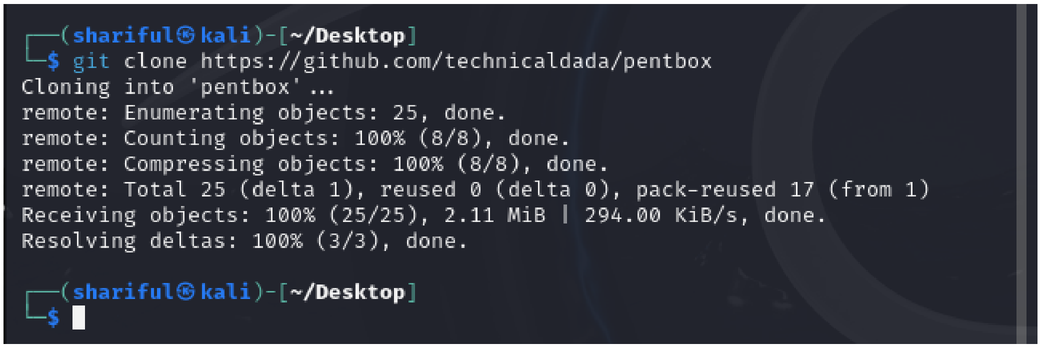
HoneyPots

HoneyPots is the process to learn how to catch hackers. Honeypot is essentially a trap designed to attract hackers such as police use various techniques to catch cyber criminals. Cyber security experts, they employ honey pots to catch hackers. Some companies install the honeypot within the network, and when hackers try to beat the company's security, the honeypot captures the attacker IP address and geolocation data.

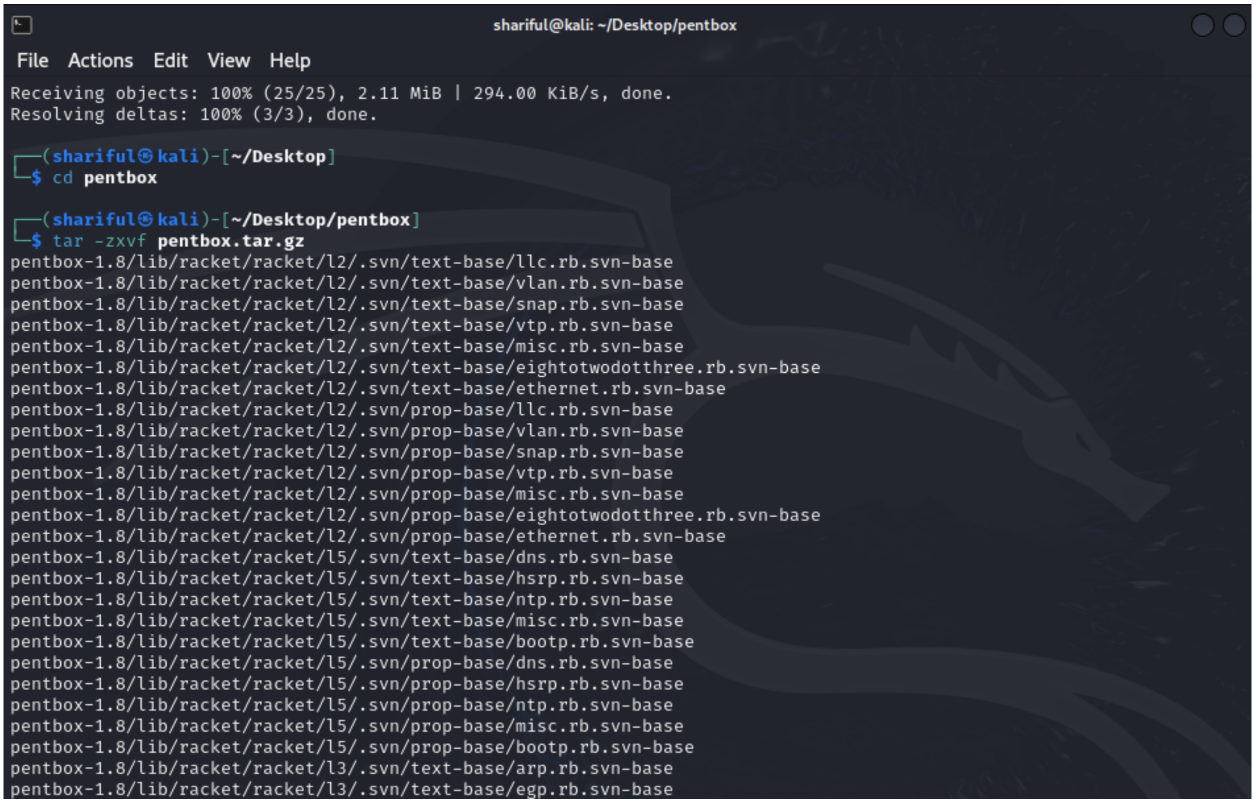
https://github.com/technicaldada/pentbox

