



Honeypot Deployment & Analysis with T-Pot

This capstone explores honeypot deployment using T-Pot for cybersecurity threat detection.

M by Mauricio Spadoni



What Is a Honeytrap?

Definition

Decoy system designed to attract and analyze attacker behavior.

Purpose

Detect, delay, and study cyber attacks deeply.

Types

- Low-interaction (e.g., Cowrie)
- High-interaction

Introduction to T-Pot

All-in-One Platform

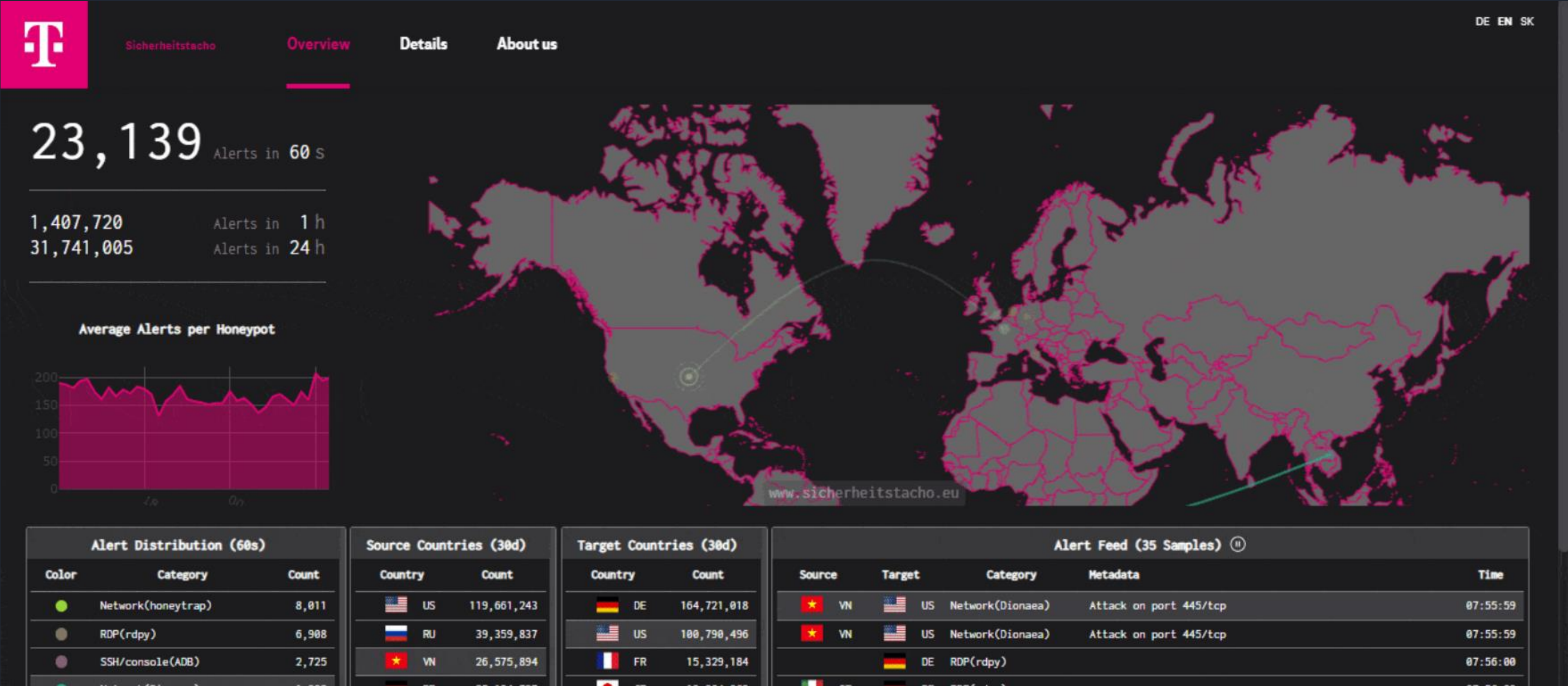
From Deutsche Telekom, integrates multiple honeypots and analytics.

Core Components

Combines sensors with ELK stack: Elastic, Logstash, Kibana.

Use Case

Detect threats and analyze malicious traffic patterns.



