INSTITUTE FOR ADVANCED COMPUTING AND SOFTWARE DEVELOPMENT AKURDI, PUNE

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

GROUP NO: 15

Abhishek Sanjeevkumar Agre (233402)
Nitin Janardan Ingle (233425)

PROJECT GUIDE

Mr. Kartik Awari

CENTRE COORDINATOR

MR. ROHIT PURANIK

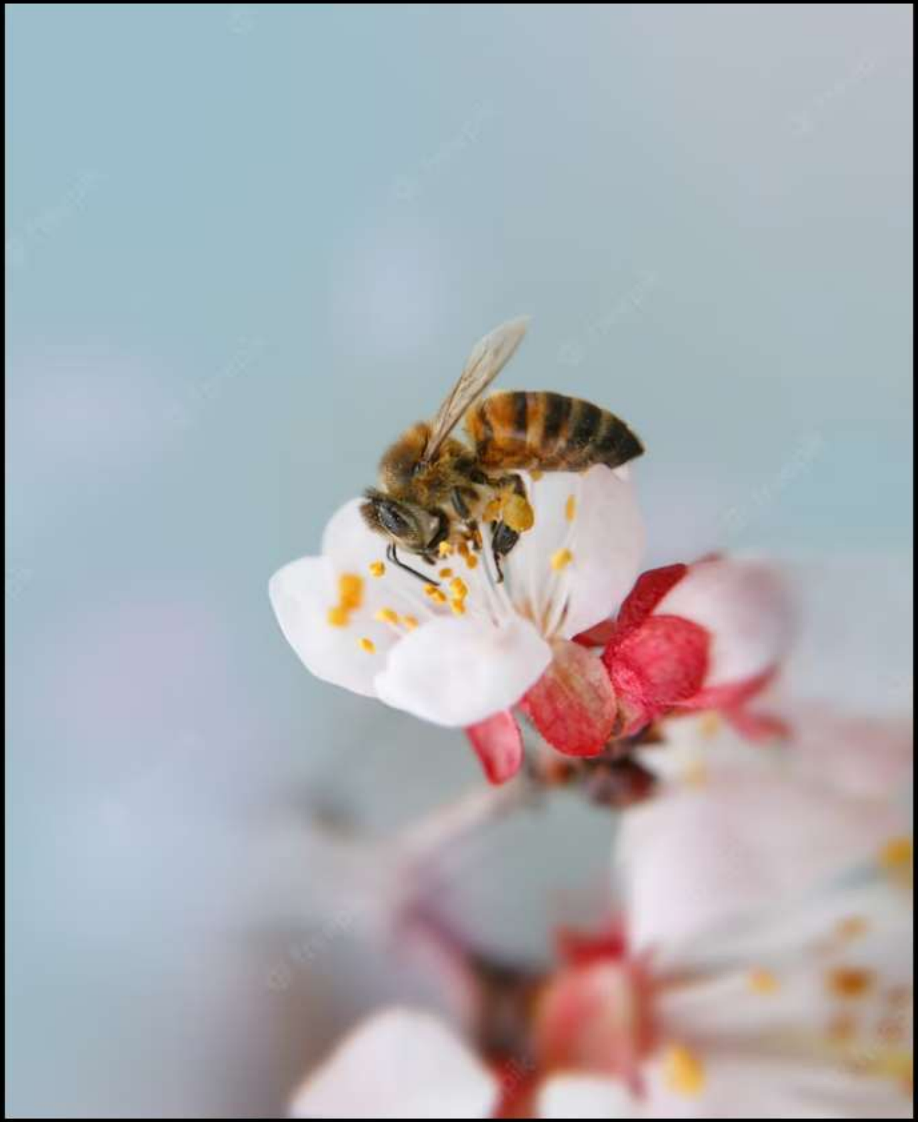
Strengthening Cybersecurity with T-POT Honeypot: An In-Depth Exploration

Introduction

Strengthening Cybersecurity with T-POT Honeypot: An In-Depth Exploration. This presentation aims to provide an overview of how T-POT honeypot can help in strengthening cybersecurity. The presentation will cover the basics of honeypots, types of honeypots, and how T-POT honeypot is different from others.

What are Honeypots?

Honeypots are decoy systems that are designed to attract attackers and help in detecting and analyzing their activities. They can be used to gather intelligence on attackers, their tactics, and their tools. Honeypots can be categorized into two types: production honeypots and research honeypots.

