Université de la Manouba
Ecole Nationale des Sciences de l'Informatique

Mastère Spécialisé en Sécurité Informatique

Modules Sécurité de Linux et des Services WEB

Projet :Mise en place d'une sonde

Proposé par :
Dr Mohamed ROMDHANI

Réalisé par :
M. Fathi BEN NASR
Mme Alia KHESSAIRI ABBASSI

Année universitaire : 2004-2005

1- Introduction

L'ouverture des systèmes et leurs interconnexion avec le réseau Internet ont fait que les attaques soient de plus en plus nombreuses et diversifiées les unes que des autres.

Outre la mise en place de par-feux et de systèmes d'authentification , il est de nos jours nécessaire de mettre en place un système de détection d'intrusion.

Principalement, nous distinguons deux catégories de systèmes de détection d'intrusion :
Le premier type est formé par les détecteurs d'intrusion basés sur l'hôte (HIDS), ceux-ci analysent et contrôlent uniquement l'activité et les informations de l'hôte sur lequel est installé le HIDS et assurent ainsi seulement la sécurité de l'hôte en question. La deuxième catégorie est formée par les détecteurs d'intrusion réseau (NIDS), ceux-ci observent et analysent le trafic réseau, cherchent des indicateurs d'attaques et envoient des alertes.
SNORT, logiciel open source se situe dans la deuxième catégorie des IDS.

Dans ce qui suit, nous allons commencer par donner une présentation générale de SNORT, ensuite nous allons présenter sa manipulation :installation, configuration et fonctionnalités. Enfin, nous allons terminer par donner une conclusion et des perspectives pour ce travail.

2- Présentation Générale

SNORT est NIDS écrit par Martin Roesch, disponible sous licence GNU, son code source est accessible et modifiable à partir de l'URL : « http://www.snort.org »

SNORT permet d'analyser le trafic réseau de type IP, il peut être configuré pour fonctionner en trois modes :

- le mode sniffer : dans ce mode, SNORT lit les paquets circulant sur le réseau et les affiche d'une façon continue sur l'écran ;
- Le mode « packet logger » : dans ce mode SNORT journalise le trafic réseau dans des répertoires sur le disque ;

- le mode détecteur d'intrusion réseau (NIDS) : dans ce mode, SNORT analyse le trafic du réseau, compare ce trafic à des règles déjà définies par l'utilisateur et établi des actions à exécuter ;
- le mode Prévention des intrusion réseau (IPS), c'est SNORT-inline.

2-1 NIDS

le NIDS est un logiciel qui, installé sur un matériel généralement dédié, place la carte réseau du système hôte en mode promiscuité (toutes les trames sont remontées à la couche IP indépendamment de l'adresse MAC de destination) afin de remonter tout le trafic réseau au logiciel NIDS.

Ce trafic est alors analysé en fonction d'un ensemble de règles et de signatures d'attaques pour déterminer s'il faut générer des actions (log, alerte, …).

2-2 Positionnement de SNORT dans le réseau

L'emplacement physique de la sonde SNORT sur le réseau a un impact considérable sur son efficacité.

Dans le cas d'une architecture classique, composée d'un Firewall et d'une DMZ, trois positions sont généralement envisageables :

- avant le Firewall ou le routeur filtrant : dans cette position, la sonde occupe une place de premier choix dans la détection des attaques de sources extérieures visant l'entreprise. SNORT pourra alors analyser le trafic qui sera éventuellement bloqué par le Firewall. Les deux inconvénients de cette position du NIDS sont: primo, le risque engendré par un trafic très important qui pourrait entraîner une perte de fiabilité et secondo, étant situé hors du domaine de protection du firewall, le NIDS est alors exposé à d'éventuelles attaques pouvant le rendre inefficace.
- sur la DMZ : dans cette position, la sonde peut détecter tout le trafic filtré par le Firewall et qui a atteint la zone DMZ. Cette position de la sonde permet de surveiller les attaques dirigées vers les différents serveurs de l'entreprises accessibles de l'extérieur.
- sur le réseau interne :le positionnement du NIDS à cet endroit nous permet

d'observer les tentatives d'intrusion parvenues à l'intérieur du réseau d'entreprise ainsi que les tentatives d'attaques à partir de l'intérieur. Dans le cas d'entreprises utilisant largement l'outil informatique pour la gestion de leur activités ou de réseaux fournissant un accès à des personnes peu soucieuses de la sécurité (réseaux d'écoles et d'universités), cette position peut revêtir un intérêt primordial.

