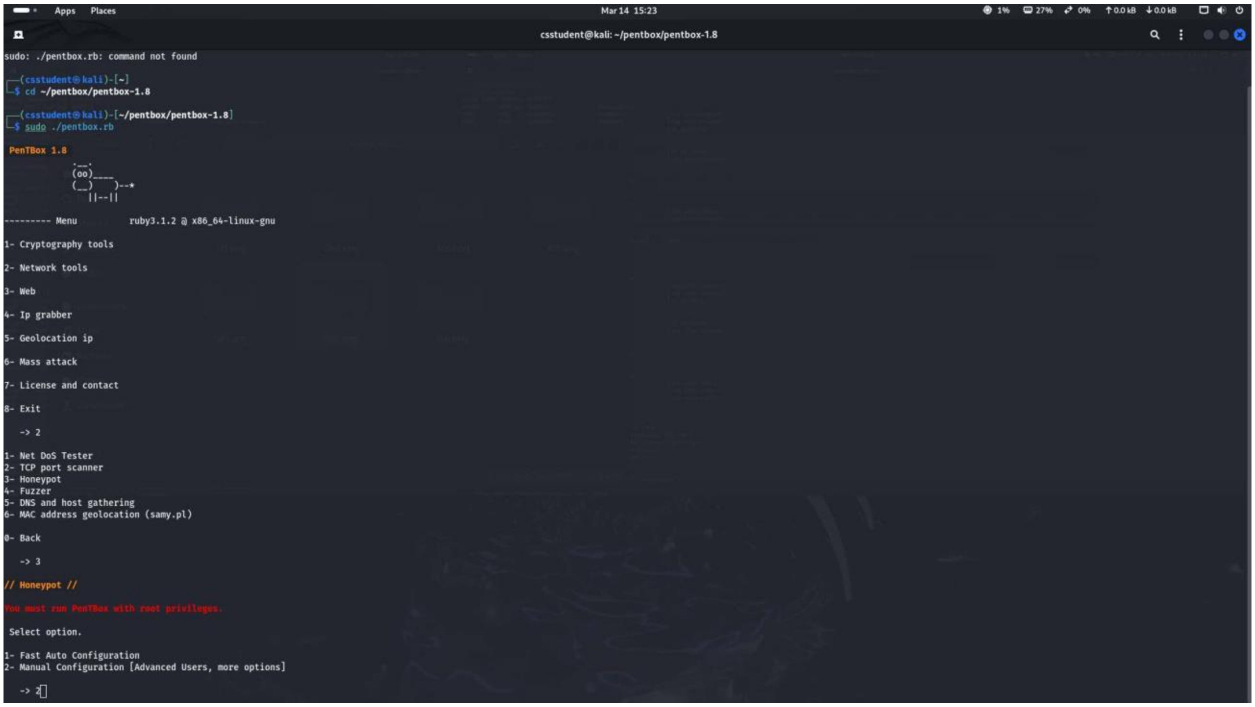
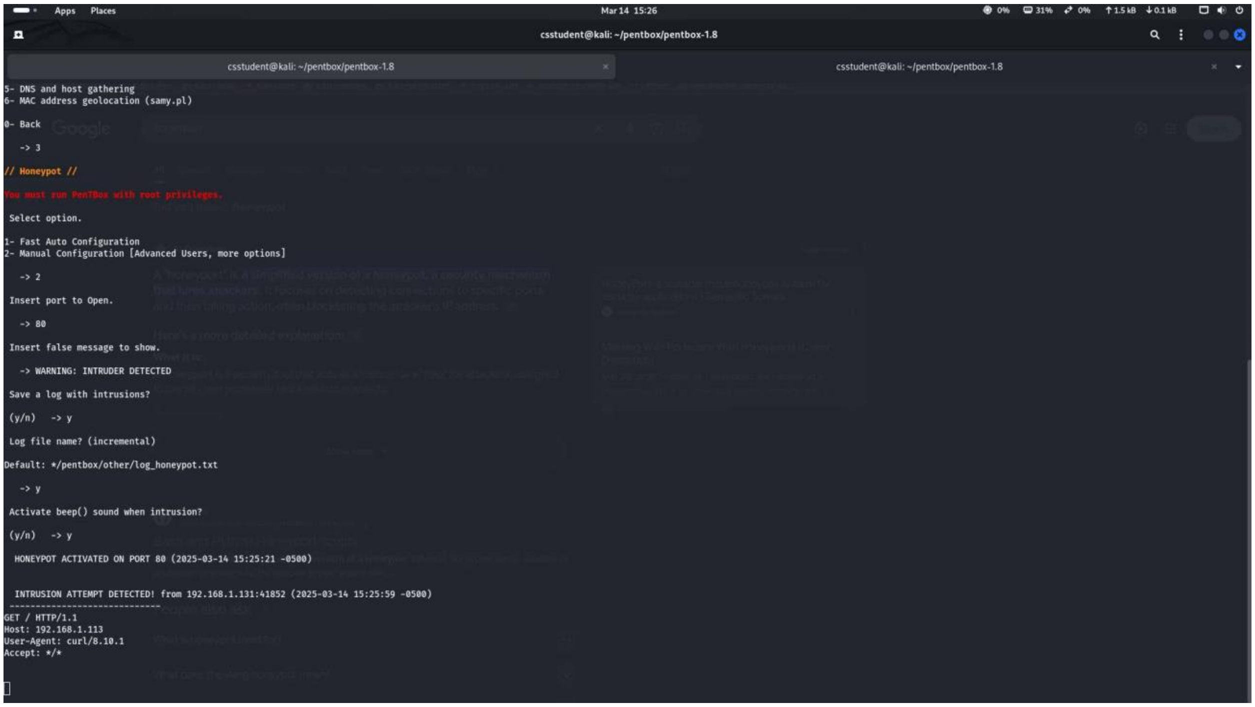
Lab Project: Honeypot Project

