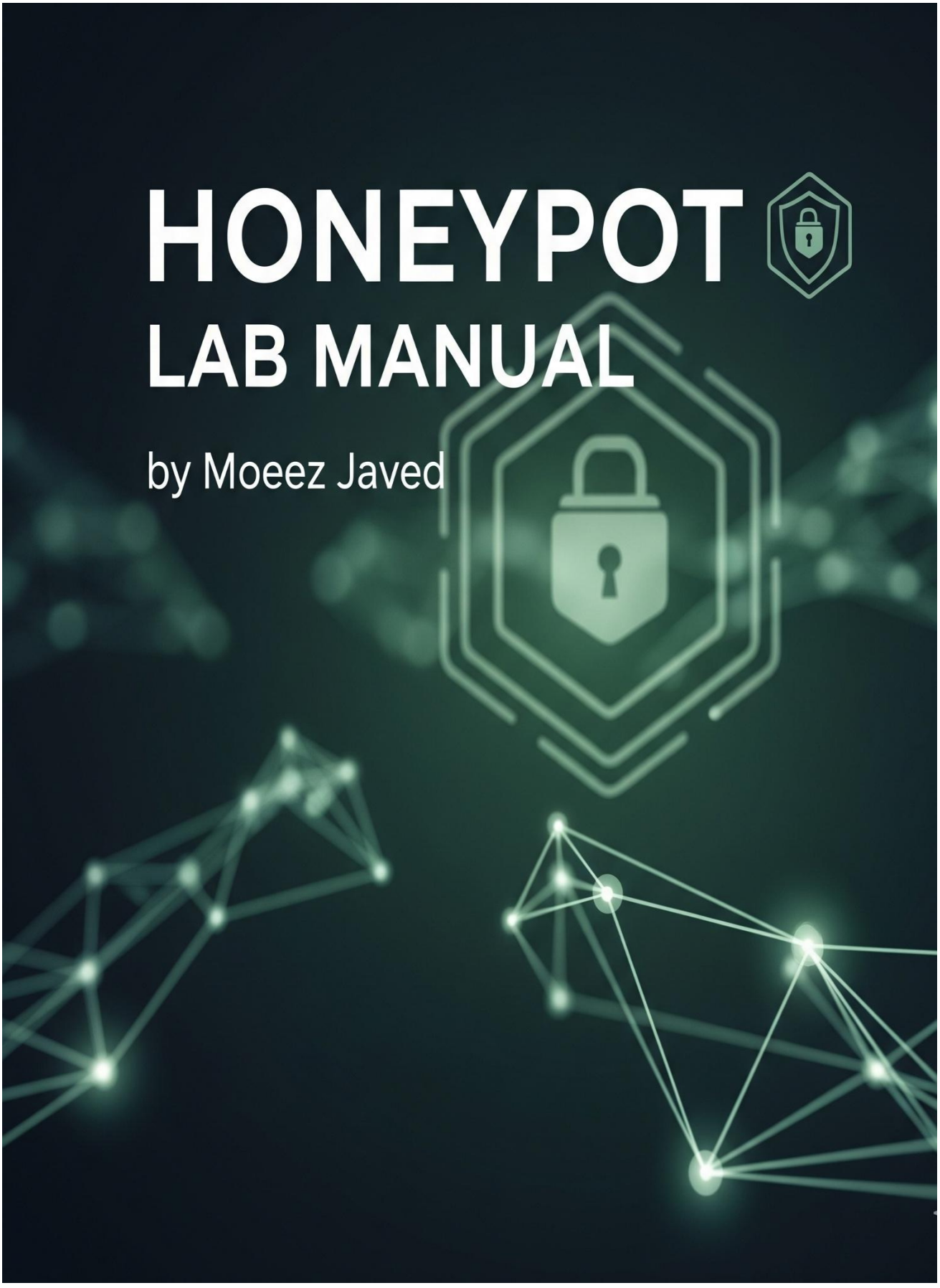

HONEYPOT
LAB MANUAL
by Moeez Javed

Honeypot Lab Manual

Audience: Cybersecurity / SOC Analyst /Ethical Hacker / Penetration Tester
Skill Level: Beginner → Intermediate
Target OS: Ubuntu/Kali Linux (VM recommended)

1) Introduction — What is a Honeypot & Why It Matters

A **honeypot** is a decoy system or service designed to look enticing to attackers. Instead of protecting real assets directly, it **attracts** and **observes** malicious activity so defenders can learn from it.

Why it's important for students: - **Hands-on detection practice:** See real(istic) attacker behavior and artifacts in logs. - **Threat intel:** Identify common scanning and exploitation attempts in your environment. - **Low risk when isolated:** Purpose-built to be probed; great for controlled learning. - **SOC skill building:** Parsing logs, crafting alerts, and writing incident notes.

> ⚠️ **Safety & Ethics:** Run this lab in an **isolated VM network**. Do **not** deploy to the public internet without written authorization. Do not interact with found malware or share captured data outside the class.

2) Lab Outcomes

By the end, you will be able to: 1. Explain honeypot/honeytoken concepts and use-cases. 2. Deploy two popular honeypots: **OpenCanary** (multi-protocol) and **Cowrie** (SSH/Telnet). 3. Generate benign "attacks" to produce logs. 4. Parse and triage events, then write a brief incident note.

3) Lab Topology (Recommended)

- **Attacker VM:** Kali/Ubuntu (your workstation can play this role)
- **Honeypot VM:** Ubuntu Server 22.04+ (2 vCPU, 2–4 GB RAM)
- **Network:** Host-only or NAT network (no inbound from the public internet)

[Attacker VM] <—— same private lab network ——> [Honeypot VM]

> Tip: Take snapshots before the lab. Name them pre-honeypot and post-honeypot for easy rollback.

4) Quick Theory: Types of Deception

- **Honeypot:** Fake system/service (e.g., fake SSH, FTP, SMB) to log interaction.
- **Honeyservice:** Decoy instance of a real protocol (e.g., HTTP on port 80).
- **Honeytoken:** Fake data (API key, doc link, email) that alerts when touched.

5) Prerequisites (Run on Honeypot VM)

*sudo apt update **&&** sudo apt -y upgrade*
sudo apt -y install python3 python3-venv python3-pip git iptables-persistent

```
ubuntu@ubuntu-VirtualBox:~$ sudo apt install python3.10 python3.10-venv
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libpython3.10-minimal libpython3.10-stdlib python3.10-distutils
  python3.10-lib2to3 python3.10-minimal
Suggested packages:
  binfmt-support
The following NEW packages will be installed:
  libpython3.10-minimal libpython3.10-stdlib python3.10 python3.10-distutils
  python3.10-lib2to3 python3.10-minimal python3.10-venv
0 upgraded, 7 newly installed, 0 to remove and 78 not upgraded.
Need to get 8,007 kB of archives.
After this operation, 24.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ppa.launchpad.net/deadsnakes/ppa/ubuntu focal/main amd64 libpython
3.10-minimal amd64 3.10.18-1+focal1 [826 kB]
Get:2 http://ppa.launchpad.net/deadsnakes/ppa/ubuntu focal/main amd64 python3.1
0-minimal amd64 3.10.18-1+focal1 [2,081 kB]
Get:3 http://ppa.launchpad.net/deadsnakes/ppa/ubuntu focal/main amd64 libpython
3.10-stdlib amd64 3.10.18-1+focal1 [1,765 kB]
Get:4 http://ppa.launchpad.net/deadsnakes/ppa/ubuntu focal/main amd64 python3.1
0 amd64 3.10.18-1+focal1 [92.5 kB]
Get:5 http://ppa.launchpad.net/deadsnakes/ppa/ubuntu focal/main amd64 python3.1
0-lib2to3 all 3.10.18-1+focal1 [126 kB]
Get:6 http://ppa.launchpad.net/deadsnakes/ppa/ubuntu focal/main amd64 python3.1
0-distutils all 3.10.18-1+focal1 [187 kB]
Get:7 http://ppa.launchpad.net/deadsnakes/ppa/ubuntu focal/main amd64 python3.1
```

If using Kali: Python3 is preinstalled; still run apt update and install missing packages.

