

La détection d'intrusions est-elle morte en 2003 ?

Présentation pour



Le 4 mai 2011

Par Eric Gingras Ph.D., directeur de la R&D pour Gardien Virtuel

Contenu

- ✓ Définitions et concepts
- ✓ État de l'art de la détection d'intrusions
- ✓ Réponses de la communauté scientifique aux problématiques
- ✓ Remarques philosophiques sur les mécanismes de protection existants

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

Introduction

- Gartner a annoncé la mort des IDS et IPS en 2003
 - Sont ils morts ?
 - Si oui, ont ils été remplacés ?
 - Par quoi ?
- Confusion !

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

Les risques

- Les logiciels malveillants
 - Virus, vers, chevaux de troie, etc.
- Les fraudes
 - Utilisation non-autorisée de ressources, phishing, etc.
- Les attaques
 - Différents niveaux : réseau, OS, applicatif, etc.

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

Qu'est-ce qu'une intrusion

Définition informatique du terme intrusion¹

« Opération qui consiste à accéder, sans autorisation, à un système informatique ou à un réseau, en contournant ou en désamorçant les dispositifs de sécurité mis en place »

« Une intrusion informatique peut être perpétrée pour diverses raisons, notamment pour modifier ou voler de l'information confidentielle, fausser, contaminer ou détruire les données du système, ou encore exploiter les ressources »

1 – Grand Dictionnaire Terminologique de l'Office québécois de la langue française : <http://www.granddictionnaire.com>

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

Qu'est-ce qu'un IDS

Définition du terme système de détection d'intrusion¹

« Système combinant logiciel et matériel, qui permet de détecter en temps réel les tentatives d'intrusion sur un réseau interne ou sur un seul ordinateur hôte, de neutraliser ces attaques réseaux ou systèmes et d'assurer ainsi la sécurité du réseau d'entreprise. »

1 – Grand Dictionnaire Terminologique de l'Office québécois de la langue française : <http://www.granddictionnaire.com>

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

Détection

- Deux méthodes : la reconnaissance de signatures et la détection d'anomalies.
- La reconnaissance de signatures est une approche consistant à rechercher dans l'activité de l'élément surveillé les signatures (ou empreintes) d'attaques connues.
- De son côté, la détection d'anomalies utilise l'analyse de statistiques du système.

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

Forces et faiblesses (détection)

Signatures :

- Force : Définitions précises (peu de faux positifs)
- Faiblesse : Détecte ce qui est défini (risques de faux négatifs)

Détection d'anomalies :

- Force : Peut théoriquement détecter les menaces inconnues (moins de faux négatifs)
- Faiblesse : Apprentissage vs dynamique (plus de faux positifs)

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

Réaction

- En général, il y a deux mécanismes qui peuvent être utilisés comme modèle pour le développement d'un outil de sécurité : les filtres et les générateurs d'alertes
- Les filtres peuvent agir dans le but d'empêcher à un attaquant d'atteindre ses buts : fermeture de port, isolement d'utilisateur, arrêt d'exécution, etc.
- Un outil peut avoir comme objectif de générer des alertes qui peuvent être catégorisées selon l'impact ou le degré de complétude de l'action présumée malveillante

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

Forces et faiblesses (réaction)

Filtres :

- Force : Réaction plus rapide
- Faiblesse : Risque de déni de service

Mécanismes d'alertes :

- Force : Aucun impact
- Faiblesse : Efforts de supervisions

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

Les IDS réseau (NIDS)

- Principe : capture et analyse des informations circulant sur le réseau.
- Exemple de détection d'intrusion réseau : le monitoring des requêtes ARP (ArpWatch)

Contenu :

Introduction

Définitions

Concepts

État de l'art

- **Solutions existantes**
- **Problèmes**

Réponses
scientifiques

Perspectives

Les IDS réseau (NIDS)

- Snort
 - Demande beaucoup de ressources matérielles et logicielles (multi-thread, capture, stockage)
 - Sélectionner les points d'écoute
 - Comment traiter les communications chiffrées
 - Résultats = alertes

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

Les IDS réseau (NIDS)

- SourceFire
 - Équipement (appliance)
 - Contextualisation passive : ajustement par l'analyse du trafic (mapping du réseau et des utilisateurs par LDAP et autre)
 - Pour le chiffrement : proxy vs au milieu (MITM)
 - Résultats = IPS

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

... mais il n'y a pas que les NIDS

- HIDS : Bâtit une BD contenant les attributs (taille, permission, empreinte, etc.) des objets surveillés. Exemple : Samhain, TripWire, OSSEC, etc.
- Les antivirus : contraintes, attaques sur mesure
- Analyse dynamique au niveau du code exécuté
 - White et black lists
 - Analyse dynamique de la mémoire (ECAT)
 - etc.

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

...peut-on aller plus loin

- L'utilisation d'un grand nombre d'outils apporte le besoin de centralisation pour l'analyse :
 - Format de données universel
 - Point de défaillance et d'engorgement
 - redondance et haute disponibilité
- LIDS et SIEM
 - Visualisation et présentation des résultats (volume)
 - Problèmes du stockage (types de données)

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

**Réponses
scientifiques**

Perspectives

Problématiques abordées

1) Comment détecter les nouvelles menaces

2) Comment réduire le nombre de faux positifs

3) Et tout le reste...

