au-dessus de ce qui se passe ?
Est-ce que les entrepreneurs évaluent les dangers du piratage sur leur organisation ?
Seront-ils préparés à investir dans un travail de piratage éthique ?
Auront-ils recours à leur propre département informatique ou choisiront-ils l'externalisation ?

C'est notre travail en tant qu'ingénieur des systèmes informatiques de valoriser notre système par rapport aux directeur et employés. Il ne suffit pas d'avoir un système opérationnel, mais il faut prévoir un plan de contrôle et de sécurisation à long terme. Il faut rester au courant des nouveaux risques menaçants, concevoir et développer des nouvelles normes de sécurisation et inciter les directeurs à investir pour une amélioration continue des systèmes informatiques.

Bibliographie

Attaques et arnaques, http://www.aidenet.com/encyclopedie/attaques/attaques.htm, 16/6/2009

Backtrack-linux, http://www.backtrack-linux.org/downloads/, 30/6/2010

BEIVER K., 2004. *Hacking for dummies*, Wiley Publishing, Inc., Indianapolis, Indiana, 387 p.

Casser une clé wep/wpa avec la suite Aircrack-ng, http://wiki.backtrack-fr.net/index.php/Casser_une_cl%C3%A9_wep/wpa_avec_la_suite_Aircrack-ng, 17/05/2010

Certified Ethical Hacker Course V5, http://www.eccouncil.org, 17/6/2009

CHANTUCK W., 2002, *Conducting a Penetration Test on an Organization*, SANS Institute, Malaysia, 16 p.

Cisco Systems, Inc., 2008. *Network Security Baseline*, Cisco Systems, Inc., USA, 184 p.

Disaster Recovery, http://eolastechnologies.com/what-we-do/it-management/disaster-recovery/, 1/12/2010

Ethical Hacking Techniques to Audit and Secure Web-enabled Applications, http://www.cgisecurity.com/pen-test/Auditing-and-Securing-Web-enabled-Applications.pdf, 26-6-09

Guide Oracle, http://oracle.developpez.com/guide/administration/adminrole/, 3/11/2010

Hacker, http://fr.wikipedia.org/wiki/Hacker, 04/06/2009

Injection SQL, http://fr.wikipedia.org/wiki/Injection_SQL, 26/06/2009

Introduction au piratage, http://www.commentcamarche.net/contents/attaques/attaques.php3, 13/6/2009

IT baseline protection, http://en.wikipedia.org/wiki/IT_baseline_protection, 30/11/2010

L0phtcrack, http://www.l0phtcrack.com/download.html, 20/07/2010

La sécurité physique, http://www.cases.public.lu/fr/publications/fiches/pdf/Fiche_securite_physique.pdf, 09/03/2010

Le piratage informatique, http://projet.piratage.free.fr/techniques.html, 17/06/2009

Le piratage informatique, http://znsoft.be/Securite/Hackers, 05/06/2009

Les attaques par dénis de service,

http://www.linux-france.org/prj/inetdoc/securite/tutoriel/tutoriel.securite.destruction.dos.html, 16/06/2009

Network Security & Survivability, http://nsl.cs.columbia.edu/projects/sos/, 16/06/2009

Nmap, http://nmap.org/index.html, 04/05/2010

Oracle9i Database Concepts, Release 2 (9.2), Privileges, Roles, and Security Policies, http://download.oracle.com/docs/cd/B10500_01/server.920/a96524/c24privs.htm, 15/10/2010

Router Hacking Part 4 (SNMP Attacks using SNMPCheck), http://www.securitytube.net/Router-Hacking-Part-4-(SNMP-Attacks-using-SNMPCheck)-video.aspx, 15/07/2010

SCAMBRAY J., MCCLURE S., 2001, *Hacking Exposed – Network Security Secrets and Solutions*, MCGraw-Hill, USA, 736 p.

SCAMBRAY J., MCCLURE S., 2008, *Hacking Exposed Windows - Windows Security Secrets & Solutions*, MCGraw-Hill,USA, 482 p.

Security Checklists, http://iase.disa.mil/stigs/checklist/index.html, 6/12/2010

Sécurité TCP/IP, http://www.hsc.fr/ressources/presentations/cruscantools/img0.htm, 14/06/2009

SYN flood, http://fr.wikipedia.org/wiki/SYN_flood, 15/06/2010

System administrator checklist, http://www.scribd.com/doc/4623275/System-Administrator-Checklist, 5/12/2010

Taking advantage of opportunities – avoiding risks, https://www.bsi.bund.de/cln_156/EN/Home/home_node.html, 30/11/2010

TCP/IP, http://www.commentcamarche.net/contents/internet/tcpip.php3, 19/07/2010

The IT disaster recovery plan, http://www.continuitycentral.com/feature0524.htm, 01/12/2010

University Of California, 2005, *Business & Finance Bulletin IS-3, Electronic Information Security*, University Of California, California, 35 p.

Utilisation de Sslstrip pour une attaque man in the middle sur du https (SSL), *arpspoof et hack paypal*, http://www.crack-wifi.com/tutoriel-sslstrip-hijacking-ssl-mitm-https.php, 08/07/2010

Liste des figures

Liste des tableaux