6) Option A — OpenCanary (Multi-Protocol Honeypot)

OpenCanary is light, flexible, and great for beginner SOC exercises.

6.1 Install & Configure

1) Create a non-privileged user (optional but recommended)
sudo adduser --disabled-password --gecos "" canary

```
ubuntu@ubuntu-VirtualBox:~$ sudo adduser --disabled-password --gecos "" canary
[sudo] password for ubuntu:
Adding user `canary' ...
Adding new group `canary' (1001) ...
Adding new user `canary' (1001) with group `canary' ...
Creating home directory `/home/canary' ...
Copying files from `/etc/skel' ...
```

Optional:{

sudo adduser newuser
sudo usermod -aG sudo newuser

```
ubuntu@ubuntu-VirtualBox:~$ sudo usermod -aG sudo newuser
```

sudo usermod -aG sudo canary
sudo passwd canary

```
ubuntu@ubuntu-VirtualBox:~$ sudo passwd canary
New password:
Retype new password:
passwd: password updated successfully
```

su – canary

```
ubuntu@ubuntu-VirtualBox:~$ su - canary
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

}

sudo apt install python3.10 python3.10-venv
which python3.10
python3.10 -- version

```
ubuntu@ubuntu-VirtualBox:~$ sudo apt install python3.10 python3.10-venv
Reading package lists... Done
Building dependency tree
Reading state information... Done
python3.10 is already the newest version (3.10.18-1+focal1).
python3.10-venv is already the newest version (3.10.18-1+focal1).
0 upgraded, 0 newly installed, 0 to remove and 78 not upgraded.
ubuntu@ubuntu-VirtualBox:~$ which python3.10
/usr/bin/python3.10
ubuntu@ubuntu-VirtualBox:~$ python3.10 --version
Python 3.10.18
ubuntu@ubuntu-VirtualBox:~$
```

 # 2) Switch to the canary user

sudo -iu canary

```
ubuntu@ubuntu-VirtualBox:~$ sudo -iu canary
canary@ubuntu-VirtualBox:~$ python3.10 -m venv ~/venv
```

 # 3) Make a Python virtual environment

python3.10 -m venv ~/venv

source ~/venv/bin/activate

```
canary@ubuntu-VirtualBox:~$ python3.10 -m venv ~/venv
canary@ubuntu-VirtualBox:~$ source ~/venv/bin/activate
(venv) canary@ubuntu-VirtualBox:~$ source ~/venv/bin/activate
```

 # 4) Install OpenCanary

pip install --upgrade pip wheel

```
(venv) canary@ubuntu-VirtualBox:~$ pip install --upgrade pip wheel
Requirement already satisfied: pip in ./venv/lib/python3.10/site-packages (23.0
.1)
Collecting pip
  Downloading pip-25.2-py3-none-any.whl (1.8 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.8/1.8 MB 1.6 MB/s eta 0:00:00
Collecting wheel
  Downloading wheel-0.45.1-py3-none-any.whl (72 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 72.5/72.5 kB 4.0 MB/s eta 0:00:00
Installing collected packages: wheel, pip
  Attempting uninstall: pip
    Found existing installation: pip 23.0.1
    Uninstalling pip-23.0.1:
      Successfully uninstalled pip-23.0.1
Successfully installed pip-25.2 wheel-0.45.1
```

pip install opencanary

```
(venv) canary@ubuntu-VirtualBox:~$ pip install opencanary

Collecting opencanary
  Downloading opencanary-0.9.6.tar.gz (3.0 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 3.0/3.0 MB 919.3 kB/s  0:00:03
  Preparing metadata (setup.py) ... done
Collecting Twisted==24.11.0 (from opencanary)
  Downloading twisted-24.11.0-py3-none-any.whl.metadata (20 kB)
Collecting pyasn1==0.4.5 (from opencanary)
  Downloading pyasn1-0.4.5-py2.py3-none-any.whl.metadata (1.5 kB)
Collecting cryptography==38.0.1 (from opencanary)
  Downloading cryptography-38.0.1-cp36-abi3-manylinux_2_28_x86_64.whl.metadata
(5.3 kB)
Collecting simplejson==3.16.0 (from opencanary)
  Downloading simplejson-3.16.0.tar.gz (81 kB)
  Preparing metadata (setup.py) ... done
Collecting requests==2.31.0 (from opencanary)
  Downloading requests-2.31.0-py3-none-any.whl.metadata (4.6 kB)
Collecting zope.interface==7.2 (from opencanary)
  Downloading zope.interface-7.2-cp310-cp310-manylinux_2_5_x86_64.manylinux1_x8
6_64.manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (44 kB)
Collecting PyPDF2==1.26.0 (from opencanary)
  Downloading PyPDF2-1.26.0.tar.gz (77 kB)
  Preparing metadata (setup.py) ... done
Collecting fpdf==1.7.2 (from opencanary)
  Downloading fpdf-1.7.2.tar.gz (39 kB)
  Preparing metadata (setup.py) ... done
```

 # 5) Create a default config file

pip install setuptools

 # 6) Edit the configuration

nano ~/.opencanary.conf

Suggested beginner config (paste into ~/.open-canary.conf):

```
{
 "device.node_id": "opencanary-1",
 "logger": {
  "class": "PyLogger",
  "kwargs": {
   "formatters": {
    "plain": {
     "format": "%(asctime)s %(message)s"
    }
   },
   "handlers": {
    "file": {
```

```
        "class": "logging.FileHandler",
        "filename": "/tmp/opencanary.log",
        "formatter": "plain"
      }
    }
  }
},
"ssh.enabled": true,
"ftp.enabled": true,
"http.enabled": true,
"http.banner": "Apache/2.4.1 (Unix)",
"http.port": 80,
"telnet.enabled": true,
"telnet.port": 23,
"ntp.enabled": true,
"ntp.port": 123,
"mysql.enabled": true,
"mysql.port": 3306,
"snmp.enabled": true,
"snmp.port": 161,
"vnc.enabled": true,
"vnc.port": 5900,
"rdp.enabled": true,
"rdp.port": 3389,
"tftp.enabled": true,
"tftp.port": 69,
"portscan.enabled": true,
"portscan.logfile": "/tmp/portscan.log",
"smb.enabled": true,
"smb.port": 445,
"mssql.enabled": true,
"mssql.port": 1433,
"redis.enabled": true,
"redis.port": 6379,
"tcpbanner.enabled": true,
"tcpbanner.port": 8000,
"tcpbanner.banner": "Welcome to OpenCanary",
"tcpbanner.regex": [],
"tcpbanner.logfile": "/tmp/tcpbanner.log"
}
```

Keep it simple. Enable **HTTP, FTP, SSH** for varied logs. You can enable more later.

6.2 Start / Stop / Status

 # Start

opencanaryd –start

