

Détection d'Intrusion

Séminaire Sécurité 01 Réseaux
25 Septembre 2002

Yann Berthier

<Yann.Berthier@hsc.fr>

Hervé Schauer Consultants

<<http://www.hsc.fr/>>



Copyright Hervé Schauer Consultants 2000-2002 - Reproduction Interdite

Détection d'Intrusion

Plan

- Définitions / Principes
- Dispositifs de détection d'attaque / d'intrusion
 - ▶ (IDS, journaux, flux réseaux)
- Limites des IDS
 - ▶ Techniques d'évasion des IDS
- Critères de choix d'une solution IDS
- Conclusions

Détection d'Intrusion

Définitions

- Attaque

- ▶ Découverte systématique d'information, tentative d'intrusion, Déni de Service

- Intrusion

- ▶ Prise de contrôle partielle ou totale d'un système

- IDS

- ▶ HIDS

- ▶ NIDS

Détection d'Intrusion

Définitions (2)

- Détection d'attaque / d'intrusion
 - ▶ Ensemble de mécanismes dont : journaux, activité réseau, IDS

Détection d'Intrusion

HIDS

- Logiciels de scellement d'intégrité
- Logiciels surveillant l'activité système (appels systèmes, processus, etc)
- Pas de faux positifs
- Longs à configurer

Détection d'Intrusion

NIDS

- Sonde écoutant sur le réseau
- Basé (principalement) sur des signatures
- Faux positifs
- Faux négatifs
 - ▶ Signatures pas à jour
 - ▶ Signatures mal conçues
 - ▶ Système en (sur)charge

Détection d'Intrusion

Journalisation

- Centralisation des journaux

- ▶ Journaux des éléments filtrants (gardes-barrières, routeurs)
- ▶ Journaux systèmes
- ▶ Journaux applicatifs

- But :

- ▶ Conserver une copie saine en cas d'incident
- ▶ Pouvoir faire de la corrélation et de l'analyse

Détection d'Intrusion

Journalisation (2)

Outils

- De nombreux outils disponibles (commerciaux ou OpenSource)
- A commencer par les outils standard Unix (grep, perl, sed, awk)

Détection d'Intrusion

Journalisation (3)

Analyse des journaux

- Scans (éléments filtrants)
- Arrêts de démons non prévus
- Connexions d'utilisateurs / escalade de privilèges
- Demande de versions (version.bind CH TXT)
- Erreurs (requêtes Apache 'curieuses')

Détection d'Intrusion

Trafic réseau

- Cisco NetFlow, tcdump, argus, pour enregistrer le trafic
- Flow-tools, argus, Shadow, pour l'analyse
- Etude du trafic
 - ▶ Trafic depuis des serveurs (SYN, SYN-ACK)
 - ▶ Horaires des flux
 - ▶ Durée des flux
 - ▶ Trafic depuis un port 'non connu' vers un port 'non connu'

Détection d'Intrusion

Trafic réseau (2)

- Pas dépendants de signatures
- Permet de mettre en évidence des attaques difficiles à voir avec un IDS
 - ▶ Scans lents, scans distribués, vers, chevaux de Troie et canaux cachés, DoS
- La sauvegarde du trafic permet de procéder à de l'analyse en cas d'incident (forensique)

Détection d'Intrusion

Limites des IDS

- Nécessite des signatures à jour (et bien conçues)
- Pollution des IDS
 - ▶ Dénis de Service sur l'IDS (ou sur l'opérateur)
 - ▶ => Attaque réelle non traitée
- Evasion des IDS
 - ▶ Fragmentation
 - ▶ Insertion de paquets avec des TTL courts
 - ▶ URL encodées

Détection d'Intrusion

Attaques contre les IDS

- Génération de beaucoup de paquets contenant une signature (pollution)
 - ▶ Consommation des ressources de l'IDS (mémoire, disque, CPU)
 - ▶ Perte de paquets
 - ▶ => Déni de Service (IDS ou opérateur)
 - ▶ IDSwakeup
 - ▶ tcpreplay

Détection d'Intrusion

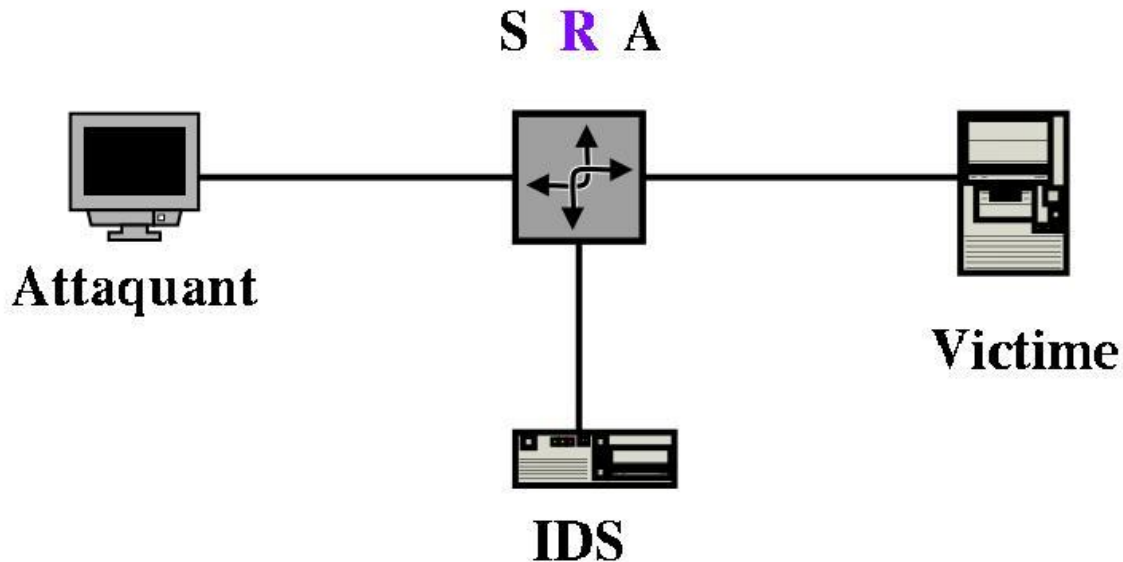
Attaques contre les IDS (2)

