TP N°5 : Etude du Format PE

1) Le PE (Portable Executable) est le format de fichier exécutable utilisé par Windows. Il structure les programmes pour que le système puisse les charger et les exécuter en mémoire.

2) Extensions de fichiers PE : .exe, .dll, .sys, .ocx, .scr

3) Signature HEXA **:** `4D 5A` (MZ) au début du fichier, puis `50 45 00 00` (PE\0\0) dans l'en-tête PE

4)Systèmes d'exploitation **:** Windows uniquement.

5) Si Windows ne reconnaît pas le format PE**,** le fichier ne s'exécute pas, message d'erreur "n'est pas une application Win32 valide".

6) TimeDateStamp - Localisation : Dans le PE Header (IMAGE_FILE_HEADER)
TimeDateStamp - Signification : Date et heure de compilation du fichier (timestamp UNIX)

Oui, c’est utile pour l’analyse de fichier car :

- Permet de détecter des fichiers suspects (dates incohérentes)
- Analyser l'âge du malware
- Vérifier l'authenticité

7) Nombre de sections : Maximum 96 sections

8) La partie de la section est dans le .text (ou .code)

9) Un packet est logiciel qui compresse/chiffre un exécutable. On l’utilise pour :
- réduire la taille
- protéger le code (anti-reverse engineering)
- cacher des malwares

10) Logiciels d'analyse PE :
- PE Explorer
- CFF Explorer
- PEview
- PEiD
- Detect It Easy (DIE)
- HxD (éditeur hexa)