LAB: SET UP SSH HONETYPOT WITH COWRIE

This lab is optional. Please note that there is security risk when setting up and running a honeypot; therefore, please take measures to protect your own device/ system.

Example:

- Deploy Cowrie on a separate network or a system that is not connected to your critical production systems.
- Deploy Cowrie on a **virtual machine** and configure the virtual machine to be only connected to the host machine and **not connecting to the internet** when running Cowrie. The host machine can be used as an attacker.

This lab has been tested with Ubuntu 24 Virtual machine, but it could work with other versions of Ubuntu.

A. Install Cowrie (this requires the virtual machine to be connected to the internet)

Follow the instructions from step 1- step 6 on https://docs.cowrie.org/en/latest/INSTALL.html or follow the steps as below:

# install the libraries
sudo apt-get install git python3-pip python3-venv libssl-dev libffi-dev build-essential libpython3-dev python3-minimal authbind

# add user 'cowrie' with no password
sudo adduser --disabled-password cowrie
sudo su – cowrie

```
student@student-VMware-Virtual-Platform:~$ sudo adduser --disabled-password cowrie
info: Adding user `cowrie' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `cowrie' (1001) ...
info: Adding new user `cowrie' (1001) with group `cowrie (1001)' ...
info: Creating home directory `/home/cowrie' ...
info: Copying files from `/etc/skel' ...
Changing the user information for cowrie
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `cowrie' to supplemental / extra groups `users' ...
info: Adding user `cowrie' to group `users' ...
student@student-VMware-Virtual-Platform:~$ sudo su - cowrie
```

download the cowrie source code and go to the folder "cowrie"

git clone http://github.com/cowrie/cowrie

```
cowrie@student-VMware-Virtual-Platform:~$ git clone http://github.com/cowrie/cowrie

cd cowrie
Cloning into 'cowrie'...
warning: redirecting to https://github.com/cowrie/cowrie/
remote: Enumerating objects: 20476, done.
remote: Counting objects: 100% (902/902), done.
remote: Compressing objects: 100% (322/322), done.
remote: Total 20476 (delta 796), reused 580 (delta 580), pack-reused 19574 (from 5)
Receiving objects: 100% (20476/20476), 11.28 MiB | 10.01 MiB/s, done.
Resolving deltas: 100% (14233/14233), done.
```

create virtual environment 'cowrie-env', and activate
pwd
python3 -m venv cowrie-env
source cowrie-env/bin/activate # activate the created virtual environment

```
cowrie@student-VMware-Virtual-Platform:~/cowrie$ pwd
/home/cowrie/cowrie
cowrie@student-VMware-Virtual-Platform:~/cowrie$ python3 -m venv cowrie-env
cowrie@student-VMware-Virtual-Platform:~/cowrie$ source cowrie-env/bin/activate
(cowrie-env) cowrie@student-VMware-Virtual-Platform:~/cowrie$ ls
bin                docker    INSTALL.rst  pyproject.toml           setup.py
CHANGELOG.rst      docs      LICENSE.rst  README.rst               src
CONTRIBUTING.rst   etc       Makefile     requirements-output.txt  var
cowrie-env         honeyfs   MANIFEST.in  requirements.txt
(cowrie-env) cowrie@student-VMware-Virtual-Platform:~/cowrie$ ls etc/
cowrie.cfg.dist  userdb.example
```

Upgrade pip inside the virtual environment

```
(cowrie-env) cowrie@student-VMware-Virtual-Platform:~/cowrie$ python -m pip install --upgrade pip
Requirement already satisfied: pip in ./cowrie-env/lib/python3.12/site-packages (24.0)
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 26.1 MB/s eta 0:00:00
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 24.0
    Uninstalling pip-24.0:
      Successfully uninstalled pip-24.0
Successfully installed pip-25.3
```

