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

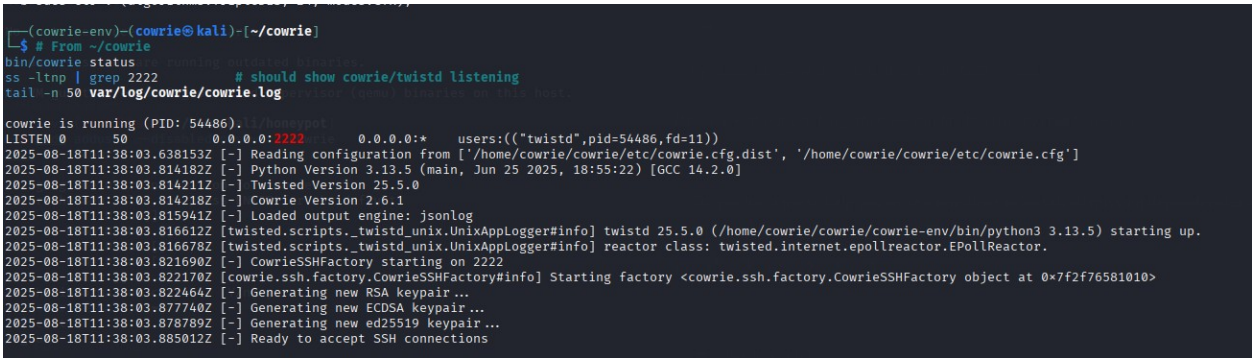
2.Steps for set up the honeypot :

2.1 Add user

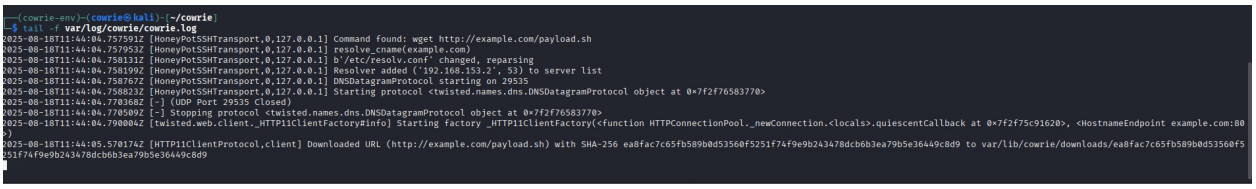
At first I have added another user on my kali linux machine and then I have cloned the git of cowrie and installed requirement package for the projet

```
┌──(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:
Sorry, try again.
[sudo] password for cowrie:
Sorry, try again.
[sudo] password for cowrie:
sudo: 2 incorrect password attempts

┌──(cowrie㉿kali)-[/home/kali]
└─$ cd ~

┌──(cowrie㉿kali)-[~]
└─$ 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)-[~]
└─$ 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 :

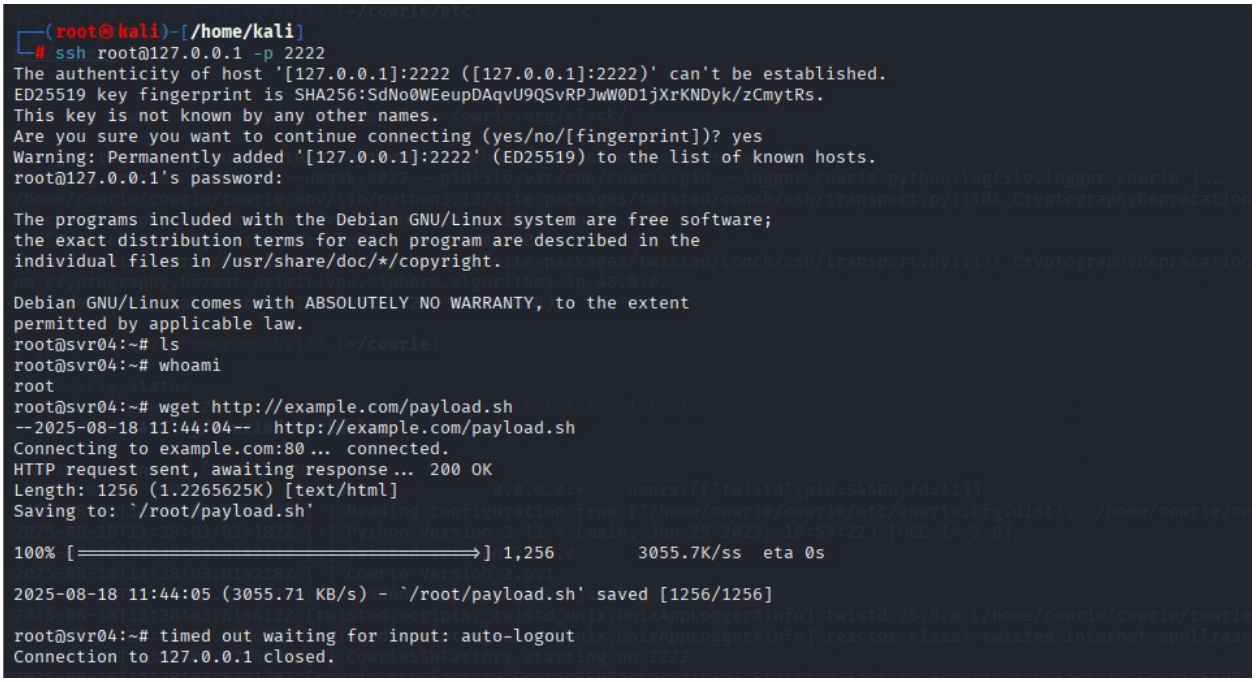


2.3 Check logs:



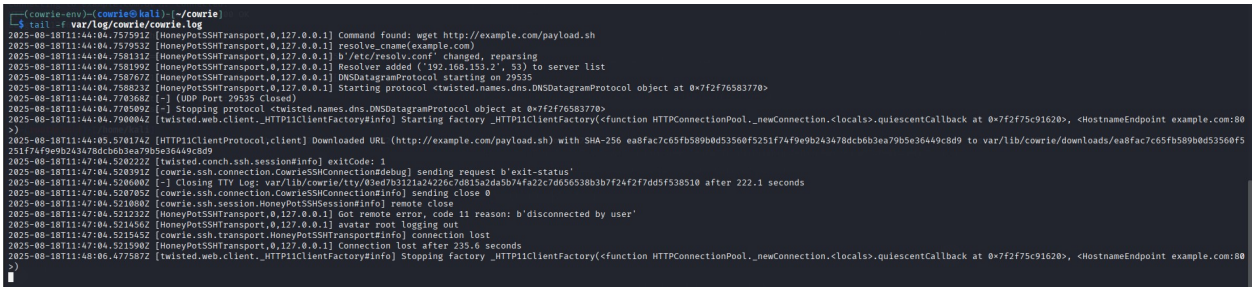
