

# Honeypot

Resiliencia y conocimiento del adversario



Universitat  
Oberta  
de Catalunya

---

**Angel Manuel Camuñas  
Hilario**

Ingeniería Informática  
Seguridad corporativa

**Nombre Tutor/a de TF**

Jorge Miguel Moneo

**Profesor/a responsable de la  
asignatura**

Pau Perea Paños

**Fecha Entrega**

11/06/2024



A) Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada [3.0 España de Creative Commons](https://creativecommons.org/licenses/by-nc-nd/3.0/es/)

## **B) GNU Free Documentation License (GNU FDL)**

Copyright © 2024 Angel Manuel Camuñas Hilario.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.

A copy of the license is included in the section entitled "GNU Free Documentation License".

## **C) Copyright**

© (Angel Manuel Camuñas Hilario)

Reservados todos los derechos. Está prohibido la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la impresión, la reprografía, el microfilme, el tratamiento informático o cualquier otro sistema, así como la distribución de ejemplares mediante alquiler y préstamo, sin la autorización escrita del autor o de los límites que autorice la Ley de Propiedad Intelectual.

<b>Título del trabajo:</b>	Honeypot: resiliencia y conocimiento del adversario
<b>Nombre del autor:</b>	Angel Manuel Camuñas Hilario
<b>Nombre del director/a:</b>	Jorge Miguel Moneo
<b>Nombre del PRA:</b>	Pau Perea Paños
<b>Fecha de entrega:</b>	11/06/2024
<b>Titulación o programa:</b>	Ingeniería Informática
<b>Área del Trabajo Final:</b>	Seguridad Corporativa
<b>Idioma del trabajo:</b>	Castellano
<b>Palabras clave:</b>	honeypot, honeynet, ciberengaño, T-Pot, amenaza, resiliencia, inteligencia

### Resumen del Trabajo

En el panorama de seguridad actual, las organizaciones se enfrentan a amenazas constantes que desafían la integridad de sus sistemas. Los métodos de seguridad tradicionales resultan inadecuados frente a ataques sofisticados, lo que impulsa la necesidad de sistemas como honeypots y honeynet. Los honeypots actúan como señuelos para atraer y desviar a posibles atacantes, mientras que las honeynet, redes interconectadas de honeypots, proporcionan una mayor cobertura.

El principal desafío de este trabajo es mejorar la detección y respuesta a estas amenazas de seguridad. Esto implica identificar amenazas no capturadas por los sistemas convencionales, entender las tácticas de los atacantes, evaluar la efectividad de las defensas existentes y mejorar las capacidades de respuesta ante incidentes. La implementación estratégica de honeypots a través de la solución virtualizada de T-Pot, junto con el análisis de los datos recopilados, proporciona una oportunidad para abordar estas necesidades.

La inteligencia adquirida dentro del marco de seguridad puede incluir patrones de comportamiento de los atacantes, tácticas utilizadas, vulnerabilidades explotadas y otros datos para fortalecer las defensas de seguridad de la organización.

**Abstract**

In today's security landscape, organizations face constant threats that challenge the integrity of their systems. Traditional security methods are proving inadequate against sophisticated attacks, thus driving the need for systems like honeypots and honeynets. Honeypots act as decoys to attract and divert potential attackers, while honeynets, interconnected networks of honeypots, provide expanded visibility.

The main challenge of this work is to enhance the detection and response to these security threats. This involves identifying threats not captured by conventional systems, understanding attackers' tactics, evaluating the effectiveness of existing defenses, and improving incident response capabilities. The strategic implementation of honeypots through the T-Pot virtualization solution, along with the analysis of collected data, provides an opportunity to address these needs.

The intelligence gained within the security framework may include attacker behavior patterns, tactics used, exploited vulnerabilities, and other data to strengthen the organization's security defenses.

## Dedicatoria

Cada segundo empleado, cada palabra escrita en esta memoria están dedicados a mi familia, pues cada uno de ellos forman parte de mi éxito:

A mi esposa Mely, por su infinita paciencia, apoyo y motivación inicial para embarcarme en este viaje de conocimiento y logros

A mis hijos Angel y Carmen, por su apoyo incondicional y ánimos constantes

A mi hermana Mamen, por ser mi referente, siendo un ejemplo de esfuerzo y dedicación

A mi hermana Lales, por su motivación y por hacer realidad mi sueño

A mi hermana Mari Mar por enseñarme a no bajar los brazos, y que el esfuerzo, constancia y paciencia tienen su recompensa

A mis hermanas Flora y María José, por su apoyo y ánimos

A mis padres Angel y Mari Carmen, por su amor infinito y eterno

A mi suegra Carmeli, por su amor, sus velas y desvelos

A mi suegro Rogelio por cada palabra de aliento y cariño

A mis cuñadas Marta y Marian, por sus ánimos y por aguantar mis charlas en momentos de frustración

A mi amigo Are, por cada palabra que me ha dedicado lleno de orgullo

¡¡GRACIAS!!

## Tabla de contenido

1	Introducción .....	8
1.1	Contexto y justificación.....	8
1.2	Objetivos.....	9
1.2.1	Generales.....	9
1.2.2	Específicos .....	10
1.3	Impacto en sostenibilidad, ético-social y de diversidad .....	11
1.4	Enfoque y método seguido.....	11
1.5	Planificación del trabajo .....	12
1.6	Breve resumen de productos obtenidos .....	15
2	Estado del arte .....	15
2.1	Historia: orígenes y conceptos Iniciales.....	16
2.2	Valoración .....	18
2.2.1	Aplicaciones del honeypot .....	18
2.2.2	Papel en la seguridad corporativa.....	19
2.2.3	Ventajas.....	19
2.2.4	Desventajas .....	20
2.3	Comparativa con otros sistemas de detección.....	20
2.3.1	Honeypot.....	20
2.3.2	IDS.....	21
2.3.3	Cortafuegos .....	21
2.4	Clasificación .....	21
2.4.1	Interacción.....	22
2.4.2	Sistema .....	22
2.4.3	Comportamiento .....	23
2.4.4	Rol.....	24
2.5	Ubicación en la red .....	24
2.5.1	Interna .....	24
2.5.2	Externa.....	24
2.5.3	DMZ .....	24
2.5.4	Varias zonas.....	24
3	Honeynet.....	25
3.1	Introducción.....	25
3.2	Objetivo honeynet .....	26

3.2.1	Control de datos .....	26
3.2.2	Captura de datos .....	26
3.2.3	Recopilación de datos.....	27
3.2.4	Generación de alertas .....	27
3.3	Arquitectura honeynet .....	27
3.3.1	Generación I .....	27
3.3.2	Generación II y III.....	27
3.4	Honeynet virtual .....	27
4	T-Pot .....	28
4.1	Historia.....	28
4.2	En detalle .....	29
4.2.1	Aplicaciones.....	29
4.2.2	Ventajas.....	30
4.2.3	Desventajas .....	31
4.2.4	Implementación .....	31
5	Ciberseguridad en España .....	31
5.1	Estado de la seguridad corporativa .....	32
5.2	Alineación entre estrategia de seguridad y negocio .....	32
5.3	Trabajo remoto y amenazas emergentes .....	32
5.4	Conciencia y aplicación de medidas .....	32
6	Hipótesis planteadas .....	32
7	Descripción de experimentos a llevar a cabo.....	33
8	Materiales y métodos .....	33
8.1	Diseño de la infraestructura .....	33
8.1.1	Entorno de pruebas.....	34
8.1.2	Hardware.....	34
8.1.3	Software .....	34
8.1.4	Componentes de seguridad.....	34
8.1.5	Red.....	34
8.1.6	Ubicación estratégica de los honeypots.....	35
8.2	Despliegue de T-Pot.....	36
8.2.1	Instalación y configuración en un entorno controlado .....	36
8.2.2	Personalización de la configuración .....	36
8.2.3	Fortaleciendo T-Pot .....	37
8.3	Configuración de honeypots básicos.....	40

8.3.1	Configuración de honeypots según el análisis previo .....	41
9	Resultados. Caso práctico en monitorización y recopilación de datos.....	45
9.1	Herramientas utilizadas en análisis y monitorización de datos.....	45
9.1.1	Propias de T-Pot .....	45
9.1.2	En línea .....	46
9.2	Análisis de datos recopilados.....	47
9.2.1	Tratamiento y estudio de los datos obtenidos.....	47
9.3	Amenazas detectadas .....	47
9.3.1	Ataque DDoS .....	48
9.3.2	Ataque por zona geográfica .....	51
9.3.3	Ataques donde se reconocen IOC: Direcciones IP, dominios y puertos.....	53
9.3.4	Ataque con explotación de vulnerabilidades .....	58
9.3.5	Inteligencia sobre explotación de vulnerabilidades.....	60
9.3.6	Ataques a servicios no usados.....	60
10	Evaluación de eficacia y generación de informes .....	61
11	Opiniones finales.....	61
11.1	Resultado y conclusión .....	61
11.2	Trabajos futuros.....	62
12	BIBLIOGRAFÍA Y REFERENCIAS CONSULTADAS .....	63
13	Glosario .....	69
14	Anexo 1.....	71
15	Anexo 2.....	75



## ILUSTRACIONES

<i>Ilustración 1 - pirámide del dolor [2]</i> .....	9
<i>Ilustración 2 - diagrama de Gantt</i> .....	14
<i>Ilustración 3 - Evolución tecnológica de engaño</i> .....	16
<i>Ilustración 4 - ejemplo de ubicación honeypot en la red</i> .....	18
<i>Ilustración 5 - Clasificación de un honeypot [26]</i> .....	21
<i>Ilustración 6 - arquitectura física vs virtual [27]</i> .....	23
<i>Ilustración 7 - Diseño básico de una honeynet</i> .....	26
<i>Ilustración 8 - Arquitectura técnica T-PoT</i> .....	29
<i>Ilustración 9 - configuración DMZ en enrutador</i> .....	35
<i>Ilustración 10 - diagrama de red para T-Pot</i> .....	36
<i>Ilustración 11 - Pantalla de bienvenida con información de acceso</i> .....	36
<i>Ilustración 12 - localización archivos configuración docker-compose</i> .....	39
<i>Ilustración 13 - ejemplo de obtención de información del sistema</i> .....	40
<i>Ilustración 14 - mapa global de ataques recibidos</i> .....	41
<i>Ilustración 15 - Puertos expuestos más atacados</i> .....	42
<i>Ilustración 16 - honeypots más activos</i> .....	43
<i>Ilustración 17 - enlace simbólico a la plantilla de configuración</i> .....	43
<i>Ilustración 18 - T-Pot iniciado con configuración personalizada</i> .....	44
<i>Ilustración 19 - información de una IP desde Spiderfoot</i> .....	46
<i>Ilustración 20 - detección ataque DDoS DNS</i> .....	49
<i>Ilustración 21 - volumen ataque DDoS DNS</i> .....	49
<i>Ilustración 22 - detección ataque DDoS NTP</i> .....	50
<i>Ilustración 23 - volumen ataque DDoS NTP</i> .....	50
<i>Ilustración 24 - Distribución geográfica de ataques</i> .....	52
<i>Ilustración 25 - Países con mayor actividad de ataque</i> .....	52
<i>Ilustración 26 - Aplicación de filtros en Kibana</i> .....	54
<i>Ilustración 27 - listado IPs maliciosas</i> .....	54
<i>Ilustración 28 - reputación de una IP con Cisco Talos</i> .....	55
<i>Ilustración 29 - análisis de una IP con Virustotal</i> .....	55
<i>Ilustración 30 - comentarios de la comunidad sobre indicador evaluado</i> .....	56
<i>Ilustración 31 - información obtenida de una IP desde Shodan</i> .....	56
<i>Ilustración 32 - obtención de información de una IP con URLScan</i> .....	57
<i>Ilustración 33 - listado de CVE vinculados con los intentos de explotación de vulnerabilidades</i> .....	59
<i>Ilustración 34 - Puertos expuestos más atacados por País</i> .....	60

## 1 Introducción

En el panorama actual de seguridad, las organizaciones se enfrentan a constantes y variadas amenazas que buscan comprometer la integridad, confidencialidad y disponibilidad de sus sistemas y datos. Estas amenazas pueden provenir de actores maliciosos externos, como hackers y grupos de ciberdelincuentes, así como de amenazas internas inesperadas.

Así, uno de los desafíos principales para las organizaciones es la detección temprana y efectiva de estas amenazas. Con frecuencia, los sistemas de seguridad tradicionales no suelen ser suficientes para detectar o incluso prevenir ataques sofisticados y desconocidos, y es aquí donde entran en juego los sistemas de honeypot y honeynet.

### 1.1 Contexto y justificación

La necesidad que se aborda es la de desarrollar sistemas más resilientes y adquirir un conocimiento profundo y actualizado sobre las amenazas de seguridad constantes a las que se enfrentan las empresas de manera continua.

Este tema se considera relevante debido al incremento constante del número de amenazas, la mayor exposición de los sistemas corporativos, y el crecimiento de los sistemas informáticos que operan de manera ininterrumpida. Con la digitalización de numerosos servicios y la creciente dependencia de las tecnologías de la información, la seguridad de los sistemas y datos se ha convertido en una prioridad para las organizaciones.

Pues bien, si se utilizan herramientas que simulen un entorno similar o idéntico al de producción, este entorno actuaría como una primera barrera para recibir los ataques y permitir su estudio, con el fin de adquirir conocimientos que preparen a los entornos de producción para futuros ataques. Estas herramientas son los honeypots.

Por una lado, un honeypot es un sistema señuelo diseñado para simular servicios reales e incluso exponer vulnerabilidades con la intención de atraer al atacante hacia un entorno ficticio controlado y, consiguiendo a la vez, desviarlo del entorno real. Por otro lado, una honeynet es una red de honeypot interconectados, que permite una mayor visibilidad y capacidad de detección por tener la posibilidad de diseminarse por distintos segmentos de red.

De este modo, en una situación en la que sea necesario comprobar el estado de seguridad de un servicio expuesto a internet, como un servicio de correo corporativo o un portal web, lo más prudente es realizar las pruebas en un activo que no esté en producción. Se debe intentar reproducir dicho servicio sin comprometer la operativa normal de la empresa y, mucho menos, exponer deliberadamente la información de la empresa a actores maliciosos que siempre están al acecho.

Aquí es donde entran en acción los honeypots y honeynet, específicamente la plataforma de código abierto T-Pot, como una solución utilizada para el despliegue de honeypots personalizados que permite detectar diferentes tipos de ataques a servicios y protocolos de comunicación utilizados frecuentemente en cualquier corporación del siglo XXI.

No se pretende, únicamente, la detección de estos ataques, sino también mantener un registro con toda la actividad necesaria para aprender sobre los métodos y tácticas utilizados por los atacantes. Esto incluye la recolección de indicadores de compromiso o IOC [1], como hashes, direcciones IP públicas usadas en ataques, nombres de dominio o de host, que sean útiles para aplicarlos a las herramientas de seguridad.



Ilustración 1 - pirámide del dolor [2]

De este modo, el problema principal a resolver está centrado en la necesidad de mejorar la capacidad de detección y respuesta ante amenazas de seguridad. Este objetivo se puede alcanzar mediante la implementación efectiva de sistemas de trampa, como honeypots y honeynet, en el entorno de una organización.

Estas herramientas recopilan datos relevantes sobre los puntos de seguridad que se desea evaluar. Tras el análisis de estos datos y la aplicación de un contexto que facilita la comprensión de las amenazas emergentes, se puede evaluar la efectividad de las defensas existentes y mejorar la capacidad de respuesta ante incidentes de seguridad.

## 1.2 Objetivos

### 1.2.1 Generales

El propósito principal de este proyecto es el uso de T-Pot para la recolección y análisis de datos, con el firme objetivo de transformarlos en información valiosa que pueda ser empleada para potenciar la eficacia de diversas herramientas de seguridad utilizadas en una corporación.

De esta forma, en el contexto de la ciberseguridad, la mera información puede resultar insuficiente, por lo que este proyecto se enfoca en dotar de contexto la información recopilada en el uso de T-Pot, permitiendo su transformación en inteligencia aplicable y en un recurso vital en la lucha constante que se mantiene contra las amenazas.

Mismamente, la inteligencia generada será útil, no solo para contrarrestar ataques genéricos, sino también ataques dirigidos de manera específica, pues al proporcionar

un contexto a la información, bajo el marco de MITRE ATT&CK [3], se puede comprender mejor las tácticas, técnicas y procedimientos empleados por los adversarios, lo que se convierte en un punto facilitador en el desarrollo de estrategias de defensa más robustas y adaptativas.

### 1.2.2 Específicos

Sin embargo, para alcanzar el objetivo principal es necesario afrontar una parte teórica y otra parte práctica con una serie de objetivos específicos de forma eficaz, ya que son de suma importancia por su contribución a alcanzar el principal. A continuación, se enumeran estos objetivos:

#### 1.2.2.1 Parte teórica

- Estudio del honeypot
  - Un poco de historia
- Puesta en valor
  - Aplicaciones del honeypot
  - Papel en la seguridad corporativa
  - Ventajas
  - Desventajas
- Comparativa con otros sistemas de detección
  - Honeypot
  - IDS
  - Cortafuegos
- Clasificación
  - Por aplicación
  - Por interacción
  - Por tipo hardware
  - Por rol
- Ubicación en la red
  - Interna
  - Externa
  - DMZ
  - En conjunto
- Honeynet
  - Definición
  - Honeywall
  - Comparativa con honeypot

#### 1.2.2.2 Parte práctica

- Preparación host
  - Instalación y configuración inicial
  - Bastionado host (Hardening)
  - Anti-Honeypot
- Algunos honeypot básicos
  - SSH
  - RDP
  - Web

- T-Pot
  - Instalación
  - Primera toma de contacto
  - Optimización
  - Recogida de datos
  - Análisis información
  - Análisis de los datos, para conseguir información (si se caza algún archivo con malware, analizarlo con técnicas forense)
  - Integración con otras herramientas (reglas yara, IOC, contexto)
  - Contexto de la información para conseguir inteligencia

### 1.3 Impacto en sostenibilidad, ético-social y de diversidad

**Dimensión sostenibilidad.** La implementación de T-Pot en infraestructura virtual para generar inteligencia de amenazas implica un ahorro en recursos tecnológicos al optimizar la detección y respuesta ante ataques, además de ser innovador en la aplicación de mejoras en la seguridad corporativa. Estas características fomentan el desarrollo tecnológico y la innovación continua en su uso, causando un impacto positivo en los ODS 9 (Industria, Innovación e Infraestructura), 12 (Producción y Consumo Responsables), y 13 (Acción por el Clima).

**Dimensión ético-social.** El uso de T-Pot aplica el software libre y código abierto bajo los requisitos de GPL. Siendo una herramienta de código abierto, garantiza que no se fomente la piratería de software ni impacto negativo en la reputación del propietario o usuario, respetando las buenas prácticas de los profesionales. En este sentido, se considera que su impacto incide de forma positiva en los ODS 8 (Trabajo Decente y Crecimiento Económico) y 16 (Paz, Justicia e Instituciones Sólidas).

**Dimensión diversidad.** En general, el desarrollo de este trabajo basado en el uso y beneficios de honeypots para mejorar la resiliencia de los sistemas de seguridad y conocer mejor las amenazas, no discriminan por etnia, religión, ideología u orientación sexual. Incluso, el estilo que se ha decidido usar para referencias bibliográficas ha sido Vancouver, que incorpora el nombre completo del autor o autora para visibilizar a las mujeres en las bibliografías. También, no afecta a la privacidad ni la propiedad intelectual por estar basado en herramientas desarrolladas, probadas y distribuidas libremente por la comunidad de software libre. Así, se presume un impacto positivo en los ODS 5 (Igualdad de Género) y 10 (Reducción de las Desigualdades).

### 1.4 Enfoque y método seguido

El desarrollo de este trabajo para el conocimiento y estudio de honeypots a través de la herramienta de código abierto T-Pot sigue una combinación de metodología de investigación aplicada y metodología experimental.

La metodología experimental se utilizará en un entorno controlado en el que se instalará y configurará T-Pot, personalizará su configuración para adaptarla a los servicios que

se pretendan simular y a las amenazas que se quieran detectar, con el fin de atraer los ataques de los actores maliciosos.

La investigación aplicada facilitará la identificación de soluciones prácticas para fortalecer la seguridad y resiliencia de los sistemas corporativos frente a diversos riesgos provocados por diferentes actores. A partir de una implementación personalizada de la herramienta T-Pot, adaptada a las necesidades específicas de la entidad, se simplificará la recopilación de datos y la generación de inteligencia para optimizar las configuraciones de las herramientas de seguridad corporativa.

En esta línea, se incluyen distintas fases por las que se irá progresando como son: estudio del estado actual de la seguridad; investigación bibliográfica para conocimiento sobre honeypots y conceptos de seguridad; literatura sobre actores maliciosos y sus tácticas, técnicas y procedimientos (TTP); estudio de la herramienta T-Pot; implantación y personalización de dicha herramienta para adaptarla a escenarios concretos de simulación de servicios; análisis y valoración de los datos recolectados; generación de inteligencia en base al contexto de la información analizada; mejorara de las herramientas de seguridad con el uso de la inteligencia generada.

### 1.5 Planificación del trabajo

Los recursos necesarios para el desarrollo del proyecto incluyen un equipo de alto rendimiento para alojar las máquinas virtuales, software de virtualización adecuado y una conexión de Internet de alta velocidad.

Respecto al equipo portátil de alto rendimiento contará con las siguientes especificaciones técnicas:

- **Microprocesador.** Intel Core i7 de 10ª generación
- **Memoria RAM.** 32 GB, distribuidos en dos módulos de 16 GB cada uno
- **Almacenamiento Interno.** Unidad NVMe SSD de cuarta generación con una capacidad de 1 TB
- **Tarjeta de Red.** Capacidad de 1 Gb

En cuanto al software de virtualización, se empleará Oracle VM VirtualBox [4] en su versión 7.0 para la arquitectura x86/amd64. Este software proporciona las funcionalidades necesarias para este proyecto, como la virtualización del equipo que alojará el software T-Pot y el equipo con funciones de cortafuegos y redirección de tráfico. Oracle VM VirtualBox es reconocido por su robustez y flexibilidad, permitiendo la gestión eficiente de múltiples máquinas virtuales con diversos sistemas operativos, lo que es esencial para probar y validar distintas configuraciones de seguridad.

Respecto al acceso a Internet, se cuenta con una conexión de banda ancha de fibra óptica con una velocidad simétrica de 600 Mb. Esta conexión de alta velocidad es necesaria para asegurar una comunicación rápida y estable entre los componentes virtualizados y otros recursos de red pública necesarios para el proyecto, además de soportar un gran volumen de tráfico en los ataques esperados. El enrutador suministrado

por el proveedor de Internet permite configuraciones avanzadas, como el mapeo de puertos, la configuración de una zona desmilitarizada (DMZ) y la redirección del tráfico de red. Estas características permiten una mayor seguridad y control sobre el tráfico de datos, facilitando la implementación y prueba de distintas políticas de seguridad en el entorno controlado donde se desplegará el proyecto.

A continuación, se realiza una lista con las tareas a realizar para alcanzar los objetivos señalados:

- **Investigación y recopilación de información**
  - Realizar una investigación exhaustiva sobre honeypots, honeynet y T-Pot, así como sobre su historia, aplicaciones, ventajas, desventajas y técnicas de implementación
  - Recopilar información relevante de fuentes confiables, como libros, artículos académicos, documentos técnicos y recursos en línea
- **Análisis de casos de uso y mejores prácticas**
  - Analizar casos de uso y ejemplos de implementación de honeypots y honeynet en entornos corporativos y de investigación
  - Identificar mejores prácticas y lecciones aprendidas de implementaciones exitosas
- **Diseño de la infraestructura**
  - Diseñar la infraestructura necesaria para el entorno de prueba
  - Definir la ubicación estratégica de los honeypots
- **Configuración de honeypots básicos**
  - Configurar los honeypots de acuerdo con los requisitos identificados durante el análisis previo
  - Establecer servicios falsos y sistemas vulnerables para atraer a posibles atacantes
- **Despliegue de T-Pot**
  - Instalar y configurar T-Pot en un entorno controlado
  - Personalizar la configuración de T-Pot para maximizar la recopilación de datos relevantes
- **Implementación de medidas de seguridad adicionales**
  - Aplicar técnicas de bastionado en los sistemas donde se implementarán los honeypots y T-Pot
  - Implementar contramedidas anti honeypot para evitar la detección por parte de posibles atacantes
- **Monitorización y recopilación de datos**
  - Establecer mecanismos de monitorización para registrar el tráfico dirigido a los honeypots
  - Recopilar y almacenar datos sobre actividades sospechosas y potenciales amenazas
- **Análisis de datos recopilados**
  - Analizar los datos recopilados utilizando herramientas de análisis forense digital y técnicas de inteligencia de amenazas
  - Identificar patrones de ataque, técnicas utilizadas por los adversarios y posibles indicadores de compromiso
- **Evaluación de eficacia y generación de informes**



- Evaluar la efectividad de T-Pot en la detección y respuesta ante amenazas
- Generar informes detallados que incluyan hallazgos, recomendaciones y lecciones aprendidas
- **Iteración y mejora continua**
  - Iterar sobre la implementación y configuración de los honeypots y T-Pot según los resultados de la evaluación
  - Implementar mejoras y ajustes necesarios para fortalecer la postura de seguridad de la organización
  - Añadir otras medidas de mejora detectadas en el desarrollo del proyecto

Conjuntamente, se presenta una planificación temporal detallada a través de un diagrama de Gantt. Este diagrama incluye todas las tareas a ejecutar, sus dependencias y la secuencia en que deben ser realizadas. La planificación proporciona una visión clara de los hitos del proyecto, la duración estimada de cada tarea, incluso los recursos asignados, facilitando una gestión eficiente y el seguimiento de su evolución a lo largo del proyecto:

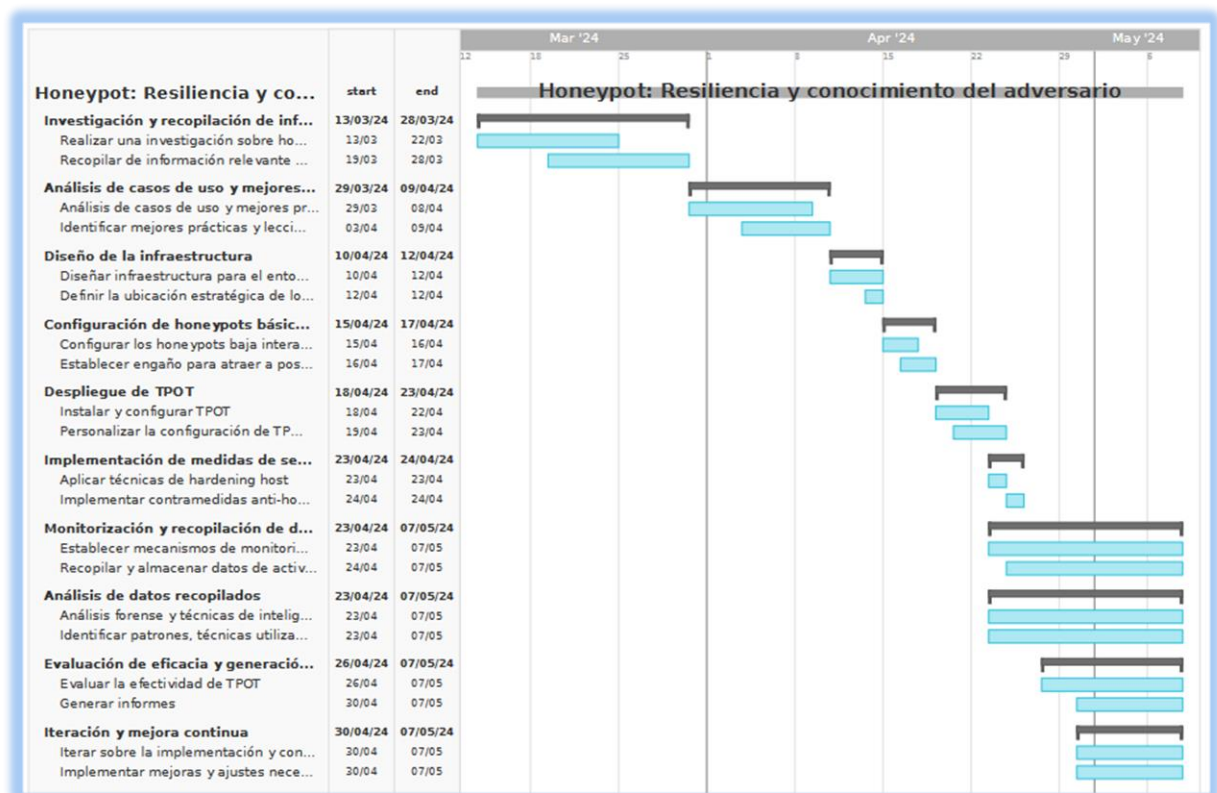


Ilustración 2 - diagrama de Gantt

En la planificación detallada del proyecto se pueden identificar varios riesgos potenciales que podrían afectar el cumplimiento del cronograma. A continuación, se identifican estos riesgos junto con sus respectivos planes de mitigación o alternativas:

- **Riesgo de fallo en el equipo de virtualización.** En caso de que el equipo principal sufra una avería o mal funcionamiento que impida su utilización para las tareas designadas, se dispone de un equipo de sobremesa alternativo. Aunque este equipo no es tan potente ni portátil, puede asumir completamente el rol del equipo



principal, aunque esto podría extender el tiempo necesario para realizar algunas de las pruebas previstas.