```
(venv) canary@ubuntu-VirtualBox:~$ opencanaryd --start
WARNING: OpenCanary will not drop root user or group privileges after launching
. Set both --uid=nobody and --gid=nogroup (or another low privilege user/group)
 to silence this warning.
Another twistd server is running, PID 10794

This could either be a previously started instance of your application or a
different application entirely. To start a new one, either run it in some other
directory, or use the --pidfile and --logfile parameters to avoid clashes.
```

 # Status

opencanaryd --status

```
(venv) canary@ubuntu-VirtualBox:~$ opencanaryd --status

  OpenCanary

       opencanaryd [ --start | --dev | --stop | --restart | --copyconfig | --u
sermodule | --version | --help ] [--uid=nobody] [--gid=nogroup]


               --start Starts the opencanaryd process
               --dev   Run the opencanaryd process in the foreground
               --stop  Stops the opencanaryd process
               --usermodule    Run opencanaryd in foreground with only usermod
ules enabled
               --copyconfig    Creates a default config file at /etc/opencanar
yd/opencanary.conf
               --version       Displays the current opencanary version.
               --
               --help  This help

       options
               --allow-run-as-root     Do not drop privileges of the opencanar
y once process starts
               --uid   Specify a user or uid to drop privileges to
               --gid   Specify a group of gid to drop privileges to
(venv) canary@ubuntu-VirtualBox:~$
```

 # Stop

opencanaryd –stop

```
(venv) canary@ubuntu-VirtualBox:~$ opencanaryd --stop
[sudo] password for canary:
```

6.3 Where Are My Logs?

- File path (based on config): /home/canary/open_canary.log
- Real-time view:

ps -ef | grep twistd

```
(venv) canary@ubuntu-VirtualBox:~$ ps -ef | grep twistd
root       10916    1814  0 12:51 ?        00:00:00 /home/canary/venv/bin/pytho
n3.10 /home/canary/venv/bin/twistd -y /home/canary/venv/bin/opencanary.tac --pi
dfile /home/canary/venv/bin/opencanaryd.pid --syslog --prefix=opencanaryd
canary     11029   10249  0 12:54 pts/1    00:00:00 grep --color=auto twistd
```

tail -f /tmp/opencanary.log

```
(venv) canary@ubuntu-VirtualBox:~$ tail -f /tmp/opencanary.log
2025-09-02 12:55:00,472 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 07:55:00.472798", "local_time_adjusted": "2025-09-02 12:55:00.472824", "log
data": {"msg": {"logdata": "Added service from class CanaryTftp in opencanary.m
odules.tftp to fake"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host":
 "", "src_port": -1, "utc_time": "2025-09-02 07:55:00.472817"}
2025-09-02 12:55:00,473 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 07:55:00.473114", "local_time_adjusted": "2025-09-02 12:55:00.473135", "log
data": {"msg": {"logdata": "Added service from class CanaryVNC in opencanary.mo
dules.vnc to fake"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host": "
", "src_port": -1, "utc_time": "2025-09-02 07:55:00.473129"}
2025-09-02 12:55:00,473 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 07:55:00.473367", "local_time_adjusted": "2025-09-02 12:55:00.473382", "log
data": {"msg": {"logdata": "Added service from class MSSQL in opencanary.module
s.mssql to fake"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host": "",
 "src_port": -1, "utc_time": "2025-09-02 07:55:00.473378"}
2025-09-02 12:55:00,473 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 07:55:00.473614", "local_time_adjusted": "2025-09-02 12:55:00.473632", "log
data": {"msg": {"logdata": "Added service from class Telnet in opencanary.modul
es.telnet to fake"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host": "
", "src_port": -1, "utc_time": "2025-09-02 07:55:00.473627"}
2025-09-02 12:55:00,474 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 07:55:00.474192", "local_time_adjusted": "2025-09-02 12:55:00.474217", "log
data": {"msg": {"logdata": "Ran startYourEngines on class CanarySamba in openca
nary.modules.samba"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host":
"", "src_port": -1, "utc_time": "2025-09-02 07:55:00.474211"}
2025-09-02 12:55:00,958 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
```

grep -i ftp /tmp/opencanary.log | tail -n 10

```
(venv) canary@ubuntu-VirtualBox:~$ grep -i ftp /tmp/opencanary.log| tail -n 10
2025-09-02 12:55:00,225 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 07:55:00.225371", "local_time_adjusted": "2025-09-02 12:55:00.225412", "log
data": {"msg": {"logdata": "Added service from class CanaryFTP in opencanary.mo
dules.ftp to fake"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host": "
", "src_port": -1, "utc_time": "2025-09-02 07:55:00.225406"}
2025-09-02 12:55:00,472 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 07:55:00.472798", "local_time_adjusted": "2025-09-02 12:55:00.472824", "log
data": {"msg": {"logdata": "Added service from class CanaryTftp in opencanary.m
odules.tftp to fake"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host":
 "", "src_port": -1, "utc_time": "2025-09-02 07:55:00.472817"}
2025-09-02 13:29:15,817 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 08:29:15.817512", "local_time_adjusted": "2025-09-02 13:29:15.817546", "log
data": {"msg": {"logdata": "Added service from class CanaryFTP in opencanary.mo
dules.ftp to fake"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host": "
", "src_port": -1, "utc_time": "2025-09-02 08:29:15.817542"}
2025-09-02 13:29:16,021 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 08:29:16.021520", "local_time_adjusted": "2025-09-02 13:29:16.021533", "log
data": {"msg": {"logdata": "Added service from class CanaryTftp in opencanary.m
odules.tftp to fake"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host":
 "", "src_port": -1, "utc_time": "2025-09-02 08:29:16.021529"}
```

6.4 Generate Test Events (from Attacker VM)

 # Scan common ports

nmap -sS -sV -Pn <HONEYPOT_IP>

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -Pn 192.168.93.31
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 03:58 EDT
Nmap scan report for 192.168.93.31
Host is up (0.00073s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           vsftpd (before 2.0.8) or WU-FTPD
22/tcp   open  ssh           OpenSSH 5.1p1 Debian 5 (protocol 2.0)
23/tcp   open  telnet        Cisco telnetd
80/tcp   open  http          Apache httpd 2.4.1 ((Unix))
1433/tcp open  ms-sql-s      Microsoft SQL Server 2012 11.00.3128; SP1+
3306/tcp open  mysql         MySQL 5.5.43-0ubuntu0.14.04.1
3389/tcp open  ms-wbt-server
5900/tcp open  vnc           VNC (protocol 3.8)
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port3389-TCP:V=7.95%I=7%D=9/2%Time=68B6A3CA%P=x86_64-pc-linux-gnu%r(Ter
SF:minalServerCookie,13,"\x03\0\0\x13\x0e\xd0\0\0\x124\0\x02\t\x08\0\x02\0
SF:\0\0")%r(TerminalServer,13,"\x03\0\0\x13\x0e\xd0\0\0\x124\0\x02\t\x08\0
SF:\x02\0\0\0");
MAC Address: 08:00:27:DE:25:ED (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: OSs: Linux, IOS, Windows; Device: router; CPE: cpe:/o:linux:lin
ux_kernel, cpe:/o:cisco:ios, cpe:/o:microsoft:windows
```

