**Created By: Dinindu Ganganath Abeysuriya**
**On: 23rd July 2025**

## 01) Local HoneyPot setup,

**Step 01: Update UBUNTU:** sudo apt update && sudo apt upgrade -y

**Step 02: Install Required Dependencies:**

sudo apt install -y git python3-venv python3-dev libssl-dev libffi-dev build-essential libpython3-dev python3-pip virtualenv

**Step 03: Create User:** sudo adduser --disabled-password cowrie

**Step 04: Download Cowrie:**

- sudo su - cowrie
- git clone https://github.com/cowrie/cowrie.git
- cd cowrie

**Step 05: Set Up Python Virtual Environment:**

- python3 -m venv cowrie-env
- source cowrie-env/bin/activate
- pip install --upgrade pip
- pip install -r requirements.txt

**Step 06: Configure Cowrie to Use Port 2222 (instead of port 22):**

Cowrie runs on port **2222** by default. Let's leave it that way for now.

**Step 07: Enable Cowrie to Start:** cp etc/cowrie.cfg.dist etc/cowrie.cfg

**Step 08: To Test;**

**Start cowrie:** bin/cowrie start
**Stop cowrie:** bin/cowrie stop (execute this when it's time to stop the cowrie firewall, **not** right after the command execution.)

## 02) Expose Honeypot to Internet (External Attackers),

**Step 01: Sign Up and Get ngrok Auth Token:**

**Sample token example: 2LhRjFz1lAbcK8YcXXXXXXXXXXX**

**Step 02: Install ngrok,**

- Download ngrok directly from the new source
  wget https://ngrok-agent.s3.amazonaws.com/ngrok.asc -O - | sudo tee /etc/apt/trusted.gpg.d/ngrok.asc >/dev/null

- Add ngrok to your APT sources
  echo "deb https://ngrok-agent.s3.amazonaws.com buster main" | sudo tee /etc/apt/sources.list.d/ngrok.list

- Update package list
  sudo apt update

- Install ngrok
  sudo apt install ngrok

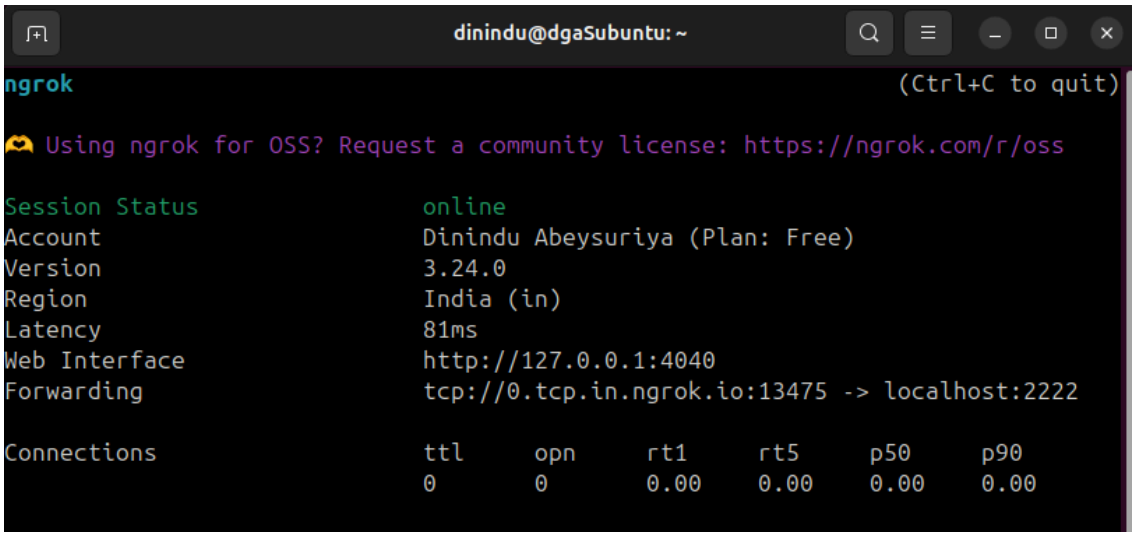
**Step 3: Add "ngrok" Authtoken,**

- ngrok config add-authtoken 2LhRjFz1lAbcK8Ycxxxxxxxxxxxxxxxxxxxx

**Step 4: Expose Cowrie SSH Port to the Internet,**

- Forward "cowrie" with "ngrok": ngrok tcp 2222

  Then the **ngrok status dashboard** will open in the current terminal,



## 03) Expose Honeypot to Internet (External Attackers),

**Step 01: Monitor Attacks Live,**
(In a new terminal)

```
                                    sudo su - cowrie
                                    cd ~/cowrie
cowrie@dgaSubuntu:~/cowrie$ nano monitor_attackers.sh
```

(Past this script)

```
—----------------------------------------------------------------------------------------------
#!/bin/bash

LOG_FILE="var/log/cowrie/cowrie.log"
OUTPUT_LOG="attackers_info.log"
SEEN_IPS=()

echo "[*] Monitoring $LOG_FILE for new attackers..."
echo "[*] Output will be saved in $OUTPUT_LOG"

tail -F "$LOG_FILE" | while read -r line; do
   if echo "$line" | grep -q "login attempt"; then
      # Extract IP address from the log line
      IP=$(echo "$line" | grep -oE '[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+')

      if [[ -n "$IP" && ! " ${SEEN_IPS[*]} " =~ " $IP " ]]; then
         SEEN_IPS+=("$IP")
         TIMESTAMP=$(date "+%Y-%m-%d %H:%M:%S")
         echo "[+] Detected new attacker IP: $IP at $TIMESTAMP"
         echo "$TIMESTAMP - $IP" >> "$OUTPUT_LOG"
      fi
   fi
done
—----------------------------------------------------------------------------------------------
```

```
cowrie@dgaSubuntu:~/cowrie$ chmod +x monitor_attackers.sh
cowrie@dgaSubuntu:~/cowrie$ ./monitor_attackers.sh
```

(now the monitoring process will start and it will look something like this)

```
cowrie@dgaSubuntu:~/cowrie$ ./monitor_attackers.sh
[*] Monitoring var/log/cowrie/cowrie.log for new attackers...
[*] Output will be saved in attackers_info.log
```

(If some threats or unauthorized access it directed the list will be updated on real time)

```
cowrie@dgaSubuntu:~/cowrie$ ./monitor_attackers.sh
[*] Monitoring var/log/cowrie/cowrie.log for new attackers...
[*] Output will be saved in attackers_info.log
[+] Detected new attacker IP: 127.0.0.1 at 2025-07-23 12:26:39
```

**:** (ex of a captured line)

## Additional,

## 04) Triggering a simulation attack,

If no attacks or intruders were detected, we can simulate a sample testing attack to make sure the cowrie honeypot is working and capturing attacker data.

**Steps,**

Open a new terminal and do a **ssh** scan using the command bellow,

```
ssh root@127.0.0.1 -p 2222
```

This will execute the script within "monitor_attackers.sh" and results in capturing attacker's data, it will be shown in the previous terminal [terminal in **(03)** part] as bellow,

```
[+] Detected new attacker IP: 127.0.0.1 at 2025-07-23 12:26:39
…….
….
```

**…… END ……**