- Riesgo de incompatibilidades con el software de virtualización. En el supuesto que se presentasen problemas de este tipo o errores insalvables durante la instalación y configuración, se ha previsto usar otro software de virtualización como el de *VMware Workstation Pro* [5] que es otro hipervisor de escritorio con licencia gratuita en el momento de la elaboración de este proyecto.
- Riesgo de integración de T-Pot. Es posible que surjan complicaciones técnicas en la integración en un entorno virtualizado. De este modo, la mitigación de este riesgo consistirá en realizar pruebas preliminares para identificar posibles problemas con antelación, que permitirán disponer del tiempo necesario para consultar la documentación técnica y solicitar soporte de la comunidad de T-Pot. Así, se podrá ajustar la planificación según el tiempo real necesario, evitando falsas expectativas en la programación de las tareas.

#### 1.6 Breve resumen de productos obtenidos

- Investigación y recopilación de información sobre honeypots, honeynet y T-Pot
- Análisis de casos de uso, mejores prácticas y ejemplos de implementación.
- Diseño de la infraestructura del entorno de prueba y ubicación estratégica de honeypots
- Configuración de honeypots básicos y despliegue de T-Pot en un entorno controlado
- Implementación de medidas de seguridad adicionales y contramedidas anti honeypot
- Monitorización y recopilación de datos sobre actividades sospechosas.
- Análisis de datos recopilados utilizando herramientas forenses y de inteligencia de amenazas
- Evaluación de la eficacia de T-Pot en la detección y respuesta ante amenazas
- Generación de informes detallados con hallazgos, recomendaciones y lecciones aprendidas
- Iteración y mejora continua de la implementación y configuración de honeypots y T-Pot

## 2 Estado del arte

En el contexto de este proyecto, se estudian tres componentes clave en el marco de la seguridad corporativa como son los honeypots, honeynet y T-Pot. Los honeypots son sistemas diseñados para atraer y engañar a los atacantes, permitiendo la observación de sus técnicas y comportamientos. Una honeynet es una red de honeypots que proporciona un entorno más amplio y diverso para el análisis de amenazas. T-Pot es una plataforma avanzada que integra múltiples honeypots y herramientas de análisis,

optimizando la detección y respuesta ante actividades maliciosas en entornos corporativos y de investigación.

## 2.1 Historia: orígenes y conceptos Iniciales

La definición de honeypot [6] es tan intuitiva como cambiante y dependiendo del autor, puede resultar de lo más variada. Sin embargo, en términos generales todas las definiciones convergen en el mismo significado y es que un honeypot es un activo de seguridad que obtiene su valor en el momento que es investigado, atacado o comprometido. Y es precisamente por esta diversidad por la que queda reflejada su adaptabilidad al contar con un diseño planificado con el que atraer y desviar de otros objetivos a los actores maliciosos, proporcionando una oportunidad perfecta para documentar las tácticas, técnicas y procedimientos empleados por los atacantes.

En el ámbito de la seguridad se ha experimentado un gran avance a medida que las amenazas informáticas se volvían más sofisticadas y omnipresentes, permitiendo que los honeypots se fuesen estableciendo como una herramienta cada vez más esencial en la detección, estudio y mitigación de ataques. Estos dispositivos, que se diseñan con el propósito de simular sistemas informáticos vulnerables con el que atraer a posibles intrusos, han experimentado una evolución constante desde sus comienzos modestos en la década de 1990 hasta hoy día.

Los honeypots, a través de una combinación de innovación tecnológica y esfuerzos de investigación, han pasado de ser simples experimentos a herramientas sofisticadas que son utilizadas por organizaciones de todo el mundo para fortalecer sus defensas. Por tal motivo, el objetivo de este apartado es explorar la fascinante historia [7] de estos sistemas, desde sus conceptos iniciales hasta su estado actual, resaltando los hitos clave y las contribuciones que han dado forma al panorama de la seguridad actual.



Ilustración 3 - Evolución tecnológica de engaño

El principio de la década de los años 90 marca un período crucial en el desarrollo de la historia de los honeypots pues, tanto Clifford Stoll como Bill Cheswick jugaron roles destacados al documentar por primera vez los conceptos básicos en sus trabajos *The Cuckoo's Egg* [8] y *An Evening with Berferd* [9], respectivamente. En estas publicaciones se puede apreciar como proporcionaron una visión pionera sobre cómo los sistemas informáticos podrían ser utilizados para las actividades de rastreo y estudio de intrusos.

En 1997, dos eventos significativos marcaron un hito en el campo de la seguridad como son el lanzamiento de la herramienta *Deception Toolkit (DTK)* [10] por Fred Cohen y el desarrollo inicial de una solución de honeypot por Marty Roesch que terminaría conociéndose como *NetFacade* y siendo precursor de *Snort* [11]. La primera herramienta es un sistema considerado como uno de los primeros sistemas honeypots disponibles para la comunidad de seguridad, ya que simulaba vulnerabilidades conocidas en sistemas UNIX para atraer a posibles atacantes y así poder estudiar sus tácticas. La segunda herramienta contribuye a la diversificación de las herramientas disponibles en este campo emergente.

El año 1998 fue especialmente significativo al marcar el surgimiento de los honeypots iniciales como verdaderos productos comerciales. Por un lado, se destaca a *CyberCop Sting* [12], que fue uno de los primeros en salir al mercado con una oferta compuesta de una solución avanzada que permitía la simulación de múltiples sistemas virtuales que contaba con sus propios servicios únicos. Por otro lado, y casi al mismo tiempo, *BackOfficer Friendly* [13], desarrollado por Marcus Ranum, que ofrecía una opción gratuita y fácil de usar, permitiendo a un público más amplio experimentar con la tecnología de honeypots.

En 1999, el Proyecto Honeynet surge como una iniciativa dedicada a la investigación de la actividad de los hackers con la que poder compartir sus descubrimientos con la comunidad, hecho que, a través del trabajo, demostraría la eficacia de los honeypots para detectar y analizar ataques en tiempo real. Además, también destacó en ese mismo año la publicación de la serie de documentos *Know Your Enemy* [14], que proporcionarían información detallada sobre las tácticas de los hackers y resaltarían la importancia de estos activos en seguridad.

Cabe destacar la interesante historia que existe detrás de los esfuerzos iniciales de Stoll y Cheswick [15], quienes fueron pioneros en el desarrollo de lo que hoy se conoce como honeypot. Es evidente que estos investigadores jugaron un papel clave al anticipar la necesidad de nuevas estrategias con las que abordar las crecientes amenazas y donde sus contribuciones sentarían las bases para evolucionar en la detección y mitigación de ataques informáticos, dejando un legado duradero en la industria de la seguridad.

La primera contribución documentada relata como el astrofísico y administrador de sistemas Clifford Stoll descubre en su laboratorio de California una discrepancia de 75 centavos en la facturación de la red informática que supervisa y, motivado por su curiosidad, Stoll rastrea al detalle a un hacker que intentaba infiltrarse en redes de ordenadores de EE.UU. Durante tres años, Stoll observó al hacker, recopiló datos cruciales y proporcionó información vital para su posterior arresto. Esta fascinante historia quedó inmortalizada en el libro *The Cuckoo's Egg*.

En la segunda aportación, el investigador de *AT&T Bell Laboratories*, Bill Cheswick explica lo que podría considerarse como el primer caso documentado de lo que en la actualidad se entiende como un verdadero honeypot. En esta documentación se expone la metodología y diseño de un sistema señuelo con vulnerabilidades para atraer a posibles atacantes con firme intención de estudiar sus movimientos y amenazas a las que se expone. En dicha documentación se narra con detalle como un cracker, o experto

malicioso, es descubierto explotando una conocida vulnerabilidad en el sistema *Sendmail Debug* de equipo de acceso a internet de *AT&T* y la forma en que es retenido en una cárcel virtual llamada *chroot Jail* para observar sus movimientos y estrategias. Esta historia también permaneció registrada en el trabajo *An Evening with Berferd*.

Estos hitos históricos no solo marcaron el inicio de una nueva era en la seguridad informática, sino que también sentaron las bases para la investigación y el desarrollo continuo en el campo de los honeypots, que sigue siendo relevante en la actualidad.

## 2.2 Valoración

El uso de honeypots en la seguridad empresarial ofrece numerosas ventajas, pues al actuar como señuelos, atraen a los atacantes y permiten a los equipos de seguridad observar sus tácticas y métodos en un entorno controlado. Esto no solo ayuda a identificar nuevas amenazas y vulnerabilidades, sino que también mejora la capacidad de respuesta ante incidentes reales. Además, los datos recolectados a través de honeypots pueden proporcionar valiosa inteligencia de amenazas, informando y fortaleciendo las defensas de la empresa. Sin embargo, es importante gestionar adecuadamente estos sistemas para evitar que se conviertan en puntos de entrada para atacantes más sofisticados que lleven a cabo ataques dirigidos.

### 2.2.1 Aplicaciones del honeypot

Cuando se diseña un señuelo para ubicarlo en un punto de la red o sistema informático es con la firme intención de detectar posibles ataques y con objetivo centrado en la recopilación de datos que, posteriormente, se convertirán en información útil a la hora de decidir qué medidas de seguridad se aplicarán para mejorar el sistema.

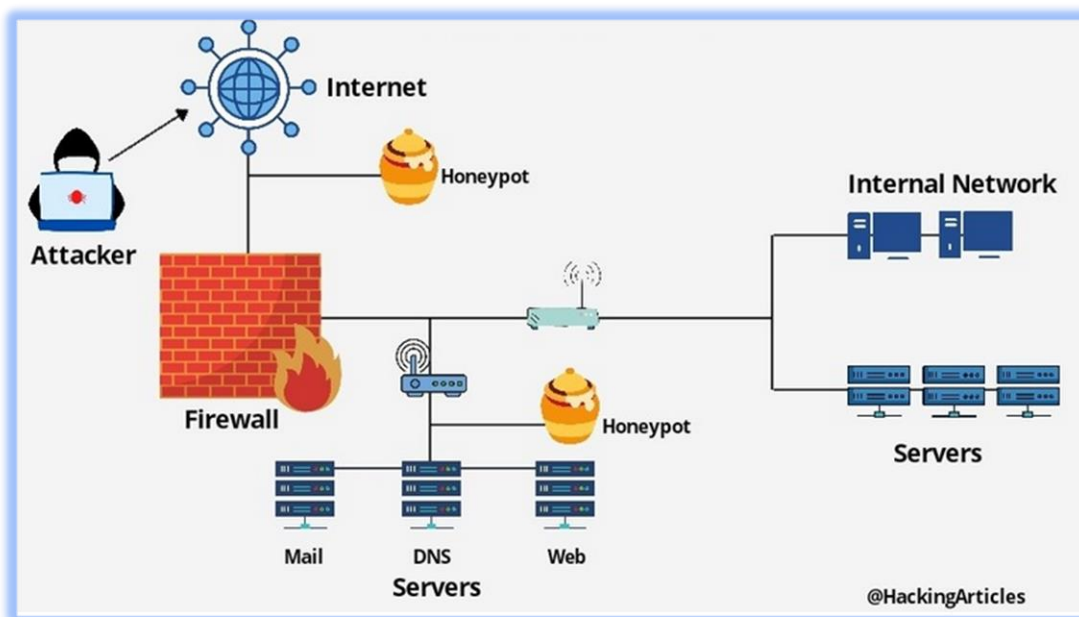


Ilustración 4 - ejemplo de ubicación honeypot en la red

Si bien es cierto, cobra especial relevancia no escatimar en la dedicación de tiempo que sea necesario para la elección de la dirección que se quiere dar al proyecto de engaño con la que conseguir que la información recopilada sea de calidad y objetiva. Así, es fácil distinguir algunas estrategias de uso que resultan interesantes para su aplicación:

- **Alerta y detección.** Los honeypots simulan un comportamiento real de un sistema para engañar a los atacantes y así observar sus acciones. La actividad registrada [16] tiene gran valor de seguridad para la corporación.
- **Investigación.** El uso que se le da a la herramienta es la captura de malware para su posterior análisis [17] respecto a tácticas, técnicas y procedimientos aplicados por los atacantes en el intento de explotación de vulnerabilidades expuestas.
- **Entrenamiento.** Resulta una herramienta útil para entrenar a los equipos de seguridad en la detección y respuesta de incidentes de seguridad [18], bajo un entorno seguro en el que practicar y aprender de tipos variados de ataques.
- **Forense.** La información recopilada de los registros de actividad de los honeypot puede servir como evidencia válida en investigaciones forenses [19], ya que disponen de información con la que rastrear actividades maliciosas detectadas.

#### 2.2.2 Papel en la seguridad corporativa

El papel que juegan estas herramientas en las empresas se torna esencial si quieren o necesitan mejorar la seguridad corporativa, pues les facilita la recopilación de información sobre las tácticas y herramientas utilizadas por los delincuentes [20], destacando que los honeypot se deben complementar con una estrategia integral de seguridad informática que incluya medidas como cortafuegos y cifrado de datos.

Sin embargo, estos dispositivos no pueden considerarse como una solución única, sino como parte de un enfoque más amplio para la seguridad pues, en la integración con otras medidas las empresas saldrán fortalecidas en su defensa contra los ataques y mejorará su postura de seguridad, en general.

#### 2.2.3 Ventajas

Las ventajas [21] son muy variadas y abarcan varios aspectos esenciales, aunque se destacan las siguientes como principales por resaltar las bondades de los honeypot.

Por una parte, resulta de gran valor los datos recopilados para su análisis que, en comparación con otras herramientas que coleccionan una enorme cantidad de datos irrelevantes, resultan de mayor calidad al capturarse solo los necesarios. Estos son más fáciles de analizar y proporcionan una visión clara de actividades maliciosas. Incluso, con un consumo liviano de los recursos, pues el tráfico analizado no tiene un volumen excesivo y solo aporta información relevante.

Por otra parte, la simplicidad también se acentúa como una de las virtudes a destacar, pues facilita su implementación y mantenimiento al no necesitar, ni algoritmos complejos ni base de datos de firmas. Además, se reducen los falsos positivos debido a que cualquier interacción será considerada como maliciosa pues nadie de la organización debe acceder a ellos.

#### 2.2.4 Desventajas

No todo es positivo y también presentan desafíos significativos [22] como la capacidad limitada de solo monitorizar las interacciones realizadas directamente contra el sistema. Esta causa puede derivar en ataques no detectados y que han evadido el honeypot.

También, al estar continuamente expuestos, si no están bastionados de manera precisa, atacantes expertos pueden utilizarlos para dirigir sus ataques a otros sistemas subyacentes, comprometiendo la seguridad de la red de forma exponencial. No obstante, si un intruso consigue desvelar la identidad del honeypot usando la técnica de *fingerprinting* [23], mediante la cual se puede obtener información del sistema operativo como su tipo y versión, una vez que los han detectado pueden cambiar su estrategia de ataque e iniciar otra táctica con la que confundir al equipo de seguridad

#### 2.3 Comparativa con otros sistemas de detección

En comparativa [24], rápidamente se puede observar que, mientras un honeypot actúa como señuelo para atraer a los atacantes y registrar sus acciones, los Sistema de Detección de Intrusiones o IDS ejercen como monitor para la detección de accesos en tiempo real, y los cortafuegos controlan el tráfico de red según reglas de seguridad previamente definidas para la prevención de accesos no autorizados. Cada uno cumple un papel importante en la seguridad de la red, complementándose entre sí para una defensa integral, pero ni son ni se usan para lo mismo.

Más detenidamente, las ventajas más destacables que se pueden enumerar en un honeypot frente a IDS, cortafuegos o herramientas similares, son las especificadas a continuación:

- **Recursos mínimos.** La puesta en marcha de un honeypot apenas necesita recursos y su consumo es muy bajo, tanto en CPU, memoria o ancho de banda. De hecho, el consumo de recursos está supeditado a la actividad que pueda producir un atacante en su interacción con el sistema atacado.
- **Ubicuidad.** Según las necesidades, su radio de acción queda acotado al segmento de red donde se instale, siendo flexible la zona en la que se quiera instalar, ya sea interna, externa o DMZ.
- **Volumen de datos pequeño.** Un honeypot genera muy pocos datos pero de gran valor, ya que están diseñados expresamente para atraer a atacantes malintencionados, con lo que no pueden existir falsos positivos. A diferencia de los otros sistemas de seguridad, mencionados anteriormente, como un cortafuegos o IDS que generan una cantidad muy voluminosa de datos en ficheros de registro de actividad y si pueden llevar a falsos positivos.

##### 2.3.1 Honeypot

Su funcionamiento tiene como objetivo actuar como una trampa para atraer a posibles atacantes y registrar sus movimiento con los que realizar un análisis de seguridad. Su comportamiento es pasivo y queda a la espera de recibir un ataque para registrar toda la actividad que se produzca. Su ubicación suele quedar localizada en el perímetro de la red, sobre todo para facilitar el control del tráfico de entrada y salida. Sin ninguna capacidad de prevención, solo observa y analiza el comportamiento de un atacante.



### 2.3.2 IDS

Funcionan inspeccionando el tráfico de red en busca de patrones maliciosos y emitiendo alertas de posibles intrusiones. Actúan de manera activa monitorizando el tráfico de red sin descanso para identificar intrusiones en tiempo real. Sin embargo, solo detectan y no son capaces de bloquear activamente el tráfico malicioso y su ubicación está en el perímetro de red.

### 2.3.3 Cortafuegos

Su función principal es controlar y filtrar todo el tráfico entrante y saliente en base a unas reglas de seguridad predefinidas con la que prevenir los accesos no autorizados. Al igual que el sistema anterior, procede activamente aplicando las reglas de seguridad al flujo del tráfico de red para permitir o bloquear los intentos de comunicación.

## 2.4 Clasificación

En función de las fuentes que se consulten, este apartado puede generar muchas discrepancias de cómo se percibe la clasificación de honeypot [25] y no quiere decir que no sean veraces, que si factibles, desde el punto de vista del que las está interpretando. Una fuente que está actualizada en referencia a la fecha actual y permite obtener una idea explicativa sobre este concepto es la consultada en el Instituto Nacional de Ciberseguridad (INCIBE), pues en comparación con el resto se percibe como la más completa y coherente. Así, las características o funcionalidades vendrán marcadas por el objetivo que se le quiera designar al honeypot en una puesta en marcha adaptada a las necesidades que se necesiten cubrir.

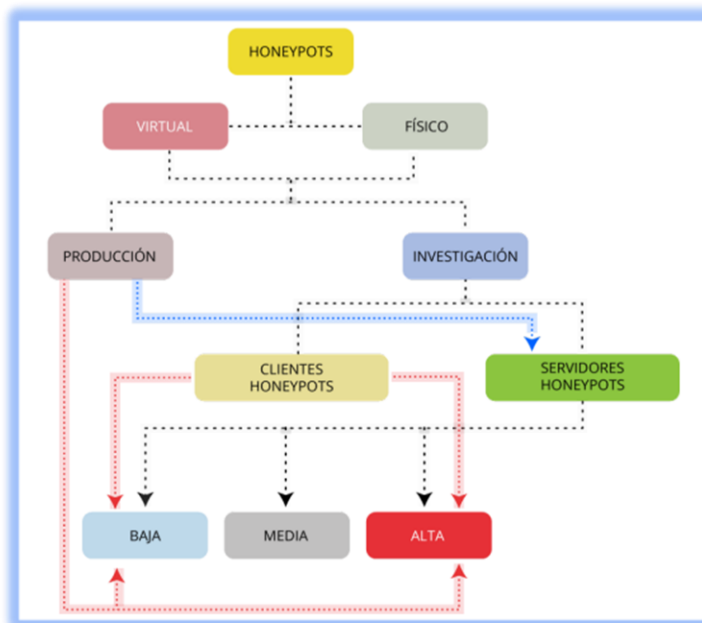


Ilustración 5 - Clasificación de un honeypot [26]

En este contexto se encuentran clasificación por:

#### 2.4.1 Interacción

- **Baja.** La simulación está basada en sistemas sencillos y fáciles de manejar, que permiten una inmediata puesta en servicio y configuración debido a que realmente no hay un servicio funcional, sino una integración parcial. Su objetivo es la detección de ataques automatizados o vulnerabilidades conocidas que afectan a servicios específicos que son fáciles de identificar por los atacantes más avanzados y bastante limitados en la recopilación de información útil generada en el acceso. Sin embargo, son servicios que tienden a virtualizarse, con lo que el riesgo de exposición frente a atacantes es mucho menor.
- **Alta.** Son servicios instalados totalmente funcionales y que resultan más complicados de identificar por un atacante. Su uso tiene como objetivo el descubrimiento de comportamientos anómalos o ataques no detectados con anterioridad. Así, gracias a la gran cantidad de datos que recopilan, son ideales para usarlos si se quiere realizar una investigación profunda de nuevos ataques. Sin embargo, el riesgo de exposición es mucho mayor si no se realiza un correcto bastionado del honeypot, pues podría comprometer otros sistemas que estuviesen al alcance.

#### 2.4.2 Sistema

Según el sistema que se quiere configurar, se puede estudiar si resulta más interesante un equipo físico u otro que esté alojado en un entorno virtual, incluso ambos, independientemente de si es de alta o baja interacción:

- **Físico.** Es un equipo tangible que está preparado para recibir ataques y que por su naturaleza resultará más complicado de que su engaño sea detectado por los atacante. No obstante, resultan más caros, económicamente, por hacer frente al coste de hardware y software necesario, además del extra en mantenimiento y de la limitación respecto a los servicios que ofrece, que vendrán dados por su funcionalidad de fábrica.
- **Virtual.** Es un sistema ejecutado en una plataforma de virtualización y que permitirá emular una variada colección de servicios emulados, siempre teniendo en cuenta la arquitectura del procesador del equipo que hospeda las máquinas virtuales para obtener compatibilidad y un buen rendimiento.



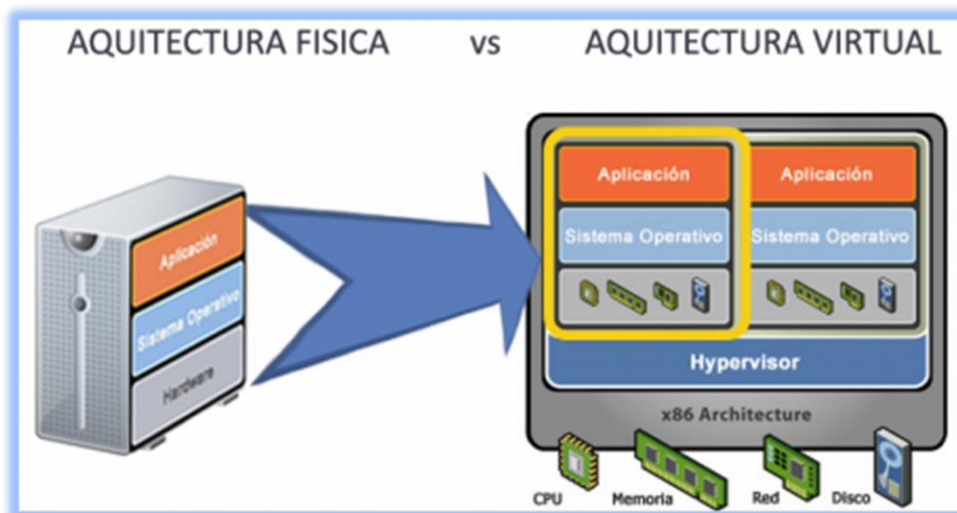


Ilustración 6 - arquitectura física vs virtual [27]

### 2.4.3 Comportamiento

Normalmente, un honeypot no presenta más de un comportamiento para no facilitar su detección y no se recomienda esa misma práctica para dificultar el engaño a los atacantes. De este modo, basados en los mecanismos de implementación aplicados a la hora de comportarse ante diferentes amenazas y con el fin de prevenir ataques de distintas formas, se pueden definir los siguientes comportamientos:

- **Detección precisa.** Con el uso de honeypots se obtiene una ventaja significativa en la detección precisa de actividades sospechosas, ya que reduce los falsos positivos y permite la captura de información esencial sobre nuevas técnicas o herramientas de explotación de vulnerabilidades. Incluso son capaces de trabajar con comunicaciones cifradas y en redes IPv6, lo que amplía su utilidad en entornos de seguridad avanzada.
- **Protección contra intrusos.** Este comportamiento se basa en distraer a los atacantes para que el equipo de seguridad pueda ganar tiempo en la detección de sus actividades y en la implementación de contramedidas con las que bloquearlos e impedir que alcancen su objetivo final.
- **Desactivar acciones.** Durante la incursión, el atacante puede ejecutar distintas acciones, pero éstas serán desactivadas antes de que pueda explotar la vulnerabilidad. Así, llega hasta lo que buscaba pero los resultados son manipulados para que no funcionen las peticiones.
- **Defensa contra ataques automatizados.** El comportamiento está basado en ralentizar las acciones del atacante para evitar la velocidad de ejecución o propagación de ataques del tipo gusano (programas maliciosos que se duplican en distintas ubicaciones hasta saturar el sistema) y que afecten a la red o al mismo sistema configurado. Por ejemplo, se puede reducir el tamaño de ventana de los paquete de red o dejarlo a cero para que quede en espera.
- **Ninguno.** No se aplica ninguna contramedida o acción frente a las actividades que realicen los atacantes y, por ende, no hay barrera ante los daños o alcance de los ataques.

