

Honeypot :

Honeypot is a network-attached system used as a trap for cyber-attackers to detect and study the tricks and types of attacks used by hackers. It acts as a potential target on the internet and informs the defenders about any unauthorized attempt to the information system.

Cowrie

Is a medium interaction SSH and Telnet honeypot designed to log brute force attacks and shell interaction performed by an attacker. Cowrie also functions as an SSH and telnet proxy to observe attacker behaviour to another system.

Virtualenv:

virtualenv is used to manage Python packages for different projects. Using virtualenv allows you to avoid installing Python packages globally which could break system tools or other projects. You can install virtualenv using pip.

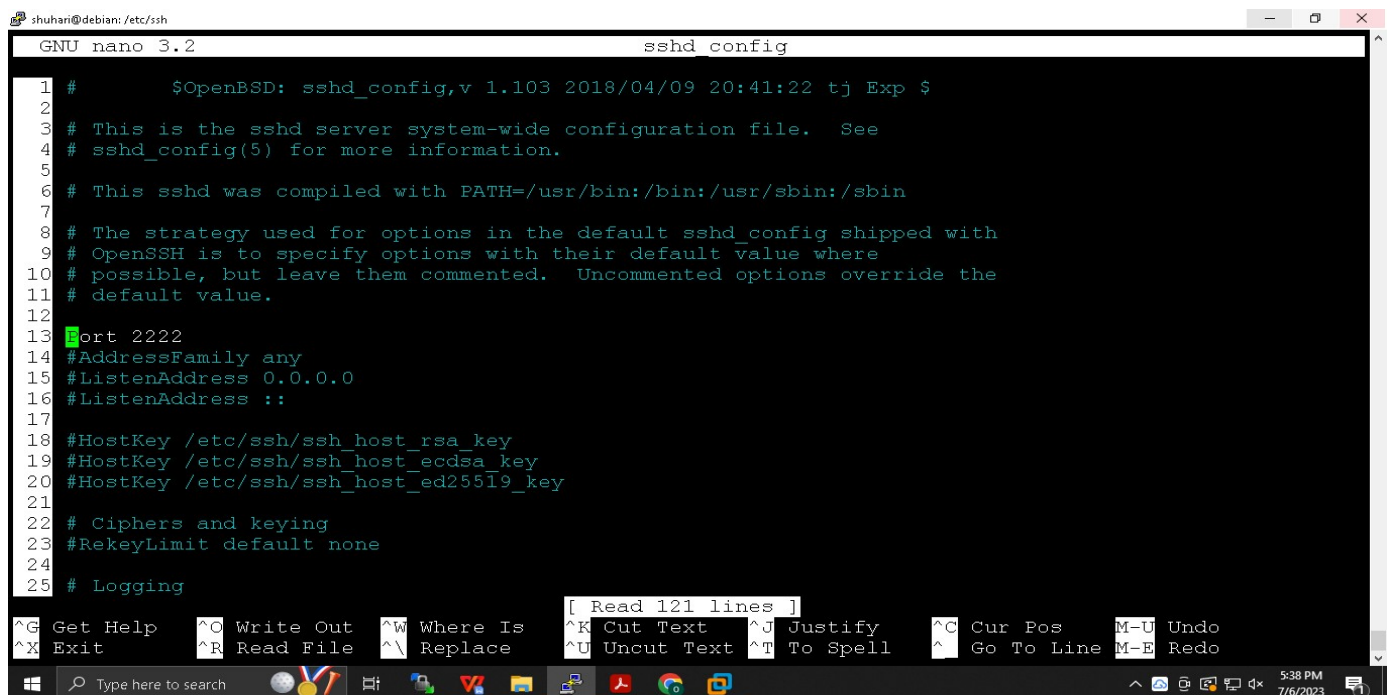
1.# Change port of ssh :

Do this changes in putty itself if not then the connection can never be established with putty after that as we already create connection it will be maintained

```
$cd /etc/ssh/
```

```
$sudo nano sshd_config
```

