Détection d’intrusion

© 2005 Tous droits réservés - Guillaume Arcas <guillaume.arcas@free.fr>

Sommaire

- Introduction
- Présentation des IDS
  - Définitions et terminologie
  - Types d'IDS
  - Méthodes de détection
  - Positionnement dans le SI
  - Limites des IDS
- Mise en pratique avec Snort
  - Installation
  - Paramétrage de base
  - Utilisation avancée

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Introduction

- Les IDS
  - Pourquoi utiliser un IDS ?
    - Complément passif des outils de sécurité actifs (pare-feux)
    - Augmente la visibilité sur le degré de sécurité du SI
      - La complexité des attaques devient telle que les données issues des éléments de filtrage (routeurs, pare-feux) ne suffisent souvent plus.
    - Avantages
      - Meilleure qualification des risques auxquels est exposé le SI
      - Permettre une meilleure réactivité des équipes d'administration
      - Surveiller en permanence l'adaptation de la politique de sécurité au risque
    - Inconvénients
      - La détection d'intrusion est une activité consommatrice en temps et en ressources humaines qualifiées.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Définitions (1)

- Système
  - Association de composants matériels et logiciels servis par des équipes d'analystes
- Détection
  - Action passive proche de la supervision et de la surveillance
- Intrusion (syn. : attaque ou événement de sécurité)
  - Action hostile : action dont le but est de compromettre volontairement la confidentialité, l'intégrité ou la disponibilité du SI.
  - Action illicite : action qui enfreint la politique de sécurité du SI.
    - Note : une attaque menée par un utilisateur autorisé entre dans la définition de l'intrusion (ex.: connexion SSH sur un serveur non motivée par des impératifs de service)
  - Notion indépendante du type d'attaquant
    - Personne (pirate, utilisateur du SI) ou outil (virus ou ver, scanner).

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Définitions (2)

- Détection d'intrusion
  - Collecte de données issues des composants d'un système d'information en vue de de leur analyse et de la recherche de toute trace d'activité hostile ou illicite.
  - Composants du SI pris en compte :
    - Systèmes : serveurs et postes de travail
    - Réseaux : équipements réseaux, pare-feux, routeurs
    - Applications
  - Analyse et recherche
    - Système de référence interne ou externe au SI.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Définitions (3)

- Collecte de données
  - Choix des sources
    - Trafic réseau
    - Journaux systèmes et d'applications
  - Choix d'une méthode de collecte
    - En temps réel
    - Différée
    - Ponctuelle ou permanente
  - Choix du mode de stockage des données recueillies

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Définitions (4)

- Analyse des données recueillies
  - Choix d'un système de référence
    - Externe
      - Signatures
      - Bases de vulnérabilité
    - Interne
      - Profil de connexion ou d'utilisation
      - Politique de sécurité du SI
  - Choix d'une méthode
    - Systématique
    - Empirique

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Définitions (5)

- Alerte
  - Une alerte est définie comme le résultat de l'analyse par un composant de l'IDS d'une ou plusieurs données qui décrivent une intrusion.
  - Elle doit permettre à l'analyste de confirmer ou d'infirmer le caractère hostile ou illicite de l'événement concerné
    - Horodatage
    - Sources et destination
    - Capture du paquet (trafic réseau) ou de la ligne d'un journal (système ou application)

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Terminologie (1)

- Un IDS est composé de plusieurs éléments.
  - Sonde : dispositif matériel ou logiciel de capture et d'analyse du trafic réseau.
  - Agent : dispositif logiciel d'analyse de journaux système ou d'applications
  - Signature : description des caractéristiques d'une intrusion réseau.
  - Règle : description des caractéristiques d'une trace d'intrusion enregistrée par un journal système ou d'application.
    - Note : une règle se présente très souvent sous la forme d'une expression régulière.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Fonctionnalités (1)

- Collecte
  - Réalisée par les sondes et agents
  - Entrée : données issues du trafic réseau, des fichiers de journalisation, de scripts, etc.
  - Sortie : messages construits à partir d'une ou plusieurs données.
- Moteur d'analyse
  - Entrée : messages produits durant la collecte.
  - Sortie : à partir d'un système de référence et d'un ou plusieurs messages, produit des alertes.
- *Note : collecte et analyse peuvent être réalisées par un seul et même composant (sonde ou agent).*

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Fonctionnalités (2)

