ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INDUSTRIALES Y DE TELECOMUNICACIÓN

UNIVERSIDAD DE CANTABRIA

Trabajo de Fin de Grado

Entorno para la concienciación de riesgos de seguridad en redes inalámbricas compartidas

(Environment for the awareness of security risks in shared wireless networks)

Para acceder al Título de

Graduado en Ingeniería de Tecnologías de Telecomunicación

Autor: Javier Rodrigo García

Julio - 2022

GRADUADO EN INGENIERÍA DE TECNOLOGÍAS DE TELECOMUNICACIÓN

CALIFICACIÓN DEL TRABAJO FIN DE GRADO

Realizado por: Rodrigo García, Javier
Director del TFG: Lanza Calderón, Jorge

Título: "Entorno para la concienciación de riesgos de seguridad en redes inalámbricas compartidas"
Title: "Environment for the awareness of security risks in shared wireless networks"

Presentado a examen el día: 27 de Julio de 2022
para acceder al Título de

GRADUADO EN INGENIERÍA DE TECNOLOGÍAS DE TELECOMUNICACIÓN

Composición del Tribunal:
Presidente (Apellidos, Nombre): Madruga Saavedra, Francisco Javier
Secretario (Apellidos, Nombre): Díez Fernández, Luis Francisco
Vocal (Apellidos, Nombre): Lanza Calderón, Jorge

Este Tribunal ha resuelto otorgar la calificación de: .....

Fdo.: El Presidente

Fdo.: El Secretario

Fdo.: El Vocal

Fdo.: El Director del TFG
(sólo si es distinto del Secretario)

Vº Bº del Subdirector

Trabajo Fin de Grado Nº
(a asignar por Secretaría)

AGRADECIMIENTOS

En primer lugar, me gustaría agradecer a Jorge Lanza por su disposición, ayuda, paciencia y, sobre todo, su gran labor de interpretación para comprender qué le estaba intentando comunicar cada vez que abría la puerta de su despacho. Sin su buen desempeño este Trabajo de Fin de Grado no hubiera sido posible.

Tras esto, no puedo dejar sin exponer por escrito lo agradecido que me siento por mi familia. Muchas gracias por vuestro apoyo y comprensión. Aunque sin olvidarme del resto, quiero mencionar a mi abuela Juliana y a mi tía Antonia; pero, sobre todo, a vosotras, Mamá y Miri.

Por otra parte, también quiero agradecer a mis amigos. Por fin ha llegado la hora de presentar, ya podéis dejar de preguntaros cuando acabaré.

Finalmente, no puedo dejar de agradecer a quienes ya no están por la gran marca que han dejado en mi vida. Empezando por mi abuela Rosa a quién no tuve la suerte de conocer, pero sé que fue una maravillosa persona; siguiendo por mis abuelos Emiliano y Agustín de los cuales aprendí la importancia del trabajo y de no olvidarte de tus raíces; y terminando por el más especial de todos, Papá, de quien espero haber heredado sus grandes valores éticos y su gran resiliencia. Espero que, si realmente existe algo más allá, estéis tan orgullosos de mí como yo lo estoy de vosotros.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

RESUMEN

Actualmente, sería impensable concebir una sociedad desapegada de los dispositivos móviles (ya sean teléfonos, ordenadores, tablets, etc.) y su conexión a Internet. Nos hemos vuelto extremadamente dependientes de esa conexión a Internet, y por ello en cuanto cabe la posibilidad de seguir consumiendo contenido online sin gastar sus “preciados” gigas de la tarifa de datos la gente tiende a conectarse a cualquier red abierta disponible.

En este proyecto se va a tratar de concienciar a los usuarios de puntos de acceso públicos para que conozcan el riesgo que conlleva para su privacidad, el convertirse en usuario de una red con un gestor de dudosas intenciones.

Para ello se instará a los usuarios a conectarse a un punto de acceso a través de un portal cautivo. Una vez conectados, se recopilarán los datos de su sesión; para finalmente, cortar el acceso a internet y redireccionar a una web en la que se advertirá de los peligros de realizar conexiones de este tipo y se adjuntará el desglose del tráfico de su sesión.

ABSTRACT

Currently, it would be unthinkable to conceive of a society detached from mobile devices (be they phones, computers, tablets...) and their Internet connection. We have become extremely dependent on that Internet connection, and for this reason, as soon as it is possible to continue consuming online content without spending their "precious" gigabytes of data rates, people tend to connect to any available open network.

This project is going to try to make users of public access points aware of the risk that it entails for their privacy, becoming a user of a network with a manager with dubious intentions.

To do this, users will be prompted to connect to an access point through a captive portal. Once connected, your session data will be collected; Finally, it cuts off Internet access and redirects to a website that warns of the dangers of making connections of this type and includes a breakdown of your session traffic.

LISTA DE ACRÓNIMOS

AP - Access Point

CHAP - Challenge-Handshake Authentication Protocol

CPD - Captive Portal Detection

CPU - Central Processing Unit

DoS - Denial-of-Service

DDoS - Distributed Denial-of-Service

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

HTTP - Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

IP - Internet Protocol

IoT – Internet of Things

ISP - Internet Service Provider

LAMP - Linux, Apache, MySQL, PHP/Perl/Python

LAN - Local Area Network

LDAP - Lightweight Directory Access Protocol

MAC - Media Access Control

MitM - Man-in-the-Middle

MSCHAP - Microsoft Software Challenge-Handshake Authentication Protocol

NDS - Nodogsplash

NFC - Near-Field Communication

NSA - National Security Agency

Oauth - Open Authorization

PEAP - Protected Extensible Authentication Protocol

QR - Quick Response

RAM - Random Access Memory

REST - REpresentational State Transfer

RFID - Radio Frequency Identification

SMS - Short Message Service

SO - Sistema Operativo

SQM - Smart Queue Management

SSID - Service Set Identifier

SSL - Secure Sockets Layer

TCP - Transmission Control Protocol

UC - Universidad de Cantabria

URL - Uniform Resource Locator

VPN - Virtual Private Network

WAN - Wide Area Network

WEF - World Economic Forum

WEP - Wired Equivalent Privacy

WPA - Wi-Fi Protected Access

WPA2 - Wi-Fi Protected Access 2

WPA3 - Wi-Fi Protected Access 3

Capitulo 1. INTRODUCCIÓN

1.1 MOTIVACIÓN

Las aplicaciones que hacen uso de Internet han despegado y se han diversificado de manera vertiginosa en los últimos años. Actualmente, la mayoría de la población hace uso de alguna red social, usa alguna aplicación de música o vídeo bajo demanda, juega a juegos online o usa aplicaciones de mensajería instantánea. El uso de Internet es indisociable de la cultura y sociedad actual, ya sea en la vida privada o en la laboral y la tendencia es que cada vez su importancia será mayor.

La dependencia de esa vida online y al acceso casi inmediato a la información hace que disponer de una tarifa de datos móviles, lo más amplia posible, para poder seguir conectados a esos contenidos en cualquier lugar y momento se haya convertido en algo casi indispensable. Dependiendo de la tarifa de datos que el usuario se pueda costear, la búsqueda y descubrimiento de redes WiFi disponibles de forma abierta hace que mucha gente, especialmente jóvenes, tienda a usarlas aceptando unos términos y condiciones de uso que ni han consultado. Así pues, sin ser conscientes de la información que están ofreciendo al gestor de esa red pública, deciden poner en riesgo su privacidad con tal de ahorrar unos pocos megabytes de datos de su tarifa móvil.

En este sentido, en las ciudades se encuentran disponibles muchos de esos puntos de acceso a Internet, algunos de ellos seguros, que proveen a los usuarios de conectividad gratuita o a modo de valor añadido al consumir en el establecimiento (consumición en un local de restauración, centro comercial, etc.).

Sin embargo, allí donde surge una oportunidad para el público general, también aparecen oportunistas con malas intenciones. Éste es el caso de algunos puntos de acceso que se hacen pasar por redes WiFi públicas gratuitas y confiables, pero que por el contrario son gestionados por gestores de red con dudosas intenciones.

Esta inocencia, mayoritariamente debida al desconocimiento o desinterés con respecto a la seguridad, hace que los usuarios que tengan la mala fortuna de acabar conectándose a esas falsas redes públicas gratuitas confiables sean presas fáciles de los ataques a su privacidad que puedan pertrechar los malhechores.

Por tanto, es necesario llevar a cabo un ejercicio de concienciación para que la gente haga un uso responsable de estos servicios. Tratando que el resultado del mismo sea conseguir que quienes tengan este hábito entiendan los riesgos a los que se exponen, puesto que sin saberlo pueden estar entregando información a aquellos con habilidad para recogerla, y traten de salvaguardar al máximo la privacidad de sus conexiones.

1.2 OBJETIVOS

Teniendo en cuenta la tendencia descrita en el apartado anterior, se ha enfocado este proyecto de modo que su resultado sea una herramienta que pueda ser utilizada en actividades de concienciación de los peligros de usar redes de este tipo.

Esta herramienta consistirá en un dispositivo portátil que actuará como punto de acceso con gestión de acceso controlado mediante portal cautivo y con capacidades para llevar a cabo un tracking de la información de la conexión de los usuarios que se conecten. Además, con esa información será capaz de realizar gráficas que muestren las tendencias de uso de los usuarios del sistema.

Por otra parte, al ser una herramienta cuya máxima será la docencia, además del sistema de recopilación de datos, se analizará la metodología para instruir a las víctimas acerca de las buenas prácticas cuando se usen puntos de acceso.

1.3 ESTRUCTURA DEL DOCUMENTO

Para abordar los objetivos de este proyecto se ha organizado el presente documento en los siguientes capítulos:

A lo largo de este primer capítulo, Introducción, se ha tratado el contexto social y tecnológico que han servido de motivación para llevar a cabo este proyecto. Además, también se han fijado los objetivos que deberá de cubrir este Trabajo.

En el segundo capítulo, Estado del arte, se desarrolla el marco tecnológico que va a sustentar la implementación de este proyecto. Por tanto, en este apartado se realiza un análisis de la tecnología WiFi, la implementación de portales cautivos y los potenciales ciberataques.

En el tercer capítulo, Diseño y arquitectura del sistema, se profundiza en el objetivo del Trabajo. Para ello, se analiza las posibilidades del sistema a través de un caso de uso y se narran los requerimientos y arquitectura funcional del proyecto.

En el cuarto capítulo, Despliegue de la solución, se desarrolla la forma en que se ha procedido para llevar a cabo la configuración del sistema. En este apartado se explica cuál ha sido el hardware requerido y se pormenoriza en cómo se pasa de ese hardware al sistema final. Además, se muestran imágenes que demuestran el correcto funcionamiento del sistema.

El quinto y último capítulo, Conclusiones, sirve como cierre para el proyecto. En este capítulo se exponen las conclusiones alcanzadas tras finalizar este Trabajo; se realiza una disertación acerca de las buenas prácticas en el uso de portales cautivos

con el objetivo de evitar que los usuarios estén totalmente indefensos e inconscientes de los peligros de este tipo de conexiones y se sopesan las posibles líneas de desarrollo futuro.

Capitulo 2. ESTADO DEL ARTE

En este capítulo se describe el marco tecnológico en el que se desarrolla este Trabajo de Fin de Grado. En él se describirán la tecnología inalámbrica WiFi, su arquitectura y seguridad; los mecanismos de compartición de redes WiFi, evolucionando desde el hotspot hasta el portal cautivo; y los potenciales ataques que pueden llegar a sufrir los usuarios de Internet en general y en concreto, por ser el objetivo final de este proyecto, los usuarios de los portales cautivos.

2.1 TECNOLOGÍA INALÁMBRICA WIFI

WiFi es una tecnología que permite la interconexión inalámbrica de dispositivos electrónicos. Su nombre hace referencia a una marca comercial de la WiFi Alliance, el conjunto de instituciones que impulsaron el desarrollo de esta tecnología. Cuando se habla de esta tecnología, se hace referencia al estándar IEEE 802.11 [1].

2.1.1 Arquitectura de redes WiFi

Las redes inalámbricas han sufrido una gran evolución, pasando de pequeñas redes de área local a su despliegue en redes de área extensa. Lo cual es posible gracias a la gran escalabilidad de la tecnología WiFi.

El concepto básico de una red WiFi es la celda, la cual se puede definir como el área en el cual una serie de dispositivos se interconectan a través de un medio aéreo. En función de los elementos que compongan esa celda se categoriza el modo de la conexión:

- En el modo Infraestructura, representado en la Figura 2.1, cada celda suele estar formada por estaciones y un único punto de acceso (AP, Access Point). En este modo, todo el tráfico de la red pasa a través del AP por lo que es un claro ejemplo de una distribución punto-multipunto. Por lo tanto, en el caso de que se use para conectar dos dispositivos de la misma red es ineficiente ya que tendrían que transmitir primero al punto de acceso; sin embargo, esta arquitectura es la apropiada si la mayor parte del tráfico va a ser recibido o transferido desde el exterior de la red.

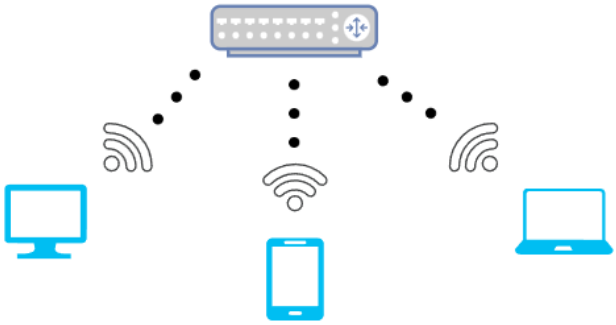

Figura 2.1 Modo Infraestructura

- En el modo ad-hoc, representando en la Figura 2.2, las celdas no cuentan con un AP, en este caso las estaciones se interconectan entre ellas y se genera una red con estructura punto a punto. Las estaciones que trabajan de este modo asumen de manera aleatoria las funciones de coordinación y el tráfico se lleva a cabo directamente entre los dispositivos implicados. Este tipo de red funciona bien cuando el número de dispositivos de la red es reducido y están próximos entre ellos.

Figura 2.2 Modo ad hoc

2.1.2 Seguridad en redes WiFi

La seguridad de la red WiFi es uno de los puntos más vitales y a la vez de los menos considerados por el usuario promedio. Una mala configuración de seguridad no solo implica que entidades no autorizadas puedan conectarse y hacer uso de la red libremente, sino que pueden aprovechar esa conexión furtiva para llevar a cabo acciones ilegales bajo el nombre del propietario, monitorizar el uso que hacen de la

misma el resto de los usuarios e incluso promover el uso y acceso a software o sitios de dudosa reputación.

Para evitar estas desagradables consecuencias, la seguridad en las redes WiFi se fundamenta en unos pilares básicos:

- Integridad: Se debe de garantizar la detección de modificaciones, por parte de usuarios maliciosos, de la información que se transfiera de un usuario a otro a través de la red.
- Confidencialidad: La información que circula por la red solo debe de poder ser visualizada por quienes estén autorizados.
- Disponibilidad: La información ha de estar presta para que quienes estén autorizados puedan acceder a ella cuando lo requieran.

Basándose en estos fundamentos, a lo largo del tiempo los algoritmos utilizados para proteger las redes inalámbricas han ido evolucionando para conseguir mayor seguridad y eficacia. Esos algoritmos son los siguientes:

- Wired Equivalent Privacy (WEP)[2]: Este protocolo fue el primero en implementarse y fue el estándar entre 1999 y 2004. Hace uso de un cifrado de 64 bits, el cual en su momento era funcional, ya que aún no se habían desarrollado demasiado las capacidades criptográficas. Sin embargo, en 2004 fue abandonado por la WiFi Alliance debido a sus múltiples vulnerabilidades.

- WiFi Protected Access (WPA)[3]: Este protocolo nació en 2003 como una evolución de WEP, facilitando la configuración e introdujo un algoritmo de integridad de clave temporal (TKIP) para mejorar la seguridad del cifrado. Debido a que este protocolo tuvo que mantener retrocompatibilidad con los dispositivos que hacían uso de la seguridad WEP, no se pudieron solventar todas las vulnerabilidades existentes, lo cual hace que actualmente la seguridad que ofrece este algoritmo pueda ser violada fácilmente.

- WiFi Protected Access 2 (WPA2)[4]: Solo un año después de desarrollar WPA, en 2004, se implementó WPA2 y desde 2006 es una certificación obligatoria para todos los dispositivos con conectividad WiFi que vayan a salir al mercado. La seguridad ofrecida por WPA2 es más robusta y sustituye TKIP por el algoritmo Advanced Encryption Standard (AES). Este protocolo hoy en día aún sigue dando cierta garantía de seguridad y su única vulnerabilidad notable es que cualquier usuario con acceso lícito a la red puede tratar de atacar al resto de usuarios.

- WiFi Protected Access 3 (WPA3)[5]: En 2017 se descubrió una vulnerabilidad en WPA2, que se denominó el ataque tipo KRACKs o ataque de reinstalación de contraseñas [6]. Para cerrar esta brecha surgió en 2018 WPA3. Este nuevo

algoritmo garantiza seguridad frente ataques de fuerza bruta, mejora la privacidad de los usuarios de redes públicas al encriptar sus datos hasta cuando la red no tiene contraseña, añade seguridad adicional para los dispositivos de Internet de las Cosas (IoT) y utiliza una encriptación de 192 bits. Sin embargo, para hacer funcionar todas estas mejoras se necesitan dispositivos con altas capacidades criptográficas. Por lo que muchos de los dispositivos existentes compatibles con la certificación WPA2 no lo son con WPA3.

2.2 PORTAL CAUTIVO

Con la democratización del uso de dispositivos electrónicos portátiles con capacidad de conectarse a Internet, surgió la necesidad de crear áreas en las que se ofreciera acceso a la red. Esto desembocó en la distribución de este servicio a modo de hotspot, el cual no es más que un AP que se encuentra disponible para que los usuarios puedan conectarse a él de manera inalámbrica.

Para generar un hotspot basta con tener un dispositivo conectado a Internet con capacidad para generar un área WiFi al que los usuarios cercanos puedan conectarse.

Sin embargo, al ofrecer este servicio, los prestadores del servicio se convierten en responsables del uso que quienes acceden a ella den a esa sesión; por ello, para evitar quedar tan expuestos al uso malintencionado de los usuarios que se beneficien del servicio ofrecido, los gestores de red comenzaron a implementar el uso de portales cautivos[7].

