Simulated Multi-Attacker SSH Honeypot Lab Using Cowrie

Abstract

This report documents the complete deployment, configuration, attack simulation, and forensic analysis of a Cowrie SSH honeypot. The objective of this project is to emulate a vulnerable SSH service, capture attacker behavior, and analyze real-world attack patterns. The honeypot was subjected to brute-force attacks from multiple simulated attacker IPs using Hydra. Captured logs were then analyzed to identify authentication attempts, successful compromises, attacker commands, session behavior, and IP-based trends. This report is structured as a professional SOC/Blue Team portfolio artifact and is suitable for resume and GitHub showcase purposes.

1. Introduction

Honeypots are security mechanisms designed to detect, deflect, or study attempts at unauthorized access. Cowrie is a medium-interaction SSH and Telnet honeypot that emulates a real Linux environment. It captures login attempts, command execution, and session metadata. In this project, Cowrie was deployed on a Kali Linux VM and subjected to multiple brute-force attacks originating from simulated network namespaces acting as different attackers.

<u>Objectives:</u>

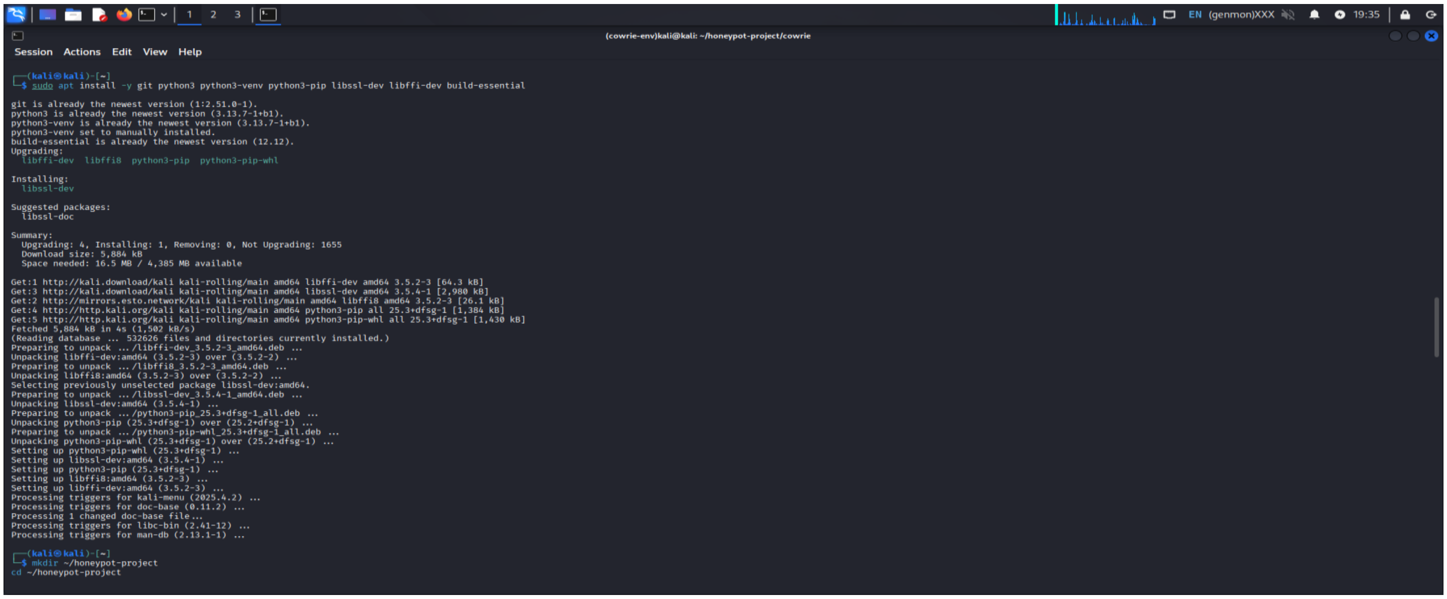
- Deploy Cowrie SSH honeypot
- Simulate brute-force attacks using Hydra
- Capture logs from multiple source IPs
- Analyze authentication patterns
- Analyze attacker behavior
- Extract indicators of compromise (IOCs)

2. Environment Setup

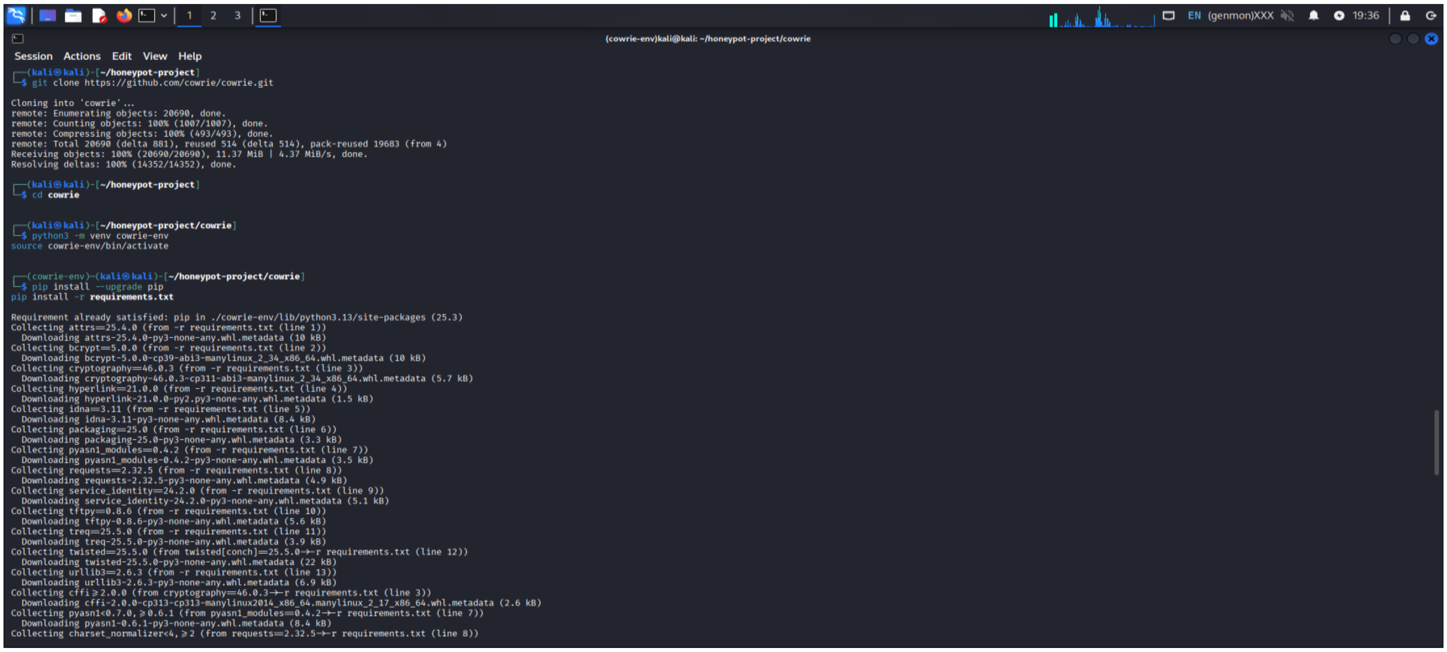
<u>Operating System:</u> Kali Linux
Honeypot: Cowrie
Attack Tool: Hydra
Logging Format: JSON
Network Simulation: Linux network namespaces

<u>Installation Steps:</u>

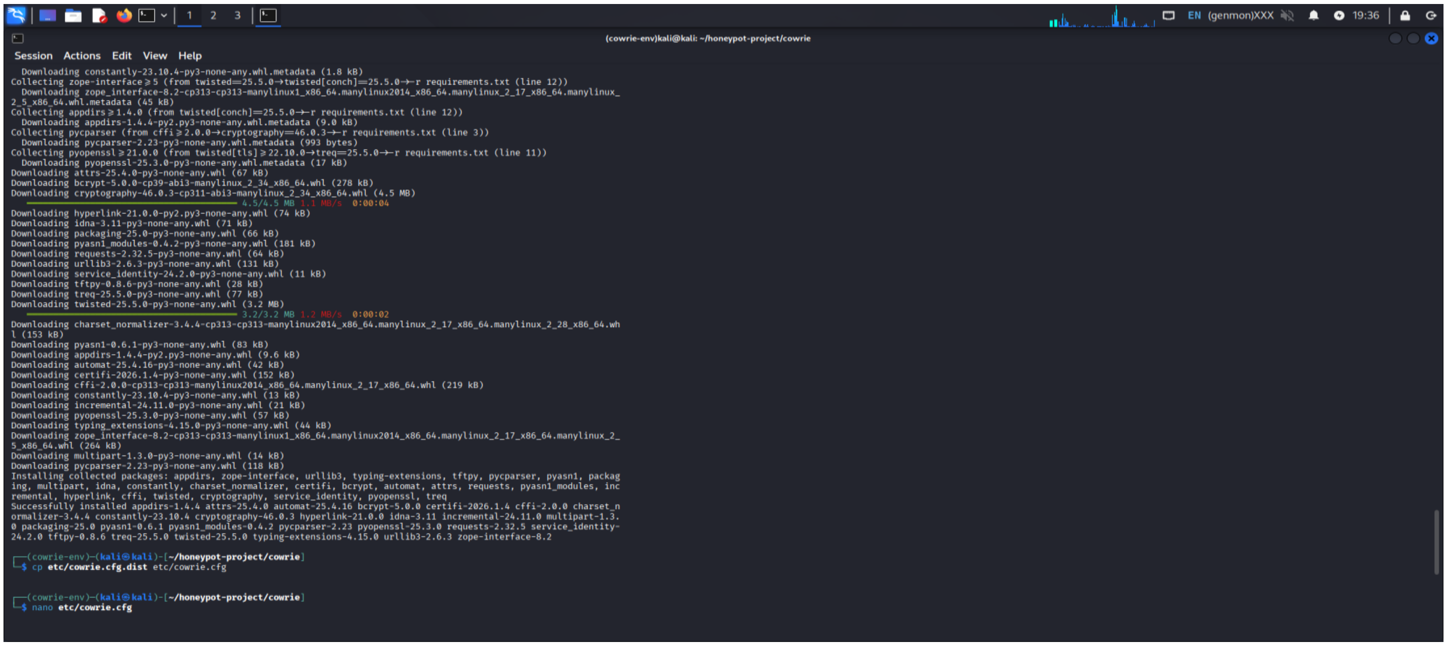
- Python virtual environment creation
- Cowrie dependency installation
- Cowrie configuration
- SSH port forwarding setup


1
2
3
EN (genmon)XXX
19:35
(cowrie-env)kali@kali: ~/honeypot-project/cowrie
Session Actions Edit View Help

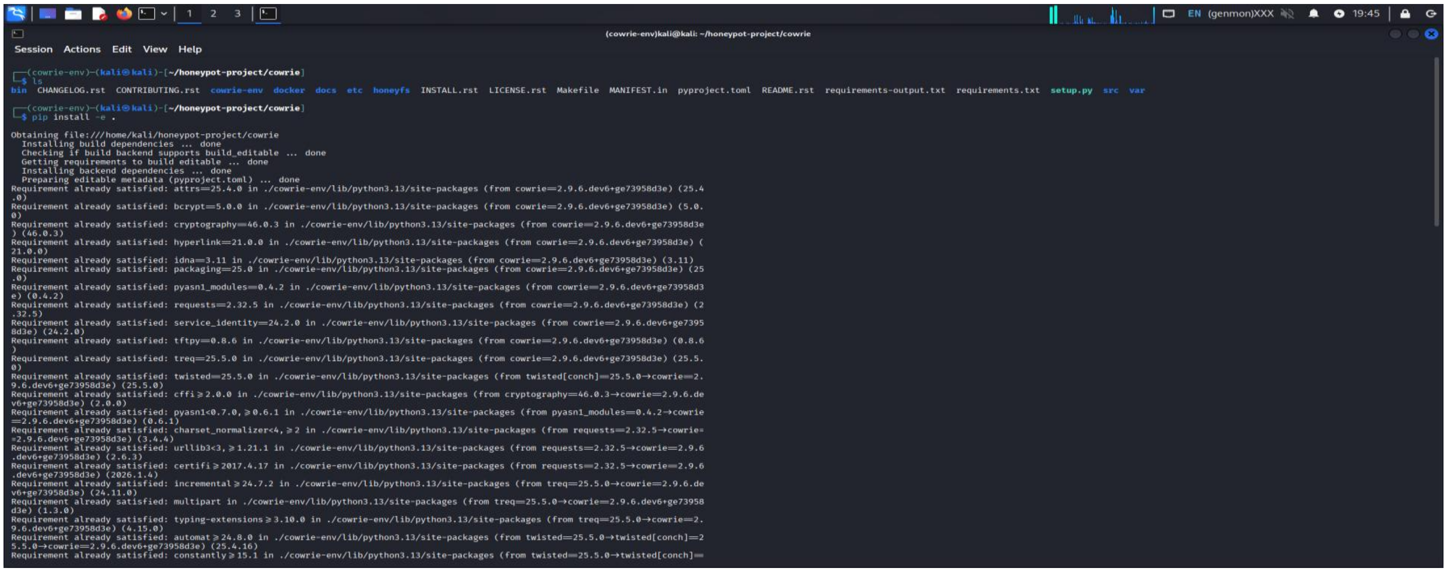
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install -y git python3 python3-venv python3-pip libssl-dev libffi-dev build-essential

git is already the newest version (1:2.51.0-1).
python3 is already the newest version (3.13.7-1+b1).
python3-venv is already the newest version (3.13.7-1+b1).
python3-venv set to manually installed.
build-essential is already the newest version (12.12).
Upgrading:
  libffi-dev  libffi8  python3-pip  python3-pip-whl

