



Détection d'intrusions et analyse forensique

Yann Berthier &
Jean-Baptiste Marchand

Hervé Schauer
Consultants

Agenda

- Agenda
- Préambule
- IDS / IPS : principes - limites
- Au delà des IDS
- Conclusion
- Démonstrations

Préambule

- Détection d'Intrusion : ensemble de processus et d'outils
 - NIDS (Network Intrusion Detection System)
 - HIDS (Host-based Intrusion Detection System)
 - Sondes réseaux
 - Journaux
 - Autre
- Détection d'intrusion \Leftrightarrow (N)IDS
- Seul l'aspect réseau est abordé aujourd'hui

NIDS / IPS

(N)IDS

Principes

- Sonde réseau en écoute de trafic
 - Mode *promiscuous* en environnement concentré
 - Recopie de trafic en environnement commuté
- Génération d'alertes en fonction d'évènements sur le réseau
 - Différentes méthodes de caractérisation des évènements
 - Les IDS implémentent généralement plusieurs méthodes
 - Dans des proportions variables

IDS

Architecture type

- Sondes réseau
 - Génère les alertes
- Consoles de gestion
 - Configuration des sondes
 - Mises à jour (signatures, logiciels)
- Serveur de centralisation
 - Stockage dans une base de données
- Consoles d'alerte
 - Traitement et visualisation et des alertes

IDS

Méthodes

Pattern Matching

- Recherche de motifs dans le trafic
 - Base de signatures
 - A jour
 - Signatures (trop) génériques : faux positifs
 - Signatures (trop) spécifiques : faux négatifs
- Pas d'état de la session applicative
 - X-IDS-Is-Lame-1: mail from: "|
 - X-IDS-Is-Lame-2: vrfy root
 - Génère une alerte sur plusieurs IDS du marché

IDS

Méthodes, cont.

Analyse des protocoles applicatifs

- Connaissance des protocoles définis dans les RFC
 - Doit prendre en compte les interprétations «libres» des RFC - voire les erreurs d'implémentation
 - Base de signature des exceptions
 - Quid des protocoles propriétaires, difficile à implémenter (et a fortiori à décoder), ...
 - Ex : SMB/CIFS, MSRPC

IDS

Méthodes, cont.

Analyse statistique

- Détermination d'un état «normal» du trafic
 - Période d'entraînement
 - **Sur du trafic sain**
 - Caractériser les évolutions normales du trafic
 - Trafic nocturne vs trafic diurne
 - Pics constatés lors de certaines échéances
 - Activité de fin de mois
 - Caractériser les évolutions normales mais non prévisibles
 - **Modification de la topologie réseau**

IDS

Méthodes, cont.

Analyse comportementale

- Détection de comportements suspects
 - Un échec de connexion FTP peut être normal
 - Plusieurs échecs répétés génèrent une alerte

IDS

Limites

- Nombreux faux positifs
- Configuration complexe et longue
 - Nombreux faux positifs après configuration
- Pas de connaissance de la plate-forme
 - De ses vulnérabilités
 - Du contexte métier
 - Intérêt de générer des alertes pour des vulnérabilités non présentes sur la plate-forme ?
 - Lightning Console (Tenable Security), module SecurityFusion de SiteProtector (ISS)

IDS

Limites, cont.

- Les attaques applicatives sont difficilement détectables
 - Injection SQL
 - Exploitation de CGI mal conçus
- Des évènements difficilement détectables
 - Scans lents / distribués
 - Canaux cachés / tunnels

IDS

Limites, cont.

- Pollution des IDS
 - Génération de nombreuses alertes
 - Consommation des ressources de l'IDS
 - Perte de paquets
 - Déni de service contre l'IDS / l'opérateur
 - Une attaque réelle peut passer inaperçue
- Attaque contre l'IDS lui-même
 - Mars 04 : vers Witty exploitant une faille dans le décodeur ICQ d'ISS
 - **Un seul** paquet UDP nécessaire pour une exploitation à distance

IPS

- Situé en coupure de trafic
 - Couplé avec des fonctionnalités de filtrage
 - Les vendeurs de firewall proposent des fonctionnalités de prévention d'intrusion
 - Les vendeurs d'IDS proposent des fonctionnalités de filtrage
- Utilisation des mêmes méthodes que les IDS
 - Pas d'avancée spectaculaire dans les algorithmes ou les méthodes employés
 - Mêmes limites que les IDS

Détection d'Intrusion : Au delà des IDS

Politique de sécurité réseau

Détection des violations

- Sonde placée dans un segment réseau
 - IDS
- Configuration des flux légitimes
 - Flux de résolution vers un serveur DNS
 - Mails vers un relais SMTP
 - Flux applicatifs : HTTP, ...
- Alerte générée pour tous les autres flux
 - Flux FTP depuis un serveur en DMZ
 - Vers un autre serveur dans la même DMZ
 - Vers un serveur sur Internet

Politique de sécurité réseau

Détection des violations, cont.