Un portal cautivo es un software que controla y gestiona el tráfico de un punto de acceso WiFi. Su utilización fuerza a que los usuarios que se conecten a esa red pasen por un registro antes de que el administrador del hotspot conceda acceso a Internet. De este modo, el uso de un portal cautivo tiene múltiples beneficios para el proveedor de este servicio.

Mediante su utilización los prestadores de servicio salvaguardan su infraestructura de accesos no autorizados y quedan exentos de responsabilidad legal por las actuaciones de los usuarios, ya que antes de proveer acceso a la red pueden requerir la aceptación de los términos y condiciones de uso del servicio. Además, los gestores de la red pueden definir políticas de tráfico que denieguen cierto contenido de red pública a los usuarios, regulen la duración de la conexión, la cantidad de terminales por usuario, el consumo de ancho de banda y/o la velocidad de descarga por sesión.

Al hacer uso de esta tecnología el gestor de la red puede monitorizar la frecuencia de uso de los usuarios, recopilar información sobre que uso están dando al servicio e incluso a los datos que cedieron a cambio de poder beneficiarse de ese

acceso a Internet. En definitiva, dispone de datos suficientes para crear una base de datos de clientes que podrían aprovechar para ofrecer productos/servicios propios a través de la red.

Por otro lado, permite que otros servicios que a priori no tienen una relación estrecha con el sector de las telecomunicaciones, ya sea un local de restauración, un hotel o un bar, tengan un valor añadido al asociar este elemento con la adquisición del servicio al que se refiera su actividad económica principal.

2.2.1 Seguridad

El acceso a Internet a través de un portal cautivo puede plantear por tanto ciertos riesgos de seguridad para sus usuarios. Quien ofrece el servicio tiene acceso a todo el tráfico de los usuarios que hacen uso de la red, por lo que a priori no hay forma de garantizar que el gestor de la red o algún otro usuario no vaya a controlar la red de forma no autorizada. Por ello, es crucial tener en cuenta que el factor más importante para garantizar la seguridad del usuario está en que este sepa discernir en qué servicio puede albergar su confianza y en cual no.

Sin embargo, esto puede no ser tan sencillo y por ello, al utilizar un servicio de este tipo, hay que tener cuidado con el uso que se va a realizar y tratar de minimizar los riesgos asumidos tratando de llevar a cabo unas sencillas buenas prácticas. Como son:

- Evitar hacer uso de puntos de acceso con algoritmos de cifrado débiles. La seguridad de este tipo de redes puede ser fácilmente violada por los atacantes, para de este modo hacerse con el control de la red y robar información personal de los usuarios.
- En caso de acceder a una red de este tipo evitar hacer uso de aplicaciones o páginas webs en las que se introduzcan datos personales importantes, ya sean webs de bancos o redes sociales.
- Usar una Red Privada Virtual (VPN) para que independientemente de la seguridad de la red, toda la información que se transmite se redirija por un túnel seguro que enmascare la información.

2.2.2 Sistemas Comerciales de Portal Cautivo

Como se viene relatando, la implementación de un servicio de este tipo resulta beneficiosa para la compañía que lo ofrezca. Sin embargo, dentro de la empresa o institución que quiera beneficiarse de este servicio pueden no tener contratado un perfil específico de empleado que se pueda dedicar a la creación y gestión de un

sistema de este tipo. Por ello, han surgido multitud de organizaciones que ofrecen este software y su gestión a quienes estén interesados.

En este sentido vamos a entrar a valorar algunas implementaciones de software libre y otra comercial. Analizando brevemente su funcionamiento y sus principales ventajas e inconvenientes.

2.2.2.1 Nodogsplash Captive Portal

Nodogsplash (NDS)[8] es una aplicación gratuita que permite generar portales cautivos haciendo un uso mínimo de los recursos del sistema en que se instale. Al instalar este software, por defecto, el sistema genera automáticamente un portal cautivo con una página web sencilla. Sin embargo, la ventaja de NDS es que los usuarios con conocimientos avanzados pueden mejorar el entorno de manera sencilla. Aprovechando el sistema NDS como base, se puede mejorar la página de bienvenida e incluso modificar el sistema de autenticación por otro más sofisticado. Sin embargo, entre sus características no cuenta con la opción de controlar el tráfico de red y es por ello que es típico complementarlo con sistemas como Smart Queue Management (SQM) [9].

La idea de funcionamiento del software NDS es la siguiente. Inicialmente, el programa bloquea todo el tráfico a excepción de las peticiones que se realicen a través del puerto 80. De tal modo que cuando reciba una solicitud de un dispositivo cliente al puerto 80, ya sea porque esté navegando manualmente o por la actuación del sistema de detección de portales cautivos (CPD), este sea redireccionado a la página de bienvenida.

Una vez en la página web, el sistema se mantendrá a la espera hasta que el usuario complete con éxito los requerimientos que se le exijan en la página. Cuando el usuario haya cumplido con los requerimientos exigidos, la página de bienvenida se conecta automáticamente con el directorio virtual de NDS. Por seguridad este directorio espera recibir del usuario el token con el que fue contestado cuando realizó la solicitud inicial al puerto 80. En caso de recibir ese token, NDS autentica al cliente y permite su acceso a Internet. Para permitir el acceso a la red o denegarlo, el programa modifica las reglas del firewall que se aplican sobre el dispositivo que se quiera conectar en función de su MAC, cortando el acceso a Internet a quienes aparezcan en la lista negra del firewall y ofreciéndolo a quienes estén en la lista blanca.

Su puesta en marcha es muy sencilla, basta con descargar el software NDS del repositorio de Github en que se encuentra alojado y establecer unos pocos parámetros básicos de su archivo de configuración. El resultado obtenido, sin modificar la página de bienvenida, se muestra en la Figura 2.3.

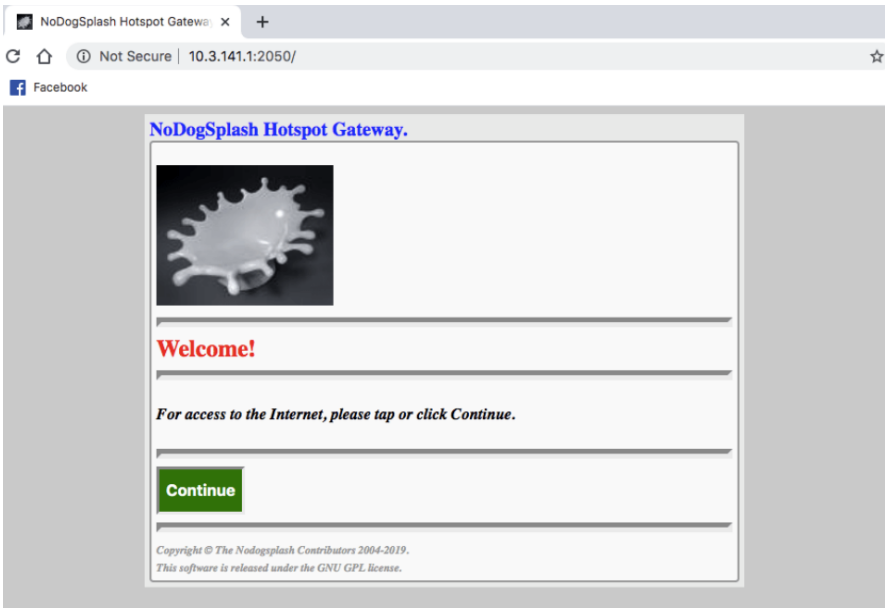

Figura 2.3 Página de bienvenida NDS

2.2.2.2 CoovaChilli Captive Portal

CoovaChilli[10] es un software de código abierto, basado en el proyecto ChilliSpot, con gran cantidad de funcionalidades que proporciona un entorno de portal cautivo con autenticación basada en RADIUS.

El sistema de redireccionamiento de usuarios a la web del portal cautivo se realiza haciendo uso del puerto 80, siendo su metodología similar a la descrita previamente en el proyecto de Nodogsplash.

Cuando un cliente se conecta a un punto de acceso gestionado por el software CoovaChilli solo puede llevar a cabo las resoluciones DNS de la página web del portal cautivo o de las aplicaciones autorizadas dentro del jardín amurallado que haya resuelto el gestor del sistema. El usuario, si quiere salir de esa situación y recibir conectividad plena, deberá de autenticarse. En este caso, la autenticación es realizada a través de un servidor FreeRadius; el cual, recibe la información que el usuario introdujo en la web de bienvenida y la compara con la información que tiene en su back-end (haciendo uso de PEAP, CHAP o MSCHAPv2). En función de la resolución de FreeRADIUS, el usuario será respondido con un mensaje de éxito o con uno de rechazo. En este caso la validación depende del sistema de back-end, el cual puede ser LDAP, Kerberos o una base de datos MySQL; siendo uno u otro en función de la elección que haya tomado el gestor para controlar la autenticación de los usuarios.

2.2.2.3 BLOOM intelligence Captive Portal

BLOOM intelligence[11] es una compañía de software que se dedica al diseño y gestión de portales cautivos. Tiene como principal ventaja que es totalmente personalizable, puesto que una vez el cliente se pone en contacto con la empresa un diseñador gráfico crea el sistema a medida de los requerimientos exigidos similar a los representados en la Figura 2.4. Además, al adquirir el servicio se ofrecen reportes con tendencias de uso, posibles estrategias de marketing a tener en cuenta y perfiles de usuarios. Por tanto, esta opción es muy útil para aquellas empresas que quieran contar con un servicio de este tipo sin tener que preocuparse por su gestión.

En este caso, poco puedo decir de la tecnología que sustenta su funcionamiento. Sin embargo, es interesante mencionar esta implementación por la idea de crear un sistema de suscripciones pagadas a cambio de la gestión del portal cautivo y el análisis de los datos.

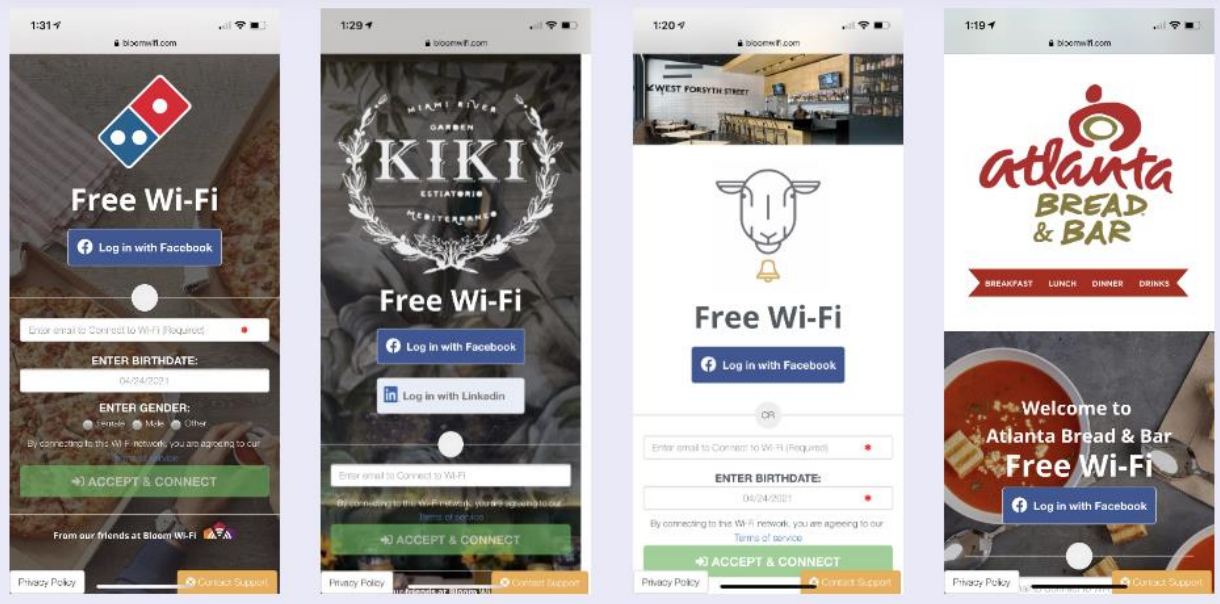

Figura 2.4 Ejemplo de diseños de página de bienvenida implementados por BLOOM intelligence

2.3 POTENCIALES CIBERATAQUES

El uso generalizado de nuevas tecnologías siempre está asociado con el interés de quienes tratan de encontrar un uso lucrativo de ellas, aunque sea a través de artimañas que vulneren la privacidad del resto de usuarios. Por lo tanto, Internet, siendo la tecnología más revolucionaria de las últimas décadas, ha sufrido en gran medida el ingenio de los usuarios malintencionados. Es por ello que la ciberdelincuencia es considerada como una de las cinco mayores amenazas para la seguridad pública según el Global Risks Perception Survey [12] y, como se puede apreciar en la Figura 2.5, una de las tendencias de riesgo que más han empeorado desde que se declaró la pandemia.

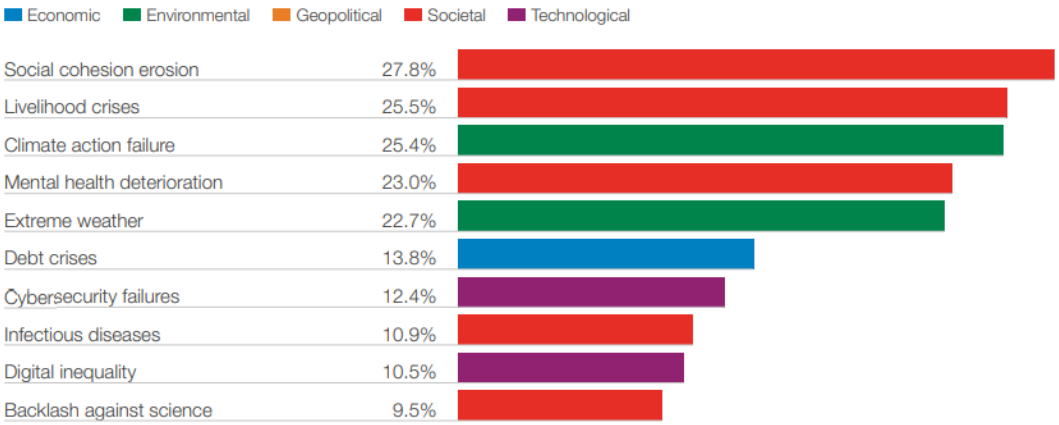

Figura 2.5 Tendencias de riesgo que más han empeorado tras la pandemia

Estos datos dejan bastante claro que los ataques cibernéticos son un problema a tener muy en cuenta por la sociedad, pero ¿por qué ha aumentado tanto la ciberdelincuencia? Pues su gran aumento se debe a varios factores: la pandemia ha hecho que el tráfico de Internet aumente, sobre todo en la aplicación sobre la que mayor partido pueden sacar los ciberdelincuentes, el teletrabajo; es una actividad muy lucrativa para quienes la ejercen de manera consistente; el riesgo de extradición, enjuiciamiento o sanción es muy bajo; y por si no fuera poco, hay menos especialistas en ciberseguridad de los que son necesarios.

Esta situación llegó a sus cotas más altas en 2020 debido al contexto de la pandemia COVID-19 que provocó confinamientos masivos para evitar su propagación y con ello aumento aún más el uso de Internet. Desde entonces la cantidad de ataques cibernéticos no ha parado de crecer a un ritmo desenfrenado, siendo la escalada de un 600% con respecto a los años anteriores a la pandemia. Por lo que para 2025 se prevé que estas actividades delictivas tendrán un costo estimado para las empresas de 10,5 billones de dólares, teniendo un creciendo interanual del 15% desde 2015. Teniendo

en cuenta que para 2024 se estima que el comercio digital crecerá en 800 billones de dólares con respecto al volumen de 2022 [13].

Sin embargo, aunque las cifras de los daños causados por los ciberataques en el mundo empresarial son muy llamativas, las empresas no son las únicas damnificadas por esta explosión de delincuencia. El público general de Internet también está sufriendo en gran medida esta situación, ya que con el uso generalizado de los smartphones se ha generado un gran "nicho de mercado" para los delincuentes. Es por ello que se han popularizado tanto los ataques de suplantación de identidad para robar credenciales bancarias, el robo de información privada a través de programas maliciosos o a través de su interceptación cuando se usa una red WiFi.

Es por ello, que mediante este proyecto se quiere concienciar a los usuarios de los peligros de las redes WiFi de cuyo gestor no puedan garantizar que vaya actuar siguiendo unas buenas prácticas.

2.3.1 Potenciales ataques aprovechando la estructura de Portal Cautivo

A continuación, se describe brevemente la dinámica de los ataques típicos que se podrían llevar a cabo aprovechando el entorno que se va a tratar en este proyecto, el de los portales cautivos.

2.3.1.1 Man-in-the-Middle (MitM)

Esta configuración de ataque se puede corresponder con la de un portal cautivo gestionado por un ciberdelincuente. MitM [14], como se aprecia en la Figura 2.6, consiste en la interceptación del flujo de datos típico que se da entre dos dispositivos que se están comunicando. En este escenario, el atacante configura su dispositivo como si fuera un router fiable y se aprovecha la confianza de los usuarios.

Mediante los ataques de este tipo el ciberdelincuente puede llegar a cortar el flujo de tráfico, aunque realmente son más funcionales cuando son utilizados para mantenerse a la escucha con el objetivo de robar la información obtenida o para manipular la transferencia de datos.

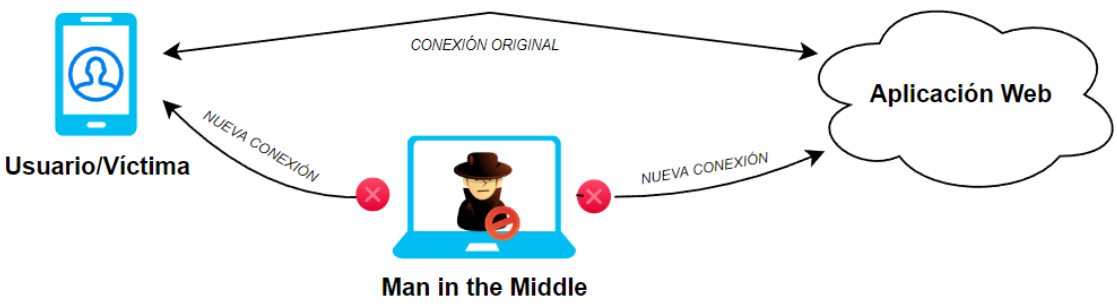

Figura 2.6 Esquema MitM

2.3.1.2 Malware y Ransomware

Este tipo de ataque [15] consiste en la infección del dispositivo de la víctima con un software malicioso. Esta infección se produce cuando el usuario, inconscientemente, instala en su sistema el programa malicioso; siendo por ello típico que su uso esté asociado a otro tipo de ataque que le sirva de vector de propagación.

