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. Manuel Tomás Giménez Albert

**Departamento de Informática**

Instituto de Enseñanza Secundaria José Rodrigo Botet

ÍNDICE

[Resumen 6](#_Toc159866850)

[Abstract 7](#_Toc159866851)

[I. Introducción 8](#_Toc159866852)

[I.II. Motivación del Proyecto 8](#_Toc159866853)

[I.II. Contexto del proyecto 8](#_Toc159866854)

[I.III. Objetivos 8](#_Toc159866855)

[II. Trabajo relacionado y tecnologías empleadas. 9](#_Toc159866856)

[III. Desarrollo 10](#_Toc159866857)

[III.I Infraestructura 10](#_Toc159866858)

[III.II Imagen T-POT 10](#_Toc159866859)

[III.II.I Creación de la Imagen 10](#_Toc159866860)

[III.II.II Imagen de T-POT en Vagrant 11](#_Toc159866861)

[III.III Creación Infraestructura en Vagrant 14](#_Toc159866862)

[III.III.I Enrutador 14](#_Toc159866863)

[III.III.II Servidor Odoo 14](#_Toc159866864)

[III.III.III Honeypot 14](#_Toc159866865)

[IV. Impacto del trabajo 16](#_Toc159866866)

[IV.I Impacto general 16](#_Toc159866867)

[V. Resultados y conclusiones 17](#_Toc159866868)

[V.I. Resultados 17](#_Toc159866869)

[V.II. Conclusiones personales 17](#_Toc159866870)

[V.III Trabajo futuro 17](#_Toc159866871)

[Bibliografía 18](#_Toc159866872)

[Anexo 19](#_Toc159866873)

Índice de Figuras

Figura 1. Infraestructura

Figura 2. Clonación del Repositorio

Figura 3. Ejecución del creador de imágenes

Figura 4. Fin de la creación de la Imagen T-POT

Figura 5. Menú de instalación de TPOT

Figura 6. Selección tipo honeypot

Figura 7. Selección de contraseña para el usuario tsec

Figuras 8 y 9. Creación del usuario para la web

Figura 10. Empaquetado de la MV

Figuras 11 y 12. Subida de la imagen a Vagrant Cloud

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.

La principal tecnología en la que se basa este proyecto es el **Honeypot**. Cuya definición es: “*Sistema informático que se “sacrifica” para atraer ciberataques, como un señuelo. Simula ser un objetivo para los hackers y utiliza sus intentos de intrusión para obtener información sobre los cibercriminales y la forma en que operan o para distraerlos de otros objetivos”*(1)*.* Utilizaremos el denominado **TPOT**, el cual se contiene numerosas herramientas. Nosotros nos centraremos en la instalación basada en entornos médicos.

La tecnología empleada para descargar la imagen del será **GitHub**, un *“servicio basado en la nube que aloja un sistema de control de versiones (VCS) llamado Git. Éste permite a los desarrolladores colaborar y realizar cambios en proyectos compartidos, a la vez que mantienen un seguimiento detallado de su progreso”*(2).

Si nos preguntamos qué es **Git**, la tecnología empleada en GitHub, Git es “el sistema de control de versiones moderno más utilizado del mundo”(3).

También se subirá el proyecto a GitHub para que haya una mayor facilidad de acceso al mismo así como llevar a cabo un control de versiones.

Se utilizará **Filezilla** para transferir la .iso del TPOT desde un Ubuntu Server a nuestro equipo anfitrión. *“Filezilla es una aplicación FTP libre y de código abierto que consta de un cliente y un servidor. Soporta los protocolos FTP, SFTP y FTP sobre SSL/TLS (FTPS)”*(4)*.*

Se utilizará **Odoo** para la creación del sistema hospitalario. *“Odoo es un software de ERP integrado. Cuenta con una versión "comunitaria" de código abierto bajo licencia LGPLv3 y una versión empresarial bajo licencia comercial que complementa la edición comunitaria con características y servicios comerciales”*(5)*.*

Utilización de **Vagrant** para la realización del proyecto. *“Vagrant es un software que nos permite configurar una instancia de una máquina virtual mediante un archivo de configuración. Este archivo nos permite configurar el sistema operativo, redes, redirección de puertos, usuarios, scripts de aprovisionamiento, etc. Vagrant es muy útil para los equipos de desarrolladores y operadores de sistemas, ya que permite aprovisionar entornos de forma automatizada y alineada.”*(6).

A la hora de cargar el Honeypot en Vagrant deberemos usar **Hyper-v** “producto de virtualización de hardware de Microsoft. Le permite crear y ejecutar una versión de software de un equipo, denominada máquina virtual. Cada máquina virtual actúa como un equipo completo, ejecutando un sistema operativo y programas.”(7). Crearemos la imagen y subirla a Vagrant Cloud para así poder utilizarla en Vagrant.

Capítulo 3

# III. Desarrollo

## III.I Infraestructura

La infraestructura Que elegida es la siguiente:

Diagrama

Descripción generada automáticamente

Fig. 1 *Infraestructura*

## III.II Imagen T-POT

### III.II.I Creación de la Imagen

Para la creación de la .iso de TPOT utilizaremos un servidor de Ubuntu en el cual, siguiendo las instrucciones de la comunidad de GitHub, crearemos la imagen del TPOT.