Installing:
  libssl-dev

Suggested packages:
  libssl-doc

Summary:
  Upgrading: 4, Installing: 1, Removing: 0, Not Upgrading: 1655
  Download size: 5,884 kB
  Space needed: 16.5 MB / 4,385 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 libffi-dev amd64 3.5.2-3 [64.3 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libssl-dev amd64 3.5.4-1 [2,980 kB]
Get:2 http://mirrors.esto.network/kali kali-rolling/main amd64 libffi8 amd64 3.5.2-3 [26.1 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 python3-pip all 25.3+dfsg-1 [1,384 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 python3-pip-whl all 25.3+dfsg-1 [1,430 kB]
Fetched 5,884 kB in 4s (1,502 kB/s)
(Reading database ... 532626 files and directories currently installed.)
Preparing to unpack .../libffi-dev_3.5.2-3_amd64.deb ...
Unpacking libffi-dev:amd64 (3.5.2-3) over (3.5.2-2) ...
Preparing to unpack .../libffi8_3.5.2-3_amd64.deb ...
Unpacking libffi8:amd64 (3.5.2-3) over (3.5.2-2) ...
Selecting previously unselected package libssl-dev:amd64.
Preparing to unpack .../libssl-dev_3.5.4-1_amd64.deb ...
Unpacking libssl-dev:amd64 (3.5.4-1) ...
Preparing to unpack .../python3-pip_25.3+dfsg-1_all.deb ...
Unpacking python3-pip (25.3+dfsg-1) over (25.2+dfsg-1) ...
Preparing to unpack .../python3-pip-whl_25.3+dfsg-1_all.deb ...
Unpacking python3-pip-whl (25.3+dfsg-1) over (25.2+dfsg-1) ...
Setting up python3-pip-whl (25.3+dfsg-1) ...
Setting up libssl-dev:amd64 (3.5.4-1) ...
Setting up python3-pip (25.3+dfsg-1) ...
Setting up libffi8:amd64 (3.5.2-3) ...
Setting up libffi-dev:amd64 (3.5.2-3) ...
Processing triggers for kali-menu (2025.4.2) ...
Processing triggers for doc-base (0.11.2) ...
Processing 1 changed doc-base file...
Processing triggers for libc-bin (2.41-12) ...
Processing triggers for man-db (2.13.1-1) ...

┌──(kali㉿kali)-[~]
└─$ mkdir ~/honeypot-project
cd ~/honeypot-project
```


1 2 3
EN (genmon)XXX 19:36
(cowrie-env)kali@kali: ~/honeypot-project/cowrie
Session Actions Edit View Help

```
┌──(kali㉿kali)-[~/honeypot-project]
└─$ git clone https://github.com/cowrie/cowrie.git

Cloning into 'cowrie'...
remote: Enumerating objects: 20690, done.
remote: Counting objects: 100% (1007/1007), done.
remote: Compressing objects: 100% (493/493), done.
remote: Total 20690 (delta 881), reused 514 (delta 514), pack-reused 19683 (from 4)
Receiving objects: 100% (20690/20690), 11.37 MiB | 4.37 MiB/s, done.
Resolving deltas: 100% (14352/14352), done.

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


┌──(kali㉿kali)-[~/honeypot-project/cowrie]
└─$ python3 -m venv cowrie-env
source cowrie-env/bin/activate


┌──(cowrie-env)─(kali㉿kali)-[~/honeypot-project/cowrie]
└─$ pip install --upgrade pip
pip install -r requirements.txt

Requirement already satisfied: pip in ./cowrie-env/lib/python3.13/site-packages (25.3)
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==46.0.3 (from -r requirements.txt (line 3))
  Downloading cryptography-46.0.3-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))
  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 (line 12))
  Downloading twisted-25.5.0-py3-none-any.whl.metadata (22 kB)
Collecting urllib3==2.6.3 (from -r requirements.txt (line 13))
  Downloading urllib3-2.6.3-py3-none-any.whl.metadata (6.9 kB)
Collecting cffi>=2.0.0 (from cryptography==46.0.3->-r requirements.txt (line 3))
  Downloading cffi-2.0.0-cp313-cp313-manylinux2014_x86_64.manylinux_2_17_x86_64.whl.metadata (2.6 kB)
Collecting pyasn1<0.7.0,>=0.6.1 (from pyasn1_modules==0.4.2->-r requirements.txt (line 7))
  Downloading pyasn1-0.6.1-py3-none-any.whl.metadata (8.4 kB)
Collecting charset_normalizer<4,>=2 (from requests==2.32.5->-r requirements.txt (line 8))
```


1 2 3
EN (genmon)XXX 19:36
(cowrie-env)kali@kali: ~/honeypot-project/cowrie
Session Actions Edit View Help

```
  Downloading constantly-23.10.4-py3-none-any.whl.metadata (1.8 kB)
Collecting zope-interface>=5 (from twisted==25.5.0->twisted[conch]==25.5.0->-r requirements.txt (line 12))
  Downloading zope_interface-8.2-cp313-cp313-manylinux1_x86_64.manylinux2014_x86_64.manylinux_2_17_x86_64.manylinux_
2_5_x86_64.whl.metadata (45 kB)
Collecting appdirs>=1.4.0 (from twisted[conch]==25.5.0->-r requirements.txt (line 12))
  Downloading appdirs-1.4.4-py2.py3-none-any.whl.metadata (9.0 kB)
Collecting pycparser (from cffi>=2.0.0->cryptography==46.0.3->-r requirements.txt (line 3))
  Downloading pycparser-2.23-py3-none-any.whl.metadata (993 bytes)
Collecting pyopenssl>=21.0.0 (from twisted[tls]>=22.10.0->treq==25.5.0->-r requirements.txt (line 11))
  Downloading pyopenssl-25.3.0-py3-none-any.whl.metadata (17 kB)
Downloading attrs-25.4.0-py3-none-any.whl (67 kB)
Downloading bcrypt-5.0.0-cp39-abi3-manylinux_2_34_x86_64.whl (278 kB)
Downloading cryptography-46.0.3-cp311-abi3-manylinux_2_34_x86_64.whl (4.5 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 4.5/4.5 MB 1.1 MB/s  0:00:04
Downloading hyperlink-21.0.0-py2.py3-none-any.whl (74 kB)
Downloading idna-3.11-py3-none-any.whl (71 kB)
Downloading packaging-25.0-py3-none-any.whl (66 kB)
Downloading pyasn1_modules-0.4.2-py3-none-any.whl (181 kB)
Downloading requests-2.32.5-py3-none-any.whl (64 kB)
Downloading urllib3-2.6.3-py3-none-any.whl (131 kB)
Downloading service_identity-24.2.0-py3-none-any.whl (11 kB)
Downloading tftpy-0.8.6-py3-none-any.whl (28 kB)
Downloading treq-25.5.0-py3-none-any.whl (77 kB)
Downloading twisted-25.5.0-py3-none-any.whl (3.2 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 3.2/3.2 MB 1.2 MB/s  0:00:02
Downloading charset_normalizer-3.4.4-cp313-cp313-manylinux2014_x86_64.manylinux_2_17_x86_64.manylinux_2_28_x86_64.wh
l (153 kB)
Downloading pyasn1-0.6.1-py3-none-any.whl (83 kB)
Downloading appdirs-1.4.4-py2.py3-none-any.whl (9.6 kB)
Downloading automat-25.4.16-py3-none-any.whl (42 kB)
Downloading certifi-2026.1.4-py3-none-any.whl (152 kB)
Downloading cffi-2.0.0-cp313-cp313-manylinux2014_x86_64.manylinux_2_17_x86_64.whl (219 kB)
Downloading constantly-23.10.4-py3-none-any.whl (13 kB)
Downloading incremental-24.11.0-py3-none-any.whl (21 kB)
Downloading pyopenssl-25.3.0-py3-none-any.whl (57 kB)
Downloading typing_extensions-4.15.0-py3-none-any.whl (44 kB)
Downloading zope_interface-8.2-cp313-cp313-manylinux1_x86_64.manylinux2014_x86_64.manylinux_2_17_x86_64.manylinux_2_
5_x86_64.whl (264 kB)
Downloading multipart-1.3.0-py3-none-any.whl (14 kB)
Downloading pycparser-2.23-py3-none-any.whl (118 kB)
Installing collected packages: appdirs, zope-interface, urllib3, typing-extensions, tftpy, pycparser, pyasn1, packag
ing, multipart, idna, constantly, charset_normalizer, certifi, bcrypt, automat, attrs, requests, pyasn1_modules, inc
remental, hyperlink, cffi, twisted, cryptography, service_identity, pyopenssl, treq
Successfully installed appdirs-1.4.4 attrs-25.4.0 automat-25.4.16 bcrypt-5.0.0 certifi-2026.1.4 cffi-2.0.0 charset_n
ormalizer-3.4.4 constantly-23.10.4 cryptography-46.0.3 hyperlink-21.0.0 idna-3.11 incremental-24.11.0 multipart-1.3.
0 packaging-25.0 pyasn1-0.6.1 pyasn1_modules-0.4.2 pycparser-2.23 pyopenssl-25.3.0 requests-2.32.5 service_identity-
24.2.0 tftpy-0.8.6 treq-25.5.0 twisted-25.5.0 typing-extensions-4.15.0 urllib3-2.6.3 zope-interface-8.2

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


┌──(cowrie-env)─(kali㉿kali)-[~/honeypot-project/cowrie]
└─$ nano etc/cowrie.cfg
```


1 2 3
EN (genmon)XXX 19:45
(cowrie-env)kali@kali: ~/honeypot-project/cowrie
Session Actions Edit View Help

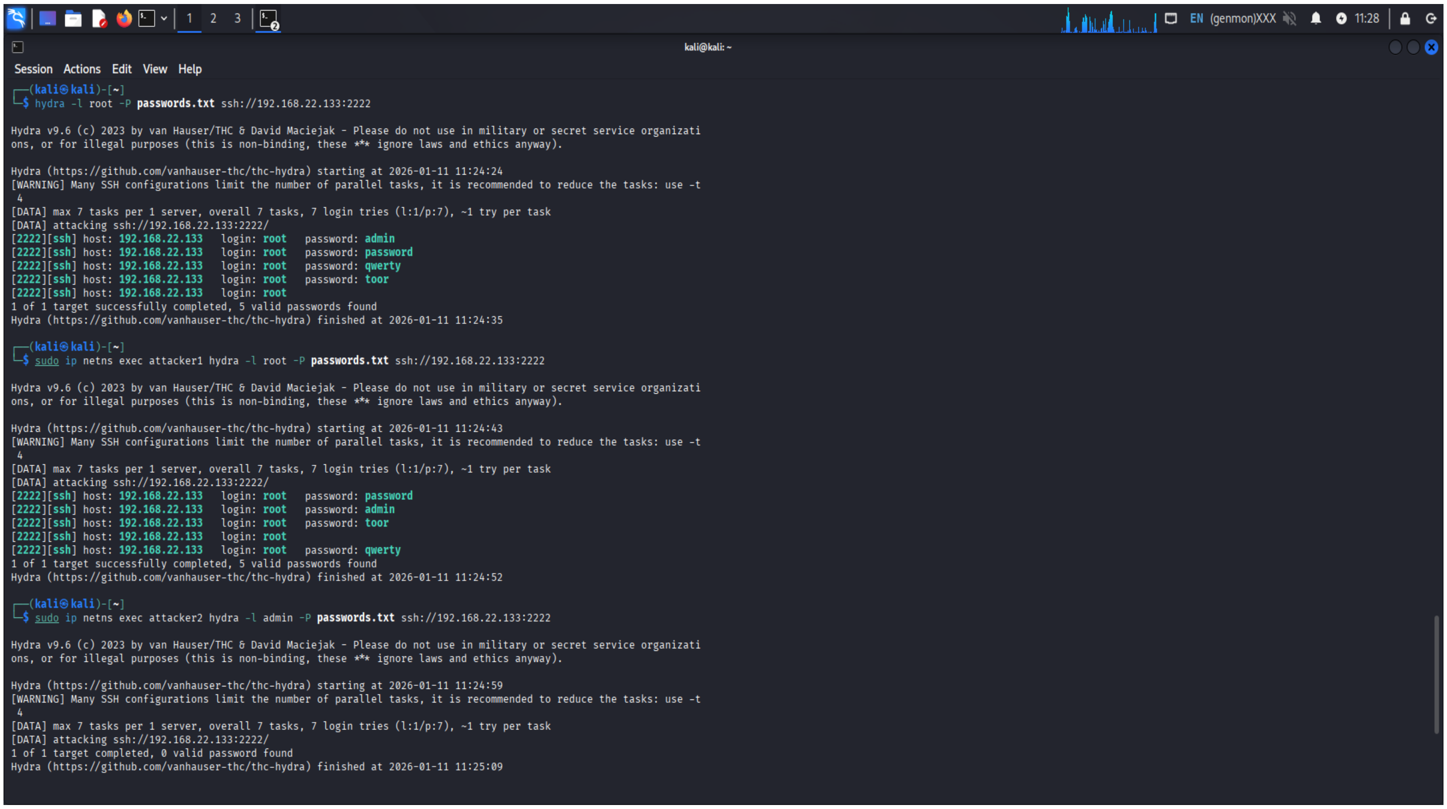
```
┌──(cowrie-env)─(kali㉿kali)-[~/honeypot-project/cowrie]
└─$ ls
bin  CHANGELOG.rst  CONTRIBUTING.rst  cowrie-env  docker  docs  etc  honeyfs  INSTALL.rst  LICENSE.rst  Makefile  MANIFEST.in  pyproject.toml  README.rst  requirements-output.txt  requirements.txt  setup.py  src  var

┌──(cowrie-env)─(kali㉿kali)-[~/honeypot-project/cowrie]
└─$ pip install -e .