Architecture of T-Pot

Container-Based

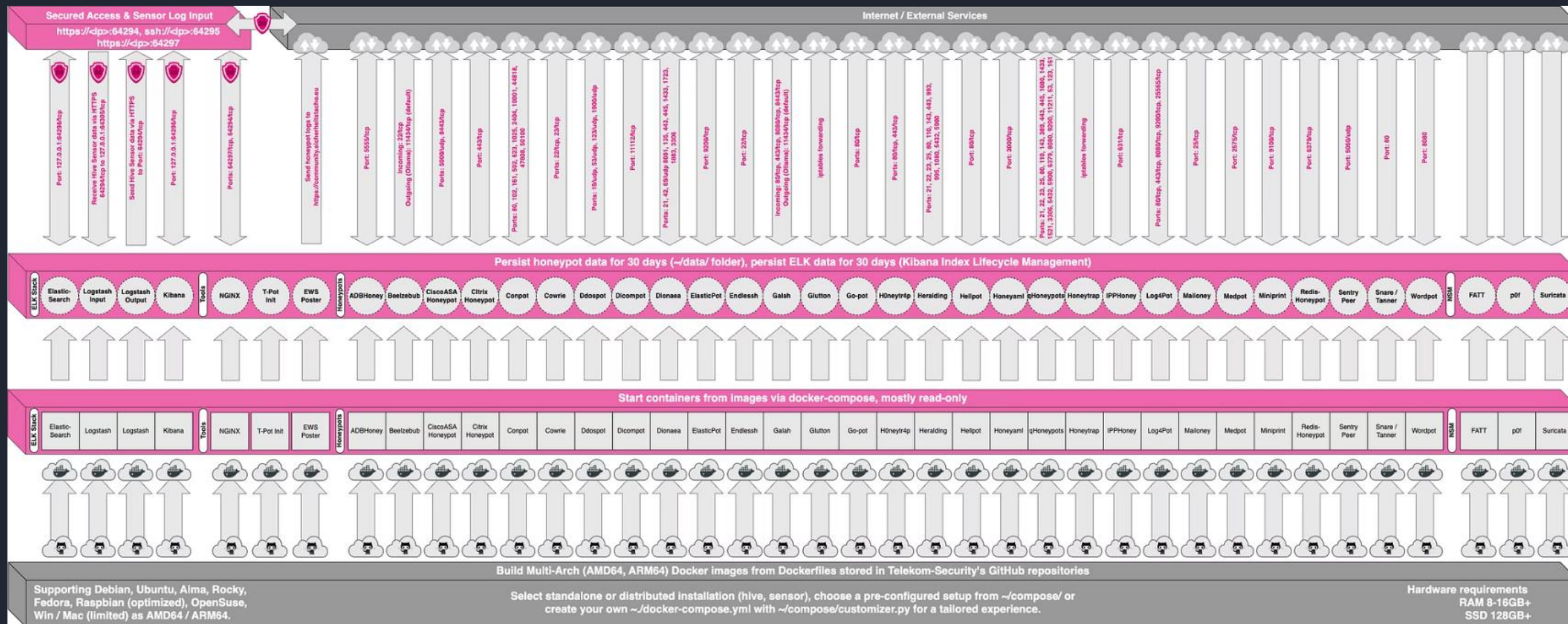
Utilizes Docker to isolate honeypot components efficiently.

Key Components

- Cowrie
- Dionaea
- Spiderfoot
- Attack Map

Network Ports

- 22 (SSH)
- 23 (Telnet)
- 80/443 (HTTP/S traps)



T-Pot_Server Tp Server 1

Handler : soflla

Handler : Aup.t/72:133:295101911

Handler : hope fraal: perringlleul.on

Tept:

Net types

Inntlaopt soft-facxerf5192

Inntlaopt ariste5.mw/steraple prerission

Sooflaopt soft-fotwe/ctervate word preager; 21f::54533

U/blottg saae

Deployment Process

Setup Server

Deployed Debian server on DigitalOcean cloud platform.

Install T-Pot

Installed with Hive for enhanced alert and case management.

Migrate Components

Upgraded from Cowrie-only to full T-Pot multi-honeypot setup.

Troubleshoot

Resolved Docker and network configuration challenges.