- Pros

- Ce qui est permis est explicitement configuré
 - Pas de base de signature
 - Pas d'analyse des protocoles
 - Pas de réassemblage de sessions
- Pas de faux positifs
 - Toutes les alertes ainsi générées correspondent à un problème réel

Politique de sécurité réseau

Détection des violations, cont.

- Cons

- Nécessite des DMZ bien conçues
- Nécessite des flux identifiés dans ces DMZ
 - Mais : conditions indispensables pour faire de la sécurité
 - Filtrage effectif
 - Détection d'Intrusion

Flux réseau

- Définition

- Ensemble de paquets possédants des caractéristiques communes
 - IP source, IP destination, protocole, port source (si pertinent), port destination (si pertinent)
 - Autre : label MPLS, numero d'AS
 - Date de début, date de fin
 - Nombre de paquets, nombre d'octets
 - Flux de résolution DNS

19 Apr 04 14:29:30 0 17 192.168.10.75.55866 <-> 192.168.10.49.53 1 1 91 156

- Flux HTTP

19 Apr 04 14:29:45 2 6 192.168.10.75.64699 -> 192.168.10.49.8082 7 7 844 3139

Flux réseau

- Génération de flux
 - Equipements de routage / commutation
 - <http://www.cisco.com/warp/public/732/Tech/nmp/netflow/index.shtml>
 - Sonde PC
 - Argus Serveur (<http://qosient.com/argus/>)
 - Nprobe (<http://www.ntop.org/nProbe.html>)
 - Fprobe (<http://fprobe.sourceforge.net/>)
 - ng_netflow (<http://cell.sick.ru/~glebius/>)

Flux réseau

- Exploitation des flux
 - Clients Argus (ra*)
 - A partir de données au format Argus
 - A partir de données Cisco NetFlow
 - Flow-tools
 - <http://www.splintered.net/sw/flow-tools/>
 - Cflowd
 - <http://www.caida.org/tools/measurement/cflowd/>
 - Rrdtool
 - <http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/>

Flux réseau - Applications

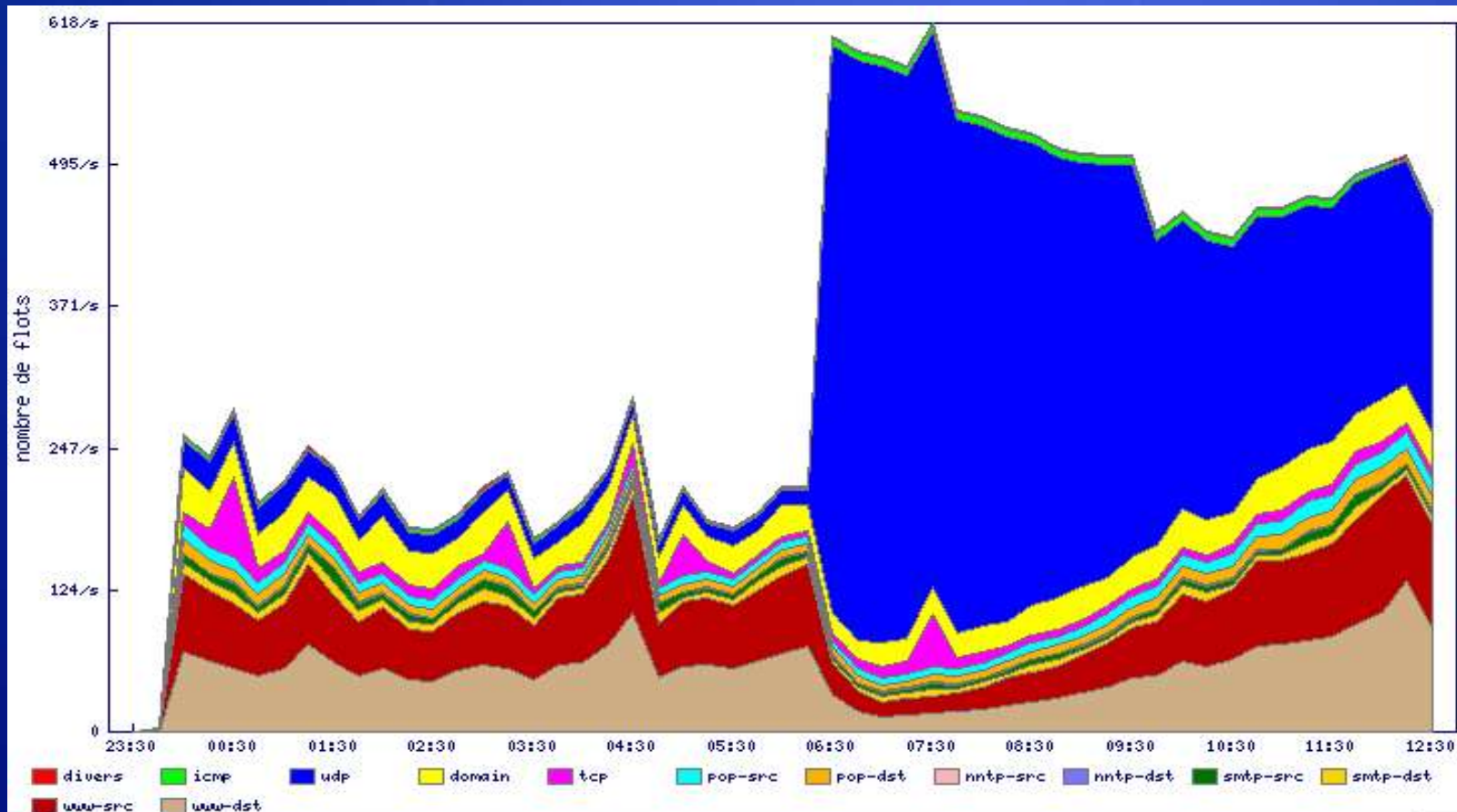
- Incident sur un serveur
 - Flux depuis ce serveur
 - Flux vers ce serveur (port non connu)
 - Application non connue ?
 - FTP ?
 - Backdoor ?
- Scans lents / distribués
 - Tri par adresses destinations après agrégation

