

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Ciencias Exactas y Naturales e Ingeniería

**TRABAJO FINAL DE
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**

ANÁLISIS DE T-POT UN HONEYPOT OPEN SOURCE

CANDIDATO: FABRICIO GABRIEL TORRICO BARAHONA
TUTOR DE TRABAJO FINAL: DR. PEDRO HECHT



CONTENIDO A DESARROLLAR

01

OBJETIVOS Y TEORÍA

02

ANÁLISIS DE T-POT

03

PRUEBA DE CONCEPTO

04

CONCLUSIONES

01

OBJETIVOS Y TEORÍA





OBJETIVO GENERAL

Analizar y describir en detalle la arquitectura del honeypot T-Pot, permitiendo un entendimiento de cada uno de sus componentes y la forma en que trabajan de manera conjunta



OBJETIVOS ESPECÍFICOS

II

Analizar en profundidad la arquitectura y herramientas que componen el honeypot T-Pot



Mostrar la utilidad de los honeypot, su clasificación, implementación, ventajas y desventajas



III

Plantear posibles mejoras o desarrollo de nuevos módulos para el honeypot T-Pot





**Un honeypot, sistema trampa o señuelo,
es aquel recurso de seguridad que es empleado para
investigación o producción,
que espera tener algún grado de interacción con los atacantes
y cuyo valor radica en ser atacado, comprometido e investigado**