Open the link and follow step by step procedure:

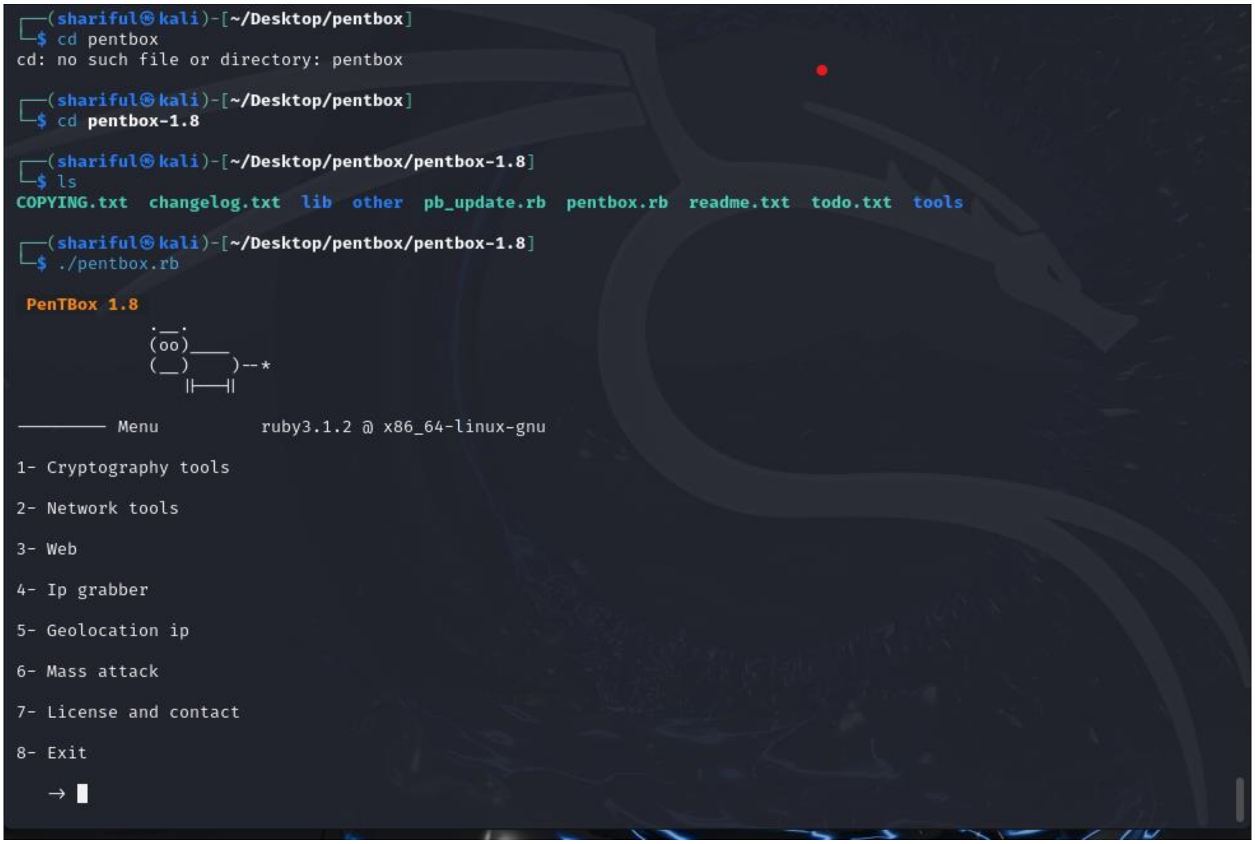
git clone https://github.com/technicaldada/pentbox



