Projet : Attaque adverseriale de réseau , système de détection d'intrusion par Machine Learning

Objectif : Modifier certaines features afin de tromper le modèle analysant le réseau.

Public visé : Néophyte au sujet des attaques adverseriales utilisant du machine learning

Etapes:

1) Trouver des datasets : bruit, features, nb de packets ect (CICIDS2017,UNSW-NB15)
2) - Utilisation de Python, Pytorch et autre bibliothéque de Machine Learning
   - Conception d'un baseline de modèle de ML pour plusieurs types de modèles (Random Forest, Resnet etc, attaque 101)
   - Prétraitement des données : normalisation, sélection (étude entropique par ex)
3) Génération d'attaques adverseriales :
   - Perturber les transferts, packets etc
   - déterminer une heuristique
   - Perturbations réalistes
4) Mesurer les performances avant et après attaques
   - Visualisation et Analyse
   - atteinte des frontières de détections
5) Défense:
   - Analyse de la robustesse vs performances

Livrable : Jupyter + rapport