Les systèmes de détection d'intrusions

Ramzi Ouafi
Assistant Technologue
ESPRIT
e-mail : Ramzi.Elouafi@esprit.ens.tn

Plan du chapitre

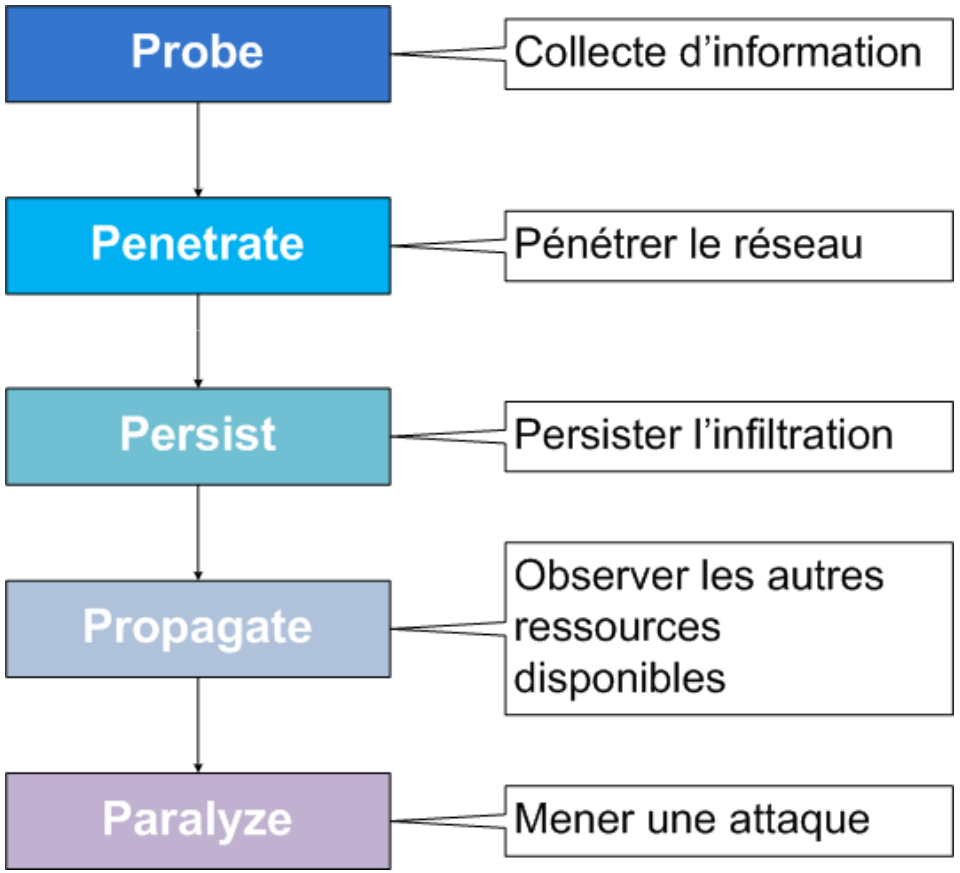
- Introduction.
- Les différents types d'attaques
- Les détection d'attaques:
  - Les méthodes de détection : types d'analyse
  - Les différents type d'IDS
- Déploiement d'un IDS
- Dérives des IDS:
  - IPS
  - Honeypots
- Conclusion

Introduction

- Outre la mise en place :
  - De pare-feux et des systèmes d'authentification,
  - Il est nécessaire d'avoir des outils de surveillance pour auditer le système d'information et « **détecter**» d'éventuelles « **intrusions ».**

- Anatomie d'une attaque: les 5P :
  - **Probe** : consiste en la collecte d'informations du système cible (**exemple**: nmap, Nessus).
  - **Penetrate** : utilisation des informations récoltées pour pénétrer un réseau (exemple : brute force, les attaques par dictionnaires)
  - **Persist** : création d'un compte avec des droits de super utilisateur pour pouvoir se ré-infiltrer ultérieurement. Une autre technique consiste à installer une application de contrôle à distance capable de résister à un reboot (ex : un cheval de Troie).
  - **Propagate :** elle consiste à observer ce qui est accessible et disponible sur le réseau local.
  - **Paralyze** : Le pirate peut utiliser le serveur pour mener une attaque sur une autre machine, détruire des données ou encore endommager le système d'exploitation dans le but de planter le serveur

Anatomie d’une attaque



Les attaques réseaux

- **Les techniques de scan**: Les scans de ports ne sont pas des attaques à proprement parler. Le but des scans est de déterminer quels sont les ports ouverts, et donc en déduire les services qui sont exécutés sur la machine cible (ex : port 80/TCP pour un service HTTP)

- **IP Spoofing**: usurper l'adresse IP d'une autre machine.

