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

Modules « auxiliary »

- scanners
  - `DCE-RPC` : services RPC Windows
  - `UDP` : scanner de services UDP
  - `HTTP` : versions et tests des requêtes PUT et DELETE
  - `Oracle` : version et comptes Oracle
  - `MS SQL Server` : informations et test du compte SA
  - `MySQL` : version et compte MySQL
  - `SMB` : version, énumération et bruteforce
- dos
  - Windows, Solaris, FreeBSD et les pilots de cartes Wi-Fi
- voIP
  - Module « SIP INVITE Spoof »
- Server
- fuzzers, admin, sqli …