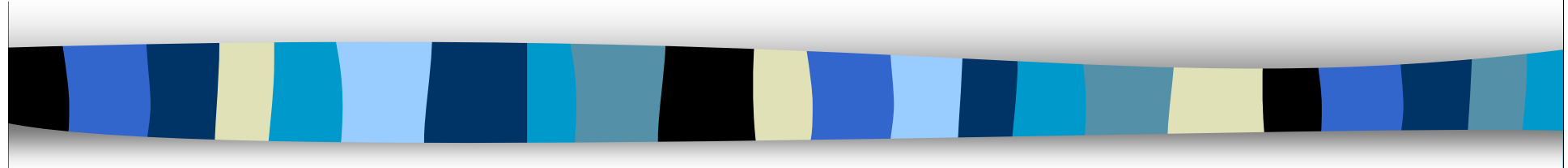


Les IDS et IPS Open Source



Alexandre MARTIN

Jonathan BRIFFAUT



Plan

- Présentation Générale des IDS
- Les différents type d'IDS
- Les méthodes de détection
- Présentation Générale des IPS
- Ou placer un IDS / IPS ?
- Outils Open Source (Aspect Pratique)
 - SNORT
 - Prelude-IDS
 - BRO



Présentation générale des IDS



Qu'est-ce qu'un IDS ?

- L'IDS (Intrusion Detection System)
 - Surveiller
 - Contrôler
 - Détecter
- Le système de détection d'intrusion est en voie de devenir un composant critique d'une architecture de sécurité informatique



Justificatif

- Nombre de failles élevés:
 - 3273 nouvelles entre Janvier et Juillet 2007
- Coût d'une attaque est élevé:
 - Code Red/Nimda est estimé à 3.2 Milliards \$ par Computer Economics
- Les outils pour lancer les attaques sont facilement disponibles et exploitables



De quoi est constitué un 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 (HTTP, Telnet)
- Selon le type de trafic, l'IDS accomplit certaines actions



Vocabulaire

- Faux-Positif
 - Fausse alerte levée par l'ids
- Faux-négatif
 - Attaque qui n'a pas été repéré par l'IDS
- Evasion
 - Technique utilisée pour dissimuler une attaque et faire en sorte qu'elle ne soit pas décelée par l'IDS
- Sonde :
 - Composant de l'architecture IDS qui collecte les informations brutes



Actions d'un IDS

- Journaliser l'événement
 - Source d'information et vision des menaces courantes
- Avertir un système avec un message
 - Exemple: appel SNMP
- Avertir un humain avec un message
 - Courrier électronique, SMS, interface web, etc.
- Amorcer certaines actions sur un réseau ou hôte
 - Exemple: mettre fin à une connexion réseau, ralentir le débit des connexions, etc. (rôle actif)



Après la Détection

- Comprendre l'attaque en cours
 - Recueillir le maximum d'information
 - Cibles
 - Sources
 - Procédé
- Archiver, tracer : Corrélation avec d'autres événements
- Préparer une réponse :
 - Sur le court terme : black-listage
 - Sur le long terme : application de patches, action en justice...



Les différents types D'IDS



Les types d'IDS

- Il existe deux types d'IDS :
 - HIDS (Host IDS)
 - NIDS (Network IDS)



Le Host IDS

- Basé dans un ordinateur hôte
- HIDS permet de surveiller le système et les applications
 - Les journaux systèmes,
 - de contrôler l'accès aux appels systèmes,
 - de vérifier l'intégrité des systèmes de fichiers
- Le HIDS à accès à des composants non-accessibles sur le réseau
 - Exemple: la base de registre de Windows
- Ne surveille qu'un seul hôte



Le Network IDS

- Un sonde placée dans le réseau
 - Surveille l'ensemble du réseau
 - Capture et analyse tout le trafic
 - Recherche de paquets suspects
 - Contenu des données
 - Adresses IP ou MAC source ou destination
 - ...
 - Envoi d'alertes



HIDS et NIDS

- Chacun répond à des besoins spécifiques
- HIDS particulièrement efficaces pour déterminer si un hôte est contaminé
- NIDS permet de surveiller l'ensemble d'un réseau \neq HIDS qui est restreint à un hôte



Les méthodes de détection



Les méthodes de détection

- 2 approches principales pour les IDS:
 - Par signature
 - Comportementale
 - Détection d'anomalie
 - Vérification d'intégrité

