Projet

Projet 1 (Altérants)

- Rapport du TP 5 (inline hooking)
- Travail à rendre du TP6

Projet 2 (non Altérants)

Création d'un Malware sous Windows.

Le Malware, une fois exécuté, devra:

- s'injecter, injecter une dll dans un processus Windows en cours d'exécution, ou le remplacer en utilisant une des techniques vues en cours.
- Modifier la base de registre pour que le malware se lance à chaque redémarrage de la machine
- Mettre en place une porte dérobée recevant des commandes d'un serveur distant (de préférence via un commentaire contenu dans une page web)

Faire évoluer le Malware

- afin que cette fois-ci il s'injecte dans le processus LSASS dans le but de récupérer le contenu du fichier SAM et le renvoyer vers le serveur distant
- afin qu'il prenne en charge une méthode d'anti-débogage

Outils: Visual Studio, WDK

Liens:

https://www.codeproject.com/Articles/1091349/Detect-SAM-File-Corruption-under-Windows-Part

http://www.cqure.net/tools/patches/pwdump2_history.patch