REPORT ON HONEYPOTS
(09/2024)

Name: Sanjeev yadav

Aim: Setup Honeypot using PenTBox

- **Gather Threat Intelligence:** Understand the tactics and techniques employed by potential attackers.
- **Enhance Security Awareness**: Identify and analyze common attack patterns and vulnerabilities.

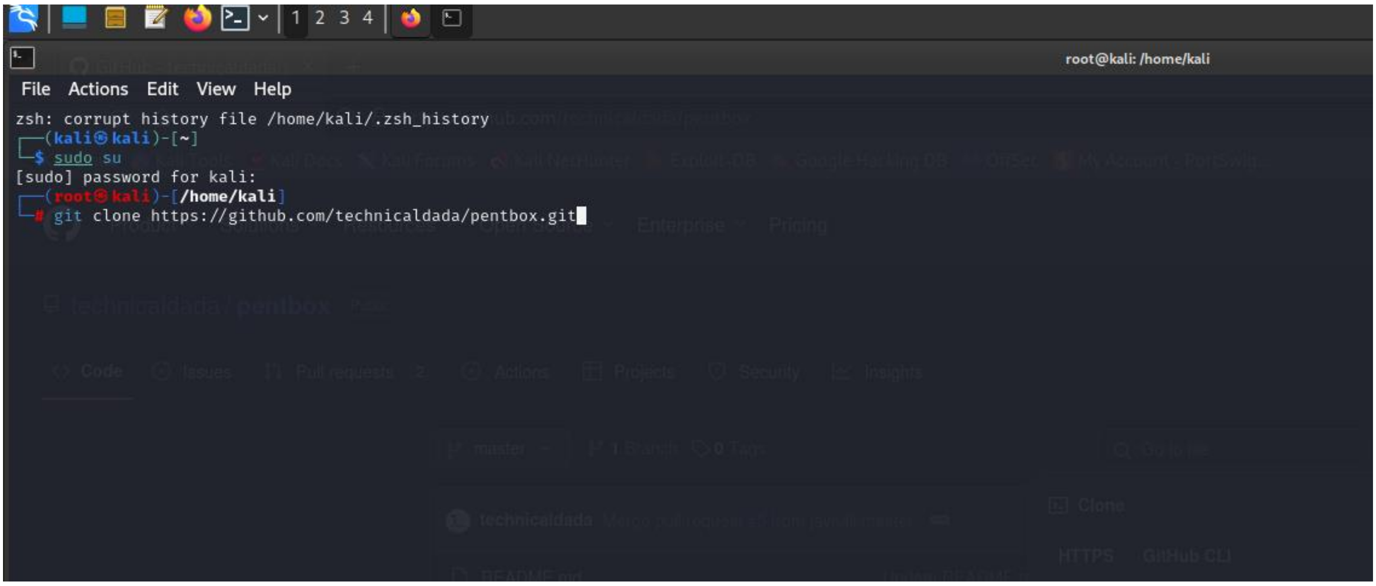
A honeypot is a decoy, or a trap, created by organizations to attract hackers into a computer system. One of the main objectives of using a honeypot is to monitor the hacker's exploit of the system's vulnerabilities. Subsequently, learn the system's weaknesses and apply the necessary security measures to strengthen it from future attacks. Another objective is to study the hacker's methodology. The final objective is to divert the hacker's attention from the main network to the decoy system.

Tools: PenTBox

Steps:

1. Run the following commands to install pentbox:

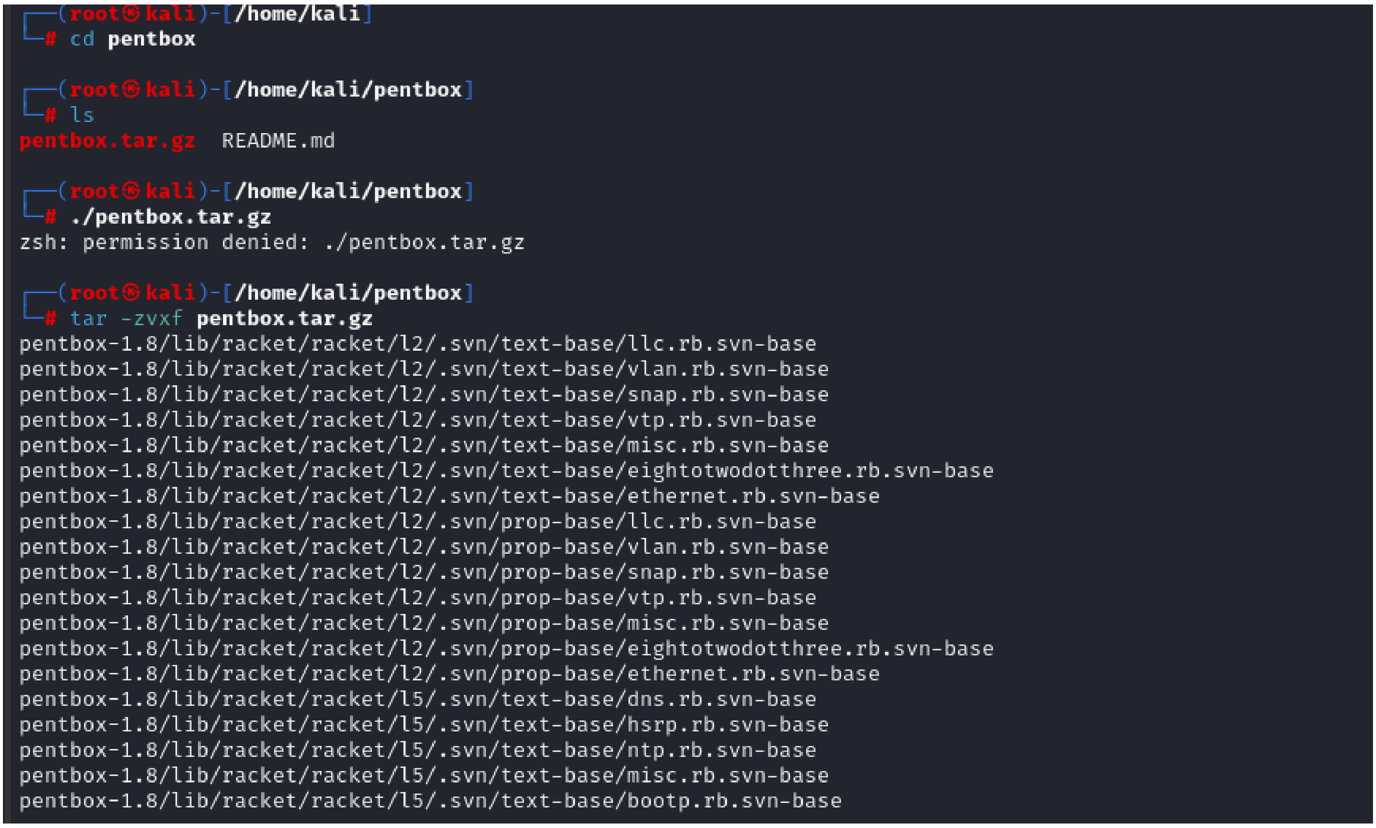
```
$ git clone https://github.com/technicaldada/pentbox
$ cd pentbox
```



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# git clone https://github.com/technicaldada/pentbox.git
```

Once in the directory of PentBox, to unzip the file use:

$ tar -zxvf pentbox.tar.gz

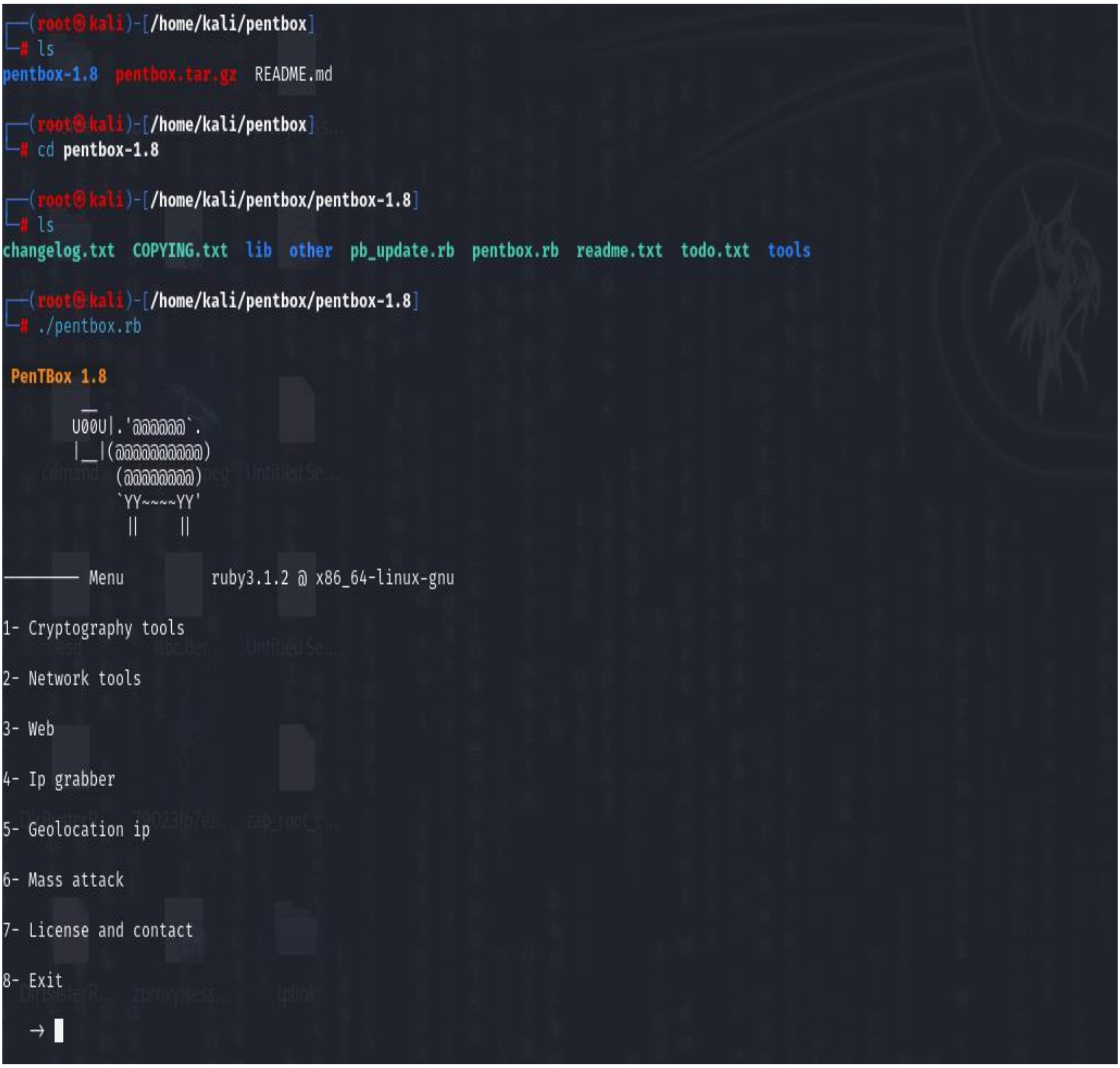