Cuando un usuario es víctima de este tipo de ataque, su dispositivo infectado verá su seguridad totalmente comprometida. Pudiendo sufrir la denegación del acceso a componentes críticos de su red, el robo de la información que tenga almacenada o malfuncionamiento del sistema e incluso su inutilización.

Una variante de este ataque sería Ransomware. En este caso el delincuente utiliza el software malicioso para encriptar la información que esté almacenada en el dispositivo y pedir a la víctima un pago a cambio de las claves que le permitan restaurarlo.

La implementación de este tipo de ataque en la estructura de un portal cautivo podría integrarse con la aceptación de los requerimientos exigidos al usuario. Al aceptar los mismos, el malhechor podría requerir al usuario la instalación de alguna aplicación maliciosa o podría instalar de forma encubierta el software malicioso que dejaría el terminal de la víctima a su merced.

2.3.1.3 Phishing

El phishing [16] es un tipo de ataque que usa técnicas de ingeniería social para conseguir su objetivo. La mecánica de funcionamiento de este tipo de ataques es sencilla, pero no por ello menos efectiva. Los ataques basan su éxito en hacer creer a la víctima que el mensaje o página web que está visualizando procede de una fuente fiable; entonces, la víctima, albergando su confianza en las buenas prácticas y el buen nombre del remitente que le ha contactado, accede a ejecutar el script malicioso que le han enviado o cede datos privados de los que el malhechor podrá sacar partido.

El modus operandi más típico de este tipo de ataque consiste en el envío masivo de correos electrónicos de apariencia legítima haciéndose pasar por remitentes confiables. Aunque también puede ser llevado a cabo a través de falsas páginas web, mediante el envío de SMS o a través de llamadas telefónicas.

En el caso de su integración en un portal cautivo delictivo, se podría utilizar este tipo de ataque en la página web de bienvenida, de forma que se puede llegar a robar credenciales de usuario y contraseña de redes sociales o correo electrónico de los usuarios que accedan a cederlas con objeto de recibir autenticación y conectarse a la red.

2.3.1.4 DoS y DDoS

Denial-of-Service (DoS) y Distributed Denial-of-Service (DDoS) [17] tienen como objetivo saturar el equipo atacado para que no pueda funcionar adecuadamente. Esta saturación depende del cuello de botella que tenga los recursos de ese equipo, pudiendo ser provocada al superarse el ancho de banda de Internet o las capacidades CPU o RAM, por ejemplo.

DoS y DDoS se diferencian entre sí por la cantidad de hosts que están involucrados en la tarea. Siendo las implementaciones DDoS las más dañinas, puesto que cuentan con mayor cantidad de recursos. En los ataques DDoS es habitual que se haga uso de botnets, redes de ordenadores que han sido infectados con el malware del atacante y que actúan según los designios del delincuente.

Con este tipo de ataques los ciberdelincuentes no obtienen ningún beneficio directo, por lo que su uso se relaciona con actividades de sabotaje empresarial o con métodos de distracción mientras se pertrecha algún ataque de otro tipo.

Su integración en el sistema de portal cautivo no sería directa, si no que los ciberdelincuentes podrían aprovechar el portal cautivo para instalar malware en el terminal de las víctimas. De este modo, los terminales infectados en la sesión del portal cautivo delictivo formarían parte de la botnet que el delincuente podría utilizar para cometer un delito de este tipo.

2.3.2 Situación actual

Para ilustrar mejor la gran magnitud de este problema, se van a exponer una serie de datos bastante llamativos [18]: cada día 30.000 páginas webs son hackeadas, el 64% de las empresas han sufrido al menos un intento de ciberataque, cada 39 segundos en algún punto de la red se está llevando a cabo algún tipo de ataque, diariamente se bloquea el uso de 24.000 aplicaciones móviles maliciosas en las tiendas oficiales, diariamente se producen 23.000 ataques DDoS y el 91% de los ataques utilizan como vector de propagación los mensajes de email.

Centrando la atención en el mundo empresarial, se debe de considerar que el 59% de los ataques se dirigen a las grandes empresas y que el coste promedio de cada violación de la seguridad cibernética en el mundo empresarial es de 3,6 millones de dólares por incidente, incluyendo ese importe las perdidas asociadas a la pérdida de datos, la interrupción del negocio con la pérdida de ingresos que ello conlleva, los costos de notificación o el daño producido en la reputación de la marca. Aunque lo que quizás es más grave, es que de media una brecha de seguridad se tarda en detectar unos 280 días; teniendo en cuenta que las mayores pérdidas se producen durante el primer año desde que sucedió el incidente, de ahí que sus costes sean tan elevados.

Por otra parte, según el reporte de ciberseguridad ofrecido por la compañía Cisco Security[19], en promedio, ocho de cada diez de las herramientas dedicadas a la ciberseguridad activa utilizadas por las empresas comienzan a dar muestras de desactualización y el 39% de las tecnologías que más se suelen utilizar en esas herramientas ya no ofrecen garantías por estar anticuadas. Por lo tanto, es necesario que se siga aumentando la inversión en ciberseguridad para tratar de evitar los ataques o al menos detectarlos lo antes posible y minimizar sus costes asociados. Sin embargo, a tenor de la información extraída del Global Risks Report 2022 del WEF [12], el 95% de los problemas que atentan contra la ciberseguridad son debidos a fallos humanos. Es por ello, que se debe destinar mayor cantidad de recursos a la concienciación en cuanto a los protocolos de ciberprotección.

Saliendo del mundo empresarial las cifras siguen siendo graves, pero son algo más alentadoras. En cuanto al número de ataques a teléfonos móviles[20], en la Figura 2.7 se puede apreciar el gran repunte que se vivió durante el mes de marzo de 2019, con casi 8,1 millones de dispositivos siendo atacados; pero, desde entonces las cifras fueron decayendo hasta los algo menos de 2,3 millones en diciembre de 2021.

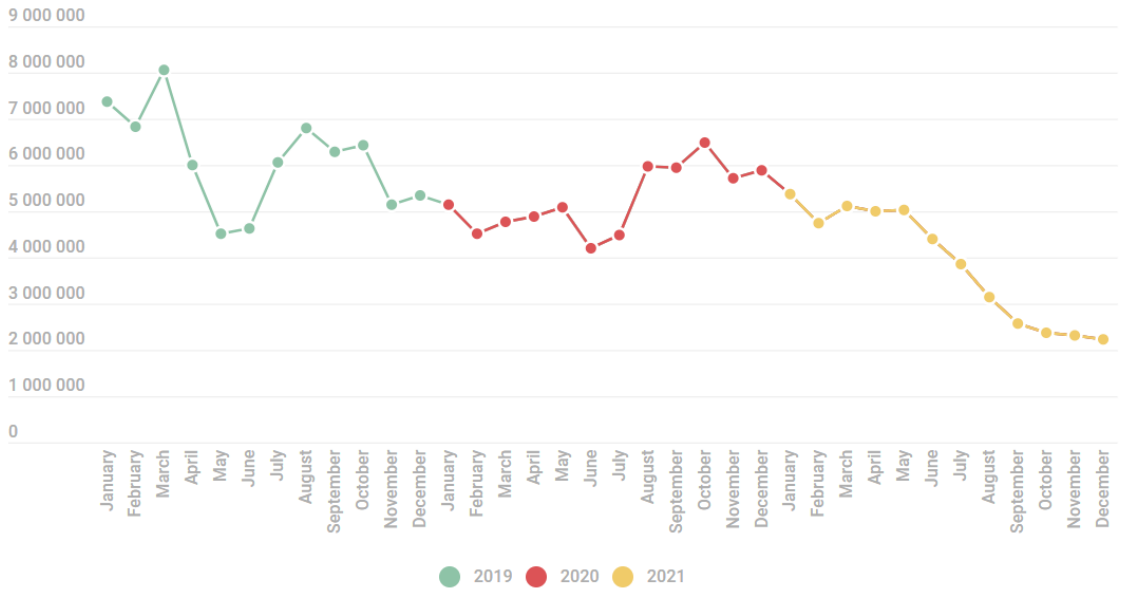

Figura 2.7 Estadística del número de ataques sobre teléfonos móviles en el periodo 2019-2021[20]

Aún con esta caída el riesgo sigue siendo muy real. En este tipo de dispositivos el modelo de ataque más habitual es el phishing y es por ello que los usuarios deben de estar atentos para evitar caer en la trampa. Puesto que, como se mencionó previamente, ser víctima de este tipo de ataque podría dar lugar a la cesión de datos personales o la instalación de algún tipo de malware. En cuanto a los ataques de tipo malware que más se implementaron el pasado 2021, en la Figura 2.8 se puede apreciar la predominancia de AdWare y RiskTool, dedicándose el primero a mostrar pop-ups con anuncios en la interfaz de usuario del dispositivo y el segundo roba los datos de ubicación. Se observa que Irán (40.22%), China (28.86%) y Arabia Saudita (27.99%) son los países en que mayor porcentaje de usuarios se encontraron siendo víctimas de amenazas móviles. Sin embargo, a pesar de no estar en las posiciones de cabeza en los datos totales de las víctimas de ciberataques, los ciudadanos españoles no debemos despreocuparnos. España se encuentra en el segundo puesto mundial de los países cuyos ciudadanos han sufrido ataques contra la seguridad de sus cuentas bancarias, siendo atacada un 1.55% de la población, solo por detrás de la ciudadanía japonesa con un 2,18%.

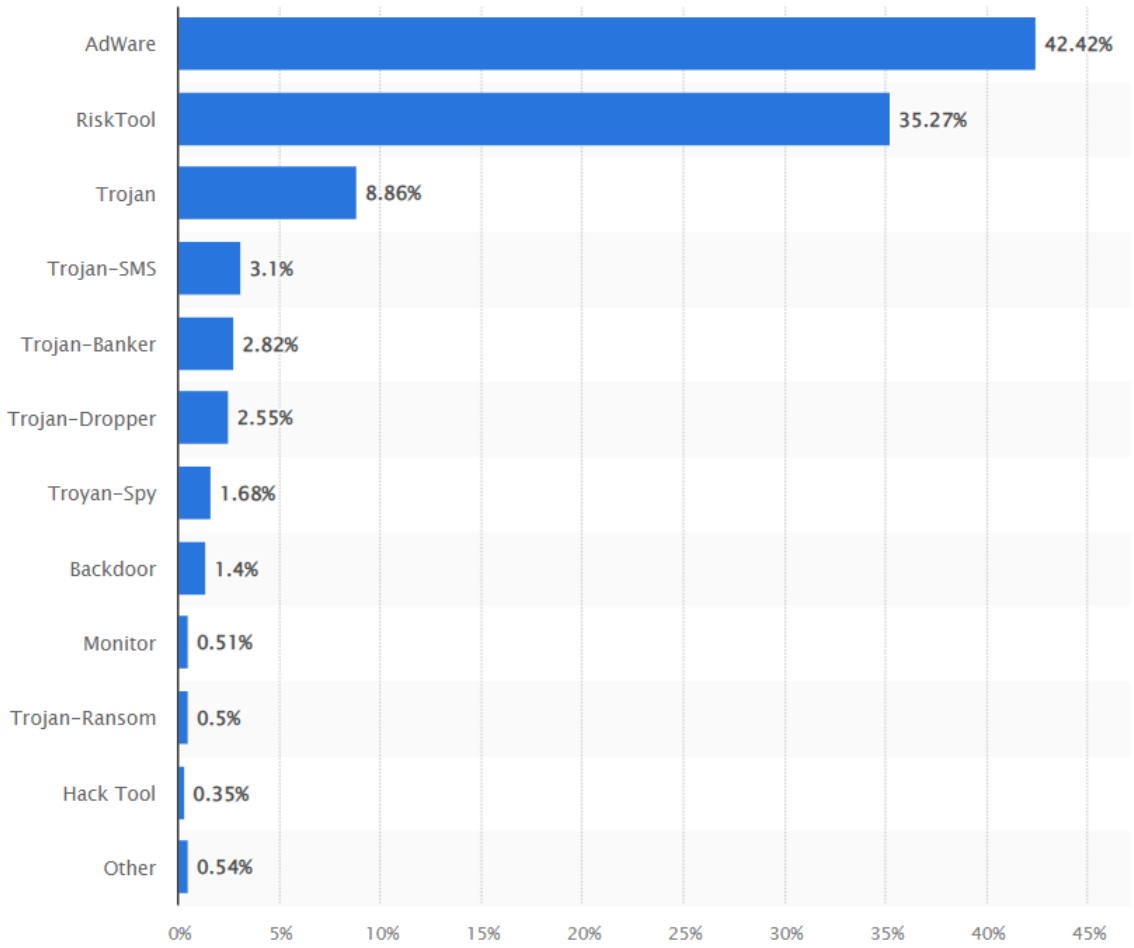

Figura 2.8 Distribución de ataques Malware a dispositivos móviles en el año 2021 [21]

En cuanto a la seguridad de los usuarios que se conectan a las redes WiFi[22], uno de los temas que se desea abordar en este proyecto, un estudio reciente determinó que un 78% de la población mundial busca activamente redes WiFi públicas, y que el 72% de esas personas se conectan a ellas sin tener en cuenta la seguridad de la red. Sin embargo, los usuarios deben tener en cuenta que la privacidad de su sesión puede ser vulnerada; los atacantes pueden aprovechar una mala configuración de red para cometer su actividad o que la vulneración se produzca porque la red en sí misma está gestionada por un ciberdelincuente.

En cuanto al primer caso, que la configuración de la red no haya sido realizada de manera adecuada, los errores típicos que suelen cometer los gestores de red son ofrecer el servicio sin que se haya modificado el SSID o la contraseña predeterminada (según una encuesta realizada por la empresa Broadband Genie [23], el 48% de los usuarios no había cambiado ninguna configuración de su router), dejar el router está en un lugar accesible para el atacante o hacer uso de un protocolo vulnerable, como lo es WEP. Este mal proceder facilita que el agresor se pueda hacer con el control del router, pudiendo con ello cambiar su configuración o el firmware, cargar scripts maliciosos o modificando el servidor DNS. Sin embargo, en el caso del protocolo, a pesar de que se haya utilizado un protocolo más seguro, como lo es WPA, esta configuración también tiene sus propias vulnerabilidades, las cuales pueden llegar a ser explotadas mediante ataques de tipo KRACK[6], en los que se aprovecha el momento del saludo a cuatro bandas para obtener la clave de cifrado de tráfico.

En cuanto a la segunda casuística referida, es decir, que el gestor de la red sea el propio delincuente, se puede dar que el gestor establezca un punto de acceso y que simplemente se dedique a capturar el tráfico de quienes se conecten a él, llevando a cabo con esto, un ataque MitM. Una variación de este ataque sería el llamado gemelo malvado. En este caso se lleva a cabo la configuración de un ataque MitM en el que además se aprovecha el nombre del establecimiento o lugar público en el que se esté para elegir el SSID. Otra opción plausible es que ese punto de acceso fuera configurado inicialmente por un gestor bienintencionado, pero que tras sufrir un ataque de tipo malware haya pasado a estar gestionado por un delincuente. Este segundo caso de ataque es más común de lo que se podría imaginar, siendo, por ejemplo, el responsable de la creación de la red de bots Mirai que llegó a acumular más de 200.000 dispositivos para perpetrar el mayor ataque DDoS visto hasta la fecha[23].

Finalmente, otro tema que llegados a este punto es interesante tratar es la aceptación de términos y condiciones. Este requerimiento es una práctica habitual, que todo usuario tiene que llevar a cabo cuando navega por Internet, descarga aplicaciones o actualiza el sistema operativo de su dispositivo. Habitualmente, esos términos y condiciones suelen hacer referencia a requerimientos típicos para el correcto funcionamiento del servicio. Sin embargo, se da el caso de organizaciones que establecen políticas de uso abusivas. En este caso, está claro que el usuario cuando lee

esas políticas las rechaza y utiliza otro servicio, pero ¿y si no las lee? Pues este es el caso más habitual.

Según una encuesta realizada a los ciudadanos estadounidenses por la consultora Deloitte el pasado 2017, el 91% de los encuestados aceptaban los términos y condiciones sin leerlos, llegando esa cifra al 97% cuando los encuestados tenían entre 18 y 34 años [24]. Otro estudio muy llamativo fue el realizado por la organización ProPrivacy.com. En este caso se ofreció una recompensa económica a los usuarios que participaran en un estudio de mercado para cuya realización tenían que aceptar unos términos abusivos. Se determinó que, de 100 usuarios, solo 19 pincharon en los términos y condiciones y de esos 19, solo uno leyó lo suficiente como para darse cuenta de las cláusulas abusivas que estaría aceptando [24].

Pero si es tan fácil caer en el engaño y casi todo el mundo cae, ¿qué pueden significar estas cláusulas? Cuando un usuario acepta estos documentos, su aprobación es legalmente vinculante. Es por ello que hay que asegurarse de leer y entender lo que se está requiriendo, puesto que con su aceptación podría estar consintiendo a una empresa el que pueda vender su información personal a terceros, rastrear sus movimientos haciendo uso de las capacidades de rastreo que tengan disponibles, recopilar identificadores de su dispositivo o rastrear la dirección u otros identificadores digitales.

Capitulo 3. DISEÑO Y ARQUITECTURA DEL SISTEMA

Atendiendo a la importancia que tiene la seguridad en las redes y la poca consideración en que se la suele tomar, se ha diseñado este proyecto con el objetivo de concienciar a la población del peligro de los puntos de acceso públicos que pueden encontrarse en su vida cotidiana.