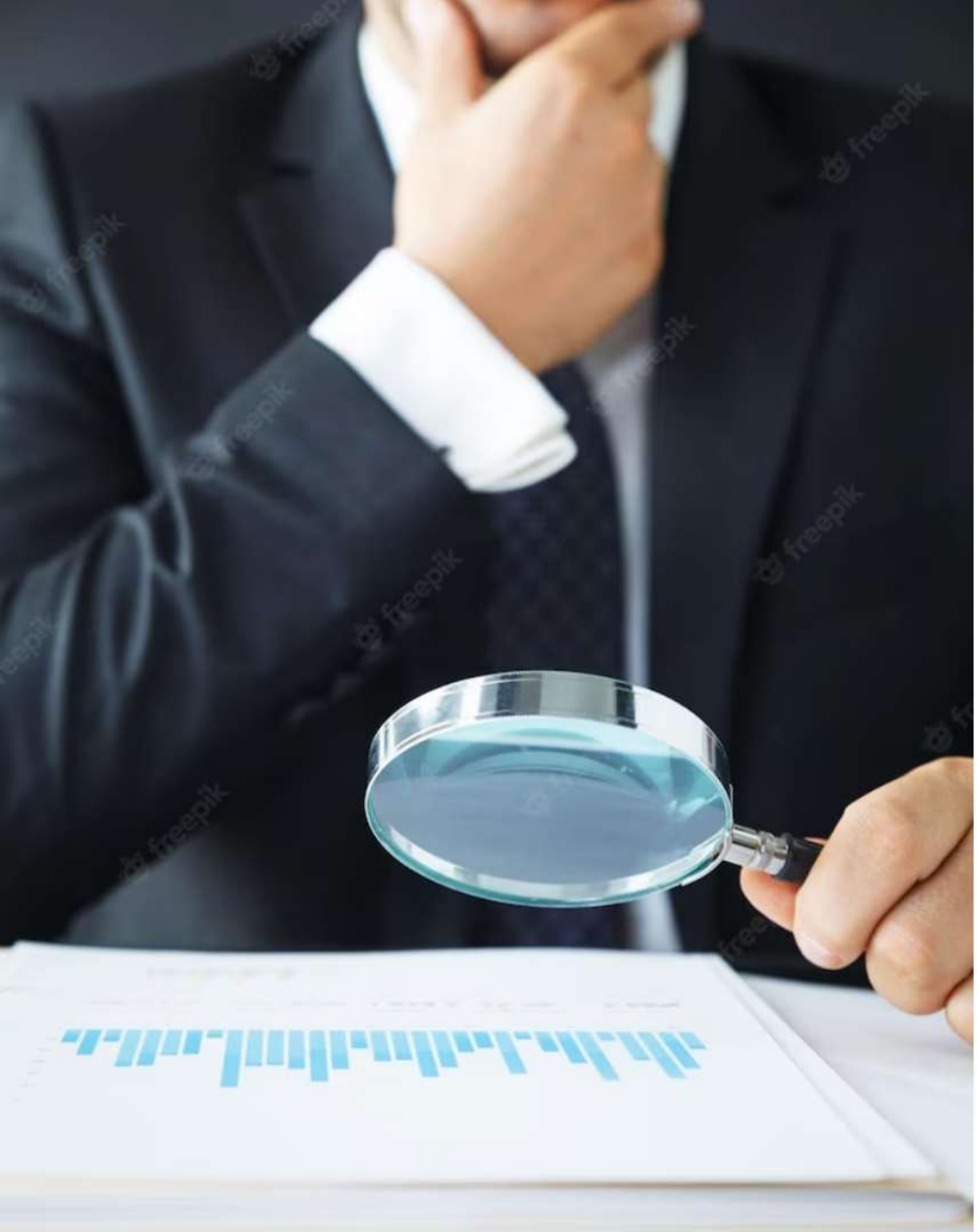


Types of Honeypots

There are several types of **honeypots** including low-interaction honeypots, high-interaction honeypots, and hybrid honeypots. Low-interaction honeypots emulate a limited number of services and are easy to deploy. High-interaction honeypots emulate complete systems and are more complex to deploy. Hybrid honeypots combine the features of both low and high-interaction honeypots.

What is T-POT Honeypot?

T-POT honeypot is an open-source honeypot platform that combines multiple honeypot technologies into a single platform. It is designed to be easy to deploy and manage, and provides a comprehensive view of attackers' activities. T-POT honeypot includes a range of tools for detecting, analyzing, and responding to attacks.