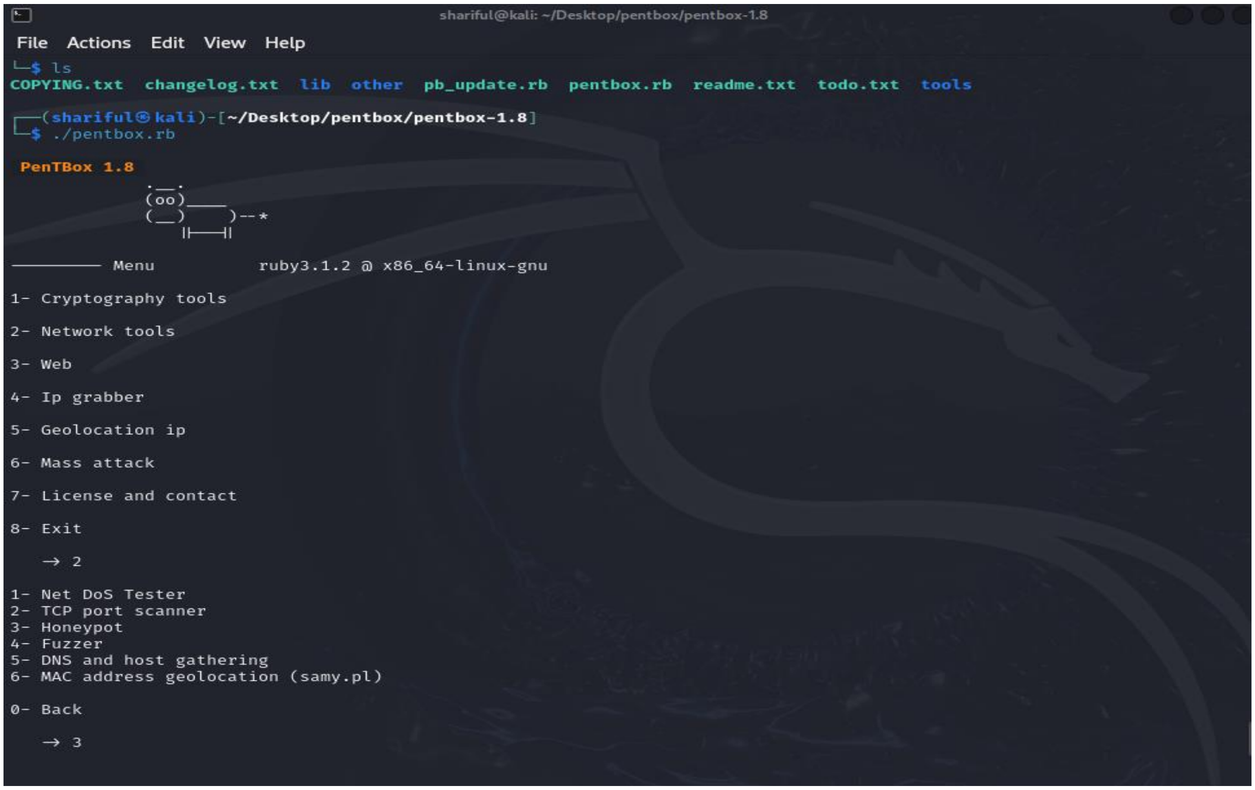
```
┌──(shariful㉿kali)-[~/Desktop]
└─$ git clone https://github.com/technicaldada/pentbox
Cloning into 'pentbox'...
remote: Enumerating objects: 25, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 25 (delta 1), reused 0 (delta 0), pack-reused 17 (from 1)
Receiving objects: 100% (25/25), 2.11 MiB | 294.00 KiB/s, done.
Resolving deltas: 100% (3/3), done.

┌──(shariful㉿kali)-[~/Desktop]
└─$ 
```