Con este fin, se plantea el diseño y despliegue de un entorno de punto de acceso con portal cautivo donde los usuarios sufrirán un ataque de suplantación de red WiFi segura y conocida. Es decir, se habilitará un acceso a Internet a través de dicho portal cautivo tras aceptar unos términos y condiciones del sistema abusivos y se capturará el tráfico transmitido durante un periodo de tiempo. Posteriormente, se les revocará los derechos de acceso informando de la brecha de seguridad que ha sufrido su privacidad. Finalmente, a título informativo y educativo, se mostrarán los datos extraídos de su sesión y se expondrán unas buenas prácticas a tener en cuenta para garantizar conexiones a Internet lo más seguras posibles.

3.1 CASO DE USO

Un usuario malicioso desea obtener información sensible de los otros usuarios a través de los datos que éstos transmiten desde sus dispositivos inalámbricos. Este atacante busca un lugar público (plaza, centro de estudios, etc.) en el que desplegar su hotspot, al que dotará de unas características que le hagan atractivo y confiable, con el fin de atraer al máximo número de usuarios. Cualquier usuario que busque una red inalámbrica a la que conectarse, descubrirá la red WiFi desplegada por el usuario malicioso, y considerando el atractivo y familiar nombre de la misma, se conectará a dicha red. Por ejemplo, un atacante en el entorno de la Universidad de Cantabria (UC) utilizará un SSID igual o similar al de otras redes existentes en la UC.

Una vez el usuario se conecte, y a fin de cumplir con la normativa legal en términos de protección de datos, etc. se redirige la conexión a una página web informativa en la que se pide se acepten los términos y condiciones de uso de la conexión, concediendo el acceso tras la confirmación de aceptación. Como suele ser habitual, el usuario no leerá los términos y condiciones de uso en los que se detalla que se trata de una red experimental y que el tráfico que circule a través de ella será capturado y analizado con fines formativos. Desde ese momento, el despreocupado usuario ya ha caído en la trampa y se encuentra en medio de un ataque tipo MitM.

Al ser este el esquema de un ataque con motivo educativo, tras recopilar información, se corta el acceso a Internet y se notifica al usuario del engaño. Mediante

esa notificación se informará de los datos que se podrían haber sustraído en caso de las intenciones hubieran sido otras, se informará de los peligros de este tipo de redes y se expondrán una serie de buenas prácticas que permiten prevenir el volver a caer en un ataque de este tipo.

A este ataque MitM, los ciberdelincuentes podrían añadir un nuevo vector de captación ilícita de datos, llevando a cabo un ataque de phishing. Su implementación sería tan sencilla como que en la página de bienvenida se requiriesen datos de usuario y contraseña de alguna red social o correo electrónico. De este modo, el gestor del portal cautivo delictivo no solo se haría con los datos de la sesión de las víctimas, si no que posiblemente también contaría con información acerca de sus cuentas y contraseñas. Sin embargo, al tener este proyecto una vocación docente, esta posibilidad no será implementada puesto que, aunque cometer este acto delictivo podría reforzar el punto que se está tratando, desembocaría en una transgresión a la privacidad de las víctimas demasiado grave.

Otro ciberataque que podría combinarse con el descrito en el caso de uso es la implementación de algún tipo de malware. En este caso, se podría requerir la descarga de algún tipo de software malicioso para cumplir con los requisitos de acceso o se podría aprovechar la aceptación de los términos y condiciones de la página de bienvenida para descargar en paralelo en el terminal de la víctima ese malware. Sin embargo, por los mismos motivos a los que se ha aducido en el supuesto anterior, no se ha valorado llevar a cabo este ataque.

Por último, también se debe de considerar la posibilidad de inyectar algún tipo de malware en las etiquetas NFC o códigos QR utilizados para facilitar la configuración de la red. Estas tecnologías podrían ser utilizadas para que tras su escaneo sugirieran la descarga de alguna aplicación “necesaria” para conseguir acceso a Internet a través del portal cautivo. De este modo, se podría engañar a los usuarios para que descargaran esa aplicación corrupta e infectaran su dispositivo con malware. Igual que se mencionó en las dos posibilidades anteriormente descritas, tampoco se ha valorado llevar a cabo esta configuración de ataque.

3.2 REQUERIMIENTOS FUNCIONALES

Ateniéndose al escenario expuesto previamente para analizar los requerimientos funcionales, existen dos entidades bien diferenciadas. De una parte, se encuentra el prestador de servicio, en este caso el gestor del portal cautivo malintencionado. De otra, se encuentra el usuario final, en este caso la víctima. Adicionalmente se considera que la solución final, al tener vocación pedagógica, se podrá desplegar en diversos entornos, como pueden ser centros de estudios o actos en los que se quiera tratar el tema de la seguridad en la red.

3.2.1 Requerimientos del atacante

La necesidad principal del atacante es disponer de la capacidad de crear un sistema que sea capaz de proveer de conexión a Internet a otros usuarios actuando como un punto de acceso. Para este proyecto, el proceso deberá de ser realizado a través de la correcta configuración del hostapd, la dnsmasq, el servidor DHCP y el firewall, es decir, sin hacer uso de software de terceros.

Además, se deberá de ampliar las capacidades de ese sistema inicial añadiendo la funcionalidad de portal cautivo. La cual deberá de ser implementada a través de la creación de un host virtual propio y el resto de dependencias que resulten necesarias. Este sistema deberá de tener la capacidad de conseguir que los usuarios que busquen acceso a Internet sean redirigidos a la página de bienvenida, gestionar su acceso a la red y a su vez, gestionar también su desconexión y redirección a una página de concienciación. Siendo todas estas tareas realizadas con el máximo grado de automatización posible.

Por último, se requiere que este sistema de punto de acceso con portal cautivo cuente con capacidades de análisis de tráfico. Para ello, en el resultado final de este proyecto se deberá de incluir procesos en los que se capture, se procese y se generen gráficas del tráfico que permitan visualizar el desarrollo de la sesión de cada usuario de manera sencilla.

Adicionalmente de los requerimientos técnicos planteados, la solución debe de tener un coste ajustado y fácil portabilidad para permitir su implementación en cualquier charla de concienciación. Siguiendo en la línea de la portabilidad, el sistema deberá de seguir el paradigma plug-and-play, de modo que el procedimiento de inicialización sea lo más sencillo y rápido posible.

En términos generales, lo requerimientos en cuanto al entorno del atacante se pueden resumir en configuración del sistema sin hacer uso de programas que provean el servicio automáticamente, capacidad de análisis de la información recabada, despliegue total con precio ajustado y portabilidad.

3.2.2 Requerimientos del usuario

El usuario es quien en principio se “beneficiará” de los servicios prestados por el atacante. Actuará como víctima durante el periodo de su sesión y podrá acceder al uso de Internet bajo las condiciones impuestas por el prestador de red. Es decir, tendrá acceso a Internet mientras que el tráfico que genere es capturado y analizado.

Este proyecto está ideado con el objetivo de concienciar a los usuarios de redes WiFi de uso libre; es por ello que teniendo en cuenta el perfil típico de los usuarios de este tipo de servicio, quizás sea más útil en charlas de concienciación en institutos o

universidades. Sin embargo, eso no quiere decir que no pueda ser utilizado en entornos compuestos por usuarios de otras edades. En definitiva, basta con que el usuario disponga de un dispositivo móvil y la intención de conectarse a la red WiFi.

Para maximizar el número de participantes de la actividad que hagan uso del servicio propuesto se debe de incitar su uso. Para ello, se deberán de utilizar estrategias que faciliten la conexión. Es decir, el sistema debe de contar con funcionalidades que posibiliten la configuración automática de la red a través del uso de códigos QR y etiquetas NFC. De tal modo, que el atacante pondrá todas las facilidades posibles a la víctima para que acceda a ingresar en la red.

Por otra parte, al ser este un sistema con vocación educativa, se deberá de garantizar que los datos recabados de las sesiones de los usuarios no serán utilizados con otro fin que no sea la concienciación del propio usuario.

En definitiva, los requerimientos en cuanto al usuario final son el acceso a la red de forma sencilla y rápida y garantizar la privacidad de su sesión una vez se haya desarrollado la actividad.

3.3 ARQUITECTURA FUNCIONAL

En la Figura 3.1 se muestra la arquitectura de la solución que se plantea para dar respuesta a los requerimientos previamente mencionados. Este sistema consta de los siguientes elementos:

- Cliente: Es el dispositivo del usuario/víctima que se ha conectado al punto de acceso generado por el dispositivo malicioso, recibe conexión inalámbrica y hace uso de la misma mientras sus datos son recabados.

- Dispositivo malicioso: Es el dispositivo de la red al que se conectan inalámbricamente los usuarios y recibe conexión a Internet a través del router privado. Este dispositivo se ha configurado a modo de router WiFi con portal cautivo para gestionar el acceso de los usuarios. Además, sin que sea obvio para el cliente, también tiene configuradas las capacidades de captura, análisis y generación de métricas de los datos de quienes hagan uso de sus servicios.

- Router Privado: Es el dispositivo que provee de conexión de red al dispositivo malicioso, la conexión de ambos elementos se lleva a cabo a través de un cable de Ethernet.

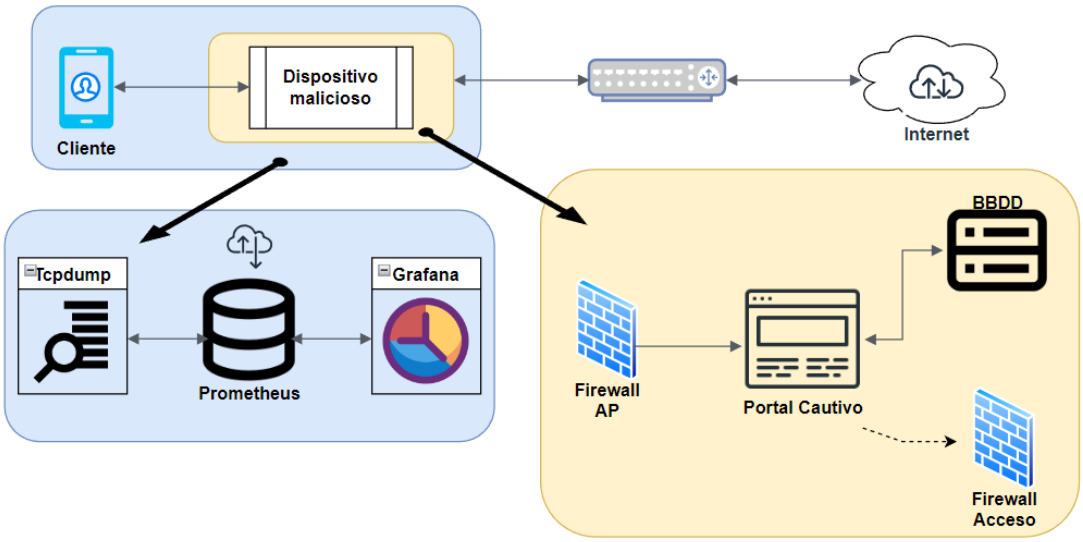

Figura 3.1 Esquema Arquitectura Funcional del sistema final

Capitulo 4. DESPLIEGUE DE LA SOLUCIÓN

En este capítulo se va a desarrollar la configuración tanto hardware, como software que da respuesta a las necesidades requeridas por este proyecto. Para ello, primero se tratará el dispositivo Raspberry Pi que se va a utilizar como dispositivo malicioso y en el que se configura el software para que funcione como un portal cautivo delictivo. Tras esto se describen los temas relacionados con la configuración que permite su desempeño de tal modo, englobando la configuración del punto de acceso, implementación del portal cautivo, integración de metodologías alternativas de conexión con la red y configuración del sistema de captura, análisis y generación de gráficas del tráfico.

4.1 DISPOSITIVO HARDWARE

Para la implementación de este proyecto se ha buscado que los elementos requeridos para su correcto funcionamiento resultaran económicos y que el resultado final fuera portable. Es por ello que su configuración software se ha realizado haciendo uso de software libre y que el dispositivo que sobre el cual se va a aplicar dicha configuración sea una Raspberry Pi 3b.

Este dispositivo es reconocido por proporcionar un entorno hardware con prestaciones bastantes buenas a un coste bastante reducido. Además, en caso de que fuera necesario para facilitar su portabilidad, se podría añadir una batería que eliminaría la dependencia de las tomas de corriente eléctrica. Para mejorar aún más su portabilidad, se podría conectar al proveedor de Internet a través de una de sus interfaces WiFi, mientras que usa otra para actuar como punto de acceso.

La Raspberry 3B se trata de una placa con un Chipset Broadcom BCM2837 que trabaja con un procesador ARM Cortex-53 de 64 bits, 4 núcleos y con una frecuencia máxima de trabajo de 1,2 GHz. Además, cuenta con una memoria RAM de 1Gb del tipo DDR2 y una ranura para insertar una tarjeta SD de capacidad suficiente para cargar un Sistema Operativo en el dispositivo. En el caso de este proyecto se ha optado por instalar Raspbian.

Raspbian es una distribución GNU/Linux basada la distribución Debian y optimizada específicamente para el hardware Raspberry Pi. Es la distribución que mejor optimiza los recursos de la Raspberry y su uso ofrece mejoras en el rendimiento del sistema al dar soporte optimizado para cálculos en coma flotante por hardware. Además, contiene un repositorio de programas descargables que asemeja su funcionalidad, guardando las distancias en términos de potencia, a la de los ordenadores convencionales.

Para poder configurar la Raspberry como un punto de acceso inalámbrico se hace uso del puerto Ethernet y de la antena WiFi-integrada, la cual soporta los estándares 802.11 b/g/n.

4.2 CONFIGURACIÓN DEL PUNTO DE ACCESO

Para dar conectividad a la Raspberry Pi se puede hacer uso de la interfaz WiFi o de la interfaz de Ethernet. Configurar la conexión a través de la interfaz WiFi tiene como ventaja que el punto de acceso ganaría en portabilidad. Sin embargo, al configurarlo de manera cableada el ancho de banda es mayor. Por tanto, al querer utilizar esta configuración en una situación en la que recibirá multitud de usuarios, se ha optado por usar la interfaz de Ethernet. Una vez resuelta esa parte, para convertirla en un punto de acceso inalámbrico es necesario instalar y configurar el software necesario.

Este software, que habilita el funcionamiento como un router inalámbrico [25], incluye los servicios hostapd, DNSmasq, el servidor DHCP y las reglas específicas para el redireccionamiento de tráfico. Seguidamente se describen cada uno de ellos y se justifica su necesidad.

4.2.1 Configuración de Hostapd

Hostapd es un software que permite que una tarjeta de interfaz de red pueda actuar como punto de acceso y servidor de autenticación.

Mediante la configuración del archivo de configuración de Hostapd se genera el punto de acceso inalámbrico y se establecen los parámetros de configuración de la red.

Para generar la estructura de este punto de acceso se debe de configurar el archivo hostapd.conf como se ve en la Figura 4.1. En él, se optó por nombrar la red inalámbrica que se iba a generar mediante el SSID WiFiJRG y se dotó de cierta seguridad a las transferencias de datos llevadas a cabo dentro de ella a través del algoritmo WPA2 con cifrado de clave WPA-PSK.

```
interface=wlan0
driver=nl80211
ssid= WiFiJRG
hw_mode=g
channel=6
wmm_enabled=0
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
wpa_passphrase=password
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
```

Figura 4.1 Configuración del archivo hostapd.conf

A continuación, se debe establecer esta configuración como la predeterminada del sistema para que se inicie automáticamente y finalmente ya se podría habilitar este nuevo servicio.

4.2.2 Configuración de DNSmasq y el servidor DHCP

Una vez se ha creado la estructura del punto de acceso, se le debe de otorgar la capacidad de proporcionar direccionamiento a los usuarios que se conecten. Esto se consigue a través de la configuración de la DNSmasq y del servidor DHCP.

DNSmasq es un software gratuito que proporciona un servidor DNS, un servidor DHCP y funciones de arranque de red. Su diseño está optimizado para consumir pocos recursos, por lo que su uso está muy recomendado cuando se quiere administrar una red a través de un dispositivo con recursos limitados, como es el caso.

Para llevar la configuración del servicio DNSmasq de este proyecto se ha editado el archivo dnsmasq.conf . En él, se ha configurado que el punto de acceso escuche el tráfico a través de la interfaz wlan0, que no responda satisfactoriamente las consultas DNS no reconocidas por /etc/hosts o el servidor DHCP y que el servidor DHCP conceda direcciones IP en el rango 192.168.42.100-200 con una validez de 12 horas.

Tras esto, hay que configurar el servidor DHCP, que es un demonio o proceso propio de la arquitectura Linux que configura dinámicamente las sesiones TCP/IP de los clientes de una red.

En el sistema que se está desarrollando, este servidor se configuró añadiendo los parámetros que se muestran en la Figura 4.2 al final del archivo dhcpcd.conf. Con estas líneas se indica al servidor DHCP que su interfaz de escucha es wlan0 y, para que la Raspberry pueda funcionar como un servidor, se declara su IP estática propia y la IP en la que responde como router.

```
nohook wpa_supplicant
interface wlan0
static ip_address=192.168.42.10/24
static routers=192.168.42.1
```

Figura 4.2 Configuración del archivo dhcpcd.conf

4.2.3 Configuración del firewall

Con la configuración actual es posible ver desde un dispositivo externo que se ha creado el punto de acceso. Sin embargo, este no es capaz de llevar a cabo las acciones que se le presupone. Antes de que actúe como un verdadero hotspot hay que habilitar el enrutamiento y configurar el firewall.

Al habilitar el enrutamiento se permite la transferencia de datos de comunicación entre la LAN y WAN, de modo que se provee de una salida a Internet a los dispositivos de la red WiFi. Para habilitar esta función hay que editar el archivo sysctl.conf y habilitar la siguiente sentencia: `net.ipv4.ip_forward=1`

Con esto, solo quedaría por configurar el firewall con una regla de enmascaramiento, de modo que las direcciones IP de los usuarios del punto de acceso sean sustituidas por la dirección IP de la red de área local que se ha generado.

