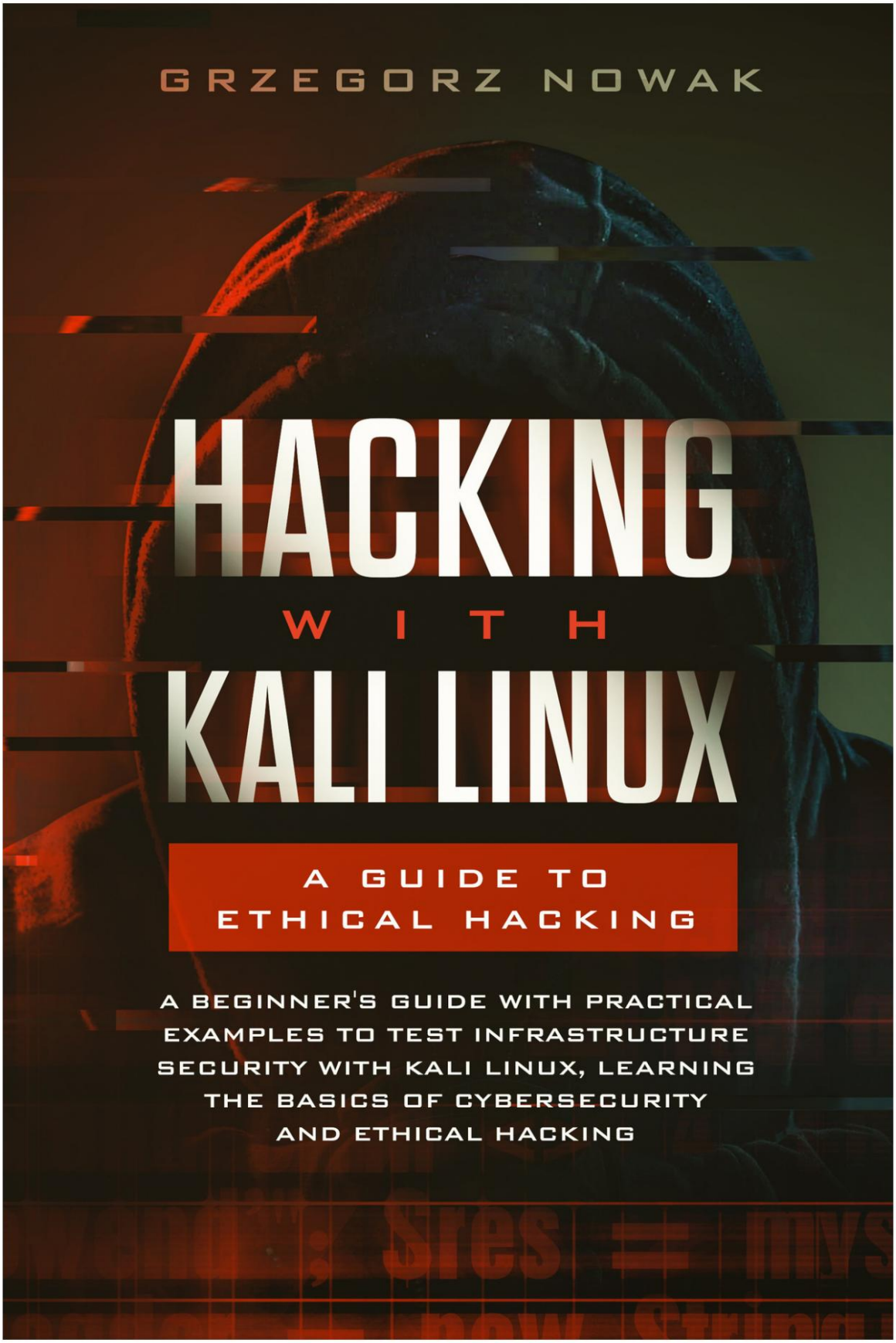
GRZEGORZ NOWAK

# HACKING WITH KALI LINUX

## A GUIDE TO ETHICAL HACKING

A BEGINNER'S GUIDE WITH PRACTICAL EXAMPLES TO TEST INFRASTRUCTURE SECURITY WITH KALI LINUX, LEARNING THE BASICS OF CYBERSECURITY AND ETHICAL HACKING



**Descargue la versión de audiolibro de este libro GRATIS** Si le encanta escuchar audiolibros mientras viaja, tengo excelentes noticias para usted.

¡Puede descargar la versión de audiolibro de este libro **GRATIS** simplemente registrándose para una prueba audible **GRATUITA** de 30 días! ¡Vea abajo para más detalles!


**Beneficios de prueba de Audible**

Como cliente de Audible, recibirá los siguientes beneficios con su prueba gratuita de 30 días: • Copia de audio GRATIS de este libro • Después de la prueba, obtendrá 1 crédito cada mes para usar en cualquier

audio libro

• Sus créditos se transfieren automáticamente al próximo mes si no lo hace.
Úselos •

Elija entre los más de 200 000 títulos de Audible • Escuche en cualquier lugar con la aplicación Audible en varios dispositivos • Haga intercambios fáciles y sin complicaciones de cualquier audiolibro que no le guste • Guarde sus audiolibros para siempre, incluso si cancela su membresía • Y mucho más

**¡Haga clic en los enlaces a continuación para comenzar!**

**Para Audible EE. UU.**

**Para Audible Reino Unido**

## Para Audible FR

## Para Audible DE

# Hackear con Kali Linux:

# Una guía para el hacking ético

*Una guía para principiantes con práctica*

*Ejemplos para aprender los conceptos básicos de*

*Ciberseguridad y Hacking Ético,*

*Probar la seguridad de la infraestructura con Kali linux*

*Grzegorz Nowak*

# Tabla de contenido

# Introducción

Los siguientes capítulos discutirán los diferentes aspectos que vienen con la piratería en el sistema operativo Kali Linux. Este es uno de los mejores sistemas operativos para usar cuando desea comenzar a aprender cómo piratear y cómo mantener segura su propia red. Garantiza que tenga todas las herramientas que necesita para comenzar y, como exploraremos en esta guía, está configurado para que podamos realizar un arranque dual con otros sistemas operativos, lo que facilita el trabajo en cualquier computadora que desee. gustaría.

Esta guía tomará un tiempo para analizar más de cerca la piratería con Kali Linux y todas las diferentes partes que lo acompañan. Comenzaremos con algunos de los conceptos básicos de la piratería, como los tipos más comunes de piratas informáticos y las diferencias entre los piratas informáticos de sombrero negro, sombrero blanco y sombrero gris. A partir de ahí, pasaremos a algunos de los trucos del proceso de piratería, incluidos los pasos que seguiría un pirata informático para ayudarlo a aprender más sobre una red y encontrar su camino hacia esa red a través de vulnerabilidades sin ser detectado.

Luego pasaremos a algunos de los pasos necesarios para trabajar con la instalación de este sistema operativo Kali Linux en nuestro sistema. Veremos cómo realizar un arranque dual en una computadora con Windows y los diferentes pasos que debemos seguir para asegurarnos de que este sistema operativo esté listo para funcionar y pueda asumir todas nuestras tareas de piratería. A partir de ahí, podemos pasar a ver una introducción a la ciberseguridad y por qué es tan importante que lo entendamos para mantener nuestras propias redes seguras.

Ahora que hemos dejado de lado parte de esa introducción, es hora de sumergirse en algunos de los diferentes tipos de ataques y cómo podemos evitarlos en nuestra propia red. Echaremos un vistazo a los ataques de malware, ciberataques y cómo escanear nuestras propias redes y servidores para obtener los mejores resultados en el proceso. Recuerde que las técnicas que usamos en esta guía sobre piratería ética son las mismas que usaría un hacker de sombrero negro o un hacker malicioso, pero esta es una excelente manera de asegurarnos de que podemos proteger nuestros sistemas y redes de aquellos con intenciones maliciosas. .

Algunos de los otros temas en los que dedicaremos tiempo en esta guía incluyen cómo mantener nuestras redes a salvo de ataques en línea, la importancia

de un firewall, y cómo comprender los conceptos básicos de la criptografía y cómo funciona esto con nuestras necesidades de piratería.

Hackear es un término que la mayoría de las personas asocian con algo malo, y pueden tener miedo incluso de aprender más sobre cómo funciona este proceso. Con esta guía, podemos echar un vistazo a cómo piratear con el sistema Linux y las mejores formas de protegernos de algunos de estos malos ataques antes de que puedan tomar nuestra información y causar estragos. Cuando esté listo para aprender más sobre la piratería con Kali Linux, ¡asegúrese de consultar esta guía para ayudarlo!

# Capítulo 1: Los diferentes tipos de piratas informáticos

Lo primero que debemos analizar aquí en esta guía son los diferentes tipos de piratas informáticos. A menudo, cuando escuchamos sobre un pirata informático, pensamos en alguien que está tratando de ingresar a un sistema, generalmente uno al que no tiene derecho a acceder y robar identidades, información personal y más cosas sobre las que no debería tener control. Pero en realidad hay algunos tipos diferentes de piratas informáticos.

El primer tipo es alguien a quien le gusta intentar ingresar a sistemas donde no están permitidos. Por lo general, esto es para sus propios fines y no les preocupa cómo afectará negativamente a la otra persona. Por ejemplo, es probable que este tipo de piratas informáticos ingresen a una base de datos para negocios y roben nombres, direcciones, números de teléfono e información de tarjetas de crédito de quienes compraron en esa tienda.

Pero este es solo un tipo de hacker que existe. Reciben la mayor atención porque son los que causan más daño, pero hay otros dos tipos de piratas informáticos que también debemos analizar. Por ejemplo, un tipo de pirata informático puede intentar ingresar a un sistema al que no tiene acceso, pero no lo hace para causar daño. En cambio, hacen esto para mostrar algunas de las debilidades de ese sistema o porque están aburridos y quieren ver si realmente pueden tener éxito con él.

Luego están los piratas informáticos que piratean legalmente. Tienen permiso para estar en el sistema y lo piratean para ver dónde están las vulnerabilidades. A menudo son contratados por la organización que están pirateando, ya sea como personal de tiempo completo o como trabajadores independientes, para ayudarlos a protegerse contra los piratas informáticos reales y mantener la información segura.

Aunque existen diferentes motivaciones detrás de los tres tipos de piratería, todos utilizarán algunas de las mismas técnicas para realizar el trabajo. Vamos a centrar nuestro trabajo con el último tipo de hacker, observando cómo puede realizar y protegerse contra una variedad de ataques, pero los mismos tipos de métodos se pueden usar con alguien que tiene intenciones maliciosas en el sistema. Con esto en mente, profundicemos un poco más en los tres tipos de piratería, incluido el hacker de sombrero negro, el hacker de sombrero gris y el hacker de sombrero blanco, y veamos cómo cada uno de estos es un poco diferente.

## El hacker de sombrero negro

El primer tipo de hacker que vamos a analizar es el hacker de sombrero negro. Este es el tipo que más se escuchará en las noticias, en el que pensamos cuando escuchamos sobre la piratería en primer lugar. Un hacker de sombrero negro será alguien que busque vulnerabilidades en un sistema de seguridad y luego las explotará. La explotación a menudo se produce con fines de lucro o algún otro tipo de motivo malicioso.

Estas personas no suelen estar preocupadas por el daño que causan a otras personas. Querrán recopilar esta información para usarla para sus propias necesidades en algún momento. A menudo, esto se hace para que puedan robar dinero y enriquecerse antes de desaparecer sin dejar rastro. No tienen ningún deseo de hacer que las cosas sean seguras para los demás. Solo se preocupan por sus propios beneficios y cómo este proceso puede ayudarlos de alguna manera.

Dependiendo de qué tan lejos en el sistema pueda llegar el hacker de sombrero negro, tiene el potencial de infligir un daño importante a los usuarios individuales de esa computadora, a los compradores en esa tienda y a la organización misma. Realmente pueden trabajar duro para robar información financiera personal, comprometer la seguridad que vemos en los sistemas principales e incluso cerrar o alterar parte del funcionamiento de las redes y sitios web.

Este tipo de piratas informáticos puede variar desde aquellos que son aficionados adolescentes que quieren propagar un virus a través de la computadora hasta redes de delincuentes que tienen el objetivo de robar números de tarjetas de crédito y otra información financiera importante.

Hay muchos métodos diferentes que el hacker de sombrero negro puede utilizar, y estos pueden ser similares a los que encontraremos con los hackers de sombrero gris y sombrero blanco también. Por ejemplo, las actividades en las que puede confiar un hacker de sombrero negro podrían incluir algo como agregar programas de monitoreo de pulsaciones de teclas a un sistema para robar datos o incluso lanzar un ataque completo que puede deshabilitar un sitio web completo y evitar que las personas accedan a él. robar la información.

A veces, estos piratas informáticos maliciosos emplearán métodos que no están en la computadora para obtener la información que necesitan. Para

Por ejemplo, podrían llamar a un sistema y asumir la identidad de otro usuario para obtener acceso a la contraseña de ese usuario y acceder al sistema de esa manera.

La principal diferencia que aparece entre este tipo de hackers y lo que vemos con un hacker de sombrero gris o un hacker de sombrero blanco es la intención. Pueden usar las mismas técnicas que los otros dos, pero su objetivo es beneficiarse a sí mismos sin preocuparse por cómo afectará a la otra parte. Esto puede ser peligroso para un negocio. Si un hacker de sombrero negro puede acceder a su sistema y robar información, podría hacerles perder su reputación, mucho dinero para sus clientes y mucho más.

.

**Pirata informático de sombrero gris**

Ahora que tenemos una mejor comprensión de lo que es un hacker de sombrero negro, es hora de echar un vistazo al hacker de sombrero gris. Un hacker de sombrero gris va a ser alguien que está rompiendo algunos principios y estándares éticos, al igual que el hacker de sombrero negro. Pero la diferencia aquí es que lo están haciendo sin las intenciones maliciosas del hacker de sombrero negro.

Lo que esto significa es que el hacker de sombrero gris puede participar en prácticas que parecen deshonestas y son ilegales. Pero lo hacen más en nombre del bien común, o al menos no con la intención de dañar a otros.
Estos piratas informáticos son una especie de término medio cuando se trata de los piratas informáticos de sombrero negro y los piratas informáticos de sombrero blanco, los que van a trabajar en nombre de la empresa que mantiene un sistema seguro, y los piratas informáticos de sombrero negro que actuarán en de manera maliciosa para explotar algunas de las vulnerabilidades que pueden aparecer en un sistema.

A menudo, cuando pensamos en hackear, asumimos que todo es en blanco y negro. Creemos que hay hackers éticos y hackers no éticos.
Sin embargo, a pesar de que la piratería informática se encuentra en algún punto intermedio, aún puede desempeñar un papel importante en el mundo de la seguridad. Uno de los ejemplos más comunes que podemos ver cuando se trata de un hacker de sombrero gris es alguien que puede explotar una vulnerabilidad en un sistema de seguridad para ayudar a difundir entre el público que esta vulnerabilidad realmente existe.

El pirata informático no logró robar dinero, causar caos y robar toda la información personal de los usuarios. Se pusieron a mostrar al público que hay algún tipo de vulnerabilidad en el sistema, con la esperanza de que esto alerte a otros para tomar decisiones más inteligentes, e incluso para algunos cambios.
que se produzca.

Sin embargo, a veces, esta información puede salir mal. Si el hacker de sombrero gris anuncia que encontró la vulnerabilidad y la empresa no trabaja para cambiar este problema y solucionarlo, es posible que los piratas informáticos de sombrero negro puedan superar esta vulnerabilidad y usarla también para sus propias necesidades. Esto puede causar mucho daño y problemas a la empresa, ya que sufren más ataques y tienen que lidiar con las consecuencias.

Técnicamente, el trabajo que realiza el hacker de sombrero gris se considerará ilegal. Todavía no tenían el permiso que necesitaban para completar el truco que hicieron, y esto lo convierte en algo que no deberían haber estado haciendo en primer lugar. Pero dado que pudieron alertar al público sobre un problema en un sistema que pueden haber estado usando, o porque alertaron a la empresa de un problema potencial con anticipación, antes de que llegaran otros piratas informáticos, a menudo es posible que no enfrenten tanto castigo. como algunos de los piratas informáticos de sombrero negro que usarán esto para ayudarse a sí mismos a obtener dinero o información u otra cosa para beneficio personal.

Hay muchos ejemplos en los que un hacker de sombrero gris pudo ingresar a un sistema y luego alertó a la empresa sobre estas vulnerabilidades. Es posible que incluso hayan explicado exactamente cómo lo hicieron y cómo podrían solucionarlo. Algunos de estos han podido obtener posiciones destacadas en estas empresas, ayudando a cerrar un poco las vulnerabilidades y luego manteniendo el sistema y la red tanto como sea posible.

### El hacker de sombrero blanco

El tercer tipo de pirata informático que debemos analizar será un profesional de la seguridad informática que ingresará en un sistema protegido y en otras redes para probar y luego evaluar la seguridad. A menudo, estos funcionarán para la empresa en la que intentan ingresar, con el objetivo de verificar que se resuelvan todas las vulnerabilidades y que ningún otro pirata informático pueda ingresar a ese sistema.

Estos piratas informáticos utilizarán sus habilidades de piratería para ayudar a mejorar la seguridad al exponer las vulnerabilidades que existen antes de que un pirata informático malicioso o el pirata informático de sombrero negro puedan encontrarlas y explotarlas para sus propias necesidades. Aunque los métodos que se utilizan con esto serán similares y, a menudo, idénticos a los que utilizará un pirata informático de sombrero negro, los piratas informáticos de sombrero blanco tienen permiso para ingresar al sistema y emplear estas tácticas para realizar el trabajo. Estos piratas informáticos también tienen la intención de proteger la información del sistema en lugar de explotarla.

Cuando se trata de un hacker de sombrero blanco, estos son los que se ven usando sus habilidades de una manera que beneficiará a la sociedad. Podrían ser piratas informáticos de sombrero negro reformados en algunos casos, o simplemente podrían estar bien versados en las técnicas y métodos que utilizan los piratas informáticos. Las empresas a menudo contratan a estas personas para realizar pruebas e implementar las mejores prácticas para ayudarlos a mantener al mínimo la piratería maliciosa y garantizar que no sean tan vulnerables como antes.

En su mayor parte, un hacker de sombrero blanco será sinónimo de un hacker ético. Harán el trabajo para ayudar a una empresa y para asegurarse de que cualquier vulnerabilidad y problema potencial se resuelva de manera oportuna en lugar de permitir que un pirata informático de sombrero negro ingrese al sistema para
causar un lío.

El hacker de sombrero blanco es a menudo alguien que ha ido a la escuela para aprender mucho sobre los sistemas informáticos y cómo funcionan. Los otros dos tipos de piratas informáticos pasarán su tiempo aprendiendo computadoras y, a menudo, son autodidactas con el trabajo que tienen. Algunos pueden tener un título en TI o computadoras de alguna forma, pero la mayoría solo tenía interés en este tipo de sistema y luego trabajó para perfeccionar sus habilidades a través de la práctica.

Con el hacker de sombrero blanco, estos son profesionales que pasaron bastante tiempo trabajando con computadoras, tecnologías informáticas y más y habrían aprendido sobre piratería en el proceso. Esto les permite estar preparados para manejar las grandes redes y sistemas de las empresas y protegerlos tanto como sea posible. Estos profesionales no hacen el trabajo de hackear para causar travesuras o para trabajar en beneficio propio. Lo hacen como parte de su trabajo para mantener a las empresas y los clientes que trabajan con estas empresas lo más seguros posible de otros piratas informáticos.

Como podemos ver, hay muchas diferencias que vienen con el mundo de la piratería, y cada uno de los tipos de piratas informáticos funcionará de una manera ligeramente diferente entre sí. El pirata informático de sombrero negro pasará su tiempo ingresando a un sistema para sus propios intentos maliciosos. El hacker de sombrero gris está en algún lugar en el medio y explotará el sistema para informar al público sobre este problema. Y luego, el hacker de sombrero blanco entrará como alguien que trabaja para la empresa y se asegura de que la información con esa empresa se mantenga lo más segura posible.

