Sessions

- Création d'une session pour chaque exploitation réussie
  - Mise en arrière-plan
  - Permet les exploitations parallèles
- Interaction avec les sessions
  - `sessions -l` : liste les sessions
  - `sessions -i <numéro>` : met la session sélectionnée en avant plan
  - `sessions -k <numéro>` : termine la session sélectionnée
  - Dans une session
    - `CTRL+C` : pour la quitter
    - `CTRL+Z` : pour la mettre en arrière plan

Meterpreter

- Fonctionne exclusivement en mémoire
  - S'injecte dans le processus compromis
  - DLL Windows injectée en mémoire par le module `dllinject`
  - N'écrit rien sur le disque et ne crée pas de nouveau processus
  - Les communications sont chiffrées
    - Mode client-serveur (serveur sur la cible)
    - Protocole TLV (type-Length_Value)
- Le code serveur doit être le plus léger possible
  - Majeure partie des traitements concentrée sur la partie cliente
  - Chargement à la volée des extensions sur la partie serveur sans à avoir à le reconstruire
  - L'extension `stdapi` est chargée par défaut. L'extension `priv` est chargé si le module dispose des droits d'administration