Line 13



```
shuhari@debian: /etc/ssh
GNU nano 3.2 sshd_config
1 # $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $
2
3 # This is the sshd server system-wide configuration file.  See
4 # sshd_config(5) for more information.
5
6 # This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin
7
8 # The strategy used for options in the default sshd_config shipped with
9 # OpenSSH is to specify options with their default value where
10 # possible, but leave them commented.  Uncommented options override the
11 # default value.
12
13 Port 2222
14 #AddressFamily any
15 #ListenAddress 0.0.0.0
16 #ListenAddress ::
17
18 #HostKey /etc/ssh/ssh_host_rsa_key
19 #HostKey /etc/ssh/ssh_host_ecdsa_key
20 #HostKey /etc/ssh/ssh_host_ed25519_key
21
22 # Ciphers and keying
23 #RekeyLimit default none
24
25 # Logging
[ Read 121 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos   M-U Undo
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line  M-E Redo
```

```
$sudo ssystemctl restart sshd
```

2.#Install Pre-requisite:

```
$ sudo apt-get install git python-virtualenv libssl-dev libffi-dev build-essential  
libpython3-dev python3-minimal authbind virtualenv
```

The authbind software allows a program that would normally require superuser privileges to access privileged network services to run as a non-privileged user

3.Install python3.8:

Install Python 3.8 on shuhari debian from source code , when we install from apt-get it gets into /usr/bin when we do with source code it gets into /usr/local/bin

Follow : <https://linuxize.com/post/how-to-install-python-3-8-on-debian-10/>

```
$sudo apt-get install build-essential zlib1g-dev libncurses5-dev libgdbm-dev  
libnss3-dev libssl-dev libsqlite3-dev libreadline-dev libffi-dev curl libbz2-dev  
$sudo curl -O https://www.python.org/ftp/python/3.8.2/Python-3.8.2.tar.xz  
$tar -xf Python-3.8.2.tar.xz  
$cd Python-3.8.2  
$./configure --enable-optimizations
```

The script performs a number of checks to make sure all of the dependencies on your system are present. The --enable-optimizations option will optimize the Python binary by running multiple tests, which will make the build process slower

```
$make -j 4
```

Modify the -j to correspond to the number of cores in your processor. You can find the number by typing nproc.

```
sudo make altinstall
```

Do not use the standard make install as it will overwrite the default system python3 binary.

```
$python3.8 --version
```

```
shuhari@debian:~/Python-3.8.2$ python3.8 --version  
Python 3.8.2  
shuhari@debian:~/Python-3.8.2$
```

4.#Configure non-root user :

`$sudo adduser --disabled-password cowrie`

```
shuhari@debian:~/Python-3.8.2$ sudo adduser --disabled-password cowrie
Adding user `cowrie' ...
Adding new group `cowrie' (1001) ...
Adding new user `cowrie' (1001) with group `cowrie' ...
Creating home directory `/home/cowrie' ...
Copying files from `/etc/skel' ...
Changing the user information for cowrie
Enter the new value, or press ENTER for the default
Full Name []: cowrie
Room Number []: cowrie
Work Phone []: cowrie
Home Phone []: cowrie
Other []: cowrie
Is the information correct? [Y/n] Y
shuhari@debian:~/Python-3.8.2$ sudo getent passwd cowrie
cowrie:x:1001:1001:cowrie,cowrie,cowrie,cowrie,cowrie:/home/cowrie:/bin/bash
shuhari@debian:~/Python-3.8.2$
```

5.#Configure authbind

`$sudo touch /etc/authbind/byport/22`

`$sudo chown cowrie:cowrie /etc/authbind/byport/22`

`$sudo chmod 777 /etc/authbind/byport/22`

6.Create virtual env:

`$sudo su - cowrie`

`$pwd`

(ensure to be in home dir)

`$git clone https://github.com/cowrie/cowrie`

`$cd cowrie`

`$virtualenv --python=python3.8 cowrie-env`

`$source cowrie-env/bin/activate`

(to activate virtual env)

`cowrie@debian: ~/cowrie`

```
(cowrie-env) cowrie@debian:~/cowrie$ source cowrie-env/bin/activate
(cowrie-env) cowrie@debian:~/cowrie$
```

7.Inside Virtual env :

`(cowrie-env) cowrie@deb1:~/cowrie$`

`$pip install --upgrade pip`

All the dependencies are stored in file called requirement.txt we can refer that for dependencies.

