INCIDENT REPORT |Oluwaseun Quadri

Title: Network Attack Detection Using Cowrie Honeypot

1. Introduction

This report documents a simulated network attack detected and analyzed using a Cowrie SSH honeypot in a controlled lab environment. The objective of the exercise was to identify malicious scanning activity, capture network traffic, and analyze attacker behavior using standard cybersecurity tools.

2. Lab Environment

The experiment was conducted in a virtualized environment using Oracle VirtualBox.

- **Honeypot System:** Ubuntu Linux
- **Attacker System:** Kali Linux
- **Honeypot Tool:** Cowrie SSH Honeypot
- **Attack Tools:** Nmap, SSH
- **Traffic Capture Tool:** tcpdump (PCAP analyzed with Wireshark)
- **Network Configuration:** VirtualBox NAT / Host-only network
- **Honeypot IP Address:** 192.168.56.102
- **Listening Port:** TCP 2222

3. Incident Description

During the lab exercise, the Cowrie honeypot was configured to listen on TCP port 2222, simulating an SSH service. An attacker machine (Kali Linux) performed reconnaissance activities against the honeypot using Nmap service and version detection scans.

The scanning activity triggered interactions with the honeypot, which logged the connection attempts. Simultaneously, network traffic was captured in PCAP format for further analysis.

4. Attack Detection and Evidence

4.1 Network Scanning

The attacker system executed the following command:

```
nmap -sV -p 2222 192.168.56.102
```

5. Honeypot Logs

Cowrie successfully logged the attack attempt, confirming that the honeypot was active and able to record malicious interactions.

6. Analysis

Analysis of the captured traffic in Wireshark revealed:

- TCP connection attempts to port 2222
- Service/version detection probes from the attacker
- Response packets generated by the Cowrie honeypot

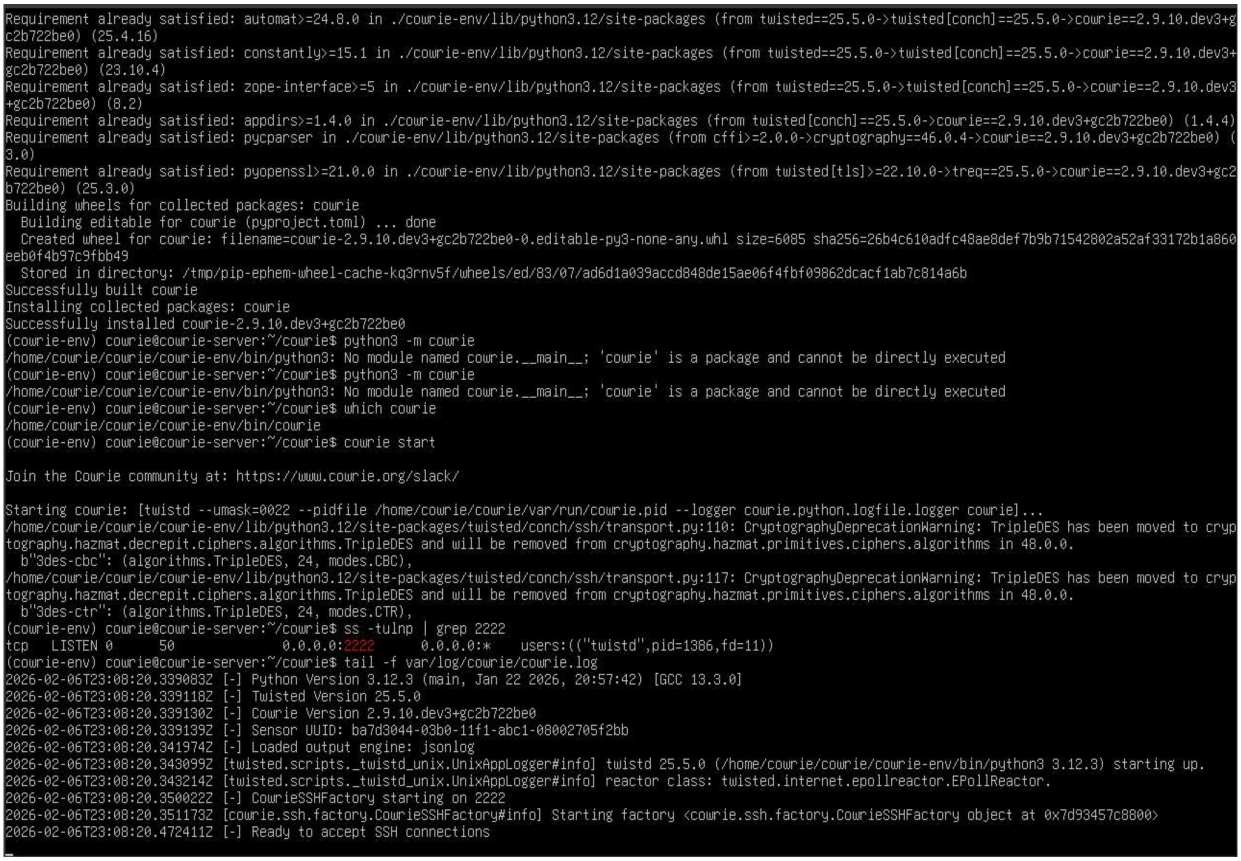
These indicators confirm reconnaissance activity consistent with the early stages of a network attack

7. **Impact Assessment**

No real systems were compromised as the target was a honeypot designed to safely capture malicious behavior. However, the activity demonstrates how exposed SSH services can be discovered and probed by attackers during reconnaissance.

