

Threat Hunting

HW12

Name: 劉定睿 ID: M11409313

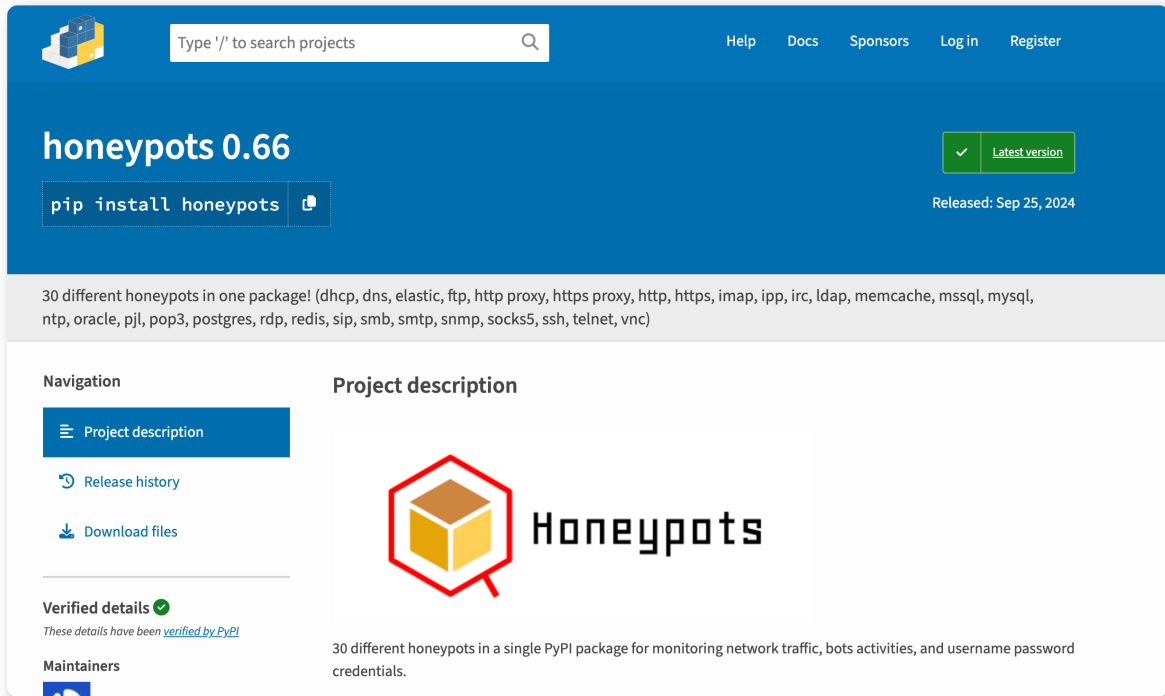
Date: 2025-12-08

目錄

- [目錄](#)
 - [Lightweight Multi-Service Honeypot: honeypots Package](#)
 - [Configurable Deception Platform: Trapster Community](#)

Lightweight Multi-Service Honeypot: honeypots Package

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



The screenshot shows the PyPI page for the `honeypots` package. At the top, there is a search bar with the text "Type '/' to search projects" and a search icon. To the right of the search bar are links for "Help", "Docs", "Sponsors", "Log in", and "Register". Below the search bar, the package name "honeypots 0.66" is displayed in large white text on a blue background. To the right of the package name is a green button with a checkmark and the text "Latest version". Below the package name is a button with the text "pip install honeypots" and a share icon. To the right of this button is the text "Released: Sep 25, 2024". Below the package name and button is a grey box containing the text: "30 different honeypots in one package! (dhcp, dns, elastic, ftp, http proxy, https proxy, http, https, imap, ipp, irc, ldap, memcache, mssql, mysql, ntp, oracle, pjl, pop3, postgres, rdp, redis, sip, smb, smtp, snmp, socks5, ssh, telnet, vnc)". Below this is a navigation menu with "Project description" selected. To the right of the navigation menu is the "Project description" section, which features the "Honeypots" logo (a yellow cube with a red outline) and the text "30 different honeypots in a single PyPI package for monitoring network traffic, bots activities, and username password credentials." Below the logo and text is a "Verified details" section with a green checkmark and the text "These details have been verified by PyPI". Below the verified details is a "Maintainers" section with a small profile picture.