 # Fake FTP login

nc <HONEYPOT_IP> 21

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.93.31 21
220 FTP Ready.
```

 # type: USER admin (press Enter)

 # type: PASS password123 (press Enter)

 # HTTP probe
curl -i http://<HONEYPOT_IP>/

```
┌──(kali㉿kali)-[~]
└─$ curl -i http://192.168.93.31/
HTTP/1.1 500 Internal Server Error
Server: Apache/2.4.1 (Unix)
Date: Tue, 02 Sep 2025 07:57:52 GMT
Content-Type: text/html
Location: /index.html
Content-Length: 95

<html><head><title>Processing Failed</title></head><body><b>Processing Failed</b></body></html>
```

 # SSH banner grab
nc <HONEYPOT_IP> 22

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.93.31 22
SSH-2.0-OpenSSH_5.1p1 Debian-5
```

6.5 Parse / Filter Events Quickly

 # Show last 25 lines
sudo tail -n 25 /tmp/opencanary.log

```
(venv) canary@ubuntu-VirtualBox:~$ sudo tail -n 25 /tmp/opencanary.log
2025-09-02 12:47:46,946 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 07:47:46.945988", "local_time_adjusted": "2025-09-02 12:47:46.946043", "log
data": {"msg": {"logdata": "Added service from class CanarySSH in opencanary.mo
dules.ssh to fake"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host": "
", "src_port": -1, "utc_time": "2025-09-02 07:47:46.946036"}
2025-09-02 12:47:46,946 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 07:47:46.946562", "local_time_adjusted": "2025-09-02 12:47:46.946587", "log
data": {"msg": {"logdata": "Canary running!!!"}}, "logtype": 1001, "node_id": "
opencanary-1", "src_host": "", "src_port": -1, "utc_time": "2025-09-02 07:47:46
.946583"}
2025-09-02 12:51:07,495 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 07:51:07.495322", "local_time_adjusted": "2025-09-02 12:51:07.495367", "log
data": {"msg": {"logdata": "Added service from class CanarySSH in opencanary.mo
dules.ssh to fake"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host": "
", "src_port": -1, "utc_time": "2025-09-02 07:51:07.495361"}
2025-09-02 12:51:07,495 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 07:51:07.495774", "local_time_adjusted": "2025-09-02 12:51:07.495795", "log
data": {"msg": {"logdata": "Canary running!!!"}}, "logtype": 1001, "node_id": "
opencanary-1", "src_host": "", "src_port": -1, "utc_time": "2025-09-02 07:51:07
.495791"}
2025-09-02 12:55:00,225 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 07:55:00.225371", "local_time_adjusted": "2025-09-02 12:55:00.225412", "log
data": {"msg": {"logdata": "Added service from class CanaryFTP in opencanary.mo
dules.ftp to fake"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host": "
", "src_port": -1, "utc_time": "2025-09-02 07:55:00.225406"}
2025-09-02 12:55:00,229 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
```

 # Grep for a service (e.g., ftp)

grep -i ftp /home/canary/open canary.log | tail -n 10

```
(venv) canary@ubuntu-VirtualBox:~$ grep -i ftp /tmp/opencanary.log | tail -n 10
2025-09-02 12:55:00,225 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 07:55:00.225371", "local_time_adjusted": "2025-09-02 12:55:00.225412", "log
data": {"msg": {"logdata": "Added service from class CanaryFTP in opencanary.mo
dules.ftp to fake"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host": "
", "src_port": -1, "utc_time": "2025-09-02 07:55:00.225406"}
2025-09-02 12:55:00,472 {"dst_host": "", "dst_port": -1, "local_time": "2025-09
-02 07:55:00.472798", "local_time_adjusted": "2025-09-02 12:55:00.472824", "log
data": {"msg": {"logdata": "Added service from class CanaryTftp in opencanary.m
odules.tftp to fake"}}, "logtype": 1001, "node_id": "opencanary-1", "src_host":
 "", "src_port": -1, "utc_time": "2025-09-02 07:55:00.472817"}
```

Task: Identify the source IP, service, and artifact (username, URL, etc.) for at least 3 events.

7) Option B — Cowrie (SSH/Telnet Interaction Honeypot)

Cowrie emulates SSH/Telnet and logs brute force attempts and attacker commands.

Optional:{

sudo adduser newuser
sudo usermod -aG sudo newuser

```
ubuntu@ubuntu-VirtualBox:~$ sudo usermod -aG sudo newuser
```

sudo usermod -aG sudo cowrie
sudo passwd cowrie

```
ubuntu@ubuntu-VirtualBox:~$ sudo usermod -aG sudo cowrie
ubuntu@ubuntu-VirtualBox:~$ sudo passwd cowrie
New password:
Retype new password:
passwd: password updated successfully
```

su – cowrie

```
ubuntu@ubuntu-VirtualBox:~$ su -cowrie
Password:
su: Authentication failure
ubuntu@ubuntu-VirtualBox:~$ su - cowrie
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

}

7.1 Install Cowrie

Create a dedicated user
sudo adduser newuser
sudo usermod -aG sudo newuser

```
ubuntu@ubuntu-VirtualBox:~$ sudo usermod -aG sudo newuser
```

sudo usermod -aG sudo cowrie
sudo passwd cowrie

```
ubuntu@ubuntu-VirtualBox:~$ sudo usermod -aG sudo cowrie
ubuntu@ubuntu-VirtualBox:~$ sudo passwd cowrie
New password:
Retype new password:
passwd: password updated successfully
```

su – cowrie

```
ubuntu@ubuntu-VirtualBox:~$ su -cowrie
Password:
su: Authentication failure
ubuntu@ubuntu-VirtualBox:~$ su - cowrie
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

Get source & set up venv
apt install git

```
cowrie@ubuntu-VirtualBox:~$ sudo apt install git
[sudo] password for cowrie:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-el git-email git-gui gitk
  gitweb git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
  git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 78 not upgraded.
Need to get 5,525 kB of archives.
After this operation, 38.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://pk.archive.ubuntu.com/ubuntu focal/main amd64 liberror-perl all 0.
17029-1 [26.5 kB]
Get:2 http://pk.archive.ubuntu.com/ubuntu focal-updates/main amd64 git-man all
1:2.25.1-1ubuntu3.13 [887 kB]
Get:3 http://pk.archive.ubuntu.com/ubuntu focal-updates/main amd64 git amd64 1:
2.25.1-1ubuntu3.13 [4,612 kB]
Fetched 5,525 kB in 9s (637 kB/s)
Selecting previously unselected package liberror-perl.
(Reading database ... 193111 files and directories currently installed.)
Preparing to unpack .../liberror-perl 0.17029-1 all.deb ...
```

