Threat Hunting

HW12

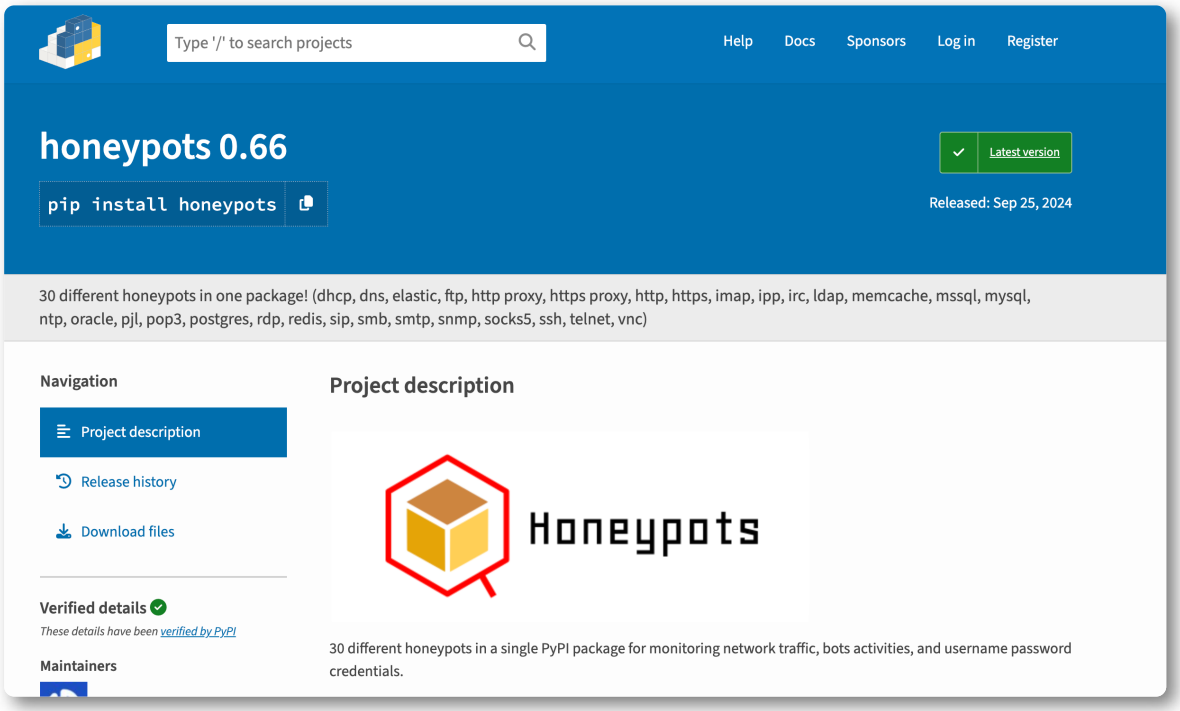
Name: 劉定睿 ID: M11409313

Date: 2025-12-08

目錄

Lightweight Multi-Service Honeypot: honeypots Package

- Find the `honeypots` package in the official python package website.



