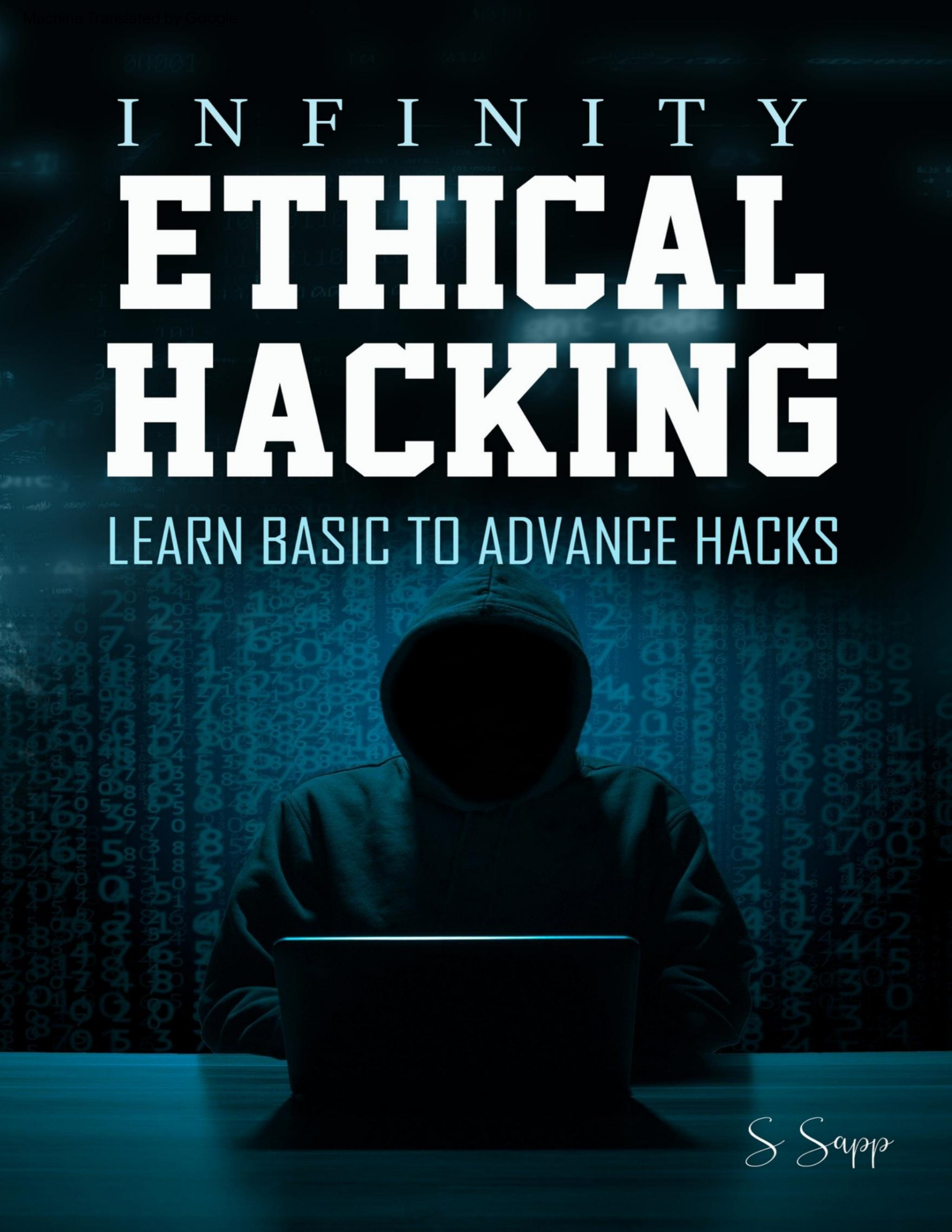
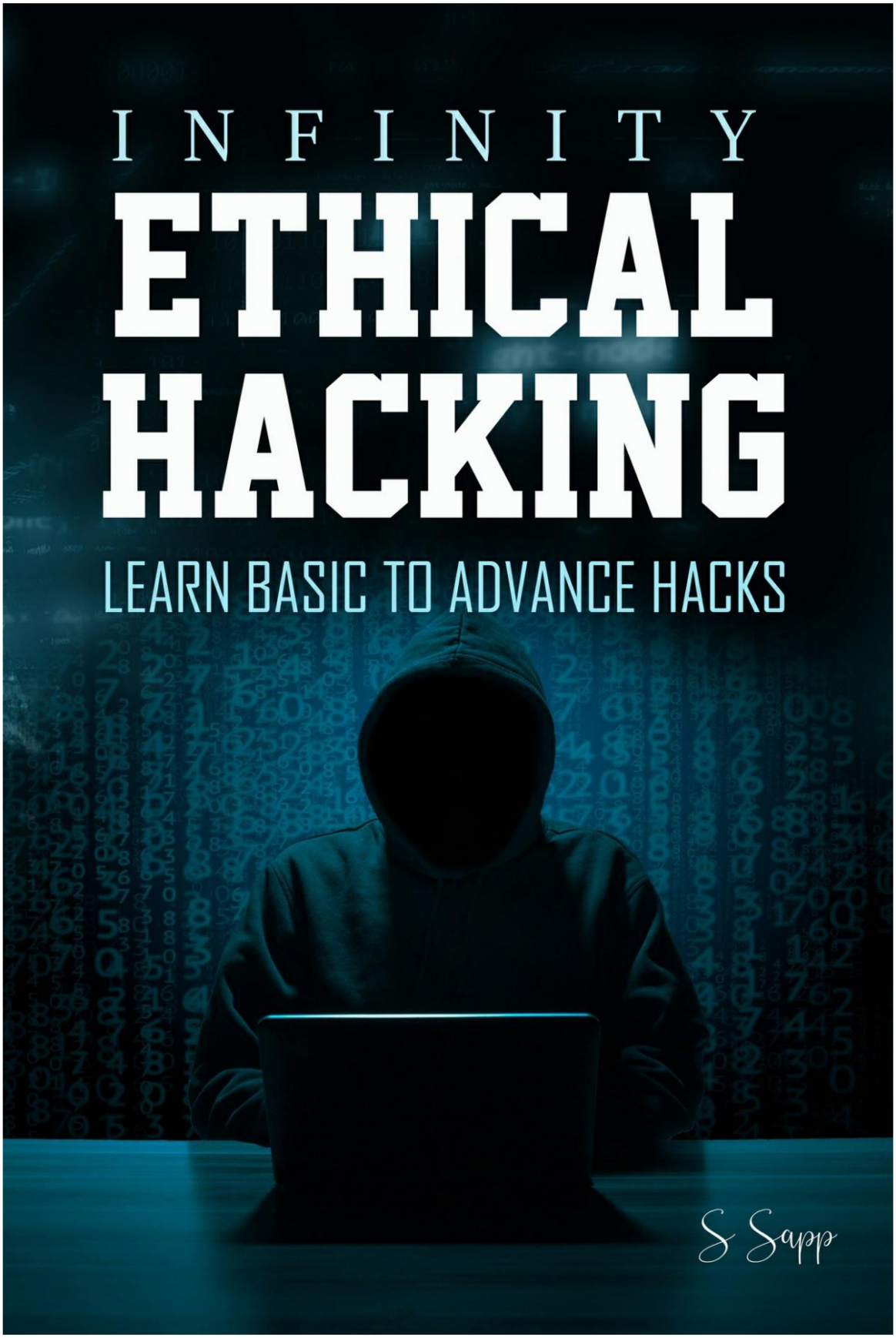
INFINITY ETHICAL HACKING

LEARN BASIC TO ADVANCE HACKS



S Sapp



Hacking Ético Infinito

Aprende trucos básicos para avanzar

arturo s sapp

https://t.me/librosdehacking

Tabla de contenido

Introducción

Pensemos en algo más de 10 años atrás. Toda el área de la seguridad informática era básicamente desconocida. En la década de 1990, apenas había profesionales que pudieran decir que estaban trabajando en ciberseguridad, y menos aún sabían cuál iba a ser el área.

La seguridad era esencialmente solo un software antivirus. Ya sabes, esa molesta ventana emergente que te grita cada vez que intentas obtener un archivo de Internet. Claro, los enrutadores de filtrado de paquetes y tecnologías similares también eran populares, pero en realidad no se consideraban importantes.

En ese momento, el concepto de hacker se parecía más a los memes de hackers que tenemos hoy. Era principalmente de películas que hizo Hollywood o simplemente una actividad que — obtuve una referencia cruzada

mientras jugaba al golf.

Fue ignorado. Nadie realmente vio la piratería como una amenaza. Después de todo, ¿qué se podía ganar en ese momento? Fue visto principalmente como una trivialidad molesta que aparece de vez en cuando. Hoy entendemos que es una gran amenaza que puede afectar a grandes empresas multimillonarias e incluso a nuestros gobiernos.

Fue ignorado y en ese momento estaba claro por qué. Desafortunadamente, más tarde, toda la industria de TI sentiría el impacto que los piratas informáticos podrían dejar atrás. Hoy, el número de profesionales de seguridad de sistemas de TI en todo el mundo es más de 61 mil. Esto no es sin razón. De hecho, el campo de la seguridad cibernética no solo está creciendo, sino que crece más rápido que la industria tecnológica que ya está creciendo, según el ISC. Ahora hay más compañías de seguridad que nadie para recordar y confiar en mí, la mayoría de ellas hacen un trabajo mucho más importante que solo un antivirus.

La seguridad cibernética incluso se ha generalizado, con innumerables personas que autorizan cosas a través de sus firewalls y usan VPN todos los días para ver videos que no están disponibles en su ubicación.

Hay tantas maneras de abordar los problemas de seguridad que pensar en ello puede ser un verdadero dolor de cabeza. Bueno, incluso considerar las alternativas de un solo programa es suficiente para provocarte migrañas debido a la gran cantidad de competencia que existe.

El mundo ha cambiado enormemente desde la década de 1990. Es decir, recuerda el último día que pasaste sin usar un dispositivo electrónico. Lo más probable es que ni siquiera lo recuerdes. Entonces, ¿qué trae todo este cambio a tu hogar? ¿Para tu computadora? ¿Significa esto que cada vez que enciende su computadora, teléfono u otro dispositivo inteligente, lo empujan a un mundo peligroso?

Bueno, eso es más o menos lo que significa, porque cada uno de esos cambios condujo a que el mundo y los criminales cambiaran en él para conocer el nuevo entorno también. En el mundo digital, encontrará un patio de recreo lleno de minas que solo necesitan un toque para detonar, si es que lo necesitan. Incluso las cosas más simples pueden causarte bastantes problemas.

Si alguna vez se conecta a Internet sin un firewall decente, es probable que su sistema sea pirateado en minutos.
Cada vez que abre un correo electrónico modesto de amigos o familiares, siempre existe la posibilidad de que el correo electrónico abra una puerta trasera a su sistema. Esto significa que un pirata informático necesita muy poco tiempo para acceder incluso a las partes más privadas de su computadora.
Si utiliza su programa de mensajería de Internet para descargar y ejecutar un archivo, no se sorprenda si su escritorio se convierte en una zona activa de virus.
Incluso cuando navega por sitios web confiables, está completamente abierto a los ataques de piratas informáticos. Cuando esto sucede, sus archivos confidenciales corren el riesgo de ser tomados o eliminados. Desafortunadamente, el miedo a ser el objetivo de un drive-by en línea a menudo es más que un miedo y puede ser atacado completamente de la nada. No es poco común.