- Transport
  - Assure les échanges de données, de messages et d'alertes entre les différents composants de l'IDS.
    - Dans le cas d'un composant qui cumule deux fonctionnalités, la fonction de transport est interne et s'appuie sur les mécanismes « classiques » de communication inter processus
    - Dans le cas d'IDS fortement distribués, le réseau est mis à contribution.
    - Dans certains cas, les messages et alertes sont échangées dans un format binaire pour des questions de performances.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Fonctionnalités (3)

- Stockage
  - Assure le stockage à long terme des alertes.
  - Les alertes peuvent être stockées « tel quel » ou bien être formatées avant leur stockage. Lorsque les alertes sont produites dans un format binaire, elles sont souvent traduites dans un « langage » lisible lors de cette étape.
  - Fichiers texte ou, plus souvent, utilisation d'un SBGD.
  - Il existe un format d'échange en cours de normalisation : IDMEF (DTD XML).

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Fonctionnalités (4)

- Dans la plupart des cas, certains composants remplissent plusieurs fonctionnalités :
  - Collecte et analyse pour les sondes et les agents
  - Transport et stockage
  - On parlera alors d'IDS distribué
- Les quatre fonctionnalités peuvent même être mises en œuvre par un seul composant qui agit en mode « boîte noire ».

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Fonctionnalités (5)

- Corrélation
  - Processus qui consiste, à partir de plusieurs alertes, à mettre en liaison celles qui présentent des caractéristiques communes ou qui sont rattachées à un même événement par un lien logique (étapes successives d'une compromission de serveur par exemple).
- Interprétation
  - Processus qui consiste à comprendre le sens exact des alertes remontées par les composants de l'IDS.
  - Tâche le plus souvent non automatisable.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Types d'IDS

- Trois grandes familles d'IDS
  - Network based IDS (NIDS)
    - Les systèmes qui appartiennent à cette catégorie utilisent le trafic réseau comme unique source de données.
  - Host based IDS (HIDS)
    - Les systèmes de cette catégorie utilisent des éléments « locaux » d'une machine comme unique source de données. Ces éléments sont les journaux systèmes et d'application mais peuvent aussi être les sorties de scripts exécutés localement.
  - Hybrid IDS (HyIDS)
    - Les systèmes de cette dernière catégorie utilisent le trafic réseau et les éléments locaux comme sources de données.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Network based IDS

- Avantages
  - Permet de surveiller tout un segment de réseau depuis un seul point d'écoute.
  - Indépendance par rapport aux autres composants du SI.
    - Pas d'impact sur le fonctionnement ni sur les performances du SI.
- Inconvénients
  - Doit être adapté à la volumétrie du trafic analysé.
- Limites
  - Ne peut pas analyser le trafic chiffré.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Host based IDS

- Avantages
  - Détecte des évènements réels
  - Permet de prendre en compte des évènements qui ne sont pas visibles autrement : consommation des ressources par une application, utilisateurs connectés, etc.
- Inconvénients
  - Nécessite souvent d'écrire des règles « sur mesure »
- Limites
  - Si la machine surveillée est compromise, les indicateurs et journaux utilisés par l'IDS peuvent être détruits ou modifiés, ce qui faussera ou empêchera l'analyse.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Hybrid IDS

- Avantages
  - Association des avantages d'un NIDS à ceux d'un HIDS
  - Vision globale de l'activité du SI
  - Permet de corréler des évènements réseaux à des traces systèmes / application
    - Ex. : un paquet d'attaque Code Red remonté par une sonde et une ligne « 404 NOT FOUND » remonté par un agent sur un serveur Web.
- Inconvénients
  - La complexité du déploiement et de la maintenance d'un tel IDS est proportionnelle à celle du SI.
- Limites
  - La volumétrie des alertes générées peut vite être handicapante.

