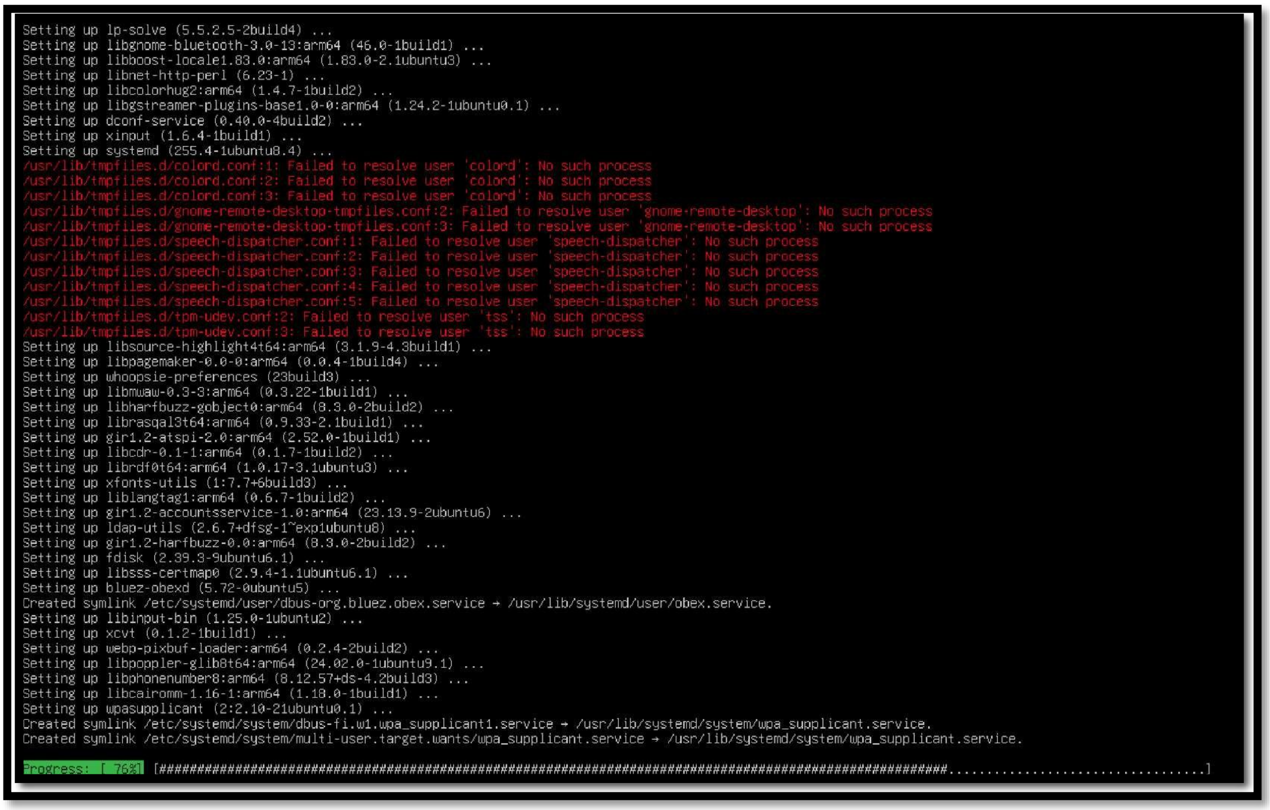
Enhancing Network Security with Snort IDS and Honeypot Integration