#### 2.4.4 Rol

- **Cliente.** Se reproduce el comportamiento de un programa que utiliza servicios en el servidor, como puede ser un navegador que visita páginas web para ser atacado aprovechando vulnerabilidades y que recopila información sobre los ataques y riesgos de seguridad mientras navega por una página web.
- **Servidor.** Esta función opera atrayendo a los atacantes hacia un entorno aislado en el que realizar estudios de investigación o, simplemente, para desviar posibles amenazas de la red real. Así, se puede simular un entorno realista para dificultar la detección por parte de los atacantes o se pueden simular aplicaciones o servicios, con el fin de captar su atención y registrar todas las acciones de los infiltrados, lo que proporciona una valiosa información para mejorar la protección y el conocimiento ante futuros ataques.

#### 2.5 Ubicación en la red

La efectividad que se alcance en la explotación de un honeypot suele estar vinculada de manera directa con la ubicación [28] que tome en la red corporativa y que, a su vez, vendrá marcada por los objetivos de seguridad que se quieran alcanzar y del tipo de información que se desee recopilar. Es decir, la ubicación va a resultar necesaria para garantizar su eficacia en detección, respuesta ante amenazas y generación de inteligencia. A continuación, la zona recomendada de la red:

##### 2.5.1 Interna

En esta zona están los servidores y recursos críticos, con lo que el honeypot queda conectado detrás del cortafuegos para que actúe de alerta temprana ante un atacante que intente adentrarse en la red corporativa. El honeypot debe detectarlo en su intento de realizar alguna acción como el movimiento lateral [29], resultando de gran ayuda para comprender la situación de amenazas provenientes del interior, incluidas la de los propios usuarios. En su formato más simple, este dispositivo se conecta a un segmento de red como cualquier otro activo, actuando de sensor de actividad ante cualquier interacción que registre.

##### 2.5.2 Externa

Se sitúa delante del cortafuegos, fuera del perímetro de seguridad de la red, con la función de detectar y registrar cualquier tipo de ataque que provenga del exterior. Su configuración permite evaluar las amenazas externas con las que conocer y entender las técnicas empleadas por los actores maliciosos.

##### 2.5.3 DMZ

Esta es una zona intermedia, entre la red interna y externa, y donde suelen estar los servidores expuestos a internet, resultando ideal para ubicar un honeypot de alta interacción con el que desviar la atención hacia el mismo. Esta táctica resulta beneficiosa para comprender a que ataques se exponen estos servidores, así como recabar información valiosa con la que mejorar la seguridad de esos servicios.

##### 2.5.4 Varias zonas

Realizando un despliegue de múltiples honeypot de baja interacción en segmentos de red críticos es una forma inteligente de detectar actividades no deseadas en zonas

críticas. De este modo, cualquier tipo de interacción que se registre se puede considerar maliciosa, actuando de alerta temprana.

### 3 Honeynet

Las honeynet son una evolución natural de los honeypot que ofrecen un alto nivel de interacción, simulando una red real de sistemas de producción estándar detrás de un dispositivo de control de acceso como un cortafuegos.

#### 3.1 Introducción

Los sistemas dentro de una honeynet son genuinos, no emulan servicios ni se crean entornos restringidos, lo que permite a los atacantes interactuar con sistemas operativos completos y aplicaciones. A diferencia de los honeypot tradicionales, una honeynet no requiere modificaciones en los sistemas y son idénticos a los utilizados en cualquier organización.

Surgieron como concepto en 1999 y dio pie al inicio de lo conocido como *Honeynet Project* [30] establecido en 2000 por un grupo de profesionales de seguridad. En este proyecto, respaldado por una amplia variedad de expertos en seguridad, se publicaron una serie de documentos titulados "*Know Your Enemy: papers*" [31], donde se detalla cómo los atacantes identifican y comprometen sistemas vulnerables, así como sus motivaciones.

En 2001 se publicó un libro basado en la investigación del proyecto, llamado "*Know Your Enemy*" [32], y se estableció la *Honeynet Research Alliance* y *Honeynet Project* para mejorar el desarrollo de tecnologías honeynet mediante la colaboración entre organizaciones de investigación y despliegue. Esta alianza representa el futuro de las tecnologías honeynet al facilitar el intercambio eficiente de información y el aprendizaje sobre las amenazas en Internet.

El valor de una honeynet reside en su flexibilidad y capacidad de desempeño de diversos roles, actuando como si fuesen activos en producción y aplicando directamente sobre una organización una capa adicional de seguridad con la que engañar a los atacantes. Este extra de seguridad les hace creer que interactúan con sistemas auténticos y aplicaciones reales, lo que dificulta sobremanera su detección. Y es por este motivo por lo que resultan eficaces en la detección de ataques, al usar gran variedad de sistemas reales y aplicando el mismo modelo de detección del honeypot ManTrap [33], actuando de jaula para monitorizar toda actividad.

Aunque tiene una complejidad elevada y unos requerimientos que demandan gran cantidad de recursos para su construcción y mantenimiento, su valor para la tarea de investigación es difícil de superar, permitiendo la obtención de información detallada sobre los atacantes, incluyendo sus métodos, herramientas y motivaciones, lo que resulta concluyente para comprender y prevenir futuros ataques.

Una honeynet destaca en el análisis de tendencias y modelado estadístico, proporcionando información útil para predecir ataques y actuando como un sistema de alerta temprana, siendo esta característica de gran valor para la respuesta ante

incidentes, pues proporcionan un entorno controlado en el que desarrollar y refinar procedimientos de respuesta, además de facilitar el intercambio de información dentro de la comunidad de seguridad. Incluso, una honeynet se puede enfocar como un banco de pruebas en el que analizar vulnerabilidades en nuevas tecnologías, antes de su implementación en entornos de producción, lo que permite minimiza los riesgos.

### 3.2 Objetivo honeynet

En una honeynet, los honeypot se despliegan detrás de una puerta de enlace que actúa en capa 2 del modelo OSI [34] denominada honeywall [35] y cuya misión es permanecer indetectable para los atacantes y registrar todas las actividades de red.

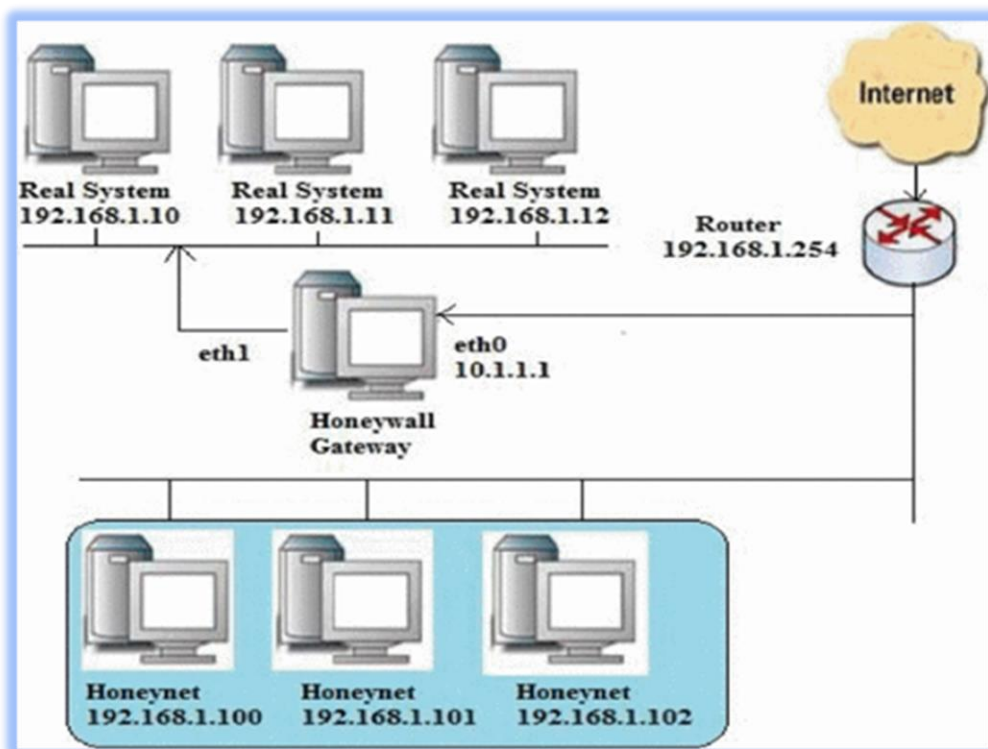


Ilustración 7 - Diseño básico de una honeynet

Dentro de una honeynet se encuentra habilitado un honeywall como centro de operaciones para las principales tareas como:

#### 3.2.1 Control de datos

Si cualquiera de los honeypots que pertenecen a una honeynet quedase comprometido, éste representaría una amenaza real para el resto de los sistemas, incluidos los que no forman parte de la propia honeynet. En una situación igual o similar a la descrita el control de datos se centra en manejar este tipo de situaciones, con una contención de las actividades dentro de la honeynet, aunque manteniendo cierto grado de libertad al atacante.

#### 3.2.2 Captura de datos

Involucra la monitorización, captura y registro de todas las actividades dentro de la honeynet con la implementación de múltiples capas de captura de datos para recopilar información relevante y minimizar el riesgo en caso de que los honeypots sean

comprometidos, además de ayudar a conocer las tácticas, técnicas y procedimientos de los atacantes.

### 3.2.3 Recopilación de datos

Los datos recopilados se envían de manera segura a un servidor de recopilación de datos centralizado.

### 3.2.4 Generación de alertas

Genera una alerta si se produce alguna actividad sospechosa dentro de la honeynet para alertar a los profesionales de seguridad sobre posibles brechas de seguridad.

## 3.3 Arquitectura honeynet

La arquitectura de una honeynet ha evolucionado principalmente en tres generaciones o arquitecturas según la tecnología adoptada y la forma en que se implementa el control, la captura y la recopilación de datos.

### 3.3.1 Generación I

La honeynet de Gen I era simple, con un firewall asistido por un IDS como honeypot de puerta de enlace. En esta arquitectura, se requerían 2 interfaces de red en el honeywall: una que conectaba con la red externa mientras que la otra enfrentaba a la red interna. La desventaja de esta arquitectura era que la puerta de enlace actuaba como dispositivo de capa 3 del modelo OSI y, por lo tanto, podía ser detectada por los atacantes.

### 3.3.2 Generación II y III

La arquitectura de las honeynet se mejoró aún más al introducir una puerta de enlace IDS o honeywall con funcionalidad de control y captura de datos. La Gen II se hizo para abordar las desventajas en la honeynet de la Gen I. La honeynet de la Gen II y III tiene una arquitectura casi similar. El Honeynet de la Gen III tiene mejoras en el despliegue y la gestión en comparación con la Gen I y II. El servidor Sebek [36] en Honeywall fue una característica añadida a la tercera generación del Honeynet. Su función principal es centralizar los datos capturados por los honeypots de alta interacción desplegados en diversas ubicaciones de la red.

## 3.4 Honeynet virtual

En una honeynet virtual se emplea la virtualización para crear múltiples máquinas virtuales, cada una ejecutando un sistema operativo independiente, de manera simultánea y en un único hardware físico. Esta tecnología permite compartir eficientemente los recursos físicos de la máquina subyacente, como la CPU, la memoria, el almacenamiento y los periféricos, entre todas las máquinas virtuales. Algunas de las herramientas especializadas como VirtualBox [37], Proxmox [38] o VMware [39], entre otras, facilitan este proceso de virtualización. De este modo, al consolidar múltiples sistemas en un único servidor físico, ofrece eficiencia, flexibilidad y escalabilidad, lo que lo convierte en una opción atractiva para la implementación de entornos de seguridad de red.

Es obvio que una de las principales ventajas de una honeynet virtual es su capacidad de reducir significativamente los costos de hardware asociados con la implementación de una honeynet tradicional. Así, en lugar de requerir múltiples dispositivos físicos, en un único servidor se pueden alojar varias máquinas virtuales, lo que se traduce en ahorros, tanto en términos de espacio físico como de inversión en hardware.

Además de que una honeynet virtual optimiza los recursos, también ofrece flexibilidad y escalabilidad, tal y como se ha mencionado anteriormente. Las máquinas virtuales pueden crearse, modificarse y eliminarse fácilmente según las necesidades del proyecto, lo que permite una adaptación rápida a cambios en los requisitos o en el entorno de seguridad como, por ejemplo, configurando un automatismo que reconfigure los parámetros de red (IP, máscara de subred, puerta de enlace) y moviendo la máquina virtual a otra red lógica dentro de la propia red física, es decir, cambiando de Vlan. Asimismo, se pueden agregar nuevas máquinas virtuales para ampliar el alcance de la honeynet según sea necesario y sin la necesidad de adquirir hardware adicional.

## 4 T-Pot

El proyecto T-Pot [40] es una plataforma de código abierto de honeypots desarrollado por la empresa Telekom Security [41]. Su concepto innovador radica en convertir todos los servicios que operan bajo el protocolo de red TCP [42], junto con algunos servicios críticos bajo el protocolo de red UDP [43], en honeypots. Esta visión revolucionaria ha permitido a los profesionales de seguridad adentrarse aún más en las tácticas, técnicas y procedimientos empleados por los atacantes, proporcionando una comprensión más profunda de las amenazas en el panorama de la seguridad digital.

### 4.1 Historia

Con el paso del tiempo, T-Pot ha experimentado un notable avance [44]. En versiones anteriores como la 16.10 y 17.10, su instalador automático se usaba de manera independiente, pero en la versión más reciente, quedó integrado directamente en el propio instalador. Esta modificación ha simplificado significativamente el proceso de implementación, lo que ha posibilitado que un mayor número de organizaciones y expertos en seguridad implementen T-Pot en sus sistemas.



También ha contemplado una considerable evolución en su proceso de instalación y expansión [45] del conjunto de herramientas que lo componen. En sus versiones más recientes se incluyen una mayor variedad de honeypot diseñados meticulosamente para la emulación de un servicio o aplicación concreta. Esta diversificación ha sido clave al permitir a T-Pot adaptarse eficientemente a las cambiantes tácticas y técnicas empleadas por los atacantes en el panorama de la seguridad. Se ha convertido en una herramienta versátil y efectiva en la detección temprana y el análisis de amenazas en entornos de seguridad informática, gracias a la amplia oferta de honeypot que ofrece.

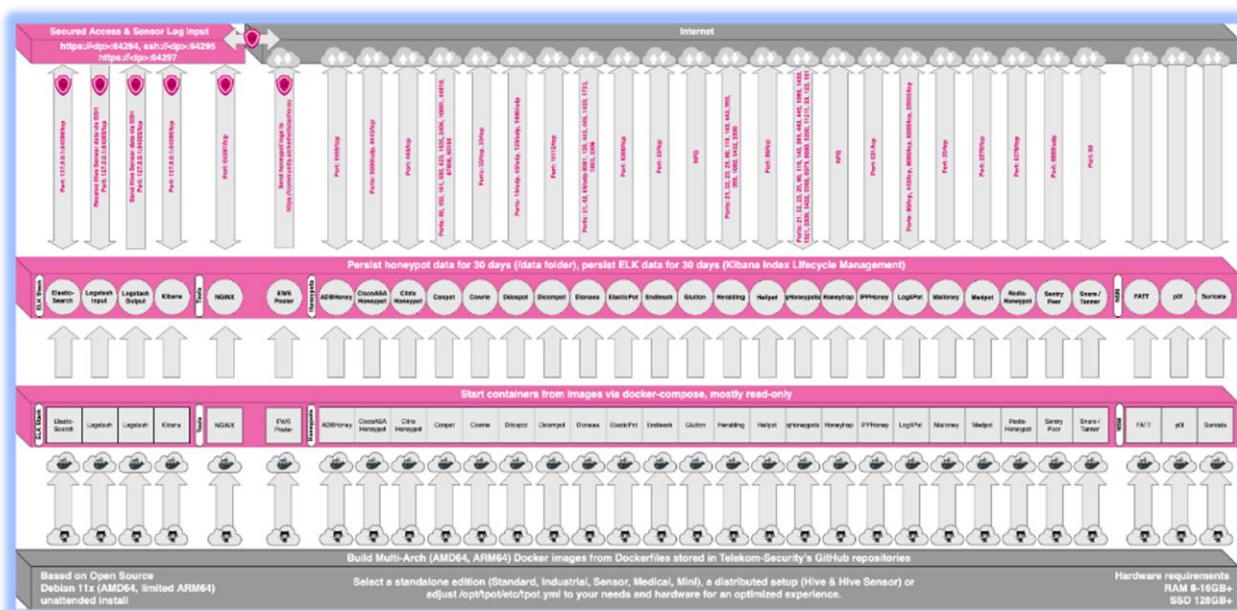


Ilustración 8 - Arquitectura técnica T-Pot

## 4.2 En detalle

T-Pot no solo es una herramienta de detección de amenazas, sino que también es un recurso indispensable para la investigación, la evaluación de seguridad, la formación y el desarrollo de soluciones de seguridad. Su versatilidad y capacidad para adaptarse a diferentes escenarios lo convierten en una herramienta esencial para los profesionales de la seguridad que buscan proteger sus sistemas y redes contra las crecientes amenazas.

### 4.2.1 Aplicaciones

Una vez que T-Pot está en funcionamiento, permite explorar una gran variedad de servicios [46] con los que auditar ataques y administrar el propio sistema:

- Servicios proporcionados por el sistema operativo
  - SSH o Secure Shell como protocolo de red para acceder y controlar equipos de forma segura
  - Cockpit para un acceso remoto basado en web, administración y terminal web
- Elastic Stack
  - Elasticsearch para almacenar eventos

- Logstash para la ingestión, recepción y envío de eventos a Elasticsearch
- Kibana para visualizar eventos en tableros altamente visuales.
- Herramientas
  - NGINX actúa como proxy inverso para facilitar acceso remoto seguro a Kibana, CyberChef, Elasticvue, GeoIP AttackMap y Spiderfoot
  - CyberChef es un recurso web que proporciona cifrado, codificación, compresión y análisis de datos
  - Elasticvue, es una aplicación web cliente que permite explorar e interactuar con una agrupación de nodos o clúster de Elasticsearch
  - Geoip Attack Map es un recurso web que muestra el mapa de ataques para T-Pot en tiempo real
  - Spiderfoot, una herramienta de automatización de código abierto
- Honeypots
  - Los honeypots mencionados anteriormente
- Supervisión de seguridad de red
  - Fatt es un script basado en PyShark [47] que es una línea de comandos para automatizar las capturas de red, facilitando el acceso y la manipulación del tráfico de red mediante el lenguaje de programación Python
  - P0f es una herramienta de identificación pasiva del sistema operativo (OS fingerprinting) y análisis de tráfico de red
  - Suricata, un motor de monitorización avanzado de seguridad de red

#### 4.2.2 Ventajas

Esta plataforma integral de honeypots ha sido diseñada para detectar y analizar actividades maliciosas, ofreciendo una serie de ventajas significativas para mejorar la seguridad en entornos corporativos. A continuación se enumeran algunas de las principales ventajas [48] de utilizar T-Pot:

- Detección avanzada de amenazas. Simula una amplia gama de servicios y aplicaciones, lo que permite detectar tanto amenazas conocidas como desconocidas. Esto brinda a los equipos de seguridad la capacidad de identificar nuevos métodos y tácticas utilizados.
- Entorno controlado y realista. Proporciona un entorno controlado para observar y analizar el comportamiento de los atacantes, permitiendo a los investigadores estudiar a fondo los ataques, identificar patrones y comprender las motivaciones detrás de las intrusiones.
- Evaluación de la postura de seguridad. La exposición a amenazas en un entorno controlado permite a las organizaciones evaluar la efectividad de sus defensas de seguridad existentes, facilitando la identificación y corrección de vulnerabilidades antes de que puedan ser explotadas en el entorno real.
- Facilidad de implementación y gestión. Gracias a un instalador integrado se simplifica el proceso de instalación y se facilita su implementación en sistemas y redes. Además, su conjunto de herramientas está diseñado para que sea fácilmente administrado y gestionado.
- Flexibilidad y adaptabilidad. Ofrece una variedad de honeypots diseñados para emular servicios y aplicaciones específicas, permitiendo la adaptación a las



cambiantes tácticas y técnicas utilizadas por los atacantes y mejorando así su eficacia como herramienta de detección de amenazas.

#### 4.2.3 Desventajas

Este apartado requiere de un análisis más riguroso debido a que algunas de las propias ventajas de la herramienta son las que se pueden convertir en desventajas en función del tipo de implementación o del entorno donde se quiera aplicar si, previamente, no se ha realizado un completo trabajo previo a la integración. Seguidamente, se enumeran las que se consideran más significativas:

- Falsos positivos. La naturaleza de un honeypot es atraer solo actividades maliciosas, pues nadie ajeno al equipo de seguridad debe conocer su existencia, no se debe descartar que se produzcan falsos positivos por diversos motivos, como pueden ser herramientas legítimas de detección de activos.
- Requerimiento de recursos. En función del entorno de producción en el que se ejecute o la dimensión de la red, T-Pot puede requerir de una gran cantidad de recursos de computación y capacidad de almacenamiento que se debe tener en cuenta si no se puede dedicar recursos en exclusiva.
- Configuración y mantenimiento. El proceso de instalación se ha simplificado, pero la configuración y mantenimiento pueden requerir una inversión considerable en esfuerzo y tiempo, sobre todo, en función de las dimensiones y complejidad del entorno, de mismo modo que ocurre con los requerimientos de recursos.
- Detección limitada. Aunque es una herramienta muy potente, no se debe descartar que existan amenazas o vulnerabilidades que no sea capaz de detectar ya que los atacantes están en continua evolución y cambio en sus técnicas y procedimientos.
- Discontinuidad del proyecto. Siendo un proyecto *open source*, no se debe descartar que el proyecto se abandone y dejen de recibirse actualizaciones, soporte y corrección de errores.

#### 4.2.4 Implementación

T-Pot representa una herramienta valiosa para aquellos dedicados a la seguridad, que buscan fortalecer su capacidad de detección de amenazas y comprender mejor las estrategias empleadas por los atacantes. Está construido sobre la imagen ISO de Debian 11 (Bullseye) *Netinstaller* y hace uso de *docker* y *docker-compose* para ejecutar múltiples herramientas de forma simultánea.

Su instalación [49] puede realizarse tanto en una máquina virtual como en hardware físico con acceso a internet y su puesta en marcha resulta relativamente simple, que implica descargar la imagen ISO desde su repositorio en GitHub, la creación de una máquina virtual y la instalación del sistema. No obstante, resulta esencial tener presente que la configuración y el mantenimiento de T-PoT podrían requerir un cierto nivel de competencia técnica.

## 5 Ciberseguridad en España

En el contexto de la seguridad corporativa en España, las opiniones y percepciones de los directivos son muy variadas, de las que se obtienen algunos hallazgos relevantes:

### 5.1 Estado de la seguridad corporativa

Según el Cybersecurity Readiness Index de Cisco, solo un 2% de las empresas españolas tiene una seguridad madura. Sin embargo, sorprendentemente, un 74% de las organizaciones cree que está preparado para enfrentarse a amenazas digitales.

El estudio [50] destaca que las empresas avanzan en su resiliencia, pero no al ritmo de la sofisticación de los ataques, existiendo una falta de alineación entre la percepción de preparación y la realidad de la seguridad.

### 5.2 Alineación entre estrategia de seguridad y negocio

Otro informe [51] revela que el 52% de los directivos españoles subestima la importancia de la seguridad en el éxito empresarial.

Existe una falta de alineación entre la estrategia de seguridad y los objetivos comerciales. Solo un 37% cree que existe una “fuerte alineación” entre ambos aspectos.

### 5.3 Trabajo remoto y amenazas emergentes

En un trabajo de investigación [52] realizado por el proveedor líder mundial de soluciones de seguridad Hornetsecurity, por una parte se destaca la falta de formación en seguridad para empleados remotos, donde se observa que un 33% de las empresas no proporcionan ninguna capacitación.

Por otra parte, a pesar de que el 74% de los trabajadores remotos tienen acceso a datos críticos, tan solo el 18% de los profesionales de IT consideran que estos empleados se mantienen seguros en este entorno. Además, aproximadamente el 44% de las organizaciones planea aumentar el trabajo remoto, lo que subraya la necesidad urgente de abordar los riesgos asociados.

Estos desafíos incluyen la falta de comprensión y confianza en las medidas de seguridad remotas, así como la prevalencia de incidentes relacionados con el teletrabajo, como el compromiso de puestos y credenciales de usuario. Es obvio que para mejorar la seguridad remota, se requiere una mayor inversión en formación y concienciación sobre seguridad, así como en la gestión efectiva de los equipos de usuario.

### 5.4 Conciencia y aplicación de medidas

Los directivos deben reconocer la importancia crítica de la seguridad y alinearla con los objetivos comerciales. Al mismo tiempo, la inversión en formación, tecnología y prácticas sólidas es esencial para proteger a las organizaciones en un mundo cada vez más hiperconectado.

## 6 Hipótesis planteadas

En el ámbito de la investigación de amenazas, el uso de una herramienta de seguridad avanzada como es T-Pot se presenta como una solución innovadora.

Se plantea el uso de dicha herramienta para la implementación de múltiples honeypots, de baja y alta interacción, con los que emular servicios y aplicaciones específicas, con la intención de detectar y analizar una gama más amplia de ataques en comparación con las soluciones de seguridad tradicionales usadas por las compañías, tratando de proporcionar una visión más detallada y precisa de las tácticas, técnicas y procedimientos utilizados por los atacantes.

De este modo, con esta estrategia de recopilación de datos de ataques en tiempo real, el equipo de seguridad de la corporación tendrá la oportunidad de analizar y comprender mejor las estrategias de los atacantes, identificar nuevas amenazas y patrones de ataque, plantear mitigaciones y elaborar estrategias de defensa más efectivas.

El planteamiento del uso de T-Pot debe proporcionar una visión más completa del panorama de amenazas, permitiendo la detección de ataques dirigidos a una variedad de servicios y aplicaciones, resultando especialmente útil en un entorno en constante evolución, donde los atacantes están desarrollando y adaptando sus métodos de forma constante.

