TELECOM SudParis

Détection d'intrusion par approche statistique sur un réseau SDN

Contexte

Un système de détection d'intrusion permet aux administrateurs systèmes de détecter les brèches d'un réseau. Il répond aux problématiques de sécurité auxquelles les entreprises et les administrations font face, notamment dans le cas de réseaux étendus et sensibles.
A ce jour, beaucoup de recherches ont été réalisés concernant des NIDS (Network Intrusion Detection System) en particulier dans le cas de réseaux SDN (Software-Defined Networking). La centralisation logique des contrôleurs d'un SDN est atout certain pour la mise en place d'algorithmes de gestion et d'analyse de trafic. C'est pourquoi les recherches liées à la détection d'intrusion s'effectuent majoritairement sur ce type de réseau. Les recherches ont été conduites dans des conditions spécifiques (systèmes, algorithmes, datasets) en utilisant les outils d'apprentissages statistiques (deep learning) permettant de produire des algorithmes théoriques d'implémentation d'un tel système de détection d'intrusion.
Cependant, les réseaux SDN sont aussi la cible de plusieurs attaques, notamment les attaques DDos (Distributed Denial of Services) qui utilisent les vulnérabilités des plateformes SDN.

Description du projet

Le projet à pour objectif d'implémenter un système de détection complet basé sur des méthodes de DeepLearning et à partir des résultats de recherches issues de différents articles scientifiques parus en 2016 et 2017.
Le projet se focalise sur la mise en application des résultats de recherches dans un système capable de fonctionner en temps réel sur un réseau SDN. La partie DeepLearning du système sera mis en place en suivant les indications des différents articles de recherches et en utilisant des Framework permettant d'implémenter rapidement ces technologies (TensorFlow ou Caffe2 par exemple).
Le projet se focalise sur la gestion des différentes entrées du système de détection et sur la mise en place d'algorithmes de traitement de flux de données permettant d'adapter le modèle de détection en continue. Ce système sera codé en Python.
La deuxième partie du projet consiste à la mise en place d'une interface web permettant d'interagir avec le système de détection, d'afficher les intrusions et de signaler les faux positif.

Pour finir, il est nécessaire d'obtenir un ensemble de données tests montrant l'activité d'un réseau lors de différentes attaques afin de pouvoir réaliser la phase d'apprentissage initiale du système. Il existe actuellement diverses bases de données en ligne permettant de récupérer ces informations, mais elles sont pour la plupart ancienne. Avec l'aide de M.Blanc,

nous espérons obtenir une base de données plus récente de la part de la communauté scientifique.

Livrables attendus

- Prototype d'IDS (Intrusion Detection System) avec une interface graphique permettant d'afficher les intrusions en temps réel
- Compte-rendu
- Poster

Contact

Tuteur principal

- Gregory Blanc (gregory.blanc@telecom-sudparis.eu)

Groupe Cassiopée

- Charles Mure (charles.mure@telecom-sudparis.eu)
- Félix Molina (felix.molina@telecom-sudparis.eu)