Obtaining file:///home/kali/honeypot-project/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==2.9.6.dev6+ge73958d3e) (25.4
.0)
Requirement already satisfied: bcrypt==5.0.0 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.6.dev6+ge73958d3e) (5.0.
0)
Requirement already satisfied: cryptography==46.0.3 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.6.dev6+ge73958d3e
) (46.0.3)
Requirement already satisfied: hyperlink==21.0.0 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.6.dev6+ge73958d3e) (
21.0.0)
Requirement already satisfied: idna==3.11 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.6.dev6+ge73958d3e) (3.11)
Requirement already satisfied: packaging==25.0 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.6.dev6+ge73958d3e) (25
.0)
Requirement already satisfied: pyasn1_modules==0.4.2 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.6.dev6+ge73958d3
e) (0.4.2)
Requirement already satisfied: requests==2.32.5 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.6.dev6+ge73958d3e) (2
.32.5)
Requirement already satisfied: service_identity==24.2.0 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.6.dev6+ge7395
8d3e) (24.2.0)
Requirement already satisfied: tftpy==0.8.6 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.6.dev6+ge73958d3e) (0.8.6
)
Requirement already satisfied: treq==25.5.0 in ./cowrie-env/lib/python3.13/site-packages (from cowrie==2.9.6.dev6+ge73958d3e) (25.5.
0)
Requirement already satisfied: twisted==25.5.0 in ./cowrie-env/lib/python3.13/site-packages (from twisted[conch]==25.5.0->cowrie==2.
9.6.dev6+ge73958d3e) (25.5.0)
Requirement already satisfied: cffi>=2.0.0 in ./cowrie-env/lib/python3.13/site-packages (from cryptography==46.0.3->cowrie==2.9.6.de
v6+ge73958d3e) (2.0.0)
Requirement already satisfied: pyasn1<0.7.0,>=0.6.1 in ./cowrie-env/lib/python3.13/site-packages (from pyasn1_modules==0.4.2->cowrie
==2.9.6.dev6+ge73958d3e) (0.6.1)
Requirement already satisfied: charset_normalizer<4,>=2 in ./cowrie-env/lib/python3.13/site-packages (from requests==2.32.5->cowrie=
=2.9.6.dev6+ge73958d3e) (3.4.4)
Requirement already satisfied: urllib3<3,>=1.21.1 in ./cowrie-env/lib/python3.13/site-packages (from requests==2.32.5->cowrie==2.9.6
.dev6+ge73958d3e) (2.6.3)
Requirement already satisfied: certifi>=2017.4.17 in ./cowrie-env/lib/python3.13/site-packages (from requests==2.32.5->cowrie==2.9.6
.dev6+ge73958d3e) (2026.1.4)
Requirement already satisfied: incremental>=24.7.2 in ./cowrie-env/lib/python3.13/site-packages (from treq==25.5.0->cowrie==2.9.6.de
v6+ge73958d3e) (24.11.0)
Requirement already satisfied: multipart in ./cowrie-env/lib/python3.13/site-packages (from treq==25.5.0->cowrie==2.9.6.dev6+ge73958
d3e) (1.3.0)
Requirement already satisfied: typing-extensions>=3.10.0 in ./cowrie-env/lib/python3.13/site-packages (from treq==25.5.0->cowrie==2.
9.6.dev6+ge73958d3e) (4.15.0)
Requirement already satisfied: automat>=24.8.0 in ./cowrie-env/lib/python3.13/site-packages (from twisted==25.5.0->twisted[conch]==2
5.5.0->cowrie==2.9.6.dev6+ge73958d3e) (25.4.16)
Requirement already satisfied: constantly>=15.1 in ./cowrie-env/lib/python3.13/site-packages (from twisted==25.5.0->twisted[conch]==
```

3. Attack Simulation Methodology-

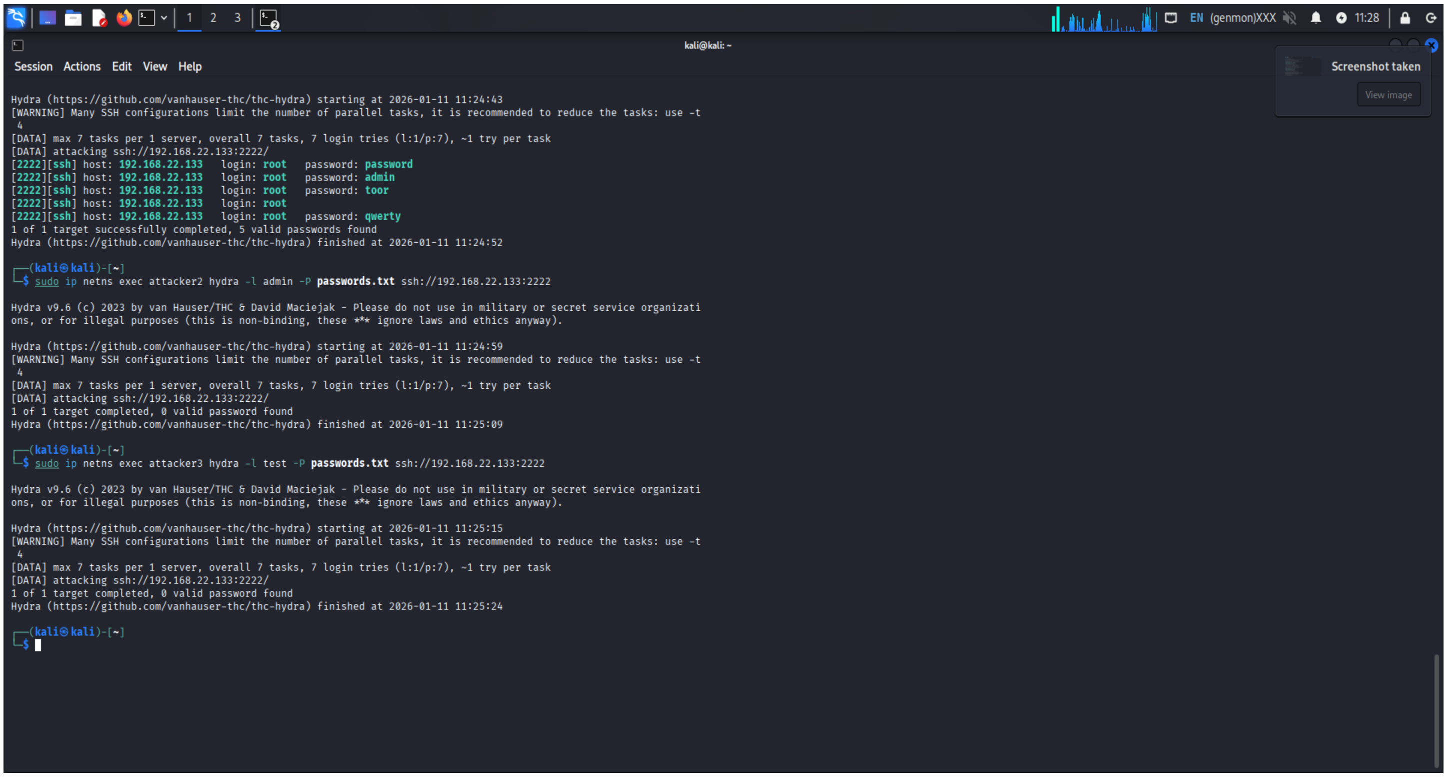
Three attacker environments were created using Linux network namespaces to simulate distinct IP addresses. Hydra was used to perform brute-force attacks against the Cowrie SSH service. Each attacker attempted different username-password combinations.

Attack Commands:

attacker1: root account brute-force
attacker2: admin account brute-force
attacker3: test account brute-force



```
┌──(kali㉿kali)-[~]
└─$ hydra -l root -P passwords.txt ssh://192.168.22.133:2222

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-11 11:24:24
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://192.168.22.133:2222/
[2222][ssh] host: 192.168.22.133   login: root   password: admin
[2222][ssh] host: 192.168.22.133   login: root   password: password
[2222][ssh] host: 192.168.22.133   login: root   password: qwerty
[2222][ssh] host: 192.168.22.133   login: root   password: toor
[2222][ssh] host: 192.168.22.133   login: root
1 of 1 target successfully completed, 5 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-11 11:24:35

┌──(kali㉿kali)-[~]
└─$ sudo ip netns exec attacker1 hydra -l root -P passwords.txt ssh://192.168.22.133:2222

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-11 11:24:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://192.168.22.133:2222/
[2222][ssh] host: 192.168.22.133   login: root   password: password
[2222][ssh] host: 192.168.22.133   login: root   password: admin
[2222][ssh] host: 192.168.22.133   login: root   password: toor
[2222][ssh] host: 192.168.22.133   login: root
[2222][ssh] host: 192.168.22.133   login: root   password: qwerty
1 of 1 target successfully completed, 5 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-11 11:24:52

┌──(kali㉿kali)-[~]
└─$ sudo ip netns exec attacker2 hydra -l admin -P passwords.txt ssh://192.168.22.133:2222

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-11 11:24:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://192.168.22.133:2222/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-11 11:25:09
```

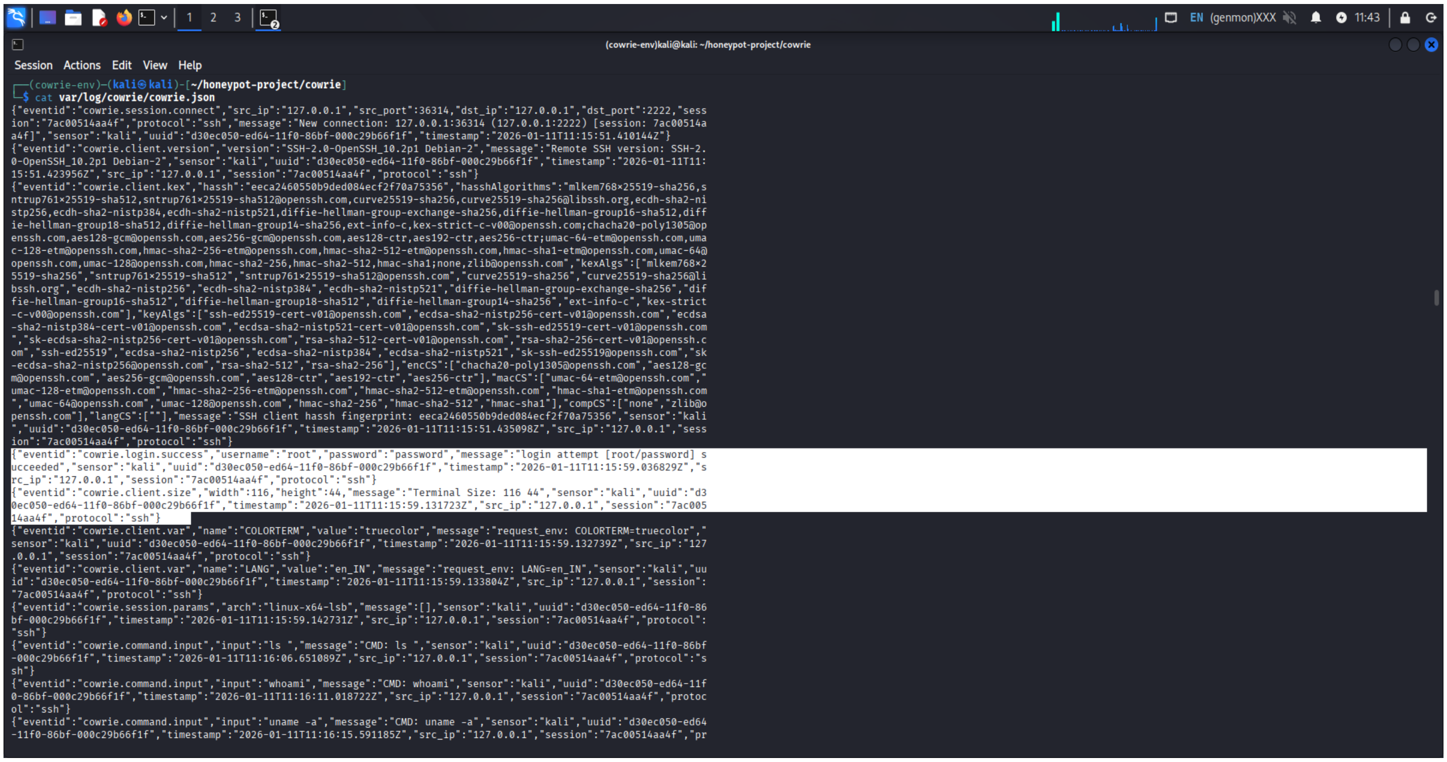


