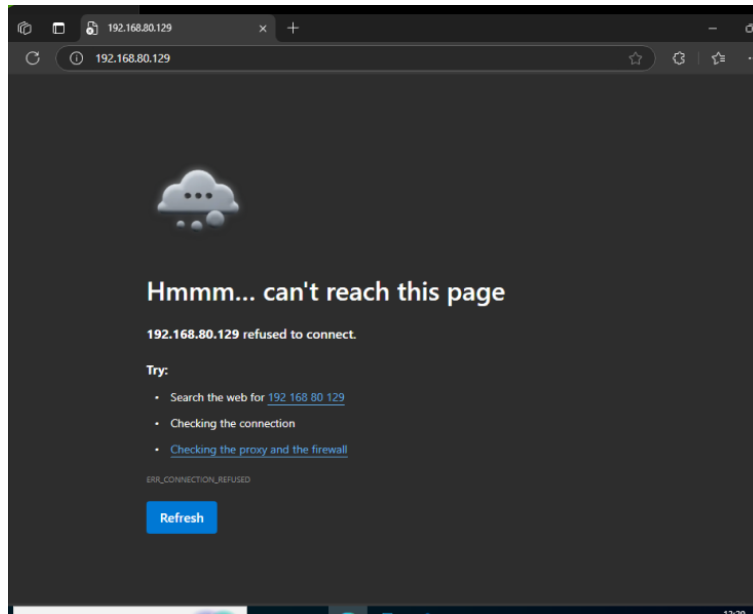


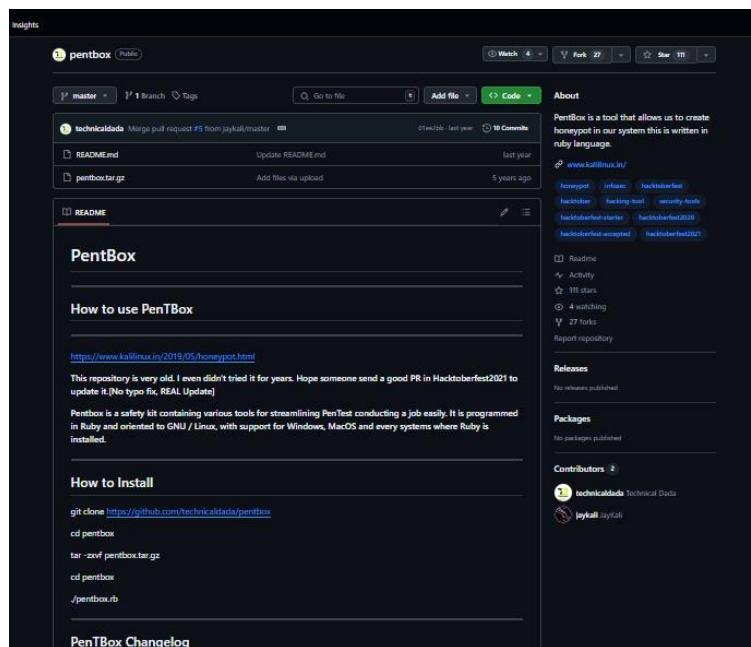
HoneyPot – Pentbox

Step 1: Without Honey Pot



Step2: Clone the pentbox from the below link

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



```
Home X kali-linux-2024.2-vmware... X Windows 10 x64 X
File Actions Edit View Help
(kali@kali)-[~]
$ 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 | 1.07 MiB/s, done.
Resolving deltas: 100% (3/3), done.

(kali@kali)-[~]
$ ls -l
total 160
-rw-rw-r-- 1 kali kali 544 Sep 3 07:09 content1.txt
-rw-rw-r-- 1 kali kali 155 Sep 3 07:04 contents_sorted.txt
-rwxrwxr-x 1 kali kali 155 Sep 3 07:00 contents.txt
drwxr-xr-x 4 kali kali 4096 Aug 29 01:23 Desktop
drwxr-xr-x 2 kali kali 4096 Aug 4 06:32 Documents
drwxr-xr-x 3 kali kali 4096 Sep 5 13:32 Downloads
drwxr-xr-x 2 kali kali 4096 Aug 4 06:32 Music
-rw-r-- 1 root root 300 Sep 5 14:14 pass.txt
drwxrwxr-x 3 kali kali 4096 Oct 20 03:23 pentbox
drwxr-xr-x 2 kali kali 4096 Oct 14 13:13 Pictures
drwxr-xr-x 2 kali kali 4096 Aug 4 06:32 Public
-rw-r-- 1 root root 1729 Sep 12 02:36 shadow
drwxr-xr-x 2 kali kali 4096 Aug 4 06:32 Templates
drwxr-xr-x 2 kali kali 4096 Aug 4 06:32 Videos
-rwxr-xr-x 1 kali kali 100206 Dec 4 2019 wordlist.txt
drwxrwxr-x 3 kali kali 4096 Aug 12 11:16 work

(kali@kali)-[~]
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
```

Step 3: Unzip the File

Tar -zfvx pentbox.tar.gz

```
kali@kali: ~/pentbox/pe
File Actions Edit View Help
(kali@kali)-[~/pentbox]
$ ls
pentbox.tar.gz README.md

(kali@kali)-[~/pentbox]
$ tar -zfvx pentbox.tar.gz
Command 'tae' not found, did you mean:
command 'tie' from deb texlive-binaries
command 'tar' from deb tar
command 'tea' from deb tea
command 'tee' from deb coreutils
command 'tre' from deb tre-command
command 'tac' from deb coreutils
command 'tde' from deb devtodo
command 'tap' from deb node-tap
command 'tao' from deb taopm
command 'tad' from deb tad
command 'toe' from deb ncurses-bin
command 'tape' from deb node-tape
Try: sudo apt install <deb name>

(kali@kali)-[~/pentbox]
$ tar -zfvx pentbox.tar.gz
tar: You must specify one of the '-Acdrtrux', '--delete' or '--test-label' options
Try 'tar --help' or 'tar --usage' for more information.

(kali@kali)-[~/pentbox]
$ tar -xvzf pentbox.tar.gz
pentbox-1.8/lib/racket/racket/l2/.svn/text-base/lrc.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

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Step 4: Open the File

./pentbox.rb

There are many types of tools available in the pentbox as show in picture below