La configuración de este firewall se ha realizado en el script firewall.sh, el cual está representado en la Figura 4.3. Una vez hecho esto, ya es posible conectarse a la red WiFi y los usuarios podrán hacer un uso funcional del punto de acceso.

```
#!/bin/sh
#Clear all rules
iptables -F
iptables -t nat -F
iptables -t mangle -F

#Whitelist mode
iptables -P INPUT ACCEPT
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

#Masquerade rule
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Figura 4.3 Configuración del Firewall para un punto de acceso

4.3 IMPLEMENTACIÓN DEL PORTAL CAUTIVO

Tras configurar el punto de acceso, toca añadir ciertos elementos al sistema y realizar algunas modificaciones en la configuración ya realizada. Se debe modificar el código del firewall y configurar un servidor LAMP.

Los cambios en el firewall tienen como objetivo cortar el acceso libre de los usuarios a la red y reenviar el tráfico saliente de los usuarios del portal cautivo a la dirección IP en la que se aloja la página web de bienvenida generada a través del servidor LAMP.

4.3.1 Reconfiguración del firewall

Como se ha indicado previamente, con la configuración de firewall actual se está redireccionando el tráfico saliente de los usuarios al destino que desean. Sin embargo, esto no puede ser así si se quiere llevar a cabo una estructura de portal cautivo.

Con el objetivo de cumplir con los requerimientos de este caso, las reglas del firewall deben de redireccionar el tráfico a la dirección IP en la que se alberga la página web de bienvenida. Para que una vez en allí, según si cumplen o no con los requerimientos que se soliciten al usuario, se vuelvan a modificar (o no) las reglas del firewall vigentes para ese dispositivo.

Centrando más la atención en el procedimiento utilizado, de lo que se encargan de hacer las líneas añadidas a este script, representado en la Figura 4.4, es lo siguiente. Primero se habilita el tráfico HTTP y HTTPS para los usuarios del punto de acceso. Tras esto, se redirecciona todo el tráfico HTTP y HTTPS que llega al firewall, definidos por su puerto destino (80 y el 443 respectivamente), a la dirección IP del portal cautivo. Finalmente, se habilita el enmascaramiento del tráfico para que puede ser reenviado a esa nueva dirección y se establece el estado de la conexión.

```
#!/bin/sh
#Clear all rules
iptables -F
iptables -t nat -F
iptables -t mangle -F

#Whitelist mode
iptables -P INPUT ACCEPT
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

#Redirect all traffic to captive portal
iptables -t nat -A PREROUTING -i wlan0 -p tcp -m tcp --dport 80
-j DNAT --to-destination 192.168.42.10:80
iptables -t nat -A PREROUTING -i wlan0 -p tcp -m tcp --dport 443
-j DNAT --to-destination 192.168.42.10:80

#Allow HTTP/HTTPS for WiFi clients
iptables -A FORWARD -j ACCEPT

#Allow NAT
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A FORWARD -i eth0 -o wlan0 -m state --state
RELATED,ESTABLISHED -j ACCEPT
```

Figura 4.4 Configuración del Firewall para un portal cautivo

4.3.2 Configuración del servidor LAMP

Con el firewall ya programado para que redireccione el tráfico a la dirección en la que se albergará la página de bienvenida. Toca crear esa página de bienvenida y el código que hará que los mecanismos de detección de portales cautivos lo reconozcan como tal y generen la petición al puerto 80 o al 443.

Para entender el funcionamiento de este sistema hay que tener en cuenta que los dispositivos cuando entran en rango de una red inalámbrica, con la opción de búsqueda de redes WiFi activada, mandan automáticamente un paquete de reconocimiento a la red para ver de qué tipo es esta. En caso de que la red esté configurada como un portal cautivo, responde de tal manera que el dispositivo la reconoce como tal y lanza un aviso al usuario de la posibilidad de conectarse a la red.

Para llevar a cabo esta configuración, se va a hacer uso de un servidor LAMP. El servidor LAMP recibe este nombre debido al acrónimo formado con las iniciales de las herramientas que suelen componerle: El sistema operativo Linux; un Servidor Web, en este caso se hace uso del servidor Apache; un gestor de bases de datos, que para esta implementación se hace uso de MariaDB; y el/los lenguajes de programación que se vayan a utilizar en el sistema.

Esta combinación de programas, en origen, no fue ideada para trabajar en conjunto. Sin embargo, al ser soluciones de código abierto y estar preinstalados al descargar cualquier distribución de Linux, la combinación es muy popular.

Para llevar a cabo la configuración del servidor LAMP, el paso inicial consiste en comprobar que se cuenta con los programas necesarios descargados y en caso de no ser así, descargarlos. En el caso que ocupa este proyecto, estas utilidades son el servidor web Apache 2, el gestor de base de datos MariaDB y los lenguajes de programación PHP y Bash.

Una vez descargados los paquetes correspondientes se debe de crear la estructura de directorios /var/www/html/wifijrg.com, que, en este caso, recibe este nombre porque así es como se va a llamar el host virtual. En este directorio se alojan los archivos escritos en código PHP en los que se describen las páginas webs (inicio, conexión establecida y política de uso) propiedad del usuario www-data a las que se redirecciona a los usuarios del portal cautivo, y cuyo contenido se desarrollará más adelante.

Antes de desarrollar el contenido de los recursos almacenados en el directorio /var/www/html/wifijrg.com, se debe de tratar la configuración del servidor Apache. Para este proceso de configuración, el paso inicial consiste en crear un archivo override.conf (Figura 4.5) en el directorio /apache2/conf-available/ . Este elemento estipula a través de una serie de parámetros la manera en que se van a regir los archivos del servidor. En el apartado Options se habilita la opción Indexes para que si se intenta acceder a un directorio que no tenga un DirectoryIndex se muestre el contenido del directorio; FollowSymLinks permite que Apache use enlaces simbólicos y Multiviews permite mostrar una página distinta en función del navegador. El apartado AllowOverride All permite que el archivo anule los parámetros de configuración prestablecidos. Con el apartado Order Allow,Deny se prohíbe el acceso a este archivo. Por último, el apartado Allow from all permite que los usuarios se conecten a las páginas del servidor desde cualquier red.

```
<Directory /var/www/>
    Options Indexes FollowSymLinks MultiViews
    AllowOverride All
    Order Allow,Deny
    Allow from all
</Directory>
```

Figura 4.5 Configuración del archivo override.conf

Siguiendo con la configuración del servidor Apache [26], hay que establecer los parámetros del host virtual. En este caso, el dominio que se va a generar es wifijrg.com; y para ello hay que crear un archivo de configuración con el nombre del host, en este caso este archivo es wifijrg.com.conf, en el directorio /etc/apache2/sites-available/ .

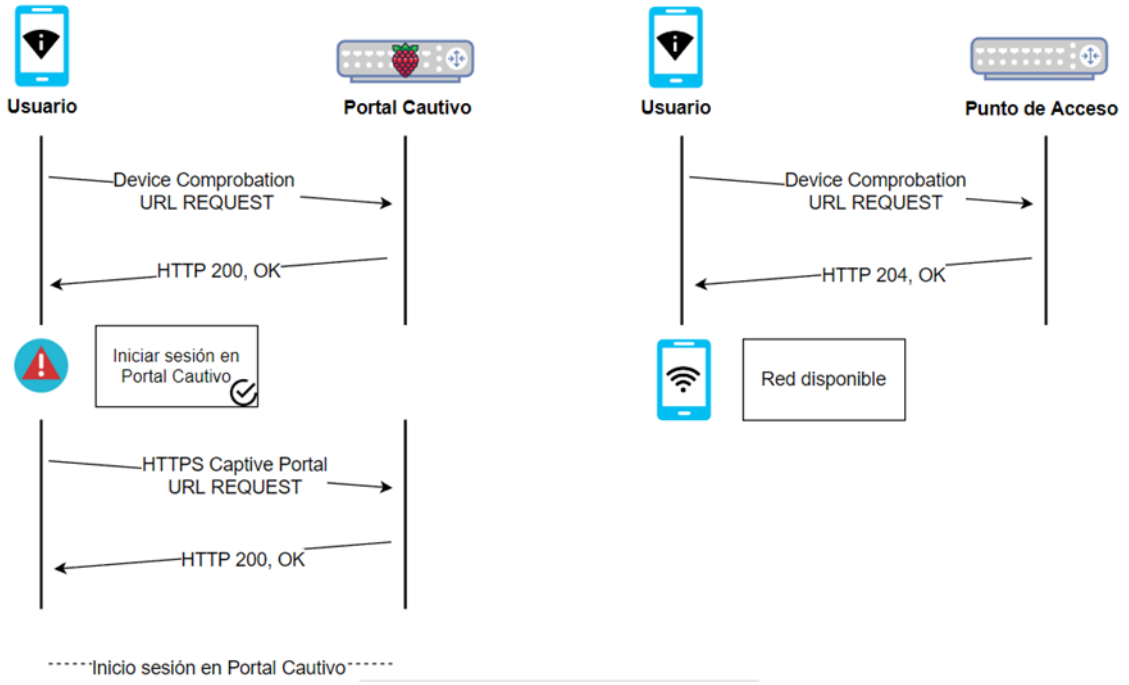

Figura 4.6 Esquema del mecanismo de detección de portales cautivos (CPD). A la izquierda se muestra la detección de un Portal cautivo y a la derecha la detección de un punto de acceso convencional

En la configuración de la Figura 4.7 se introducirán los mecanismos que posibilitarán que los dispositivos puedan detectar automáticamente la existencia del portal cautivo. Entrando un poco más en detalle en la metodología antes explicada, el CPD del dispositivo del potencial usuario basa su funcionamiento en la verificación del tipo de red a la que se corresponde el punto de acceso que está detectando (Figura 4.6). Para ello, este mecanismo de detección envía una petición a una URL específica y espera recibir un resultado conocido a través de una respuesta HTTP. Si la petición es resuelta con un resultado conocido mediante una respuesta HTTP 204, el dispositivo detecta que tiene acceso pleno a Internet puesto que la red es un punto de acceso; en caso contrario, si recibe una respuesta HTTP 200, detecta la existencia del portal cautivo y abre la página de bienvenida automáticamente.

Esta es la estrategia típica que suelen utilizar todos los dispositivos para resolver si la red que han detectado es un portal cautivo o no. Sin embargo, la URL a la que realizan la consulta inicial varía en función del SO del dispositivo que el usuario esté utilizando. Es por ello que en la configuración del host virtual se definen distintas opciones de Redirect, tratando de este modo que la detección automática funcione con el máximo de dispositivos posibles[27]. Las URL a las que se redirecciona en este proyecto son: /library/test/success.html y /hotspot-detect.html para los dispositivos de Apple; /ncsi.txt, /connecttest.txt y /fwlink/ para los dispositivos de Windows; y /generate_204 para los dispositivos Android.

El resto de la configuración indica que el servidor Apache escucha por el puerto 80 y que en el directorio /var/www/html/wifijrg.com se permite que se anulen los parámetros de configuración prestablecidos. Tras esto, se añaden las directivas que identifican al administrador del servidor, el nombre del dominio base, los nombres adicionales con los que debería de coincidir como si fuesen el nombre base y la ubicación raíz del dominio. Finalmente, hay dos directivas que indican el funcionamiento en caso de error.

```
<VirtualHost *:80>

        <Directory "/var/www/html/wifijrg.com">
                AllowOverride All
        </Directory>

        ServerAdmin xxxx@xxx.xx
        ServerName wifijrg.com
        ServerAlias www.wifijrg.com
        DocumentRoot /var/www/html/wifijrg.com

        Redirect /library/test/success.html http://192.168.42.10/index.php
        Redirect /hotspot-detect.html http://192.168.42.10/index.php
        Redirect /ncsi.txt http://192.168.42.10/index.php
        Redirect /connecttest.txt http://192.168.42.10/index.php
        Redirect /fwlink/ http://192.168.42.10/index.php
        Redirect /generate_204 http://192.168.42.10/index.php
        RewriteEngine on
        RewriteCond %{HTTP_USER_AGENT} ^CaptiveNetworkSupport(.*)$ [NC]
        RewriteRule ^(.*)$ http://192.168.42.10/index.php [L,R=301]

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
```

Figura 4.7 Configuración parámetros del host virtual

Para finalizar con la configuración de Apache se debe de dar permisos al directorio /var/www/html/wifijrg.com y habilitar los nuevos archivos de host virtual que se han configurado.

Una vez configurado el servidor Apache, se debe generar los contenidos que se van a mostrar a través de él y los procesos que debe de realizar. Es decir, es el momento de generar la estructura web de este sistema; la cual consiste en una página de bienvenida, una página que muestra los términos y condiciones del sistema, otra que gestiona el acceso a Internet y, por último, una página que emite un mensaje de bienvenida al usuario.

En la página de bienvenida, conocida como index.php, se recaban y guardan automáticamente en una base de datos MariaDB los siguientes datos del usuario: userid (valor generado por el sistema), IP, MAC, hora (hora del sistema cuando el usuario accedió al portal de bienvenida) y conectado (elemento de control de acceso

cuyo valor por defecto es 0). En esta página de bienvenida se da la posibilidad de que el usuario sea redireccionado a otra URL en la que podrá leer los términos y condiciones del servicio. Finalmente, en caso de que haya leído las condiciones de acceso y quiera conectarse o que por defecto los haya ignorado, cuenta con un botón a través de cuya pulsación se considerarán aceptados los términos y condiciones del portal cautivo y se procederá a su redireccionamiento al sistema que concederá la conexión a Internet.

El script access.php es el elemento del sistema encargado de proveer de conexión a Internet. Este archivo identifica la IP del usuario que se está tratando de conectar y establece una conexión con la base de datos generada en la página de bienvenida; de ella toma el parámetro IP de los usuarios cuyo valor de conectado sea 1 y los guarda en un array.

Con este array de IPs se establece una instancia if/else. En esta instancia se determina que, si el valor de IP tomado en este programa access.php coincide con alguno de los que están en el array extraído de la base de datos, no se debe proveer de conexión al usuario. Puesto que ya se ha conectado a la red previamente y se realiza una redirección permanente a la página web notwelcome.php.

En caso contrario, si no coinciden las IP, se envía la IP obtenida en el programa como argumento de un comando shell_exec que tiene como objetivo ejecutar el script conectar.sh. Este archivo conectar.sh es quien se encarga de añadir la regla de Iptables que otorga la conexión.

Como resulta lógico, este proceso de modificación de Iptables no está permitido por defecto para el usuario www-data; es por ello, que para su consecución se ha tenido que modificar la propiedad del archivo access.php a root y se ha tenido que crear una nueva configuración de permisos de ejecución. Esto se ha realizado añadiendo al directorio sudoers.d el archivo myOverrides con una directiva que da autorización al script conectar.sh y a disconnect.sh, script que se usará más adelante, para modificar las reglas de Iptables.

Una vez, completada la conexión en el script conectar.sh, continúan los procesos en el programa raíz. Para finalizar el proceso de conexión, se redirecciona al usuario de manera permanente a la página web welcome.php. En esta página se indica al usuario que ya puede hacer uso de su conexión a Internet. Esta configuración de conexión se representa en la Figura 4.8.

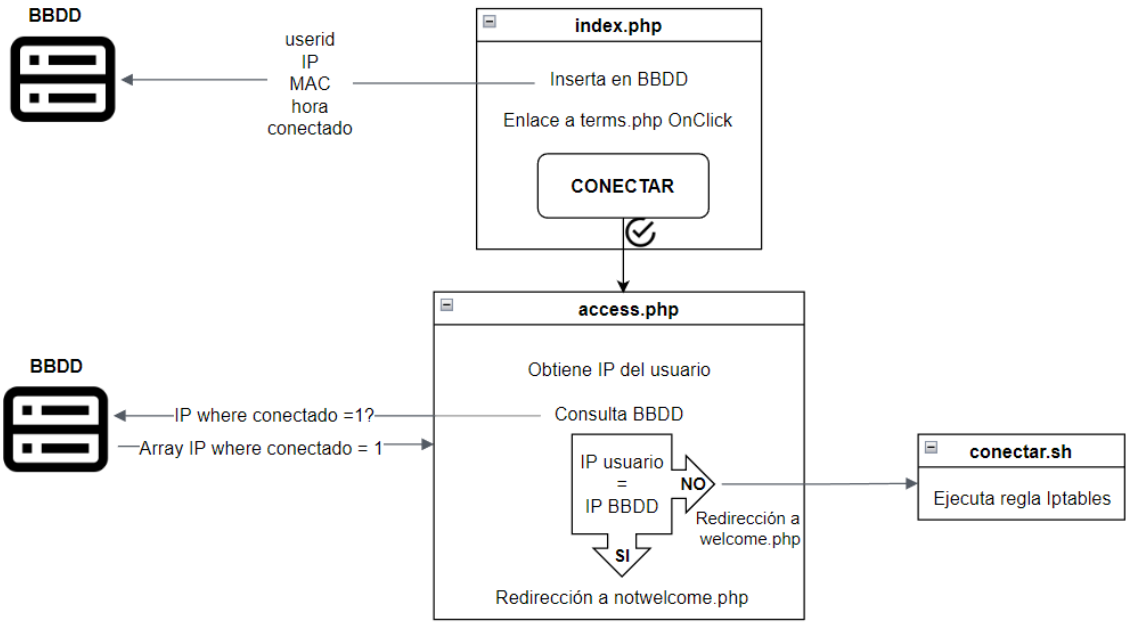

Figura 4.8 Esquema establecimiento de conexión

Ahora que ya se ha conectado a los usuarios, se debe de implementar el mecanismo de desconexión de Internet, el cual para su correcto funcionamiento se valdrá de los archivos desconectar.php y disconnect.sh. Y se puede ver representado en la Figura 4.9.

El sistema consiste en un archivo desconectar.php que se ejecuta en un bucle infinito. En el devenir de ese bucle lo que el programa hace es realizar peticiones a la base de datos MariaDB para recibir el userid, la IP y la hora de aquellas filas cuyo valor del parámetro conectado sea 0.

Según se reciben los vectores resultantes de la búsqueda, el programa los almacena en una matriz. De cada uno de esos vectores, se extrae el elemento hora, que como se indicó previamente específica el momento en que se inició la conexión, y se le compara con la hora actual del sistema. Si de esta comparación se obtiene un valor mayor al que se ha propuesto como tiempo de sesión, se procede a ejecutar a través del comando shell_exec el script disconnect.sh y se guarda el elemento userid de ese vector en otro vector llamado userlist. Para ello se envía como argumento la IP almacenada en el vector que se estaba comprobando y se ejecuta en disconnect.sh la regla de Iptables que retira la conexión a Internet a ese usuario. Tras esto, el programa raíz realiza un ciclo en que comprueba si hay algún elemento en el vector userlist, en caso afirmativo se iniciaría un proceso de actualización de la base de datos para establecer el valor de conectado a 1 para esa userid.

Ya sea porque se produzca el caso anterior o porque ningún usuario ha sobrepasado el límite el programa sigue iterando tras esperar 10 segundos.

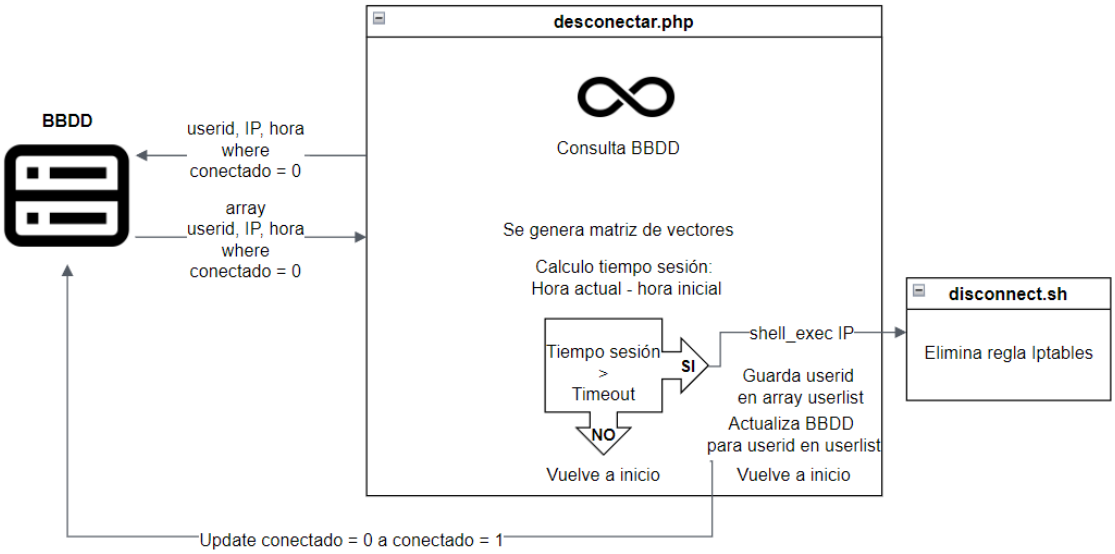

Figura 4.9 Esquema desconexión

4.4 INTEGRACIÓN DE METODOLOGÍAS ALTERNATIVAS DE CONEXIÓN CON LA RED

Típicamente, para conectar un dispositivo a una red WiFi privada se debe de tener que escribir la contraseña. Sin embargo, en este proyecto, para facilitar el acceso de los usuarios se va a añadir la opción de llevar a cabo la conexión a través de métodos alternativos como los códigos QR y las etiquetas NFC.

4.4.1 Configuración del código QR

La tecnología del código QR [28] consiste en un código de barras bidimensional en el cual se almacenan los datos codificados. Su gran ventaja es que, como dice su propio nombre Quick Response, el usuario que escanea el código accede a la información que codifica de manera instantánea. Esta tecnología es interesante puesto que ha ido actualizándose con el devenir del tiempo para incluir trazabilidad, protección de marca e incluso medidas antifalsificación; con lo que los códigos QR han ido ganando nuevos usos desde la transferencia de pagos hasta la determinación de las posiciones de los objetos dentro de la realidad aumentada.

Teniendo en cuenta esto, los códigos QR son una tecnología muy interesante y actualmente muy en boga. Además, por si no fuera poco, los códigos QR no se pueden piratear. Sin embargo, esto no quiere decir que su escaneo pueda tomarse como algo totalmente seguro; hay que tener en cuenta que estos pueden haber sido colocados o

sustituidos por un malhechor. El cual puede haber incrustado una dirección URL maliciosa que redireccione al usuario a una página que contenga malware personalizado que filtre datos su dispositivo o que redireccione a un sitio de phishing.

Es por ello que cuando se haga uso del código QR que de acceso a la red diseñada en este proyecto se hará uso de medios que eviten su reemplazo. Es decir, poniéndolo tras un cristal al que solo pueda acceder las personas de confianza.

La generación de este tipo de código debe ajustarse al formato adecuado para que el dispositivo móvil sea capaz de extraer la información del punto de acceso [29]:

```
WIFI:S:<SSID>;T:<WEP|WPA|blank>;P:<PASSWORD>;H:<true|false|blank>;;
```

Para el caso del proyecto, se ha hecho uso de la web qr-code-generator [30] y el código QR resultante es el representado en la Figura 4.10.

Figura 4.10 Código QR generado para el proyecto a través de la web qr-code-generator

4.4.2 Configuración de las etiquetas NFC

NFC (Near-Field Communication)[31] es una tecnología diseñada por una asociación de industrias sin ánimo de lucro llamada NFC Forum. Esta implementación es la evolución de la tecnología de identificación por radiofrecuencia (RFID) en la que se reduce el radio de funcionamiento a menos de 4cm para mejorar la seguridad del sistema. Su funcionamiento se basa en el principio de acoplamiento inductivo entre dos antenas; lo que implica que el dispositivo lector, cuando se va a acercar a la etiqueta que va a leer, genere un campo magnético que induce una corriente eléctrica a través de una bobina en la etiqueta. Por lo que evita tener que llevar a cabo un emparejamiento manual y la conexión se inicia automáticamente cuando la etiqueta entra en el rango del lector.

La seguridad de la tecnología NFC proviene de su alcance extremadamente corto, ya que para captar la señal el hacker tendría que estar muy cerca. Pero ya en el caso de

que el atacante se consiga posicionar tan cerca como para entrar en el rango de funcionamiento de la aplicación NFC, la función NFC solo entra en modo activo cuando se la requiere directamente. Sin embargo, esto no significa que la tecnología NFC sea totalmente segura, igual que se ha mencionado para las etiquetas QR, los atacantes pueden tratar de vulnerar la seguridad de los usuarios a través de la suplantación de etiquetas.

Es por ello, que la etiqueta NFC utilizada para este proyecto se ha protegido físicamente para evitar su reprogramación. Es decir, que tal y como se mencionó para el código QR, la manera óptima de distribuir su uso es ponerla tras un cristal al que solo puedan acceder las personas de confianza.

La configuración de las etiquetas NFC para conectarse a redes WiFi se realiza ajustando los parámetros que se quieran incluir al formato especificado por el NFC Forum y la WiFi Alliance. Es por ello que, para este caso, se debe de configurar la etiqueta siguiendo el estándar WiFi Easy Connect[32].

En este caso se ha hecho uso de la aplicación NFC Tools [33] instalada en un dispositivo móvil para aplicar la configuración sobre una tarjeta NFC MIFARE Classic. Para ello, se ha escogido la opción de escribir una etiqueta con formato WiFi network y se han aportado los datos de tipo de autenticación, encriptación, SSID y contraseña. Posteriormente, para realizar la comprobación del formato utilizado, se ha leído el contenido de la tarjeta con la aplicación NFC TagInfo de NXP[34] y se ha capturado en la Figura 4.11 el siguiente NDEF Message.

Figura 4.11 Contenido de la tarjeta NFC configurada

4.5 CONFIGURACIÓN DEL SISTEMA DE CAPTURA, ANÁLISIS Y GENERACIÓN DE GRÁFICAS DEL TRÁFICO

Una vez configurada la Raspberry como un portal cautivo toca introducir las técnicas que permitirán capturar, analizar y generar las gráficas del tráfico. La configuración de estas técnicas es la que se va a explicar en este apartado y para ello se ha utilizado como base la implementación desarrollada el repositorio de GitHub de ZaneClaes[35], sobre la cual se han realizado algunas adaptaciones para ajustarse mejor a los requerimientos de este proyecto en concreto.

En líneas generales, este mecanismo de generación de estadísticas es la concatenación del software de análisis de tráfico tcpdump[36], el software Prometheus y el software Grafana.

Prometheus[37] es un software especializado como sistema de monitorización y alertas. Recopila datos de servicios mediante el envío de solicitudes HTTP en puntos finales de métricas que se almacenan en una base de datos como series temporales.

Grafana[38] es un software de código abierto diseñado para ejecutar análisis de datos, extraer métricas a partir de estos y monitorear sistemas en línea. Estos datos se pueden obtener de cualquier fuente de datos, pero es típico su uso combinado con Prometheus. Mediante su uso se puede analizar el comportamiento del usuario, de la aplicación, la frecuencia de errores del sistema, el tipo de errores y los escenarios contextuales en que suceden. Por lo que su uso resulta muy útil para llevar a cabo análisis de series temporales.

Una vez explicadas brevemente las tecnologías que se van a utilizar, se va a dar una pequeña pincelada de la idea de interconexión del software para explicar a grandes rasgos cual es la idea de funcionamiento del sistema; la cual se ve representada en la Figura 4.12. La idea general es que el analizador de tráfico tcpdump captura las transferencias de datos que se produzcan en la red. Con esos datos Prometheus crea una base de datos que la aplicación Grafana aprovecha para extraer métricas y generar gráficas del funcionamiento del servicio.

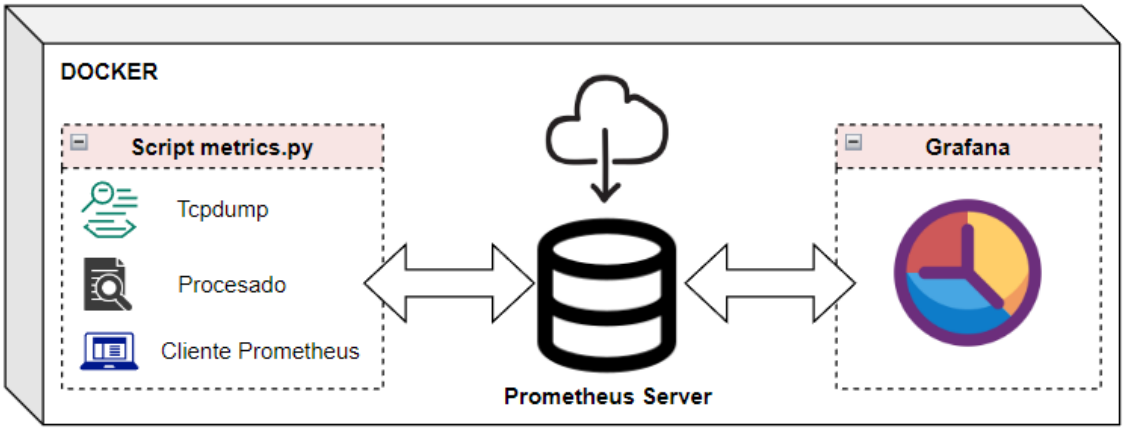

Figura 4.12 Esquema del sistema de captura, análisis y generación de gráficas del tráfico

Con el objeto de llevar a cabo una solución portable y funcional, a pesar de que se instalase en otra versión del sistema operativo GNU/Linux, el sistema de captura de datos, análisis y generación de gráficas se ha llevado a cabo haciendo uso del software Docker.

Docker [39] es un software de código abierto que permite crear, probar e implementar aplicaciones rápidamente. Su funcionamiento se basa en la utilización de la tecnología de contenedores; en los contenedores se empaqueta el servicio o función de la aplicación con todas sus bibliotecas, dependencias, partes y parámetros necesarios para operar. Cada contenedor comparte los servicios de un sistema operativo subyacente. Para ejecutar la aplicación dockerizada albergada en un contenedor en cualquier otro dispositivo tal y como está configurada en el dispositivo en que se creó, basta con que el otro ordenador tenga el mismo SO y que tenga instalado Docker.

4.5.1 Recolección de métricas de tráfico

Como se ha explicado previamente, la captura del tráfico se realiza a través del analizador de tráfico tcpdump. Sin embargo, para transferir la información a Prometheus no basta con enviar la captura de todo el tráfico, sino que hay que procesar la información capturada para que el programa Prometheus reciba solo los datos de interés.

Es por ello que para realizar este proceso se ha configurado un archivo en Python, llamado metrics.py. Este script es el encargado de inicializar el analizador de tráfico tcpdump, de procesar la información y de reenviársela a Prometheus para que pueda generar la base de datos con los eventos de tráfico que han sucedido en el sistema.

Con el objetivo de explicar más en detalle el funcionamiento de los elementos que conforman este script, se va a analizar el código implementado. En el cual se

podrían diferenciar tres procesos: la captura, el procesado de la información y su transferencia.

El paso inicial de este sistema es el establecimiento de la conexión con el servidor Prometheus, el cual, como se ha descrito previamente, será el receptor de la información que se obtenga en este script. Esta conexión se lleva a cabo inicializando un cliente Prometheus, para cuyo funcionamiento se declara que la interfaz y el puerto de salida son eth0 y el 8000, respectivamente. Finalmente, se deben de importar los subprocesos que se van a utilizar.

Una vez hecho esto, se definen las métricas que se van a enviar a través del cliente Prometheus para su posterior procesado en el servidor, en este caso se han tenido en cuenta la fuente (src), el destinatario (dst), el servicio (service) y el protocolo (proto).

Tras esto, toca inicializar la captura de los datos. Para este proceso se configura el proceso sobre la interfaz wlan0 y se aplica un filtro de captura que recopila todo el tráfico entrante y saliente de la red, descartando el tráfico interno.

```
(src net 192.168.42.0/24 and not dst net 192.168.42.0/24) or (dst net
      192.168.42.0/24 and not src net 192.168.42.0/24)
```

Este proceso de captura de datos se lleva a cabo a través de un subproceso asíncrono que permite al programa tcpdump realizar la captación de la información y que se mantendrá activo siempre y cuando siga capturando tramas. En caso de que no capturase nada, pararía su funcionamiento durante un segundo y tras el transcurso del mismo lo volvería a retomar.

Con este proceso ya activo, tcpdump comienza a capturar las tramas haciendo uso del filtro que se definió en el sistema de orquestación. Junto a ese filtro se hacen uso de las opciones -v, que detalla la información en un máximo de dos líneas por paquete, y readuntil, que asegura que cada una de esas líneas sea una cadena analizable.

Esta información obtenida es transcrita al formato UTF-8 y se analiza si contiene la información que permita determinar el servicio mediante el puerto y el protocolo que se está utilizando. Esto se consigue mediante la comparación de la trama con el archivo de sistema /etc/services, el cual contiene la información acerca de la relación de puertos TCP y su servicio asociado.

El mensaje capturado se descompone en partes, obteniendo el protocolo, la longitud, el puerto de origen y de destino y la dirección de origen y de destino.

Tras obtener estos campos de interés, se encapsulan en el string que, finalmente, será enviado a través del cliente Prometheus y que será el encargado de actualizar los contadores del servidor Prometheus.

4.5.2 Visualización de la información

Como se explicó previamente, para la orquestación del sistema se va a hacer uso de la arquitectura de Docker. Sin embargo, antes de explicar la configuración de los contendores Docker que se han utilizado, se va a describir la configuración de Prometheus y Grafana. Además, se va a ilustrar la experiencia del gestor de la red a través de capturas de pantalla del funcionamiento del software final. Los datos que se mostrarán pertenecen a una sesión de prueba propia en la que se ha hecho uso de un dispositivo móvil Android.

Si en el apartado anterior se inicializó el cliente Prometheus¸ en este apartado se va a explicar la configuración del servidor Prometheus. En este caso, el servidor ha sido configurado a través del archivo prometheus.yml; en este archivo se ha configurado la recepción de información del cliente Prometheus a través del puerto 8000, supeditada a una solicitud de actualización cada 15 segundos. Además, también se ha configurado que el puerto que usará el gestor para poder acceder a la información del servidor, el cual es el 9090.

Finalmente, la información albergada en Prometheus se puede visualizar conectándose al servidor a través de distintas URL en función de los datos que se quieran ver.

En la URL http://IPdelGestor:8000/metrics, cuyo contenido se puede visualizar en la Figura 4.13, se refleja el tráfico capturado, mostrando su origen y destino, el protocolo y el servicio. En esta captura, en concreto, se puede ver un extracto de la sesión de prueba realizada en la que se desarrollaba una búsqueda en Google.

```
# TYPE prometheus_target_interval_length_seconds summary
prometheus_target_interval_length_seconds{interval="15s",quantile="0.01"} 14.999428099
prometheus_target_interval_length_seconds{interval="15s",quantile="0.05"} 14.999428099
prometheus_target_interval_length_seconds{interval="15s",quantile="0.5"} 14.999697015
prometheus_target_interval_length_seconds{interval="15s",quantile="0.9"} 15.001190262
prometheus_target_interval_length_seconds{interval="15s",quantile="0.99"} 15.001190262
prometheus_target_interval_length_seconds_sum{interval="15s"} 105.000983701
prometheus_target_interval_length_seconds_count{interval="15s"} 7
# HELP prometheus_target_metadata_cache_bytes The number of bytes that are currently used for storing metric metadata in the cache
# TYPE prometheus_target_metadata_cache_bytes gauge
prometheus_target_metadata_cache_bytes{scrape_job="network-traffic-metrics"} 476
# HELP prometheus_target_metadata_cache_entries Total number of metric metadata entries in the cache
# TYPE prometheus_target_metadata_cache_entries gauge
prometheus_target_metadata_cache_entries{scrape_job="network-traffic-metrics"} 12
# HELP prometheus_target_scrape_pool_exceeded_label_limits_total Total number of times scrape pools hit the label limits, during sync or config reload.
# TYPE prometheus_target_scrape_pool_exceeded_label_limits_total counter
prometheus_target_scrape_pool_exceeded_label_limits_total 0
# HELP prometheus_target_scrape_pool_exceeded_target_limit_total Total number of times scrape pools hit the target limit, during sync or config reload.
# TYPE prometheus_target_scrape_pool_exceeded_target_limit_total counter
prometheus_target_scrape_pool_exceeded_target_limit_total 0
# HELP prometheus_target_scrape_pool_reloads_failed_total Total number of failed scrape pool reloads.
# TYPE prometheus_target_scrape_pool_reloads_failed_total counter
prometheus_target_scrape_pool_reloads_failed_total 0
# HELP prometheus_target_scrape_pool_reloads_total Total number of scrape pool reloads.
# TYPE prometheus_target_scrape_pool_reloads_total counter
prometheus_target_scrape_pool_reloads_total 0
# HELP prometheus_target_scrape_pool_sync_total Total number of syncs that were executed on a scrape pool.
# TYPE prometheus_target_scrape_pool_sync_total counter
prometheus_target_scrape_pool_sync_total{scrape_job="network-traffic-metrics"} 1
```

Figura 4.13 Ejemplo del tráfico capturado en una sesión haciendo uso del dispositivo Honor9, mostrando datos de la URL http://IPdelGestor:8000/metrics

En la dirección http://IPdelGestor:9090/metrics, representado en la Figura 4.14, se muestra que el servidor Prometheus está funcionando y se indican las peticiones que está realizando para obtener la información. En esta captura se pueden apreciar las peticiones de actualización que realiza el servidor Prometheus.