La mayoría de las veces, a las personas les gusta difundir los peligros del terrorismo cibernético. Sin embargo, el miedo, la incertidumbre y la duda que generalmente sienten las personas cuando se trata de este tema es todo menos injustificado. La gente suele estar ciega ante la probabilidad de una catástrofe digital. El crimen organizado y el terrorismo tienen su dedo en todas partes, incluso en el mundo digital. A menudo se allanan múltiples células terroristas organizadas. Cuando se encuentran sus computadoras, la mayor parte de lo que contienen son planes de piratería cibernética y archivos similares que muestran cómo atacarían la infraestructura de los Estados Unidos.

Quizás recuerde el 14 de agosto de 2003. Este fue el día en que ocurrió el mayor corte de energía en la historia de los Estados Unidos. Alrededor del 20 por ciento de la población estadounidense estuvo sin electricidad durante más de 12 horas. Es muy fácil hacerse creer la historia más despreocupada y decir que se han caído algunos árboles o que los fuertes vientos han dañado parte de la red. Si bien esta explicación puede ser correcta, considere esto: 3 días antes del corte de energía, el gusano Microsoft Blaster fue lanzado en Internet. Este gusano es conocido como uno de los gusanos más peligrosos y volátiles jamás creados. Si bien esto puede haber sido una coincidencia, uno solo puede ser escéptico.

Podrías pensar que todo el miedo y la severidad que provoca el ciberterrorismo no está justificado. Podrías pensar que, dado que nada ha sucedido hasta ahora, nada

pasará. Pero piense en esto: nadie esperaba que ocurriera el 11-S. Todos sabían que existía un riesgo de seguridad en lo que respecta a la seguridad del aeropuerto y el terrorismo, pero no se hizo nada al respecto.

El escepticismo es comprensible y bienvenido, ya que el escepticismo nunca es malo. Pero tiene que confiar en mí cuando digo que el terrorismo cibernético es algo muy peligroso pero probable. Tienes que confiar en los medios cuando entran en pánico por ataques cibernéticos menores porque así es como comienza todo.

Tienes que tener cuidado con esto. Un hacker es como un ladrón. Intentan vigilar su seguridad hasta que puedan señalar un lugar donde puedan ingresar a su espacio seguro y tomar sus objetos de valor. Cada segundo del día, hay grupos de piratas informáticos y delincuentes organizados que buscan su seguridad. Nunca debes dejar que tengan éxito. Nadie debería sentarse y mirar a otra persona querida y profanar su espacio seguro. Ayúdese a sí mismo aprendiendo más sobre esto y use los recursos disponibles para protegerse tanto como sea posible.

Si bien aumentar su seguridad parece algo fuera de serie, puedo asegurarle que puede hacerlo con bastante facilidad. Se trata más de lo que piensas que de nada. Puedes compararlo con el deporte o el estudio. Mientras seas inflexible y tengas un horario en el que hagas ciertas cosas, rápidamente se convertirá en parte de tu vida. Si no lo integras en tu horario diario, rápidamente comenzarás a olvidarlo y encontrarás excusas para no hacerlo.

La seguridad es un proceso y no una meta. Por eso es importante que lo hagas parte de tu rutina y pronto podrás hacerlo sin pensarlo.

Sin embargo, si evitas esto, serás golpeado tarde o temprano. Lo mejor que puede hacer por usted mismo en este momento es educarse y adquirir algunos conocimientos sobre el tema. No puedes protegerte de algo que no entiendes y debes protegerte de ello. No es tu derecho protegerte a ti mismo, sino tu deber. Conocer algo que puede ser peligroso para ti es lo mejor que puedes hacer para protegerte. Si llena los vacíos en su conocimiento, puede prepararse para la mayoría de las cosas.

Lo que es bien conocido y claro es que siempre debe mantenerse al día para protegerse de los usuarios maliciosos en todas partes. Aquí es donde entra en juego el conocimiento de este libro y salva el día. Le ofrece una forma de implementar la tecnología actualmente disponible para nosotros y el conocimiento acumulado a lo largo de los años para mantener sus sistemas seguros por un tiempo. Mantener su sistema seguro es imposible a menos que entre en la mente del usuario malicioso y use el conocimiento que obtiene. Vea qué herramientas usan y usen las mismas

herramientas para ver las debilidades en su sistema que podrían ver si estuvieran dirigidas a usted. A menos que haga esto, cualquier otra evaluación de qué tan seguro es su sistema puede ser muy imprecisa.
La piratería ética implica muchas actividades legales y seguras diferentes. Los sistemas en todo el mundo deben mejorarse y hacerse más seguros. Las actividades incluyen, entre otras, hacking blanco, pruebas de vulnerabilidad y pruebas de penetración. Si bien los beneficios de este tipo de actividad son relativamente difíciles de ver, si lo miras un poco más, se vuelve más claro que el día. La única forma de mejorar y mantenerse al día con los tiempos cambiantes es mejorar uno mismo. Esto se hace probando su sistema y mejorando los resultados que obtiene de las pruebas.

El libro cubre principalmente lo que significa ser un pirata informático ético y cómo hacerlo correctamente para encontrar contramedidas efectivas y cerrar cualquier puerta trasera que su sistema pueda tener para mantener alejados a los piratas informáticos maliciosos.

¿A quién está destinado este libro?

En primer lugar, es importante enfatizar que si elige usar el conocimiento de este libro solo para actividades maliciosas, usted tiene la culpa. Nadie más asociado con usted para adquirir el conocimiento no tiene la culpa, ni es responsable por la forma en que usa el conocimiento. El contenido de este libro puede ser utilizado tanto por hackers de sombrero blanco (hackers éticos) como por hackers de sombrero negro (crackers). El libro analiza tan de cerca la mentalidad de los crackers que se convierte en una buena fuente de estudio para los mismos crackers. Los métodos en el libro se pueden utilizar de dos maneras. La responsabilidad del uso correcto del conocimiento recae enteramente en usted. Siempre debe usarlo en formas autorizadas.

Para ser un hacker ético, concentre sus esfuerzos en detectar vulnerabilidades que pueden haberse pasado por alto y encontrar formas de llenar esos agujeros. Independientemente de la prueba que ejecute en su sistema, lo ayudará a administrar y mejorar su sistema, así como cualquier otro sistema para el que pueda hacer esto. La seguridad informática no es nada de lo que burlarse. Es un tema que siempre debe tomarse en serio.
Lo mismo se puede decir si haces esto por otro. Su objetivo es proteger su sistema de usuarios malintencionados y cerrar las brechas que parezcan más problemáticas.
Si lee este libro detenidamente y obtiene todo el conocimiento, siempre estará en su mejor momento cuando se trata de seguridad informática. Se sentirá autosuficiente en ese sentido y también disfrutará del honor de ser una persona útil para cualquier persona preocupada por la seguridad de las computadoras. No importa de qué sistema estemos hablando y qué tan lejos esté ese sistema, siempre habrá cientos, si no miles, de formas de descifrarlo.

Este libro le ayuda a entender lo siguiente:

• Los resultados de varios estudios de casos importantes e impactantes realizados por diferentes expertos en el campo • Varios ataques de piratería ampliamente utilizados en la comunidad okupa y todos los matices subyacentes • Las contramedidas que puede tomar para protegerse Para estar preparado para las tareas que se avecinan y para hackear sus sistemas adecuadamente, necesita aprender la información en la Parte 1 del libro. Hay un viejo dicho que dice: "Si no planeas, planeas fracasar". Esto es especialmente cierto para la piratería, especialmente cuando se trata de la parte ética de la misma. Hay varios pasos que debe seguir antes de poder empezar a trabajar. Primero debe obtener el permiso del propietario del sistema y desarrollar un plan de juego general sobre cómo lo manejará. Algunos pueden ver la información de este libro y decir que fue creado para convertir a los niños guionistas, personas que usan herramientas automatizadas para descifrar sistemas con poco o ningún conocimiento técnico, en piratas informáticos reales. Sin embargo, esto es incorrecto. El conocimiento presentado en este libro se le proporciona con fines éticos. Debe usarlo para piratear sus propios sistemas o los sistemas que tiene permitido piratear para que el sistema sea más seguro y la información del sistema más segura.

Hay algunos capítulos que puede omitir en este libro. Por ejemplo, si no está utilizando un sistema operativo Windows, no tiene sentido leer los capítulos que describen cómo usarlos.
El libro entra en la explicación, asumiendo algunas cosas: • Tiene una comprensión promedio de los conceptos y términos relacionados con la seguridad de la información, la computadora y la red • Puede distinguir a los piratas informáticos éticos de los crackers • Tiene una computadora y una red a la que puede aplique estas técnicas • Puede acceder a Internet y obtener las herramientas que puede necesitar para algunas tareas • El propietario del sistema le ha dado permiso para utilizar los métodos y técnicas contenidos en el libro.

El libro está dividido en siete partes. Debes conocer bien el formato, ya que es posible que tengas que saltar de una parte a otra. Cada uno de estos capítulos le brinda diferentes métodos y técnicas que lo ayudarán a mejorar sus habilidades de piratería ética.

La diferencia entre hacking ético y cracking Ha habido mucha controversia sobre el término 'hacker' durante mucho tiempo.

La población en general asume automáticamente que un pirata informático es alguien que hace el trabajo de manera poco ética e intenta piratear sistemas para su propio beneficio. Sin embargo, esto no siempre fue así.

Antes de que la piratería se convirtiera en una actividad delictiva generalizada, la palabra 'hacker' tenía un significado muy positivo. Fue utilizado para lo mejor de lo mejor cuando se trata de programación. El testamento de Linus Torvalds fue declarado hacker. Esta imagen de la palabra cambió muy rápidamente cuando comenzaron los brotes de ciberdelincuencia. Los medios se encargaron de esclarecer los hechos mientras oscurecían los nombres de los mejores programadores de la época. La comunidad de programación se indignó por esto y surgieron muchos debates acalorados sobre este tema. Muchos nombres influyentes de ambas comunidades se acercaron para dar su opinión. Pero desafortunadamente todo fue en vano. La historia impulsada por los medios ya era ampliamente aceptada por el público y era demasiado tarde para cambiarla. La palabra 'piratería' fue etiquetada como negativa. Esto no fue ayudado por la comunidad de cracking que hizo cumplir la historia de que la piratería es estrictamente una actividad maliciosa. A la gente de la comunidad okupa le gusta llevar el título de "hacker" con gran orgullo. Esto es visto como un insulto por la comunidad de programación, ya que un hacker debería ser un título otorgado solo a aquellos que han demostrado una gran experiencia en programación.

Deben trazarse varios paralelos en la discusión. Aunque la subcultura cracker es parte de la comunidad de programación, la comunidad de programación se esfuerza por suprimir y exponer todos los esfuerzos de la subcultura cracker. De ahí viene el término "galleta". La comunidad de programación ve a los crackers como los individuos más peligrosos y horribles.