Una vez tenemos nuestro servidor Ubuntu listo, procederemos a clonar el repositorio del tpot.

Texto

Descripción generada automáticamente

Fig. 2 Clonación del repositorio

Nos dirigimos al nuevo directorio tpotce con el comando *cd* y ejecutamos el creador de imágenes.



FIG. 3 Ejecución del creador de imagenes

Una vez ejecutado, se nos abrira el T-POT – ISO CREATOR. Seleccionamos la arquitectura de la imagen según lo deseado (en nuestro caso amd64).

Siguiendo la creación de la imagen tendremos que elegir si configurar o no un proxy, si añadir un certificado de anfitrión 802.1x y si queremos configurar un sistema NTP.

En nuestro caso hemos denegado todo esto y procedemos a finalizar.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Fig. 4 Fin creación de la imagen

Por último, elegimos que no queremos grabar la imagen en un USB.

Si listamos el contenido veremos que tenemos la .iso. Ahora solo falta que la pasemos a nuestro equipo anfitrión con Filezilla y creemos una máquina en VirtualBox.

### III.II.II Imagen de T-POT en Vagrant

Comenzamos creando la MV en Vbox. Seleccionamos la iso de T-POT y configuramos la maquina con 4GB de RAM y 30GB de almacenamiento como mínimo. La tarjeta de red la dejaremos en modo adaptador puente. cOMPROBAMOs que la arquiteCTura seleccionada sea 64 bits. Tras iniciar la máquina veremos el menú de instalación. Seleccionamos la primera opción.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Fig. 5 Menú de instalación de TPOT

Se iniciará la instalación donde deberemos indicar nuestra zona geográfica, el mapeado del teclado a utilizar, el país del Debian mirror, el archivo del Debian mirror, si queremos usar un proxy (e indicar cual). Una vez termine de instalarse el sistema pasaremos al menú de configuración de TPOT. Una vez termine, se reiniciará.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Fig. 6 Selección tipo honeypot

Una vez seleccionada la versión, introducimos la contraseña del usuario *tsec* (el ususario por defecto) Sebas123

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

Fig. 7 Selección de contraseña para el usuario tsec

Creamos el usuario para la web.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Fig. 8 y 9 Creación del usuario para la web

Una vez creado terminará de realizarse la instalación del honeypot. La máquina se reiniciará al acabar este proceso.

Llega el momento de cerrar la máquina y empaquetarla como Vagrant box. Para ello utilizaremos comandos de Vagrant.



FIG. 10 Empaquetado de la MV

A la hora de subir la box a Vagrant Cloud lo haremos a través de la web. Seguimos los pasos hasta que nos pida el archivo a subir.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Fig. 11 y 12 Subida de la imagen a Vagrant Cloud

Haremos lo mismo para subir una imagen de Ubuntu Server 22.

## III.III Creación Infraestructura en Vagrant

Una vez terminamos los preparativos, vamos a configurar toda nuestra infraestructura a través de Vagrant.

### III.III.I Enrutador

### III.III.II Servidor Odoo

### III.III.III Honeypot

# III.IV Monitoreo y Análisis de Vulnerabilidades

## III.IV.I Monitorización

## III.IV.II Puertos

## III.IV.III Ataques

## III.IV.IV SIM Swapping

## III.IV.V Ataques comunes

En este fragmento del TFG hablaremos de los ataques más peligrosos del año 2023 así como de algunos datos importantes a tener en cuenta.

Durante todo 2023 entre los ataques más comunes realizados encontramos los siguientes:

* Dispositivos inteligentes como objetivo: con el aumento de las IAs y Machine Learning, cada vez se estima que se vaya a utilizar más herramientas de ciberseguridad con IA implementada. Hemos podido observar cómo ha habido brechas de seguridad en vehículos automatizados y han podido ser controlados parcialmente por personas ajenas a las empresas automovilísticas o los dueños.
* Phishing e ingeniería social: ya en 2022 los ataques de phising se dispararon. Los ciberdelincuentes encuentran este tipo de ataques muy beneficiosos ya que, no es más que probar para ver a quien se puede engañar. Igual pasa con la ingeniería social (de hecho, el phishing no deja de serlo muchas veces debido a los mails).
* Delincuencia como servicio: se ha estimado que el coste de los servicios de ciberdelincuencia será algo que alcanzará los 10,5 billones de USD en 2025. A medida que el ciberdelito se establece cada vez más como fuente de ingresos para los actores maliciosos, algunos están optando por ofrecer sus servicios a una comunidad más amplia a cambio de una tarifa.
* Ataques de denegación de servicios: hoy en día podemos llegar a observar que el calibre de este tipo de ataques puede ser inmenso. El verano de 2022 se registró el mayor de toda la historia, con más de 5000 IP contribuyendo yen 132 paises. Esto nos deja claro el peligro al que puede enfrentarse una empresa de prestación de servicios como un ISP. Sin ir más lejos, Un ataque de DDoS acabó por tirar el servicio de telecomunicaciones de Andorra hace 2 años.
* Ransomware: este tipo de ataques consisten en cifrar los datos del objetivo con software malicioso (malware) para impedir el acceso a los mismos y pedir un rescate paraliberar los datos. Es por esto que es conocido como malware de rescate.