Cada uno de estos tipos de piratas informáticos será vital para el mundo de la piratería, y debemos poder explorar cada uno de ellos y cómo funcionan. Recuerda que cada uno va a utilizar las mismas técnicas. Las diferencias aquí son que necesitamos ver algunas de las intenciones detrás de esas acciones y las razones por las que cada hacker está haciendo la actividad que es. Una vez que podemos entender cómo funciona eso, se vuelve más fácil ver cómo usar las técnicas que tenemos de una manera ética y segura.

# Capítulo 2: Los fundamentos del proceso de piratería

Muchos principiantes no entienden que la piratería o cualquier tipo de prueba de penetración seguirán un proceso que es muy lógico. Asumen que simplemente tienen suerte cuando pueden encontrar una vulnerabilidad en el sistema y que no vale la pena su tiempo para aprender un proceso. Pero en realidad, el proceso de piratería es bastante lógico y podemos dividirlo en tareas y objetivos que debemos seguir para hacer las cosas.

Al igual que todos los demás proyectos de TI o seguridad con los que desea trabajar, un plan de piratería ética será algo que debemos crear con anticipación. Las cuestiones de estrategia y tácticas en la piratería ética deben determinarse y acordarse con anticipación. Para asegurarse de ver algún éxito con los esfuerzos que está utilizando, también debe dedicar algo de tiempo a planificar las cosas con anticipación. No importa en qué tipo de proceso esté trabajando, este plan puede ser importante.

Es importante notar los pasos que se necesitan cuando un hacker está listo para comenzar a trabajar contra su objetivo. Estos pasos van a ser similares ya sea que estén trabajando con un objetivo que conocen o con alguien que no conocen, ya sea que se trate de un individuo, o si están más interesados en atacar a una gran empresa y toda la información personal que contiene. . Estos pasos asegurarán que podamos manejar todas las diferentes partes que vienen con un ataque de piratería. Todos los piratas informáticos seguirán alguna forma de estos para ayudarlos a comenzar.

Hay cinco pasos principales que debemos analizar cuando se trata de algunos de los conceptos básicos del proceso de piratería. Estos van a incluir:

## Reconocimiento

La primera fase del proceso de piratería que vamos a ver se conoce como reconocimiento. Para que podamos recopilar la mayor cantidad de datos posible, se puede utilizar este proceso. Dado que toda la información y los datos que podemos recopilar durante este tiempo pueden sernos útiles cuando lleguemos a las fases posteriores, a menudo se considera que esta es la fase más importante de todas.

Por supuesto, algunas personas piensan que esta frase es aburrida. No involucra algunas de las técnicas más avanzadas, y lo incluirá simplemente sentado

y observar el sistema para ver qué información aparecerá en el sistema y cómo puede usarla más adelante. También hay muchas herramientas y técnicas que puede usar para ayudar con esta fase, y algunas de ellas son de uso gratuito según sus propias necesidades.

Dentro de esta fase, habrá dos tipos de reconocimiento con los que podremos trabajar. El primer tipo es el reconocimiento pasivo. Cuando estamos trabajando con la forma pasiva, vamos a entrar en el sistema, pero nuestra interacción no será directa con el sistema de destino. Por ejemplo, cuando revisamos y miramos alrededor del sitio web de la empresa, nos gusta apuntar o si nos gusta ver las contrataciones de trabajo en esa empresa específica.

Durante esta fase, queremos hacer una búsqueda rápida en Google y revisar algunos de los registros públicos, incluidos los de WHOIS, para ayudarnos a recopilar datos de la empresa a la que nos gustaría apuntar, así como su sitio web y demás. Ahora, todas las técnicas que usamos no van a incluir una interacción directa con la empresa objetivo en sí. En su mayoría, es solo una investigación realizada sobre la compañía por ahora. Estos ejemplos se denominarán reconocimiento pasivo.

El alcance de lo que recopilaremos durante esta fase no incluirá solo los sistemas, servidores y hosts. Pero también podemos usarlo para incluir algunos de los clientes de nuestro sistema de destino y los empleados que creemos que podemos usar para nuestros objetivos. La ingeniería social podría entonces ayudarnos a recopilar más datos de los empleados. La ingeniería social va a ser una técnica que un hacker puede usar para manipular a una persona para que dé cualquier dato que no suele dar.

El hacker espera que, con la ayuda de la ingeniería social, pueda engañar a la otra persona para que proporcione información personal. Incluso pueden solicitar información como el nombre de usuario y la contraseña del empleado para que puedan ingresar al sistema cuando estén listos.

Otro ejemplo de lo que se puede hacer con este proceso es el conocido como dumpster diving. Este es un lugar donde vamos a buscar a través de diferentes medios para encontrar información importante. Puede incluir buscar en la basura, pero a veces, solo obtener acceso a algunos sitios web, el escritorio de los empleados y más puede ayudarnos a obtener los recibos de cajero automático, números de teléfono y estados de cuenta bancarios que estamos buscando.

El segundo tipo de reconocimiento con el que podemos trabajar aquí se conocerá como reconocimiento activo. Con este tipo de búsqueda, vamos a trabajar para interactuar activamente con el objetivo que queremos hackear. Dado que este tipo de proceso nos involucrará interactuando directamente con el objetivo, surgirá un nivel adicional de desafío. Hacer llamadas telefónicas directamente al objetivo y hacer que hable sería uno de los ejemplos de cómo funciona este proceso.

Además, a algunos piratas informáticos les gusta trabajar con un servicio de ping. La razón por la que les gusta trabajar con esto es que les permite determinar si el sistema responderá o no. Si no responde, entonces puede ser el momento de buscar otro método para ingresar al sistema en lugar del que estaba buscando antes.

Ahora, este es a menudo uno de los últimos tipos de reconocimiento con los que queremos trabajar. Es difícil saber qué va a estar presente en el otro lado.
El método pasivo suele ser más fácil porque nos permite permanecer ocultos un poco más y aún podemos recopilar mucha de la información que necesitamos. Sin embargo, si el servicio de ping se usa para hacer ping a uno de los servidores de su objetivo, entonces tenga en cuenta que está activo porque todavía está tocando activamente el servidor.

Siempre que trabajemos con el proceso activo aquí, debemos tener cuidado.
Siempre existe la posibilidad de que estés dejando tu marca atrás. Si hay algún rastro con usted en algún momento, entonces es posible que pueda llevar a la empresa objetivo de regreso a usted.

## Exploración

Después del proceso de recopilación de información en el paso anterior, es hora de pasar a la fase de escaneo. En esta fase, vamos a utilizar una variedad de herramientas para recopilar más información que necesitamos sobre el objetivo. Hay una variedad de herramientas que podemos sacar cuando lleguemos a este punto, pero algunas de estas herramientas incluirán escáneres de vulnerabilidades, barredores, herramientas de ping, mapeadores de red y escáneres de puertos. Con todas estas herramientas para escanear, es sorprendente la cantidad de información que podemos recopilar sobre la red de destino.

Por ejemplo, estas herramientas se utilizarán para determinar los puertos cerrados y abiertos en un momento dado. También sabremos qué tipo de sistemas operativos

utiliza la empresa y qué tipos de dispositivos hay en esa red, por nombrar algunas cosas que podemos buscar.

Notará con esta fase que el escaneo será más activo que antes, pero la buena noticia es que también podemos usar las otras formas pasivas de escaneo. Entonces, al determinar el tipo de sistema operativo que se utiliza, podemos enviar algo de tráfico de red a los sistemas. La respuesta que obtengamos del sistema operativo a ese tráfico variará según el tipo de sistema que se utilice.

Todos los sistemas operativos van a responder al tráfico que se envía de diferentes maneras. Esto significa que una computadora con el sistema operativo Windows responderá a cualquier tráfico que se envíe de manera diferente en comparación con una computadora Linux y una computadora Mac. Y lo mismo puede decirse de todos los demás sistemas operativos.

Un ejemplo que podemos ver cuando se trata de escanear pasivamente es olfatear el tráfico en la red. Podemos trabajar con algunas herramientas para esto, pero Wireshark es una excelente opción para ayudarnos a detectar el tráfico de la red. Conocer toda la infraestructura de la red será más fácil como resultado de esta fase.

A partir de aquí, podemos trabajar para dar sentido a algunos de los datos que hemos recopilado en esta fase, así como en la primera fase. Entonces podemos convertir todos los datos en información útil. Esta es una gran cosa para trabajar porque nos proporciona un plano de lo que está pasando en toda la red en la que estamos.

## Ganando acceso

Ahora que hemos tenido algo de tiempo para recopilar un poco de información sobre el sistema de destino con el que queremos trabajar, y hemos podido agregar un poco más de actividad y ver cómo escanear algunas de las redes para obtener una buena blueprint, es hora de trabajar en el tercer paso para obtener acceso. Esta es en realidad la fase en la que se llevará a cabo parte de la piratería real.

Cuando estemos en esta fase, intentaremos ingresar al sistema de destino y ver cómo podemos usar las vulnerabilidades que pudimos usar durante la fase de escaneo. Encontrar un buen camino que nos ayude a nosotros, el atacante,

entrar en la infraestructura de la red es importante para que podamos tomar el control de todo.

Hay una variedad de métodos que podemos ver para obtener el acceso que queremos a la red. Y es probable que tenga que usar al menos algunos antes de poder obtener ese acceso. Podemos obtener acceso a través de la red, a través de una vulnerabilidad en una aplicación que está en esa red, o incluso a través del sistema operativo específico que está en la red.

Cuando estamos en la fase de obtención de acceso de este proceso, también existen algunos métodos diferentes que pueden ayudarnos a alcanzar nuestros objetivos. Podemos hacer algo como un ataque de denegación de servicio o secuestro de sesión en algunos casos. El ataque de denegación de servicio o DOS en un sistema es una buena opción para trabajar porque expondrá algunas de las vulnerabilidades ocultas que aparecen en el sistema.

Tan pronto como podamos encontrar al menos una vulnerabilidad, pero con suerte más, podrá usarlas para ayudarnos a obtener acceso al sistema. Esto puede llevar algún tiempo, especialmente si hay un hacker de sombrero blanco que trabaja para la empresa y trata de mantener a otras personas fuera del sistema. Pero una vez que hemos obtenido el acceso que queremos al sistema, estamos haciendo esta fase del proceso con piratería.

Obtener acceso es una parte que puede llevarnos algo de tiempo para hacer las cosas. Queremos usar algunas de las diferentes partes que discutimos anteriormente, la información que pudimos descubrir y aprender sobre el negocio y la red, y luego obtener acceso. Recuerde que con este, el mejor lugar para ingresar es buscar esas vulnerabilidades y enfocarse en cómo podemos explotar algunas de ellas para nuestras necesidades.

Muchos sistemas tienen algún tipo de vulnerabilidad que les sucede. Pero a veces, lleva tiempo encontrarlos. Podría ser una vulnerabilidad que aparece en el sistema operativo u otra pieza de hardware o software que está utilizando la red. A veces, será encontrando un puerto que no esté cerrado y monitoreado de la manera que debería. Pero a menudo, la forma en que encuentra una vulnerabilidad y la explota es a través de un error humano.

Para muchos piratas informáticos, un error humano será la forma más fácil de ingresar a un sistema, sin importar en qué sistema operativo se encuentren o cualquier otra cosa. Cuando los humanos no están prestando atención a lo que están haciendo y no siguen los protocolos de seguridad adecuados, lo mejor para el hacker es obtener lo que le gustaría. Los piratas informáticos pueden participar cuando los usuarios comparten su información con otros, cuando no cierran sesión en el sistema, cuando abren correos electrónicos que no deberían, o incluso cuando no tienen cuidado con los sitios web que visitan y la información. que comparten en esos sitios web mientras están en el trabajo y en la red.

Encontrar dónde está esta vulnerabilidad e implementar algunos protocolos en el camino para asegurarse de que todos sigan las reglas y no pongan en riesgo todo el sistema puede ser muy importante para su red. Ya sea parte del software con el que está trabajando o alguien que está en la red que está creando estas aperturas, es hora de encontrar las mejores formas de solucionar estos problemas como podamos.

**Mantenimiento del acceso**

Una vez que hemos tenido algo de tiempo para penetrar en la red y tenemos el acceso que necesitamos al sistema, el próximo desafío en el que debemos trabajar es mantener el acceso. Si algo en la red sospecha que usted está allí, será expulsado y la vulnerabilidad que explotó se solucionará. Entrar en el sistema y tener cuidado hasta que esté listo para realizar el ataque es clave aquí.

Una vez que hemos tenido la oportunidad de acceder a la red, es probable que nos gustaría, en el futuro, volver al mismo nivel de acceso o superior. Para hacer esto, necesitaríamos implementar algunas funciones para lograrlo, incluida una puerta trasera, un troyano o un rootkit que pueda ayudarnos a obtener acceso a esa misma red incluso en el futuro.

Tenga en cuenta que será mejor para nosotros si mantenemos el control del sistema por un período más largo. Luego, este sistema puede usarse como una fuente que puede ayudarnos a infectar algunos de los otros dispositivos que están en la red hasta que alcancemos nuestro objetivo final con este proceso.

Mientras estemos en este sistema y mantengamos nuestro acceso, estamos en la posición perfecta para hacer muchas cosas. Podemos interceptar algunos de los correos electrónicos que vemos llegar. Podemos ver lo que los usuarios están recibiendo en el

sistema y lo que están haciendo allí. Podemos observar el tráfico de red que ingresa y causa problemas. E incluso podemos trabajar para agregar un registrador de teclado para que podamos aprender las contraseñas y los nombres de usuario para acceder a más del sistema.

Hay muchos beneficios que el pirata informático puede obtener cuando trabaja con acceso continuo a la red. Estos beneficios podrían incluir la manipulación de datos y el monitoreo de la red durante mucho tiempo, lo que incluye tiempo adicional para lanzar algunos ataques adicionales en el proceso.

El objetivo general aquí es que permanezca en el sistema todo el tiempo que pueda. Cuanto más tranquilo estés aquí, y cuanto mejor seas pirateando, más fácil será para ti quedarte quieto y pasar desapercibido. Sé más un observador al principio, al menos hasta que hagas tu ataque. Es poco probable que incluso con una vulnerabilidad presente, la red de destino no tenga nada para ayudar a mantener las cosas protegidas y seguras. Si realiza el movimiento equivocado y no tiene cuidado antes de su ataque, es probable que algo en la red lo encuentre y pierda su acceso y su control .

Y ahora, estamos en la última fase de piratería en este punto. Esta fase incluirá limpiar o cubrir nuestras huellas. Los profesionales de TI de la red no deben notar que los piratas informáticos están en su sistema. Ese debería ser el objetivo principal del hacker. Si hemos hecho algo malicioso en la red o el sistema, debemos intentar ocultarlo.

La razón es que nosotros, como piratas informáticos, aún podemos continuar y mantener el acceso a la red si nadie se da cuenta de lo que hemos hecho. Dado que nadie ha detectado o notado el ataque, no seremos expulsados del sistema y aún podremos tener acceso en el futuro. Cuanto más sutil pueda ser y menos ruido haga en el proceso, mejor será para usted en general.

El pirata informático también debe asegurarse de ocultar sus huellas en el sistema sobrescribiendo, destruyendo o eliminando cualquier registro que pueda documentar sus actividades en el sistema. Esto garantiza que nadie pueda echar un vistazo a los registros más adelante y notar que hay alguna actividad extraña o un sistema que no debería estar presente causando problemas.

Es muy importante que salga y borre sus huellas cuando haya terminado con su trabajo. Dejar algo atrás cuando haya terminado puede parecer una buena idea, pero recuerde que otros piratas informáticos, como los piratas informáticos de sombrero blanco que trabajan para la empresa, a menudo estarán mirando alrededor. Es posible que los haya vencido en esa vulnerabilidad y haya ingresado al sistema, pero, en algún momento, la encontrarán y pueden usar eso para encontrarlo a usted también.

Limpiar tus huellas ayuda a finalizar el proceso y hace que sea más fácil que no te atrapen. Hay un nivel de anonimato que está presente en este tipo de piratería. Pero tan pronto como alguien te encuentra y se da cuenta de lo que estás haciendo, puede rastrearte e incluso cortar el punto de acceso que tenías en primer lugar, y ninguna de estas cosas es buena para ti ni para la piratería que estás haciendo. quiero hacer.

Y estas son las partes básicas que vienen con el proceso de piratería. El objetivo es ingresar al sistema de la manera más secreta y silenciosa posible, con la esperanza de que nadie se dé cuenta de que está allí o cause un revuelo porque ve que sucede algo extraño. Si puede completar los cinco pasos anteriores, es mucho más fácil obtener el acceso que desea a un sistema y luego puede completar el ataque que desea realizar.

# Capítulo 3: Cómo instalar y usar el sistema operativo Kali Linux para hackear

Ahora que hemos tenido algo de tiempo para ver algunos de los conceptos básicos que vienen con los métodos de piratería, es hora de descargar el sistema operativo que queremos usar para realizar esta piratería. Si bien podemos trabajar con algunas de estas opciones de piratería sin importar en qué sistema operativo estemos, nos centraremos en cómo podemos hacer esto con Kali Linux. Sin embargo, antes de que podamos utilizar esto, debemos instalar el sistema operativo y prepararlo para su computadora.

Linux suele ser el principal sistema operativo que utilizarán los piratas informáticos, principalmente porque es fácil trabajar con él y tendrá todo el software necesario para completar un proyecto de piratería. Es gratuito y de código abierto, lo que significa que podemos hacer modificaciones y utilizarlas de la forma que queramos.

La instalación de Kali Linux a veces es un poco complicada para los principiantes, pero eso es a lo que dedicaremos un tiempo en este capítulo. Vamos a echar un vistazo a cómo hacer un arranque dual con Kali Linux y luego a ver cómo podemos trabajar con esto en los otros sistemas operativos, incluidos Windows y Mac OS, para nuestras necesidades.

.

## Un arranque dual de Kali Linux

La primera opción que vamos a ver en esta guía es cómo trabajar con un arranque dual de Kali Linux. Esto nos ayuda a asegurarnos de que podemos hacerlo funcionar con un sistema operativo Windows, principalmente Windows 7 8 u 8.1. Entonces, si no eres fanático de trabajar con la versión más nueva de Windows, también podemos controlarlo. ¡Comencemos entonces!

Antes de comenzar con el impulso dual, debemos asegurarnos de que tenemos los materiales adecuados para trabajar aquí. Algunos de estos incluyen:

1. Windows 10 o cualquiera de las otras versiones de Windows que están ya está instalado en su computadora.
2. Una computadora portátil o PC que pueda manejar algunos de los diferentes procesos de piratería que queremos hacer.

3. Un Pendrive mínimo de 4 GB 4. Al

menos un Dual Core en su sistema, ya sea AMD o Intel, funciona bien para esto, y la memoria RAM debe ser como mínimo de 1 GB.

5. La última versión de Kali Linux 6. Rufus
7. Y paciencia para hacerlo todo.

Para comenzar, sabremos cómo usar el programa de Windows 10 para hacer un arranque dual de Kali Linux v2019.2. El primer paso es descargar el último archivo ISO de Kali Linux. Podrá obtener esto visitando kali.org. Puede elegir si desea descargar el bit 32 o el bit 64 mientras está allí. Después de que Kali Linux haya tenido tiempo de descargarse, el siguiente paso es crear nuestro propio USB de arranque. Para ello, necesitamos trabajar con la extensión Rufus. Esta es una utilidad que puede ayudarnos a crear estas unidades flash USB que son de arranque. Vaya a Rufus.ie para descargar la extensión antes de instalarla en el sistema.

