TP sur la

Sécurité des systèmes d'information

Table des matières

1. L’IDS c’est quoi ?

Dans ce TP, nous allons découvrir les principes de base des systèmes de détection d'intrusion (IDS) et de l'outil open-source Snort. Les IDS sont des outils de sécurité réseau qui surveillent le trafic réseau pour détecter les activités suspectes et les tentatives d'intrusion. Snort est un logiciel IDS open-source populaire qui utilise des règles pour détecter les attaques et générer des alertes en temps réel. Nous allons apprendre à configurer Snort pour surveiller le trafic réseau et à analyser les alertes générées pour identifier les tentatives d'intrusion.

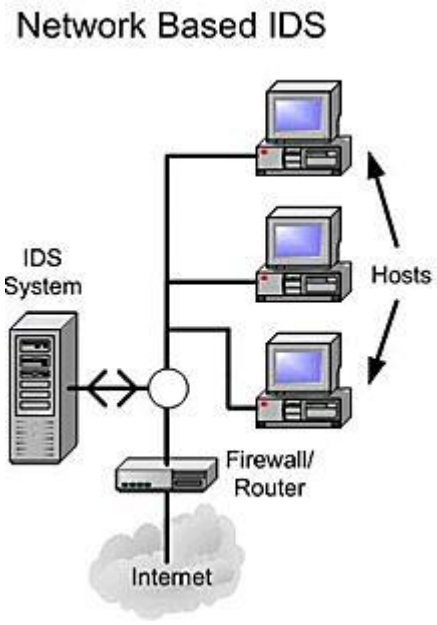
Ce TP permettra de comprendre comment les IDS peuvent contribuer à renforcer la sécurité de votre réseau.

Voici un tutoriel étape par étape pour installer et configurer Snort sur Kali Linux :

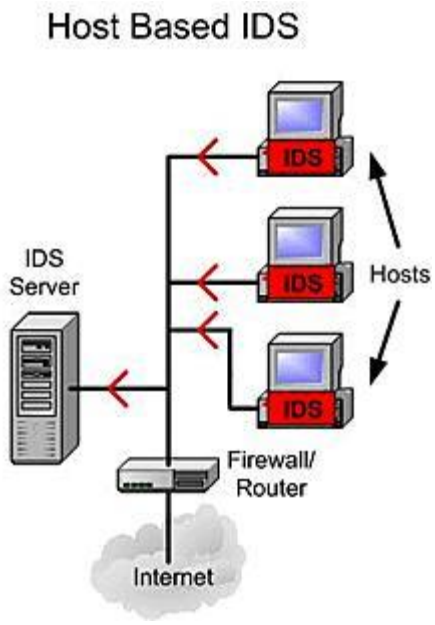
Les IDS sont des outils permettant de détecter les attaques/intrusions du réseau sur lequel il est placé. C'est un outil complémentaire aux firewall, scanneurs de failles et antivirus.

Il existe deux niveaux d'IDS : les IDS systèmes et les IDS réseaux.

- Les IDS systèmes (Host IDS) analysent le fonctionnement et l'état des machines sur lesquels ils sont installés afin de détecter les attaques en se basant sur des démons (tels que syslogd par exemple). L'intégrité des systèmes est alors vérifiée périodiquement et des alertes peuvent être levées. Par nature, ces IDS sont limités et ne peuvent détecter les attaques provenant des couches réseaux (tels que les attaques de type DOS).



- Les IDS réseaux (Network IDS), quant à eux, analysent en temps réel le trafic qu'ils aspirent à l'aide d'une sonde (carte réseau en mode "promiscuous").
- Rappel du mode promiscuous : c’est un mode de fonctionnement d'une carte réseau qui lui permet de recevoir tous les paquets de données qui circulent sur le réseau, y compris ceux qui ne sont pas destinés à son adresse MAC. En temps normal, une carte réseau ne reçoit que les paquets qui sont destinés à son adresse MAC ou aux adresses de broadcast.
- Ensuite, les paquets sont décortiqués puis analysés. En cas, de détection d'intrusion, des alertes peuvent être envoyées.



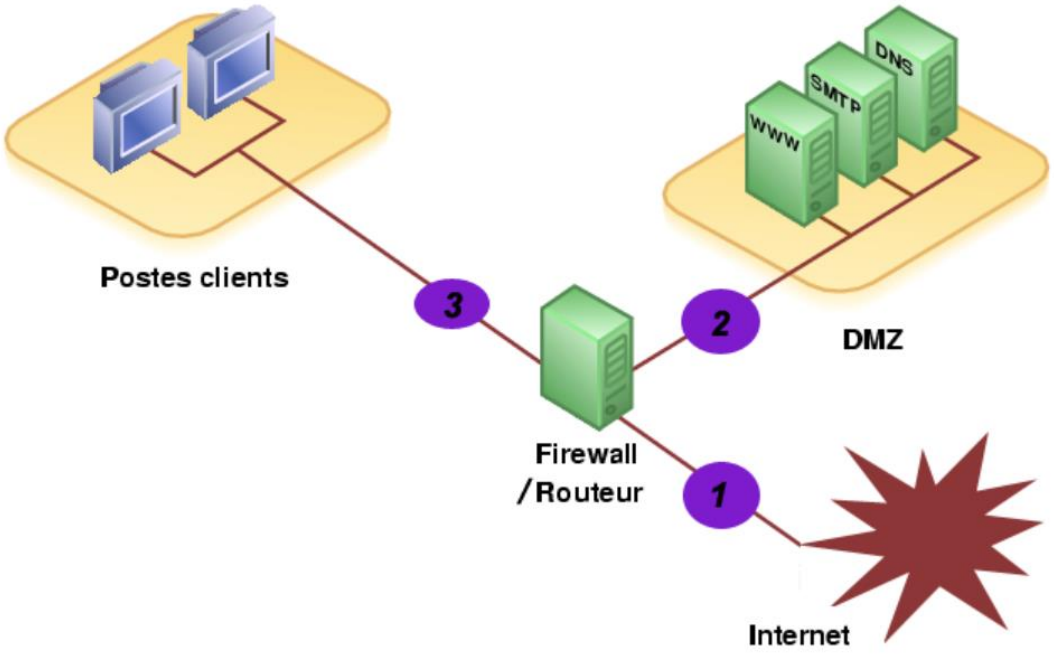
2. Où positionner son IDS ?