Para evitar que tantas personas como sea posible utilicen el término 'hacker' para estas personas, se han encargado de encontrar un nuevo término para reemplazarlo en la historia. Aquí es donde entra en juego el término "galleta". Después de que el término fue acuñado y ampliamente aceptado por los programadores, inmediatamente se introdujo en los medios. Se han hecho grandes esfuerzos para aclarar la diferencia.

Si bien inicialmente parecía que iba a alguna parte y había algo en el horizonte, finalmente cayó al agua. Los medios de comunicación insistieron en impulsar su historia y, además, la gente de la comunidad okupa se autodenominó piratas informáticos.

Los programadores generalmente usan esta diferenciación y llaman crackers a los hackers maliciosos. Algunas personas fuera de la comunidad también se adhieren a él, pero la mayoría del público ya estaba tan afectado que el daño es irreversible.

Sin embargo, es importante distinguir. Es imperativo que nunca lo olvidemos porque hay grandes nombres como el mencionado Linus Torvalds cuyo

Los nombres siempre se han asociado con el término "hacker".
Lo que debe tener en cuenta es que la piratería es como cualquier otro comercio.
Siempre hay un paralelismo entre dibujado y cerrajería. ¿Por qué? Porque los principios fundamentales de los dos son bastante similares. Los piratas intentan encontrar debilidades en el sistema, pero esto es legal si se hace con buenas intenciones y con el permiso del propietario del sistema. La selección de cerraduras se considera altamente ilegal y es un delito en sí mismo, pero un cerrajero debe hacerlo de vez en cuando para satisfacer las necesidades de sus clientes. Imagine estar atrapado fuera de su propia casa y dejar las llaves adentro. Realmente no quieres romper la puerta o dañar las ventanas, así que llama a un cerrajero para que te ayude a entrar en tu propia casa, sin importar lo divertido que suene. La piratería funciona con un principio similar. Si bien el acto en sí puede ser ilegal, siempre querrá la ayuda de un pirata informático experimentado cuando trabaje para mejorar la seguridad de su sistema.
El hecho es que, para ser precisos, los piratas informáticos con un sombrero blanco son necesarios para la industria actual. Muchas empresas y organizaciones ofrecen clases y nóminas para hackers experimentados. ¿Por qué? Un sistema informático es como un organismo. Construyes inmunidad al enfermarte. La situación es comparable a los sistemas informáticos. La única forma de mejorar realmente su seguridad es pasar por un ataque. Una debilidad se vuelve muy evidente tan pronto como alguien se aprovecha de ella. Hoy en día, muchas empresas contratan piratas informáticos expertos para mejorar la seguridad de sus sistemas. La mayoría de los ataques de piratería tienen lugar en un patrón. Si ataca su sistema y lo modifica para evitar un ataque de este tipo en el futuro, podrá evitar o al menos ralentizar todos los ataques del mismo tipo. Sin embargo, solo las personas más calificadas son contratadas para estos trabajos. No querrías que un médico inepto tratara tus enfermedades. Por lo tanto, no querrá que un hacker inepto juegue con las complejidades de su sistema. Las personas que hacen este trabajo generalmente son consideradas piratas informáticos por toda la comunidad de programación. Esta es la cosa más respetable que puede hacer con sus habilidades de piratería, ya que requiere mucha experiencia y se hace por una buena causa.
Cuando se habla de los diferentes tipos de piratas informáticos, es importante tener en cuenta que existen categorías basadas en la legalidad y legitimidad de sus actividades, no en el nivel de habilidad que poseen. En base a esto, tenemos las siguientes categorías:
White Hats: los hackers de sombrero blanco son piratas informáticos que quieren ser programadores bien intencionados. Trabajan para mantener los sistemas seguros. Encuentran debilidades en el sistema y encuentran formas de eliminarlas. La línea de trabajo que tienen los sombreros blancos suele estar muy bien pagada y son considerados uno de los más valiosos.

activos tecnológicos. El trabajo de los hackers de sombrero blanco no es ilegal. Los hackers de sombrero blanco tienen permiso del propietario cuando trabajan en un sistema.
Sombreros negros: los piratas informáticos de sombrero negro son los típicos crackers.
Su trabajo suele estar alimentado por intenciones maliciosas y egoísmo. Trabajan para descifrar un sistema para encontrar datos que ellos u otra persona puedan querer. Esto se considera muy ilegal y es la razón por la que la palabra "hacker" tiene connotaciones tan negativas. Hacen lo mismo que los sombreros blancos, pero por malas razones y sin el permiso del dueño. Hay un subgrupo de sombreros negros llamados script kiddies. A nadie en la comunidad le gustan los script kiddies, ni siquiera los propios sombreros negros. ¿Por qué? Porque los script kiddies casi no tienen habilidades de línea de trabajo y usan scripts por adelantado para hacer todo el trabajo.
Grey Hats: los hackers de sombrero gris se encuentran en algún lugar en el medio del espectro. Sus actividades son ilegales, pero no roban ni destruyen los datos, sino que lo hacen por deporte. Por lo general, se comunican con el propietario del sistema que han descifrado para que les proporcione una solución a la vulnerabilidad.

La ética del hacker

Hay dos reglas que marcan la diferencia entre los crackers y los hackers reales. Las dos reglas se han hecho con respecto a la legalidad y legitimidad del proceso de piratería. Estos son los siguientes: Compartir información es bueno para todos. Todo hacker tiene el deber de compartir su conocimiento. Lo hacen escribiendo código fuente abierto y ayudando a las personas a mejorar sus sistemas tanto como sea posible. • Usar el conocimiento de alguien para descifrar sistemas por diversión y para practicar está bien, siempre y cuando no se realicen actividades ilegales a través de esta actividad.

Estos principios son ampliamente utilizados, pero no por todos. La mayoría de los piratas informáticos trabajan bajo la primera ética al escribir software de código abierto. Esto es llevado un paso más allá por algunas personas más extremas que creen que toda la información debería estar disponible para todos. El Proyecto GNU apoya esta filosofía y cree que cualquier forma de control sobre la información debe considerarse mala.

La segunda ética suele considerarse un poco más controvertida porque hay quienes creen que cualquier tipo de okupación debe considerarse inmoral e ilegal. Lo que distingue a los sombreros grises de los sombreros negros es el hecho de que no utilizan su experiencia para destruir o robar información. Es por eso que se consideran algo benignos en la comunidad. Hay diferentes reglas de cortesía entre los piratas informáticos. Tan pronto como un hacker de sombrero gris ingresa al sistema de alguien, siempre debe comunicarse con el propietario del sistema para informarle

cómo se realizó el ataque y cómo proteger el sistema de ataques similares.

Casi todos los piratas informáticos están dispuestos a compartir sus conocimientos y habilidades al respecto. Esta es la forma más confiable en que se manifiestan las dos éticas. Hay redes enormes que funcionan como lugares donde la comunidad puede reunirse y donde las personas pueden intercambiar experiencias y herramientas, así como técnicas y consejos.

Capítulo 1: ¿Qué es el hacking ético?

Los ciberdelincuentes son uno de los mayores problemas que cualquier persona puede enfrentar en el mundo digital. Hubo un tiempo en que los piratas informáticos no se tomaban tan en serio, pero las cosas han cambiado drásticamente en los últimos años. En India, por ejemplo, hay muchas empresas que pagan fuertes sumas de dinero a los piratas informáticos para proteger parte de su información confidencial y valiosa. En 2013, se informó que solo en ese año, las empresas indias perdieron $ 4 mil millones como resultado de ataques cibernéticos.

A medida que el mundo de los negocios evoluciona y se vuelve más dependiente de la tecnología, muchas empresas se han visto obligadas a ingresar al ecosistema digital y utilizar las tecnologías que ofrece el ecosistema para funcionar de manera más eficiente. La necesidad de formas más eficientes de proteger la información es cada vez más importante debido a la amenaza de infracciones de seguridad cada vez más intensas y dañinas. Todos estos cambios dejaron en claro la escasez de personas con talento en el sector de la seguridad de la información.

Nasscom informó que la necesidad de sombreros blancos era mucho mayor que la cantidad de sombreros blancos que tenían en 2015. Había 15ÿ000 hackers éticos certificados en India, en comparación con los 77ÿ000 que realmente se necesitaban.

¿Qué es el hacking ético?

La piratería ética es el uso de técnicas de piratería para ayudar a los sistemas a proteger la información importante almacenada en ellos. Esta es una nueva competencia en programación de TI que está ganando cada vez más reconocimiento. En esta industria, las personas trabajan para piratear sistemas de seguridad e identificar debilidades y encontrar una manera de solucionarlas.

Las técnicas utilizadas por los sombreros blancos y los sombreros negros son muy similares y suelen ser las mismas. La diferencia es que los sombreros blancos deben realizar mejoras en estas técnicas para mantenerse al día con las contrapartes maliciosas en el cuadro. Las empresas que utilizan sistemas de seguridad y trabajan con grandes cantidades de información sensible contratan hackers de sombrero blanco para evitar que personas malintencionadas

acceder a la información almacenada en el sistema. El trabajo de un hacker de sombrero blanco es piratear el sistema del empleador para ubicar las partes del sistema que están en riesgo y arreglar los agujeros. El primer paso que da todo sombrero blanco se llama prueba de penetración. Esta es una forma de encontrar vulnerabilidades en los sistemas. Es una manera fácil de evaluar la fuerza del sistema.

La piratería ética incluye muchos servicios. Algunos de estos son: • Pruebas de aplicaciones: detecta las fallas en un sistema • Remoto o guerra: prueba conexiones de módem Pruebas de red local: trabaja para analizar el trabajo de protocolos y dispositivos en el sistema. • Seguridad inalámbrica: comprueba la seguridad general de todo el marco. • Fortalecimiento del sistema: fortalece el sistema y repara los agujeros en el sistema. • Laptop robada: Esto se hace a través de la PC de un empleado que tiene acceso a poca información. Comprueba la información personal almacenada en el software. • Ingeniería social: utiliza la personalidad del hacker para acceder a un sistema.

La necesidad de hackers éticos

Como he dicho en varias ocasiones, el ciberdelito es cada vez más importante. Las galletas se están volviendo cada vez más sofisticadas. También obtienen acceso a más y más fondos debido a las muchas organizaciones maliciosas que quieren robar información de fuentes importantes.

Todos los días, las empresas necesitan mejorar sus propios sistemas para mantenerse al día con los avances en tácticas y técnicas de piratería. Los piratas informáticos encuentran cada vez más vulnerabilidades ocultas en las computadoras, por lo que para proteger su sistema siempre debe mejorar su seguridad. Esto es lo mismo para cualquier empresa que procese información altamente sensible. Los sombreros blancos suelen ser profesionales bien capacitados que trabajan para mejorar estos sistemas.

Algunas empresas tradicionales tienen un problema a la hora de entender el hacking de sombrero blanco. Los bancos en la India a menudo se han enfrentado a viciosos ataques de hackers que les han costado mucho dinero. Su falta de confianza en los beneficios de la piratería ética los llevó a su minúscula defensa contra el ciberdelito.

Existe un malware llamado "darkhotel" que afecta a hoteles y otras partes de la industria. Esto demostró que la industria se estaba quedando atrás en lo que respecta a la seguridad cibernética. El malware en sí se usó para recopilar información sobre las personas interesadas en los hoteles que utilizan el acceso inalámbrico del hotel.

