

SYSTÈME DE DÉTECTION D'INTRUSION.

<http://nassih.com>

© MOHAMED NASSIH.

1. Introduction.

La croissance de l'Internet et l'ouverture des systèmes ont fait que les attaques dans les réseaux informatiques soient de plus en plus nombreuses. D'une part les vulnérabilités en matière de sécurité s'intensifient, au niveau de la conception des protocoles de communication ainsi que au niveau de leur implantation et d'autre part les connaissances, les outils et les scripts pour lancer les attaques sont facilement disponibles et exploitables. D'où la nécessité d'un système de détection d'intrusions (SDI).

Cette technologie consiste à rechercher une suite de mots et/ou de paramètres caractérisant une attaque dans un flux de paquets. Les systèmes de détection d'intrusion ont devenus un composant essentiel et critique dans une architecture de sécurité informatique.

Un SDI doit être conçu dans une politique globale de sécurité. L'objectif d'un **SDI** est de détecter toute violation liée à la politique de sécurité, il permet ainsi de signaler les attaques.

Nous commençons par une brève explication de quelques notions et définitions de base, puis Nous décrivons la mise en place et la configuration de SNORT, un système de détection d'intrusion gratuit sous Linux.

2. Définitions et concepts.

2.1. Les systèmes de détection d'intrusion.

On parle d'intrusion lorsqu'une tierce partie essaie d'avoir de l'information et/ou accéder à un système ou plusieurs systèmes connectés en réseau. Le rôle d'un système de détection d'intrusion est de détecter et avertir l'administrateur système de l'existence d'une telle intrusion.

Un système de détection d'intrusion (SDI) est basé sur un renifleur (sniffer) avec un moteur qui analyse le trafic capturé selon des règles qui décrivent les caractéristiques d'un trafic à

signaler. Un SDI est capable d'analyser le trafic à tous les niveaux, liaison de données, réseau, transport et application.

2.2. Les signatures.

La signature est en général une chaîne de caractère, que vous recherchez à l'intérieur d'un paquet de données. Par exemple la présence de “/scripts/iisadmin/default.htm” dans un paquet à destination d'un serveur Web IIS (Internet Information Services), pourra indiquer une intrusion. (tentative d'accès à la page d'administration de IIS).

Dans le cas du système SNORT, la reconnaissance des attaques est basée sur le concept d'analyse de chaînes de caractères présente dans le paquet. Pour que le système puisse être capable de détecter une attaque, cette dernière doit être décrite par une signature. C'est avec cette signature qu'on pourra être capable d'écrire la règle que le SDI va utiliser pour la détection. La figure 2.1 représente la règle qui va permettre de signaler les paquets qui contient (dans URL) la chaîne “/scripts/iisadmin/default.htm”.

