

Fábio de Magalhães  
Network Security



TIMOR-LESTE NETWORK  
OPERATORS' GROUP


**Community  
Event/Gathering  
2024** CONFERENCE



# About me:

 Fábio de Magalhães

 fabio-de-magalhaes-3a328a124

 @f4bio\_rosano

# contents

- What is Honeytrap & Honeytrap
- Types of Honeytrap
- Deploy Honeytrap
- How scenario of Honeytrap?
- Honeytrap Tools
- Example/use case
- Benefit of Honeytrap

Credits: **Mr. Adli Wahid**

(APNIC Community Honeytrap Project)  
for the some of the contents of  
this slide. [adli@apnic.net](mailto:adli@apnic.net)



## Lance Spitzner, The HoneyNet Project

How can we defend  
against an enemy, when  
we don't even know who  
the enemy is?

KNOW  
YOUR ENEMY

LEARNING ABOUT SECURITY THREATS



The HoneyNet  
PROJECT

what is

**HONEYPOT ?**



# HONEYPOT

- A honeypot is a system or software designed to mimic a real system or network, but actually serves only as a trap for attackers.
- Its purpose is to attract the attention of attackers, learn their attack methods, and gather information that can be used to improve the security of the real system.

# HONEYNET

is a decoy network that contains more of honeypots.



# Types of Honeypot

## Low & Medium Interaction Honeypot:

- Emulate the behavior of a more limited system. Typically used to detect more general attacks without exposing too much detail information's.
- Easier to deploy, configure and requires less maintenance.

Example: Emulate SSH (22) / Telnet (23) Service and wait for connection

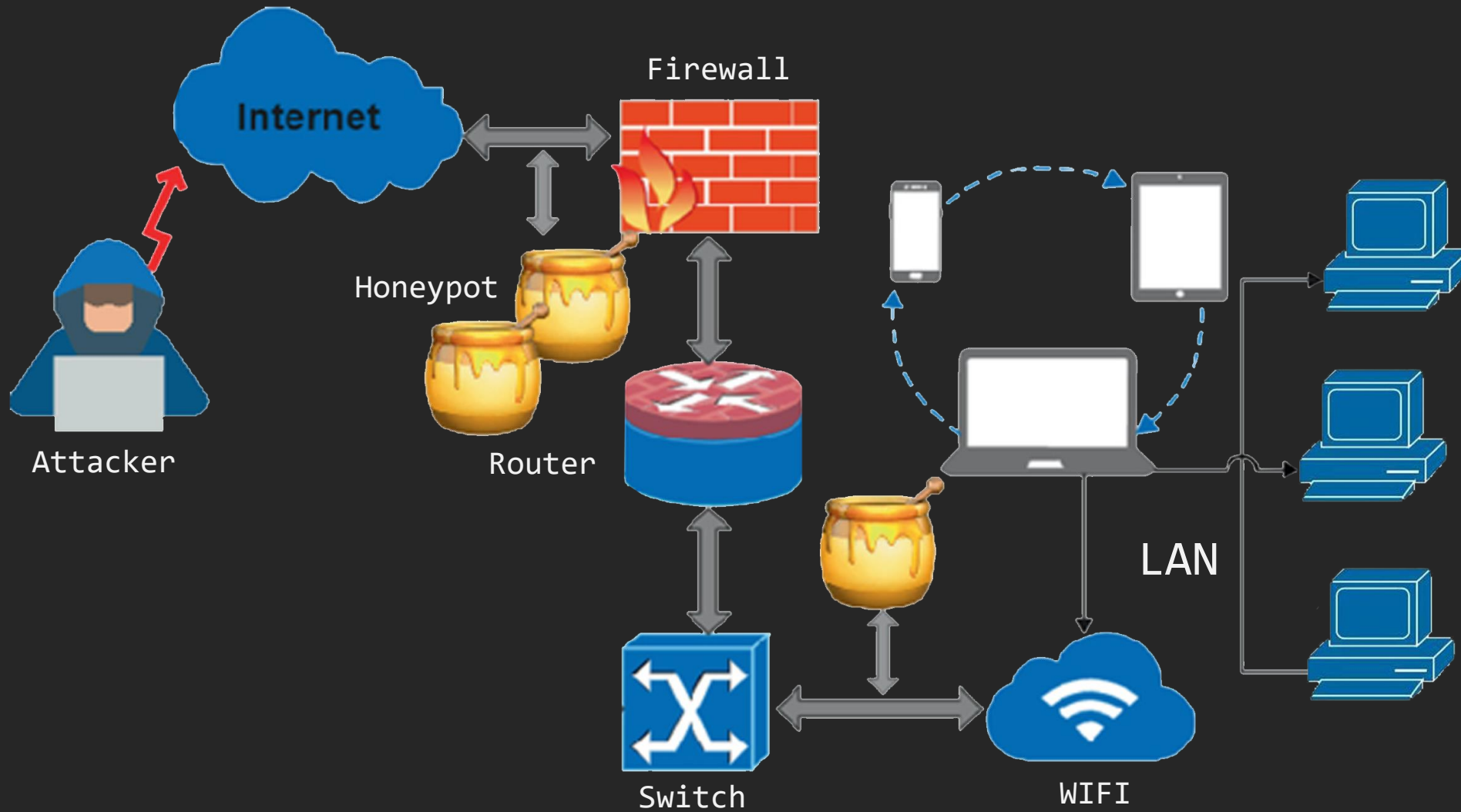
## High Interaction Honeypot:

- Type of honeypot that simulates many aspects of a real operating system and applications.
- Allows for deep interaction with the attacker.
- Tends to be more difficult to set up and requires more intensive maintenance.

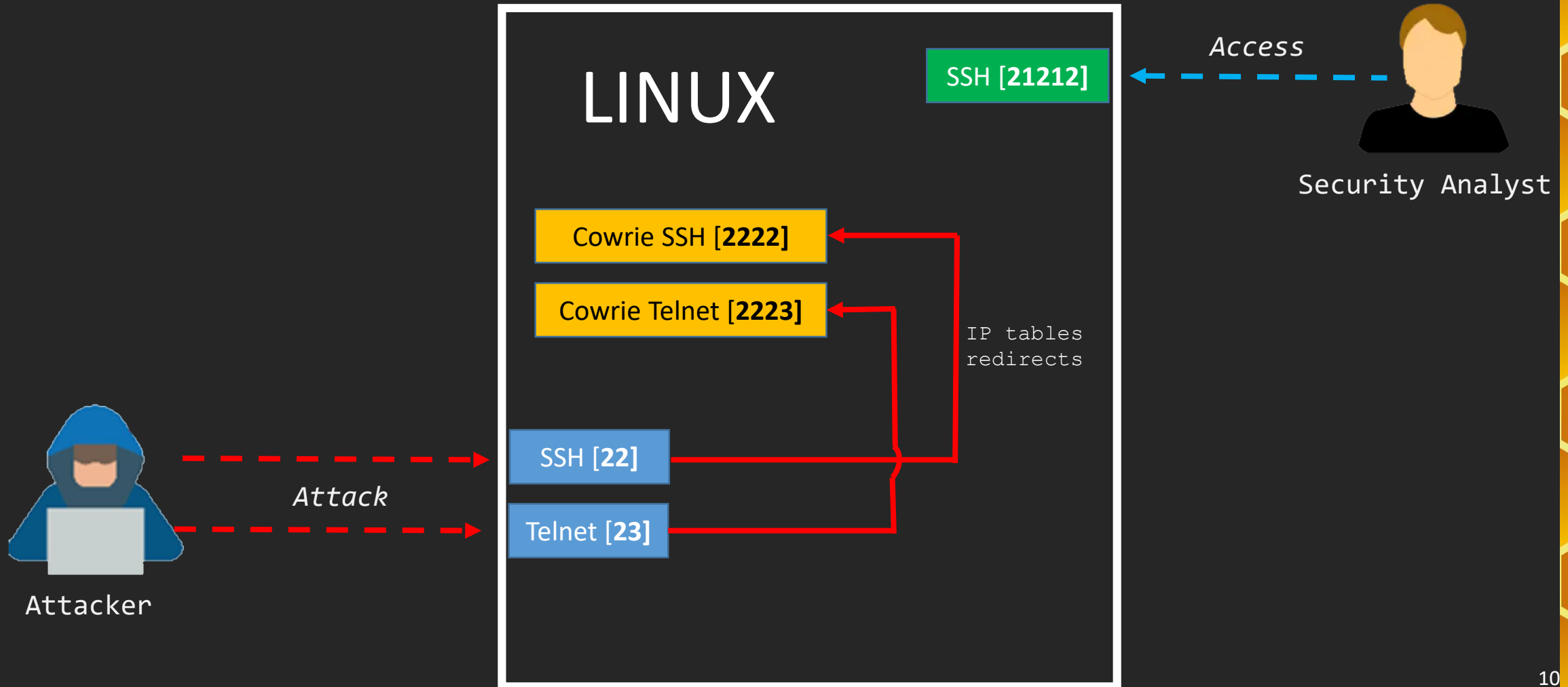
Example: Setup a real system with services enabled