INSTALL URUNTU (LINUX OS) SYSTEM

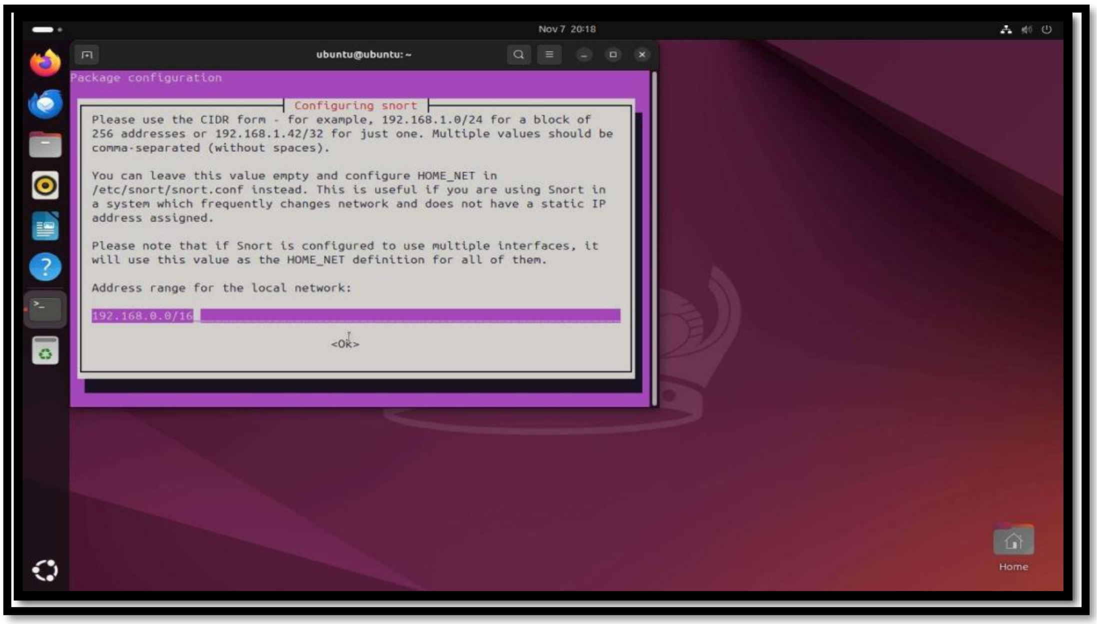


```
Setting up lp-solve (5.5.2.5-2build4) ...
Setting up libgnome-bluetooth-3.0-13:arm64 (46.0-1build1) ...
Setting up libboost-locale1.83.0:arm64 (1.83.0-2.1ubuntu3) ...
Setting up libnet-http-perl (6.23-1) ...
Setting up libcolorhug2:arm64 (1.4.7-1build2) ...
Setting up libgstreamer-plugins-base1.0-0:arm64 (1.24.2-1ubuntu0.1) ...
Setting up dconf-service (0.40.0-4build2) ...
Setting up xinput (1.6.4-1build1) ...
Setting up systemd (255.4-1ubuntu8.4) ...
/usr/lib/tmpfiles.d/colord.conf:1: Failed to resolve user 'colord': No such process
/usr/lib/tmpfiles.d/colord.conf:2: Failed to resolve user 'colord': No such process
/usr/lib/tmpfiles.d/colord.conf:3: Failed to resolve user 'colord': No such process
/usr/lib/tmpfiles.d/gnome-remote-desktop-tmpfiles.conf:2: Failed to resolve user 'gnome-remote-desktop': No such process
/usr/lib/tmpfiles.d/gnome-remote-desktop-tmpfiles.conf:3: Failed to resolve user 'gnome-remote-desktop': No such process
/usr/lib/tmpfiles.d/speech-dispatcher.conf:1: Failed to resolve user 'speech-dispatcher': No such process
/usr/lib/tmpfiles.d/speech-dispatcher.conf:2: Failed to resolve user 'speech-dispatcher': No such process
/usr/lib/tmpfiles.d/speech-dispatcher.conf:3: Failed to resolve user 'speech-dispatcher': No such process
/usr/lib/tmpfiles.d/speech-dispatcher.conf:4: Failed to resolve user 'speech-dispatcher': No such process
/usr/lib/tmpfiles.d/speech-dispatcher.conf:5: Failed to resolve user 'speech-dispatcher': No such process
/usr/lib/tmpfiles.d/tpm-udev.conf:2: Failed to resolve user 'tss': No such process
/usr/lib/tmpfiles.d/tpm-udev.conf:3: Failed to resolve user 'tss': No such process
Setting up libsource-highlight4t64:arm64 (3.1.9-4.3build1) ...
Setting up libpagemaker-0.0-0:arm64 (0.0.4-1build4) ...
Setting up whoopsie-preferences (23build3) ...
Setting up libmwaw-0.3-3:arm64 (0.3.22-1build1) ...
Setting up libharfbuzz-gobject0:arm64 (8.3.0-2build2) ...
Setting up librasqal3t64:arm64 (0.9.33-2.1build1) ...
Setting up gir1.2-atspi-2.0:arm64 (2.52.0-1build1) ...
Setting up libcdr-0.1-1:arm64 (0.1.7-1build2) ...
Setting up librdf0t64:arm64 (1.0.17-3.1ubuntu3) ...
Setting up xfonts-utils (1:7.7+6build3) ...
Setting up liblangtag1:arm64 (0.6.7-1build2) ...
Setting up gir1.2-accountsservice-1.0:arm64 (23.13.9-2ubuntu6) ...
Setting up ldap-utils (2.6.7+dfsg-1~exp1ubuntu8) ...
Setting up gir1.2-harfbuzz-0.0:arm64 (8.3.0-2build2) ...
Setting up fdisk (2.39.3-9ubuntu6.1) ...
Setting up libsss-certmap0 (2.9.4-1.1ubuntu6.1) ...
Setting up bluez-obexd (5.72-0ubuntu5) ...
Created symlink /etc/systemd/user/dbus-org.bluez.obex.service → /usr/lib/systemd/user/obex.service.
Setting up libinput-bin (1.25.0-1ubuntu2) ...
Setting up xcvt (0.1.2-1build1) ...
Setting up webp-pixbuf-loader:arm64 (0.2.4-2build2) ...
Setting up libpoppler-glib8t64:arm64 (24.02.0-1ubuntu9.1) ...
Setting up libphonenumber8:arm64 (8.12.57+ds-4.2build3) ...
Setting up libcairomm-1.16-1:arm64 (1.18.0-1build1) ...
Setting up wpasupplicant (2:2.10-21ubuntu0.1) ...
Created symlink /etc/systemd/system/dbus-fi.w1.wpa_supplicant1.service → /usr/lib/systemd/system/wpa_supplicant.service.
Created symlink /etc/systemd/system/multi-user.target.wants/wpa_supplicant.service → /usr/lib/systemd/system/wpa_supplicant.service.

Progress: [ 76%] [########################################################################################################..................................]
```

- Install Ubuntu on a dedicated machine or virtual machine. This will be used for Snort.
- A lightweight Linux distribution like Debian is recommended for the honeypot (Pentbox).

INSTALL SORT TOOL

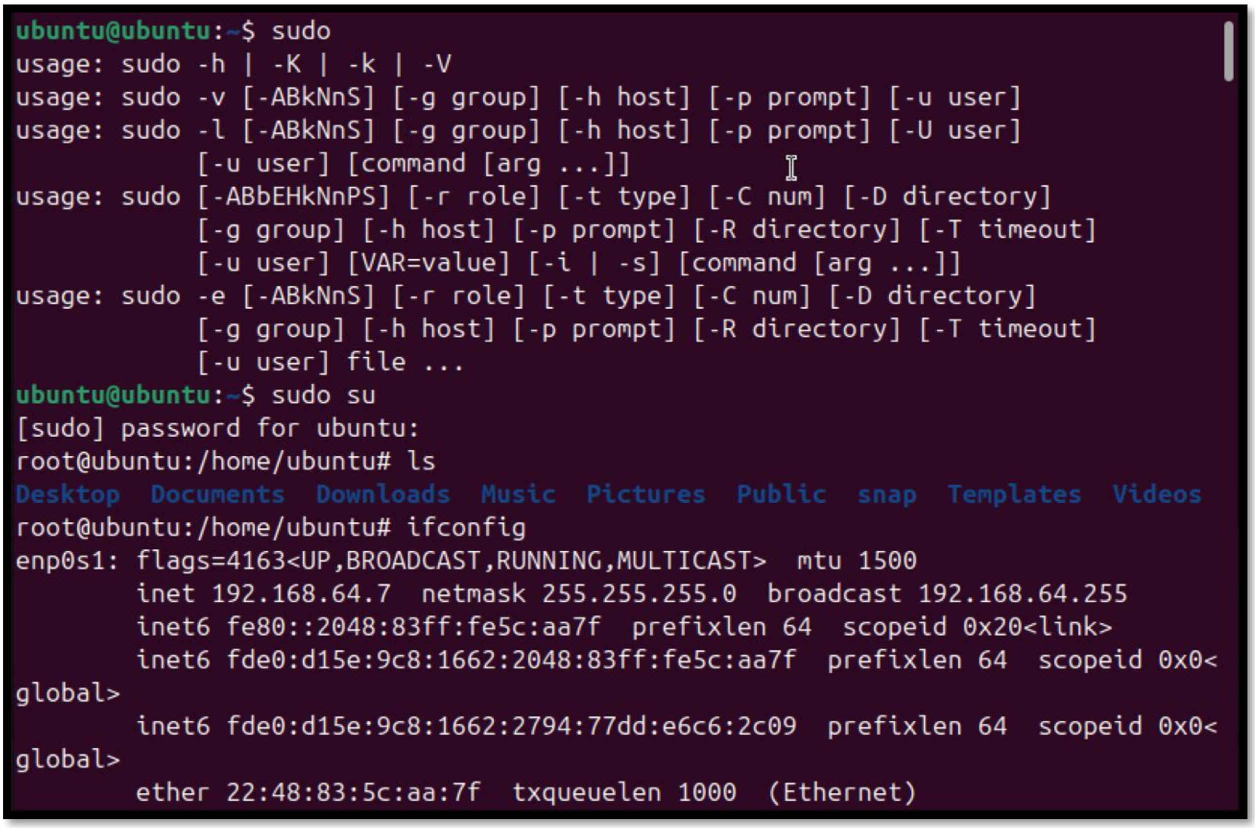
- Install Snort on the Ubuntu system. This typically involves downloading the Snort package, configuring dependencies, and compiling/installing.



```
Package configuration

                  Configuring snort
Please use the CIDR form - for example, 192.168.1.0/24 for a block of
256 addresses or 192.168.1.42/32 for just one. Multiple values should be
comma-separated (without spaces).

You can leave this value empty and configure HOME_NET in
/etc/snort/snort.conf instead. This is useful if you are using Snort in
a system which frequently changes network and does not have a static IP
address assigned.

Please note that if Snort is configured to use multiple interfaces, it
will use this value as the HOME_NET definition for all of them.

Address range for the local network:

192.168.0.0/16

                         <Ok>
```

