Diseño e implementación de una plataforma web de iniciación en la ciberseguridad

Antonio Javier Galán Herrera

Escuela Técnica Superior de Ingeniería Informática

29 de septiembre de 2023

Índice

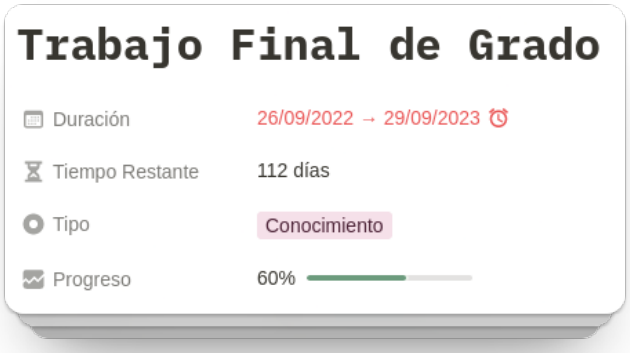
Introducción

Motivación

- Estrategia Andaluza de Ciberseguridad 2022 - 2025
- Proyecto para estudiantes, desarrollado por un estudiante
- Algo distinto a los CTFs, sin *banderas*

Metodología

- Desarrollo incremental
- *Getting Things Done*
- Gantt y Kanban



Proceso creativo

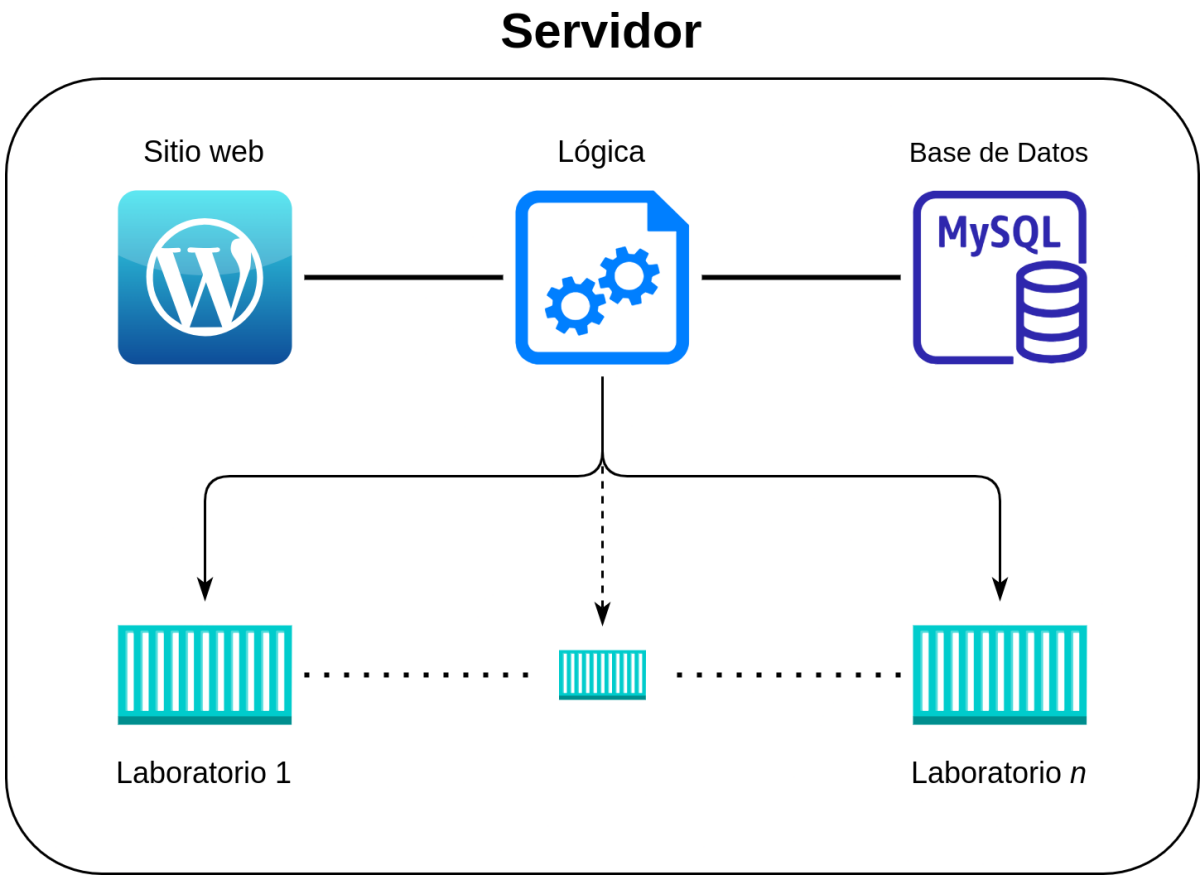
- Plataforma de CTFs
- Portal de descargas
- **Laboratorios**

