Facultad de ingeniería

Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO

ACTIVIDAD DE APRENDIZAJE 1:

Indagación

Fase Transversal - Interpretación, aprehensión y transferencia conceptual / temática.

En esta actividad se nos presentan conceptos relacionados con el hacking, las motivaciones que este tiene y las implicaciones que ha tenido en el mundo. En la película elegida, Hacker (1995) se ve un mundo en donde la tecnología y la información eran ya una parte vital de la sociedad, lo cual generaba interés por parte de delincuentes y personas aficionadas a la tecnología y la ciberseguridad. Apegado a la película, podemos dar un salto de tres décadas al reporte de Hacker One del 2021, en especial al articulo relacionado a las motivaciones de los hackers, en donde la principal motivación de los aficionados y profesionales de la ciberseguridad es el poder aprender, el obtener nuevos conocimientos en base a las actividades de intrusión a sistemas.

Luego podemos ver el papel de la ciberseguridad en la actualidad, desde el conflicto cibernético entre Estados Unidos y Rusia (también están involucrados otros países) el cual ha llegado a tener implicaciones en aspectos relacionados a las relaciones internacionales, los servicios bancarios (en general a cualquier servicio prestado por la red) y la economía. Muy apegado a esto se debe mencionar a Stuxnet, la primera ciberarma que logro generar un daño de miles de millones en infraestructura que tenía Iran para la creación de armas atómicas, y por otro lado se debe mencionar a Pegasus, el malware de espionaje que ha generado conmoción en el mundo debido a su forma en que puede acceder a nuestra información contenida en nuestros dispositivos móviles.

Todos estos temas o elementos se relacionan entre sí, ya que nos ayudan a tener un panorama mucho más amplio con relación a la ciberseguridad, la forma en que las personas sin conocimientos sobre esta la pueden ver y la capacidad de daño que puede tener el conocimiento de ciberseguridad empleado en actividades delictivas o ilegales, las cuales pueden desembocar en problemas de gran magnitud.

Fase Uno – Planteamiento de estudio de casos o actividad

Facultad de ingeniería

Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO

1. *Ir al cine, selecciona una de estas tres películas, Hackers, Juegos de Guerra, o Who Am I; tomar apuntes de cada una de las técnicas que se muestran en estas películas para vulnerar los sistemas informáticos. Las películas están en internet.*
2. *Leer el reporte de Hacker Report 2021 de HackerOne, seleccionar un artículo y escribir una reflexión al respecto. Debes buscarle en internet.*
3. *Indagar sobre el conflicto entre Estados unidos y Rusia en cuanto a los ataques cibernéticos entre estos dos países, su origen, sus implicaciones, posibles consecuencias y breve recuento de estos incidentes.*
4. *Indagar cual fue la primera ciberarma, cuando y donde fue usada.*
5. *Por último, indagar sobre el software Pegasus utilizad por el gobierno israelí y que ha sido blanco de un escándalo reciente por su uso.*

Los siguientes puntos fueron expuestos en clase y no se incluyeron en el correo electrónico enviado:

6. Explicar el concepto de Jailbreak
7. Explicar los conceptos de Hacking ético, Escaneo de vulnerabilidades y Pentesting

Facultad de ingeniería

Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO

Fase Dos – Planteamiento de la respuesta y solución de la actividad

1. Película: Hackers (1995)

Hackers (Softley, 1995) es una de las películas más interesantes relacionadas con el mundo del hacking, la historia se desarrollado en las décadas de los 80s y 90s y cuenta la historia de Dade, un hacker que desde los 11 años demostró sus habilidades en el mundo de la tecnología y la seguridad, y que a los 18 años se va a volver a enfrentar a un reto para sus habilidades: detener el virus Da Vinci creado por Plaga. Alguno de los ataques o técnicas que muestran en la película son los siguientes:

- Virus creado por Dade que bloqueo a 1507 ordenadores, generando una caída en la bolsa de valores de Wall Street.
- Ataque de **ingeniería social** en el que Dade se hace pasar por uno de los encargados de los sistemas de una cadena de televisión para obtener el código de un modem y así controlar la transmisión. En este mismo ataque se conoce con Kathe o Acid Burn, y entre los dos luchan para tener el control de la trasmisión, ganando esta pelea Kathe.
- Ramon muestra que teniendo una grabación del sonido de una moneda cayendo dentro de una cabina telefónica se podia llamar gratis. También Ramon muestra en la cárcel que se podía acceder a una llamada con la operadora presionando 4 veces el botón de colgado del teléfono.
- Dade, debido a como Kathe lo engaño para subir a la azotea del colegio, desde su casa logra tener acceso al sistema de aspersores del colegio donde estudia y programo que los aspersores se activaran a las 9:30 AM.
- Dade también logro tener acceso al sistema de gestión de clases de su colegio y de esta forma cambio sus clases para estar inscrito en una clase con Kathe.
- El **virus Leonardo Da Vinci** creado por Plaga, el cual era capaz de generar una falla en el funcionamiento de 10 barcos de una empresa petrolera. En torno a este virus gira el nudo de la historia. Aquí se debe mencionar la intrusión de Joey a Gibson, una super computadora, de la cual extrae el archivo donde se encontraba este virus por medio del uso de un diccionario de contraseñas más usadas. Este virus solo era una distracción para poder desviar dinero de las transacciones de la empresa.
- Intrusión en el sistema de un banco en donde se da la orden de destruir la tarjeta de Gill.
- Infiltración en el sistema de la policía para dar la orden de arresto a Gill, haciendo uso del phreaking.
- Gusano (**worm**) dentro de un sistema (asumo que era un sistema de alguna entidad bancaria) el cual tenía la función de robar dinero y a su vez devoraba ciertas partes del código base del sistema. Este virus fue creado por Plaga.
- Programa el cual controlaba los semáforos de la ciudad, creado por Dade para ganar tiempo.

- Uso de las cabinas telefónicas para acceder a internet, a esto se le llama **phreaking**, y era usado por los hackers para realizar ataques desde cualquier teléfono sin comprometer su lugar de residencia.
- Para detener al virus Leonardo Da Vinci, Dade, Kathe y sus amigos se unieron con hacker alrededor del mundo para sobrecargar a la super computadora Gibson y de esta forma inhabilitar al virus. En este momento se hace uso de phreaking y se menciona un virus Conejo el cual se replicaba dentro del sistema de la super computadora para provocar su colapso.
- Emmanuel, con el fin de exponer a Plaga quien estaba detrás del virus gusano y Leonardo Da Vinci, se apodera de la transmisión de un canal de televisión.
- Finalmente, cuando Dade y Kathe tienen su cita, él se había apoderado previamente del sistema de iluminación de un edifico, con el cual escribe una frase con las luces de algunos pisos y habitaciones.

La película me presento una era en donde el Hacking, aun estando limitado por la tecnología, era capaz de detener ciudades o generar grandes problemas ambientales, sin olvidar a los disquetes en donde pasaban información y hasta virus. Fue muy interesante mirar la película, tanto por su trama, la información que presentaba y hasta por su estética.

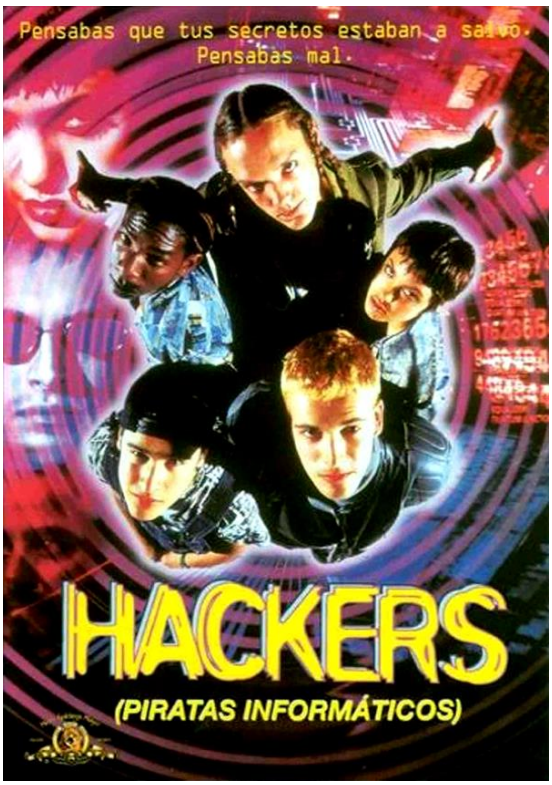


Ilustración 1 Poster de la pelicula

Facultad de ingeniería

Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO

2. Hacker Report 2021 – Hacker Motivations

En este artículo (HackerOne, 2021) se nos presenta las razones por las cuales los hackers hacen sus actividades, exponiéndonos una realidad asociada al mundo de la ingeniería de sistemas (y puede que se aplique en otras profesiones) en donde buscamos principalmente obtener habilidades y conocimiento esto precisamente a como el mundo de la tecnología está en constante cambio y esto es mucho más tangible en el ámbito de la ciberseguridad, en donde los ciberdelincuentes tampoco se detienen y siempre crean nuevas formas por medio de las cuales puedan obtener información y generar daños a los sistemas informáticos, aquí es donde podemos analizar cada uno de las respuestas a la pregunta de ¿Por qué los hackers hackean? (traducida al español suena un poco extraño), en donde un 85% afirma que lo hace para aprender, y es cierto, en el mundo de la informática el hacer y el saber se conectan directamente, sin probar los conocimientos que un hacker posee sobre seguridad no podrá saber si estos son correctos o no, aquí se pueden mencionar los programas VDP que permiten al hacker un espacio para probar sus habilidades y conocimientos, por otro lado, no se puede negar que el hacking es una actividad que genera dinero, lo cual se comprueba con el 76% de los encuestados que indica como no solo se puede generar conocimiento sino ingresos, ya que es una necesidad en la actualidad el manejo de la seguridad de los sistemas informáticos y esto se apega mucho a como el manejo de distintos campos de los sistemas informáticos es una fuente de ingresos que ir creciendo día con día.