- use `pip install` to install it.

```
┌──$ pip install honeypot --break-system-packages
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: honeypot in ./.local/lib/python3.13/site-packages (0.1.1)
Requirement already satisfied: flask in /usr/lib/python3/dist-packages (from honeypot) (3.1.2)
Requirement already satisfied: prompt-toolkit in /usr/lib/python3/dist-packages (from honeypot) (3.0.52)
Requirement already satisfied: rich in /usr/lib/python3/dist-packages (from honeypot) (13.9.4)
Requirement already satisfied: blinker>=1.9.0 in /usr/lib/python3/dist-packages (from flask->honeypot) (
1.9.0)
Requirement already satisfied: click>=8.1.3 in /usr/lib/python3/dist-packages (from flask->honeypot) (8.
1.8)
Requirement already satisfied: itsdangerous>=2.2.0 in /usr/lib/python3/dist-packages (from flask->honeyp
ot) (2.2.0)
Requirement already satisfied: jinja2>=3.1.2 in /usr/lib/python3/dist-packages (from flask->honeypot) (3
.1.6)
Requirement already satisfied: markupsafe>=2.1.1 in /usr/lib/python3/dist-packages (from flask->honeypot
) (3.0.2)
Requirement already satisfied: werkzeug>=3.1.0 in /usr/lib/python3/dist-packages (from flask->honeypot)
(3.1.3)
Requirement already satisfied: wcwidth in /usr/lib/python3/dist-packages (from prompt-toolkit->honeypot)
 (0.2.13)
Requirement already satisfied: markdown-it-py>=2.2.0 in /usr/lib/python3/dist-packages (from rich->honey
pot) (3.0.0)
Requirement already satisfied: pygments<3.0.0,>=2.13.0 in /usr/lib/python3/dist-packages (from rich->hon
eypot) (2.18.0)
Requirement already satisfied: mdurl~=0.1 in /usr/lib/python3/dist-packages (from markdown-it-py>=2.2.0-
>rich->honeypot) (0.1.2)
```

- use python to run the module. And open port `8080` http server on the local.

```
└─$ python3 -m honeypots --setup http --port 8080
/[redacted]/lib/python3.13/site-packages/paramiko/pkey.py:82: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  "cipher": algorithms.TripleDES,
/[redacted]/lib/python3.13/site-packages/paramiko/transport.py:256: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  "class": algorithms.TripleDES,
[INFO] For updates, check https://github.com/qeeqbox/honeypots
[WARNING] Using system or well-known ports requires higher privileges (E.g. sudo -E)
[INFO] Use [Enter] to exit or python3 -m honeypots --kill
[INFO] Parsing honeypot [normal]
{"action": "process", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "0.0.0.0", "src_port": "8080", "status": "success", "timestamp": "2025-12-05T04:55:32.270731"}
[INFO] servers http running...
[INFO] Everything looks good!
```

- use `dirb` to scan and enumeration the directory.

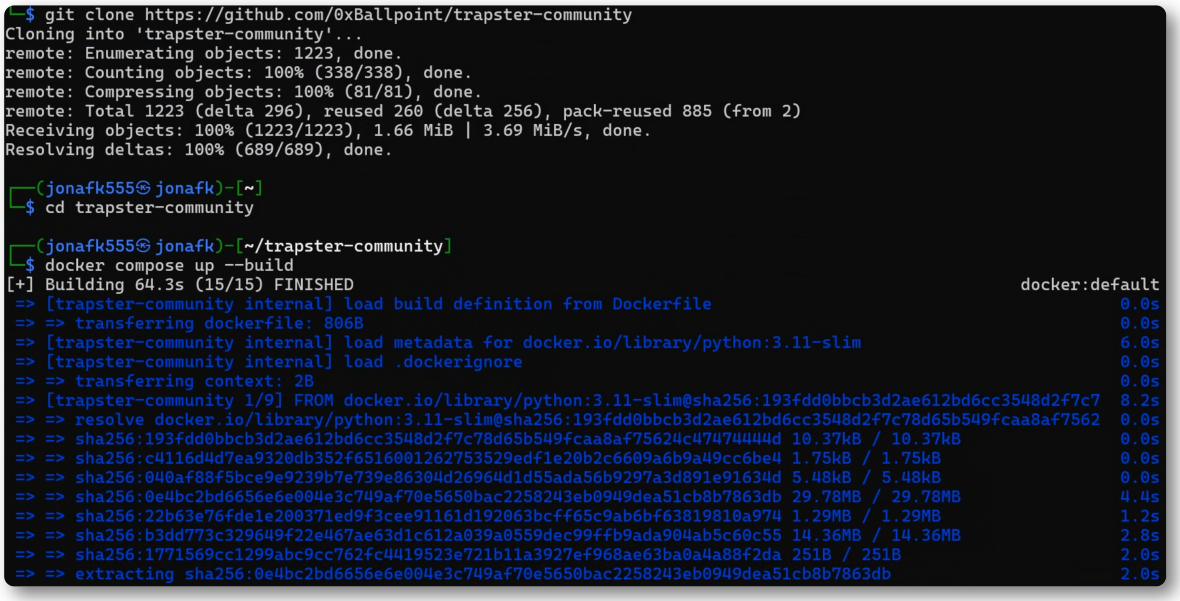
```
└─$ dirb http://0.0.0.0:8080 -w

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Dec  5 12:58:18 2025
URL_BASE: http://0.0.0.0:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://0.0.0.0:8080/ ----
(!) WARNING: All responses for this directory seem to be CODE = 500.
    (Use mode '-w' if you want to scan it anyway)
(!) WARNING: All responses for this directory seem to be CODE = 500.
    (Use mode '-w' if you want to scan it anyway)
(!) WARNING: All responses for this directory seem to be CODE = 500.
    (Use mode '-w' if you want to scan it anyway)
(!) WARNING: All responses for this directory seem to be CODE = 500.
    (Use mode '-w' if you want to scan it anyway)
(!) WARNING: All responses for this directory seem to be CODE = 500.
    (Use mode '-w' if you want to scan it anyway)
(!) WARNING: All responses for this directory seem to be CODE = 500.
    (Use mode '-w' if you want to scan it anyway)
(!) WARNING: All responses for this directory seem to be CODE = 500.
    (Use mode '-w' if you want to scan it anyway)
(!) WARNING: All responses for this directory seem to be CODE = 500.
    (Use mode '-w' if you want to scan it anyway)
(!) WARNING: All responses for this directory seem to be CODE = 500.
    (Use mode '-w' if you want to scan it anyway)
(!) WARNING: All responses for this directory seem to be CODE = 500.
```