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS /scripts/iisadmin/default.htm access"; flow:to_server,established; uricontent:"/scripts/iisadmin/default.htm"; nocase; classtype:web-application-attack; sid:994; rev:6;)
```

Figure 2.1 : exemple de règle SNORT

La performance d'un SDI dépend du nombre, de l'efficacité et de précision des signatures prédéfinies. Cette base de données des signatures doit être toujours à jour pour que le SDI puisse être capable de détecter les nouvelles attaques.

2.3. Les systèmes de détection d'intrusion d'hôte et de réseau.

On pourra distinguer deux catégories des systèmes de détection d'intrusion. La première catégorie a pour objectif la surveillance de l'activité d'une machine en examinant les différents fichiers système de journalisation. Ce type de système de détection est appelé « host-based IDS (HIDS) » et il est installé sur la machine comme un agent. La seconde catégorie de système de

détection d'intrusion est liée à surveillance de l'activité de réseau en capturant et en analysant les paquets, on les appelle « network-based IDS (NIDS) ». Un NIDS (Network Intrusion Detection System) est un SDI réseau basé sur une base de données des signatures qui décrivent les différentes attaques. En sniffant le trafic, ce dernier va examiner chaque paquet pour savoir s'il vérifie une des signatures. Dans le cas de correspondance Une alerte est générée.

3. Le système de détection d'intrusion SNORT.

SNORT est un Système de Détection d'Intrusion de réseau (NIDS) en Open Source, capable d'analyser en temps réel le trafic sur les réseaux IP. SNORT utilise l'analyse des protocoles et la recherche des chaînes de caractères dans les paquets pour la détection des attaques. On l'utilise pour détecter une variété d'attaques tels que des scans de ports, des attaques CGI, des débordements de tampons, et bien plus.

3.1. L'architecture de SNORT.

L'architecture de SNORT est organisée en modules, elle est composée de quatre grands modules : Le décodeur de paquets, les préprocesseurs, le moteur de détection et le système d'alerte et d'enregistrement de log.

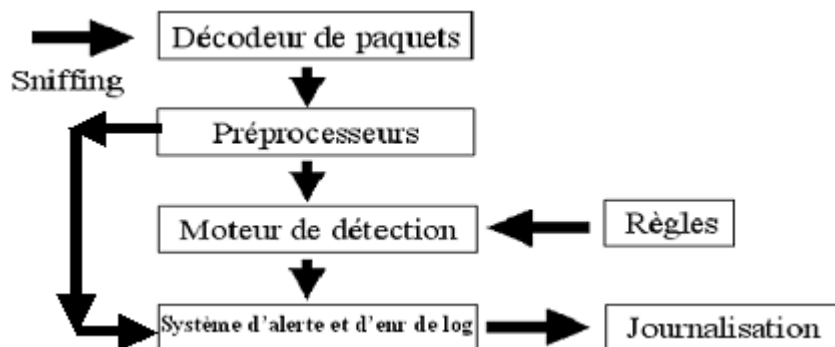


Figure 3.1 : Architecture de SNORT.

3.2. Le décodeur de paquets .

Un système de détection d'intrusion active un ou plusieurs interfaces réseau de la machine en mode espion (promiscuous mode), ceci va lui permet de lire et analyser tous les paquets qui passent par le lien de communication. SNORT utilise la bibliothèque libpcap pour faire la capture des trames.

Un décodeur de paquets est composé de plusieurs sous décodeurs qui sont organisés par protocole (Ethernet, IP, TCP..), ces décodeurs transforme les éléments des protocoles en une structure de données interne. (Voir figure 3.2).

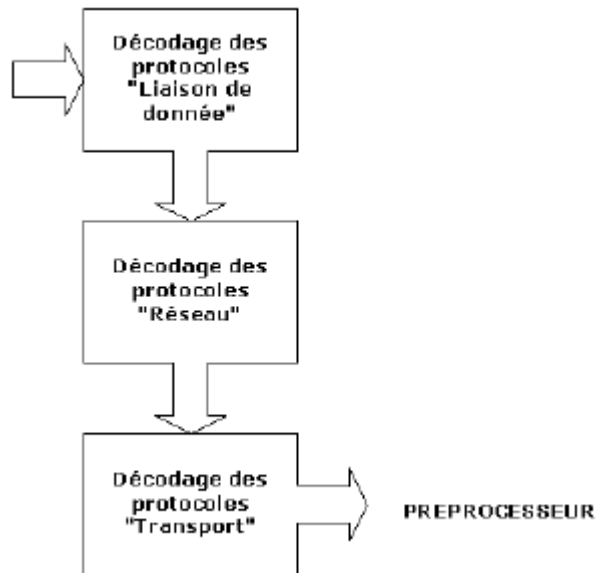


Figure 3.2 : Le décodeur de paquets.

3.3. Les préprocesseurs.

Les préprocesseurs s'occupent de la détection d'intrusion en cherchant les anomalies, un préprocesseur envoie une alerte si les paquets ne respectent pas les normes des protocoles utilisées. Un préprocesseur est différent d'une règle de détection, il est un programme qui vise à aller plus en détail dans l'analyse de trafic. Nous allons voir à travers un exemple comment les préprocesseurs fonctionnent.

3.4. Moteur de détection.

C'est la partie la plus importante dans un SDI. Le moteur de détection utilise les règles pour faire la détection des activités d'intrusion. Si un paquet correspond à une règle une alerte est générée. Les règles sont groupées en plusieurs catégories sous forme de fichiers. SNORT vient avec un ensemble de règles prédéfini, voir figure 3.3.