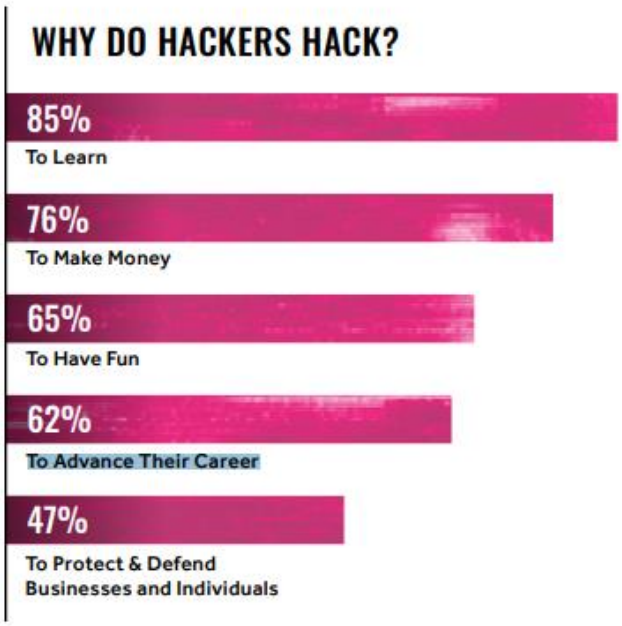


Ilustración 2 Respuestas a la pregunta" Why do hackers hack?"

Las dos motivaciones anteriormente expuestas son las dos más fuertes, pero debemos considerar como un 65% de los encuestados toman al hacking como una fuente de diversión

o entretenimiento, lo cual demuestra que esta actividad, que aun teniendo implicaciones legales, no debe ser tomado con un tema serio o que solo se debe emplear con fines educativos, laborales o corporativos, y está muy bien saber que se deje de ver a la seguridad o en general a los sistemas informáticos como fuentes de aburrimiento. Finalmente se ve como el Hacking es tomado por un 62 % como una actividad que solo es requerida para avanzar en el curso de su carrera, como un requisito, al igual que el 47% que la ve como una forma de defensa para negocios o personas, estas dos últimas motivaciones pueden ser las más serias y que solo exponen un grado de obligatoriedad en el aprendizaje de la seguridad para los sistemas informáticos.

Concluyendo, se puede tener presente que los hackers en la actualidad tienen como motivación el obtener conocimiento, de modo tal se puedan comenzar a suplir otros elementos, como el factor monetario, ya que al tener cierto nivel de conocimientos se puede ser más útil en ciertas tareas y dichas tareas que se realicen van a generar un beneficio en la adquisición de conocimientos y habilidades, sin olvidar que el aprendizaje, como en cualquier profesión, es una actividad del día a día, y que si nos dedicamos a lo que nos apasiona, sea el hacking, el desarrollo o la ciencia de datos, los trabajos que realicemos nos brindaran emoción, y para mí eso es muy importante, porque, ¿de qué sirve ganar dinero si no se es feliz o si no nos genera satisfacción a lo que nos dedicamos?

Facultad de ingeniería

Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO

3. EE. UU vs. Rusia y Ciberataques

Los conflictos entre países han sido un motor de cambios, tanto positivos como negativos, los cuales han ido poblando la historia de la humanidad, y debemos dirigir nuestra mira al último evento bélico que sacudió a todo el mundo: la segunda guerra mundial. La guerra en general dejo marcado a la humanidad, desde los actos inhumanos cometidos como la Alemania Nazi, los millones de muertos aportados por la mayoría de los países del mundo y no podemos olvidar las marcas que dejo en la historia de Japón las dos bombas nucleares que acabaron con miles de vidas, marcando estos eventos el fin de la guerra con la rendición de Japón. Y es al final de la guerra donde tenemos uno de los primeros trabajos de espionaje que marcarían el inicio de la Guerra Fría. El 4 de agosto de 1945, los lideres de Estados Unidos y la URSS (actualmente Rusia) se reunieron para fijar el futuro del mundo, una reunión que se veía como un acto de buena voluntad por dos de las naciones que estuvieron al frente del evento bélico más grande del siglo pasado y este evento se cerró con un regalo entregado al cual se le nombro La Cosa (The Thing en inglés). Dicho detalle reposo siete años en la casa de **Averell Harriman** (1891,1986), embajador de Estados Unidos quien fue en representación de su país a dicho encuentro, sin revisión alguna y sin saber que detrás de su creación se encontraba **Leon Theremin** (1896, 1993), un genio del sonido, quien podemos recordar por la creación del Theremin, el instrumento que no requiere de ser tocado para generar sonidos. (Espert, 2017; Harford, 2019)

Ilustración 3 Henry Cabot Lodge y La Cosa.

La historia detrás de la construcción de La cosa nunca ha sido clara, pero se define que después del regreso de Theremin a la unión soviética en 1938 fue retenido por el gobierno y obligado en los campos de concentración a construir el elemento de espionaje mas sofisticado en esa época. El funcionamiento de la cosa era demasiado simple: dentro del armatroste de madera con el símbolo del águila de Estados Unidos, se encontraba una antena única a una

cavidad con una lamina plateada encima, sin ninguna batería, este dispositivo era capaz de alimentarse por ondas de radio emitidas por los soviéticos, y emitiendo a su vez por las ondas de radio que recibía las ondas de sonido que chocaban con la placa plateada. Gracias a que los sonidos que chocaban con La Cosa se emitían por las emisoras de Estados Unidos, en donde se escuchaban conversaciones privadas de Harriman, es como se pudo rastrear a La Cosa. (Espert, 2017; Harford, 2019)

Toda esta larga historia de preámbulo nos ayuda a contextualizar el inicio de la lucha entre Estados Unidos y Rusia, incluyendo los sucesos que marcaron la Guerra Fría, como lo fueron la carrera espacial (1955-72), la crisis de los misiles en Cuba (1962) la Alemania dividida hasta la caída del muro de Berlín (1989) (Kelly, 2014), nos dejaron una guerra que se puede considerar mucho más fría debido a como ya no se requieren de armas de fuego o grandes ejércitos: la ciberguerra. Esta guerra se vive detrás de ordenadores y ha ido teniendo un mayor impacto en las vidas de todos debido al avance de la tecnología y como esta cada vez nos facilita mucho más las vidas. Y a su vez les facilita a los contendientes en esta guerra cibernética el poder atacar a sus adversarios. A continuación, se van a exponer algunos eventos que han marcado esta guerra:

1. **Pegasus**: este software de espionaje cambio el paradigma de como el malware puede tener acceso a nuestros datos personales almacenados en nuestros dispositivos móviles. (ver Pegasus)
2. **Stuxnet**: la primera ciberarma, la cual se le adjudicó su creación a la NSA y a Israel, la cual fue capaz de generar un daño inmenso en la central de energía eléctrica de Natanz (ver Stuxnet)
3. **Estados Unidos Vs. China**: no se puede hablar de ciberguerra sin mencionar a China, una de las potencias en ciberseguridad tanto que ha llevado a sus habitantes a vivir ciber-aislados del mundo. Pero esto no ha evitado que los productos que se fabrican en China hallan sido fichados por el gobierno de Estados Unidos como elementos por medio de los cuales el gobierno chino obtenga información sobre Estados Unidos. El ejemplo más conocido de este tema se dio con el veto a la empresa de telecomunicaciones y tecnologías móviles Huawei en el 2019, esto debido a las obligaciones que tienen las empresas chinas de proveerle información al gobierno sobre los ciudadanos del país oriental, esta obligación fue tomada por el gobierno de Donald Trump como una amenaza a la información y privacidad de los estadounidenses. (Alonso, 2020; DW Redacción, 2021)
4. **Rusia interviniendo las elecciones estadounidenses**: ciberdelincuentes asociados al Kremlin fueron fijados como los responsables de intervenir los resultados de las elecciones, según la CIA, para favorecer a Donald Trump en las elecciones del 2016. Aunque el presidente electo si resulto ser Donald Trump, este mismo negó lo comunicado por la CIA, sin olvidar que Trump, en su campaña presidencial hizo la invitación al gobierno ruso de hackear a su contrincante en las elecciones, Hillary Clinton. El incidente fue ignorado por el Trump y despreciando totalmente la ciberseguridad del gobierno. (Reacción El Periódico, 2017)
5. **Solar Winds**: este es el nombre de una empresa que presta servicios de software de TI para entidades gubernamentales estadounidenses, la cual sufrió un ataque en el

2020 que comprometió la actualización de su sistema y a su vez el servicio de sus clientes de mayor importancia: el Ejército de EE.UU., el Pentágono, el Departamento de Estado, de Comercio, el de Tesoro y la Oficina presidencial estadounidense. Este ataque fue atribuido por el secretario de Estado, Mike Pompeo, a Rusia. (Corera, 2020)

