TP4 : Comparaison des types d’analyse

A partir du lien donné, vous déterminez:

→ les avantages et les inconvénients de l’analyse statique et de l’analyse dynamique
→ Les logiciels gratuits pouvant être utilisés pour réaliser les analyses
→ Lien : *https://fr.wikipedia.org/wiki/Analyse_des_logiciels_malveillants*

Analyse statique

- **Avantages** :
    - Pas besoin d’exécuter le programme → pas de risque.
    - Rapide pour analyser beaucoup de fichiers.
    - Permet rétro-ingénierie et création de signatures.
- **Inconvénients** :
    - Contournée par obfuscation, packing, chiffrement.
    - Fausse vision du comportement réel → faux négatifs.
    - Risque de faux positifs.

Analyse dynamique

- **Avantages** :
    - Observe le comportement réel du malware.
    - Détecte obfuscation, packing, chiffrement.
    - Utile pour malwares inconnus ou “zéro-day”.
- **Inconvénients** :
    - Nécessite environnement sécurisé (sandbox/VM).
    - Lent et gourmand en ressources.
    - Ne montre que ce qui s’exécute → parties du code non testées peuvent passer inaperçues.
    - Certains malwares détectent la VM et se cachent.

Outils gratuits

- **Statique** : Ghidra, IDA Free, désassembleurs, debuggers, radare2 analyseurs de chaînes/imports.
- **Dynamique** :
    - Process Monitor, Process Explorer
    - LTRACE

- PTRACE
- Wireshark
- GDB
- Regshot
- Sandbox gratuits (Norman Sandbox, ThreatExpert, Ether)
- Volatility (analyse mémoire)