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
  - …

Meterpreter : module « stdapi »

- Commandes de base
  - Toutes les commandes sont exécutées dans des « `channels` »
    - `channel -l` : liste les canaux actifs
    - `close` : ferme un canal
      - `close <channel>`
    - `interact` : permet l'interaction avec un canal (`CTRL+C` pour en sortir)
      - `interact <channel>`
    - `read/write` : lit/écrit depuis/dans un canal
      - `read<channel> / write <channel>`
  - `migrate` : migre le serveur meterpreter dans un autre processus
  - `run` : exécute un script meterpreter
  - `use priv` : charge l'extension « `priv` »