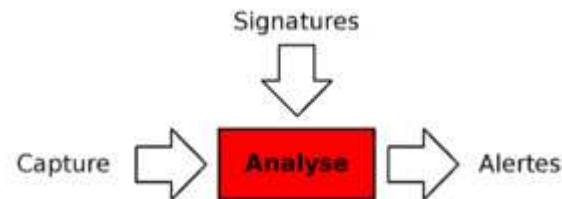


Méthodes de détection : Par Signature

- Par signature:
 - Basé sur la reconnaissance de schémas déjà connus
 - Utilisation d'expressions régulières
 - Les signatures d'attaques connues sont stockées dans une base; et chaque événement est comparé au contenu de cette base
 - Si correspondance l'alerte est levée
 - L'attaque doit être connue pour être détectée
 - Peu de faux-positifs

Méthodes de détection : Par Signature

- Méthode la plus simple, basé sur :
 - Si **EVENEMENT** matche **SIGNATURE** Alors **ALERTE**



- Facile à implémenter pour tout type d'IDS
- L'efficacité des ids est liée à la gestion de leur base de signatures
 - MAJ
 - Nombre de règles
 - Signatures suffisamment précises
- Exemples
 - Trouver le « motif `/winnt/system32/cmd.exe` » dans une requête http
 - Trouver le motif « failed su for root » dans un log système



Méthodes de détection : Par Signature

■ Recherche de motif (pattern matching)

– Différents algorithmes

- Ceux pour envoyer les négatifs
 - E2XB
- Ceux pour peu de signature
 - BOYER MOORE
 - [Knuth](#)-Morris-Pratt (KMP).
- Nombreuse Signature :
 - AHO-CORASICK
 - » AUTOMATE DETERMINISTE A*X
 - » A = alphabet
 - » X ensemble fini de mots à rechercher



Méthodes de détection : Par Signature

■ Avantage

- Simplicité de mise en œuvre
- Rapidité de diagnostic
- Précision (en fonction des règles)
- Identification du procédé d'attaque
 - Procédé
 - Cibles
 - Sources
 - Outils

■ Inconvénients

- Ne détecte que les attaques connues
- Maintenance de la base
- Techniques d'évasion possibles dès lors que les signatures sont connues



Méthodes de détection : Par anomalie

- Basée sur le comportement « normal » du système
- Une déviation par rapport à ce comportement est considérée suspecte
- Le comportement doit être modélisé : on définit alors un profil
- Une attaque peut être détectée sans être préalablement connue



Méthodes de détection : Par anomalie

- Modélisation du système : création d'un profil normal
 - Phase d'apprentissage
 - Détecter une intrusion consiste à détecter un écart
 - Exemple de profil :
 - Volumes des échanges réseau
 - Appels systèmes d'une application
 - Commandes usuelles d'un utilisateur
 - Repose sur des outils de complexité diverses
 - Seuils
 - Statistique
 - Méthodes probabilistes
 - Etc.
 - Complexité de l'implémentation et du déploiement



Méthodes de détection : Par anomalie

■ Avantages

- Permet la détection d'attaque inconnue
- Facilite la création de règles adaptées à ces attaques
- Difficile à tromper

■ Inconvénients

- Les faux-positifs sont nombreux
- Générer un profil est complexe
 - Durée de la phase d'apprentissage
 - Activité saine du système durant cette phase ?
- Diagnostics long et précis en cas d'alerte



Méthodes de détection : Par intégrité

- Vérification d'intégrité
 - Génération d'une somme de contrôle sur des fichiers d'un système
 - Une comparaison est alors effectuée avec une somme de contrôle de référence
 - Exemple : une page web
 - Méthode couramment employée par les HIDS



Points négatifs des IDS

- Technologie complexe
- Nécessite un degré d'expertise élevé
- Long à optimiser
- Réputer pour générer de fausses alertes
- Encore immature



Présentation générale des IPS



Les IPS

- IPS = Intrusion Prevention System
 - Mieux vaut prévenir que guérir
- Constat :
 - On suppose pouvoir détecter une intrusion
 - Pourquoi alors, ne pas la bloquer, l'éliminer ?
- IDS vers IPS
 - Terme à la base plutôt marketing
 - Techniquement :
 - Un IPS est un IDS qui ajoute des fonctionnalités de blocage pour une anomalie trouvée
 - IDS devient actif => IPS



Les IPS : SUITE

- Objectifs :
 - Interrompre une connexion
 - Ralentir la connexion
 - Blacklister les sources
- Moyens :
 - Règle Firewall
 - QoS
 - Intervention applicatif (Proxy)