## 7 Descripción de experimentos a llevar a cabo

- Instalación y configuración inicial de T-Pot. Partiendo de una configuración básica, donde verificar el funcionamiento y respuesta de la herramienta, así como para familiarizarse con uso del aplicativo.
- Evaluación de la efectividad de la detección de amenazas. Comparando la capacidad de detección de amenazas de la herramienta con otras soluciones de seguridad existentes en empresas.
- Análisis de la vulnerabilidad de la red. Identificando posibles puntos débiles en la infraestructura de red y evaluando el riesgo asociado.
- Simulación de ataques controlados. Ejecutando ataques simulados para monitorizar la respuesta de la herramienta y para evaluar su capacidad para detectar y responder a amenazas.
- Evaluación del impacto en el rendimiento del sistema. Investigando cómo afecta la implementación de T-Pot al rendimiento del sistema, como la velocidad de la red y el uso de recursos.
- Estudio de la inteligencia de amenazas. Analizando los datos recopilados para identificar patrones y tendencias en los ataques y utilizando esta información para mejorar las estrategias de seguridad.

## 8 Materiales y métodos

### 8.1 Diseño de la infraestructura

En esta fase se ha realizado una labor de investigación con la que adquirir mayor conocimientos sobre la variedad de diseños con los que se cuentan para la

implementación de honeypot. Así, se han revisado multitud de diseños como instalaciones de pruebas, proyectos de fin de grado y producción, entre otros. Finalmente, se ha decidido realizar un diseño más realista con entornos corporativos, pero orientado al objetivo de este TFG de alcanzar sistemas más resilientes, conocer las tácticas, técnicas y procedimientos de los actores amenaza, análisis de malware (programas informáticos maliciosos) e inteligencia de amenazas.

#### 8.1.1 Entorno de pruebas

En una instalación normal donde se cubriese todo lo necesario para desplegar un conjunto de honeypot de alta-media-baja interacción, incluyendo herramientas de gestión y monitorización, estaría compuesta por los siguientes elementos:

En una propuesta de infraestructura, para que fuese robusta y segura habría que considerar una arquitectura basada en software empaquetado, como son los contenedores [53], para facilitar la gestión y escalabilidad de los recursos. Un ejemplo puede ser el siguiente:

#### 8.1.2 Hardware

##### Equipo de Pruebas

- CPU 8 núcleos
- RAM 32 GB
- Almacenamiento del sistema en disco de estado sólido (SSD) de 500 GB
- Almacenamiento de datos en disco SSD de 1TB
- Almacenamiento conectado a la red (NAS) para copia de respaldo y almacenamiento de datos críticos

#### 8.1.3 Software

- Sistema Operativo GNU/Linux Debian [54] como base para la instalación de otros componentes
- Plataforma de software para contenedores. Docker [55] es una tecnología de tiempo de ejecución de contenedores para la creación, pruebas e implementación de aplicaciones o servicios contenerizado
- Orquestador de Contenedores. Kubernetes [56] para la administración, coordinación y automatización de gran número de contenedores de forma más sencilla y controlada

#### 8.1.4 Componentes de seguridad

- Honeypot de baja, media y alta interacción con los que emular una variedad de servicios y aplicaciones, vulnerabilidades y defectos de configuración
- Honeywall para monitorizar y registrar el tráfico de red
- Herramientas de monitorización como Elasticsearch [57], Logstash [58] y Kibana [59] (ELK Stack) para almacenar, visualizar y analizar los logs
- Cortafuegos para controlar el tráfico entrante y saliente

#### 8.1.5 Red

- Segmentación de red para la separación de redes del entorno de pruebas y producción

- VPN configurada para conexiones seguras y acceso remoto al entorno de pruebas desde ubicaciones externas

Pues bien, todos los elementos anteriores, con la excepción del cortafuegos, se pueden instalar y configurar de manera sencilla y eficiente en el hardware designado, y a través de la herramienta T-Pot, facilitando enormemente este proceso.

T-Pot se encarga de la instalación y configuración de estos componentes, así como de su integración, permitiendo que trabajen en conjunto de manera eficaz, simplificando enormemente el proceso y permitiendo centrarse en otros aspectos del sistema.

Sin embargo, el cortafuegos es una excepción a esta regla, ya que su instalación y configuración requieren un proceso independiente, que no está cubierto por T-Pot. Este proceso queda detallado en un **anexo 1** a este trabajo, donde se proporciona una guía paso a paso para la instalación y configuración.

#### 8.1.6 Ubicación estratégica de los honeypots

En un entorno realista, la zona que se puede considerar más expuesta a ataques es la DMZ [60], zona de red que es donde se presentan servicios hacia el exterior como un servidor web o un reenviador de correo, entre otros. En el diseño desarrollado se ha aplicado una configuración al enrutador para habilitar un equipo como DMZ, quedando redireccionado todo el tráfico entrante hacia los puertos abiertos TCP / UDP pertenecientes a los honeypot activos de T-Pot. De esta forma, se facilitan la captura de los ataques que se produzcan sobre los honeypot configurados para tal efecto. Además, en el cortafuegos OPNSense [61] es necesario habilitar las reglas necesarias para permitir el tráfico hacia este equipo, tal y como puede observarse en la ilustración número 9 ubicada más abajo.

**Configuración de DMZ**

---

Configuración DMZ de ordenador  
La DMZ actual es: **192.168.1.11**

---

 Tienes que asociar una dirección IP estática con este dispositivo en la configuración de DHCP

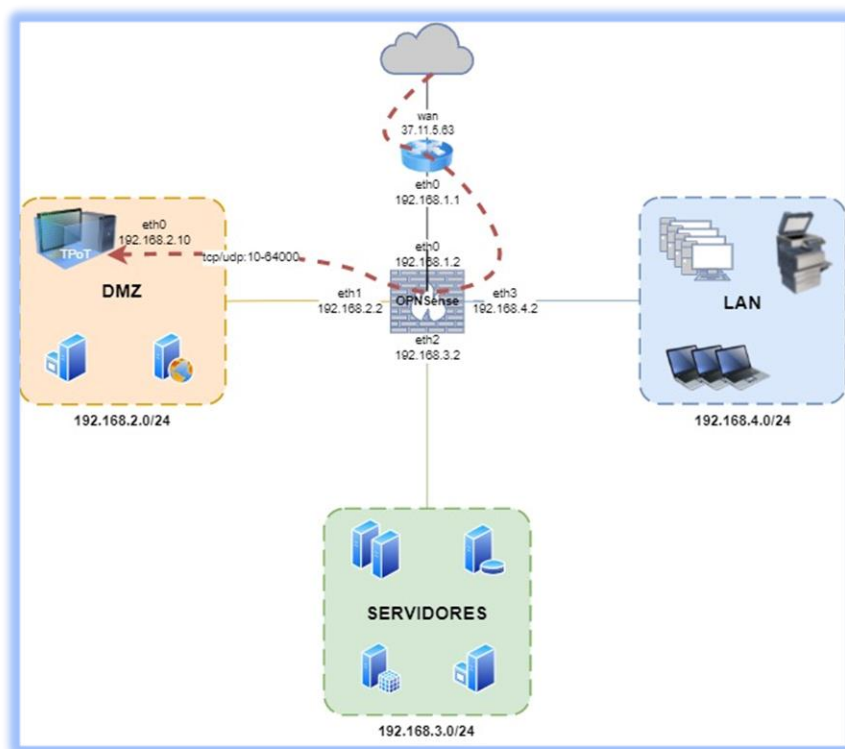
---

La DMZ actual es:

nombre	dirección IP	
automaticexile	192.168.1.11	<b>guardar</b>

*Ilustración 9 - configuración DMZ en enrutador*

El diagrama de red que representa el diseño y la ubicación se muestra en la ilustración número 10, a continuación:



Il·lustració 10 - diagrama de red para T-Pot

## 8.2 Despliegue de T-Pot

### 8.2.1 Instalación y configuración en un entorno controlado

Este proceso queda detallado en un **anexo 2** a este trabajo, donde se proporciona una guía paso a paso para la instalación y configuración.

### 8.2.2 Personalización de la configuración

Si la instalación ha finalizado con éxito, el siguiente paso es probar los accesos que existen a la solución para acceder por consola o a los distintos paneles de administración disponibles:

Il·lustració 11 - Pantalla de bienvenida con información de acceso

El sistema está fundamentado en una arquitectura basada en contenedores utilizando



Docker, lo que facilita enormemente la gestión y administración de los distintos

honeypots implementados. Resulta sencillo familiarizarse con algunos de sus comandos básicos, permitiendo el control y supervisión de los contenedores individuales en los que se despliegan estos honeypots. A continuación, se detallan diversas acciones y sus comandos correspondientes para la gestión efectiva de los contenedores:

- Listar. Enumerando tanto los activos como los inactivos
  - `docker ps -a`
- Listar solo los activos. Mostrando solo los que están en ejecución
  - `docker ps`
- Detener. Si está en ejecución, lo para
  - `docker stop [ID o nombre del contenedor]`
- reiniciar. Realizar un reinicio de un contenedor específico
  - `docker restart [ID o nombre del contenedor]`
- Eliminar. Borra un contenedor específico, aunque dentro del entorno de T-Pot no se recomienda su eliminación, sino detener su ejecución y evitar la carga del honeypot comentando las líneas necesarias desde el fichero de configuración. El proceso queda explicado más adelante
  - `docker rm [ID o nombre del contenedor]`
- Estadísticas y logs. Permite visualizar información estadística detallada por uso de recursos, así como logs de ejecución, propios del contenedor
  - `docker stats [ID o nombre del contenedor]`
  - `docker logs [ID o nombre del contenedor]`
- Ejecutar comandos. Permite la ejecución de comandos dentro del contenedor
  - `docker exec -it [ID o nombre del contenedor] [comando]`

La instalación predeterminada implementa configuraciones que son significativas para garantizar la estabilidad y el rendimiento del sistema. Entre estas configuraciones se incluyen la actualización automática de paquetes, el reinicio del sistema en caso de errores graves, la protección contra ataques de fuerza bruta en servicios de administración web y de acceso remoto, así como tareas programadas para la actualización de contenedores, la rotación de logs y la limpieza de datos según el periodo de retención establecido.

Para ajustar la configuración de T-Pot al entorno deseado, es necesario y muy importante conocer la ubicación de ciertos directorios y archivos clave, los cuales se pueden localizar en:

- instalación: `/opt/tpot`
- configuración del servicio: `/etc/systemd/system/tpot.service`
- plantilla ejecución: `/opt/tpot/etc/tpot.yml`
- rotación log: `/opt/tpot/etc/logrotate/logrotate.conf`
- datos persistentes para contenedores: `/data`

### 8.2.3 Fortaleciendo T-Pot

Después de la instalación inicial es posible personalizar y ajustar la configuración de T-Pot para adaptarla a las necesidades específicas del entorno. Con esta práctica no solo se va a mejorar la seguridad y la eficacia de los honeypots desplegados, sino que también se va a enmascarar su uso, haciendo que pasen desapercibidos.



Además, es fundamental mantener actualizado el sistema sobre el cual se ejecuta T-Pot para corregir vulnerabilidades en el sistema base. También se debe personalizar los permisos y privilegios de usuario para restringir el acceso a los recursos sensibles, garantizando una gestión de identidad y acceso seguros.

Otro aspecto importante es configurar reglas de cortafuegos, tanto en local como en perimetral, y otras configuraciones relacionadas con la conectividad para asegurar y optimizar el tráfico hacia y desde los honeypots. En la versión instalada se configura el cortafuegos de Linux con el comando *iptables*, tomando como parámetros los puertos identificados en la plantilla cargada desde *"/opt/tpot/etc/compose"* con la configuración de T-Pot.

T-Pot aprovecha la tecnología de contenedores al ejecutar cada honeypot en contenedores Docker. Esta integración con *Docker*, junto con *Docker-compose* [62] cuando se necesita trabajar con más de un contenedor a la vez, ofrece la capacidad de ejecutar múltiples contenedores con el uso de un solo adaptador de red, lo que dificulta la detección de la solución por parte de los atacantes.

Estas acciones están pensadas para disimular el entorno ficticio, haciendo creer al atacante que se encuentra en un sistema real, y están diseñadas para prolongar al máximo la interacción de este actor malicioso, permitiendo así un estudio más exhaustivo de sus movimientos y la recopilación de información. Esta información puede luego ser analizada para generar inteligencia contra amenazas y fortalecer las defensas de seguridad.

A continuación, se enumeran los apartados que se consideran más importantes en base a la experiencia adquirida durante la consulta bibliográfica realizada durante la elaboración de este trabajo y que se recomienda tener en cuenta en la personalización de T-Pot, y por ende, del entorno simulado:

#### 8.2.3.1 Servicios

Activando solo los que se quieran evaluar, reduciendo a un número imprescindible que sea suficiente para alcanzar el objetivo de la investigación que se quiera realizar. Es decir, en un escenario donde se quiere evaluar un servicio web y una base de datos SQL (Structured Query Language), tan solo se deberían activar los honeypot involucrados.

La solución ofrece varias plantillas prediseñadas que se adaptan a situaciones concretas y que pueden modificarse para ajustar la configuración con mayor detalle. Además, es posible crearlas personalizadas para adecuar la configuración a entornos más específicos, incluyendo distintos apartados de otras plantillas. Estos archivos, se pueden encontrar en el directorio de instalación de la aplicación, cuya ubicación puede variar según las opciones seleccionadas durante el proceso de implantación o la versión de T-Pot. En el entorno desarrollado, las plantillas están localizadas en *"/opt/tpot/etc/compose"*:



```
[tsec@automaticexile:/opt/tpot/etc/compose]$ ls -alh
total 132K
drwxr-xr-x 2 root root 4.0K Apr 13 21:21 .
drwxr-xr-x 5 root root 4.0K Apr 14 13:48 ..
-rw-r--r-- 1 root root 5.6K Apr 13 21:13 collector.yml
-rw-r--r-- 1 root root 160 May  1 11:49 elk_environment
-rw-r--r-- 1 root root 13K Apr 13 21:13 hive_sensor.yml
-rw-r--r-- 1 root root 3.1K Apr 13 21:13 hive.yml
-rw-r--r-- 1 root root 11K Apr 13 21:13 industrial.yml
-rw-r--r-- 1 root root 5.5K Apr 13 21:13 log4j.yml
-rw-r--r-- 1 root root 5.4K Apr 13 21:13 medical.yml
-rw-r--r-- 1 root root 5.8K Apr 13 21:13 mini.yml
-rw-r--r-- 1 root root 14K Apr 13 21:13 nextgen.yml
-rw-r--r-- 1 root root 13K Apr 13 21:13 sensor.yml
-rw-r--r-- 1 root root 16K Apr 14 13:48 standard.yml
-rw-r--r-- 1 root root 6.2K Apr 13 21:13 tarpit.yml
[tsec@automaticexile:/opt/tpot/etc/compose]$
```

Ilustración 12 - localización archivos configuración docker-compose

Realmente, estos archivos funcionan como parámetros de ejecución para “*Docker-compose*” y contienen la configuración requerida para iniciar el entorno multi contenedor. Su contenido abarca ajustes y recursos necesarios para la ejecución de cada contenedor, como los puertos de entrada y salida utilizados, el estado de los servicios, las redes y el montaje de volúmenes de almacenamiento temporales y permanentes, entre otros.

#### 8.2.3.2 Credenciales y usuarios

Es imprescindible, siempre revisar y actualizar las credenciales incluidas en la configuración inicial de T-Pot para garantizar la seguridad del sistema. De este modo, se deben sustituir por credenciales que no estén relacionadas ni documentadas previamente. Respecto a los usuarios utilizados, si es necesario mantener algunos específicos, se recomienda cambiar los nombres predeterminados para evitar posibles correlaciones con el honeypot utilizado. Además, para una mayor seguridad, es preferible utilizar un archivo o base de datos que contenga las credenciales utilizadas por el contenedor, en lugar de credenciales preconfiguradas o de prueba que puedan ser fácilmente identificadas.

#### 8.2.3.3 Pantalla de bienvenida

Cuando se accede a un sistema y se muestra la pantalla de bienvenida es determinante que no esté incluida información que resulte familiar o pueda identificar la solución que se encuentra detrás del servicio simulado. Por lo tanto, es necesario modificar los archivos relacionados con esta configuración y ajustar la plantilla predeterminada que se aplica.

#### 8.2.3.4 Directorios

Es necesario variar cualquier ruta configurada que no esté relacionada con una instalación típica de un sistema real. Es decir, se debe evitar dejar indicios que sean fácilmente identificables, como nombres de archivo o directorios específicos de la instalación original de T-Pot. Incluso, en el lado opuesto, se deben completar los que sean más comunes y que se puedan echar en falta, como por ejemplo en un honeypot que permita el acceso para administración remota a través del protocolo *Secure Shell* o

SSH [63], se deben incluir directorios comunes en la estructura de archivos de un sistema operativo, como la carpeta *temp* o *home*, junto con algunos archivos representativos.

#### 8.2.3.5 Información del sistema

Quizás, esta sea una de las partes en las que se puede dedicar más tiempo a la personalización, con el fin de convencer al intruso de que se encuentra en un sistema auténtico. Esta tarea implica personalizar las respuestas esperadas del sistema al ejecutar un comando para obtener información sobre el servicio al que se ha accedido.

Cuando un atacante obtiene acceso a un servicio, su primer paso suele ir en dirección a identificarlo consultando archivos que contienen información del sistema. Este proceso es especialmente evidente en algunos sistemas como Linux, donde es posible obtener datos desde archivos ubicados en el directorio */proc* e incluso desde variables de entorno con la ejecución del comando *printenv*. En este escenario, es significativo asegurarse de que el contenido de estos archivos proporcione la información necesaria para que el servicio parezca creíble y auténtico.

```
[tsec@automaticexile:/proc]$ cat cpuinfo
processor      : 0
vendor_id    : GenuineIntel
cpu family   : 6
model        : 141
model name   : 11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz
stepping     : 1
cpu MHz      : 2304.008
cache size   : 24576 KB
physical id  : 0
siblings     : 4
core id      : 0
cpu cores    : 4
```

Ilustración 13 - ejemplo de obtención de información del sistema

### 8.3 Configuración de honeypots básicos

La instalación original de T-Pot ofrece una amplia variedad de servicios que se clasifican en cinco grupos:

#### 1. Servicios proporcionados por el sistema operativo anfitrión

- SSH como protocolo de acceso remoto seguro

#### 2. Elastic Stack

- Elasticsearch, para almacenar eventos
- Logstash acepta el envío y recepción de eventos hacia Elasticsearch
- Kibana, para mostrar eventos en paneles y que resulten visualmente atractivos

#### 3. Herramientas

- Nginx [64], actuando como proxy inverso [65] para proporcionar acceso remoto seguro a Kibana, CyberChef, Elasticvue, GeolIP, AttackMap, Spiderfoot, y permite que los sensores de T-Pot transmitan de manera segura los eventos a su núcleo

- CyberChef es una aplicación web para cifrado, codificación, compresión y análisis de datos
- Elasticvue actúa como la parte visible hacia el usuario y permite navegar e interactuar con un clúster (agrupación de nodos) de Elasticsearch
- AttackMap es un mapa de ataques animado para T-Pot que resulta muy atractivo de visualizar
- Spiderfoot [66] es una herramienta utilizada para automatizar la generación de inteligencia a partir de los datos obtenidos desde fuentes abiertas.

#### 4. Honeypots

- Forman un conjunto de 23 honeypots disponibles basados en el archivo docker-compose.yml que se haya seleccionado

#### 5. Monitorización de seguridad de red o NSM

- Fatt es un script basado en pyshark para la extracción de metadatos de red y fingerprinting, o identificación característica, de archivos pcap y tráfico de red en línea
- P0f es una herramienta para el fingerprinting de tráfico puramente pasivo
- Suricata es un motor de monitorización de seguridad de red

##### 8.3.1 Configuración de honeypots según el análisis previo

En las pruebas iniciales realizadas desde la instalación estándar de T-Pot, en concreto 17 días, se analizan los datos recolectados para obtener los servicios con mayor volumen de ataques y los honeypots involucrados.

De este primer análisis se observa un elevado número de ataques que se han producido en un periodo muy corto de tiempo, llegando a un total de más de 70 mil, lo que supone una media de casi 3.500 diarios.

*Ilustración 14 - mapa global de ataques recibidos*

Los servicios expuestos que han recibido mayor número de conexiones o intentos de ataques han sido los relacionados con los puertos 53/udp para resolución de nombres de dominio o DNS, 445/tcp para recursos compartidos o SMB y 22/tcp para acceso remoto seguro o SSH:

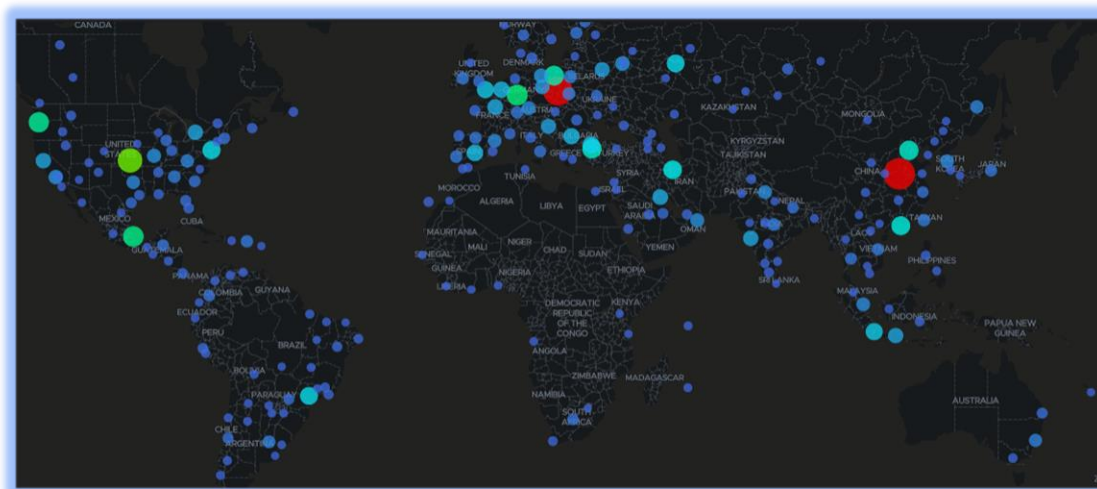




Ilustración 15 - Puertos expuestos más atacados

Por otra parte, de la variedad de honeypots [67] que ofrece T-Pot, los que mayor incidencia han tenido en el mismo periodo de tiempo han sido los siguientes:

**Ddospot** con 18.706. Es utilizado para rastrear y monitorizar ataques de denegación de servicio distribuida o DDoS.

**Dionaea** con 18.230. Destinado a detectar fragmentos de código expresamente diseñado para la ejecución de una función específica en un sistema comprometido, con el que lograr acceso no autorizado o tomar el control del sistema. Ideal para la captura y análisis de malware.

**Honeytrap** con 11.036. Es de baja interacción y solo observa ataques en servicios TCP y UDP, capturando el tráfico de red generado para su posterior análisis

**Cowrie** con 8.293. Es de media y alta interacción, registra ataques de fuerza bruta en los inicios de sesión y captura de la interacción del atacante con el terminal.

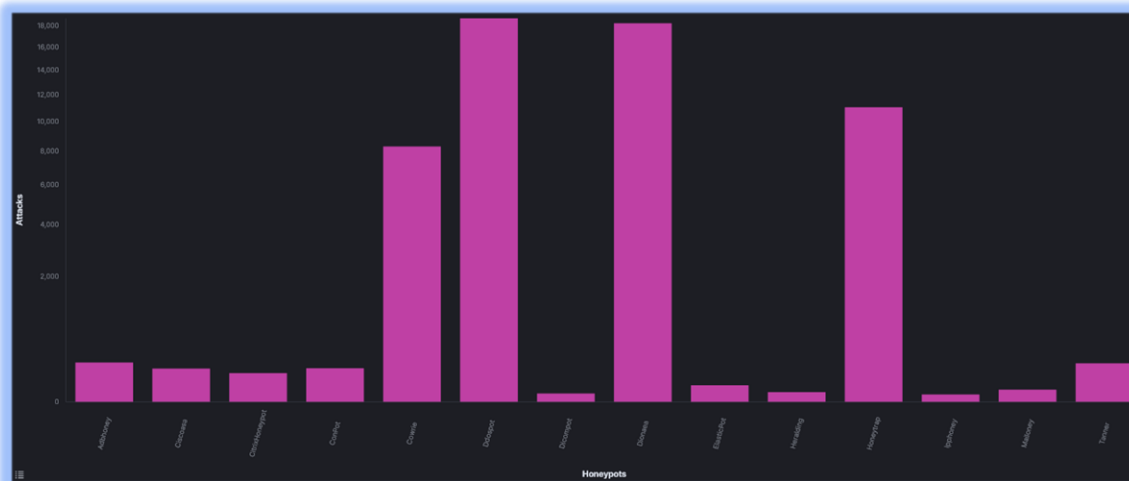


Ilustración 16 - honeypots más activos

Teniendo en cuenta esta información, se recomienda una configuración básica que priorice la monitorización y captura de tráfico en estos puertos utilizando honeypots específicos adaptados a estas necesidades. De esta forma, la propuesta recomendada es la siguiente:

- Puerto 53/udp para el servicio DNS. Se recomienda DDospot
- Puerto 445/tcp (SMB). Se recomienda Dionaea.
- Puerto 22/tcp (SSH). Se recomienda Cowrie

A pesar de su alta tasa de ataques, se opta por descartar el uso de Honeytrap debido a su baja interacción, lo que lo hace más fácil de detectar en comparación con otros, como Cowrie, que ofrece una mayor interacción y, por lo tanto, se considera una mejor alternativa.