Con estos dos elementos en su computadora, queremos comenzar haciendo un USB de arranque. En primer lugar, conectamos el USB que queramos usar. Como dijimos anteriormente, esto necesita tener al menos 4 GB de memoria para funcionar y tener suficiente espacio para manejar la extensión Rufus y Kali Linux. Cuando el USB está dentro de la computadora, podemos ejecutar Rufus y usar los pasos a continuación para crear una unidad USB de arranque.

1. Primero, aparecerá una imagen en la pantalla sobre el Rufus
   programa que está ejecutando.
2. Verifique que la unidad USB sea la seleccionada allí, luego haga clic en
   en el icono de la unidad pequeña para el CD.
3. Localice el archivo ISO para Kali Linux que descargamos anteriormente y luego
   haga clic en Iniciar. Espere unos minutos para que se complete este proceso
   antes de continuar.
4. Una vez que se complete el proceso, puede hacer clic en el botón Cerrar
   para que la ventana de Rufus se cierre. Esto le dará la unidad USB de arranque para Kali Linux.

un. Además de usar esto para ayudar con el arranque dual de Kali Linux en Windows, también puede hacer un arranque en vivo de Kali usando este USB. Esto significa que podemos ejecutar Kali sin tener que instalarlo en nuestro sistema.

> Tenga en cuenta que limita un poco las funciones y las características cuando trabaja en este asunto.

A partir de este punto, para la instalación de Kali Linux, se debe crear una partición separada. Entonces, para hacer esta parte, podemos abrir la configuración para la administración de discos, o podemos ejecutar en Windows el comando de "diskmgmt.msc". Si creamos una partición de tamaño mínimo de 15 a 20 GB, podría reducir el volumen que ya tenemos.

En este punto, notamos que los primeros procesos habían terminado. Se descargó la ISO de Kali Linux, se creó una unidad USB de arranque programada y se creó una partición separada para la instalación de Kali Linux.
Antes de continuar, debemos recordar que las opciones Fast Boot y Disable Secure Boot están disponibles en el BIOS si deseamos usarlas en nuestro programa.

Ya podemos reiniciar nuestro portátil o PC. Vaya al administrador de arranque ya que se inicia de nuevo. Elija USB en la opción de arranque. Recuerde que las diferentes marcas tendrán opciones ligeramente diferentes. Ahora puede ver la instalación de Kali Linux en su pantalla. Hay algunas opciones que surgen en este punto sobre cómo instalar Kali Linux. Deberá elegir la opción de "Instalación gráfica" para ayudar a que Kali Linux comience con cierta facilidad.
Podemos llevar esto más allá y agregar algunas de las configuraciones y características que queremos. Por ejemplo, puede elegir qué idioma le gustaría usar para el proceso de instalación y también el país.

Después de haber podido revisar y agregar algunas de las preferencias anteriores y las otras opciones que solicita el sistema, es hora de trabajar en el nombre de host. Su instalación le pedirá el nombre de host. Puede elegir cualquier nombre que desee porque será como su nombre de usuario. Luego se debe ingresar la contraseña para el usuario root. Después de ingresar la contraseña que desea para la cuenta administrativa, puede hacer clic en continuar.

Ahora, queremos elegir el método de partición que queremos usar, y la opción con la que trabajaremos es Manual. El siguiente paso necesita algo de precaución. Solo queremos elegir la partición que nos tomamos el tiempo de crear anteriormente para la instalación de Kali y luego presionar Continuar. Cuando esté seguro de haber elegido la opción correcta, puede seleccionar "Eliminar la partición"

Antes de continuar. Si hizo esto de la manera correcta, notará el "ESPACIO LIBRE", que es la partición en la instalación de Kali. Queremos elegir esta partición de espacio libre antes de continuar con el proceso.

Aquí, la instalación nos va a preguntar cómo nos gustaría usar ese espacio libre. Nuestro objetivo es hacer clic en "Particionar automáticamente el espacio libre" y luego continuar. Después de eso, seleccione la opción que dice "Todos los archivos en una partición". Esta será la opción recomendada para los nuevos usuarios en caso de que esté redactada de manera diferente con su versión. Y luego, queremos elegir la opción que dice "Finalizar partición y escribir cambios en el disco".
Quiere que le conceda permiso para escribir estos cambios en el disco. Puede elegir Sí y luego Continuar.

Aquí es donde se llevará a cabo el proceso de instalación de Kali Linux. Esto puede llevar un poco de tiempo, así que espere unos 15 minutos antes de que finalice el proceso. Aproximadamente a la mitad del proceso, la red solicitará un espejo de red. Seleccione el que desee. Esta configuración se trata de la opción de actualización, por lo que es mejor si puede elegir no por ahora y luego hacer cambios más tarde si lo desea.

A continuación, la instalación le pedirá que instale el cargador de arranque GRUB. Desea hacer clic en Sí antes de continuar. A continuación, le preguntará dónde desea instalar el cargador de arranque Kali GRUB. La mejor elección será el disco duro que tenga la 2ª opción. Queremos que GRUB suceda en su disco duro, o la opción para seleccionar los sistemas operativos no se mostrará con la instalación de Kali Linux cuando se inicie la computadora, y ese es un gran objetivo nuestro con este proceso.

Una vez que haya completado estos pasos y tenga éxito con el proceso de instalación de Linux, ahora verá una pantalla que le preguntará si desea continuar o regresar. Haga clic en Continuar y luego expulse la unidad USB. Deberá reiniciar el sistema en este punto.
Durante el proceso de Start-Up, podrá ver Kali Linux a través de nuestro GRUB Loader. La computadora se puede iniciar con Kali Linux seleccionando Kali GNU/Linux. O, si solo desea trabajar con su entorno de Windows, puede elegir la opción que dice Entorno de recuperación de Windows.

Y eso es todo lo que hay que hacer. Solo necesita seguir algunos de los pasos que hicimos anteriormente, y puede configurarlo para que la distribución de Kali Linux esté lista para funcionar, y puede usarla en cualquier momento que desee.
Cada vez que reinicie su computadora, podrá elegir si desea trabajar con el sistema operativo Kali Linux o el sistema operativo Windows según sus necesidades, lo que facilita alternar entre los dos.

# Capítulo 4: Introducción a la seguridad cibernética

El siguiente tema que debemos analizar aquí es la idea de la ciberseguridad y de qué se trata. Como alguien que está trabajando en Kali Linux como parte del proceso de piratería, es importante saber tanto como sea posible sobre ciberseguridad y cómo puede proteger su sistema y todas las redes que necesita proteger de amenazas externas. Entonces, entremos de lleno.

La ciberseguridad va a ser el estado o el proceso de proteger y recuperar programas, dispositivos y redes de cualquier tipo de ataque cibernético en el que un hacker u otra persona pueda querer entrar. Estos ciberataques son más comunes que nunca. Hay muchos piratas informáticos y otras personas que desean obtener acceso a una gran cantidad de computadoras, ya sea una gran cantidad de computadoras personales y la información de esas o de una gran empresa que tiene un gran conjunto de datos sobre su clientes.

Hay muchos beneficios para alguien que completa estos ataques cibernéticos. Si tienen éxito y nadie los atrapa o lo que están haciendo, entonces esto realmente puede ayudarlos a obtener acceso a información que no deberían tener. Muchos piratas informáticos quieren hacer esto para destruir un negocio, robar información personal de clientes y empleados e incluso robar dinero. Algunas empresas pueden intentar atacar de manera poco ética a otro competidor para obtener información sobre nuevos productos y servicios y apoderarse de ellos.

No importa cuál sea el motivo del ataque, habrá algún beneficio para el pirata informático y, a menudo, causará un desastre para la empresa y para todos los demás que se vean afectados en el proceso. Y es el trabajo de un hacker de sombrero blanco y el resto del equipo de profesionales de TI mantener algunos de estos ciberataques al mínimo.

Estos ciberataques son un peligro en evolución para los consumidores, empleados y organizaciones. Se diseñarán de una manera que les ayude a acceder o destruir cualquier información confidencial que pueda estar en un sistema o incluso para extorsionar dinero cuando sea necesario. Pueden, cuando tienen éxito y dependiendo de su escala, realmente destruir negocios y dañar las vidas financieras y personales de aquellos que estaban en el sistema.

Muchas empresas gastan mucho tiempo y dinero tratando de proteger la información que tienen para sus clientes. Cada vez que compra en línea o realiza otra actividad, también se deja atrás bastante información personal. Esto podría incluir su nombre, dirección, teléfono, características definitorias (como sexo, edad, ocupación, etc.) y su información de pago.

.

Estas empresas saben que si la información cae en las manos equivocadas, podría provocar el caos. El pirata informático podría robar muchas identidades y usar las opciones de pago tanto como quisiera, causando una gran pérdida de dinero y tiempo en el proceso antes de que alguien pudiera darse cuenta. Y esto efectivamente causaría una gran cantidad de daño a las empresas que permitieron que sucediera.

Entonces, ¿cuál será la mejor defensa para frenar esto y asegurarse de que no vuelva a suceder? Básicamente, un sistema de seguridad cibernética sólido tendrá múltiples capas de protección que se distribuyen en programas, redes y computadoras. Pero un sistema de seguridad cibernética fuerte dependerá no solo de la tecnología de defensa cibernética, sino también de las personas que pueden tomar decisiones inteligentes para la defensa cibernética.

La buena noticia aquí es que no necesita tener un especialista en seguridad cibernética, y no tiene que serlo para comprender y practicar algunas de las tácticas de defensa cibernética. Este capítulo puede ser un excelente lugar para comenzar con este proceso y puede hacerlo todo por usted. Vamos a echar un vistazo más de cerca a la ciberseguridad y cómo podemos usar esto para defendernos, tanto como sea posible, contra estas amenazas. Podría ser exactamente lo que necesita para ayudar a reconocer y evitar algunas de estas amenazas en línea antes de que tengan la oportunidad de ingresar a su dispositivo o su red:

**Los diferentes tipos de amenazas cibernéticas**

Lo primero que debemos analizar aquí son los diferentes tipos de amenazas cibernéticas. Hay bastantes de estos en nuestro mundo, y a medida que la tecnología cambia y los piratas informáticos se vuelven más expertos en lo que pueden hacer en línea, es probable que este problema empeore. Algunos de los tipos más comunes de amenazas cibernéticas que todas las empresas e incluso las personas deben tener en cuenta en su sistema incluyen:

1. Ingeniería social: Este va a ser un proceso donde el hacker va a manipular psicológicamente a otros. el objetivo es

para lograr que el objetivo realice ciertas acciones o entregue información importante.

2. Amenazas persistentes avanzadas o APT. Estos van a atacar donde el usuario no autorizado puede infiltrarse en la red sin ser atrapado y luego permanecerá en esa red por un período de tiempo más largo sin ser detectado.
3. Malware: Este es un tipo de software que ha sido diseñado para ayudar específicamente al pirata informático a obtener acceso al sistema o causar algún daño a la computadora sin que el propietario sepa lo que está sucediendo.
4. Ransomware: Este va a ser un ejemplo de malicioso software. Ha sido diseñado de una manera que extorsionará el dinero bloqueando el acceso a los archivos o al sistema de la computadora hasta que el objetivo haya trabajado para pagar el rescate. Si bien el pirata informático puede tomar el rescate y hacer que parezca que ha abandonado el sistema, este pago no garantizará que se recuperarán todos los archivos o que el sistema se restaurará a lo que usted desea. De hecho, es probable que el hacker guarde algo en la computadora para que pueda volver a ella más tarde si lo desea. E incluso es posible que cojan el dinero y desaparezcan sin arreglar nada.

5. Suplantación de identidad. Otro tipo de ataque al que las personas y las empresas deben prestar atención se conoce como phishing. Este es el proceso de enviar correos electrónicos que son fraudulentos y que se parecerán a los correos electrónicos de algunas fuentes confiables. El objetivo de este es robar algunos de los datos confidenciales del individuo, incluida su información de inicio de sesión y números de tarjetas de crédito. Este es en realidad uno de los tipos de ataque más comunes. Puede protegerse contra esto yendo directamente al sitio web que solicita la información, en lugar de proporcionarla por correo electrónico, y trabajar con una solución tecnológica que pueda filtrar algunos de estos correos electrónicos maliciosos.

En realidad, existen algunos tipos diferentes de amenazas cibernéticas que pueden atacar sus redes y sus dispositivos, y es importante prestar atención a cuáles son y cómo podemos evitarlas. En general, sin embargo, se dividirán en tres categorías. Estos van a incluir ataques contra el

disponibilidad, integridad y confidencialidad de nuestros sistemas. Echemos un vistazo a cada uno de estos que podemos experimentar si no proporcionamos el tipo correcto de ciberseguridad en nuestras redes y sistemas.

El primero de la lista son los ataques a la confidencialidad. Estos incluirán cualquier ataque que pueda robar su información de identidad personal, como la información de su tarjeta de crédito o su cuenta bancaria. Muchos de estos atacantes tomarán su información y luego la venderán en la web oscura, generalmente para que otros la compren y la usen como quieran.

Luego están los ataques que suceden a su integridad. Estos van a ser los ataques que consisten en sabotaje empresarial o personal, y a menudo son lo que escuchamos como filtraciones. Un ciberdelincuente puede acceder y luego divulgar cualquier información confidencial que tenga, generalmente con el fin de exponer realmente esos datos e influir en el público para que comience a desconfiar de esa empresa.

Y el tercer tipo de amenaza cibernética que debemos tener en cuenta incluye los ataques a la disponibilidad. El objetivo de un pirata informático que usa este tipo de ataque es hacer que sea imposible que los usuarios obtengan sus propios datos hasta que puedan pagar una tarifa o un rescate al pirata informático. Por lo general, el ciberdelincuente trabajará para ingresar a la red y le impedirá obtener datos importantes hasta que pueda pagar un rescate. .

En algunos casos, es probable que la empresa pague el rescate para intentar recuperar sus datos y hacer que el ataque desaparezca. Pueden hacer esto para evitar detener algunas de las actividades comerciales que deben llevarse a cabo. Sin embargo, esto no siempre resuelve el problema y, a menudo, el hacker deja algo en el sistema que le permite volver a encenderlo, a menos que un hacker de sombrero blanco u otro profesional de TI pueda venir y solucionar ese problema.

Como mencionamos antes, estos son algunos otros tipos de amenazas cibernéticas que una empresa debe tener en cuenta, y debemos estar siempre atentos a que sucedan algunas de estas cosas. Volviendo a la ingeniería social de la que hablamos antes, el hacker es capaz de convencer o manipular a alguien para que entregue su información personal.

La ingeniería social, como mencionamos, es un tipo de ataque a la confidencialidad. Es el proceso en el que el hacker será manipulado para realizar una

acción que el hacker quiere o regalar su información. A menudo, esto incluiría un ataque de phishing con un correo electrónico engañoso. Por ejemplo, el correo electrónico puede parecer que proviene del banco del objetivo y le pide que verifique un mensaje en su cuenta. El usuario hará clic en él, proporcionará su nombre de usuario y contraseña, y luego el pirata informático tendrá acceso a esta información en cualquier momento que lo desee.

Volviendo a las APT, o Amenazas Persistentes Avanzadas, de las que hablábamos antes, podemos ver un tipo de ataque a la integridad. Básicamente, con este, un usuario no autorizado puede ingresar a la red de destino sin que nadie se dé cuenta de que está allí, y luego puede permanecer en esa red de destino durante un largo período de tiempo. El objetivo principal de este, aunque puede llevar algo de tiempo, es robar datos sin dañar la red, al menos por ahora. Es más probable que estos ataques sucedan con empresas y sectores que tienen mucha información valiosa. Podemos ver esto en la industria financiera, la fabricación y la defensa nacional, por ejemplo.

Y luego podemos volver a la idea de malware que discutimos brevemente anteriormente. Este es básicamente un software malicioso, y será un buen ejemplo de un ataque a la disponibilidad. Se va a referir al software que está diseñado para obtener acceso o dañar una computadora, sin que el propietario tenga conocimiento de lo que está sucediendo. Hay muchos tipos diferentes de malware a los que podemos prestar atención, y pueden incluir cosas como gusanos, virus verdaderos, registradores de teclas y spyware.

## ¿De qué se trata esta ciberseguridad?

Un enfoque exitoso de la ciberseguridad tendrá muchas capas diferentes de protección que se distribuirán en todos los datos, programas, redes y computadoras que le gustaría mantener sanos y salvos. En los negocios, los procesos, la tecnología y las personas deben poder complementarse entre sí para garantizar que tengamos una defensa muy efectiva contra los ataques cibernéticos. Si uno o más de estos están apagados o falta un enlace, entonces se romperá la armadura y puede aumentar la cantidad de riesgo que existe para todos.

Un sistema unificado de gestión de amenazas puede automatizar las integraciones en todos sus procesos y facilitará mantener toda su red y la información que contiene lo más segura posible. Tenemos que

Sin embargo, asegúrese de que todas estas partes se unan y funcionen de la manera que queremos.

Lo primero a considerar es la gente. Esta suele ser la parte más débil del proceso. Alguien en la organización puede volverse descuidado, caer en una estafa de phishing o hacer algo más que pueda poner en riesgo la seguridad de toda la red. Los usuarios de esa red deben comprender y estar dispuestos a cumplir con los principios básicos de seguridad de datos que establece su empresa. Esto puede incluir cosas como elegir una contraseña que sea segura, hacer una copia de seguridad de sus datos y tener cuidado con los archivos adjuntos que pueden aparecer en los correos electrónicos.

Lo siguiente que debemos analizar aquí son algunos de los procesos que pueden aparecer en su red. Su organización debe tener algún tipo de marco establecido sobre cómo van a lidiar con todos los tipos de ataques, incluidos los que se intentaron y fallaron, y los que tienen éxito. Un marco muy respetado es capaz de guiar a todos en la red. Ayudará a todos a ver cómo pueden identificar estos ataques, proteger todo el sistema, detectar y responder a algunas de las amenazas e incluso cómo recuperarse de los ataques que terminan siendo exitosos.

Y por último, tenemos que centrarnos en la tecnología. Si la tecnología no es segura y no se cuida de la manera correcta, como hacer las actualizaciones necesarias y los cambios de software, entonces dejará muchas oportunidades para que un pirata informático experimentado ingrese al sistema. La tecnología va a ser esencial cuando se trata de brindar a las personas y organizaciones las herramientas de seguridad informática que necesitan para asegurarse de estar protegidos contra estos ataques.

Hay tres entidades principales en su red que debe asegurarse de que estén siempre protegidas para mantener segura toda la red. Estos incluyen los dispositivos de punto final, como los enrutadores, los dispositivos inteligentes y las computadoras, las redes y la nube. La tecnología común que se usa a menudo para ayudar a proteger estas entidades incluirá muchas funciones, incluidas soluciones de seguridad de correo electrónico, software antivirus, protección contra malware, filtrado de DNS y firewalls de última generación, por nombrar algunas.

Estas tres partes deben unirse para crear un sistema que sea seguro y protegido. Cuando una de estas partes falla o no mantiene el trabajo que debería, eso significa que todas las demás podrían estar en riesgo, y

es probable que alguien intente acceder a su sistema y utilice las vulnerabilidades que existen. Recuerde que si hay una manera de acceder a su sistema, ya sea a través de las personas, los procesos o la tecnología, entonces hay un hacker que intentará hacerlo.

Tener un hacker de sombrero blanco, o incluso un gran equipo de estos profesionales de TI si su empresa es más grande, trabajar para encontrar y protegerse contra las vulnerabilidades puede ser su mayor activo en general. Esto asegurará que pueda encontrar los problemas y resolverlos antes de que un hacker de sombrero negro pueda encontrar la información y explotarla en su beneficio.