IPS : suite

- **Avantages**

- Attaque bloquée immédiatement

- **Inconvénients**

- Les faux-positifs
- Peut paralyser le réseau



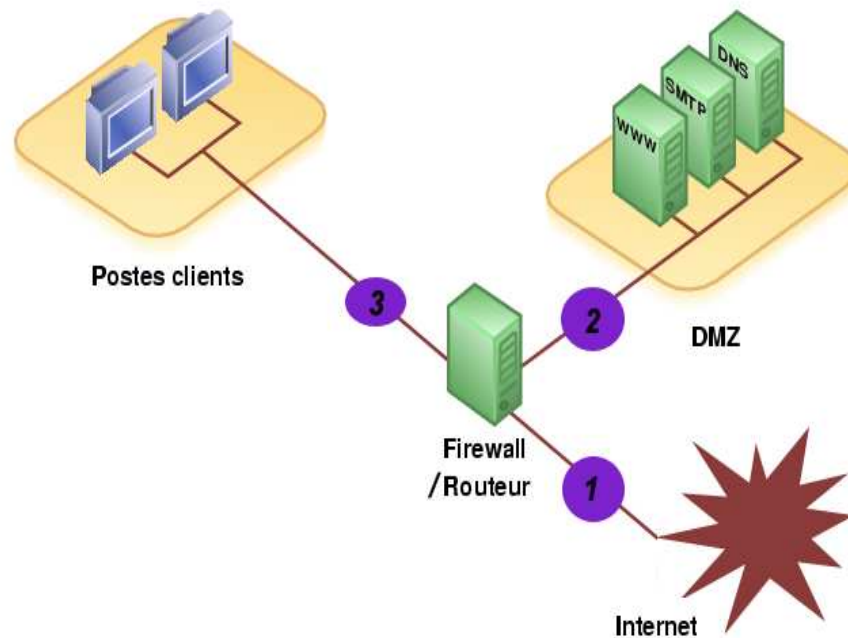
Où placer un IDS IPS ?



Placer un IDS

- Dépend de ce que l'ont veut ?
 - Voir les attaques (HoneyPot)
 - Connaitre les failles de sécurité
 - surveiller les attaques sur un réseau :
 - Extérieur
 - Intérieur

Où placer un IDS IPS



Position (1):

- Détection de toutes les attaques
- Problèmes
 - Log trop complet analyse trop complexe :
 - bon pour un Honeypot (pot de miel)

Position (2):

- Placer dans la DMZ
- Détection des attaques
 - non filtrer par le par feu
 - Complexe
 - Non bénigne log clair

Position (3):

- Comme 2 + Attaque interne
- Judicieux car 80% des attaques sont de l'intérieur
 - Trojans
 - Virus
 - Etc.



Un autre IDS particulier: le Honeypot

- Ordinateur ou programme volontairement vulnérable destiné à attirer et à piéger les pirates
- But:
 - Occuper le pirate
 - Découvrir de nouvelles attaques
 - Garder le maximum de traces de l'attaque



Les 2 types Honeypot

- Faible interaction:
 - Les plus simple (ex: Honeyd)
 - Émulation de services sans réel système sous-jacent
- Forte interaction:
 - Utilisation d'un réel système d'exploitation plus ou moins sécurisé



Fonctionnement de Honeyd

- Démon qui crée plusieurs hôtes virtuels sur le réseau
- Simule l'existence de services actifs sur les hôtes virtuels
- Les informations sur l'OS simulé sont issues d'un fichier d'empreinte nmap
- Toutes les connexions entrantes et sortantes sont enregistrées



Les Honeypots

■ Littérature:

- **Virtual Honeypots: From Botnet Tracking to Intrusion Detection**
 - Niels Provos, Thorsten Holz



Aspect pratique

- Etude de différents outils OpenSource
 - Snort
 - Fonctionnement et mise en place
 - Bro
 - Comparaison avec snort
 - Fonctionnement et Mise en place
 - Prelude-IDS
 - Généralité



Snort (NIDS)

- IDS *open source*
- Conçu en 1998 par Marty Roesch racheté par SourceFire
- Le plus répandu
 - + 2 000 000 de téléchargements
- MAJ Temps réel
 - (OINKMAster) Payant via SourceFire
 - Sinon attendre version de mise à jour
 - Bleeding gratuit , CERT



Snort

■ Fonctionnalité

- Permet d'interagir avec le firewall pour bloquer des intrusion (IPS) « snort natif, snort-inline, autres plugins »
- Possibilité de créer ses propres règles et plugins
- Ne permet pas l'envoi d'email ou SMS pour avertir
 - Utilisation d'autre logiciel en complément
 - LogSurfer ou Swatch
- Installation
 - Binaire/sources (Au choix)