La comunidad de ocupantes ilegales está en constante crecimiento en lo que respecta a herramientas y técnicas. Todos los días se crean nuevos tipos de malware, gusanos y virus. Como resultado, las empresas son cada vez más conscientes de los beneficios de la ética.

piratería y cómo puede ayudar a proteger sus redes.
La conclusión es que poseer un negocio hoy en día es tan arriesgado como podría ser debido a la cantidad de usuarios maliciosos que tienen acceso a tantas herramientas diferentes. Por lo tanto, cada sistema debe probarse regularmente para mantenerse al día. Existe un enfoque holístico involucrado en la evaluación de un sistema debido a la complejidad del campo de la seguridad informática y de redes.
Hay muchas interacciones y operaciones involucradas en cualquier sistema de seguridad, y algunas de ellas pueden ser muy vulnerables. Los hackers éticos son las mejores personas para esto. Son las personas con la capacidad y el conocimiento que pueden ayudar a cualquier persona a refinar su sistema.

¿Cuál es la diferencia entre hacking ético y cracking?

Como he dicho algunas veces, las técnicas que usan todos los piratas informáticos son similares, si no las mismas. Las herramientas y técnicas utilizadas son universalmente aceptadas por todas las personas que se dedican a esta actividad. La única diferencia entre los hackers éticos y los demás es por qué hacen lo que hacen. Los crackers o sombreros negros son alimentados por sus propias razones egoístas y malvadas, como ganancias o acoso. Los esfuerzos de los sombreros blancos están hechos para evitar que los sombreros negros se aprovechen de los sistemas.
Hay varias otras cosas que pueden ayudarlo a distinguir los sombreros negros de los sombreros blancos: El propósito de la actividad: si bien es cierto que los sombreros blancos usan todas las técnicas desarrolladas por los sombreros negros, lo hacen para ayudar a una persona o empresa.

Esto se hace para determinar cómo se acercaría un sombrero negro al sistema para detectar y ayudar a corregir defectos.
Legalidad: la principal distinción entre los hackers éticos y los crackers es el hecho de que, si bien hacen lo mismo de la misma manera, solo un lado es legalmente aceptable. Los sombreros blancos tienen el permiso del propietario del sistema antes de hacerlo, mientras que los sombreros negros infringen la ley al hacerlo sin el conocimiento del propietario.

Propiedad: Varias empresas contratan a los sombreros blancos para que les ayuden a mejorar sus sistemas. Los sombreros negros no son propiedad del sistema y no son empleados por nadie que lo sea.

Roles y responsabilidades de un hacker ético

El lado ético de la piratería no es fácil. Si bien los sombreros blancos a menudo son muy apreciados en la comunidad de programación, así como entre los empresarios, muchos todavía los consideran delincuentes. La actividad en sí es considerada inmoral por muchos. Muchos sombreros blancos prefieren no tener la connotación de "hacker" junto a

su nombre debido a las respuestas que pueden obtener.
Para mantener sus prácticas legales y evitar que otros los perciban como criminales, los hackers de sombrero blanco deben ser muy conscientes de sus responsabilidades y cumplir con las pautas. Las siguientes reglas son algunas de las más importantes para los hackers de sombrero blanco: • Siempre se espera que un hacker ético busque el permiso del propietario del sistema antes de iniciarlo. Necesitará la aprobación del propietario para cualquier actividad que realice en el sistema y se espera que proporcione al propietario la información obtenida a través de sus actividades. • Una vez que el hacker haya analizado el sistema, debe informar sus hallazgos y planes al propietario antes de tomar medidas. • El hacker debe informar al propietario de lo que encontró durante la búsqueda. • Se espera que el hacker mantenga la confidencialidad de sus hallazgos y actividades. Debido a la naturaleza de la piratería ética que promueve la seguridad de un sistema, el pirata informático no debe revelar la información a nadie más. • Elimine todas las vulnerabilidades encontradas después de encontrarlas para evitar que los sombreros negros ingresen al sistema sin permiso.

Para tener éxito en la industria, necesita un cierto conjunto de habilidades. El conocimiento que debe poseer un hacker de sombrero blanco es amplio y profundo. Debe cubrir diferentes partes del campo de la tecnología informática y debe ser muy detallada. Algunas de las habilidades requeridas son: • Conocimientos detallados de programación: cualquier profesional que trabaje en el ciclo de vida de desarrollo de software y seguridad de aplicaciones debe poseer este conocimiento. • Conocimiento de secuencias de comandos: este tipo de conocimiento es importante para cualquier persona que trabaje en ataques basados en host y ataques basados en red. • Habilidades de red: la mayoría de las amenazas al sistema provienen de las redes. Debido a esto, necesita saber qué dispositivos están conectados a la red y cómo los manejan. • Conocimiento de diferentes plataformas utilizadas en diferentes tipos de dispositivos Conocimiento del uso de herramientas y técnicas de hackeo disponibles en el mercado • Conocimiento de servidores y motores de búsqueda

Capítulo 2: Hackear como carrera

Es seguro decir que identificarse como hacker llamará la atención y le dará algunas miradas desagradables porque las personas que no conocen el

La diferencia entre sombreros negros y sombreros blancos asume inmediatamente que lo que estás haciendo es muy ilegal. Hagas lo que hagas, ya sea ayudar a un departamento militar a mejorar la seguridad de la información clasificada o piratear la base de datos de una escuela para ver qué lagunas pueden explotar los usuarios no autorizados para acceder a los datos, tus esfuerzos generalmente serán desaprobados hasta cierto punto por otros. . La gente suele suponer que trabajas como parte de una sociedad clandestina de vándalos y no lo consideran una elección de carrera válida.

Esto es cualquier cosa menos cierto. La piratería puede hacer una carrera como ninguna otra. Para trabajar correctamente como un hacker ético certificado, deberá realizar una gran cantidad de trabajo preparatorio y capacitación. Un diploma o certificado en el campo de la seguridad informática no siempre es obligatorio, pero es bueno tenerlo. Lo que necesitas es un amplio conocimiento del tema. Saber cómo funcionan e interactúan las computadoras es la parte más importante al buscar un trabajo. A muchas películas y programas de televisión les gusta ver la piratería como algo encantador. Nunca muestran todo lo que viene en la caja. La experiencia y el conocimiento son excelentes ofertas cuando se trata de piratería, que a veces se pasa por alto fácilmente.

Con eso en mente, si ya aprendió usted mismo usando sus sistemas, esta forma de trabajar puede ser más desafiante de lo que parecía inicialmente.

Si ha practicado con su propio equipo, el siguiente paso lógico es el trabajo independiente, donde puede obtener más experiencia y apoyo para sus actividades. Sin embargo, como era de esperar, el trabajo independiente de piratas informáticos no es exactamente la posición más estable de la historia, por lo que podría experimentar algunos puntos bajos en lo que respecta a las finanzas. Es una excelente manera de obtener más experiencia y algo de dinero. También es una excelente manera de crear un currículum impresionante. El trabajo independiente suele ser un gran lugar para comenzar.

Después de obtener una cantidad significativa de experiencia, debe comenzar a enviar solicitudes de empleo a empresas de tecnología para ver si se necesita su experiencia. Puede enviar solicitudes a muchas grandes empresas. Esto es inteligente porque tienden a pagar más por estos servicios. Sin embargo, hay muchas empresas más pequeñas que están felices de contratarte y están dispuestas a pagar un poco más por tus servicios si eres lo suficientemente bueno. Siempre mantenga la vista abierta, ya que puede encontrar trabajo en esta industria si tiene las habilidades.

Ser un hacker ético es una tarea bastante desafiante porque un verdadero hacker blanco necesita saber todo sobre sistemas y redes. Es por eso que ciertas organizaciones han comenzado a emitir certificaciones que respaldan a los hackers talentosos cuando se trata de trabajar. Los aspirantes a hackers éticos han estado buscando

para tales certificaciones como evidencia de habilidad. Hay varias certificaciones que brindan algunos beneficios importantes. Algunos de estos beneficios incluyen: • Los hackers con estas certificaciones tienen el conocimiento necesario para construir y mantener sistemas de seguridad. Si eres bueno en este campo, eres un gran activo para cualquier organización que quiera contratarte. • Los piratas informáticos con estas certificaciones tienen más probabilidades de recibir salarios más altos.
Un hacker ético certificado puede aspirar a un salario de 90.000 dólares. • Valida tus esfuerzos y te facilita conseguir un trabajo en empresas y te hace destacar entre tus colegas. • La mayoría de las organizaciones prefieren personas certificadas cuando se trata de la seguridad del sistema debido a las crecientes necesidades del campo. • Las empresas emergentes buscan personas certificadas. Estas empresas pagan un centavo por las personas que hacen este trabajo.

Los diferentes tipos de piratería ética Cuando se trata de piratería ética, se utilizan diferentes tipos de prácticas.
Debido a la gran variedad de posibles ciberataques, todas las empresas quieren probar tantas posibilidades como sea posible. Es por eso que emplean a personas con diferentes niveles de conocimiento. Estas son las llamadas cajas. Hay tres tipos.

Caja negra Hacking ético

Los piratas informáticos éticos de la caja negra no saben nada acerca de la organización a cuyos sistemas están tratando de ingresar. Estas personas no se enfocan en una parte particular del sistema o en un método particular. Utilizan todas las herramientas a su disposición para descifrar el sistema. El atacante no tiene foco porque no tiene información sobre la organización que está atacando.

Hacking ético Caja Blanca

Los hackers éticos de caja blanca están preocupados por la cantidad de tiempo y dinero que se dedica a un trabajo. Cuando un hacker ético comienza a trabajar en un sistema con una caja blanca, sabe todo sobre la organización. Se utilizan para imitar un ataque que puede llevar a cabo alguien cercano o dentro de la empresa. Estos ataques apuntan a partes específicas del sistema para fortalecerlas. La desventaja de este método es que el hacker atacará las vulnerabilidades ya conocidas y posiblemente pasará por alto otras vulnerabilidades.
Los hackers éticos de caja blanca suelen trabajar con equipos de diferentes personas, desde Recursos Humanos, Alta Dirección y Gestión de Soporte Técnico.

Hacking ético de caja gris La piratería de cajas grises está en algún lugar entre los dos anteriores. Combina

los dos ataques. Tiene cierta cantidad de información sobre la empresa, pero esa información puede cambiar de vez en cuando. Tiene el mismo inconveniente que la piratería ética de caja blanca debido a las vulnerabilidades obvias.

La historia del White Hat Hacking El hacking ético no es algo de la nueva era. Ha existido bajo diferentes nombres durante mucho tiempo. El primer caso documentado de piratería ética ocurrió cuando la Fuerza Aérea de los Estados Unidos realizó una llamada evaluación de seguridad de sus sistemas. El sistema operativo Multics ha sido probado para ver si se puede utilizar para almacenar archivos y documentos secretos. Durante esta prueba, se determinó que Multics era mejor que las otras opciones disponibles para ellos, pero aún faltaba y tenía muchas vulnerabilidades en lo que respecta a la seguridad que podrían ser explotadas por el lado del cracker con poco esfuerzo. La prueba se hizo lo más realista posible porque pensaron que esta es la única forma de obtener resultados precisos que puedan considerarse evidencia. Las pruebas variaron desde la simple recopilación de información hasta ataques completos que pusieron en peligro los sistemas completos.