# How to Deploy Honeytrap?



# How scenario of Honeyypot?



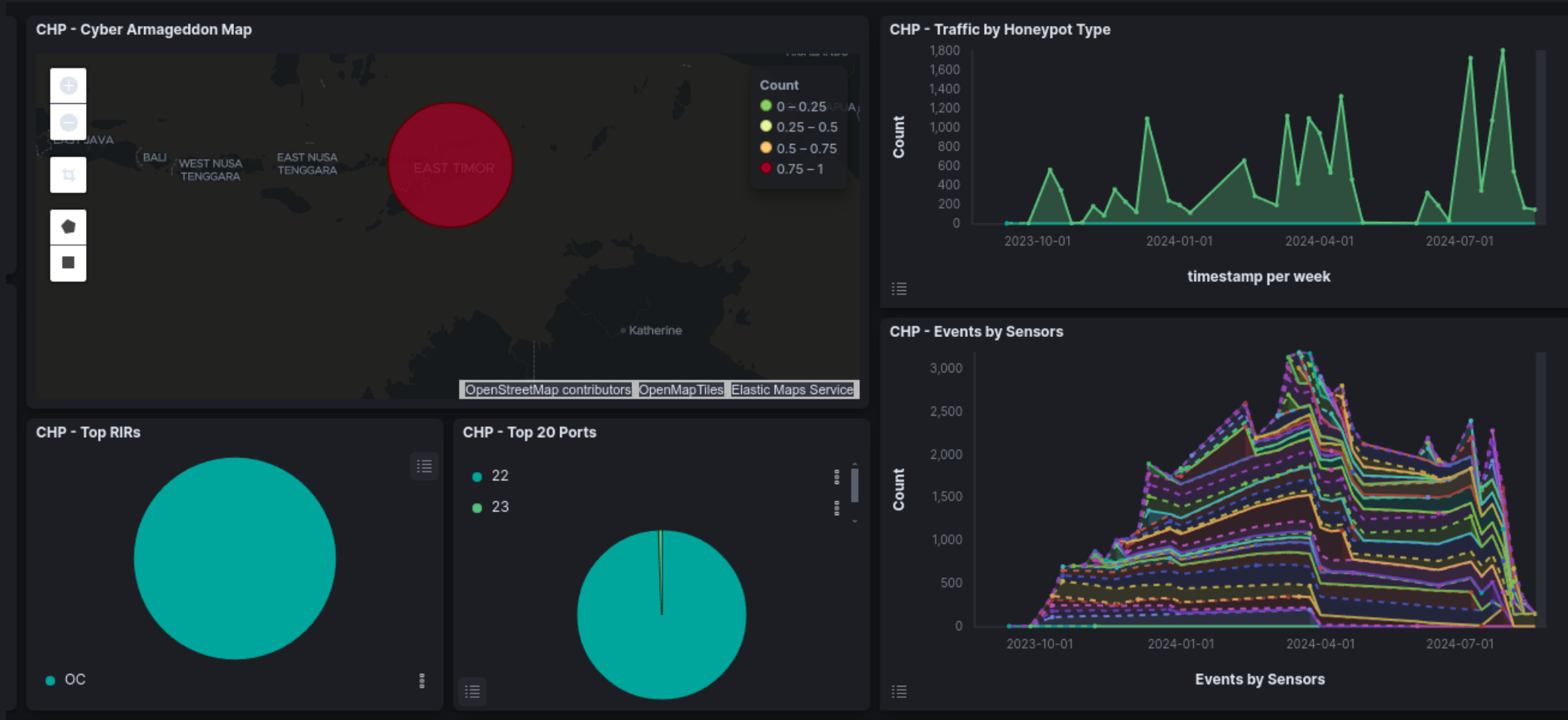
# Honeypot Software (1)

