Analyse visuelle pour la détection des intrusions

David Pierrot, Nouria Harbi

Université Lumière Lyon 2, Laboratoire ERIC 69676 BRON Cedex, FRANCE
{david.pierrot1,nouria.harbi}@univ-lyon2.fr

Résumé. La démocratisation d'Internet, couplée à l'effet de la mondialisation, a pour résultat d'interconnecter les personnes, les états et les entreprises. Le côté déplaisant de cette interconnexion mondiale des systèmes d'information réside dans un phénomène appelé "Cybercriminalité". Nous proposons une méthode de visualisation de grands "graphes" et l'exploitation d'analyses statiques des flux permettant de détecter les comportements anormaux et dangereux afin d'appréhender les risques d'une façon compréhensible par tous les acteurs.

1 Introduction

De nos jours, le maintien opérationnel d'un Système d'Information est devenu un des critères essentiels pour toute entreprise, ou personne cherchant à délivrer un service, ou simplement souhaitant communiquer. Le côté déplaisant de l'interconnexion mondiale des Systèmes d'Information réside dans un phénomène appelé "Cybercriminalité". Des personnes, des groupes mal intentionnés ont pour objectif de nuire aux informations d'une entreprise, d'une personne voire d'un Etat. Conséquemment, la détection des intrusions doit permettre de protéger le Système d'Information. L'objectif de cet article est de présenter dans un premier temps l'état de l'art en matière de détection d'intrusions et dans un second temps d'aborder les travaux menés afin de faciliter la visualisation des flux. La première partie de cet article sera consacrée à l'étude de l'existant dans laquelle nous présenterons les différentes approches de détection d'intrusions et leurs limites. Ensuite, nous nous intéresserons à la motivation de nos travaux et nous proposerons une solution. Nous détaillerons par la suite, la première phase de nos travaux ainsi que les résultats et nous terminerons par une conclusion et les perspectives.

2 Étude de l'existant

Une multitude d'outils (Antivirus, IDS, IPS, HIDS, Firewall) permettent aujourd'hui de mettre en place une sécurité "relative" pour l'ensemble du Système d'Information. Les principaux risques résiduels sont l'absence de constat en temps réel sur le signalement des comportements anormaux et sur l'exploitation des vulnérabilités. Il convient donc de répondre en fournissant des contremesures dans des délais raisonnables.

2.1 Les différentes solutions de détection d'intrusions

Les systèmes de détection des intrusions sont divisés selon les 3 familles distinctes :

— NIDS (Network Intrusion Detection System) est une sonde chargée d'analyser l'activité réseau du segment où elle est placée et de signaler les transactions anormales (Bhruyan et al (2011)).
— HIDS (Host-Based Intrusion Detection System) est basée sur l'analyse d'un hôte selon les produits utilisés, une HDIS surveille le trafic à destination de l'interface réseau, l'activité système et logiciel, les périphériques amovibles pouvant être connectés.
— HYBRIDES, qui rassemble les informations des NIDS et HIDS et produit des alertes aussi bien sur des aspects réseau qu'applicatifs.

Il existe aussi une variante appelée "IPS" (Intrusion Prevention System) étant capable d'appliquer une politique de sécurité lors d'une intrusion. Un autre concept nommé CIDN [1] décrit par Fung (2011) offre la possibilité de partager des informations au travers un espace communautaire sur Internet. Les différentes solutions s'appuient sur deux méthodes, la première est fondée sur une comparaison d'une tentative d'intrusion par rapport à une base de signatures. Ce type de système recherche dans les trames réseau un schéma qui correspond à une signature connue via de l'extraction de motifs. Il est possible d'ajouter de nouvelles signatures, c'est à dire de créer une expression régulière qui correspondra par son contenu à une activité malveillante ou abusive. La seconde méthode repose sur des modèles comportementaux appelés "profils". Ils sont utilisés pour détecter les comportements déviant des profils définis. Les anomalies peuvent "signaler" une intrusion ou un nouveau comportement. Dans le second cas, il convient d'ajouter ces nouveaux comportements afin de diminuer les " faux positifs". Le concept de détection des anomalies repose sur une analyse statistique et un apprentissage temporel des comportements. Plusieurs principes de mise en place sont disponibles comme "IDES" [2] (Lunt et al, 1992), ou "EMERALD" [3] (Porras et Neumann, 1997).
Le Tableau 1 liste les avantages et inconvénients des différentes solutions de détection. L'intérêt