IP GATHERING

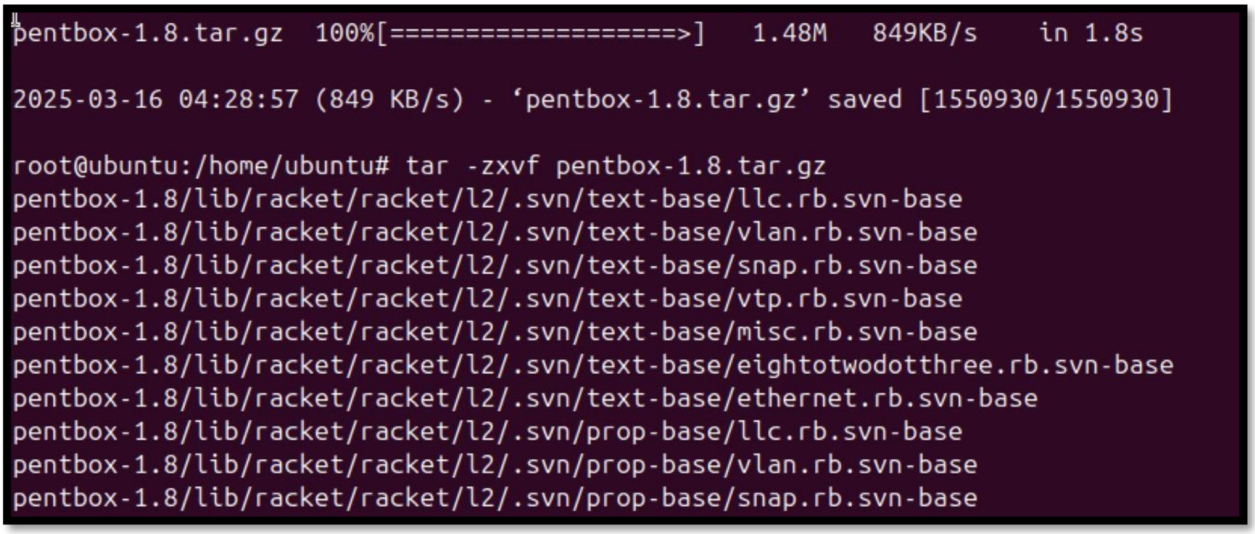
- Gather IP addresses:
  - Identify the IP address of the Ubuntu system where Snort is installed.
  - Determine the IP address that the Pentbox honeypot will use. This IP should be on an isolated network segment.
- (This step might be better named "Network Configuration")



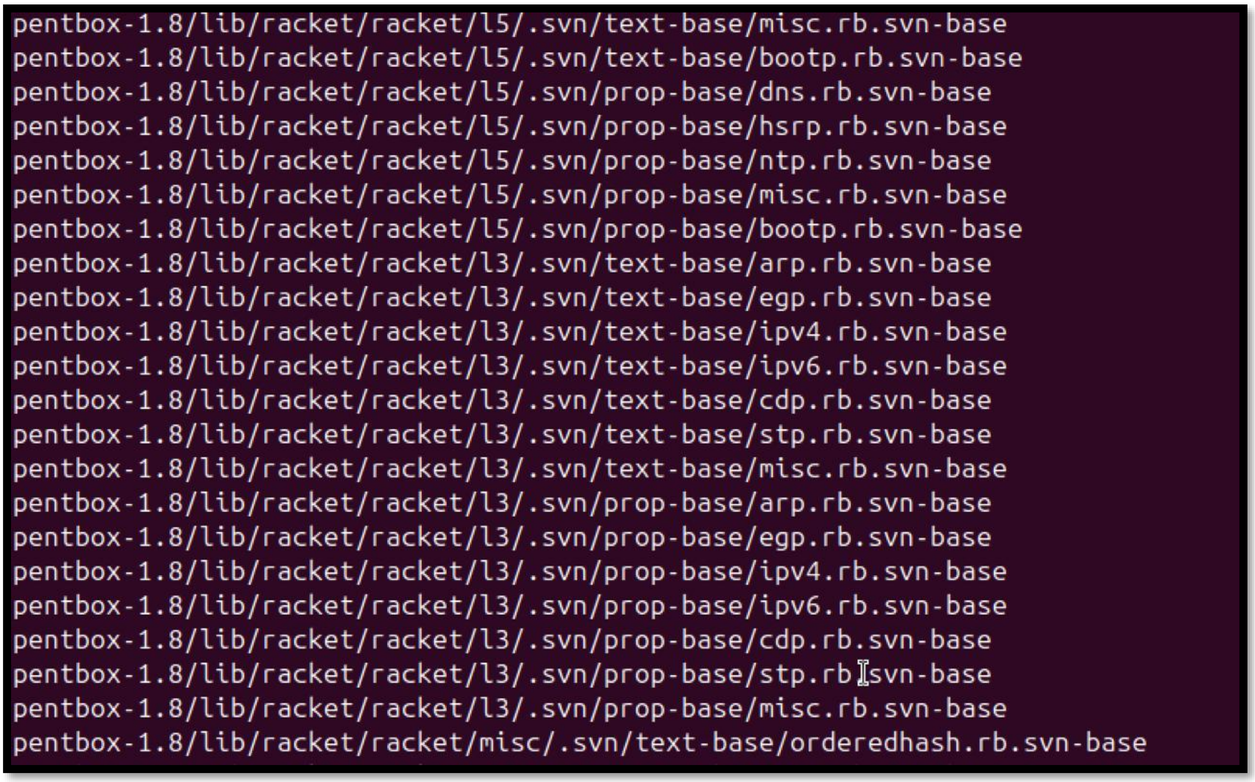
```
ubuntu@ubuntu:~$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-ABkNnS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-ABkNnS] [-g group] [-h host] [-p prompt] [-U user]
            [-u user] [command [arg ...]]
usage: sudo [-ABbEHkNnPS] [-r role] [-t type] [-C num] [-D directory]
            [-g group] [-h host] [-p prompt] [-R directory] [-T timeout]
            [-u user] [VAR=value] [-i | -s] [command [arg ...]]
usage: sudo -e [-ABkNnS] [-r role] [-t type] [-C num] [-D directory]
            [-g group] [-h host] [-p prompt] [-R directory] [-T timeout]
            [-u user] file ...
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu# ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos
root@ubuntu:/home/ubuntu# ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.64.7  netmask 255.255.255.0  broadcast 192.168.64.255
        inet6 fe80::2048:83ff:fe5c:aa7f  prefixlen 64  scopeid 0x20<link>
        inet6 fde0:d15e:9c8:1662:2048:83ff:fe5c:aa7f  prefixlen 64  scopeid 0x0<
global>
        inet6 fde0:d15e:9c8:1662:2794:77dd:e6c6:2c09  prefixlen 64  scopeid 0x0<
global>
        ether 22:48:83:5c:aa:7f  txqueuelen 1000  (Ethernet)
```