I ran Pentbox to set up a honeypot on port 80

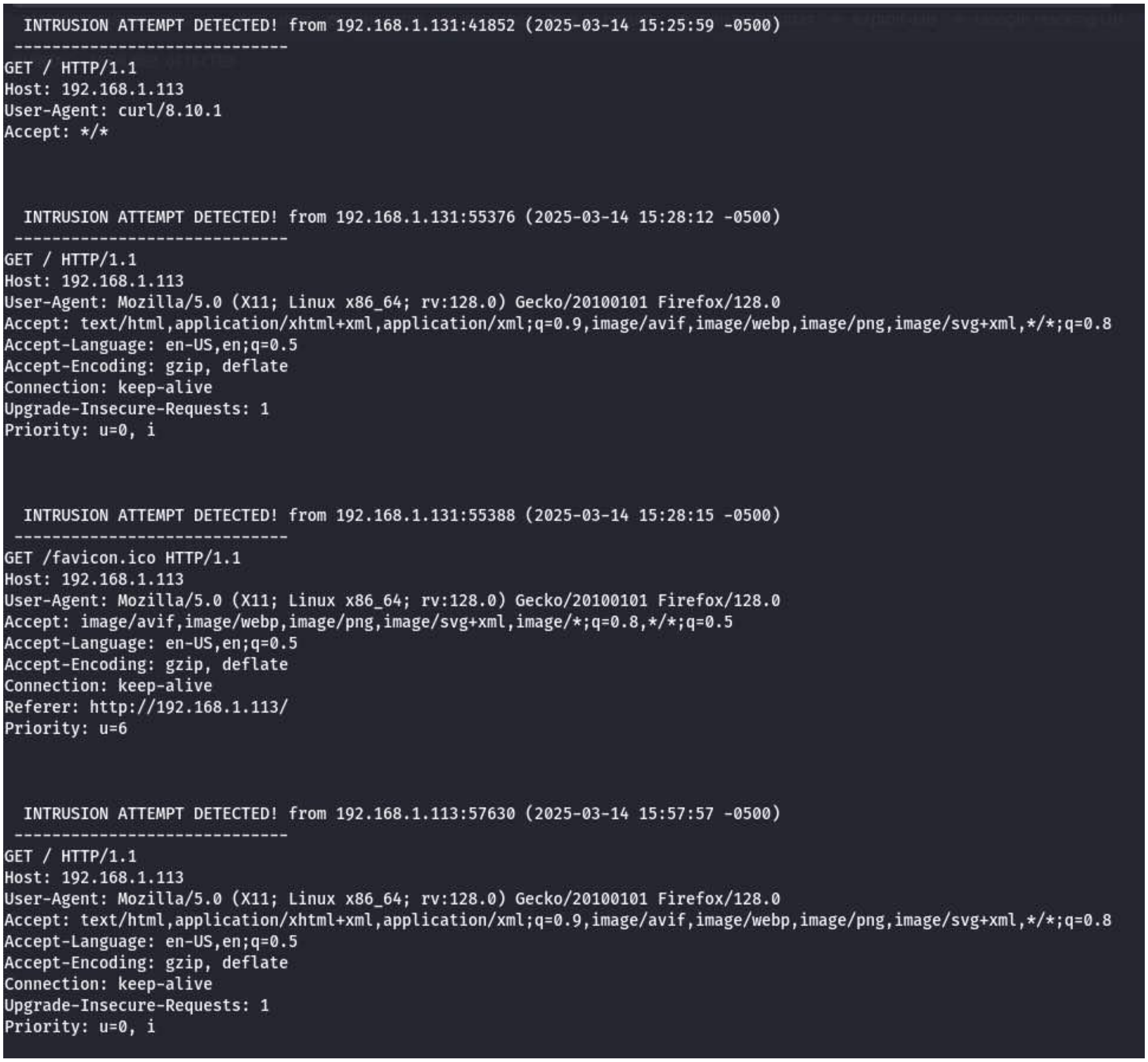


```
sudo: ./pentbox.rb: command not found

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

┌──(csstudent㉿kali)-[~/pentbox/pentbox-1.8]
└─$ sudo ./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

// Honeypot //

You must run PenTBox with root privileges.

 Select option.

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

   -> 2
```

