

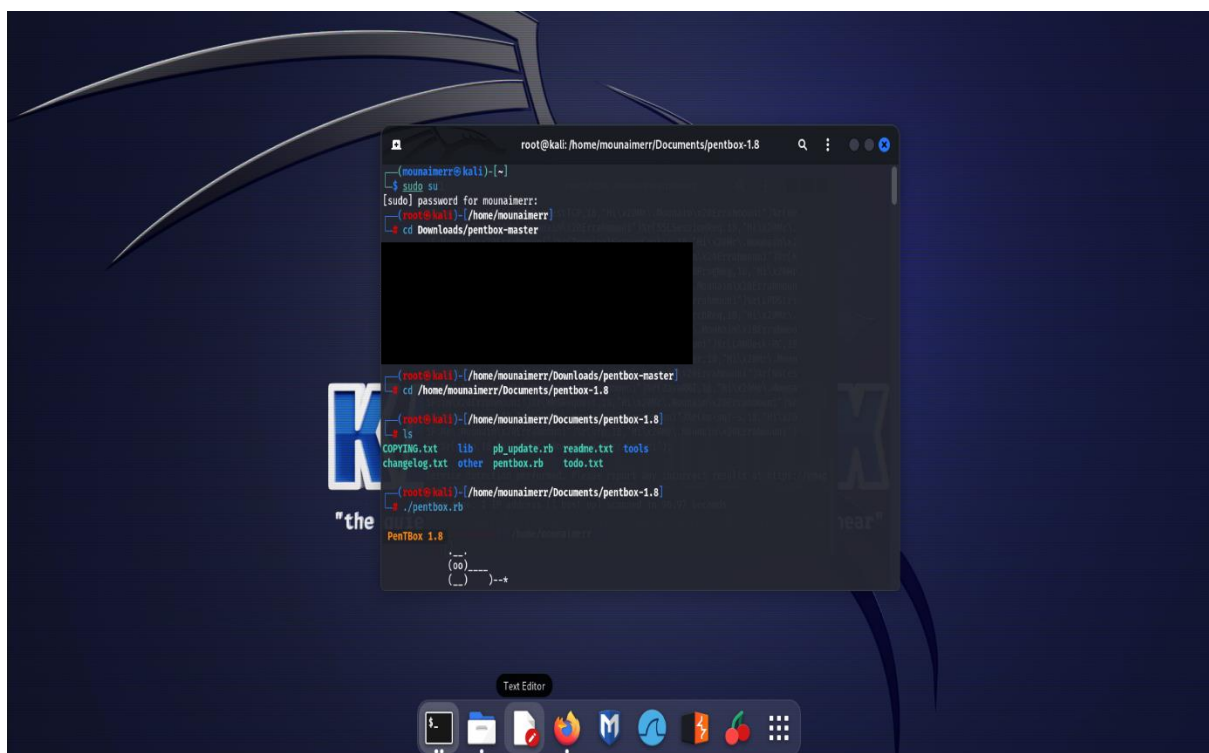
First of all, you have to do all this in your virtual machine using Linux.

The first step is downloading the file from github.

After downloading the file you have to extract it because it is a zip file.

After doing this you have to follow what is written in the next steps.

You have to change your directory from the user to the root, as you can see in the first line.



