Name: Harshil Amit
Buch
Class: TY CSF 1
Roll No: 14

KALI LINUX LAB

LAB 09

TITLE: Set up a honeypot to detect and analyze potential intrusions

Set up a Cowrie honeypot to detect, analyze, and understand potential intrusion attempts in a controlled environment.

What is a Honeypot?

A **honeypot** is a security mechanism designed to:

- **Attract** potential attackers
- **Decoy** them away from real systems
- **Monitor** and **analyze** their techniques
- **Learn** about attack methodologies

Types of Honeypots

- **Low-Interaction**: Emulates services (like our Cowrie SSH honeypot)
- **High-Interaction**: Real systems with extensive monitoring
- **Production**: Protect organizational assets
- **Research**: Study attacker behavior

What is Cowrie (and how it fits into honeypots)?

Cowrie is an open-source, medium-interaction SSH and Telnet honeypot written in Python.
It emulates a fake shell environment and services that attackers try to log into, captures their commands, uploaded files, and attempted payloads, and records network/session activity for analysis. Cowrie is widely used for research and detection because it provides rich logs (including full sessions), can collect malware, and supports integration with logging stacks.

Why use Cowrie (quick benefits)

- **Captures attacker behavior**: Commands typed, attempted uploads, interactive sessions.
- **Collects malware**: Files attackers try to upload (e.g., Linux binaries, scripts).
- **Medium interaction**: More realistic than low-interaction emulators (better telemetry) but safer than exposing a real system.

- **Extensible & scriptable**: Plugins, logging backends (JSON, database, Elastic), and custom shell prompts.

COMMANDS:

PHASE 1: SETUP

1. Update and install

```
sudo apt update
sudo apt install -y git python3-virtualenv
```

2. Create user and get Cowrie

```
sudo adduser --disabled-password cowrie
sudo su - cowrie
git clone https://github.com/cowrie/cowrie.git
cd cowrie
```

PHASE 2: INSTALL AND CONFIGURE

3. Setup environment

```
virtualenv --python=python3 cowrie-env
source cowrie-env/bin/activate
```

4. Install requirements

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

5. Install in development mode (SOLUTION 1 - CREATES bin/cowrie)

```
pip install -e .
```

6. Quick config

```
cd etc/
cp cowrie.cfg.dist cowrie.cfg
cp userdb.example userdb.txt
echo "root:password123" >> userdb.txt
cd ..
```

PHASE 3: START HONEYPOT

7. Start honeypot (NOW bin/cowrie EXISTS)

```
bin/cowrie start
```

TROUBLESHOOT ISSUES:

Problem: Missing bin/cowrie Script
Symptoms: bin/cowrie: No such file or directory

```
ls -la              # Check directory structure
ls -la bin/         # Verify script existence
```

Solution 1: Development Installation

```
pip install -e .    # Creates required scripts
```

Solution 2: Manual Script Creation

```
cat > bin/cowrie << 'EOF'
#!/usr/bin/env python3
from cowrie.scripts import cowrie
if __name__ == '__main__':
    cowrie.main()
EOF

chmod +x bin/cowrie
```

PHASE 4: TEST HONEYPOT

8. In NEW terminal, test the honeypot

```
ssh root@localhost -p 2222   # Password: password123
```

You will be asked something like this…..
Are you sure you want to continue connecting (yes/no/[fingerprint])? **TYPE YES**

try normal kali linux commands (whoami, pwd. Ls, uname -a)

9. Back in honeypot terminal, check logs

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

```
└─$ sudo apt update
[sudo] password for     kali
Hit:1 http://http.kali.org/kali kali-rolling InRelease
120 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(kali㉿kali)/㉿ vbox)-[~]
└─$ sudo apt install -y git python3-virtualenv
git is already the newest version (1:2.51.0-1).
git set to manually installed.
python3-virtualenv is already the newest version (20.35.3+ds-1).
python3-virtualenv set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 120

┌──(kali㉿kali)/㉿ vbox)-[~]
└─$ sudo adduser --disabled-password cowrie
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
```

```
┌──(kali㉿kali)/㉿ vbox)-[~]
└─$ sudo su - cowrie
┌──(cowrie㉿ vbox)-[~]
└─$ git clone https://github.com/cowrie/cowrie.git
Cloning into 'cowrie'...
remote: Enumerating objects: 20277, done.
remote: Counting objects: 100% (783/783), done.
remote: Compressing objects: 100% (373/373), done.
remote: Total 20277 (delta 696), reused 410 (delta 410), pack-reused 19494 (fro
 4)
Receiving objects: 100% (20277/20277), 11.18 MiB | 4.77 MiB/s, done.
Resolving deltas: 100% (14121/14121), done.

┌──(cowrie㉿ vbox)-[~]
└─$ cd cowrie

┌──(cowrie㉿ vbox)-[~/cowrie]
└─$ virtualenv --python=python3 cowrie-env
created virtual environment CPython3.13.7.final.0-64 in 1560ms
  creator CPython3Posix(dest=/home/cowrie/cowrie/cowrie-env, clear=False, no_vcs
_ignore=False, global=False)
  seeder FromAppData(download=False, pip=bundle, via=copy, app_data_dir=/home/co
wrie/.local/share/virtualenv)
```