← Back to Droplets



debian-s-4vcpu-8gb-nyc3-01

in [first-project](#) / 8 GB Memory / 4 Intel vCPUs / 160 GB Disk / NYC3 - Debian 12 x64

Upsize Droplet

ON

ipv4: 161.35.137.206

ipv6: [Enable now](#)

Private IP: 10.108.0.2

Reserved IP: [Enable now](#)

Console: [📄](#) [?](#)

Graphs

Access

Power

Volumes

Resize

Networking

Backups

Snapshots

Kernel

History

Destroy

Tags

Recovery

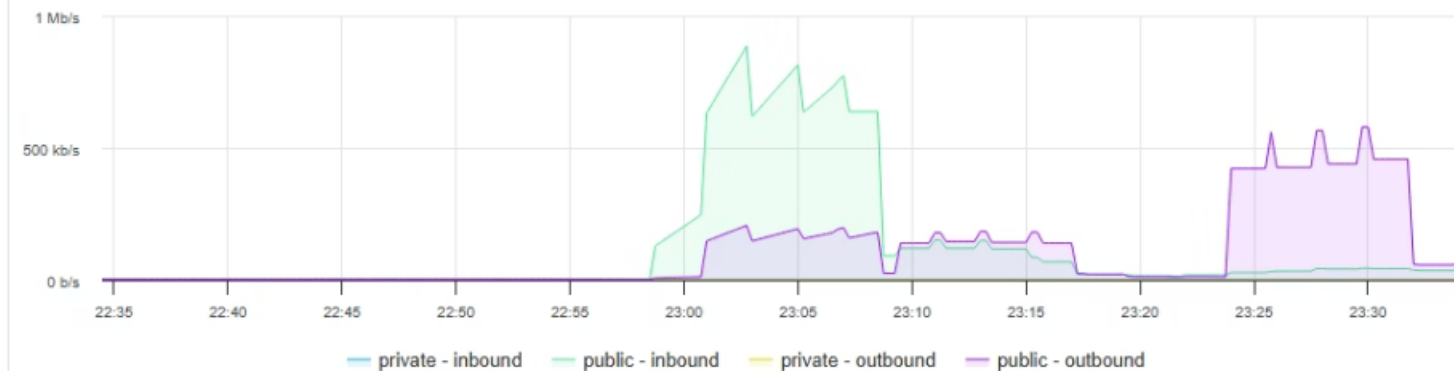
Upgrade your Droplet for additional metrics and alerting.

[Learn How to Update](#)

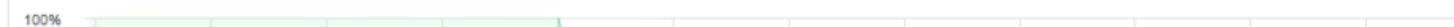


Select period
1 hour

Bandwidth



CPU Usage



Cloud Setup

Debian server on DigitalOcean

Requirements

- Debian 11, 4+ cores, 16 GB RAM, 256 GB SSD
- Internet and root access

Tools

Docker, Hive for case management

Challenges

Networking and Docker troubleshooting

```
maudy@debian-s-4vcpu-8gb x + v
C:\Users\Mauricio>ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:\Users\Mauricio/.ssh/id_ed25519):
Created directory 'C:\Users\Mauricio/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Passphrases do not match. Try again.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\Mauricio/.ssh/id_ed25519
Your public key has been saved in C:\Users\Mauricio/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:4Z7yFOV5Sf7Sub7IqpqomVKEWnHKN2eDuFdYjKAT2ck mauricio@DESKTOP-TESB9A9
The key's randomart image is:
+--[ED25519 256]--+
|.+.o.o|
|.oE.o.o|
|oo = + . . .|
|..* = =. + + .|
|.o.o = .S.o.+|
|.o.o .o.o.o.|
|. . . + . +|
|.o.o = .o.o.|
|. +..o.o...o.+|
+-----[SHA256]-----+

C:\Users\Mauricio>explorer .
C:\Users\Mauricio>ssh 161.35.137.206
```

```
maudy@debian-s-4vcpu-8gb x + v
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian-s-4vcpu-8gb-nyc3-01:~# env bash -c "$(curl -sL https://github.com/telekom-security/tpotce/raw/master/install
.sh)"
This script should not be run as root. Please run it as a regular user.

root@debian-s-4vcpu-8gb-nyc3-01:~# adduser maudy
Adding user 'maudy' ...
Adding new group 'maudy' (1000) ...
Adding new user 'maudy' (1000) with group 'maudy (1000)' ...
Creating home directory '/home/maudy' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for maudy
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:

Is the information correct? [Y/n]
Adding new user 'maudy' to supplemental / extra groups 'users' ...
Adding user 'maudy' to group 'users' ...
root@debian-s-4vcpu-8gb-nyc3-01:~# sumaudy
-bash: sumaudy: command not found
root@debian-s-4vcpu-8gb-nyc3-01:~# su maudy
maudy@debian-s-4vcpu-8gb-nyc3-01:/root$ env bash -c "$(curl -sL https://github.com/telekom-security/tpotce/raw/master/in
stall.sh)"^C
```