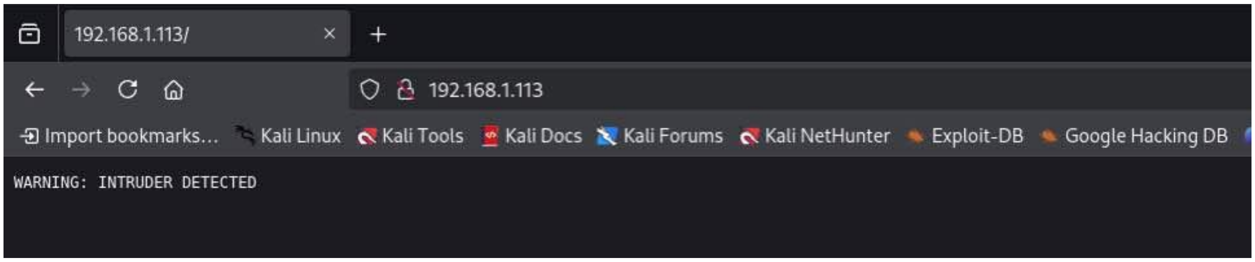

Apps
Places
Mar 14 15:26
csstudent@kali: ~/pentbox/pentbox-1.8
csstudent@kali: ~/pentbox/pentbox-1.8

```
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.

   -> WARNING: INTRUDER DETECTED

 Save a log with intrusions?

 (y/n)   -> y

 Log file name? (incremental)

Default: */pentbox/other/log_honeypot.txt

   -> y

 Activate beep() sound when intrusion?

 (y/n)   -> y

  HONEYPOT ACTIVATED ON PORT 80 (2025-03-14 15:25:21 -0500)


  INTRUSION ATTEMPT DETECTED! from 192.168.1.131:41852 (2025-03-14 15:25:59 -0500)
 -----------------------------
GET / HTTP/1.1
Host: 192.168.1.113
User-Agent: curl/8.10.1
Accept: */*
```

Honeypot is working well in spotting intruders:



```
  INTRUSION ATTEMPT DETECTED! from 192.168.1.131:41852 (2025-03-14 15:25:59 -0500)
 -----------------------------
GET / HTTP/1.1
Host: 192.168.1.113
User-Agent: curl/8.10.1
Accept: */*



  INTRUSION ATTEMPT DETECTED! from 192.168.1.131:55376 (2025-03-14 15:28:12 -0500)
 -----------------------------
GET / HTTP/1.1
Host: 192.168.1.113
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i



  INTRUSION ATTEMPT DETECTED! from 192.168.1.131:55388 (2025-03-14 15:28:15 -0500)
 -----------------------------
GET /favicon.ico HTTP/1.1
Host: 192.168.1.113
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.1.113/
Priority: u=6



  INTRUSION ATTEMPT DETECTED! from 192.168.1.113:57630 (2025-03-14 15:57:57 -0500)
 -----------------------------
GET / HTTP/1.1
Host: 192.168.1.113
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

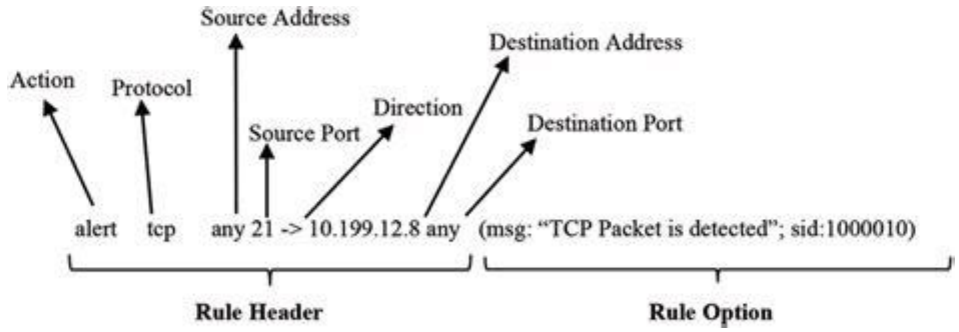