Install Cowrie inside the virtual environment

```
(cowrie-env) cowrie@student-VMware-Virtual-Platform:~/cowrie$ python -m pip install -
e .
Obtaining file:///home/cowrie/cowrie
  Installing build dependencies ... done
  Checking if build backend supports build_editable ... done
  Getting requirements to build editable ... done
  Installing backend dependencies ... done
  Preparing editable metadata (pyproject.toml) ... done
Collecting attrs==25.4.0 (from cowrie==2.9.1.dev6+g922cfc3be)
  Downloading attrs-25.4.0-py3-none-any.whl.metadata (10 kB)
Collecting bcrypt==5.0.0 (from cowrie==2.9.1.dev6+g922cfc3be)
  Downloading bcrypt-5.0.0-cp39-abi3-manylinux_2_34_x86_64.whl.metadata (10 kB)
Collecting cryptography==46.0.3 (from cowrie==2.9.1.dev6+g922cfc3be)
  Downloading cryptography-46.0.3-cp311-abi3-manylinux_2_34_x86_64.whl.metadata (5.7
```

#Create the configuration file “etc/cowrie.cfg”.
vi etc/cowrie.cfg
#Copy the following content to the new file and save it
[telnet]
enabled = true

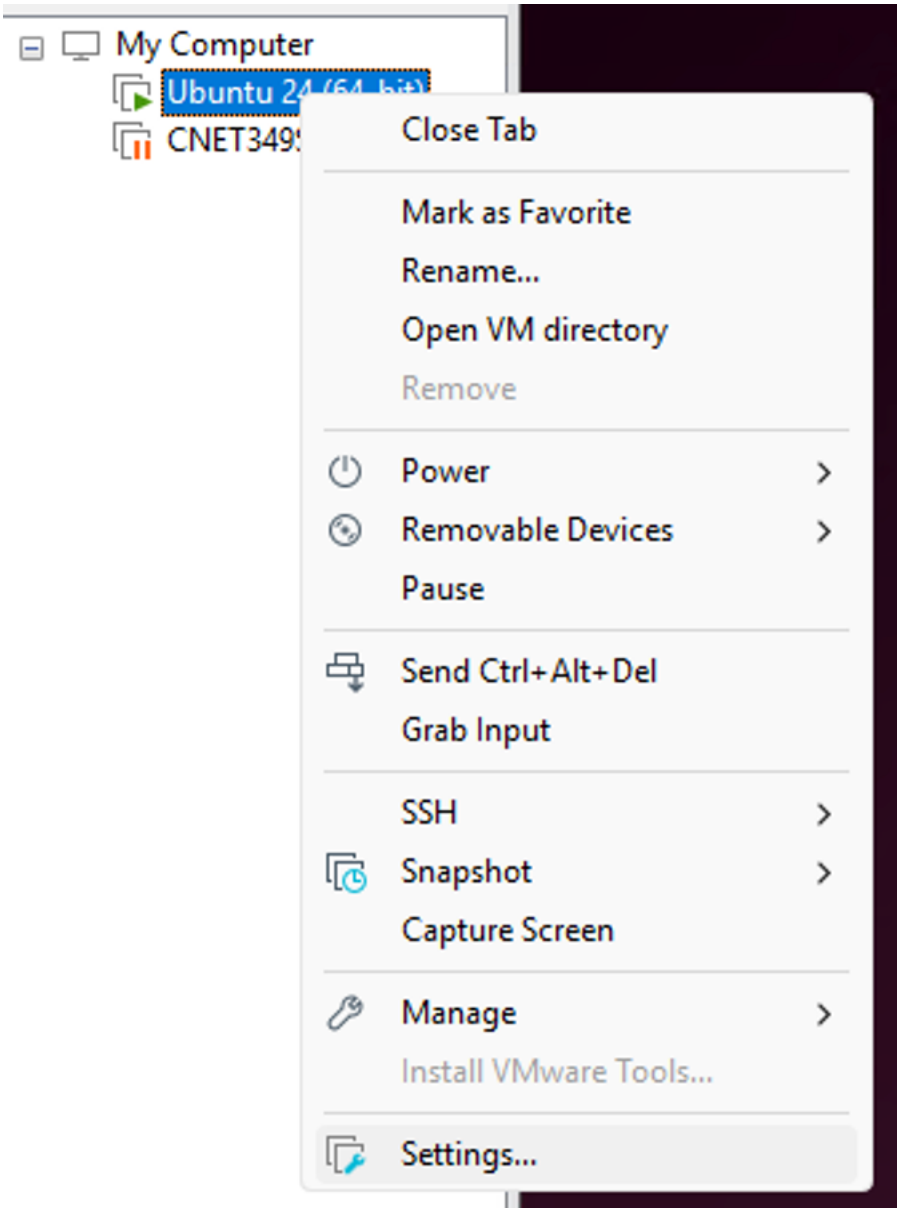
#Create a user and password for cowrie:
vi etc/userdb.txt

```
(cowrie-env) cowrie@student-VMware-Virtual-Platform:~/cowrie$ vi etc/userdb.txt
```