2-2 architecture de SNORT

L'architecture de SNORT est modulaire et est composée de :

- un noyau de base :au démarrage, ce noyau charge un ensemble de règles ,compile, optimise et classe celles-ci. Durant l'exécution, le rôle principal du noyau est la capture de paquets.
- Une série de pré – processeurs, ceux-ci améliorent les possibilités de SNORT en matière d'analyse et de recomposition du trafic capturé. Ils reçoivent les paquets directement capturés, éventuellement les retravaillent puis les fournissent au moteur de recherche de signatures.
- Une série d'analyses est ensuite appliquée aux paquets. Ces analyses se composent principalement de comparaisons de différents champs des headers des protocoles (IP, ICMP, TCP et UDP) par rapport à des valeurs précises.
- Après la détection d'intrusion, une série de « output plugins » permet de traiter cette intrusion de plusieurs manières : envoie vers un fichier log, envoie d'un message d'alerte vers un serveur syslog, stocker cette intrusion dans une base de données SQL.

2-3 Pré-processeurs de SNORT

Les pré-processeurs permettent d'étendre les fonctionnalités de SNORT. Il sont exécutés avant le lancement du moteur de détection et après le décodage du paquet IP. Le paquet IP peut être modifié ou analysé de plusieurs manières en utilisant le mécanisme de pré-processeur.

les pré-processeurs sont chargés et configurés avec le mot-clé preprocessor. Le format de la directive preprocessor dans les règles de SNORT est :

preprocessor <nom> : <options>

Exemple de pré-processeurs :

Le détecteur portscan : ce pré-processeur permet de :

- enregistrer le début et la fin d'un scan de ports à partir d'une seule adresse IP.
- lorsqu'un fichier de log est spécifié, ce pré-processeur journalise les IP et les ports scannés ainsi que le type du scan.

Exemple :

Preprocessor portscan 192.168.1.0/24 /var/log/snort

2-4 les règles de SNORT

Les règles de SNORT sont composées de deux parties distinctes : le header et les options.

Le header permet de spécifier le type d'alerte à générer (alert, log et pass) et d'indiquer les champs de base nécessaires au filtrage : le protocole ainsi que les adresses IP et ports sources et destination.

Les options, spécifiées entre parenthèses, permettent d'affiner l'analyse, en décomposant la signature en différentes valeurs à observer parmi certains champs du header ou parmi les données.

Exemple de règle :

Alert tcp any any -> 192.168.1.0/24 80 (flags :A ;\content : "passwd"; msg: "detection de `passwd' " ;)

Cette règle permet de générer un message d'alerte "detection de passwd" lorsque le trafic à destination d'une machine du réseau local 192.168.1.0/24 vers le port 80, contient la chaîne « passwd » (spécifié par l'utilisation du mot-clé « content »), et que le flag ACK du header TCP est activé (flags : A).