6. **La NSA**: la Agencia de Seguridad de Estados Unidos ha sido una entidad de interés en el panorama de la ciberseguridad ya que se han revelado varios casos de ciber espionaje, tanto dentro del territorio estadounidense como en otros países, de los cuales esta agencia se ha deslindado o han dicho que su único interés es obtener información que les ayude a prevenir problemas futuros. (Thiber, 2013)
7. **Ataques contra infraestructuras prestadoras de servicios**: se han presentado varios ataques a lo largo de los años los cuales van dirigidos a centrales de energía, ya que se considera como un servicio de vital importancia en el mundo digital en el que nos movemos. De este tipo de ataques tenemos el sufrido por una central eléctrica en Ucrania el 23 de diciembre del 2015, el cual se adjudico a Rusia. Otros ataques contra centrales eléctricas se dieron en Estados Unidos contra compañías eléctricas y la planta nuclear Wolf Creek en Kansas. También se han dado indicios de intentos de Estados Unidos en irrumpir en los sistemas eléctricos de Rusia. (Lima, 2019)

Todos estos eventos de ciberataques han desembocado en generar un malestar general por los gobiernos de los países involucrados y otros países que también han sido tocados por esta ciberguerra, ya que, como hemos visto, el impacto de estos eventos ha tenido que ver con las relaciones internacionales, la economía, las comunicaciones, la prestación de servicios básicos, los cuerpos electorales y la privacidad de todas las personas, todo esto nos presenta un escenario muy oscuro, en donde no se requieren de muertes para demostrar la supremacía o poder de un país, sino de genios en la informática que sean capaces de afectar la calidad de vida de un país y este escenario se hace cada día más palpable al ver cómo, servicios que antes se realizaban manualmente o presencialmente, se han trasladado a la red. Esto último demandará a que cualquier empresa que posea o desarrolle tecnología se blinde a más no poder de los ataques que puedan sufrir, entre mas critico sea el servicio, producto o información que posea una empresa, más cuidado deberá tener de ser afectado por la guerra cibernética. (Armapedia, 2021)

Facultad de ingeniería

Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO

4. Primer Ciberarma – STUXNET

Los conflictos entre naciones han sido parte de nuestra historia, y por muchos años se creyó que la violencia, las invasiones con grandes ejércitos llenos de armas y la obtención de territorios o cualquier objeto de interés son alguno de los pilares que han definido el concepto de guerra. Pero como muchas actividades humanas, la guerra ha evolucionado al pie del mismo avance tecnológico, pasando de usar armas de fuego a armas que se mueven por los sistemas informáticos en los cuales se fundamenta casi toda nuestra vida. Este último elemento es el cual hace tan letal a las ciberarmas: el poder de acabar con vidas humanas limitando el acceso a servicios de vital importancia, estropear sistemas informáticos de vital importancia que al fallar pueden generar un daño fatal. Esto fue lo que tanto preocupo a organizaciones sobre seguridad informática, naciones y cualquier entidad en general al aparecer STUXNET, antes de todo, se debe hablar del contexto histórico en el que apareció este virus. (Romero, 2018)

Contexto histórico

La segunda guerra mundial había terminado y los estragos que dejaron las bombas lanzadas sobre Hiroshima y Nagasaki demostraron la letalidad de la energía nuclear utilizada con fines bélicos, lo cual dejo al mundo el mensaje claro de la letalidad de estas armas y en general definió estándares de control con relación al manejo de energía nuclear, aquí podemos recordar el tratado de no proliferación de las armas nucleares (*Tratado de No Proliferación Nuclear*, 1970), este tratado define la posesión de armas nucleares por ciertos países, de los cuales el más importante es Estados Unidos, quienes controlan en su mayoría la creación de los programas nucleares alrededor del mundo y vigilan las actividades que se ejecutan sobre estos. Recordemos que el tratado entro en vigor hasta 1970, y tuvo dos años para que se lograran obtener la firma de los líderes políticos de 191 países.

Pero aquí debemos movernos 5 años después del fin de la segunda guerra mundial, en 1950, donde Estados Unidos tenia por presidente a Harry Truman, en Irán se vivía un momento muy bueno, conocido como la Época del poderoso Sha de Persia: **Reza Pahlevi**. En el gobierno de Reza se vio la oportunidad de crear energía mediante la tecnología nuclear, todo esto con fines pacíficos y siendo apoyados por el gobierno estadounidense. Estos ideales se vieron detenidos por la Revolución de 1979, en la cual se derroco a la familia Pahleví motivados por temas como el descontento social con los lideres del país y la occidentalización, todo esto termino todos los proyectos de la dinastía que controlaba el país, y aquí fue donde el programa nuclear cerro. (Gómez, 2017; Romero, 2018)

Ilustración 4 La revolución iraní le dio una vuelta de 180° a todos los aspectos del país.

Con la revolución Iraní, Estados Unidos inicio un conflicto con dicho país, siempre teniendo presente la existencia de los sistemas nucleares y temiendo por un mal uso de estos. Los líderes del país siempre declararon que hacían uso del programa nuclear solamente para proveer energía a su país, pero el 2002, Estados unidos, la OIEA (Organismo Internacional de Energía Atómica), ONU y otras naciones interesadas se dieron cuenta de cómo Iran construía instalaciones secretas en las cuales se realizaban procesos de enriquecimiento de uranio muy cerca de la ciudad de Natanz, lo cual genero un gran malestar ya que Irán, mientras la dinastía Pahleví gobernaba el país, había firmado el Tratado de no proliferación Nuclear (*Tratado de No Proliferación Nuclear*, 1970) y el no comunicarle a los demás países que integraban el tratado de la existencia de dichas instalaciones era una violación total al tratado y la preocupación creció mucho más al obtener la información de que, el tamaño de las instalaciones no era acorde al de un sistema que podría proveer energía a las ciudades, siendo cerrada dicha instalación en el 2003 y reabierta en el gobierno de **Mahmoud Ahmadinejad**, en el 2009, creando un ambiente tenso en el cual el presidente israelí, **Benjamín Netanyahu**, le exigió a la ONU que controlara la situación y presionara a Irán a cerrar por completo dichas instalaciones, si esto no se cumplía, Israel bombardearía dichas instalación es, lo cual generaría un daño de grandes magnitudes debido a los materiales que se almacenan en dichas instalaciones nucleares. (Gómez, 2017; Romero, 2018)

Una nueva preocupación: Stuxnet

Sumándole a este ambiente tan tenso, en Julio de 2010, Kaspersky, una de las empresas con mayor conocimiento en ciberseguridad alrededor del mundo la cual es conocida por su antivirus NOD32 (Gentile, 2017; Langnet, 2011), recibió en sus laboratorios de investigación ubicados en Rusia un nuevo virus, esto demandaba realizar las siguientes actividades:

- Tomar muestra del programa malicioso

- Decodificarlo hasta el nivel de código maquina base
- Analizar el código y buscar instrucciones, patrones, elementos que permitan conocer el funcionamiento del programa
- Dar a conocer los hallazgos
- Incluir el virus y toda la información que permita detectarlo en una base de datos para ser usada por un antivirus.

Estos procesos duraban días y como máximo una semana, pero cuando llego la muestra de Stuxnet, se gastaron 6 meses en poder obtener información, además de requerir del subir el código extraído del programa malicioso para que otras entidades de ciberseguridad lo estudiaran y ayudaran en el proceso de neutralización del virus (Gentile, 2017; Langnet, 2011). Algunas de las características que hicieron a Stuxnet un virus de cuidado eran las siguientes:

- **Tamaño**: los virus convencionales sueles tener un tamaño en ficheros muy pequeño, pero Stuxnet tenia un tamaño 6 veces más grande lo común.
- **Forma de infección**: los ordenadores se infectaban por medio de un USB/Pendrive el cual tuviera el virus.
- **Zero-Day vulnerabilidades**: para que un virus pueda entrar a cualquier sistema requiere de hacer uso de las vulnerabilidades de seguridad que este posee, aquí es donde entra el concepto de exploits (software especializado en la explotación y aprovechamiento de vulnerabilidades). En este caso, Stuxnet aprovechaba cuatro vulnerabilidades de Windows de Zero-Days, las cuales son todas aquellas vulnerabilidades que no han sido detectadas por los distribuidores y desarrolladores de cualquier sistema y que se mantienen ocultas y desde el día de lanzamiento del sistema.
- **Empresas firmantes**: todo programa en su distribución cuenta con una firma digital la cual ayuda a detectar de donde provienen, en el caso de Stuxnet se encontró la firma de Realtek, empresa conocida por ser la encargada del desarrollo de los drivers y programas básicos de Windows. Lo cual preocupa demasiado ya que solo las placas de sonido pueden tener esta firma y esta no se puede extraer, solamente se puede obtener desde los puntos de fabricación de las placas.
- **Comportamiento**: sumándole a los elementos anteriores, los ordenadores que se infectaban con Stuxnet no realizaban nada, no se veían afectaciones o problemas generados por dicho virus.
- **Elementos del código**: al analizar el largo código que componía a este virus, se encontraron partes en las cuales se hacia referencia a la empresa Siemens, empresa conocida por la producción de maquinas para el sector industrial, y en especial se hacia referencia a un modelo especifico creado por la empresa alemana.

La última característica fue la que genero mayor interés por parte de los expertos en seguridad, ya que el modelo que se indicaba en el código hacia referencia a una maquina PCL (SRC, 2018), maquinas que se dedican especialmente a la ejecución de ciertas tareas de control de maquinas de manufactura y procesos industriales, tales como los brazos mecánicos que podemos ver en las líneas de producción. Dichas maquinas son de vital importancia, y el que un virus busque inyectar código que afecte su funcionamiento aumentaba mucho más las dudas sobre Stuxnet, debido a lo difícil que es llegar a contagiar o afectar el comportamiento de estas máquinas y la estructuración del código que se les inyectaba.