8. Conclusion

This lab successfully demonstrated the use of a Cowrie honeypot for detecting and logging network-based attacks. By combining honeypot technology with packet capture and analysis tools, malicious activity was effectively identified and documented. Such techniques are essential for improving network visibility and strengthening defensive security measures.

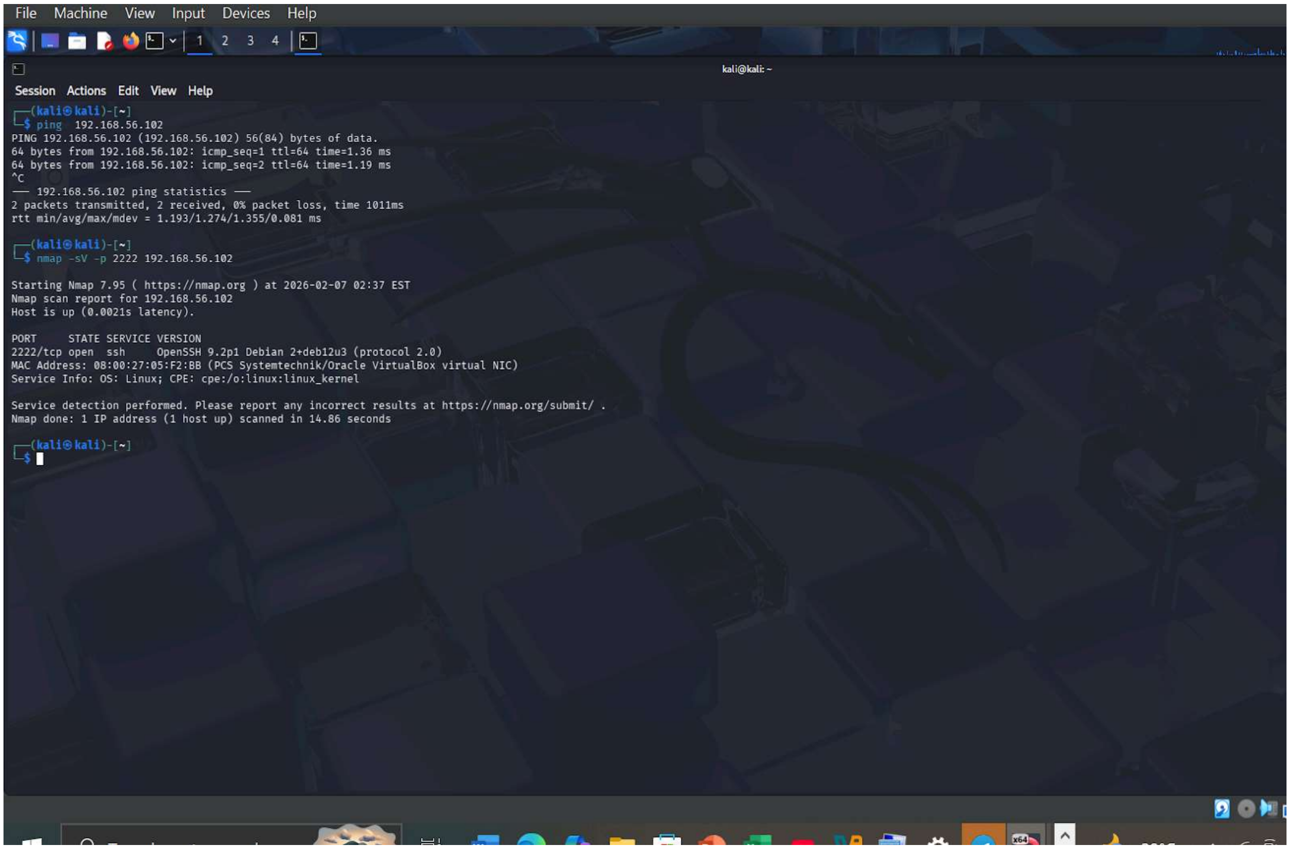


```
Requirement already satisfied: automat>=24.8.0 in ./cowrie-env/lib/python3.12/site-packages (from twisted==25.5.0->twisted[conch]==25.5.0->cowrie==2.9.10.dev3+g
c2b722be0) (25.4.16)
Requirement already satisfied: constantly>=15.1 in ./cowrie-env/lib/python3.12/site-packages (from twisted==25.5.0->twisted[conch]==25.5.0->cowrie==2.9.10.dev3+
gc2b722be0) (23.10.4)
Requirement already satisfied: zope-interface>=5 in ./cowrie-env/lib/python3.12/site-packages (from twisted==25.5.0->twisted[conch]==25.5.0->cowrie==2.9.10.dev3
+gc2b722be0) (8.2)
Requirement already satisfied: appdirs>=1.4.0 in ./cowrie-env/lib/python3.12/site-packages (from twisted[conch]==25.5.0->cowrie==2.9.10.dev3+gc2b722be0) (1.4.4)
Requirement already satisfied: pycparser in ./cowrie-env/lib/python3.12/site-packages (from cffi>=2.0.0->cryptography==46.0.4->cowrie==2.9.10.dev3+gc2b722be0) (
3.0)
Requirement already satisfied: pyopenssl>=21.0.0 in ./cowrie-env/lib/python3.12/site-packages (from twisted[tls]>=22.10.0->treq==25.5.0->cowrie==2.9.10.dev3+gc2
b722be0) (25.3.0)
Building wheels for collected packages: cowrie
  Building editable for cowrie (pyproject.toml) ... done
  Created wheel for cowrie: filename=cowrie-2.9.10.dev3+gc2b722be0-0.editable-py3-none-any.whl size=6085 sha256=26b4c610adfc48ae8def7b9b71542802a52af33172b1a860
eeb0f4b97c9fbb49
  Stored in directory: /tmp/pip-ephem-wheel-cache-kq3rnv5f/wheels/ed/83/07/ad6d1a039accd848de15ae06f4fbf09862dcacf1ab7c814a6b
Successfully built cowrie
Installing collected packages: cowrie
Successfully installed cowrie-2.9.10.dev3+gc2b722be0
(cowrie-env) cowrie@cowrie-server:~/cowrie$ python3 -m cowrie
/home/cowrie/cowrie/cowrie-env/bin/python3: No module named cowrie.__main__; 'cowrie' is a package and cannot be directly executed
(cowrie-env) cowrie@cowrie-server:~/cowrie$ python3 -m cowrie
/home/cowrie/cowrie/cowrie-env/bin/python3: No module named cowrie.__main__; 'cowrie' is a package and cannot be directly executed
(cowrie-env) cowrie@cowrie-server:~/cowrie$ which cowrie
/home/cowrie/cowrie/cowrie-env/bin/cowrie
(cowrie-env) cowrie@cowrie-server:~/cowrie$ cowrie start

Join the Cowrie community at: https://www.cowrie.org/slack/