Category	Name	Feature / Purpose
SSH	Cowrie	SSH and Telnet Honeypot designed to log brute force attacks.
	Kippo	SSH Honeypot designed to log brute force attacks.
Database	mysql-honeypotd	low interaction MySQL honeypot written in C.
	ElasticPot	an Elasticsearch Honeypot.
Web	Glastopf	Web Application Honeypot.
	Wordpot	WordPress Honeypot.
	Drupo	Drupal Honeypot.
Service	DDospot	NTP, DNS, SSDP, Chargen and generic UDP-based amplification DDoS honeypot.
	Dionaea	using libemu to detect shell codes (ftp, http, mssql, mysql).

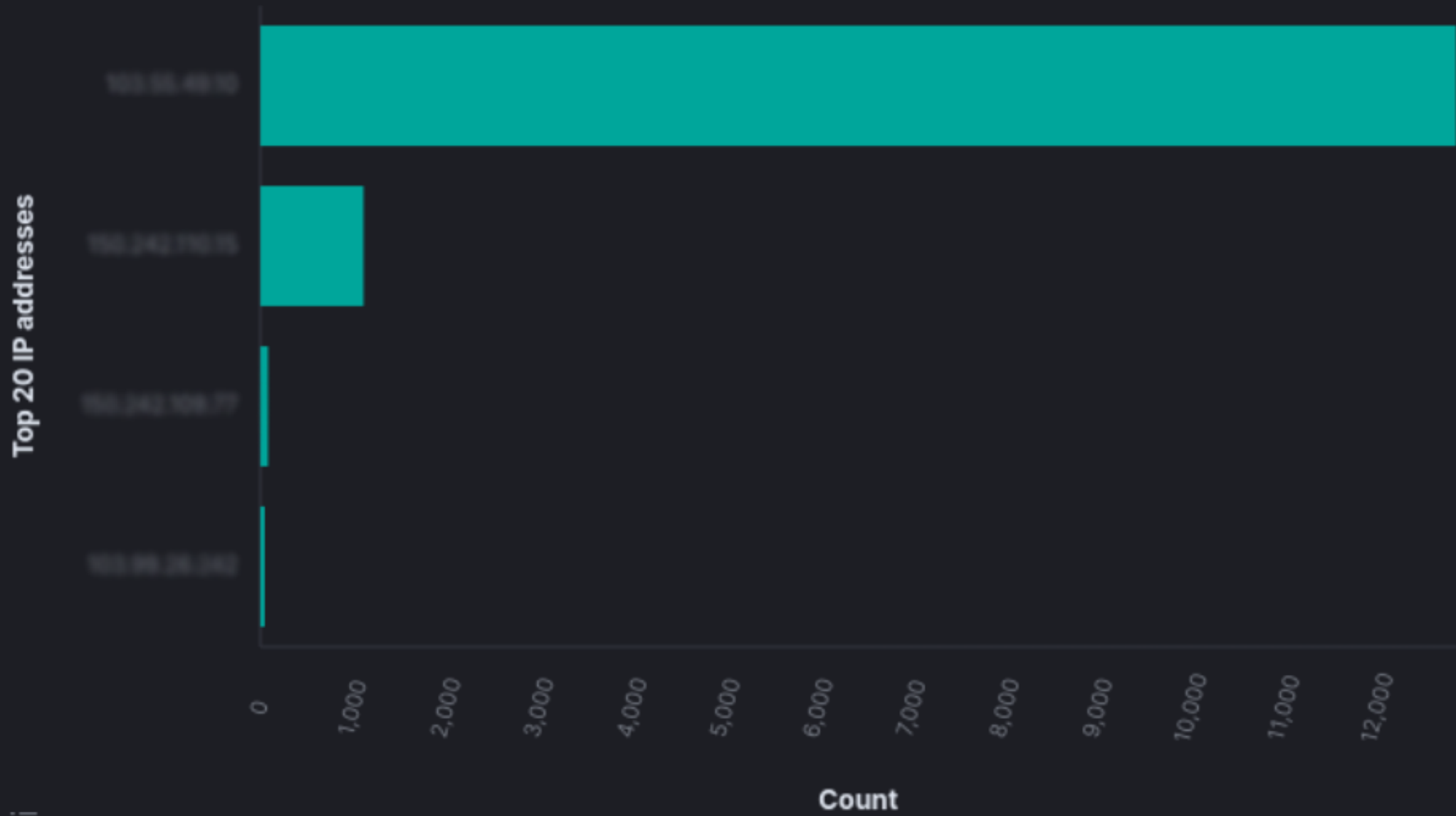
# Honeypot Software (2)