```
┌──(root㉿kali)-[/home/kali]
└─# cd pentbox

┌──(root㉿kali)-[/home/kali/pentbox]
└─# ls
pentbox.tar.gz  README.md

┌──(root㉿kali)-[/home/kali/pentbox]
└─# ./pentbox.tar.gz
zsh: permission denied: ./pentbox.tar.gz

┌──(root㉿kali)-[/home/kali/pentbox]
└─# tar -zvxf 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
```

To open the latest and most recent tool on the file:
$ cd pentbox-1.8

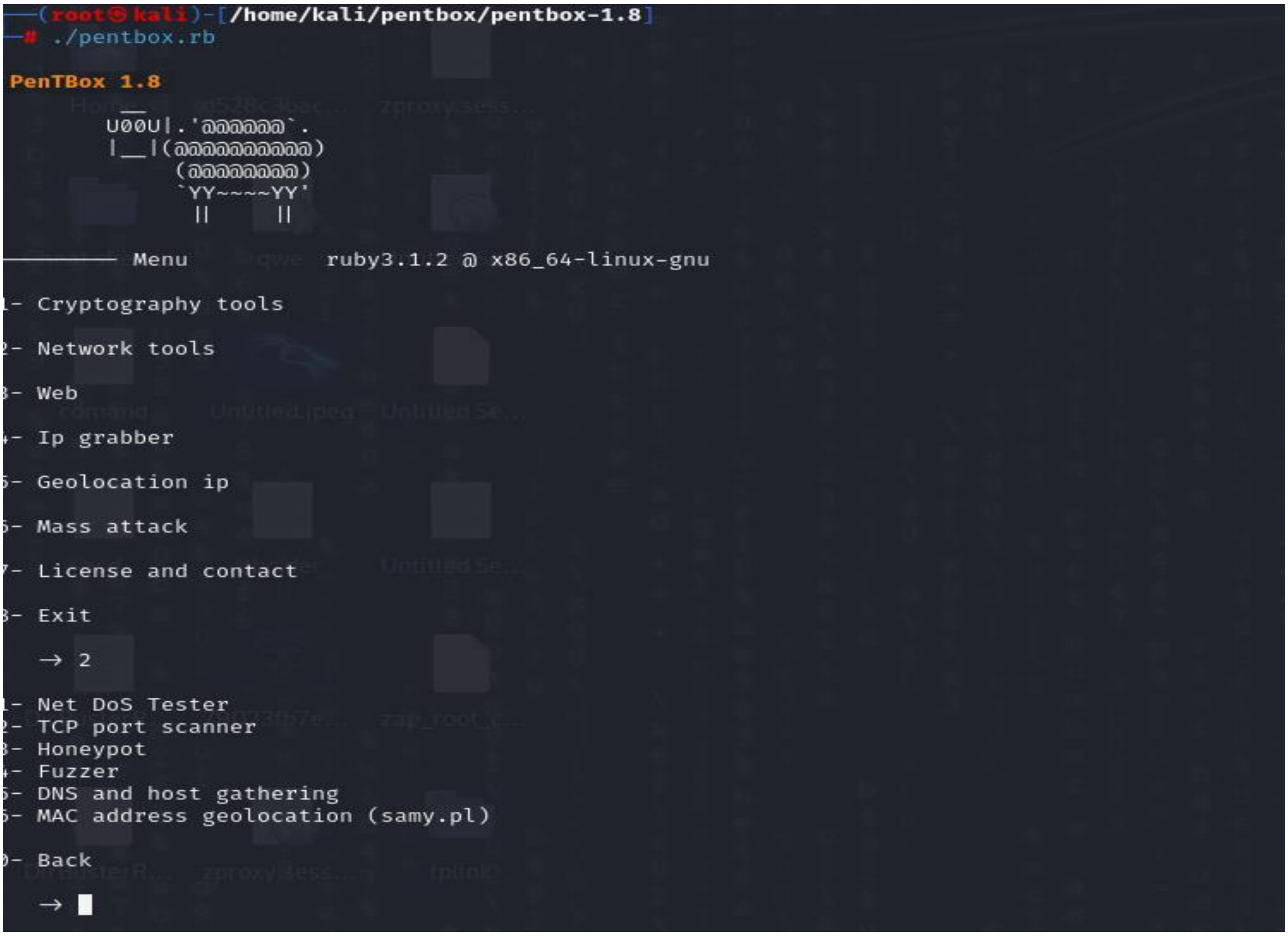
To run the tool:
$ ./pentbox.rb

2. The pentbox menu is then displayed as following:



```
┌──(root㉿kali)-[/home/kali/pentbox]
└─# ls
pentbox-1.8  pentbox.tar.gz  README.md

┌──(root㉿kali)-[/home/kali/pentbox]
└─# cd pentbox-1.8

┌──(root㉿kali)-[/home/kali/pentbox/pentbox-1.8]
└─# ls
changelog.txt  COPYING.txt  lib  other  pb_update.rb  pentbox.rb  readme.txt  todo.txt  tools

┌──(root㉿kali)-[/home/kali/pentbox/pentbox-1.8]
└─# ./pentbox.rb

 PenTBox 1.8

        __
       U00U|.'@@@@@@`.
       |__|(@@@@@@@@@@@)
            (@@@@@@@@@)
            `YY~~~~YY'
             ||    ||

──────── 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

   -> █
```

3. Now since we plan on configuring a honeypot it’s important to include network tools in your configuration, with network tools, you can see who’s trying to interact with it, what methods they’re using, and if they’re trying to exploit any weaknesses. Therefore, we’ll select option 2 (Network tools)



```
┌──(root㉿kali)-[/home/kali/pentbox/pentbox-1.8]
└─# ./pentbox.rb

PenTBox 1.8
             __
         U00U|.'@@@@@@`.
         |__|(@@@@@@@@@@@)
              (@@@@@@@@)
              `YY~~~~YY'
               ||    ||