Advantages of T-POT Honeypot

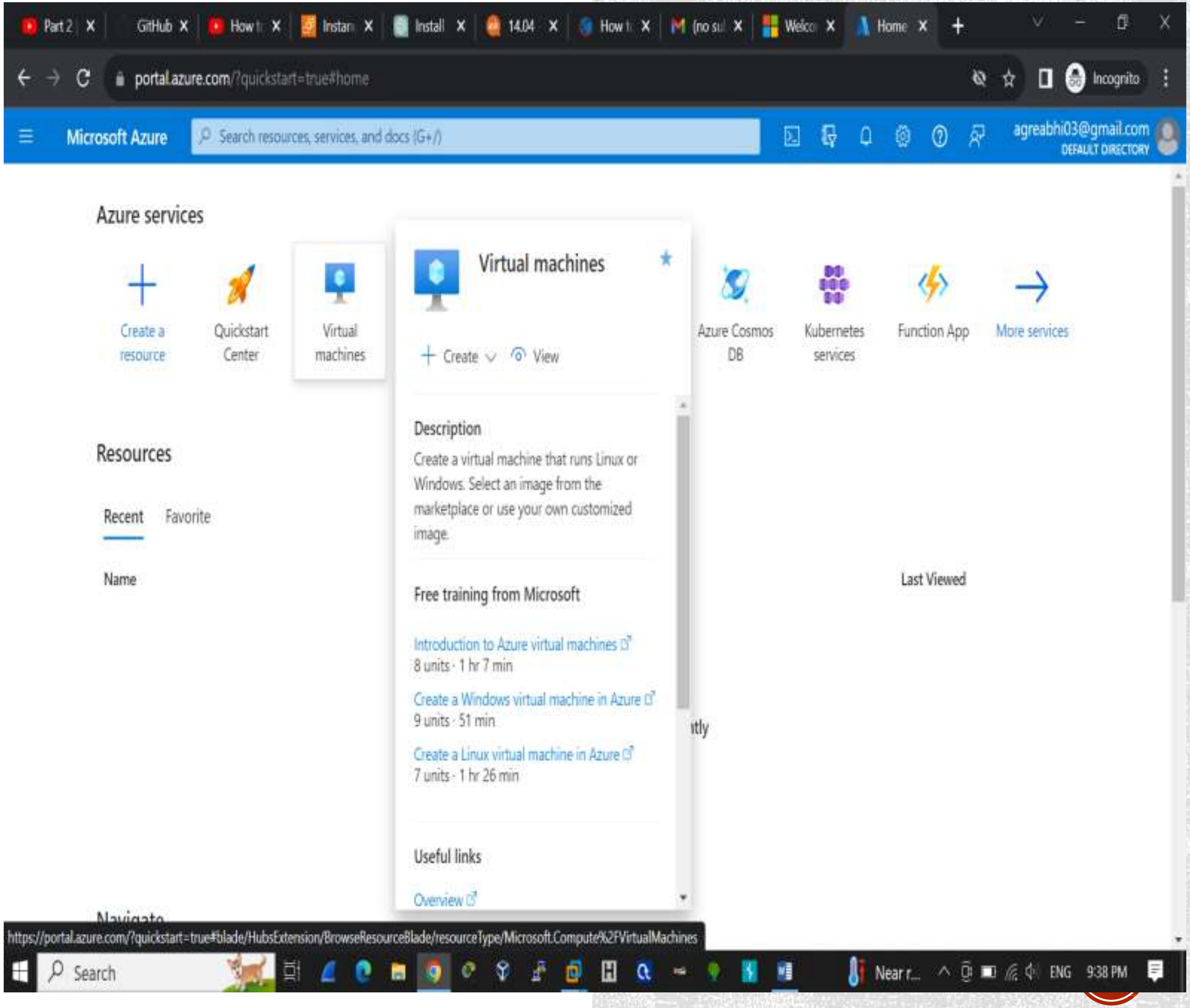
There are several advantages of **T-POT honeypot** including its ease of deployment, comprehensive view of attackers' activities, and ability to detect and respond to attacks in real-time. T-POT honeypot also provides a range of tools for analyzing and reporting on attackers' activities, which can help in strengthening cybersecurity.

Business activity of company and subdivisions
Relative activity of subdivitions of main company

Deploying T-POT in the Cloud: Step-by-Step Installation Guide

PREREQUISITES

Before starting installation process, make sure have **Cloud account** , a virtual machine running on debian



Description

Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.