```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-11 11:24:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://192.168.22.133:2222/
[2222][ssh] host: 192.168.22.133   login: root   password: password
[2222][ssh] host: 192.168.22.133   login: root   password: admin
[2222][ssh] host: 192.168.22.133   login: root   password: toor
[2222][ssh] host: 192.168.22.133   login: root
[2222][ssh] host: 192.168.22.133   login: root   password: qwerty
1 of 1 target successfully completed, 5 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-11 11:24:52

┌──(kali㉿kali)-[~]
└─$ sudo ip netns exec attacker2 hydra -l admin -P passwords.txt ssh://192.168.22.133:2222

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-11 11:24:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://192.168.22.133:2222/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-11 11:25:09

┌──(kali㉿kali)-[~]
└─$ sudo ip netns exec attacker3 hydra -l test -P passwords.txt ssh://192.168.22.133:2222

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-11 11:25:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://192.168.22.133:2222/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-11 11:25:24

┌──(kali㉿kali)-[~]
└─$ 
```

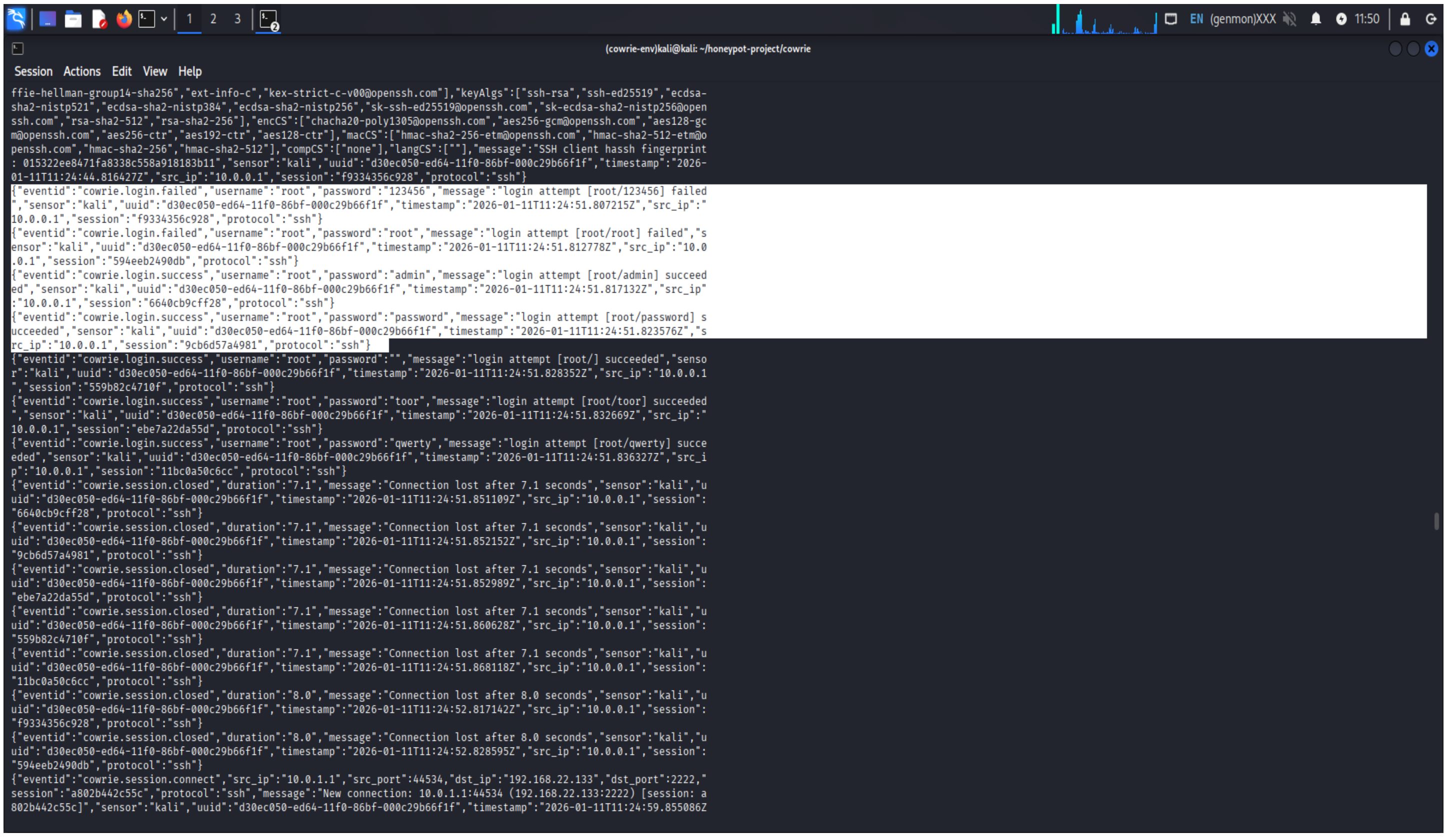
4. Log Collection

Cowrie stores logs in JSON format. The following event types were extracted:

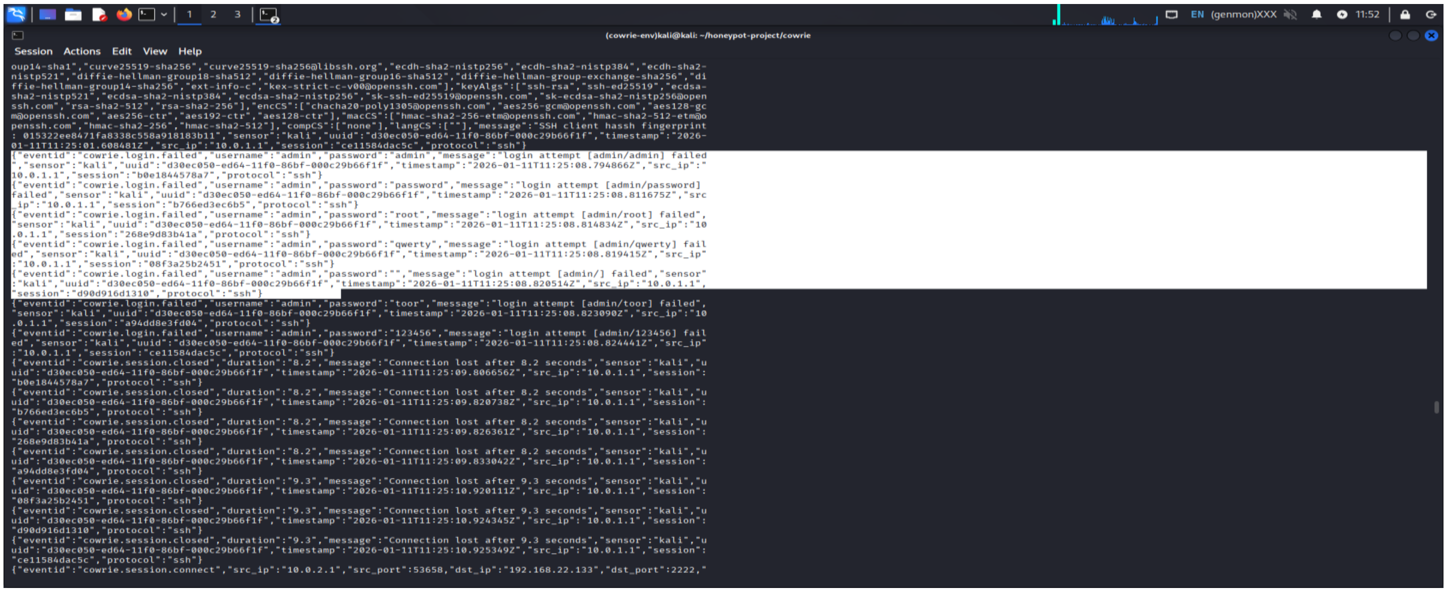
- cowrie.session.connect
- cowrie.login.failed
- cowrie.login.success
- cowrie.command.input
- cowrie.session.closed



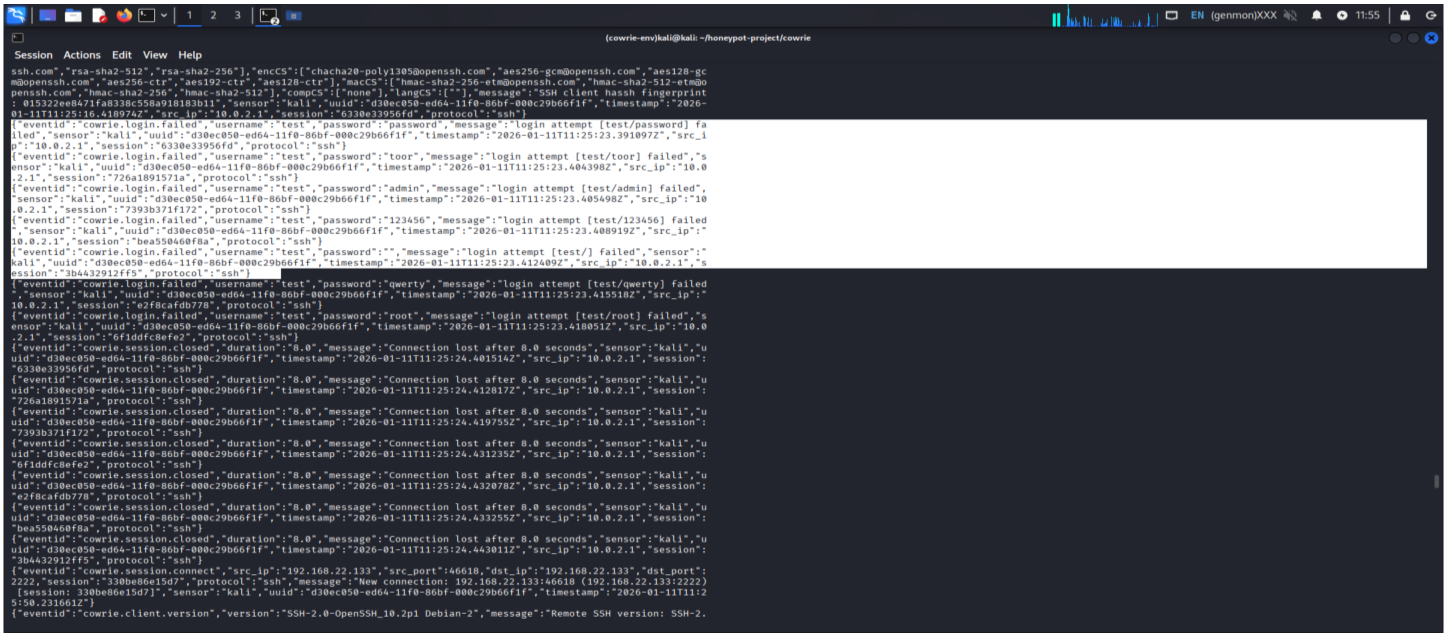
```
┌──(cowrie-env)─(kali㉿kali)-[~/honeypot-project/cowrie]
└─$ cat var/log/cowrie/cowrie.json
{"eventid":"cowrie.session.connect","src_ip":"127.0.0.1","src_port":36314,"dst_ip":"127.0.0.1","dst_port":2222,"sess
ion":"7ac00514aa4f","protocol":"ssh","message":"New connection: 127.0.0.1:36314 (127.0.0.1:2222) [session: 7ac00514a
a4f]","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:15:51.410144Z"}
{"eventid":"cowrie.client.version","version":"SSH-2.0-OpenSSH_10.2p1 Debian-2","message":"Remote SSH version: SSH-2.
0-OpenSSH_10.2p1 Debian-2","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:
15:51.423956Z","src_ip":"127.0.0.1","session":"7ac00514aa4f","protocol":"ssh"}
{"eventid":"cowrie.client.kex","hassh":"eeca2460550b9ded084ecf2f70a75356","hasshAlgorithms":"mlkem768×25519-sha256,s
ntrup761×25519-sha512,sntrup761×25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-ni
stp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diff
ie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com;chacha20-poly1305@op
enssh.com,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr;umac-64-etm@openssh.com,uma
c-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":["mlkem768×2
5519-sha256","sntrup761×25519-sha512","sntrup761×25519-sha512@openssh.com","curve25519-sha256","curve25519-sha256@li
bssh.org","ecdh-sha2-nistp256","ecdh-sha2-nistp384","ecdh-sha2-nistp521","diffie-hellman-group-exchange-sha256","dif
fie-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-nistp256-cert-v01@openssh.com","rsa-sha2-512-cert-v01@openssh.com","rsa-sha2-256-cert-v01@openssh.c
om","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-gc
m@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@o
penssh.com"],"langCS":[""],"message":"SSH client hassh fingerprint: eeca2460550b9ded084ecf2f70a75356","sensor":"kali
","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:15:51.435098Z","src_ip":"127.0.0.1","sess
ion":"7ac00514aa4f","protocol":"ssh"}
{"eventid":"cowrie.login.success","username":"root","password":"password","message":"login attempt [root/password] s
ucceeded","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:15:59.036829Z","s
rc_ip":"127.0.0.1","session":"7ac00514aa4f","protocol":"ssh"}
{"eventid":"cowrie.client.size","width":116,"height":44,"message":"Terminal Size: 116 44","sensor":"kali","uuid":"d3
0ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:15:59.131723Z","src_ip":"127.0.0.1","session":"7ac005
14aa4f","protocol":"ssh"}
{"eventid":"cowrie.client.var","name":"COLORTERM","value":"truecolor","message":"request_env: COLORTERM=truecolor","
sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:15:59.132739Z","src_ip":"127
.0.0.1","session":"7ac00514aa4f","protocol":"ssh"}
{"eventid":"cowrie.client.var","name":"LANG","value":"en_IN","message":"request_env: LANG=en_IN","sensor":"kali","uu
id":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:15:59.133804Z","src_ip":"127.0.0.1","session":
"7ac00514aa4f","protocol":"ssh"}
{"eventid":"cowrie.session.params","arch":"linux-x64-lsb","message":[],"sensor":"kali","uuid":"d30ec050-ed64-11f0-86
bf-000c29b66f1f","timestamp":"2026-01-11T11:15:59.142731Z","src_ip":"127.0.0.1","session":"7ac00514aa4f","protocol":
"ssh"}
{"eventid":"cowrie.command.input","input":"ls ","message":"CMD: ls ","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf
-000c29b66f1f","timestamp":"2026-01-11T11:16:06.651089Z","src_ip":"127.0.0.1","session":"7ac00514aa4f","protocol":"s
sh"}
{"eventid":"cowrie.command.input","input":"whoami","message":"CMD: whoami","sensor":"kali","uuid":"d30ec050-ed64-11f
0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:16:11.018722Z","src_ip":"127.0.0.1","session":"7ac00514aa4f","protoc
ol":"ssh"}
{"eventid":"cowrie.command.input","input":"uname -a","message":"CMD: uname -a","sensor":"kali","uuid":"d30ec050-ed64
-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:16:15.591185Z","src_ip":"127.0.0.1","session":"7ac00514aa4f","pr
```



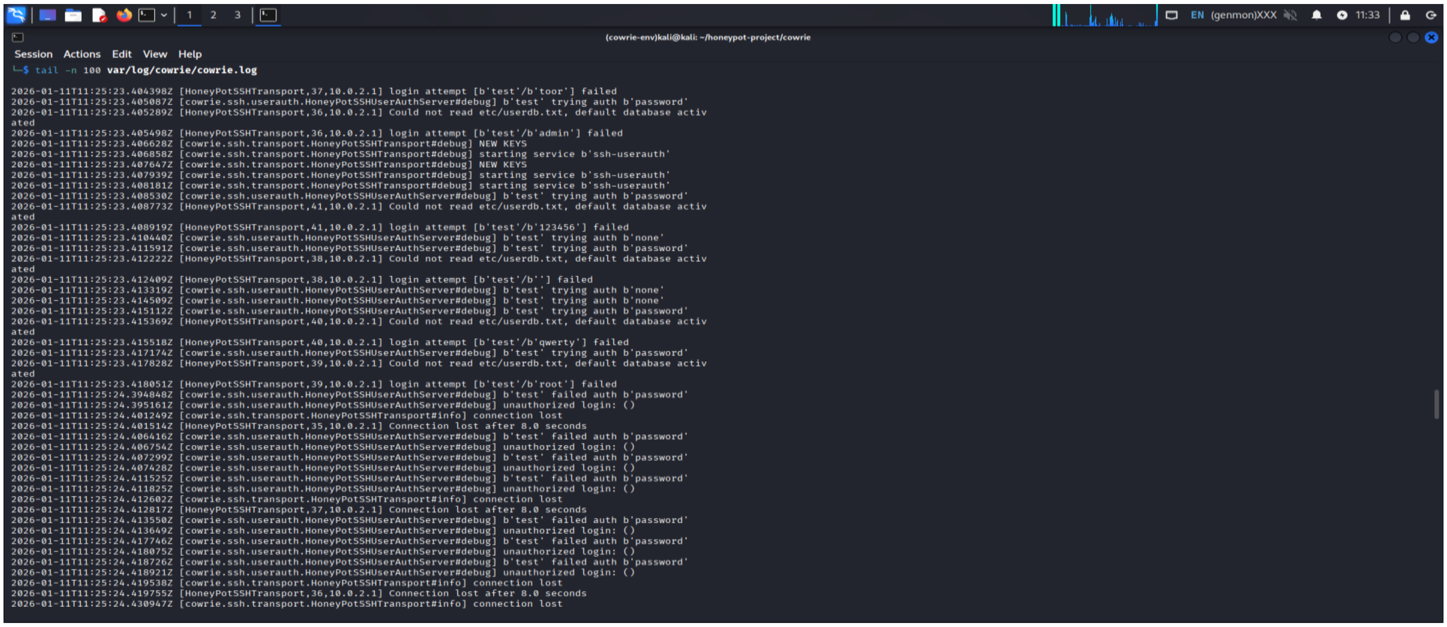
```
ffie-hellman-group14-sha256","ext-info-c","kex-strict-c-v00@openssh.com"],"keyAlgs":["ssh-rsa","ssh-ed25519","ecdsa-
sha2-nistp521","ecdsa-sha2-nistp384","ecdsa-sha2-nistp256","sk-ssh-ed25519@openssh.com","sk-ecdsa-sha2-nistp256@open
ssh.com","rsa-sha2-512","rsa-sha2-256"],"encCS":["chacha20-poly1305@openssh.com","aes256-gcm@openssh.com","aes128-gc
m@openssh.com","aes256-ctr","aes192-ctr","aes128-ctr"],"macCS":["hmac-sha2-256-etm@openssh.com","hmac-sha2-512-etm@o
penssh.com","hmac-sha2-256","hmac-sha2-512"],"compCS":["none"],"langCS":[""],"message":"SSH client hassh fingerprint
: 015322ee8471fa8338c558a918183b11","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-
01-11T11:24:44.816427Z","src_ip":"10.0.0.1","session":"f9334356c928","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"root","password":"123456","message":"login attempt [root/123456] failed
","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:51.807215Z","src_ip":"
10.0.0.1","session":"f9334356c928","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"root","password":"root","message":"login attempt [root/root] failed","s
ensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:51.812778Z","src_ip":"10.0
.0.1","session":"594eeb2490db","protocol":"ssh"}
{"eventid":"cowrie.login.success","username":"root","password":"admin","message":"login attempt [root/admin] succeed
ed","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:51.817132Z","src_ip"
:"10.0.0.1","session":"6640cb9cff28","protocol":"ssh"}
{"eventid":"cowrie.login.success","username":"root","password":"password","message":"login attempt [root/password] s
ucceeded","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:51.823576Z","s
rc_ip":"10.0.0.1","session":"9cb6d57a4981","protocol":"ssh"}
{"eventid":"cowrie.login.success","username":"root","password":"","message":"login attempt [root/] succeeded","senso
r":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:51.828352Z","src_ip":"10.0.0.1
","session":"559b82c4710f","protocol":"ssh"}
{"eventid":"cowrie.login.success","username":"root","password":"toor","message":"login attempt [root/toor] succeeded
","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:51.832669Z","src_ip":"
10.0.0.1","session":"ebe7a22da55d","protocol":"ssh"}
{"eventid":"cowrie.login.success","username":"root","password":"qwerty","message":"login attempt [root/qwerty] succe
eded","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:51.836327Z","src_i
p":"10.0.0.1","session":"11bc0a50c6cc","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"7.1","message":"Connection lost after 7.1 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:51.851109Z","src_ip":"10.0.0.1","session":
"6640cb9cff28","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"7.1","message":"Connection lost after 7.1 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:51.852152Z","src_ip":"10.0.0.1","session":
"9cb6d57a4981","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"7.1","message":"Connection lost after 7.1 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:51.852989Z","src_ip":"10.0.0.1","session":
"ebe7a22da55d","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"7.1","message":"Connection lost after 7.1 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:51.860628Z","src_ip":"10.0.0.1","session":
"559b82c4710f","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"7.1","message":"Connection lost after 7.1 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:51.868118Z","src_ip":"10.0.0.1","session":
"11bc0a50c6cc","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"8.0","message":"Connection lost after 8.0 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:52.817142Z","src_ip":"10.0.0.1","session":
"f9334356c928","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"8.0","message":"Connection lost after 8.0 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:52.828595Z","src_ip":"10.0.0.1","session":
"594eeb2490db","protocol":"ssh"}
{"eventid":"cowrie.session.connect","src_ip":"10.0.1.1","src_port":44534,"dst_ip":"192.168.22.133","dst_port":2222,"
session":"a802b442c55c","protocol":"ssh","message":"New connection: 10.0.1.1:44534 (192.168.22.133:2222) [session: a
802b442c55c]","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:24:59.855086Z
```


1 2 3
EN (genmon)XXX 11:52
(cowrie-env)kali@kali: ~/honeypot-project/cowrie
Session Actions Edit View Help