- check the honeypot log in the server.

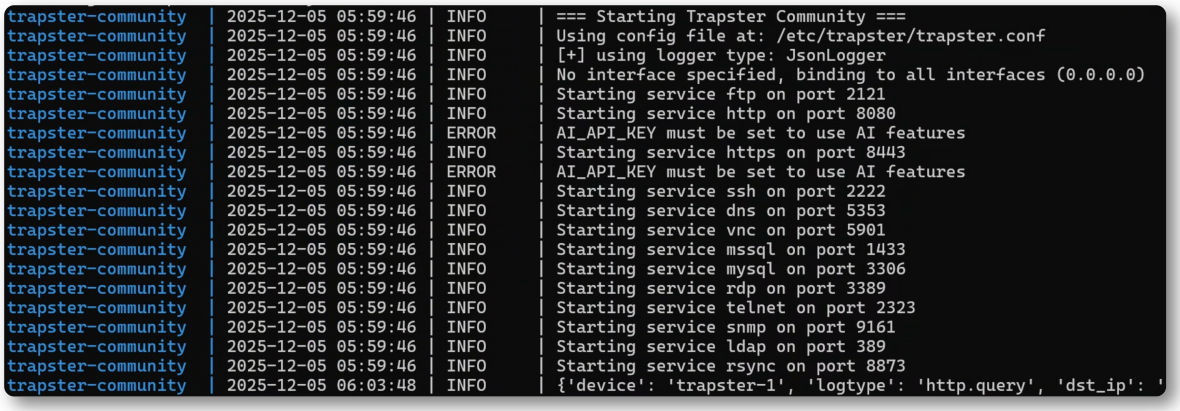

```
{"action": "GET", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "src_por
t": "54076", "timestamp": "2025-12-05T04:58:21.076318"}
{"action": "connection", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "
src_port": "54076", "timestamp": "2025-12-05T04:58:21.076955"}
{"action": "GET", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "src_por
t": "54076", "timestamp": "2025-12-05T04:58:21.077075"}
{"action": "connection", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "
src_port": "54076", "timestamp": "2025-12-05T04:58:21.078333"}
{"action": "GET", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "src_por
t": "54076", "timestamp": "2025-12-05T04:58:21.078503"}
{"action": "connection", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "
src_port": "54076", "timestamp": "2025-12-05T04:58:21.079486"}
{"action": "GET", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "src_por
t": "54076", "timestamp": "2025-12-05T04:58:21.079670"}
{"action": "connection", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "
src_port": "54076", "timestamp": "2025-12-05T04:58:21.080626"}
{"action": "GET", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "src_por
t": "54076", "timestamp": "2025-12-05T04:58:21.080805"}
{"action": "connection", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "
src_port": "54076", "timestamp": "2025-12-05T04:58:21.081861"}
{"action": "GET", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "src_por
t": "54076", "timestamp": "2025-12-05T04:58:21.081998"}
{"action": "connection", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "
src_port": "54076", "timestamp": "2025-12-05T04:58:21.083011"}
{"action": "GET", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "src_por
t": "54076", "timestamp": "2025-12-05T04:58:21.083151"}
{"action": "connection", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "
src_port": "54076", "timestamp": "2025-12-05T04:58:21.084323"}
{"action": "GET", "dest_ip": "0.0.0.0", "dest_port": "8080", "server": "http_server", "src_ip": "127.0.0.1", "src_por
t": "54076", "timestamp": "2025-12-05T04:58:21.084548"}
```