3- Manipulations

3-1 Topologie du réseau de test utilisé et emplacement des sondes SNORT

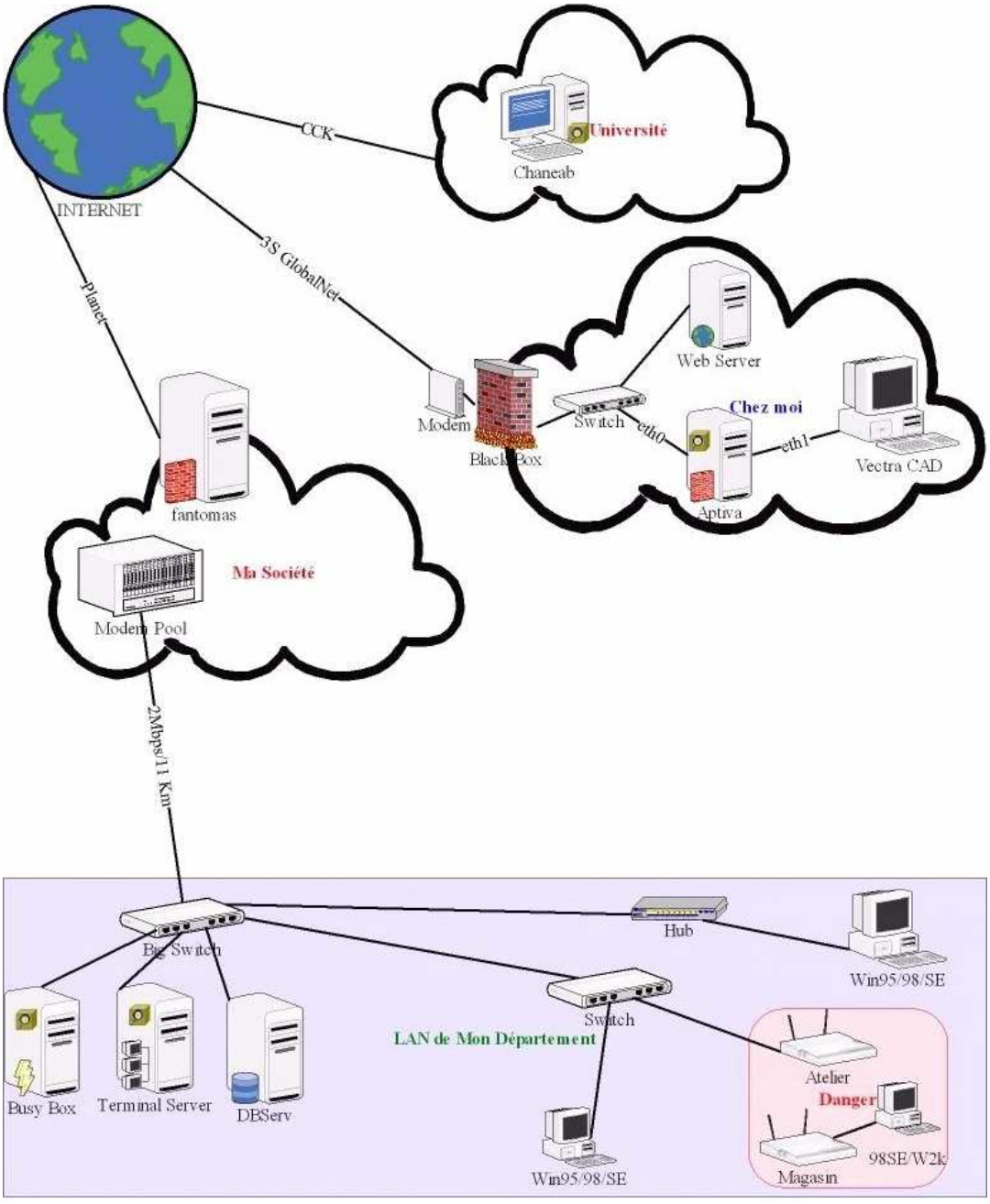

Figure Sc.1

Topologie du réseau de test utilisé pour le projet Snort

Indique la présence d'une sonde (installation snort) sur la machine.

3-2 Installation de SNORT et de ses pré-requis

Remarques :

Nous avons choisit de décrire l'installation et la configuration de snort en mode ligne de commandes pour deux raisons :

i) Pour sécuriser un système il faut le faire dès le début et l'installation d'une interface graphique sur un système qui servira uniquement de détecteur d'intrusions ne peut que le rendre plus vulnérable aux attaques, en lui ajoutant les failles des paquetages graphiques X.

ii) Il y a plusieurs distributions Linux sur le marché, chacune avec une interface graphique personnalisée et surtout des outils d'administration et de manipulation des paquetages différents et qui ne cessent d'être améliorés, donc modifiés, au cours des différentes versions. La ligne de commande est toujours la même et invariable.

La plate-forme de travail est une machine Intel PIII 667Mhz sous ***Linux Mandrake 10.1*** quotidiennement mise à jour.

3-2-1 Installation des pré-requis

Etapes à suivre :

1) Lisez entièrement ce document avant de commencer les manipulations.

2) Obtenez et installer ***Mandrake 10.1*** depuis le site miroir le plus proche.

3) Mettez à jour votre installation Linux en utilisant par exemple le miroir ftp.belnet.be à l'aide des commandes :

```
[root@uinf root]# urpmi.addmedia  update_source
http://ftp.belnet.be/linux/Mandrake/official/updates/10.1/main_updates  with
media_info/synthesis.hdlist.cz
[root@uinf root]# urpmi  --auto-select  --auto
```

Remarque : Si vous êtes derrière un Firewall et que vous ne pouvez accéder à Internet qu'au travers d'un Proxy avec authentification; éditez, en le créant au besoin, le fichier **/etc/urpmi/proxy.cfg** en y ajoutant les informations nécessaires à ***urpmi*** pour se connecter à Internet et récupérer des paquetages, comme indiqué ci-après:

```
[root@uinf root]# echo  'http_proxy=a.b.c.d:xyzt
proxy_user=mon_login_proxy:mon_proxy_pass'  >  /etc/urpmi/proxy.cfg
```

4) L'installation ***Mandrake*** à partir des cdroms téléchargés gratuitement sur le net ne contient pas tous les paquetages nécessaires pour reproduire ce TP.

