Cowrie SSH Honeypot Project

Overview

This project demonstrates the deployment of a Cowrie SSH honeypot on Ubuntu running in VMware. The honeypot was designed to simulate an exposed SSH server and capture attacker activity, including brute-force login attempts and command executions. The goal was to analyze attacker behavior, credentials used, and generate SOC-style reports to better understand real-world threats.

⚙️ Setup

Platform: VMware Workstation with Ubuntu VM

Honeypot Tool: Cowrie SSH Honeypot

Configuration:

Cowrie is installed and configured to emulate an SSH server

Default services are exposed to attract automated scanners and bots

Logging is enabled to capture attacker commands and failed logins

---

🎯 Objectives

Deploy a controlled honeypot to attract brute-force attempts

Capture attacker behavior, including login attempts and commands

Analyze credential patterns used by attackers

Generate SOC-style reports on observed malicious activity

🔍 Methodology

Deployment: Installed Cowrie on an Ubuntu VM and configured it to accept SSH connections.

Attack Simulation: Exposed the VM to simulate internet-facing access.

Data Collection: Cowrie logged all incoming SSH connections, login attempts, and commands.

Analysis: Parsed log files to extract:

Common usernames and passwords attempted

Frequency of brute-force login attempts

Attacker interaction with the honeypot shell

📊 Results

Total SSH brute-force attempts recorded: 220+

Failed login events collected: 200+

Top credentials attempted:

root/123456

admin/password

test/test

Patterns observed:

Automated scripts attempting weak/default credentials

Attackers primarily targeting root/admin accounts

These findings demonstrate the constant nature of brute-force attacks on exposed SSH endpoints and emphasize the importance of strong authentication controls.

VM & Environment Setup

sudo apt update && sudo apt upgrade -y

sudo apt install git python3 python3-venv python3-pip libssl-dev libffi-dev build-essential virtualenv sshpass -y

Cowrie Installation

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

cd cowrie

python3 -m venv cowrie-env

source cowrie-env/bin/activate

pip install --upgrade pip

pip install -r requirements.txt

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

nano etc/cowrie.cfg # set listen_port = 2222

Run Cowrie

bin/cowrie start

bin/cowrie stop

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

Test Login (fake SSH session)

ssh root@localhost -p 2222

Simulated Attack Loop (Brute Force) - Basic

```
for u in root admin test user; do
  for p in 123456 password admin qwerty letmein; do
    sshpass -p "$p" ssh -o StrictHostKeyChecking=no -p 2222 "$u"@localhost "exit"
2>/dev/null || true
  done
done
```

Simulated Attack Loop (Brute Force)

```
for u in root admin test user dev; do
  for p in 123456 password admin qwerty letmein toor dragon shadow iloveyou default; do
    sshpass -p "$p" ssh -o StrictHostKeyChecking=no -p 2222 "$u"@localhost "exit" 2>/dev/null || true
  done
done
```

