
INSTITUTE FOR ADVANCED COMPUTING

AND

SOFTWARE DEVELOPMENT

AKURDI, PUNE

DOCUMENTATION ON

# Cloud-Based Honeypot Deployment for Advanced Threat Intelligence and Cyber Defense

SUBMITTED BY:

**GROUP NO. 15**

**ABHISHEK AGRE (233402)**

**NITIN INGLE (233425)**

**MR.KARTIK AWARI**

**PROJECT GUIDE**

**MR. ROHIT PURANIK**

**CENTRE CO-ORDINATOR**

## ABSTRACT

In the ever-evolving landscape of cyber threats and attacks, proactive cybersecurity measures are crucial to staying ahead of malicious actors. This project introduces a comprehensive approach to enhancing threat intelligence and bolstering cyber defense strategies through the deployment of a cloud-based honeypot system. A honeypot is a deceptive system designed to mimic real targets, attracting and engaging potential attackers while collecting valuable data about their methods and intentions. Leveraging the scalability and flexibility of cloud infrastructure, our project focuses on designing and implementing an advanced honeypot framework, enabling dynamic deployment and monitoring of diverse honeypot instances.

The proposed cloud-based honeypot system combines various honeypot types, such as high-interaction and low-interaction honeypots, to effectively mimic a wide range of services and systems. By strategically distributing these honeypots across different virtualized environments, the system can simulate an authentic network ecosystem, enticing attackers to interact with the decoy resources. The collected data includes attack patterns, malware samples, and indicators of compromise, all of which contribute to an enriched threat intelligence repository.

# TABLE OF CONTENTS

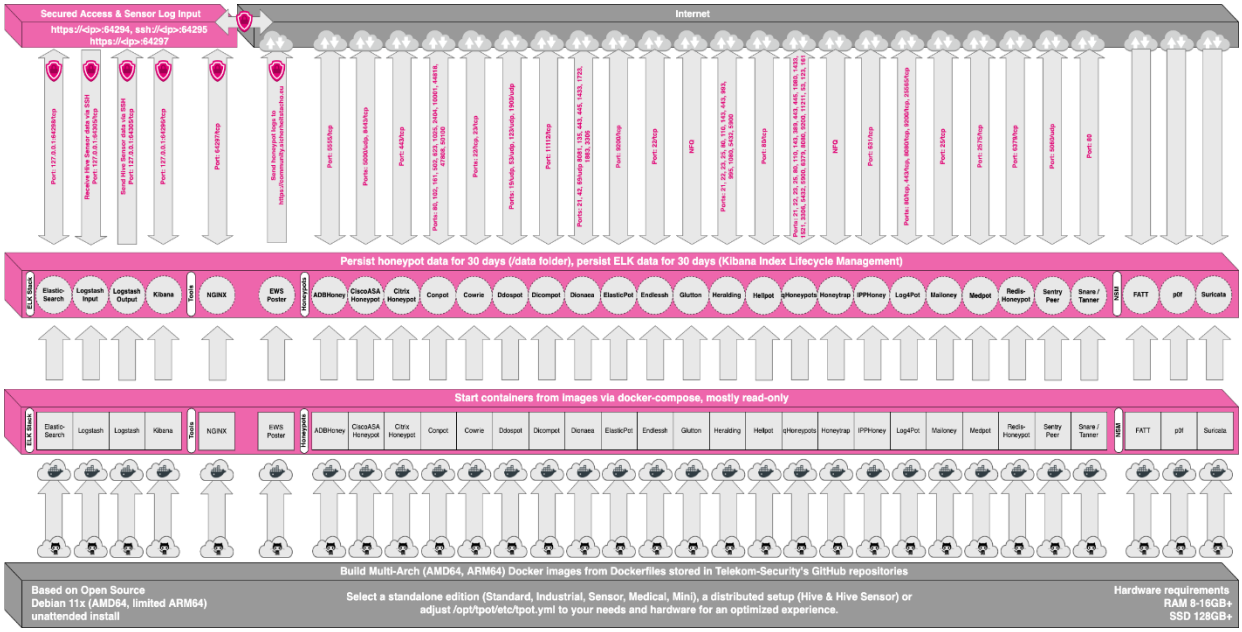
# 1.INTRODUCTION

In this project, we will implement and analyze a honeypot environment using T-Pot, an open-source honeypot framework. T-Pot allows us to deploy and monitor various honeypot services to attract and analyze malicious activities. Throughout the project, we will set up the T-Pot environment, configure honeypot services, and analyze the collected data to gain insights into potential threats and vulnerabilities.