Nous avons besoin d'autres paquetages, disponibles dans les versions payantes de ***Mandrake***, mais que l'on peut également obtenir et installer automatiquement à partir de l'arborescence ***contrib*** des sites de téléchargement, une fois qu'on les a ajoutés à la liste des média d'installation à l'aide de la commande suivante :

```
[root@uinf root]# urpmi.addmedia  BelNet\ Contrib
http://ftp.belnet.be/linux/Mandrake/official/10.1/i586/media/contrib with
media_info/hdlist.cz

[root@uinf root]# urpmi.addmedia  BelNet\ Cooker\ Contrib
http://ftp.belnet.be/linux/Mandrake/devel/cooker/i586/media/contrib with
media_info/hdlist.cz
```

Remarque :
Avant de commencer à installer des paquetages depuis ces deux nouveaux emplacements, nous devons indiquer à ***rpm*** que nous faisons confiance à leur origine. Pour ce faire, nous devons ajouter la clé publique ***gpg*** avec laquelle l'équipe de développement de ***Mandrake*** signe ses paquetage, pour authentifier leurs origine, à la liste des clés auxquelles ***rpm*** fait confiance. Ceci se fait à l'aide des commandes suivantes :

```
[root@uinf root]# wget  -nd
http://ftp.belnet.be/linux/Mandrake/official/10.1/i586/media/contrib/media_info/p
ubkey

[root@uinf root]# rpm  –import  pubkey
```

Ceci nous évitera de devoir confirmer manuellement à chaque fois l'installation des paquetages provenant de ces sources, car leurs signature est différente de celle des paquetages des cdroms d'installation.

5) Installez le serveur web ***Apache***, la base de données ***MySQL***, l'interpréteur ***PHP***, le connecteur de php aux bases de données mysql, la librairie graphique de haut niveau ***JpGraph***, la couche d'abstraction aux bases de données ***ADOdb***, l'interface ***ACID***, les librairies de développement ***zlib-devel***, ***libpcap-devel*** et ***pcre-devel*** à l'aide de la commande suivante :

```
[root@uinf root]# urpmi  --auto  apache  MySQL  mysql-devel  php-mysql  JpGraph
ADOdb acid  zlib-devel  libpcap-devel  pcre-devel
```

3-2-2 Installation de SNORT

Maintenant nous allons télécharger, personnaliser, compiler, installer et configurer snort pour l'utilisation d'une base de données ***mysql*** comme emplacement de stockage des logs et des alertes et la consultation des ces derniers via l'interface web d'***acid***.

6) Placez-vous dans un répertoire de votre choix et tapez les commandes suivantes dans l'ordre :

```
[root@uinf tmp]# wget -nd http://www.snort.org/dl/current/snort-2.3.2.tar.gz
[root@uinf tmp]# tar -zxvf snort-2.3.2.tar.gz
[root@uinf tmp]# cd snort-2.3.2
[root@uinf snort-2.3.2]# ./configure --with-mysql=/usr && make && make install
[root@uinf snort-2.3.2]# mv /usr/local/man/man8/snort.8 /usr/share/man/man8/
[root@uinf snort-2.3.2]# mv /usr/local/bin/snort /usr/sbin/
[root@uinf snort-2.3.2]# mkdir /etc/snort
[root@uinf snort-2.3.2]# cp -pauvfr etc/* /etc/snort/
[root@uinf snort-2.3.2]# mv rules/ /etc/snort/
[root@uinf snort-2.3.2]# mv rpm/snort.sysconfig /etc/sysconfig/snort
[root@uinf snort-2.3.2]# mv rpm/snortd /etc/rc.d/init.d/
[root@uinf snort-2.3.2]# chmod +x /etc/rc.d/init.d/snortd
[root@uinf snort-2.3.2]# chkconfig --add snortd
[root@uinf snort-2.3.2]# chkconfig --level 235 snortd on
```

3-3 Configurations

3-3-1 Configuration de mysql

7) Nous avons décidé d'utiliser une base ***mysql*** pour le stockage des logs et des alertes. Cette configuration est fortement recommandée dans le cas où vous auriez plusieurs sondes snort installées sur votre (vos) réseau(x) local (locaux) car elle permet d'avoir une vue d'ensemble de toutes les activités suspectes en centralisant toutes les alertes en un seul endroit.
   Nous commençons donc par créer la base de données ***mysql*** qui accueillera les logs et alertes de snort à l'aide de la commande suivante :

```
[root@uinf snort-2.3.2]# mysqladmin create snort
```

8) Ensuite, nous créons les tables de cette base à l'aide d'un script sql fournit avec le package snort comme suit :

```
[root@uinf snort-2.3.2]# mysql snort < 'schemas/create_mysql'
```