	Avantages	Inconvénients
NIDS	Alarme en cas d'anomalie Positionnement multiple Temps réel	Signatures à mettre à jour Absorption du trafic Inopérant pour les flux chiffrés Gestion des faux positifs Expertise souhaitée
HIDS	Protège les stations Temps réel	Inefficace contre les attaques sur plusieurs hôtes Différentes configurations selon les systèmes utilisés
Hybride	Diminution des faux positifs Temps réel Corrélation des événements	Sources plus nombreuses, gestion et interprétation des alarmes plus difficiles

TAB. 1: Avantages et inconvénients des IDS "classiques".

de la maîtrise des comportements et des événements de sécurité a même donné lieu à une convergence de plusieurs technologies et outils. Ainsi, la société "Arkoon-Netasq" [4] propose via son produit "Stormshield" [5] une solution capable de détecter les comportements anormaux à destination d'un poste de travail (complétée par des fonctionnalités comme le contrôle des

1. Collaborative Intrusion Detection Networks
2. Intrusion-Detection Expert System
3. Event Monitoring Enabling Responses to Anomalous Live Disturbances
4. Arkoon-Netasq, http ://www.stormshield.eu/
5. Solutions de sécurité de bout-en-bout pour la protection des réseaux

périphériques amovibles, l'application d'une politique de sécurité selon le réseau utilisé : interne, sans fil). Le groupe "Thalès" via son Laboratoire d'Innovation (Lagadec, 2012), propose une solution d'analyse typologique des vulnérabilités du Système d'Information nommée "TVA". Cette solution génère des graphiques qui permettent la définition et la mise en place d'une stratégie pour la prévention des attaques et limitent le plus possible les risques résiduels. Elle permet ainsi un déploiement des Sondes de détection d'intrusions plus efficientes afin de couvrir les infrastructures sensibles et prioritaires.

2.2 Limitation des solutions existantes

Les principales limites des outils présentés dans les chapitres précédents résident dans le fait que l'analyse des événements et journaux systèmes est souvent considérés comme fastidieuse. De plus, ils ne prennent pas encore en compte l'évolution quasi permanente d'un Système d'Information. Par exemple, la sécurité d'un entrepôt de données peut être mise en cause par la non réévaluation du ou des serveurs hébergeant ce dernier. La structuration organisationnelle et l'analyse de risques s'avèrent donc indispensables.

3 Motivations et proposition

La mise en place d'une supervision du Système d'information doit permettre d'analyser les flux de données de type événement et attaque, et d'être en mesure de réagir en temps réel, et ainsi de prévoir les risques encourus par les différents actifs connus et suivis. Notre étude porte sur quatre phases qui se décomposent de la façon suivante :

- Phase 1 : "Monitoring et visualisation" des données réseau, représentation graphique des activités d'un réseau informatique via un modèle de données.
- Phase 2 : "Extraction des profils d'attaque", phase qui s'appuiera sur des méthodes de Data Mining.
- Phase 3 : "Scoring" des risques et phase d'évaluation.
- Phase 4 : Détermination d'un plan d'actions.

3.1 Réalisation de la première phase

Cette phase constitue un tout en soi dans la mesure où la visualisation des données pour les utilisateurs est un enjeu crucial en terme de prise de décisions sur les problématiques de sécurité. Il s'agit du préambule à la "fouille de données" qui sera effectuée dans les phases suivantes. Un des principaux équipements de sécurité est le "Pare-Feu" [6] ou plus communément appelé "Firewall". Il a pour mission comme le décrit Al-Shaer et Hamed (2003) de filtrer, selon une politique fondée sur les flux autorisés à pénétrer dans un réseau par rapport leurs provenances, leurs destinations et les services souhaités (navigation internet, transfert de fichiers, etc...). Par son positionnement, il donne une visibilité totale de l'ensemble des flux. Cet équipement offre aussi la possibilité "d'historiser" vers des journaux les flux ayant été autorisés ou interdits. Il est opportun de capturer les flux réseau à partir de cet équipement et d'exporter les traces de connexion vers un conteneur de données.