Partiendo de la instalación básica de T-Pot se va a adaptar la plantilla de configuración de Docker-compose para personalizar los servicios y honeypot activos que se quieren establecer para la captura de información. Los pasos que se siguen son los siguientes:

- Las plantillas de configuración están localizadas según el proceso de instalación. En este proyecto las plantillas están ubicadas en **/opt/tpot/etc/compose**
- Se accede a la ruta y se copia una de las plantillas que contenga los honeypots seleccionados, por ejemplo standard.yml, en un archivo con nombre "personalizado.yml"

```
drwxr-xr-x 5 root root 4096 May  2 21:59 .
drwxr-xr-x 12 root root 4096 Apr 13 21:13 ..
drwxr-xr-x 2 root root 4096 May  2 21:51 compose
drwxr-xr-x 2 root root 4096 May  2 18:16 logrotate
drwxr-xr-x 2 root root 4096 Apr 13 21:13 objects
lrwxrwxrwx 1 root root   39 May  2 21:59 tpot.yml -> /opt/tpot/etc/compose/personalizado.yml
lrwxrwxrwx 1 root root   34 Apr 13 22:27 tpot.yml.bak -> /opt/tpot/etc/compose/standard.yml
```

Ilustración 17 - enlace simbólico a la plantilla de configuración

- Se modifica la plantilla creada desactivando las redes y honeypot seleccionados no seleccionados. Se puede comentar o eliminar las líneas que no se necesiten y se mantienen las herramientas y utilidades necesarias para el correcto funcionamiento de T-Pot.
- Por último, se ejecutan los siguientes comandos para completar el cambio de plantilla:
  - `sudo /opt/tpot/bin/dps.sh` (muestra el estado de los contenedores)
  - `sudo systemctl stop tpot` (detiene T-Pot)
  - `sudo mv tpot.yml tpot.yml.bak` (se renombra enlace)
  - `sudo ln -s /opt/tpot/etc/compose/personalizado.yml tpot.yml` (nuevo enlace)
  - `sudo systemctl start tpot` (inicia T-Pot)
  - `sudo /opt/tpot/bin/dps.sh` (muestra el estado de los contenedores)

```
[tsec@automaticexile:/opt/tpot/etc]$ sudo systemctl start tpot
[tsec@automaticexile:/opt/tpot/etc]$ sudo /opt/tpot/bin/dps.sh
[ *****] System [***** ]
DATE: Thu 02 May 2024 10:02:19 PM CEST
UPTIME: 22:02:19 up 3:45, 1 user, load average: 1.77, 0.99, 1.11
T-POT: ACTIVE
BLACKHOLE: DISABLED

NAME          STATUS          PORTS
cowrie        Up 36 seconds  0.0.0.0:22-23->22-23/tcp
ddospot       Up 37 seconds  0.0.0.0:19->19/udp, 0.0.0.0:53->53/udp, 0.0.0.0:123->123/udp, 0.0.0.0:1900->1900/udp
dionaea       Up 36 seconds (healthy)  0.0.0.0:20-21->20-21/tcp, 0.0.0.0:42->42/tcp, 0.0.0.0:81->81/tcp, 0.0.0.0:135->135/tcp, 0.0.0.0:445->445/tcp, 0.0.0.0:1433->1433/tcp, 0.0.0.0:1723->1723/tcp, 0.0.0.0:1883->1883/tcp, 0.0.0.0:3306->3306/tcp, 0.0.0.0:27017->27017/tcp, 0.0.0.0:69->69/udp
elasticsearch Up 36 seconds (healthy)  127.0.0.1:64298->9200/tcp
fatt          Up 38 seconds
kibana        Up 5 seconds (health: starting)  127.0.0.1:64296->5601/tcp
logstash      Up 5 seconds (health: starting)
map_data      Up 5 seconds
map_redis     Up 36 seconds
map_web       Up 36 seconds  127.0.0.1:64299->64299/tcp
nginx         Up 38 seconds
p0f           Up 38 seconds
sentrypeer    Up 36 seconds  0.0.0.0:5060->5060/udp
spiderfoot    Up 36 seconds (healthy)  127.0.0.1:64303->8080/tcp
suricata      Up 38 seconds
```

Ilustración 18 – T-Pot iniciado con configuración personalizada

Para futuras reconfiguraciones de T-Pot, se puede considerar la inclusión de distintos honeypots que utilicen los mismos puertos en análisis de los detectados en el análisis previo. Esto permitiría obtener información diversa o enfoques variados según la configuración personalizada aplicada a cada honeypot. A continuación, se enumeran varios honeypots que detectan los mismos tipos de puertos seleccionados (destacados en **negrita**), junto con otros adicionales:

- DNS
  - qHoneypots - **53**, 123, 161, 5060
  - Ddospot - 19, **53**, 123, 1900
- SMB
  - Dionaea - 21, 42, 135, 443, **445**, 1433, 1723, 1883, 3306, 8081
  - qHoneypots - 21, 22, 23, 25, 80, 110, 143, 389, 443, **445**, 631, 1080, 1433, 1521, 3306, 3389, 5060, 5432, 5900, 6379, 6667, 8080, 9100, 9200, 11211
- SSH
  - Cowrie – **22,23**
  - Endlessh – **22**
  - Heralding - 21, **22**, 23, 25, 80, 110, 143, 443, 993, 995, 1080, 5432, 5900
  - qHoneypots - 21, **22**, 23, 25, 80, 110, 143, 389, 443, 445, 631, 1080, 1433, 1521, 3306, 3389, 5060, 5432, 5900, 6379, 6667, 8080, 9100, 9200, 11211



## 9 Resultados. Caso práctico en monitorización y recopilación de datos

El propósito de esta investigación radica en emplear una herramienta de detección y recolección de información para identificar vulnerabilidades y actividades maliciosas, con el fin de evaluar y mejorar la eficacia de las medidas de protección implementadas en un entorno expuesto a una red pública como Internet.

Aunque no todos los servicios gestionados por una empresa están accesibles públicamente, aquellos que sí lo están pueden representar puntos de acceso indirectos si no se protegen adecuadamente. Cobra gran importancia realizar pruebas continuas para evaluar la robustez de la infraestructura y las aplicaciones activas que ofrecen servicios esenciales a la organización.

Esta evaluación no solo implica mantener actualizados los sistemas, sino también identificar posibles vulnerabilidades o configuraciones incorrectas que puedan ser explotadas por actores malintencionados para comprometer la integridad del sistema o acceder a información confidencial.

De esta forma, es fundamental someter a prueba los activos a proteger para detectar dichas situaciones, analizar los datos recopilados para obtener información relevante que permita mejorar las medidas de seguridad existentes, y transformar estos hallazgos en inteligencia práctica aplicable a las herramientas de seguridad corporativas con el fin de fortalecer la resiliencia del sistema.

### 9.1 Herramientas utilizadas en análisis y monitorización de datos

Estas herramientas abarcan sistemas de análisis de tráfico, soluciones de inteligencia de amenazas, y plataformas de visualización, todas diseñadas para facilitar la interpretación y gestión de datos complejos. De esta forma, se encuentran los sistemas de análisis de tráfico que permiten la monitorización y examen del flujo de datos en la red, detectando actividades anómalas y potencialmente maliciosas. Igualmente, las soluciones de inteligencia de amenazas proporcionan información actualizada sobre nuevas amenazas y vulnerabilidades, ayudando a la anticipación y prevención de ataques. Del mismo modo, las plataformas de visualización convierten grandes volúmenes de datos en representaciones gráficas intuitivas, permitiendo a los analistas la identificación rápida de patrones de comportamiento malicioso.

En consecuencia, al integrar múltiples fuentes de datos y aplicar técnicas avanzadas de análisis, estas herramientas no solo mejoran la visibilidad y la seguridad de la red, sino que también optimizan la capacidad de respuesta ante incidentes de seguridad, asegurando una protección proactiva y eficaz.

#### 9.1.1 Propias de T-Pot

La versión de T-Pot implementada (v22.04) corresponde con la última disponible a la fecha de inicio de este proyecto, e incluye herramientas de monitorización y de análisis con las que iniciarse en la detección y estudio de diferentes tipos de ataques aplicados a los servicios simulados correspondientes con activos reales de la corporación.

**Elastic Stack.** Desempeña una función primordial en T-Pot al posibilitar la recopilación y tratamiento exhaustivo de los registros generados por los honeypots en activo. Esta



paquete de herramientas constituye una plataforma integral para la gestión de datos de seguridad:

- Elasticsearch, mediante la indexación y el almacenamiento de eventos
- Logstash, que facilita la ingestión y el procesamiento de datos
- Kibana, que proporciona una interfaz de usuario intuitiva para la visualización y el análisis de datos accesible desde la URL <https://192.168.1.11:64297/kibana/app/dashboards>

Estas capacidades son esenciales para la detección y respuesta efectiva ante amenazas en entornos de seguridad corporativos.

**Spiderfoot.** Es del tipo OSINT [68] o inteligencia de fuentes abiertas, y se utiliza para la obtención activa de conocimiento a partir de fuentes de acceso público. Este proceso implica la búsqueda, selección y adquisición de información, seguido por un análisis para obtener conocimientos aplicables en diversos contextos.

Está accesible desde la URL <https://192.168.1.11:64297/spiderfoot>

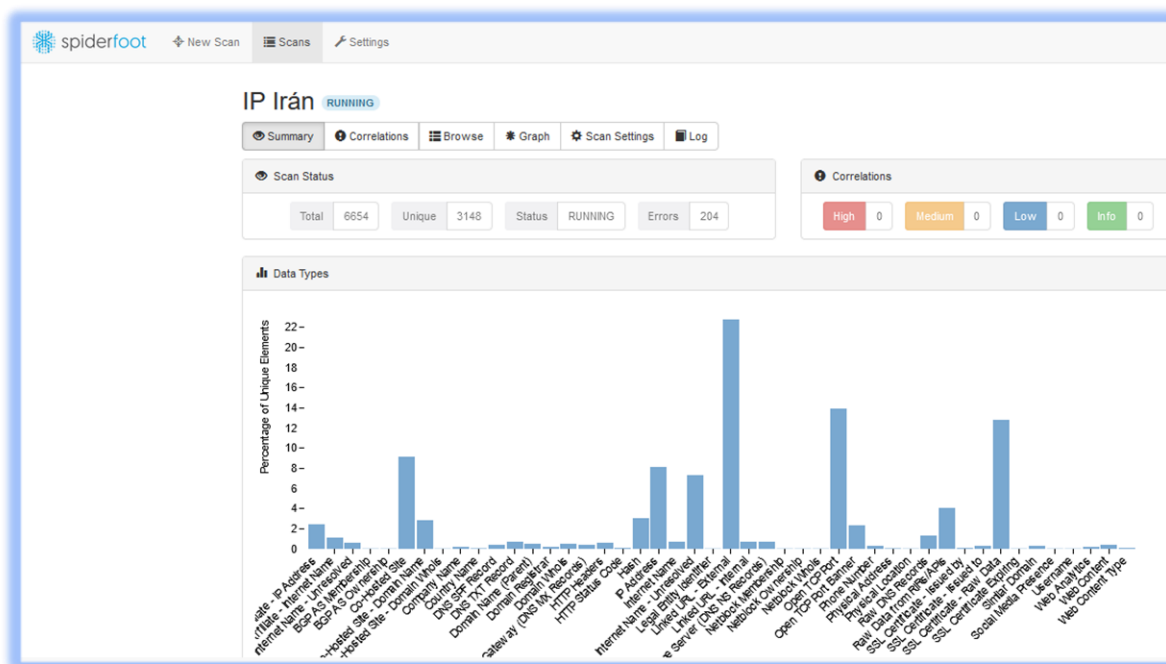


Ilustración 19 - información de una IP desde Spiderfoot

### 9.1.2 En línea

**Cisco Talos.** El Centro de Inteligencia ofrece herramientas en línea que permiten la verificación de diversos indicadores de compromiso, tales como direcciones IP, dominios, URLs y hashes, entre otros. Estas herramientas facilitan el acceso a la vasta inteligencia de amenazas recopilada por su grupo de seguridad a lo largo de los años, proporcionando a los usuarios información valiosa para proteger sus sistemas.

Esta herramienta de consulta está accesible desde la URL [https://www.talosintelligence.com/reputation\\_center](https://www.talosintelligence.com/reputation_center)

**Virustotal.** Es un servicio en línea gratuito que permite analizar archivos y URLs en busca de malware, utilizando múltiples motores antivirus para detectar amenazas.

Además, facilita la verificación de indicadores de compromiso como direcciones IP, dominios y hashes, proporcionando inteligencia de amenazas recopilada por su grupo de seguridad. Es una herramienta de gran utilidad para identificar y protegerse contra contenido malicioso y actividades sospechosas.

Esta accesible desde la URL <https://www.virustotal.com/gui/home/upload>

**UrlScan.** También es un servicio en línea gratuito para analizar y verificar URLs en busca de contenido malicioso y actividades sospechosas. Utilizando múltiples motores de análisis, ayuda a identificar y prevenir amenazas. También facilita la verificación de indicadores de compromiso como direcciones IP, dominios y recursos cargados por las URLs, proporcionando inteligencia de amenazas recopilada por su equipo de seguridad. Es una herramienta esencial para identificar y mitigar riesgos asociados con URLs potencialmente peligrosas.

Se accede a esta herramienta desde la URL <https://urlscan.io>

**Shodan,** Es un motor de búsqueda especializado en dispositivos conectados a Internet, proporciona información detallada sobre direcciones IP, incluyendo detalles del dispositivo como fabricante y modelo, puertos abiertos que indican servicios expuestos, protocolos y servicios disponibles, posibles vulnerabilidades conocidas, ubicación geográfica aproximada, información del banner que revela detalles del software y versión, así como certificados SSL/TLS en caso de HTTPS. Esta amplia variedad de datos permite comprender la infraestructura de red, evaluar la seguridad y realizar investigaciones de seguridad.

La URL de acceso está disponible en <https://www.shodan.io>

## 9.2 Análisis de datos recopilados

Después de un período de recopilación de datos adecuado, ha llegado el momento esperado de analizar la información recopilada utilizando herramientas disponibles, como las de análisis forense digital y aquellas relacionadas con la inteligencia de amenazas. No obstante, se puede comenzar con las que proporciona la propia herramienta.

### 9.2.1 Tratamiento y estudio de los datos obtenidos

Cuando se opta por implementar una solución de honeypots, es esencial reconocer la necesidad de asignar personal dedicado exclusivamente al mantenimiento continuo. Esta tarea implica realizar ajustes, actualizaciones y monitorización de forma regular para evitar que el honeypot se convierta en un depósito de malware o, peor aún, en un punto de apoyo para los atacantes. El mantenimiento diario es necesario para garantizar la efectividad de los honeypots y prevenir posibles brechas de seguridad que podrían comprometer la red corporativa, tanto interna como externamente.

### 9.3 Amenazas detectadas

Durante el intervalo de tiempo designado para la observación, se ha procedido con un examen detallista de los datos obtenidos a través de T-Pot, un recurso que ha resultado fundamental al emplearlo para la identificación proactiva de amenazas y la recopilación sistemática de información en este proyecto de investigación en seguridad corporativa.

Los resultados de este análisis han posibilitado la adquisición de un conocimiento más descriptivo con relación a los ataques identificados, así como a las tendencias entendidas en el comportamiento del flujo de datos en la red.

Esta evaluación ha resultado útil para aclarar el entendimiento sobre una variedad de aspectos necesarios para la comprensión de las dinámicas subyacentes en las estrategias de ataque, proporcionando una valiosa información que puede ser empleada en la mejora continua de las defensas y la formulación de políticas de seguridad más eficaces en el ámbito corporativo.

#### 9.3.1 Ataque DDoS

Los ataques DDoS [69] son del tipo distribuido y enfocados a provocar un cese del servicio atacado. Se ejecutan mediante redes de dispositivos infectados, conocidos como *botnets*, y suelen estar controlados por un atacante de forma remota. Estos dispositivos envían solicitudes al objetivo seleccionado, lo que puede saturar el servicio expuesto o incluso la red, provocando una denegación de servicio. Además, distinguir este tráfico del tráfico normal puede resultar difícil debido a que los *bots* son dispositivos legítimos de Internet, aunque una buena indicación para que sea considerado tráfico malicioso puede ser el gran volumen que se puede llegar a alcanzar en periodos breves de tiempo.

##### 9.3.1.1 Detección DDoS

El honeypot responsable de identificar y registrar este tipo de ataque masivo ha sido DDOSPot, que es una herramienta especializada en la detección de ataques de denegación de servicio distribuido (DDoS), lo que lo convierte en el recurso idóneo para monitorizar y defenderse contra este tipo de amenazas.

**Puerto 53/udp.** Se ha observado un patrón consistente de ataques dirigidos al puerto UDP 53, utilizados comúnmente para el servicio de resolución de nombres de dominio o DNS (Domain Name System). Estos ataques se caracterizan por su naturaleza masiva, con un volumen significativo de tráfico generado desde múltiples direcciones IP e incluso diversas ubicaciones geográficas.

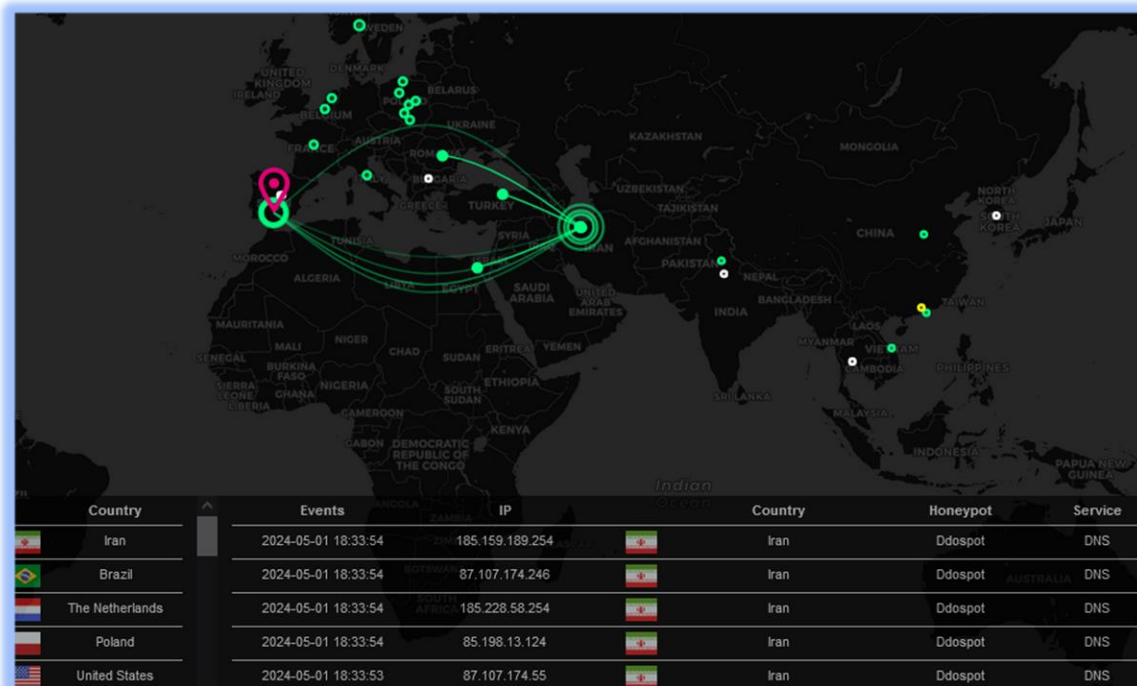


Ilustración 20 - detección ataque DDoS DNS

La velocidad de los ataques ha alcanzado niveles altos, con picos d más de **180 Mbits** por segundo en determinados momentos. Esta actividad indica un intento deliberado de saturar el servicio DNS y potencialmente interrumpir la conectividad de red.

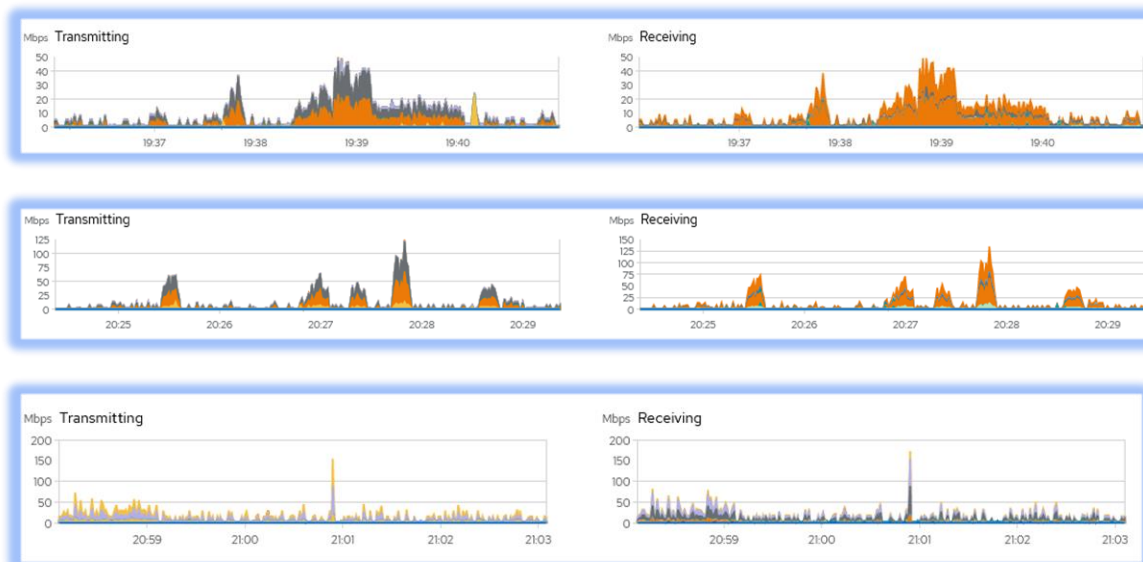


Ilustración 21 - volumen ataque DDoS DNS

**Solicitudes TCP al Puerto 123.** También se han detectado solicitudes a este puerto, utilizado por el protocolo Network Time Protocol (NTP) y que es usado para mantener sincronizados los relojes de los sistemas informáticos, ya que una suspensión de este servicio puede tener graves implicaciones en distintas áreas como la económica o de seguridad. Aunque estas solicitudes han sido menos frecuentes que las producidas en

los ataques al puerto DNS, si han sido más intensas llegando a **ráfagas preocupantes de más de 300 Mbts por segundo**.

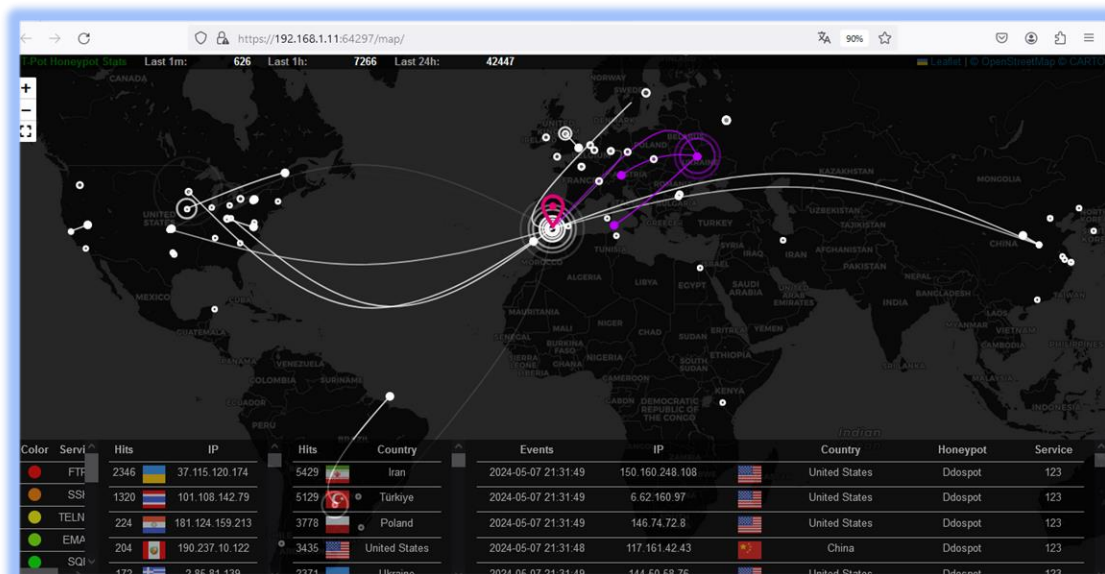


Ilustración 22 - detección ataque DDoS NTP

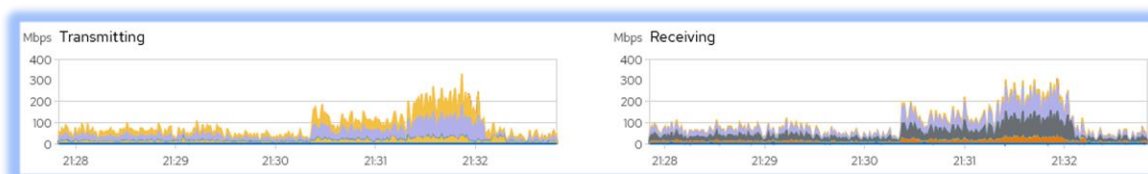


Ilustración 23 - volumen ataque DDoS NTP

Además, su presencia puede suscitar interrogantes sobre la intención y el origen de este tráfico, ya que las solicitudes UDP al puerto 123 pueden indicar intentos de escaneo de puertos o exploración de vulnerabilidades en el protocolo NTP, lo que podría representar una amenaza potencial para la integridad y la seguridad de la red corporativa.

### 9.3.1.2 Mitigación DDoS

La motivación de los atacantes para realizar ataques DDoS puede ser muy variada, como la búsqueda de extorsión a empresas solicitando pagos a cambio del cese de los ataques para permitir la continuidad de sus operaciones. Otros, simplemente actúan por motivos personales, como venganza o deseo de perjudicar la reputación de una empresa. También existen quienes ejecutan estos ataques por motivos de activismo, buscando promover causas sociales o políticas. Además, hay casos de ciberguerra o guerra digital, donde intereses gubernamentales buscan debilitar infraestructuras críticas de otras naciones. Incluso, la competencia desleal puede llevar a empresas a realizar ataques para perjudicar a sus rivales, mientras que algunos ciberdelincuentes solo buscan el reconocimiento personal o son contratados por las propias empresas para evaluar su seguridad. Estas diversas motivaciones reflejan la complejidad y diversidad de los ataques DDoS en el panorama actual de seguridad.

Para la mitigación de ataques DDoS se pueden emplear diversas estrategias como el filtrado y limitación de tráfico mediante cortafuegos; el uso de servicios de redes de contenido distribuido o CDN para distribuir el tráfico web y usar sus mecanismos de

mitigación del ataque; sistemas de balanceo de carga, detección y respuesta automatizada ante patrones maliciosos; redundancia en servidores y sistemas; limitación de la tasa de solicitud; participación en redes de mitigación de DDoS; y una monitorización constante del tráfico y rendimiento del sistema para detectar y responder rápidamente ante cualquier anomalía que pueda indicar un ataque en curso.

Para la detección de patrones de ataques DDoS, monitorización y limitación controlada de ancho de banda existen soluciones comerciales [70] en formato físico o *appliance*. Además, para fortalecer esta solución se puede complementar con la aportada por el propio operador que también suele ofrecer soluciones en primera barrera de seguridad.

#### 9.3.1.3 Inteligencia obtenida DDoS

La detección de un ataque DDoS (Distributed Denial of Service) en T-Pot puede proporcionar una variada y valiosa inteligencia de seguridad.

Por una parte, permite la identificación de vectores de ataque, determinando qué protocolos y servicios están siendo atacados en las distintas capas del modelo OSI (por ejemplo, HTTP, DNS, TCP, etc.) y comprendiendo las técnicas utilizadas por los atacantes, como amplificación [71] e inundación de solicitudes, en función de la capa de la red informática atacada.

Por otra parte, facilita el análisis de las fuentes del ataque, identificando las direcciones IP y los rangos de IP de los dispositivos involucrados, y localizando geográficamente las fuentes del ataque para entender la distribución geográfica de los atacantes.

La detección también revela patrones de comportamiento, observando patrones de tráfico anómalo, incluyendo la frecuencia, el volumen y la duración de los picos de tráfico. También permite identificar la hora del día y la duración del ataque, ofreciendo pistas sobre la planificación y ejecución del ataque.

A través del análisis, se puede perfilar a los atacantes, recopilando información sobre las herramientas y métodos utilizados, lo que ayuda a atribuir el ataque a grupos específicos de amenazas o actores maliciosos conocidos. También se puede analizar la motivación detrás del ataque, que puede variar desde extorsión hasta sabotaje o pruebas de capacidad.

Asimismo, se pueden identificar vulnerabilidades explotadas durante el ataque, determinando si se han explotado vulnerabilidades específicas en el sistema o infraestructura. Esto ayuda a evaluar la efectividad de las medidas de defensa actuales y a descubrir posibles puntos débiles que necesitan ser fortalecidos.