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

┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie]
└─$ pip install -r requirements.txt
Collecting attrs==25.4.0 (from -r requirements.txt (line 1))
  Downloading attrs-25.4.0-py3-none-any.whl.metadata (10 kB)
Collecting bcrypt==5.0.0 (from -r requirements.txt (line 2))
  Downloading bcrypt-5.0.0-cp39-abi3-manylinux_2_34_x86_64.whl.metadata (10 kB)
Collecting cryptography==46.0.2 (from -r requirements.txt (line 3))
  Downloading cryptography-46.0.2-cp311-abi3-manylinux_2_34_x86_64.whl.metadata
(5.7 kB)
Collecting hyperlink==21.0.0 (from -r requirements.txt (line 4))
  Downloading hyperlink-21.0.0-py2.py3-none-any.whl.metadata (1.5 kB)
Collecting idna==3.11 (from -r requirements.txt (line 5))
  Downloading idna-3.11-py3-none-any.whl.metadata (8.4 kB)
Collecting packaging==25.0 (from -r requirements.txt (line 6))
  Downloading packaging-25.0-py3-none-any.whl.metadata (3.3 kB)
Collecting pyasn1_modules==0.4.2 (from -r requirements.txt (line 7))
  Downloading pyasn1_modules-0.4.2-py3-none-any.whl.metadata (3.5 kB)
Collecting requests==2.32.5 (from -r requirements.txt (line 8))
  Downloading requests-2.32.5-py3-none-any.whl.metadata (4.9 kB)
Collecting service_identity==24.2.0 (from -r requirements.txt (line 9))
```

```
sted-25.5.0 typing-extensions-4.15.0 urllib3-2.5.0 zope-interface-8.0.1

┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie]
└─$ cd etc/

┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie/etc]
└─$ cp cowrie.cfg.dist cowrie.cfg

┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie/etc]
└─$ cp userdb.example userdb.txt

┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie/etc]
└─$ echo "root:password123" >> userdb.txt

┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie/etc]
└─$ cd ..

┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie]
└─$ bin/cowrie start
-bash: bin/cowrie: No such file or directory

┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie]
└─$ ls -la
total 152
```

```
┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie]
└─$ ls -la bin/
total 16
drwxrwxr-x  2 cowrie cowrie 4096 Nov  2 15:34 .
drwxrwxr-x 12 cowrie cowrie 4096 Nov  2 15:37 ..
-rwxrwxr-x  1 cowrie cowrie  256 Nov  2 15:34 createdynamicprocess
-rwxrwxr-x  1 cowrie cowrie  193 Nov  2 15:34 regen-dropin.cache

┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie]
└─$ 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
Requirement already satisfied: attrs==25.4.0 in ./cowrie-env/lib/python3.13/site
-packages (from cowrie==2.8.2.dev25+g807881d8f) (25.4.0)
Requirement already satisfied: bcrypt==5.0.0 in ./cowrie-env/lib/python3.13/site
-packages (from cowrie==2.8.2.dev25+g807881d8f) (5.0.0)
Requirement already satisfied: cryptography==46.0.2 in ./cowrie-env/lib/python3
13/site-packages (from cowrie==2.8.2.dev25+g807881d8f) (46.0.2)
Requirement already satisfied: hyperlink==21.0.0 in ./cowrie-env/lib/python3.13/
```

```
┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie]
└─$ bin/cowrie start
-bash: bin/cowrie: No such file or directory

┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie]
└─$ cat > bin/cowrie << 'EOF'
#!/usr/bin/env python3
from cowrie.scripts import cowrie
if __name__ == '__main__':
    cowrie.main()
EOF

┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie]
└─$ chmod +x bin/cowrie

┌──(cowrie-env)(cowrie㉿vbox)-[~/cowrie]
└─$ bin/cowrie start
cowrie is already running (PID: 8854).
```