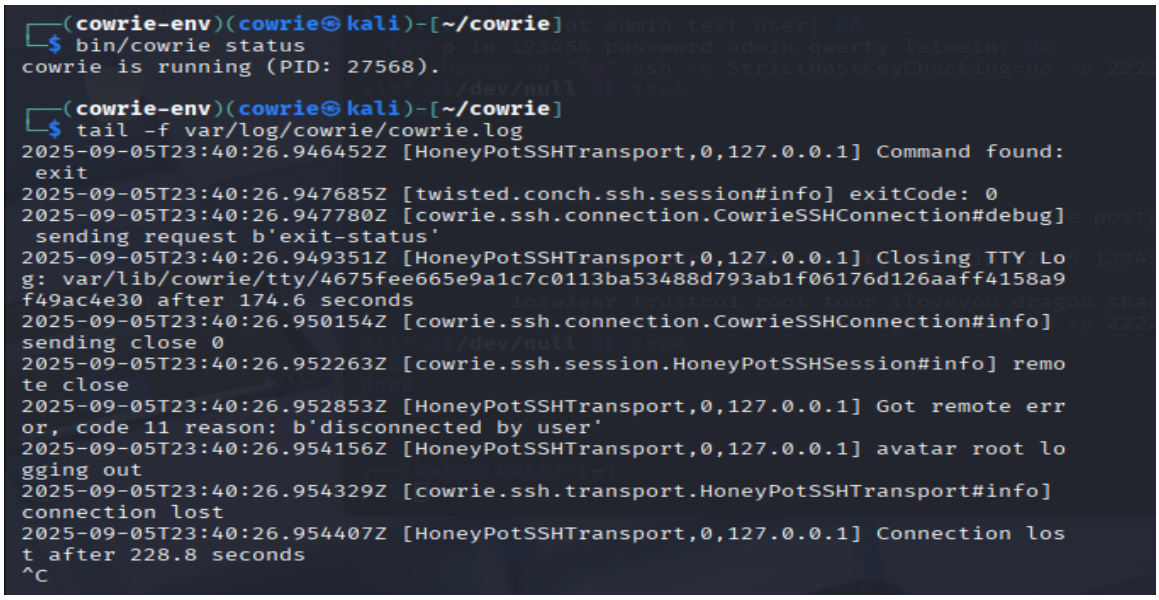
View Logs

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

ls var/lib/cowrie/tty/
```

Save Project for GitHub

```
mkdir -p ~/cowrie_honeypot_project/{logs,screenshots,docs}

cp ~/cowrie/var/log/cowrie/cowrie.json ~/cowrie_honeypot_project/logs/cowrie.json

cp -r ~/cowrie/var/lib/cowrie/tty ~/cowrie_honeypot_project/logs/tty_logs

head -n 100 ~/cowrie/var/log/cowrie/cowrie.json > ~/cowrie_honeypot_project/logs/cowrie_sample.json

nano ~/cowrie_honeypot_project/docs/setup_instructions.md

cd ~

tar -czvf cowrie_honeypot_project.tar.gz cowrie_honeypot_project
```

SCREENSHOTS



```
┌──(cowrie-env)(cowrie㉿kali)-[~/cowrie]
└─$ tail -f var/log/cowrie/cowrie.json
{"eventid":"cowrie.client.var","name":"LANG","value":"en_US.UTF-8","message":
"request_env: LANG=en_US.UTF-8","sensor":"kali","timestamp":"2025-09-05T23:37
:32.335633Z","src_ip":"127.0.0.1","session":"fcc6383c8c62"}
{"eventid":"cowrie.session.params","arch":"linux-x64-lsb","message":[],"senso
r":"kali","timestamp":"2025-09-05T23:37:32.338094Z","src_ip":"127.0.0.1","ses
sion":"fcc6383c8c62"}
{"eventid":"cowrie.command.input","input":"ls","message":"CMD: ls","sensor":"
kali","timestamp":"2025-09-05T23:39:48.544752Z","src_ip":"127.0.0.1","session
":"fcc6383c8c62"}
{"eventid":"cowrie.command.input","input":"pwd","message":"CMD: pwd","sensor"
:"kali","timestamp":"2025-09-05T23:39:54.742747Z","src_ip":"127.0.0.1","sessi
on":"fcc6383c8c62"}
{"eventid":"cowrie.command.input","input":"whoami","message":"CMD: whoami","s
ensor":"kali","timestamp":"2025-09-05T23:39:59.090116Z","src_ip":"127.0.0.1",
"session":"fcc6383c8c62"}
{"eventid":"cowrie.command.input","input":"uname -a","message":"CMD: uname -a
","sensor":"kali","timestamp":"2025-09-05T23:40:07.931489Z","src_ip":"127.0.0
.1","session":"fcc6383c8c62"}
{"eventid":"cowrie.command.input","input":"cat /etc/passwd","message":"CMD: c
at /etc/passwd","sensor":"kali","timestamp":"2025-09-05T23:40:14.773452Z","sr
c_ip":"127.0.0.1","session":"fcc6383c8c62"}
{"eventid":"cowrie.command.input","input":"exit","message":"CMD: exit","senso
r":"kali","timestamp":"2025-09-05T23:40:26.945911Z","src_ip":"127.0.0.1","ses
sion":"fcc6383c8c62"}
{"eventid":"cowrie.log.closed","ttylog":"var/lib/cowrie/tty/4675fee665e9a1c7c
0113ba53488d793ab1f06176d126aaff4158a9f49ac4e30","size":1414,"shasum":"4675fe
e665e9a1c7c0113ba53488d793ab1f06176d126aaff4158a9f49ac4e30","duplicate":false
,"duration":"174.6","message":"Closing TTY Log: var/lib/cowrie/tty/4675fee665
e9a1c7c0113ba53488d793ab1f06176d126aaff4158a9f49ac4e30 after 174.6 seconds","
sensor":"kali","timestamp":"2025-09-05T23:40:26.949351Z","src_ip":"127.0.0.1"
,"session":"fcc6383c8c62"}
{"eventid":"cowrie.session.closed","duration":"228.8","message":"Connection l
ost after 228.8 seconds","sensor":"kali","timestamp":"2025-09-05T23:40:26.954
407Z","src_ip":"127.0.0.1","session":"fcc6383c8c62"}
{"eventid":"cowrie.session.connect","src_ip":"127.0.0.1","src_port":37814,"ds
t_ip":"127.0.0.1","dst_port":2222,"session":"534c9871c0d3","protocol":"ssh","
message":"New connection: 127.0.0.1:37814 (127.0.0.1:2222) [session: 534c9871
c0d3]","sensor":"kali","timestamp":"2025-09-05T23:45:57.074582Z"}
{"eventid":"cowrie.client.version","version":"SSH-2.0-OpenSSH_10.0p2 Debian-8
","message":"Remote SSH version: SSH-2.0-OpenSSH_10.0p2 Debian-8","sensor":"k
ali","timestamp":"2025-09-05T23:45:57.089409Z","src_ip":"127.0.0.1","session"
:"534c9871c0d3"}
{"eventid":"cowrie.client.kex","hassh":"eeca2460550b9ded084ecf2f70a75356","ha
sshAlgorithms":"mlkem768x25519-sha256,sntrup761x25519-sha512,sntrup761x25519-
sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-n
istp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-s
ha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hell
man-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com;chacha20-poly1305@
openssh.com,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-ctr,aes192-c
```