Il existe plusieurs endroits stratégiques où il convient de placer un IDS.

Le schéma suivant illustre un réseau local ainsi que les trois positions que peut y prendre un IDS :

- **Position (1):** Sur cette position, l'IDS va pouvoir détecter l'ensemble des attaques frontales, provenant de l'extérieur, en amont du firewall. Ainsi, beaucoup (trop?) d'alertes seront remontées ce qui rendra les logs difficilement consultables.
- **Position (2):** Si l'IDS est placé sur la DMZ, il détectera les attaques qui n'ont pas été filtrées par le firewall et qui relèvent d'un certain niveau de compétence. Les logs seront ici plus clairs à consulter puisque les attaques bénignes ne seront pas recensées.
- **Position (3):** L'IDS peut ici rendre compte des attaques internes, provenant du réseau local de l'entreprise. Il peut être judicieux d'en placer un à cet endroit étant donné le fait que 80% des attaques proviennent de l'intérieur. De plus, si des trojans ont contaminé le parc informatique (navigation peu méfiante sur internet) ils pourront êtres ici facilement identifiés pour être ensuite éradiqués.

Idéalement, on placerait des IDS sur les trois positions puis on délèguerait la consultation des logs à l'application "acid" (cf http://acidlab.sourceforge.net/) qui permet d'analyser les alertes et d'en présenter clairement les résulats via une interface web complète. Si une seule machine peut être déployée, autant la mettre sur la position 2, crutiale pour le bons fonctionnement des services.



3. Installation et configuration de Snort

Étape 1: Installer Snort

Ouvrez le terminal et exécutez la commande suivante pour installer Snort :

```
sudo apt-get install snort
```

Étape 2: Configuration de Snort

Pour configurer Snort, vous devez créer un fichier de configuration. Exécutez la commande suivante pour créer un fichier de configuration par défaut :

```
sudo cp /etc/snort/snort.conf /etc/snort/snort.conf.bak
```

Étape 3: Vérifier la configuration de l'interface réseau

Snort doit être configuré pour écouter le trafic sur l'interface réseau appropriée. Vous pouvez vérifier la configuration de votre interface réseau avec la commande suivante :

```
ifconfig
```

Assurez-vous de noter le nom de votre interface réseau.

Étape 4: Configurer Snort pour votre interface réseau

Ouvrez le fichier de configuration de Snort avec la commande suivante :

```
sudo nano /etc/snort/snort.conf
```

Recherchez la ligne suivante :

```
# Setup the network addresses you are protecting ipvar HOME_NET any
```

Remplacez "any" par l'adresse IP de votre réseau, par exemple :

```
ipvar HOME_NET 192.168.1.0/24
```

Recherchez la ligne suivante :

```
# Set up the external network addresses. Leave as "any" in most situations ipvar EXTERNAL_NET !$HOME_NET
```

Assurez-vous que la valeur est définie sur "!$HOME_NET".

Recherchez la ligne suivante :

```
# Set the network interface name # Setup network interface for sniffing # EXAMPLES: # eth0 for Ethernet # wlan0 for wireless # sn0 for Apple Airport # lo for local traffic # # network_interface eth0
```

Décommentez la ligne et remplacez "eth0" par le nom de votre interface réseau, par exemple :

```
network_interface eth0
```

4. phase de tests

Étape 5: Tester la configuration de Snort

Pour tester la configuration de Snort, vous pouvez suivre les étapes suivantes :

1. Ouvrir une console et lancer Snort en mode verbose :

   ```
   sudo snort -i eth0 -c /etc/snort/snort.conf -T
   ```

   Cela va vous permettre de voir les informations de configuration de Snort et les éventuels avertissements ou erreurs.

2. Envoyer du trafic réseau simulé pour voir si Snort détecte les règles que vous avez configurées. Vous pouvez le faire en utilisant un outil comme Scapy ou en utilisant un fichier PCAP contenant du trafic réseau.
   Par exemple, si vous avez configuré une règle pour détecter les paquets contenant le mot "attaque" dans la charge utile, vous pouvez envoyer un paquet avec ce mot à l'aide de Scapy :

   ```
   sudo scapy
   send(IP(dst="192.168.0.1")/TCP(dport=80)/"GET / HTTP/1.1\r\nHost: example.com\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36\r\nattaque")
   ```

Si Snort est configuré correctement, il devrait détecter le paquet et afficher un message d'alerte dans la console.

3. Vous pouvez également consulter les journaux de Snort pour vérifier si les alertes sont enregistrées correctement. Les journaux se trouvent généralement dans /var/log/snort/.

Si vous rencontrez des problèmes lors de la configuration ou du test de Snort, consultez la documentation de Snort