Compte rendu :
état de l'art IDS

Nous avons fait des recherches sur le différents types d'IDS pour mieux comprendre les méthodes de détections d'attaques et pouvoir les incorporer dans notre outil.

Ce qui a été fait :

- Recherche sur les différents type d'IDS (HIDS & NIDS)
- Recherche sur les différentes implémentations (stream-based, connexion-based)
- Recherche sur les différents types de signatures
- Recherche sur les faux positifs et comment les limiter
- Recherche d'IDS déjà existant (SURICATA, POSEIDON, SNORT)

Ce qu'il reste à faire :

- Approfondir les implémentations des signatures
- Comprendre les méthodes d'évasion