Free training from Microsoft

Introduction to Azure virtual machines
8 units · 1 hr 7 min

Create a Windows virtual machine in Azure
9 units · 51 min

Create a Linux virtual machine in Azure
7 units · 1 hr 26 min

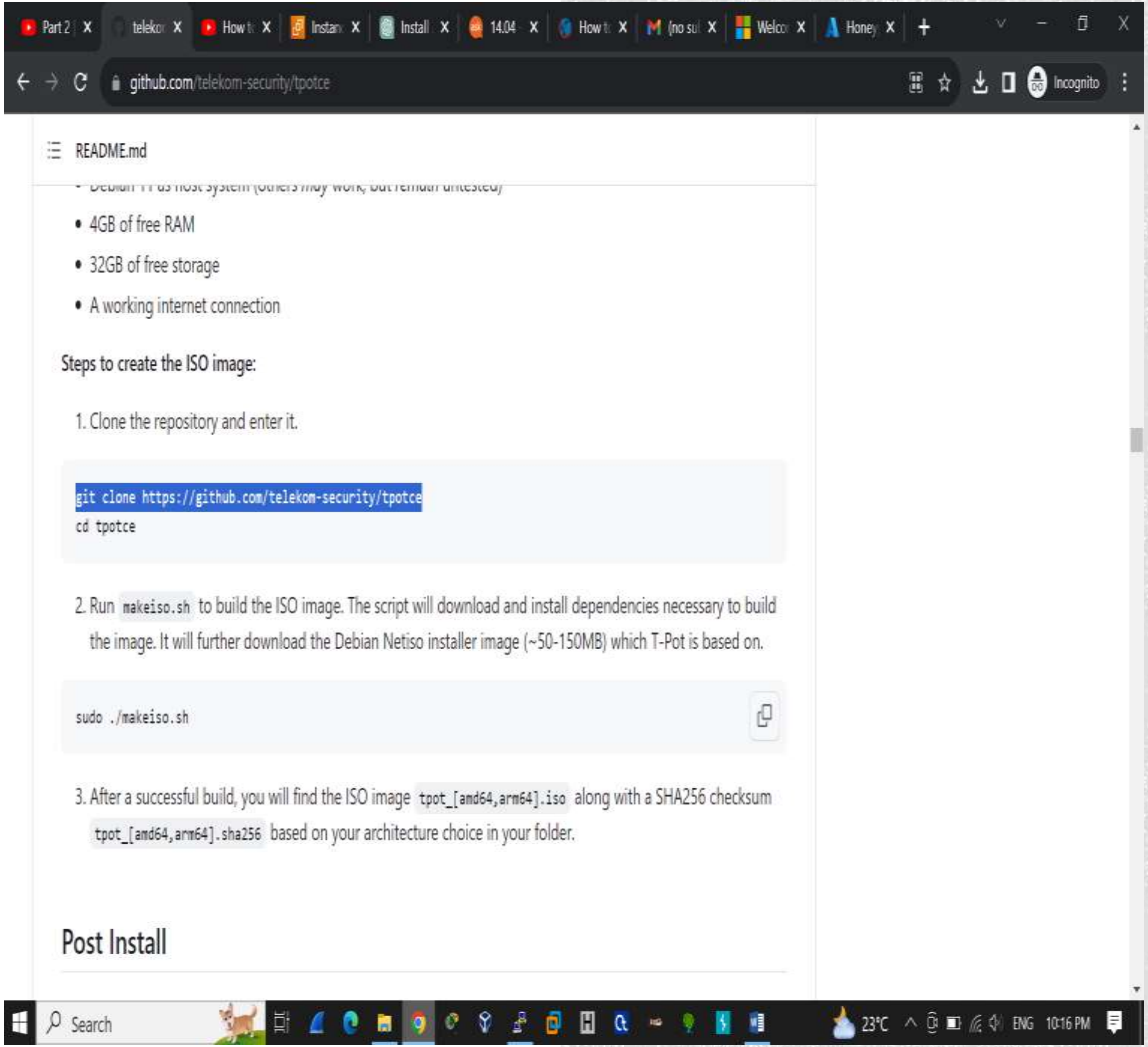
Useful links

Overview

https://portal.azure.com/?quickstart=true#blade/HubsExtension/BrowseResourceBlade/resourceType/Microsoft.Compute%2FVirtualMachines

Installing T-POT

To install T-POT, you will need to clone the T-POT repository from GitHub and run the installation script. Once the installation is complete, you can access the T-POT dashboard through your web browser.



- 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
```

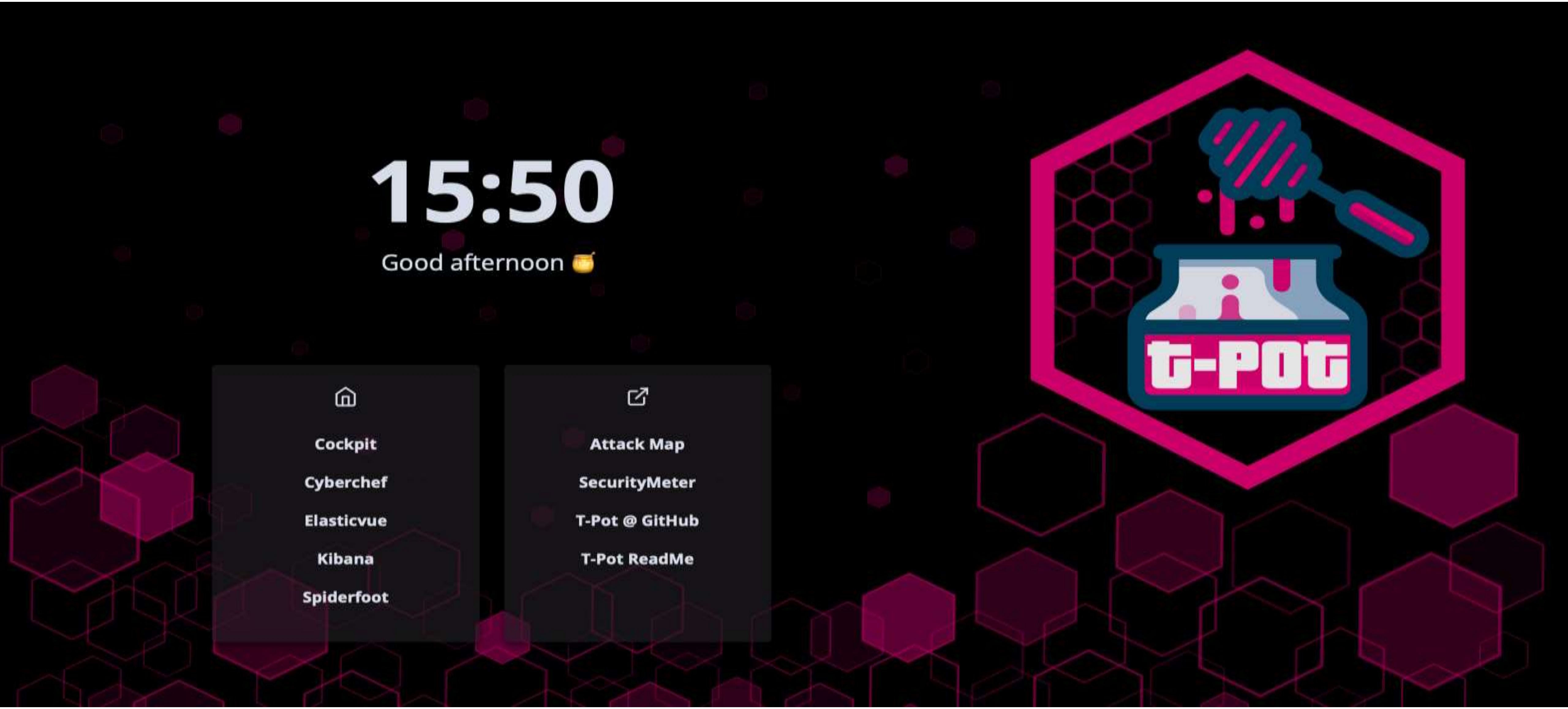
2. Run `makeiso.sh` to build the ISO image. The script will download and install dependencies necessary to build the image. It will further download the Debian Netiso installer image (~50-150MB) which T-Pot is based on.