T-POT stands out from other honeypot solutions because of its flexibility and ease of use. It includes a wide range of pre-configured honeypots, such as Dionaea, Cowrie, and Glastopf, as well as other security tools like Suricata and the ELK stack. T-POT is also designed to be customizable, allowing organizations to tailor their honeypot deployments to meet their specific needs. This makes it a powerful tool for improving threat intelligence capabilities and identifying and mitigating cyber threats. Additionally, T-POT is open-source software, which means that it is free to use and can be modified to meet the unique needs of individual organizations.

## 2.TECHNICAL ARCHITECTURE

T-POT Architecture. T-POT is designed as a modular system that can be easily extended with additional components and tools. At its core, T-POT is built on top of a Debian operating system and includes multiple pre-configured honeypots, security tools, and data analysis tools.



## 3.SERVICE

- T-Pot offers a number of services which are basically divided into five groups:

**1.System services provided by the OS:**

- SSH for secure remote access.
- Cockpit for web based remote acccess, management and web terminal.

**2.Elastic Stack:**

- Elasticsearch for storing events.
- Logstash for ingesting, receiving and sending events to Elasticsearch.
- Kibana for displaying events on beautyfully rendered dashboards.

**3.Tools**

- NGINX for providing secure remote access (reverse proxy) to Kibana, CyberChef, Elasticvue, GeoIP AttackMap and Spiderfoot.
- CyberChef a web app for encryption, encoding, compression and data analysis.
- Elasticvue a web front end for browsing and interacting with an Elastic Search cluster.
- Geoip Attack Map a beautifully animated attack map for T-Pot.
- Spiderfoot a open source intelligence automation tool.

**4.Honeypots**

- A selection of the 22 available honeypots based on the selected edition and / or setup.

**5.Network Security Monitoring (NSM)**

- Fatt a pyshark based script for extracting network metadata and fingerprints from pcap files and live network traffic.
- P0f is a tool for purely passive traffic fingerprinting.

Suricata a Network Security Monitoring engine

# 4.SYSTEM REQUIREMENTS

Depending on the installation setup, edition, installing on real hardware, in a virtual machine or cloud there are different kind of requirements to be met regarding OS, RAM, storage and network for a successful installation of T-Pot (you can always adjust /opt/tpot/etc/tpot.yml to your needs to overcome these requirements).

- | T-Pot Type | RAM | Storage | Description | Standalone | 8-16GB | >=128GB SSD | RAM requirements depend on the edition,
- storage on how much data you want to persist. | | Hive | >=8GB | >=256GB SSD | As a rule of thumb, the more sensors & data,
- the more RAM and storage is needed. | | Hive_Sensor | >=8GB | >=128GB SSD | Since honeypot logs are persisted (/data) for 30 days, storage depends on attack volume.
- All T-Pot installations will require an IP address via DHCPa working, non-proxied, internet connection for an installation to succeed.
- If you need proxy support or static IP addresses please review the Debian and / or Docker documentation.

# 5.CREATE ISO IMAGE

**Create your own ISO Image:**

In case you want to modify T-Pot for your environment or simply want to take things into your own hands you can use the ISO Creator to build your own ISO image.

**Requirements to create the ISO image:**

- Debian 11 as host system (others may work, but remain untested)
- 4GB of free RAM
- 32GB of free storage
- A working internet connection

**Steps to create the ISO image:**

1.Clone the repository and enter it.

***git clone https://github.com/telekom-security/tpotce***

***cd tpotce***

2.Run makeiso.sh to build the ISO image. The script will download and install dependencies necessary to build the image. It will further download the Debian Netiso installer image (~50-150MB) which T-Pot is based on.

**sudo ./makeiso.sh**

3.After a successful build, you will find the ISO image tpot_[amd64,arm64].iso along with a SHA256 checksum tpot_[amd64,arm64].sha256 based on your architecture choice in your folder.

