HONEYPOT

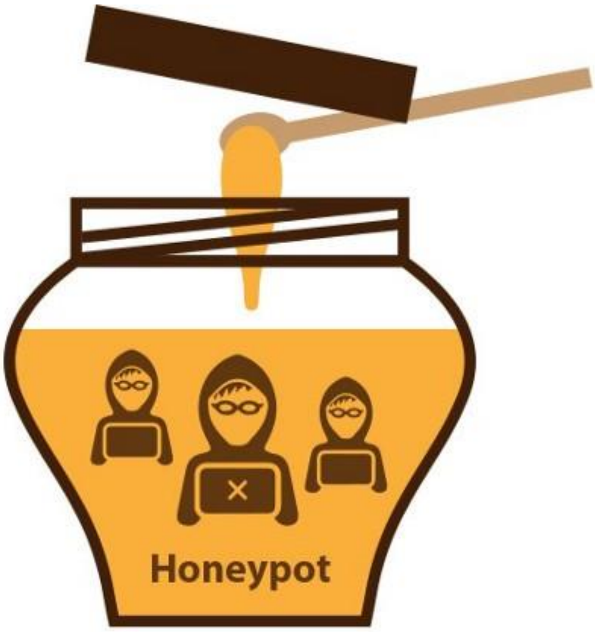
MIS-311 Information Security Systems Design and Applications Project Documentation

Furkan Kahraman-16030411039
Simge Kavalcı-17030411025
Muhammed Kok-16030411055

1

What is Honeypot?

Honeypots are decoy servers that are used to gather information about attackers or users who access information systems without authorization. A honeypot can often be a computer that appears to be part of a network, or any server hosting data. In fact, it is an isolated and specially monitored resource that, to attackers, looks like a target of information or value that could cause them to attack.



In answer to the question of why it is called a honeypot, if we compare the attacker to someone who loves honey, as soon as he sees the honeypot - and if there is a feeling of hunger - he will want to put his hand inside. Because when viewed from the outside, you will have the impression that there is honey in it, so when you put your hand into the honeypot, it will be stung by the bees.

Honeypots are divided into three according to their level of interaction;

The risks and benefits of each level of interaction are different; While low-level interaction provides less protection, it is also low-cost and does not require much training, as the level of interaction increases, the cost and the level of education required increase, while the protection increases proportionally.

It is aimed to keep the benefits and risks of other levels in the middle with honeypots interacting at a relatively medium level, which can be considered the middle of both levels.

Also Honeypots are divided into two according to their intended use;

Production honeypots are easy to use. They contain limited information. Production honeypots are generally placed in the production network together with other production servers.And Research honeypots are used to gather information about the purpose and attack tactics of attacker groups targeting different networks, and to investigate the threats that organizations face and learn how organizations can better protect against these threats.

Honeypots do not have complex algorithms, unlike the big works they do. It has a very simple logic. The working logic of honeypots is parallel to the working logic of IDS (Intrusion Detection System) intrusion detection systems.

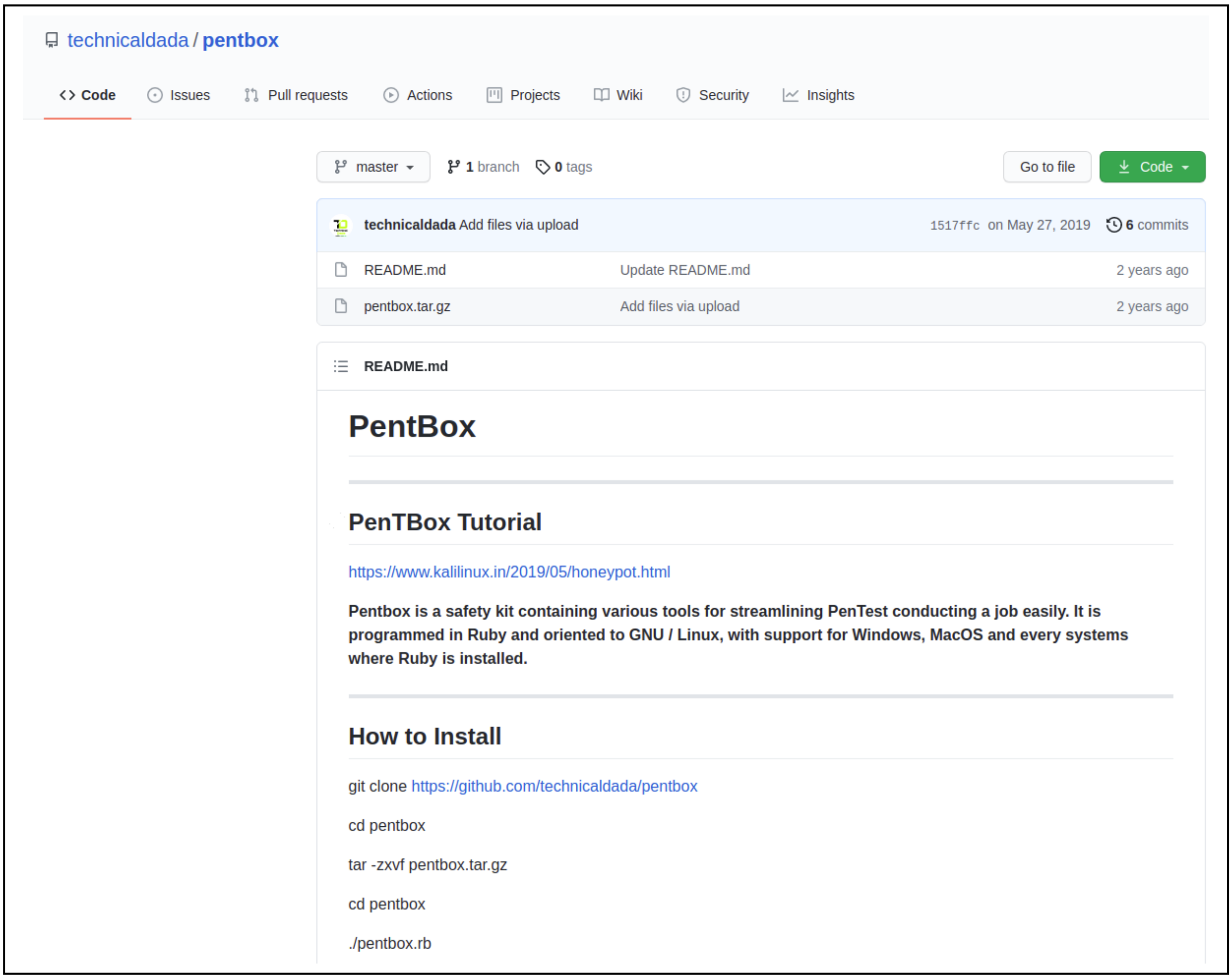
It can show us the log records by analyzing the attacks on the services running on the port we have determined. When the attacker sends an exploit, he can analyze it with the help of antivirus. They can be configured in many ways according to their usage areas. For example, they can even be used to detect spam activity.