- **ARP Spoofing (ou ARP Redirect**): rediriger le trafic d'une machine vers une autre.

- **DNS Spoofing**: fournir de fausses réponses aux requêtes DNS

- **TCP Session Hijacking:** le but de cette attaque est de rediriger un flux TCP afin de pouvoir outrepasser une protection par mot de passe. Finalité : le contrôle l'authentification s'effectuant uniquement à l'ouverture de la session.

- **Déni de service**: SYN Flooding, UDP Flooding, Packet Fragment (ping of death).

Les attaques applicatives

- Se basent sur des failles dans les programmes utilisés, ou encore des erreurs de configuration
  - **Les problèmes de configuration**: Une mauvaise configuration d'un serveur peut entraîner l'accès à des fichiers importants, ou mettant en jeu l'intégrité du système d'exploitation.
  - **Les bugs** :Liés à des problèmes dans le code source,
  - **Les buffer overflows:** ou dépassement de la pile Issus d'une erreur de programmation.
  - **Les scripts**: Principalement web (ex : Perl, PHP, ASP), ils s'exécutent sur un serveur et renvoie un résultat au client.
  - **Les injections SQL**: le but est d'injecter du code SQL dans une requête de base de données. Ainsi, il est possible de récupérer des informations se trouvant dans la base (exemple : des mots de passe) ou encore de détruire des donnés

Détection d’intrusion : les IDS

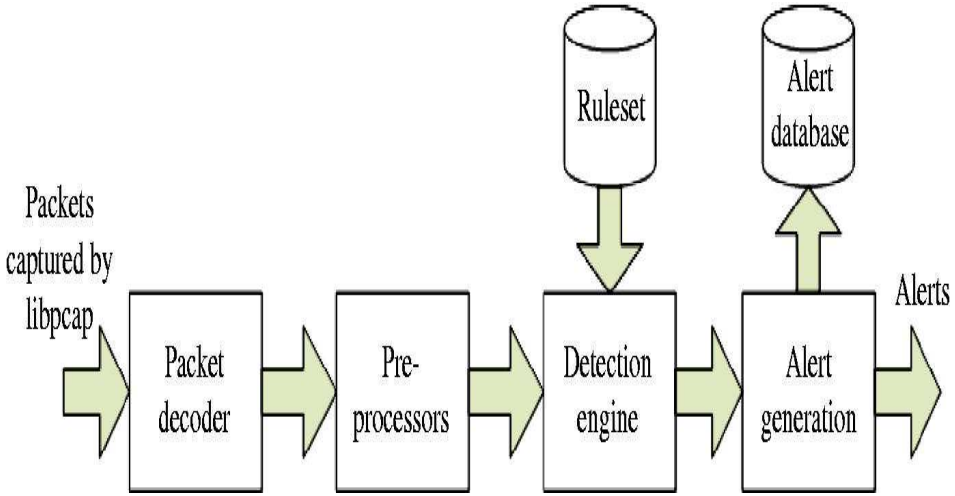
La notion d'intrusion

- Qu'entend-on ici par « intrusion »?.
  - **« utilisation d'un système informatique à des fins autres que celles prévues, généralement dues à l'acquisition des privilèges de façon illégitimes »** (*)
  - Tentative [**attaque**] ou réussite [**intrusion**] ayant pour objectif de compromettre (nuire) sur un système ou sur un réseau:
    - La confidentialité
    - L'intégrité
    - La disponibilité.
- « Détection d'intrusion » ?
  - La détection d'intrusions est l'activité qui correspond à:
    - **1)** La surveillance des évènements au niveau des systèmes, des applications et des réseaux.
    - **2)** L'analyse de ces évènements à la recherche de « signes » d'intrusions.
- **Les Systèmes de Détection d'Intrusion (Intrusion Detection Systems) sont des produits ou du matériel qui automatisent les processus de surveillance et d'analyse.**

(*) Philippe. Biondi « Architecture expérimentale pour la détection d'intrusions dans un système informatique»

IDS ?

