Departamento de Informática

**Honeypots y Análisis de Vulnerabilidades**

**En la Administración de redes**

**Trabajo Fin de Grado**

GRADO SUPERIOR EN ADMINISTRACIÓN DE SISTEMAS Y INFORMÁTICOS EN RED

Junio de 2024

Autor:

**SEBASTIÁN DAVID GARCÍA SAIZ**

07260252A

Tutor:

Prof. XXXXXXXXXXXXXXXXXXX

**Departamento de Informática**

Instituto de Enseñanza Secundaria José Rodrigo Botet

Tabla de contenido

[I. Introducción 8](#_Toc157441798)

[I.II. Motivación del Proyecto 8](#_Toc157441799)

[I.II. Contexto del proyecto 8](#_Toc157441800)

[I.III. Objetivos 8](#_Toc157441801)

[II. Trabajo relacionado y tecnologías empleadas. 9](#_Toc157441802)

[III. Desarrollo 10](#_Toc157441803)

[III.I Infraestructura 10](#_Toc157441804)

[III.II Creación Infraestructura 10](#_Toc157441805)

[III.II.I Instalación TPOT 10](#_Toc157441806)

[IV. Impacto del trabajo 11](#_Toc157441807)

[IV.I Impacto general 11](#_Toc157441808)

[V. Resultados y conclusiones 12](#_Toc157441809)

[V.I. Resultados 12](#_Toc157441810)

[V.II. Conclusiones personales 12](#_Toc157441811)

[V.III Trabajo futuro 12](#_Toc157441812)

[Bibliografía 13](#_Toc157441813)

[Anexo 14](#_Toc157441814)

Índice de Figuras

Índice de Tablas

Resumen

«Aquí va el resumen del TFG. Extensión máxima 2 páginas.»

Palabras Clave:

Abstract

«Abstract of the Final Degree Project. Maximum length: 2 pages.»

Keywords:

Capítulo 1

# I. Introducción

En este capítulo se explicará el porqué del proyecto, los objetivos y la estructura del mismo.

## I.II. Motivación del Proyecto

Cuando me planteé la posible idea del proyecto, la primera palabra que me vino a la mente fue *Ciberseguridad*. El término ciberseguridad es muy amplio, por lo que quise centrarme en algo concreto. La idea que más me llamaba la atención fue la de hacer análisis de vulnerabilidades dentro de la red de Conselleria lo cual, como cabía esperar, fue imposible. Fue entonces cuando, con esta idea y, un poco perdido al no saber que hacer, uno de mis profesores, Tomás, me dio la idea de los Honeypots. Fue, así pues, cómo llegué a hacer este proyecto.

El proyecto está enfocado en mi futuro académico y profesional. Así pues, es como decidí realizar un proyecto que me ayudase de cara a la especialización en ciberseguridad.

## I.II. Contexto del proyecto

«Contexto del desarrollo de este TFG, previos trabajos, el estado actual del campo del tema de este TFG, etc.»

## I.III. Objetivos

Este trabajo está orientado a la creación de una infraestructura de servidores simulando la infraestructura informática de un hospital pequeño. Se pretende observar las vulnerabilidades más típicas y monitorizar los ataques a nuestra red, en la que se incluyen datos de pacientes, trabajadores…

* Montaje de la infraestructura
* Montaje del Honeypot
* Análisis de vulnerabilidades
* Monitorización mediante el Honeypot

Capítulo 2

# II. Trabajo relacionado y tecnologías empleadas.

Durante el desarrollo de este proyecto, se observará cómo se emplean diferentes tecnologías. Muchas de ellas ya son utilizadas diariamente en casi cualquier empresa. A continuación, el desarrollo de los conceptos necesarios para así entender las tecnologías empleadas en este proyecto.

Para empezar, Honeypot. Herramienta de seguridad informática que simula ser un sistema o servicio vulnerable para atraer y detectar posibles amenazas. Utilizaremos el denominado **Medpot**, el cual se centra en emular sistemas médicos y de salud, con el objetivo de detectar posibles amenazas dirigidas a este sector.

La tecnología empleada para descargar el honeypot será GitHub, un portal creado para alojar el código de las aplicaciones de cualquier desarrollador y que Microsoft compró. La plataforma se creó para que los desarrolladores suban el código de sus aplicaciones y herramientas para que, no solo puedas descargarla, sino que puedas entrar al perfil para leer sobre ella y/o colaborar en su desarrollo.

También se subirá el proyecto a GitHub para que haya una mayor facilidad de acceso al mismo.

Utilización de Vagrant para la realización del proyecto. Vagrant es una herramienta para la creación y configuración de entornos de desarrollo virtualizados.

En cuanto a las APKs médicas utilizadas usaremos:

|  |  |
| --- | --- |
| APK | Definición |
| OpenMRS | Plataforma de registros médicos electrónicos de código abierto y altamente configurable. Es utilizado para gestionar información de pacientes, historias clínicas y datos de atención médica. |
| GNU Health | Sistema de información sanitaria de código abierto que abarca atención primaria y gestión hospitalaria. Ofrece características como gestión de pacientes, laboratorio, farmacia, facturación y más. |
| OpenEMR | Solución de registros médicos electrónicos y gestión de prácticas médicas. Incluye características como programación de citas, facturación, recetas electrónicas y más. |
| Oscar EMR | Sistema de registros médicos electrónicos basado en web utilizado en entornos clínicos. Ofrece módulos para la gestión de pacientes, recetas, laboratorio y más. |
| FreeMED | Sistema de información médica de código abierto que se centra en la atención ambulatoria. Proporciona características para la gestión de pacientes, programación de citas y facturación. |

*Tabla 1. Aplicaciones Médicas*

Capítulo 3

# III. Desarrollo

## III.I Infraestructura

La infraestructura Que elegida es la siguiente:

Diagrama

Descripción generada automáticamente

*Fig 1*

## III.II Creación Infraestructura

A la hora de la creación de la infraestructura, se levantará mediante Vagrant.

### III.II.I Enrutador

### III.II.II Base de datos hospitalaria

### III.II.III Coreo y Comunicaciones

### III.II.IV Honeypot

## III.II.I Instalación TPOT

Capítulo 4

# IV. Impacto del trabajo

«Breve explicación, por secciones, de los contenidos de este capítulo»

## IV.I Impacto general

«Análisis del impacto potencial de los resultados obtenidos durante la realización del TFG, en los diferentes contextos para los que se aplique. Además, se harán notar aquellas decisiones tomadas a lo largo del trabajo que tienen como base la consideración del impacto.»

IV.II Objetivos de desarrollo

Capítulo 5

# V. Resultados y conclusiones

«Breve explicación, por secciones, de los contenidos de este capítulo»

## V.I. Resultados

«Resumen de resultados obtenidos en el TFG»

## V.II. Conclusiones personales

«Conclusiones personales del estudiante sobre el trabajo realizado»

## V.III Trabajo futuro

«Trabajo futuro que no se haya podido realizar o siguientes pasos que tomará el desarrollo realizado en este TFG»

# Bibliografía

[1] T-POT: TU PRIMER HONEYPOT PASO a PASO. (2021, 2 febrero). Stackfire. <https://www.stackfire.com/t-pot-tu-primer-honeypot-paso-a-paso/>

[2] *¿Qué es un honeypot?* (2023, 19 abril). latam.kaspersky.com. <https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot>

Apendice A

# Anexo

«Este capítulo (anexo) es opcional, y se escribirá de acuerdo con las indicaciones del Tutor.»