Another example is different network structures may exist within a large organization. This can create a vulnerability when an attacker tries to infiltrate a non-honeypot network when he starts to attack. In this, a honeypot network can be installed by configuring many honeypots in different networks. Such systems are called HoneyNet.

2

What we used ?

Here we used a tool called pentbox. This program contains many pentest tools. Honeypot is just one of them. Pentbox is a program written in ruby language, so first of all, it is necessary to install ruby on the computer, and after installing git, we can clone and use the program from github.



technicaldada Add files via upload 1517ffc on May 27, 2019 6 commits

README.md	Update README.md	2 years ago
pentbox.tar.gz	Add files via upload	2 years ago

README.md

PentBox

PenTBox Tutorial

https://www.kalilinux.in/2019/05/honeypot.html

Pentbox is a safety kit containing various tools for streamlining PenTest conducting a job easily. It is programmed in Ruby and oriented to GNU / Linux, with support for Windows, MacOS and every systems where Ruby is installed.

How to Install

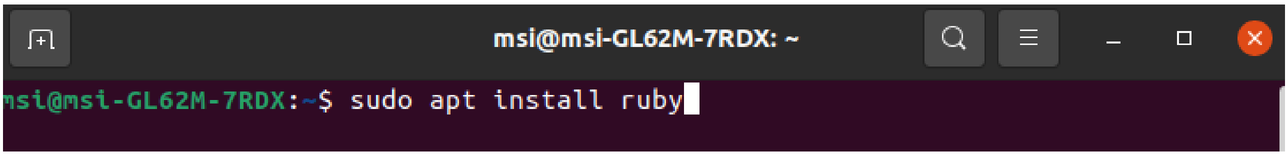
```
git clone https://github.com/technicaldada/pentbox

cd pentbox

tar -zxvf pentbox.tar.gz

cd pentbox

./pentbox.rb
```

https://github.com/technicaldada/pentbox

3

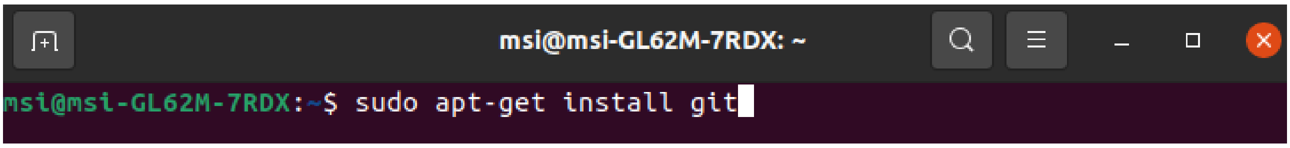
Installations

1.First of all we need to instal ruby,because the pentbox program written in ruby language



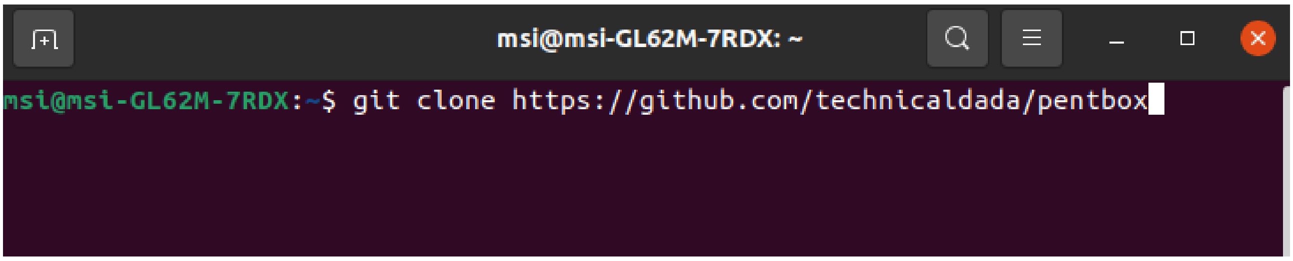
```
msi@msi-GL62M-7RDX:~$ sudo apt install ruby
```

2.Then install git,because we clone the program from github.



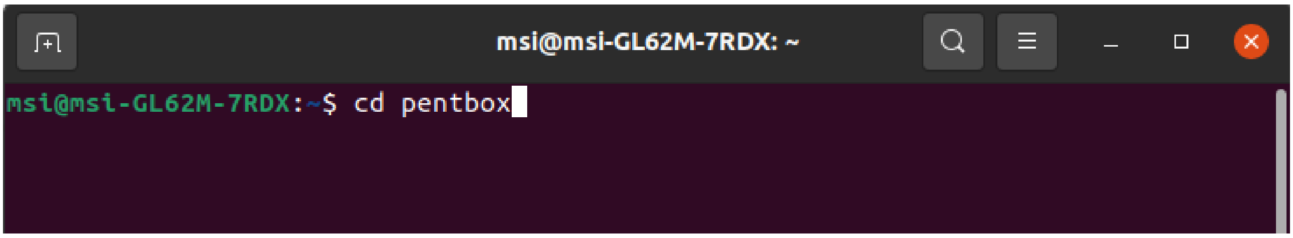
```
msi@msi-GL62M-7RDX:~$ sudo apt-get install git
```

3.Now,clonning the pentbox program.



