**AVANCEMENT PROJET**

**Détection d’intrusions sur un réseau**

**21/04 – 28/04 : Début**

* Etude du projet, analyse des différentes features dans le dataset grâce aux fichiers donnés.
* La dataset : CIC-IDS-2018 de AWS
* Téléchargement de la dataset puis conversion en fichier csv afin de les exploiter.
* Résultat : 10 fichiers
* Découverte de GitHub

**04/05 : Point avancement 1**

* Chacun a travaillé sur 3 fichiers (nous avons laissé le 10ème car il faisait plus de 3Go)
  + Charles
    - Friday-02-03-2018\_TrafficForML\_CICFlowMeter
    - Friday-16-02-2018\_TrafficForML\_CICFlowMeter
    - Friday-23-02-2018\_TrafficForML\_CICFlowMeter
  + Théodore
    - Thursday-15-02-2018\_TrafficForML\_CICFlowMeter
    - Thursday-22-02-2018\_TrafficForML\_CICFlowMeter
    - Thursday-01-03-2018\_TrafficForML\_CICFlowMeter
  + Cécile
    - Wednesday-14-02-2018\_TrafficForML\_CICFlowMeter
    - Wednesday-21-02-2018\_TrafficForML\_CICFlowMeter
    - Wednesday-28-02-2018\_TrafficForML\_CICFlowMeter
* Analyse du fichier 🡪 génération d’un Report Profiling pour chaque dataset grâce à la librairie Pandas Profiling
  + On a pu voir les différents éléments présents dans chaque features et leur nombre d’apparition
  + On a remarqué que pour trois fichiers, le type de toutes les colonnes était ‘objet’, ainsi nous n’avons pu en tirer aucun résultat. Voici les trois fichiers à mettre de côté pour le moment :
    - Wednesday-28-02-2018\_TrafficForML\_CICFlowMeter
    - Thursday-01-03-2018\_TrafficForML\_CICFlowMeter
    - Friday-16-02-2018\_TrafficForML\_CICFlowMeter
  + On a donc pu en tirer comme conclusion quelle features retirer car l’ensemble de la feature a des valeurs nulles
* Voici les 10 features à supprimer pour les 6 datasets restantes :
  + Bwd PSH Flags
  + Fwd URG Flags
  + Bwd URG Flags
  + CWE Flag Count
  + Fwd Byts/b Avg
  + Fwd Pkts/b Avg
  + Fwd Blk Rate Avg
  + Bwd Byts/b Avg
  + Bwd Pkts/b Avg
  + Bwd Blk Rate Avg
* Intrusions présentes pour chaque fichier avec leur nombre d’apparition, et aussi les intrusions bénignes :
  + Wednesday-21-02-2018\_TrafficForML\_CICFlowMeter
    - DDOS attack-HOIC 686012
    - Benign 360833
    - DDOS attack-LOIC-UDP 1730
  + Wednesday-14-02-2018\_TrafficForML\_CICFlowMeter
    - Benign 667626
    - FTP-BruteForce 193360
    - SSH-Bruteforce 187589
  + Thursday-22-02-2018\_TrafficForML\_CICFlowMeter
    - Benign 1048213
    - Brute Force -Web 249
    - Brute Force -XSS 79
    - SQL Injection 34
  + Thursday-15-02-2018\_TrafficForML\_CICFlowMeter
    - Benign 996077
    - DoS attacks-GoldenEye 41508
    - DoS attacks-Slowloris 10990
  + Friday-02-03-2018\_TrafficForML\_CICFlowMeter
    - Benign 762384
    - Bot 286191
  + Friday-23-02-2018\_TrafficForML\_CICFlowMeter
    - Benign 1048009
    - Brute Force -Web 362
    - Brute Force -XSS 151
    - SQL Injection 53