- Setting up SSH Key and adding user access to WebUI


```

TASK [Gathering Facts] *****
ok: [127.0.0.1]

TASK [Setup a randomized daily reboot (All)] *****
changed: [127.0.0.1]

PLAY RECAP *****
127.0.0.1          : ok=36   changed=21   unreachable=0   failed=0   skipped=1   rescued=0   ignored=1

### Playbook was successful.

### Choose your T-Pot type:
### (H)ive    - T-Pot Standard / HIVE installation.
###           Includes also everything you need for a distributed setup with sensors.
### (S)ensor  - T-Pot Sensor installation.
###           Optimized for a distributed installation, without WebUI, Elasticsearch and Kibana.
### (L)LM     - T-Pot LLM installation.
###           Uses LLM based honeypots Beelzebub & Galah.
###           Requires Ollama (recommended) or ChatGPT subscription.
### M(i)ni    - T-Pot Mini installation.
###           Run 30+ honeypots with just a couple of honeypot daemons.
### (M)obile  - T-Pot Mobile installation.
###           Includes everything to run T-Pot Mobile (available separately).
### (T)arpit  - T-Pot Tarpit installation.
###           Feed data endlessly to attackers, bots and scanners.
###           Also runs a Denial of Service Honeypot (ddospot).

### Install Type? (h/s/l/i/m/t) i|

```

- Installing Hive T-Pot after initially installing Mini due to ability to access Elastic Search, Kibana, and other Dashboard Metrics.

```

tcp        0      0 0.0.0.0:5355          0.0.0.0:*            LISTEN     996      17569      471/systemd-resolv
e
tcp6       0      0 :::64295              :::*                  LISTEN     0        35518      6768/sshd: /usr/sb
i
tcp6       0      0 ::1:25                :::*                  LISTEN     0        19371      1900/exim4
tcp6       0      0 :::5355               :::*                  LISTEN     996      17577      471/systemd-resolv
e
udp        0      0 127.0.0.54:53         0.0.0.0:*             996      17582      471/systemd-resolv
e
udp        0      0 127.0.0.53:53         0.0.0.0:*             996      17580      471/systemd-resolv
e
udp        0      0 0.0.0.0:5355          0.0.0.0:*             996      17568      471/systemd-resolv
e
udp6       0      0 :::5355               :::*                  996      17576      471/systemd-resolv
e

```

Done. Please reboot and re-connect via SSH on tcp/64295.

```
maudy@debian-s-4vcpu-8gb-nyc3-01:~$ sudo reboot
```

Broadcast message from root@debian-s-4vcpu-8gb-nyc3-01 on pts/1 (Fri 2025-05-02 04:37:13 UTC):

The system will reboot now!

```
maudy@debian-s-4vcpu-8gb-nyc3-01:~$ Connection to 161.35.137.206 closed by remote host.
Connection to 161.35.137.206 closed.
```

```
C:\Users\Mauricio>
```


📄 Rebooting Server after installation


debian-s-4vcpu-8gb-nyc3-01 - x | debian-s-4vcpu-8gb-nyc3-01 - x | T-Pot x +


Not secure https://161.35.137.206:64297

00:41 | 02/05/2025

T-Pot 24.04.1




Attack Map
Cyberchef
Elasticvue
Kibana
Spiderfoot


SecurityMeter
T-Pot ReadMe
T-Pot @ Github




Honeytrap Overview & Attack Volume

- **Total Attacks Logged: 151,000+**
- **Top Honeypots by Volume:**
 - **Cowrie:** 70,000+ attacks
 - **Honeytrap:** 37,000+ attacks
 - **Dionaea:** 20,000+ attacks
- Multiple attack vectors captured across SSH, Telnet, and other protocols



- **Top Source Countries:** USA 46%, Netherlands 12%, China 9%
- **Frequent Destination Ports:** 5060(non encrypted signaling traffic), 445 Server Message Blocking to share files and printers over TCP/IP, 22 SSH to connect to device and issue commands
- **Common Username Tags:** Root(2911), ubuntu(514), Administrator(514), 345gs5662d34(242), sa(207)
- **Top Password Tags:** 123456(1063), 123(246), 3245gs5662d34(242)

