NetFlow et ALCASAR

Analyse de flux IP avec le protocole NetFLow

Emmanuel BAUDVIN
Lucien CASSAGNES
Antoine PUISSANT

Enseignant : M. REY

2014 - 2015

Résumé

ALCASAR est un projet libre de contrôle d'accès au réseau, un NAC. Au sein de ce dernier, il est possible de retrouver l'utilisation du protocole NetFlow. ALCASAR bénéficie alors d'une sonde réseau lui permettant d'analyser les flux réseaux le traversant avec beaucoup de finesse.
Durant ce projet, le but est d'assimiler le fonctionnement du protocole NetFlow seul et au sein d'ALCASAR.
Une fois cet apprentissage fait, nous devrons comparer la version de NetFlow présente dans ALCASAR à la dernière version. Cette comparaison devra permettre de savoir s'il est utile de faire évoluer la version d'ALCASAR. En cas de résultats positifs, la mise à jour devra être réalisée et testée.

Table des matières

1 Introduction

1.1 Le projet ALCASAR

Le projet ALCASAR est né suite à une demande d'une entité gouvernementale voulant assurer la traçabilité et l'imputabilité des connexions de tous les utilisateurs connectés à leur réseau.
Après une rapide étude de marché, les responsables de projet se sont rendu compte qu'il n'existait pas de solution libre de droits permettant de remplir les demandes précises de l'entité : intercepter, authentifier, filtrer et imputer l'accès aux utilisateurs à internet.
Ainsi, les chefs du projet ont alors décidé de réaliser eux-mêmes un contrôleur d'accès pouvant répondre aux besoins du projet. C'est ainsi que le projet ALCASAR à vu le jour.

FIGURE 1: Logo d'ALCASAR

Afin de pouvoir réaliser ces fonctions d'interception ou de filtrage, ALCASAR va embarquer plusieurs outils d'analyse de flux. Parmi ces outils, nous allons pouvoir retrouver NetFlow.

1.2 NetFlow

NetFlow est un protocole qui a été conçu par Cisco Systems. Il va permettre de réaliser une surveillance des réseaux en collectant des informations sur les flux IP. Ce produit va permettre à un administrateur réseau de déterminer différentes informations telles que la source et la destination du trafic, le type de service utilisé ou encore la cause de nœuds de congestion.

1.3 IPFIX

A voir : `http://www.bradreese.com/blog/netflow-vs-ipfix-exporter.htm`

2 NetFlow

2.1 Indtoduction

NetFlow est un protocole développé par la société Cisco dans le but de faire une analyse des trames passant au travers de leurs équipements réseau. Ce projet ayant une très grande popularité lors de sa sortie, le protocole devint alors accessible à tous.
Ainsi, ici, afin d'utiliser le protocole NetFlow, nous pouvons retrouver plusieurs parties :

2.1.1 La sonde

La mise en place du protocole NetFlow est ici faite grâce un module noyau, *ipt_NETFLOW*.
TODO
Cette sonde va envoyer toutes ses données à une adresse IP et un port bien spécifique (ici, 127.0.0.1 :2055).

2.1.2 Le collecteur

Afin de récolter toutes les données fournies par la sonde NetFlow, nous devons aussi avoir un collecteur. Son rôle est d'écouter à l'adresse sur laquelle la sonde NetFlow envoie ses données. Il va ainsi réaliser un fichier au format « *NetFlow* » toutes les 5 minutes.
Ici, le rôle du collecteur est réalisé par le daemon *Nfcapd*.

2.1.3 L'interpréteur

Cependant, les données fournies par Nfcapd au format « *NetFlow* » ne sont pas lisible. Afin de palier à cela, il est possible d'utiliser un interpréteur. Dans notre cas, ce rôle est joué par *Nfdump*.
Il est alors possible d'avoir le contenu des captures de la sonde NetFlow à n'importe quel moment.

2.1.4 Le grapheur

Cependant, au sein de l'interface de gestion d'ALCASAR (ACC [1]), il est intéressant de pouvoir retrouver de manière graphique les résultats des captures de la sonde NetFlow.
Afin de réaliser cela, nous utilisons le grapheur Nfsen. Ce dernier va récupérer les données fournies par le collecteur afin de réaliser des graphes représentatifs de l'état des connexion (charges, nombre de connexion, serveurs les plus demandés, etc...).

2.2 Mise à jour

Afin de mettre toute la partie NetFlow à jour au sein d'ALCASAR, nous avons tout d'abord chercher quelles étaient les versions installées sur la dernière version du NAC.

1. ALCASAR Control Center

	Version au sein d'ALCASAR	**Dernière version**
ipt_NETFLOW	1.7.2	2.2-36
Nfdump	1.6.9	1.6.14
Nfsen	1.3.7	1.3.7
Nfcapd	1.6.9	1.6.14

TABLE 1: Comparaison des versions des modules

Comme vous pouvons le voir sur le tableau 1, nous devons mettre à jour la sonde ipt_NETFLOW, Nfdump ainsi ue Nfcapd.
Actuellement, Nfcapd est inclut au sein de Nfdump. Ainsi, nous devons mettre à jour la sonde et l'interpréteur.
Pour cela, nous avons récupéré les sources des deux paquets sur leurs sources officielles :

ipt_NETFLOW `https://github.com/aabc/ipt-netflow`

Nfdump `https://github.com/phaag/nfdump`

Références

[1] ALCASAR. *Projet ALCASAR*. 2015. URL : http://www.alcasar.net/.

[2] AUTHOR. *REF TITLE*. ORG. 2015. URL : http://www.url.com/.