Desde entonces, ha habido algunos informes más del ejército de los Estados Unidos realizando este tipo de actividades.

Hasta 1981, la piratería de sombrero blanco no era conocida como un término para muchas personas, pero fue entonces cuando The New York Times introdujo y etiquetó el término como una forma positiva de la tradición de la piratería. Había un empleado en el CSS nacional que escribía un software para descifrar contraseñas. Cuando decidió lanzar este software, se indignó. La empresa no estaba enfadada por la existencia del software, sino por el hecho de que ocultaba la existencia del software. En la reprimenda, el NCSS afirmó que la empresa encuentra y alienta el hecho de que los empleados que encuentran fallas de seguridad son beneficiosos para la empresa.

Dun Farmer y Wietse Venma fueron los primeros en ver el potencial de la piratería de sombrero blanco. Fueron las personas que lo convirtieron en una técnica que se puede utilizar para evaluar la seguridad de un sistema y mejorarlo más tarde. Señalaron que después de una cierta cantidad de tiempo, una vez que han recopilado cierta cantidad de información, pueden invadir un sistema y causar mucho daño si así lo desean.

Hablando sobre lo que se puede hacer a través de la piratería de sombrero blanco, dieron varios ejemplos de cómo se puede recopilar y usar la información y cómo usar este conocimiento para prevenir ataques. Hicieron una aplicación de todas las herramientas que usaron durante su investigación y las pusieron a disposición de cualquier persona que pudiera estar interesada para descargarlas. El programa se llama Security Administrator Tool for Analyzing Networks, también conocida como SATAN. El programa recibió mucha atención de los medios en 1992.

Capítulo 3: Ganar dinero por cuenta propia

La piratería ética es un campo enorme. La cantidad de trabajos disponibles es enorme, lo que hace que paguen cada vez más a medida que pasa el tiempo, ya que no hay suficientes hackers éticos para cumplir con todas estas funciones en todo momento.

En mi opinión, trabajar independientemente es la mejor manera de ganar dinero con la piratería ética. En este capítulo, analizamos los pros y los contras del trabajo independiente, qué tan bien puede ganar y cómo convertirse en un trabajador independiente.

¿Qué es el trabajo independiente?

Freelancing es, de hecho, convertirse en una empresa usted mismo. Aunque no tienes que actuar como director ejecutivo o algo así, sirve para pintar una buena imagen. Un profesional independiente es en realidad un negocio de un solo hombre. Tienes que ser tu propio marketing, tu propio PR, tu propio contador y tu propio empleado. Esto requiere mucho esfuerzo, por lo que si eres alguien que está satisfecho con un trabajo normal de 9 a 5, no recomendaría ir por la ruta independiente. Por otro lado, si eres alguien que quiere dar lo mejor de sí mismo, llegar a lo más alto del campo y traer cantidades ridículas, esta área es para ti.

Trabajar por cuenta propia básicamente significa abandonar el concepto tradicional de empleo y convertirse en una especie de contratista a tiempo completo. Tienes que elegir tus propios clientes y encontrarlos tú mismo. Esto puede ser bastante difícil para los principiantes, aunque a continuación enumeramos algunas formas excelentes.

Como autónomo, también puedes dictar tus propios horarios, lo cual es genial. Si eres madrugador, puedes comenzar a trabajar al amanecer, pero si eres tardío, nadie te juzgará por comenzar tu jornada laboral a las 4 am. Esto también significa que no tiene que hacer todo su trabajo a la vez y puede segmentar su trabajo para que solo trabaje durante el tiempo que realmente es productivo.

Además, solo se le paga por las cosas que hace, así que asegúrese de incluir esto en su tarifa por hora. No es raro que los trabajadores independientes estén en un área que generalmente paga $ 20 por hora para cobrar $ 30 por hora o tarifas más altas. Por lo general, se considera que los trabajadores independientes también son más competentes que los empleados internos, así que asegúrese de que su conocimiento refleje esto.

Finalmente, trabajar como freelance significa renunciar a cualquier concepto de seguridad laboral. Los clientes van y vienen como el viento, pero si puede mantener un flujo constante de ellos, ganará mucho más que su contraparte interna.

Los pros y los contras de ser autónomo Veamos qué obtienes cuando te conviertes en autónomo por primera vez, ¿verdad?

Beneficios

En primer lugar, obtienes libertad en más de un sentido. Los más importantes son la ubicación y el tiempo. Puedes trabajar donde quieras. Esta es la causa del estilo de vida del "nómada digital". Ahí es donde dejas una ubicación física constante y simplemente viajas por el mundo con tus ingresos independientes apoyándote.
Esta es una excelente forma de vida, y muchas personas la han tomado con entusiasmo porque es muy cómodo saber que, literalmente, siempre puedes cambiar de ubicación e ir a otro lado. Tener la libertad de emprender una aventura cuando quieras es extremadamente emocionante.

Por otro lado, esto también tiene muchos más usos cotidianos. ¿Tu día alguna vez tuvo un mal comienzo porque tus paseos matutinos fueron desordenados o molestos?
Pues eso no volverá a pasar nunca más porque tus desplazamientos... ¡no existen!
Simplemente te levantas de la ⋯ espera un minuto, tú solo acuéstate EN tu cama y trabaja.
cama Este tipo de libertad generalmente no está disponible para todos, excepto para los más ricos de la sociedad, pero trabajar por cuenta propia lo hace bastante fácil.
Aparte de eso, el trabajo a menudo se mete en tu tiempo cuando no quieres. Esto significa, por ejemplo, que querías salir con un amigo a las 9 de la mañana, pero no podías por motivos de trabajo. Si fuera un profesional independiente, no tendría este problema, ya que puede mover todo su trabajo más tarde en el día y seguir saliendo con su amigo. Esto también significa que si realmente tuviste un día horrible (por ejemplo, alguien rompió contigo), puedes tomarte un día libre en el trabajo si lo compensas más tarde.

Esto también es excelente para la productividad, ya que todos tienen varias horas durante el día en las que se consideran productivos. En lugar de tratar de encajar en las horas de trabajo de una empresa, puede elegir usted mismo.
La segunda razón por la que debería considerar trabajar independientemente es el dinero. Los freelancers exitosos ganan MUCHO más dinero que sus contrapartes en su escritorio.
Por ejemplo, algunos de los hackers éticos independientes más exitosos ganan más de $ 500,000 al año. Deja que ese número se derrumbe. Por otro lado, no es que los principales hackers éticos en las empresas no ganen mucho dinero, pero eso no suele ser ni la mitad.

Esto, por supuesto, tiene algunas salvedades. Si se une al FBI, es probable que reciba ofertas que avergonzarán a cualquier trabajador independiente, pero para comenzar con el FBI, debería haber tenido una gran cartera de trabajadores independientes de antemano.
Por esta razón, si lo único que buscas es dinero, te recomendaría que consideres trabajar como freelance mucho más que trabajar en una agencia.
La tercera razón para ser autónomo es, bueno, divertida. No me tomes ahora como una de esas personas que disfrutan de todo el trabajo, pero si eres autónomo puedes elegir

tus posibilidades

¿Conoces esa sensación cuando tu jefe te asigna una tarea que realmente odias y tienes que hacerla, incluso si prefieres duplicar ese tiempo, solo trabajar en otra cosa? Bueno, como autónomo, no tienes que hacerlo. Si hay un área específica de piratería ética que realmente no le gusta, puede evitarla y no volver a interactuar con ella en su vida.

Esta libertad también le permite asumir mayores y mejores desafíos. No tiene que esperar a que su jefe le confíe una tarea que cree que está fuera de sus posibilidades. ¡Solo tómalo y pruébalo! En el peor de los casos, no cumple con las expectativas del cliente y su reputación se ve afectada temporalmente.

Contras

El primer inconveniente del trabajo independiente es, bueno, la libertad. Pero espera, dices, ¿no dijiste que la libertad era un profesional? Lo es, si puedes soportarlo. Puede ser extremadamente fácil caer en la trampa de no trabajar lo suficiente porque no está sujeto a un contrato, ubicación o similar.

Esto a menudo lleva a los 'trabajadores autónomos', personas que en realidad están desempleadas y han conservado su último trabajo y han contratado a autónomos junto a él con la esperanza de que suene mejor. Después de todo, sin nada a lo que comprometerse, puede ser muy fácil volar demasiado cerca del sol.

El segundo escollo (relativamente similar al primero) en el que muchos caen son las asignaciones tardías. A partir de la primera vez que dices: "Oh, sí, esto se está haciendo tarde", todo continuará de ahora en adelante. De un encargo a otro.

Esto a menudo puede suceder incluso sin molestar a los clientes, pero hacer cosas de última hora generalmente es una mala idea, aunque solo sea por el estrés que causa.

El estrés en sí mismo a menudo causa problemas que caen en cascada, lo que significa que si está un poco estresado un día, está bastante estresado al día siguiente y luego se derrumba.

Ahora el tercero es encontrar clientes. Encontrar clientes es... difícil, especialmente para aquellos que recién comienzan. Si se encuentra en un país de clase superior (Reino Unido, EE. UU., Rusia, etc.), es posible que la mayoría de los trabajos de nivel de entrada en su campo se paguen por debajo de la tarifa. Si bien la mayoría de los trabajadores independientes ganan más que sus contrapartes en sus escritorios, esta relación es excelente cuando se trata de puestos de nivel de entrada. Después de todo, un trabajo de nivel de entrada generalmente lo puede hacer alguien de la India (con un salario promedio bajo) y alguien de los EE. UU. Afortunadamente, cuando se trata de piratería ética, hay muchos más trabajos que autónomos.

Esto significa que este tipo de amortización de las tarifas de autónomos en realidad no se produce.

Por otro lado, aunque haya tantos puestos de trabajo, eso no significa que llegar a los clientes no sea difícil y no sean selectivos. Encontrar tu primer trabajo independiente siempre es muy difícil, por lo que te recomendaría que primero comiences a trabajar en un escritorio, al menos hasta que te mojes en la industria.
Esto se debe a que las personas generalmente confían en la experiencia cuando se trata de encontrar clientes. Los freelancers querrán trabajar con personas que estén conectadas con sus antiguos clientes, y sus antiguos clientes buscarán freelancers experimentados. Como regla general, la experiencia es el rey en el mundo freelance.

Esto nos lleva a otra desventaja del trabajo independiente. Ser tu propio jefe es sorprendentemente difícil. Debe poder crear su propio sitio web y debe anunciarse. Debes prestar atención tanto al SEO como a tus habilidades en el campo en el que trabajas. Aunque trabajar por cuenta propia es un trabajo con muchas horas libres, en cierto sentido es un trabajo de 24 horas al día, 7 días a la semana, en el sentido de que nunca dejas de trabajar por un tiempo.

Empezar a trabajar independientemente

Ahora, suponiendo que haya superado los pros y los contras del trabajo independiente y decidiera comenzar, ¿qué debe hacer? (Si ha decidido que no es para usted, no dude en omitir esta parte).
Ahora quiero dividir esto en dos partes. En uno recomiendo un camino a alguien que ya tiene experiencia en TI, mientras que en el otro dirijo el texto a un principiante completo.