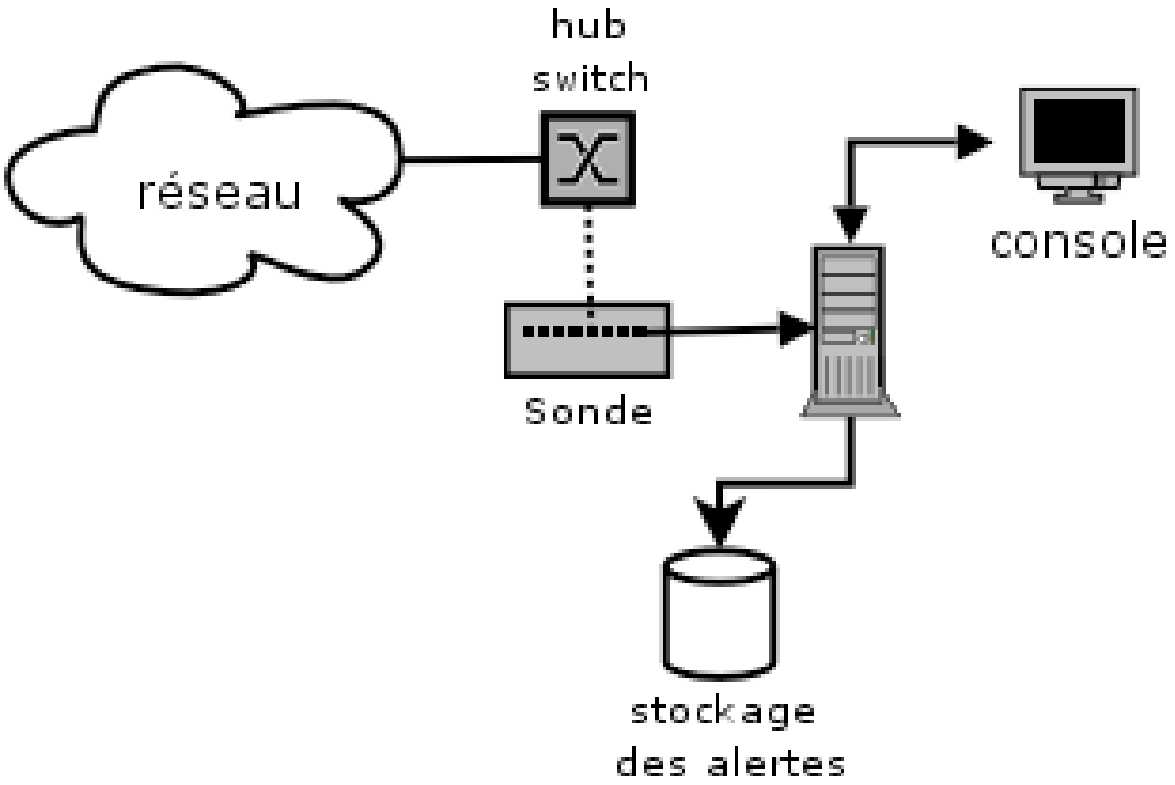
© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Modes d'analyse

- Signatures et règles
  - Décrivent les caractéristiques d'une intrusion
    - Signature : ports source et destination, valeurs des drapeaux et options, contenu du paquet, etc.
    - Règle : mots-clefs contenus dans une ligne d'un journal système (Ex. `LOGIN FAILED`) ou d'application (Ex. `ACCESS FORBIDDEN`).
- Analyse comportementale
  - Traduction de la politique de sécurité dans un langage compris du moteur d'analyse de l'IDS.
    - Ex. : heures ouvrables, services autorisés, etc.
- Analyse statistique ou heuristique
  - Traduction de la « normalité » à partir de l'observation et d'un historique. Tout événement qui sort de cette normalité sera considéré comme une intrusion.