## ¿Por qué es tan importante esta seguridad cibernética?

Lo siguiente que debemos analizar aquí es por qué esta ciberseguridad es tan importante. En el mundo conectado que vemos hoy, todos pueden beneficiarse cuando podemos avanzar en algunos de los programas de defensa cibernética. Podemos llevar esto hasta la más alta cooperación y hasta el nivel individual. Cuando miramos esto desde el nivel individual, el ataque puede resultar en muchos problemas, incluyendo intentos de extorsión por dinero, robo de identidad e incluso la pérdida de algunos datos importantes, incluidas fotos familiares.

Además de algunos de los problemas individuales que pueden surgir con estos problemas de ciberseguridad, todo el mundo va a depender de algunas de las infraestructuras más críticas de nuestro mundo moderno, incluidas las empresas de servicios financieros, los hospitales y las centrales eléctricas. Ser capaz de mantener este tipo de industrias y negocios a salvo de un ataque puede ser esencial para muchas personas en nuestra sociedad.

Todos también se beneficiarán en lo que respecta al trabajo que pueden hacer los investigadores de ciberamenazas. Un ejemplo de estos investigadores será el equipo de 250 investigadores de amenazas de Talos. Estas personas investigan algunas de las amenazas nuevas y emergentes y las estrategias de ciberataque que utilizan los piratas informáticos en nuestro mundo moderno.

Este grupo puede ser útil porque realizará una serie de tareas que ayudarán con la ciberseguridad de la que hemos estado hablando. Pueden revelar algunas vulnerabilidades nuevas que se han encontrado, educar al público sobre la importancia de la ciberseguridad y pueden fortalecer algunas de las herramientas de código abierto y fácilmente disponibles. Básicamente, el trabajo que este

El equipo y otros pueden hacer garantizará que Internet se mantenga lo más seguro posible para todos.

**Maneras de protegerse contra los ataques de seguridad cibernética** Por

supuesto, como empresa e incluso como individuo que desea mantener su información lo más segura posible, probablemente tenga curiosidad acerca de algunos de los métodos que pueden ayudarlo a hacerlo. Muchos hackers de sombrero blanco que trabajan para empresas están llenos de conocimientos sobre las mejores formas de evitar un ataque y cómo asegurarse de que puedan mantenerse a salvo. Pero cualquier persona, ya sea un profesional de TI o no, puede tener los recursos para mantener segura su información. Algunos de los mejores pasos para ayudarlo a mantenerse seguro con su red incluyen los siguientes:

1. Cuando proporcione su información personal, asegúrese de que solo está trabajando con sitios en los que confía. Una buena regla general para esto es verificar la URL. Si el lado incluye el https:// al principio, entonces sabemos que es un sitio seguro.
   Si a la URL le falta esa "s", es importante evitar ingresar cualquier tipo de información confidencial, como su número de seguro social o datos de su tarjeta de crédito, porque podría ser un sitio incorrecto.
2. Nunca debe abrir archivos adjuntos de correo electrónico ni hacer clic en enlaces que se encuentran en correos electrónicos de fuentes que no conoce. También debe asegurarse de que otros estén en la misma red que usted. Una de las formas más comunes en que las personas van a ser atacadas es con estos correos electrónicos que están disfrazados y enviados, pareciendo que provienen de alguien en quien realmente confías.
3. Mantenga los dispositivos actualizados. Si usted personalmente, o su lugar de trabajo, no mantiene los dispositivos lo más actualizados posible, esto puede causar algunos problemas para todos. Las actualizaciones de software serán importantes porque contienen algunos de los parches que necesita para solucionar problemas de seguridad y evitar los ataques cibernéticos. A los atacantes cibernéticos les encanta cuando un dispositivo está desactualizado porque es mucho más fácil para ellos ingresar a esa red y causar problemas.
4. Asegúrese de realizar copias de seguridad de sus archivos periódicamente para evitar ataques a su ciberseguridad. Si te atacan y necesitas borrar todos tus dispositivos para evitar el ataque

su computadora, será mucho mejor tener los archivos almacenados en otro lugar para que pueda recuperarlos cuando los necesite.

La ciberseguridad va a ser algo que siempre está evolucionando, lo que a veces hará que sea aún más difícil para nosotros mantenernos actualizados y actualizados sobre toda la información que debemos cuidar. Pero ya sea que estemos hablando de una empresa o de un individuo, es importante asegurarnos de que podamos mantener nuestra red segura para que nadie pueda entrar y robar nuestra información personal, pedir dinero o causar alguna de las otras problemas también.

Mantenerse informado y asegurarse de que usted y las personas que lo rodean sean lo más cautelosos posible en línea son dos de las mejores maneras de asegurarse de que está protegido y de que es probable que nadie le cause este tipo de ataques.

# Capítulo 5: Ataques de malware

Ahora que hemos dedicado un poco de tiempo a hablar sobre la importancia de la ciberseguridad para garantizar que nuestras redes y sistemas puedan mantenerse seguros, es hora de pasar a conocer algunos de los diferentes tipos destacados de ataques de malware que podemos observar. en contra Estos van a ser similares si está tratando de proteger su propia computadora personal o si está protegiendo grandes cantidades de datos e información personal para una gran empresa.

Los ataques de malware son un gran problema para muchas empresas y pueden ser uno de los mayores problemas en lo que respecta al mundo de la ciberseguridad. Si incluso una parte del sistema, ya sean los procesos, la tecnología o una de las personas en la red, cae presa de esto, entonces puede significar problemas para toda la organización. Es importante reconocer algunos de los ataques de malware más comunes y cómo funcionan para que podamos estar protegidos y a salvo de todos ellos mientras nos aseguramos de que nuestra información personal esté siempre sana y salva.

### Tres categorías de ataques cibernéticos

A pesar de toda la supuesta mística y misterio que rodea a las cosas conocidas como ataques cibernéticos, en realidad son casi todos los mismos delitos financieros y contra la propiedad, pero a veces agregan algunas herramientas nuevas. Debido al supuesto anonimato que las personas pueden asumir cuando usan Internet, hay muchas personas que se verán tentadas a cometer estos delitos, y muchas personas deben estar atentas antes de que se aprovechen de ellos en general.

Muchos de estos ciberdelincuentes podrán entrar y salir sin que te des cuenta, a menos que estés atento y observando tu sistema y cómo van las cosas. Otros pueden pasar demasiado tiempo alardeando de lo que hicieron y se meterán en problemas de esa manera. Pero una cosa es segura, debido al anonimato, muchas personas no querrían intentar entrar a una casa o cometer cualquier otro delito y podrían verse tentadas a probar el ciberdelito porque creen que no las atraparán.

Para el usuario promedio, esto significa que hay más ataques a sus sistemas y redes que nunca. Esto puede ser un problema para aquellos que quieren aprender a mantener segura su información, incluso si esa información son solo sus fotos familiares. La buena noticia es que hay formas en que podemos protegernos, solo debemos estar atentos con anticipación para que no se aprovechen de nosotros.

Para ayudarnos a comenzar, necesitamos echar un vistazo a algunas de las cosas que vienen con un ataque cibernético y cómo estar atentos a ellas. En su mayor parte, estos ataques cibernéticos se clasificarán en una de tres categorías que incluyen:

1. El objetivo y el criminal se van a conocer de alguna manera. El factor motivador en este a menudo puede ser la venganza o el dinero, y las muchas características distintivas que buscaremos son que el perpetrador culpable tenga o haya tenido acceso a la computadora de su objetivo. Esto les da tiempo para prepararse para el ataque con anticipación, plantar algún malware y más. En esta categoría, veremos cosas como el espionaje cibernético asumiendo un papel más importante con la ayuda de registradores de teclas, micrófonos y cámaras web.
2. La segunda opción es que exista algún tipo de relación entre el criminal y el objetivo, o, al menos, el criminal conoce a la víctima. Es posible que hayan hecho una conexión en cualquier plataforma de redes sociales, sean famosos o ricos, o posean algo que el hacker quería. La selección de una víctima no es aleatoria, aunque aún no se han conocido físicamente y no tienen acceso físico a la computadora del objetivo. La ganancia financiera será la motivación en este tipo de situación.

3. La víctima no es conocida por el criminal o es solo una persona que fue atrapada en la estafa de phishing del criminal u otra técnica similar. Ni la víctima ni el criminal tienen idea de quién es el otro.

## Ejemplos de ataques de malware

Con esta información en mente, es hora de echar un vistazo a algunos de los ataques de malware que existen y cómo podemos estar atentos a algunos de ellos. A menudo, la razón por la que estos ataques funcionan es un error humano. Una persona, el objetivo, no va a estar al acecho de problemas y dará

información que nunca tendrían si estuvieran pensando críticamente.
Esto puede ser una buena noticia si aprende a usarlo para su beneficio y se mantiene atento.

Descubrirá que los ciberdelincuentes, los ciberespías y los piratas informáticos van a utilizar muchas técnicas y vectores para ingresar a una red informática y robar información de los clientes, propiedad intelectual, información confidencial que puede identificar a una persona, incluida la seguridad social y crédito. números de tarjetas, registros de seguros médicos y de salud, planes comerciales, registros personales, registros de impuestos y cualquier otro dato del que puedan obtener dinero o utilizar para explotar en su propio beneficio.

Recuerda que cualquiera puede ser un objetivo. Muchas personas asumen que no necesitan tener cuidado en absoluto, pero los piratas informáticos incluso lo perseguirán. Pueden robar la información de su tarjeta de crédito, su información personal y más para obtener lo que quieren, y podría llevar años volver a poner las cosas en orden después de que esto suceda. No importa la ubicación, la industria o el tamaño del objetivo; el hacker irá tras ellos si creen que hay algo que ganar.

Hay una serie de métodos diferentes que el pirata informático puede emplear para realizar su trabajo y ver algunos de los resultados que desea.
Algunos de los ataques de malware más comunes que un objetivo debe tener en cuenta incluyen:

Correos electrónicos que tienen un archivo adjunto con malware y virus. Esta es una técnica más antigua que la mayoría de la gente sabe cómo evitar. Es bien sabido que debemos evitar abrir archivos adjuntos a menos que estemos seguros de que conocemos al remitente y que la información que contiene es legítima. Y, sin embargo, todavía hay muchas personas que se enamoran de este, y resulta exitoso para el hacker una y otra vez. Este puede ser uno de los métodos más conocidos para diseminar malware, y todo lo que incluye para el pirata informático es ocultar el software malicioso en un archivo adjunto en un correo electrónico. Una vez que el objetivo abre el archivo adjunto, el software malicioso se ejecutará o lo descargará en la computadora.

Lo mejor que puede hacer para evitar que esto suceda es no abrir archivos adjuntos de correos electrónicos no seguros. A menos que esté esperando un archivo adjunto de alguien específico, a menudo es mejor simplemente ignorar los correos electrónicos que tienen este tipo de cosas. Con suerte, la detección de spam que tiene en su

cuenta de correo electrónico hará que la mayoría de estos se pierdan de vista, pero a veces algunos se escabullen, y es mejor tener cuidado en lugar de tener malware en su computadora.

El segundo ataque de malware del que debemos estar atentos es similar al anterior, pero en lugar de un archivo adjunto, el problema será el enlace dentro del correo electrónico. Esto va a ser algo que se conoce como phishing.
A menudo, estos correos electrónicos aparecerán como correspondencia legítima de una institución, generalmente su banco, en la que es probable que el destinatario confíe y responda.

Sin embargo, el pirata informático ha diseñado el correo electrónico para rastrear el objetivo, y el enlace, cuando se hace clic en él, llevará al objetivo a un sitio web falso para que ese objetivo envíe información confidencial al pirata informático. Esto podría incluir cosas como el número de cuenta o el nombre de usuario y la contraseña del banco. Además, el sitio web malicioso a veces puede instalar spyware, virus o malware en la computadora del destinatario, lo que hace que sea más peligroso trabajar con él.

Lo mejor que puede hacer para evitar este tipo de ataque es tener mucho cuidado con los sitios web que elige visitar a través de enlaces. Verifica que el correo electrónico sea realmente de donde crees que es. Aún mejor, si es algo como su banco u otro sitio web en el que confíe, vaya directamente a ellos a través de una búsqueda en lugar de hacer clic en el enlace. De esta forma, tienes protegido si el enlace es bueno o no.

.

El siguiente en la lista será un perfil de red social o una página que tenga enlaces a un sitio web malicioso. Esto va a ser algo similar a lo que vemos con los correos electrónicos y los enlaces, pero este es un método que está creciendo en popularidad gracias a todo el bombo publicitario en las redes sociales. Se puede encontrar en casi cualquier cuenta de redes sociales que pueda usar, incluidos LinkedIn, Twitter y Facebook, por nombrar algunos.

Esta técnica es bastante efectiva ya que es menos probable que muchas personas estén alertas cuando están en las redes sociales, y es posible que no desconfíen tanto de estos sitios como lo harían con algunos de los otros sitios web que están fuera. allí. Sin embargo, con este método, el pirata informático configurará un perfil falso que atraerá a los usuarios reales a seguir los enlaces que hay allí.
Estos enlaces llevarán al usuario a un sitio web malicioso.

A veces, el perfil falso puede incluso hacer que los objetivos proporcionen información personal que es confidencial para obtener lo que el pirata informático desea.

Siempre tenga cuidado con lo que está haciendo en las redes sociales. Incluso si el enlace parece provenir de un amigo cercano o de otra persona, primero verifíquelo con ellos. Demasiadas veces, se puede crear una cuenta falsa y se verá exactamente como un amigo o familiar. Si tiene cuidado y verifica todo antes de hacer clic, descubrirá que es mucho más fácil mantenerse protegido en línea.

.

Otro ataque con el que debemos tener cuidado es probar los firewalls, DS y PS en busca de debilidades, incluida una puerta trasera. Esto es algo que el hacker va a hacer entre bastidores. El objetivo generalmente no tiene que hacer clic en nada para que esto suceda, pero si usa ciertas aplicaciones y sitios, o si no mantiene la protección adecuada en su computadora, podría dejar una oportunidad para que el hacker entre.

Con este, el pirata informático simplemente enviará transmisiones, generalmente en masa, con la esperanza de comprometer cualquier tipo de firewall u otra cosa que pueda encontrar. La esperanza aquí es que puedan obtener algún acceso a una computadora y al sistema que está detrás de ella. Este método será más o menos un juego de números para el pirata informático, y el sistema en el que se incorporen no tendrá ninguna conexión con ellos en absoluto. El pirata informático a menudo envía millones de transmisiones y espera atrapar incluso unas pocas computadoras en el proceso que tienen equipos sin parches, mal configurados o que funcionan mal. Este tipo de ataque también será difícil de rastrear sin alguna captura de paquetes en el camino.

La mejor forma en que podemos protegernos contra este tipo de ataque es asegurarnos de que su sistema esté lo más actualizado posible. Esto puede cerrar muchas de las vulnerabilidades que pueden existir, y hace que sea mucho más difícil para un pirata informático ingresar a su sistema y causar algunos problemas. Si puede mantener el sistema actualizado y tener cuidado con el tipo de software y más que pone en el sistema, encontrará resultados tremendos sobre lo que puede hacer con su sistema.

Los piratas informáticos también pueden optar por insertar algunos paquetes maliciosos en un flujo de comunicación legítimo para obtener los resultados que desean. Esto se verá como un nuevo tipo de técnica, una que dependerá del hacker.

poder acceder a un establo de computadoras zombies. Cuando pueden hacer esto, se pueden enviar grandes cantidades de paquetes a una gran cantidad de destinatarios, que apuntan a un determinado puerto que parece tener la vulnerabilidad que el pirata informático desea.

La esperanza con este es que, por casualidad, el pirata informático pueda acceder a un firewall o enrutador con ese puerto abierto, y luego usarlo como su forma de acceder a todo el sistema. Este es un tipo de ataque más difícil. Pero si el pirata informático tiene éxito con él, es prácticamente imposible que alguien rastree quién ingresó al sistema sin una captura de paquetes.

Otro tipo de ataque de malware con el que debemos tener cuidado son los anuncios que pueden enviar malware a los espectadores. Este es aún más difícil de evitar para las personas simplemente porque algunos de estos pueden aparecer, incluso cuando visitas una página que es legítima. Si uno de sus sitios web favoritos, por ejemplo, no está cuidando sus firewalls, puede ingresar y obtener malware en su computadora haciendo clic en una de las opciones allí.

Este método de ataque será difícil de evitar para nosotros debido a todos los anuncios pagados que podemos encontrar en los sitios web de Internet. Es posible que un ciberdelincuente coloque estos anuncios, que tienen un código malicioso, en sitios web legítimos y, por lo demás, seguros en los que los visitantes confiarían. Esto lo hace difícil porque, si bien debería poder ingresar y confiar en ese sitio web, es poco probable que a propósito elija un sitio web malo. Estos piratas informáticos aún pueden causar problemas.

Hay algunas formas en que el pirata informático puede obtener sus anuncios en el sitio web en primer lugar. A veces, en realidad compran el espacio publicitario directamente y luego colocan el malware dañino allí. A veces, secuestrarán el servidor de anuncios. Y otras veces, pueden infiltrarse en la cuenta publicitaria de otra persona y usarla para sus necesidades.

Siempre tenga cuidado con los tipos de anuncios en los que hace clic. Incluso si es un sitio web que parece seguro, asegúrese de que el anuncio sea algo que parezca legítimo y que pueda funcionar para lo que cree que afirma. Hay muchas veces que el anuncio se verá falso y como si fuera a causar un problema, y si alguna vez su intuición habla y le dice que no haga clic en algo, entonces continúe y escúchelo.

También podemos ver que el malware preinstalado puede ser un problema. En los últimos años, ha habido muchos informes sobre equipos de TI fabricados en el extranjero, incluidos conmutadores, enrutadores y computadoras. Y estas partes ya tienen malware preinstalado. De hecho, este es un problema tan generalizado que en 2012, Microsoft declaró que descubrió que ya había malware preinstalado en las computadoras nuevas vendidas. HP también anunció públicamente, más tarde ese mismo año, que hay Flashcards cargados con malware en algunos de los conmutadores que enviaron el año anterior.

Esto significa que debemos tener mucho cuidado con las computadoras y los programas que usamos regularmente. Estos, cuando no se compran a fuentes confiables y, a menudo, cuando provienen de otros países, podrían poner en riesgo nuestra información y seguridad. Verificar dos veces de dónde obtiene sus productos y qué problemas pueden surgir de esa área puede garantizar que obtengamos los programas y computadoras más seguros y sus partes a medida que lata.

Otro problema que puede surgir aquí es el malware que se vende como un tipo de software legítimo. Comprar malware de un vendedor sin nombre también puede presentar algunos peligros. Aunque el software puede proporcionar la función prometida en algunos casos, es posible que también tenga algún software malicioso incluido en el grupo.

Por ejemplo, los programas antivirus falsos han podido infectar millones de computadoras a lo largo de los años. Y de la misma manera, cualquier cosa, desde spyware hasta troyanos, se puede agregar a su computadora si se permite que el malware esté allí. En una investigación que IPCopper pudo realizar en 2013, se encontró que había al menos algunas instancias de software gratuito que estaba fácilmente disponible a través de Internet e incluiría opciones como reproductores de audio y video gratuitos, incluidos ejecutables maliciosos.

Para evitar este tipo de problemas, debemos tener cuidado con los tipos de programas que se nos permiten en nuestros sistemas y ser conscientes de cómo podrían causar algún daño a nuestros sistemas y a nosotros. Por ejemplo, cuando descargue algo gratis de Internet, asegúrese de verificar si es legítimo y si otros se han quejado del producto y las extensiones maliciosas que lo acompañan.

El último tipo de amenaza de malware que debemos analizar aquí incluirá APT o amenazas persistentes avanzadas. El término no significa un cierto tipo de técnica o tipo de ataque. En cambio, nos va a referir a un esfuerzo múltiple persistente y sostenido de irrumpir en la red de datos de una institución u organización.