6. Équipement de sécurité basé sur le filtrage des entrées/sorties des flux réseau.

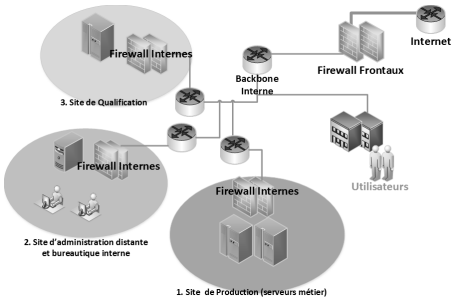

FIG. 1: Schéma du réseau étendu SP1,SQ1,SAB1

3.1.1 Description de l'architecture

Il a été possible de tester la phase 1 sur une architecture réseau d'une entreprise publique dans le domaine de la santé composée de 92 000 employés. Notre étude porte sur 3 réseaux interconnectés au sein d'un réseau étendu (WAN : Wide Area Network) distant géographiquement. Ces derniers sont tous pourvus d'équipements de filtrages, l'objectif est d'être en mesure d'analyser les événements liés aux règles de filtrage via une exportation vers un conteneur de données. La figure 1 détaille sommairement l'architecture étudiée. Afin de simplifier les références aux différents réseaux, le nommage suivant sera utilisé :

— Site de production : **SP1**
— Site de qualification : **SQ1**
— Site d'administration distante et bureautique : **SAB1**

Ces trois sites sont opérationnels [7], les données brutes envoyées en temps réel par l'ensemble des équipements de filtrage sont traitées selon une extraction de motifs .

3.1.2 Description des données

Le réseau SP1 propose des services à destination de **14 millions** de personnes. Les données peuvent être considérées comme sensibles et portent sur une quantité de 9.2 Teraoctets et plusieurs dizaines de millions d'euros par jours. Ces données sont hétérogènes et proviennent de plusieurs sources différentes.
Le contenu des variables listées ci-dessous est exporté vers les conteneurs de données. La phase 1 se focalisera uniquement sur l'analyse et la représentation graphique de ces dernières.

— adresse ip source, adresse ip de destination, port de destination, protocole (udp et tcp)
— date et heure de la connexion
— numéro de la règle du pare feu appliquée, action appliquée par la politique de filtrage.

Le tableau 2 synthétise le volume en nombre de lignes traitées par les équipements de filtrage.

	flux traités par journée	moyenne par minute
SP1	9 886 928	6 865
SAB1	572 272	397
SQ1	20 670	14

TAB. 2: Flux traités par SP1, SQ1, SAB1 en nombre de lignes

7. Pour des raisons de **confidentialité** les adresses IP ont été anonymisées

4 Scénario de visualisation

La représentation graphique de l'ensemble des flux autorisés selon la période souhaitée relève du problème de vision de grands graphes (voir figure 2), mais il est possible d'extraire des "sous graphes" basés sur du "requêtage" qui visent à sélectionner les modalités de certaines variables (adresses source et de destination ainsi que les services et protocoles). En revanche, l'analyse d'un graphique fondé sur les flux rejetés (même agrégés) comme le montre la figure 3 s'avère simple mais aussi efficace. Une adresse IP tente de se connecter à plusieurs autres adresses sur le port "135". Une recherche de répertoires partagés peut être à l'origine de ce type de comportement.

