Raspberry Pi Cowrie Honeypot + Cloudflare Tunnel Setup Guide

1. Install Cowrie

- Create cowrie user and install prerequisites.

- Clone Cowrie into /home/cowrie/cowrie.

- Create virtualenv and install requirements.

- Copy cowrie.cfg.dist to cowrie.cfg.

- Enable Cowrie as a systemd service:

sudo systemctl enable --now cowrie

2. Confirm Cowrie is running

- Check service:

sudo systemctl status cowrie

- Check listening port:

sudo ss -tulpn | grep 2222

3. Install Cloudflared

- Download cloudflared and install:

sudo apt install cloudflared or manual deb install.

- Log into Cloudflare:

cloudflared tunnel login

- Create tunnel:

cloudflared tunnel create honeypot

- Copy credentials to system directory:

sudo mkdir -p /etc/cloudflared

sudo cp ~/.cloudflared/* /etc/cloudflared/

sudo chown root:root /etc/cloudflared/*

sudo chmod 600 /etc/cloudflared/*

4. Create Cloudflare Tunnel config

Create /etc/cloudflared/config.yml with:

tunnel:

credentials-file: /etc/cloudflared/.json

ingress:

- hostname: honeypot.

service: ssh://localhost:2222

- service: http_status:404

Restart cloudflared:

sudo systemctl restart cloudflared

Check status:

systemctl status cloudflared

5. Cloudflare DNS

- Automatically created by tunnel route:

honeypot. CNAME .cfargotunnel.com

6. Cloudflare Zero Trust SSH Browser App

- Create new application → SSH app.

- Set domain to honeypot..

- Use One-Time PIN as login method.

- No client installation required for students.

- Ensure the app is linked to the same hostname as tunnel.

7. Verify end-to-end

Local test:

ssh -p 2222 test@localhost

Cloudflare browser test:

- Visit https://honeypot..

- Enter username → forwarded to Cowrie.

- Commands show up in Cowrie logs.

8. Cowrie Logging

Active log directory:

/home/cowrie/cowrie/var/log/cowrie/

Live logs:

sudo tail -f /home/cowrie/cowrie/var/log/cowrie/cowrie.log

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

9. Protect the real Pi

- Change real user password:

passwd

- Disable password auth for real SSH:

Edit /etc/ssh/sshd_config:

PasswordAuthentication no

PermitRootLogin no

sudo systemctl restart ssh

- Use SSH keys for your own access.

10. Safe shutdown

- Turn off Pi:

sudo shutdown now

- Cloudflare tunnel goes offline automatically, site becomes inaccessible.

11. On next boot

Everything starts automatically:

- Wi-Fi/Ethernet

- Cowrie service

- Cloudflared tunnel

Students reconnect normally.