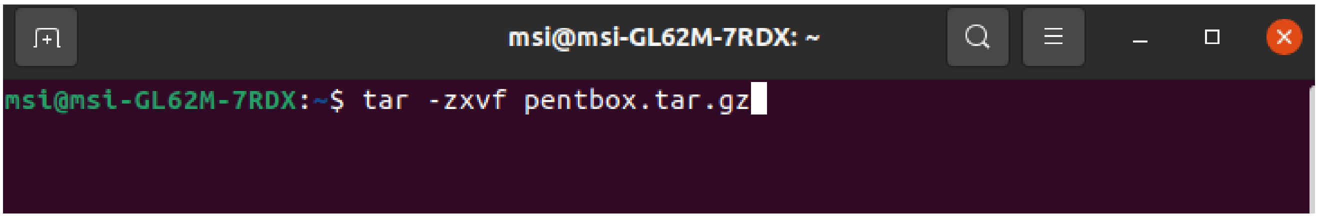
```
msi@msi-GL62M-7RDX:~$ git clone https://github.com/technicaldada/pentbox
```

4.Go to the project that we copied.



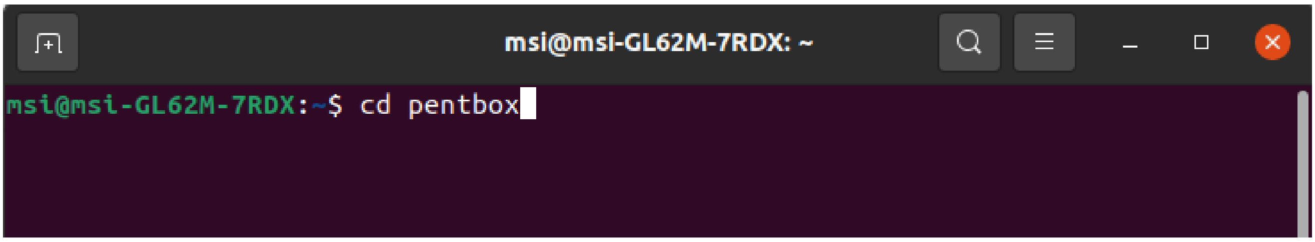
```
msi@msi-GL62M-7RDX:~$ cd pentbox
```

5. Decompress the .tar file.



```
msi@msi-GL62M-7RDX:~$ tar -zxvf pentbox.tar.gz
```

6.Now go to directory again.

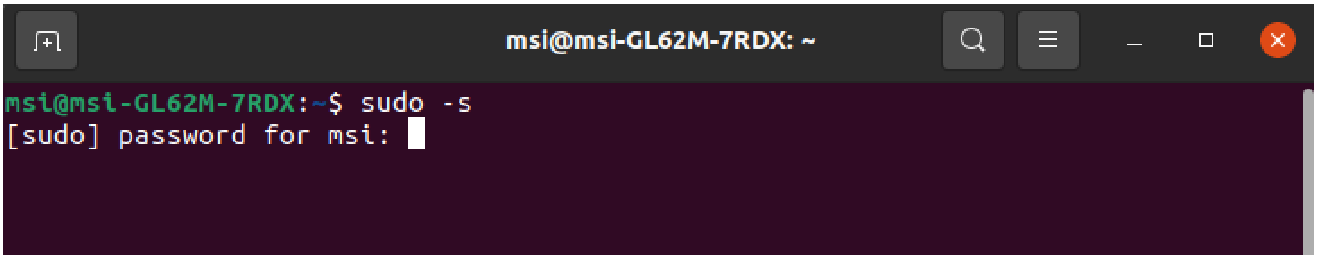


```
msi@msi-GL62M-7RDX:~$ cd pentbox
```

4

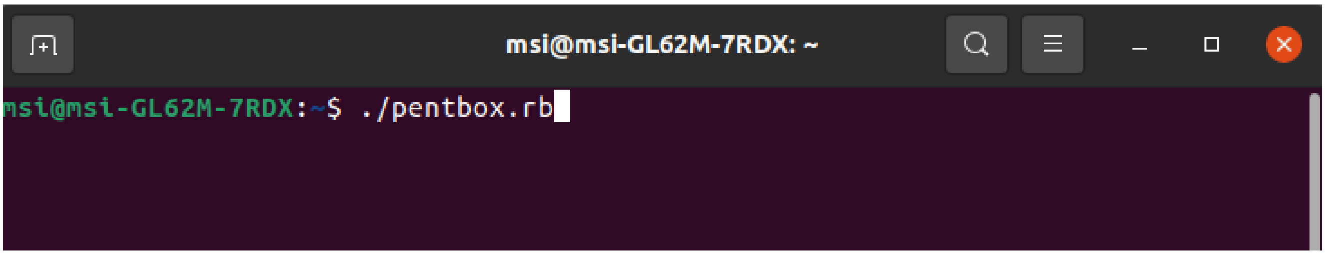
Usage

7.Before starting the program,permit the terminal with root previlages.