## 6.POST INSTALL USER METHOD

In some cases it is necessary to install T-Pot after you installed Debian, i.e. your provider does not offer you the option of an ISO based installation, you need special drivers for your hardware to work, or you want to experiment with ARM64 hardware that is not supported by the ISO image. In that case you can clone the T-Pot repository on your own. Make sure

**The post method install must be executed by the root (sudo su -, su -), just follow the following steps:**

**git clone https://github.com/telekom-security/tpotce**

**cd tpotce/iso/installer/**

**./install.sh --type=user**

The installation will now start, you can now move on to the T-Pot Installer section**.**

# 7.INSTALLATION TYPES

In the past T-Pot was only available as a standalone solution with all services, tools, honeypots, etc. installed on to a single machine. Based on demand T-Pot now also offers a distributed solution. While the standalone solution does not require additional explanation the distributed option requires you to select different editions (or flavors).

**1.Standalone**

With T-Pot Standalone all services, tools, honeypots, etc. will be installed on to a single host. Make sure to meet the system requirements. You can choose from various pre-defined T-Pot editions (or flavors) depending on your personal use-case (you can always adjust /opt/tpot/etc/tpot.yml to your needs). Once the installation is finished you can proceed to First Start.

**2.Distributed**

The distributed version of T-Pot requires at least two hosts the T-Pot HIVE, which will host the Elastic Stack and T-Pot tools (install this first!), and a T-Pot HIVE_SENSOR, which will host the honeypots and transmit log data to the HIVE's Elastic Stack. To finalize the HIVE_SENSOR installation continue to Distributed Deployment.

## 8.START PROCESS

Once the T-Pot Installer successfully finishes, the system will automatically reboot and you will be presented with the T-Pot login screen. Logins are according to the User Types:

**user: [tsec or <os_username>]**

**pass: [password]**

You can login from your browser and access Cockpit: **Error! Hyperlink reference not valid.** or via SSH to access the command line: ssh -l [tsec,<os_username>] -p 64295 <your.ip>:

**user: [tsec or <os_username>]**

**pass: [password]**

You can also login from your browser and access the Nginx (T-Pot Web UI and tools): **Error! Hyperlink reference not valid.**

**user: [<web_user>]**

**pass: [password]**

# 9.REMOTE ACCESS AND TOOLS

According to the User Types you can login from your browser and access Cockpit: **Error! Hyperlink reference not valid.** or via SSH to access the command line: **ssh -l [tsec,<os_username>] -p 64295 <your.ip>:**