```
WARNING: INTRUDER DETECTED
```

For the IDS, I configure two rules:

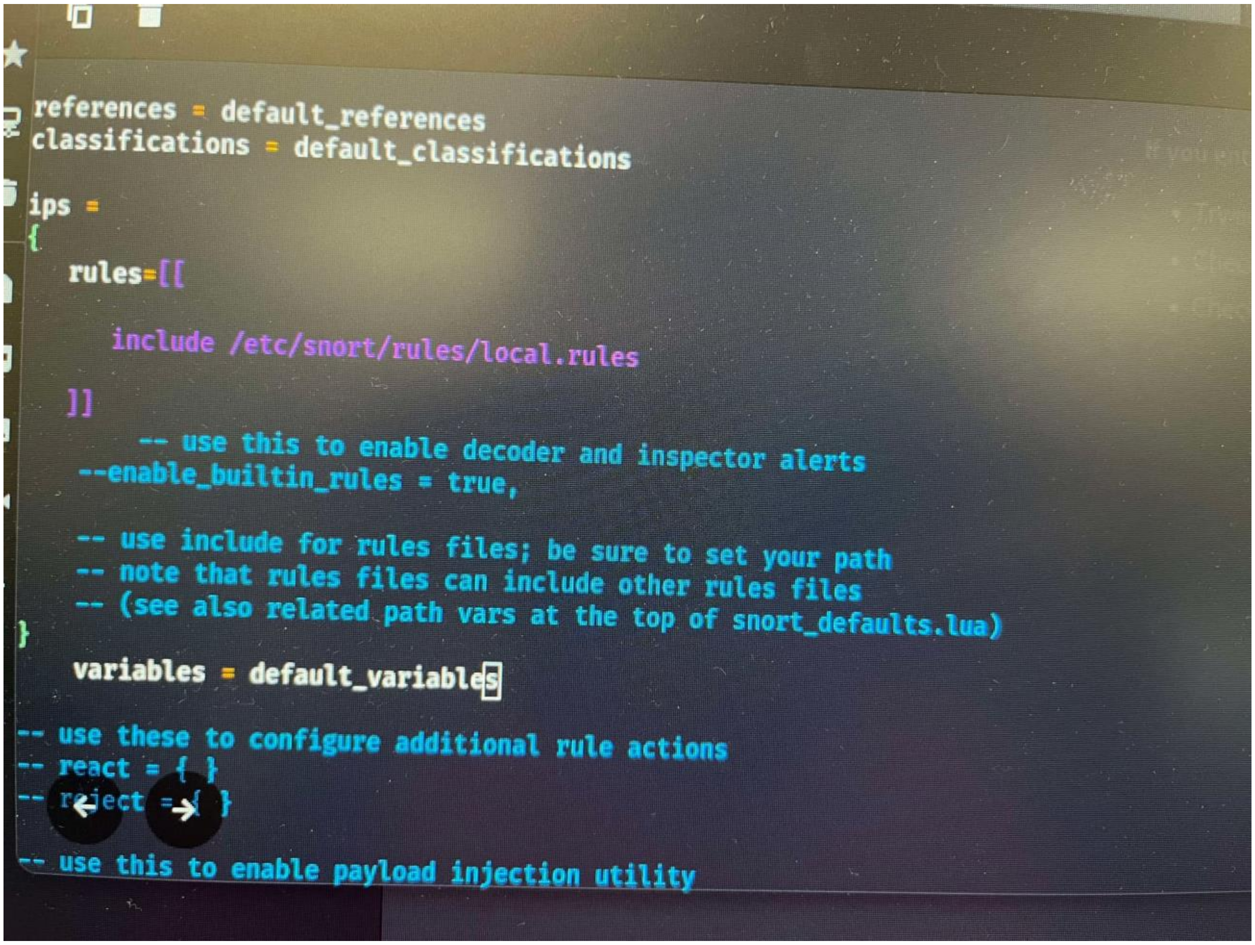
1. ICMP detection
2. FTP connection attempt
3. ssh connection attempt

Following the format below:



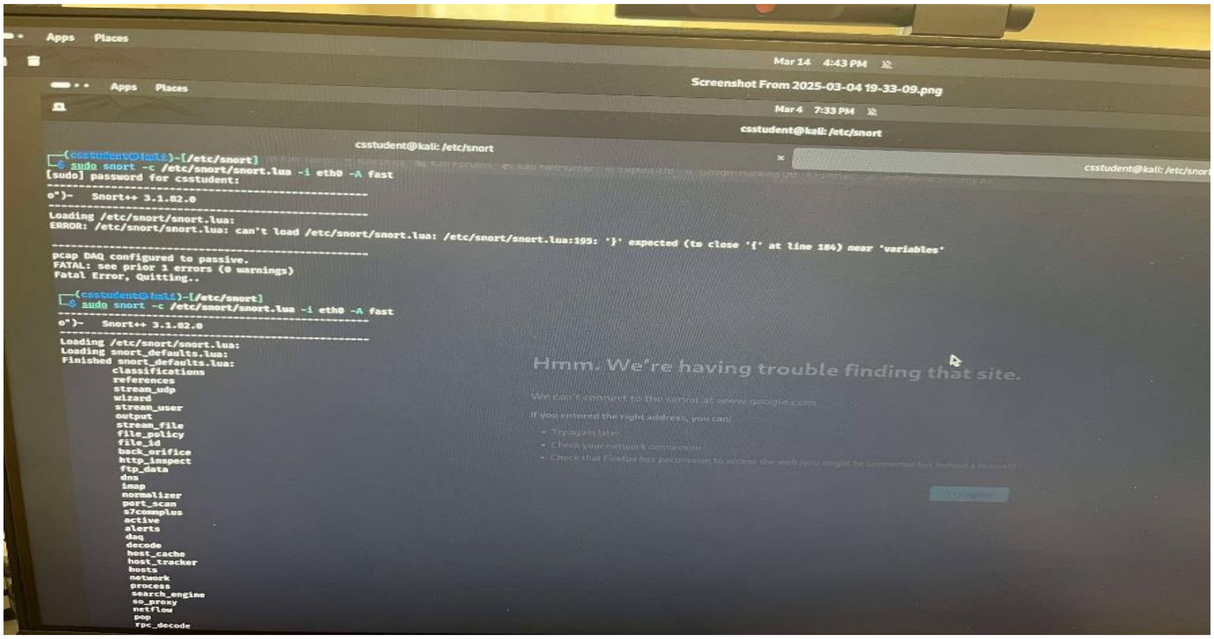
```
alert tcp any 21 -> 10.199.12.8 any (msg: "TCP Packet is detected"; sid:1000010)
```

First add folder to configuration file:



```
references = default_references
classifications = default_classifications

ips =
{
   rules=[[

      include /etc/snort/rules/local.rules

   ]]
          -- use this to enable decoder and inspector alerts
    --enable_builtin_rules = true,

    -- use include for rules files; be sure to set your path
    -- note that rules files can include other rules files
    -- (see also related path vars at the top of snort_defaults.lua)
}
    variables = default_variables