Con estos APT, el pirata informático utilizará una serie de vectores de ataque, desde lo creativo hasta lo mundano, e incluso puede llegar a enviar algunos materiales promocionales falsos. Estos pueden variar según el objetivo del pirata informático y podrían ser algo así como una unidad flash gratuita para alguien que está más arriba en la organización. Sin embargo, cuando se usa, la intención es darle al hacker lo que quiere. La unidad flash podría cargar e instalar un archivo malicioso en la computadora y permitirle al pirata informático el acceso que desea.

Estos APT a menudo serán utilizados por grupos de atacantes que buscan obtener cierta información que desean de una organización u otra empresa. Estos tampoco son a corto plazo. A menudo, estos pueden durar al menos unos meses y, a menudo, unos pocos años o más.

Como podemos ver aquí, hay muchos tipos diferentes de ataques de malware con los que debemos tener cuidado regularmente. A los piratas informáticos nada les gustaría más que ingresar a un sistema al que no tienen acceso, ya sea una cuenta individual o la cuenta de una gran organización, y luego obtener la información financiera, personal y más de ese sistema. Aprender a reconocer los diferentes tipos de malware y descubrir las mejores formas de evitar ser víctima de él puede ser de gran ayuda para mantener su sistema lo más protegido posible.

# Capítulo 6: Ataques cibernéticos

Ahora que tenemos una idea un poco mejor de qué se trata el malware y cómo va a funcionar, es hora de que pasemos a algo conocido como ciberataque. Esto va a ser un gran problema tanto para las empresas como para las personas, y es importante que podamos reconocer las diferentes formas en que un pirata informático puede intentar ingresar a nuestro sistema y causar problemas.

Los ciberataques van a afectar a las empresas de forma regular. Según el ex director ejecutivo de Cisco, John Chamers, "Hay dos tipos de empresas: las que han sido pirateadas y las que aún no saben que han sido pirateadas". Esto significa que incluso si siente que nunca han sido pirateados y que la información que almacenan en sus sistemas está segura, es posible que haya un pirata informático en este momento que esté trabajando para ingresar a su sistema y explotar cualquier vulnerabilidad que tal vez existe o que en realidad tiene un hacker en su sistema y aún no se ha dado cuenta.

La verdad es que la ciberdelincuencia es algo que va en aumento año tras año, y tanto quienes utilizan computadoras como quienes se encargan de proteger mucha información personal y confidencial deben estar más atentos que nunca. Las personas están trabajando para cometer este tipo de delitos porque creen que pueden permanecer ocultos y quieren poder beneficiarse de ello de alguna manera. A menudo, los atacantes harán esto para obtener algún tipo de rescate. De hecho, el 53 por ciento de los ataques cibernéticos que ocurrieron recientemente resultaron en daños de $500,000 o más. Y muchos más fueron por montos menores.

Estas amenazas cibernéticas también se pueden lanzar con algunos motivos ocultos adjuntos. Por ejemplo, hay algunos piratas informáticos que realizarán este proceso como una forma de borrar un sistema y los datos que contiene. Pueden ver esto como una forma de hacktivismo que puede ayudar a proteger a otros.

Sin embargo, antes de continuar con esto, debemos echar un vistazo a un término más que nos ayudará a comprender qué está pasando con algo de esto.
Este término es botnet. Esta va a ser una red de dispositivos que han sido infectados con algún tipo de software malicioso, incluido un virus. Los atacantes pueden controlar este botnet o esta red como un grupo, sin el conocimiento del propietario, con el objetivo de aumentar la fuerza y la potencia de sus ataques en el futuro.

A menudo, el hacker quiere hacer esto lentamente y puede contener la red de bots por un momento, observando la información y esperando el momento adecuado para atacar. Pero una vez que decidan que es el momento adecuado para atacar, la botnet estará bajo el control del hacker y el propietario de esa red no lo sabrá. A menudo, la botnet se puede usar para ayudar a abrumar el sistema en un ataque DDoS o algo similar.

## Malware

El primer tipo de ataque cibernético del que debemos estar atentos es el malware. El malware es un tipo de software malicioso. En pocas palabras, el malware será cualquier tipo de software que se haya escrito con la intención de dañar los dispositivos, robar datos y causar problemas. Ransomware, spyware, troyanos y virus se encuentran entre los diferentes tipos de malware con los que podemos tener que lidiar.

El malware a menudo es algo que va a ser creado por un equipo de piratas informáticos, generalmente cuando quieren ganar dinero difundiendo el malware por su cuenta o vendiéndolo al mejor postor en la Dark Web. Sin embargo, hay ocasiones en que es una herramienta que utiliza un hacker para protestar, para probar la seguridad de un sistema, o incluso como arma de guerra entre diferentes tipos de gobiernos. No importa por qué o cómo surge el malware, nunca es una buena noticia cuando termina en su propia computadora.

En primer lugar, debemos ser capaces de comprender qué es capaz de hacer el malware. El malware es capaz de hacer todo tipo de cosas. Va a ser una categoría muy amplia, y lo que hace el malware o cómo funciona va a cambiar según el hacker y el tipo de archivo que intente usar. Los siguientes serán algunos de los tipos de malware más comunes y lo que pueden hacer cuando infectan una computadora o un sistema:

1. Virus: al igual que el homónimo del que provienen, estos virus pueden adherirse a algunos archivos limpios y luego infectarán otros archivos que estén limpios. Estos tienen el potencial de propagarse sin control, dañando las funciones principales del sistema e incluso eliminando o corrompiendo archivos. Estos a menudo van a aparecer como un archivo que es ejecutable.

2. Troyanos: esta será una opción de malware que puede disfrazarse como un tipo de software legítimo, o se ocultará dentro de algún software legítimo que el pirata informático haya podido manipular. Actuará de una manera más discreta y puede crear algunas puertas traseras en su seguridad, permitiendo efectivamente la entrada de otros tipos de malware en el proceso.

3. Spyware: Este va a ser un tipo de malware que es diseñado para realmente espiarte. Puede ocultarse en segundo plano y luego tomar notas e información sobre todo lo que haces en línea. Puede incluir sus hábitos de navegación, números de tarjetas de crédito y sus contraseñas.

4. Gusanos: el ataque de malware conocido como warm puede infectar una red completa de dispositivos, ya sea local o a través de Internet, con el uso de interfaces de red. Utilizará cada máquina infectada consecutivamente para ayudar a infectar algunas más en el camino.

5. Ransomware: este será un tipo de malware que puede bloquear su computadora y sus archivos y puede amenazar con borrar todo a menos que obtenga un rescate que ellos quieran. A menudo, esto no va a resolver el problema, pero el hacker aún obtiene el dinero.

6. Adware: aunque esto no siempre es algo malicioso, el software publicitario agresivo a veces puede socavar la seguridad de su sistema solo para mostrarle más anuncios. Y si esto continúa ocurriendo, proporcionará al malware un método fácil de ingresar. Piense en las ventanas emergentes cuando se trata de este tipo de ataque.

7. Botnets: Y finalmente, podemos hacer frente a un ataque de malware que es conocido como botnet. Estas serán redes de computadoras que ya están infectadas y que funcionarán juntas según el trabajo que el hacker quiera que realicen.

Hay ciertos tipos de malware que serán más fáciles de detectar en comparación con otros. Algunos, como el adware y el ransomware, darán a conocer su presencia de inmediato, ya sea cifrando sus archivos o transmitiendo una cantidad interminable de anuncios para usted. Podrás detectar estos

de inmediato y puede tomar las medidas necesarias para ayudar a eliminarlos de su sistema y evitar más problemas .

Luego, hay otras opciones, como el software espía y los troyanos, que se esforzarán por ocultarse de usted el mayor tiempo posible porque se utilizan cuando el hacker quiere poder permanecer en el sistema durante una buena cantidad de tiempo. hora. Esto significa que estarán en el sistema durante días, semanas e incluso meses, y no tienes ni idea de que están allí.

Y luego está el tercer tipo. Estos pueden incluir opciones como gusanos y virus que podrán operar y hacer su trabajo en secreto durante algún tiempo, y luego comienzan a aparecer los síntomas de su presencia y la infección que causan. En estos casos, es probable que veamos algunos problemas como archivos congelados, eliminados o reemplazados, el sistema se apaga repentinamente o un procesador hiperactivo.

La única forma segura de detectar todo este malware antes de que pueda infectar nuestra computadora o nuestro dispositivo móvil es instalar un software antimalware, que estará empaquetado con herramientas de detección y escaneos que pueden detectar cualquier del malware que ya está en el dispositivo y luego puede bloquear cualquier malware que intente infectarlo.

Cada forma de malware que encuentre vendrá con su propia forma de dañar e infectar datos y computadoras, lo que significa que cada uno necesitará un método diferente de eliminación. Trabajar con software anti malware, sin importar qué tipo de computadora o sistema operativo use, puede ayudar a evitar algunos de estos ataques.

**Phishing**

Hay ocasiones en las que un hacker va a utilizar una técnica que se conoce como phishing. Este será un tipo de delito cibernético en el que el objetivo es contactado por mensajes de texto, teléfono o correo electrónico por alguien que se hace pasar por una institución legítima para atraer a las personas para que les proporcionen datos confidenciales, como datos bancarios y de tarjetas de crédito. detalles, información personal y contraseñas para el uso de los piratas informáticos.

El hacker quiere hacer esto para obtener la mayor cantidad de información posible del objetivo. Esperan que el objetivo, sin prestar atención, les entregue

sobre esta información, y luego el pirata informático puede acceder a cualquier sitio web u otra cuenta que desee en función de la información que se le proporciona.

Hay algunas características comunes que aparecerán cuando veamos un correo electrónico de phishing. Primero, la oferta en el correo electrónico es demasiado buena para ser verdad. Es posible que este tipo de mensajes de texto o correos electrónicos ofrezcan puntos lucrativos y muchas declaraciones que llamen la atención. Estos están diseñados básicamente para captar la atención del objetivo de inmediato. ¡Podría ser algo tan simple como decir que ganó un gran premio si simplemente hace clic aquí! Asegúrese de que si recibe alguno de estos tipos de correo electrónico, no haga clic en él. Si algo parece demasiado bueno para ser verdad, entonces lo más probable es que lo sea.

Otra cosa a tener en cuenta con este tipo de ataques es que hay una sensación de urgencia que se proporciona en el interior. Una táctica favorita con la que les gusta trabajar a muchos ciberdelincuentes es pedirle al objetivo que actúe rápido porque el trato es solo por un tiempo limitado. A menudo, este tipo de ataques solo le darán unos minutos para responder. A menudo es mejor simplemente ignorarlos y ni siquiera abrirlos.

Recuerda que una empresa de confianza nunca te va a apurar. Si alguien va a cerrar tu cuenta, por ejemplo, porque hace tiempo que no la usas, te darán un mes más o menos para ir a revisar y decidir si quieres mantenerla o no. Si el correo electrónico dice que debe actuar ahora mismo, es una buena señal de que se trata de un intento de phishing. Nunca proporcione información sobre esto porque le dará al pirata informático exactamente lo que quiere, y esto realmente podría arruinarlo financieramente y más.

Los hipervínculos deberían ser otra señal de alerta de la que está atento. Un enlace no siempre es lo que parece, y si no tenemos cuidado con los enlaces que estamos usando, entonces nos puede llevar a algún lugar que no queremos.
Pasar el cursor sobre un enlace es una buena manera de ver a dónde nos llevará esa URL real si hacemos clic en ella.

Siempre queremos verificar dos veces cuando se trata de este tipo de cosas.
Los piratas informáticos son buenos para tomar un sitio web conocido y luego cambiarlo un poco, haciéndonos creer que el sitio web es seguro. Pero si lo miramos un poco más de cerca, veríamos que hay algo mal y

que este no es realmente el sitio web en el que queremos estar. Por ejemplo, un pirata informático podría tomar el sitio web de Bank of America y cambiar el motor a una r y una n para confundirnos, y luego enviarnos a un sitio web no seguro.

Si no está seguro de si el sitio web es el correcto o no, siempre es mejor hacer su propia verificación. Escriba el nombre de la empresa que cree que le está enviando un correo electrónico y vaya directamente a su sitio web sin hacer clic en el enlace. Si realmente te enviaron un mensaje por algo, podrás averiguarlo de esta manera. y si no, evitaste un ataque de un hacker.

También debemos estar al tanto de los archivos adjuntos que ingresan con nuestros correos electrónicos. Si ve un archivo adjunto que está en un correo electrónico que no esperaba recibir, o si realmente no tiene sentido que ese archivo adjunto esté allí en el correo electrónico, ¡nunca lo abra! Estos archivos adjuntos contendrán muchas herramientas para el pirata informático, como virus y ransomware, y descargarlos realmente puede causar un desastre en su computadora. El único archivo en el que siempre es seguro hacer clic es un archivo .txt, o si realmente está esperando un archivo adjunto de alguien en primer lugar.

Y lo último que debemos observar aquí cuando tengamos cuidado con el phishing es el remitente. Si el remitente es inusual, entonces esto es al menos una invitación a mirar un poco más de cerca lo que está sucediendo. Ya sea que parezca que se trata de alguien que no conoces o de alguien que realmente conoces, si revisas el correo electrónico y sientes que algo está fuera de lugar, inesperado, fuera de lo común o te hace sospechar, entonces es es mejor no hacer clic en él en absoluto.

Tenga en cuenta que, en la mayoría de los casos, los correos electrónicos enviados por estos ciberdelincuentes se enmascararán de manera que parezcan enviados por una empresa cuyos servicios son utilizados por el objetivo o el destinatario. Un banco y otras compañías no le pedirán información personal por correo electrónico ni suspenderán su cuenta si no actualiza algunos de los datos personales dentro de un cierto período de tiempo. En cambio, proporcionarán los datos personales y el número de cuenta en el correo electrónico para ayudarlo a ver que proviene de una fuente confiable.

## Hombre en el medio

El siguiente tipo de ataque que vamos a ver es el ataque del hombre en el medio. Aquí es donde el usuario malicioso, o el hacker, va a

insertarse entre dos partes en la comunicación, y luego intentará hacerse pasar por ambos lados de ese intercambio. Luego, el atacante interceptará, enviará y recibirá datos destinados a cualquiera de los dos usuarios, incluidas cosas como contraseñas y números de cuenta.

Por lo general, cuando hay alguna comunicación con nuestras computadoras, el flujo se producirá entre el cliente y el servidor. Entonces, si desea acceder a su propia cuenta bancaria a través del sitio web del banco, entonces su propia computadora, que es el cliente, enviará la información de inicio de sesión necesaria a los servidores del banco. Si los servidores del banco ven que esta información es correcta, devolverán la verificación de un intento de inicio de sesión exitoso y luego podrá acceder a la cuenta.

Otro ejemplo de esto es cuando compras en Amazon. Es necesario crear una interacción entre la entidad financiera y el servidor, que se utilizará para cargar su cuenta al realizar una compra. En cualquiera de los dos escenarios, el hombre en el ataque del medio puede aparecer y cambiar el flujo de esta información de manera dramática.

El usuario malicioso establecerá un relé de comunicación entre el servidor y el cliente real donde podrá modificar y monitorear toda la comunicación compartida entre ambas personas. En lugar de que el servidor reciba la información directamente del cliente, la información se dirigirá directamente al usuario malicioso primero.

Ahora, hay algunas cosas que pueden suceder aquí. A veces, el ataque del hombre en el medio simplemente está sucediendo para que el pirata informático pueda obtener información útil. Pueden recopilar los datos, revisarlos y luego enviarlos a su destino. Esto les permite quedarse por un tiempo y aprender más sobre el sistema antes de que hagan más con el ataque. Además, es posible que el hacker tome la información y la use para sus propias necesidades, como con nombre de usuario y contraseñas, o puede alterar la información y enviarla en su lugar.

Por ejemplo, es posible que el remitente comunique que le gustaría que el número de cuenta bancaria receptora sea 123456789 para una transacción específica. Pero un hacker que está usando el ataque del hombre en el medio podría interceptar esa información y cambiar el número de cuenta bancaria. El número de cuenta será luego notificado al banco, y porque

no se dan cuenta de que algo está mal aquí, enviarán el dinero a la cuenta que especificó el pirata informático, en lugar de a la que el usuario realmente quería. Y a menudo, esto no se detecta hasta que es demasiado tarde.

Hay una serie de otros ataques que pueden encajar en este tipo de categoría. El ataque del hombre en el medio es básicamente una forma de secuestro de sesión. Una sesión va a ser un período de actividad que ocurre entre un usuario y un servidor durante un período de tiempo específico. Por ejemplo, cada vez que accede a su propia cuenta bancaria y luego interactúa con ella de manera activa, se trata de una sesión. Cuando cierra sesión en esa cuenta, significa que la sesión ha finalizado.

Por supuesto, en realidad hay bastantes otros tipos de ataques que se aprovecharán del secuestro de sesión similar a lo que vamos a ver con un ataque de hombre en el medio, y estos pueden incluir algunos de los siguientes:

1. Rastreo: Esto implicará que el pirata informático use un software que pueda interceptar los datos que se envían desde o hacia el dispositivo que está utilizando.
2. Sidejacking: este tipo de ataque consiste en detectar paquetes de datos que se envían entre el cliente y el servidor para robar las cookies de la sesión y poder acceder a una sesión. Estas cookies son importantes para el hacker porque incluyen cierta información de inicio de sesión sin cifrar, ya sea que el sitio sea seguro o no en primer lugar.

3. Gemelo malvado: a veces, el pirata informático llevará este proceso tan lejos que creará una red inalámbrica no autorizada que parece ser legítima. Los usuarios sin saberlo se unirán a esa red y luego la usarán para una actividad regular en línea sin darse cuenta de que, durante este tiempo, se recopila su información. Esto a menudo hace que sea más fácil para uno de los ataques de los hombres en el medio.

Hay algunas cosas que podemos hacer para asegurarnos de que este ataque de hombre en el medio sea menos probable que nos suceda a nosotros. En el lado del cliente, no hay tantas defensas con las que podamos trabajar para este ataque. La mayoría de las medidas de protección que ocurren en el lado del servidor serán en forma de fuertes protocolos de encriptación entre el servidor y el cliente. Para

ejemplo, un servidor puede autenticarse presentando un certificado digital, que es básicamente una verificación que permite que el cliente y el servidor establezcan su propio canal encriptado para intercambiar datos. Pero esto solo funciona si el servidor tiene este tipo de medidas de cifrado implementadas en primer lugar.

Desde la perspectiva del cliente, el mejor tipo de estrategia que podemos emplear es asegurarnos de que nunca nos conectemos a enrutadores inalámbricos abiertos, o debemos asegurarnos de que usamos complementos de navegador como HTTPS.

**Ataque de denegación de servicio**

Otro tipo de ataque con el que puede trabajar un pirata informático se conoce como ataque de denegación de servicio o DoS. Este va a ser un tipo de ataque cibernético intencional que se lleva a cabo en sitios web, recursos en línea y redes para que se pueda restringir el acceso que los usuarios legítimos tienen a esa fuente.
Este ataque va a ser muy notable y podría durar todo el tiempo que quisiera el hacker. A veces, esto es solo unas pocas horas mientras entran y salen con la información que desean. Y otras veces, podría durar unos meses. Por ejemplo, un ataque DoS que prevalece bastante en la web en este momento se conoce como ataque DDoS o Denegación de servicio distribuida.

Los ataques DoS están aumentando porque muchos consumidores y empresas están trabajando con más plataformas digitales para realizar transacciones y comunicarse entre sí. Estos ciberataques van a tener como objetivo la propiedad intelectual y las infraestructuras digitales. A menudo, estos se lanzarán para robar parte de la información de identificación personal que se encuentra en ese sistema, lo que puede causar un daño considerable a las finanzas y la reputación de esa empresa.

Las brechas de datos, por ejemplo, van a atacar a una empresa determinada o a un grupo de empresas en el mismo período. Los protocolos de alta seguridad colocados con anticipación por una empresa aún podrían enfrentar un ataque a través de un miembro de su cadena de suministro si ese miembro no cuenta con las medidas de seguridad adecuadas.

