

# Cowrie Honeypot

## Complete Installation & Testing Guide

Prepared for: Red Team Lab / Threat Intelligence Testing

### 1. Installation & Setup

```
sudo apt update && sudo apt upgrade -y
sudo apt install -y python3 python3-pip python3-venv git libssl-dev libffi-dev build-essential authbind

sudo adduser --disabled-password --gecos "" cowrie
sudo su - cowrie

git clone https://github.com/cowrie/cowrie.git
cd cowrie

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

cp etc/cowrie.cfg.dist etc/cowrie.cfg

sudo touch /etc/authbind/byport/22
sudo chown cowrie:cowrie /etc/authbind/byport/22
sudo chmod 500 /etc/authbind/byport/22

source cowrie-env/bin/activate
bin/cowrie start
```

### 2. Module Testing Checklist

No.	Module	Service/Protocol	Test Command
1	SSH	SSH (22/tcp)	ssh root@<IP> -p 22
2	Telnet	Telnet (23/tcp)	telnet <IP> 23
3	Session Recording	-	ls var/lib/cowrie/tty
4	Credential Logging	-	cat var/log/cowrie/cowrie.json   grep login
5	File Upload	SCP/SFTP	scp -P 22 file root@<IP>:/tmp/
6	File Download	HTTP/FTP	wget http://example.com/file
7	Command Emulation	-	uname -a, ls -la, ps aux
8	Virtual Filesystem	-	cd /etc; ls
9	SSH Proxy Mode	-	Configure in etc/cowrie.cfg
10	JSON Logging	-	tail -f var/log/cowrie/cowrie.json
11	Malware Collection	-	scp malware.sh root@<IP>:/tmp/
12	Plugins	-	Elastic, Docker, Slack notification

### 3. Monitoring & Operations

```
ps aux | grep cowrie | grep -v grep
sudo lsof -i -n -P | grep cowrie
tail -f var/log/cowrie/cowrie.log
```

Malware sample storage: var/lib/cowrie/downloads/

### 4. Notes

- Do NOT run Cowrie as root in production. Always create an unprivileged user.
- Test in isolated VM or container environment.
- Combine Cowrie logs with ELK / Wazuh for advanced threat intelligence workflows.