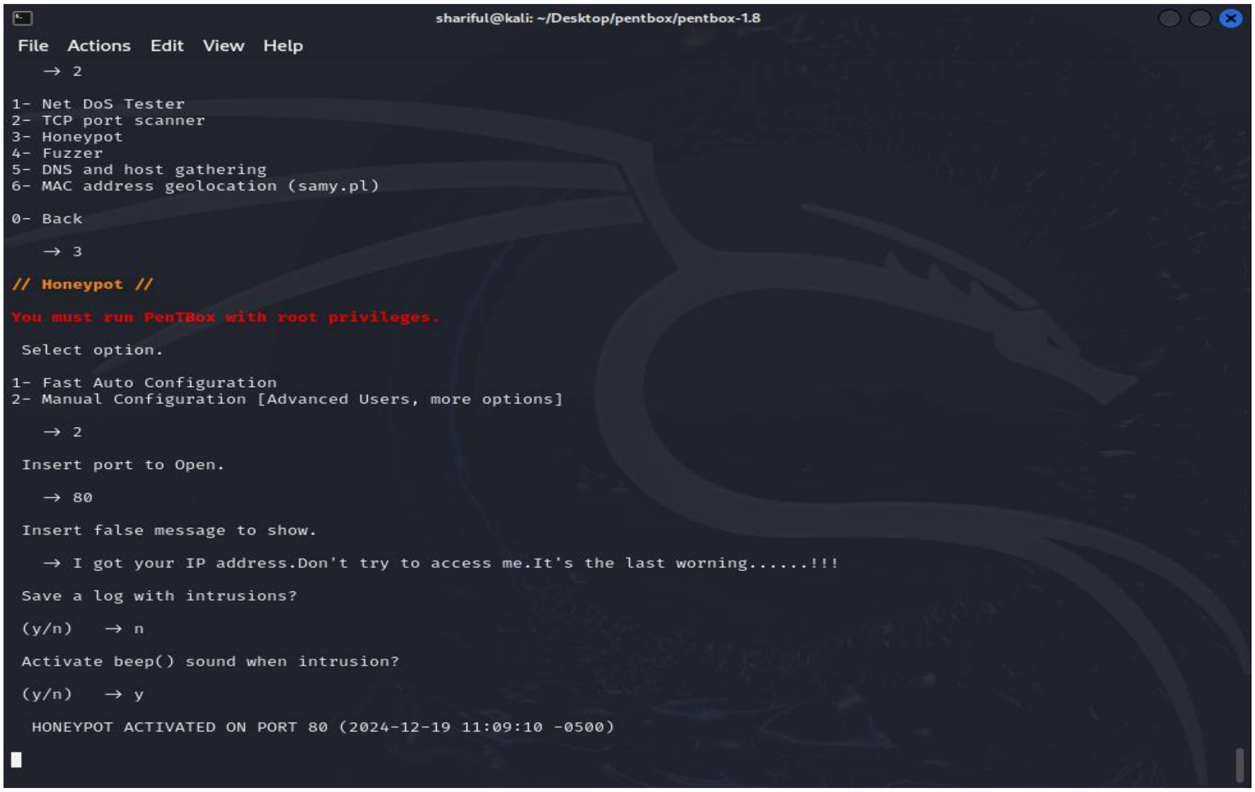
```
Receiving objects: 100% (25/25), 2.11 MiB | 294.00 KiB/s, done.
Resolving deltas: 100% (3/3), done.

┌──(shariful㉿kali)-[~/Desktop]
└─$ cd pentbox

┌──(shariful㉿kali)-[~/Desktop/pentbox]
└─$ tar -zxvf pentbox.tar.gz
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/llc.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/vlan.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/snap.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/vtp.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/misc.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/eightotwodotthree.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/ethernet.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/prop-base/llc.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/prop-base/vlan.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/prop-base/snap.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/prop-base/vtp.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/prop-base/misc.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/prop-base/eightotwodotthree.rb.svn-base
pentbox-1.8/lib/racket/racket/l2/.svn/prop-base/ethernet.rb.svn-base
pentbox-1.8/lib/racket/racket/l5/.svn/text-base/dns.rb.svn-base
pentbox-1.8/lib/racket/racket/l5/.svn/text-base/hsrp.rb.svn-base
pentbox-1.8/lib/racket/racket/l5/.svn/text-base/ntp.rb.svn-base
pentbox-1.8/lib/racket/racket/l5/.svn/text-base/misc.rb.svn-base
pentbox-1.8/lib/racket/racket/l5/.svn/text-base/bootp.rb.svn-base
pentbox-1.8/lib/racket/racket/l5/.svn/prop-base/dns.rb.svn-base
pentbox-1.8/lib/racket/racket/l5/.svn/prop-base/hsrp.rb.svn-base
pentbox-1.8/lib/racket/racket/l5/.svn/prop-base/ntp.rb.svn-base
pentbox-1.8/lib/racket/racket/l5/.svn/prop-base/misc.rb.svn-base
pentbox-1.8/lib/racket/racket/l5/.svn/prop-base/bootp.rb.svn-base
pentbox-1.8/lib/racket/racket/l3/.svn/text-base/arp.rb.svn-base
pentbox-1.8/lib/racket/racket/l3/.svn/text-base/egp.rb.svn-base
```



```
┌──(shariful㉿kali)-[~/Desktop/pentbox]
└─$ cd pentbox
cd: no such file or directory: pentbox

┌──(shariful㉿kali)-[~/Desktop/pentbox]
└─$ cd pentbox-1.8

┌──(shariful㉿kali)-[~/Desktop/pentbox/pentbox-1.8]
└─$ ls
COPYING.txt  changelog.txt  lib  other  pb_update.rb  pentbox.rb  readme.txt  todo.txt  tools

┌──(shariful㉿kali)-[~/Desktop/pentbox/pentbox-1.8]
└─$ ./pentbox.rb

 PenTBox 1.8
               .__.
               (oo)____
               (__)    )--*
                  ||--||

 ──────── Menu          ruby3.1.2 @ 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

   -> █
```