2.4 Test the Honeypot

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



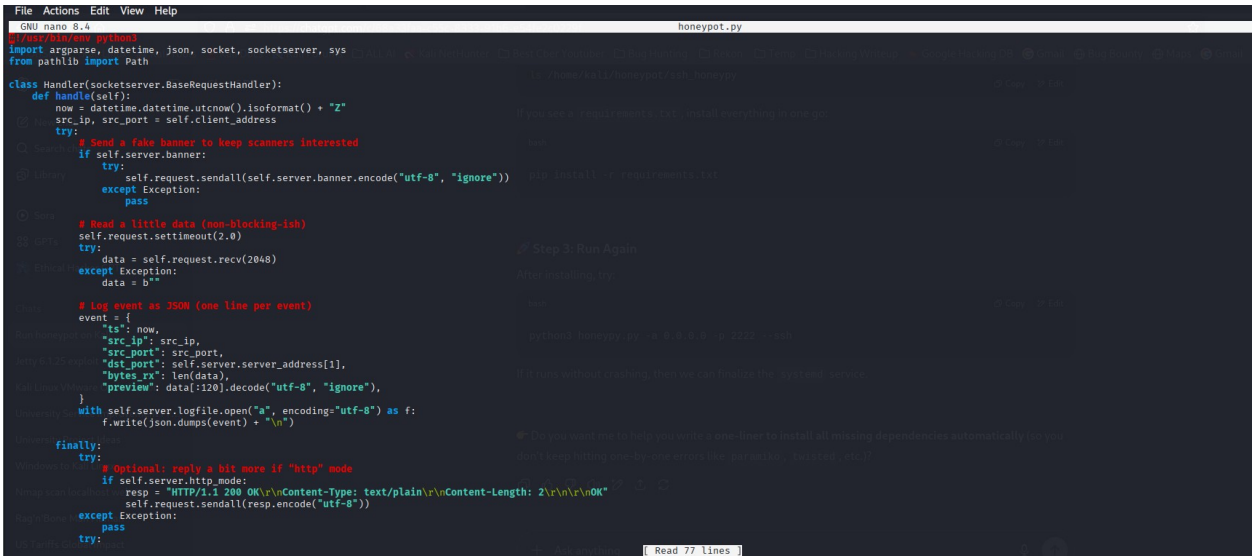
2.5 Capture & Analyze Attacks

Analyze the live capture of honeypot

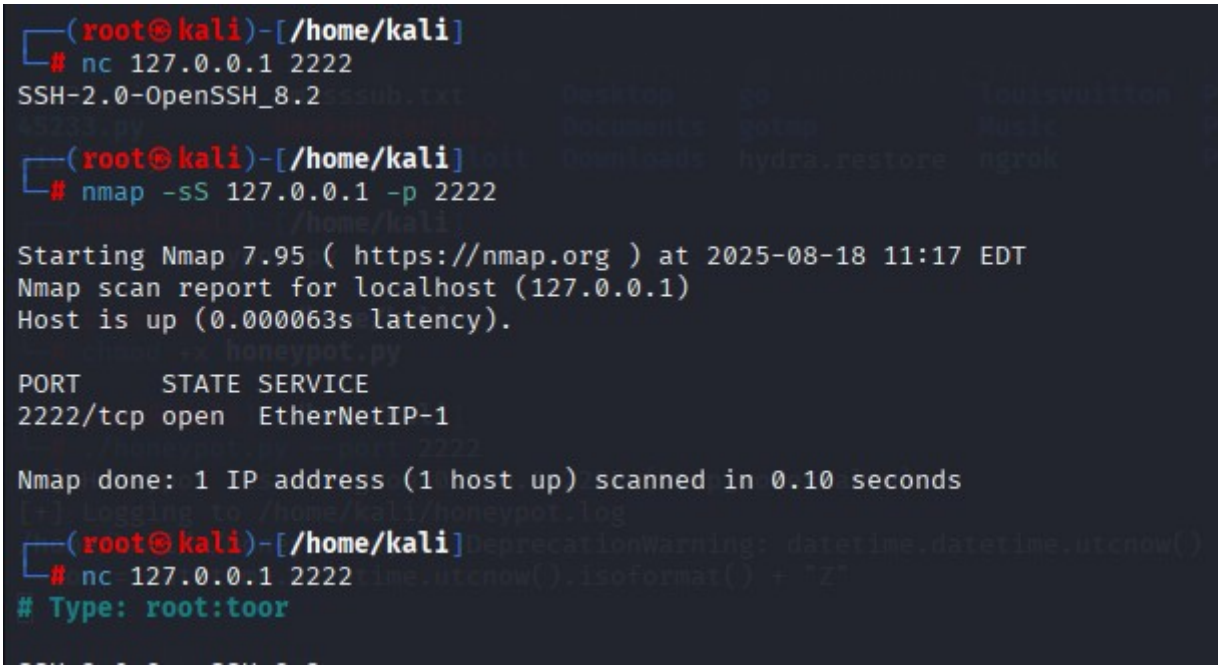


3. Custom made Honeypot

3.1 writing Code for honeypot and execute it on kali linux



3.2 Scan nmap on the target port :



3.3: Analyze the logs :