UNZIPPING PENTBOX PACKAGES

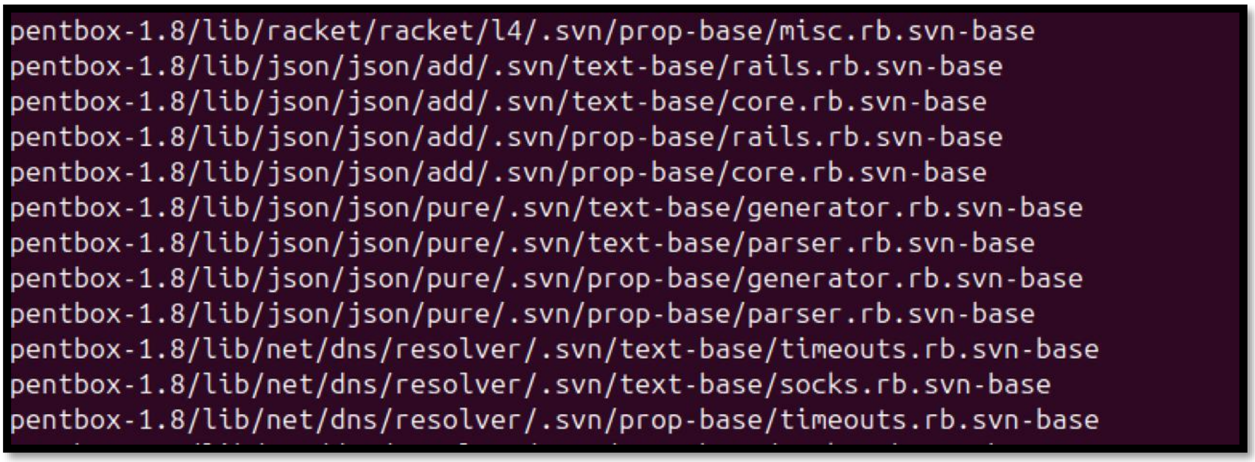
- Unzip the Pentbox package on the Debian system.



```
pentbox-1.8.tar.gz  100%[===================>]   1.48M   849KB/s    in 1.8s

2025-03-16 04:28:57 (849 KB/s) - ‘pentbox-1.8.tar.gz’ saved [1550930/1550930]

root@ubuntu:/home/ubuntu# tar -zxvf pentbox-1.8.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
```