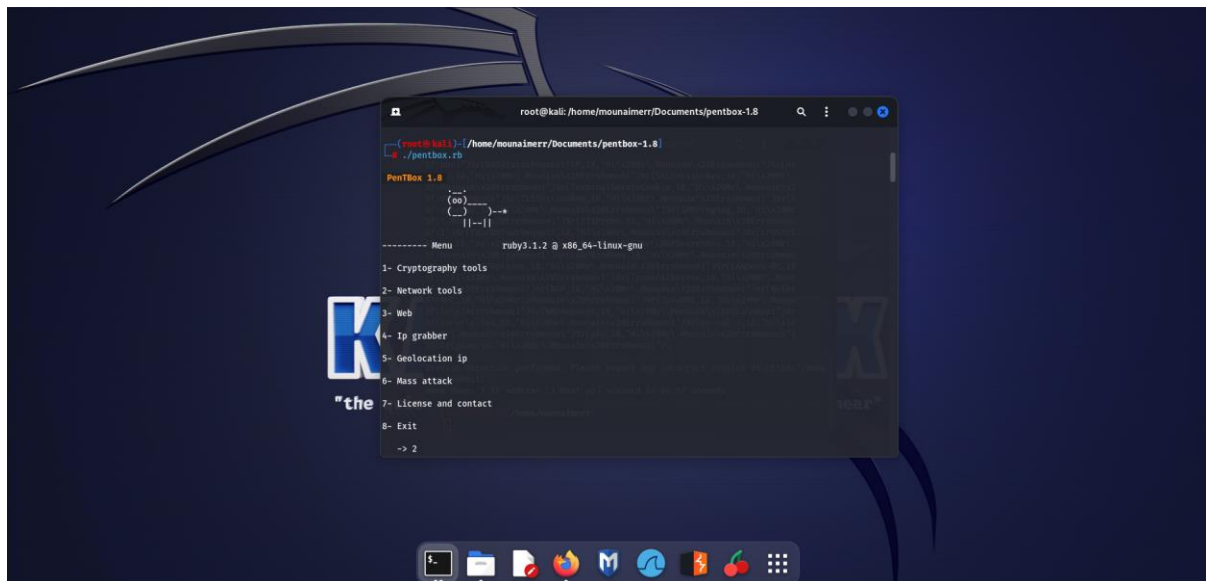
```
root@kali: /home/mounaimerr/Documents/pentbox-1.8
(mounaimerr@kali) ~
$ sudo su
[sudo] password for mounaimerr:
(root@kali) /home/mounaimerr/
$ cd Downloads/pentbox-master
[REDACTED]
(root@kali) /home/mounaimerr/Downloads/pentbox-master
$ cd /home/mounaimerr/Documents/pentbox-1.8
(root@kali) /home/mounaimerr/Documents/pentbox-1.8
$ ls
COPYING.txt  lib  pb_update.rb  readme.txt  tools
changelog.txt  other  pentbox.rb  todo.txt
(root@kali) /home/mounaimerr/Documents/pentbox-1.8
$ ./pentbox.rb
PentBox 1.8
  ____
 (oo)____
 (_____)--*
```

Then type [cd](#) with the location of the file.

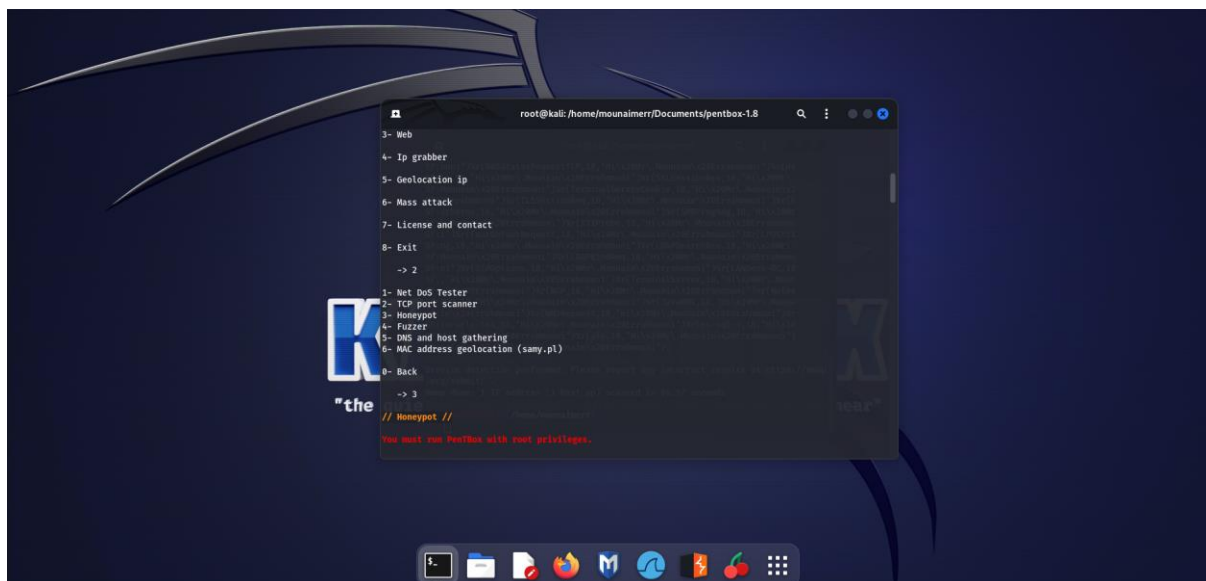
After that type [ls](#) to see the documents on the file.