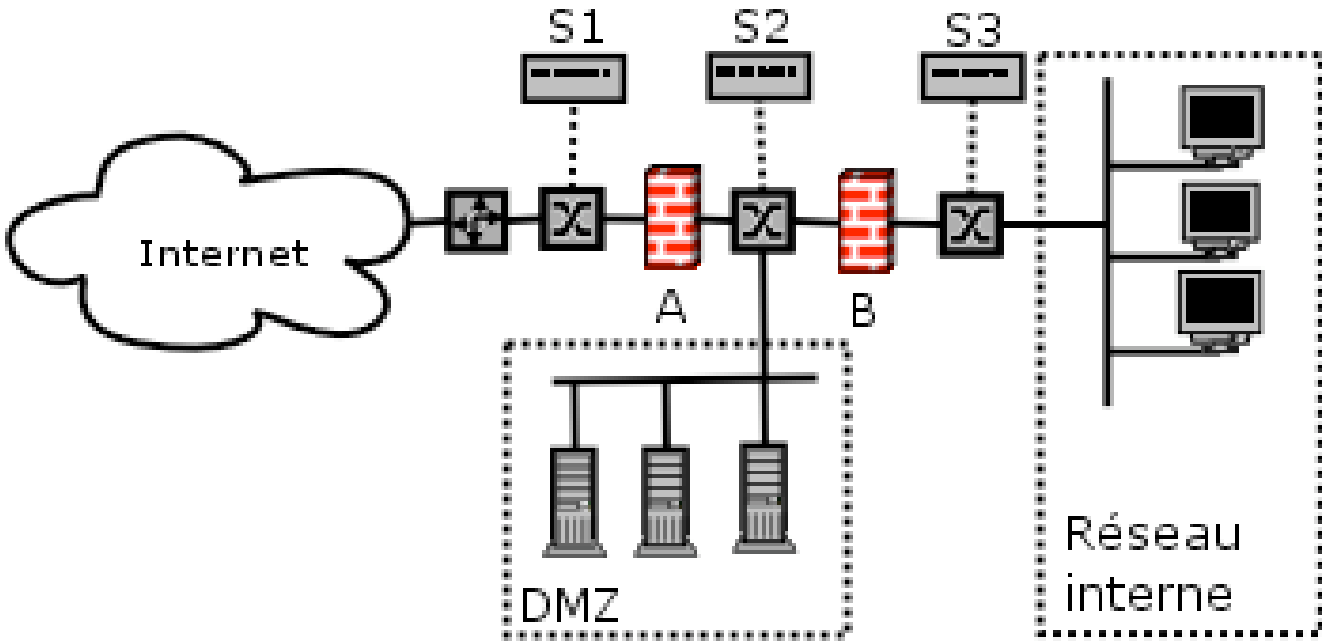
© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Architecture (2)



© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Architecture (3)



© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Déploiement d'un IDS

- Choix des sources de données à prendre en compte
  - Dépend fortement de l'architecture et de la topologie du SI
  - Suppose une bonne connaissance du fonctionnement du SI
  - Travail d'équipe transverse
    - Implique les exploitants, les équipes d'ingénierie, éventuellement les développeurs
- Choix des modes de collecte, d'analyse et de stockage
- Choix des outils
- Déploiement
  - Peut nécessiter une refonte partielle de l'infrastructure du SI (Ex.: utilisation d'un réseau dédié à l'IDS)

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Exploitation

- Tâche récurrente et quotidienne
  - Phase d'apprentissage initiale
  - Aucune solution n'est entièrement automatique : le recours à l'analyste reste la règle et c'est lui qui a le dernier mot.
- Légalité
  - La surveillance effectuée par l'IDS doit s'inscrire dans le cadre légal et réglementaire.
- Déontologie
  - Rendre anonymes les données qui doivent être échangées si l'on fait appel à une aide extérieure
    - Avec snort : option -o

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Attaques contre les IDS (1)

- Pollution
  - L'attaquant génère un trafic très important dans le but :
    - d'atteindre ses limites de l'IDS qui ne peut plus traiter le trafic assez rapidement ce qui permet à l'attaquant de camoufler son attaque.
      - Limites de l'IDS : taille des disques, mémoire, processeur, carte réseau
    - de générer un très grand nombre de fausses alertes dans le but de noyer l'analyste qui n'aura plus le temps de détecter les vraies attaques.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Attaques contre les IDS (2)

- Attaques contre l'IDS lui-même
  - Déni de service
    - Envoi de paquets malformés qui provoqueront un gel de l'IDS
  - Compromission
    - Dans certains cas, la même technique peut être utilisée pour compromettre l'IDS par l'intermédiaire du logiciel utilisé
      - Failles tcpdump, ethereal, ISS.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Perspectives (1)

- Limites des IDS actuels
  - Faux positifs
  - Consommateur en temps
    - Collecte et analyse peuvent être automatisées, mais l'interprétation reste encore essentiellement une tâche d'expert.
  - Nécessité de disposer de personnels qualifiés
    - Plus le SI surveillé est complexe, plus il y aura besoin de faire appel à des compétences particulières.
  - Trafic chiffré

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Perspectives (2)

- Convergences avec les outils de sécurité actifs
  - Mise en œuvre de contre-mesures à partir d'une alerte
    - Modification des règles de routage
    - Ajout de filtres sur les pare-feux
  - Apparition des IPS (Intrusion Prevention Systems)
- Convergences avec les outils de supervision
  - Aide au calcul du niveau de la qualité de service
  - Identification des centres de consommation inutile de ressources.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Quelques logiciels

