Cowrie Honeypot Setup Report

apt update/upgrade — update packages to avoid installation errors.

Install git (to clone the repository), python3 and python3-venv (Cowrie runs on Python and is recommended to be run in an isolated virtual environment), and dev dependencies (libssl-dev, libffi-dev, build-essential) — needed to build some libraries.

```
┌──(vbox㉿vbox)-[~]
└─$ sudo apt update && sudo apt upgrade -y
Hit:1 http://http.kali.org/kali kali-rolling InRelease
1183 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
  amass-common            libobjc-14-dev          python3-gpg
  gir1.2-girepository-2.0 libplacebo349           python3-kismetcapturebtgeiger
  libarmadillo14          libportmidi0            python3-kismetcapturefreaklabszigbee
  libbluray2              librav1e0.7             python3-kismetcapturertl433
  libbson-1.0-0t64        libsqlcipher1           python3-kismetcapturertladsb
  libdisplay-info2        libtheoradec1           python3-kismetcapturertlamr
  libgdal37               libtheoraenc1           python3-protobuf
  libgeos3.14.0           libudfread0             python3-xlutils
  libgirepository-1.0-1   libwireshark18          python3-xlwt
  libinstpatch-1.0-2      libwiretap15            python3-zombie-imp
  libjs-jquery-ui         libwsutil16             samba-ad-dc
  libjs-underscore        libx264-164             samba-ad-provision
  libmongoc-1.0-0t64      python3-bluepy          samba-dsdb-modules
  libnet1                 python3-click-plugins
Use 'sudo apt autoremove' to remove them.

Upgrading:
  7zip                              libqt5qmlmodels5
  accountsservice                   libqt5quick5
  adduser                           libqt5quickwidgets5
  adwaita-icon-theme                libqt5sql5-sqlite
  aircrack-ng                       libqt5sql5t64
  amass                             libqt5svg5
  apt                               libqt5test5t64
  apt-utils                         libqt5waylandclient5
  arping                            libqt5waylandcompositor5
  aspell                            libqt5webchannel5
```

2. Create Cowrie User

```
sudo adduser --disabled-password cowrie
sudo su - cowrie
```

It's best to run the honeypot as a non-root user—if someone were to exploit the Cowrie vulnerability, the attacker would be within the restricted user's scope.

```
┌──(vbox㉿vbox)-[~]
└─$ sudo adduser --disabled-password --gecos "" cowrie
usermod: no changes
```

3. Making Clone of cowrie

Let's take the latest version of the project from GitHub.

```
┌──(vbox㉿vbox)-[~]
└─$ sudo su - cowrie
┌──(cowrie㉿vbox)-[~]
└─$ git clone https://github.com/cowrie/cowrie.git
Cloning into 'cowrie' ...
remote: Enumerating objects: 20352, done.
remote: Counting objects: 100% (836/836), done.
remote: Compressing objects: 100% (392/392), done.
remote: Total 20352 (delta 742), reused 444 (delta 444), pack-reused 19516 (from 4)
Receiving objects: 100% (20352/20352), 11.21 MiB | 6.60 MiB/s, done.
Resolving deltas: 100% (14166/14166), done.
```

4.. Create Python Virtual Environment

```
python3 -m venv cowrie-env
source cowrie-env/bin/activate
```

The virtual environment isolates Cowrie's dependencies from the system Python. requirements.txt contains the libraries needed to run it.

```
┌──(cowrie㉿vbox)-[~]
└─$ cd cowrie

┌──(cowrie㉿vbox)-[~/cowrie]
└─$ python3 -m venv cowrie-env

┌──(cowrie㉿vbox)-[~/cowrie]
└─$ source cowrie-env/bin/activate

┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie]
└─$ pip install --upgrade pip
Requirement already satisfied: pip in ./cowrie-env/lib/python3.13/site-packages (25.2)
Collecting pip
  Downloading pip-25.3-py3-none-any.whl.metadata (4.7 kB)
Downloading pip-25.3-py3-none-any.whl (1.8 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.8/1.8 MB 9.7 MB/s  0:00:00
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 25.2
```

5. Install Dependencies

```
pip install --upgrade pip
pip install -e .
```

```
┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie/bin]
└─$ pip install -e

Usage:
  pip install [options] <requirement specifier> [package-index-options] ...
  pip install [options] -r <requirements file> [package-index-options] ...
  pip install [options] [-e] <vcs project url> ...
  pip install [options] [-e] <local project path> ...
  pip install [options] <archive url/path> ...

-e option requires 1 argument
```

