Meterpreter : module « stdapi »

- Commandes système
  - `sysinfo` : informations générales sur le système
  - `execute, kill` : exécution et arrêt de processus
    - `execute -f <commande> -a <paramètres>`
    - `execute -f cmd.exe -i -H`
    - `kill <pid>`
  - `getpid, getuid, ps` : informations sur les processus du système
  - `reg` : modification et accès à des clés de registre
    - `reg enumkey -k <clé>`
    - `reg queryval -k <clé> -v <valeur>`
    - Mais aussi `setval, deleteval, createkey, deletekey`
  - `reboot, shutdown`

Meterpreter : module « stdapi »

- Interactions réseau
  - `ipconfig` : liste les interfaces réseau et leur configuration
  - `Route` : informations sur les routes du système
    - `route [list]`
    - `route add [sous-réseau] [masque] [passerelle]`
    - `route del [sous-réseau] [masque] [passerelle]`
- `portfwd` : création de tunnels au travers de la cible
  - Fonctionne comme un tunnel SSH
    - `portfwd list`
    - `portfwd add -l <port-source> -r <ip_destination> -p <port_destination>`
    - `portfwd del -l <port-source> -r <ip_destination> -p <port_destination>`