- Snort - www.snort.org
  - Référence en matière de détection réseau
- Prelude-IDS - www.prelude-ids.org
  - IDS hybride, utilise Snort comme sonde et fournit des agents.
- Sguil - sguil.sourceforge.net
  - Construit au-dessus de Snort. Permet de reconstituer les sessions complètes à partir d'une alerte.
- Il existe de nombreuses solutions proposées par des éditeurs commerciaux : ISS, etc.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Snort

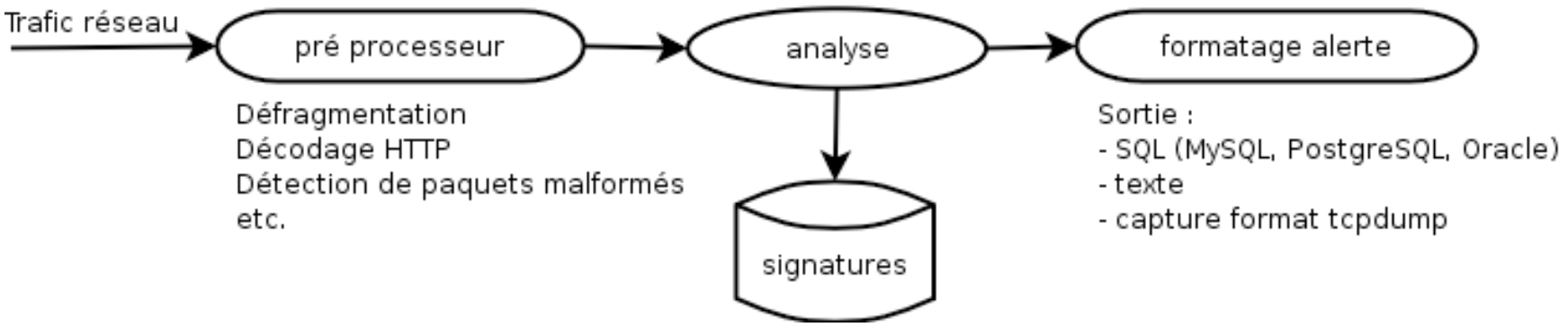
© 2005 Tous droits réservés - Guillaume Arcas <guillaume.arcas@free.fr>

Présentation

- Logiciel de détection d'intrusion réseau distribué sous licence GPL.
- S'appuie sur la bibliothèque de fonctions libpcap (tcpdump).
- Est rapidement devenu la référence en matière de logiciel de détection réseau.
- Utilise des signatures comme système de référence.
- Intègre des modules de pré-traitement des paquets.
- Propose plusieurs modes de stockage.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Fonctionnement



© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Collecte

- Capture du trafic réseau TCP/IP
  - La carte utilisée doit être adaptée aux besoins, notamment dans le cas de réseaux à fort trafic ou à haut débit.
  - L'interface réseau doit être configurée en mode passif sans adresse IP. Sous Linux, une règle IPTables peut être ajoutée pour interdire toute émission de paquet par la sonde (ce qui en trahirait la présence)
- Snort peut aussi traiter en entrée des fichiers de capture au format PCAP.
  - Utile si l'on doit analyser un trafic qui nécessite un décodage (détunnelisation par exemple).

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Pré traitements (1)

- Opérations effectuées sur les paquets par des pré processeurs avant leur transfert au moteur d'analyse.
- Objectifs :
  - Nettoyage du trafic inutile ou inexploitable
    - Améliorer les performances d'analyse
  - Prise en compte de l'état d'un paquet
    - Appartenance à une session établie
    - Prise en compte du sens du flux
  - Protéger le moteur des attaques
  - Eviter au mieux les techniques de contournement.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Pré traitements (2)

- Détection des balayages de ports (portscan)
  - Portscan, sfPortscan
    - L'utilisation de ces pré processeurs peut engendrer des volumes très importants d'alertes.
    - Ces pré processeurs sont assez délicats à configurer.
- Défragmentation
  - Frag2
    - Détection des attaques DoS basées sur la fragmentation des paquets IP (Teardrop, Jolt, fragroute).