6. Run cowrie

```
bin/cowrie start
bin/cowrie status
bin/cowrie stop
```

Cowrie Logs

```
tail -f var/log/cowrie/cowrie.log
tail -f var/log/cowrie/cowrie.json
```

```
┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie]
└─$ cowrie start

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

Starting cowrie: [twistd --umask=0022 --pidfile /home/cowrie/cowrie/var/run/cowrie.pid --logger cowrie.python.logfile.logger cowrie] ...
/home/cowrie/cowrie/cowrie-env/lib/python3.13/site-packages/twisted/conch/ssh/transport.py:110: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/home/cowrie/cowrie/cowrie-env/lib/python3.13/site-packages/twisted/conch/ssh/transport.py:117: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
```

7. Simultaneously doing try of brutforce to test our honeypot

```
┌──(vbox㉿vbox)-[~]
└─$ hydra -l root -P /usr/share/wordlists/rockyou.txt -s 2222 127.0.0.1 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-24 15:30:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the task
s: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries p
er task
[DATA] attacking ssh://127.0.0.1:2222/
[2222][ssh] host: 127.0.0.1   login: root   password: password
[2222][ssh] host: 127.0.0.1   login: root   password: abc123
[2222][ssh] host: 127.0.0.1   login: root   password: 123456789
[2222][ssh] host: 127.0.0.1   login: root   password: 12345
[2222][ssh] host: 127.0.0.1   login: root   password: iloveyou
[2222][ssh] host: 127.0.0.1   login: root   password: princess
[2222][ssh] host: 127.0.0.1   login: root   password: 1234567
[2222][ssh] host: 127.0.0.1   login: root   password: rockyou
[2222][ssh] host: 127.0.0.1   login: root   password: 12345678
[2222][ssh] host: 127.0.0.1   login: root   password: nicole
[2222][ssh] host: 127.0.0.1   login: root   password: daniel
[2222][ssh] host: 127.0.0.1   login: root   password: babygirl
[2222][ssh] host: 127.0.0.1   login: root   password: monkey
[2222][ssh] host: 127.0.0.1   login: root   password: lovely
[2222][ssh] host: 127.0.0.1   login: root   password: jessica
1 of 1 target successfully completed, 15 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-24 15:30:08
```

8. Honeypot is succesfull monitoring attempts of hydra to brutforce passwords.

```
2025-11-24T15:30:07.388700Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-conne
ction'
2025-11-24T15:30:07.389471Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'pa
ssword'
2025-11-24T15:30:07.390249Z [HoneyPotSSHTransport,33,127.0.0.1] login attempt [b'root'/b'princess'] succee
ded
2025-11-24T15:30:07.397039Z [HoneyPotSSHTransport,33,127.0.0.1] Initialized emulated server as architectur
e: linux-x64-lsb
2025-11-24T15:30:07.397659Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated wi
th b'password'
2025-11-24T15:30:07.397859Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-conne
ction'
2025-11-24T15:30:07.397987Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'pa
ssword'
2025-11-24T15:30:07.398244Z [HoneyPotSSHTransport,26,127.0.0.1] login attempt [b'root'/b'nicole'] succeede
d
2025-11-24T15:30:07.398485Z [HoneyPotSSHTransport,26,127.0.0.1] Initialized emulated server as architectur
e: linux-x64-lsb
2025-11-24T15:30:07.398581Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated wi
th b'password'
2025-11-24T15:30:07.398657Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-conne
ction'
2025-11-24T15:30:07.398776Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'pa
ssword'
2025-11-24T15:30:07.398909Z [HoneyPotSSHTransport,18,127.0.0.1] login attempt [b'root'/b'123456'] failed
2025-11-24T15:30:07.399728Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'pa
ssword'
2025-11-24T15:30:07.399889Z [HoneyPotSSHTransport,31,127.0.0.1] login attempt [b'root'/b'iloveyou'] succee
ded
2025-11-24T15:30:07.400083Z [HoneyPotSSHTransport,31,127.0.0.1] Initialized emulated server as architectur
e: linux-x64-lsb
2025-11-24T15:30:07.400167Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated wi
th b'password'
2025-11-24T15:30:07.400230Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-conne
ction'
2025-11-24T15:30:07.400300Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'pa
ssword'

┌──(cowrie-env)(cowrie㉿vbox)-[~]
└─$ cowrie status
cowrie is running (PID: 47699).
```