```
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.

Post Install

T-POT LANDING PAGE



15:50

Good afternoon 🍯

Cockpit

Cyberchef

Elasticvue

Kibana

Spiderfoot

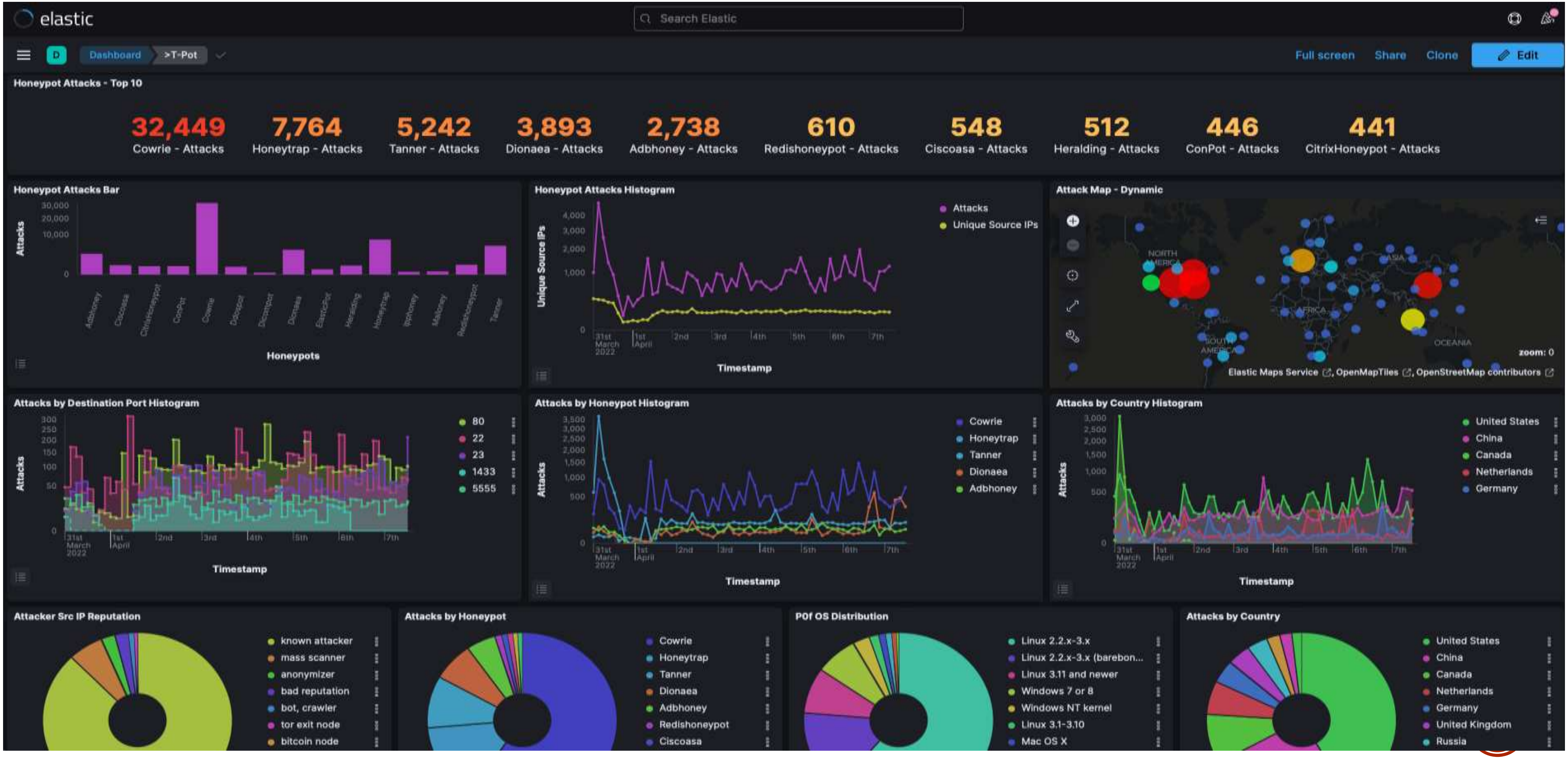
Attack Map

SecurityMeter

T-Pot @ GitHub

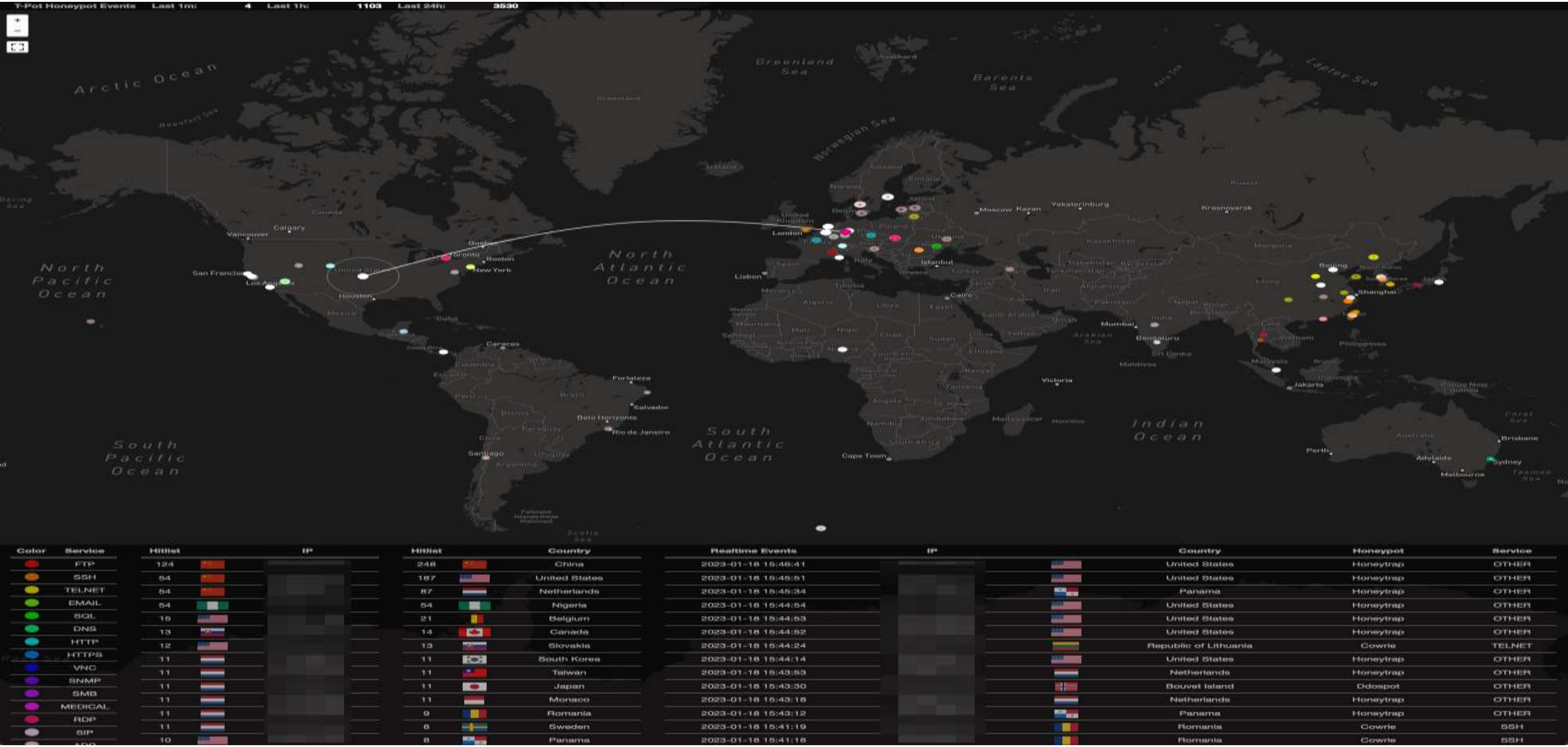
T-Pot ReadMe

KIBANA DASHBOARD



32,449	Cowrie - Attacks
7,764	Honeytrap - Attacks
5,242	Tanner - Attacks
3,893	Dionaea - Attacks
2,738	Adbhoney - Attacks
610	Redishoneypot - Attacks
548	Ciscoasa - Attacks
512	Heralding - Attacks
446	ConPot - Attacks
441	CitrixHoneypot - Attacks