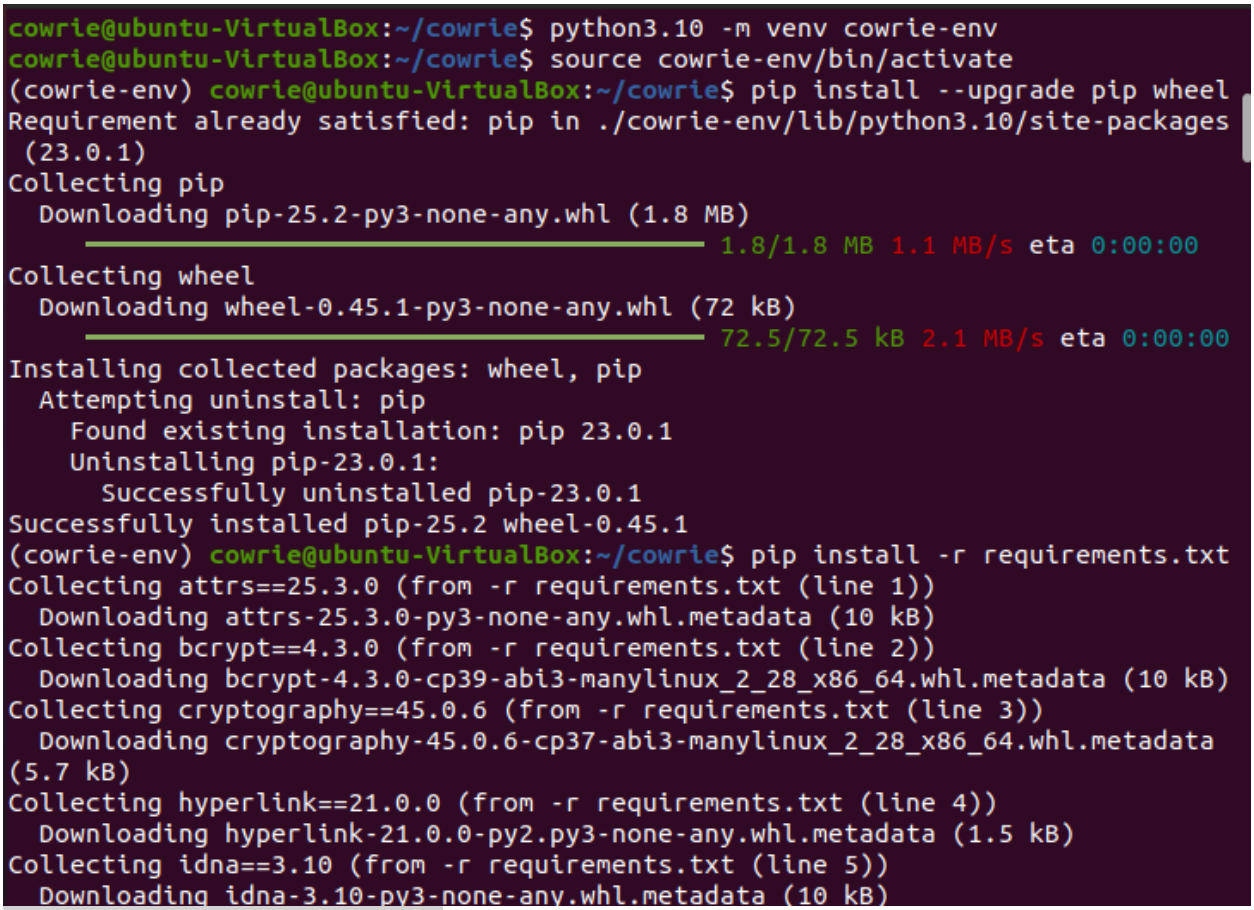
git clone https://github.com/cowrie/cowrie.git
cd cowrie

```
cowrie@ubuntu-VirtualBox:~$ git clone https://github.com/cowrie/cowrie.git
Cloning into 'cowrie'...
remote: Enumerating objects: 19466, done.
remote: Counting objects: 100% (458/458), done.
remote: Compressing objects: 100% (268/268), done.
remote: Total 19466 (delta 389), reused 194 (delta 189), pack-reused 19008 (fro
m 3)
Receiving objects: 100% (19466/19466), 10.62 MiB | 1.45 MiB/s, done.
Resolving deltas: 100% (13656/13656), done.
cowrie@ubuntu-VirtualBox:~$ cd cowrie
```

python3.10 -m venv cowrie-env
which python 3.10

```
cowrie@ubuntu-VirtualBox:~/cowrie$ sudo apt install python3.10 python3.10-venv
Reading package lists... Done
Building dependency tree
Reading state information... Done
python3.10 is already the newest version (3.10.18-1+focal1).
python3.10-venv is already the newest version (3.10.18-1+focal1).
0 upgraded, 0 newly installed, 0 to remove and 78 not upgraded.
cowrie@ubuntu-VirtualBox:~/cowrie$ which python3.10
/usr/bin/python3.10
```

source cowrie-env/bin/activate
pip install --upgrade pip wheel



pip install -r requirements.txt

```
(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ pip install -r requirements.txt
Collecting attrs==25.3.0 (from -r requirements.txt (line 1))
  Downloading attrs-25.3.0-py3-none-any.whl.metadata (10 kB)
Collecting bcrypt==4.3.0 (from -r requirements.txt (line 2))
  Downloading bcrypt-4.3.0-cp39-abi3-manylinux_2_28_x86_64.whl.metadata (10 kB)
Collecting cryptography==45.0.6 (from -r requirements.txt (line 3))
  Downloading cryptography-45.0.6-cp37-abi3-manylinux_2_28_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==3.10 (from -r requirements.txt (line 5))
  Downloading idna-3.10-py3-none-any.whl.metadata (10 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))
  Downloading service_identity-24.2.0-py3-none-any.whl.metadata (5.1 kB)
Collecting tftpy==0.8.6 (from -r requirements.txt (line 10))
  Downloading tftpy-0.8.6-py3-none-any.whl.metadata (5.6 kB)
Collecting treq==25.5.0 (from -r requirements.txt (line 11))
  Downloading treq-25.5.0-py3-none-any.whl.metadata (3.9 kB)
Collecting twisted==25.5.0 (from twisted[conch]==25.5.0->-r requirements.txt (l
ine 12))
  Downloading twisted-25.5.0-py3-none-any.whl.metadata (22 kB)
```

Create configuration

cp etc/cowrie.cfg.dist etc/cowrie.cfg

```
(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ cp etc/cowrie.cfg.dist etc/cowr
ie.cfg
```

Don’t change anything

{

nano etc/cowrie.cfg

Minimum edits in etc/cowrie.cfg:

Optional{
[ssh]
listen_endpoints = tcp:2222:interface=0.0.0.0

[telnet]
enabled = false

[honeypot]
hostname = ubuntu

[output_jsonlog]
enabled = true
logfile = var/log/cowrie/cowrie.json

> *Leave SSH on port **2222** for the lab to avoid root binding. We'll connect to 2222 explicitly when testing.*

}

7.2 Start / Stop / Status

 # Start (from cowrie directory)
bin/cowrie start

```
(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ bin/cowrie start
Using activated Python virtual environment "/home/cowrie/cowrie/cowrie-env"

DEPRECATION: Python<3.9 is no longer supported by Cowrie.

Starting cowrie: [twistd  --umask=0022 --pidfile=var/run/cowrie.pid --logger co
wrie.python.logfile.logger cowrie ]...
/home/cowrie/cowrie/cowrie-env/lib/python3.10/site-packages/twisted/conch/ssh/t
ransport.py:110: CryptographyDeprecationWarning: TripleDES has been moved to cr
yptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed fro
m cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/home/cowrie/cowrie/cowrie-env/lib/python3.10/site-packages/twisted/conch/ssh/t
ransport.py:117: CryptographyDeprecationWarning: TripleDES has been moved to cr
yptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed fro
m cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
Another twistd server is running, PID 11067

This could either be a previously started instance of your application or a
different application entirely. To start a new one, either run it in some other
directory, or use the --pidfile and --logfile parameters to avoid clashes.
```

 # Status
bin/cowrie status

```
(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ bin/cowrie status
cowrie is running (PID: 11067).
```