-- use these to configure additional rule actions
-- react = { }
-- reject = { }

-- use this to enable payload injection utility
```

Then, create new local rules. File names local.rules


Apps
Places
Mar 14 4:43 PM
Screenshot From 2025-03-04 19-33-09.png
Apps
Places
Mar 4 7:33 PM
csstudent@kali: /etc/snort
csstudent@kali: /etc/snort
csstudent@kali: /etc/snort

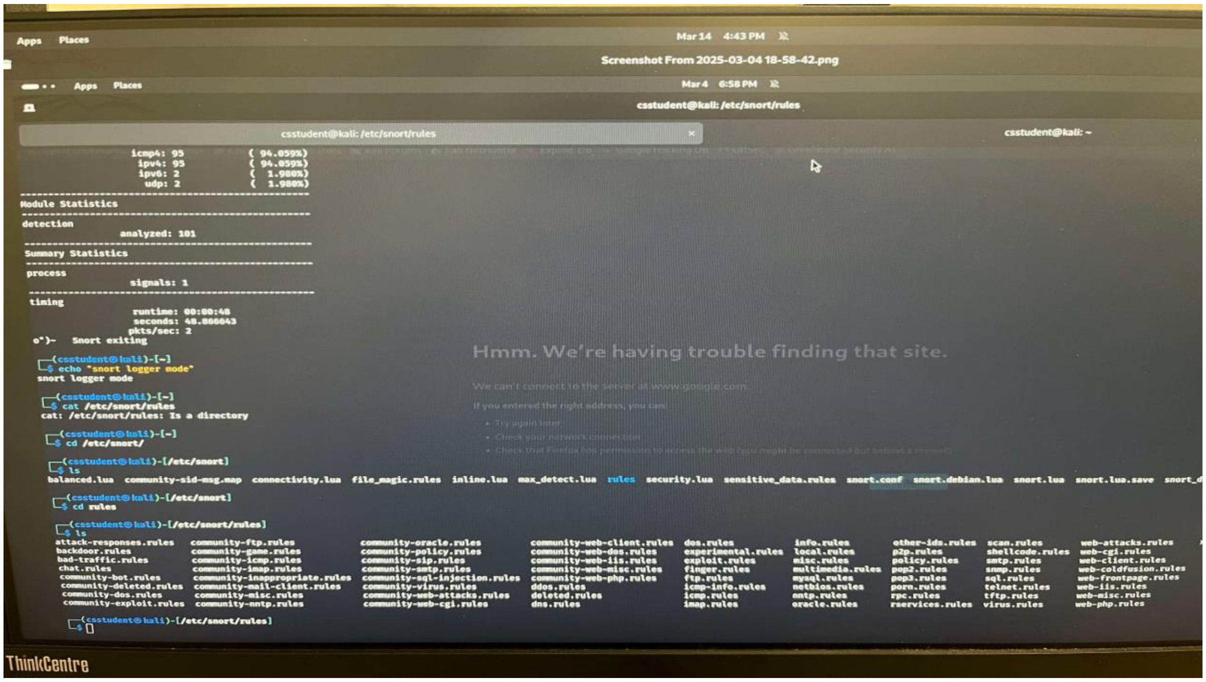
```
┌──(csstudent㉿kali)-[/etc/snort]
└─$ sudo snort -c /etc/snort/snort.lua -i eth0 -A fast
[sudo] password for csstudent:
--------------------------------------------------
o")~   Snort++ 3.1.82.0
--------------------------------------------------
Loading /etc/snort/snort.lua:
ERROR: /etc/snort/snort.lua: can't load /etc/snort/snort.lua: /etc/snort/snort.lua:195: '}' expected (to close '{' at line 184) near 'variables'

--------------------------------------------------
pcap DAQ configured to passive.
FATAL: see prior 1 errors (0 warnings)
Fatal Error, Quitting..

┌──(csstudent㉿kali)-[/etc/snort]
└─$ sudo snort -c /etc/snort/snort.lua -i eth0 -A fast
--------------------------------------------------
o")~   Snort++ 3.1.82.0
--------------------------------------------------
Loading /etc/snort/snort.lua:
Loading snort_defaults.lua:
Finished snort_defaults.lua:
        classifications
        references
        stream_udp
        wizard
        stream_user
        output
        stream_file
        file_policy
        file_id
        back_orifice
        http_inspect
        ftp_data
        dns
        imap
        normalizer
        port_scan
        s7commplus
        active
        alerts
        daq
        decode
        host_cache
        host_tracker
        hosts
        network
        process
        search_engine
        so_proxy
        netflow
        pop
        rpc_decode
```

Hmm. We're having trouble finding that site.

We can't connect to the server at www.google.com.

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)


Apps
Places
Mar 14 4:43 PM
Screenshot From 2025-03-04 18-58-42.png
Apps
Places
Mar 4 6:58 PM
csstudent@kali: /etc/snort/rules
csstudent@kali: /etc/snort/rules
csstudent@kali: ~
ThinkCentre

```
                  icmp4: 95          ( 94.059%)
                   ipv4: 95          ( 94.059%)
                   ipv6: 2           (  1.980%)
                    udp: 2           (  1.980%)
--------------------------------------------------
Module Statistics
--------------------------------------------------
detection
               analyzed: 101
--------------------------------------------------
Summary Statistics
--------------------------------------------------
process
                signals: 1
--------------------------------------------------
timing
                runtime: 00:00:48
                seconds: 48.866643
               pkts/sec: 2
o")~   Snort exiting

┌──(csstudent㉿kali)-[~]
└─$ echo "snort logger mode"
snort logger mode

┌──(csstudent㉿kali)-[~]
└─$ cat /etc/snort/rules
cat: /etc/snort/rules: Is a directory