```
{"eventid":"cowrie.client.kex","hassh":"eeca2460550b9ded084ecf2f70a75356","ha
sshAlgorithms":"mlkem768×25519-sha256,sntrup761×25519-sha512,sntrup761×25519-
sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-n
istp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-s
ha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hell
man-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com;chacha20-poly1305@
openssh.com,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-ctr,aes192-c
tr,aes256-ctr;umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-
etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-
64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1;non
e,zlib@openssh.com","kexAlgs":["mlkem768×25519-sha256","sntrup761×25519-sha51
2","sntrup761×25519-sha512@openssh.com","curve25519-sha256","curve25519-sha25
6@libssh.org","ecdh-sha2-nistp256","ecdh-sha2-nistp384","ecdh-sha2-nistp521",
"diffie-hellman-group-exchange-sha256","diffie-hellman-group16-sha512","diffi
e-hellman-group18-sha512","diffie-hellman-group14-sha256","ext-info-c","kex-s
trict-c-v00@openssh.com"],"keyAlgs":["ssh-ed25519-cert-v01@openssh.com","ecds
a-sha2-nistp256-cert-v01@openssh.com","ecdsa-sha2-nistp384-cert-v01@openssh.c
om","ecdsa-sha2-nistp521-cert-v01@openssh.com","sk-ssh-ed25519-cert-v01@opens
sh.com","sk-ecdsa-sha2-nistp256-cert-v01@openssh.com","rsa-sha2-512-cert-v01@
openssh.com","rsa-sha2-256-cert-v01@openssh.com","ssh-ed25519","ecdsa-sha2-ni
stp256","ecdsa-sha2-nistp384","ecdsa-sha2-nistp521","sk-ssh-ed25519@openssh.c
om","sk-ecdsa-sha2-nistp256@openssh.com","rsa-sha2-512","rsa-sha2-256"],"encC
S":["chacha20-poly1305@openssh.com","aes128-gcm@openssh.com","aes256-gcm@open
ssh.com","aes128-ctr","aes192-ctr","aes256-ctr"],"macCS":["umac-64-etm@openss
h.com","umac-128-etm@openssh.com","hmac-sha2-256-etm@openssh.com","hmac-sha2-
512-etm@openssh.com","hmac-sha1-etm@openssh.com","umac-64@openssh.com","umac-
128@openssh.com","hmac-sha2-256","hmac-sha2-512","hmac-sha1"],"compCS":["none
","zlib@openssh.com"],"langCS":[""],"message":"SSH client hassh fingerprint:
eeca2460550b9ded084ecf2f70a75356","sensor":"kali","timestamp":"2025-09-05T23:
48:28.912538Z","src_ip":"127.0.0.1","session":"24af3ae912e8"}
{"eventid":"cowrie.login.failed","username":"root","password":"123456","messa
ge":"login attempt [root/123456] failed","sensor":"kali","timestamp":"2025-09
-05T23:48:28.976393Z","src_ip":"127.0.0.1","session":"24af3ae912e8"}
{"eventid":"cowrie.session.closed","duration":"1.1","message":"Connection los
t after 1.1 seconds","sensor":"kali","timestamp":"2025-09-05T23:48:29.983139Z
","src_ip":"127.0.0.1","session":"24af3ae912e8"}
{"eventid":"cowrie.session.connect","src_ip":"127.0.0.1","src_port":54498,"ds
t_ip":"127.0.0.1","dst_port":2222,"session":"c8ba001786e4","protocol":"ssh","
message":"New connection: 127.0.0.1:54498 (127.0.0.1:2222) [session: c8ba0017
86e4]","sensor":"kali","timestamp":"2025-09-05T23:48:30.037817Z"}
{"eventid":"cowrie.client.version","version":"SSH-2.0-OpenSSH_10.0p2 Debian-8
","message":"Remote SSH version: SSH-2.0-OpenSSH_10.0p2 Debian-8","sensor":"k
ali","timestamp":"2025-09-05T23:48:30.051590Z","src_ip":"127.0.0.1","session"
:"c8ba001786e4"}
{"eventid":"cowrie.client.kex","hassh":"eeca2460550b9ded084ecf2f70a75356","ha
sshAlgorithms":"mlkem768×25519-sha256,sntrup761×25519-sha512,sntrup761×25519-
sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-n
istp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-s
ha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hell
man-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com;chacha20-poly1305@
openssh.com,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-ctr,aes192-c
```