Análisis de tecnologías

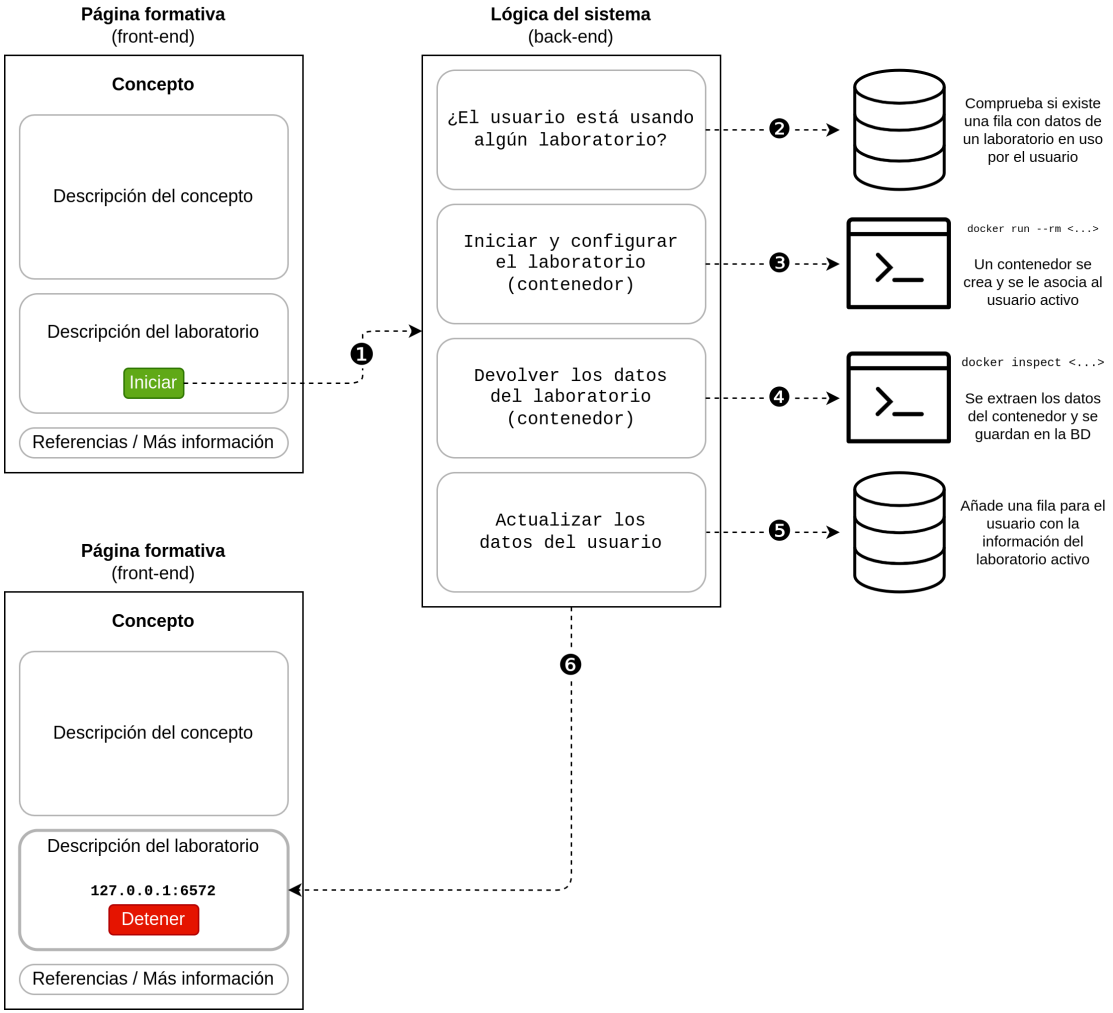
- **Sitio web**: Astro / WordPress / Drupal
- **Base de datos**: SQLite / MySQL
- **Almacenamiento**: Local / Remoto (AWS, Linode, GCP)