Configurable Deception Platform: Trapster Community

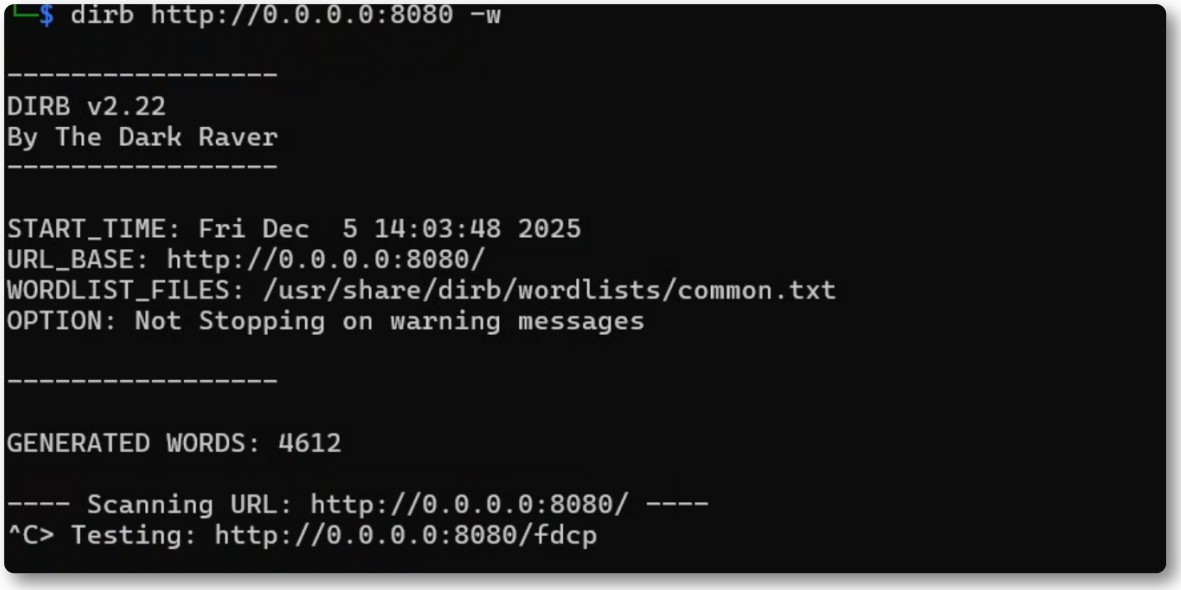
- `git clone` the trapster repo to the local.



- after use docker to run the dockerfile. We can see that there's many different kind of service were been activated.



- use `dirb` to generate the scanning traffic.



- Later, check the log in the local server. We can see more details such as: user-agent, target(directory), http request header, comparing with `honeypots`.