Snort : Constitution

■ Modulaire

- Décodeur De Paquets (Packet decoder)
- Préprocesseurs (Preprocessors)
- Moteur De Détection (Detection Engine)
 - ALGO : AHO-CORASICK
- Système d'alerte et d'enregistrement de log (Logging and Alerting System)
- Modules De Sortie (Output Module) :
Possibilité d'enregistrer les logs dans une BDD (MYSQL/PSQL)



Snort : Constitution

■ Configuration sous Unix

– /etc/snort/snort.conf

- 1 Configuration des variables pour le réseau
 - Configuration des reseaux a écouter
 - Configuration des services à logger (http/dns/etc...)
- 2 Configuration des pré-processeurs
- 3 Configuration des plugins de sortie
 - Mysql/psql/ecran/etc...
- 4 Choix des règles à utiliser

– **/etc/snort/rules** (ensemble des signatures)



Les règles Snort

■ Exemples de règles:

- Pour détecter les tentatives de login sous l'utilisateur root, pour le protocole ftp (port 21):
 - `alert tcp any any -> 192.168.1.0/24 21 (content: "USER root"; nocase; msg: "FTP root user access attempt");`
- Tentative d'accès à des sites non autorisés:
 - `alert tcp any any <> 192.168.1.0/24 any (content-list: "adults"; msg: "Adults list access attempt"; react: block;)`



Snort et les interfaces Graphiques

■ ACID/BASE

- Permet de voir les log dans une BDD
- Catégorise
- Lien vers failles de sécurité

Base

Basic Analysis and Security Engine (BASE)

Accueil | Rechercher | Préférences Utilisateur | Logout

[Back]

Interrogé le : Sat January 12, 2008 18:29:12

Meta critères	time >= [01 / 12 / 2008] [any time] ...Effacer...
Critères IP	any
Layer 4 Criteria	none
Critères de contenu (payload)	any

Statistiques

- ◆ Sondes
- ◆ Alertes Uniques (Classifications)
- ◆ Adresses uniques : Source | Destination
- ◆ Liens IP Uniques :
- ◆ Source Port: TCP | UDP
- ◆ Destination Port: TCP | UDP
- ◆ Répartition temporelle des alertes

Affichage des alertes 1-48 sur 204 au total

<input type="checkbox"/>	ID	< Signature >	< Horodatage >	< Adresse Source >	< Adresse Dest. >	< Protocole de niveau 4 >
<input type="checkbox"/>	#0-(3-2)	FTP root user access attempt	2008-01-12 18:24:56	192.168.1.201:55002	192.168.1.150:21	TCP
<input type="checkbox"/>	#1-(3-1)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2008-01-12 18:24:37	82.249.39.73:54874	192.168.1.150:8080	TCP
<input type="checkbox"/>	#2-(1-12659)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2008-01-12 18:24:37	82.249.39.73:54874	192.168.1.150:8080	TCP
<input type="checkbox"/>	#3-(1-12658)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2008-01-12 18:23:44	82.249.39.73:54874	192.168.1.150:8080	TCP
<input type="checkbox"/>	#4-(1-12657)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2008-01-12 18:20:51	82.249.39.73:54874	192.168.1.150:8080	TCP
<input type="checkbox"/>	#5-(1-12656)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2008-01-12 18:10:47	82.249.39.73:54874	192.168.1.150:8080	TCP
<input type="checkbox"/>	#6-(1-12655)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2008-01-12 18:10:47	82.249.39.73:54874	192.168.1.150:8080	TCP
<input type="checkbox"/>	#7-(1-12654)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2008-01-12 18:09:20	82.249.39.73:54874	192.168.1.150:8080	TCP
<input type="checkbox"/>	#8-(1-12653)	[snort] (http_inspect) BARE BYTE UNICODE ENCODING	2008-01-12	82.249.39.73:54874	192.168.1.150:8080	TCP



Le NIDS Bro

■ NIDS Open Source

- Développé par Berkeley (Chercheurs)
- Langage de script propre à Bro
- Utilisation d'expressions régulières dans les signatures
- Possibilité d'exécuter des programmes tiers après détection d'intrusion
 - Exemple: reconfigurer un routeur
- Compatible avec les règles Snort
 - Grâce à snort2bro
- Dynamic Protocol Detection



Le fonctionnement de Bro

- Architecture en 3 couches:
 - Module Packet Capture: sniffe le trafic réseau et l'envoie à la couche supérieure
 - Module Event Engine: Analyse les flux et les paquets
 - Module Policy Layer: utilise les scripts Bro pour traiter les événements et appliquer les politiques