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

Solutions proposées

- IA (Classification) : réseau neuronaux, SVM, chaînes de Markov, logique floue...
- Contextualisation (baseline)
 - Apprentissage
 - Passive (fingerprinting d'OS, users, application)
 - Active (nmap, CMS, etc.)
- Événementiel (temps réel)
 - Monitoring (des preuves ?)
 - Vulnérabilités

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

Innovations

- Pour le trafic chiffré
 - Catégorisation sans déchiffrement
 - Entropie
 - Keystroke
 - horodatage des paquets
 - taille des données
 - S2E2
 - Ajouter : direction du trafic, séquence, dynamique des frappes
 - Déduction : identification du client et de ses buts par l'évaluation d'arbres d'attaques

Innovations

Contenu :

Introduction

Définitions

Concepts

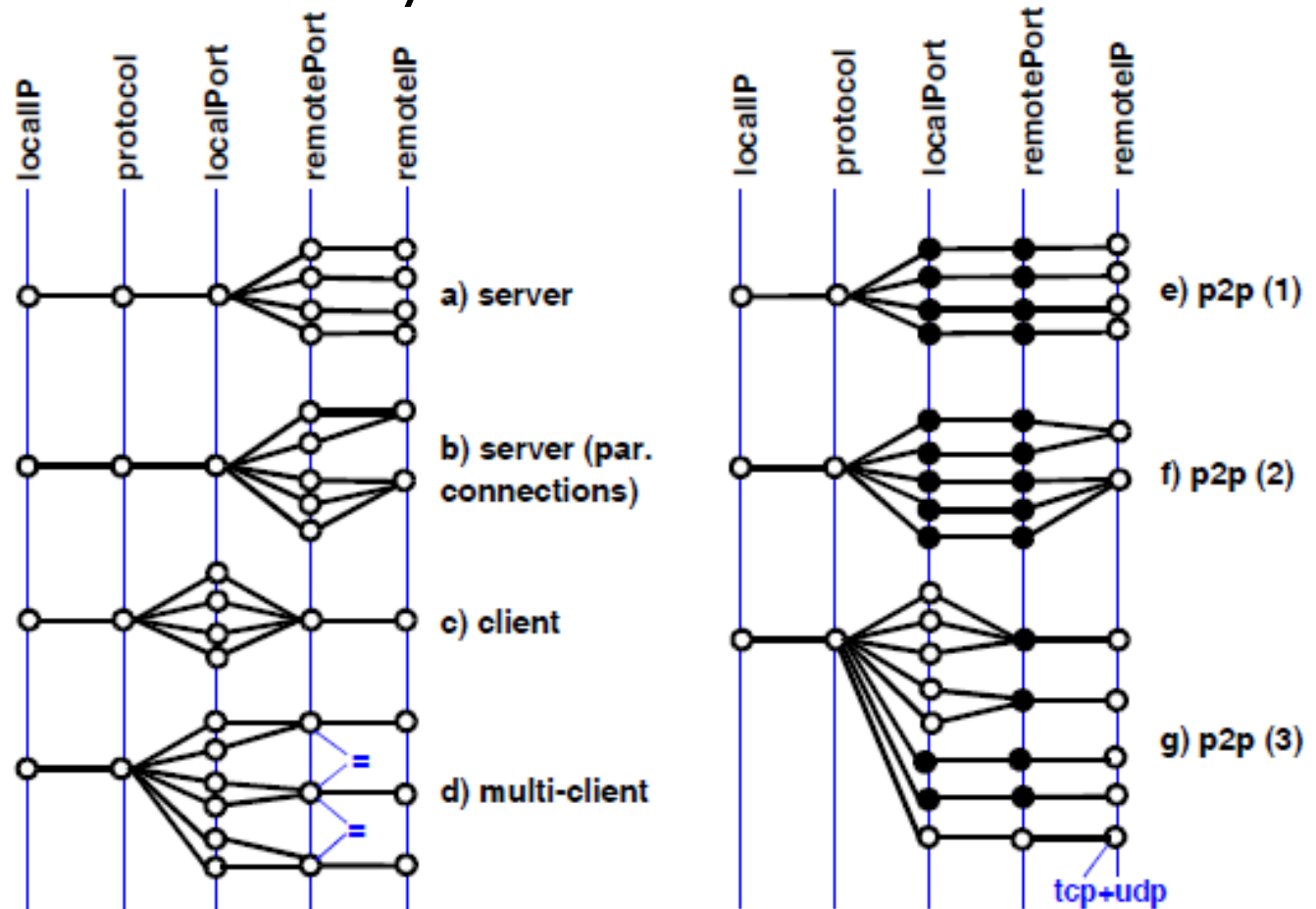
État de l'art

- Solutions
existantes
- Problèmes

Réponses
scientifiques

Perspectives

- Pour l'analyse du trafic



Source : Glatz, Eduard : *Visualizing Host Traffic through Graphs*

La détection d'intrusions est-elle morte en 2003 ?

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

**Réponses
scientifiques**

Perspectives

Où sont ces solutions

- Pourquoi autant de solutions
 - Inutilisées ?
 - Communication et collaboration

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

Conclusions

- Les solutions présentées se comparent à des cadenas, des clôtures, des chiens de garde, etc. L'intervention de l'humain reste donc nécessaire
- La difficulté est de trouver le juste équilibre entre :
 - Les restrictions et l'utilisabilité
 - Les configurations et la granularité des contrôles
- Mais il ne faut pas oublier la difficulté qui réside dans la coordination des solutions

Contenu :

Introduction

Définitions

Concepts

État de l'art

- Solutions existantes
- Problèmes

Réponses scientifiques

Perspectives

Constats et perspectives

- Besoin du changement de paradigme
 - Passer de la syntaxe à la sémantique
 - Passer de l'invincibilité à l'adaptativité
- Modèle collaboratif (TDC)
 - Détection : exemple du modèle épidémique
 - Interprétation
 - Réaction

Venez nous rencontrer



Sur le Web :

www.gardienvirtuel.ca

ou suivez-nous sur Twitter :

GardienVirtuel