```
kali@kali: ~/pentbox/pentbox-1.8
File Actions Edit View Help
(kali@kali)~[~/pentbox]
$ cd pentbox-1.8
(kali@kali)~[~/pentbox/pentbox-1.8]
$ ls
changelog.txt  COPYING.txt  lib  other  pb_update.rb  pentbox.rb  readme.txt  todo.txt  tools
(kali@kali)~[~/pentbox/pentbox-1.8]
$ ./pentbox.rb

PentBox 1.8
      (oo)
      (oo)  --*
      |H--|

Menu
-----
1- Cryptography tools
2- Network tools
3- Web
4- Ip grabber
5- Geolocation ip
6- Mass attack
7- License and contact
```

Step 5:

Network Tools → Honeypot →
Fast auto Configuration.

If Manual configuration Skip to
Step 7.

```
File Actions Edit View Help
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 //

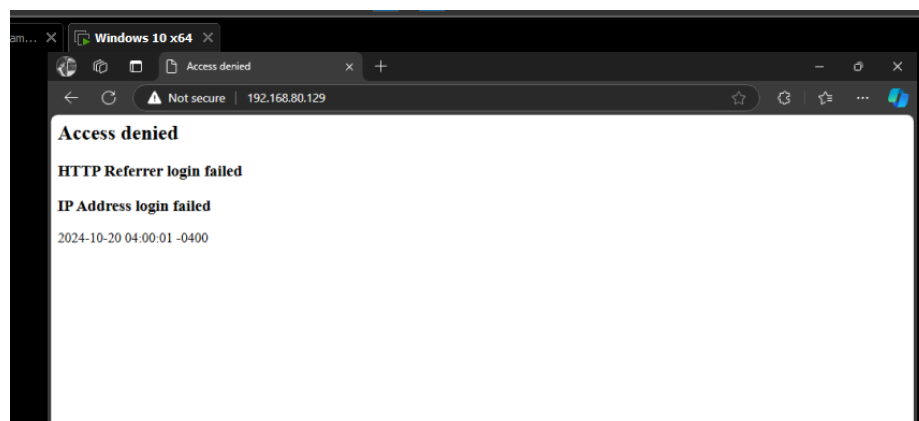
You must run PentBox with root privileges.

Select option.
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
  → 1

HONEYPOT ACTIVATED ON PORT 80 (2024-10-20 03:33:31 -0400)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Step 6: With Honeypot Activation



Intrusion is detected when ip address of this device (Kali Linux) is entered in the windows web browser.

```
File Actions Edit View Help

INTRUSION ATTEMPT DETECTED! from 192.168.80.134:49825 (2024-10-20 03:49:50 -0400)

GET / HTTP/1.1
Host: 192.168.80.129
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36 Edg/130.0.0.0
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=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

INTRUSION ATTEMPT DETECTED! from 192.168.80.134:49826 (2024-10-20 03:49:51 -0400)

GET /favicon.ico HTTP/1.1
Host: 192.168.80.129
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36 Edg/130.0.0.0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://192.168.80.129/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

^C
[*] EXITING ...

(kali@kali)-[~/pentbox/pentbox-1.8]
```

Step 7: Set the settings since it is Manual Configuration.

```

File Actions Edit View Help
Select option.

1- Fast Auto Configuration (ST, RUNNING, MULTICAST) mtu 1500
2- Manual Configuration [Advanced Users, more options] broadcast 192.168.1.255
   interface 192.168.1.10 netmask 255.255.0.0 prefixlen 64 scopeid 0x10
   → 2 other 00:0c:29:b8:05:77 txqueuelen 1000 (Ethernet)
      RX packets 79 bytes 6864 (6.6 KiB)

Insert port to open. dropped 0 overruns 0 frame 0
   tx packets 24 bytes 3120 (3.0 KiB)
   → 80 errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Insert false message to show. NO mtu 65536
   interface 192.168.1.1 netmask 255.0.0.0
   → Forebiden Access txlen 120 scopeid 0x10 hosts
      txqueuelen 1000 (Local Loopback)

Save a log with intrusions? 80 (480.0 B)
   errors 0 dropped 0 overruns 0 frame 0
(y/n) → y txs 0 bytes 480 (480.0 B)
      errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Log file name? (incremental)

Default: */pentbox/other/log_honeypot.txt
→

Activate beep() sound when intrusion?

(y/n) → y

HONEYPOT ACTIVATED ON PORT 80 (2024-10-20 04:40:06 -0400)

```

```
File Actions Edit View Help
(y/n) → y

HONEYPOT ACTIVATED ON PORT 80 (2024-10-20 04:40:06 -0400)

INTRUSION ATTEMPT DETECTED! from 192.168.80.134:49773 (2024-10-20 04:41:32 -0400)

GET / HTTP/1.1
Host: 192.168.80.129
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36 Edg/130.0.0.0
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=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

INTRUSION ATTEMPT DETECTED! from 192.168.80.134:49772 (2024-10-20 04:41:33 -0400)

GET /favicon.ico HTTP/1.1
Host: 192.168.80.129
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36 Edg/130.0.0.0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://192.168.80.129/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
```

Intrusion is Detected and false message to Show is also displayed.