Los expertos de seguridad previamente ya habían comunicado a compañías de seguridad alrededor del mundo para que detectaran los casos de infección con este virus y se encontró que Irán era el país con mas casos reportados, lo cual genero mucha mayor tensión, todo esto debido al programa nuclear que generaba tanta turbulencia en el mundo (Davila, 2014). Y dichas preocupaciones se hicieron materiales al armar una especie de rompecabezas compuesto por las siguientes piezas:

- **Maquina PCL**: se definió que el modelo de máquina que se describía en el código hacia referencia a una caja gris, sin pantalla, la cual estaba destinada para la automatización de los procesos de centrifugado de uranio, procesos mediante los cuales se enriquece el uranio y de esta forma obtener energía nuclear.
- **Planta de la ciudad de Natanz**: esta planta, como se describió antes, tiene una historia particular, paso de ser una infraestructura que operaba principalmente en los edificios de la superficie a tener más construcciones subterráneas y un nivel de vigilancia elevado.
- **Armas nucleares**: unido al punto anterior, el secretismo que el gobierno iraní estaba generando sobre dichas instalaciones aumentaba más las sospechas de que se estuvieran creando armas nucleares.
- **Amenaza de Israel:** recordemos la amenaza de bombardeo de Israel, la cual podía transformarse en un ataque mucho más sutil, rompiendo por completo algún proceso de vital importancia en las instalaciones nucleares de Israel.

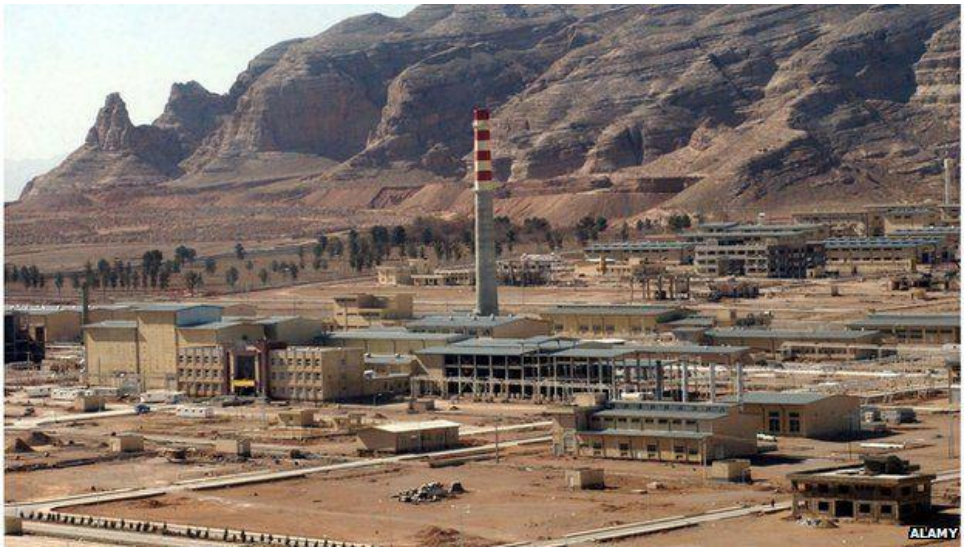


Ilustración 5 Central nuclear de Natanz, objetivo del ataque

Finalmente, el ataque se efectuó, llegando el virus a dicha planta, la cual como medida de seguridad no contaba con conexión a internet, pero, recordemos que el virus se trasmitía por medio de USBs/Pendrives, por lo que, alguien que tenia acceso a la planta y a sus instalaciones conecto uno de estos dispositivos con el virus en alguno de los computadores que controlaban las maquinas PCL, el virus al finalmente llegar a su objetivo, duro dos semanas en las que se dedicó a recopilar cada uno de los datos emitidos por las maquinas PCL conectadas a la centrifugadoras, esto con el fin de analizar el comportamiento de estas y generar un efecto espejo, en el que, al computador controlador de las PCL los datos que se le eran reportados eran una reproducción en bucle de los datos recopilados las dos semanas pasadas, y detrás de ese espejo o ilusión de buena operación de las maquinas, se alteró el código con las instrucciones de centrifugado, generando un comportamiento fuera de lo normal, en que se llevaba a un limite de velocidad y se detenía abruptamente, esto generaba que las maquinas de centrifugado quedaran insensibles, la poca información que se pudo obtener de la magnitud del daño generado por Stuxnet fue el de haber dañado al menos a 1000 maquinas de centrifugado, las cuales representaban una gran inversión del gobierno Iraní, el cual si estaba usando dichas máquinas para la creación de maquinas nucleares. (Gentile, 2017; Langnet, 2011)

Facultad de ingeniería

Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO

Ilustración 6 Caricatura con relación al ataque del virus Stuxnet a Iran

Después del ataque

Irán seguramente realizo su investigación (o simplemente lo dedujeron) y realizo varios ataques de negación de servicios DOs a varios servicios alojados en Estados Unidos, desde entidades bancarias hasta sitios web de vital importancia duraron algún par de horas sin poder ser accedidos. Tanto el altercado de Stuxnet como la respuesta de Iran son antecedentes que se juntan a la lista de la guerra cibernética, pero aun faltaba algo importante ¿Quién estaba detrás de Stuxnet? Esta respuesta llego en el 2013 (Del Palacio, 2013) cuando el consultor tecnológico y periodista estadounidense Edward Joseph Snowden revelo que los creadores de este virus tan elaborado eran la NSA (Agencia de seguridad nacional de Estados Unidos) e Israel, la atención se centro en la agencia estadounidense la cual ha tenido varios altercados al ser acusados de espionaje y de atentar contra la seguridad de otro países, defendiéndose de que todas estas actividades de espionaje se hacen con el fin de tener control de futuros altercados o problemas, tal como en este caso, que se detuvo las operaciones de una central dedicada a generar armas que podrían atentar contra toda la humanidad.

Facultad de ingeniería

Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO

5. Pegasus

A lo largo de la historia hemos observado cómo la información se convirtió en el oro del cual muchas personas se quieren hacer acreedores, esto lo podemos ver desde los inicios de la guerra fría cibernética hasta la actualidad en donde desde empresas hasta gobiernos buscan el poder de la información que podamos poseer nosotros como personas naturales hasta personas de gran interés como son los presidentes, periodistas y cualquier objetivo del cual se necesita tener control de la información que éste emite y recibe. Aquí es donde podemos encontrar a Pegasus, un malware el cual fue desarrollado por la empresa israelí **NSO Group**, enfocado en el ataque y la infección a teléfonos con sistemas operativos iOS y Android, obteniendo acceso a la información sin dejar ningún rastro del proceso de instalación, dándole cabida a que los atacantes puedan tener acceso tanto a fotografías, vídeos, historial de llamadas, micrófono, cámara y todo lo que esté dentro del dispositivo, pasando totalmente desapercibido a los ojos del propietario del dispositivo. (Gascón, 2021; Meza, 2021)

Se tuvo conocimiento de este malware con gran rapidez por un reportaje del periódico The Guardian el cual demostró una lista de 50,000 objetivos que fueron afectados por Pegasus, de los cuales su mayoría venían de México teniendo entre éstos personas de gran interés dentro del poder tales como 43 normalistas, 25 periodistas y personas que hacen parte de centros de protección de Derechos Humanos. El hallazgo se pudo realizar gracias a la investigación realizada por 17 organizaciones de medios tales como la ONG Forbidden Storie y Amnistía Internacional quienes pudieron rescatar la lista previamente indicada, a partir de esto se pudo evidenciar casos de periodistas alrededor del mundo de los cuales denunciaron el estar infectados con este malware. (Cid, 2021; Reyes, 2021)

