POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

INF4420: Éléments de Sécurité Informatique

Sécurité des réseaux : Partie 2

Contenu du cours

- Détection d'intrusion
  - Partie 1 : Différents types d'IDS
  - Partie 2 : Synthèse et exemples
- Protection contre les attaques par inondation
  - Partie 1 : Exemples d'attaques par inondation
  - Partie 2 : Comment se protéger
- VPN
  - Partie 1 : Concept de VPN
  - Partie 2 : VPN IPSec

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Étapes d'une attaque standard sur le réseau

1. Définitions et identification d'objectifs
   - Quelle est la cible ?
2. Reconnaissance
   - Où se trouve la cible ?
3. Caractérisation (« Fingerprinting »)
   - Identification de vulnérabilité
4. Pénétration
   - Exploitation de vulnérabilité
5. Exploitation
   - Garder l'accès
   - Ne pas se faire prendre
   - Accomplir les objectifs

Systèmes de détection d'intrusion (IDS)

- But d'un IDS Réseau :
  - Détecter la présence de vecteurs d'attaque en examinant le trafic réseau
- Méthode de base
  - Le trafic est capturé à un ou plusieurs endroits sur le réseau
  - Examen de chacun des paquets capturés
    - En-tête IP (ICMP, TCP ou UDP)
    - En-tête spécifiques aux applications (e.g. HTTP, FTP)
    - Message ("payload")
  - Un mécanisme de détection est appliqué
  - Des alertes sont générées et enregistrées dans un journal

Systèmes de détection d'intrus (IDS)

- Définitions importantes
- Faux positif
  - Fausse alerte
  - Une alerte est générée par l'IDS alors qu'il n'y a pas d'attaque
- Faux négatif
  - Absence de détection
  - Pas d'alerte alors qu'il y a une attaque

- On peut tester expérimentalement les IDS pour mesurer le taux de faux positifs et de faux négatifs qu'ils génèrent

IDS/IPS

- Le positionnement des IDS/IPS réseau doit se baser sur la capacité des IDS
  - Bande passante
  - Nombre d'alarmes générées
  - Trafic qu'il est possible d'inspecter
  - Règle vs anomalie
- On ne peut pas inspecter ce qu'on ne peut pas « sniffer »
  - Trafic chiffré
  - Trafic passant sur d'autres segments réseau
- On doit placer les IDS en fonction des risques qu'on cherche à détecter
  - Attaque de Hacker
  - Ver informatique
  - Attaque interne

IDS/IPS

- Il existe deux types principaux d'IDS
  - Détection par règle
    - Utilise des signatures pour déterminer si une attaque est en cours. Si le trafic intercepté contient une signature, une alarme est levée.
    - Détecte uniquement des attaques pour lesquelles des signatures existent
  - Détection par anomalie
    - Utilise la déviation statistique à partir de l'utilisation normale (baseline) pour déterminer si une attaque est en cours. Si le trafic intercepté dévie de façon trop grande de la normale, une alarme est levée.
    - Doit avoir une situation normale avec un profil statistique très délimité
- Les deux types fonctionnent à partir d'alertes
  - Un humain doit traiter les alertes
  - Les alertes peuvent être regroupées et combinés

IDS/IPS

- Détection « par règle »
  - Ou par « signature »
  - Examen de chacun des paquets capturés
    - En-tête IP (ICMP, TCP ou UDP)
    - Payload (DPI – Deep Packet Inspection)
  - Application de règles pour détection d'attaques
    - Signatures d'attaques réseaux (e.g. "Land attack")
    - Signatures de code malveillant (e.g. traîneau de NOP, /bin/sh)
    - Signature spécifique à un outil (e.g. message spécifique envoyé par un Botnet pour activer les machines esclaves)

IDS/IPS

- Paradigme général des IDS par « signature »
  - « X évènements de type Y dans un temps Z »
- Exemples de règles possibles
  - 1 paquet dont la « payload » contient une suite de plus de 25 « A » ou « C » (bourrage typique pour les buffer overflow)
  - 1 paquet dont la configuration des drapeaux ne suit pas la spécification du protocole (x-mas scan)
  - 10 paquets provenant de la même source sur des ports différents (port scan)
  - 20 paquets de type SYN vers la même destination sans paquet ACK correspondant (SYN flood)