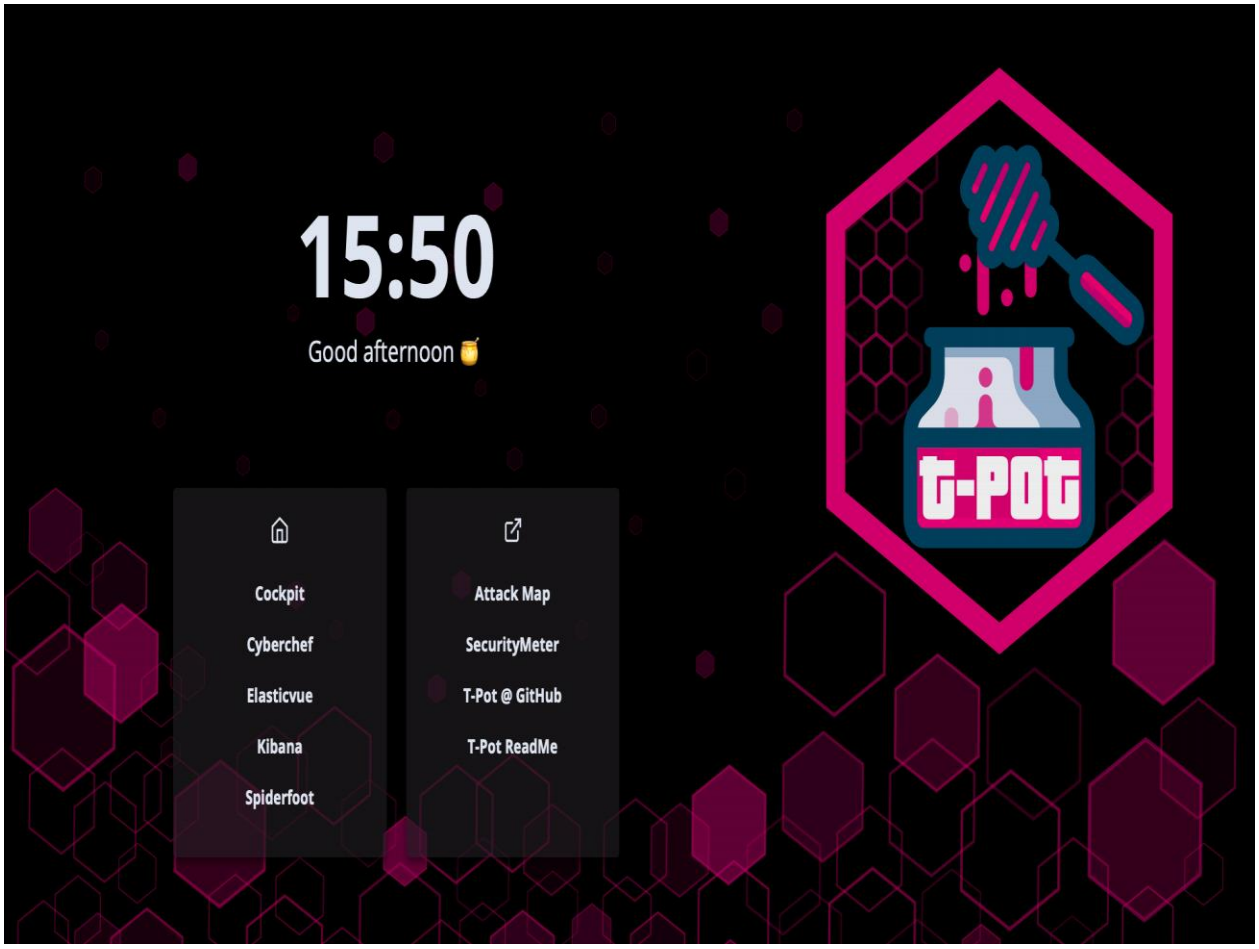
**user: [tsec or <os_username>]**

**pass: [password]**

Especially if you do not have a SSH client at hand and still want to access the machine with a command line option you can do so by accessing Cockpit. You can also add two factor authentication to Cockpit just by running 2fa.sh on the command line.

## 10.T-POT LANDING PAGE

According to the User Types you can open the T-Pot Landing Page from your browser via **Error! Hyperlink reference not valid.**:

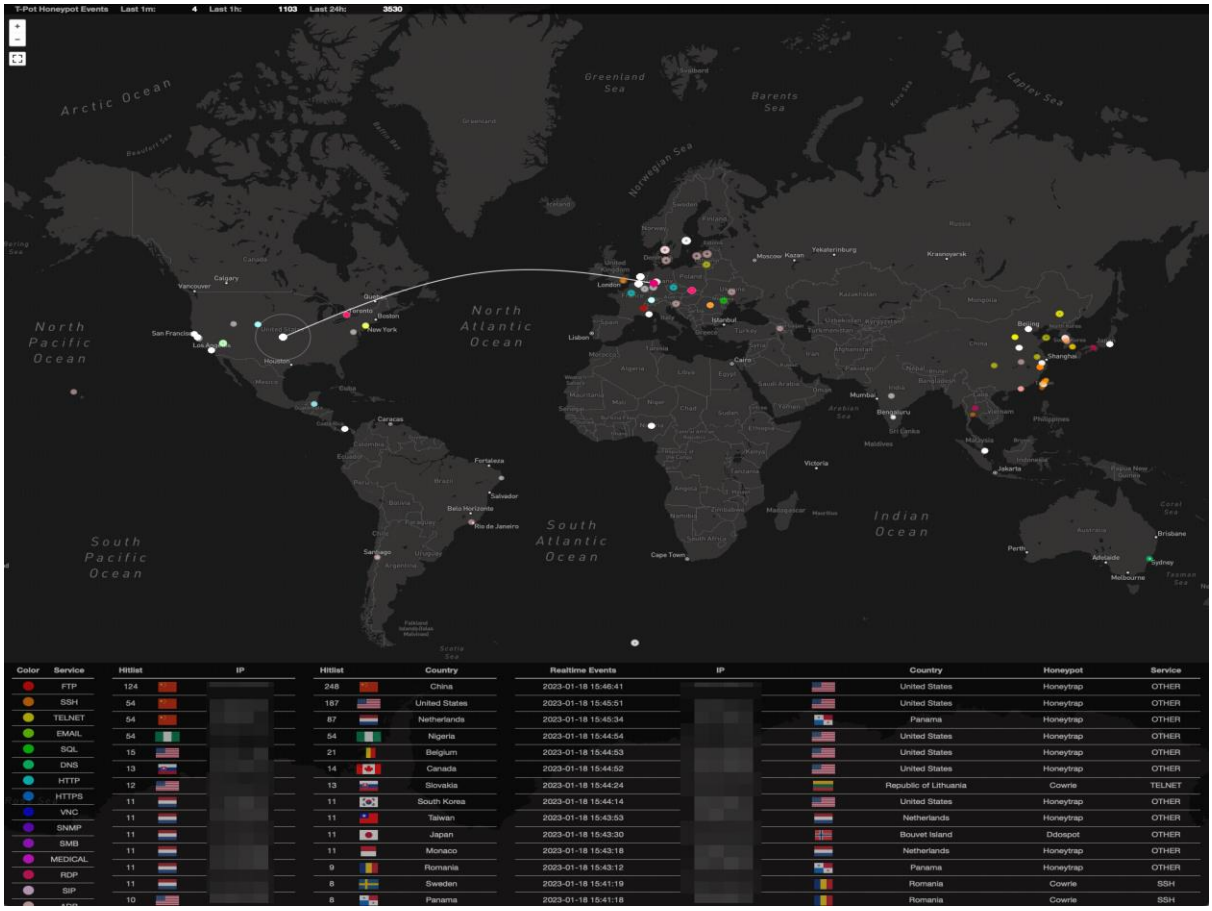


# 11.KIBANA DASHBOARD

On the T-Pot Landing Page just click on Kibana and you will be forwarded to Kibana. You can select from a large variety of dashboards and visualizations all tailored to the T-Pot supported honeypots

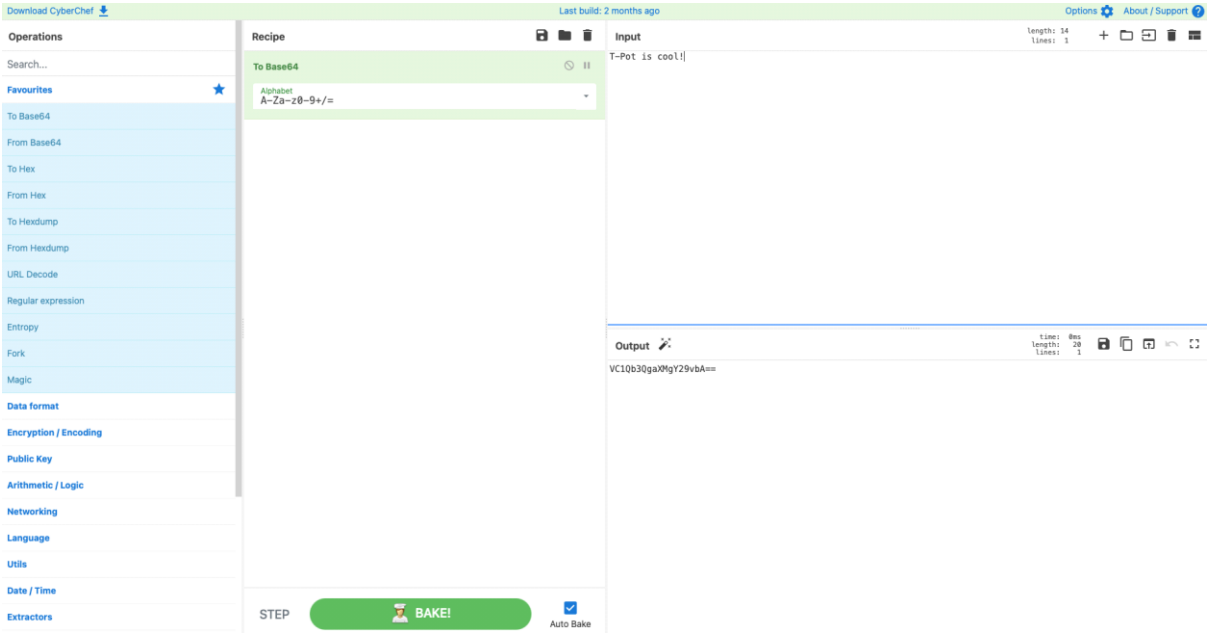
# 12.ATTACK MAP

On the T-Pot Landing Page just click on Attack Map and you will be forwarded to the Attack Map. Since the Attack Map utilizes web sockets you need to re-enter the <web_user> credentials.