────────── 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

   -> █
```

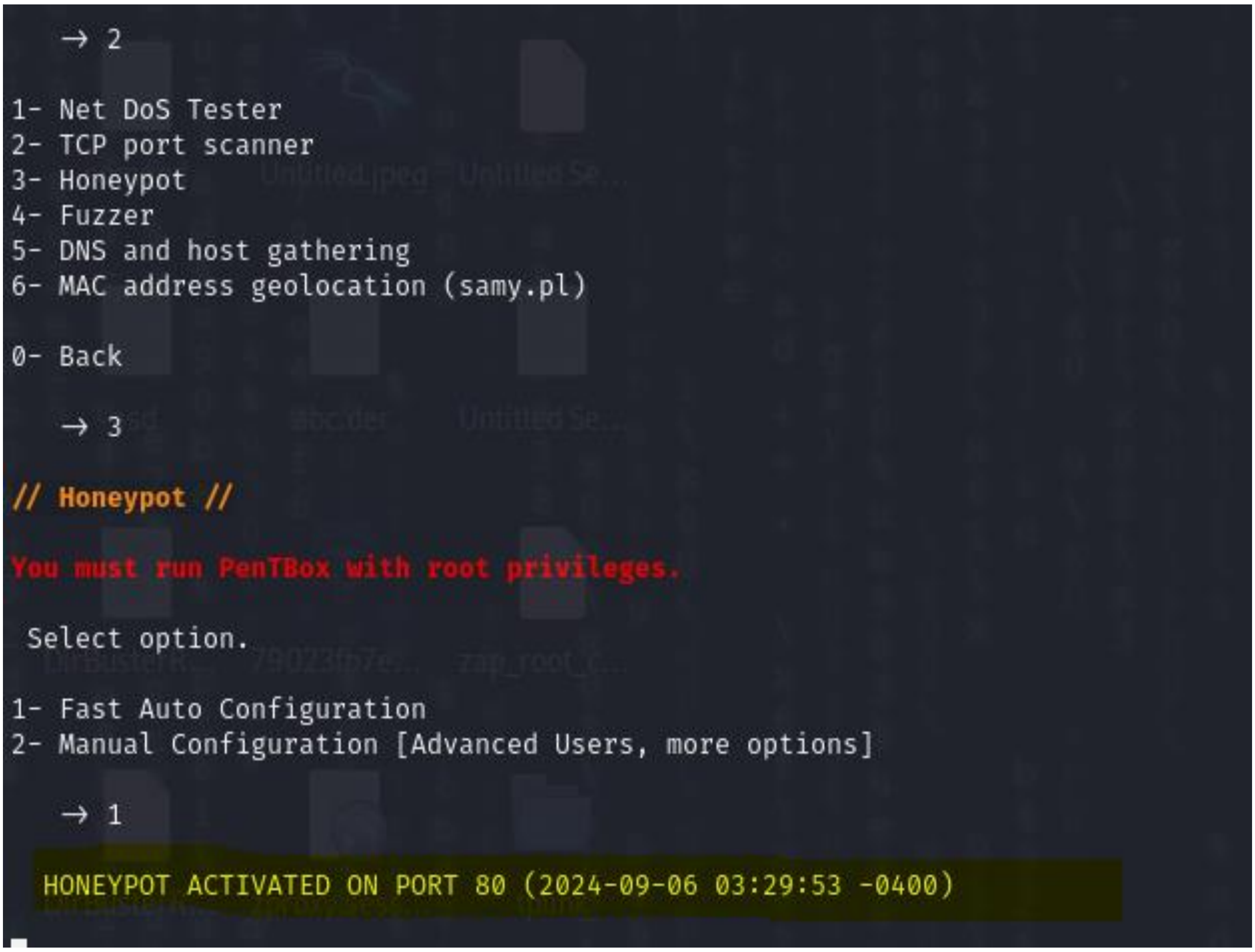
4. Thereafter, we select option 3 i.e Honeypot

5. In Honeypot, we are presented with 2 options:

   Option 1. Fast Auto Configuration

   Option 2. Manual Configuration

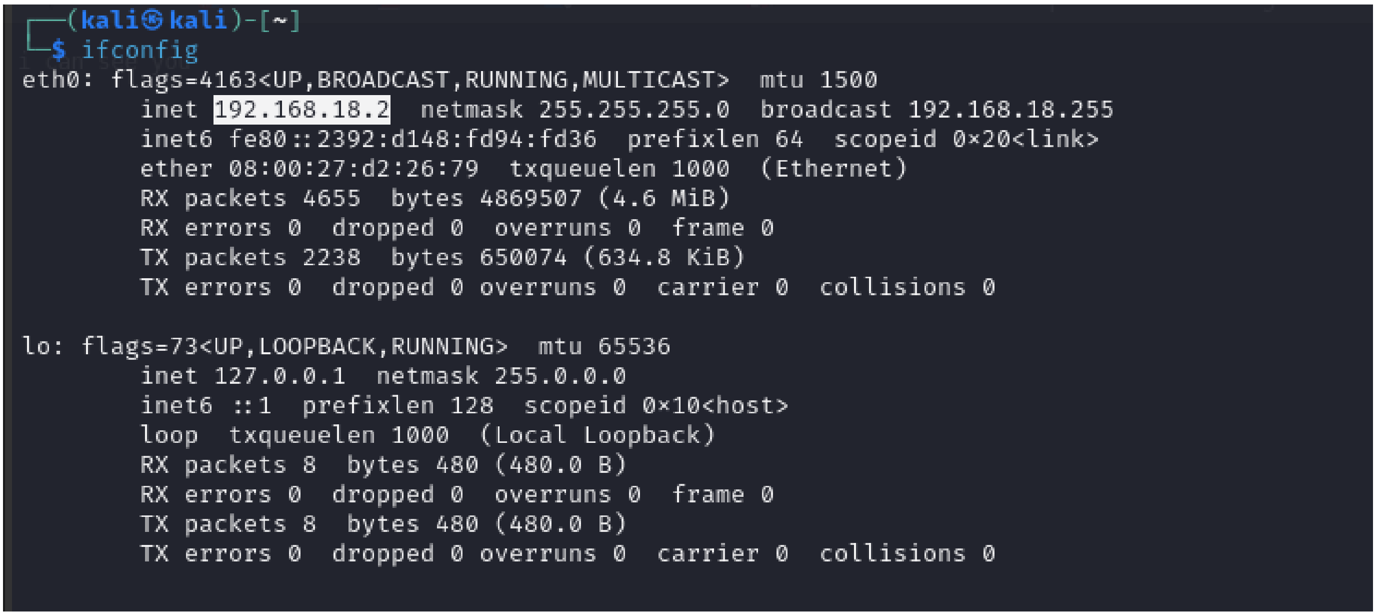
6. Starting with option 1., Honeypot is activated on port 80.



```
   → 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]