En términos de respuesta y mitigación, permite evaluar la efectividad de las estrategias de mitigación implementadas durante el ataque y recopilar datos para mejorar las estrategias de defensa y desarrollar mejores procedimientos de respuesta a incidentes.

#### 9.3.2 Ataque por zona geográfica

Desde el punto de vista de una organización que recibe ataques desde distintos países, es importante realizar un análisis geográfico de estos ataques, identificando los patrones y la naturaleza de las amenazas según su origen para conocer como adaptar las



estrategias de defensa, priorizar la protección contra regiones más agresivas y ajustar medidas de seguridad específicas. Así, esta comprensión mejora la capacidad de respuesta y la resiliencia general de la organización ante incidentes de seguridad.

### 9.3.2.1 Detección por zona geográfica

Numerosos ataques han sido identificados provenientes de países de los cuales puede no existir vinculación alguna. En la ilustración 24 se puede observar como un gran número de ataques proviene de la zona más oriental. Si se decide bloquear el tráfico desde la zona geográfica de Irán y China se estaría evitando ataques dirigidos desde estas zonas, además de ahorrar en ancho de banda consumido por dichos ataques.

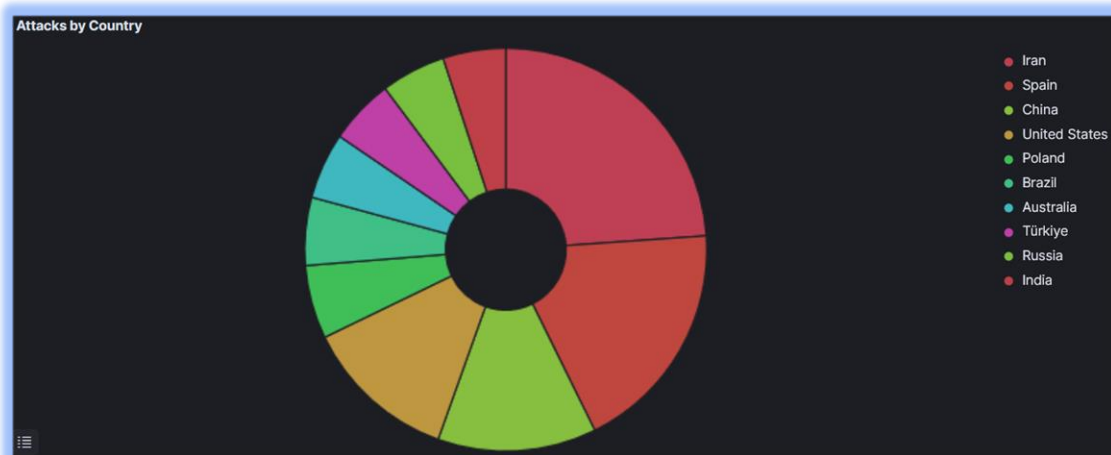


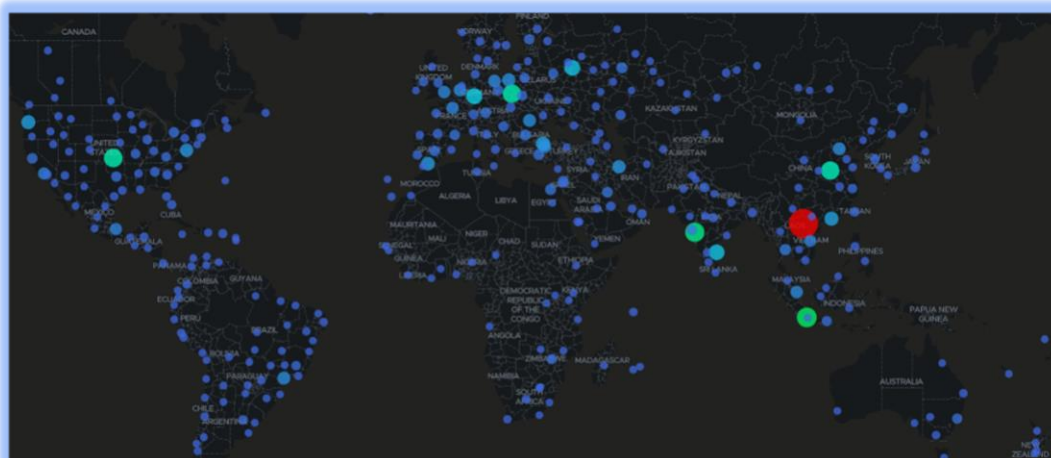
Ilustración 24 - Distribución geográfica de ataques

Visualizando el detalle de los países desde donde se reciben mayor número de ataques, se observan perfectamente en la ilustración 25 los principales países más destacados respecto al resto.

Ilustración 25 - Países con mayor actividad de ataque

### 9.3.2.2 Mitigación por zona geográfica

Una medida efectiva de mitigación en estos casos es la limitación geográfica del tráfico



de red, ya sea por geolocalización o por rangos específicos de red. De este modo, si



una empresa dirige sus servicios exclusivamente a clientes europeos, ésta puede filtrar el tráfico procedente de otras regiones mediante el uso de cortafuegos u otras soluciones de seguridad que permitan aplicar estas medidas. Incluso si no se quiere llegar a bloquear, se puede reducir el número de solicitudes permitidas de ciertos países.

Este enfoque reduce significativamente la exposición a posibles amenazas provenientes de ubicaciones geográficas no relevantes para las operaciones comerciales de la empresa.

#### 9.3.2.3 *Inteligencia obtenida Zona geográfica*

Al analizar un ataque recibido desde una zona geográfica en concreto se puede obtener información relativa al país o ciudad, así como identificar las redes (IP) y los proveedores de servicios desde los que proviene el ataque.

En este contexto, es posible identificar zonas de mayor actividad, tendencias temporales y geográficas con las que prever futuras amenazas, incluso identificar actores amenazas conocidos al relacionar la red, zona geográfica y herramientas utilizadas para elaborar las ofensivas.

#### 9.3.3 Ataques donde se reconocen IOC: Direcciones IP, dominios y puertos

Los ataques se originan desde diversas direcciones IP y hacia diversos números de puerto de comunicaciones, lo que facilita la identificación y el control de los más activos para la toma de decisiones eficaces en la mitigación de ataques dirigidos.

Estas direcciones IP pueden estar asociadas a infraestructuras de red utilizadas por APTs (Amenazas Persistentes Avanzadas), que son un conjunto de ataques informáticos sigilosos y continuos perpetrados por organizaciones criminales, empresas o estados con el objetivo de infiltrarse en sistemas objetivo mediante la explotación de vulnerabilidades o la ejecución de ataques específicos para la obtención de información sensible o tomar el control de los sistemas afectados, a menudo utilizando la instalación de malware o elementos hardware especialmente manipulados.

##### 9.3.3.1 *Detección de IOC*

Es recomendable, sanitizar los indicadores de compromiso (IOC) como direcciones IP, dominios, URLs, entre otros, para evitar el acceso accidental a los recursos maliciosos. Este proceso consiste en reemplazar los puntos con corchetes en los IOC. Por ejemplo, un dominio debería presentarse así: undominio[.]com. Esto garantiza que no se produzcan clics accidentales o accesos involuntarios a sitios potencialmente peligrosos mientras se comparten o analizan estos indicadores..

Para identificar algunos de los ataques recibidos, se aplican filtros en el panel de administración de Kibana con el fin de focalizar la atención en un conjunto de direcciones IP que puedan estar vinculadas a organizaciones maliciosas conocidas. Estos filtros se centran en el puerto destino 53, así como en la zona geográfica de Irán y las IP asociadas a alguna actividad maliciosa.

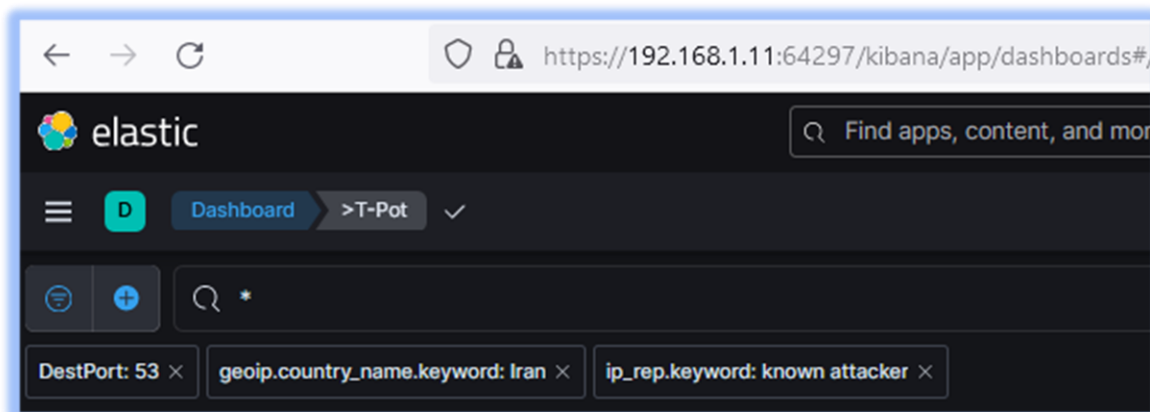


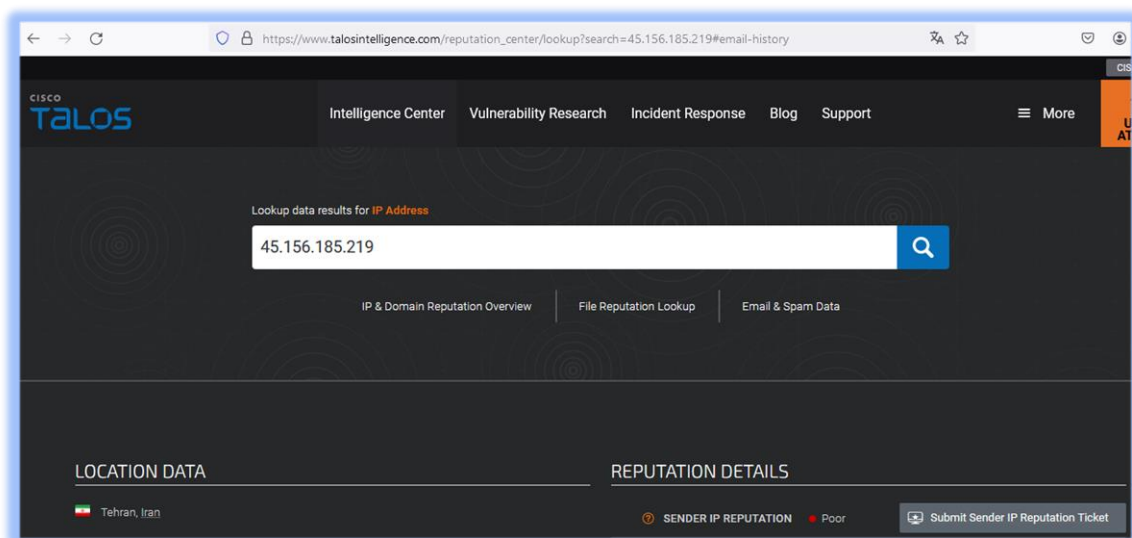
Ilustración 26 - Aplicación de filtros en Kibana

La aplicación de estos filtros permite acotar la información recopilada, centrándose en los datos relevantes que se utilizarán junto con otras herramientas OSINT, como Spiderfoot, Cisco Talos, Virustotal y UriScan, entre otras. Como resultado, se obtiene un listado de direcciones IP inicialmente consideradas como maliciosas, lo que facilita el inicio de una investigación más detallada sobre su origen y actividades:

Source IP	Count
193.151.149.70	4
193.151.145.227	3
193.151.152.95	3
45.156.185.219	3
185.221.239.121	2
193.151.151.186	2
185.221.239.103	1
185.255.91.132	1
185.255.91.197	1
193.151.130.128	1

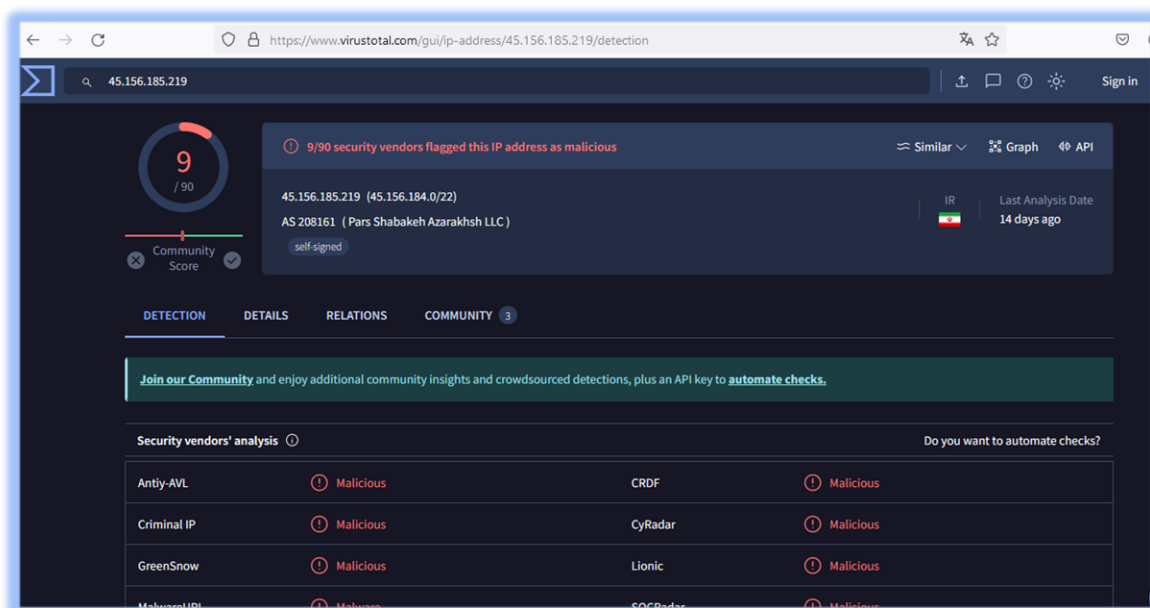
Ilustración 27 - listado IPs maliciosas

Después de llevar a cabo varias pruebas de investigación sobre las direcciones IP, comenzamos a obtener información relevante sobre su origen, actividades y posibles conexiones. En concreto, con la dirección 45.[.]156[.]185[.]219. Desde Cisco Talos se etiqueta con una reputación pobre:



Il·lustració 28 - reputación de una IP con Cisco Talos

Desde Virustotal se considera maliciosa por el análisis reciente de múltiples fabricantes conocidos, estando involucrada esta dirección IP en distribución de malware y envío de correo basura o spam:



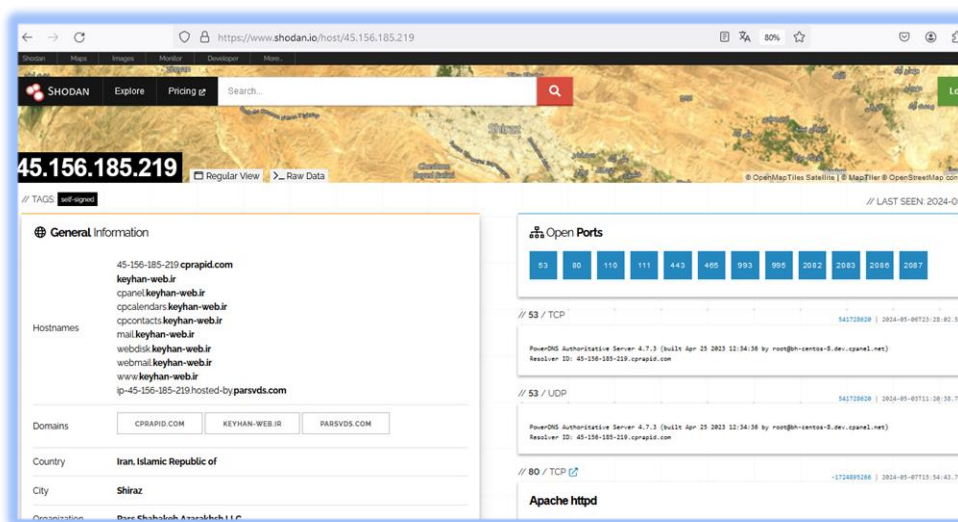
Il·lustració 29 - análisis de una IP con Virustotal

Además, según algunos de los comentarios que suele aportar la comunidad sobre investigaciones propias donde se ha relacionado el indicador evaluado, la dirección IP ha estado involucrada con ataques a servicios web configurados con *WordPress*:



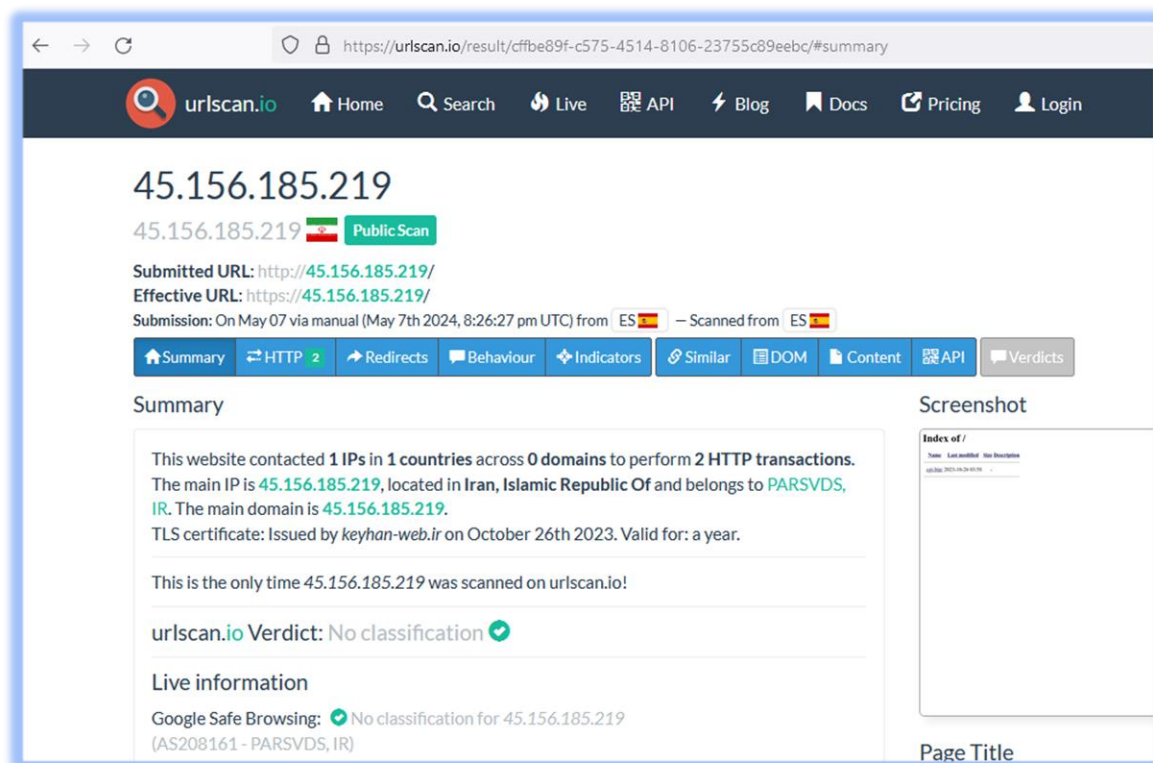
Il·lustració 30 - comentaris de la comunitat sobre indicador evaluado

Desde Shodan, la información obtenida de los puertos activos sugiere, entre otras, la presencia de un servicio de correo, un servicio web y un panel de administración típicamente asociados con negocios de alojamiento web. Al correlacionar esta información con otros datos recopilados en T-Pot, como el tipo de ataque recibido y la reputación de las direcciones IP, es posible deducir que el servidor de correo, o alguna de sus cuentas configuradas, han podido verse comprometidas para el envío de *spam*. De manera similar, el servicio web podría haber sido comprometido mediante la explotación de vulnerabilidades relacionadas con versiones obsoletas en el aplicativo, lo que facilitaría el alojamiento de malware con el fin de realizar ataques dirigidos a otros objetivos.



Il·lustració 31 - informació obtenida de una IP desde Shodan

Al ingresar una dirección IP en urlscan.io, se puede obtener información como los detalles de la solicitud HTTP, capturas de pantalla de la página web asociada, detalles del dominio y del Sistema Autónomo (ASN), recursos cargados por la página, así como metadatos y análisis de seguridad que pueden ayudar a identificar posibles amenazas como malware o phishing.



The screenshot shows the URLScan.io interface. At the top, the URL is <https://urlscan.io/result/cffbe89f-c575-4514-8106-23755c89eebc/#summary>. The main IP address is 45.156.185.219, with a 'Public Scan' badge. The submitted URL is <http://45.156.185.219/> and the effective URL is <https://45.156.185.219/>. The submission was on May 07 via manual (May 7th 2024, 8:26:27 pm UTC) from ES, scanned from ES. The interface includes navigation tabs for Summary, HTTP (2), Redirects, Behaviour, Indicators, Similar, DOM, Content, API, and Verdicts. The Summary section states: 'This website contacted 1 IPs in 1 countries across 0 domains to perform 2 HTTP transactions. The main IP is 45.156.185.219, located in Iran, Islamic Republic Of and belongs to PARSVDS, IR. The main domain is 45.156.185.219. TLS certificate: Issued by keyhan-web.ir on October 26th 2023. Valid for: a year. This is the only time 45.156.185.219 was scanned on urlscan.io! urlscan.io Verdict: No classification. Live information: Google Safe Browsing: No classification for 45.156.185.219 (AS208161 - PARSVDS, IR). A Screenshot section is visible on the right, showing an 'Index of /' directory listing.

Ilustración 32 - obtención de información de una IP con URLScan

El certificado asociado está activo, pero el dominio vinculado no dirige a la IP investigada. En cuanto al comportamiento de navegación, únicamente se produce una redirección a través de HTTP y HTTPS, sin mostrar otro contenido aparte de un directorio vacío denominado "cgi-bin". Esta situación puede indicar la ocultación de software malicioso o la preparación de una plataforma para llevar a cabo un ataque.

Dado que no se ha llegado a una conclusión definitiva sobre la asociación de esta IP con un grupo malicioso, se puede optar por bloquearla en las herramientas disponibles o continuar investigando para obtener más información sobre su actividad. Esto podría incluir la recopilación de URL, nombres de dominio y otros datos relacionados con actividades sospechosas, lo que permitiría una evaluación más exhaustiva de la amenaza potencial que representa esta dirección IP.

Una estrategia complementaria sería invertir el enfoque, comenzando por recopilar información sobre APTs activos actualmente y que estén vinculados [72] con la zona geográfica desde donde se originan los ataques, como APT33 y APT34. En este caso, llevar a cabo un estudio detallado de un APT proporcionaría una comprensión más profunda de sus TTP (Tácticas, Técnicas y Procedimientos) asociados, lo que podría facilitar la identificación de vínculos con los indicadores detectados en los datos recopilados con T-Pot. Esta aproximación inversa podría revelar conexiones y patrones que no se hayan evidenciado inicialmente, permitiendo así una evaluación más completa y precisa de la amenaza.

#### 9.3.3.2 Mitigación de ataques con el uso de IOCs

Esta mitigación implica una serie de estrategias diseñadas para detectar, bloquear y responder a amenazas. En primer lugar, se deben identificar y catalogar todos los IOC relevantes, como direcciones IP, dominios, URLs y hashes de archivos. Posteriormente,

se deben configurar cortafuegos y sistemas de detección y prevención de intrusiones (IDS/IPS) en base a estos IOC para bloquear el tráfico malicioso, así como implementar reglas de filtrado en servidores de correo y proxis web.

Mantener actualizadas las listas negras y blancas permite asegurar que solo se permita el acceso a direcciones confiables, mientras que la monitorización continua y el uso de herramientas para la gestión de eventos e información de seguridad (SIEM) [73] ayudan a detectar y alertar sobre actividades sospechosas. La respuesta a incidentes debe incluir la investigación y contención de amenazas, y en casos necesarios, el aislamiento de sistemas afectados para evitar la propagación.

Además, educar y concienciar al personal sobre la identificación y manejo seguro de IOCs fortalece la postura de seguridad interna. Incluso, colaborar con otras organizaciones y compartir información sobre IOCs a través de plataformas de inteligencia de amenazas como MISP [74] puede mejorar la seguridad colectiva y la respuesta ante amenazas.

#### 9.3.3.3 *Inteligencia con IOCs*

El análisis de los Indicadores de Compromiso (IOCs) detectados en un ataque facilita la identificación de patrones que pueden ser bloqueados en las herramientas de seguridad implementadas en la organización. Así, correlacionar esta información con datos de ataques previos permite descubrir tácticas, técnicas y procedimientos (TTP) utilizados por los atacantes. Además, compartir esta inteligencia con otras organizaciones, a través de plataformas como MISP, mejora la capacidad colectiva para identificar, prevenir y responder ante nuevos ataques.

#### 9.3.4 *Ataque con explotación de vulnerabilidades*

Los ataques que explotan vulnerabilidades publicadas en CVE (Common Vulnerabilities and Exposures) representan una de las amenazas más significativas. Estos identificadores son únicos y están asignados a vulnerabilidades conocidas en software y hardware, facilitando el intercambio de información sobre fallos de seguridad. Los atacantes aprovechan estas vulnerabilidades para comprometer sistemas, robar datos sensibles, o causar interrupciones en el servicio. La explotación dichos identificadores es particularmente peligrosa porque los detalles de la vulnerabilidad y, a menudo, el código de explotación, están públicamente disponibles, lo que permite a los atacantes desarrollar y lanzar ataques rápidamente.

##### 9.3.4.1 *Detección vulnerabilidades*

Una parte interesante del proceso implica detectar el tipo de ataque recibido y su posible conexión con un boletín de seguridad o CVE relacionado con una lista de vulnerabilidades de seguridad conocidas. Estos boletines detallan la vulnerabilidad registrada, junto con su nivel de criticidad y el impacto potencial en la triada de confidencialidad, integridad y disponibilidad de los sistemas afectados. Además, suelen incluir enlaces a la página del fabricante para ampliar la información sobre la vulnerabilidad, así como las posibles medidas correctivas o de mitigación.



El panel de administración de Kibana proporciona acceso al listado de vulnerabilidades que los actores maliciosos han intentado explotar en los honeypots configurados, cada una de ellas identificada con su respectivo CVE asignado:



CVE ID	Count
CVE-2020-11899	4,135
CVE-2012-0152	201
CVE-2001-0540	168
CVE-2002-0013 CVE-2002-0012 CVE-1999-0517	83
CVE-2002-0013 CVE-2002-0012	73
CVE-1999-0675	16
CVE-2001-0414	16
CVE-2019-11500 CVE-2019-11500	10
CVE-2020-11910	10
CAN-2001-0540	8

Ilustración 33 - listado de CVE vinculados con los intentos de explotación de vulnerabilidades

#### 9.3.4.2 Mitigación vulnerabilidades

La gestión proactiva de parches y la actualización constante de sistemas son esenciales para protegerse contra estas amenazas. Sin embargo, si se detecta una vulnerabilidad publicada en un CVE que figura en el listado de detección de Kibana, es imperativo aplicar las medidas de mitigación recomendadas publicadas en el boletín CVE correspondiente. En la mayoría de los casos, una actualización de seguridad proporcionada por el fabricante y/o un ajuste en la configuración activa pueden ser suficientes para cerrar la brecha de seguridad. Además, es importante realizar un análisis exhaustivo del impacto potencial de la vulnerabilidad en el entorno específico de la organización y tomar medidas adicionales según sea necesario, como la implementación de controles de acceso adicionales o la aplicación de reglas de cortafuegos específicas para bloquear el tráfico malicioso asociado con la explotación de la vulnerabilidad.