`$pip install --upgrade -r requirements.txt`

`$cd etc`

`$cp cowrie.cfg.dist cowrie.cfg (in current dir there is etc folder)`

`$nano etc/cowrie.cfg`

`Line 585 listen_endpoint = tcp:22:interface=0.0.0.0`


```
GNU nano 3.2                                cowrie.cfg                                Modified
573 compression = zlib@openssh.com,zlib,none
574
575 # Endpoint to listen on for incoming SSH connections.
576 # See https://twistedmatrix.com/documents/current/core/howto/endpoints.html#servers
577 # (default: listen_endpoints = tcp:2222:interface=0.0.0.0)
578 # (use systemd: endpoint for systemd activation)
579 # listen_endpoints = systemd:domain=INET:index=0
580 # For both IPv4 and IPv6: listen_endpoints = tcp6:2222:interface=\:\:
581 # Listening on multiple endpoints is supported with a single space separator
582 # e.g listen_endpoints = "tcp:2222:interface=0.0.0.0 tcp:1022:interface=0.0.0.0" will result lis
583 # use authbind for port numbers under 1024
584
585 listen_endpoints = tcp:22:interface=0.0.0.0
586
587 # Enable the SFTP subsystem
588
```

\$nano etc/userdb.txt

root:x:!rootroot (the user or attacker password of rootroot will not be accepted)

root:x:* (all other password will be accepted)

Attacker will feel that he is root user but he is not

 cowrie@debian: ~/cowrie/etc

```
GNU nano 3.2
root:x:!rootroot
root:x:*
```

\$bin/cowrie status

\$bin/cowrie start

```
cowrie@debian: ~/cowrie
Successfully installed Automat-22.10.0 appdirs-1.4.4 attrs-23.1.0 bcrypt-4.0.1 certifi-2023.5.7 cffi-1.
15.1 charset-normalizer-3.1.0 configparser-5.3.0 constantly-15.1.0 cryptography-41.0.1 hyperlink-21.0.0
idna-3.4 incremental-22.10.0 packaging-23.1 pyasn1-0.5.0 pyasn1_modules-0.3.0 pycparser-2.21 pyopenssl
-23.2.0 pyparsing-3.1.0 python-dateutil-2.8.2 requests-2.31.0 service_identity-23.1.0 six-1.16.0 tftpy-
0.8.2 treq-22.2.0 twisted-22.10.0 typing-extensions-4.7.1 urllib3-2.0.3 zope.interface-6.0
(cowrie-env) cowrie@debian:~/cowrie$ bin/cowrie status

Join the Cowrie community at: https://www.cowrie.org/slack/

cowrie is not running.
(cowrie-env) cowrie@debian:~/cowrie$ bin/cowrie start

Join the Cowrie community at: https://www.cowrie.org/slack/

Using activated Python virtual environment "/home/cowrie/cowrie/cowrie-env"
Starting cowrie: [twistedd --umask=0022 --pidfile=var/run/cowrie.pid --logger cowrie.python.logfile.logg
er cowrie ]...
/home/cowrie/cowrie/cowrie-env/lib/python3.8/site-packages/twisted/conch/ssh/transport.py:97: Cryptogr
aphyDeprecationWarning: Blowfish has been deprecated
  b"blowfish-cbc": (algorithms.Blowfish, 16, modes.CBC),
/home/cowrie/cowrie/cowrie-env/lib/python3.8/site-packages/twisted/conch/ssh/transport.py:101: Cryptogr
aphyDeprecationWarning: CAST5 has been deprecated
  b"cast128-cbc": (algorithms.CAST5, 16, modes.CBC),
/home/cowrie/cowrie/cowrie-env/lib/python3.8/site-packages/twisted/conch/ssh/transport.py:106: Cryptogr
aphyDeprecationWarning: Blowfish has been deprecated
  b"blowfish-ctr": (algorithms.Blowfish, 16, modes.CTR),
/home/cowrie/cowrie/cowrie-env/lib/python3.8/site-packages/twisted/conch/ssh/transport.py:107: Cryptogr
aphyDeprecationWarning: CAST5 has been deprecated
  b"cast128-ctr": (algorithms.CAST5, 16, modes.CTR),
(cowrie-env) cowrie@debian:~/cowrie$
```