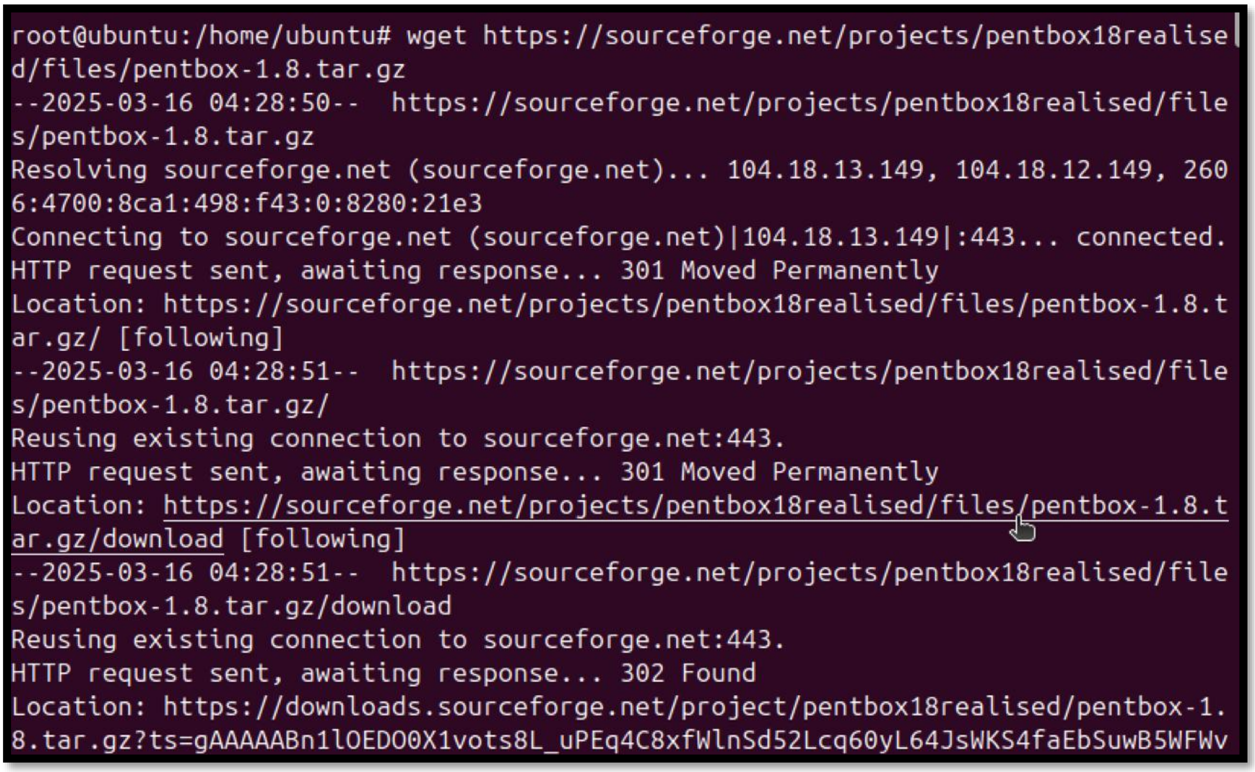
```
pentbox-1.8/lib/racket/racket/l5/.svn/text-base/misc.rb.svn-base
pentbox-1.8/lib/racket/racket/l5/.svn/text-base/bootp.rb.svn-base
pentbox-1.8/lib/racket/racket/l5/.svn/prop-base/dns.rb.svn-base
pentbox-1.8/lib/racket/racket/l5/.svn/prop-base/hsrp.rb.svn-base
pentbox-1.8/lib/racket/racket/l5/.svn/prop-base/ntp.rb.svn-base
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
pentbox-1.8/lib/racket/racket/l3/.svn/text-base/ipv4.rb.svn-base
pentbox-1.8/lib/racket/racket/l3/.svn/text-base/ipv6.rb.svn-base
pentbox-1.8/lib/racket/racket/l3/.svn/text-base/cdp.rb.svn-base
pentbox-1.8/lib/racket/racket/l3/.svn/text-base/stp.rb.svn-base
pentbox-1.8/lib/racket/racket/l3/.svn/text-base/misc.rb.svn-base
pentbox-1.8/lib/racket/racket/l3/.svn/prop-base/arp.rb.svn-base
pentbox-1.8/lib/racket/racket/l3/.svn/prop-base/egp.rb.svn-base
pentbox-1.8/lib/racket/racket/l3/.svn/prop-base/ipv4.rb.svn-base
pentbox-1.8/lib/racket/racket/l3/.svn/prop-base/ipv6.rb.svn-base
pentbox-1.8/lib/racket/racket/l3/.svn/prop-base/cdp.rb.svn-base
pentbox-1.8/lib/racket/racket/l3/.svn/prop-base/stp.rb.svn-base
pentbox-1.8/lib/racket/racket/l3/.svn/prop-base/misc.rb.svn-base
pentbox-1.8/lib/racket/racket/misc/.svn/text-base/orderedhash.rb.svn-base
```



```
pentbox-1.8/lib/racket/racket/l4/.svn/prop-base/misc.rb.svn-base
pentbox-1.8/lib/json/json/add/.svn/text-base/rails.rb.svn-base
pentbox-1.8/lib/json/json/add/.svn/text-base/core.rb.svn-base
pentbox-1.8/lib/json/json/add/.svn/prop-base/rails.rb.svn-base
pentbox-1.8/lib/json/json/add/.svn/prop-base/core.rb.svn-base
pentbox-1.8/lib/json/json/pure/.svn/text-base/generator.rb.svn-base
pentbox-1.8/lib/json/json/pure/.svn/text-base/parser.rb.svn-base
pentbox-1.8/lib/json/json/pure/.svn/prop-base/generator.rb.svn-base
pentbox-1.8/lib/json/json/pure/.svn/prop-base/parser.rb.svn-base
pentbox-1.8/lib/net/dns/resolver/.svn/text-base/timeouts.rb.svn-base
pentbox-1.8/lib/net/dns/resolver/.svn/text-base/socks.rb.svn-base
pentbox-1.8/lib/net/dns/resolver/.svn/prop-base/timeouts.rb.svn-base
```

INSTALLATION PENTBOX HONEYPOT

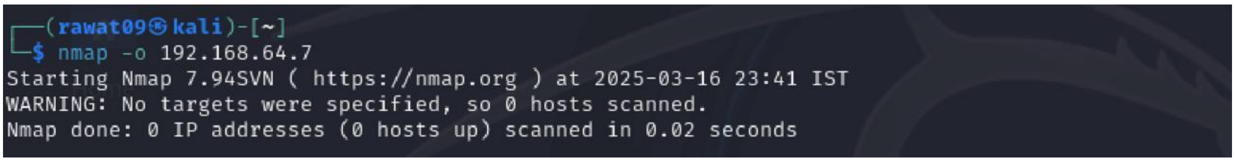
- Install Pentbox on the Debian system. This likely involves extracting the Pentbox files and potentially running an installation script.



```
root@ubuntu:/home/ubuntu# wget https://sourceforge.net/projects/pentbox18realise
d/files/pentbox-1.8.tar.gz
--2025-03-16 04:28:50--  https://sourceforge.net/projects/pentbox18realised/file
s/pentbox-1.8.tar.gz
Resolving sourceforge.net (sourceforge.net)... 104.18.13.149, 104.18.12.149, 260
6:4700:8ca1:498:f43:0:8280:21e3
Connecting to sourceforge.net (sourceforge.net)|104.18.13.149|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://sourceforge.net/projects/pentbox18realised/files/pentbox-1.8.t
ar.gz/ [following]
--2025-03-16 04:28:51--  https://sourceforge.net/projects/pentbox18realised/file
s/pentbox-1.8.tar.gz/
Reusing existing connection to sourceforge.net:443.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://sourceforge.net/projects/pentbox18realised/files/pentbox-1.8.t
ar.gz/download [following]
--2025-03-16 04:28:51--  https://sourceforge.net/projects/pentbox18realised/file
s/pentbox-1.8.tar.gz/download
Reusing existing connection to sourceforge.net:443.
HTTP request sent, awaiting response... 302 Found
Location: https://downloads.sourceforge.net/project/pentbox18realised/pentbox-1.
8.tar.gz?ts=gAAAABn1lOEDO0X1vots8L_uPEq4C8xfWlnSd52Lcq60yL64JsWKS4faEbSuwB5WFWv
```