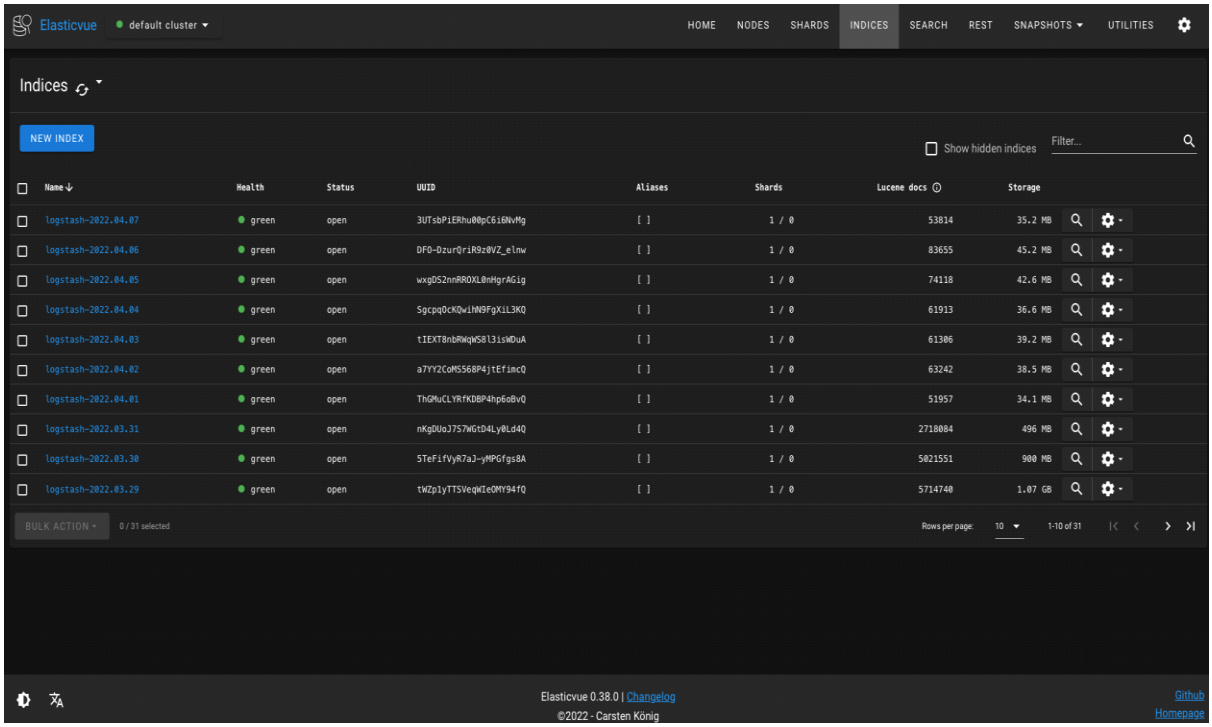
# 13.CYBERCHEF

On the T-Pot Landing Page just click on Cyberchef and you will be forwarded to Cyberchef.