El último paso en la mitigación de una vulnerabilidad es realizar un nuevo escaneo para verificar que la mitigación ha sido efectiva y que la vulnerabilidad ya no puede ser explotada. Este paso permite asegurar que las medidas de seguridad implementadas



han sido exitosas y que el sistema está protegido de manera adecuada contra futuros ataques relacionados.

### 9.3.5 Inteligencia sobre explotación de vulnerabilidades

Cuando se detecta intentos o explotación de vulnerabilidades se pueden identificar su criticidad, priorizando su parcheo y gestionando mejor los riesgos, pues no es lo mismo un servicio vulnerable expuesto a internet que otro que sea exclusivamente de uso interno. Además, se revelan patrones de ataque, como las tácticas y herramientas utilizadas por los atacantes, y los vectores de entrada más comunes, lo que ayuda a fortalecer las defensas como en casos anteriores. También facilita la atribución, construyendo perfiles de los atacantes en cuanto a su sofisticación y motivaciones, y vinculando sus actividades a grupos de amenaza específicos mediante la comparación de técnicas y herramientas.

### 9.3.6 Ataques a servicios no usados

Si se presentan servicios activos pero no utilizados puede sumar un riesgo significativo para la seguridad de una red o sistema, ya que estos servicios pueden actuar como puntos de entrada potenciales para atacantes, incluso si no se utilizan activamente por los usuarios legítimos. Los servicios no utilizados pueden contener vulnerabilidades desconocidas o sin parchear que podrían ser explotadas por actores maliciosos, aumentando la superficie de ataque y la complejidad de la gestión de la seguridad, requiriendo recursos adicionales en la monitorización y mantenimiento. De este modo, es necesario la identificación y desactivación de cualquier servicio que no sea necesario para reducir el riesgo de exposición a amenazas.

#### 9.3.6.1 Detección de servicios sin uso

Un aspecto fundamental es identificar el tipo de protocolo que está siendo atacado y determinar si realmente debería estar expuesto o activo. Desde el panel de Kibana se muestran los puertos que se detectan y que están asociados a protocolos en funcionamiento:



Ilustración 34 - Puertos expuestos más atacados por País

### 9.3.6.2 Mitigación de servicios no usados

La forma más razonable y efectiva pasa por mitigar el ataque con la desactivación o filtrado de estos servicios detectados, a través de las herramientas de seguridad como cortafuegos de red o web. Esta medida ayuda directamente a reducir la superficie de ataque y a fortalecer la seguridad de la infraestructura.

### 9.3.6.3 Inteligencia sobre servicios no usados

El análisis de servicios no utilizados y expuestos identifica y reduce riesgos al desactivar puntos de entrada vulnerables, detecta y gestiona vulnerabilidades en servicios desactualizados, y asegura el cumplimiento de políticas de seguridad y normativa corporativa.

## 10 Evaluación de eficacia y generación de informes

- Evaluar la efectividad de T-Pot en la detección y respuesta ante amenazas de seguridad
- Generar informes detallados que incluyan hallazgos, recomendaciones y lecciones aprendidas

## 11 Opiniones finales

### 11.1 Resultado y conclusión

Para valorar los resultados es necesario concebir que este trabajo se propone para establecer unos cimientos firmes que faciliten la comprensión del concepto de inteligencia de amenazas, explorando los fundamentos de la seguridad informática y centrándose específicamente en la herramienta T-Pot para detectar y/o desviar los ataques de actores maliciosos.

Durante la lectura, es imperativo que se comprenda que esta herramienta está diseñada para recopilar datos, pero su efectividad depende de una organización adecuada de éstos para transformarlos en información significativa. Asimismo, es fundamental contextualizar esta información para convertirla en inteligencia aplicable a una solución global de seguridad corporativa que la haga más resiliente.

Se ha buscado una introducción a la historia de los honeypots y su evolución, y como se han ido adaptando para formar parte de las soluciones de seguridad actuales, trabajando en conjunto con otras herramientas de seguridad, y sin que sean necesariamente excluyentes.

Con una base sólida referente a ciberseguridad, se debe comprender mejor el objetivo del uso de la herramienta T-Pot, así como las bondades de su implementación en un entorno empresarial, alineando estrategia de seguridad y negocio.

Sin embargo, este trabajo a cubierto un amplio espectro de la seguridad corporativa, llegando a ser demasiado ambicioso y, por ende, con mucho contenido que puede percibirse como incompleto, aun siendo de gran extensión por todos los apartados que se han querido incluir, considerándolos necesarios para alcanzar el objetivo principal del trabajo. No obstante, también han quedado algunos apartados excluidos como los informes, evaluación de la eficacia y análisis de malware, entre otros. De otra forma, la

extensión se hubiese ampliado en unas cuantas decenas de páginas más, así como su complejidad.

Para finalizar, cabe destacar el análisis de malware como una parte integral de la seguridad, pero que se ha decidido no incluir en el proyecto por demandar un nivel de conocimiento y experiencia que se puede equiparar a un trabajo de fin de máster, y que no se había percibido en primera instancia.

## 11.2 Trabajos futuros

- Iterar sobre la implementación y configuración de los honeypots y T-Pot según los resultados de la evaluación
- Implementar mejoras y ajustes necesarios para fortalecer la postura de seguridad de la organización
- Instalación distribuida de T-Pot que implica configurar al menos dos hosts
  - T-Pot HIVE, que albergará las herramientas Elastic Stack y T-Pot y que se debe instalar en primer lugar
  - T-Pot HIVE\_SENSOR, que será responsable de alojar los honeypots en cada segmento de red a evaluar y enviar datos de registro al Elastic Stack del HIVE principal
- Implantación e integración con un sistema de gestión de eventos e información de seguridad (SIEM)
- Implantación e integración de una herramienta de inteligencia de amenazas como el proyecto de código abierto MISP
- Captura de malware para su análisis y estudio

## 12 BIBLIOGRAFÍA Y REFERENCIAS CONSULTADAS

- [1] Instituto Nacional de Ciberseguridad. La «otra manera» de identificar malware. Lugar de publicación: web incibe; año de publicación 2014; consultado el 04 abril 2024. Disponible en: <https://www.incibe.es/incibe-cert/blog/indicadores-de-compromiso>
- [2] Seguridad para Empresas. Threat Hunting: la práctica de detectar amenazas ocultas en nuestra red. Lugar de publicación: web welivesecurity; año de publicación 2021; consultado el 04 abril 2024. Disponible en <https://www.welivesecurity.com/la-es/2021/08/24/threat-hunting-que-es-practica-detectar-amenazas-ocultas-la-red>
- [3] Ciberseguridad. Qué es el Marco MITRE ATT&CK y cómo implementarlo. Lugar de publicación: web ciberseguridad; año de publicación 2024; consultado el 04 abril 2024. Disponible en <https://ciberseguridad.com/herramientas/marco-mitre-att-ck>
- [4] VirtualBox. Welcome to VirtualBox.org!. Lugar de publicación: web VirtualBox; año de publicación 2023; consultado el 07 abril 2024. Disponible en: <https://www.virtualbox.org/wiki/WikiStart>
- [5] VMware. VMware Desktop Hypervisors. Lugar de publicación: web VMware; año de publicación 2024; consultado el 07 abril 2024. Disponible en: <https://www.vmware.com/products/desktop-hypervisor.html>
- [6] Joshi RC, Sardana Anjali. Honeypot : a new paradigm to information security / R.C. Joshi, Anjali Sardana. Enfield, N.H: Science Publishers; 2011. p. 6-8
- [7] Spitzner Lance. Honeypots : tracking hackers / Lance Spitzner. 1st edition. Boston: Addison-Wesley; 2002. p. 1-10
- [8] Kluepfel HM. In search of the cuckoo's nest (computer security). In: Proceedings 25th Annual 1991 IEEE International Carnahan Conference on Security Technology. IEEE; 1991. p. 181–91.
- [9] Cheswick WR, Rubin AD, Bellovin SM. Firewalls and Internet Security: Repelling the Wily Hacker. 2nd ed. Place of publication not identified: Addison Wesley Professional; 2003. Ch. 16
- [10] Provos N, Holz T. Virtual honeypots : from botnet tracking to intrusion detection. 1st edition. Place of publication not identified: Addison Wesley; 2008. Charter 3-sec 2
- [11] Baker AR, Caswell Brian, Poor Mike, Beale Jay. Snort 2.1 intrusion detection Andrew R. Baker, Brian Caswell, Mike Poor ; foreword by Stephen Northcutt ; with Raven Alder ... [et al.]. 2nd ed. Rockland, MA: SyngressPub; 2004. p 53-56.
- [12] Spitzner Lance. Honeypots : tracking hackers / Lance Spitzner. 1st edition. Boston: Addison-Wesley; 2002. Chapter: How I Got Started with Honeypots

- [13] Spitzner Lance. Honeypots : tracking hackers / Lance Spitzner. 1st edition. Boston: Addison-Wesley; 2002. Chapter: The History of Honeypots
- [14] Spitzner Lance. Honeypots : tracking hackers / Lance Spitzner. 1st edition. Boston: Addison-Wesley; 2002. Chapter: Foreword, Giving the Hackers a Kick Where It Hurts
- [15] Spitzner Lance. Honeypots : tracking hackers / Lance Spitzner. 1st edition. Boston: Addison-Wesley; 2002. Chapter 16. Future of Honeypots
- [16] Panda Security. Honeypot [Internet]. Web Pandasecurity.com: Pandasecurity; Consultado el 24 marzo 2024. Disponible en: <https://www.pandasecurity.com/es/security-info/honeypot>
- [17] Incibe. Honeypot, una herramienta para conocer al enemigo [Internet]. Lugar de publicación: Incibe; año de publicación 2018; consultado el 24 marzo 2024. Disponible en: <https://www.incibe.es/incibe-cert/blog/honeypot-herramienta-conocer-al-enemigo>
- [18] GlobalTechnology. Averigua como te pueden atacar [Internet]. Lugar de publicación: web globalTechnology; año de publicación 2023; consultado el 24 marzo 2024. Disponible en: <https://globalt4e.com/honeypot-averigua-como-te-pueden-atacar>
- [19] Globatika Lab. Informática forense y honeypot [Internet]. Lugar de publicación: web peritosinformaticos.es; consultado el 24 marzo 2024. Disponible en: <https://peritosinformaticos.es/informatica-forense-y-honeypot>
- [20] Imagar. Qué es y cómo ayuda a la ciberseguridad de tu empresa [Internet]. Lugar de publicación: web imagar.com; publicado en febrero 2023; consultado el 25 marzo 2024. Disponible en: <https://www.imagar.com/blog-desarrollo-web/honeypot-como-ayuda-ciberseguridad-empresa>
- [21] Mohammed M, Rehman H ur. Honeypots and routers : collecting internet attacks / Mohssen Mohammed, Habib-ur Rehman. Boca Raton ; CRC Press; 2016. p. 100-102.
- [22] Mohammed M, Rehman H ur. Honeypots and routers : collecting internet attacks / Mohssen Mohammed, Habib-ur Rehman. Boca Raton ; CRC Press; 2016. p. 102-103.
- [23] Spitzner Lance. Honeypots : tracking hackers / Lance Spitzner. 1st edition. Boston: Addison-Wesley; 2002. Chapter: Disadvantages of Honeypots
- [24] Shi L, Li Y, Feng H. Performance analysis of honeypot with Petri nets. Information (Basel). 2018;9(10):245-.
- [25] Incibe. Honeypot, una herramienta para conocer al enemigo [Internet]. Lugar de publicación: Incibe; año de publicación 2019; consultado el 31 marzo 2024. Disponible en: [https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe-cert\\_guia\\_implantacion\\_honeypot\\_industrial.pdf](https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe-cert_guia_implantacion_honeypot_industrial.pdf)

- [26] Smith JE, Nair R. Virtual Machines: Versatile Platforms for Systems and Processes. 1st ed. San Diego, CA, USA: Elsevier Science; 2005. Chapter 1: Introduction to Virtual Machines.
- [27] Isavel. Virtualización. Lugar de publicación: web isavel; año de publicación 2024; consultado el 02 abril 2024. Disponible en: <https://isavelcloud.com/virtualizacion>
- [28] Pathan ASK, editor. The state of the art in intrusion prevention and detection / edited by Al-Sakib Khan Pathan. 1st edition. Boca Raton, [Florida: CRC Press/Taylor & Francis Group; 2014. Chapter 1-10.
- [29] Check Point. What is Lateral Movement? [Internet]. Lugar de publicación: web checkpoint; año de publicación 2024; consultado el 02 abril 2024. Disponible en: <https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-lateral-movement>
- [30] The Honeynet Project. HN/P [Internet]. Lugar de publicación: web honeynet project; año de publicación 2024; consultado el 04 abril 2024. Disponible en: <https://www.honeynet.org>
- [31] The Honeynet Project. Papers. Lugar de publicación: web honeynet project; año de publicación 1999-2024; consultado el 04 abril 2024. Disponible en: <https://www.honeynet.org/papers>
- [32] Amazon. Books . Lugar de publicación: web Amazon; año de publicación 2024; consultado el 04 abril 2024. Disponible en: <https://www.amazon.com/Know-Your-Enemy-Revealing-Community/dp/0201746131>
- [33] Spitzner Lance. Honeypots : tracking hackers / Lance Spitzner. 1st edition. Boston: Addison-Wesley; 2002. Chapter 10
- [34] Wikipedia. Modelo OSI . Lugar de publicación: web de Wikipedia; año de publicación 2024; consultado el 04 abril 2024. Disponible en: [https://es.wikipedia.org/wiki/Puerta\\_de\\_enlace](https://es.wikipedia.org/wiki/Puerta_de_enlace)
- [35] R. Gautam, S. Kumar and J. Bhattacharya, "Optimized virtual honeynet with implementation of host machine as honeywall," 2015 Annual IEEE India Conference (INDICON), New Delhi, India, 2015, pp. 1-6, doi: 10.1109/INDICON.2015.7443696.
- [36] The honeynet project. Sebek homepage . Lugar de publicación: web The honeynet project; año de publicación 2006; consultado el 04 abril 2024. Disponible en: <https://honeynet.onofri.org/tools/sebek>
- [37] Virtualbox. Welcome to VirtualBox.org!. Lugar de publicación: web virtualbox; año de publicación 2023; consultado el 07 abril 2024. Disponible en: <https://www.virtualbox.org/wiki/WikiStart>
- [38] Proxmox. Proxmox Virtual Environment. Lugar de publicación: web proxmox; año de publicación 2024; consultado el 07 abril 2024. Disponible en: <https://www.proxmox.com/en/proxmox-virtual-environment/overview>

- [39] VMWare. What is a hypervisor?. Lugar de publicación: web vmware; año de publicación 2024; consultado el 07 abril 2024. Disponible en: <https://www.vmware.com/topics/glossary/content/hypervisor.html>
- [40] Introducción a los honeypots » Hacking Lethani. Lugar de publicación: web Hacking Lethani; año de publicación 2018; consultado el 08 abril 2024. Disponible en: <https://hackinglethani.com/es/honeypots>
- [41] Telekom Security. About. Lugar de publicación: web Telekom Security; año de publicación 2022; consultado el 08 abril 2024. Disponible en: <https://telesec.de/en/about-telekom-security>
- [42] Wikipedia. Transmission Control Protocol. Lugar de publicación: web de Wikipedia; año de publicación 2024; consultado el 08 abril 2024. Disponible en: [https://en.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol)
- [43] Wikipedia. User Datagram Protocol. Lugar de publicación: web de Wikipedia; año de publicación 2024; consultado el 08 abril 2024. Disponible en: [https://en.wikipedia.org/wiki/User\\_Datagram\\_Protocol](https://en.wikipedia.org/wiki/User_Datagram_Protocol)
- [44] Honeypot: Instalación y uso de T-Pot18.11. Lugar de publicación: web programmerclick; año de publicación 2018; consultado el 08 abril 2024. Disponible en: <https://programmerclick.com/article/9544414597>
- [45] WeLiveSecurity. Qué es un honeypot y cómo implementarlo en nuestra red. Lugar de publicación: web WeLiveSecurity; año de publicación 2020; consultado el 08 abril 2024. Disponible en: <https://www.welivesecurity.com/la-es/2020/07/31/que-es-honeypot-como-implementarlo-nuestra-red>
- [46] Waidroc. Implementación de un Honeypot con T-Pot. Lugar de publicación: web Waidroc; año de publicación 2023; consultado el 08 abril 2024. Disponible en: <https://waidroc.github.io/posts/TPot>
- [47] ] Github. KimiNewt/pyshark. Lugar de publicación: Repositorio pyshark/README.md; año de publicación 2023; consultado el 08 abril 2024. Disponible en: <https://pypi.org/project/pyshark>
- [48] Esed. Qué es un honeypot en ciberseguridad: ventajas para las empresas. Lugar de publicación: web Esed; año de publicación 2024; consultado el 08 abril 2024. Disponible en: <https://www.esedsl.com/blog/que-es-un-honeypot>
- [49] Github. T-Pot - The All In One Multi Honeypot Platform. Lugar de publicación: Repositorio Telekom-security/tpotce readme; año de publicación 2024; consultado el 08 abril 2024. Disponible en: <https://github.com/telekom-security/tpotce/blob/master/README.md>
- [50] Computer World. Las empresas españolas suspenden en ciberseguridad: solo el 7% tienen un nivel de preparación maduro. Lugar de publicación: web Computer World; año de publicación 2024; consultado el 09 abril 2024. Disponible en:



<https://cso.computerworld.es/tendencias/solo-un-2-de-las-empresas-espanolas-tiene-una-ciberseguridad-madura-aunque-el-74-cree-tenerla>

[51] Cyber Security News. El 52% de los directivos españoles subestiman la importancia de la ciberseguridad en el éxito empresarial. Lugar de publicación: web Cyber Security News; año de publicación 2023; consultado el 09 abril 2024. Disponible en: <https://cybersecuritynews.es/el-52-de-los-directivos-espanoles-subestiman-la-importancia-de-la-ciberseguridad-en-el-exito-empresarial>

[52] IT Digital Security. Los riesgos de seguridad relacionados con el trabajo remoto siguen sin abordarse. Lugar de publicación: web ITdigitalsecurity; año de publicación 2023; consultado el 09 abril 2024. Disponible en: <https://www.itdigitalsecurity.es/endpoint/2023/04/los-riesgos-de-seguridad-relacionados-con-el-trabajo-remoto-siguen-sin-abordarse>

[53] Netapp. ¿Qué son los contenedores?. Lugar de publicación: web Netapp; año de publicación 2024; consultado el 16 abril 2024. Disponible en: <https://www.netapp.com/es/devops-solutions/what-are-containers>

[54] Debian. Razones para escoger Debian. Lugar de publicación: web Debian; año de publicación 2024; consultado el 18 abril 2024. Disponible en: [https://www.debian.org/intro/why\\_debian](https://www.debian.org/intro/why_debian)

[55] Docker.Docs. Docker overview. Lugar de publicación: web Docker; año de publicación 2024; consultado el 18 abril 2024. Disponible en: <https://docs.docker.com/get-started/overview>

[56] Kubernetes. ¿Qué es Kubernetes?. Lugar de publicación: web Kubernetes; año de publicación 2022; consultado el 18 abril 2024. Disponible en: <https://kubernetes.io/es/docs/concepts/overview/what-is-kubernetes>

[57] Elastic. What is Elasticsearch?. Lugar de publicación: web Elastic; año de publicación 2024; consultado el 18 abril 2024. Disponible en: <https://www.elastic.co/guide/en/elasticsearch/reference/current/elasticsearch-intro.html>

[58] Elastic. Logstash, centraliza, transforma y almacena tus datos. Lugar de publicación: web Elastic; año de publicación 2024; consultado el 18 abril 2024. Disponible en: <https://www.elastic.co/es/logstash>

[59] Elastic. Kibana, descubre, itera y resuelve con ES|Q. Lugar de publicación: web Elastic; año de publicación 2024; consultado el 18 abril 2024. Disponible en: <https://www.elastic.co/es/kibana>

[60] Fortinet. ¿Qué es una red DMZ?. Lugar de publicación: web Fortinet; año de publicación 2024; consultado el 18 abril 2024. Disponible en: <https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz>

[61] OPNSense. About OPNSense. Lugar de publicación: web OPNSense; año de publicación 2024; consultado el 22 abril 2024. Disponible en: <https://opnsense.org/about/about-opnsense>

- [62] Docker.Docs. Docker Compose overview. Lugar de publicación: web Docker; año de publicación 2024; consultado el 29 abril 2024. Disponible en: <https://docs.docker.com/compose>
- [63] Wikipedia. Secure Shell. Lugar de publicación: web Wikipedia; año de publicación 2024; consultado el 29 abril 2024. Disponible en: [https://es.wikipedia.org/wiki/Secure\\_Shell](https://es.wikipedia.org/wiki/Secure_Shell)
- [64] Nginx. Nginx. Lugar de publicación: web Nginx; año de publicación 2024; consultado el 1 mayo 2024. Disponible en: <https://nginx.org/en>
- [65] Wikipedia. Proxy inverso. Lugar de publicación: web Wikipedia; año de publicación 2024; consultado el 1 mayo 2024. Disponible en: [https://es.wikipedia.org/wiki/Proxy\\_inverso](https://es.wikipedia.org/wiki/Proxy_inverso)
- [66] smicallef / spiderfoot. Spiderfoot. Lugar de publicación: web Github; año de publicación 2022; consultado el 5 mayo 2024. Disponible en: <https://github.com/smicallef/spiderfoot/blob/master/README.md>
- [67] telekom-security / tpotce. Credits. Lugar de publicación: web Github; año de publicación 2024; consultado el 5 mayo 2024. Disponible en: <https://github.com/telekom-security/tpotce/blob/master/README.md#credits>
- [68] Wikipedia. OSINT. Lugar de publicación: web Wikipedia; año de publicación 2024; consultado el 5 mayo 2024. Disponible en: [https://es.wikipedia.org/wiki/Inteligencia\\_de\\_fuentes\\_abiertas](https://es.wikipedia.org/wiki/Inteligencia_de_fuentes_abiertas)
- [69] Cloudflare. ¿Qué es un ataque DDoS?. Lugar de publicación: web Cloudflare; año de publicación 2024; consultado el 5 mayo 2024. Disponible en: <https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack>
- [70] Check Point. DDoS Protector de Quantum. Lugar de publicación: web Checkpoint; año de publicación 2024; consultado el 5 mayo 2024. Disponible en: <https://www.checkpoint.com/es/quantum/ddos-protector>
- [71] Akamai. ¿Qué es un ataque por amplificación de DNS?. Lugar de publicación: web Akamai; año de publicación 2024; consultado el 7 mayo 2024. Disponible en: <https://www.akamai.com/es/glossary/what-is-a-dns-amplification-attack>
- [72] Mandiant. Advanced Persistent Threats. Lugar de publicación: web Mandiant; año de publicación 2024; consultado el 7 mayo 2024. Disponible en: <https://www.mandiant.com/resources/insights/apt-groups>
- [73] IBM. ¿Qué es la SIEM?. Lugar de publicación: web IBM; año de publicación 2024; consultado el 7 mayo 2024. Disponible en: <https://www.ibm.com/es-es/topics/siem>
- [74] Misp Threat Sharing. Home. Lugar de publicación: web misp-project; año de publicación 2024; consultado el 7 mayo 2024. Disponible en: <https://www.misp-project.org>

## 13 Glosario

**Actor malicioso.** Persona u organización que realiza actividades dañinas o ilegales en un sistema informático.

**Algoritmo.** Conjunto de instrucciones para resolver un problema.

**Base de datos.** Conjunto organizado de datos almacenados electrónicamente.

**Bastionado.** Proceso de asegurar un sistema informático mediante la implementación de medidas de seguridad adicionales.

**Cortafuegos.** Sistema de seguridad de red que controla el tráfico de red basado en reglas predefinidas para permitir o bloquear la comunicación entre redes.

**Cracker.** Individuo que utiliza conocimientos y habilidades técnicas avanzadas para obtener acceso no autorizado a sistemas informáticos con fines maliciosos.

**Digitalización.** Procedimiento mediante el cual se transforma información analógica en datos digitales, facilitando su almacenamiento, modificación y transmisión a través de medios electrónicos.

**DMZ.** Zona intermedia entre la red interna y externa de una organización, utilizada para alojar servicios públicos y mejorar la seguridad de la red.

**Fingerprinting.** Proceso de identificar dispositivos, sistemas o aplicaciones mediante la recopilación y análisis de sus características únicas o "huellas digitales".

**GPL.** Licencia de software que asegura a los usuarios la libertad para utilizar, examinar, compartir y adaptar el software según sus necesidades, al ser de código abierto.

**Hacker.** Persona experta en el manejo de sistemas informáticos, capaz de encontrar y solucionar problemas complejos en sistemas de computación.

**Hardware.** Todos los componentes físicos de un sistema informático, incluyendo dispositivos como procesadores, memoria, discos duros, tarjetas de red, etc.

**Hipervisor.** Software que permite la virtualización de sistemas operativos, permitiendo se ejecuten en un mismo hardware de manera independiente.

**IDS.** Herramienta de seguridad que observa y evalúa el flujo de datos en una red o los registros de actividad en un sistema, con el propósito de detectar cualquier actividad que pueda ser considerada sospechosa o maliciosa.

**IOC.** Un indicador de Compromiso es una pista o evidencia que indica la presencia de actividad maliciosa en un sistema informático, como direcciones IP, nombres de dominio, hashes de archivos, etc.

**IPv6.** Última versión del protocolo de internet que utiliza direcciones IP de 128 bits y se diseñó para reemplazar a IPv4.

**OSI.** El modelo de interconexión de sistemas abiertos es una estructura teórica que detalla las diferentes funciones de comunicación en una red, organizadas en siete capas distintas.

**Open Source.** Software con código abierto accesible al público

**Puerta enlace.** Un dispositivo o software que conecta redes diferentes permitiendo su comunicación.

**Yara.** Reglas de detección de malware que se utilizan en herramientas de seguridad para identificar patrones específicos en archivos o memoria que podrían indicar la presencia de amenazas.

**SSD.** Dispositivo de almacenamiento que utiliza celdas de memoria.

**SSH.** Protocolo de red seguro para acceso remoto.

**TCP.** Protocolo de Internet para comunicación fiable.

**UDP.** Protocolo de Internet para comunicación rápida.

**Vlan.** Segmentación de red para mejor control y seguridad.

**Vulnerabilidades.** Debilidad en un sistema de seguridad que podría ser explotada por un atacante para comprometer la integridad, confidencialidad o disponibilidad de la información.