ATTACK MAP



T-Pot Honeypot Events Last 1m: 4 Last 1h: 1103 Last 24h: 3530

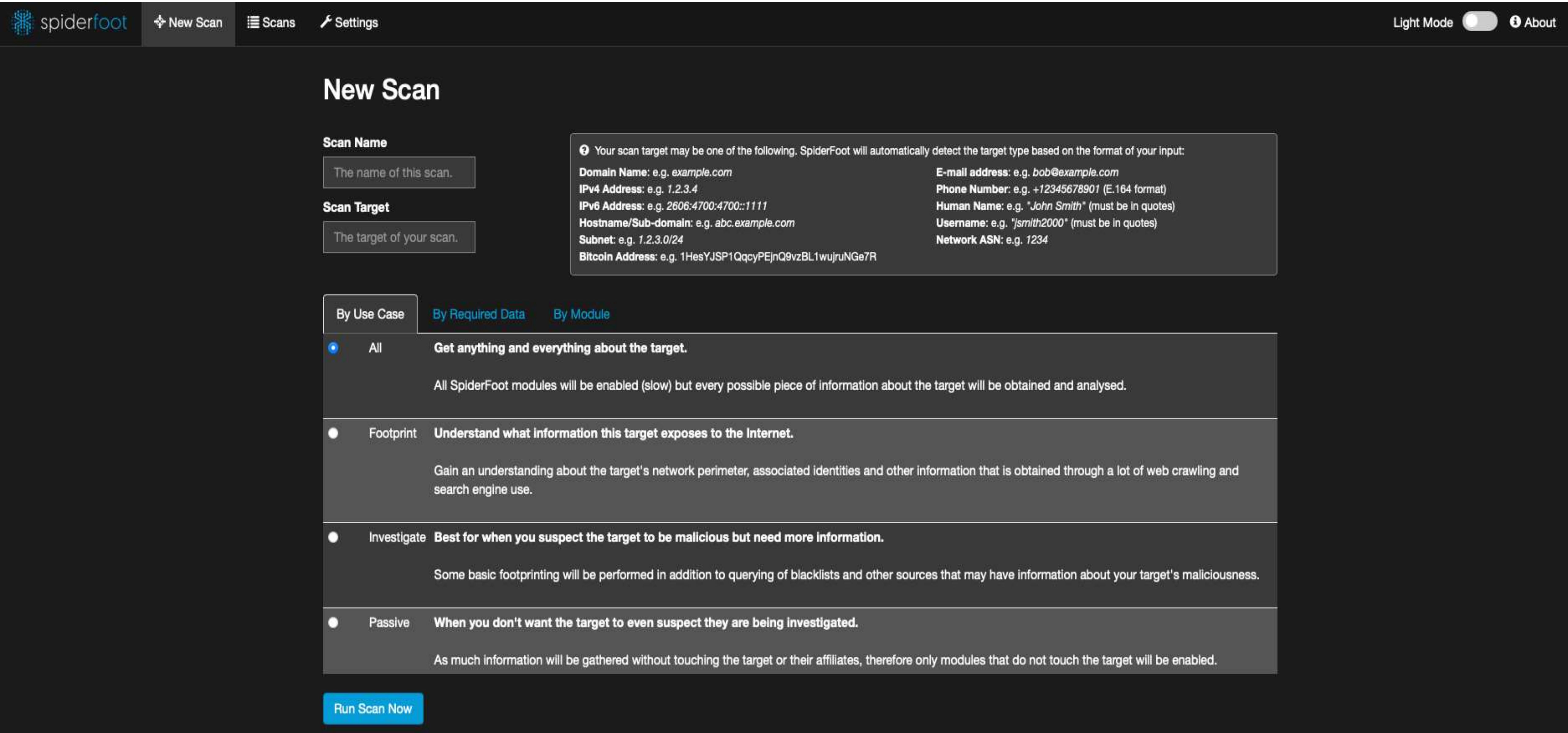
Color	Service
●	FTP
●	SSH
●	TELNET
●	EMAIL
●	SQL
●	DNS
●	HTTP
●	HTTPS
●	VNC
●	SNMP
●	SMB
●	MEDICAL
●	RDP
●	SIP
●	ADB

Hitlist		IP
124	🇨🇳	[redacted]
54	🇨🇳	[redacted]
54	🇨🇳	[redacted]
54	🇳🇬	[redacted]
15	🇺🇸	[redacted]
13	🇸🇰	[redacted]
12	🇺🇸	[redacted]
11	🇳🇱	[redacted]
11	🇳🇱	[redacted]
11	🇳🇱	[redacted]
11	🇳🇱	[redacted]
11	🇳🇱	[redacted]
11	🇳🇱	[redacted]
10	🇺🇸	[redacted]

Hitlist		Country
248	🇨🇳	China
187	🇺🇸	United States
87	🇳🇱	Netherlands
54	🇳🇬	Nigeria
21	🇧🇪	Belgium
14	🇨🇦	Canada
13	🇸🇰	Slovakia
11	🇰🇷	South Korea
11	🇹🇼	Taiwan
11	🇯🇵	Japan
11	🇲🇨	Monaco
9	🇷🇴	Romania
8	🇸🇪	Sweden
8	🇵🇦	Panama

Realtime Events	IP		Country	Honeypot	Service
2023-01-18 15:46:41	[redacted]	🇺🇸	United States	Honeytrap	OTHER
2023-01-18 15:45:51	[redacted]	🇺🇸	United States	Honeytrap	OTHER
2023-01-18 15:45:34	[redacted]	🇵🇦	Panama	Honeytrap	OTHER
2023-01-18 15:44:54	[redacted]	🇺🇸	United States	Honeytrap	OTHER
2023-01-18 15:44:53	[redacted]	🇺🇸	United States	Honeytrap	OTHER
2023-01-18 15:44:52	[redacted]	🇺🇸	United States	Honeytrap	OTHER
2023-01-18 15:44:24	[redacted]	🇱🇹	Republic of Lithuania	Cowrie	TELNET
2023-01-18 15:44:14	[redacted]	🇺🇸	United States	Honeytrap	OTHER
2023-01-18 15:43:53	[redacted]	🇳🇱	Netherlands	Honeytrap	OTHER
2023-01-18 15:43:30	[redacted]	🇧🇻	Bouvet Island	Ddospot	OTHER
2023-01-18 15:43:18	[redacted]	🇳🇱	Netherlands	Honeytrap	OTHER
2023-01-18 15:43:12	[redacted]	🇵🇦	Panama	Honeytrap	OTHER
2023-01-18 15:41:19	[redacted]	🇷🇴	Romania	Cowrie	SSH
2023-01-18 15:41:18	[redacted]	🇷🇴	Romania	Cowrie	SSH