Tengo experiencia, ¿ahora qué?

Si tiene experiencia ahora, tiene una ventaja sobre casi todos los que no la tienen. Lo primero que debe hacer es crear un sitio web.
¿Una página web? ¿No debería ser suficiente un currículum? Aunque sí, la mayoría de las funciones de oficina solo requieren un currículum, pero ten en cuenta que competirás directamente con otras personas. Esto significa que cada punto que has ganado en la liga se ve genial. También te presentas menos como empleado y más como socio comercial, y ¿qué tipo de socio comercial no tiene un sitio web?
La primera pregunta que debe hacerse es: "¿Tengo contactos cercanos?"
Lo más probable es que, si ha trabajado en la industria de TI, conozca a bastantes personas con sitios web. Con la mayoría de los profesionales de TI, esta puede ser incluso la mayor parte de las personas que conoce. Si este es el caso, está bien que tengas algunos clientes potenciales allí. Ponte en contacto con todas estas personas una a una y comprueba si tienen problemas para encontrar un profesional de ciberseguridad.
Si alguien dice que sí, ¡genial! Tienes tu primera actuación, así que asegúrate de

clavarlo por completo. Si lo haces, definitivamente te recomendarán a sus amigos. Esta es la parte más importante del trabajo independiente: crear una red de contactos útiles que puedan ser clientes cuando te metas en problemas. Asegúrese de que todos sus empleadores / clientes anteriores sepan en qué está trabajando actualmente y dígales que lo recomienden si alguien que conocen tiene problemas de seguridad cibernética.

Esto es genial porque: •
Construye tu reputación. Será mucho más conocido en su campo si incluso las personas que no están involucradas en seguridad cibernética saben su nombre. Además, contar con personas dispuestas a garantizar tu calidad es una excelente señal para futuros clientes. • Construye una clientela constante. Después de obtener algunos conciertos exitosos, es probable que los clientes lleguen automáticamente. El boca a boca se está extendiendo rápidamente en los círculos técnicos, y existen pocos profesionales profesionales en ciberseguridad.

Entonces, ¿qué pasa si tus clientes anteriores no te dan conciertos? ¿O simplemente no son lo suficientemente entusiastas como para recomendarte a sus conocidos? En ese caso, vaya a las redes sociales y sitios de trabajo como Indeed.
Hay innumerables publicaciones para expertos en ciberseguridad externos/independientes y hackers éticos en estos sitios. Asegúrate de usarlo de manera óptima. Ponga "hacker ético", "probador de penetración" o "experto en seguridad cibernética" en su biografía. Aparte de eso, asegúrese de usar Linkedin, ya que es muy popular entre los gerentes de contratación y, a veces, incluso un perfil bien elaborado es suficiente para obtener algunos clientes potenciales.

De hecho, generalmente es mejor para puestos remotos a largo plazo, pero tampoco es malo para los trabajadores independientes. Tenga en cuenta que Indeed es un juego de números. Muchos de los listados son falsos o están desactualizados, así que asegúrese de solicitar toneladas.
Si ninguno de estos ha funcionado, entonces es hora de dirigirse a un sitio recopilado.
Este sería un sitio como UpWork o Freelancer, estos son sitios diseñados para promover la oferta de trabajo entre los trabajadores independientes.
En general, desaconsejaría el uso de estos sitios, ya que suelen ofrecer tarifas más bajas que los clientes encontrados individualmente. Por otro lado, si tiene una buena cartera de experiencia, pasa rápidamente los trabajos de nivel principiante (de los cuales hay muchos) y pasa a trabajos que realmente están bien pagados.

No tengo experiencia, ¿qué debo hacer?

Si acabas de entrar en el mundo del hacking ético y no tienes ninguna experiencia de la que hablar, no te desesperes. Después de todo, tienes una base sólida.

de conocimiento y un impulso para tener éxito!
En este caso, le aconsejaría que alguien hiciera su sitio web para usted.
Lo más probable es que no sepa lo suficiente como para hacerlo usted mismo o se pierda ante la parálisis de opciones. Si siente que sabe lo suficiente y es lo suficientemente decidido como para hacerlo bien, al menos hágalo usted mismo. Por otro lado, contratar a un profesional siempre es una buena idea.

Una vez que haya terminado con eso, le recomiendo tener algunas piezas de cartera. Puede ser trabajo de práctica que haya hecho en la universidad, o simplemente cosas que hizo para divertirse, pero lo importante es que es algo que puede mostrar a los clientes potenciales.

En ese momento, dirígete a uno de los sitios de recopilación de trabajos independientes como UpWork o Freelancer (de estos dos recomendaría UpWork porque parece más profesional) y busca trabajos. No tengas miedo si solo te aceptan para trabajos mal pagados, ya que estos sitios son conocidos por su reputación y experiencia. Asegúrate de moverte siempre hacia arriba. Cada uno de sus clientes debe pagar mejor que el último.

Después de ganar mucha experiencia en uno de estos sitios, regrese aquí y aplique los consejos en "Tengo experiencia, ¿ahora qué?" sección.

Primas En ambos casos (con o sin experiencia), las primas son una forma sólida, aunque extremadamente difícil, de ganar dinero. Los premios están dirigidos principalmente a personas con experiencia, pero se han dado casos en los que han sido obtenidos por personas con menos experiencia.

Una prima es cuando una empresa decide que quiere probar su seguridad cibernética y luego hace que todos lo intenten. Si un sombrero blanco logra romper la defensa de una empresa, recibe la llamada 'prima'. Así que, esencialmente, fingirías ser un cracker malicioso que intenta ingresar a los sistemas de la empresa y, si lo logras, obtendrás dinero. Suena genial, ¿verdad?

El problema con las recompensas, sin embargo, es que para los piratas informáticos menos hábiles, a menudo tienen más problemas de lo que valen. Después de todo, aquellos que valen la pena son generalmente tomados por el 5% de los mejores piratas informáticos en todo el mundo, en lugar del ciudadano promedio del mundo de la piratería ética.

Capítulo 4: Los tres sombreros

Espera, ¿sombreros? Sí, por extraño que parezca, los piratas informáticos en realidad están separados de todas las cosas del mundo por sombreros. Como ya hemos explorado, esto no solo significa que alguien es un hacker, sino que está involucrado en actividades ilegales o

Cualquier cosa como eso. Descubrirá que la mayoría de las personas, en línea o no, se refieren a los piratas informáticos bajo una de tres etiquetas. Estos son sombrero blanco, gris y negro. El sombrero gris a veces se considera un subconjunto específico de negro. Estos son términos creados para definir diferentes piratas informáticos en función de lo que hacen, y los discutimos brevemente en la introducción.

Asimismo, puede ser bastante difícil definir 'hacker' ya que el uso técnico del término es bastante diferente de la forma en que se usa en la mayoría de las culturas populares.
Dicho esto, definitivamente podemos decir que un hacker es alguien que usa un agujero en un sistema digital para encontrar formas de aprovecharlo y aprovecharlo personalmente. En el caso de los hackers de sombrero blanco, esta ganancia sería el dinero proporcionado por la empresa que los contrató o la satisfacción de saber que hicieron algo bueno.

Entonces, ¿cuáles son exactamente los tres sombreros de los piratas informáticos y qué hacen?

Sombreros

negros Los piratas informáticos de sombrero negro, comúnmente conocidos como 'sombrero negro', son aquellos piratas informáticos que son más comunes en la cultura pop, los programas de televisión y las películas. Este es el tipo de hacker en el que piensas cuando escuchas la palabra hacker. Los piratas informáticos de sombrero negro son aquellos que violan la ley, pero también violan la seguridad de una computadora para perseguir una agenda egoísta. Esto puede variar desde robar números de tarjetas de crédito hasta robar identidades completas de personas.
En otros casos, esto simplemente sucede por enojo, por lo que un hacker de sombrero negro puede crear una red de bots simplemente para crear sitios web DDOS que no son muy aficionados.
Los sombreros negros no solo encajan en el estereotipo de que los hackers son delincuentes, sino que también son la razón de su existencia. De hecho, son el equivalente en PC de los ladrones altamente calificados. No es difícil ver por qué a otros grupos de hackers generalmente no les gustan los sombreros negros porque humillan los nombres de los demás.
Los sombreros negros suelen ser esos sombreros que encuentran vulnerabilidades de día cero en la seguridad de un sitio o empresa y luego las venden a otras organizaciones, o simplemente las usan para sus propias agendas egoístas.

¿Vulnerabilidad de día cero?

Un día cero es un error en una pieza particular de hardware, software o firmware que es desconocido para una de las partes que, de lo contrario, tendría la tarea de resolver el error. El término en sí puede referirse a la vulnerabilidad en sí o a un ataque que tarda 0 días entre el descubrimiento de la vulnerabilidad y el ataque.

Cuando se hace pública una vulnerabilidad de día cero, se la conocerá como vulnerabilidad de día n o de un día, siendo ambas igualmente peligrosas.
Por lo general, cuando se detecta un error de este tipo, la persona que lo detectó toma este

error a la empresa cuyo software es defectuoso. Ocasionalmente, anuncian públicamente el error en caso de que no puedan comunicarse con la empresa por sí mismos. Esto generalmente se hace para parchar ese agujero.

Después de un tiempo, la empresa que creó el programa normalmente puede arreglarlo y distribuir el parche. A veces esto significa que el producto debe retrasarse un poco, pero después de todo, ¿no vale la pena hacerlo si significa que la empresa está ahorrando mucho dinero? Incluso si la vulnerabilidad se hace pública, a menudo los sombreros negros pueden tardar un tiempo en aprovecharla. En estos escenarios es una carrera entre los sombreros negros y los sombreros blancos.

Por otro lado, a veces es un sombrero negro el primero en descubrir la vulnerabilidad. Si no se sabe de antemano, los sombreros blancos de la empresa no tienen idea de que el exploit existe antes de ser utilizado en su contra. Por lo general, estas empresas utilizarán piratas informáticos éticos para encontrar dichas vulnerabilidades de día cero para que puedan remediarse antes de que su producto salga al mercado.

Los investigadores de seguridad están trabajando con proveedores de información que a menudo acordarán no compartir información de vulnerabilidades de día cero hasta que se les permita. Por ejemplo, Project Zero de Google sugiere que si descubre una vulnerabilidad como empleado que no pertenece a la empresa, debe esperar al menos 90 días antes de hacer pública la vulnerabilidad. Por otro lado, si la vulnerabilidad es algo muy crítico, Google sugiere que solo hay que esperar unos 7 días para ver si la empresa cierra el agujero que dejaron abierto accidentalmente. Por otro lado, si la vulnerabilidad ya está siendo explotada, ¡dispara!

Ejemplo de hacker de sombrero negro

Como en las escenas iniciales de una película con Daniel Craig, allá por 1994, Vladimir Levin usó su computadora portátil en su departamento de San Petersburgo para llevar a cabo el primer robo a un banco por Internet en la historia.

Depositó $ 10 millones de cuentas de varios clientes de Citibank a varias cuentas que poseía en todo el mundo. Afortunadamente, este robo no le fue tan bien a Levin. Solo tres años después, fue capturado y encarcelado.