CHECKING 0 HOST UP IN ATTACKING MACHINE

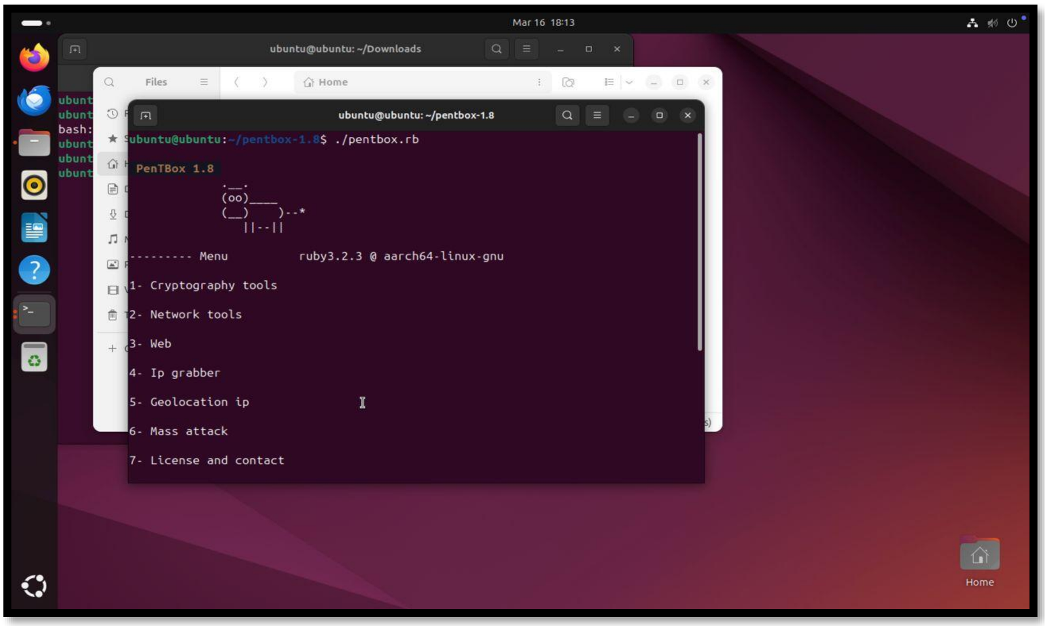
- This step is unclear and requires more context. It seems to refer to a check from the attacker's perspective, verifying that the honeypot appears to be a live host.
- Clarification is needed on what "0 host up" specifically means.



```
┌──(rawat09㉿kali)-[~]
└─$ nmap -o 192.168.64.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-16 23:41 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds
```

SETTING UP PENTBOX HONEYPOT

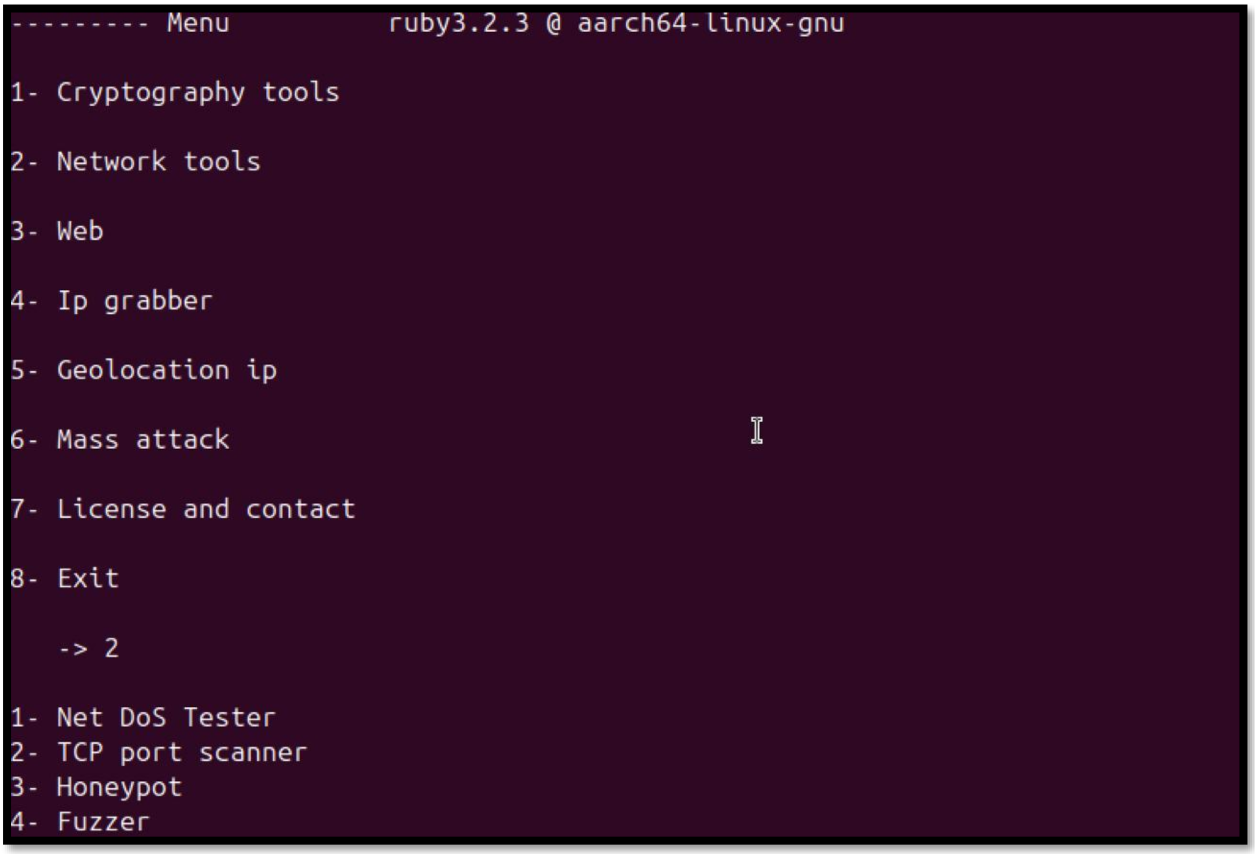
- Configure Pentbox to simulate the desired services (e.g., SSH, Telnet). This involves editing Pentbox configuration files.



```
ubuntu@ubuntu:~/pentbox-1.8$ ./pentbox.rb

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

--------- Menu          ruby3.2.3 @ aarch64-linux-gnu

1- Cryptography tools

2- Network tools

3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact
```