VENTAJAS Y DESVENTAJAS



Valor de los datos

Simplicidad

Retorno de inversión

Pocos recursos de hardware

**Ayuda al personal de TI y
seguridad**



Riesgo

Huellas digitales

Campo de visión estrecho

**Personal y tiempo para
análisis y mantenimiento**

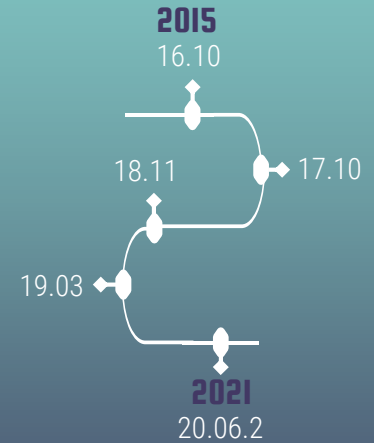


02

ANÁLISIS DE T-POT



LIDERAZGO Y DESARROLLO

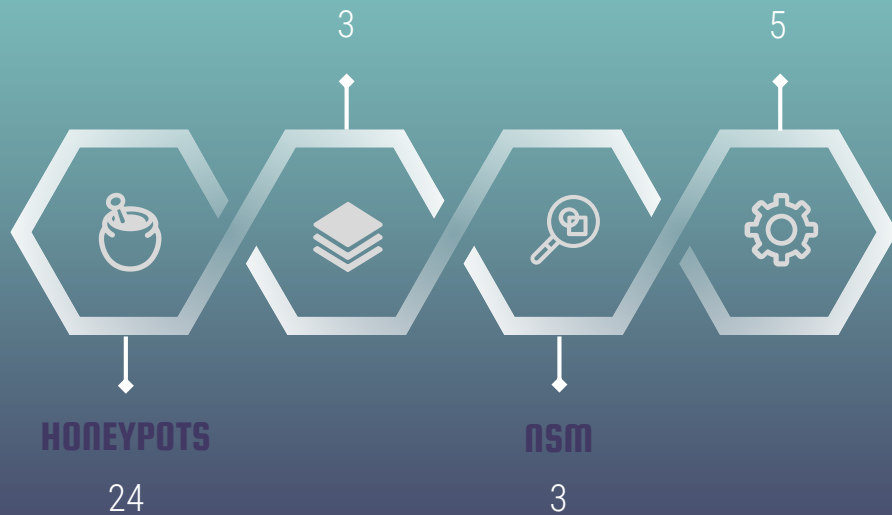


COMPONENTES



ELK STACK

HERRAMIENTAS





HONEYPOTS



docker

HONEYPOTS

Cisco ASA



CVE 2018-0101
RCE y DoS
8443, 5000udp

Conpot



ICS/SCADA

DDoSPot



SSDP
CharGEN
UDP



19, 53, 123 Y 1900

Dionaea

MSSQL
FTP
UPnP
HTTP
MySQL



PPTP
SIP
SMB
TFTP
Mongo DB

EndleSSH



Tarpit
22

ADB Honey



Android Debug Bridge
5555

Citrix ADC



CVE 2019-19781
Path Traversal
443

Cowrie



22 y 23

Dicompot



Digital Imaging and
Communications
in Medicine
11112

ElasticPot



9200

Heralding

HTTP/S
POP3/S
Telnet
SMTP
SSH
FTP



PostgreSQL
IMAP/S
Socks5
MySQL
RDP
VNC

HONEYPOTS

Honeypots



Honey SAP



SAPRouterService
3299

Log4Pot



CVE-2021-44228

Medpot



Fast Healthcare
Interoperability
Resources
2575

Redis Honeypot



6379

Hell Pot



Motor de Markov
80

HoneyPy



Telnet, DNS, NTP,
SMTP, TFTP, HTTP,
etc.

IPP Honey



631

Mailoney



25

RDPY



3389

Snare & Tanner

LFI **NGINX** XSS
RFI CMD-EXEC

80

HONEYPOTS

Glutton



Modo Host
NextGen

Honeytrap



Modo Host
Otra Instalación

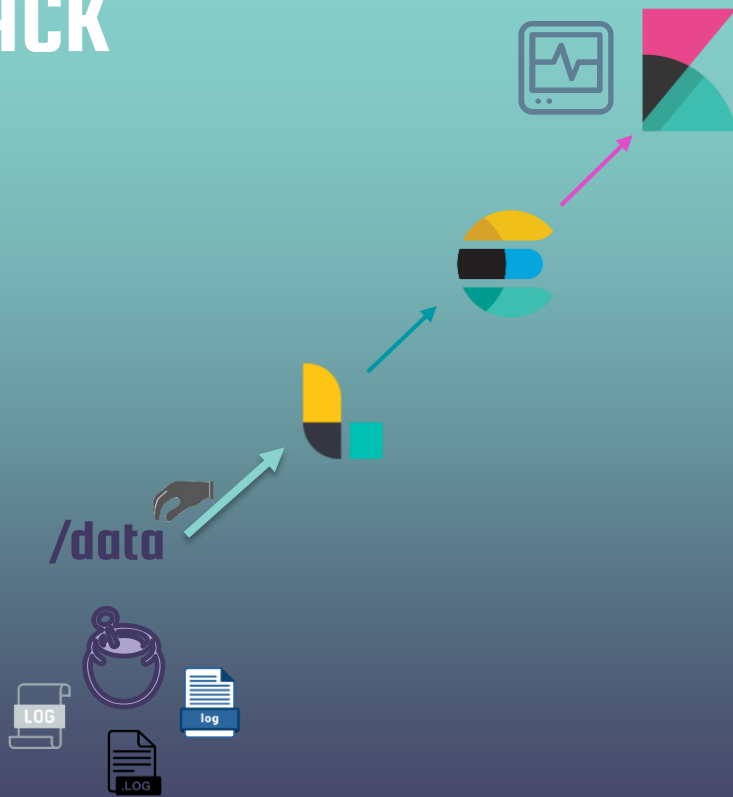
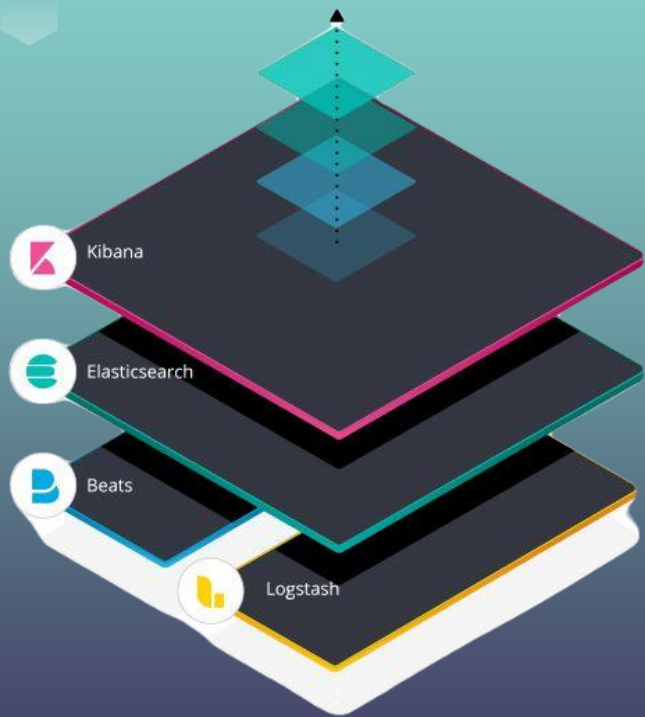