Cuando el pirata informático selecciona más de una empresa para este ataque, los perpetradores pueden utilizar el ataque de denegación de servicio para ingresar al sistema y causar más problemas antes. En el ataque DoS, el

Por lo general, el pirata informático utilizará solo un dispositivo y una conexión a Internet para enviar una solicitud rápida y continua al servidor de destino. El objetivo de hacer esto es sobrecargar el ancho de banda del servidor y provocar que se bloquee.

.

Los piratas informáticos de este tipo de ataque intentarán explotar la vulnerabilidad del software en el sistema, y luego pasarán a agotar la RAM o la CPU del servidor si pueden. La pérdida o el daño del servicio causado por este ataque se puede reparar bastante rápido con la ayuda de un firewall y permitiendo y denegando reglas, pero lleva un poco de tiempo lograrlo.

Dado que este tipo de ataque solo funcionará con una dirección IP por parte del pirata informático, es más fácil encontrar esta dirección IP y luego negarle el acceso con la ayuda del firewall. Esto hace que sea más fácil detener el ataque DoS si puede hacer que el firewall haga su trabajo. Sin embargo, algunos tipos de ataques, como este, por ejemplo, pueden ser un poco más difíciles de detectar y detener, y eso se conoce como ataque de denegación de servicio distribuido o DDoS.

Cuando observamos un ataque DDoS, significa que el pirata informático está trabajando con conexiones y dispositivos infectados varias veces, por lo general, los que están repartidos por todo el mundo y se han convertido en una red de bots. Esta va a ser una red de dispositivos personales que han sido comprometidos por un pirata informático sin que el propietario de ese dispositivo tenga idea de lo que está sucediendo.

El hacker infectará las computadoras que quiera usar. Para que puedan tener el control del sistema, utilizarán algún software malicioso. Luego pueden enviar solicitudes falsas y spam a otros servidores y dispositivos.
Si este ataque ataca a un servidor de destino, básicamente experimentará una cierta sobrecarga porque cientos o miles de tráfico falso los afectará, todo al mismo tiempo.

Debido a que el servidor está siendo atacado desde muchas ubicaciones, en lugar de solo desde una, la detección de todas las direcciones IP es más difícil y podría resultar realmente difícil. Y el cortafuegos tiene el problema adicional de separar el tráfico legítimo del tráfico falso, y el servidor descubrirá que es casi imposible resistir uno de estos ataques.

A diferencia de algunos de los otros tipos de ataques cibernéticos que se inician para robar información que es más confidencial, los ataques DDoS iniciales se lanzan para hacer que el sitio web sea inaccesible para los usuarios legítimos. Sin embargo, a veces, estos ataques son más una pantalla para otros actos maliciosos. Cuando los servidores han sido derribados con éxito, los culpables pueden ir tras bambalinas para desmantelar los cortafuegos del sitio web o debilitar la seguridad para que puedan continuar con algunos de los otros planes de ataque que tienen.

A veces, un ataque DDoS se puede utilizar más como un ataque a la cadena de suministro digital. Si el pirata informático no puede penetrar y atravesar el sistema de seguridad de otros sitios web, puede encontrar un enlace débil que esté conectado de una forma u otra con todos los demás objetivos. Luego, el hacker elegirá atacar ese enlace en lugar de trabajar en los grandes individualmente. Cuando este enlace se ha visto comprometido, los objetivos principales también se verían automáticamente afectados de manera indirecta.

**Exploit de día cero** El

último tipo de ataque que vamos a analizar se conoce como exploit de día cero o vulnerabilidad de día cero. Esta va a ser una vulnerabilidad que ocurre en la seguridad del software, que el proveedor del software conoce, pero no tiene un parche en el momento para corregir la falla. Esto significa que tiene cierto potencial para que un ciberdelincuente lo use y haga un lío.

En el mundo de la ciberseguridad, estas vulnerabilidades serán las fallas no deseadas que se encuentran en nuestros programas o sistemas operativos. Estos pueden ser el resultado de configuraciones informáticas o de seguridad incorrectas y, a veces, son solo un error de programación. Si no se maneja, estos van a causar algunos agujeros en la seguridad que un ciberdelincuente estará más que feliz de explotar.

Estos van a representar un gran riesgo de seguridad para alguien que esté usando ese programa o sistema operativo. Los piratas informáticos van a escribir un código destinado a apuntar a la inseguridad de debilidad específica que existe. Luego pueden empaquetarlo en un malware que se denomina exploit de día cero. El software malicioso que se diseña aquí está configurado para aprovechar, tanto como sea posible, la vulnerabilidad para comprometer un sistema informático o causar

algún otro comportamiento que no es intencionado. En la mayoría de los casos, si la empresa puede crear un parche para la vulnerabilidad, el ataque se detendrá.

Pero entonces, tenemos que preocuparnos por lo que sucederá si su computadora es una de las opciones que se infecta. Este tipo de malware puede robar sus datos, lo que le permite al pirata informático obtener el control que desee sobre el sistema. El software que está en su computadora a veces también se puede usar de una manera que no estaba prevista al principio, como instalar otro malware que corromperá los archivos o accederá a su lista de contactos para enviar mensajes de spam a cualquier persona en la cuenta. También podría instalar algún software espía que robe información confidencial de la computadora. Básicamente, si el pirata informático es capaz de atravesar una de estas vulnerabilidades antes de que se diseñe un parche para ello, entonces puede hacer lo que quiera en su sistema.

El término día cero se refiere a una vulnerabilidad recién descubierta en el software. Debido a que el desarrollador ya se enteró de la falla, también significa que no ha tenido tiempo de publicarse un parche oficial o una actualización para solucionar los problemas. Entonces, la idea de día cero se referirá al hecho de que los desarrolladores tienen cero días para solucionar el problema que acaban de exponer y que los piratas informáticos ya lo están explotando. Una vez que el público conoce la vulnerabilidad, es trabajo del proveedor trabajar lo más rápido posible para solucionar este problema y asegurarse de que los usuarios estén protegidos.

Tenga en cuenta que debido a que la vulnerabilidad ya se encontró, es probable que el proveedor del software no lance un parche antes de que los piratas informáticos puedan explotar el agujero en la seguridad. Esto lo convierte en un ataque de día cero y muchos usuarios de ese software podrían estar en riesgo. Lo mejor que puede hacer aquí es asegurarse de estar protegido contra estas vulnerabilidades de día cero. Estos pueden presentar un gran riesgo de seguridad que lo dejaría susceptible a muchas cosas, incluido el daño a sus datos personales y su información personal.

Para asegurarse de que sus datos y su computadora estén seguros, es mejor tomar medidas de seguridad reactivas y proactivas. La primera línea de defensa en la que puede confiar será ser proactivo mediante el uso de un software de seguridad completo cada vez que pueda. Esto puede ayudar a garantizar que esté protegido contra amenazas conocidas y desconocidas todo el tiempo. Luego, la segunda línea de defensa se conoce como reactiva, y será cuando instalemos de inmediato algunas actualizaciones nuevas para software nuevo cada vez que

estar disponible del fabricante. Esto nos ayuda a reducir el riesgo de que seamos dañados por una infección de malware.

La actualización de software adecuada nos ayudará a instalar todas las revisiones necesarias del sistema operativo o del software. Estos podrían incluir cosas como agregar algunas funciones nuevas, eliminar cualquier función que esté desactualizada, actualizar los controladores, corregir algunos errores en el sistema e incluso corregir algunos de los agujeros de seguridad que hemos descubierto.

Sin embargo, hay algunos otros pasos que podemos tomar para asegurarnos de que no nos atrape uno de estos ataques de día cero. Estos pasos van a incluir:

1. Mantenga sus parches de seguridad y todo su software actualizado tanto como sea posible. Puede hacerlo descargando las versiones y actualizaciones del software. Cuando agrega los parches de seguridad a medida que aparecen, ayuda a corregir cualquier error que una versión anterior del software pueda haber pasado por alto en algún momento.
2. Establezca algunos hábitos personales de seguridad en línea seguros y efectivos en cualquier momento que se conecte.
3. Configure los ajustes de seguridad en su sistema operativo, su software de seguridad y su navegador de Internet.
4. Asegúrese de instalar un software de seguridad integral y proactivo que nos ayude a bloquear las amenazas y vulnerabilidades conocidas y desconocidas en su sistema.

Como podemos ver aquí, un pirata informático tiene muchas herramientas en su arsenal cuando es hora de que se conecten e intenten tomar su información personal, o incluso cuando les gustaría secuestrar su sistema y su red para sus propios fines personales. ganar. Reconocer algunos de estos ataques y observar algunos de los pasos que puede seguir para evitar estos ataques y mantener seguros sus datos e información personal puede marcar una gran diferencia en los resultados que obtendrá.

# Capítulo 7: Cómo escanear los servidores y el La red

Una cosa en la que debemos dedicar algo de tiempo mientras estamos aquí es cómo podemos escanear nuestros servidores y la red en la que estamos. Esto puede parecer una pérdida de tiempo, ¿no deberíamos conocer todos los puertos, sistemas y dispositivos que hay en nuestra red? Pero, sorprendentemente, muchos profesionales no tienen idea de lo que hay en su red. Incluso si lo hace, esto también significa que puede tomarse el tiempo para asegurarse de que no haya usuarios no autorizados en el sistema y le da la oportunidad de expulsarlos si están allí. Echemos un vistazo a algunos de los pasos que podemos seguir para ayudarnos a escanear los servidores y la red, y asegurarnos de que todo esté sano y salvo como debería ser:

**Primeros pasos**

Necesitamos asegurarnos de tomarnos el tiempo para revisar nuestro sistema y pensar como un hacker. ¿Dónde es más probable que entren en la red y traten de causar problemas? ¿Qué información le interesaría más al hacker en la reunión si quisiera obtenerla si pudiera? Algunas de las otras preguntas que puede responder cuando sea el momento de comenzar con su propio escaneo de red para ayudarlo a dirigir sus actividades incluyen:

- Si alguien intentara atacar el sistema, ¿qué parte terminaría causando más problemas o qué parte sería realmente difícil si perdiera la información?
- Si tuvo un ataque al sistema, qué parte del sistema es la más vulnerable; por lo tanto, el que es más probable que su hacker utilizar.
- ¿Hay alguna parte del sistema que no esté tan bien documentada o que apenas se controle? ¿Hay incluso algunos que están allí que no le son familiares (o que ni siquiera ha visto en el pasado)?

Con estas preguntas respondidas y una buena idea de hacia dónde le gustaría llevar este proceso, y comenzó una buena lista de algunas de las aplicaciones y

sistemas que más le interese ejecutar, es hora de seguir los pasos para asegurarse de que todas las partes de su sistema estén cubiertas. Queremos ejecutar estas pruebas en todas las partes dentro de nuestra computadora, verificando dos veces que todo sea seguro. Algunas de las diferentes partes de este proceso que debemos recordar incluirán lo siguiente:

- Sus enrutadores y sus conmutadores
- Cualquier cosa que esté conectada al sistema. Esto incluiría cosas como tabletas, estaciones de trabajo y computadoras portátiles.
- Todos los sistemas operativos, incluidos el servidor y el cliente.
  unos.
- Los servidores web, las aplicaciones y la base de datos.
- Asegúrese de que todos los cortafuegos estén en su lugar.
- Los servidores de correo electrónico, archivo e impresión.

Ejecutará muchas pruebas diferentes durante este proceso, pero esto asegurará que revise todo en el sistema y encuentre las vulnerabilidades que existen. Cuantos más dispositivos y sistemas necesite comprobar, más tiempo le llevará organizar el proyecto. Puede realizar algunos cambios en la lista y simplemente elegir las opciones que considere más importantes para ahorrar tiempo y mantener su sistema seguro.

## ¿Qué pueden ver los demás con mi sistema?

Una cosa que debemos tener en cuenta al pasar por todo este proceso es lo que otros pueden ver cuando miran a la empresa. Con suerte, su seguridad es bastante buena en este punto, y solo verán algunos de los aspectos básicos, como su sitio web y la información financiera que se requiere.

Pero desea asegurarse de que no haya nada más en su sistema o red que muestre que otros puedan acceder fácilmente.

Cualquier pirata informático que intente acceder a su sistema dedicará tiempo a investigar su red y su sistema y ver dónde pueden estar las vulnerabilidades. Si usted es el propietario de este sistema, es posible que se pierda algunas de estas partes más obvias, por lo que es importante echarles un vistazo desde un ángulo completamente nuevo. Hay algunas opciones que podemos usar cuando

queremos recopilar información en nuestra propia red, pero el primer lugar para ir aquí es una búsqueda en línea.

Para hacer esto, solo necesitamos hacer una búsqueda en línea sobre la empresa o el individuo y ver qué información hay que se relacione con nosotros. Luego puede trabajar para completar una sonda para averiguar qué otra persona podrá ver con su sistema. A veces, un escáner de puerto local también puede ayudar. Tenga en cuenta que esta búsqueda en Internet no tiene que ser tan compleja, pero puede profundizar y realmente buscar para no perderse algunas de las cosas que se envían al mundo a través de su computadora. Algunas de las cosas en las que debe centrarse en la búsqueda de su sistema incluyen las siguientes:

- Cualquier información de contacto que le permita a otra persona ver quién está conectado con el negocio. Algunos de los buenos lugares para visitar incluyen USSearch, ZabaSearch y ChoicePoint.
- Revise los comunicados de prensa que hablen sobre cambios importantes en la empresa.
- Cualquiera de las adquisiciones o fusiones que se han producido para la empresa.
- Documentos de la SEC que están disponibles.
- Cualquiera de las patentes o marcas que son propiedad de la empresa.
- Las presentaciones de incorporación que a menudo se realizan ante la SEC, pero en algunos casos, también pueden estar en otros lugares.

Esta es una gran cantidad de información para buscar, pero puede ser valiosa para un pirata informático, y debe poder determinar cuánto hay disponible para que lo use el pirata informático. Una búsqueda por palabra clave no será suficiente; necesita profundizar aún más y hacer algunas búsquedas avanzadas para encontrar esta información.
Tómese el tiempo para escribir parte de esta información para que tenga una mejor idea de qué tan grande es la red, qué información se está revelando al público y otras vulnerabilidades que pueden dañar su red.

**Cómo mapear la red** Una vez que hayamos

podido completar toda la información anterior y podamos comenzar un poco de nuestra investigación también, es hora de comenzar el proceso real de un truco ético. Su sistema o red va a tener muchos

información y dispositivos en él, y debemos asegurarnos de que esté protegido, incluso cuando también hay una tonelada de usuarios en el sistema. Los dispositivos deben ser seguros, y todos los empleados deben cumplir con estándares más altos para garantizar que no utilicen la red ni ningún dispositivo de manera inapropiada.

Para este punto, necesitamos poder crear un mapa de la red que controlamos. La razón de esto es ver todo lo que está incluido en la red y ver mejor, generalmente de forma visual, dónde podrían terminar todos los problemas en el sistema. Esta también es una buena manera de ver qué huella está dejando nuestra red o sistema en línea para que otros, incluidos los piratas informáticos, también la vean y la exploten para sus propias necesidades.

Un buen lugar para ayudarnos a comenzar con esto es la opción Whois. En realidad, este fue un sitio que se diseñó originalmente para ayudarnos a determinar si un nombre de dominio estaba abierto para usar, pero también es un excelente lugar para comenzar si desea ver qué información hay en el registro de cualquier nombre de dominio. Si ingresa aquí y realiza una búsqueda, y ve que aparece su propio nombre de dominio, muestra que la información personal sobre usted y la empresa, incluidos los nombres de las personas que dirigen la empresa y las direcciones de correo electrónico, se transmite al menos a través de este sitio, si en ningún otro lugar.

Whois puede proporcionar información sobre todos los servidores DNS que se encuentran en un dominio en particular, así como un poco de información sobre su soporte técnico que utiliza el proveedor de servicios. Un lugar que realmente necesita buscar es en DNSstuf para que pueda encontrar mucha de la información que se muestra sobre su nombre de dominio, que incluye:

- La información sobre cómo el anfitrión puede manejar todos los correos electrónicos para este nombre en particular.
- Dónde se encuentran todos los hosts Parte
- de la información general que puede ser útil para un hacker sobre el registro del dominio.
- Información sobre si esto tiene un host de spam con él.

Este es solo uno de los sitios que puede visitar para encontrar parte de esta información, y es una buena idea revisar algunos de ellos. Esto ayuda a dar un buen comienzo en la información que puede estar disponible en línea para su dominio y su empresa, pero hay algunos otros lugares que debe consultar, incluidos:

Además de trabajar con la opción Whois anterior, es posible echar un vistazo a través de Foros y Grupos de Google, y algunas otras opciones similares.
Estos serán útiles para los piratas informáticos porque hay una tonelada de información que se puede publicar sobre su negocio o red en estos foros y más, aunque usted no haya sido quien los revisó y publicó la información.

Dependiendo del tipo de información que alguien más fue y publicó aquí para que otros la vean, podría haber problemas de seguridad en los que deba concentrarse y obtener más información. A veces, si un pirata informático ya ha estado en su red y quiere vender la información a otros, es posible que cosas como su dirección IP, nombre de dominio y nombres de usuario estén en el sitio. Una simple búsqueda de su propio nombre de dominio o nombre de la empresa suele ser suficiente para averiguar si hay algún problema de seguridad presente en el sitio.
.

La buena noticia con este es que si está en uno de estos foros y descubre que su información de seguridad está allí, es posible revisar y eliminar esa información antes de que más personas la descubran y la utilicen para su beneficio. Tienes que mostrar cómo el dominio o negocio es tuyo, con las credenciales correctas, pero esto no debería ser un problema si estás haciendo este tipo de escaneo. Luego puede ir al área para el personal de soporte en estos sitios y presentar su propio informe para eliminar esa información lo más rápido posible.

**Completar el escaneo** A

medida que avanzamos en algunos de los pasos que se enumeraron anteriormente, debemos recordar que el objetivo principal es averiguar cuánto de nuestro sistema o red ya está disponible en línea para obtener una mejor imagen. sobre dónde podría mirar el hacker para iniciar uno de sus propios ataques. Por supuesto, este es un proceso que no es fácil y puede llevar algún tiempo completarlo. Los piratas informáticos no se dan por vencidos fácilmente y están decididos a ingresar al sistema. Tu trabajo es atraparlos y llegar a las vulnerabilidades antes que ellos para detener el caos que puedan intentar.

Ahora que hemos realizado algunos de los otros pasos y tenemos la información necesaria, es hora de que nosotros, como piratas informáticos éticos, completemos algunos pasos más para asegurarnos de que la red esté cerrada y que las vulnerabilidades

son manejados. Y podemos hacer todo eso con la ayuda de un escaneo de toda la red antes de tiempo.

Estos escaneos son útiles porque nos mostrarán algunas de las vulnerabilidades que hay en nuestro sistema, lo que facilita saber por dónde empezar cuando queremos proteger la red. Algunos de los diferentes escaneos que los piratas informáticos éticos pueden considerar hacer para mantener su información sana y salva incluyen los siguientes:

1. Visite Whois como mencionamos anteriormente y luego mire el nombres de host y las direcciones IP. Vea cómo se presentan en este sitio, y también puede tomarse el tiempo para verificar la información que se encuentra allí.
2. Ahora, es el momento de escanear algunos de sus hosts internos para que pueda ver qué usuarios pueden acceder al sistema. Es posible que el pirata informático provenga de la red, o que pueda obtener algunas de las credenciales de un empleado que no tiene cuidado, así que asegúrese de que todos tengan las credenciales correctas según el lugar en el que se encuentren en la empresa.

3. Lo siguiente que deberá hacer es verificar el ping utilidad del sistema. A veces, una utilidad de terceros ayudará con esto para que pueda hacer ping en más de una dirección a la vez. SuperScan es una excelente opción para usar. También puede visitar el sitio www.whatismyip.com si no está seguro del nombre de la dirección IP de su puerta de enlace.