 # Stop
bin/cowrie stop

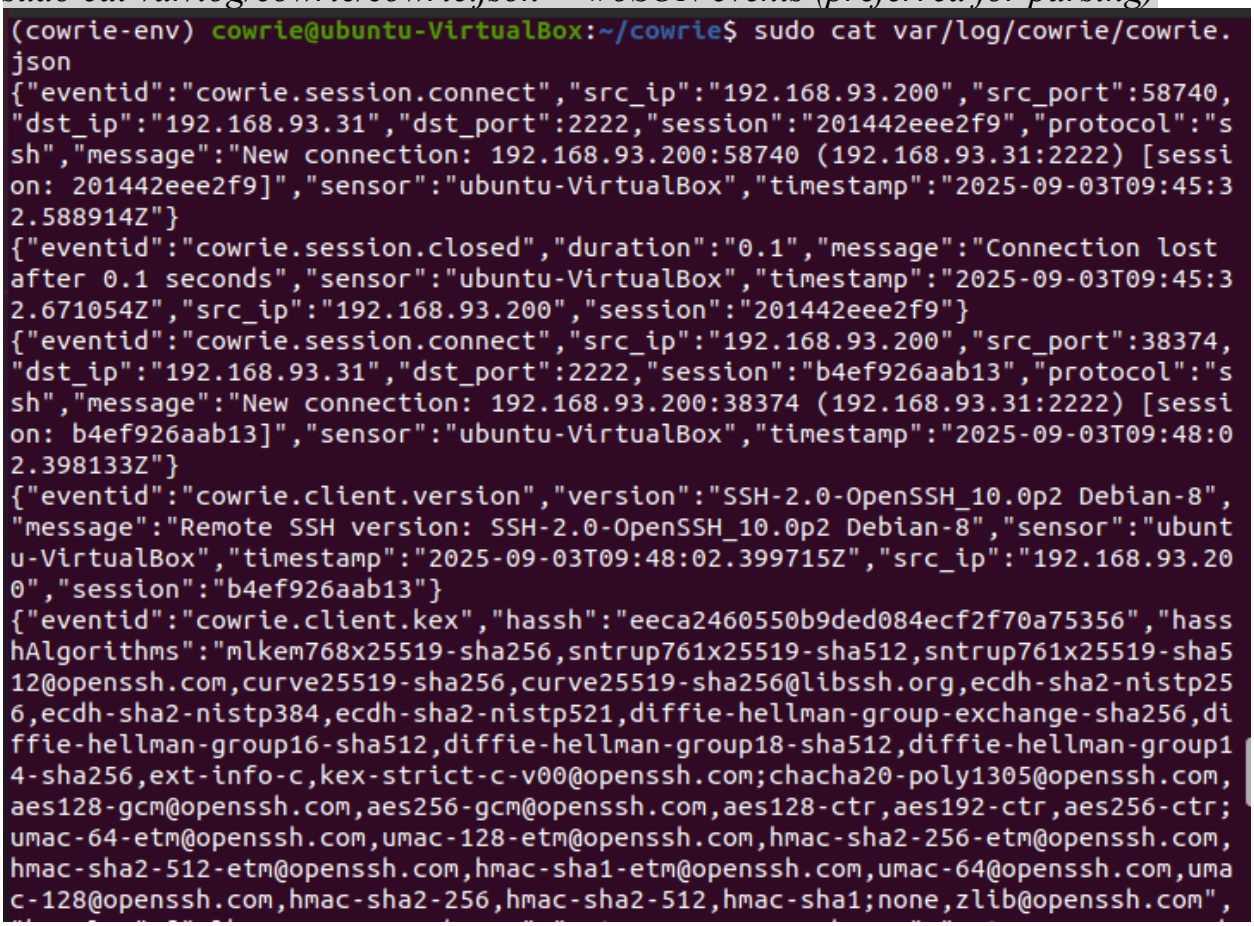
7.3 Log Locations

Sudo cat var/log/cowrie/cowrie.log # human-readable events

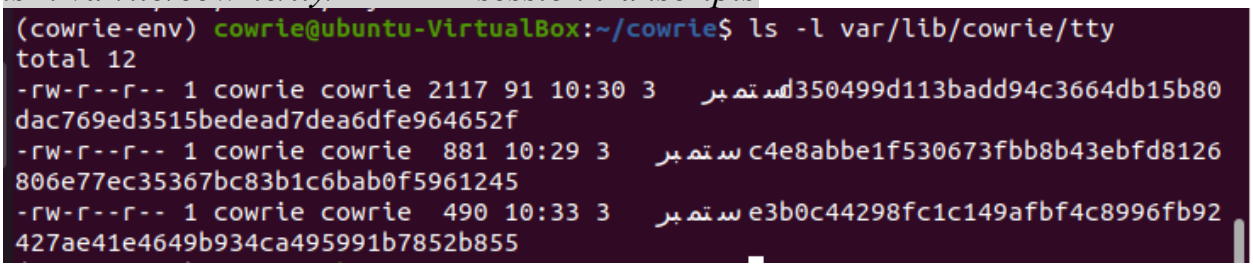
```
(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ sudo cat var/log/cowrie/cowrie.
log
2025-09-03T09:43:58.710944Z [-] Reading configuration from ['/home/cowrie/cowri
e/etc/cowrie.cfg.dist', '/home/cowrie/cowrie/etc/cowrie.cfg']
2025-09-03T09:43:59.136879Z [-] Python Version 3.10.18 (main, Jun  4 2025, 08:5
6:00) [GCC 9.4.0]
2025-09-03T09:43:59.136923Z [-] Twisted Version 25.5.0
2025-09-03T09:43:59.136936Z [-] Cowrie Version 2.6.1
2025-09-03T09:43:59.140635Z [-] Loaded output engine: jsonlog
2025-09-03T09:43:59.141871Z [twisted.scripts._twistd_unix.UnixAppLogger#info] t
wistd 25.5.0 (/home/cowrie/cowrie/cowrie-env/bin/python3.10 3.10.18) starting u
p.
2025-09-03T09:43:59.142012Z [twisted.scripts._twistd_unix.UnixAppLogger#info] r
eactor class: twisted.internet.epollreactor.EPollReactor.
2025-09-03T09:43:59.149554Z [-] CowrieSSHFactory starting on 2222
2025-09-03T09:43:59.150397Z [cowrie.ssh.factory.CowrieSSHFactory#info] Starting
 factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7f819ba29a20>
2025-09-03T09:43:59.151084Z [-] Generating new RSA keypair...
2025-09-03T09:43:59.279726Z [-] Generating new ECDSA keypair...
2025-09-03T09:43:59.281631Z [-] Generating new ed25519 keypair...
2025-09-03T09:43:59.290503Z [-] Ready to accept SSH connections
2025-09-03T09:45:32.585001Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no
 diffie-hellman-group-exchange-sha1
2025-09-03T09:45:32.585780Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no
 diffie-hellman-group-exchange-sha256
2025-09-03T09:45:32.588914Z [cowrie.ssh.factory.CowrieSSHFactory] New connectio
n: 192.168.93.200:58740 (192.168.93.31:2222) [session: 201442eee2f9]
2025-09-03T09:45:32.669716Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] co
```

```
2025-09-03T09:45:32.671054Z [HoneyPotSSHTransport,0,192.168.93.200] Connection
lost after 0.1 seconds
2025-09-03T09:48:02.394685Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no
 diffie-hellman-group-exchange-sha1
2025-09-03T09:48:02.396358Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no
 diffie-hellman-group-exchange-sha256
2025-09-03T09:48:02.398133Z [cowrie.ssh.factory.CowrieSSHFactory] New connectio
n: 192.168.93.200:38374 (192.168.93.31:2222) [session: b4ef926aab13]
2025-09-03T09:48:02.399715Z [HoneyPotSSHTransport,1,192.168.93.200] Remote SSH
version: SSH-2.0-OpenSSH_10.0p2 Debian-8
2025-09-03T09:48:02.406493Z [HoneyPotSSHTransport,1,192.168.93.200] SSH client
hassh fingerprint: eeca2460550b9ded084ecf2f70a75356
2025-09-03T09:48:02.410044Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] k
ex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2025-09-03T09:48:02.410554Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] o
utgoing: b'aes128-ctr' b'hmac-sha2-256' b'none'
2025-09-03T09:48:02.410689Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] i
ncoming: b'aes128-ctr' b'hmac-sha2-256' b'none'
2025-09-03T09:48:48.459669Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] co
nnection lost
2025-09-03T09:48:48.460886Z [HoneyPotSSHTransport,1,192.168.93.200] Connection
lost after 46.1 seconds
```

sudo cat var/log/cowrie/cowrie.json # JSON events (preferred for parsing)



ls -l var/lib/cowrie/tty/ # session transcripts



7.4 Generate Test Events (from Attacker VM)

 # Port scan(Honey Pot is Convany)

nmap -p 2222 -sV -Pn <HONEYPOT_IP>

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 2222 -sV -Pn 192.168.93.31
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 04:07 EDT
Nmap scan report for 192.168.93.31
Host is up (0.0018s latency).

PORT     STATE  SERVICE      VERSION
2222/tcp closed EtherNetIP-1
MAC Address: 08:00:27:DE:25:ED (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

 # Port scan (Honey Pot is Cowrie)

nmap -p 2222 -sV -Pn <HONEYPOT_IP>

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 2222 -sV -Pn 192.168.93.31
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 00:45 EDT
Nmap scan report for 192.168.93.31
Host is up (0.0013s latency).

PORT     STATE SERVICE VERSION
2222/tcp open  ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
MAC Address: 08:00:27:DE:25:ED (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
```

#Banner grap with netcat

nc 192.168.93.31 2222

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.93.31 2222
SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u2
```

#Try some login, they will failed but it will be logged

ssh -p 2222 root@192.168.93.31

```
┌──(kali㉿kali)-[~]
└─$ ssh -p 2222 root@192.168.93.31
The authenticity of host '[192.168.93.31]:2222 ([192.168.93.31]:2222)' can't be established.
ED25519 key fingerprint is SHA256:ju0YUj2lR0frbrWGsU7n4PA6v9wH1asmrfbtwUPTKq8.
This key is not known by any other names.
```

7.5 View & Parse Logs

 # Tail text log

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

```
(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ tail -f var/log/cowrie/cowrie.l
og
2025-09-03T09:50:56.699588Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] co
nnection lost
2025-09-03T09:50:56.699911Z [HoneyPotSSHTransport,2,192.168.93.200] Connection
lost after 105.2 seconds
2025-09-03T09:50:59.157104Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no
 diffie-hellman-group-exchange-sha1
2025-09-03T09:50:59.159188Z [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no
 diffie-hellman-group-exchange-sha256
2025-09-03T09:50:59.160698Z [cowrie.ssh.factory.CowrieSSHFactory] New connectio
n: 192.168.93.200:47094 (192.168.93.31:2222) [session: ae834d4a551b]
2025-09-03T09:50:59.164684Z [HoneyPotSSHTransport,3,192.168.93.200] Remote SSH
version: SSH-2.0-OpenSSH_10.0p2 Debian-8
2025-09-03T09:50:59.169882Z [HoneyPotSSHTransport,3,192.168.93.200] SSH client
hassh fingerprint: eeca2460550b9ded084ecf2f70a75356
2025-09-03T09:50:59.173034Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] k
ex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2025-09-03T09:50:59.173549Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] o
utgoing: b'aes128-ctr' b'hmac-sha2-256' b'none'
2025-09-03T09:50:59.174032Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] i
ncoming: b'aes128-ctr' b'hmac-sha2-256' b'none'
2025-09-03T09:52:59.226627Z [-] Timeout reached in HoneyPotSSHTransport
2025-09-03T09:52:59.228019Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] co
nnection lost
2025-09-03T09:52:59.229435Z [HoneyPotSSHTransport,3,192.168.93.200] Connection
lost after 120.1 seconds
```

 # Show last 10 SSH login attempts in JSON

jq -r 'select(.eventid=="cowrie.login.failed") | [.src_ip, .username, .password] | @tsv' var/log/cowrie/cowrie.json | tail -n 10

```
(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ jq -r &#39;select(.eventid==&qu
ot;cowrie.login.failed&quot;) | [.src_ip, .username, .password] |
[3] 8545
```

If jq isn't installed: sudo apt -y install jq

7.6 (Optional) Redirect Real Ports → Cowrie Lab Ports

Only if you understand NAT rules and your lab allows it. Not needed for this exercise.