ELK STACK



docker

ELK STACK





nsm



docker



NETWORK SECURITY MONITOR



**Fingerprint
All The Things**

JA3, HASSH,
RDFP, HTTP



**Passive Operating
System Fingerprinting**

SO, SW, Falsificaciones
X-Mailer o User-Agent



Suricata

Firmas y
Scripting LUA

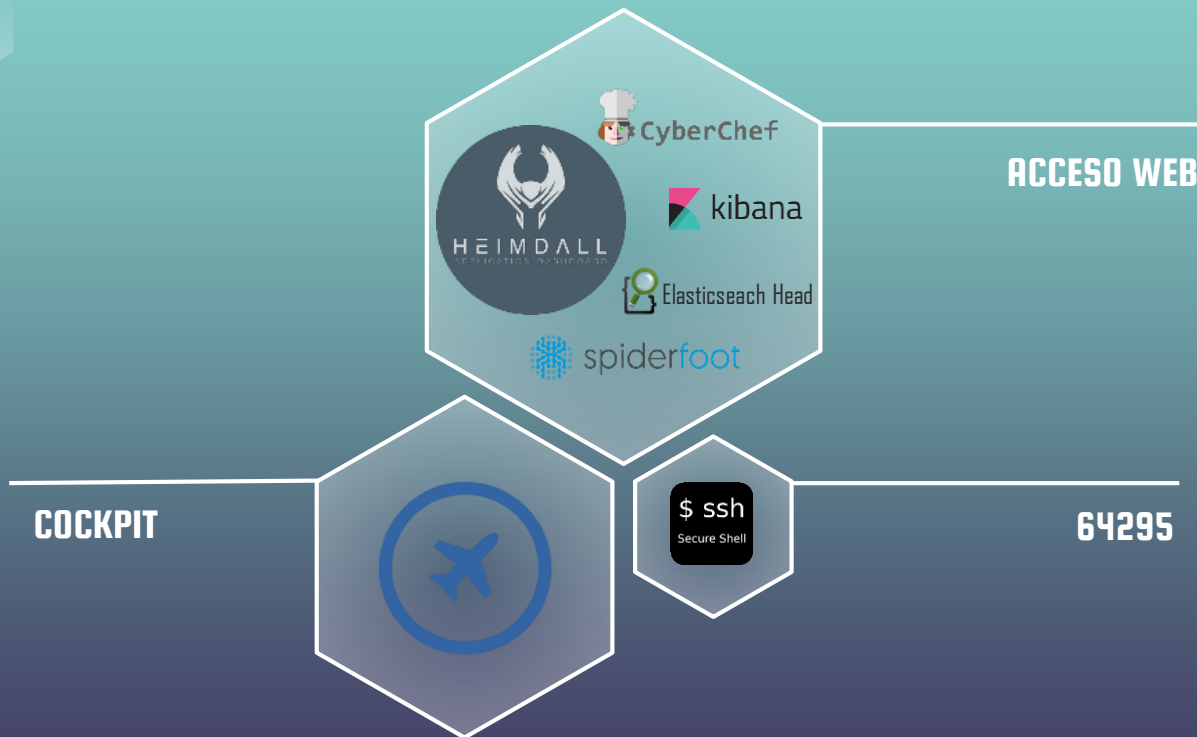


HERRAMIENTAS

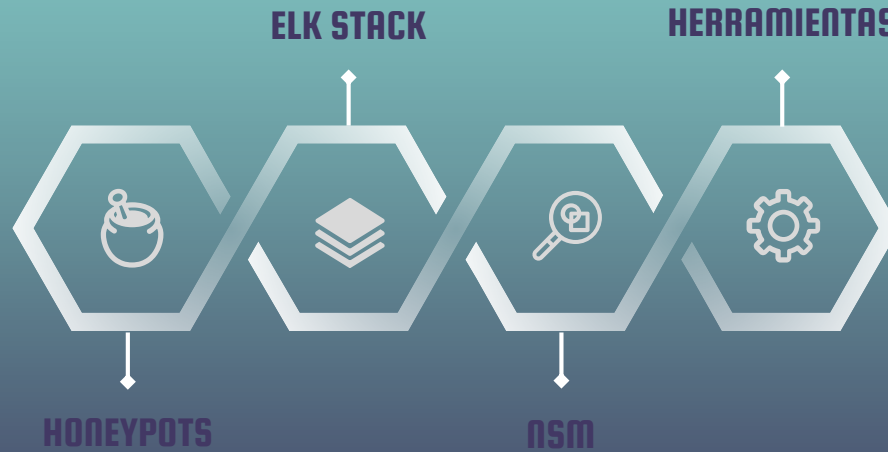


docker

HERRAMIENTAS

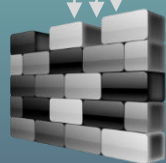


FUNCIONAMIENTO SINERGICO



CONEXIONES

RADAR
T-Sec



Iptables



fatt.

pOf

SURICATA



CISCO

LOG4J



Glutton



Honeytrap



\$ ssh
Secure Shell



CyberChef



Elasticsearch Head



spiderfoot

kibana

docker



/data

Stack





03

PRUEBA DE CONCEPTO





📦 Crédito de prueba gratuita

USD300
Crédito de prueba gratuita
De USD300

90
Días restantes
Finaliza el 24 de mayo de 2022