```
{"eventid":"cowrie.client.kex","hassh":"eeca2460550b9ded084ecf2f70a75356","ha
sshAlgorithms":"mlkem768×25519-sha256,sntrup761×25519-sha512,sntrup761×25519-
sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-n
istp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-s
ha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hell
man-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com;chacha20-poly1305@
openssh.com,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-ctr,aes192-c
tr,aes256-ctr;umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-
etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-
64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1;non
e,zlib@openssh.com","kexAlgs":["mlkem768×25519-sha256","sntrup761×25519-sha51
2","sntrup761×25519-sha512@openssh.com","curve25519-sha256","curve25519-sha25
6@libssh.org","ecdh-sha2-nistp256","ecdh-sha2-nistp384","ecdh-sha2-nistp521",
"diffie-hellman-group-exchange-sha256","diffie-hellman-group16-sha512","diffi
e-hellman-group18-sha512","diffie-hellman-group14-sha256","ext-info-c","kex-s
trict-c-v00@openssh.com"],"keyAlgs":["ssh-ed25519-cert-v01@openssh.com","ecds
a-sha2-nistp256-cert-v01@openssh.com","ecdsa-sha2-nistp384-cert-v01@openssh.c
om","ecdsa-sha2-nistp521-cert-v01@openssh.com","sk-ssh-ed25519-cert-v01@opens
sh.com","sk-ecdsa-sha2-nistp256-cert-v01@openssh.com","rsa-sha2-512-cert-v01@
openssh.com","rsa-sha2-256-cert-v01@openssh.com","ssh-ed25519","ecdsa-sha2-ni
stp256","ecdsa-sha2-nistp384","ecdsa-sha2-nistp521","sk-ssh-ed25519@openssh.c
om","sk-ecdsa-sha2-nistp256@openssh.com","rsa-sha2-512","rsa-sha2-256"],"encC
S":["chacha20-poly1305@openssh.com","aes128-gcm@openssh.com","aes256-gcm@open
ssh.com","aes128-ctr","aes192-ctr","aes256-ctr"],"macCS":["umac-64-etm@openss
h.com","umac-128-etm@openssh.com","hmac-sha2-256-etm@openssh.com","hmac-sha2-
512-etm@openssh.com","hmac-sha1-etm@openssh.com","umac-64@openssh.com","umac-
128@openssh.com","hmac-sha2-256","hmac-sha2-512","hmac-sha1"],"compCS":["none
","zlib@openssh.com"],"langCS":[""],"message":"SSH client hassh fingerprint:
eeca2460550b9ded084ecf2f70a75356","sensor":"kali","timestamp":"2025-09-05T23:
48:36.911265Z","src_ip":"127.0.0.1","session":"69956072d6da"}
{"eventid":"cowrie.login.failed","username":"test","password":"123456","messa
ge":"login attempt [test/123456] failed","sensor":"kali","timestamp":"2025-09
-05T23:48:36.974284Z","src_ip":"127.0.0.1","session":"69956072d6da"}
{"eventid":"cowrie.session.closed","duration":"1.1","message":"Connection los
t after 1.1 seconds","sensor":"kali","timestamp":"2025-09-05T23:48:37.987020Z
","src_ip":"127.0.0.1","session":"69956072d6da"}
{"eventid":"cowrie.session.connect","src_ip":"127.0.0.1","src_port":55216,"ds
t_ip":"127.0.0.1","dst_port":2222,"session":"d6dec814b0c6","protocol":"ssh","
message":"New connection: 127.0.0.1:55216 (127.0.0.1:2222) [session: d6dec814
b0c6]","sensor":"kali","timestamp":"2025-09-05T23:48:38.038378Z"}
{"eventid":"cowrie.client.version","version":"SSH-2.0-OpenSSH_10.0p2 Debian-8
","message":"Remote SSH version: SSH-2.0-OpenSSH_10.0p2 Debian-8","sensor":"k
ali","timestamp":"2025-09-05T23:48:38.054073Z","src_ip":"127.0.0.1","session"
:"d6dec814b0c6"}
```