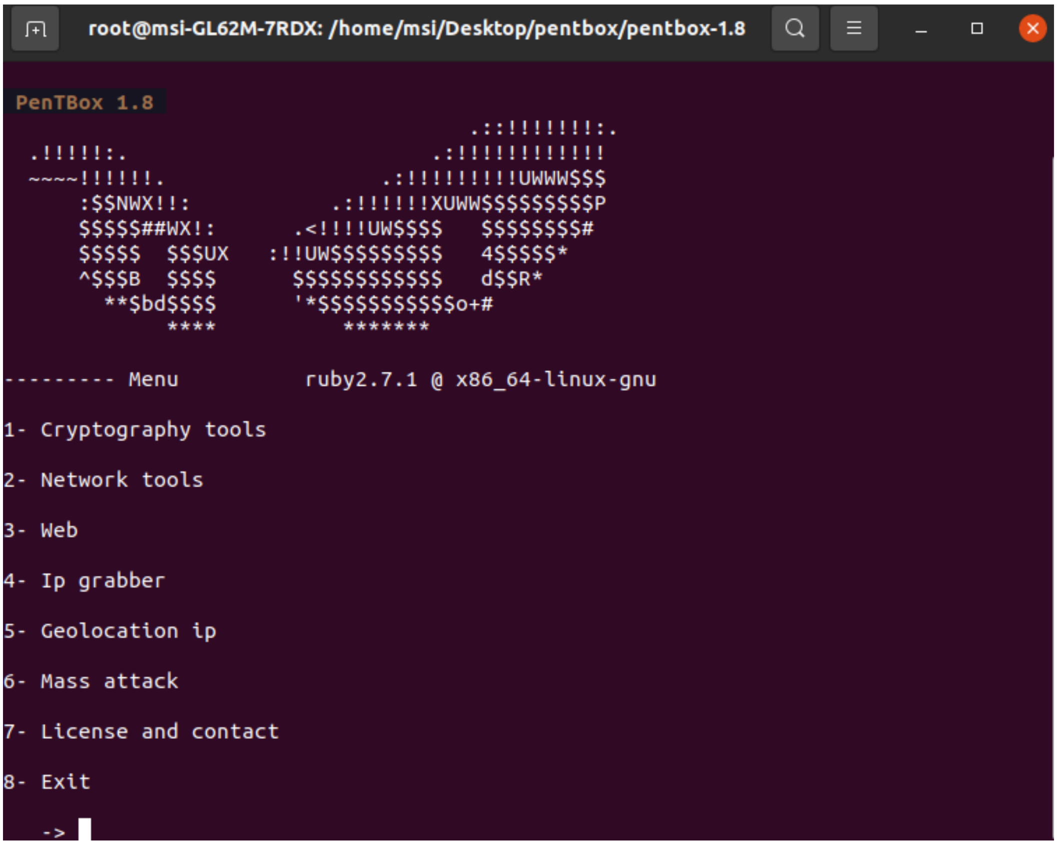
```
msi@msi-GL62M-7RDX:~$ sudo -s
[sudo] password for msi:
```

8.Now start the program.



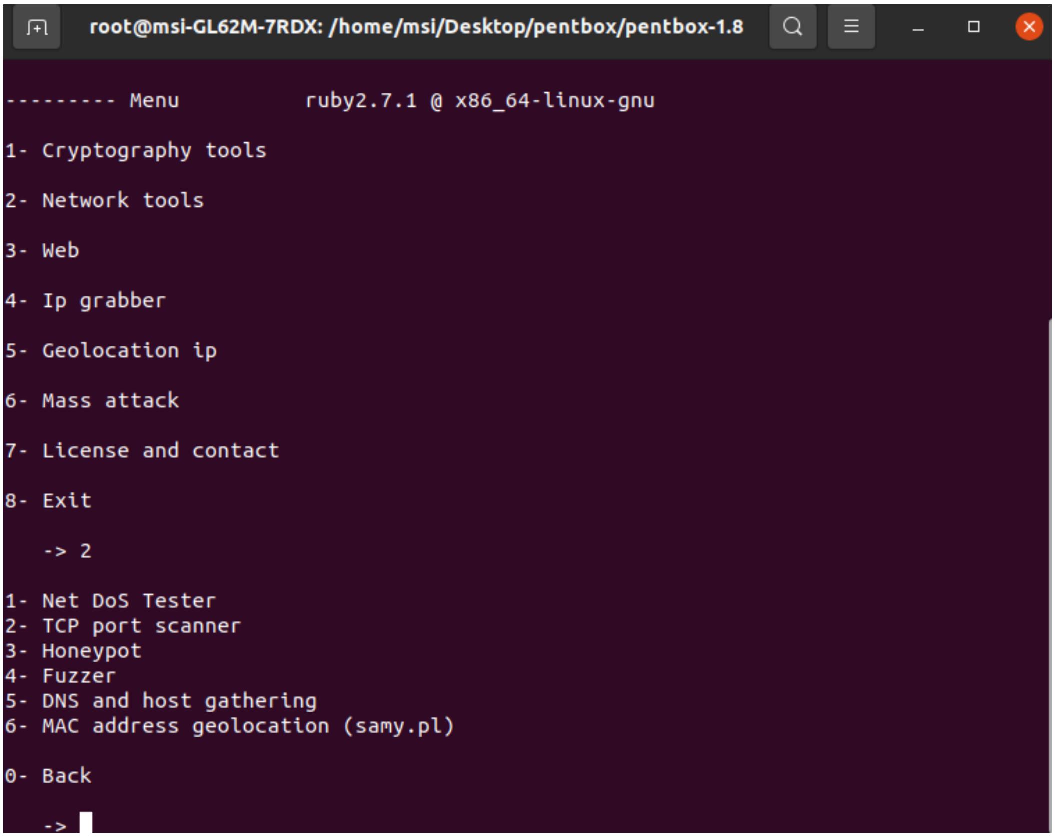
```
msi@msi-GL62M-7RDX:~$ ./pentbox.rb
```

9.Here is the pentbox’s main menu.