9) Enfin, nous créons l'utilisateur mysql qui alimentera la base de snort en logs et en alertes, à l'aide des commandes suivantes :

```
[root@uinf snort-2.3.2]# mysql
mysql> GRANT INSERT, DELETE, UPDATE ON snort.* TO 'snort'@'localhost' IDENTIFIED BY 'snort';
mysql> GRANT INSERT, DELETE, UPDATE ON snort.* TO 'snort'@'%' IDENTIFIED BY 'snort';
mysql> FLUSH PRIVILEGES;
mysql> \q
```

Nous vous recommandons de ne pas utiliser le couple (nom d'utilisateur/mot de passe) snort/snort que nous avons utilisé ici mais d'en choisir un autre plus difficile à deviner.

A moins d'utiliser une configuration avec serveur de base de données mysql et serveur web indépendants et dédiés, vous devez créer l'utilisateur snort deux fois pour qu'il puisse se connecter depuis localhost et depuis n'importe quelle autre adresse ip. Mais il serait toutefois plus prudent de créer un sous-domaine dédié et de n'autoriser les connections à la base mysql avec l'identifiant snort que depuis ce sous-domaine. Dans ce cas, remplacez 'snort'@'%' par 'snort'@'ids.mondomaine' dans la dernière ligne ci-dessus.

Une autre recommandation est d'utiliser des vlans ou des vpns afin de séparer le trafic entre sondes snort et base mysql du reste du trafic réseau et s'assurer que personne ne puisse se connecter à ce vlan/vpn afin de garantir l'intégrité des données transmises par les sondes à la base de données. Dans le cas contraire, il est toujours possible pour un intrus de manipuler et fausser les alertes afin de masquer sa présence ou son activité belligérante sur votre réseau.

3-3-2 Configuration de Snort

10) Editez votre fichier de configuration /etc/snort/snort.conf et changez la ligne "var HOME_NET any" par celle correspondant à votre réseau p.ex. "var HOME_NET [10.2.0.0/16,10.0.0.0/24]".

1. Recherchez les lignes commençant par "# output database:" et ajoutez-y une ligne comme celle-ci en remplaçant user et password par ceux de votre installation

   "output database : alert,mysql, dbname=snort user=snort password=snort host=10.2.9.44 sensor_name=fwgw".

   Si vous travaillez dans un environnement très ouvert, tel qu'une université ou chez un

fournisseur d'accès où vous n'avez pas beaucoup de contrôle sur ce que peuvent faire les utilisateurs de votre réseau, nous vous recommandons d'installer également les règles développées par BleedingEdge en plus des règles officielles distribuées avec snort et de les activer dans votre fichier de configuration de snort. Il s'agit de règles en cours de développement et qui doivent encore faire l'objet d'un processus de validation avant d'être intégrées officiellement à snort (ou rejetées) et qui peuvent donc donner lieu à quelques fausses alertes. Ces règles sont développées par une communauté très active d'utilisateurs de snort pour répondre le plus rapidement possible aux dernières menaces sur internet.

11) Editer votre fichier /etc/rc.d/init.d/snortd pour y supprimer toute référence au répertoire de log (-l $LOGDIR/$i), car nous voulons enregistrer les alertes dans une base mysql.

12) Démarrer snort à l'aide de la commande :

```
[root@uinf Chantier Snort]# service snortd start
Starting snort:                                    [  OK  ]
```

13) Vérifiez que snort est bien en cours d'exécution et qu'il n'est pas en train d'enregistrer ses messages dans le système de fichier (présence de l'argument -l dans la sortie de la commande ps) :

```
[root@uinf Chantier Snort]# ps ax | grep snort
18962 ?        Ds     0:02 /usr/sbin/snort -A fast -b -d -D -i eth0 -u snort -g snort -c
/etc/snort/snort.conf
```

3-4 Fonctionnalités

SNORT a été testé sous ses trois modes de fonctionnement :

- le mode sniffer ;
- Le mode « packet logger » ;
- le mode détecteur d'intrusion réseau (NIDS) : dans ce mode, SNORT analyse le trafic du réseau, compare ce trafic à des règles déjà définies par l'utilisateur et établi des actions à exécuter.

3-4-1 Mode Sniffer

C'est le mode basic, il permet de lire et afficher à l'écran les paquets TCP/IP circulant sur le réseau :

```
[root@uinf Chantier Snort]# snort –v
```

Cette commande permet d'exécuter et d'afficher les entêtes des paquets TCP/IP.

```
[root@uinf Chantier Snort]# snort –vd
```

Cette commande permet d'exécuter SNORT et d'afficher tout le paquet TCP/IP (entête et données).

```
[root@uinf Chantier Snort]# snort –vde
```

Cette commande permet d'exécuter SNORT et d'afficher tout le paquet TCP/IP (entête et données) ainsi que de l'entête de la couche liaison de données.