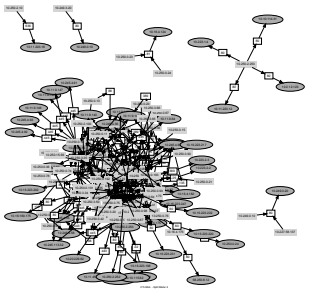

FIG. 2: Exemple de transactions

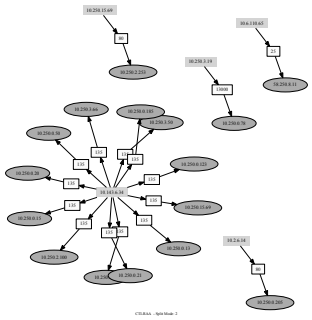

FIG. 3: Exemple de transactions rejetées

4.1 Traitement et résultat

4.1.1 Traitement des données

Il convient de détailler les opérations et configurations mises en place. Les différents moyens décrits dans cette section permettent de réaliser le pré-traitement. Ces derniers dispensent à partir des événements bruts envoyés par les équipements de filtrage un format exploitable via le conteneur de données. Par la suite, un traitement est réalisé via un script Perl [8], créé par nos soins, ayant pour objectif de préparer le résultat des différentes requêtes. Enfin, les programmes issus de la suite Graphviz [9] et du script Afterglow [10] sont utilisés pour la création des graphiques comme démontré par Marty (2008). L'utilisateur [11] n'a en fait besoin que d'un navigateur Internet pour être en mesure de visualiser les flux.

4.1.2 Résultat

A l'issue de la phase 1, Le traitement des informations recueillies sur les différents équipements de filtrage permet de visualiser rapidement les tentatives de connexion depuis plusieurs sources vers plusieurs destinations. Ceci rend possible de soulever des interrogations sur cette transaction et de mettre en place une action de surveillance. D'autres options ont été créées afin d'offrir une visualisation des règles de filtrage les plus utilisées. En cas de doute sur une

8. https ://www.perl.org/
9. Logiciel de visualisation graphique, http ://www.graphviz.org
10. AfterGlow, outil de génération graphique, http ://afterglow.sourceforge.net/
11. Responsables de la sécurité du système d'information, ingénieurs sécurité, administrateurs réseau

adresse Ip, il est possible de lister toutes les activités de cette dernière selon des critères de temps, de destination, de protocoles et de ports utilisés.

5 Conclusions et perspectives

A l'issue de la phase 1, l'ensemble des événements liés au filtrage est exporté en temps réel vers des conteneurs de données. La lecture graphique permet de visualiser les tentatives de connexion depuis plusieurs sources vers plusieurs destinations. Il peut s'agir d'une tentative d'intrusion ou d'une prise de renseignement ou encore d'une mauvaise configuration d'un script. L'inconvénient de la solution réside dans le fait que la surveillance est encore manuelle et demande des connaissances techniques sur l'interprétation des graphiques proposés.

Il convient de poursuivre les phases 2 à 4 à savoir l'utilisation de méthodes de Data Mining sur un espace de représentation graphique. Ces phases permettront de générer des règles d'association en fonction des actifs visés selon plusieurs vecteurs d'attaques. Il conviendrait de créer un système évolutif et adaptatif en temps réel permettant en fonction des changements intervenant sur un système d'information d'offrir une véritable aide à la décision.

Références

Al-Shaer, E. et H. Hamed (2003). Firewall policy advisoor for anomaly detction and rules. *Integrated Network Management, 2003. IFIP/IEEE Eighth International Symposium on*.

Bhruyan, H. et al (2011). Survey on incremental approaches for network anomaly detection. *International Journal of Communication Networks and Information Security 3*.

Fung, C. (2011). Collaborative intrusion detection networks and insider attacks.

Lagadec, P. (2012). Visualisation et analyse de risque dynamique pour la cyber-défense.

Lunt, T. F. et al (1992). A real-time intrusion-detection expert system (ides). Technical report, SRI International, Menlo Park, California.

Marty, R. (2008). *Applied Security Visualization*.

Porras, P. A. et P. G. Neumann (1997). EMERALD: event monitoring enabling responses to anomalous live disturbances. In *1997 National Information Systems Security Conference*.

Summary

The democratization of the Internet, coupled with the effect of globalization, resulting interconnect individuals, states and businesses. The unpleasant side of this global interconnection of information systems is a phenomenon called "Cybercrime". Individuals, groups malicious therefore aim to undermine the integrity of information systems for financial gain or to serve a "cause". We propose a method to visualize large "graphs" and operation of static flow analysis to detect abnormal and dangerous behavior and understand the risks in an understandable by all stakeholders.