```
ntm_packets_total{dst="Honor_9-b155129cb8ee786d",proto="tcp",service="https",src="cloudfront.net"} 5488.0
ntm_packets_total{dst="104.19.150.54",proto="tcp",service="https",src="Honor_9-b155129cb8ee786d"} 47.0
ntm_packets_total{dst="elmundo.es",proto="tcp",service="https",src="Honor_9-b155129cb8ee786d"} 53.0
ntm_packets_total{dst="Honor_9-b155129cb8ee786d",proto="tcp",service="https",src="104.19.150.54"} 112.0
ntm_packets_total{dst="akamaitechnologies.com",proto="tcp",service="https",src="Honor_9-b155129cb8ee786d"} 69.0
ntm_packets_total{dst="Honor_9-b155129cb8ee786d",proto="tcp",service="https",src="akamaitechnologies.com"} 107.0
ntm_packets_total{dst="googleusercontent.com",proto="tcp",service="https",src="Honor_9-b155129cb8ee786d"} 109.0
ntm_packets_total{dst="Honor_9-b155129cb8ee786d",proto="tcp",service="https",src="googleusercontent.com"} 138.0
ntm_packets_total{dst="104.18.10.207",proto="tcp",service="https",src="Honor_9-b155129cb8ee786d"} 50.0
ntm_packets_total{dst="Honor_9-b155129cb8ee786d",proto="tcp",service="https",src="104.18.10.207"} 103.0
ntm_packets_total{dst="104.18.10.207",proto="udp",service="",src="Honor_9-b155129cb8ee786d"} 5.0
ntm_packets_total{dst="adnexus.net",proto="tcp",service="https",src="Honor_9-b155129cb8ee786d"} 30.0
ntm_packets_total{dst="Honor_9-b155129cb8ee786d",proto="tcp",service="https",src="adnexus.net"} 28.0
ntm_packets_total{dst="googleusercontent.com",proto="udp",service="",src="Honor_9-b155129cb8ee786d"} 15.0
ntm_packets_total{dst="185.64.189.112",proto="tcp",service="https",src="Honor_9-b155129cb8ee786d"} 16.0
ntm_packets_total{dst="185.86.138.123",proto="tcp",service="https",src="Honor_9-b155129cb8ee786d"} 95.0
ntm_packets_total{dst="Honor_9-b155129cb8ee786d",proto="tcp",service="https",src="185.64.189.112"} 18.0
ntm_packets_total{dst="your-server.de",proto="tcp",service="https",src="Honor_9-b155129cb8ee786d"} 67.0
ntm_packets_total{dst="213.19.162.21",proto="tcp",service="https",src="Honor_9-b155129cb8ee786d"} 18.0
ntm_packets_total{dst="Honor_9-b155129cb8ee786d",proto="tcp",service="https",src="185.86.138.123"} 87.0
ntm_packets_total{dst="Honor_9-b155129cb8ee786d",proto="tcp",service="https",src="your-server.de"} 45.0
ntm_packets_total{dst="Honor_9-b155129cb8ee786d",proto="tcp",service="https",src="213.19.162.21"} 18.0
```

Figura 4.14 Ejemplo del tráfico capturado en una sesión haciendo uso del dispositivo Honor9, mostrando datos de la URL http://IPdelGestor:9090/metrics

Por último, mediante la URL http://IPdelGestor:9090/graph, Figura 4.15, se pueden visualizar los datos recabados a modo de contadores o en gráficas en una aplicación web. En este último caso, esos contadores y gráficas son interactivos y permiten al gestor visualizar la información de todos los parámetros, definidos y enviados al servidor Prometheus, del archivo metrics.py. En el caso de la captura se optó por pedir que se mostraran el número de paquetes enviados a cada dirección destino; sin embargo, como se mencionó previamente, se podrían haber solicitado tablas o gráficas de cualquiera de los parámetros que se han enviado al servidor Prometheus.

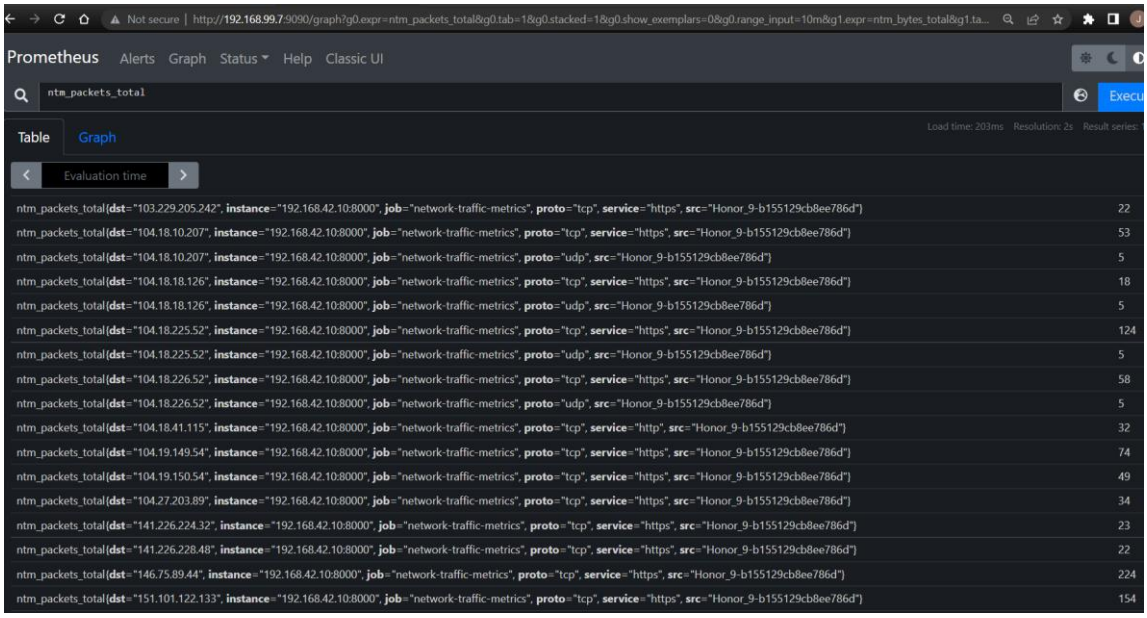

Figura 4.15 Ejemplo del tráfico capturado en una sesión haciendo uso del dispositivo Honor9, mostrando datos de la URL http://IPdelGestor:9090/graph. En este caso se visualiza la cantidad de paquetes que se han enviado

Una vez configurado Prometheus hay que enlazarlo con Grafana para que el primero actúe como base de datos y el segundo como generador de gráficas. Esta combinación se lleva a cabo a través de un sistema de tipo REST, en el que la aplicación web de Grafana va realizando peticiones de tipo REQUEST, de las que espera recibir actualizaciones de los datos en mensajes de tipo RESPONSE.

Para que esto suceda, se debe de establecer al servidor Prometheus como fuente de datos de Grafana. Para ello, se debe de incluir el archivo prometheus.yaml en la carpeta datasources del directorio grafana que se ha creado previamente. En este archivo se determina que, para actualizar la información, debe de hacerse a través de peticiones a la URL http://prometheus:9090 y que se debe de descargar el plugin grafana-piechart-panel para permitir la generación de gráficas. Adicionalmente, se establece que el puerto por el que recibirá tanto tráfico como solicitudes de contenido es el 3000.

Una vez configurada la recepción de los datos, llega el momento de diseñar la interfaz gráfica que verá el gestor de la red cuando se conecte a la aplicación online de Grafana. Esta interfaz gráfica es muy útil, puesto que permite la creación de consolas personalizadas para la visualización de los parámetros de interés. En este caso, la consola ha sido configurada para que muestre gráficas con el tráfico de la red filtrado por la IP del usuario, los Bytes transferidos por usuario y por servidor, el tráfico de subida y de bajada por el servidor y el throughput. Esta aplicación web puede ser visualizada por el gestor de la red a través de la URL http://IPdelGestor:3000/ y un ejemplo de su contenido se muestra en la Figura 4.16, la Figura 4.17 y la Figura 4.18. En estas capturas se puede apreciar el momento inicial de la conexión y esa búsqueda en Google que se mencionó previamente. Esto se puede apreciar en que la dirección de servidor más requerida, tanto en tráfico de subida como de bajada, es 1e100.net, un nombre de dominio de Google que identifica a sus servidores. Además, también se puede apreciar la gran diferencia de tráfico que hay en el throughput, viendo que es mucho mayor el tráfico de bajada que el de subida, siendo esto algo típico en las sesiones de este tipo.

Figura 4.16 Ejemplo del tráfico capturado en una sesión haciendo uso del dispositivo Honor9, mostrando datos de la URL http://IPdelGestor:3000. En este caso se visualizan el tráfico generado y los Bytes transferidos por la dirección IP que se está controlando

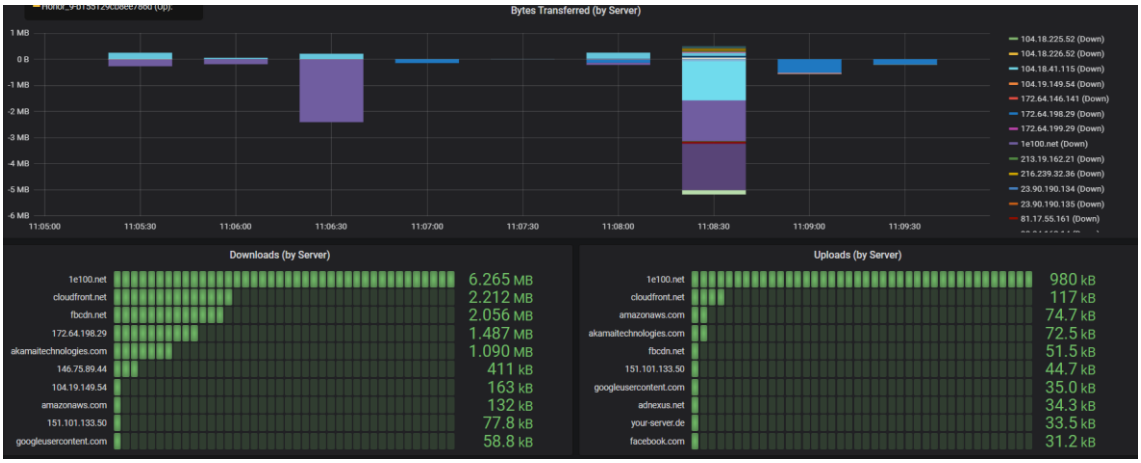

Figura 4.17 Ejemplo del tráfico capturado en una sesión haciendo uso del dispositivo Honor9, mostrando datos de la URL http://IPdelGestor:3000. En este caso se visualiza la información de cada servidor consultado por el usuario

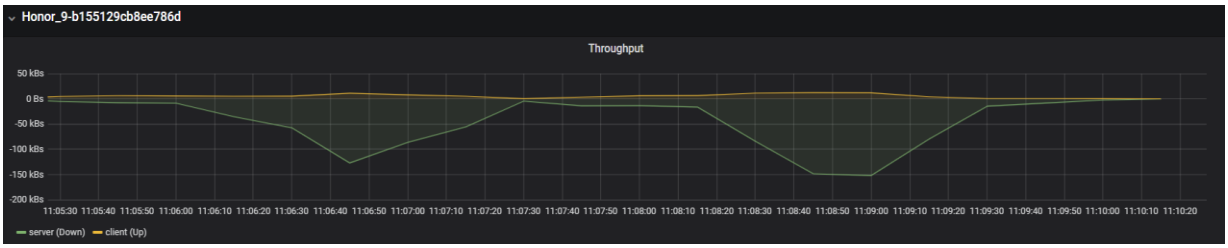

Figura 4.18 Ejemplo del tráfico capturado en una sesión haciendo uso del dispositivo Honor9, mostrando datos de la URL http://IPdelGestor:3000. En este caso se visualiza el throughput del dispositivo Honor

4.5.3 Orquestación de los elementos de la solución

Una vez definidos los elementos que conforman el sistema, hay que explicar el mecanismo que hace que todo funcione de manera cohesionada. En este caso, como se indicó previamente, se va a hacer uso de la estructura de Docker. La cual basa su funcionamiento en el uso de contenedores que albergan todas las dependencias de la aplicación que se desea implementar.

Para crear esta estructura de contenedor lo primero es crear un directorio con los siguientes elementos: Dockerfile, docker-compose.yml, services, requirements.txt y los archivos propios de la aplicación (en este caso, las carpetas de Grafana, Prometheus y el archivo metrics.py).

El archivo Dockerfile, Ilustración 2 del Anexo, es un archivo de texto plano que contiene las instrucciones para crear la imagen del contenedor. Mediante este archivo se indica la imagen base sobre la que se construye la aplicación, que en este caso es debian:buster-slim, se otorga permisos de root al sistema y se actualiza e instala el software que se va a necesitar para desarrollar la aplicación, para este caso se instala Python, prometheus_client y tcpdump. Además, se elimina los archivos temporales no utilizados. Se copia el archivo services propio del sistema para que la aplicación obtenga la relación de puertos y pueda comunicarse. Tras esto, se ejecuta metrics.py y finalmente se indica el puerto TCP/IP a través del cual se puede acceder a los servicios del contenedor, en este caso es el 8000. El archivo requirements.txt es necesario para que Dockerfile pueda crear la imagen del sistema.

Como se ha mencionado previamente, la configuración de este sistema requiere de la orquestación de varios contenedores, el generado a través de Dockerfile, el de Prometheus y el de Grafana. Para simplificar su interconexión y arranque, se hace uso de la utilidad docker-compose. La cual es configurada a través del archivo docker-compose.yml y permite una automatización completa del proceso, una vez ha sido configurado, al ejecutar el comando docker-compose up.

Entrando en el contenido de este archivo docker-compose.yml, Ilustración 1 del Anexo. El archivo consta de tres partes: version, que hace referencia a la versión de docker-compose que se está utilizando, en este caso es la 3.8; services, que indica los contenedores que se van a utilizar para generar el sistema, siendo, como se ha mencionado previamente, monitor, grafana y prometheus; y volumes, que define la información que se va a preservar una vez se elimine el contenedor, para este sistema será la de prometheus-data y grafana-data.

Concretando más la configuración del apartado services. En la sección monitor se crea el contenedor referido a la imagen del Dockerfile, el cual contiene información esencial para el funcionamiento del script metrics.py. En él, como se refirió previamente, se establece su funcionamiento como host a través de la interfaz wlan0 y el filtro de captura.

La sección prometheus indica la imagen del repositorio dockerhub que se utiliza como base para la configuración. En esta sección es donde se establece la distribución que se explicó previamente cuando se trató la configuración del servidor Prometheus.

Finalmente, la sección de grafana indica la imagen que se ha utilizado. Se establece la configuración de Grafana tal y como se indicó previamente en su sección propia.

Finalizado este proceso de orquestación de los elementos utilizados en el sistema de captura, se puede dar por concluido este cuarto capítulo en el que se ha desarrollado el despliegue de la solución. Puesto que, con esta configuración final, se ha conseguido finalizar el proceso de convertir la Raspberry Pi en un dispositivo capaz de actuar como punto de acceso con portal cautivo con capacidad para realizar la captura y análisis del tráfico de los usuarios que se conecten a la red.

Capitulo 5. CONCLUSIONES

Tras haber finalizado con la configuración del proyecto, es momento de evaluar si se han conseguido completar los objetivos previamente propuestos. Asimismo, en este capítulo también se aportarán una serie de recomendaciones para los usuarios derivadas del aprendizaje que se ha tenido con el desarrollo de este trabajo. Así mismo se expondrán posibles líneas futuras para la mejora del sistema propuesto.

Tras un análisis de los requisitos funcionales expuestos en el apartado 3.2, se puede concluir que se han conseguido completar todos los objetivos propuestos. De modo que la solución ofrecida como resultado de este proyecto cumple con las expectativas de que resultara económica y portable. Adicionalmente, en cuanto su implementación software, se ha conseguido desarrollar la solución sin hacer uso de software de terceros en los que para su configuración bastara con editar los archivos instalados. Obteniendo, gracias a realizarlo de este modo, una mejor comprensión del funcionamiento y un mayor control sobre el sistema que se estaba configurando.

Sin embargo, a pesar de que los objetivos se hayan cumplido, el camino recorrido hasta su consecución no ha sido simple. Puesto que cada una de las decisiones que se han ido tomando a lo largo del proyecto, ha sido fruto de la reflexión y valoración de las ventajas e inconvenientes derivados de su elección. Ejemplos de estas disyuntivas podrían ser la decisión de hacer uso de la interfaz de Ethernet sobre la interfaz WiFi para proveer de conexión a Internet a la Raspberry; la utilización de un método de autorización propio para evitar que los usuarios tuvieran que ingresar credenciales de acceso, en vez de utilizar algún otro modelo más típico; o el uso de Prometheus y Grafana para desarrollar el entorno gráfica. Disposiciones en las que finalmente siempre se ha decidido por la opción que garantizase la mejor experiencia de usuario posible.

Por tanto, creo que con el presente Trabajo de Fin de Grado se ha podido desarrollar una herramienta cuyo uso podrá resultar útil en charlas de concienciación al ciudadano sobre los peligros del uso de redes públicas, como las impartidas en los Talleres Teleco o las Noches de los Investigadores.

5.1 RECOMENDACIONES DE SEGURIDAD PARA LOS USUARIOS

Una vez llegados a este punto, lo que todos nos estamos preguntando es: ¿cómo podemos evitar este tipo de ataques? La respuesta para este caso concreto es muy sencilla, leyendo los términos y condiciones que aceptan al conectarse a la red WiFi. En

caso de así hacerlo, hubieran sido advertidos del propósito que tiene el gestor de red para proveer de esa conexión gratuita y podrían haber rechazado su uso. Por ello, la primera recomendación y la más básica que se puede hacer es la siguiente: antes de aceptar unos términos y condiciones, se debe de leer lo que se está aceptando.

Sin embargo, en el mundo real los ciberdelincuentes que llevan a cabo un ataque de este tipo no suelen ser tan considerados como para avisar de sus intenciones de manera tan expresa. Por ello, con el fin de preservar la seguridad de nuestras conexiones a internet, los usuarios debemos de tomar medidas.

Por una parte, es obvio que, si se quiere minimizar las posibilidades de verse afectado por un ataque MitM de este tipo, hay que tratar de evitar conectarse en redes inalámbricas de cuyo administrador no se esté totalmente seguro de sus intenciones. Sin embargo, en ocasiones no queda otra opción que conectarse a alguna red de este tipo; pero no por ello se ha de asumir que si esta red inalámbrica tiene fines delictivos está todo perdido.

Por lo tanto, en este capítulo, basándose en la información obtenida del Cybersecurity Information Sheet de la NSA [40], se tratará de realizar unas recomendaciones de seguridad que sería conveniente tener en cuenta.

5.1.1 Minimizar la distribución de información

Cuando se inicia la conexión en un punto de acceso de este tipo, lo más importante es desconfiar del administrador. Con esto se hace referencia a que no se deben rellenar campos de datos que requieran información que no se esté dispuesto a compartir tales como: nombre, apellidos, correo electrónico o teléfono. Además, lo más común es que los ciberdelincuentes no sean tan poco sutiles de requerir esos datos así tal cual; si no que, mediante técnicas basadas en el engaño, traten de hacer ver que el usuario se está conectando a través de tu cuenta de Google, Facebook o Apple (por ejemplo) y de ese modo consigan robar los datos de usuario y contraseña. Un ejemplo de esta técnica se puede ver en la Figura 5.1.

Por ello es muy importante desconfiar de lo que se muestra, no dar datos que puedan resultar importantes y comprobar la veracidad de los sistemas de autenticación de los que dispone el punto de acceso.

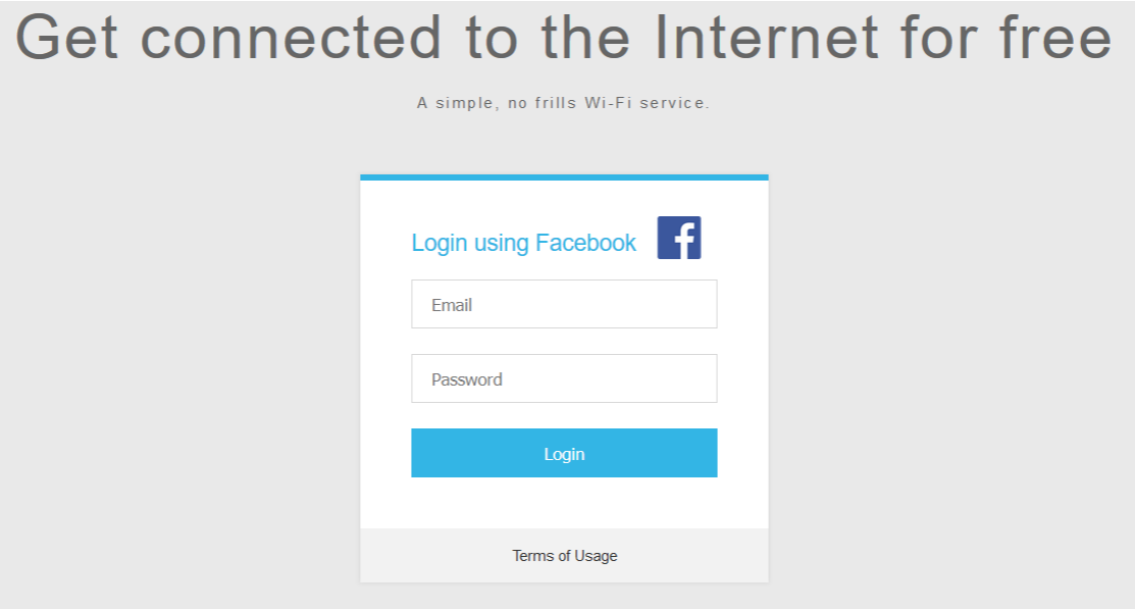

Figura 5.1 Ejemplo página de bienvenida a un portal cautivo con esquema phishing

5.1.2 Conexión HTTPS

HTTP es un protocolo de comunicación de datos que resulta muy útil pero que cuenta con un grave problema en lo referido a la seguridad digital. Por ello, cuando el usuario se conecta a Internet, el protocolo sobre el cual deben de funcionar las páginas webs a las que se conecten debe de ser HTTPS.

Mediante este protocolo se garantiza que los datos de conexión vayan cifrados; con lo que, aunque sean capturados y en cierto modo interpretados, su contenido exacto no puede ser descifrado.

Sin embargo, que la página web de acceso al portal cautivo funcione bajo el amparo del protocolo HTTPS no implica que este por fuerza no tenga carácter delictivo y que los datos que en ella se ingresen estén seguros, puesto que existe la posibilidad de que haya conseguido que funcione utilizando HTTPS gracias al uso de un certificado SSL autofirmado u obtenido de una entidad certificadora de dudosa confianza.

Para evitar ser engañado es recomendable comprobar el certificado de la página web del portal cautivo. Para ello, en caso de que el navegador no mande un aviso automático, bastaría con hacer uso de la conexión de datos móviles y comprobar la URL de la web en alguna de las herramientas de comprobación de certificados SSL que se pueden encontrar en Internet; como son: https://www.digicert.com/help/ o https://www.ssllabs.com/ssltest/ .

5.1.3 Desactivar la descarga de orígenes desconocidos

Los ciberdelincuentes pueden tratar de ir más allá del robo de datos de sesión e instalar algún tipo de software en el terminal del usuario, haciendo que el robo de datos no se limite al tiempo en que los usuarios estén conectados al punto de acceso y puedan mantener su actividad delictiva más allá en el tiempo.

Esta dinámica podría ser implementada en el momento en que los usuarios aceptan entrar en el portal cautivo. Por ello, es recomendable tener desactivado en la configuración de los ajustes del teléfono la posibilidad de realizar descargas de orígenes desconocidos. De este modo, al intentar iniciarse una de estas descargas no autorizadas, se notificará y se advertirá al usuario si realmente quiere iniciar esa descarga.

5.1.4 Verificación en dos pasos

A pesar de llevar a cabo una política de uso de Internet responsable, siempre cabe la posibilidad de caer en la trampa de los ciberdelincuentes. Por ello, es tremendamente recomendable aprovechar la posibilidad de utilizar un sistema de seguridad en dos pasos siempre que sea posible.

De este modo, aunque el atacante consiga hacerse con datos relativos al usuario y contraseña de cualquiera de las cuentas del usuario, no pueda hacer un uso efectivo de esta información; ya que para ello además será requerida una confirmación en alguno de los dispositivos seguros de la víctima.

Esta verificación se puede realizar a través de mecanismos que hagan uso del protocolo OAuth 2[41]. Este protocolo permite autorizar el acceso a un recurso en base a si el usuario dispone de un token válido, del cual se dispone una vez el usuario se haya validado a través de la cuenta de una red social, por un PIN o a través de medidas biométricas. Las posibilidades que brinda esta tecnología pueden ser mejoradas a través del uso de Open ID; esta implementación hace que en el proceso anterior se añada la identificación del usuario final, proveyendo con ello a la aplicación en la que se está conectando de la información básica de su perfil.

5.1.5 Mantener actualizado el software

Cuando se adquiere un dispositivo electrónico, la compañía fabricante suele realizar actualizaciones en el software del mismo para mejorar el rendimiento del dispositivo, corregir fallos, actualizar la versión del sistema operativo o actualizar el

parche de seguridad. Es por ello, que los usuarios deben de encargarse de actualizar su dispositivo a la última versión del sistema disponible.

Con esta sencilla verificación, los usuarios se aseguran tener implementada la mejor versión del sistema que los desarrolladores han conseguido implementar para su dispositivo. De este modo, si se ha detectado y corregido alguna brecha de seguridad, esta estará solventada y no afectará al sistema.

5.1.6 Uso de VPN

Una de las mejores prácticas que se pueden llevar a cabo para mejorar la seguridad cuando se navega por Internet es hacer uso de una VPN, ya que mediante su uso se puede proteger totalmente la privacidad del usuario.

El uso de esta tecnología resulta muy útil ya que protege el tráfico entre el dispositivo y el servidor VPN. De este modo, en caso de que el usuario estuviera haciendo uso de un punto de acceso de vocación delictiva, el ISP no podrá llevar a cabo un ataque MitM puesto que los datos están encriptados y la ubicación real del dispositivo falsificada.

5.2 LÍNEAS FUTURAS

Con el objetivo de mejorar la implementación desarrollada en este proyecto y añadir más funcionalidades, aunque algunas podrían salirse de la filosofía con la que se ha desarrollado este proyecto, se van a plantear distintas líneas de trabajo.

La primera, encajaría en el requerimiento de portabilidad del sistema. En este sentido, se plantearía añadir una batería a la Raspberry para que su funcionamiento no dependa de la disposición de una toma de corriente. Siguiendo en esta línea, se debería de valorar la sustitución de la conexión a Internet a través de la interfaz de Ethernet por una metodología que permitiera mayor movilidad; pudiendo ser esta el acceso a través de la interfaz WiFi o a través del uso de un módem portátil.

Otra mejora plausible sería la mejora del sistema de desconexión. La idea para su desarrollo sería que el servidor notificase al usuario cuando se le haya retirado la conexión a Internet. Para ello, enviaría una notificación PUSH al dispositivo, de esta forma se generaría un pop-up en la pantalla del usuario que avisaría de la situación y que al pinchar en él redireccionaría a una web de concienciación; donde se expondrían las métricas que se han obtenido de su sesión junto con información relativa al buen uso de las redes públicas.

Finalmente, otro elemento que se ajustaría a la filosofía del proyecto y que podría resultar interesante implementar sería un díptico informativo. El objetivo de

este díptico sería resumir un compendio de buenas prácticas en redes públicas de manera visual, atractiva y fácil de asimilar. De modo que se podría facilitar la asimilación de la información sobre la que se quiere concienciar.

En cuanto a los desarrollos que se saldrían de la idiosincrasia actual del sistema estaría el uso del portal cautivo como vector para la implantación de ataques de tipo phishing y malware. O su uso para recabar métricas de las que se el gestor se podría valer para llevar a cabo estrategias de marketing focalizadas.

En este sentido, se podría desarrollar un proyecto que aunara las tres vertientes. Pudiendo realizar un ataque de suplantación de DNS que redireccionara a los usuarios que traten de conectarse a una determinada URL a otra en la que el gestor suplantaría a la página original, y que podría ser aprovechada para robar credenciales de usuario. Por otra parte, se podría realizar un estudio de los tipos de ataques de tipo malware disponibles y llevar a cabo la implementación de dos de ellos. Uno con capacidades para hacerse con el control total, en la sombra, del dispositivo para poder utilizarlo como elemento de una botnet en un ataque DDoS. Y otro cuyo objetivo sería hacer spam de anuncios de productos, este se valdría de la información sustraída en la sesión para realizar ese spam de manera personalizada.

Otra variante de desarrollo en cuanto al marketing, sería simplemente hacer uso de la información recabada para generar una base de datos que podría ser utilizada de manera comercial.

Una vez explicadas las posibles líneas futuras, concluiría este quinto y último capítulo. Finalizando de este modo las conclusiones de este Trabajo de Fin de Grado.

ANEXO