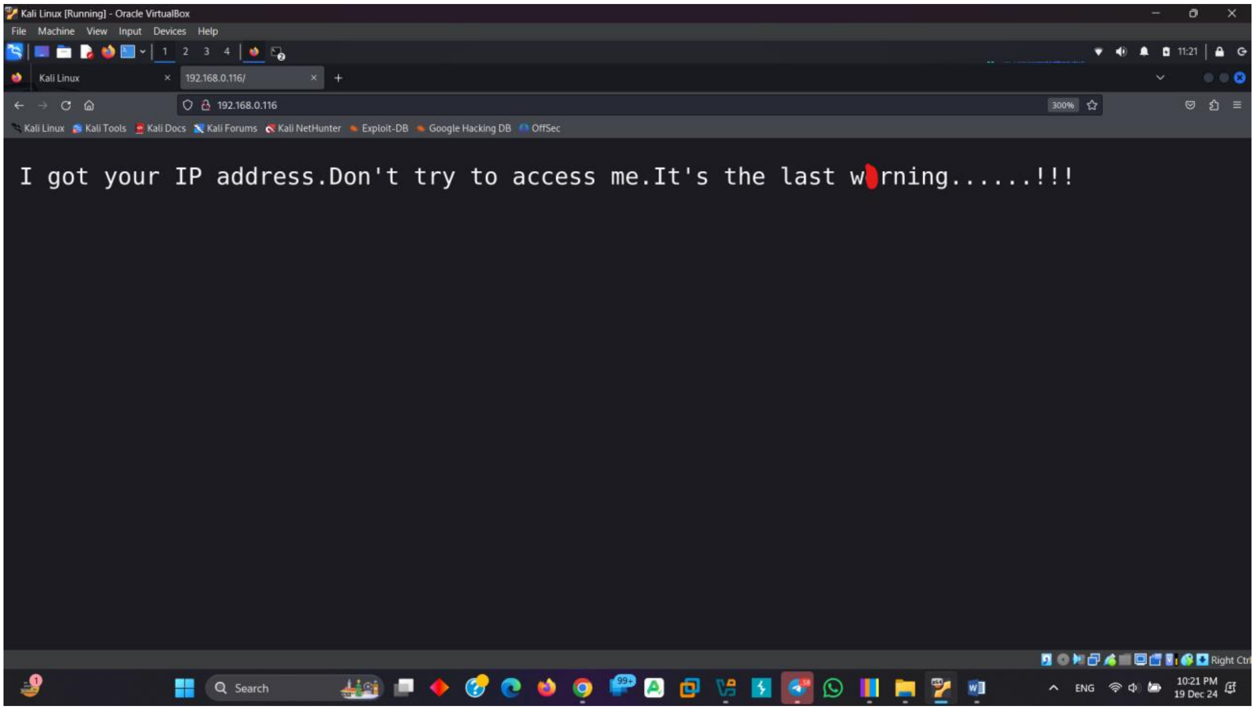


```
└─$ ls
COPYING.txt  changelog.txt  lib  other  pb_update.rb  pentbox.rb  readme.txt  todo.txt  tools

┌──(shariful㉿kali)-[~/Desktop/pentbox/pentbox-1.8]
└─$ ./pentbox.rb

 PenTBox 1.8
               .__.
               (oo)____
               (__)    )--*
                  ||--||

 ──────── Menu          ruby3.1.2 @ 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

   -> 3
```