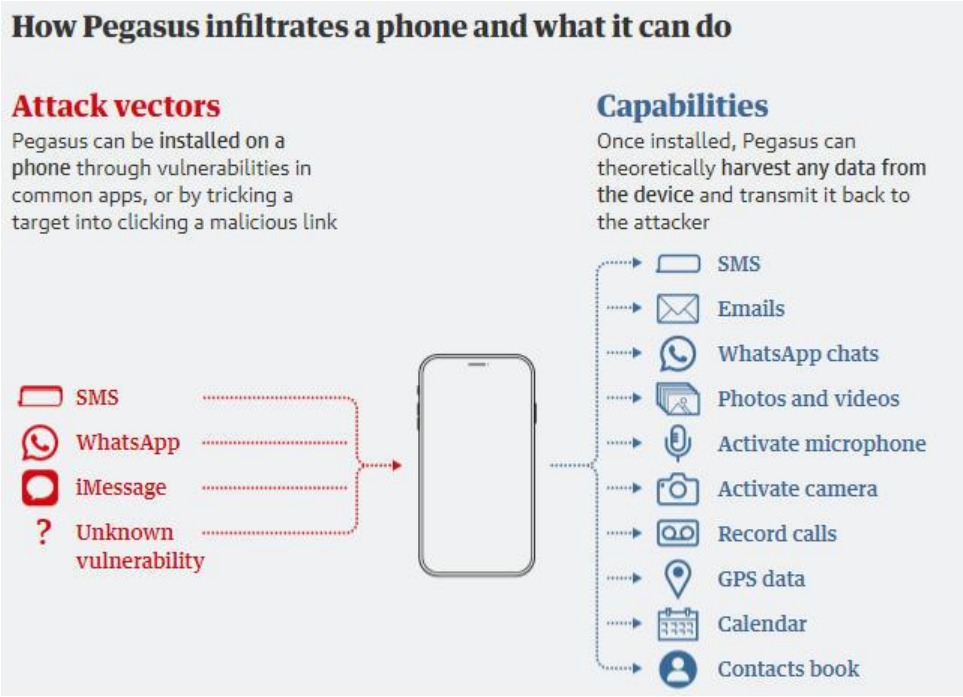


Ilustración 7 funcionamiento de Pegasus

La preocupación que ha generado Pegasus en la Comunidad de la ciberseguridad está enfocada en la forma en cómo los dispositivos son infectados ya que se han dado casos desde métodos en los cuales se puede tener acceso al teléfono por medio de mensajes de texto, URLs de correos electrónicos o cualquier elemento que el usuario requiera hacer clic, hasta llegar al límite de sólo requerir que el dispositivo del objetivo reciba algún mensaje o llamada y de esta forma comenzará el proceso de instalación de Pegasus aprovechando cualquier tipo de vulnerabilidades que pueden basarse de llegar a alterar el kernel del dispositivo para esta forma permitirle a los atacantes tener acceso a los datos de los objetivos. El grado de complejidad que pueda tener la infección de Pegasus tiene mucha relación con el dispositivo que va a ser infectado y el sistema operativo que éste posea hará la diferencia en cómo podrá ser infectado, por ejemplo, debido a las libertades que presenta Android en los procesos de instalación de aplicación, se puede deducir que Pegasus requerirá un grado de complejidad en su instalación mucho menor que el requerido para su instalación en iOS, sistema operativo conocido por su hermetismo. Cabe recordar que el grado de seguridad que tengan nuestros dispositivos también es nuestra responsabilidad, por lo que se recomienda no realizar modificaciones en el sistema operativo que puedan dejar puertas abiertas o vulnerabilidades a usar por los atacantes, no instalar aplicaciones de fuentes desconocidas y tener mucho cuidado con las URLs a las que tenemos acceso. (Blaich et al., 2020)

Facultad de ingeniería

Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO

Particularidades

1. **Zero click**: Pegasus genero la preocupación del mundo de la seguridad del software malicioso que se pueda ejecutar o desplegar sin que el objetivo tenga que intervenir lo cual hace mucho más difícil el poder detener los ataques de los ciberdelincuentes, y más en el caso de los dispositivos móviles, los cuales cuentan con mecanismos de seguridad mucho más bajos que otros dispositivos pero que a su vez tienen información de gran interés para los ciberdelincuentes. Esto podría requerir que Google y Apple mejores los mecanismos de seguridad de sus sistemas operativos y dispositivos. (Blaich et al., 2020)
2. **Responsabilidad de NSO Group:** la empresa israelí creadora Pegasus se ha deslindado sus responsabilidades con el uso que sus clientes le han dado, lo cual puede sonar como lo que llamamos como una lavada de manos por parte de la empresa, la cual solo da a conocer que sus clientes son gobiernos nacionales, y peor aún, negando que Pegasus ha sido usado después del 2018 lo cual se ha comprobado con los casos recientes en los que se ha denunciado el espionaje que han sufrido personas importantes en México y en distintos lugares del mundo. (Reyes, 2021)
3. **Derechos humanos:** las implicación con el derecho a la privacidad que tiene Pegasus son una preocupación que ha llegado a varias organizaciones que protegen los derechos humanos, tal cual como Amnistía Internacional ha declarado al opinar que Pegasus genera una “crisis internacional de derechos humanos”, ya que, al existir software por medio del cual el gobierno o cualquier organización obtengan información tan precisa y de primera mano sin autorización de nosotros, pues se pierde por completo la intimidad, el cual es un derecho que tenemos todas las personas. (Reyes, 2021)

6. Jailbreak

En el mundo, los dos sistemas operativos que dominan los mercados son Android, lanzado como sistema operativo por Google en el 2007, y iOS, lanzado en 2007 por Apple como sistema operativo para el primer iPhone. Cada uno de estos sistemas operativos presentan al usuario ciertas características, por un lado, tenemos a Android, un sistema que se caracteriza por ser más abierto con temas como la personalización, instalación de aplicaciones e implementación en dispositivos, por otro lado, tenemos a iOS, el cual es un sistema muy hermético, limitante en características como la personalización, pero que a su vez presenta mayor nivel de seguridad que Android. En el tema de la seguridad debemos tener en cuenta que Android, al ser un sistema dado a la implementación y modificación por parte de empresas desarrolladoras de móviles, ha sido abierto a modificaciones por parte de los usuarios, esto realizándose por medio de aplicaciones o programas, hasta llegar al punto de hacer uso del Root, proceso mediante el cual se modifica el Kernel del dispositivo. En iOS también existe este proceso, el cual se conoce con **Jailbreak**. (Magaudda, 2010)

El proceso de Jailbreak (Se puede traducir al español como Fuga, ya que se abren todas las puertas de la prisión, como se le llama al sistema operativo iOS), según (Ortega, 2017), está enfocado en romper el **Code-spining** (medida de seguridad en dispositivos con iOS que limita la descarga, instalación y ejecución de aplicación no autorizadas), además de realizar una modificación en el Kernel que permite un acceso completo a todo el sistema. Recordemos que iOS, al ser un sistema enfocado a solo dispositivos Apple, es mucho más controlado ya que no se debe tener control de tantas arquitecturas y dispositivos (caso contrario de Android), por lo que Apple no permite el uso de aplicaciones que no hayan sido firmadas por alguna entidad de confianza, controlando así problemas de malware o de aplicaciones que afecten la experiencia del usuario.

Historia del Jailbreak

Desde la aparición del primer iPhone, en el 2007, se ha venido realizando el Jailbreak, siempre motivado por las limitaciones que el sistema le presentaba a sus usuarios, como fue en caso del primer IPhone, el cual ya tenía el método de Jailbreak 11 días después de su lanzamiento, todo esto era información que rondaba en foros de internet, y constaba de una gran cantidad de pasos para poder realizarse (clic aquí para ver el método de Jailbreak para el primer IPod Touch), y en el mundo del Jailbreak tenemos nombres conocidos como **Gerge Hotz** (1989) conocido como **Geohot** (Buendia, 2015), quien desarrollo a sus 17 años (2007) a , **blackra1n** un método mediante el cual se podía eliminar el bloqueo de operador (medida que se aplicaba en ese entonces a los iPhones para que estos solo fueran usados con la compañía telefónica AT&T), también siguió detectando vulnerabilidades en iOS por medio de las cuales pudo generar varias versiones de Jailbreak y finalmente conocido por ser demandado por Sony al romper la seguridad del sistema de la PlayStation 3.

Otro nombre muy conocido es el de **Nicholas Allegra** o conocido también por su alias **Comex** (Chipana, 2013; Moses, 2011), que a sus 19 años (2011) creo una página web desde la cual

se podía realizar el proceso de Jailbreak a dispositivos con sistema operativo iOS, Comex logro notoriedad al ser contratado por Apple con el fin de mejorar la seguridad en sus dispositivos móviles y su sistema operativo, todo esto después de lanzar la tercera versión de

Ilustración 8 En orden, Geohot y Comex

JailbreakMe en el verano del 2011. Aunque solo duro un año en la compañía, dejo en estos grandes avances en para la seguridad del sistema iOS. Y la historia del Jailbreak no se ha detenido, hasta hoy en día en las redes podemos seguir encontrando herramientas de autores anónimos las cuales le permiten a quienes las emplee el poder comenzar a manipular sus dispositivos como lo requieran. (Ortega, 2017; Sami, 2013)

Tipos de Jailbreak

La clasificación que se le ha dado a los distintos métodos que existen para aplicar Jailbreak a dispositivos iOS se ha dado con relación a la dependencia de un computador para su realización y su permanencia después de que el dispositivo sea realizado. Los tipos de Jailbreak son los siguientes, ordenados desde el más eficiente al menos eficiente con base a lo expuesto por (Ortega, 2017):

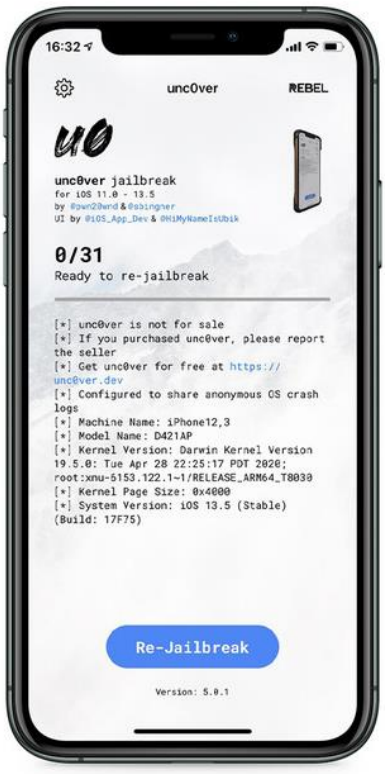
- **Untethered**: este primer tipo de Jailbreak no depende de usar un computador para su aplicación en el dispositivo y garantiza que al reiniciar el dispositivo no se perderá el desbloqueo realizado con el Jailbreak, esto debido a que, al iniciar el dispositivo iniciara con el Kernel de Apple y luego se ejecutara un **exploit** (programa o secuencia de comandos que aprovecha las vulnerabilidades para desencadenar un comportamiento o actividad no permitía por el sistema) el cual dejara al kernel parcheado. Este tipo de Jailbreak se considera como el más efectivo, pero a su vez requiere de mucho conocimiento de ingeniería a la inversa para su implementación.

