SCHOEN Adrien

Rapport de réunion n°1

Date de la réunion : 2/02/2021

Date de la prochaine réunion : 05/02/2021

Ordre du jour : Lancement du stage

1. Ce que le stagiaire a dit

L'objectif de ce stage est de concevoir une méthode d'évaluation d'IDS (détecteur d'intrusion). Pour cela il nous faut du trafic normal et du trafic d'attaque. Nous devons générer ces deux types de trafic. L'objectif et la problématique exacte devront émerger d'une analyse de la littérature scientifique existante.

Nous avons commencé à lire le rapport du doctorant, mais il nous faut faire une analyse plus sérieuse avec des fiches de lecture.

2. Ce que les encadrants ont ajoutés

Ce stage doit être réalisé en autonomie, il ne faut pas hésiter à contacter les encadrants s'il y a un problème, autrement ils supposeront que tout se passe bien.

Il faut que les travaux soit le plus clair et le plus reproductible possible, on pensera notamment à des outils comme Git, Wiki ou bien au MOOC « reproductibilité scientifique »

Les premiers jours consisteront essentiellement en de la lecture d'articles afin de bien cerner le sujet. Il faut que cette lecture soit active et qu'il en résulte des traces écrites (ce qui a été lu, quelles sont les idées…)

La recherche pourra commencer par le rapport du doctorant et se continuer sur ses références afin de se poursuivre sur les documents citant ces mèmes références (à l'aide de Google doc, on peut essayer de trouver les articles citant un papier spécifique)

Essayer de télécharger assez vite les dataset (CICIDS2018 notamment) car ils sont plutôt volumineux.

Nous travaillerons à l'étude de graphe d'attaque, ceux-ci représentent les étapes par lesquels un système passe durant une attaque. Ils peuvent être de plusieurs formes. On peut imaginer un graphe d'attaque où les nœuds seraient les états des privilèges qu'un attaquant aurait sur les différentes machines d'un réseau, et les arcs serait les opérations pour parvenir à ces états.

3. Ce qu'il faut faire pour la prochaine séance

Lire le compte rendu du doctorant et en faire une fiche. Faire de même avec les références qu'il a utilisées

Télécharger les jeux de données

Informer quotidiennement les organisateurs de notre avancement

Essayer de faire le MOOC « reproductibilité scientifique ».