- Un IDS est essentiellement un ***sniffer*** *couplé* avec un moteur qui analyse le trafic selon des règles
- Ces règles décrivent un trafic à signaler
- L'IDS peut analyser
  - Couche Réseau (IP, ICMP)
  - Couche Transport (TCP, UDP)
  - Couche Application
- Selon le type de trafic, l'IDS accomplit certaines actions



Les types d'analyse

- Comment une intrusion est elle détectée par un tel système ?
- Quel critère différencie un flux contenant une attaque d'un flux normal ?
- Deux techniques mises en place dans la détection d'attaques.
  - **Par signatures** d'attaques connues dans les paquets circulant sur le réseau.
    - Exemple : /bin/sh vers un serveur HTTP.
  - **Les évènements** liés à des activités anormales.
    - Exemple : un utilisateur se met à utiliser des outils de gestion réseau.
- Ces deux techniques, aussi différentes soient-elles, peuvent être combinées au sein d'un même système afin d'accroître la sécurité.

L’analyse par signatures

- Elle s’appuie sur la connaissance des techniques utilisées par les attaquants pour déduire des scénarios typiques.
- Basée sur la reconnaissance de schémas connus
  - Pattern matching.
  - Analyse de protocoles.

- **Pattern Matching**
  - Utilisation d'expressions régulière
    - si **Evenement** matche **Signature** alors **Alerte**
  - Les signatures d'attaques connues sont stockées dans une base, et chaque événement est comparé au contenu de cette base
    - si un événement (paquet réseau, log système) correspond à une signature de la base, l'alerte correspondante est levée par l'IDS
  - l'attaque doit être connue pour être détectée
    - Exemples :
      - trouver le motif **/winnt/system32/cmd.exe** dans une requête HTTP
      - **alert tcp any any -> $MY_NET any (flags: S; msg: "SYN packet";)**

L’analyse par signatures

- **Analyse de protocoles:**
  - Cette méthode se base sur une vérification de la conformité (**par rapport aux RFC**) des flux, ainsi que sur l’observation des champs et paramètres suspects dans les paquets.
  - L’intérêt fort de l’analyse protocolaire est qu’elle permet de détecter des attaques inconnues,
  - Inconvénients : Les éditeurs de logiciels et les constructeurs respectent rarement à la lettre les RFC et cette méthode n’est pas toujours très performante.
  - L’analyse protocolaire est souvent implémentée par un ensemble de **préprocesseurs**, où chaque préprocesseur est chargé d’analyser un protocole particulier (FTP, HTTP, ICMP, etc..
  - Exemple:
    - **preprocessor http_decode: 80 8080**

L’analyse par signatures

- Avantages:
  - Facile à implémenter pour tout type d’IDS
  - L'efficacité de ces IDS est liée à la gestion de la base de signatures
    - mise à jour
    - nombre de règles
    - signatures suffisamment précises
  - rapidité du diagnostic

- Inconvénients
  - ne détecte que les attaques connues de la base de signatures
  - maintenance de la base

L’approche comportementale (Anomaly Detection)

- Cette technique consiste à détecter une intrusion en fonction du comportement passé de l’utilisateur.
- il faut préalablement faire une modélisation du système : création d'un profil normal
  - phase d'apprentissage pour définir ce profil
  - la détection d'intrusion consistera à déceler un écart suspect entre le comportement du réseau et son profil
- Exemples de profil : Plusieurs métriques sont possibles :
  - la charge CPU,
  - le volume de données échangées,
  - le temps de connexion sur des ressources,
  - la répartition statistique des protocoles et applications utilisés,
  - les heures de connexion,
- Repose sur des outils de complexités diverses
  - Statistiques, seuils
  - méthodes probabilistes
  - réseaux de neurones