De los $ 10 millones que robó, nunca se encontraron $ 400,000. La forma en que Levin hizo esto fue increíblemente simple. Simplemente pirateó las llamadas telefónicas de los clientes, anotó los detalles de su cuenta, luego fue y se entregó su dinero.

sombreros blancos

¡Oye, somos nosotros! Los hackers de sombrero blanco, también conocidos como hackers éticos, son lo opuesto a los hackers de sombrero negro. También son expertos en comprometer

sistemas de seguridad informática, tanto es así que muchos de ellos fueron sombreros negros y reformados en el pasado. Estos son los piratas informáticos que pueden ser sombreros negros, pero prefieren usar sus habilidades y conocimientos para el bien y con fines éticos en lugar de sus propias motivaciones egoístas (aunque se podría argumentar que buscar el bien es egoísta en sí mismos).

Las empresas utilizan la mayoría de los sombreros blancos para tratar de "simular" un sombrero negro, por lo que intentarán piratear los sistemas de seguridad de una organización lo mejor que puedan. Luego, la organización autoriza a los piratas informáticos de sombrero blanco a utilizar su conocimiento de los sistemas de seguridad para comprometer a toda la organización. ¿Suena esto como algo que haría un sombrero negro? Exactamente. Necesitan simular exactamente lo que haría un pirata informático de sombrero negro para saber si pueden detenerlo antes de causar un daño significativo a la empresa. Los ataques de un hacker de sombrero blanco generalmente se utilizan para mejorar las defensas de la organización contra los ataques cibernéticos. Por lo general, estas dos cosas las hacen las mismas personas, pero algunas empresas tienen a los hackers de sombrero blanco y a los profesionales de la ciberseguridad separados.

El método de pretender ser un pirata informático de sombrero negro para acceder a los archivos confidenciales de una empresa para ayudarlos con su sistema se conoce como prueba de penetración.

Descubrirá que los piratas informáticos de sombrero blanco que encuentran vulnerabilidades en los valores preferirían revelarlo al desarrollador del programa, en lugar de cumplir sus propios deseos egoístas.

Si usted, como hacker ético, encuentra accidentalmente una vulnerabilidad, es su obligación moral informar al desarrollador. Esto les permite parchear su producto antes de que un hacker de sombrero negro pueda entrar y arruinarlo por completo.

También vale la pena señalar que, como mencionamos anteriormente, algunas organizaciones pagan primas incluso por sombreros blancos anónimos que son lo suficientemente buenos para ingresar a su sistema. Al hacer esto, se aseguran de estar protegidos de los sombreros negros que pueden haber entrado en sus filas como sombreros blancos y haber llegado a un público más amplio.

Ejemplo de hacker de sombrero blanco

Kevin Mitnick es el rostro del movimiento de piratería ética en estos días, pero no siempre fue así. Muchos incluso especulan que el motivo de su fama y sus habilidades se debe a que su sombrero no siempre fue precisamente el más blanco de todos. Hace 26 años, en 1995, la policía atrapó a Mitnick por un arresto notable. Había emprendido una serie de actividades de piratería que duraron más de dos años.

Todo era completamente ilegal. Algunas de sus hazañas fueron realmente enormes. Para

Por ejemplo, durante una de sus escapadas, se abrió paso en los sistemas de seguridad de Digital Equipment Corp. Una vez dentro, decidió copiar y copiar todo lo que había.

Después de cumplir su sentencia de prisión, se le otorgó una liberación supervisada, pero antes de que se acabara el tiempo, Mitnick había vuelto a su antigua forma de hacer las cosas. Antes de que cumpliera su sentencia, incluso se le dio acceso a las computadoras de correo de voz de Pacific Bell. Se cree que ingresó ilegalmente en varios otros lugares utilizando métodos como la interceptación de contraseñas, aunque esto nunca se ha confirmado realmente.

Le dieron la friolera de 46 meses y 22 además por violar el tiempo en el que se suponía que debía estar bajo vigilancia. Este fue el final de su carrera como hacker de sombrero negro.

Después de cumplir su condena en 2000, Mitnick decidió que se convertiría en un hacker de sombrero blanco. Eligió convertirse en un consultor pagado, y lo hizo. Las compañías Fortune 500 e incluso el FBI acudieron en masa a Mitnick en busca de ayuda. Después de todo, tenía una gran cantidad de talentos y conocimientos para compartir. Multitudes de personas han acudido a él a lo largo de los años para aprender de la experiencia que tuvo. El conocimiento y las ideas que poseía se transfirieron luego a su muy popular trabajo de oratoria y escritura.

Mitnick incluso dio clases él mismo, dirigiendo clases de ingeniería social con el mismo conocimiento que antes. Estas eran habilidades esenciales que todavía necesitamos hoy. Incluso hoy en día, Mitnick está ocupado con las pruebas de penetración, aunque ahora lo son para algunas de las empresas más exitosas y poderosas del mundo.

Sombreros grises Nada en la vida es blanco o negro. Más adelante, esa broma divertida en realidad refleja muy bien la piratería. De hecho, como en la vida, siempre hay una zona gris entre el blanco y el negro en el mundo de la piratería.

Como habrás adivinado, un hacker de sombrero gris se encuentra en el lugar incómodo entre un hacker de sombrero negro y un hacker de sombrero blanco. El hacker de sombrero gris no trabaja exactamente para su propio beneficio, ni siquiera para causar daño, pero a veces comete delitos y hace cosas que otros consideran poco éticas. En otras ocasiones, hacen algo que es ilegal pero al mismo tiempo ético.

Tratemos de explicar esto. Un hacker de sombrero negro es el tipo de persona que ingresa a un sistema informático sin obtener el permiso de alguien y luego roba los datos para obtener una ventaja personal o destruir el sistema. Un sombrero blanco pediría permiso, no probarían la seguridad del sistema hasta después de recibirlo, y no harían nada más que informar al

organización sobre la vulnerabilidad y cómo solucionarla.
Por otro lado, un hacker de sombrero gris normalmente no haría estas cosas.
Aunque no lo hicieron con fines maliciosos, de todos modos irrumpieron en un sistema sin permiso. En un extremo del espectro, un hacker de sombrero gris solo haría esto por diversión, y luego está mucho más cerca del sombrero negro que del sombrero blanco. Por otro lado, puede que lo hayan hecho para ayudar a la organización incluso sin permiso, en cuyo caso estarían mucho más cerca de sombrero blanco.

Cuando un hacker con sombrero gris descubre una enorme vulnerabilidad, es difícil adivinar lo que haría. Cualquier cosa entre simplemente no hacer nada y notificar inmediatamente a la empresa sería posible. Por otro lado, la respuesta, creo, revela públicamente la falla, por lo que la empresa tiene promedio
tiempo para arreglarlo, pero tampoco se molesta en contactarlos directamente.
Vale la pena señalar que todas estas cosas caen al agua cuando se hacen para beneficio personal. En ese caso, esto cae bajo el comportamiento de los sombreros negros. Incluso si la divulgación luego causa caos (porque un sombrero negro lo encontró) o ayuda a la empresa (porque un sombrero blanco lo encontró), eso no cambia el sombrero gris.

Ejemplo de hacker de sombrero gris

En agosto de 2013, Khalil Shreateh era un experto en seguridad informática desempleado.
Decidió que piratearía la página de Facebook de Mark Zuckerberg.
De, Mark Zuckerberg. Sorprendentemente, tuvo éxito. El CEO de Facebook se vio obligado a enfrentarse a algo que Khalil les venía contando desde hace tiempo.

La verdad era que Khalil había descubierto un error que permitía a las personas publicar en casi cualquier página sin su permiso. Intentó sin éxito informar a Facebook sobre esto. Después de escuchar repetidamente que esto no era un error, Khalil tomó el asunto en sus propias manos.

Khalil hackeó la página del CEO y señaló cuán problemático podría ser este error. Después de todo, los spammers maliciosos pueden usarlo para una variedad de cosas, y eso es solo la superficie de los posibles abusos que esto podría tener.
Después de que esto sucedió, Facebook finalmente decidió solucionar este problema, lo que podría haberles causado pérdidas millonarias. Desafortunadamente, Khalil no fue compensado por su trabajo del programa White Hat de Facebook por violar sus políticas para encontrar el problema.

Además de saber qué significan los términos, es importante tener en cuenta que las personas pueden tener múltiples funciones y que los términos se pueden usar para el comportamiento, no solo para las personas. Por ejemplo, alguien puede hacer ambas pruebas de penetración para una

empresa, mientras piratea maliciosamente a otra. Esto los convertiría en un hacker de sombrero blanco y negro.

El comportamiento es mucho más fácil de entender cuando se explica. De hecho, pregúntese: "Si alguien hiciera esto todos los días, ¿qué tipo de hacker consideraría?". Y ya tienes tu respuesta sobre qué tipo de hacker son.

Capítulo 5: Explicación del hacking ético

Cuando se trata de seguridad, ser un hacker es uno de los términos más utilizados. Aparece en todas partes, e incluso la industria del entretenimiento y muchos autores a menudo lo usan en sus películas, libros, programas de televisión y otros medios.

Por lo tanto, la palabra "hacker" suele verse como una mala profesión y siempre se asocia con una actividad delictiva oscura o real. Entonces, cuando las personas escuchan que alguien está involucrado en la piratería, inmediatamente ven a esa persona como alguien que no tiene buenas intenciones. Suelen presentarse como "operadores de las sombras", incluso antisociales. Por otro lado, también es visto como un activista social. Esta etiqueta se volvió especialmente popular después de algunas cosas como WikiLeaks. Muchos piratas informáticos participaron en la obtención de muchos documentos importantes de gobiernos, políticos y empresas que mostraban información muy diferente a la información que se brinda al público. Los grupos organizados como Anonymous o Lizard Squad también han tenido un gran impacto en la experiencia de piratería en los últimos años.

La evolución del hacking Al principio, el hacking apareció por curiosidad. Los entusiastas de la tecnología querían saber cómo funcionaban los sistemas y qué podían hacer con ellos. Hoy también tenemos muchos de esos a los que les gusta experimentar, ajustar y mejorar diseños originales. A principios de la década de 1970, los piratas informáticos eran en realidad personas a las que se podía encontrar en sus hogares al desarmar radios, las primeras computadoras y otros dispositivos de la época y descubrir cómo funcionaban. Este tipo de personas siguió el avance de la tecnología. Más tarde, en la década de 1980, cuando la PC era la mejor tecnología, los piratas informáticos se mudaron a ese entorno y comenzaron a participar en actividades aún más sospechosas, a menudo de manera maliciosa. La razón de esto también fue el hecho de que los ataques podían afectar a más sistemas, ya que cada vez más personas tenían PC. Cuando Internet se convirtió en una cosa en la década de 1990, todos los sistemas conectados también estaban interconectados. El resultado fue claro: la curiosidad mezclada con malas intenciones ahora estaba disponible en todo el mundo, y como era más fácil piratear diferentes sistemas informáticos, aparecieron más y más piratas informáticos.