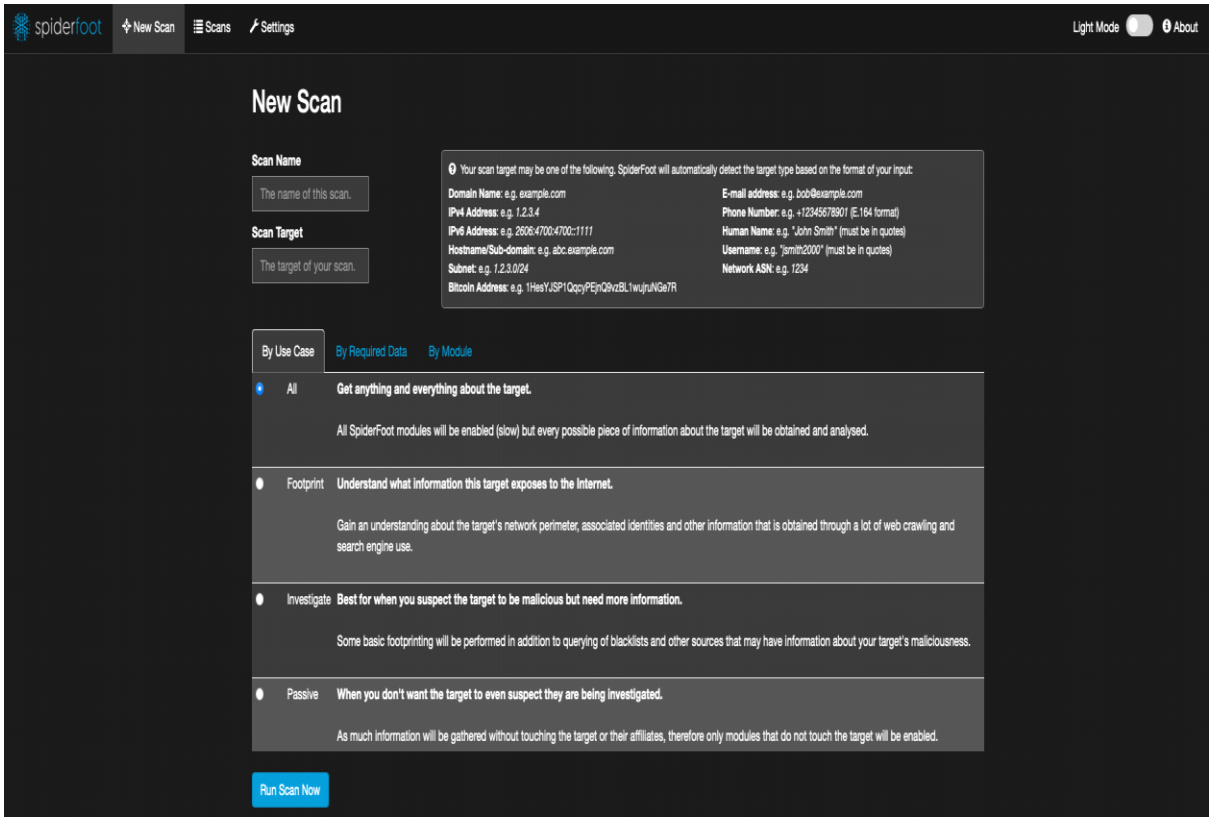
# 14.ELASTICVUE

On the T-Pot Landing Page just click on Elastivue and you will be forwarded to Elastivue.



## 15.SPIDERFOOT

On the T-Pot Landing Page just click on Spiderfoot and you will be forwarded to Spiderfoot.



## 16.CONCLUSION

**T-POT honeypot** is an effective tool for strengthening. It provides a comprehensive view of attackers activities and include a range of tools for detecting, analyzing, and responding to attacks. T-POT honeypot is easy to deploy and manage and can help in gathering intelligence on attackers tactics and tools.

The benefits of cloud-based honeypots are numerous. They offer scalable and elastic resources, enabling the creation of diverse and dynamic virtual environments that closely mimic real production systems. This realism not only sentences attackers but also provides security analysts with a comprehensive view of evolving attack vectors. Moreover, the centralized management and data collection afforded by cloud platforms streamline the analysis process, facilitating the extraction of actionable threat intelligence.

## 17.REFERENCES


1. *Artail, H., Safa, H., Sraj, M., Kuwatly, I. & Al-Masri, Z. A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks. Comput. Secur.* ***25****, 274–288. https://doi.org/10.1016/j.cose.2006.02.009 (2006).*

2. *Sharma, S. & Kaul, A. A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETS and VANET cloud. Vehic. Commun.* ***12****, 138–164 (2018).*

**3.** *Franco, J., Aris, A., Canberk, B. & Uluagac, A. S. A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems. IEEE Commun. Surv. Tutorials* ***23****, 2351–2383. https://doi.org/10.1109/COMST.2021.3106669 (2021).*