   → 1

  HONEYPOT ACTIVATED ON PORT 80 (2024-09-06 03:29:53 -0400)
```

7. Knowing your IP address is essential when setting up a honeypot for a few key reasons. First, it allows you to configure the honeypot to mimic areal system, as attackers typically target specific IP addresses. Secondly, ithelps in monitoring and logging providing insight on attack patterns.

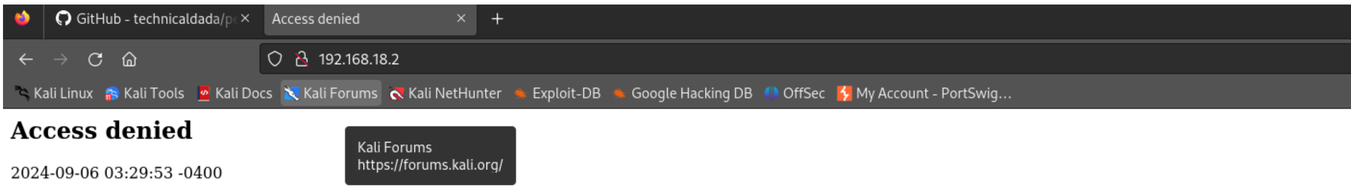
   To obtain and figure out our IP address open another terminal and use this command: $ ifconfig



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.18.2  netmask 255.255.255.0  broadcast 192.168.18.255