┌──(csstudent㉿kali)-[~]
└─$ cd /etc/snort/

┌──(csstudent㉿kali)-[/etc/snort]
└─$ ls
balanced.lua  community-sid-msg.map  connectivity.lua  file_magic.rules  inline.lua  max_detect.lua  rules  security.lua  sensitive_data.rules  snort.conf  snort.debian.lua  snort.lua  snort.lua.save  snort_d

┌──(csstudent㉿kali)-[/etc/snort]
└─$ cd rules

┌──(csstudent㉿kali)-[/etc/snort/rules]
└─$ ls
attack-responses.rules    community-ftp.rules                community-oracle.rules          community-web-client.rules  dos.rules           info.rules        other-ids.rules   scan.rules       web-attacks.rules
backdoor.rules            community-game.rules               community-policy.rules          community-web-dos.rules     experimental.rules  local.rules       p2p.rules         shellcode.rules  web-cgi.rules
bad-traffic.rules         community-icmp.rules               community-sip.rules             community-web-iis.rules     exploit.rules       misc.rules        policy.rules      smtp.rules       web-client.rules
chat.rules                community-imap.rules               community-smtp.rules            community-web-misc.rules    finger.rules        multimedia.rules  pop2.rules        snmp.rules       web-coldfusion.rules
community-bot.rules       community-inappropriate.rules      community-sql-injection.rules   community-web-php.rules     ftp.rules           mysql.rules       pop3.rules        sql.rules        web-frontpage.rules
community-deleted.rules   community-mail-client.rules        community-virus.rules           ddos.rules                  icmp-info.rules     netbios.rules     porn.rules        telnet.rules     web-iis.rules
community-dos.rules       community-misc.rules               community-web-attacks.rules     deleted.rules               icmp.rules          nntp.rules        rpc.rules         tftp.rules       web-misc.rules
community-exploit.rules   community-nntp.rules               community-web-cgi.rules         dns.rules                   imap.rules          oracle.rules      rservices.rules   virus.rules      web-php.rules