## 14 Anexo 1

Corresponde con la instalación guiada de OPNSense en su versión 24.1.

La descarga se realiza directamente desde la página original del proyecto, garantizando así la autenticidad y seguridad del archivo. A continuación, se proporcionan los enlaces para descargar la imagen ISO, así como su hash correspondiente. Es importante verificar el hash después de la descarga para asegurar la integridad del archivo descargado y confirmar que no ha sido alterado.

### Imagen ISO

<https://mirror.ams1.nl.leaseweb.net/opnsense/releases/24.1/OPNsense-24.1-vga-amd64.img.bz2>

### Hash

OPNsense-24.1-vga-amd64.img.bz2 (SHA256) :

ec08755245017cd449a8d174b6ea7c4e2038c454a8abecfad0d0378729d8b331

Para asegurar la integridad del archivo descargado es necesario verificar su hash. Esta verificación se realiza comparando el hash del archivo descargado con el proporcionado en la URL del repositorio. Desde PowerShell:

```
PS C:\Users\angel\Downloads> Get-FileHash .\OPNsense-24.1-dvd-amd64.iso.bz2

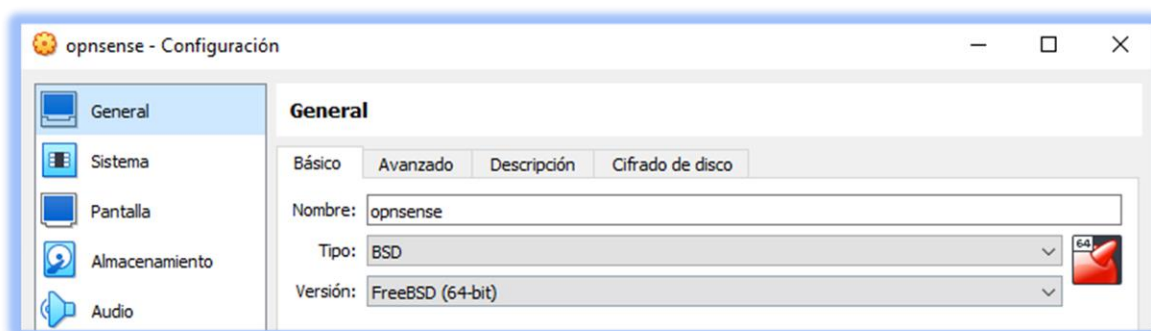
Algorithm      Hash
-----
SHA256         6D1E22713BF031D0A36A73B3820CD1564F426CAE9C67A6ADE4B7FA6518AFA2D5
```

Los requerimientos de la instalación de esta herramienta se localizan en la propia página del proyecto. Se han utilizado las recomendaciones del enlace <https://opnsense.org/users/get-started> para las características estándar:

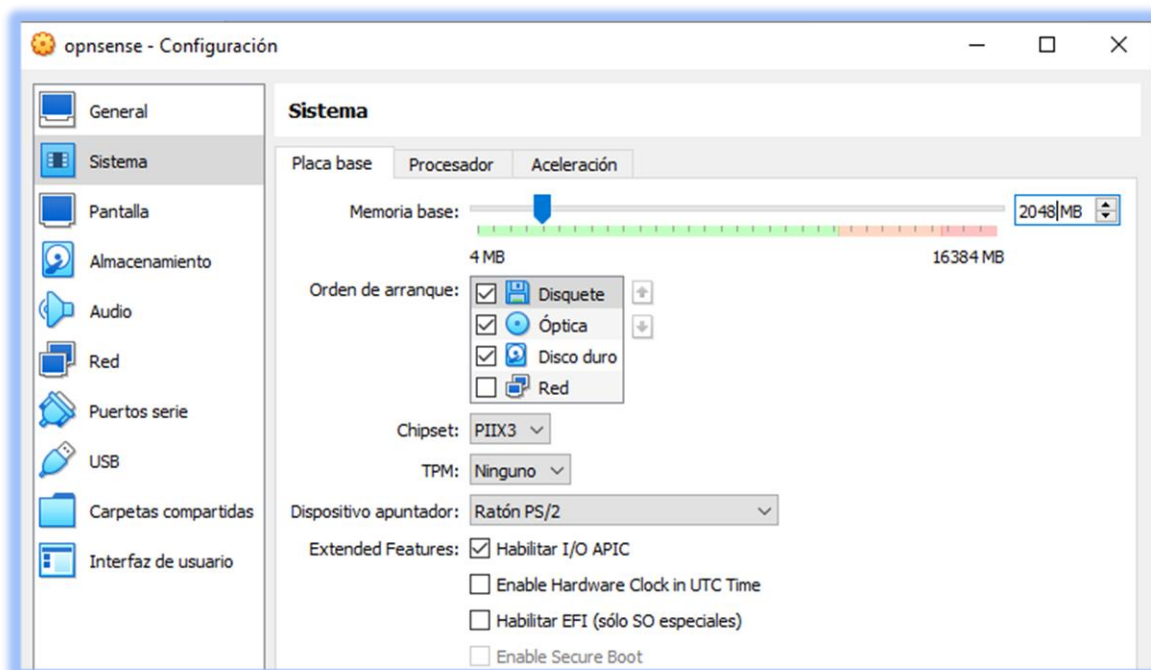
Type	Description
Processor	1 GHz dual core cpu
RAM	2 GB
Install method	Serial console or video (vga)
Install target	40 GB SSD, a minimum of 2GB memory is needed for the installer to run.

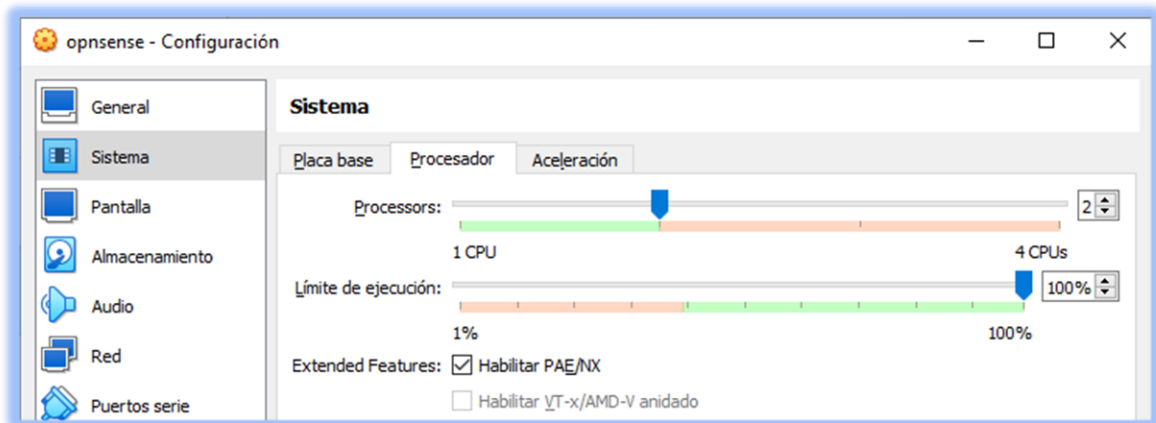
En VirtualBox se crea una nueva máquina virtual y se configura con las siguientes opciones:

### General

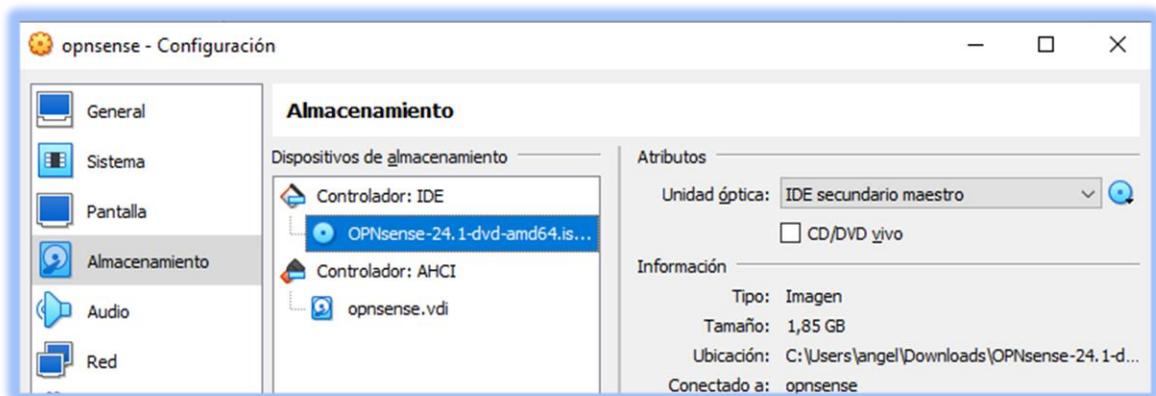


### Sistema





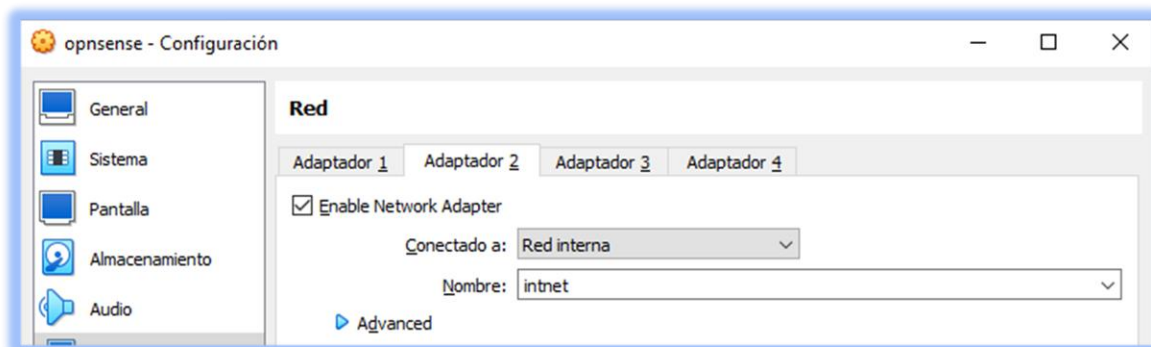
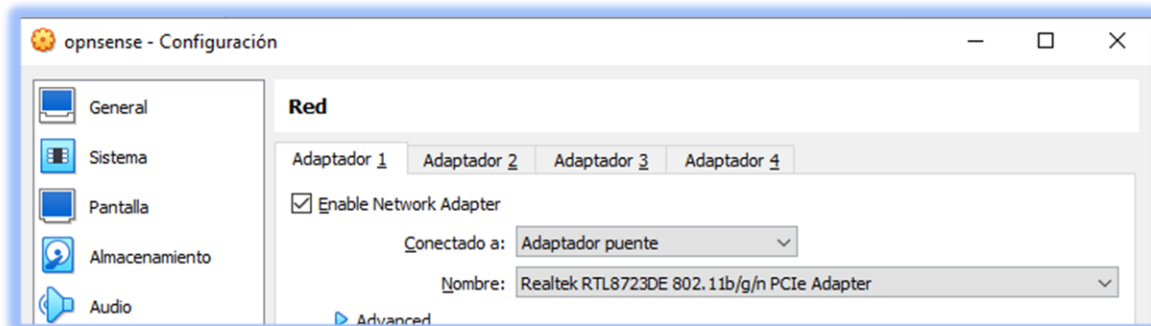
Como la instalación se va a realizar cargando la imagen ISO en el DVD virtual de la máquina, se configura de la siguiente forma el almacenamiento:



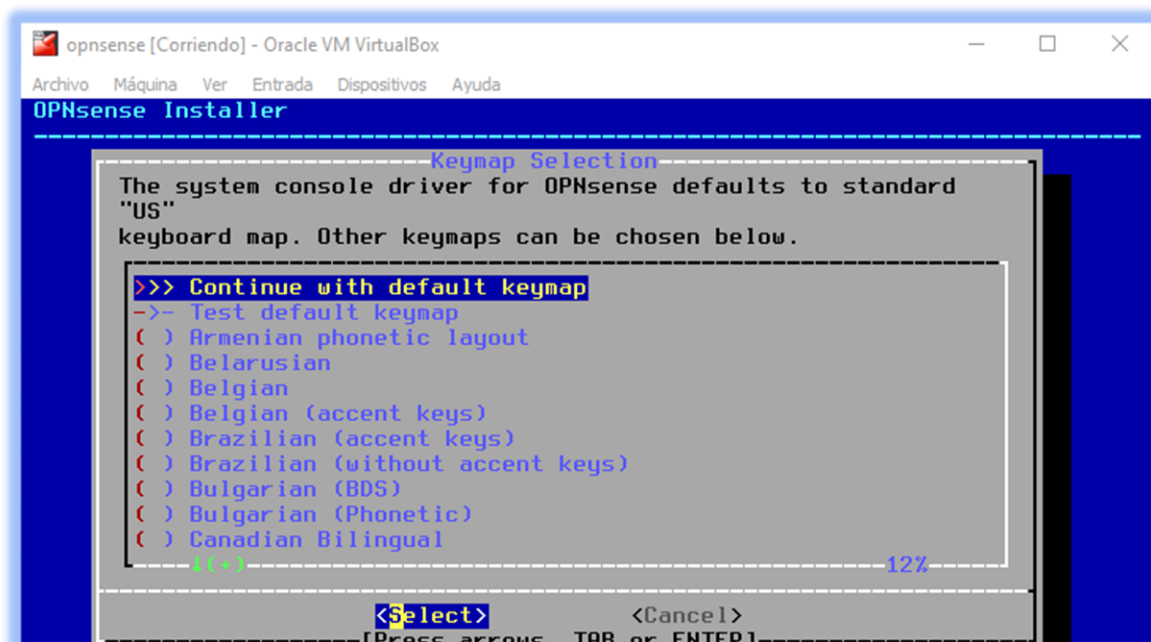
Para el entorno de red planificado se utilizan dos tarjetas de red:

- la primera configurada en modo puente para conectar con internet a través del enrutador
- la segunda para conectar con la DMZ donde está configurada la máquina con T-Pot
- por cada red que se quiera conectar se debe agregar una tarjeta de red configurada según las necesidades





- Una vez configurada la máquina para que arranque desde USB, donde estará cargada la ISO con el sistema a instalar. A los pocos segundos se inicia el entorno Live y se inicia sesión con el usuario *installer* y la contraseña *OpnSense* para continuar con la instalación.



Se siguen las instrucciones hasta completar la instalación, se extrae la imagen .iso del del dvd virtual y se reinicia la máquina virtual.

El primer adaptador se configura con WAN y con IP 192.168.1.2/24

El segundo adaptador se configura como LAN y con IP 192.168.2.2/24

El tercer adaptador se configura como SERVIDORES y con IP 192.168.3.2/24

El cuarto adaptador se configura como LAN y con IP 192.168.4.2/24

El acceso web GUI es accesible solo desde la red servidores desde la URL <https://192.168.3.2>

En Instalaciones virtuales en VirtualBox, VMware, etc, es recomendable instalar las *virtual tools* para obtener el máximo rendimiento y compatibilidad.

En un primer arranque del sistema se establecen algunas configuraciones predeterminadas que se pueden consultar en la documentación en línea accesible desde la URL <https://docs.opnsense.org>:

- **Asignaciones de puertos:** Por defecto, el sistema se configurará con 2 interfaces: LAN y WAN. El primer puerto de red encontrado se configurará como LAN y el segundo como WAN.
- **Rangos de IP y DHCP:** El puerto WAN tendrá un cliente DHCP y espera recibir una dirección IP. El puerto LAN tendrá un servidor DHCP, una IP estática de 192.168.1.1/24 y ofrecerá direcciones IP en el rango de 192.168.1.100-200.
- **Usuarios y contraseñas:** Usuario predeterminado: root / Contraseña: OpnSense.

Por razones de seguridad, SSH está deshabilitado por defecto y el acceso a la consola está protegido por contraseña.

## 15 Anexo 2

Corresponde con la instalación guiada de T-Pot en su versión 22.04.0.

La descarga se realiza directamente desde el repositorio original de GitHub del proyecto TPOTCE, garantizando así la autenticidad y seguridad del archivo. A continuación, se proporcionan los enlaces para descargar la imagen ISO, así como su hash correspondiente. Es importante verificar el hash después de la descarga para asegurar la integridad del archivo descargado y confirmar que no ha sido alterado.

## Imagen ISO

[https://github.com/telekom-security/tpotce/releases/download/22.04.0/tpot\\_amd64.iso](https://github.com/telekom-security/tpotce/releases/download/22.04.0/tpot_amd64.iso)

## Hash

[https://github.com/telekom-security/tpotce/releases/download/22.04.0/tpot\\_amd64.sha256](https://github.com/telekom-security/tpotce/releases/download/22.04.0/tpot_amd64.sha256)

Para asegurar la integridad del archivo descargado es necesario verificar su hash. Esta verificación se realiza comparando el hash del archivo descargado con el proporcionado en la URL del repositorio. Desde PowerShell:

```
PS C:\Users\resiliencia\Downloads> Get-FileHash .\tpot_amd64.iso

Algorithm      Hash
-----
SHA256         6FCEDA96994F9E0EF2A6C61BA7BFB1C8C4BF27568625770CB5488E71F91253EB

PS C:\Users\resiliencia\Downloads> cat .\tpot_amd64.sha256
6fceda96994f9e0ef2a6c61ba7bfb1c8c4bf27568625770cb5488e71f91253eb  tpot_amd64.iso
```

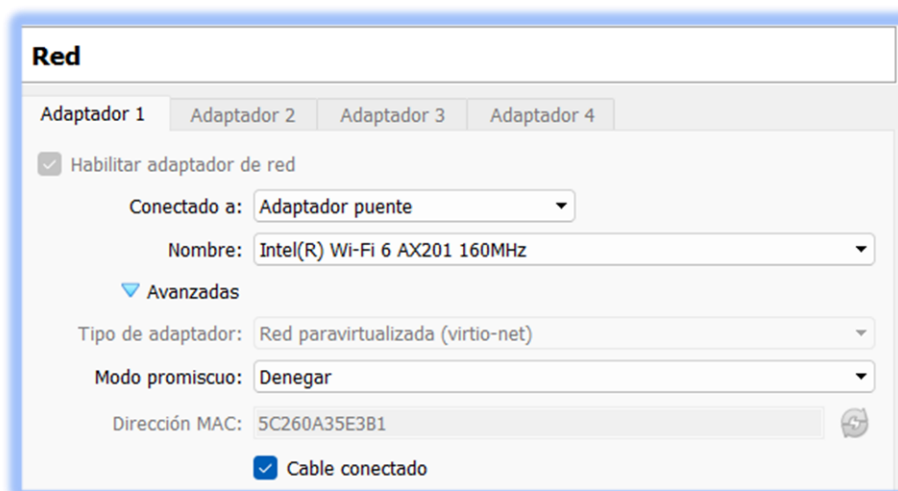
Los requerimientos de la instalación de esta herramienta se localizan en el *readme* facilitado en el mismo repositorio con URL <https://github.com/telekom-security/tpotce/blob/master/README.md> :

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.

Los requisitos de configuración para la máquina virtual destinada a la instalación de la herramienta se determinan en función de los requerimientos especificados en el análisis previo. Estos requisitos aseguran que la máquina virtual disponga de los recursos necesarios para un funcionamiento óptimo y eficiente de la herramienta:

- 4 Cores
- 8gb RAM
- 128 disco

Al no ser unos requerimientos estándar, no facilita su reconocimiento como máquina virtual. Además, se debe prestar especial atención a la configuración de red, ya que se modifica la dirección MAC para que la parte correspondiente al fabricante coincida con DELL®. Esta medida forma parte de la estrategia de ocultación de información, diseñada para dificultar la detección de la herramienta.



El uso del instalador de T-Pot es intuitivo, ya que hace de guía paso a paso a través del proceso de configuración. Una vez seleccionada la opción de instalación *STANDARD*, el instalador proporcionará todas las indicaciones necesarias para completar el proceso de forma sencilla y eficiente.

Las credenciales configuradas en los usuarios de administración y gestión son los siguientes:

Administración: tsec / fk3d-A)Uh58Ks!

Web y SSH: angelux / W9shReg3425\$)2

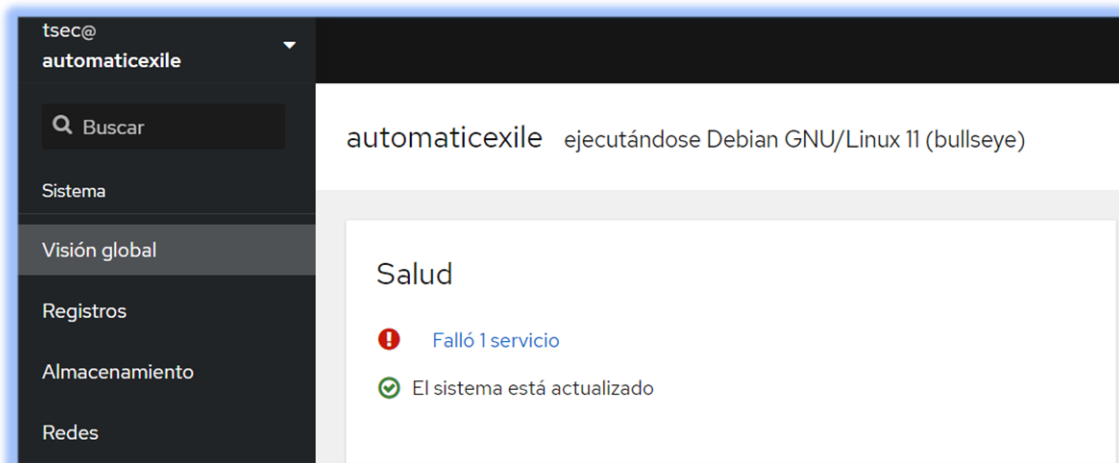
Una vez finalizada la instalación, la pantalla que queda en consola de la máquina instalada con T-Pot indica las distintas formas para iniciar sesión en la herramienta:



```
-----  
T-POT 2.5.0.0  
-----  
---- [ automaticexile ] [ Sat Apr 13 2024 ] [ 19:21:30 ]  
IP: 192.168.1.11 (37.11.180.64)  
SSH: ssh -l tsec -p 64295 192.168.1.11  
WEB: https://192.168.1.11:64297  
ADMIN: https://192.168.1.11:64294  
BLACKHOLE: [ DISABLED ]  
-----
```

Se observa que los puertos de administración asignados son superiores al 64000. Esto permite que la configuración de Traducción de Direcciones de Puerto (PAT) del enrutador hacia la IP de la máquina expuesta se limite únicamente a los puertos inferiores. Esta estrategia añade una capa adicional de protección a la máquina expuesta.

En un primer acceso la web de administración se detecta un servicio que ha quedado en error y no se puede recuperar:



Una simple consulta en la documentación oficial ha sido suficiente para obtener la solución en el siguiente enlace: <https://github.com/telekom-security/tpotce?tab=readme-ov-file#network-interface-fails>

Resumiendo la documentación consultada, la solución pasa por editar la configuración de la red en `/etc/network/interfaces`, cambiando el nombre de la tarjeta por defecto por el que corresponda del sistema:

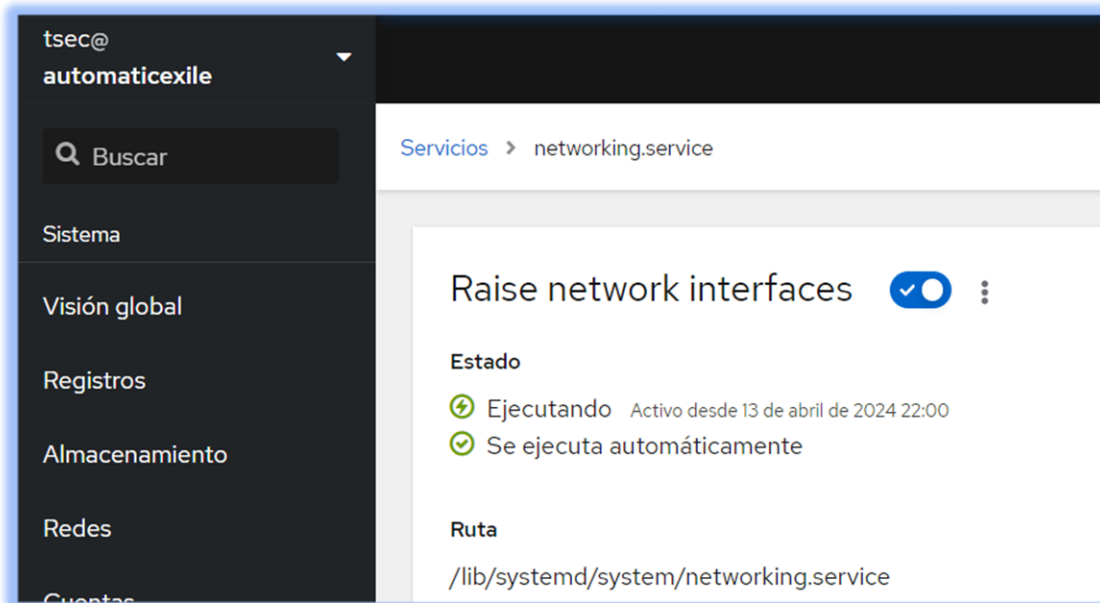
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#auto enp0s3
auto eth0
#iface enp0s3 inet dhcp
iface eth0 inet dhcp
```

Cambiada la configuración, se fuerza el inicio del servicio y, ahora sí, queda activo y sin errores registrados:



En la configuración inicial se utiliza DHCP para la configuración de red. Sin embargo esta configuración puede resultar poco práctica para el uso de esta herramienta, con lo que se considera cambiar la configuración de red para el uso de IP fija ejecutando la siguiente secuencia de comandos:

- parar T-Pot
  - `sudo systemctl stop tpot`
- ajustar la configuración de red modificando el fichero `/etc/network/interfaces` según las siguientes preferencias de red

```
tsec@automaticexile:~$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#auto enp0s3
auto eth0
#iface enp0s3 inet dhcp
iface eth0 inet dhcp

### Example static ip config
### Replace <eth0> with the name of your physical interface name
#
#auto eth0
#iface eth0 inet static
# address 192.168.1.11
# netmask 255.255.255.0
# network 192.168.1.0
# broadcast 192.168.1.255
# gateway 192.168.1.1
# dns-nameservers 192.168.1.1
```



- recargar o reiniciar la red
  - `sudo /etc/init.d/networking reload | restart`
- iniciar T-Pot
  - `sudo systemctl stop tpot`

Colocar T-Pot detrás del cortafuegos OPNSense permite reenviar todo el tráfico TCP/UDP en el rango de puertos 1 a 64000 a T-Pot. Al mismo tiempo, solo se concede acceso a los puertos superiores a 64000 desde direcciones IP confiables o se exponen únicamente los puertos necesarios para el caso de uso específico. Para capturar tráfico de malware en puertos desconocidos no se debe limitar los puertos reenviados, pues Glutton y Honeytrap asignan dinámicamente cualquier puerto TCP no utilizado por otros servicios honeypot, ofreciendo una visión más completa de los riesgos a los que está expuesta la configuración.

Para verificar desde línea de comandos si todos los servicios y honeypots se han iniciado correctamente:

- `sudo /opt/tpot/bin/dps.sh 1`