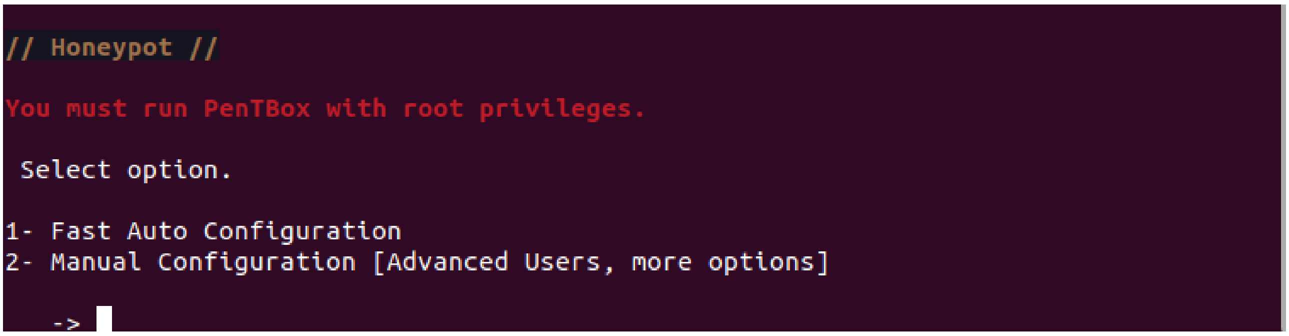
```
root@msi-GL62M-7RDX: /home/msi/Desktop/pentbox/pentbox-1.8

PenTBox 1.8
                                     .::!!!!!!!:.
  .!!!!!:.                        .:!!!!!!!!!!!!
  ~~~~!!!!!!.                 .:!!!!!!!!!!UWWW$$$
      :$$NWX!!:           .:!!!!!!XUWW$$$$$$$$$P
      $$$$$##WX!:      .<!!!!UW$$$$   $$$$$$$$#
      $$$$$  $$$UX   :!!UW$$$$$$$$$$   4$$$$$*
      ^$$$B  $$$$      $$$$$$$$$$$$   d$$R*
        **$bd$$$$      '*$$$$$$$$$$$o+#
             ****          *******

--------- Menu          ruby2.7.1 @ x86_64-linux-gnu

1- Cryptography tools

2- Network tools

3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit

   ->
```

10.Choose here secont option “Network tools” and choose the honeypot.



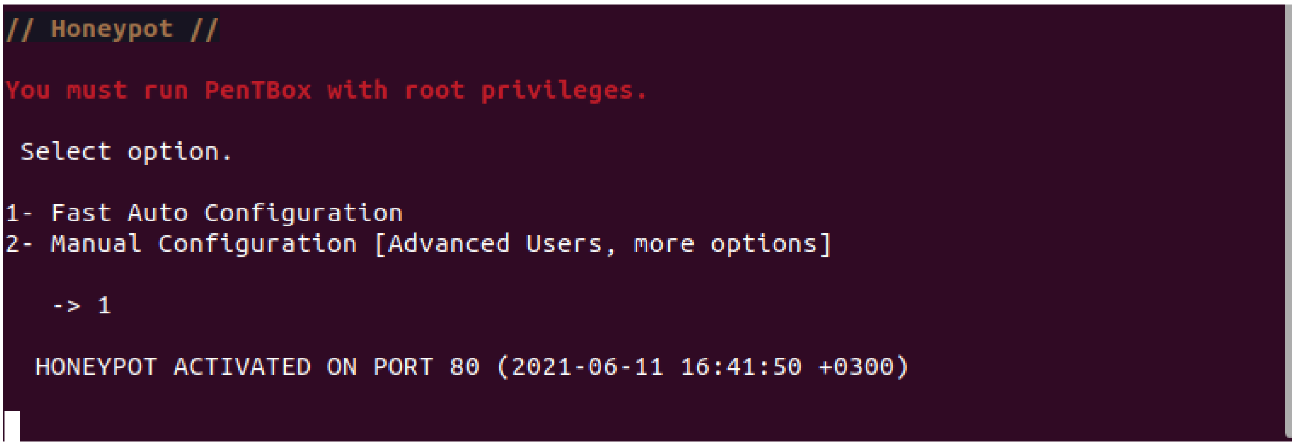
```
root@msi-GL62M-7RDX: /home/msi/Desktop/pentbox/pentbox-1.8

--------- Menu          ruby2.7.1 @ x86_64-linux-gnu

1- Cryptography tools

2- Network tools

3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit

   -> 2

1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back

   ->
```

11.This is honeypot’s option menu.



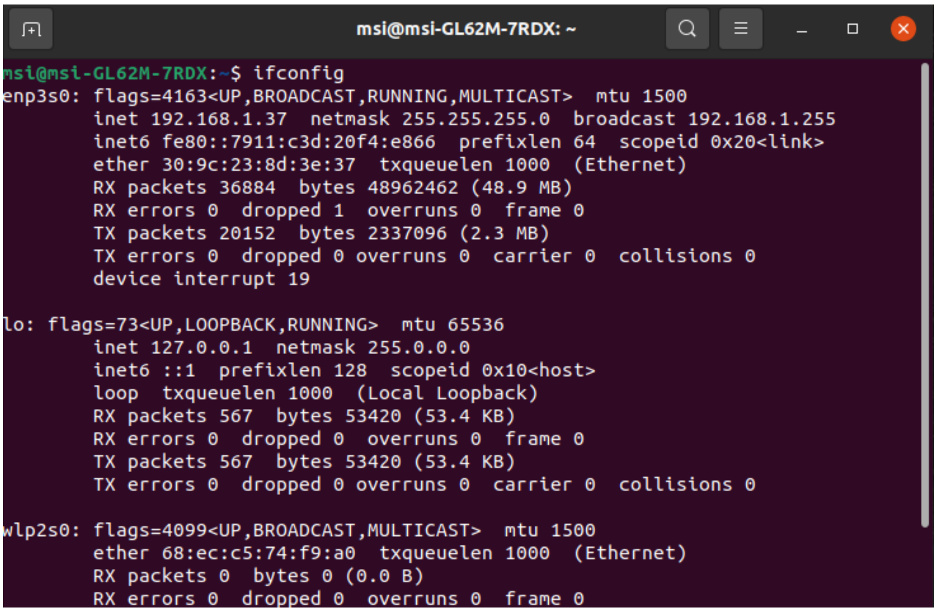
```
// Honeypot //