- 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->honeypot) (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->honeypot) (3.0.0)
Requirement already satisfied: pygments<3.0.0,>=2.13.0 in /usr/lib/python3/dist-packages (from rich->honeypot) (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)
```


- 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_port": "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_port": "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_port": "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_port": "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_port": "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_port": "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_port": "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_port": "54076", "timestamp": "2025-12-05T04:58:21.084548" }
```

Configurable Deception Platform: Trapster Community

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

```
└─$ git clone https://github.com/0xBallpoint/trapster-community
Cloning into 'trapster-community'...
remote: Enumerating objects: 1223, done.
remote: Counting objects: 100% (338/338), done.
remote: Compressing objects: 100% (81/81), done.
remote: Total 1223 (delta 296), reused 260 (delta 256), pack-reused 885 (from 2)
Receiving objects: 100% (1223/1223), 1.66 MiB | 3.69 MiB/s, done.
Resolving deltas: 100% (689/689), done.

jonafk555@jonafk- [~]
└─$ cd trapster-community

jonafk555@jonafk- [~/trapster-community]
└─$ docker compose up --build
[+] Building 64.3s (15/15) FINISHED                                docker:default
=> [trapster-community internal] load build definition from Dockerfile                                0.0s
=> => transferring dockerfile: 806B                                                                    0.0s
=> [trapster-community internal] load metadata for docker.io/library/python:3.11-slim                    6.0s
=> [trapster-community internal] load .dockerignore                                                       0.0s
=> => transferring context: 2B                                                                              0.0s
=> [trapster-community 1/9] FROM docker.io/library/python:3.11-slim@sha256:193fdd0bbcb3d2ae612bd6cc3548d2f7c7  8.2s
=> => resolve docker.io/library/python:3.11-slim@sha256:193fdd0bbcb3d2ae612bd6cc3548d2f7c78d65b549fcaa8af7562  0.0s
=> => sha256:193fdd0bbcb3d2ae612bd6cc3548d2f7c78d65b549fcaa8af75624c47474444d 10.37kB / 10.37kB          0.0s
=> => sha256:c4116d4d7ea9320db352f6516001262753529edf1e20b2c6609a6b9a49cc6be4 1.75kB / 1.75kB          0.0s
=> => sha256:040af88f5bce9e9239b7e739e86304d26964d1d55ada56b9297a3d891e91634d 5.48kB / 5.48kB          0.0s
=> => sha256:0e4bc2bd6656e6e004e3c749af70e5650bac2258243eb0949dea51cb8b7863db 29.78MB / 29.78MB        4.4s
=> => sha256:22b63e76fde1e200371ed9f3cee91161d192063bcff65c9ab6bf63819810a974 1.29MB / 1.29MB         1.2s
=> => sha256:b3dd773c329649f22e467ae63d1c612a039a05592dec99fffb9ada904ab5c60c55 14.36MB / 14.36MB       2.8s
=> => sha256:1771569cc1299abc9cc762fc4419523e721b11a3927ef968ae63ba0a4a88f2da 251B / 251B             2.0s
=> => extracting sha256:0e4bc2bd6656e6e004e3c749af70e5650bac2258243eb0949dea51cb8b7863db 2.0s
```

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

```
trapster-community | 2025-12-05 05:59:46 | INFO | === Starting Trapster Community ===
trapster-community | 2025-12-05 05:59:46 | INFO | Using config file at: /etc/trapster/trapster.conf
trapster-community | 2025-12-05 05:59:46 | INFO | [+] using logger type: JsonLogger
trapster-community | 2025-12-05 05:59:46 | INFO | No interface specified, binding to all interfaces (0.0.0.0)
trapster-community | 2025-12-05 05:59:46 | INFO | Starting service ftp on port 2121
trapster-community | 2025-12-05 05:59:46 | INFO | Starting service http on port 8080
trapster-community | 2025-12-05 05:59:46 | ERROR | AI_API_KEY must be set to use AI features
trapster-community | 2025-12-05 05:59:46 | INFO | Starting service https on port 8443
trapster-community | 2025-12-05 05:59:46 | ERROR | AI_API_KEY must be set to use AI features
trapster-community | 2025-12-05 05:59:46 | INFO | Starting service ssh on port 2222
trapster-community | 2025-12-05 05:59:46 | INFO | Starting service dns on port 5353
trapster-community | 2025-12-05 05:59:46 | INFO | Starting service vnc on port 5901
trapster-community | 2025-12-05 05:59:46 | INFO | Starting service mssql on port 1433
trapster-community | 2025-12-05 05:59:46 | INFO | Starting service mysql on port 3306
trapster-community | 2025-12-05 05:59:46 | INFO | Starting service rdp on port 3389
trapster-community | 2025-12-05 05:59:46 | INFO | Starting service telnet on port 2323
trapster-community | 2025-12-05 05:59:46 | INFO | Starting service snmp on port 9161
trapster-community | 2025-12-05 05:59:46 | INFO | Starting service ldap on port 389
trapster-community | 2025-12-05 05:59:46 | INFO | Starting service rsync on port 8873
trapster-community | 2025-12-05 06:03:48 | INFO | {'device': 'trapster-1', 'logtype': 'http.query', 'dst_ip': '}
```