        inet6 fe80::2392:d148:fd94:fd36  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d2:26:79  txqueuelen 1000  (Ethernet)
        RX packets 4655  bytes 4869507 (4.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2238  bytes 650074 (634.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

8. Now we open our browser and search for the same IP address.

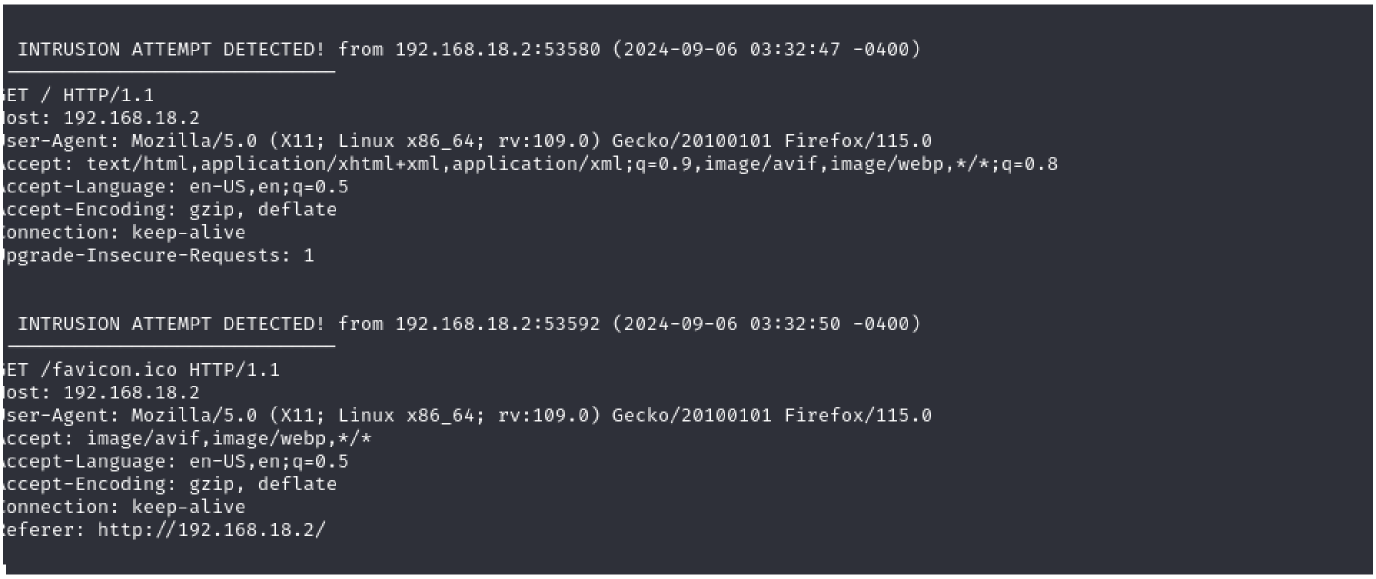
   An "**Access denied**" message appears on the web page.



Access denied

2024-09-06 03:29:53 -0400

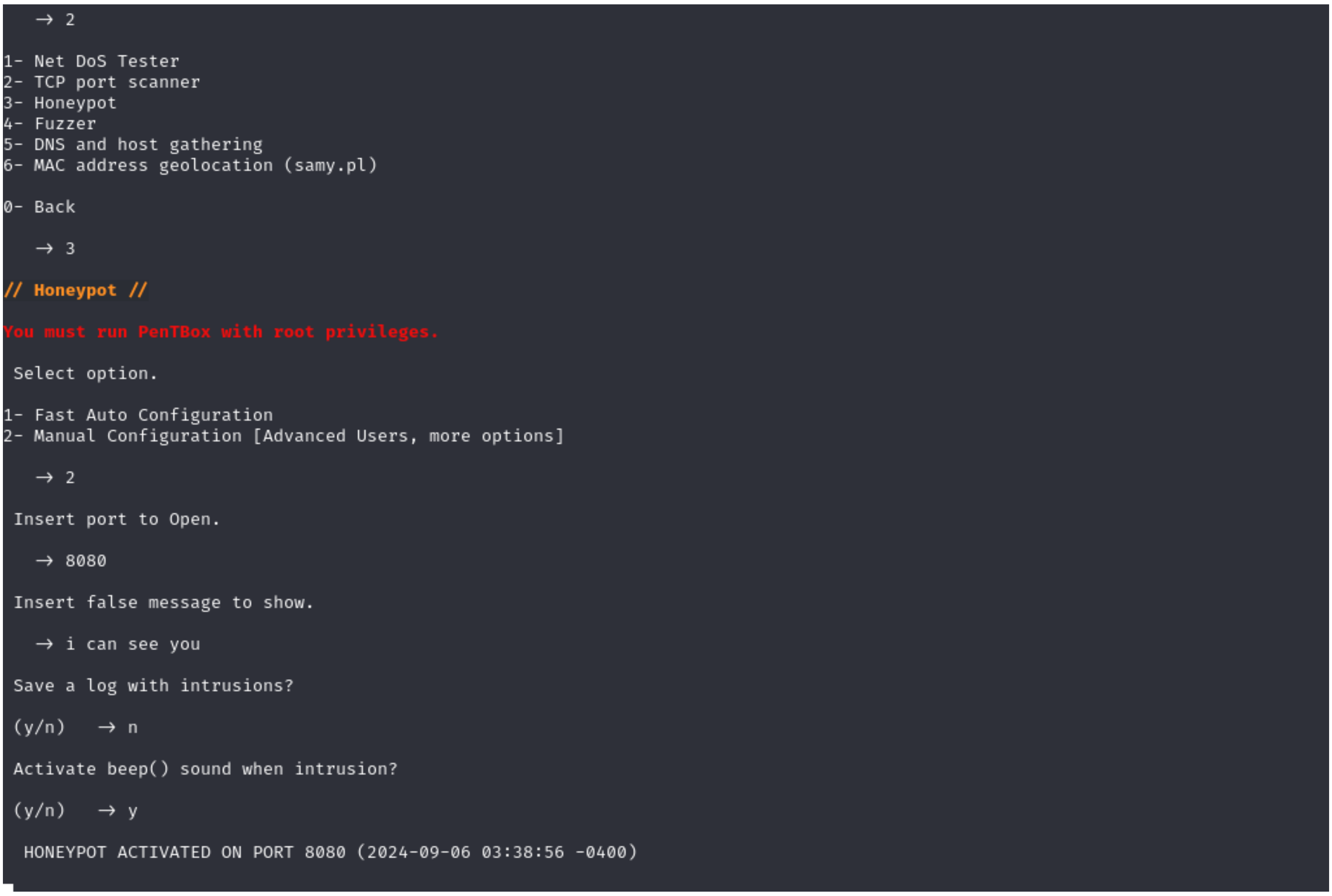
9. The Kali terminal window displays **INTRUSION ATTEMPT DETECTED from 192.168.18.2**