┌──(csstudent㉿kali)-[/etc/snort/rules]
└─$ ▯
```

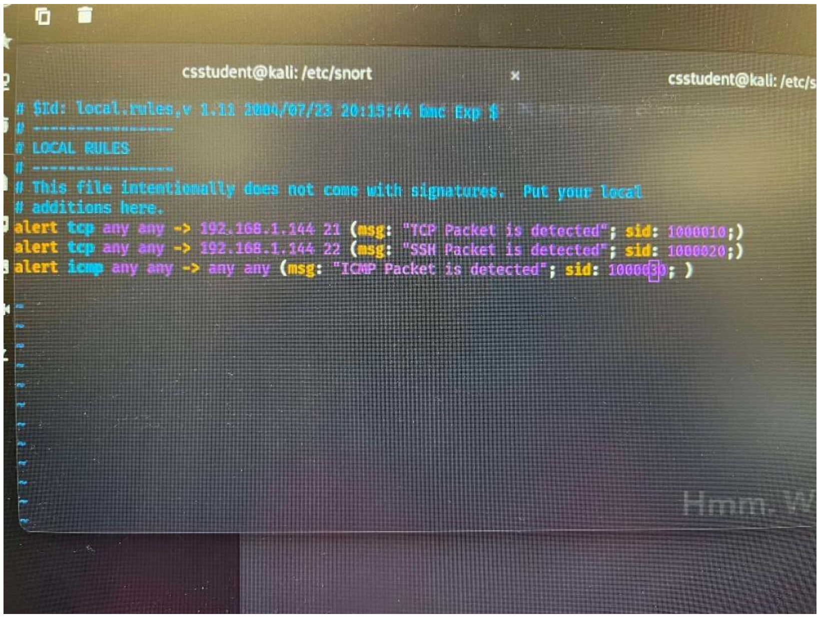
Hmm. We're having trouble finding that site.

We can't connect to the server at www.google.com.

If you entered the right address, you can:

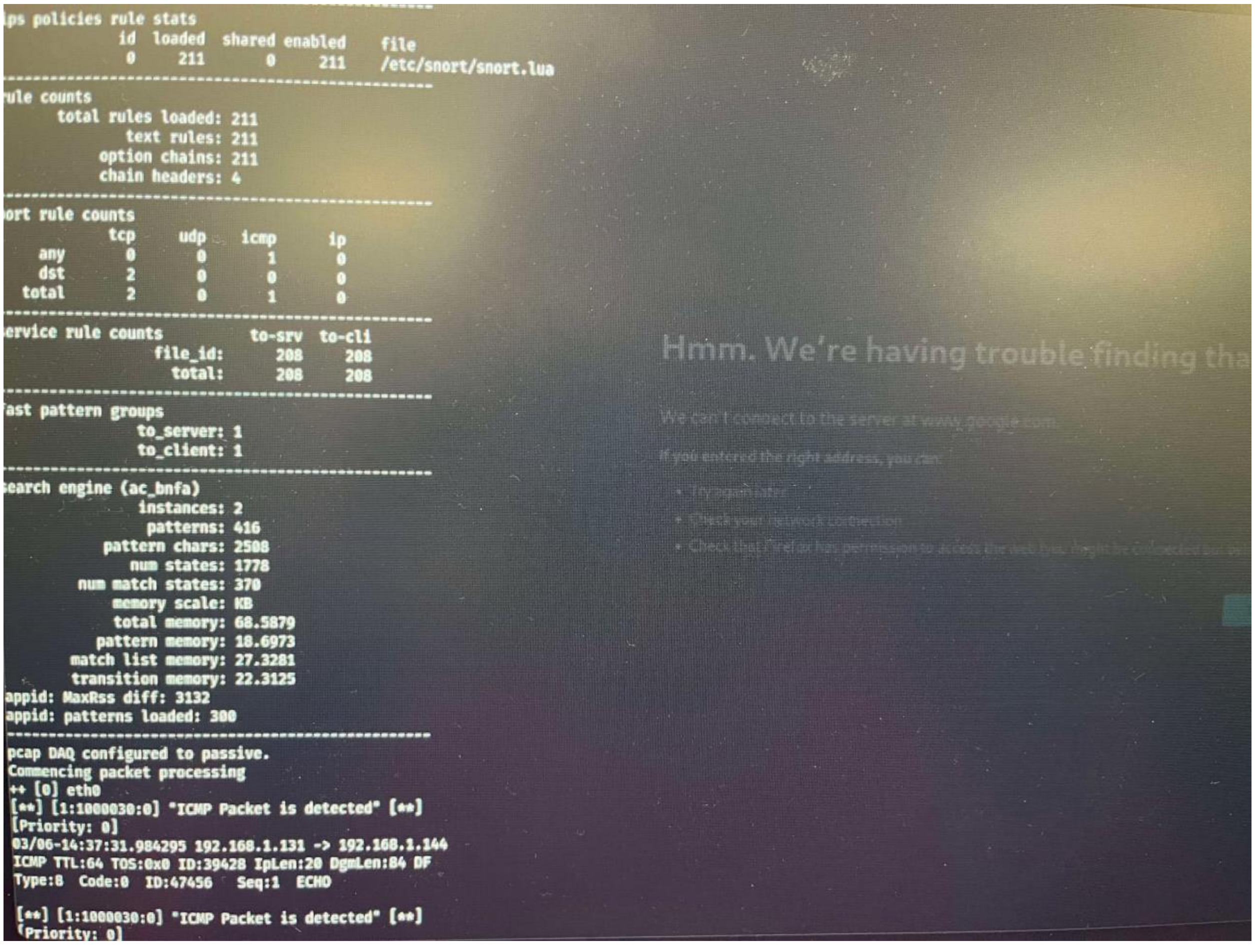
- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

Add rules for ICMP detection, FTP connection attempt, SSH connection attempt

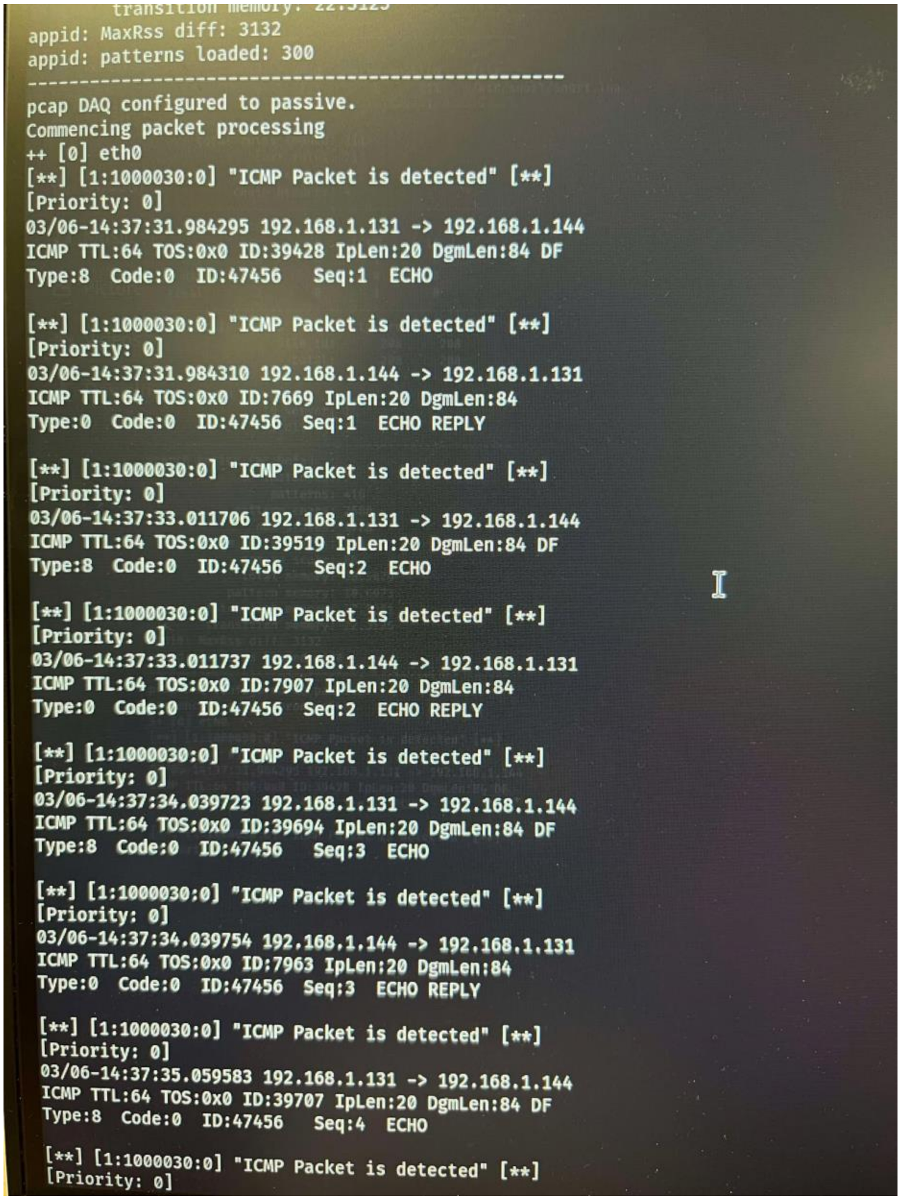


