

TP 6 : Comprendre l'outil d'analyse

Présentation

CFF Explorer

Avantages:

- gratuit
- on peut éditer les fichiers
- analyse complète

Inconvénients:

- seulement Windows
- installation obligatoire
- interface ancienne

Pas portable / Windows

PE Studio

Avantages:

- portable (juste dézipper)
- facile
- code couleur pour voir si suspect
- bien pour sécurité

Inconvénients:

- seulement Windows
- pas d'édition possible
- version gratuite limitée

Portable / Windows

Tuto PE Studio

Installation

Dézipper et lancer pestudio.exe

Utilisation

- 1) Ouvrir fichier Glisser le .exe dans la fenêtre
- 2) Vérifier couleur (onglet file) Vert = ok / Jaune = suspect / Rouge = dangereux
- 3) Infos (onglet headers) time-date-stamp = date création subsystem = type programme

4) Sections (onglet sections) .text = code programme .data = données

.rsrc = ressources

5) Imports (onglet imports) Liste DLL utilisées Rouge = fonction suspecte

Test avec calc.exe

Ouvrir C:\Windows\System32\calc.exe Résultat: vert, sections normales, rien de bizarre