Signature Bro

Exemple de Signature Bro:

```
signature sid-1327 {  
  ip-proto == tcp  
  src-ip != local_nets  
  dst-ip == local_nets  
  dst-port == 22  
  event "EXPLOIT ssh CRC32 overflow"  
  tcp-state established,originator  
  payload ^\x00\x01\x57\x00\x00\x00\x18/  
  payload /.{7}\xFF\xFF\xFF\xFF\x00\x00/  
}
```



Comparatif Snort - Bro

	Snort	Bro
Avantages	<ul style="list-style-type: none">+ nouvelles règles très régulièrement proposées+ nombreux plugins, frontends, consoles de management, ...+ mise en œuvre basique rapide+ beaucoup de documentations+ fichiers d'alertes très complets (header des paquets, lien vers description de l'attaque, ...)	<ul style="list-style-type: none">+ forte customisation -> IDS très difficile à détecter par un pirate+ langage de script puissant+ configuration très simple grâce à un script interactif
Inconvénients	<ul style="list-style-type: none">- configuration essentiellement par édition de fichiers texte- de nombreuses fonctionnalités payantes	<ul style="list-style-type: none">-fichiers d'alertes pas très compréhensibles-peu d'informations dans les rapports d'alertes-documentation incomplète-aucune interface graphique



Prelude-IDS (Hybride)

- IDS hybride 1998:
 - *NIDS* : NetWork Intrusion Detection System ;
 - *HIDS* : Host based Intrusion Detection System
 - *LML* : Log Monitoring Lackey.
- Standard IDMEF (Intrusion Detection Message Exchange Format)
- Possibilité de stocker les logs dans une BDD
 - MYSQL/PSQL
- Supporte :
 - SNORT / NESSUS et + de 30 analyseurs de logs
- Documentation diffuse et peu abondante



Prelude-IDS (Hybride)

■ Framework

- Une bibliothèque de génération de messages IDMEF
- gestionnaire d'événements
- un analyseur de logs et d'une console de visualisation des alertes.



Prelude-IDS (Hybride)

■ Fonctionnement

- Les capteurs remontent des alertes à un manager Prelude.
 - Snort
 - Syslog
 - Prelude lml
- Le manager :
 - Collecte les alertes
 - Transforme les alertes au format de Prelude en un format lisible
 - Permet des contre-mesures à une attaque
- La communication entre les différents programmes se fait au format IDMEF (Intrusion Detection Message Exchange Format).
 - Utilisation du format XML car très générique comme format



Prelude-IDS

■ Composition

- Libprelude (la librairie Prelude) : la base
 - Gestion de la connexion et communication entre composants
 - Interface permettant l'intégration de plugins
- Prelude-LML (la sonde locale)
 - Alerte locale
 - Basée sur l'application à des « objets »
 - Pour la surveillance des systèmes
 - Unix : syslog
 - Windows : ntsyslog.
- Prelude-Manager (le contrôleur)
 - Prelude-manager centralise les messages des sondes réseaux et locales, et les traduit en alertes.
 - responsable de la centralisation et de la journalisation



Prelude-IDS (Hybride)

■ Configuration

- Installation de l'ensemble du framework
- Configuration du manager
 - `/etc/prelude-manager/prelude-manager.conf`
- Configuration de lml
 - `/etc/prelude-lml/prelude-lml.conf`
- Configuration de prelude
 - `/etc/prelude/default/`
 - `Client.conf`
 - `Idmef-client.conf`
 - `Global.conf`
- Ajout de sonde : exemple snort
 - `prelude-admin register snort "idmef:w" x.x.x.x --uid=0 --gid=0`



Prelude-IDS

■ Frontend

- Prewikka (officiel)
- Php-frontend (mort)
- Perl Frontend Prelude (Austère)



Conclusion

- IDS/IPS en plein Essor
- Algorithme de recherche de signature
- Outils essentiels
 - pour surveiller un réseau
 - Pour connaitre les attaques
- Attention
 - Faille de sécurité sur IDS
 - IPS pas encore mature



Bibliographie

- <http://dbprog.developpez.com/securite/ids/>
- Cours CEA (Vincent Glaume)
- Wikipedia.org
- Ecriture de règles:
 - http://www.groar.org/trad/snort/snort-faq/writing_snort_rules.html
- <https://trac.prelude-ids.org/wiki/PreludeHandbook>
- <http://lehmann.free.fr/>