- Ptacek et Newsham, 98 : Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
- Phrack54-10
 - ▶ fragrouter
 - ▶ fragroute
- Insertion de paquets avec un TTL court

Détection d'Intrusion

Attaques contre les IDS (3)

- Insertion de RESET avec un TTL court

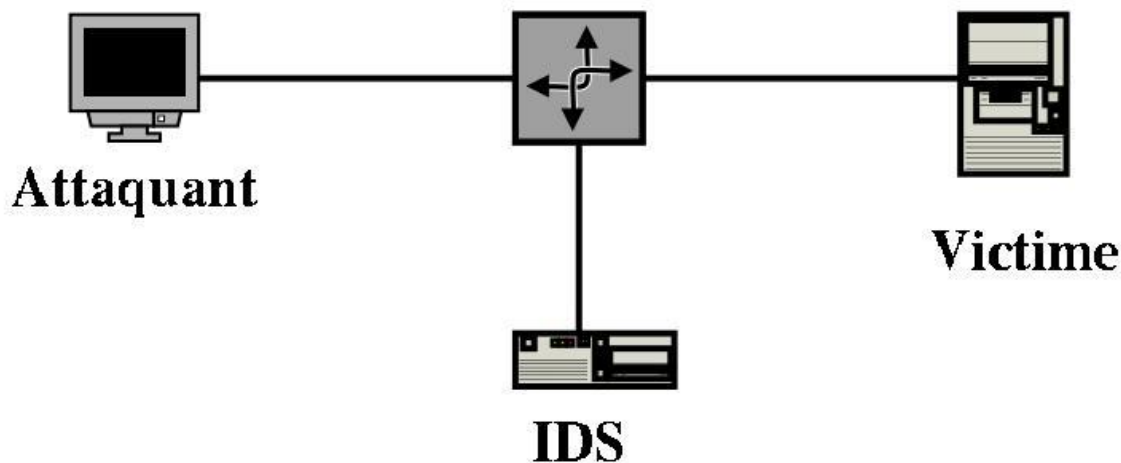


Détection d'Intrusion

Attaques contre les IDS (4)

- Insertion de données avec un TTL court

GET /CGI-BIN/PH 00F HTTP/1.0



Détection d'Intrusion

Attaques contre les IDS (5)

● Whisker

- ▶ Encodage (GET `/%63%67%69%2D%62%69%6E%2F%70%68%66 HTTP/1.0`)
- ▶ Insertion de `./` dans les URL (HEAD `./cgi-bin/./phf HTTP/1.0`)
- ▶ Insertion de HTTP/1.0 avant la fin de la requête
- ▶ Longues URL
- ▶ Utilisation de tabulations à la place des espaces (pas sur IIS)
- ▶ Répartition de la requête sur plusieurs paquets TCP

Détection d'Intrusion

Attaques contre les IDS (6)

- Anonymisation des attaques
 - ▶ Option DECOY de nmap
 - ▶ Utilisation de relais ouverts sur Internet
 - ▶ Attaques coordonnées

Détection d'Intrusion

Critères de choix d'un IDS

- Bien tester un IDS avant de le déployer

- ▶ Résistance aux DoS
- ▶ Ré-assemblage des sessions TCP ?
- ▶ Peut on définir ses propres signatures ?
- ▶ Résistance à la montée en charge
- ▶ Mode ligne de commande ?
- ▶ ...

Détection d'Intrusion

Conclusions

- La détection d'attaque est un processus, pas un produit
- Elle repose entièrement sur des équipes formées, pas sur un produit
- Attention aux réponses automatiques des IDS
 - ▶ Très facile de générer des DoS
 - ▶ Surtout ne pas penser que ça dispense de faire de la sécurité !

Détection d'Intrusion

Liens

● HIDS

- ▶ <http://www.tripwire.org/>
- ▶ <http://www.cs.tut.fi/~rammer/aide.html>
- ▶ <http://la-samhna.de/samhain/>
- ▶ <http://osiris.shmoo.com/>
- ▶ <http://www.prelude-ids.org/>

● NIDS

- ▶ <http://www.snort.org/>
- ▶ <http://www.prelude-ids.org/>

Détection d'Intrusion

Liens (2)

● Journalisation

- ▶ <http://www.enteract.com/~lspitz/swatch.html>
- ▶ <http://www.cert.dfn.de/eng/logsurf/>
- ▶ <http://www.da-experts.com/tlp/>
- ▶ <http://www.logtrend.org/english/>
- ▶ <http://www.conostix.com/ipfc/>

● Outils pour tester les IDS

- ▶ <http://www.hsc.fr/ressources/outils/idswakeup/index.html.fr>
- ▶ <http://www.monkey.org/~dugsong/fragroute/>
- ▶ <http://packetstorm.widexs.nl/UNIX/IDS/nidsbench/nidsbench.html>

Détection d'Intrusion

Liens (3)

- Flux réseau

- ▶ <http://www.tcpdump.org/>
- ▶ <http://www.ethereal.com/>
- ▶ <http://qosient.com/argus/>
- ▶ <http://www.splintered.net/sw/flow-tools/>
- ▶ <http://www.hsc.fr/ressources/outils/nstreams/index.html.fr>