```
[root@localhost rules]# ls
attack-responses.rules  icmp.rules          other-ids.rules     telnet.rules
backdoor.rules          imap.rules          p2p.rules           tftp.rules
bad-traffic.rules      info.rules          policy.rules        virus.rules
chat.rules              local.rules         pop2.rules          web-attacks.rules
ddos.rules              Makefile            pop3.rules          web-cgi.rules
deleted.rules           Makefile.am         porn.rules           web-client.rules
dns.rules               Makefile.in         rpc.rules            web-coldfusion.rules
dos.rules               misc.rules          rservices.rules     web-frontpage.rules
experimental.rules      multimedia.rules    scan.rules           web-iis.rules
exploit.rules           mysql.rules          shellcode.rules     web-misc.rules
finger.rules            netbios.rules       smtp.rules           web-php.rules
ftp.rules               nntp.rules          snmp.rules          x11.rules
icmp-info.rules         oracle.rules        sql.rules
[root@localhost rules]# _
```

Figure 3.3 : les fichiers des règles prédéfinies dans SNORT.

Ces règles ne sont pas activées automatiquement, il faut les activer dans le fichier de configuration snort.conf. Chaque fichier contient des règles décrit un type de trafic à signaler. (Voir figure 3.4).

```
include $RULE_PATH/local.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/telnet.rules
include $RULE_PATH/rpc.rules
include $RULE_PATH/rservices.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/tftp.rules
```

Figure 3.4 : Une partie du fichier snort.conf.

3.5. Système d'alerte et d'enregistrement des logs.

Le système d'alerte et d'enregistrement des logs s'occupe de la génération des logs et des alertes. Les alertes sont stockées par défaut dans le répertoire `/var/log/snort/`.

Dés que le système devient opérationnel, on pourra consulter les alertes générées directement dans les fichiers textes ou bien utilisé une console de gestion. ACID (Analysis Console for Intrusion Detection), est une application qui fournit une console de gestion et qui permet la visualisation des alertes en mode graphique. Les alertes dans ce cas sont stockées dans une base de données mysql.

3.6. SNORT en interne.

SNORT est une application écrite en C. Les programmes sources sont dans le répertoire `snort-2.1.0/src/`. Le programme `snort.c` représente la routine principale de SNORT, le décodeur des paquets est implémenté dans le programme `decode.c`. `rules.c` est la routine qui s'occupe des règles. Le moteur de détection est implémenté dans le programme `detect.c` et le moteur d'enregistrement est dans `log.c`.

Il est très utile de consulter le contenu de ces programmes et voir comment SNORT capture les paquets et détecte les attaques.

4. Un système de détection d'intrusion dans le réseau.

L'emplacement d'un SDI dépend de types d'activités d'intrusion qu'on veut détecter. Si l'entreprise a une seule connexion WAN alors le meilleur emplacement peut être juste derrière le routeur. Dans le cas où l'entreprise a plusieurs connexions, on peut placer un SDI sur chaque liaison.

La figure 4.1 montre un exemple de réseau avec un SDI. Dans ce cas il est connecté à un concentrateur entre le réseau local et le pare-feu. Le trafic est donc visible dans les deux directions.

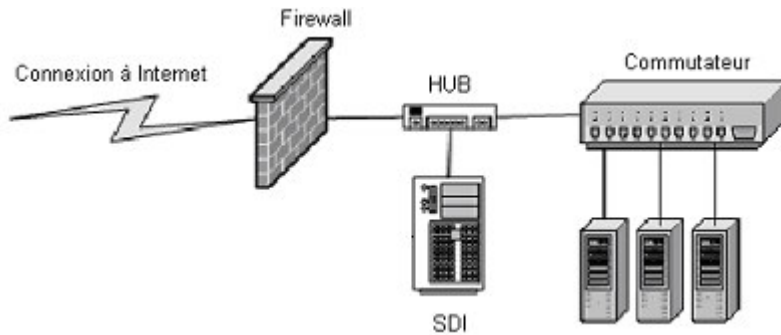


Figure 4.1 : l'emplacement d'un SDI.

Dans le cas d'un réseau avec une zone démilitarisée, un SDI peut être placé dans cette zone, de cette façon on pourra détecter les attaques qui visent les serveurs de l'entreprise. Les attaques peuvent être lancées de l'intérieur de l'entreprise, il est donc préférable d'avoir un SDI qui contrôle le trafic interne et signale les anomalies.