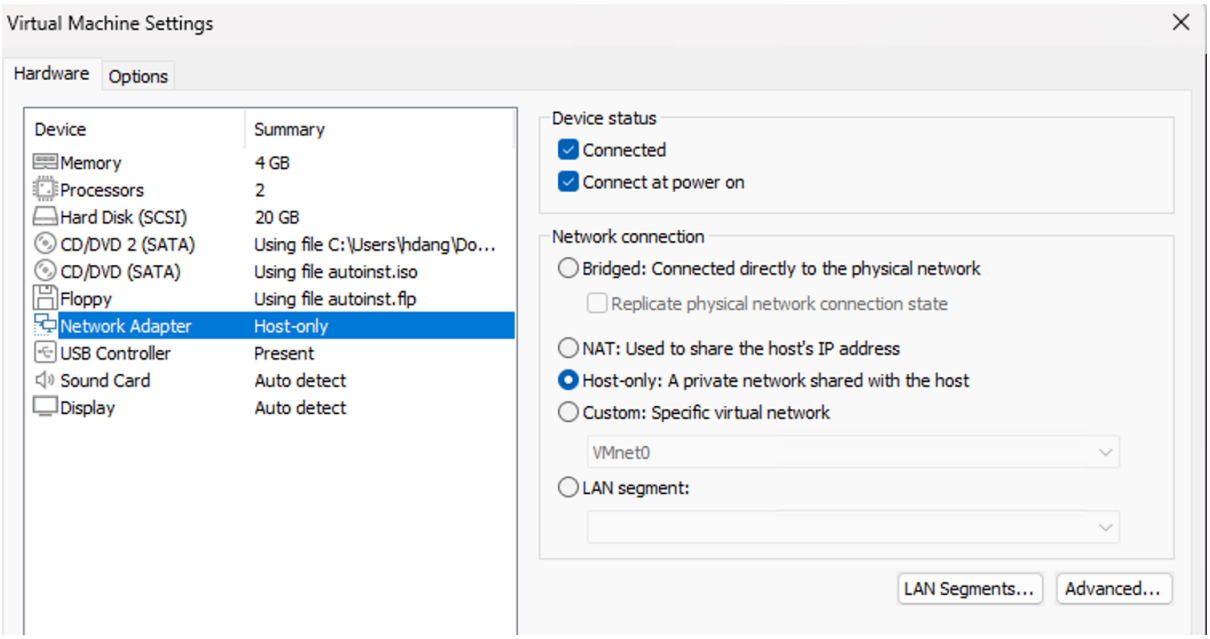
#Copy the following content to the new file and save it
admin:0:1234

B. Reconfigure the network of the virtual machine to make sure it is not connected to the internet (to avoid the security risk due to the honeypot)

Right click the virtual machine and choose “Settings”



Choose “Network adapter” -> Host-only



C. Starting Cowrie

```
(cowrie-env) $ cowrie start
```

```
(cowrie-env) cowrie@student-VMware-Virtual-Platform:~/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.pi
d --logger cowrie.python.logfile.logger cowrie]...
/home/cowrie/cowrie/cowrie-env/lib/python3.12/site-packages/twisted/conch/ssh/transpo
rt.py:110: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.h
azmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.haz
mat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/home/cowrie/cowrie/cowrie-env/lib/python3.12/site-packages/twisted/conch/ssh/transpo
rt.py:117: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.h
azmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.haz
mat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
```