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Pré traitements (3)

- Réassemblage de paquets
  - Stream4, stream4_reassemble
  - Permet de conserver l'état d'un paquet
    - Détecte les paquets qui n'appartiennent pas à une session établie à la manière d'un pare-feu « state full »
    - Détecte les balayages furtifs à la nmap et les tentatives de contournement.
  - Permet également de conserver des statistiques sur les sessions :
    - Nombre, adresses source et destination, durée, volume.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Pré traitements (4)

- Pré processeurs « applicatifs »
- Objectifs : faciliter la détection d'attaques contre des applications particulières.
- Exemples de décodeurs
  - Décodeur RPC
  - Décodeur HTTP
    - Détection UNICODE dans les URL
  - Décodeur Telnet

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Analyse

- Utilisation de signatures
  - Signature : description des caractéristiques d'un paquet qui appartient ou qui suit une attaque.
  - Chaque paquet est comparé à toutes les signatures chargées en mémoire au démarrage de Snort.
- Les signatures sont fournies sous forme de fichiers texte.
- Disponibles :
  - sur le site officiel Snort
    - Depuis mars 2005 : nouvelle licence d'utilisation
  - Sur le site Bleeding-snort.com

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Signature

```
alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg:"mountd access";)
```

- Une en-tête suivie des options (entre parenthèses)
- L'en-tête
  - Définit quelle action doit être effectuée si un paquet correspond à la signature
  - Décrit les caractéristiques générales IP du paquet
    - Protocole
    - Adresses IP source et destination
    - Ports utilisés.
- Options
  - Définissent les caractéristiques particulières du paquet et fournissent des informations complémentaires.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Format des en-têtes (1)

- Action
  - alert : génère une alerte puis logue le paquet
  - log : logue le paquet sans générer d'alerte
  - pass : n'effectue aucune action
  - activate : génère une alerte et déclenche l'action définie par une signature de type dynamic.
  - dynamic : définit une action qui sera déclenchée par une signature de type activate
    - Note : les signatures activate/dynamic marchent par paires.
  - Il est aussi possible de définir ses propres actions.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Formats des en-têtes (2)

- Caractéristiques du trafic IP
  - Protocole tcp,udp, ip, icmp
  - Adresses IP
    - Littérale : 192.168.1.2
    - Masque réseau :192.168.1.0/24
    - Groupées : [192.168.1.0/24,192.168.2.0/24]
  - Ports
    - Forme littérale : 111, 80
    - Range littéral complet : 1:1024
    - Range complété : :1024, 1024:
  - Sens du trafic : <>, ->, <-

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Options

- msg : intitulé de l'alerte qui sera remontée par la signature
- sid et rev : identifiant (unique) de la signature et numéro de version
- classtype et priority : catégorie et degré de sévérité
- Caractéristiques du paquet
  - Valeurs des drapeaux TCP, type de service, TTL, etc.
- Contenu du paquet
  - Mot-clef, bits et position dans le paquet
    - Pour la recherche de mots-clefs, Snort s'appuie sur la bibliothèque de fonctions PCRE qui permet d'utiliser les expressions régulières PERL dans une signature.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Stockage

- Les modes de stockage des alertes sont définis à l'aide de module output
  - Fichiers texte
    - Fichiers dédiés ou syslog
  - SQL
    - MySQL, PostgreSQL, Oracle,
  - Format PCAP
    - Les paquets sont stockés sur disque dans un format binaire qui pourra être lu par des outils comme tcpdump ou ethereal
- Note : il est possible d'utiliser plusieurs modules output.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Autres fonctionnalités

- Perfmon
  - Suivi des performances : nombre de paquets traités, nombre de paquets non traités, etc.
- Event thresolding
  - Permet de définir des seuils au-delà desquels une action différente de celle définie par une signature est prise.
- Event Suppression
  - Permet de supprimer à la volée certaines alertes.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Outils complémentaires

- Stockage
  - SGBD de type MySQL ou PostgresQL
- Gestionnaire de signatures
  - Oinkmaster pour automatiser les mises à jour des signatures
- Console de visualisation et de gestion des alertes
  - Très souvent une application PHP pour serveur Apache
    - BASE
- Ethereal
  - Analyse des paquets capturés en format PCAP
    - Très utile en cas de trafic encapsulé.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Evolutions en cours