No se te facturará durante la prueba gratuita. Actualiza a una cuenta paga para mantener tus proyectos en ejecución después de la prueba gratuita.

13°C 13:41 23/2/2022

- Debian 10 (Buster)
- 4 vCPU
- 16 GB RAM
- 128 GB SSD

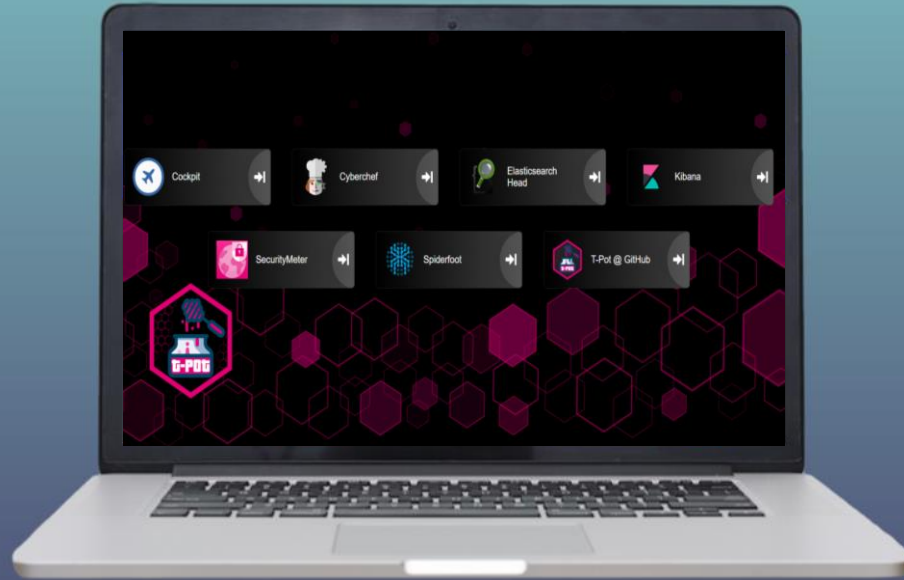
[Choose Your T-Pot Edition]

Required: 8GB RAM, 128GB SSD
Recommended: 8GB RAM, 256GB SSD

STANDARD	Honeypots, ELK, NSM & Tools
LOG4J	Log4jPot, ELK, NSM & Tools
SENSOR	Just Honeypots, EWS Poster & NSM
INDUSTRIAL	Conpot, RDPY, Vnclospot, ELK, NSM & Tools
COLLECTOR	Heralding, ELK, NSM & Tools
NEXTGEN	NextGen (Glutton, HoneyPy)
MEDICAL	Dicompot, Medpot, ELK, NSM & Tools

100%

< OK >



04

CONCLUSIONES



RECOMENDACIONES

Documentación no actualizada



Web personalizada y Data Sanatization



Otros honeypots

(Laravel Application Honeypot, Nodepot,
phpmyadmin honeypot, tomcat-manager-honeypot)



