# Malware Development for Dummies

**Exercice 3**

**1) Objectif**
Le but était de montrer comment rendre un code injecté plus discret pour éviter la détection par les antivirus. J'ai voulu tester le fait de chiffrer le payload puis le déchiffrer seulement au moment de l'exécution.

**2) Outils utilisés**
J'ai repris le même shellcode mais je l'ai chiffré avec XOR.

**3) Méthodologie**

- J'ai créé un petit programme qui chiffre le shellcode avec une clé XOR.
- Ensuite j'ai fait un programme principal qui déchiffre le shellcode seulement au moment de l'utiliser.
- Il cherche le processus cible, réserve la mémoire, injecte le shellcode puis l'exécute.

**4) Résultat**
Les tests montrent que le programme fonctionne et exécute le shellcode tout en étant moins détecté par certains antivirus. Le processus cible continue de fonctionner normalement.

**5) Conclusion**
Cet exercice m'a montré que même un simple chiffrement peut rendre un payload plus difficile à détecter. Comprendre ces techniques est important en cybersécurité pour savoir comment fonctionnent certaines attaques et comment s'en protéger.