3-4-2 Mode « packet-logger »

Dans ce mode SNORT journalise le trafic réseau dans des répertoires sur le disque :

```
[root@uinf Chantier Snort]# snort –dev –l ./log
```

Cette commande permet d'exécuter SNORT et de loguer dans le répertoire log, tous les paquets TCP/IP (entête et données) ainsi que de l'entête de la couche liaison de données. Il faut créer au préalable le répertoire log.

```
[root@uinf Chantier Snort]# snort –v –l ./log –h 192.168.1.0/24
```

Cette commande permet d'exécuter SNORT et de loguer dans le répertoire log, toutes les entêtes des paquets TCP/IP relatifs au sous-réseau 192.168.1.0/24. Toutes les entêtes des paquets vont être loguées dans des sous-répertoires du répertoire log.

3-4-3 Mode de détecteur d'intrusion réseau

Dans ce mode, SNORT analyse le trafic du réseau, compare ce trafic à des règles déjà définies par l'utilisateur et établi des actions à exécuter.
Il faut tout d'abord installer tous les pré-requis (voir plus haut le paragraphe installation) puis configurer le fichier ***snort.conf*** (voir le paragraphe configuration).

Exploitation des alertes à l'aide de l'interface web ACID :

L'interface ACID ayant été installée par urpmi, nous devons éditer le fichier de configuration /var/www/html/admin/acid/acid_conf.php pour y renseigner les valeurs de $alert_dbname, $alert_host, $alert_user et $alert_password correspondantes aux valeurs de notre installation.

ACID a besoin d'autres tables que celles de snort pour y stocker des informations propres à son bon fonctionnement. Nous devons créer ces tables dans la base de données de snort à l'aide de la commande suivante :

```
[root@uinf tmp]# mysql  snort  <  '/usr/share/doc/acid-
0.9.6b23/create_acid_tbls_mysql.sql'
```

Maintenant, nous devons sécuriser l'accès à la l'interface web d'ACID afin que seul l'administrateur puisse y accéder. Pour celà, nous éditons le fichier de configuration du serveur web, dans notre cas apache, /etc/httpd/conf/httpd.conf pour y ajouter les lignes suivantes :

```
<Location /admin/acid>
AuthType Basic
AuthName "Restricted Admin Area"
AuthUserFile /etc/httpd/conf/passwd
   <Limit GET POST OPTIONS PROPFIND>
      require user snortadmin
      Order deny,allow
      Deny from all
      Allow from adminconsole.ids.mondomaine
   </Limit>
</Location>
```

Si notre serveur web n'est pas déjà sécurisé par un accès par mots de passe, nous ajoutons le fichier des mots de passe et l'utilisateur snortadmin à l'aide de la commande suivante :

```
[root@uinf admin]# htpasswd  -c  /etc/httpd/conf/passwd  snortadmin
New password:
Re-type new password:
Adding password for user snortadmin
```

Ensuite, nous (re)démarrons le serveur web et nous nous rendons à l'adresse https://monserveurweb/admin/acid/ pour y découvrir la console de visualisation des alertes d'ACID.

```
[root@uinf conf]# service httpd restart
```

Comme le montre la figure ci-après, lors d'une installation à partir de zéro, la base de données de snort peut ne contenir aucune alerte.

