

Auteurs : DE VOS Loan – IBOS Corentin – MANDON Anaël

CONTEXTE ET OBJECTIF

SAFRAN Electronics & Defense est l'une des dix entités du groupe international **SAFRAN** opérant dans le domaine de l'aéronautique, de l'espace et de la défense.



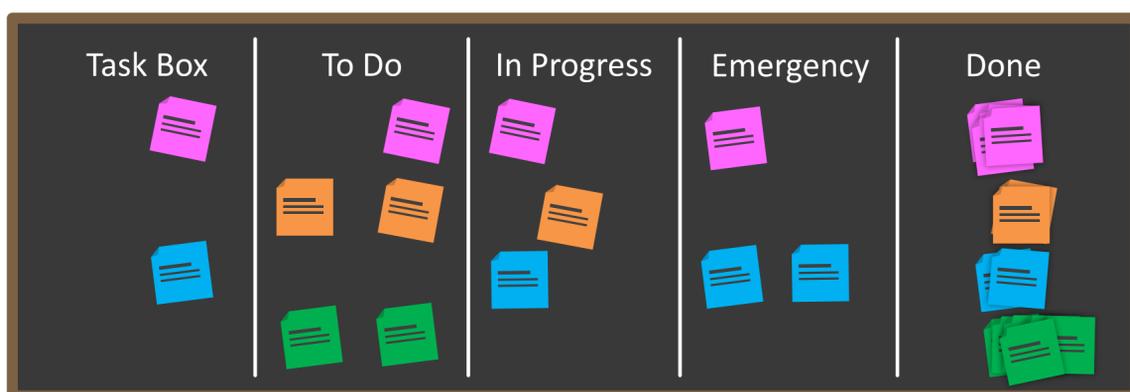
Safran ED a besoin de développer des outils de test afin de s'assurer de la sûreté et du bon fonctionnement de ses équipements et de ses systèmes en cas d'attaque potentielle.

L'outil permettra à la red team de l'entreprise d'identifier de potentielles vulnérabilités dues à des attaques Man In The Middle. Les enjeux de ce projet sont de concevoir et développer un outil de test étant le moins visible possible sur le réseau et implémentant deux parties majeures : TLS 1.3 et la spécification 802.1X.

MÉTHODES ET DÉVELOPPEMENTS



Le projet a été structuré avec un tableau Kanban dans lequel nous avons placé toutes les tâches à accomplir. Celles-ci sont classées en quatre catégories différentes correspondant aux quatre couleurs de post-it : *Documentation & Livrable, Logistique, Veille, Développement & Tests.*



Afin d'assurer la réalisation des tâches dans le temps imparti, nous avons utilisé la méthode de *Test Driven Development*.

Des réunions matinales quotidiennes ont permis de définir l'attribution des missions.

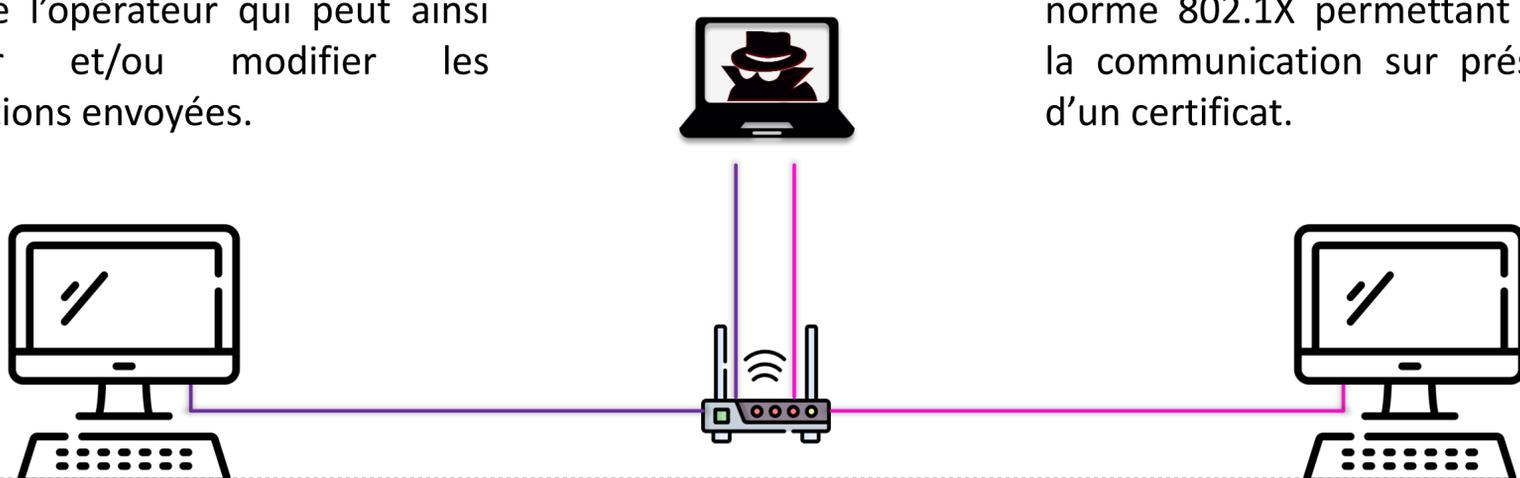
Le développement s'est fait en Python afin de modifier le logiciel open source choisi par l'équipe et l'entreprise : Mitmproxy. Les fonctionnalités ajoutées ont ensuite été présentées à l'entreprise lors des réunions pour être validées.



RÉSULTATS ET CONCLUSION

Dans la solution finale, un routeur GL.iNet Beryl détourne le trafic vers le PC de l'opérateur qui peut ainsi observer et/ou modifier les informations envoyées.

Le routeur implémente les fonctionnalités nécessaires à la norme 802.1X permettant l'accès à la communication sur présentation d'un certificat.



MOTS-CLÉS : Man In The Middle, 802.1X, Routeur, Python, TLS 1.3