# 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

# Meterpreter

- Actions possibles par défaut : module « `StdApi` »
  - Exécution et manipulation de commandes
  - Interactions avec le registre et le système de fichiers
  - Information sur le système et les interfaces réseaux
  - Création d'un tunnel TCP
  - Ajout de script d'automatisation
- Extensions meterpreter
  - « `priv` » : empreintes de mots de passe, dates d'accès aux fichiers
  - « `incognito` »: permet d'usurper l'identité d'un utilisateur connecté
  - …