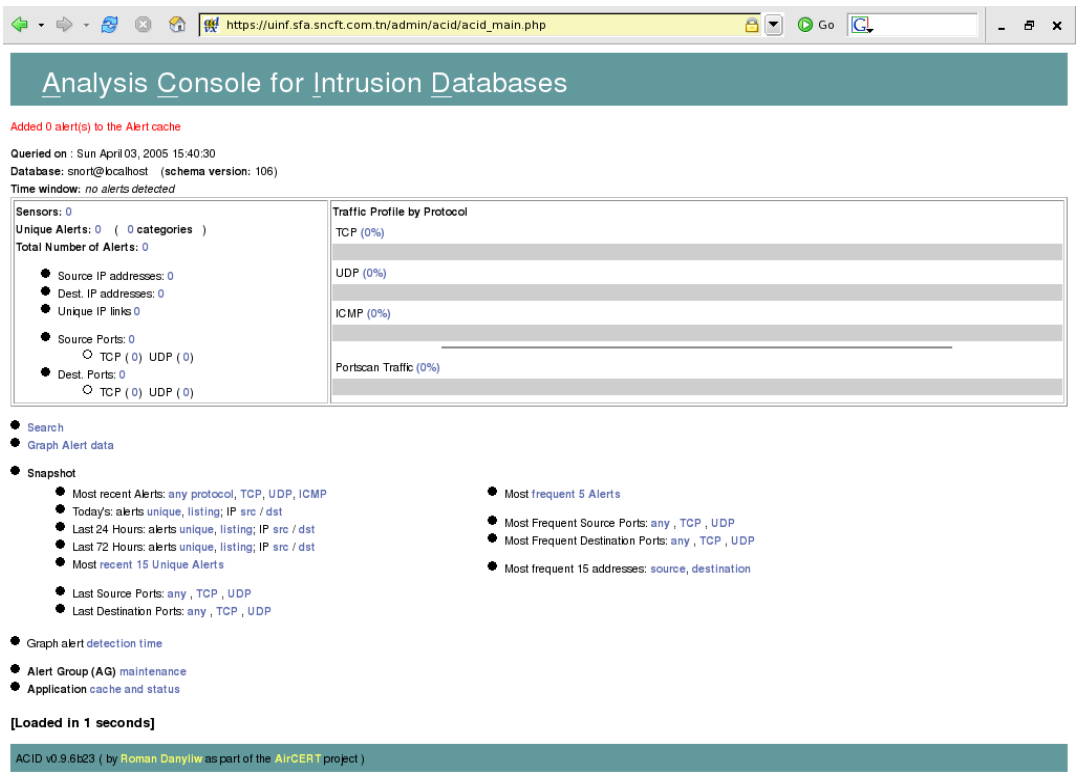

Figure Sc.2

La figure [Sc.2] montre l'écran de bienvenue d'ACID avant que snort ne commence à consigner des alertes dans la base de données mysql. Connectons-nous alors à Internet et attendons.

Dans le cadre de ce travail, la sonde snort nous a permis de déceler une activité anormale entre la machine désignée par VectraCAD sur la figure [Sc.1] et l'hôte 72.9.239.226 port

5005 tel qu'illustré sur la figure [Sc.3] ci-après.

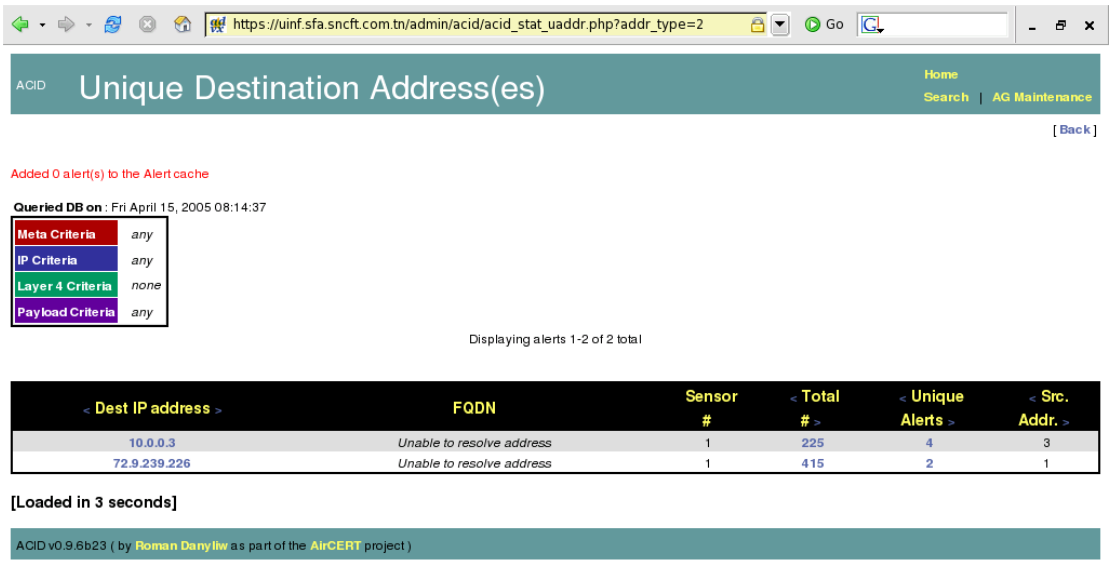

Figure Sc.3

Un telnet sur l'hôte suspect à l'adresse fournie par snort (voir figure [Sc.4]) nous confirme qu'il s'agit bien d'une machine servant à récolter des informations depuis des postes compromis.