Verify if cowrie is running by opening another terminal and check if the port 2222 is open

netstat -tan

```
student@student-VMware-Virtual-Platform:~$ netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2223            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2222            0.0.0.0:*               LISTEN
tcp        0      1 192.168.20.132:57378    192.168.20.1:53         SYN_SENT
tcp6       0      0 ::1:631                 :::*                    LISTEN
```

D. Get IP address of the VM
ifconfig

```
student@student-VMware-Virtual-Platform:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.20.132  netmask 255.255.255.0  broadcast 192.168.20.255
        inet6 fe80::20c:29ff:fe6a:e8db  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:6a:e8:db  txqueuelen 1000  (Ethernet)
        RX packets 84417  bytes 120302346 (120.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15644  bytes 1847006 (1.8 MB)
        TX errors 0  dropped 4 overruns 0  carrier 0  collisions 0
```

E. Simulating attacks by using the host machine
Open the terminal/ windows shell of the host machine
Connect SSH to the targeted VM using the above username and password
ssh admin@ip_address_of_VM -p 2222
Password: 1234

```
ssh admin@192.168.20.132 -p 2222
```

Assuming you connect ssh successfully to Cowrie, run a few command lines as a simulated intrusion as below:

```
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.
admin@svr04:~$ pwd
/home/admin
admin@svr04:~$ ls
admin@svr04:~$ mkdir test
admin@svr04:~$
```

F. In the virtual machine, view the log of the simulated intrusion above
cat var/log/cowrie.log

```
(cowrie-env) cowrie@student-VMware-Virtual-Platform:~/cowrie$ cat var/log/cowrie/cowrie.log
```

You will see the log of the above command lines (e.g. pwd, ls, mkdir test)

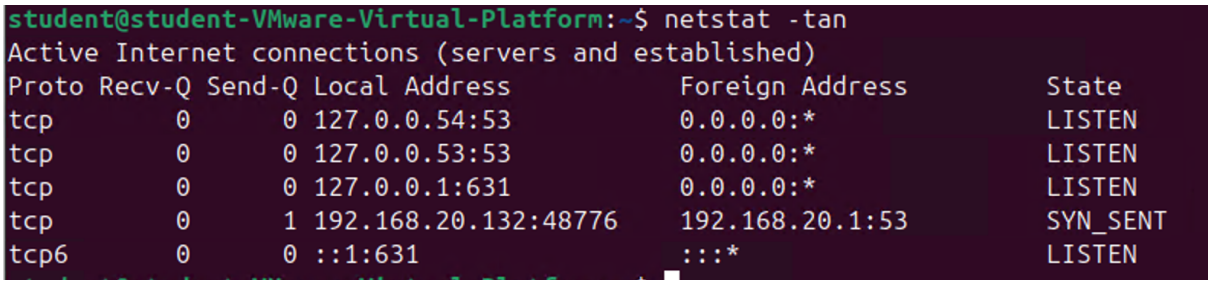
```
2025-12-04T11:56:40.125009Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSS
HTransport,5,192.168.20.1] Terminal Size: 120 30
2025-12-04T11:56:40.125352Z [twisted.conch.ssh.session#info] Getting shell
2025-12-04T11:56:43.143445Z [HoneyPotSSHTransport,5,192.168.20.1] CMD: pwd
2025-12-04T11:56:43.143790Z [HoneyPotSSHTransport,5,192.168.20.1] Command found: pwd
2025-12-04T11:56:44.550677Z [HoneyPotSSHTransport,5,192.168.20.1] CMD: ls
2025-12-04T11:56:44.551013Z [HoneyPotSSHTransport,5,192.168.20.1] Command found: ls
2025-12-04T11:56:50.532443Z [HoneyPotSSHTransport,5,192.168.20.1] CMD: mkdir test
2025-12-04T11:56:50.532785Z [HoneyPotSSHTransport,5,192.168.20.1] Command found: mkdir test
```

G. Stop Cowrie

```
(cowrie-env) cowrie@student-VMware-Virtual-Platform:~/cowrie$ cowrie stop
Stopping cowrie...
```

Verify if cowrie is NOT running by opening another terminal and check if the port 2222 is NOT open

netstat -tan



H. Deactivate the virtual environment

```
deactivate
```