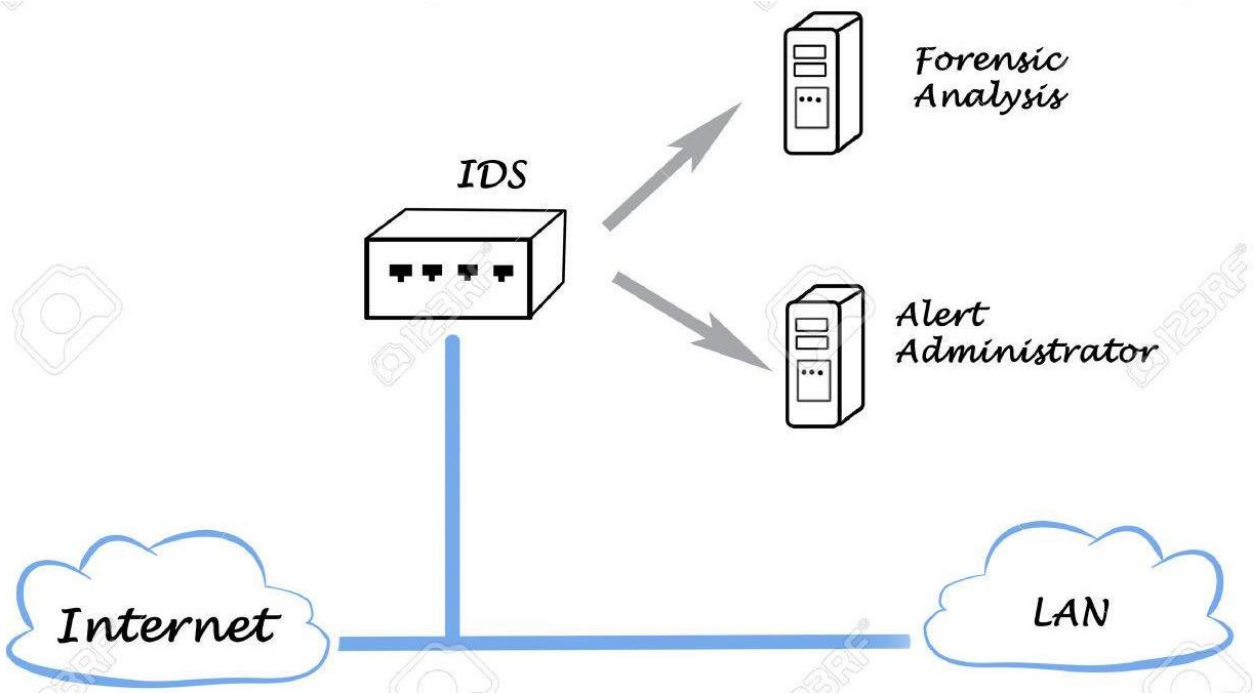
Méthodologie de la sécurité informatique

(La Détection d’Intrusion)

les systèmes de détection d'intrusion

est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible traitée (un réseau ou une machine) en utilisant une base de connaissance

Ce mécanisme consiste à révéler l'activité intrusive d'un attaquant vers/depuis un système informatique en basant à une observation de l'activité générée par les utilisateur



classification des IDS :

On distingue 3 classifications des IDS :

- ✓ Selon la méthode de détection
- ✓ Selon l’emplacement de l’IDS (la cible analysée)
- ✓ Selon le comportement de réaction

1 classification selon la méthode de détection :

A. Par scénario (détection des malveillants):

- Détection d'attaque a base de règles prédéfinies (scénarios)

Mise en œuvre:

- ✓ Systèmes experts
- ✓ Raisonnement sur modèle
- ✓ Réseaux de neurones
- ✓ Analyses d'état
- ✓ Datamining et classification

Inconvénients:

- ✓ Bases de signatures difficile à construire (peut-on couvrir tous les scénarios possibles
- ✓ Pas de détection des attaques inconnues

1 classification selon la méthode de détection :

B. Par comportement (détection d'anomalies):

- Détecter les changements dans le comportement d'utilisateurs

Mise en œuvre:

- ✓ Observation des seuils
- ✓ Profilage statique d'utilisateurs, de groupes, de programmes
- ✓ Profilage adaptatif des utilisateurs et à base de règles
- ✓ Approche immunologique

Inconvénients:

- ✓ Choix délicat des différents paramètres du modèle statistique.
- ✓ Hypothèse d'une distribution normale des différentes mesures non prouvée.
- ✓ Choix des mesures à retenir pour un système cible donné délicat.
- ✓ Difficulté à dire si les observations faites pour un utilisateur particulier correspondent à des activités que l'on voudrait prohiber.
- ✓ Pour un utilisateur au comportement erratique, toute activité est normale.
- ✓ Pas de prise en compte des tentatives de collusion entre utilisateurs.
- ✓ En cas de profonde modification de l'environnement du système cible, déclenchement d'un flot ininterrompu d'alarmes (ex : guerre du Golfe).
- ✓ Utilisateur pouvant changer lentement de comportement dans le but d'habituer le système à un comportement intrusif

2. classification selon le comportement de la réaction :

IDS Passif:

- ✓ Ne fait que signaler les messages sans affecter l'action suspecte

IDS Actif:

- ✓ Peut réagir tout seul contre une action suspecte sans même pas l'intervention de l'administrateur par fois

3. classification selon l'emplacement d'IDS :

IDS hôte (HIDS)

- ✓ Analyse et protège une hôte (ordinateur, serveur…etc.)

IDS réseau (NIDS)

- ✓ Analyse et protège un réseau local (s'installe entre le réseau local et l'internet)

IDS hybride

- ✓ Analyse et protège un réseau local vis-à-vis l'internet ainsi que les machines du réseau enter elles

les limites des IDS

Les attaquants ont développé des techniques afin de contourner l'IDS, ces techniques peuvent être classées en six (6) catégories :

L'insertion

Cette technique consiste à insérer des données aux flux suspects afin de perturber le fonctionnement de l'IDS

L'élimination

Pénétrer l'IDS et le rendre inutile en le saturant par les flux.

La fragmentation

La fragmentation des données peut cacher quelques attaques afin de ne les pas détecter

La substitution

Cette technique consiste à échanger le contenu de flux suspect avec son code hexadécimale

La distribution

C'est la répartition de l'attaque sur plusieurs ressources (attaque DDOS par exemple)

La confusion

C'est une technique permettant de rendre le contenu incompréhensible.

L’IDS en pratique (SNORT)

- open source.
- analyse de trafic et journalisation des paquets IP transitant le réseau local
- Utilise un ensemble de règles

Action	Protocole	Adresse	Port	Direction	Adresse	Port

- Contrôlé à partir de l’invite de commande par la commande « snort »

Détection d'Intrusion et systèmes intelligents

- ✓ Utilise les techniques d'intelligence artificielle pour la classification
- ✓ Considérée comme détection à base de scenario
- ✓ Plusieurs approches proposées:
  - En utilisant le machine learning
  - En utilisant le deep learning
  - Approche par re-ranking
- ✓ Plusieurs benchmark proposés:
  - ✓ **KDD'99 (KDD cup 1999):** environ 3.310.000 données structurées en 42 features contenant plusieurs données normales ou données des différentes attaques
  - ✓ D'autres concernant DDOS comme: **CICDDOS2019, CSE-CIC-IDS2018, NDSec-1 et CICIDS2017**