```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert tcp any any -> 192.168.1.144 21 (msg: "TCP Packet is detected"; sid: 1000010;)
alert tcp any any -> 192.168.1.144 22 (msg: "SSH Packet is detected"; sid: 1000020;)
alert icmp any any -> any any (msg: "ICMP Packet is detected"; sid: 1000030; )
```

Test with ICMP, use another computer to ping this computer



```
ips policies rule stats
              id  loaded  shared enabled    file
               0     211       0     211    /etc/snort/snort.lua
--------------------------------------------------
ule counts
       total rules loaded: 211
               text rules: 211
            option chains: 211
            chain headers: 4
--------------------------------------------------
ort rule counts
             tcp     udp    icmp      ip
     any       0       0       1       0
     dst       2       0       0       0
   total       2       0       1       0
--------------------------------------------------
ervice rule counts          to-srv  to-cli
                  file_id:     208     208
                    total:     208     208
--------------------------------------------------
ast pattern groups
                to_server: 1
                to_client: 1
--------------------------------------------------
earch engine (ac_bnfa)
                instances: 2
                 patterns: 416
            pattern chars: 2508
               num states: 1778
         num match states: 370
             memory scale: KB
             total memory: 68.5879
           pattern memory: 18.6973
        match list memory: 27.3281
        transition memory: 22.3125
appid: MaxRss diff: 3132
appid: patterns loaded: 300
--------------------------------------------------
pcap DAQ configured to passive.
Commencing packet processing
++ [0] eth0
[**] [1:1000030:0] "ICMP Packet is detected" [**]
[Priority: 0]
03/06-14:37:31.984295 192.168.1.131 -> 192.168.1.144
ICMP TTL:64 TOS:0x0 ID:39428 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:47456   Seq:1  ECHO

[**] [1:1000030:0] "ICMP Packet is detected" [**]
[Priority: 0]
```



```
        transition memory: 22.3125
appid: MaxRss diff: 3132
appid: patterns loaded: 300
--------------------------------------------------
pcap DAQ configured to passive.
Commencing packet processing
++ [0] eth0
[**] [1:1000030:0] "ICMP Packet is detected" [**]
[Priority: 0]
03/06-14:37:31.984295 192.168.1.131 -> 192.168.1.144
ICMP TTL:64 TOS:0x0 ID:39428 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:47456   Seq:1  ECHO

[**] [1:1000030:0] "ICMP Packet is detected" [**]
[Priority: 0]
03/06-14:37:31.984310 192.168.1.144 -> 192.168.1.131
ICMP TTL:64 TOS:0x0 ID:7669 IpLen:20 DgmLen:84
Type:0  Code:0  ID:47456  Seq:1  ECHO REPLY

[**] [1:1000030:0] "ICMP Packet is detected" [**]
[Priority: 0]
03/06-14:37:33.011706 192.168.1.131 -> 192.168.1.144
ICMP TTL:64 TOS:0x0 ID:39519 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:47456   Seq:2  ECHO

[**] [1:1000030:0] "ICMP Packet is detected" [**]
[Priority: 0]
03/06-14:37:33.011737 192.168.1.144 -> 192.168.1.131
ICMP TTL:64 TOS:0x0 ID:7907 IpLen:20 DgmLen:84
Type:0  Code:0  ID:47456  Seq:2  ECHO REPLY

[**] [1:1000030:0] "ICMP Packet is detected" [**]
[Priority: 0]
03/06-14:37:34.039723 192.168.1.131 -> 192.168.1.144
ICMP TTL:64 TOS:0x0 ID:39694 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:47456   Seq:3  ECHO

[**] [1:1000030:0] "ICMP Packet is detected" [**]
[Priority: 0]
03/06-14:37:34.039754 192.168.1.144 -> 192.168.1.131
ICMP TTL:64 TOS:0x0 ID:7963 IpLen:20 DgmLen:84
Type:0  Code:0  ID:47456  Seq:3  ECHO REPLY

[**] [1:1000030:0] "ICMP Packet is detected" [**]
[Priority: 0]
03/06-14:37:35.059583 192.168.1.131 -> 192.168.1.144
ICMP TTL:64 TOS:0x0 ID:39707 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:47456   Seq:4  ECHO

[**] [1:1000030:0] "ICMP Packet is detected" [**]
[Priority: 0]
```

Through the lab exercises, I learned about how to prevent cyber-attacks and malware by setting up Firewall rules in Windows and Iptables in Kali Linux. How to set up an IDS called Snort to detect attacks and intruders. And I learned how to create a honeypot with Pentbox to protect the server by trapping the attackers with the honeypot.

The most interesting thing to me is the honeypot, it works well by playing as a trap for intruders, and we can get notices when someone tries to get into the server.