```
version: '3.8'
services:
  monitor:
    image: network-traffic-metrics:arm
    network_mode: host
    environment:
      - "NTM_INTERFACE=wlan0"
      - "NTM_FILTERS=((src net 192.168.42.0/24 and not dst net 192.168.42.0/24) or (dst net 192.168.42.0/24 and not src net 192.168.42.0/24))"

  prometheus:
    image: prom/prometheus:main
    ports:
      - 9090:9090
    volumes:
      - ./prometheus:/etc/prometheus
      - prometheus-data:/prometheus
    command: --web.enable-lifecycle  --config.file=/etc/prometheus/prometheus.yml
    extra_hosts:
      - "monitor:192.168.42.10"


  grafana:
    image: grafana/grafana:6.6.2
    ports:
      - 3000:3000
    volumes:
      - grafana-data:/var/lib/grafana
      - ./grafana/provisioning:/etc/grafana/provisioning
    links:
      - "prometheus:prometheus"
    environment:
      - "GF_INSTALL_PLUGINS=grafana-piechart-panel"


volumes:
  prometheus-data:
  grafana-data:
```

Ilustración 1 Configuración dockercompose.yml

```
FROM debian:buster-slim

MAINTAINER Javier Rodrigo García

USER root

RUN apt-get clean -y && apt-get update -y && \
    apt-get install --no-install-recommends -y python3-pip python3-setuptools && \
    apt-get clean && rm -rf /var/lib/apt/lists/* /tmp/* /var/tmp/*

RUN pip3 install argparse prometheus_client

RUN apt-get update -y && apt-get install -y tcpdump

COPY services /etc/services
COPY network-traffic-metrics.py /usr/bin/network-traffic-metrics.py
RUN chmod +x /usr/bin/metrics.py
CMD /usr/bin/metrics.py

EXPOSE 8000
```

Ilustración 2 Configuración Dockerfile

BIBLIOGRAFÍA

[1] "WiFi," *https://www.webopedia.com/definitions/wifi/*.

[2] "WEP." [Online]. Available: http://www.cs.sjsu.edu/~stamp/CS265/projects/Spr05/papers/WEP.pdf

[3] "WPA," *https://www.techopedia.com/definition/4166/wi-fi-protected-access-wpa*.

[4] "WPA2," *https://www.wi-fi.org/news-events/newsroom/wpa2-security-now-mandatory-for-wi-fi-certified-products*. https://www.wi-fi.org/news-events/newsroom/wpa2-security-now-mandatory-for-wi-fi-certified-products

[5] "WPA3," *https://www.wi-fi.org/discover-wi-fi/security*.

[6] "KRACK attack." [Online]. Available: file:///C:/Users/javie/Downloads/mark_vink.pdf

[7] "Portal Cautivo." https://www.techtarget.com/searchmobilecomputing/definition/captive-portal

[8] "Nodogsplash," *https://nodogsplashdocs.readthedocs.io/en/stable/index.html*.

[9] "Smart Queue Management," *https://taktikalnetwork.com/pages/smart-queue-management-qos*.

[10] "CoovaChilly," *https://help.ubuntu.com/community/WifiDocs/CoovaChilli#:~:text=CoovaChilli%20takes%20control%20of%20the,to%20and%20from%20the%20WAN.*

[11] "BLOOM," *https://bloomintelligence.com/captive-portals/*.

[12] "WEF Global Risks Report 2022." [Online]. Available: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

[13] "Estadísticas ciberataques," *https://www.embroker.com/blog/cyber-attack-statistics/*.

[14] "MitM," *https://www.csoonline.com/article/3340117/man-in-the-middle-attack-definition-and-examples.html*.

[15] "Malware," *https://www.csoonline.com/article/3649363/malware-explained-definition-examples-detection-and-recovery.html*.

[16] "Phishing," *https://www.csoonline.com/article/2117843/what-is-phishing-examples-types-and-techniques.html*.

[17] "DoS y DDoS," *https://www.csoonline.com/article/3648530/ddos-attacks-definition-examples-and-techniques.html*.

[18] “Estadísticas ciberataques,” *https://techjury.net/blog/how-many-cyber-attacks-per-day/#gref*.

[19] “Cisco Security report.” [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/security/security-outcomes-study-vol-2-report.pdf?ccid=cc000160&oid=rptsc027923&dtid=odicdc001478

[20] “Ciberataques en teléfonos móviles.” https://securelist.com/mobile-malware-evolution-2021/105876/

[21] “Distribución de ataques Malware en dispositivo móviles,” *https://www.statista.com/statistics/653688/distribution-of-mobile-malware-type/*.

[22] “Ataques tipo sobre redes WiFi”, [Online]. Available: https://www.e-channelnews.com/top-5-most-dangerous-public-wifi-attacks/

[23] “Estadísticas ataques en redes WiFi.” https://securelist.com/router-security-2021/106711/

[24] “Estadísticas aceptación de Términos y condiciones - USA Today,” *https://eu.usatoday.com/story/tech/2020/01/28/not-reading-the-small-print-is-privacy-policy-fail/4565274002/*.

[25] “Configuración AP,” *https://raspberrypi-guide.github.io/networking/create-wireless-access-point*.

[26] “Configuración del Servidor Apache,” *https://httpd.apache.org/docs/2.4/configuring.html*.

[27] “Detección automática de portal cautivo,” *https://success.tanaza.com/s/article/How-Automatic-Detection-of-Captive-Portal-works*.

[28] “Códigos QR ,” *https://ieeexplore.ieee.org/document/7966807*.

[29] “Códigos QR - Formato WiFi.” https://en.wikipedia.org/wiki/QR_code

[30] “qr-code-generator,” *https://es.qr-code-generator.com/solutions/wifi-qr-code/*.

[31] “Etiqueta NFC,” *https://electronics.howstuffworks.com/nfc-tag.htm*.

[32] “WiFi Easy Connect,” *https://www.wi-fi.org/discover-wi-fi/wi-fi-easy-connect*.

[33] “NFC Tools,” *https://play.google.com/store/apps/details?id=com.wakdev.wdnfc&hl=es&gl=US*.

[34] “NFC TangInfo by NXP,” *https://play.google.com/store/apps/details?id=com.nxp.taginfolite&hl=es&gl=US*.

[35] “Zane Claes - GitHub .” https://github.com/zaneclaes/network-traffic-metrics

[36] “tcpdump,” *https://www.tcpdump.org/index.html*.

[37] “Prometheus,” *https://prometheus.io/docs/introduction/overview/*.

[38] “Grafana,” *https://grafana.com/grafana/?plcmt=footer*.

[39] “Docker,” *https://docs.microsoft.com/es-es/dotnet/architecture/microservices/container-docker-introduction/docker-defined*.

[40] “NSA - Cybersecurity Information Sheet.” [Online]. Available: https://media.defense.gov/2021/Jul/29/2002815141/-1/-1/0/CSI_SECURING_WIRELESS_DEVICES_IN_PUBLIC.PDF

[41] “OAuth 2 y Open ID”, [Online]. Available: https://medium.com/flux-it-thoughts/c%C3%B3mo-asegurar-aplicaciones-con-oauth-openid-identityserver4-23587ec27bbb