IDS/IPS

- Limites de l'approche par « signature »
- Limite 1
  - Seules les attaques connues (pour lesquelles une signature existe) seront détectées
  - Ne permet pas de détecter les nouvelles attaques (« zero-day » en anglais)
  - Conséquence : Il est nécessaire de mettre à jour régulièrement le base de signatures (comme un anti-virus)
- Limite 2
  - Les signatures correspondent à des motifs en général fixes.
  - Or, une attaque n'est pas toujours identique à 100%.
  - Le moindre octet différent par rapport à la signature provoquera la non détection de l'attaque
- Limite 3
  - Il est nécessaire d'adapter la base de signatures en fonction du système à protéger
  - Inutile d'appliquer une signature d'attaque pour Windows si on est sous Linux

IDS/IPS

- Détection « par anomalie »
  - On parle aussi d'approche comportementale
  - Examen de chacun des paquets capturé
  - Application de calculs statistiques pour déterminer si une attaque est en cours
    - Variation dans le volume de trafic
    - Communication à des heures anormales
    - Trafic sur des ports « anormaux »
    - Etc.

IDS/IPS

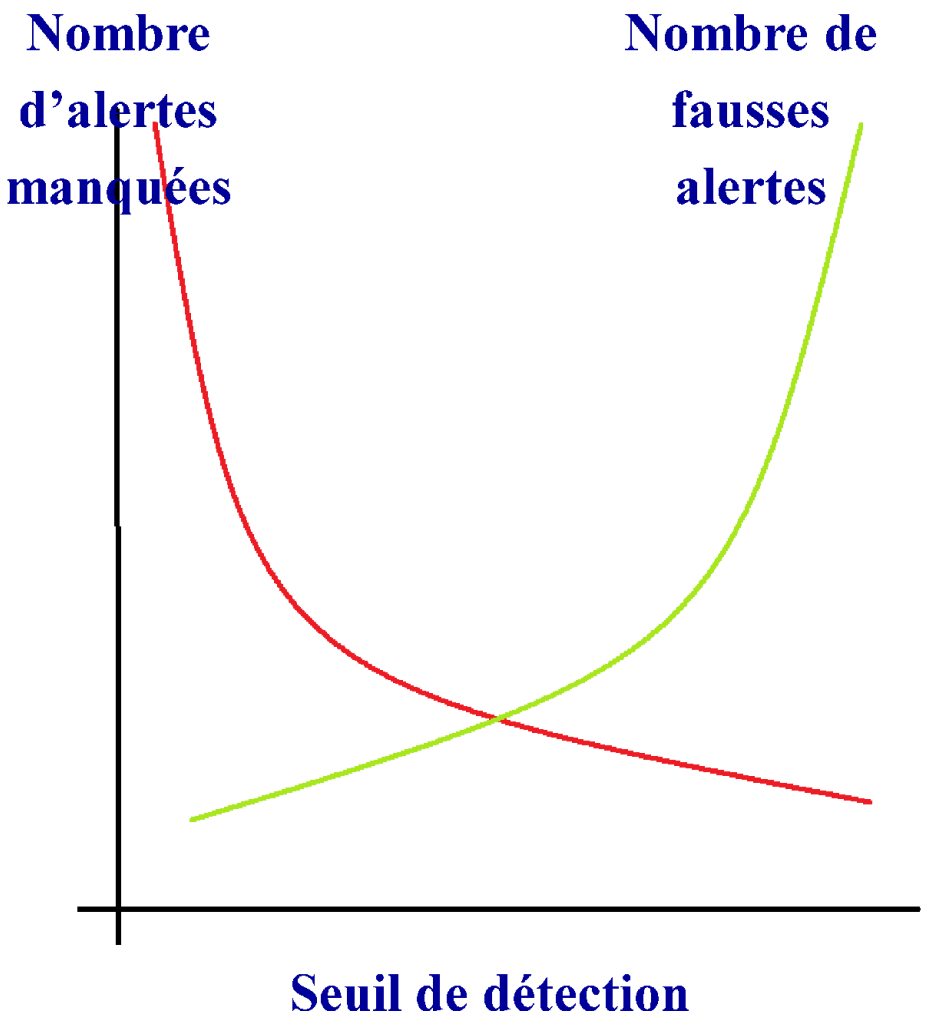
- Paradigme général
  - « X évènements déviant du baseline dans un temps Z »
- Construction d'un profil « normal »
  - Besoin des choisir des attributs représentatifs
  - On parle de métriques ou d'indicateurs (« features » en Anglais)
- Utilisation de techniques d'apprentissage reposant sur l'Intelligence Artificielle
  - Machine Learning
  - Deep Learning