```
┌──(cowrie-env)(cowrie㉿kali)-[~/cowrie]
└─$ tail -f var/log/cowrie/cowrie.json | tee ~/cowrie_honeypot_project/logs/cowrie_session.log
{"eventid":"cowrie.session.connect","src_ip":"127.0.0.1","src_port":55786,"dst_ip":"127.0.0.1","dst_port":2222,"session":"3eee54064c94","protocol":"ssh","message":"New connection: 127.0.0.1:55786 (127.0.0.1:2222) [session: 3eee54064c94]
","sensor":"kali","timestamp":"2025-09-06T00:43:48.774205Z"}
{"eventid":"cowrie.client.version","version":"SSH-2.0-OpenSSH_10.0p2 Debian-8","message":"Remote SSH version: SSH-2.0-OpenSSH_10.0p2 Debian-8","sensor":"kali","timestamp":"2025-09-06T00:43:48.793883Z","src_ip":"127.0.0.1","session":"3ee
e54064c94"}
{"eventid":"cowrie.client.kex","hassh":"eeca2460550b9ded084ecf2f70a75356","hasshAlgorithms":"mlkem768×25519-sha256,sntrup761×25519-sha512,sntrup761×25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp2
56,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com;chacha20-poly1305@openssh.co
m,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr;umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,
umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1;none,zlib@openssh.com","kexAlgs":["mlkem768×25519-sha256","sntrup761×25519-sha512","sntrup761×25519-sha512@openssh.com","curve25519-sha256","curve25519-sha256@libssh.org","ecdh-
sha2-nistp256","ecdh-sha2-nistp384","ecdh-sha2-nistp521","diffie-hellman-group-exchange-sha256","diffie-hellman-group16-sha512","diffie-hellman-group18-sha512","diffie-hellman-group14-sha256","ext-info-c","kex-strict-c-v00@openssh.com"]
,"keyAlgs":["ssh-ed25519-cert-v01@openssh.com","ecdsa-sha2-nistp256-cert-v01@openssh.com","ecdsa-sha2-nistp384-cert-v01@openssh.com","ecdsa-sha2-nistp521-cert-v01@openssh.com","sk-ssh-ed25519-cert-v01@openssh.com","sk-ecdsa-sha2-nistp25
6-cert-v01@openssh.com","rsa-sha2-512-cert-v01@openssh.com","rsa-sha2-256-cert-v01@openssh.com","ssh-ed25519","ecdsa-sha2-nistp256","ecdsa-sha2-nistp384","ecdsa-sha2-nistp521","sk-ssh-ed25519@openssh.com","sk-ecdsa-sha2-nistp256@openssh
.com","rsa-sha2-512","rsa-sha2-256"],"encCS":["chacha20-poly1305@openssh.com","aes128-gcm@openssh.com","aes256-gcm@openssh.com","aes128-ctr","aes192-ctr","aes256-ctr"],"macCS":["umac-64-etm@openssh.com","umac-128-etm@openssh.com","hmac-
sha2-256-etm@openssh.com","hmac-sha2-512-etm@openssh.com","hmac-sha1-etm@openssh.com","umac-64@openssh.com","umac-128@openssh.com","hmac-sha2-256","hmac-sha2-512","hmac-sha1"],"compCS":["none","zlib@openssh.com"],"langCS":[""],"message"
:"SSH client hassh fingerprint: eeca2460550b9ded084ecf2f70a75356","sensor":"kali","timestamp":"2025-09-06T00:43:48.805681Z","src_ip":"127.0.0.1","session":"3eee54064c94"}
{"eventid":"cowrie.login.failed","username":"dev","password":"shadow","message":"login attempt [dev/shadow] failed","sensor":"kali","timestamp":"2025-09-06T00:43:48.867116Z","src_ip":"127.0.0.1","session":"3eee54064c94"}
{"eventid":"cowrie.session.closed","duration":"1.1","message":"Connection lost after 1.1 seconds","sensor":"kali","timestamp":"2025-09-06T00:43:49.874478Z","src_ip":"127.0.0.1","session":"3eee54064c94"}