```
oup14-sha1","curve25519-sha256","curve25519-sha256@libssh.org","ecdh-sha2-nistp256","ecdh-sha2-nistp384","ecdh-sha2-
nistp521","diffie-hellman-group18-sha512","diffie-hellman-group16-sha512","diffie-hellman-group-exchange-sha256","di
ffie-hellman-group14-sha256","ext-info-c","kex-strict-c-v00@openssh.com"],"keyAlgs":["ssh-rsa","ssh-ed25519","ecdsa-
sha2-nistp521","ecdsa-sha2-nistp384","ecdsa-sha2-nistp256","sk-ssh-ed25519@openssh.com","sk-ecdsa-sha2-nistp256@open
ssh.com","rsa-sha2-512","rsa-sha2-256"],"encCS":["chacha20-poly1305@openssh.com","aes256-gcm@openssh.com","aes128-gc
m@openssh.com","aes256-ctr","aes192-ctr","aes128-ctr"],"macCS":["hmac-sha2-256-etm@openssh.com","hmac-sha2-512-etm@o
penssh.com","hmac-sha2-256","hmac-sha2-512"],"compCS":["none"],"langCS":[""],"message":"SSH client hassh fingerprint
: 015322ee8471fa8338c558a918183b11","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-
01-11T11:25:01.608481Z","src_ip":"10.0.1.1","session":"ce11584dac5c","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"admin","password":"admin","message":"login attempt [admin/admin] failed
","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:08.794866Z","src_ip":"
10.0.1.1","session":"b0e1844578a7","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"admin","password":"password","message":"login attempt [admin/password]
failed","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:08.811675Z","src
_ip":"10.0.1.1","session":"b766ed3ec6b5","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"admin","password":"root","message":"login attempt [admin/root] failed",
"sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:08.814834Z","src_ip":"10
.0.1.1","session":"268e9d83b41a","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"admin","password":"qwerty","message":"login attempt [admin/qwerty] fail
ed","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:08.819415Z","src_ip"
:"10.0.1.1","session":"08f3a25b2451","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"admin","password":"","message":"login attempt [admin/] failed","sensor"
:"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:08.820514Z","src_ip":"10.0.1.1",
"session":"d90d916d1310","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"admin","password":"toor","message":"login attempt [admin/toor] failed",
"sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:08.823090Z","src_ip":"10
.0.1.1","session":"a94dd8e3fd04","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"admin","password":"123456","message":"login attempt [admin/123456] fail
ed","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:08.824441Z","src_ip"
:"10.0.1.1","session":"ce11584dac5c","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"8.2","message":"Connection lost after 8.2 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:09.806656Z","src_ip":"10.0.1.1","session":
"b0e1844578a7","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"8.2","message":"Connection lost after 8.2 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:09.820738Z","src_ip":"10.0.1.1","session":
"b766ed3ec6b5","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"8.2","message":"Connection lost after 8.2 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:09.826361Z","src_ip":"10.0.1.1","session":
"268e9d83b41a","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"8.2","message":"Connection lost after 8.2 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:09.833042Z","src_ip":"10.0.1.1","session":
"a94dd8e3fd04","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"9.3","message":"Connection lost after 9.3 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:10.920111Z","src_ip":"10.0.1.1","session":
"08f3a25b2451","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"9.3","message":"Connection lost after 9.3 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:10.924345Z","src_ip":"10.0.1.1","session":
"d90d916d1310","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"9.3","message":"Connection lost after 9.3 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:10.925349Z","src_ip":"10.0.1.1","session":
"ce11584dac5c","protocol":"ssh"}
{"eventid":"cowrie.session.connect","src_ip":"10.0.2.1","src_port":53658,"dst_ip":"192.168.22.133","dst_port":2222,"
```


1 2 3
EN (genmon)XXX 11:55
(cowrie-env)kali@kali: ~/honeypot-project/cowrie
Session Actions Edit View Help