 Elasticvue

● default cluster ▼

HOME NODES SHARDS INDICES SEARCH REST SNAPSHOTS ⚙️

tpotcluster

4jj9gCyOTeGBM9SWnMqGSQ

✓ green

1 nodes

1 master
1 data

37 shards

37 primaries
0 replicas

37 indices

2390047 docs
1.15 GB on disk

Cluster Information

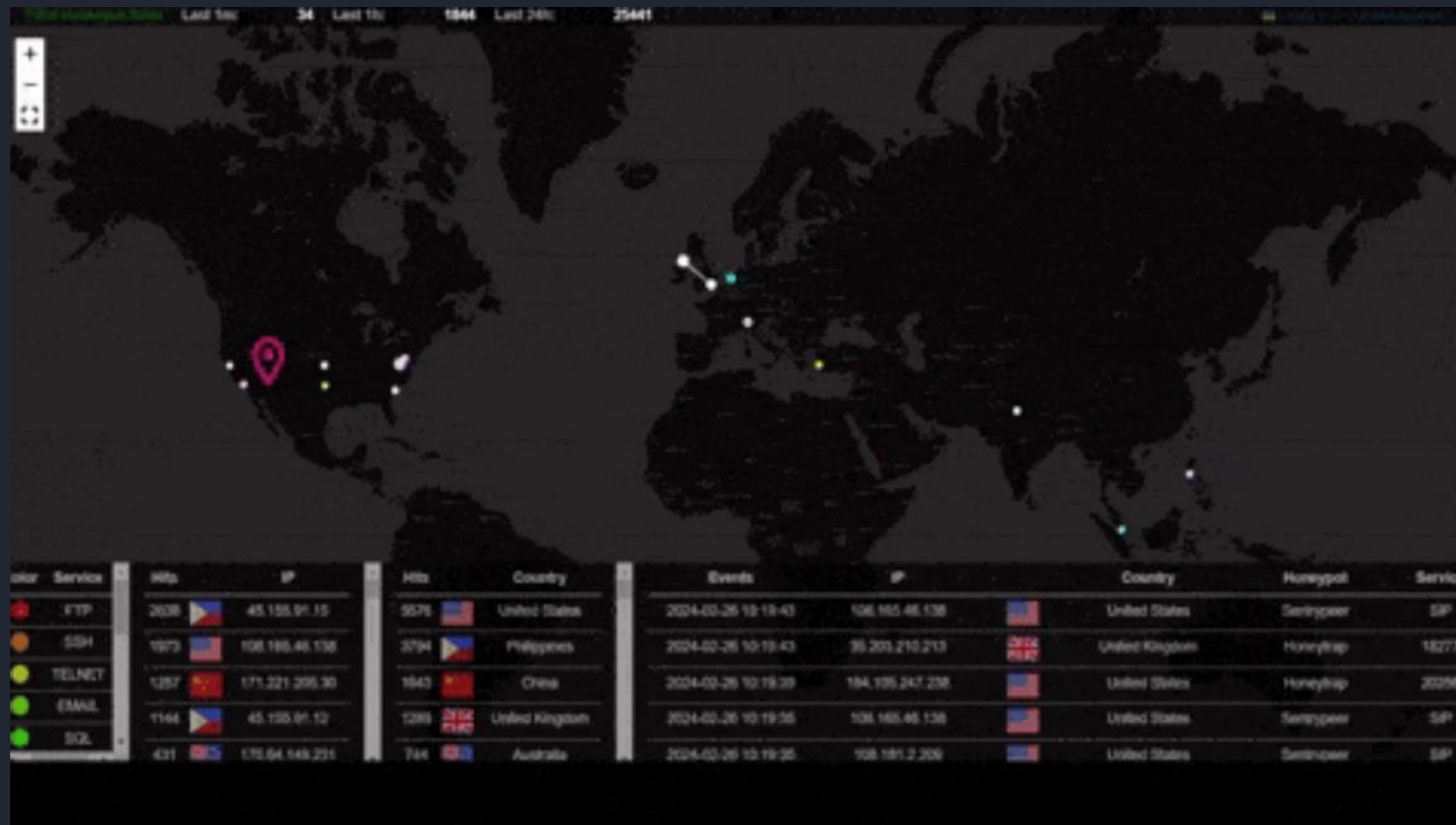
Node Name	tpotcluster-node-01
Cluster name	tpotcluster
Cluster uuid	4jj9gCyOTeGBM9SWnMqGSQ
Tagline	You Know, for Search
Version	
Number	8.17.3
Build flavor	default
Build type	deb
Build hash	a091390de485bd4b127884f7e565c0cad59b10d2
Build date	2025-02-28T10:07:26.089129809Z
Lucene version	9.12.0
Minimum wire compatibility version	7.17.0
Minimum index compatibility version	7.0.0