{"eventid":"cowrie.session.connect","src_ip":"127.0.0.1","src_port":55800,"dst_ip":"127.0.0.1","dst_port":2222,"session":"30a2c2a406cc","protocol":"ssh","message":"New connection: 127.0.0.1:55800 (127.0.0.1:2222) [session: 30a2c2a406cc]
","sensor":"kali","timestamp":"2025-09-06T00:43:49.944215Z"}
{"eventid":"cowrie.client.version","version":"SSH-2.0-OpenSSH_10.0p2 Debian-8","message":"Remote SSH version: SSH-2.0-OpenSSH_10.0p2 Debian-8","sensor":"kali","timestamp":"2025-09-06T00:43:49.959057Z","src_ip":"127.0.0.1","session":"30a
2c2a406cc"}
{"eventid":"cowrie.client.kex","hassh":"eeca2460550b9ded084ecf2f70a75356","hasshAlgorithms":"mlkem768×25519-sha256,sntrup761×25519-sha512,sntrup761×25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp2
56,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com;chacha20-poly1305@openssh.co
m,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr;umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,
umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1;none,zlib@openssh.com","kexAlgs":["mlkem768×25519-sha256","sntrup761×25519-sha512","sntrup761×25519-sha512@openssh.com","curve25519-sha256","curve25519-sha256@libssh.org","ecdh-
sha2-nistp256","ecdh-sha2-nistp384","ecdh-sha2-nistp521","diffie-hellman-group-exchange-sha256","diffie-hellman-group16-sha512","diffie-hellman-group18-sha512","diffie-hellman-group14-sha256","ext-info-c","kex-strict-c-v00@openssh.com"]
,"keyAlgs":["ssh-ed25519-cert-v01@openssh.com","ecdsa-sha2-nistp256-cert-v01@openssh.com","ecdsa-sha2-nistp384-cert-v01@openssh.com","ecdsa-sha2-nistp521-cert-v01@openssh.com","sk-ssh-ed25519-cert-v01@openssh.com","sk-ecdsa-sha2-nistp25
6-cert-v01@openssh.com","rsa-sha2-512-cert-v01@openssh.com","rsa-sha2-256-cert-v01@openssh.com","ssh-ed25519","ecdsa-sha2-nistp256","ecdsa-sha2-nistp384","ecdsa-sha2-nistp521","sk-ssh-ed25519@openssh.com","sk-ecdsa-sha2-nistp256@openssh
.com","rsa-sha2-512","rsa-sha2-256"],"encCS":["chacha20-poly1305@openssh.com","aes128-gcm@openssh.com","aes256-gcm@openssh.com","aes128-ctr","aes192-ctr","aes256-ctr"],"macCS":["umac-64-etm@openssh.com","umac-128-etm@openssh.com","hmac-
sha2-256-etm@openssh.com","hmac-sha2-512-etm@openssh.com","hmac-sha1-etm@openssh.com","umac-64@openssh.com","umac-128@openssh.com","hmac-sha2-256","hmac-sha2-512","hmac-sha1"],"compCS":["none","zlib@openssh.com"],"langCS":[""],"message"
:"SSH client hassh fingerprint: eeca2460550b9ded084ecf2f70a75356","sensor":"kali","timestamp":"2025-09-06T00:43:49.969586Z","src_ip":"127.0.0.1","session":"30a2c2a406cc"}
{"eventid":"cowrie.login.failed","username":"dev","password":"default","message":"login attempt [dev/default] failed","sensor":"kali","timestamp":"2025-09-06T00:43:50.031386Z","src_ip":"127.0.0.1","session":"30a2c2a406cc"}
{"eventid":"cowrie.session.closed","duration":"1.1","message":"Connection lost after 1.1 seconds","sensor":"kali","timestamp":"2025-09-06T00:43:51.039461Z","src_ip":"127.0.0.1","session":"30a2c2a406cc"}
^C
```