shariful@kali: ~/Desktop/pentbox/pentbox-1.8
File Actions Edit View Help

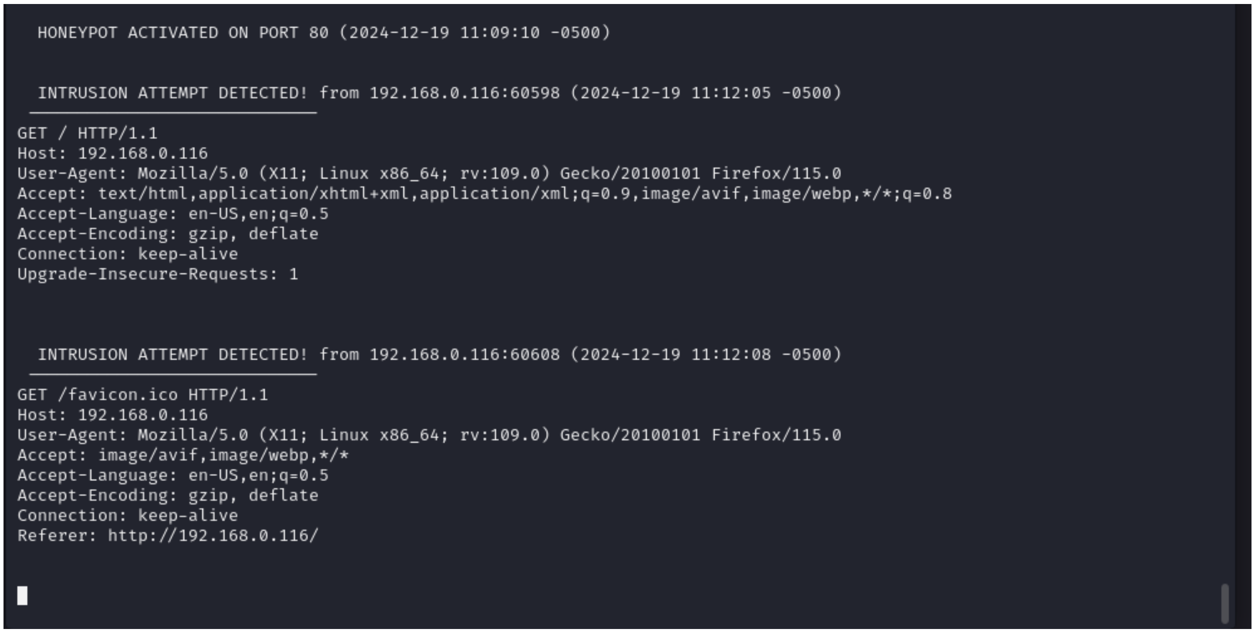
```
   → 2

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

   → 3

// Honeypot //

You must run PenTBox with root privileges.

 Select option.

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

   → 2

 Insert port to Open.

   → 80

 Insert false message to show.

   → I got your IP address.Don't try to access me.It's the last worning......!!!

 Save a log with intrusions?

 (y/n)   → n

 Activate beep() sound when intrusion?

 (y/n)   → y

  HONEYPOT ACTIVATED ON PORT 80 (2024-12-19 11:09:10 -0500)
```

When anyone enter my IP address with port 80 there will show a message and in my terminal there will show hacker ip and location.



```
I got your IP address.Don't try to access me.It's the last worning......!!!
```

Here is the hacker details:



```
  HONEYPOT ACTIVATED ON PORT 80 (2024-12-19 11:09:10 -0500)


  INTRUSION ATTEMPT DETECTED! from 192.168.0.116:60598 (2024-12-19 11:12:05 -0500)

GET / HTTP/1.1
Host: 192.168.0.116
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1



  INTRUSION ATTEMPT DETECTED! from 192.168.0.116:60608 (2024-12-19 11:12:08 -0500)

GET /favicon.ico HTTP/1.1
Host: 192.168.0.116
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.0.116/
```

Shariful Islam
shariful.stu20181@juniv.edu
https://github.com/sharifuliitju