ACTVATE HONEYPOT ON ANYPOT

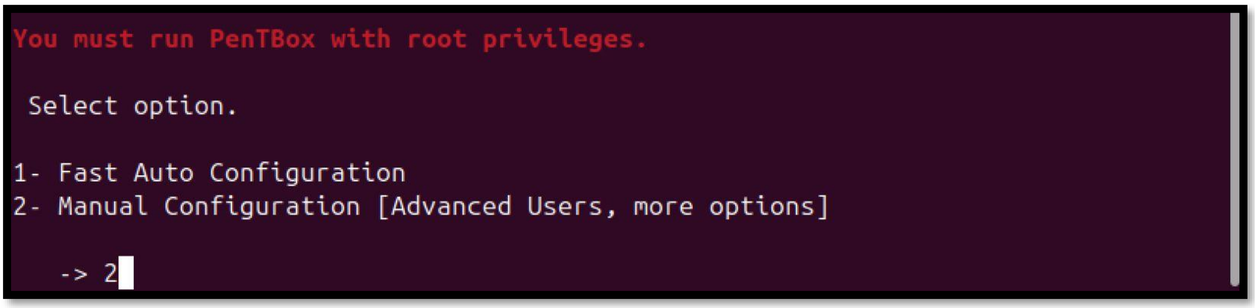
- This step is unclear. It likely refers to starting the Pentbox honeypot service.
- Clarification is needed on what "ANYPOT" refers to.



```
--------- Menu          ruby3.2.3 @ aarch64-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
```

MANUAL CONFIGURATION OF HONEYPOT

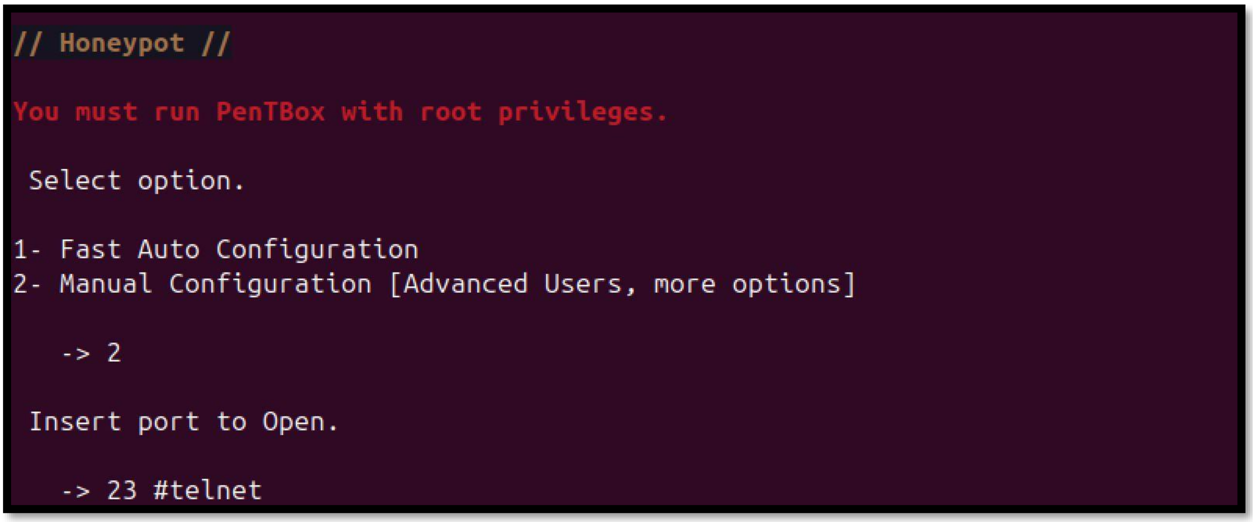
- This is part of step 7, configuring Pentbox to define its behavior, the services it emulates, and how it interacts with attackers.



```
You must run PenTBox with root privileges.

 Select option.

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

   -> 2
```

GIVING PORT

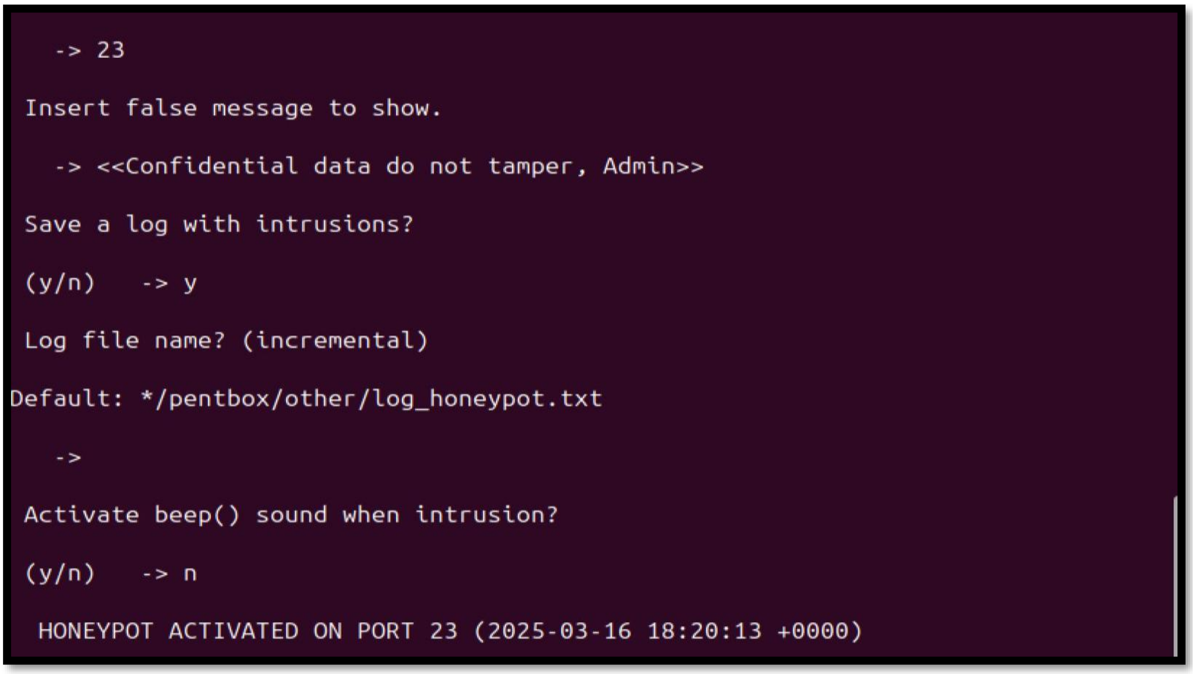
- Configure the ports that the honeypot services will listen on (e.g., port 22 for SSH, port 23 for Telnet).



```
// 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.

   -> 23 #telnet
```