Security Dashboard Local



CONCLUSIONES



Contenedores. Escalabilidad y seguridad



Excelente caso de estudio



Comunidad activa



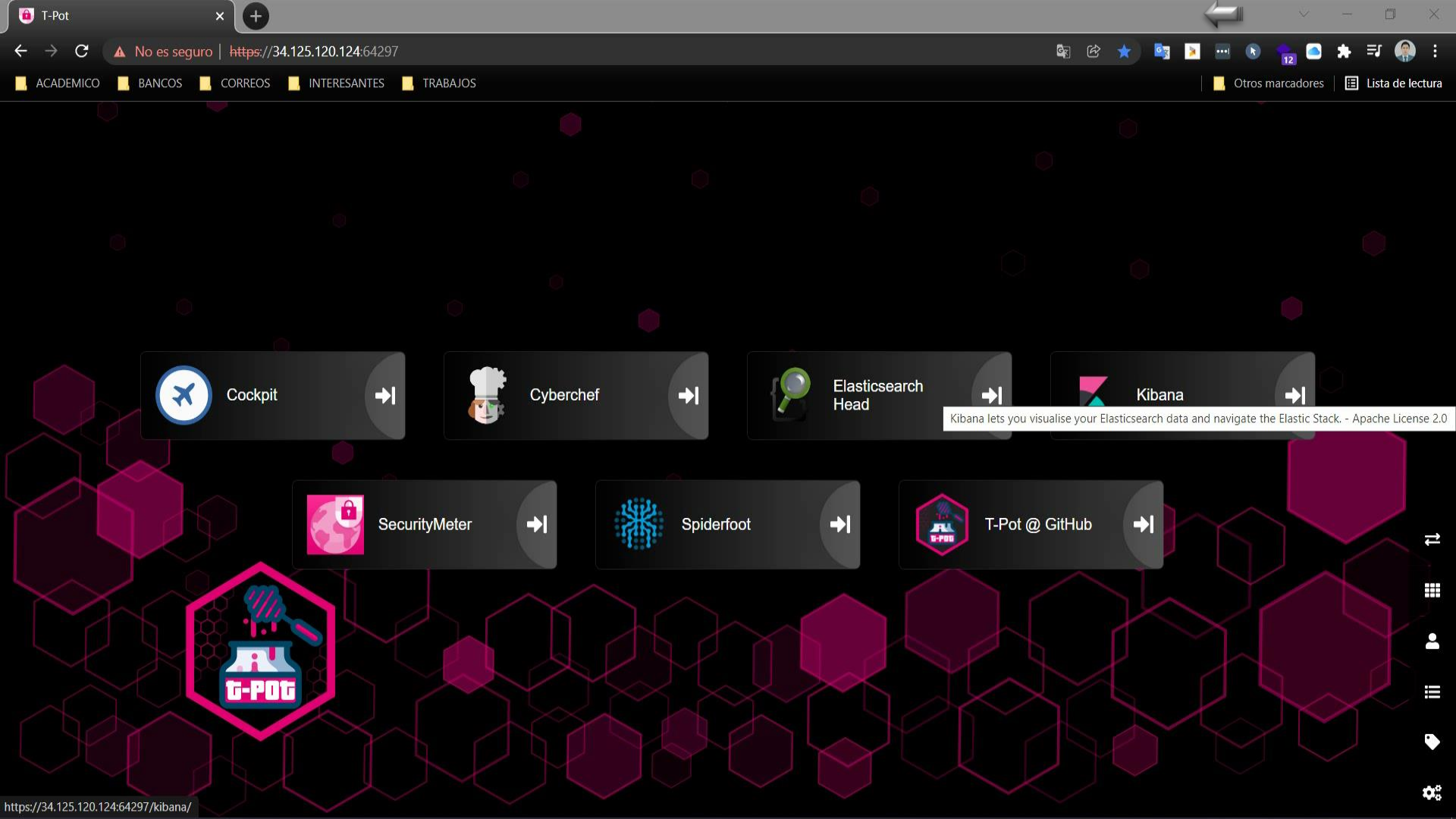
Ayuda a justificar inversiones

GRACIAS

¿Preguntas?

*Nunca consideres el estudio como
una obligación, sino como una
oportunidad para ingresar en el bello
y maravilloso mundo del saber*

Albert Einstein



Cockpit



Cyberchef



Elasticsearch
Head



Kibana



Kibana lets you visualise your Elasticsearch data and navigate the Elastic Stack. - Apache License 2.0



SecurityMeter



Spiderfoot



T-Pot @ GitHub