L’approche comportementale (Anomaly Detection)

- Avantages:
  - permet la détection d'attaques non connues a priori
  - facilite la création de règles adaptées à ces attaques
  - difficile à tromper

- Inconvénients :
  - peu fiable : tout changement dans les habitudes de l’utilisateur provoque une alerte.
  - nécessite une période de non fonctionnement pour mettre en oeuvre les mécanismes d’auto-apprentissage
  - L’établissement du profil doit être souple afin qu’il n’y ait pas trop de fausses alertes

Les méthodes répandues

- En général, les IDS mélangent les différentes techniques de détection par scénario en proposant du pattern matching, de l'analyse protocolaire et de la détection d'anomalies.
- De nombreuses techniques et algorithmes sont utilisés dans la détection d'intrusions :
  - Pattern Matching :
    - Algorithmes de recherche de motifs (ex : Boyer-Moore) ,
    - Algorithmes de comptage
    - Algorithmes génétiques
  - Analyse Protocolaire ⇒ conformité aux RFC
  - Détection d'anomalies ⇒ méthodes heuristiques
  - Analyse statistique ⇒ modèles statistiques
  - Analyse probabiliste ⇒ réseaux bayésiens
  - Autre analyse comportementale réseaux de neurones, systèmes experts + data mining, immunologie, graphes, ...

Les différents types d'IDS

- La fonction d'un IDS est la détection des techniques de sondage (balayages de ports, fingerprinting), des tentatives de compromission de systèmes, d'activités suspectes internes, des activités virales ou encore audit des fichiers de journaux (logs).
- Deux types d'IDS
  - Réseau: NIDS : Network Intrusion Detection System
    - principe : contrôler le trafic réseau
      - contenu
      - volume
      - une sonde permet de surveiller plusieurs machines
  - Système :HIDS : Host-based Intrusion Detection System
    - principe : contrôler l'activité système
      - logs
      - fichiers
      - processus
    - une machine nécessite une sonde propre

Network based IDS (NIDS)

- Objectif : analyser de ***manière passive*** les flux en transit sur le réseau et détecter les intrusions en temps réel.

- Un NIDS 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.

- Les NIDS étant les IDS plus intéressants et les plus utiles.

- Un NIDS réassemble les datagrammes IP et les connexions TCP et applique les techniques suivantes:
  - ***Vérification de la pile protocolaire***: mettre en évidence les paquets invalides et signaler les violations des protocoles utilisées par certains types d'attaques.
  - **Reconnaissance des attaques par "*Pattern Matching* », par conformité aux RFCs**

Avantages/inconvénients des NIDS

- Avantages:
  - Avec seulement quelques NIDS bien positionnés on peut surveiller de très grand réseaux.
  - Déployer un NIDS a un faible impact sur le réseau:
    - En effet un NIDS est un équipement passif écoutant le trafic sur sa carte réseau
    - Invisible aux attaquants (pas besoin d'avoir une adresse sur le réseau).

- Inconvénients:
  - Problèmes de charges réseaux : ⇒ une attaque peut ne pas être détectée.
  - Les réseaux switchés gênent le fonctionnment : ⇒ certains switch ne supporte pas le **port-monotoring**.
  - Impossible d'analyser le trafic chiffré (**VPN**, **IPSec**, **HTTPS**, **SSH**).
  - Problèmes liés aux paquets mal formés : ⇒ faux positifs.
  - Base de signatures toujours incomplètes et à mettre à jour.

Produits NIDS

- Libre
  - bro ids : http://bro-ids.org/
  - snort : http://www.snort.org/
  - prelude ID : http://www.prelude-ids.org/
  - Realeyes IDS: http://realeyes.sourceforge.net/
- Propriétaire
  - Cisco Secure IDS : http://www.cisco.com/
  - NetProwler : http://www.symantec.com/index.jsp
  - RealSecure: www.ibm.com
- Outils de test de fiabilité des IDS:
  - isic: http://isic.sourceforge.net/
  - fragroute: http://monkey.org/~dugsong/fragroute/
  - whisker: http://openports.se/security/whisker

Les Host IDS

- Système de détection d'intrusion basé sur l'analyse des informations provenant du système.