```
 INTRUSION ATTEMPT DETECTED! from 192.168.18.2:53580 (2024-09-06 03:32:47 -0400)
 ──────────────────────────────
ET / HTTP/1.1
ost: 192.168.18.2
ser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
ccept-Language: en-US,en;q=0.5
ccept-Encoding: gzip, deflate
onnection: keep-alive
pgrade-Insecure-Requests: 1


 INTRUSION ATTEMPT DETECTED! from 192.168.18.2:53592 (2024-09-06 03:32:50 -0400)
 ──────────────────────────────
ET /favicon.ico HTTP/1.1
ost: 192.168.18.2
ser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
ccept: image/avif,image/webp,*/*
ccept-Language: en-US,en;q=0.5
ccept-Encoding: gzip, deflate
onnection: keep-alive
eferer: http://192.168.18.2/
```

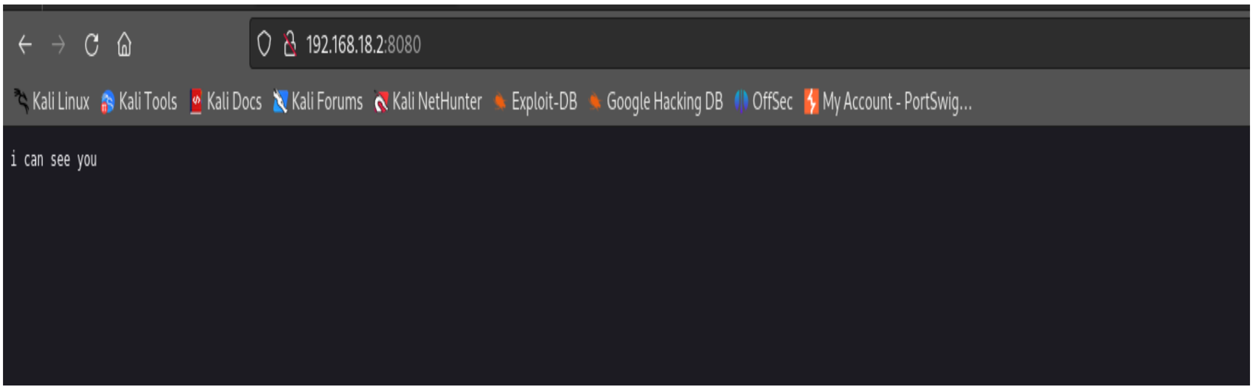
The IDS (Intrusion Detection System) message alerts us about the attempt, the port it is operating on, and the IP address it’s coming from.

10. Now with option 2., we manually configure our honeypot.
    Enter the port number.
    Using port 8080.



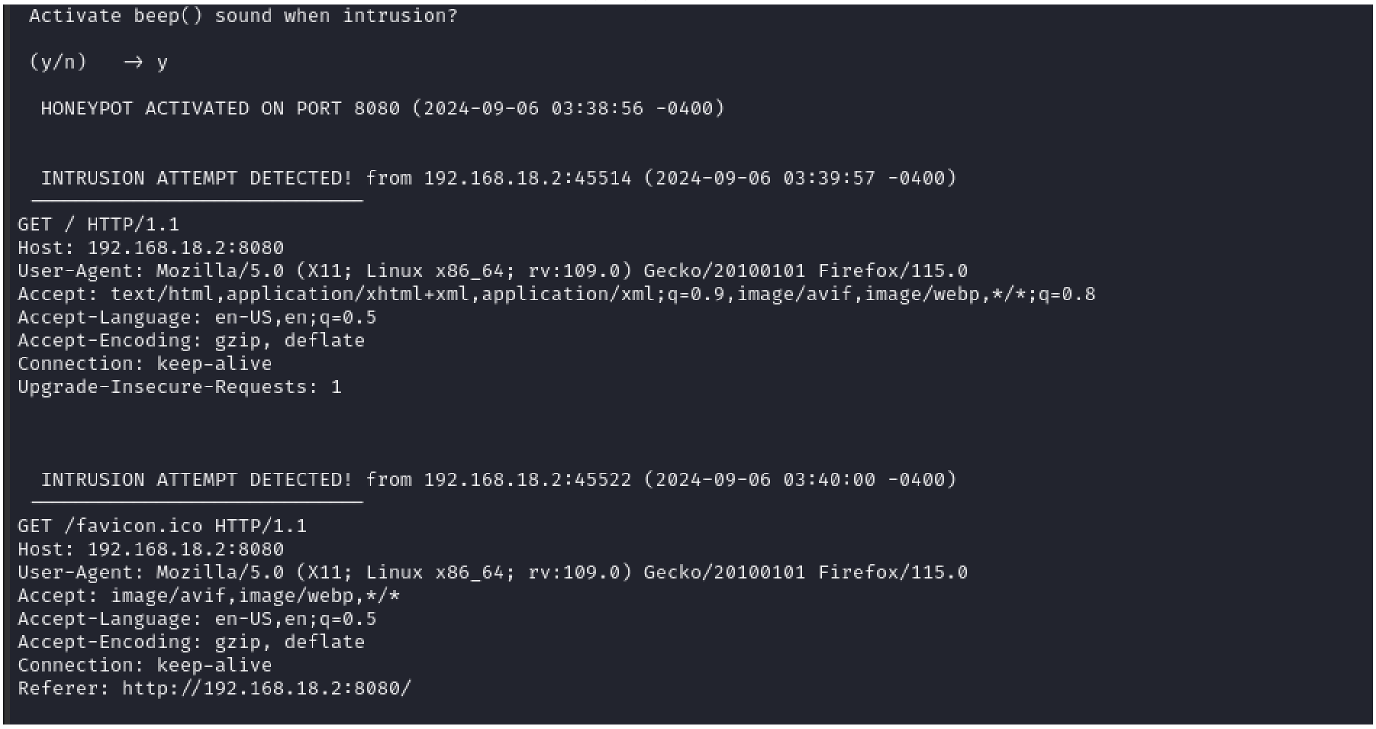
```
   → 2

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.

   → 8080

 Insert false message to show.

   → i can see you

 Save a log with intrusions?

 (y/n)   → n

 Activate beep() sound when intrusion?

 (y/n)   → y

  HONEYPOT ACTIVATED ON PORT 8080 (2024-09-06 03:38:56 -0400)
```

11. An “Access denied” message appears on the web page.



i can see you

12. The Kali terminal window displays **INTRUSION ATTEMPT DETECTED.**



```
 Activate beep() sound when intrusion?

 (y/n)   → y

  HONEYPOT ACTIVATED ON PORT 8080 (2024-09-06 03:38:56 -0400)


  INTRUSION ATTEMPT DETECTED! from 192.168.18.2:45514 (2024-09-06 03:39:57 -0400)
 ─────────────────────────────
GET / HTTP/1.1
Host: 192.168.18.2:8080
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 192.168.18.2:45522 (2024-09-06 03:40:00 -0400)
 ─────────────────────────────
GET /favicon.ico HTTP/1.1
Host: 192.168.18.2:8080
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://192.168.18.2:8080/
```

We see that the attempt was logged and where the IP was originated from.

13. These intrusion attempt alerts by the IDS are logged.

Conclusion: Overall, setting up a Honeypot on Kali Linux using PenTBox was quite useful for me as a student. It provided a hands-on opportunity to apply academic knowledge in a real-world cybersecurity scenario. Configuring the honeypot provided me with useful insights into the complexity of building a simulated environment that attracts and monitors potential cyber threats.