Cluster Health

Status	green
Timed out	false
Relocating shards	0
Initializing shards	0
Unassigned shards	0
Delayed unassigned shards	0
Active shards	37
Active shards percent	100.00%
Pending tasks	0
In flight fetch	0


Elasticvue – T-Pot Cluster Insights

- Lightweight web GUI to explore Elasticsearch data from T-Pot
- View cluster health, node status, and storage usage
- Browse and query honeypot logs (Cowrie, Dionaea, Honeytrap, etc.)
- Inspect attack data: source IPs, ports, protocols, credentials, malware
- Filter logs by time, honeypot type, geolocation, ASN, and more
- Useful for quick threat analysis and data validation without Kibana



T-Pot Attack Map Overview

- **Real-Time Visualization** of global honeypot attacks
- Displays attacker geolocation based on source IPs
- Shows target ports, protocols, and affected honeypot sensors
- Highlights top attacking countries and IP addresses
- Visual clustering of attacks by intensity and region
- Useful for identifying trends, hotspots, and threat origins

New ScanScansSettingsLight Mode

New Scan

Scan Name

The name of this scan.

Scan Target

The target of your scan.

Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input.

Domain Name: e.g. example.com	E-mail address: e.g. bob@example.com
IPv4 Address: e.g. 1.2.3.4	Phone Number: e.g. +12345678901 (E.164 format)
IPv6 Address: e.g. 2809:4700:4700::1111	Human Name: e.g. "John Smith" (must be in quotes)
Hostname/Sub-domain: e.g. abc.example.com	Username: e.g. "jsmith2000" (must be in quotes)
Subnet: e.g. 172.31.0/24	Network ASN: e.g. 1234
Bitcoin Address: e.g. 1HesYJSP1QgcYFEjnQ8vzBL1wujruNQs7R	

By Use Case

By Required Data

By Module

☒ All

Get anything and everything about the target.

All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

☐ Footprint

Understand what information this target exposes to the Internet.

Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

☐ Investigate

Best for when you suspect the target to be malicious but need more information.

Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

☐ Passive

When you don't want the target to even suspect they are being investigated.

As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

Run Scan Now

SpiderFoot Overview

- **Automated OSINT (Open Source Intelligence) Tool** for threat intelligence gathering
- **Monitors** various data sources like IPs, domains, ASN, WHOIS, and social media
- **Comprehensive Scans** for vulnerabilities, leaks, and footprints of a target
- Provides detailed **reports** on attack surface and security risks
- Supports **multiple data sources**: Shodan, DNS, WHOIS, Pastebin, and more
- **Customizable** with modules to suit specific intelligence needs
- **Visualization** of findings through graphs and maps for easy analysis
- Used for profiling threat actors, identifying exposed assets, and proactive defense

Analytics with T-Pot (ELK Stack)

Kibana

Visualizes logs via interactive dashboards.

Elasticsearch

Indexes and stores honeypot event data efficiently.

Attack Map

Real-time global visualization of attack sources.

Spiderfoot

Automates Open Source Intelligence (OSINT) collection.



What I Learned

Linux CLI

Enhanced proficiency in the command line environment.

Docker Orchestration

Managed containerized honeypot components effectively.

Log Analysis

Used SIEM principles for attack pattern detection.

Troubleshooting

Diagnosed and fixed deployment and network issues.



Key Findings

Common Attack Ports

Targeted ports: 22, 23, 80, 443, 445.

Attack Types

- Brute force attempts
- Default credential use
- Network scanning activities

Traffic Sources

Attacks originated from diverse global IP addresses.

Future Improvements

Enhance Integration

Leverage Splunk or Security Onion platforms for deeper analysis.

Automate Alerts

Use TheHive and Cortex for real-time alerting.

Expand OSINT

Integrate Spiderfoot with Maltego for rich intelligence.

Use Threat Feeds

Incorporate MISP and OTX for updated threat intel.

Conclusion

Summary

Successfully deployed T-Pot and analyzed honeypot data.

Next Steps

Build advanced operational security and OSINT skills.

Learning Outcome

Hands-on experience in cyber defense and threat analysis.