```
ssh.com","rsa-sha2-512","rsa-sha2-256"],"encCS":["chacha20-poly1305@openssh.com","aes256-gcm@openssh.com","aes128-gc
m@openssh.com","aes256-ctr","aes192-ctr","aes128-ctr"],"macCS":["hmac-sha2-256-etm@openssh.com","hmac-sha2-512-etm@o
penssh.com","hmac-sha2-256","hmac-sha2-512"],"compCS":["none"],"langCS":[""],"message":"SSH client hassh fingerprint
: 015322ee8471fa8338c558a918183b11","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-
01-11T11:25:16.418974Z","src_ip":"10.0.2.1","session":"6330e33956fd","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"test","password":"password","message":"login attempt [test/password] fa
iled","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:23.391097Z","src_i
p":"10.0.2.1","session":"6330e33956fd","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"test","password":"toor","message":"login attempt [test/toor] failed","s
ensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:23.404398Z","src_ip":"10.0
.2.1","session":"726a1891571a","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"test","password":"admin","message":"login attempt [test/admin] failed",
"sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:23.405498Z","src_ip":"10
.0.2.1","session":"7393b371f172","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"test","password":"123456","message":"login attempt [test/123456] failed
","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:23.408919Z","src_ip":"
10.0.2.1","session":"bea550460f8a","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"test","password":"","message":"login attempt [test/] failed","sensor":"
kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:23.412409Z","src_ip":"10.0.2.1","s
ession":"3b4432912ff5","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"test","password":"qwerty","message":"login attempt [test/qwerty] failed
","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:23.415518Z","src_ip":"
10.0.2.1","session":"e2f8cafdb778","protocol":"ssh"}
{"eventid":"cowrie.login.failed","username":"test","password":"root","message":"login attempt [test/root] failed","s
ensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:23.418051Z","src_ip":"10.0
.2.1","session":"6f1ddfc8efe2","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"8.0","message":"Connection lost after 8.0 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:24.401514Z","src_ip":"10.0.2.1","session":
"6330e33956fd","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"8.0","message":"Connection lost after 8.0 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:24.412817Z","src_ip":"10.0.2.1","session":
"726a1891571a","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"8.0","message":"Connection lost after 8.0 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:24.419755Z","src_ip":"10.0.2.1","session":
"7393b371f172","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"8.0","message":"Connection lost after 8.0 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:24.431235Z","src_ip":"10.0.2.1","session":
"6f1ddfc8efe2","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"8.0","message":"Connection lost after 8.0 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:24.432078Z","src_ip":"10.0.2.1","session":
"e2f8cafdb778","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"8.0","message":"Connection lost after 8.0 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:24.433255Z","src_ip":"10.0.2.1","session":
"bea550460f8a","protocol":"ssh"}
{"eventid":"cowrie.session.closed","duration":"8.0","message":"Connection lost after 8.0 seconds","sensor":"kali","u
uid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:25:24.443011Z","src_ip":"10.0.2.1","session":
"3b4432912ff5","protocol":"ssh"}
{"eventid":"cowrie.session.connect","src_ip":"192.168.22.133","src_port":46618,"dst_ip":"192.168.22.133","dst_port":
2222,"session":"330be86e15d7","protocol":"ssh","message":"New connection: 192.168.22.133:46618 (192.168.22.133:2222)
 [session: 330be86e15d7]","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:2
5:50.231661Z"}
{"eventid":"cowrie.client.version","version":"SSH-2.0-OpenSSH_10.2p1 Debian-2","message":"Remote SSH version: SSH-2.
```


1 2 3
EN (genmon)XXX 11:33
(cowrie-env)kali@kali: ~/honeypot-project/cowrie
Session Actions Edit View Help

```
└─$ tail -n 100 var/log/cowrie/cowrie.log

2026-01-11T11:25:23.404398Z [HoneyPotSSHTransport,37,10.0.2.1] login attempt [b'test'/b'toor'] failed
2026-01-11T11:25:23.405087Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' trying auth b'password'
2026-01-11T11:25:23.405289Z [HoneyPotSSHTransport,36,10.0.2.1] Could not read etc/userdb.txt, default database activ
ated
2026-01-11T11:25:23.405498Z [HoneyPotSSHTransport,36,10.0.2.1] login attempt [b'test'/b'admin'] failed
2026-01-11T11:25:23.406628Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-01-11T11:25:23.406858Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-01-11T11:25:23.407647Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-01-11T11:25:23.407939Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-01-11T11:25:23.408181Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-01-11T11:25:23.408530Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' trying auth b'password'
2026-01-11T11:25:23.408773Z [HoneyPotSSHTransport,41,10.0.2.1] Could not read etc/userdb.txt, default database activ
ated
2026-01-11T11:25:23.408919Z [HoneyPotSSHTransport,41,10.0.2.1] login attempt [b'test'/b'123456'] failed
2026-01-11T11:25:23.410440Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' trying auth b'none'
2026-01-11T11:25:23.411591Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' trying auth b'password'
2026-01-11T11:25:23.412222Z [HoneyPotSSHTransport,38,10.0.2.1] Could not read etc/userdb.txt, default database activ
ated
2026-01-11T11:25:23.412409Z [HoneyPotSSHTransport,38,10.0.2.1] login attempt [b'test'/b''] failed
2026-01-11T11:25:23.413319Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' trying auth b'none'
2026-01-11T11:25:23.414509Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' trying auth b'none'
2026-01-11T11:25:23.415112Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' trying auth b'password'
2026-01-11T11:25:23.415369Z [HoneyPotSSHTransport,40,10.0.2.1] Could not read etc/userdb.txt, default database activ
ated
2026-01-11T11:25:23.415518Z [HoneyPotSSHTransport,40,10.0.2.1] login attempt [b'test'/b'qwerty'] failed
2026-01-11T11:25:23.417174Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' trying auth b'password'
2026-01-11T11:25:23.417828Z [HoneyPotSSHTransport,39,10.0.2.1] Could not read etc/userdb.txt, default database activ
ated
2026-01-11T11:25:23.418051Z [HoneyPotSSHTransport,39,10.0.2.1] login attempt [b'test'/b'root'] failed
2026-01-11T11:25:24.394848Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' failed auth b'password'
2026-01-11T11:25:24.395161Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-11T11:25:24.401249Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-11T11:25:24.401514Z [HoneyPotSSHTransport,35,10.0.2.1] Connection lost after 8.0 seconds
2026-01-11T11:25:24.406416Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' failed auth b'password'
2026-01-11T11:25:24.406754Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-11T11:25:24.407299Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' failed auth b'password'
2026-01-11T11:25:24.407428Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-11T11:25:24.411525Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' failed auth b'password'
2026-01-11T11:25:24.411825Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-11T11:25:24.412602Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-11T11:25:24.412817Z [HoneyPotSSHTransport,37,10.0.2.1] Connection lost after 8.0 seconds
2026-01-11T11:25:24.413550Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' failed auth b'password'
2026-01-11T11:25:24.413649Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-11T11:25:24.417746Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' failed auth b'password'
2026-01-11T11:25:24.418075Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-11T11:25:24.418726Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'test' failed auth b'password'
2026-01-11T11:25:24.418921Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] unauthorized login: ()
2026-01-11T11:25:24.419538Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2026-01-11T11:25:24.419755Z [HoneyPotSSHTransport,36,10.0.2.1] Connection lost after 8.0 seconds
2026-01-11T11:25:24.430947Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
```

5. Data Analysis-

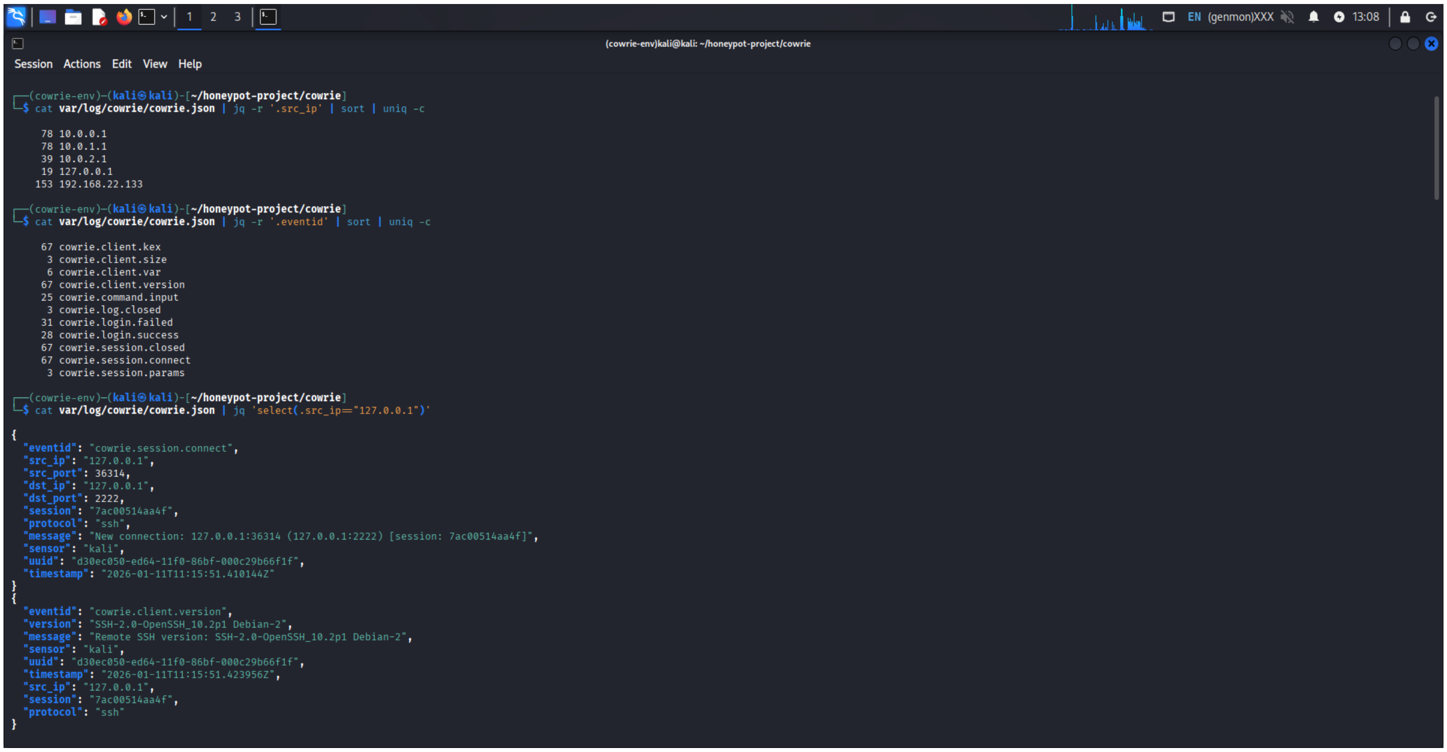
The following tables summarize the captured data.

Table 1: Event Type Frequency

Event Type	Count
cowrie.session.connect	67
cowrie.login.failed	31
cowrie.login.success	28
cowrie.command.input	25
cowrie.session.closed	67

Table 2: Source IP Frequency

Source IP	Events
10.0.0.1	78
10.0.1.1	78
10.0.2.1	39
127.0.0.1	19
192.168.22.133	153



```
┌──(cowrie-env)─(kali㉿kali)-[~/honeypot-project/cowrie]
└─$ cat var/log/cowrie/cowrie.json | jq -r '.src_ip' | sort | uniq -c

     78 10.0.0.1
     78 10.0.1.1
     39 10.0.2.1
     19 127.0.0.1
    153 192.168.22.133

┌──(cowrie-env)─(kali㉿kali)-[~/honeypot-project/cowrie]
└─$ cat var/log/cowrie/cowrie.json | jq -r '.eventid' | sort | uniq -c

     67 cowrie.client.kex
      3 cowrie.client.size
      6 cowrie.client.var
     67 cowrie.client.version
     25 cowrie.command.input
      3 cowrie.log.closed
     31 cowrie.login.failed
     28 cowrie.login.success
     67 cowrie.session.closed
     67 cowrie.session.connect
      3 cowrie.session.params

┌──(cowrie-env)─(kali㉿kali)-[~/honeypot-project/cowrie]
└─$ cat var/log/cowrie/cowrie.json | jq 'select(.src_ip=="127.0.0.1")'