- **Principe**:
  - Contrôle d'intégrité des fichiers:
    - Contenu : calcul d'empreinte avec MD5 par exemple.
    - Attributs : à comparer aux valeurs originales.
  - Utilisation de « l'audit trail » (kernel) et des logs systèmes:
    - l'analyse des logs : tri, visualisation, suivi, sauvegarde,etc..

- **Déploiement** :
  - installation courante de plusieurs HIDS (des sondes appelées ***sensors***) sur des machines sensibles .
  - remontée des alertes vers un point central (console d'administration).

Les Host IDS

- **Avantages:**
  - La capacité des HIDS à traiter des évènements locaux qu'un NIDS ne peut pas voir.
  - Les HIDS ne sont pas affectés par l'utilisation des réseaux switchés.
  - Les HIDS utilisant « audit trails» peuvent aider à détecter des chevaux de Trois ou d'autres problèmes d'intégrité.

- **Inconvénients:**
  - Difficultés d'administration : HIDS à configurer et à manager pour chaque machine surveillée.
  - Certains types d'attaques exemple Déni de service peuvent gêner le fonctionnement d'un HIDS (il ne sont pas invisibles).
  - L'utilisation de « l'audit trail » implique un traitement colossal de données (problèmes de stockage)

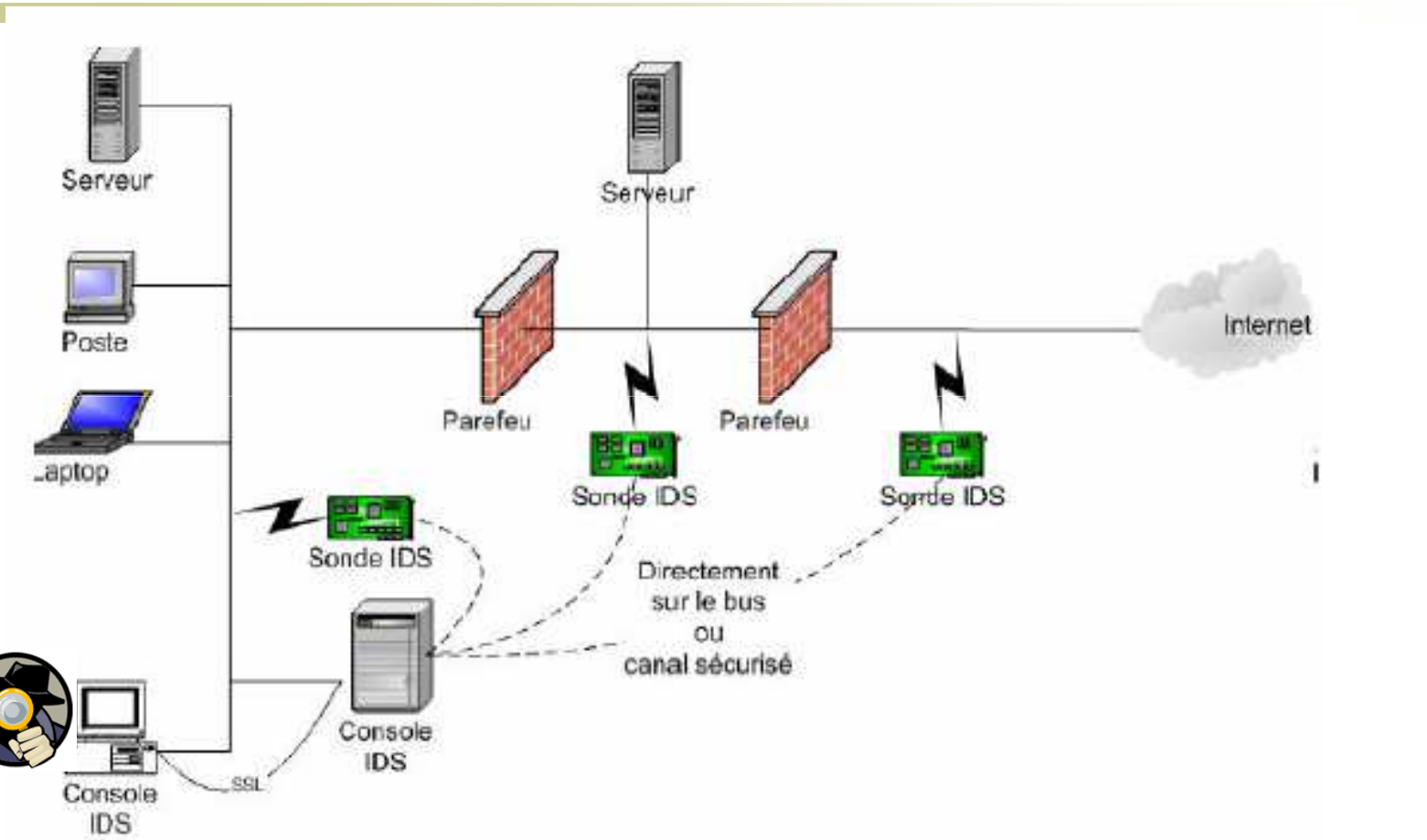
Les IDS hybrides : Prelude-IDS

- Un IDS hybride rassemble les caractéristiques de plusieurs IDS.
  - Surveillance du réseau et de terminaux
  - NIDS + HIDS
- Placement de sondes sur des points stratégiques. Remontée des alertes à une machine centrale, qui va agréger le tout.