(8),(9)

Si realizamos una pequeña búsqueda por internet, podremos encontrarnos con datos bastante alarmantes en cuanto a ciberdelincuencia.

Si analizamos los datos de las industrias que más han sido atacadas encontramos que, durante el año 2023 más del 17% de los ataques fueron a instituciones gubernamentales y que más del 10%fue a la industria tecnológica. Entre el top 5 encontramos también los servicios financieros, educación y defensa.

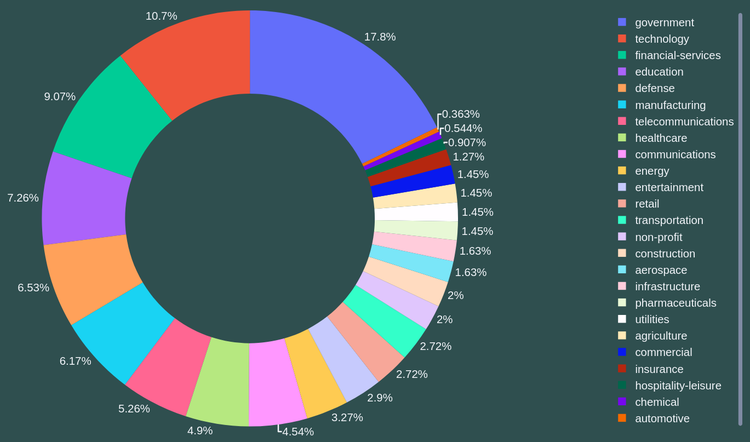


Fig. Porcentaje de ataques según la industria

Los objetivos más comunes han sido:

* Ganancia de dinero
* Espionaje/Robo de información
* Interrupción de servicios
* Uso y control no autorizado de recursos
* Establecimiento de control para futuros ataques
* Filtración de datos
* Reconocimiento
* Promoción ideológica y/o política
* Distribución de Malware
* Guerra cibernética

Datos contrastados (10)

Además, según el FBI las pérdidas por ciberdelincuencia alcanzaron un nuevo récord, superando los 12.500 millones de dólares en 2023. (11).

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. latam.kaspersky.com [Internet]. 2023 [citado 22 de diciembre de 2023]. ¿Qué es un honeypot? Disponible en: https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot

2. B G. Qué es GitHub y cómo empezar a usarlo [Internet]. Tutoriales Hostinger. 2019 [citado 11 de febrero de 2024]. Disponible en: https://www.hostinger.es/tutoriales/que-es-github

3. Atlassian. Atlassian. [citado 11 de febrero de 2024]. Qué es Git | Atlassian Git Tutorial. Disponible en: https://www.atlassian.com/es/git/tutorials/what-is-git

4. FileZilla. En: Wikipedia, la enciclopedia libre [Internet]. 2024 [citado 11 de febrero de 2024]. Disponible en: https://es.wikipedia.org/w/index.php?title=FileZilla&oldid=158118388

5. Odoo. En: Wikipedia, la enciclopedia libre [Internet]. 2024 [citado 11 de febrero de 2024]. Disponible en: https://es.wikipedia.org/w/index.php?title=Odoo&oldid=158016832

6. Deloitte Spain [Internet]. [citado 11 de febrero de 2024]. ¿Qué es Vagrant? Disponible en: https://www2.deloitte.com/es/es/blog/todo-tecnologia/2022/que-es-vagrant.html

7. BenjaminArmstrong. Información general sobre la tecnología Hyper-V [Internet]. 2023 [citado 25 de marzo de 2024]. Disponible en: https://learn.microsoft.com/es-es/windows-server/virtualization/hyper-v/hyper-v-technology-overview

8. Powell O. Cyber Security Hub. 2022 [citado 5 de abril de 2024]. The most dangerous cyber security threats of 2023. Disponible en: https://www.cshub.com/attacks/articles/the-most-dangerous-cyber-security-threats-of-2023

9. Malwarebytes [Internet]. [citado 5 de abril de 2024]. Ransomware: qué es y cómo eliminarlo. Disponible en: https://es.malwarebytes.com/ransomware/

10. Chiscariu RE. Analysis of the top Cyber Threats in 2023 | Keysight Blogs [Internet]. [citado 5 de abril de 2024]. Disponible en: https://www.keysight.com/blogs/en/tech/nwvs/2024/01/22/threatsin2023-jan-2024

11. Merino PP. Las pérdidas por ciberdelincuencia alcanzan un nuevo récord superando los 12.500 millones de dólares en 2023, según el FBI [Internet]. CyberSecurity News. 2024 [citado 5 de abril de 2024]. Disponible en: https://cybersecuritynews.es/las-perdidas-por-ciberdelincuencia-alcanzan-un-nuevo-record-superando-los-12-500-millones-de-dolares-en-2023-segun-el-fbi/

Apendice A

# Anexo

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