- **Semi – Untethered**: este tipo de Jailbreak se basa en la modificación del Kernel mediante una serie de aplicaciones que deben ser instaladas en el dispersivo, pero dado sea el caso que se reinicie el dispositivo, el kernel volverá a su estado original y nos permitirá usar el dispositivo, para volver a activar todos los cambios ejecutados con el Jailbreak se debe recurrir a las aplicaciones previamente indicadas. La ventaja de este tipo de Jailbreak radica en no requerir del uso de un ordenador para su aplicación.
- **Semi – Tethered**: A comparación del anterior tipo de Jailbreak, en este si requerimos del uso de un computador y una herramienta en este que permita la modificación del kernel, y al momento de que reiniciemos el dispositivo, volveremos a tener el kernel original y se nos permitirá usar el dispositivo normalmente, deberemos volver a acudir al computador para recuperar la modificación del kernel y del comportamiento del dispositivo.
- **Tethered**: este último tipo de Jailbreak es el peor de todos, yaz que requiere del uso de un ordenador para su aplicación, pero dado sea el caso que reiniciemos el dispositivo, este se quedara en un loop infinito de reinicios hasta que volvamos a aplicar la modificación del kernel mediante el computador y la herramienta requerida.

Proceso de Jailbreak

Para el proceso de Jailbreak seguiremos los siguientes pasos, estos siendo descritos por (Aguilar, 2020; IONOS, 2020):

1. Para procurar que nuestros datos almacenados en nuestro dispositivo no se vean afectados por el proceso, realizaremos una copia de seguridad y conectaremos nuestro dispositivo a un computador con el fin de pasar archivos que requeríamos.
2. Desactivaremos también el bloqueo mediante código de seguridad, y dado sea el caso que nuestro dispositivo tenga Touch ID también desactivaremos el bloqueo mediante este medio, para esto nos dirigimos a los Ajustes y buscamos la opción Touch ID y código, ahí desactivaremos todos los elementos de desbloqueo existentes.
3. En este punto seleccionaremos la herramienta por medio de la cual realizaremos el proceso de Jailbreak, se recomienda hacer uso de métodos en donde se requieran instalar aplicaciones dentro del móvil, ya que en el caso que se reinicie el dispositivo se podrá recuperar más fácilmente todo lo realizado con el Jailbreak.



Dado a que el realizar Jailbreak a los dispositivos con iOS ya es un deporte o una actividad que denota un reto, se ha dado el caso de que se ha podido implementar Jailbreak a versiones del sistema

operativo desde el día cero, como se dio con la versión 13.5, lanzada en mayo del 2020, en (Aguilar, 2020) exponer lo simple que es realizar el proceso (sin olvidar que los pasos anteriormente expuestos se realizan con el fin de preservar la información personal antes del Jailbreak). Dicho proceso se resume en los siguientes pasos:

1. Instalar AltStore en el Mac o PC e introducir el Apple ID des dispositivo.
2. Instalar AltStore en nuestro dispositivo (iPhone o iPad).
3. Descargar Unc0ver (aplicación para realizar Jailbreak desde el mismo celular) desde Safari y lo instalamos con AltStore.
4. Abrir Unc0ver y hacemos el Jailbreak. Al finalizar el proceso debemos encontrar a Cydia (Slye, 2024), aplicación que permite la modificación del móvil (aspecto, aplicaciones, etc.).
5. Abrimos Cydia e iniciar la personalización del dispositivo.

Unc0ver es una aplicación para realiza Jailbreak del tipo Semi – Untethered.

Ventajas y desventajas del Jailbreak

En la siguiente tabla se expondrás algunas de las ventajas y desventajas que se obtendrán al realizarle Jailbreak a un dispositivo con iOS, todas estas con base a lo encontrado en (Aguilar, 2020; IONOS, 2020; Ortega, 2017)

Ventajas	Desventajas
Se podrán instalar aplicaciones que no se encuentren disponibles en la App Store.	Al instalar aplicaciones que no cuenten con la firma digital de alguna entidad autorizada, se puede instalar Malware o dejar la puerta abierta para ataques y perdida de datos.
Podrá personalizar la apariencia de su dispositivo por completo implementando iconos, animaciones, widgets y demás elementos que proviene de Cydia. A estas modificaciones a la apariencia en iOS se le llaman **tweaks**	El uso en excesivo de **tweaks** podrá mucho más rápido la batería del dispositivo.
Se puede acceder a archivos ocultos del sistema.	La manipulación sin conocimiento de archivos del sistema puede dejar inservible el dispositivo.

Se pueden eliminar las recciones de conexiones Bluetooth que tenga el dispositivo.	
Se pueden desinstalar las aplicaciones instaladas por el fabricante.	
	Si se requiere de hacer uso de la garantía o sustitución de dispositivo que brinda Apple no se podrá realizar efectivo.
	No se podrá actualizar el sistema operativo a las nuevas versiones que lance el fabricante, por ende, no se podrían instalar los nuevos parches de seguridad.
	El dispositivo queda totalmente expuesto a cualquier software o ataque, hasta puede ser parte de una red de dispositivos con algún fin delictivo.

Ilustración 10 ventajas y desventajas del Jailbreak

Recordemos que el realizar Jailbreak a los iPhones es legal desde el 2010, ya que se eliminó de la ley de derechos de autor de Estados Unidos (Moren, 2010), y en los años siguientes se incluyeron a los iPads, pero que sea legal no elimina los problemas que esta práctica que pueda conllevar, además que Apple no se hará responsable por ningún daño que tenga los dispositivos a los que se les realice Jailbreak.

Facultad de ingeniería

Programa Ingeniería de sistemas

Docente: J Eduar Criollo S

Asignatura: TECNICAS DE ATAQUE

Código estudiante: 30000050832 – LUIS FELIPE VELASCO TAO

7. Hacking ético Vs Escaneo de vulnerabilidad Vs. Pentesting

Estos tres conceptos entre si guardan una gran relación ya que todos están relacionados al mundo de la seguridad informática, siendo practicas por medio de las cuales se puede buscar la detección de problemas de seguridad en los sistemas de información de una empresa, pero cada concepto requiere de su explicación ya que ninguno de estos es lo mismo.

Hacking Ético

A lo largo de la era digital en la que nos movemos se ha asociado muy mal el concepto de hacker o de hacking con actividades delincuenciales, y todo esto se debe a factores como el entretenimiento que nos presentaba la imagen de una persona con conocimientos en informática que está detrás de una computadora buscando robar los datos de una organización, obtener dañar un sistema y/o ganar dinero. Y este concepto está alejado de la realidad, ya que, como nos cuenta (), un hacker es quien busca conocimiento el cual le permita beneficiar al sistema de cierta entidad, por lo que la primera definición es mucho más la de un ciberdelincuente o un cracker. Un hacker y un cracker pueden tener los mismos conocimientos de seguridad informática pero los diferencia la forma en que aplican dichos conocimientos. (Gacharná, 2009; Villalobos, 2012)

Ahora, centrándonos en el concepto de Hacking ético nos referimos a cualquier actividad autorizada por una organización con el fin de detectar problemas de seguridad en los sistemas de información, siendo también conocido como Pentesting, ya que lo que se busca es obtener los puntos débiles dentro de un sistema, dichas actividades se apegan con relación a la legislación de ciberseguridad de cada país, en Colombia debemos tener presente la ley 1273 del 2009 en la cual se definen los delitos informáticos con el fin de interpelar acciones legales a quien cometa dichas actividades. Por lo que el hacking ético esta apegado a la legalidad, no solo por ser una actividad permitida por quien será el objetivo del hackeo sino también por la ley, teniendo en Colombia un panorama aún muy oculto de lo que es el Hacking ético y su función en la seguridad, no solo de las organizaciones sino de nosotros como usuarios de estos. (Ojeda-Pérez et al., 2010)

Cabe aclarar que el hacking ético no solo queda reservado las actividades que un profesional de seguridad en sistemas informáticos puede desarrollar, también entrar personas que son entusiastas o que estas iniciando la adquisición de conocimientos sobre la seguridad informática, que pueden realizar pequeños ejercicios con relación a como se puede penetrar un sistema, que tienen conocimientos sobre cómo se comporta un sistema, como fluyen los datos en estos y que, en un futuro, podrán prestar sus conocimientos para reforzar la seguridad de una empresa. (Gacharná, 2009; Serrano, 2017; Villalobos, 2012)

Ilustración 11 El hacking busca prevenir los ataques de los ciberdelincuentes

Escaneo de vulnerabilidades

El escaneo de vulnerabilidades hace relación a la actividad desempeñada, ya sea por un software especializado o por un profesional de seguridad, por medio de la cual se obtiene información sobre las vulnerabilidades que puede tener un elemento en concreto, sea un sistema o un elemento de este. Esta actividad se puede considerar como parte del Pentesting, ya que se busca es detectar los puntos débiles de un elemento, rescatar información de estos y hacer uso de esta, ya sea para ser documentada, comunicada a los dueños del sistema o elemento analizado o explotarla. Esta actividad se puede definir como parte del ciclo de vida de la gestión de vulnerabilidades, siendo su primera fase, en la cual se descubren y especifican las vulnerabilidades que requieren ser eliminadas. (Guerrero et al., 2015)

Aquí podemos definir ciertas herramientas que sirven para realizar escaneos sobre distintos componentes de un sistema, de modo tal se pueda rescatar información sobre las vulnerabilidades que este posee (Ramos, 2013; Vanegas, 2019):

- **NMAP**: este software multiplataforma nos permitirá explorar información sobre las redes de comunicación de un sistema, los servicios que se usan, los sistemas operativos de los equipos que componen la red y de modo tal extraer las vulnerabilidades de estos componentes. Cabe recalcar que la extracción de las vulnerabilidades no la realiza el mismo software, por lo que es tarea del usuario el analizar la información entregada por NMAP y así definir las vulnerabilidades en base a esta.