- Basé sur l'intégrité du système
  - **Tripwire**
    - Vérifie les empruntes de fichiers (MD5, SHA, etc.)
    - Base de référence des fichiers à analyser
    - Emprunte des fichiers de configuration et base de données de TripWire
  - **Logsurfer**
    - Analyse les logs en se basant sur des règles (regex)
- D'autres solutions:
  - Swatch, Nocol, Osiris, Prelude (Hybride), etc

Déploiement d'un IDS

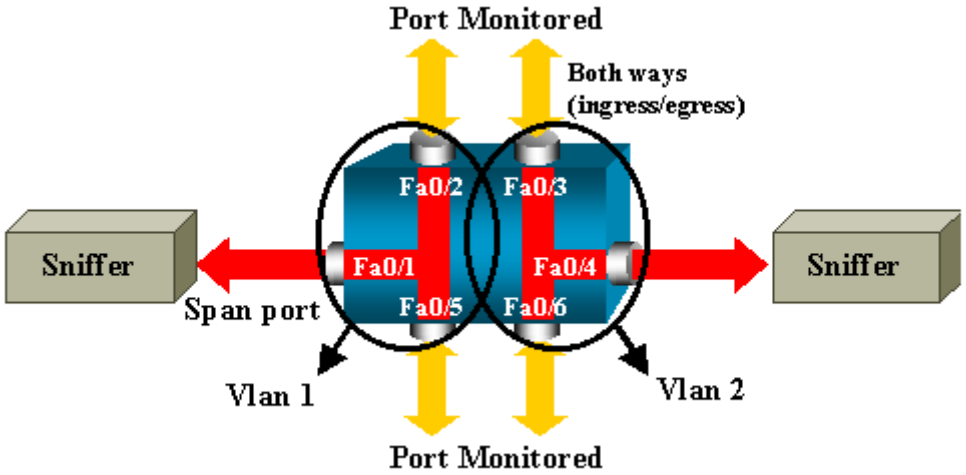
- Lors de la mise en place d'un système de détection d'intrusions au sein d'un réseau, il est important de :
  - Le déployer correctement d'une part,
  - Aussi comprendre son fonctionnement interne pour pouvoir le configurer efficacement.
- Toute erreur lors de l'installation d'un IDS pourra le rendre inefficace ou inutilisable.
- L'emplacement des sondes IDS dépend de la politique de sécurité
  - zone démilitarisée DMZ (attaques contre les systèmes publics)
  - réseau privé (intrusions vers ou depuis le réseau interne)
  - segment extérieur du pare-feu (détection de signes d'attaques parmi tout le trafic entrant et sortant avant filtration)

Exemple de déploiement



Modes de connexion

- Le système IDS doit se connecter sur un segment d'un réseau
- Divers modes sont possibles :
  - Utilisation d'un *hub sur le segment*
  - SPAN (Switch Port Analyzer). : utilisation d'un port sur un équipement de commutation réseau, ce port est un **miroir** de l'ensemble du trafic sur le commutateur