{
  "eventid": "cowrie.session.connect",
  "src_ip": "127.0.0.1",
  "src_port": 36314,
  "dst_ip": "127.0.0.1",
  "dst_port": 2222,
  "session": "7ac00514aa4f",
  "protocol": "ssh",
  "message": "New connection: 127.0.0.1:36314 (127.0.0.1:2222) [session: 7ac00514aa4f]",
  "sensor": "kali",
  "uuid": "d30ec050-ed64-11f0-86bf-000c29b66f1f",
  "timestamp": "2026-01-11T11:15:51.410144Z"
}
{
  "eventid": "cowrie.client.version",
  "version": "SSH-2.0-OpenSSH_10.2p1 Debian-2",
  "message": "Remote SSH version: SSH-2.0-OpenSSH_10.2p1 Debian-2",
  "sensor": "kali",
  "uuid": "d30ec050-ed64-11f0-86bf-000c29b66f1f",
  "timestamp": "2026-01-11T11:15:51.423956Z",
  "src_ip": "127.0.0.1",
  "session": "7ac00514aa4f",
  "protocol": "ssh"
}
```

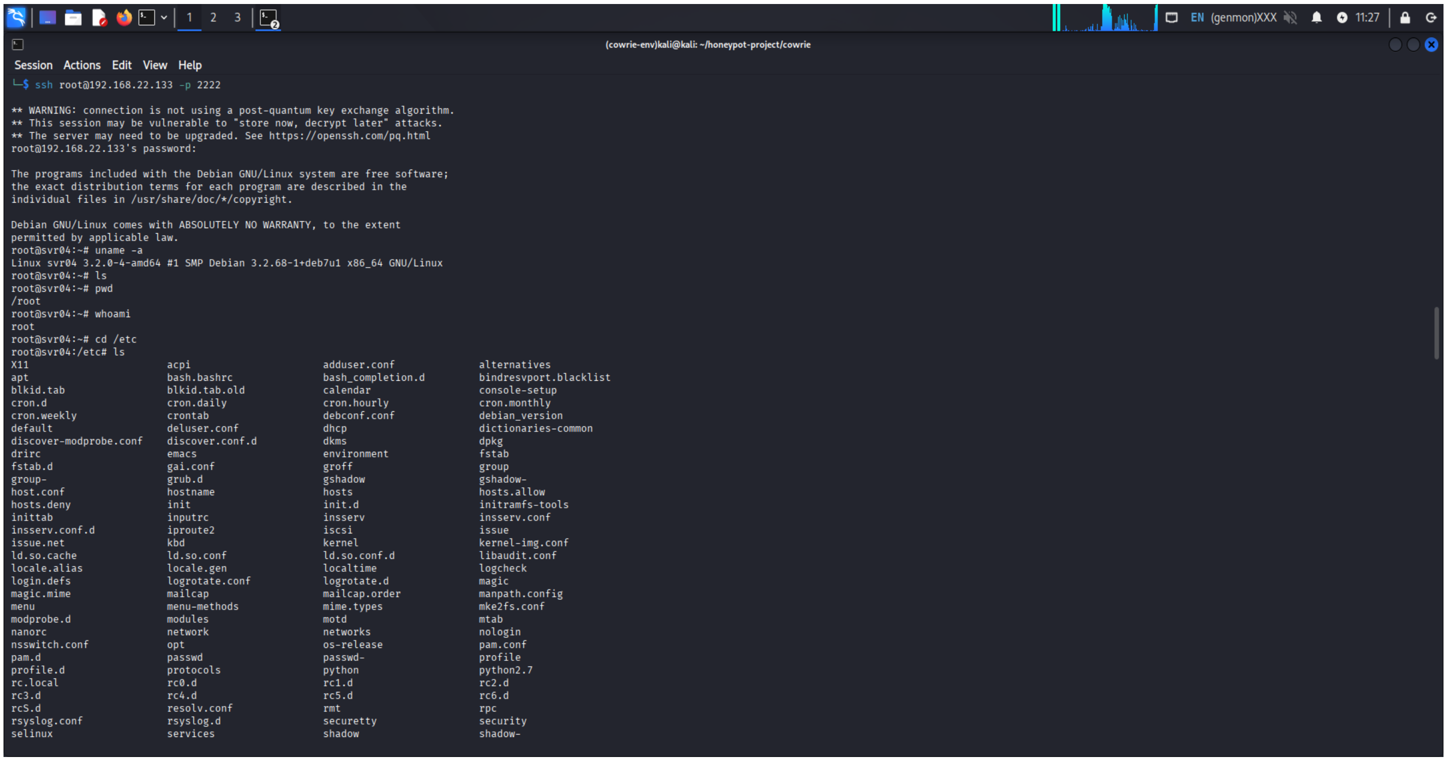
The frequency of authentication-related events indicates that brute-force activity predominates in the attack behavior. As is common with automated password-guessing systems like Hydra, a large number of cowrie.login.failed events indicates frequent incorrect credential attempts.

The honeypot gradually accepted weak or commonly used passwords, as evidenced by multiple cowrie.login.success events. This poses a substantial risk since many real-world attacks are brought on by poor credential hygiene.

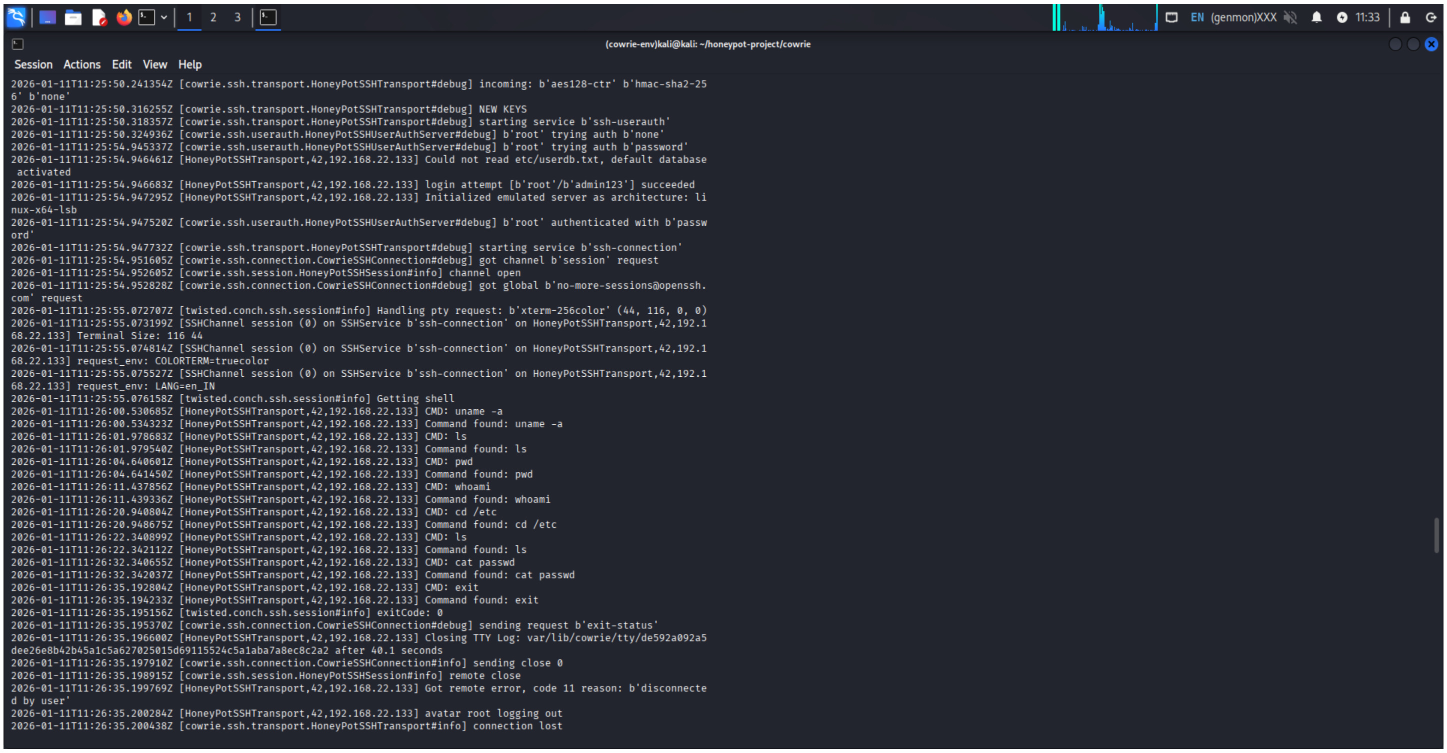
The spread of events across multiple IP addresses confirms that the attacks originated from multiple simulated sources. This proves the effectiveness of the network namespace method used in this project. Overall, the data shows a clear attack lifecycle that consists of scanning, brute-force authentication, successful login and post-compromise reconnaissance.

6. Attacker Behavior Analysis-

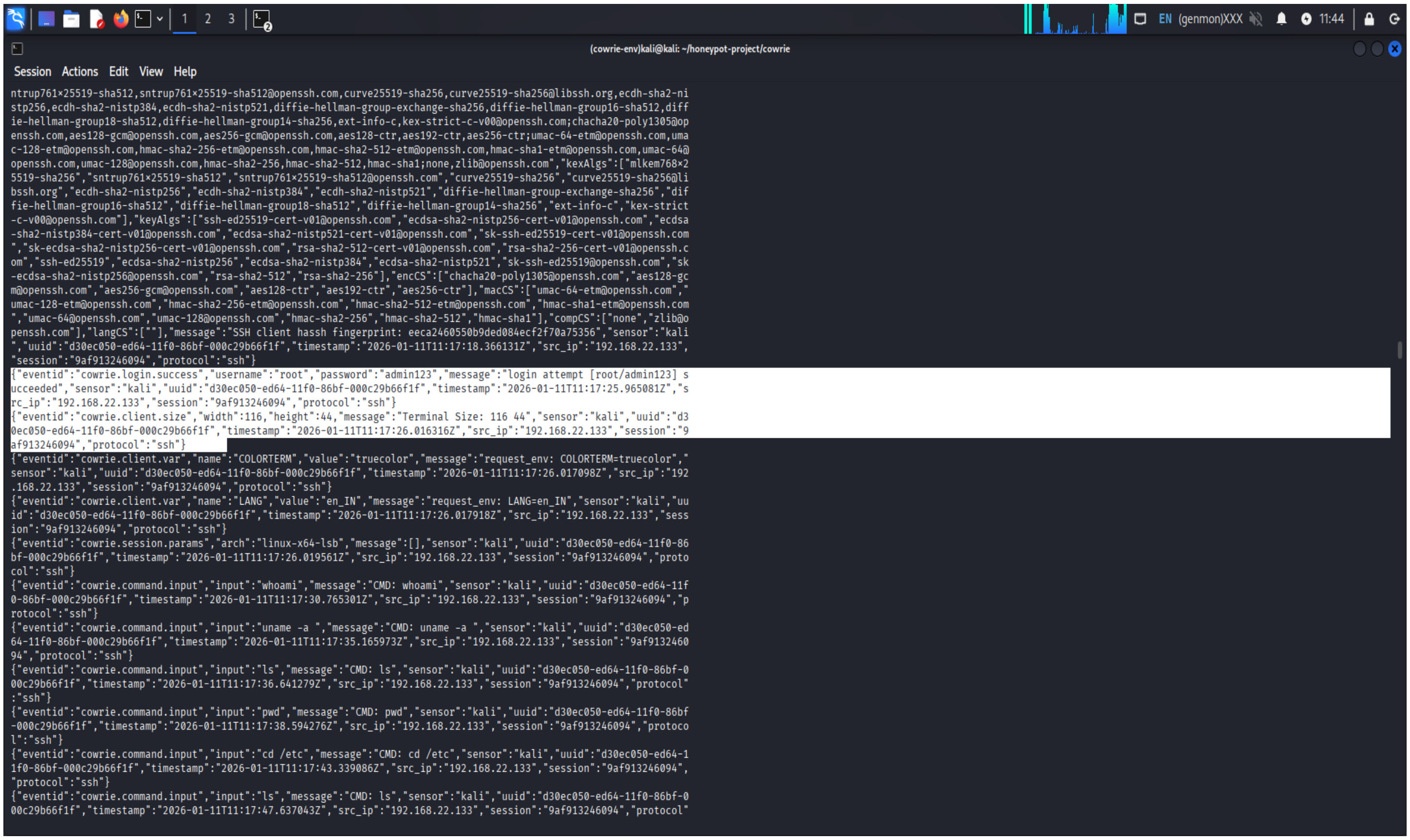
After gaining access, attackers used simple reconnaissance commands to learn more about the compromised machine. While uname -a was used to gather kernel and system information, commands like whoami were used to determine privilege level. To investigate the file system, directory listing tools like ls and pwd were run. This action is indicative of a common early-stage intrusion pattern in which attackers try to evaluate the environment before determining what to do next. In this scenario, neither privilege escalation nor advanced lateral movement were seen. This pattern is in line with actual attacks, in which environmental detection comes after initial access. The usefulness of honeypots in determining attacker intent is demonstrated by capturing these actions.


1 2 3
EN (genmon)XXX 11:27
(cowrie-env)kali@kali: ~/honeypot-project/cowrie
Session Actions Edit View Help