Now open [./pentbox.rb](#)

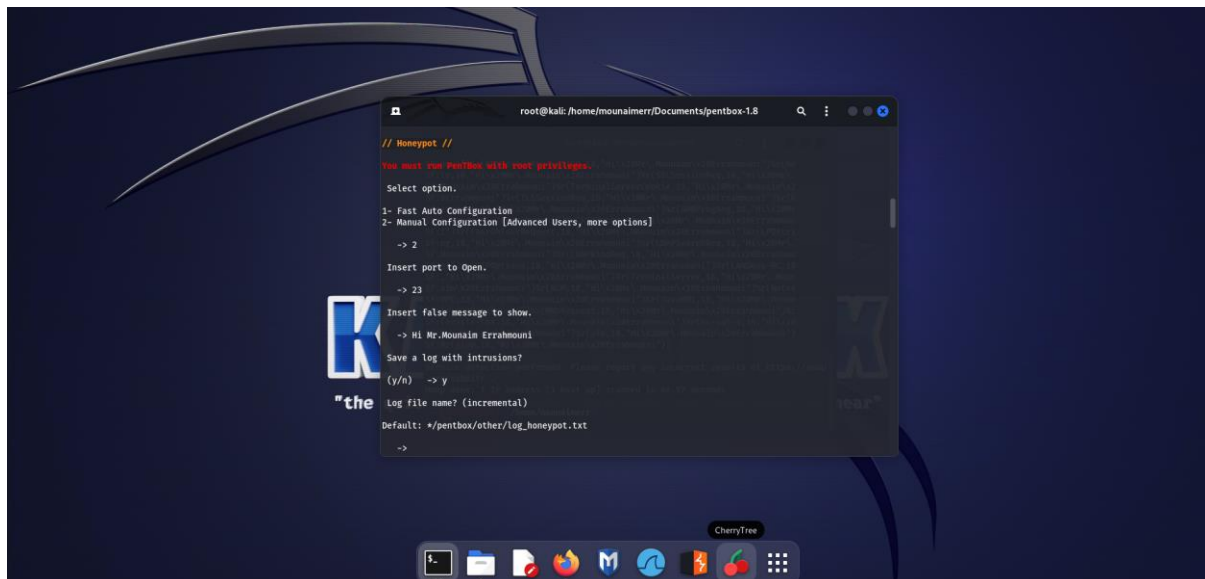
This menu will show up, choose the second option by typing 2.



Choose the third option by typing 3.



Now try to follow these steps by doing the following command:



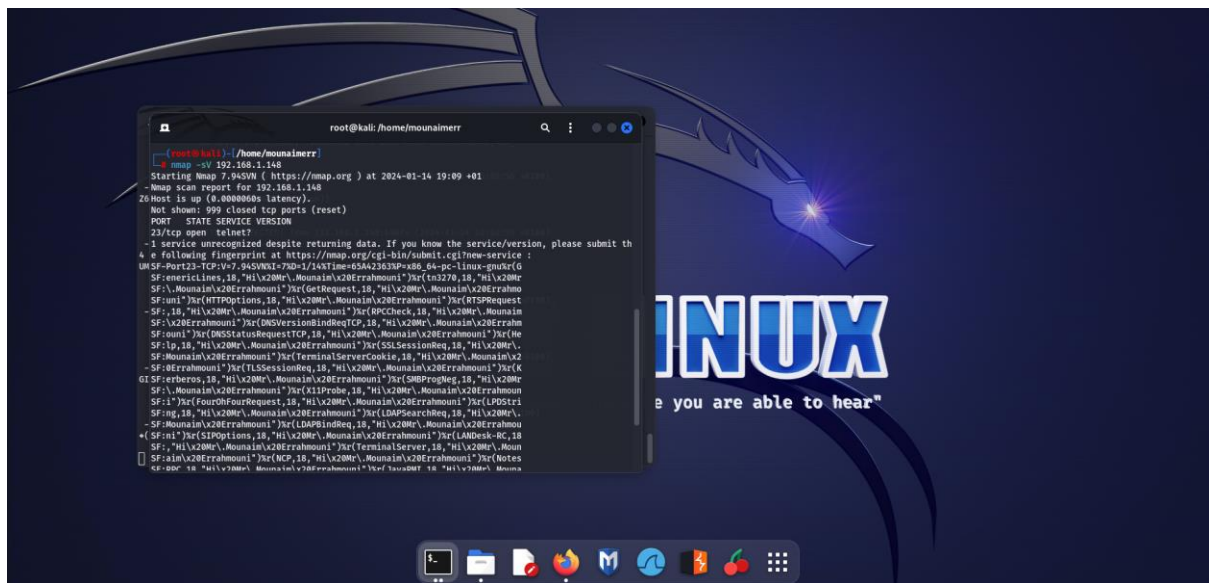
-You have to choose the manual configuration to have more options. It will ask you to insert the port you want it to be open. It will not be open actually, but it will only trick the hacker in order that he will try to have access from it.

-Insert the message that you want to be shown to the hacker to make him believe that he gained access to your computer.

-Select y/yes so every log it will be saved.

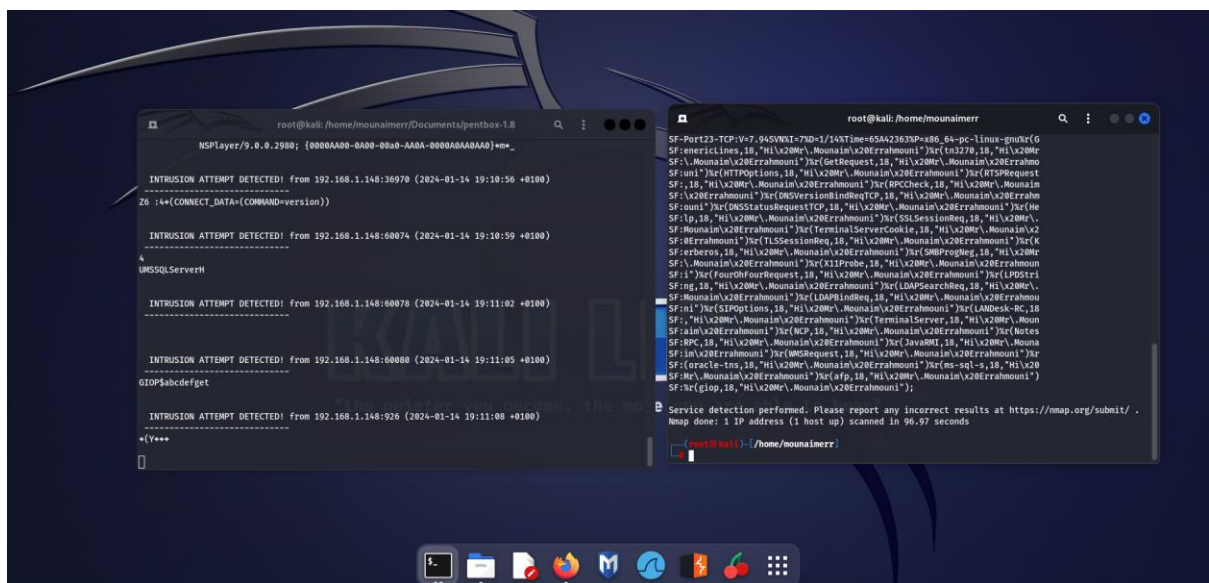
-Press enter.

Check your ip address to perform a test on it.



As you can see we performed an analysis using nmap, and we found that the port 23 is open.

At the mean time the hacker performing his analysis.



Our honeypot is doing his work b catching every logs the hacker doing.