\$ss -ant

```
(cowrie-env) cowrie@debian:~/cowrie$ ss -ant
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
LISTEN     0            128         0.0.0.0:2222             0.0.0.0:*
LISTEN     0            50          0.0.0.0:22              0.0.0.0:*
ESTAB      0            64          192.168.1.107:22        192.168.1.82:50786
LISTEN     0            128         [::]:2222              [::]:*
LISTEN     0            128         *:80                   *:*
```

The fake ssh is on 22 while real one is at 2222

Testing :

Deb2 :

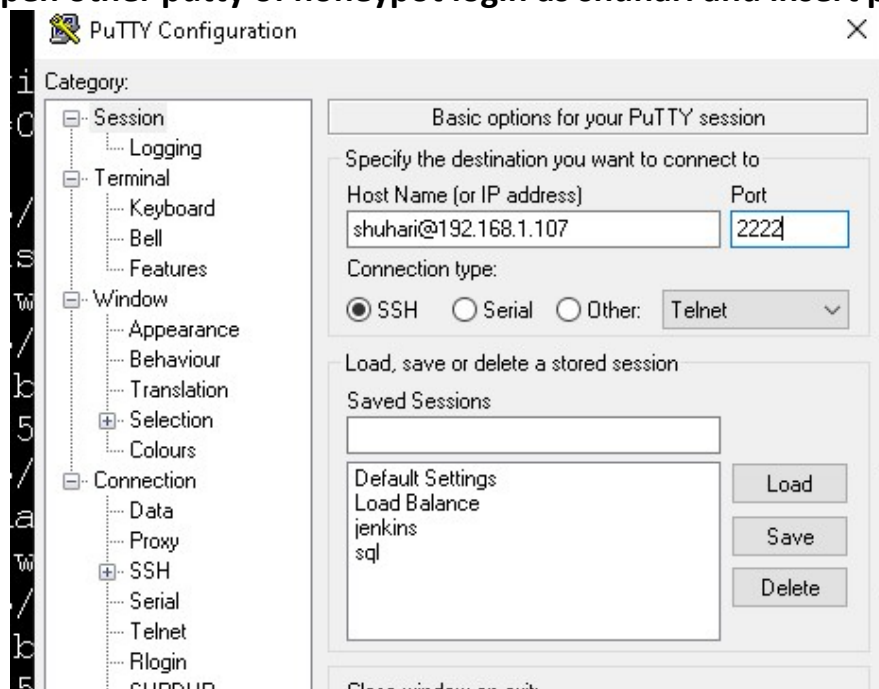
\$ssh -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no root@ip of honeypot

```
shuhari@debian: ~
shuhari@debian:~$ ssh -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no root@192.168.1.107
Warning: Permanently added '192.168.1.107' (ECDSA) to the list of known hosts.
root@192.168.1.107'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@svr04:~#
```

8.Log checking : Open other putty of honeypot login as shuhari and insert port 2222.



\$sudo tail -f /home/cowrie/cowrie/var/log/cowrie/cowrie.log


```
2023-07-06T10:22:24.972102Z [twisted.conch.ssh.session#info] Getting shell
2023-07-06T10:22:39.662756Z [HoneyPotSSHTransport,2,192.168.1.113] CMD: whoami
2023-07-06T10:22:39.663668Z [HoneyPotSSHTransport,2,192.168.1.113] Command found: whoami
2023-07-06T10:22:42.942858Z [HoneyPotSSHTransport,2,192.168.1.113] CMD: ls
2023-07-06T10:22:42.943757Z [HoneyPotSSHTransport,2,192.168.1.113] Command found: ls
2023-07-06T10:22:48.270835Z [HoneyPotSSHTransport,2,192.168.1.113] CMD: sudo apt-get install apache
2023-07-06T10:22:48.271784Z [HoneyPotSSHTransport,2,192.168.1.113] Command found: sudo apt-get install
apache
```