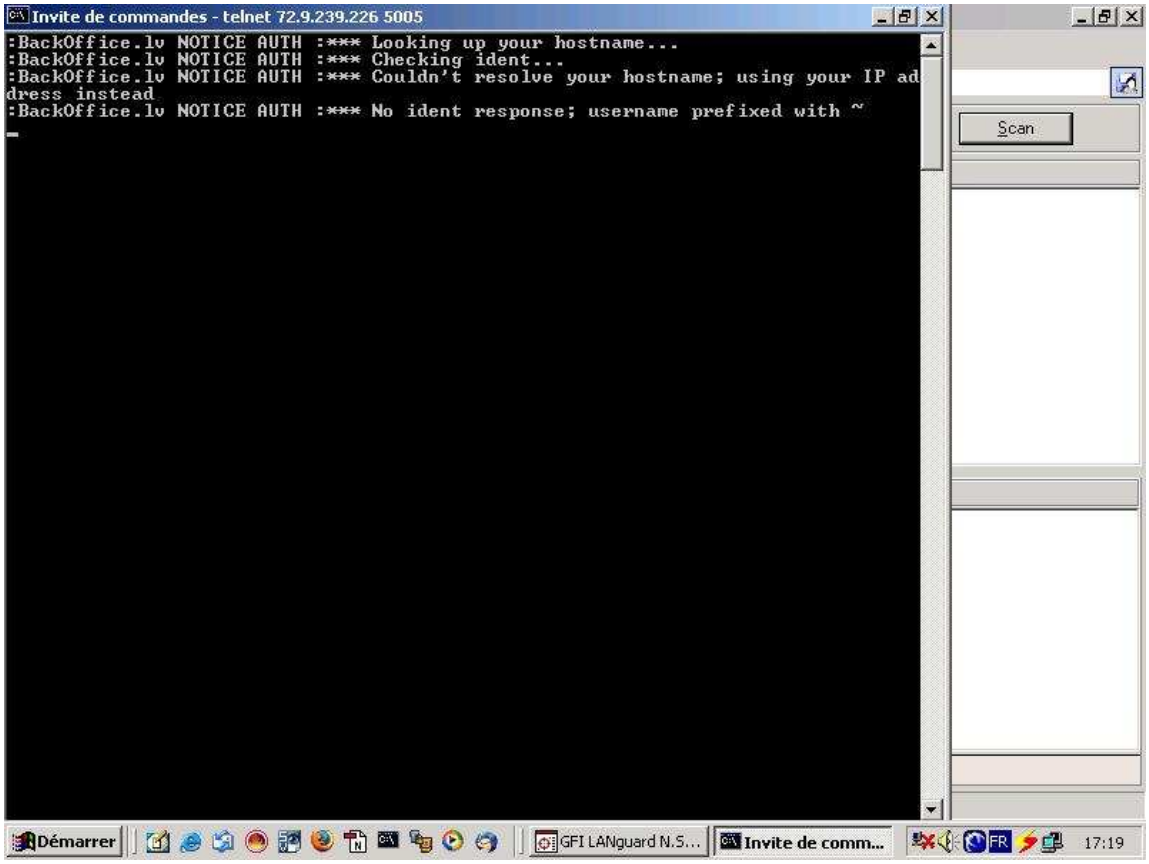

Figure Sc.4

4- Conclusion et perspectives

Ce travail nous a permis de découvrir un outil libre de détection d'intrusion très puissant.

De nombreux problèmes ont été rencontrés et surmontés pour l'élaboration de ce travail. Principalement, des difficultés rencontrées lors de l'installation des rpm et le nombre important des pacquages complémentaires à SNORT qu'il faut installer et bien configurer.

Comme perspectives à ce travail, nous préconisons l'intégration de iptables et de transformer SNORT d'un IDS vers un IPS (Système de PREVENTION d'Intrusions).

Liens Utiles et Bibliographie :

Site web de Mandrake : www.mandrakelinux.com
Site web de Snort : www.snort.org

Site web de ACID : acidlab.sourceforge.net
Site web de JpGraph : www.aditus.nu/jpgraph
Site web de AdoDB : adodb.sourceforge.net
Site web de Bleedind Edge Snort : www.bleedingsnort.com
Site web des dernières versions, revues et corrigées, de ce document et du script contenant toutes les commandes d'installation et de configuration citées dans ce document : www.fathi.info

Moez ESSEGHIR : Réalisation d'un serveur de détection d'intrusion SNORT personnalisé, Mémoire de fin d'Etudes, ENSI 2002.

S. NORTHCUTT, J. NOVAK, D. MCLACHAN: Détection des intrusions réseaux, Editions CampusPress.