SPECIFYING AND CONFIGUATION IF HONEYPOT BEFORE DEPLOYMENT

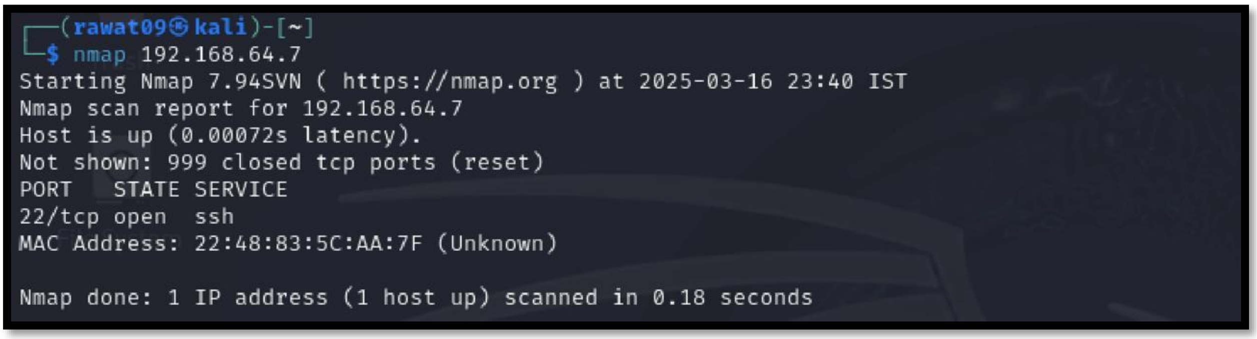
- This encompasses steps 7, 9, and 10: Setting up Pentbox's services, ports, and other settings before it's put into operation.



```
   -> 23

 Insert false message to show.

   -> <<Confidential data do not tamper, Admin>>

 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)   -> n

  HONEYPOT ACTIVATED ON PORT 23 (2025-03-16 18:20:13 +0000)
```

ATTACK

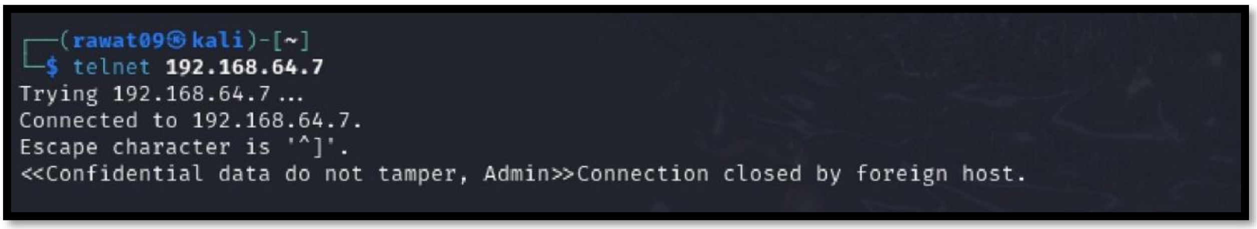
- Simulate an attack from a separate system to test the honeypot and Snort. This could involve using tools like Nmap, Metasploit, or manual attempts to connect to the honeypot services.



```
┌──(rawat09㉿kali)-[~]
└─$ nmap 192.168.64.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-16 23:40 IST
Nmap scan report for 192.168.64.7
Host is up (0.00072s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 22:48:83:5C:AA:7F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

AFTER DEPLOYMENT ATTACK

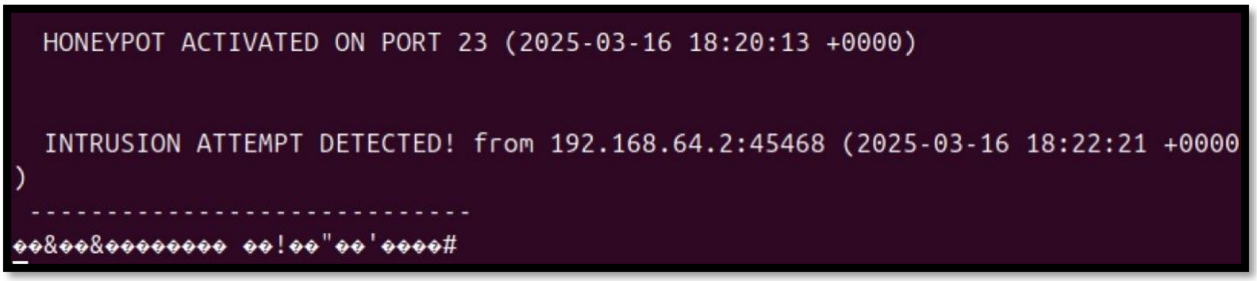
- This is the same as step 12, attacking the honeypot to see if it works.



```
┌──(rawat09㉿kali)-[~]
└─$ telnet 192.168.64.7
Trying 192.168.64.7 ...
Connected to 192.168.64.7.
Escape character is '^]'.
<<Confidential data do not tamper, Admin>>Connection closed by foreign host.
```

CAPTURE IN HONEYPOT AND FOUND IP OF ATTACKER

- Verify that the honeypot (Pentbox) logs the attacker's activity, including their IP address.
- Also, verify that Snort detects the attack and generates an alert.



```
  HONEYPOT ACTIVATED ON PORT 23 (2025-03-16 18:20:13 +0000)


  INTRUSION ATTEMPT DETECTED! from 192.168.64.2:45468 (2025-03-16 18:22:21 +0000
)
 -----------------------------
��&���&�������� ��!��"��'����#
```

<u>Result : Honeypot and IDS (Snort)</u>

We enhanced its defence against cyberattacks by integrating a honeypot and Intrusion Detection System (IDS). This integration provides proactive threat detection, detailed attack intelligence, improved incident response, and a cost-effective security enhancement by leveraging open-source tools.

- A dedicated Ubuntu system with Snort IDS for active network traffic monitoring.
- A separate Debian system with Pentbox honeypot, emulating services on an isolated segment to attract and log attackers.
- Integrated threat detection: Snort detects attacks on the honeypot, and Pentbox logs attacker details.
- System testing confirms successful attack attraction, logging, and Snort alerting.