- use `dirb` to generate the scanning traffic.

```
└─$ dirb http://0.0.0.0:8080 -w

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

START_TIME: Fri Dec  5 14:03:48 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/ ----
^C> Testing: http://0.0.0.0:8080/fdcp
```

- 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`.

```
trapster-community | 2025-12-05 06:03:48 | INFO | {'device': 'trapster-1', 'logtype': 'http.query', 'dst_ip': '127.0.0.1', 'dst_port': 8080, 'src_ip': '127.0.0.1', 'src_port': 42986, 'timestamp': '2025-12-05 06:03:48.956099', 'data': '', 'extra': {'skin': 'demo_api', 'method': 'GET', 'target': '/frand2', 'headers': {'host': '0.0.0.0:8080', 'user-agent': 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)', 'accept': '*/*'}, 'status_code': 404}}
trapster-community | 2025-12-05 06:03:48 | INFO | {'device': 'trapster-1', 'logtype': 'http.query', 'dst_ip': '127.0.0.1', 'dst_port': 8080, 'src_ip': '127.0.0.1', 'src_port': 42986, 'timestamp': '2025-12-05 06:03:48.960456', 'data': '', 'extra': {'skin': 'demo_api', 'method': 'GET', 'target': '/.bash_history', 'headers': {'host': '0.0.0.0:8080', 'user-agent': 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)', 'accept': '*/*'}, 'status_code': 404}}
trapster-community | 2025-12-05 06:03:48 | INFO | {'device': 'trapster-1', 'logtype': 'http.query', 'dst_ip': '127.0.0.1', 'dst_port': 8080, 'src_ip': '127.0.0.1', 'src_port': 42986, 'timestamp': '2025-12-05 06:03:48.964279', 'data': '', 'extra': {'skin': 'demo_api', 'method': 'GET', 'target': '/.bashrc', 'headers': {'host': '0.0.0.0:8080', 'user-agent': 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)', 'accept': '*/*'}, 'status_code': 404}}
trapster-community | 2025-12-05 06:03:48 | INFO | {'device': 'trapster-1', 'logtype': 'http.query', 'dst_ip': '127.0.0.1', 'dst_port': 8080, 'src_ip': '127.0.0.1', 'src_port': 42986, 'timestamp': '2025-12-05 06:03:48.967724', 'data': '', 'extra': {'skin': 'demo_api', 'method': 'GET', 'target': '/.cache', 'headers': {'host': '0.0.0.0:8080', 'user-agent': 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)', 'accept': '*/*'}, 'status_code': 404}}
trapster-community | 2025-12-05 06:03:48 | INFO | {'device': 'trapster-1', 'logtype': 'http.query', 'dst_ip': '127.0.0.1', 'dst_port': 8080, 'src_ip': '127.0.0.1', 'src_port': 42986, 'timestamp': '2025-12-05 06:03:48.970682', 'data': '', 'extra': {'skin': 'demo_api', 'method': 'GET', 'target': '/.config', 'headers': {'host': '0.0.0.0:8080', 'user-agent': 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)', 'accept': '*/*'}, 'status_code': 404}}
trapster-community | 2025-12-05 06:03:48 | INFO | {'device': 'trapster-1', 'logtype': 'http.query', 'dst_ip': '127.0.0.1', 'dst_port': 8080, 'src_ip': '127.0.0.1', 'src_port': 42986, 'timestamp': '2025-12-05 06:03:48.973876', 'data': '', 'extra': {'skin': 'demo_api', 'method': 'GET', 'target': '/.cvs', 'headers': {'host': '0.0.0.0:8080', 'user-agent': 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)', 'accept': '*/*'}, 'status_code': 404}}
trapster-community | 2025-12-05 06:03:48 | INFO | {'device': 'trapster-1', 'logtype': 'http.query', 'dst_ip': '127.0.0.1', 'dst_port': 8080, 'src_ip': '127.0.0.1', 'src_port': 42986, 'timestamp': '2025-12-05 06:03:48.976892', 'data': '', 'extra': {'skin': 'demo_api', 'method': 'GET', 'target': '/.cvsignore', 'headers': {'host': '0.0.0.0:8080', 'user-agent': 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)', 'accept': '*/*'}, 'status_code': 404}}
```