You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   ->
```

12.Firstly,we choose option 1,Fast Auto Configuration.



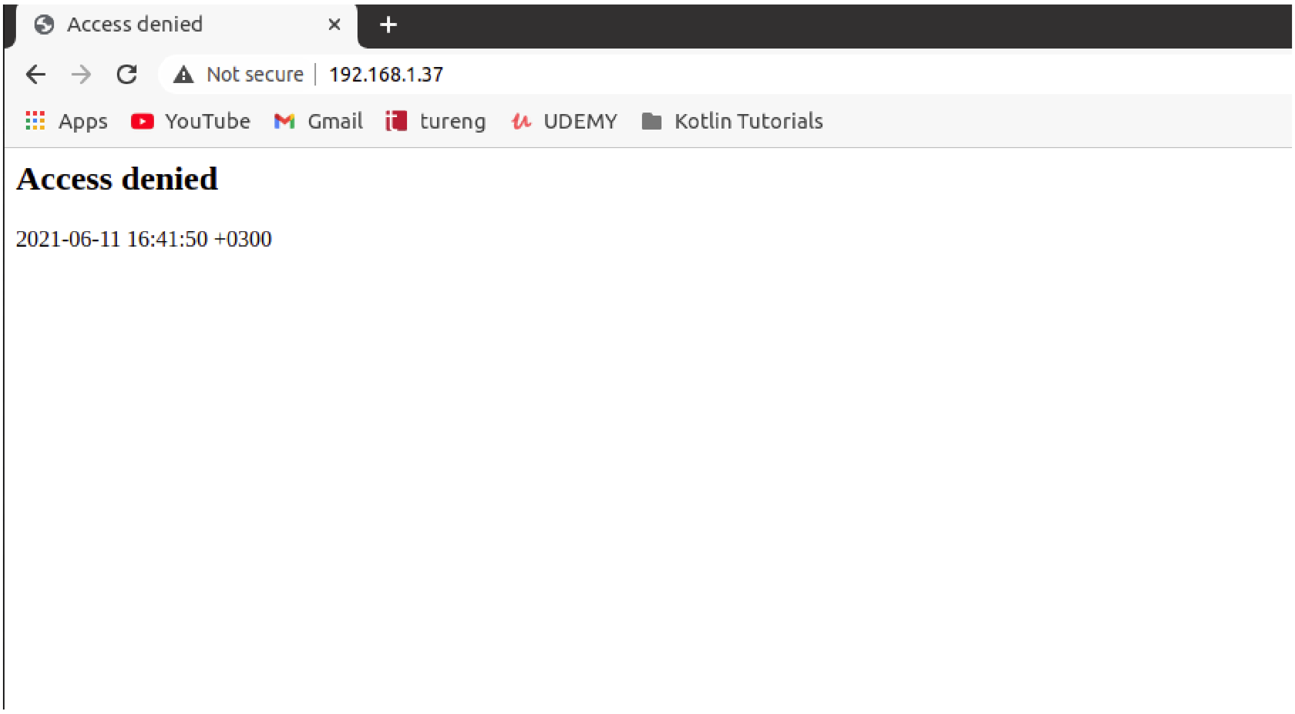
```
// Honeypot //

You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   -> 1

  HONEYPOT ACTIVATED ON PORT 80 (2021-06-11 16:41:50 +0300)
```

13.After the warning “Honeypot Activated” we are going to try to intruse the server.To do that we need to now server’s IP adress.In this example our server is local machine,to learn the IP adress we go terminal and type ifconfig.