Ilustración 12 Logo de Nmap

- **Nessus**: es uno de los escáneres de vulnerabilidades más usados, ya que cuenta con una se las bases de datos más grandes en donde se recopilan las vulnerabilidades de los equipos, por lo que es un software que se mantiene muy actualizado. Su funcionamiento es simple, ya que se le dan las IPs de los hosts (equipos a analizar) y comienza a analizar los puestos de cada uno de estos, realizando exploits (actividades y software de explotación de una vulnerabilidad) y rescatando la información resultante de todo el proceso.

Ilustración 13 Logo de Nessus

- **OpenVAS**: principal competencia de Nessus, ya que presenta una base de datos muy fortalecida con más de 50.000 test de los cuales se obtiene información sobre las vulnerabilidades que puede tener cualquier equipo. Este software libre presenta entre sus funcionalidades pruebas autenticadas y no autenticadas, protocolos a nivel industrial y de internet de alto y bajo nivel, todo esto lo hace una herramienta de gran valor para la detección de amenazas dentro de un sistema.

Ilustración 14 Logo de OpenVAS

- **Nexpose**: esta herramienta de escaneo de vulnerabilidades y Pentesting, por medio de la cual se puede obtener información de vital importancia sobre una red de equipos, de modo tal se presenta un sistema de administración para el escaneo continuo de

vulnerabilidades, siendo muy completo al presentar informes, la inclusión de motores externos, especiación de fechas y horarios de escaneo, alertas y demás elementos para obtener la información requerida.

Ilustración 15 Logo de Nexpose

Pentesting

Como parte de las actividades por medio de las cuales se puede medir la seguridad de cualquier sistema de información y obtener información que permitía su continua mejora, ya que en cualquier sistema informático, sea una página web, una base de datos de una organización, una aplicación móvil, un dispositivo o componente de software y/o hardware se requiere reconocer cualquier punto de mejora con relación a su rendimiento y seguridad, aquí es donde el Pentesting entra en acción, ya, como nos relata (Guillen, 2017; Vanegas, 2019), es una actividad o metodología mediante la cual se pueden obtener los puntos débiles o vulnerabilidades de cualquier sistema mediante la recolección de información que permitan la penetración dentro del sistema y así poder conocer cuanto daño se puede generar en dicho sistema. Esta actividad es de vital importancia en los sistemas de información, ya que hace parte del proceso de auditorías internas y externas en los cuales se obtiene información sobre el estado de seguridad del sistema de información, tal cual como lo especifica la ISO 27001. (Organización Internacional de Estándares, 2013)

Las actividades de penetración a un sistema se pueden clasificar de distintas formas, algunas de estas son las siguientes (Ramos, 2013; Vanegas, 2019):

- **Según el objetivo**: este tipo de Pentesting hace referencia a si existe o no un objetivo en específico.
    - Pentesting con objetivo: este tipo de pruebas tienen fijados los elementos a los cuales se les van a realizar las pruebas, comúnmente se realizan sobre los puntos críticos de un sistema.
    - Pentesting sin objetivo: al ser sin objetivo, a lo que se le realizaran las pruebas será al sistema total, analizando cada uno de sus componentes, por lo que son pruebas mucho más laboriosas pero que a su vez buscan conocer el estado de seguridad de todo el sistema y a su vez detectar aquellos elementos que requieran atención.

- **Según la información que se tenga del objetivo**: previamente a que se realiza una prueba de penetración sobre un sistema, quien o quienes lo vayan a realizar deben medir el conocimiento que tengan sobre el objetivo, de aquí tenemos dos tipos:
    - Pentesting a ciegas: las pruebas se van a realizar con solo la información pública que se tenga del objetivo, por lo que se busca la perspectiva de un atacante externo.
    - Pentesting informado: este tipo de pruebas se realizan con el consentimiento de la empresa poseedora del objetivo y por medio de esta se rescatará información útil para realizar las pruebas.
- **Según su origen**: las pruebas se pueden realizar desde el interior de la organización que posee el objetivo o no, por lo que obtenemos dos tipos pruebas:
    - Pentesting externo: se realiza desde un lugar externo a la organización, sin hacer uso de su infraestructura tecnológica. También se puede llamar Pentesting remoto.
    - Pentesting interno: este tipo de pruebas se realizan dentro de la organización indicando los recursos de su infraestructura tecnológica que se van a utilizar. También se le puede llamar Pentesting local.

A parte de los tipos previamente presentado, se pueden definir tres tipos de Pentesting los cuales son los más conocidos y que mezclan elementos de los tipos de pruebas previamente expuestos, buscando s}de cierto modo obtener ciertos puntos de vista o escenarios en los que el sistema puede ser atacado (Ramos, 2013; Vanegas, 2019):

- **Pruebas de caja negra (Black-box)**: este tipo de penetración se realiza sin tener ningún conocimiento de la composición y estructura del sistema, por lo que se busca es tener el punto de vista de un atacante y así tener conocimiento de cuáles son los puntos que un ciberdelincuente puede aprovechar para perjudicar el sistema y a la organización. Este tipo de pruebas se aplican comúnmente a paginas o aplicaciones web, o a cualquier punto de acceso externo al sistema.
- **Pruebas de caja gris (Gray-box)**: este tipo de pruebas se enfocan en obtener el punto de vista de un componente humano interno de la organización, como un empleado el cual tiene cierto conocimiento del sistema, y de esta forma poder prevenir los ataques que se generen desde adentro del mismo sistema y organización.
- **Pruebas de caja blanca (White-box)**: en este tipo de pruebas el pentester tendrá pleno conocimiento del sistema, sus componentes, los usuarios que tienen acceso a este y los datos que el sistema almacena, por lo que se define como el peor escenario de ataque al que un sistema se puede enfrentar, de modo tal se busca obtener información de gran valor con el finde prevenir ataques de gran impacto en el sistema.

Ilustración 16 Herramientas de Pentesting

La estructura o metodología mediante la cual se aplican pruebas de penetración sobre un sistema se puede definir mediante cuatro pasos o etapas, aunque esto variara dependiendo de la metodología empleada (Ramos, 2013; Vanegas, 2019):

1. **Fase de recolección de información**: en esta etapa se recogerá la mayor cantidad de información sobre el objetivo, por ejemplo, se encontrará información sobre la red, los equipos que la componen, los servicios que estos equipos consumen y los datos que estos pueden manejar. El objetivo de esta fase es conocer lo más posible el sistema y para esto se puede hacer uso de herramientas como FOCA (herramienta para la extracción de metadatos en archivos), NMAP (herramienta para la extracción de información sobre alguna red, equipo de esta o servicio) y distintos servicios de internet de los cuales se pueda extraer información sobre las vulnerabilidades el objetivo. Si esta fase no se realiza con rigurosidad y total cuidado no se podrá tener éxito en las pruebas.

2. **Fase de análisis de vulnerabilidades**: con toda la información recopilada previamente, se van a detectar o elegir las vulnerabilidades por medio de las cuales se va a realizar la instrucción al sistema/objetivo y se contemplan las formas en que se pueden explotar dichas vulnerabilidades, de modo tal se tiene que tener presente aquí el ciclo de vida de la gestión de vulnerabilidades, conjunto de pasos por medio de los cuales se busca descubrir las vulnerabilidades, clasificarlas según su nivel de impacto sobre los activos, reportar las vulnerabilidades, corregir las vulnerabilidades y verificar que las amenazas se hayan eliminado.

3. **Fase de explotación de vulnerabilidades**: con todo el conocimiento previamente adquirido se va a proceder a la instrucción del sistema mediante las vulnerabilidades detectadas y la aplicación de ciertos procesos que permitan comprometer al sistema, de modo tal se pueda medir las implicaciones que esto podría provocar si un ciberdelincuente las efectúa. Aquí aparece el concepto de **exploit**, la cual es una herramienta de software que permite la explotación de vulnerabilidades detectadas en un sistema.

4. **Fase de documentación**: esta fase en realizar se debe ejecutar en cada una de las anteriores, esto con el fin de dejar plasmada la información rescatada, los procesos realizados y expresarle a la organización los resultados de las pruebas, recordemos que la documentación cumple un papel importante en cualquier actividad en la ingeniería.

Relación entre los conceptos

Con los análisis que se presentaron de cada uno de los conceptos podremos comprender que el Hacking ético son todas las actividad por medio de las cuales se mide la seguridad de un sistema, dentro de estas actividades tenemos al Pentesting el cual es un conjunto de actividades de recolección de datos sobre las vulnerabilidades de un sistema para explotarlas, dentro de las actividades de recolección de datos o información nos encontramos con el escaneo de vulnerabilidades, actividad por medio de la cual se emplean mecanismos para estudiar los componentes de un sistema y extraer las vulnerabilidades de esta para ser empleado en otras actividades, por ejemplo, en la eliminación de las vulnerabilidades o explotación de estas, como se da en el Pentesting.