4. Y finalmente, necesita hacer un escaneo externo de su sistema con la ayuda de todos los puertos que están abiertos. Puede abrir el SuperScan nuevamente y luego verificar lo que otra persona puede ver en la red con la ayuda de Wireshark.

Todos estos escaneos son excelentes para ayudarlo a descubrir qué está enviando su dirección IP en línea y qué pueden ver los piratas informáticos cuando intentan ingresar a su sistema. Básicamente, un hacker puede hacer algunos de los mismos pasos que usted acaba de hacer en el sistema para ingresar y ver qué sucede para ver los correos electrónicos que se transmiten de un lado a otro, e incluso aprender cómo obtener la información correcta para tener control remoto. acceso. El objetivo de estos escaneos es encontrar

averigüe por dónde puede entrar el hacker para que pueda cerrarlo y mantener el sistema seguro.

Una vez que nos hemos tomado el tiempo para tener una buena idea de cómo un pirata informático puede ingresar a nuestra red, a menudo es mucho más fácil aprender la forma exacta en que cualquier pirata informático intentará atacar esa red o la computadora. Tenga en cuenta que el pirata informático no quiere trabajar más de lo necesario, por lo que se quedará con el método más fácil disponible, mientras se mantiene oculto en el sistema. A veces, es lo primero que intenta y, a veces, tiene que probar algunas cosas para mantener alejado al hacker.

Estos escaneos son importantes y son algo que debemos seguir haciendo de manera regular. No es suficiente para nosotros simplemente hacer los escaneos y luego llamarlo bueno para siempre. A medida que comience a usar la red y tal vez incluso crezca un poco más con el tiempo, la información que se envía cambiará y los piratas informáticos siempre encontrarán algunas de esas vulnerabilidades.
Realizar estos escaneos regularmente, según el cronograma que sea bueno para su empresa y los profesionales de TI, puede ayudar a mantener alejados a todos los piratas informáticos que no pertenecen allí.

# Capítulo 8: Los fundamentos de la seguridad web

El siguiente tema que debemos analizar es nuestra seguridad web. Si no tenemos cuidado cuando trabajamos en línea y visitamos una variedad de sitios web, nos estamos preparando para un gran ataque. Los piratas informáticos tienen muchos métodos diferentes que pueden utilizar cuando se trata de estar en línea y en una variedad de sitios web. Y si el usuario desprevenido no tiene cuidado con lo que sucede a su alrededor, es probable que invite al hacker directamente a su sistema.

Los sitios web serán propensos a muchos riesgos de seguridad, al igual que cualquier red que esté conectada a un servidor web. Dejando de lado algunos de los riesgos que surgen debido al uso por parte de los empleados o porque los recursos de la red están siendo mal utilizados, su servidor web y el sitio que aloja presentan sus fuentes más serias de riesgo de seguridad.

Los servidores web, por diseño, abrirán una ventana que vinculará su red con el mundo. El cuidado que se tenga con el mantenimiento del servidor, las actualizaciones de la aplicación web y la codificación de su sitio web definirá el tamaño que vemos con esta ventana y puede limitar la cantidad y el tipo de información que puede pasar a través de la ventana. Si está codificado de la manera adecuada y está configurado de la manera que le gustaría, entonces nos ayudará a tener algo de seguridad web que tendrá cuando se conecte a Internet. .

La seguridad web va a ser más relativa y tiene dos componentes, incluido uno público y otro interno. Su seguridad relativa será alta si ya tiene algunos recursos de red que tienen un valor financiero más alto, su empresa y sitio no presentan nada controvertido de ninguna manera, y su red ha tenido algunos permisos estrictos. Agregue que el servidor web está actualizado con parches con todas las configuraciones hechas de la manera correcta, sus aplicaciones en el servidor web están todas parcheadas y actualizadas, y el código del sitio web está hecho con altos estándares, y usted tiene una red segura .

Puede imaginar que mantenerse al día con todo esto va a ser un poco difícil, y es posible que no le brinde todos los resultados que está buscando. Si uno de estos falla un poco, o termina con alguien en el sistema que no tiene cuidado con la forma en que se comporta en línea, entonces su seguridad terminará siendo un poco más baja.

Además, verá que hay algunos factores que nos mostrarán que la seguridad web es relativamente menor para su empresa. Algunos de los problemas que debemos analizar aquí cuando se trata de ver nuestra seguridad web más baja de lo normal incluyen:

1. La empresa tiene muchos activos financieros importantes a los que se aferra. Esto podría incluir mucha información sobre números de tarjetas de crédito o información sobre la identidad de los clientes.
2. Si el contenido de su sitio web o con su red es más controvertido.
3. Si sus servidores, aplicaciones y el código del sitio son más complejos o si es más antiguo y si los mantiene un departamento de TI subcontratado o uno que no recibe los fondos que necesita.

Tenga en cuenta que todos los departamentos de TI se enfrentarán a desafíos en lo que respecta al departamento de presupuesto, por lo que esto puede ser difícil de manejar para muchas empresas. La escasez de personal a veces puede hacer que tengamos problemas de mantenimiento diferido que le hacen el juego al pirata informático que quisiera desafiar la seguridad web con la que está trabajando.

Si tiene activos que son valiosos, o si hay algo sobre su negocio o sitio que podría ponerlo en el centro de atención del público, entonces es probable que los piratas informáticos trabajen para probar su seguridad web. Esperamos que la información proporcionada aquí evite que usted y su empresa tengan uno de estos piratas informáticos en el sistema y pueda evitar que su empresa se avergüence en el proceso.

Una de las cosas que pueden causar un gran problema de seguridad es el software mal escrito. La cantidad de errores que pueden crear problemas con la seguridad web será directamente proporcional al tamaño y la complejidad del servidor web y las aplicaciones que tiene en su red. Lo que esto significa es que todos los programas complejos que se escriben tendrán errores o algún otro tipo de debilidad en el proceso.

Además de todo esto, los servidores web ya se ven como programas complejos en la forma en que se utilizan. Los sitios web, por sí solos, son complejos y, a menudo, pueden invitar intencionalmente a una mayor interacción con el público simplemente por la forma en que están diseñados. Debido a la forma en que funcionan estas cosas, y cómo el

empresa quiere que se utilice su red, está dejando muchos agujeros de seguridad en el proceso y las oportunidades para un hacker pueden ser muchas.

El problema que técnicamente surge aquí es que la misma programación que funcionará para aumentar el valor de nuestro sitio web, es decir, que queremos que interactúe con los visitantes, también permitirá que se ejecuten comandos SQL y scripts en la base de datos y los servidores web en respuesta a las solicitudes de los visitantes. Cualquier formulario o script basado en la web que esté instalado en el sitio podría tener algunas debilidades o incluso errores, y cada uno de estos, que podrían ser muchos en un sistema complejo, puede representar un gran riesgo para nuestra seguridad web en general.

.

Contrariamente a algunos de los conocimientos comunes sobre el equilibrio entre permitir a los visitantes el sitio web, cierto acceso a sus recursos corporativos y mantener a los visitantes fuera de la red resulta ser una tarea realmente delicada.
No hay una configuración o incluso un solo interruptor que ayude a obtener la seguridad en el nivel correcto automáticamente para manejar todo esto. Hay docenas, e incluso cientos, de estas configuraciones en un servidor web por sí mismas, y luego cada uno de estos servicios, aplicaciones y puertos abiertos también pueden agregar una nueva capa. Y luego podemos agregar el código al sitio web, y en poco tiempo, vemos dónde entrará en juego la complejidad.

Algunas empresas incluso agregarán algunos de los diferentes permisos que desean agregar al sistema para otorgar a empleados, socios, clientes, prospectos, visitantes del sistema, y las variables que vienen con esta seguridad web se disparan.

Como puede ver aquí, hay muchos problemas potenciales en los que podría haber muchos problemas de seguridad web. Y cuantas más capas agregue, más interacción desee y cuantos más permisos intente agregar al sistema, peor puede ser todo esto. Esto agrega la posibilidad de errores y más agujeros de seguridad, y si no tiene un buen departamento de TI al frente, se vuelve más fácil para los piratas informáticos obtener acceso y hacer lo que quieran en el sistema.

Ahora, una de las mejores defensas que puede usar cuando es el momento de protegerse contra los diversos ataques que un pirata informático puede usar contra su sitio web es asegurarse de realizar un escaneo regular al dominio de configuración. Esto debe ocurrir regularmente para asegurarse de que no haya errores, agujeros y vulnerabilidades.

se encuentran, y para garantizar que un pirata informático no haya podido escabullirse y descubrir cómo ingresar a su sitio web.

Probar el sitio web, que también se puede conocer como el proceso de auditoría o escaneo, será un servicio alojado que muchas empresas pueden ofrecer. Hay muchos que no nos proporcionarán ninguna instalación de hardware y software, y las empresas pueden usar esto para verificar la seguridad del proceso y el sitio web, sin interrumpir el uso del sitio web para otros usuarios. .

También puede ser importante tener cuidado con la forma en que administra su página web y todas las diferentes partes que la acompañan. Cuando se asegure de que se realiza un escaneo regular y de que no está divulgando ninguna información que pueda incriminar a su empresa, descubrirá que es mucho más difícil para un pirata informático obtener el acceso que desea a su sistema y hace que las cosas sean mucho más fáciles para usted para mantener su información y la información de sus clientes lo más segura posible.

Dado que gran parte de nuestro mundo sucede en línea y el hecho de que muchas empresas llegan a sus clientes a través de sitios web y otros medios en línea, no sorprende que los piratas informáticos también se estén mudando a este ámbito. Si no brinda a sus clientes la seguridad que desean, y no cubre algunos de los agujeros y otros problemas que pueden estar presentes en su sistema, entonces es probable que los clientes se aprovechen y perjudiquen. en el proceso.

Por ejemplo, tal vez tenga una tienda minorista en línea a través de la cual vende sus productos. Cuando un cliente realiza una compra, debe proporcionarle su nombre, dirección, información de la tarjeta de crédito y, a veces, alguna otra información importante en el camino. Esto se hace para que pueda finalizar la transacción y obtener los resultados que desea de vender el producto, y ellos pueden obtener el producto.

Pero, ¿qué sucede con esa información del cliente cuando se realiza la transacción? Es probable que su empresa la almacene en una base de datos, pero si no existe el tipo de seguridad adecuado, entonces un pirata informático definitivamente querrá recopilar toda esa información y usarla para sus propias necesidades. Si simplemente lo dejas solo y no lo cuidas, y tu negocio

comienza a crecer, un hacker no tardará mucho en encontrar esa información y usarla .

Cuando los clientes descubren que su información ha sido robada, generalmente porque el pirata informático intentó robar su dinero y cometer otros tipos de fraude, ¿qué pasará con su negocio? Habrá muchas reacciones violentas, no va a terminar nada bien para ti y tu reputación se verá afectada en poco tiempo. Como podemos ver aquí, es mucho mejor para usted dar un paso atrás y asegurarse de que la seguridad de su web sea lo más organizada y de la mejor calidad posible, asegurándose de que los piratas informáticos no puedan robar esa información.

A medida que una mayor cantidad de nuestra información esté en línea y nos familiaricemos más con hablar con nuestros clientes y otras personas en línea, la idea de la seguridad web crecerá y se volverá más importante. Cuidar la seguridad web que tiene y garantizar que pueda mantener segura toda la información en su red, ya sea su propia información personal o la información del cliente, evite que los piratas informáticos obtengan lo que quieren.

# Capítulo 9: Comprensión de su cortafuegos

Durante esta guía, hemos dedicado un poco de tiempo a hablar sobre la seguridad y lo importante que es para el proceso general de protección de su sistema y su red. También nos tomamos un poco de tiempo para hablar sobre un firewall y cómo es tan importante para ayudarlo a protegerse contra algunos de los grandes hacks y ataques que podrían atacarlo. Ahora, es hora de que llevemos esto un poco más allá y tratemos de ver un poco más sobre qué es este firewall y cómo podemos usarlo, ya sea en una red grande o en nuestra propia red individual, para realmente asegurarnos de que están protegidos contra todo tipo de piratas informáticos.

Para empezar, un firewall será un enrutador consciente de la seguridad que estará allí, sentado entre Internet y su red con una tarea única en mente. Y esta tarea es evitar que los piratas informáticos y otros ingresen. El firewall actuará como un gran guardia de seguridad entre Internet y su LAN, o red de área local. Todo el tráfico que entra y sale de esta LAN debe pasar a través del cortafuegos que instale, que es una de las mejores formas de ayudarnos a evitar accesos no autorizados a la red que no queremos allí.

Una cosa que debe recordar aquí es que algunos de los tipos de firewalls que existen se consideran imprescindibles si su red tiene una conexión a Internet. Esto importa si la conexión se considera de banda ancha o alguna otra conexión de alta velocidad. Sin este cortafuegos, se expone a muchos riesgos porque, en algún momento, ya sea ahora o más adelante, un hacker lo descubrirá. Verán que su red no está protegida, entrarán y harán lo que quieran, e incluso se lo contarán a sus amigos. Si desea ver que una red se brinde en solo unas pocas horas, continúe y trabaje en línea sin un buen firewall en su lugar.

La buena noticia aquí es que hay dos métodos que podemos usar cuando sea el momento de configurar un firewall. La forma más fácil que podemos usar es comprar un dispositivo de firewall. Básicamente, será un enrutador autónomo que tiene algunas características integradas del firewall. La mayoría de los dispositivos que incluyen esto también tendrán una interfaz basada en web. Esto significa que podemos conectar este firewall en particular desde cualquiera de las computadoras en nuestra red, con la ayuda de un navegador. A continuación, puede revisar todas las configuraciones y personalizarlas según las necesidades que tenga.

Ese es el primer método, pero también hay otro método que puede ser útil cuando desea configurar su propio firewall. Por ejemplo, puede configurar su propia computadora servidor para que funcione como una computadora con firewall. Puede ejecutar el servidor en casi cualquiera de los sistemas operativos de la red, pero tenga en cuenta que uno de los sistemas de firewall más dedicados se ejecutará con el sistema operativo Linux.

Ya sea que elija proteger su red con una computadora con firewall, un dispositivo con firewall o una computadora con firewall, el firewall debe ubicarse en un punto entre la red que está utilizando e Internet si desea que tenga éxito.

**Tipos de cortafuegos a usar** Lo

siguiente que debemos ver aquí son los diferentes tipos de cortafuegos que están disponibles. Hay algunas opciones, pero los tres tipos básicos en los que nos vamos a centrar se conocen como la capa de aplicación, con estado y filtrado de paquetes, o sin estado.

Primero está el filtrado de paquetes o el tipo de cortafuegos sin estado. Estos cortafuegos van a funcionar porque pueden detener e inspeccionar los paquetes individuales de forma aislada. Debido a esto, desconocen el estado de la conexión y tienen la capacidad de denegar o permitir paquetes en función de los encabezados de paquetes que reciben, independientemente del origen de ese paquete.

Luego tenemos los cortafuegos con estado con los que podemos trabajar. Estos son un poco diferentes porque pueden mostrarnos el estado de conexión de nuestros paquetes, lo que agregará un poco más de flexibilidad que lo que podemos ver con los firewalls sin estado. Estos firewalls funcionarán recopilando los paquetes relacionados hasta que puedan determinar el estado de la conexión. Luego, cuando se da cuenta de esto, puede aplicar todas las reglas que tiene el firewall para ese tipo de tráfico.

Y por último, el tercer tipo de cortafuegos con el que podemos trabajar es el cortafuegos de aplicaciones. Estos nos van a llevar un paso más en el camino analizando cualquiera de los datos que estamos viendo transmitidos. Esto nos permite hacer coincidir el tráfico de la red con las reglas del firewall que son específicas para aplicaciones o servicios individuales. Estos también se conocerán como cortafuegos basados en proxy.

Además de parte del software del que acabamos de hablar con los cortafuegos, que está disponible en todos los sistemas operativos que se utilizan en este momento, la funcionalidad del cortafuegos también se puede proporcionar con algunos dispositivos de hardware. Podemos ver esto con los dispositivos de firewall e incluso con algunos enrutadores. Vamos a pasar mucho tiempo aquí hablando sobre los firewalls de software con estado que están disponibles y que se ejecutan en cualquier servidor que pretendan proteger, pero tenga en cuenta que algunos de los otros también son importantes.

**Reglas del cortafuegos**

Como mencionamos un poco más arriba, el tráfico en una red que llega a un firewall se comparará con algunas de las reglas de ese firewall para determinar si ese tráfico se puede dejar pasar o no. Una manera fácil de explicar cómo son estas reglas es mostrar algunos ejemplos, y lo haremos a continuación.

Para esto primero, supongamos que tenemos un servidor con una lista de reglas para el firewall que se aplica a todo el tráfico entrante. Algunos ejemplos de las reglas que podríamos tener presentes incluyen:

1. Puede aceptar tráfico entrante nuevo y establecido a la interfaz de red pública en los puertos 80 y 443. Estos incluirán opciones como tráfico web HTTPS y HTTP.
2. Puede dejar todo el tráfico entrante que proviene de cualquier dirección IP que sea un empleado no técnico a la oficina, y puede hacerlo a través del puerto 22 o el puerto SSH.
3. Puede aceptar cualquiera de los tráficos nuevos y establecidos de la rango de oficina de IP a la red de interfaz privada en el puerto 22 o el puerto SSH.

Tenga en cuenta que las primeras palabras de todas estas reglas tendrán algo como aceptar, rechazar o descartar asociado con ellas. Esto va a especificar la acción que queremos que haga el cortafuegos cuando ocurra un evento. Cuando ocurre algún tipo de tráfico y coincide con una de las reglas, el firewall sabrá lo que debe hacer.

.

Por ejemplo, cuando configuramos una regla para Aceptar, significa que el firewall debe dejar pasar el tráfico. Cuando configuramos una regla para Rechazar, significa que el cortafuegos va a bloquear el tráfico, pero responderá a ese tráfico con un error de inaccesibilidad. Y cuando trabajamos con una regla de eliminación, significa que el firewall debe bloquear el tráfico sin enviar ninguna respuesta. El resto de cada regla será responsable de consistir en la condición con la que se comparará cada paquete.

Resulta que el tráfico de la red se comparará con la lista de reglas que se han configurado con su firewall en una cadena o secuencia, desde la primera hasta la última. Para ser más específicos con esto, una vez que se ha hecho coincidir una regla en este proceso, la acción asociada se aplicará al tráfico de red que está tratando de pasar, y luego el firewall podrá determinar, en función de los diferentes las reglas que configura con él, ya sea para permitir que la información o el tráfico lleguen.

Cuando miramos un ejemplo, si tenemos un empleado de contabilidad que ha intentado establecer una conexión SSH a nuestro servidor, entonces el firewall lo rechazaría debido a la segunda regla que tenemos. Y dado que la segunda regla puede rechazarla, la conexión o el tráfico no se verificarán en absoluto. Pero el administrador del sistema sería aceptado porque solo van a coincidir con la tercera regla. .

Una cosa a tener en cuenta aquí es que la cadena típica de reglas de firewall no puede cubrir todas las condiciones posibles que existen. Hay un montón de cambios diferentes que van a surgir con el tiempo y, a menudo, los resultados que su firewall tiene que sortear también van a cambiar constantemente. Por esta razón, las cadenas en tu firewall deben tener una política por defecto que se especifica desde el principio, la cual va a consistir en una sola acción.

Entonces, supongamos que configuró un firewall y la política predeterminada para la cadena de ejemplo que tenemos arriba se configuró para eliminar el tráfico. Entonces, si hay algún tipo de computadora que intente ingresar a su oficina y establecer una conexión SSH con el servidor, pero esa computadora está fuera de su oficina, entonces el tráfico se interrumpirá. Esa computadora externa no va a coincidir con ninguna de las tres reglas que teníamos arriba, por lo que se eliminará de inmediato.