SPIDERFOOT



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*
IPv4 Address: e.g. *1.2.3.4*
IPv6 Address: e.g. *2606:4700:4700::1111*
Hostname/Sub-domain: e.g. *abc.example.com*
Subnet: e.g. *1.2.3.0/24*
Bitcoin Address: e.g. 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R
E-mail address: e.g. *bob@example.com*
Phone Number: e.g. *+12345678901* (E.164 format)
Human Name: e.g. *"John Smith"* (must be in quotes)
Username: e.g. *"jsmith2000"* (must be in quotes)
Network ASN: e.g. *1234*

● 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.

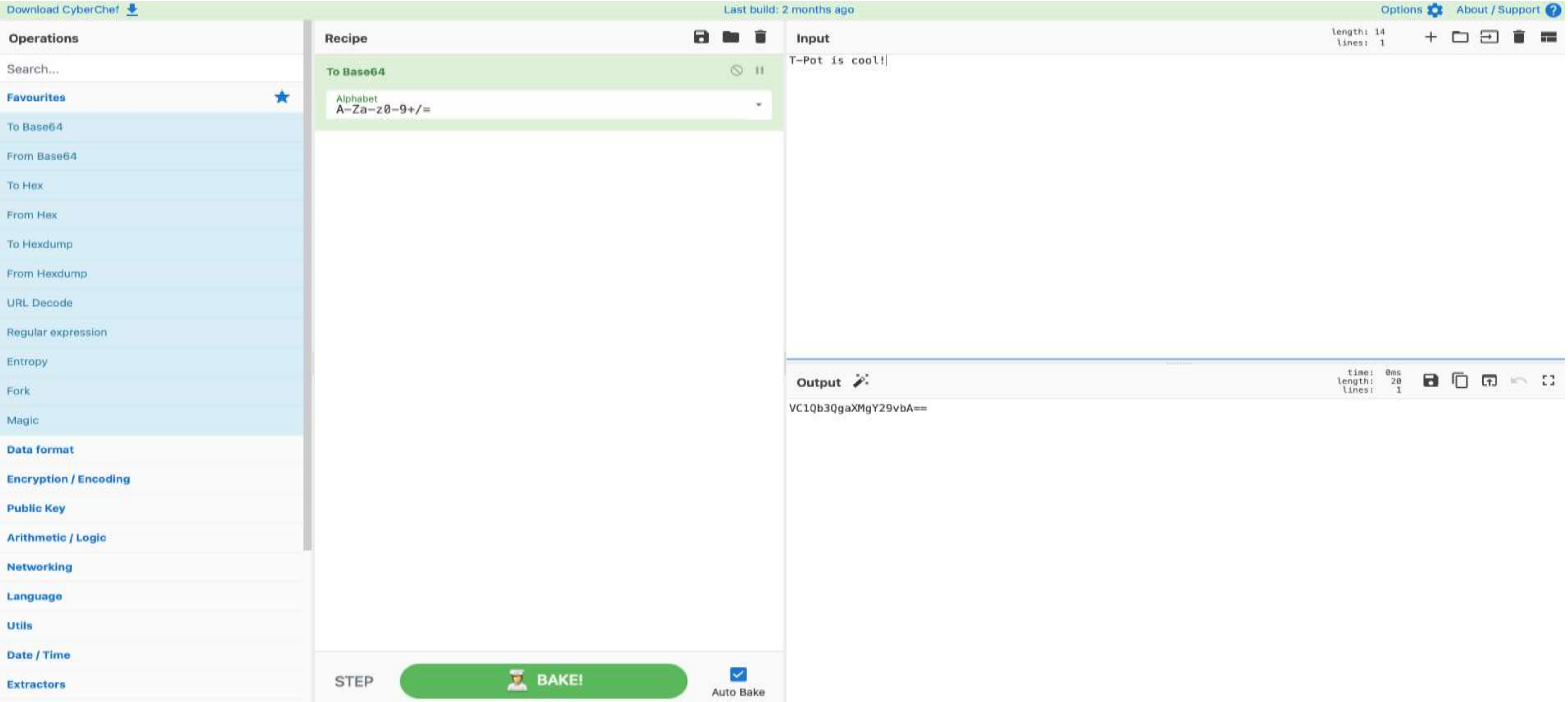
○ Investigate — **Best for when you suspect the target to be malicious but need more information.**

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.

CYBERCHEF



To Base64

Alphabet
A-Za-z0-9+/=

☑ Auto Bake

Input

```
length: 14
 lines:  1
```

```
T-Pot is cool!
```

Output

```
  time:  0ms
length:  20
 lines:   1
```

```
VC1Qb3QgaXMgY29vbA==
```

Conclusion

In conclusion, **T-POT honeypot** is an effective tool for strengthening cybersecurity. It provides a comprehensive view of attackers' activities and includes 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.

THANK YOU