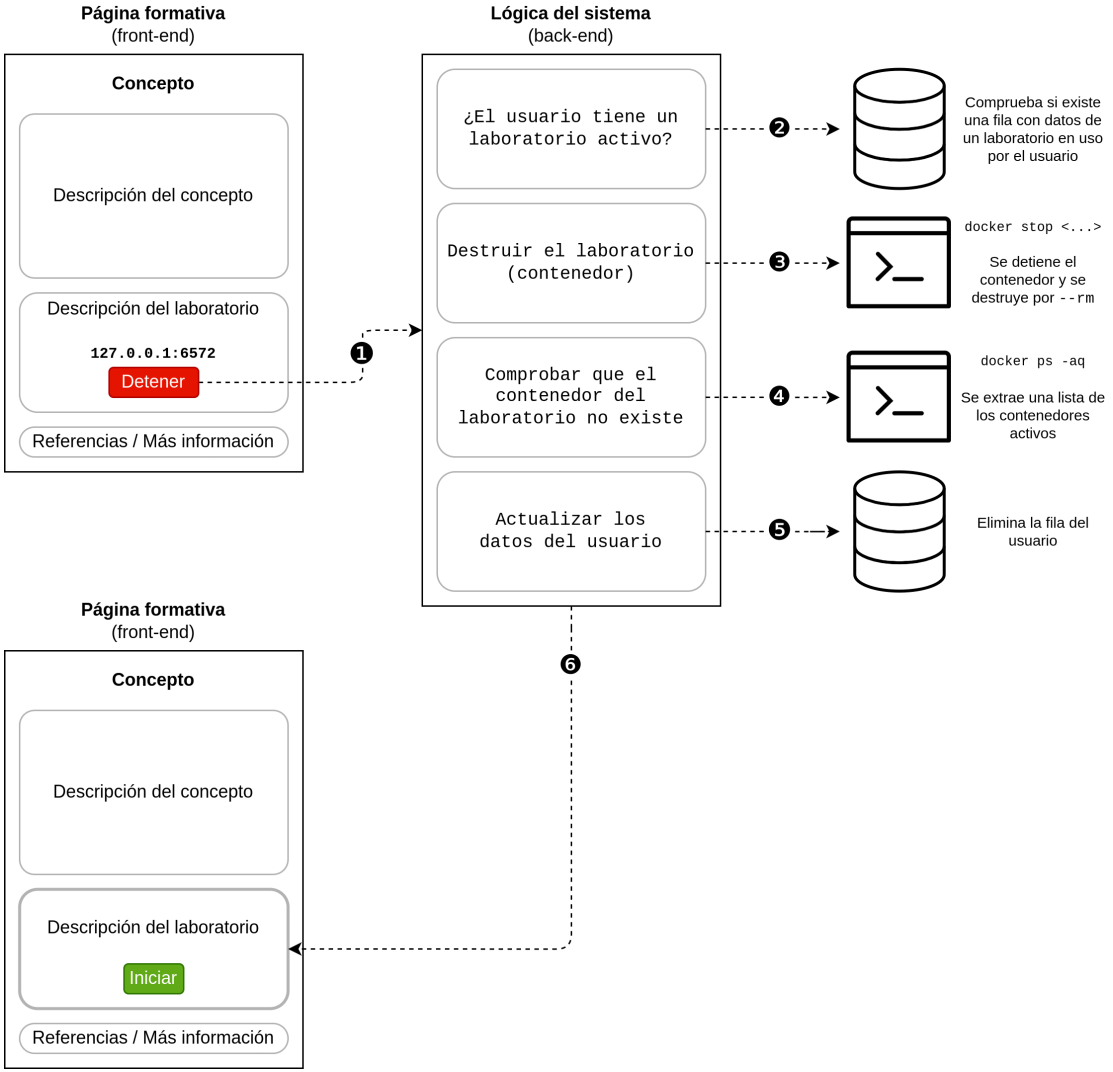
Diseño y desarrollo

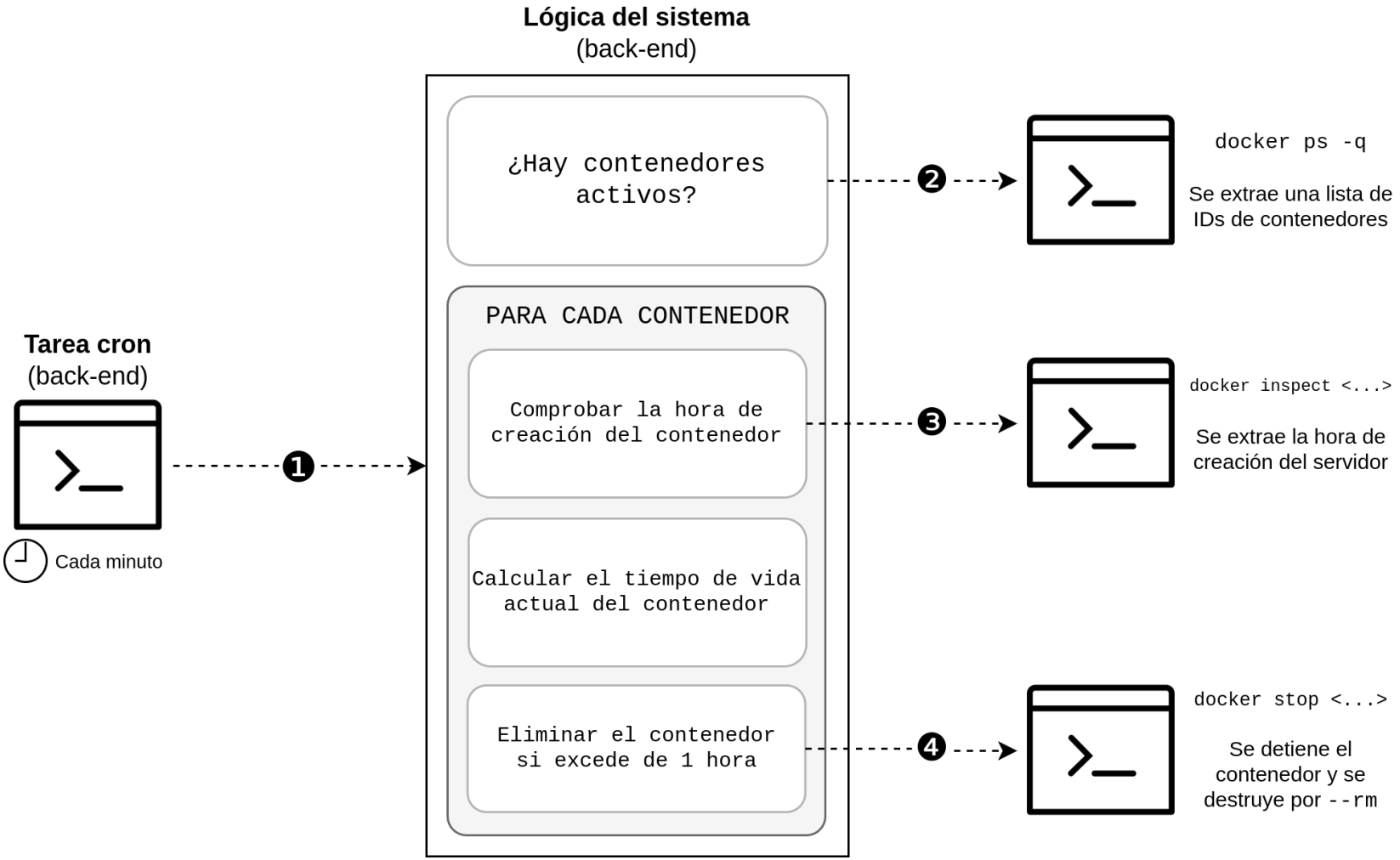
Arquitectura



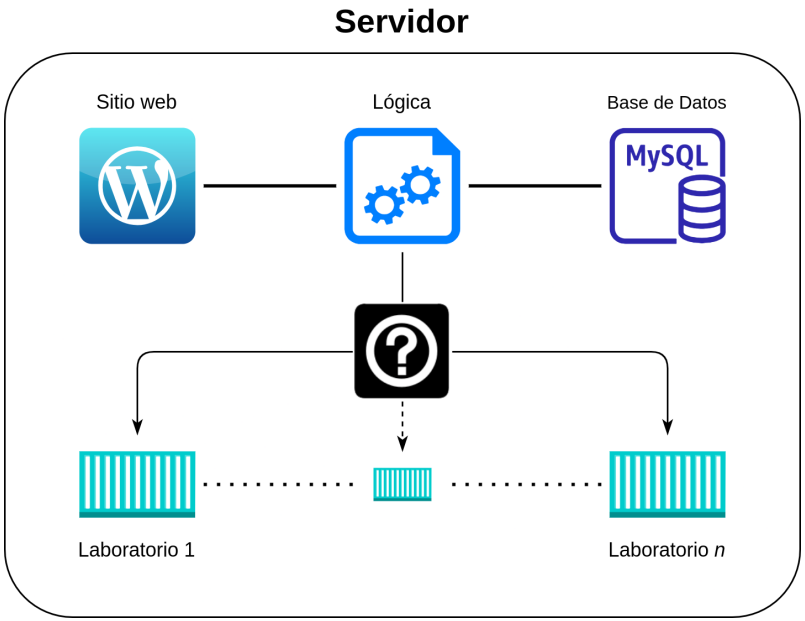
Modelado de procesos

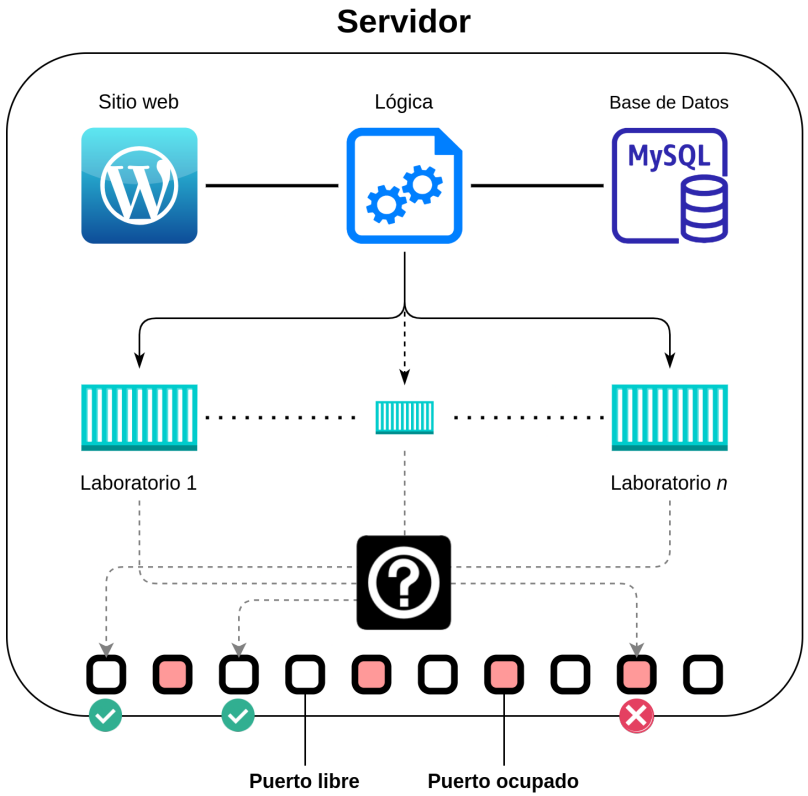



Página formativa
(front-end)
Concepto
Descripción del concepto
Descripción del laboratorio
127.0.0.1:6572
Detener
Referencias / Más información
Lógica del sistema
(back-end)
¿El usuario tiene un laboratorio activo?
Destruir el laboratorio (contenedor)
Comprobar que el contenedor del laboratorio no existe
Actualizar los datos del usuario
1
2
3
4
5
6
Comprueba si existe una fila con datos de un laboratorio en uso por el usuario
docker stop <...>
Se detiene el contenedor y se destruye por --rm
docker ps -aq
Se extrae una lista de los contenedores activos
Elimina la fila del usuario
Página formativa
(front-end)
Concepto
Descripción del concepto
Descripción del laboratorio
Iniciar
Referencias / Más información


Lógica del sistema
(back-end)
¿Hay contenedores activos?