```
msi@msi-GL62M-7RDX:~$ ifconfig
enp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.37  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::7911:c3d:20f4:e866  prefixlen 64  scopeid 0x20<link>
        ether 30:9c:23:8d:3e:37  txqueuelen 1000  (Ethernet)
        RX packets 36884  bytes 48962462 (48.9 MB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 20152  bytes 2337096 (2.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 567  bytes 53420 (53.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 567  bytes 53420 (53.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 68:ec:c5:74:f9:a0  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
```

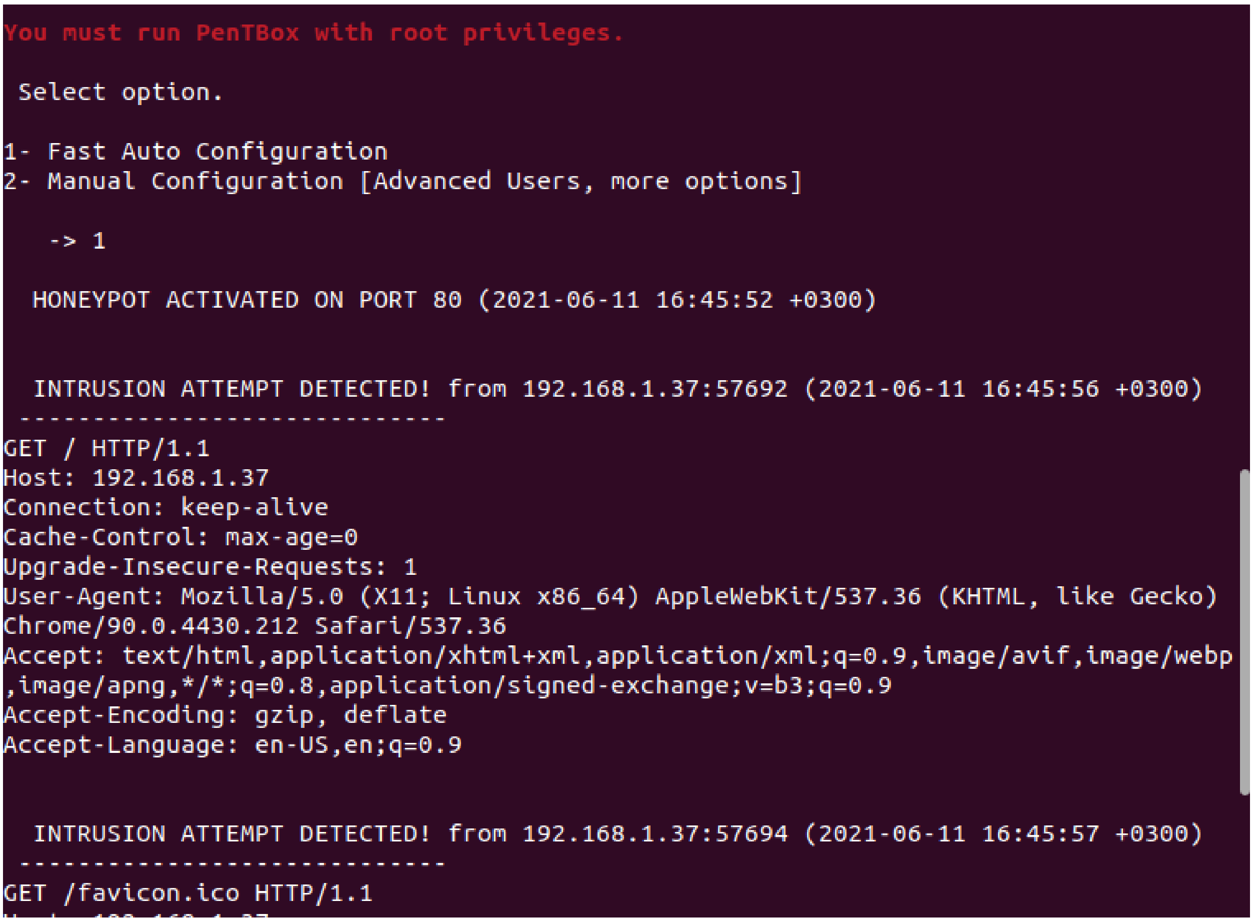
13.We got the IP adress,now we go a browser and try to intruse server.



Access denied

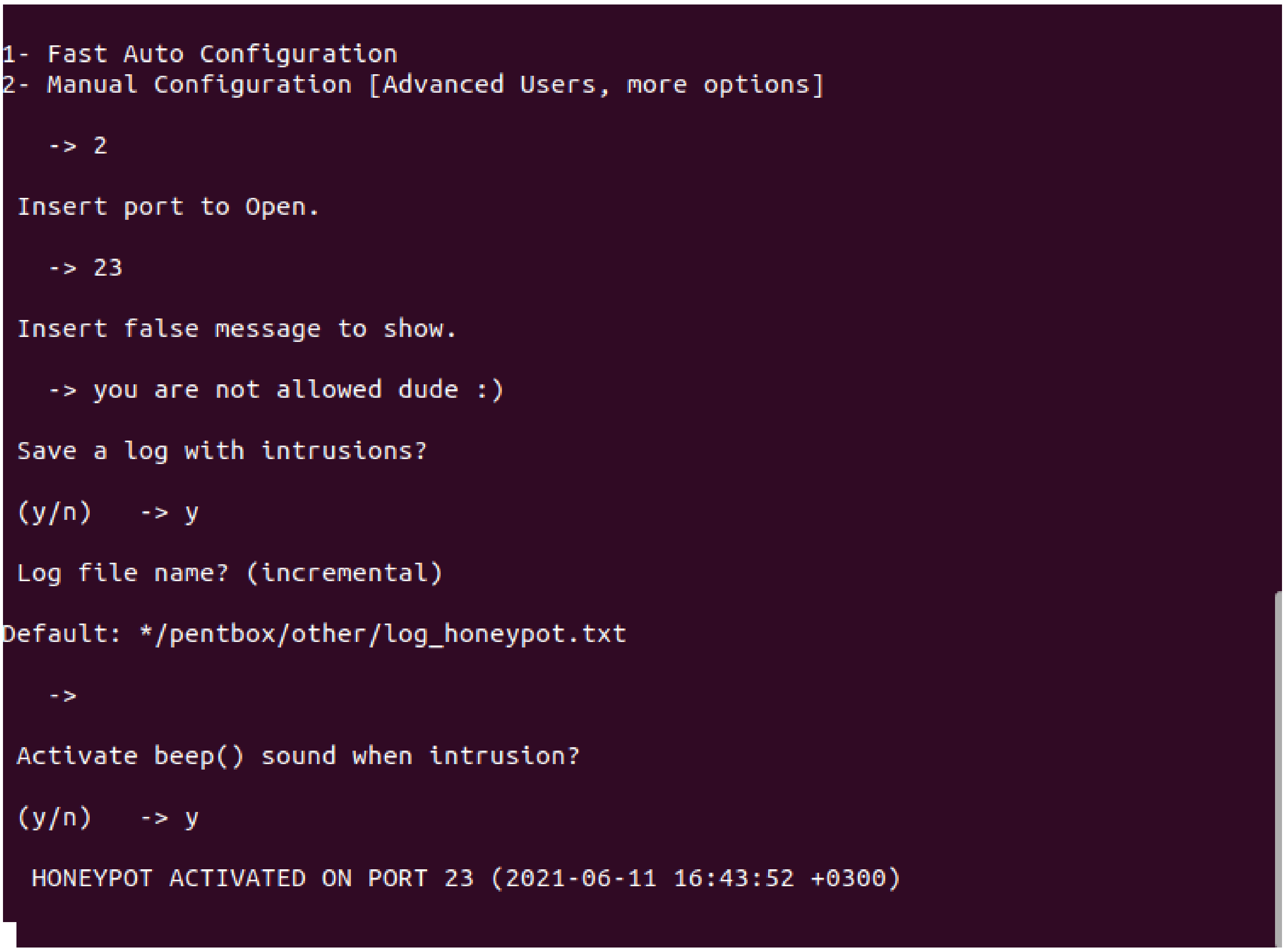
2021-06-11 16:41:50 +0300

14.Host says “Acces denied”.Lets go back to honeypot and check the logs.



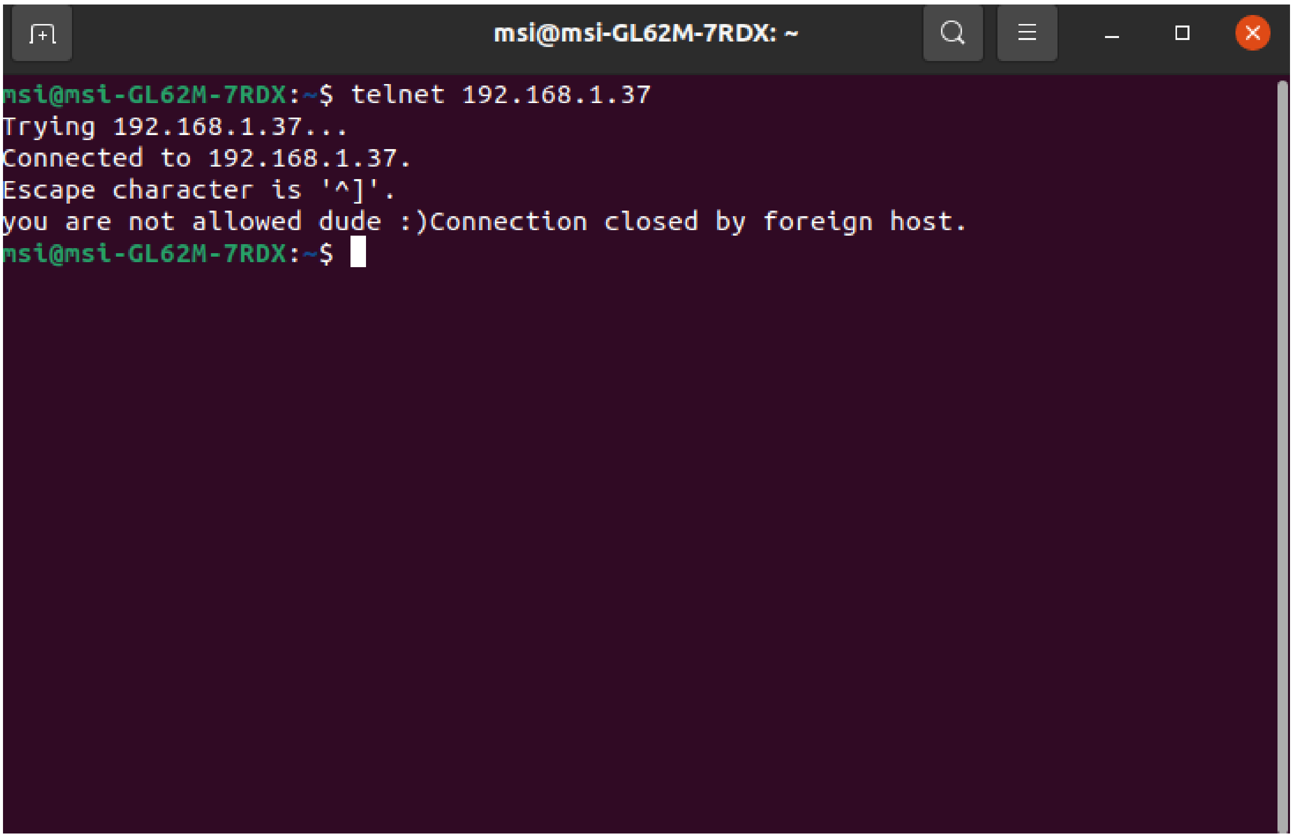
```
You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   -> 1

