Module « exploits »

- Les codes d'exploitation sont très liés
  - À la version du système
  - À la langue du système (notion d'offset)
- Les conséquences d'une mauvaise prise d'empreinte
  - Code d'exploitation ne marche pas
    - Cas d'une mauvaise version
    - Mauvaise langue (pour Windows notamment)
  - Crash de l'application
    - Code d'exploitation pas toujours fiables à 100%
  - Crash du système
    - Cas de quelques codes d'exploitation (sous Windows notamment)

Charges utiles « payloads »

- Shell_*_tcp
  - Obtention d'une ligne de commande
  - Connexion vers la cible : « `bind` » ou depuis la cible : « `reverse` »
- Windows
  - `adduser` : ajout d'un utilisateur sur le système distant
  - `download_exec` : envoi et exécution d'un programme
  - `exec` : exécution d'une commande distante
  - `dllinject` : injection d'une DLL dans un processus
    - Exploitation entièrement en mémoire, aucune trace sur le disque
    - `vncinject` : injection d'une DLL faisant office de serveur VNC
  - `passiveX` : injection d'un contrôle ActiveX dans *Internet Explorer*
  - `meterpreter` : « meta-interpreter »