La sécurité active (Intrusion Prevention System)

- les IPS sont des outils aux fonctions « actives », qui en plus de détecter une intrusion, tentent de la bloquer.
  - Prévention des intrusions sur le réseau/hôtes.
  - Défense proactive
  - Fonctionnalité intégrée aux firewalls
    - Un IPS ne remplace pas un firewall
- Plusieurs stratégies de prévention d'intrusions existent :
  - **host-based memory and process protection :** surveille l'exécution des processus et les tue s'ils ont l'air dangereux (buffer overflow). Cette technologie est utilisée dans les KIPS (Kernel Intrusion Prevention System).
  - **Session interception / session sniping :** termine une session TCP avec la commande TCP Reset : « RST ». Ceci est utilisé dans les NIPS (Network Intrusion Prevention System).
  - **gateway intrusion detection :** si un système NIPS est placé en tant que routeur, il bloque le trafic sinon il envoie des messages à d'autres routeurs pour modifier leurliste d'accès.

Avantages / inconvénients

- Le premier est qu'il bloque toute activité qui lui semble suspecte. Or, il est impossible d'assurer une fiabilité à 100% dans l'identification des attaques.

- Le deuxième inconvénient est qu'un pirate peut utiliser sa fonctionnalité de blocage pour mettre hors service un système:
  - Prenons l'exemple d'un individu mal intentionné qui attaque un système protégé par un IPS, tout en spoofant son adresse IP. Si l'adresse IP spoofée est celle d'un noeud important du réseau (routeur, service Web, ...), les conséquences seront catastrophiques. Pour palier ce problème, de nombreux IPS disposent des « white lists », c'est-à-dire des listes d'adresses réseaux qu'il ne faut en aucun cas bloquer.

- Un IPS est peu discret. En effet, à chaque blocage d'attaque, il montre sa présence. Cela peut paraître anodin, mais si un pirate remarque la présence d'un IPS, il tentera de trouver une faille dans celui-ci afin de réintégrer son attaque

Dérive des IDS : Honeypot

- «honeypot is a security ressource whose value lies in being probed, attacked or compromised » **L. Spitzner.**

- Un système volontairement vulnérable à une ou plusieurs failles connues visant à attirer les pirates afin d'étudier leurs stratégies d'attaque pour mieux les comprendre et les anticiper.

- Utilité
  - Le pot de miel peut faire perdre du temps à un attaquant
  - Aide à la génération de nouvelles signatures.
- Interaction
  - Faible interaction
    - Simulation de services sans réel système sous-jacent
    - Relative simplicité au niveau de l'émulation
  - Forte interaction
    - Le honeypot représente un véritable système d'exploitation

Critères pour le choix d’un IDS

- Critères pour le choix d’un IDS
  - IDS s'intègre dans un contexte et dans une architecture imposant des contraintes très diverses
  - Certains critères peuvent être dégagés:
    - Fiabilité
    - Réactivité
    - Facilité de mise en oeuvre et adaptabilité
    - Flexibilité
    - Performance
    - Intégration dans un environnement technologique existant

Bibliographie

- **[1]** F. Meunier, « Détection d'intrusions: notions avancées de NIDS axées sur le logiciel ManHunt (Recourse Technologies) », Rapport, Watch4net, Août 2002.
- **[2]** K. Müller, « IDS - Systèmes de Détection d'Intrusion, Partie I », May 2003, http://www.linuxfocus.org/Francais/May2003/article292.shtml.
- **[3]** K. Müller, « IDS - Systèmes de Détection d'Intrusion, Partie II », July 2003, http://www.linuxfocus.org/Francais/July2003/article294.shtml
- **[4]** http://cosy.univ-reims.fr/~fnolot/Download/Cours/reseaux/m2pro/SESY0708/ids-ips.pdf
- **[5]** http://taz.newffr.com/TAZ/Reseaux/Admin/IDS-NIDS/IDS_struct.pdf
- **[6]** http://cosy.univ-reims.fr/~fnolot/Download/Cours/reseaux/m2pro/SESY0708/ids-ips.pdf