```
└─$ ssh root@192.168.22.133 -p 2222

** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
root@192.168.22.133'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@svr04:~# uname -a
Linux svr04 3.2.0-4-amd64 #1 SMP Debian 3.2.68-1+deb7u1 x86_64 GNU/Linux
root@svr04:~# ls
root@svr04:~# pwd
/root
root@svr04:~# whoami
root
root@svr04:~# cd /etc
root@svr04:/etc# ls
X11                       acpi                      adduser.conf              alternatives
apt                       bash.bashrc               bash_completion.d         bindresvport.blacklist
blkid.tab                 blkid.tab.old             calendar                  console-setup
cron.d                    cron.daily                cron.hourly               cron.monthly
cron.weekly               crontab                   debconf.conf              debian_version
default                   deluser.conf              dhcp                      dictionaries-common
discover-modprobe.conf    discover.conf.d           dkms                      dpkg
drirc                     emacs                     environment               fstab
fstab.d                   gai.conf                  groff                     group
group-                    grub.d                    gshadow                   gshadow-
host.conf                 hostname                  hosts                     hosts.allow
hosts.deny                init                      init.d                    initramfs-tools
inittab                   inputrc                   insserv                   insserv.conf
insserv.conf.d            iproute2                  iscsi                     issue
issue.net                 kbd                       kernel                    kernel-img.conf
ld.so.cache               ld.so.conf                ld.so.conf.d              libaudit.conf
locale.alias              locale.gen                localtime                 logcheck
login.defs                logrotate.conf            logrotate.d               magic
magic.mime                mailcap                   mailcap.order             manpath.config
menu                      menu-methods              mime.types                mke2fs.conf
modprobe.d                modules                   motd                      mtab
nanorc                    network                   networks                  nologin
nsswitch.conf             opt                       os-release                pam.conf
pam.d                     passwd                    passwd-                   profile
profile.d                 protocols                 python                    python2.7
rc.local                  rc0.d                     rc1.d                     rc2.d
rc3.d                     rc4.d                     rc5.d                     rc6.d
rcS.d                     resolv.conf               rmt                       rpc
rsyslog.conf              rsyslog.d                 securetty                 security
selinux                   services                  shadow                    shadow-
```


1 2 3
EN (genmon)XXX 11:33
(cowrie-env)kali@kali: ~/honeypot-project/cowrie
Session Actions Edit View Help

```
2026-01-11T11:25:50.241354Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b'hmac-sha2-25
6' b'none'
2026-01-11T11:25:50.316255Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2026-01-11T11:25:50.318357Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2026-01-11T11:25:50.324936Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2026-01-11T11:25:54.945337Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2026-01-11T11:25:54.946461Z [HoneyPotSSHTransport,42,192.168.22.133] Could not read etc/userdb.txt, default database
 activated
2026-01-11T11:25:54.946683Z [HoneyPotSSHTransport,42,192.168.22.133] login attempt [b'root'/b'admin123'] succeeded
2026-01-11T11:25:54.947295Z [HoneyPotSSHTransport,42,192.168.22.133] Initialized emulated server as architecture: li
nux-x64-lsb
2026-01-11T11:25:54.947520Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'passw
ord'
2026-01-11T11:25:54.947732Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2026-01-11T11:25:54.951605Z [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2026-01-11T11:25:54.952605Z [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2026-01-11T11:25:54.952828Z [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.
com' request
2026-01-11T11:25:55.072707Z [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (44, 116, 0, 0)
2026-01-11T11:25:55.073199Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,42,192.1
68.22.133] Terminal Size: 116 44
2026-01-11T11:25:55.074814Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,42,192.1
68.22.133] request_env: COLORTERM=truecolor
2026-01-11T11:25:55.075527Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,42,192.1
68.22.133] request_env: LANG=en_IN
2026-01-11T11:25:55.076158Z [twisted.conch.ssh.session#info] Getting shell
2026-01-11T11:26:00.530685Z [HoneyPotSSHTransport,42,192.168.22.133] CMD: uname -a
2026-01-11T11:26:00.534323Z [HoneyPotSSHTransport,42,192.168.22.133] Command found: uname -a
2026-01-11T11:26:01.978683Z [HoneyPotSSHTransport,42,192.168.22.133] CMD: ls
2026-01-11T11:26:01.979540Z [HoneyPotSSHTransport,42,192.168.22.133] Command found: ls
2026-01-11T11:26:04.640601Z [HoneyPotSSHTransport,42,192.168.22.133] CMD: pwd
2026-01-11T11:26:04.641450Z [HoneyPotSSHTransport,42,192.168.22.133] Command found: pwd
2026-01-11T11:26:11.437856Z [HoneyPotSSHTransport,42,192.168.22.133] CMD: whoami
2026-01-11T11:26:11.439336Z [HoneyPotSSHTransport,42,192.168.22.133] Command found: whoami
2026-01-11T11:26:20.940804Z [HoneyPotSSHTransport,42,192.168.22.133] CMD: cd /etc
2026-01-11T11:26:20.948675Z [HoneyPotSSHTransport,42,192.168.22.133] Command found: cd /etc
2026-01-11T11:26:22.340899Z [HoneyPotSSHTransport,42,192.168.22.133] CMD: ls
2026-01-11T11:26:22.342112Z [HoneyPotSSHTransport,42,192.168.22.133] Command found: ls
2026-01-11T11:26:32.340655Z [HoneyPotSSHTransport,42,192.168.22.133] CMD: cat passwd
2026-01-11T11:26:32.342037Z [HoneyPotSSHTransport,42,192.168.22.133] Command found: cat passwd
2026-01-11T11:26:35.192804Z [HoneyPotSSHTransport,42,192.168.22.133] CMD: exit
2026-01-11T11:26:35.194233Z [HoneyPotSSHTransport,42,192.168.22.133] Command found: exit
2026-01-11T11:26:35.195156Z [twisted.conch.ssh.session#info] exitCode: 0
2026-01-11T11:26:35.195370Z [cowrie.ssh.connection.CowrieSSHConnection#debug] sending request b'exit-status'
2026-01-11T11:26:35.196600Z [HoneyPotSSHTransport,42,192.168.22.133] Closing TTY Log: var/lib/cowrie/tty/de592a092a5
dee26e8b42b45a1c5a627025015d69115524c5a1aba7a8ec8c2a2 after 40.1 seconds
2026-01-11T11:26:35.197910Z [cowrie.ssh.connection.CowrieSSHConnection#info] sending close 0
2026-01-11T11:26:35.198915Z [cowrie.ssh.session.HoneyPotSSHSession#info] remote close
2026-01-11T11:26:35.199769Z [HoneyPotSSHTransport,42,192.168.22.133] Got remote error, code 11 reason: b'disconnecte
d by user'
2026-01-11T11:26:35.200284Z [HoneyPotSSHTransport,42,192.168.22.133] avatar root logging out
2026-01-11T11:26:35.200438Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
```



```
ntrup761×25519-sha512,sntrup761×25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-ni
stp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diff
ie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com;chacha20-poly1305@op
enssh.com,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr;umac-64-etm@openssh.com,uma
c-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":["mlkem768×2
5519-sha256","sntrup761×25519-sha512","sntrup761×25519-sha512@openssh.com","curve25519-sha256","curve25519-sha256@li
bssh.org","ecdh-sha2-nistp256","ecdh-sha2-nistp384","ecdh-sha2-nistp521","diffie-hellman-group-exchange-sha256","dif
fie-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-nistp256-cert-v01@openssh.com","rsa-sha2-512-cert-v01@openssh.com","rsa-sha2-256-cert-v01@openssh.c
om","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-gc
m@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@o
penssh.com"],"langCS":[""],"message":"SSH client hassh fingerprint: eeca2460550b9ded084ecf2f70a75356","sensor":"kali
","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:17:18.366131Z","src_ip":"192.168.22.133",
"session":"9af913246094","protocol":"ssh"}
{"eventid":"cowrie.login.success","username":"root","password":"admin123","message":"login attempt [root/admin123] s
ucceeded","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:17:25.965081Z","s
rc_ip":"192.168.22.133","session":"9af913246094","protocol":"ssh"}
{"eventid":"cowrie.client.size","width":116,"height":44,"message":"Terminal Size: 116 44","sensor":"kali","uuid":"d3
0ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:17:26.016316Z","src_ip":"192.168.22.133","session":"9
af913246094","protocol":"ssh"}
{"eventid":"cowrie.client.var","name":"COLORTERM","value":"truecolor","message":"request_env: COLORTERM=truecolor","
sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:17:26.017098Z","src_ip":"192
.168.22.133","session":"9af913246094","protocol":"ssh"}
{"eventid":"cowrie.client.var","name":"LANG","value":"en_IN","message":"request_env: LANG=en_IN","sensor":"kali","uu
id":"d30ec050-ed64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:17:26.017918Z","src_ip":"192.168.22.133","sess
ion":"9af913246094","protocol":"ssh"}
{"eventid":"cowrie.session.params","arch":"linux-x64-lsb","message":[],"sensor":"kali","uuid":"d30ec050-ed64-11f0-86
bf-000c29b66f1f","timestamp":"2026-01-11T11:17:26.019561Z","src_ip":"192.168.22.133","session":"9af913246094","proto
col":"ssh"}
{"eventid":"cowrie.command.input","input":"whoami","message":"CMD: whoami","sensor":"kali","uuid":"d30ec050-ed64-11f
0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:17:30.765301Z","src_ip":"192.168.22.133","session":"9af913246094","p
rotocol":"ssh"}
{"eventid":"cowrie.command.input","input":"uname -a ","message":"CMD: uname -a ","sensor":"kali","uuid":"d30ec050-ed
64-11f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:17:35.165973Z","src_ip":"192.168.22.133","session":"9af9132460
94","protocol":"ssh"}
{"eventid":"cowrie.command.input","input":"ls","message":"CMD: ls","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-0
00c29b66f1f","timestamp":"2026-01-11T11:17:36.641279Z","src_ip":"192.168.22.133","session":"9af913246094","protocol"
:"ssh"}
{"eventid":"cowrie.command.input","input":"pwd","message":"CMD: pwd","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf
-000c29b66f1f","timestamp":"2026-01-11T11:17:38.594276Z","src_ip":"192.168.22.133","session":"9af913246094","protoco
l":"ssh"}
{"eventid":"cowrie.command.input","input":"cd /etc","message":"CMD: cd /etc","sensor":"kali","uuid":"d30ec050-ed64-1
1f0-86bf-000c29b66f1f","timestamp":"2026-01-11T11:17:43.339086Z","src_ip":"192.168.22.133","session":"9af913246094",
"protocol":"ssh"}
{"eventid":"cowrie.command.input","input":"ls","message":"CMD: ls","sensor":"kali","uuid":"d30ec050-ed64-11f0-86bf-0
00c29b66f1f","timestamp":"2026-01-11T11:17:47.637043Z","src_ip":"192.168.22.133","session":"9af913246094","protocol"
```

7. MITRE ATT&CK Mapping

Several strategies and tactics from the MITRE ATT&CK framework are consistent with the observed attacker behaviour in this project. T1110 (Brute Force), which is frequently used by attackers to obtain initial access, corresponds to the brute-force authentication attempts. The attackers successfully logged in after finding legitimate credentials, which corresponds to T1078 (Valid Accounts).

Attackers used system-level reconnaissance commands including whoami, uname -a, and ls after authentication. T1082 (System Information Discovery) and T1083 (File and Directory Discovery) correspond to this behaviour. These behaviours show that the attacker is trying to comprehend the compromised environment before moving forward.

This mapping shows that even basic brute-force attacks adhere to organized behavioural patterns that are consistent with threat models. By using MITRE ATT&CK, defenders may better understand how an attack fits into the larger kill chain and develop detection and response techniques.

8. Indicators of Compromise (IOCs)

- Suspicious IP addresses
- Repeated login attempts
- Default credential usage
- Enumeration commands

Log analysis revealed a number of compromise indicators. These include the use of well-known default credentials, frequent login failures followed by successful logins, and repeated authentication attempts from the same source IP addresses. Furthermore, post-compromise actions like running reconnaissance commands (whoami, pwd, uname -a, ls) function as a behavioral IOC, signifying that the attacker is enumerating the system. Additionally, the existence of several brief sessions points to automated tools as opposed to human involvement. These IOCs can be used to create detection criteria for SIEM platforms or intrusion detection systems. The time needed to detect and address early-stage incursions can be greatly decreased by keeping an eye out for such patterns in actual situations.

9. Security Insights

This research demonstrates that weak credentials remain one of the most common entry points for attackers. Strong password restrictions and account lockout procedures are crucial, as seen by the quick effectiveness of brute-force attacks.

Furthermore, the reconnaissance activity that has been observed indicates that attackers frequently prioritize comprehending the system before carrying out any harmful acts. Defenders have the chance to identify and stop invasions early thanks to this window. Cowrie and other honeypots are useful instruments for gathering threat intelligence without endangering actual assets. They make it possible for defenders to watch how attackers behave in a secure setting.

10. Limitations

The controlled laboratory setting in which this experiment was carried out may not accurately represent the complexity of attackers in the real world. To reduce unpredictability, the attacks were replicated using well-known techniques and wordlists. There was no actual lateral movement or malware execution. The project accurately depicts early-stage infiltration behaviour in spite of these drawbacks.

11. Future Enhancements

Integrating the honeypot with a SIEM platform, such ELK or Splunk, for real-time viewing and alerting is one of the project's future enhancements. To map attacker sources and spot regional attack trends, GeoIP enrichment can be included. It is possible to imitate file uploads and malware execution by deploying additional honeypot modules. Defensive capabilities would be further improved by automating detection criteria based on observed trends.

12. Conclusion

This project successfully demonstrates the deployment of a Cowrie SSH honeypot, the simulation of multi-source brute-force attacks, and the forensic analysis of captured logs. By observing authentication attempts, session behaviour, and attacker commands, valuable insights into real-world intrusion techniques were obtained. The project reflects practical SOC workflows and defensive monitoring practices. It serves as a strong portfolio artifact for blue team, SOC analyst, and cybersecurity monitoring roles.