Ahora, también podemos optar por configurar nuestra política predeterminada para que esté en Aceptar. Esto significa que cualquier persona, excepto sus propios empleados no técnicos, podría acceder a la conexión y establecerse allí en cualquiera de los servicios abiertos que se encuentran en el servidor. Este sería un ejemplo de un firewall que no está bien configurado porque solo mantendrá alejados a algunos de sus empleados, y cualquier otra persona que quisiera estar allí, incluso un pirata informático, podría encontrar fácilmente su propio camino hacia el servidor.

## Vigilancia del tráfico entrante y saliente

Como el tráfico de red, cuando lo miramos desde la perspectiva del servidor, puede ser entrante o saliente, el firewall mantendrá un conjunto de reglas que serán distintas para cada caso. El tráfico que puede originarse en otro lugar, el tráfico entrante, se tratará de manera diferente a lo que vemos con el tráfico saliente que envía su servidor o su propio sistema. Usted no está en peligro de enviar su propia información. Pero podría estar en peligro cuando ingrese algo nuevo al sistema, por lo que el firewall manejará cada uno de estos de manera diferente.

Es bastante común que un servidor permita la mayor parte del tráfico saliente que intenta enviar a otras ubicaciones, principalmente porque tiende a ser confiable. Aún así, queremos asegurarnos de que existen algunas reglas salientes para evitar comunicaciones no deseadas en el caso de que un servidor se vea comprometido por un ejecutable malicioso o un atacante de esa manera también.

Para ayudarnos a aprovechar al máximo nuestros beneficios de seguridad con la ayuda de un firewall, necesitamos identificar todas las formas en que le gustaría que otros sistemas interactúen con usted. Cómo crear reglas que las permitan explícitamente y luego descartar todo el resto del tráfico. Debemos tener en cuenta con esto que algunas de las reglas salientes apropiadas deben estar en su lugar para asegurarse de que el servidor pueda permitirse enviar reconocimientos salientes a las conexiones entrantes según lo elija.

Otra cosa para recordar aquí es que, dado que el servidor normalmente tendrá que ser el que inicie su propio tráfico saliente por muchas razones diferentes, incluida la descarga de actualizaciones o la conexión a la base de datos,

es importante que también podamos incluir esos casos en el conjunto de reglas salientes.

Desde aquí, podemos escribir algunas de nuestras propias reglas salientes. Digamos que vamos a configurar un firewall que eliminará el tráfico saliente, y este es nuestro valor predeterminado. Esto significa que las reglas de aceptación entrantes serían inútiles sin tener las reglas salientes correctas en su lugar. Para ayudar a complementar las reglas de firewall entrantes (que eran 1 y 3 desde arriba), de la sección Reglas de firewall anterior, y para asegurarse de que haya una cantidad adecuada y adecuada de comunicación en esas direcciones y que los puertos funcionen correctamente, algunos de las reglas salientes que podemos querer configurar para el firewall podrían incluir lo siguiente:

1. Acepte el tráfico saliente establecido que llega a la interfaz de red pública utilizando los puertos 90 y 443.
2. Aceptar el tráfico saliente establecido a la red privada en puerto 22

Tenga en cuenta, con este, que no estamos obligados y no es necesario que escribamos una regla para el tráfico entrante que debe eliminarse (esta fue la regla 2 en la sección anterior) porque el servidor no va a necesidad de establecer o incluso reconocer este tipo de conexión.

Tener un buen firewall en su lugar será muy importante cuando se trata de mantener su red y su sistema lo más seguros posible. Puede establecer las reglas sobre lo que está permitido en el sistema y lo que debe mantenerse fuera del sistema desde el principio. Sin la protección de firewall adecuada, es posible que cualquier persona, y cualquier pirata informático, pueda ingresar a su sistema y causar el caos y los estragos que les gustaría. Elija un buen firewall y asegúrese de que puede configurar las reglas que funcionan mejor para su sistema y la seguridad que le gustaría tener en general.

# Capítulo 10: Comprender la criptografía

El capítulo final del que vamos a hablar cuando trabajemos en esta guía es la idea de la criptografía. Si queremos asegurarnos de que los mensajes que enviamos y los que recibimos se mantengan seguros y protegidos de los demás, debemos asegurarnos de que podemos agregar algún nivel de criptografía a la mezcla tanto como sea posible. La criptografía va a ser el método de protección de la información y las comunicaciones mediante el uso de códigos. El objetivo de hacer esto es que solo aquellos que están destinados a ver el mensaje son los que pueden leerlo al final.

El punto de esto es que queremos asegurarnos de que la información se mantenga en secreto. Ya sea que se trate solo de un correo electrónico que desea enviar a otra persona o de información segura que desea ocultar a los demás, esta criptografía puede garantizar que los piratas informáticos y otras personas que puedan estar realizando ataques de intermediarios y más se mantienen fuera de su sistema y no causarán algunos problemas en el camino.

Cuando lo miramos a través de la lente de la informática, esta criptografía se referirá a técnicas seguras de información y comunicación que se derivarán de una variedad de conceptos matemáticos y un conjunto de cálculos basados en reglas.

**Técnicas de criptografía** Necesitamos

comenzar con algunas de las diferentes técnicas que podemos usar cuando se trata de agregar algo de criptografía a nuestro sistema y los mensajes que tratamos de enviar. La criptografía va a estar bastante relacionada con las ideas de criptoanálisis y criptología. Incluirá técnicas como micropuntos, combinación de palabras con imágenes y otros métodos destinados a ayudarnos a ocultar nuestra información almacenada o en tránsito, para que nadie más sin la autorización adecuada pueda obtener ese mensaje. .

Sin embargo, cuando observamos el mundo y cómo es hoy, y todas las computadoras y cosas digitales que están sucediendo en este momento, es más probable que la criptografía se asocie con la codificación de texto sin formato (que será texto ordinario) en texto cifrado en un proceso que se conoce como cifrado.

Luego, cuando los mensajes lleguen a la persona adecuada, volverán al texto normal o sin formato nuevamente en un proceso conocido como descifrado. Las personas que pueden practicar este campo se conocen como criptógrafos.

Ahora, habrá cuatro objetivos o preocupaciones principales que vienen con el proceso de criptografía, y estos incluirán lo siguiente:

1. Confidencialidad: Aquí es donde tratamos de asegurarnos de que la la información no es entendida por nadie para quien no está destinada. Cuando trabajamos con criptografía, confiamos en códigos y otros procesos para mantener seguros nuestros mensajes y nuestra información hasta que llegue a la persona deseada.
2. Integridad: La criptografía se preocupa de si la información se altera durante el almacenamiento o el tránsito. El objetivo aquí es no permitir que la información se altere en ninguno de estos dos procesos entre el remitente y la persona que se supone que debe recibir el mensaje, y si esta alteración ocurre, se detecta de inmediato.
3. No repudio: Aquí es donde el creador o el remitente de la información no puede negar, en una etapa posterior, cuáles son sus intenciones en la creación de la transmisión de la información cuando todo está hecho.
4. Autenticación: Aquí es donde el remitente y el receptor están capaz de confirmar la identidad de uno al otro, y el origen o el destino del mensaje o la información.

Cuando tenemos un protocolo o un procedimiento que es capaz de cumplir con al menos algunos, pero con suerte todos, los criterios anteriores, entonces tenemos algo que se conoce como criptosistema. A menudo se piensa que estos se refieren solo a procedimientos matemáticos y algunos de los programas que podemos hacer en nuestra computadora. Sin embargo, también van a incluir alguna regulación del comportamiento humano, como elegir contraseñas que sean difíciles de adivinar, desconectarse cuando el sistema no esté en uso y no discutir ningún procedimiento que pueda ser sensible para el negocio con alguien que no lo sepa. No es necesario saber la información.

## Algoritmos con Criptografía

Como estamos trabajando con criptografía, es importante que nos tomemos un momento para hablar sobre algunos de los algoritmos que vienen con este tipo de proceso. Los criptosistemas van a utilizar un conjunto de procedimientos, que son los algoritmos, para ayudarnos a cifrar y descifrar los mensajes que se envían entre unos pocos sistemas. El punto aquí es asegurarse de que la comunicación que se comparte entre los sistemas informáticos sea lo más segura posible. Esto funciona no solo en sistemas informáticos, sino también en aplicaciones y otros dispositivos como tabletas y teléfonos inteligentes.

Un conjunto de cifrado, o el algoritmo, utilizará un algoritmo para ayudarnos con la parte de cifrado del proceso, otro para ayudar a enviar mensajes de autenticación y luego la clave final para finalizar el intercambio que está ocurriendo. Este proceso, que se integrará en los protocolos y luego se escribirá en el software que se ejecuta en los sistemas operativos y los sistemas informáticos en red, necesita generar dos claves para tener éxito.

Con esto, tenemos que asegurarnos de que haya una clave privada y una clave pública que se genere para hacer todo el trabajo que le gustaría en este proceso. Algunas de las formas en que podemos usar estas dos claves para incluir el descifrado y el cifrado de datos, la firma digital y la verificación para la autenticación del mensaje pueden ser importantes, al igual que el intercambio de la clave.

**Tipos de criptografía** Mientras

estamos aquí, debemos dedicar un tiempo a analizar los diferentes tipos de criptografía que están disponibles. Para empezar, los algoritmos de cifrado de clave única o clave simétrica crearán para nosotros una longitud fija de bits conocida como cifrado de bloque. Este va a contener una clave especial que el creador o el remitente usarán para ayudarlos a cifrar o encriptar los datos. Luego, el receptor obtendrá esta clave y puede usarla para ayudarlo a descifrar la información que tiene.

Hay muchos tipos diferentes de criptografía de clave simétrica, y uno de ellos incluirá el AES o Estándar de cifrado avanzado. AES porque una especificación establecida en 2001 por el Instituto Nacional de Estándares y Tecnología como el Estándar Federal de Procesamiento de la Información, y se utilizó para ayudar a proteger cualquier información que se consideraba

sensible. El estándar es obligatorio para su uso con el gobierno de los EE. UU., y muchas personas en el sector privado también lo usarán para ayudarlos a hacer las cosas y mantenerse seguros.

Además, unos años después, en 2003, se aprobó el AES para ser utilizado en la información que fuera clasificada por el gobierno de los Estados Unidos. Ahora mismo, es una especificación que está libre de regalías y está implementada en software y hardware en todo el mundo. Este es en realidad el sucesor del DES o el Estándar de cifrado de datos que funcionaría con longitudes de clave más largas y podría evitar cosas como ataques de fuerza bruta.

Luego, también hay opciones para algoritmos de cifrado asimétrico o de clave pública. Estos son un poco diferentes porque van a usar un par de llaves en lugar de solo una. Va a haber una clave que es la pública, y esta está asociada con el remitente o el creador para cifrar los mensajes. Luego también está la clave privada, la que solo el creador va a conocer (a menos que un pirata informático pueda ingresar y exponer esta clave o el creador decida compartir la información), para ayudarlos a descifrar su información.

Hay una serie de opciones de criptografía de clave pública que incluyen RSA, que se usa a menudo en Internet para mantener las cosas seguras, Elliptic Curve Digital Signature Algorithm que se usa con Bitcoin y otras criptomonedas, Digital Signature Algorithm que se usó como estándar para digital firmas y el intercambio de claves Diffie-Hellman.

Para ayudar a garantizar que la integridad de los datos se mantenga en la criptografía, las funciones, que pueden devolvernos una salida determinista del valor de entrada, se utilizarán para ayudarnos a asignar todos los datos a un tamaño de datos fijo. . Esto asegurará que su información pueda permanecer lo más segura posible, y le facilitará el envío y la recepción de mensajes, sin que un hacker pueda meterse en el medio y causar un lío.

## ¿Cómo comenzó la criptografía?

Lo siguiente que debemos ver aquí es la historia de la criptografía y cómo comenzó. La palabra "criptografía" en realidad proviene de una palabra griega conocida como kryptos, que significa oculto. El origen de este se data alrededor del año 2000 aC con la práctica egipcia de los jeroglíficos.

Estos eran consistentes con pictogramas complejos, cuyo significado completo solo era conocido por unas pocas personas.

En tiempos más recientes, la criptografía se ha convertido en una especie de campo de batalla de algunos de los mejores matemáticos e informáticos del mundo que trabajan para crear el mejor código. La capacidad de almacenar y transferir, de manera segura, cualquier información confidencial que se necesite ha sido un factor crítico en los negocios y, a veces, también en la guerra.·

Debido a que los gobiernos no desean que ciertas entidades dentro y fuera de sus países tengan acceso a los diferentes métodos de recepción y envío de información que podría ser secreta y podría representar una amenaza para los intereses nacionales, no es de extrañar que la criptografía haya sido un gran tema. a las restricciones en diferentes países. Esto puede incluir algunas limitaciones de exportación y uso del software al público y más.

Por supuesto, la forma en que se usa la criptografía es diferente ahora que en el pasado. Muchas veces, vamos a ver este tipo de criptografía en cualquier transacción en la que la información deba mantenerse segura. Si bien se usa bastante en el gobierno, puede aparecer en los bancos que usamos y en muchas de las transacciones que ocurren en línea cuando hacemos compras. El punto es permitirnos enviar información personal y confidencial a otra persona o empresa, sin el riesgo de que alguien se haga cargo y use los datos para sus propias necesidades.

**Problemas con** la criptografía En

ocasiones, los atacantes pueden eludir parte de la criptografía.
Y cuando pueden hacer esto, les permite piratear computadoras que son responsables de realizar el cifrado y el descifrado de los datos para empezar. El pirata informático, una vez que está allí, puede explotar algunas de las implementaciones más débiles que existen, como usar las claves predeterminadas para ayudarlo. ·

Sin embargo, es cierto que esta criptografía dificultará que un atacante acceda a los mensajes y cualquier dato que esté protegido por los algoritmos de cifrado.
Es por eso que es tan importante agregar esto a su sistema. Es posible que no pueda ocultar todo todo el tiempo, especialmente con un hacker realmente hábil. Pero puede hacer las cosas más difíciles y puede resolver muchos problemas en el proceso.

Las crecientes preocupaciones surgen con el poder de procesamiento de la computación cuántica para romper algunos de los estándares actuales de cifrado para criptografía liderados por el Instituto Nacional de Estándares y Tecnología. Esto tiene como objetivo realizar una convocatoria de artículos sobre la comunidad científica y matemática para nuevos estándares en criptografía. Si algunos estándares se decidieran antes de tiempo, haría la vida más fácil para la mayoría de las empresas y aseguraría que sepan lo mínimo que pueden esperar al usar uno de estos servicios.

A diferencia de los sistemas informáticos actuales, la computación cuántica utilizará lo que se conoce como bits cuánticos que pueden representar tanto los 1 como los 0. Debido a esto, es capaz de completar dos cálculos en uno.
Si bien una versión a gran escala de este tipo de computadora no es algo que probablemente se haga en la próxima década, la infraestructura requiere la estandarización de algoritmos conocidos y entendidos públicamente que puedan ofrecernos un enfoque seguro.

Si desea asegurarse de que sus mensajes y su información estén lo más seguros posible, es importante que nos aseguremos de que se implemente alguna forma de criptografía desde el principio. El sistema Kali Linux podrá ayudarnos con esto y garantizará que realmente podamos ver qué tan seguros pueden ser nuestros propios mensajes, incluso cuando tenemos que enviar cosas fuera de la red en primer lugar.

Sin esta criptografía en su lugar, es posible que un hacker ingrese a su sistema y robe los mensajes que están allí. Con el tipo adecuado de criptografía y la ayuda del sistema Linux, es más fácil para las personas y las empresas ocultar su información y enviar mensajes seguros de un lado a otro con menos posibilidades de que alguien pueda interceptar la información y leer lo que hay allí.

# Conclusión

Hackear es un término con el que muchas personas no están tan familiarizadas. Es posible que hayan escuchado sobre la piratería cuando le sucedió a una gran corporación, y tal vez tengan un antivirus en su computadora para mantener alejados a aquellos que pueden intentar dañar sus sistemas, pero no están seguros de todos los diferentes tipos de piratería. disponible, o incluso que existen diferentes tipos de piratas informáticos. Esta guía intentó repasar todos los diferentes aspectos que necesitábamos saber sobre la piratería para que podamos mantener nuestras propias redes y sistemas a salvo de aquellos con intenciones maliciosas.

Esta guía dedicó mucho tiempo a hablar sobre los diferentes tipos de piratería, cómo prepararse para un ataque y algunos consejos sobre cómo mantener su computadora y sus redes seguras. Echamos un vistazo a esto desde un punto de vista más ético, pero nos damos cuenta de que las técnicas y habilidades que usará un hacker ético son similares a las que usaría un hacker malintencionado. Esta es una buena noticia para el hacker ético porque le permite revisar el sistema, encontrar algunas de las mayores vulnerabilidades y asegurarse de que nadie intente piratear el sistema.

No importa qué tipo de sistema esté tratando de proteger, ya sea una base de datos de bits para una corporación o su propia computadora personal, siempre es bueno tener una buena idea de cómo protegerse de los piratas informáticos y todos los problemas que pueden causar. . Puede ahorrar mucho tiempo, dinero y molestias y puede mantenerlo a usted, junto con muchos otros a salvo. Cuando esté listo para obtener más información sobre cómo el sistema operativo Kali puede ayudarnos con todas nuestras necesidades de piratería, asegúrese de consultar esta guía para comenzar.

# Descripción

¿Está interesado en aprender más sobre la piratería y cómo puede usar estas técnicas para mantenerse a usted y a su red lo más seguros posible?
¿Le gustaría trabajar con Kali Linux para proteger la red y asegurarse de que los piratas informáticos no puedan ingresar a su computadora y causar problemas o robar su información personal? ¿Alguna vez te ha interesado aprender más sobre el proceso de piratería, cómo evitar que se aprovechen de ti y cómo puedes usar algunas de las técnicas para tus propias necesidades?

Esta guía nos brindará toda la información que necesitamos saber sobre la piratería con Linux. A muchas personas les preocupa que la piratería sea un mal proceso y que no sea la opción adecuada para ellos. La buena noticia aquí es que la piratería puede funcionar bien no solo para tomar información y dañar a otros, sino también para ayudarlo a mantener su propia red e información personal lo más segura posible.

Dentro de esta guía, vamos a tomarnos un tiempo para explorar el mundo de la piratería y por qué el sistema Kali Linux es uno de los mejores para ayudarlo a hacerlo. Exploramos los diferentes tipos de hacking y por qué es beneficioso aprender algunas de las técnicas que se necesitan para realizar tus propios hacks y ver los resultados que queremos con nuestras propias redes.

En esta guía, veremos muchos de los diferentes temas y técnicas que necesitamos saber cuando se trata de trabajar con piratería en el sistema Linux. Algunos de los temas que vamos a ver aquí incluyen:

1. Los diferentes tipos de hackers que podemos encontrar y en qué se parecen y en qué se diferencian.
2. Cómo instalar Kali Linux en su sistema operativo para obtener empezado.
3. Los conceptos básicos de seguridad cibernética, seguridad web y ataques cibernéticos y cómo estos pueden afectar su sistema informático y cómo un hacker intentará utilizarlo.
4. Los diferentes tipos de malware que los piratas informáticos pueden usar en su contra.
5. Cómo un hombre en el medio, DoS, troyanos, virus y phishing pueden ser herramientas del hacker.

6. Y mucho más.

La piratería a menudo es una opción que la mayoría de las personas no considerará porque les preocupa que sea malo o que solo se use para dañar a otros. Pero como discutiremos en esta guía, hay mucho más en el proceso que esto. Cuando esté listo para aprender más sobre la piratería con Kali Linux y cómo esto puede beneficiar su propia red y computadora, ¡asegúrese de consultar esta guía para comenzar!