Starting cowrie: [twistd --umask=0022 --pidfile /home/cowrie/cowrie/var/run/cowrie.pid --logger cowrie.python.logfile.logger cowrie]...
/home/cowrie/cowrie/cowrie-env/lib/python3.12/site-packages/twisted/conch/ssh/transport.py:110: CryptographyDeprecationWarning: TripleDES has been moved to cryp
tography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/home/cowrie/cowrie/cowrie-env/lib/python3.12/site-packages/twisted/conch/ssh/transport.py:117: CryptographyDeprecationWarning: TripleDES has been moved to cryp
tography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),
(cowrie-env) cowrie@cowrie-server:~/cowrie$ ss -tulnp | grep 2222
tcp   LISTEN 0      50             0.0.0.0:2222      0.0.0.0:*    users:(("twistd",pid=1386,fd=11))
(cowrie-env) cowrie@cowrie-server:~/cowrie$ tail -f var/log/cowrie/cowrie.log
2026-02-06T23:08:20.339083Z [-] Python Version 3.12.3 (main, Jan 22 2026, 20:57:42) [GCC 13.3.0]
2026-02-06T23:08:20.339118Z [-] Twisted Version 25.5.0
2026-02-06T23:08:20.339130Z [-] Cowrie Version 2.9.10.dev3+gc2b722be0
2026-02-06T23:08:20.339139Z [-] Sensor UUID: ba7d3044-03b0-11f1-abc1-08002705f2bb
2026-02-06T23:08:20.341974Z [-] Loaded output engine: jsonlog
2026-02-06T23:08:20.343099Z [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 25.5.0 (/home/cowrie/cowrie/cowrie-env/bin/python3 3.12.3) starting up.
2026-02-06T23:08:20.343214Z [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor.
2026-02-06T23:08:20.350022Z [-] CowrieSSHFactory starting on 2222
2026-02-06T23:08:20.351173Z [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7d93457c8800>
2026-02-06T23:08:20.472411Z [-] Ready to accept SSH connections
```

Fig.1 Image indicating cowrie starting



File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
Session Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ping  192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=1.36 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=1.19 ms
^C
── 192.168.56.102 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1011ms
rtt min/avg/max/mdev = 1.193/1.274/1.355/0.081 ms

┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 2222 192.168.56.102

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-07 02:37 EST
Nmap scan report for 192.168.56.102
Host is up (0.0021s latency).

PORT     STATE SERVICE VERSION
2222/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
MAC Address: 08:00:27:05:F2:BB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.86 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Fig.2 image indicating Nmap scan result on kali linux