PARA CADA CONTENEDOR
Comprobar la hora de creación del contenedor
Calcular el tiempo de vida actual del contenedor
Eliminar el contenedor si excede de 1 hora
Tarea cron
(back-end)
Cada minuto
1
2
3
4
docker ps -q
Se extrae una lista de IDs de contenedores
docker inspect <...>
Se extrae la hora de creación del servidor
docker stop <...>
Se detiene el contenedor y se destruye por --rm

Toma de decisiones





Catálogo de conceptos

Laboratorios de introducción

Linux

Jerarquía de ficheros y directorios, y gestión de usuarios y permisos.

Bash

Sintaxis básica, variables, condicionantes, bucles y funciones.

Redes

Protocolos, tipos y topologías de red, y ataques más comunes.

OSINT

Descripción y herramientas útiles de recolección de información.

Laboratorios normales

Análisis de tráfico

Captura de tráfico, paquetes y herramientas.

Esteganografía

Definición y herramientas comunes.

Fuerza bruta

Definición y puesta en práctica.

Hash-cracking

Descripción y herramientas comunes.

Criptografía

Tipos de cifrado y clasificación, y herramientas criptográficas.

Escalada de privilegios

Descripción y casos de uso.

Bypass

Descripción a través de la vulnerabilidad CVE-2017-8386.

Ransomware

Prueba de concepto de un ransomware.

Código auxiliar

Scripts de despliegue

`instalar.sh`

1. Obtiene los laboratorios.
2. Para cada uno:
3. Si ya existe, lo actualiza.
4. Si no existe, lo construye.

```
Imagen: 01_intro-linux
    Actualizando...
    Actualizada.

Imagen: 02_intro-bash
    Actualizando...
    Actualizada.

Imagen: 03_intro-redes
    No tiene Dockerfile.

Imagen: 04_analisis-trafico
    Creando...
    Creada.

(...)

Resumen:
* 01_intro-linux
* 02_intro_bash
* 04_analisis-trafico
* (...)
```

stop-1h-container.sh

1. Obtiene los laboratorios activos y su inicio.
2. Para cada uno:
3. Muestra un mensaje informativo.
4. Si pasó 1 hora, lo destruye.

```
Ejecución actual: 13:14:06

Hay 4 contenedores activos.

592cd7fed0cc:   903 / 3600 segundos. Disponible
d37127f27ae4:   3000 / 3600 segundos. Disponible
6159264a6115:   3545 / 3600 segundos. Destrucción inminente
31e11305ce36:   3610 / 3600 segundos. Tiempo de vida alcanzado
```

Proyectos para laboratorios

`ip-osint`

Proyecto escrito en Python que recibe una IP o lista de IPs y devuelve información sobre ellas obtenidas de diversas fuentes.

`stockholm.py`

Script escrito en Python que cifra (y descifra) los ficheros de un directorio específico del sistema, simulando un ransomware.

Conclusiones y futuras líneas de trabajo

Conclusiones

1. Aumentar mi conocimiento en ciberseguridad
2. Aprender sobre Docker y sus posibilidades
- Aprender sobre desarrollo web mediante WordPress

Futuras líneas de trabajo

- Trasladar el proyecto a un servicio de alojamiento
- Expandir el contenido de Pentesting
- Optimizar la plataforma (no usar WordPress)
- Generalizar el cotenido (no solo Pentesting)
- Organizar el contenido (categorías, rutas, módulos...)

Muchas gracias