  HONEYPOT ACTIVATED ON PORT 80 (2021-06-11 16:45:52 +0300)


  INTRUSION ATTEMPT DETECTED! from 192.168.1.37:57692 (2021-06-11 16:45:56 +0300)
 -----------------------------
GET / HTTP/1.1
Host: 192.168.1.37
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.212 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


  INTRUSION ATTEMPT DETECTED! from 192.168.1.37:57694 (2021-06-11 16:45:57 +0300)
 -----------------------------
GET /favicon.ico HTTP/1.1
```

15.We have seen all of intrusion attempts successfuly on Fast Auto Configuration.Now lets try other option,Manuel Configuration.In the manuel configration we can choose port number that we want to deploy on it and also we can choose a warning message to show the attacker.



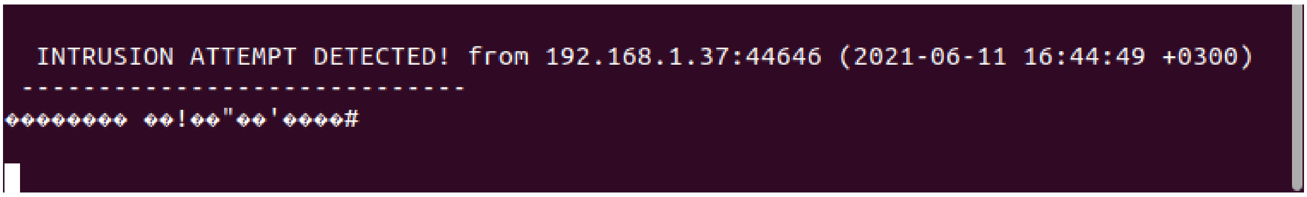
```
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   -> 2

 Insert port to Open.

   -> 23

 Insert false message to show.

   -> you are not allowed dude :)

 Save a log with intrusions?

 (y/n)   -> y

 Log file name? (incremental)

Default: */pentbox/other/log_honeypot.txt

   ->

 Activate beep() sound when intrusion?

 (y/n)   -> y

  HONEYPOT ACTIVATED ON PORT 23 (2021-06-11 16:43:52 +0300)
```

16.After we deploy the honeypot on port 23,lets try to connect via telnet.And see the result.



```
msi@msi-GL62M-7RDX:~$ telnet 192.168.1.37
Trying 192.168.1.37...
Connected to 192.168.1.37.
Escape character is '^]'.
you are not allowed dude :)Connection closed by foreign host.
msi@msi-GL62M-7RDX:~$ 
```

17.As you see in the screenshot,the attacker sees the message that we arranged before,Now lets go back and check the honeypot client.



```
 INTRUSION ATTEMPT DETECTED! from 192.168.1.37:44646 (2021-06-11 16:44:49 +0300)
 -----------------------------
�������� ��!��"��'����#
```

All of logs are attached into log_honeypot.txt file.