Bibliografía

Aguilar, R. (2020, May 26). *He hecho jailbreak a mi iPhone en pleno 2020 y no me arrepiento de ello*. Xataka Movil. https://www.xatakamovil.com/apple/he-hecho-jailbreak-a-mi-iphone-pleno-2020-no-me-arrepiento-ello

Tratado de No Proliferación Nuclear, (1970) (testimony of Albania, Alemania, Andorra, Angola, Antigua y Barbuda, Arabia Saudí, Argelia, Argentina, Armenia, Australia, Austria, Azerbaiyán, Bahamas, Baréin, Bangladés, Barbados, Bélgica, Belice, Benín, … Zimbabue). https://www.un.org/disarmament/wp-content/uploads/2018/08/NPTSpanish_Text.pdf

Alonso, R. (2020, March 9). Ciberguerra fría: así es como los países utilizan la red para atacarse. *ABC Software*. https://www.abc.es/tecnologia/informatica/software/abci-ciberguerra-fria-como-paises-utilizan-para-atacarse-202002110358_noticia.html?ref=https%3A%2F%2Fwww.abc.es%2Ftecnologia%2Finformatica%2Fsoftware%2Fabci-ciberguerra-fria-como-paises-utilizan-para-atacarse-202002110358_noticia.html

Armapedia. (2021, May 14). *¿Cómo Funciona la Guerra Cibernética? - YouTube*. YouTube. https://www.youtube.com/watch?v=s0DJqoV_trs

Blaich, A., Bazaliy, M., & Hardy, S. (2020, January 8). *Mobile Espionage in the Wild: Pegasus and Nation-State Level Attacks - YouTube*. Black Hat. https://www.youtube.com/watch?v=Y6e_ctKqSqM

Buendia, J. (2015, December 17). *¿Quién es George Hotz?* MCPRO. https://www.muycomputerpro.com/2015/12/17/quien-es-george-hotz

Chipana, R. (2013). HACKERS QUE SE PASARON AL BANDO DE LA EMPRESAS. *Revista de Información, Tecnología y Sociedad*, *1*(8). http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442013000100009&script=sci_arttext&tlng=es

Cid, G. (2021, July 19). *Qué es Pegasus: así funciona el "software" espía israelí que "hackea"*

a medio mundo. El Confidencial. https://www.elconfidencial.com/tecnologia/2021-07-19/pegasus-espia-israeli-marruecos-programa-nso-group_3190996/

Corera, G. (2020, December 20). *SolarWinds: 5 ataques informáticos de Rusia que transformaron la ciberseguridad en Estados Unidos - BBC News Mundo*. BBC News Mundo. https://www.bbc.com/mundo/noticias-internacional-55381892

Davila, J. (2014). Cuando el malware se viste de ciberarma. *En Construcción*, *1*(109), 92–94. https://revistasic.es/archivo/images/pdf/109-en-construccion.pdf

Del Palacio, G. (2013, July 8). *La NSA colaboró en la creación de Stuxnet, según Snowden*. Hipertextual. https://hipertextual.com/2013/07/la-nsa-colaboro-en-la-creacion-de-stuxnet-segun-snowden

DW Redacción. (2021, March 13). *EE.UU. declara a Huawei una amenaza para su seguridad | El Mundo | DW | 13.03.2021*. DW. https://www.dw.com/es/eeuu-declara-a-huawei-una-amenaza-para-su-seguridad/a-56860457

Espert, R. (2017). *Leon Theremin: La cosa (El espionaje perfecto) - video Dailymotion*. Daily Motion. https://www.dailymotion.com/video/x5g3725

Gacharná, F. I. (2009). Hacker ético vs. delincuente informático: Una mirada en el contexto colombiano. *INVENTUM*, *4*(6), 46–49. https://doi.org/10.26620/UNIMINUTO.INVENTUM.4.6.2009.46-49

Gascón, M. (2021, July 19). *Así funciona Pegasus, el programa de espionaje israelí utilizado para "hackear" móviles de periodistas de todo el mundo*. 20 Bits. https://www.20minutos.es/noticia/4325938/0/asi-funciona-pegasus-el-programa-de-espionaje-israeli-utilizado-contra-torrent-y-otros-politicos-catalanes/?autoref=true

Gentile, N. (2017, December 6). *LA CIBERGUERRA: El caso de Stuxnet - YouTube*. YouTube. https://www.youtube.com/watch?v=FaeP6xoZOXc

Gómez, D. A. (2017). *ANÁLISIS DEL CIBERATAQUE PARA LA SEGURIDAD DE LOS ESTADOS Y SU INCIDENCIA EN LA TRANSFORMACIÓN DEL STATUS QUO: STUXNET EL VIRUS INFORMATICO.* . https://repository.urosario.edu.co/bitstream/handle/10336/13705/GomezLlinas-DanielAlejandro-2017.pdf?sequence=5&isAllowed=y

Guerrero, H. A., Lasso, L. A., & Legarda, P. A. (2015). *IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN EL CONTROL DE ACCESO AL SISTEMA DE GESTIÓN DOCUMENTAL, MEDIANTE PRUEBAS DE TESTEO DE RED EN LA EMPRESA INGELEC S.A.S*. https://repository.unad.edu.co/bitstream/handle/10596/3451/5203676.pdf?sequence=1

Guillen, L. J. (2017). *Introducción al pentesting* [Universidad de Barcelona]. http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf

HackerOne. (2021). *The 2021 Hacker Report*. https://www.hackerone.com/resources/reporting/the-2021-hacker-report

Harford, T. (2019, August 24). *La tecnología de espionaje de la Guerra Fría que todos usamos - BBC News Mundo*. BBC News. https://www.bbc.com/mundo/noticias-49442319

IONOS. (2020, February 3). *Jailbreak iOS: ¿Qué es jailbreak y cómo funciona? - IONOS*. Digital Guide IONOS. https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/jailbreak-ios/

Kelly, J. (2014, April 2). *Seis sucesos clave que definieron la Guerra Fría - BBC News Mundo*. BBC News Mundo. https://www.bbc.com/mundo/noticias/2014/04/140402_guerra_fria_revive_finde_ng

Langnet, R. (2011, March 29). *Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon - YouTube*. YouTube. https://www.youtube.com/watch?v=CS01Hmjv1pQ

Lima, L. (2019, June 19). *Estados Unidos vs Rusia: cómo el hackeo de las redes eléctricas se convirtió en un nuevo campo de batalla entre Washington y Moscú - BBC News Mundo*. BBC News Mundo. https://www.bbc.com/mundo/noticias-internacional-48668879

Magaudda, P. (2010). Hacking Practices and their Relevance for Consumer Studies: The Example of the ’ Hacking Practices and their Relevance for Consumer Studies: The Example of the “Jailbreaking” of the iPhone. *Jailbreaking’ of the IPhone*, *12*(1). http://csrn.camden.rutgers.edu/newsletters/12-1/magaudda.htm

Meza, A. (2021). Pegasus: cuatro preguntas clave sobre el escándalo de espionaje. *France 24 Revista Digital*, *1*(1). https://www.france24.com/es/programas/revista-digital/20210728-pegasus-escandalo-espionaje-internet-software

Moren, D. (2010, July 26). *Jailbreaking officially granted DMCA exemption*. Macworld. https://www.macworld.com/article/206764/jailbreak_exemption.html

Moses, A. (2011, August 30). iPhone hacker golden boy hired by Apple. *The Sydney Morning Herald*. https://www.smh.com.au/technology/iphone-hacker-golden-boy-hired-by-apple-20110830-1jj18.html

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010). Delitos informaticos y entorno juridico vigente en Colombia. *Cuadernos de Contabilidad*, *11*, 41–66. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&nrm=iso

Organización Internacional de Estándares. (2013). *ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online*. NORMA ISO 27001:2013. https://normaiso27001.es/#h4

Ortega, S. (2017). *Jailbreak en iOS: ventajas y riesgos* [Escuela Politécnica Superior de Alcalá de Henares]. https://ebuah.uah.es/xmlui/bitstream/handle/10017/31995/TFG-Ortega-Bel-2017.pdf?sequence=1&isAllowed=y

Ramos, J. L. (2013). *PRUEBAS DE PENETRACIÓN O PENT TEST*. http://tenable.com/

Reacción El Periódico. (2017, June 27). EEUU y Rusia se enzarzan en la ciberguerra fría. *El Periódico Internacional*. https://www.elperiodico.com/es/internacional/20161210/trump-ataca-a-la-cia-por-sus-conclusiones-sobre-el-espionaje-ruso-5681874

Reyes, I. (2021). Pegasus y el ciberespionaje en México. *Kasblog*, *1*(1). https://www.kas.de/documents/266027/13395798/KASBlog_semana_6_ciberseguridad.pdf/fb010bf5-f9c3-82e1-b656-e652b6cebcdd?version=1.0&t=1627922515880

Romero, G. (2018, May 16). *STUXNET: La primera ciberarma de la historia*. Crónicas Seguridad. https://cronicaseguridad.com/2018/05/16/stuxnet-primera-ciberarma-historia/

Sami, B. (2013, February 4). *La historia del jailbreak | Historia del jailbreak*. IPhone Islam. https://iphoneislam.com/es/2013/02/the-history-of-jailbreaking/25430

Serrano, E. (2017, October 18). *La necesidad de apoyar el hacking ético | Enrique Serrano | TEDxYouth@PaseodelPrado - YouTube*. TEDx Talks. https://www.youtube.com/watch?v=wyspktH7o6w

Slye, A. (2024, February 25). *What is Cydia? How to Use Cydia After Jailbreaking - YouTube*.

https://www.youtube.com/watch?v=lgvInNI3Wos&t=2s

Softley, I. (1995, September 15). *Hackers: Piratas Informáticos (1995)*. Metro-Goldwyn-Mayer. https://cuevana3.so/359/hackers-piratas-informaticos-1995

SRC. (2018, January 14). *¿Qué es un PLC? ¿Cómo funciona? ¿Para qué sirve?* SRC. https://srcsl.com/que-es-un-plc/

Thiber. (2013). La Agencia de Seguridad Nacional (NSA), el espionaje y colaboración público-privada en EEUU. *Real Instituto Eleano*, *41*.

Vanegas, A. Y. (2019). *Pentesting, ¿Por qué es importante para las empresas?* http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6286/00005220.pdf?sequence=1

Villalobos, J. (2012). Hacktivismo y DDoS: Tendencias actuales de ataque. *Seguridad, Cultura de Prevención TI*, *1*(12). https://www.ru.tic.unam.mx/bitstream/handle/123456789/1761/63.pdf?sequence=1&isAllowed=y

Tabla de ilustraciones