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 »

Meterpreter

- Inject the meterpreter server DLL via Reflective Dll Injection payload (staged):
  - Reverse_http(s)
  - Reverse_https_proxy
    - Proxy http + proxy tor hidden service
  - Reverse_ipv6_http(s)
  - Reverse_ipv6_tcp
  - Reverse_nonx_tcp
    - Contournement de la protection du bit NoExecute (windows DataExecutionPrevention)
  - Reverse_ord_tcp
    - Avantage: marche sur des windows 9x
    - Inconvénients: moins stable et dépend de la dll ws2_32.dll
  - Reverse_tcp(dns)
    - Par ip (tcp) ou nom de domaine(tcp_dns)
  - Reverse_tcp_allports
    - Connect back sur les 65535 ports de l'attaquant (?)
  - Reverse_tcp_rc4(dns)
    - Chiffrer les coms avec l'algorithme de chiffrement rc4