Category	Name	Feature / Purpose
Honeypot deployment	Community Honey Network	deploys honeypots and honeypot management tools.
	Modern Honey Network	Multi-snort and honeypot sensor management
	T-Pot	is the all in one, optionally distributed, multi arch (amd64, arm64) honeypot platform, supporting 20+ honeypots.
	Community Honey Network	deploys honeypots and honeypot management tools.
USB	Ghost	for malware that propagates via USB storage devices.
Server	Amun	Vulnerability emulation honeypot.
Honeytokens	CanaryTokens	Self-host able honey token generator and reporting dashboard.

# Example/use case



### CHP - Top 20 IP addresses



||||



ironman changeme bpoint V398LjABNszc Qaz123qaz Password17 Z123456z abcd123456789  
1111 fernando Wy.123456 Galaxy123 elk 1qazxsw2 123456789000 1q2w3e4r5t6y florin1989  
kali flatron1 cartorio test12345678 patrick123 secret 111...aaa 123qwe1 Password developer  
david123 Qwert123@ 123456789Ab P@\$w0rd#123456 !@#QWEasd andrea multimedia admin123456@  
10 P@ssw0rd1 11111111 elastic@123 3245gs5662d34 ubuntu20svm Linux a1b2c3d4  
ding Aa123456 test1234 Aa888888 p@ssw0rd ftp123 666666 Testing@123  
alliswell 123!@# Hs123456! password@123 pass 12 123321 1234567 test123 acs access 321 abc test123456 a123..+  
1q@W3e\$R red 121212 ad1tzprinde 345gs5662d34 12345678 123456789 1qaz@WSX P@ssw0rd123 nvidia 168168 Tj123456  
diego !qwe!@#123 !@#QAZ123 admin 000000 Aa@123456 0000 1q2w3e Password123 ray 5rdx\$ESZ a!  
@ 123qweASD test anil Admin123! P@ssw0rd password 123456 123 12345 1q2w3e4r 1234qwer Password@1 556677 assist  
ABC1234%^ passwd 11223344 Abcd1234 root 123123 password123 M3gaP33! 123qwe qwertyuiop LI123456 qwer123. Asd123456  
black asdf !@#qweASDzxc 1qq2w3e4r5t 1qaz2wsx abc123 1234567890 admin123 123.com Admin@123 !QAZ@wsx Passw0rd!!  
Zxcv1234. 123qweasd centos8svm @123qwe Password@123 passw0rd neeraj@123 mysql 123465. carl acct erpNext  
debug Qwerty123 !1qaz@2wsx#3edc minecraft gitpass guest qqqq123 1234Root Qwerty654321 ansible@123  
asd@123321 Wy123456! 87654321 12345679a 123456qwerty 1qaz!QAZ Aa12341234 rural live  
francisco 14 a1 deployer admin\_123 Sm123456. Pa55word ess Qp123456789 a12345678. abcl1234567 changeme123  
cameron dev@ jake lixiao

ssh\_password.keyword: Descending - Count





// LAST SEEN: 2024-08-14

### Open Ports

1723 8291

// 1723 / TCP

1692829151 | 2024-08-14T21:46:42.893366

### PPTP

PPTP:

Firmware: 1  
Hostname: MikroTik  
Vendor: MikroTik

// 8291 / TCP

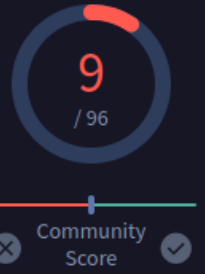
-919922242 | 2024-08-06T06:14:17.986776

### MikroTik Winbox

MikroTik Winbox:

```
list:
  advtool.jpg: 7.15.3
  container.jpg: 7.15.3
  dhcp.jpg: 7.15.3
  hotspot.jpg: 7.15.3
  icons.png: 7.15.3
  icons24.png:
  icons32.png:
  ipv6.jpg: 7.15.3
  ppp.jpg: 7.15.3
  roteros.jpg: 7.15.3
  secure.jpg: 7.15.3
  ups.jpg: 7.15.3
  wave2.jpg: 7.15.3
  wlan6.jpg: 7.15.3
```





9/96 security vendors flagged this URL as malicious

Reanalyze Search Graph API

Status: 504 | Content type: text/html | Last Analysis Date: 15 days ago

text/html ip

DETECTION DETAILS COMMUNITY

Crowdsourced context

HIGH 0 MEDIUM 0 LOW 0 INFO 1 SUCCESS 0

Find more information on CrowdSec CTI - according to source CrowdSec - 2 months ago  
Behaviors: SSH Bruteforce

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Malicious	BitDefender	Phishing
Criminal IP	Malicious	CrowdSec	Malicious
G-Data	Phishing	GreenSnow	Malicious
IPsum	Malicious	Lionic	Malicious
SOCRadar	Malicious	AlphaSOC	Suspicious
ArcSight Threat Intelligence	Suspicious	BlockList	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean

## IP Abuse Reports for 103.55.49.10

This IP address has been reported a total of **4,178** times from 943 distinct sources. 103.55.49.10 was first reported on December 2nd 2023, and the most recent report was **31 minutes ago**.



**Recent Reports:** We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	IoA Timestamp in UTC	Comment	Categories
<a href="#">serverobot.de</a>	2024-08-19 03:06:37 (31 minutes ago)	Aug 19 05:05:35 mailserver sshd[915068]: pam_unix(sshd:auth): authentication failure; logname= uid=0 ... <a href="#">show more</a>	<span>Brute-Force</span> <span>SSH</span>
<a href="#">taipei101.xyz</a>	2024-08-19 02:28:06 (1 hour ago)	Aug 18 22:22:52 us1-bms-f7b96252 sshd[479153]: Failed password for invalid user csserver from 103.55 ... <a href="#">show more</a>	<span>Brute-Force</span> <span>SSH</span>
<a href="#">agreppin</a>	2024-08-19 02:27:56 (1 hour ago)	2024-08-19 02:27:56 albla SSH	<span>Brute-Force</span> <span>SSH</span>
<a href="#">PulseServers</a>	2024-08-19 02:21:49 (1 hour ago)	SSH Brute-Force Attack on a server hosted by PulseServers.com - CA10 Honeypot ...	<span>Brute-Force</span> <span>SSH</span>
<a href="#">MazenHost</a>	2024-08-19 01:16:01 (2 hours ago)	Aug 19 04:14:13 alek-test sshd[964959]: pam_unix(sshd:auth): authentication failure; logname= uid=0 ... <a href="#">show more</a>	<span>Brute-Force</span> <span>SSH</span>
<a href="#">jbgalleries.net</a>	2024-08-19 00:11:51 (3 hours ago)	Multi Failed Login Attempts	<span>Brute-Force</span> <span>SSH</span>
<a href="#">nohacefaltapapel-et.net</a>	2024-08-18 23:59:58 (3 hours ago)	2024-08-19T01:58:49.102771milloweb sshd[4591]: Failed password for invalid user mail from 103.55.49 ... <a href="#">show more</a>	<span>Brute-Force</span> <span>SSH</span>
<a href="#">LoNET</a>	2024-08-18 21:33:02 (6 hours ago)	Report 1303604 with IP 1935787 for SSH brute-force attack by source 2310384 via ssh-honeypot/0.2.0+h ... <a href="#">show more</a>	<span>Brute-Force</span> <span>SSH</span>



# Benefit of Honeypot

- ***Early Detection:***  
Honeypot can detect attacks before they reach the actual system.
- ***Attacker Behavior:***  
Allows in-depth analysis of attacker attack methods and tactics.
- ***Information Gathering:***  
Provides valuable data about security threats that can be used to improve overall security.
- ***Education and Training:***  
Honeypot can be used to train and educate security personnel about possible attacks.



**Happy Honeypotting....!!!**