IDS/IPS

- Exemples d'indicateurs
  - Charge CPU
  - Volume de données échangées
  - Temps de connexion sur des ressources
  - Répartition statistique des protocoles et applications utilisés
  - Heures de connexion, …
- Plus la normale est facilement identifiable, plus les attaques seront facilement identifiées comme des « outliers » statistique
  - Éviter des indicateurs qui changent de façon aléatoire
  - Difficulté pour analyser du trafic Web

IDS/IPS

- L'approche comportementale doit être calibrée pour notre réseau
- Si on augmente le seuil de détection, on réduit le nombre d'alertes manquées, mais on augmente le nombre de fausses alertes
- Il faut faire un compromis en fonction du coût opérationnel d'investiguer les alertes



IDS/IPS

- Avantage de l'approche comportementale
  - En théorie, possibilité de détecter de nouvelles attaques (zero-day)
    - Dès lors que la nouvelle attaque conduit à une déviation des indicateurs choisis
  - Dans la pratique, peu de résultats probants
    - Notamment, difficulté de séparer la nouvelle attaque des faux positifs

IDS/IPS

- Limites des approches comportementales
- Limite 1
  - Risque de faux positifs : tout changement dans les habitudes de l'utilisateur provoque une alerte
- Limite 2
  - Nécessite une période de fonctionnement sans intrusion pour mettre en œuvre les mécanismes d'apprentissage
  - Si un pirate attaque pendant cette période, ses actions seront assimilées à un profil utilisateur, et donc passeront inaperçues lorsque le système de détection sera complètement mis en place
- Limite 3
  - Attaque adverse contre l'apprentissage
  - Le pirate peut discrètement intervenir pour modifier le profil de l'utilisateur afin d'obtenir après plusieurs jours ou semaines, un profil qui lui permettra de mettre en place son attaque sans qu'elle ne soit détectée

Types d'implantation

- Network-based IDS (NIDS)
  - Vu dans la partie 1
- Host-based IDS (HIDS)
  - Logiciel ajouté sur un serveur ou un client
  - Objectifs
    - Analyser les logs systèmes et applicatifs
    - Intercepter et analyser les commandes systèmes
    - Détecter les modifications illégales de logiciel (attaque par Rootkit)
  - Avantages
    - Configuration des règles plus précises, étant donné que le contexte est connu
    - Débit plus bas, donc moins demandant en terme de puissance de calcul
  - Peut être intégré dans un anti-virus

IDS/IPS : Tendances actuelles

- Combiner approche par signature et approche comportementale
- Utilisation des techniques de « Machine Learning » pour l'approche comportementale
  - Les réseaux de neurones et le « Deep Learning » sont à la mode
  - Mais on utilise aussi d'autres méthodes
    - Arbres de décision, Random Forest, SVM (Support Vector Machine), Algorithme génétique, etc.
- Intégrer les connaissances métiers dans l'IDS
  - Organisation du travail (workflow)
  - Processus industriel
  - Etc.

IDS/IPS : Tendances actuelles

- « Intrusion Prevention Systems » (IPS)
  - Associe des actions de protection aux alertes
  - Actions typiques
    - Bloquer un port
    - Bloquer une machine ou un sous réseau
    - Rejeter des paquets
  - Peut être dangereux sur des faux positifs
- « Network Appliances »
  - Peuvent intégrer
    - Pare-feu
    - IDS et IPS
    - Détecteur de virus
  - Utilise du matériel spécialisé (e.g. FPGA) pour pouvoir analyser des hauts débits (Gbit/s)

Exemple d'IDS : Snort

- Snort est un NIDS reposant sur l'approche par signature
  - Snort est aujourd'hui la propriété de SourceFire

- Snort est un logiciel « ouvert »
  - Possibilité de définir sa propre base de signatures d 'attaques
  - De nombreuses bases de signatures ont déjà été développées pour Snort
  - Possibilité de réutiliser ou de compléter les bases existantes