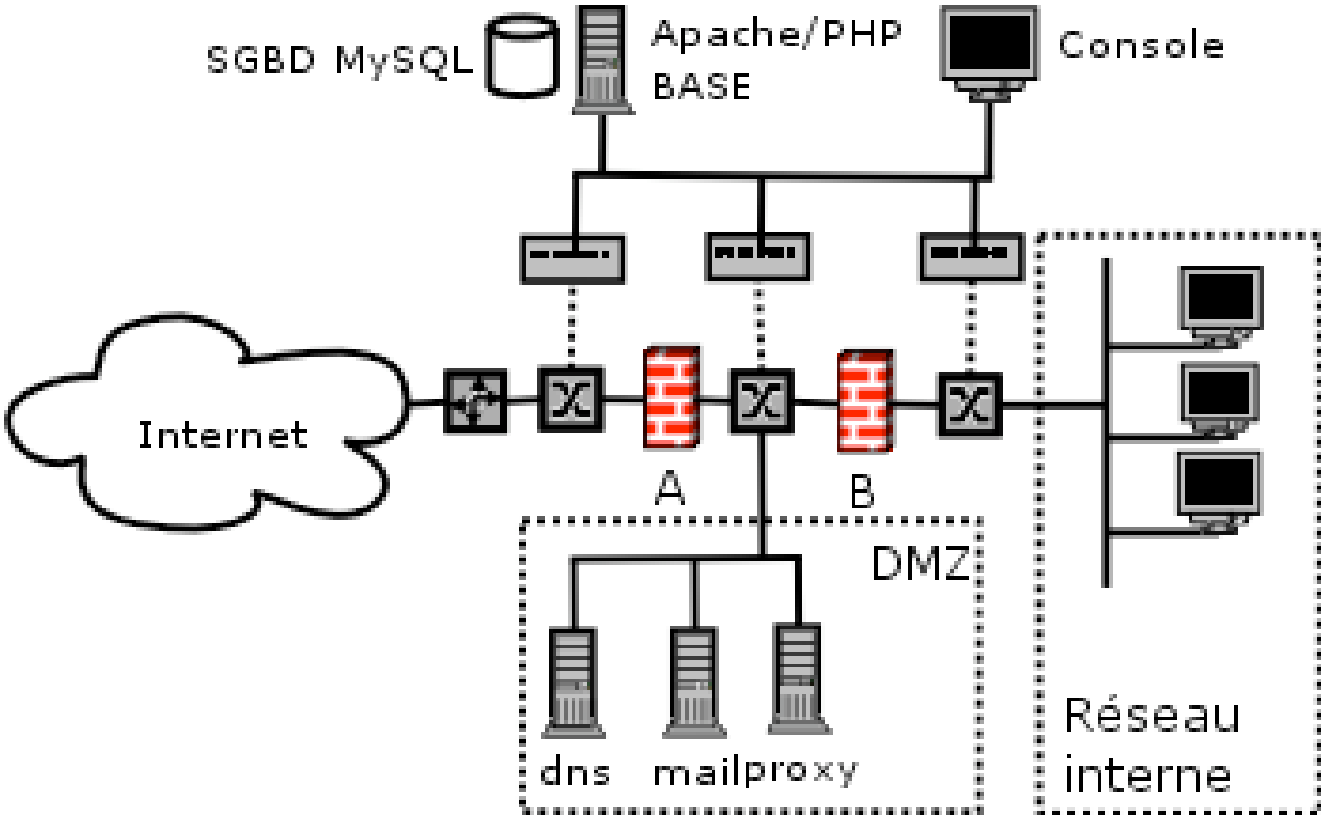
- Snort inline
  - De l'IDS à l'IPS (Intrusion Prevention System)
    - L'outil devient actif.
    - Notion de pare-feu intelligent
      - Pare-feu traditionnel :
        - Règles statiques fondées sur les caractéristiques générales des paquets
      - Snort Inline :
        - Règles évoluées qui prennent en compte le contenu et le contexte applicatif du trafic.

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Travaux pratiques

© 2005 Tous droits réservés - Guillaume Arcas <guillaume.arcas@free.fr>

Schéma type d'un IDS Snort



© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>

Références

- Projet Snort
  - Section Documentation – http://www.snort.org
- Projet SGUIL
  - http://sguil.sourceforge.net
- Projet Prelude-IDS
  - http://www.prelude-ids.org

© 2005 Tous droits réservés – Guillaume Arcas <guillaume.arcas@free.fr>