 # Redirect inbound 22 → 2222 (requires root; persists if saved)

sudo iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-ports 22 22

```
(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ sudo iptables -t nat -A PREROUT
ING -p tcp --dport 22 -j REDIRECT --to-ports 2222
```

sudo apt install netfilter-persistent

```
(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ sudo apt install netfilter-pers
istent
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  iptables-persistent
The following NEW packages will be installed:
  netfilter-persistent
0 upgraded, 1 newly installed, 0 to remove and 78 not upgraded.
Need to get 7,268 B of archives.
After this operation, 38.9 kB of additional disk space will be used.
Get:1 http://pk.archive.ubuntu.com/ubuntu focal-updates/universe amd64 netfilte
r-persistent all 1.0.14ubuntu1 [7,268 B]
Fetched 7,268 B in 6s (1,143 B/s)
Selecting previously unselected package netfilter-persistent.
(Reading database ... 194063 files and directories currently installed.)
Preparing to unpack .../netfilter-persistent_1.0.14ubuntu1_all.deb ...
Unpacking netfilter-persistent (1.0.14ubuntu1) ...
Setting up netfilter-persistent (1.0.14ubuntu1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/netfilter-persisten
t.service → /lib/systemd/system/netfilter-persistent.service.
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for systemd (245.4-4ubuntu3.20) ...
```

sudo netfilter-persistent save

```
(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ sudo netfilter-persistent save
(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ sudo netfilter-persistent reloa
d
```

```
(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ sudo iptables -t nat -L --line-
numbers
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    REDIRECT   tcp  --  anywhere             anywhere             tcp dpt:ssh
redir ports 2222

Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
num  target     prot opt source               destination
```

sudo ss -tuln | grep :22

```
(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ sudo ss -tuln | grep :22
tcp    LISTEN  0       50             0.0.0.0:2222         0.0.0.0:*

(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ sudo ss -tuln | grep :2222
tcp    LISTEN  0       50             0.0.0.0:2222         0.0.0.0:*
```

When we start the connection with ssh ip of honeypot device than it connect with it

bin/crowie start

```
(cowrie-env) cowrie@ubuntu-VirtualBox:~/cowrie$ bin/cowrie start
Using activated Python virtual environment "/home/cowrie/cowrie/cowrie-env"

DEPRECATION: Python<3.9 is no longer supported by Cowrie.

Starting cowrie: [twistd  --umask=0022 --pidfile=var/run/cowrie.pid --logger co
wrie.python.logfile.logger cowrie ]...
/home/cowrie/cowrie/cowrie-env/lib/python3.10/site-packages/twisted/conch/ssh/t
ransport.py:110: CryptographyDeprecationWarning: TripleDES has been moved to cr
yptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed fro
m cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/home/cowrie/cowrie/cowrie-env/lib/python3.10/site-packages/twisted/conch/ssh/t
ransport.py:117: CryptographyDeprecationWarning: TripleDES has been moved to cr
yptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed fro
m cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
```

ssh -p 2222 root@192.168.93.31

```
┌──(kali㉿kali)-[~]
└─$ ssh -p 2222 root@192.168.93.31
root@192.168.93.31'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@ubuntu:~#
```

8) Honeytokens (Super Lightweight Deception)

*A **honeytoken** is a fake credential or resource that alerts when used.*

8.1 Simple DIY Token (Local Web Log)

1. *Create a bogus URL and log any request to it.*

```
# On Honeypot VM
mkdir -p ~/token && cd ~/token
cat > token.py <<'PY'
from http.server import HTTPServer, BaseHTTPRequestHandler
import time

class H(BaseHTTPRequestHandler):
   def do_GET(self):
      print(time.strftime('%F %T'), 'TOKEN TOUCHED FROM', self.client_addres
```

```
s, 'PATH', self.path)
        self.send_response(200)
        self.end_headers()
        self.wfile.write(b"OK")

HTTPServer(('0.0.0.0', 8088), H).serve_forever()
PY
python3 token.py
```

2. *Share the fake URL http://<HONEYPOT_IP>:8088/secret-key* ***only inside the lab****. Any hit prints to the console.*

8.2 What to Observe

- *Source IP and timestamp*
- *URI path that was touched (e.g., /secret-key)*
- *Correlate with Nmap/SSH probes seen earlier*

9) Collecting & Centralizing Logs (Mini-Stack)

For this lab, you'll triage logs locally. If you want a light central view for multiple students, use rsyslog.

9.1 Enable rsyslog Client (Honeypot VM)

```
sudo sed -i 's/^#*\$ModLoad imtcp/\$ModLoad imtcp/' /etc/rsyslog.conf
sudo sed -i 's/^#*\$InputTCPServerRun.*/\$InputTCPServerRun 514/' /etc/rsyslog.conf
sudo systemctl restart rsyslog
```

9.2 Send Custom Logs to Syslog (Example)

```
# OpenCanary file → syslog (quick & dirty)
sudo tail -F /home/canary/open_canary.log | logger -t opencanary &

# Cowrie json → syslog (parsed usernames)
jq -r 'select(.eventid=="cowrie.login.failed") | "SSH_FAIL src=" + .src_ip + " user=" + .username' var/log/cowrie/cowrie.json | logger -t cowrie &
```

10) Cleanup / Reset

```
# OpenCanary
sudo -iu canary bash -lc 'open-canaryd --stop || true'
```

```
# Cowrie (from cowrie directory)
bin/cowrie stop || true

# Kill token script (Ctrl+C), or:
pkill -f token.py || true

# Optional: Remove iptables rule
sudo iptables -t nat -D PREROUTING -p tcp --dport 22 -j REDIRECT --to-ports 2
222 || true
sudo netfilter-persistent save
```

11) Troubleshooting

- **Port already in use:** Change the service port in config or stop the process holding it (sudo lsof -i :80).
- **No logs appear:**
  - Is the service started? (open-canaryd --status or bin/cowrie status)
  - Are you on the correct IP/port? ip addr, ss -lnt
  - Try generating local traffic: curl http://127.0.0.1/
- **Permission errors:** Use the correct user (sudo -iu canary or sudo -iu cowrie).
- **Firewall/NAT issues:** Validate lab network and use ping/nmap between VMs.

13) Extensions (Optional, Instructor-Only)

- Add more OpenCanary services (SMB, MySQL, Redis) and compare attack volumes.
- Forward logs to a SIEM (Elastic, Wazuh, or Splunk Free) and build a dashboard.
- Write detection rules: e.g., alert on ≥5 SSH failures from one IP in 2 minutes.
- Compare deception depth: low-interaction (OpenCanary) vs. medium (Cowrie).

14) Reference Commands Quick Sheet

```
# OpenCanary lifecycle
open-canaryd --copyconfig
open-canaryd --start
open-canaryd --status
open-canaryd --stop
```

Cowrie lifecycle (inside repo)
bin/cowrie start
bin/cowrie status
bin/cowrie stop

Log viewing
tail -f /home/canary/open_canary.log
tail -f var/log/cowrie/cowrie.log
jq '.' var/log/cowrie/cowrie.json | head

Test traffic
nmap -sS -sV -Pn <HONEYPOT_IP>
curl -i http://<HONEYPOT_IP>/
ssh -p 2222 root@<HONEYPOT_IP>

End of Manual