Flux réseau - Applications

- Défis de Service / Prolifération d'un ver
 - Augmentation importante du nombre de paquets/seconde
 - Augmentation importante du nombre d'octets/paquet

Flux réseau - Applications

Ver Slammer - nombre de flux/seconde entre le 24 et le 25 Jan 2003



Flux réseau - Applications

- Transferts de données illégitimes
 - Backdoors
 - Chevaux de Troie
 - Tunnels
 - Canaux cachés
 - Canal de communication qui peut être exploité pour transférer de l'information en violation de la politique de sécurité
 - US DOD 1985, Trusted Computer System Evaluation Criteria

Flux réseau - Applications

- Transferts de données illégitimes, cont.
 - Flux à des heures anormales
 - Depuis des postes clients
 - Flux sur des durées importantes
 - Flux de plus de 20 mn depuis des postes clients
 - Flux possédant des caractéristiques 'anormales'
 - Nombre de paquets entrée / nombre de paquets sortie
 - Nombre d'octets entrée / nombre d'octets sortie
 - Nombre d'octets par paquet

Flux réseau - Applications

- Permet de disposer de données réseau dans l'éventualité d'un incident
 - Analyse forensique

Adresses «noires»

Dark address space

- Surveillances des plages d'adresses non occupées
- Pas d'enregistrements au niveau du DNS
- Mécanisme de réponse au niveau réseau
 - Redirection du trafic vers une machine
 - Netcat pour capturer le trafic
 - Utilisation d'outils de simulation de réseau
 - Honeyd (<http://www.honeyd.org/>)
- <http://noc.ilan.net.il/research/riverhead/>
- <http://www.switch.ch/security/services/IBN/>

Adresses «noires»

- Pros

- Tout le trafic à destination de ces adresses est suspect
 - Pas de faux positifs

- Cons

- Détection du bruit de fond d'Internet
 - Scans
 - Vers
 - Mauvaises configurations
 - Retour de flammes (backscatter) dus à l'usurpation des adresses dans une attaque

Conclusion

- Il est possible de faire de la détection d'intrusion sans IDS
- Les IDS déployés sont souvent ineffectifs
- La détection d'intrusion n'est pas un produit
 - Mais des ressources
 - Et du temps
- Des traces réseau sont nécessaires pour faire de l'analyse post-incidents

Références

- Les IDS : Les systèmes de détection d'intrusions informatiques
 - Thierry Evangelista, Dunod, 2004.
- Magazine MISC n°3 (Juillet-Août 2002) : IDS : la détection d'intrusions
- FAQ: Network Intrusion Detection Systems
 - <http://www.robertgraham.com/pubs/network-intrusion-detection.html>

Analyse forensique réseau : Une étude de cas

Analyse forensique réseau

- Analyse réalisée post incident
 - Déterminer la nature d'un incident
 - Déterminer la cause d'un incident
 - Déterminer la portée d'un incident
- A partir de données réseau
 - Trace complète des paquets
 - Données de type flux réseau

Analyse forensique réseau

Etude de cas

- Pot de miel placé sur Internet en sept. 03
- Plusieurs vulnérabilités majeures
- Trace réseau détaillée
 - 24 heures de capture
 - 19 Mo de trace
 - 192 700 paquets

Analyse forensique réseau

Etude de cas

- Analyse par flux de la trace réseau
 - Moment probable de la compromission
 - La vulnérabilité exploitée
 - *Backdoors* installées
 - Utilisation du Pot de Miel
 - Téléchargement de rootkits
 - IRC
 - Scans massifs sur Internet
 - Nombreux /16 : port 139

Analyse forensique réseau

Etude de cas

- Démonstration de l'utilisation d'un outil d'analyse réseau sur la trace capturée :
Ethereal
 - <http://www.ethereal.com/>