A principios del siglo XXI, las computadoras ya no eran los únicos dispositivos que

podría ser pirateado. Mientras tanto, hemos comprado otras tecnologías, como teléfonos inteligentes, dispositivos Bluetooth, tabletas y muchas otras cosas a las que los piratas informáticos pueden apuntar. Es muy fácil. La tecnología no solo está evolucionando, sino también los hackers. Entonces, si el sistema es complicado, el ataque del hacker será más difícil de escapar. Y cuando Internet se convirtió en parte de todo lo que hacemos, se hizo más fácil acceder a diferentes tipos de datos. Los ataques de Internet de los primeros piratas informáticos en la década de 1990 estaban relacionados principalmente con la desfiguración de sitios web, y muchos de estos ataques cibernéticos se convirtieron en bromas, a veces divertidas e interesantes, pero a veces muy serias, incluso criminales. Comenzaron a ocurrir ataques más agresivos, como piratear sitios web de diferentes gobiernos, o algo con lo que probablemente esté más familiarizado: piratear sitios web de películas que resultó en muchos sitios web piratas que están activos incluso hoy.

Como mencionamos, los ataques cibernéticos se volvieron cada vez más comunes y maliciosos desde principios de la década de 2000. Además, estos ataques progresaron rápidamente. En ese entonces había actividades de piratería clasificadas como avances. Muchos de estos piratas informáticos tenían motivos delictivos y, aunque no podemos decir que haya una calificación estándar para ellos, los ubicaremos en varias categorías: • Hubo piratas informáticos que usaron sus habilidades para manipular los precios de las acciones, lo que causó muchas complicaciones financieras. Algunos de ellos han pirateado la información personal de las personas, robando la identidad • Uno de los ataques de piratas informáticos más comunes estuvo relacionado con el robo de tarjetas de crédito o el vandalismo en el ciberespacio • Como mencionamos anteriormente, la piratería también era muy común y en un momento incluso popular • El último, pero no menos importante, el tipo de ataque de piratería que generalmente surgió a principios de la década de 2000 fue una denegación de servicio y ataques de servicio.

Como sabe, la mayoría de las transacciones financieras se han realizado en línea en las últimas décadas, lo cual es un campo atractivo para los estafadores. Pero no solo eso, la apertura de los teléfonos móviles, portátiles, tabletas y dispositivos similares que usamos a diario también ha aumentado el espacio y cómo se puede robar todo tipo de información. Un número cada vez mayor de usuarios de Internet, usuarios de varios dispositivos y productos de software similares que conectan a las personas y sus dispositivos de múltiples maneras ha aumentado el número de personas interesadas en adquirir algunos de ellos.

Todas estas actividades traviesas a lo largo de los años han dado lugar a nuevas leyes en casi todos los países del mundo. Estas leyes surgen de la necesidad de tomar el control de la actividad criminal en el ciberespacio. Aunque el número de piratas informáticos en los sitios web

disminuyó, el cibercrimen organizado aumentó.

Ejemplos: ¿travesura o criminal?

La piratería no es un fenómeno que haya aparecido de la noche a la mañana. Existió en varias formas y evolucionó desde la década de 1960. Sin embargo, al principio nunca se abordó como una actividad delictiva. Veremos algunos casos que analizarán más de cerca algunos de los ataques y ejemplos genéricos que han cambiado gradualmente esa imagen.

Uno de los grupos de hackers más famosos del mundo, llamado "Anonymous", apareció en 2003. Fueron responsables de una serie de ataques contra sitios web gubernamentales y otras redes. También piratearon muchas agencias de noticias y otras organizaciones. Estos múltiples invasores exitosos los convirtieron en uno de los grupos ciberorganizados más activos de la historia. Curiosamente, todavía están activos y comprometidos con atacar objetivos de alto perfil.

Un nuevo virus informático fue descubierto a mediados de la década de 2000. El nombre de este virus era Stuxnet y tenía un diseño específico que solo atacaba los sistemas conectados a la producción de uranio. La característica única de este programa era el hecho de que ignoraba otros sistemas y atacaba solo si se cumplían los requisitos anteriores.

Otro caso interesante es el caso de una joven hacker rusa llamada Kristina Vladimirovna Scechinskaya que estuvo involucrada en un complot para defraudar a algunos de los bancos más grandes de Gran Bretaña y Estados Unidos. Todo comenzó en 2009 cuando utilizó el famoso virus "Caballo de Troya" para abrir miles de cuentas mientras atacaba a otras. La cantidad total de dinero que logró robar en la estafa fue de $ 3 mil millones. La llamaron la hacker más sexy del mundo, lo que ayudó a romper el estereotipo de los hackers como criaturas antisociales que viven en el sótano, etc.

Todos estos casos son algunos de los incidentes de piratería de alto perfil más famosos que han ocurrido, aunque es posible que algunos de ellos no hayan recibido tanta atención de los medios. De hecho, muchos de los casos de delitos cibernéticos que aparecen en las noticias siguen sin resolverse, pero muchos otros han tenido un gran impacto en varias industrias, pero nunca llegaron a las últimas noticias o fueron procesados por delitos cibernéticos.

Ahora que hemos revisado algunos incidentes concretos, enumeraremos algunas de las otras actividades que se consideran ciberdelincuencia. Los llamamos ejemplos genéricos, pero ten en cuenta que estos no son los únicos. Muchas otras formas pueden considerarse ilegales. • Acceder a servicios o recursos para los que no tiene permiso de uso. Esto es

generalmente llamado robo de nombres de usuario y contraseñas. En algunos casos, obtener esta información sin permiso se considera un delito cibernético, incluso si no la usa o como cuentas de amigos o familiares. • Existe una forma de delito digital denominada intrusión en la red que también se considera delito cibernético. En esencia, al igual que con las infracciones ordinarias, esto significa que usted fue a algún lugar sin permiso para entrar (o en este caso, acceder). Entonces, en caso de que alguien obtenga acceso a un sistema o grupo de sistemas sin permiso, podemos decir que la persona violó la red y, por lo tanto, cometió un delito cibernético. Sin embargo, algunas intrusiones en la red pueden tener lugar sin utilizar herramientas de piratas informáticos. A veces, iniciar sesión en cuentas de invitado sin permiso previo puede verse como un delito cibernético. • Una de las formas más complejas pero simples de piratería es perseguir al elemento más vulnerable del sistema: las personas. Este tipo de ciberdelincuencia se conoce como ingeniería social, y decimos que puede ser simple porque la persona es una parte del sistema mucho más accesible que cualquier otra, y es más fácil de tratar. Sin embargo, las personas pueden proporcionar pistas que son difíciles de entender, ya sea habladas o no, lo que dificulta que el hacker obtenga la información que necesita. • El problema de publicar o enviar material ilegal generalmente se ha vuelto difícil de abordar, especialmente en la última década. Las redes sociales recibieron mucha atención y muchos otros servicios relacionados con Internet aumentaron en uso y popularidad. Esto permitió que muchos materiales ilegales se movieran de un lugar a otro en el menor tiempo posible, lo que permitió que se propagara muy rápidamente. • El fraude también es común, especialmente en Internet, y también se considera un delito cibernético. Al igual que el término original, fraude en el ciberespacio también significa que una parte o partes generalmente han sido engañadas para obtener ganancias o daños financieros.

¿Qué significa ser un hacker ético?

Todo lo que mencionamos anteriormente en este capítulo se refería a los piratas informáticos en general. Sin embargo, el objetivo real es aprender a ser un hacker ético y explorar las habilidades que debe tener.

Los hackers éticos son personas que suelen ser empleadas por organizaciones para probar su seguridad. Suelen trabajar a través de empleo directo oa través de contratos temporales. La clave es que usan las mismas habilidades que todos los demás piratas informáticos, pero hay una gran diferencia: se les permite atacar el sistema directamente desde el propietario del sistema. Además, un hacker ético significa que revela las debilidades del sistema que ha evaluado (porque todos los sistemas del mundo las tienen) solo al propietario y a nadie más. Además,

Las organizaciones o personas que contratan a hackers éticos utilizan contratos muy estrictos que especifican qué partes del sistema están autorizadas para un ataque y cuáles están prohibidas. El papel de un hacker ético también depende del trabajo al que tiene derecho, es decir, de las necesidades del empleador. Hoy en día, algunas organizaciones tienen equipos de personal permanente y su trabajo es realizar actividades de piratería ética.

Los piratas informáticos se pueden dividir en 5 categorías. Tenga en cuenta que este formato puede variar, pero podemos decir que estos son los más comunes: • La primera categoría también se conoce como "Script Kiddies". Estos hackers no suelen tener formación ni hacer, pero muy limitados. Saben cómo usar solo algunas de las herramientas y técnicas básicas de piratería y, dado que no son lo suficientemente competentes, es posible que a veces no entiendan completamente sus actividades o las consecuencias de su trabajo. • La segunda categoría se refiere a los piratas informáticos conocidos como "piratas informáticos de sombrero blanco".
Atacan el sistema informático, pero son los buenos, lo que significa que no dañan su trabajo. Este tipo de hackers suelen ser hackers éticos, pero también pueden ser pentesters. • Los "hackers de sombrero gris" son la tercera categoría de piratas informáticos. Como su nombre indica, están entre el bien y el mal, pero su decisión final es elegir el lado correcto. Aún así, estos tipos de piratas informáticos luchan por ganarse la confianza porque pueden sospechar.
• La cuarta categoría que mencionamos en esta sección se denomina "piratas informáticos de sombrero negro". Esta categoría se refiere a los piratas informáticos que mencionamos anteriormente en este capítulo. Estas personas suelen trabajar del 'otro lado' de la ley y suelen estar asociadas con actividades delictivas. • Por último, pero no menos importante, están los "hackers suicidas". Se llaman así porque su objetivo es probar el punto, razón por la cual quieren eliminar a su objetivo. Estos piratas informáticos no tienen que preocuparse por ser atrapados, porque su objetivo no es esconderse, sino probar, para que sean más fáciles de encontrar.

Responsabilidades de un hacker ético Lo más importante que un hacker ético debe aprender y nunca olvidar es que siempre debe tener permiso para cualquier tipo de ataque al sistema.
El código ético que usted como hacker ético debe implementar en cada tarea dice que ninguna red o sistema debe ser probado o atacado si no es de su propiedad o si no tiene permiso para hacerlo. De lo contrario, puede ser declarado culpable de múltiples delitos que pueden haber ocurrido mientras tanto. Primero, puede dañar tu carrera, y segundo, si es algo realmente serio, puede incluso

amenazar su libertad.
Lo más inteligente es obtener un contrato de su empleador en el momento en que prueba o ataca el objetivo requerido. El contrato es una autorización por escrito, pero debe tener en cuenta que solo debe examinar las partes del sistema especificadas en ese contrato. Entonces, si su empleador quiere darle permiso para piratear partes adicionales del sistema o eliminar la autorización para algunas, primero debe cambiar el contrato y no debe continuar trabajando hasta que obtenga el nuevo permiso. Tenga en cuenta que lo único que distingue a un hacker ético de un ciberdelincuente es el contrato. Por ello, siempre debes prestar especial atención al vocabulario relacionado con cuestiones de privacidad y confidencialidad, ya que suele suceder que te encuentras con información íntima de tu cliente, tanto empresarial como personal.

Esa es una razón más por la que su contrato debe incluir con quién puede hablar sobre las cosas que encontró mientras investigaba el sistema y quién tiene prohibido escuchar sus actualizaciones. En general, los clientes suelen querer ser las únicas personas que saben todo lo que finalmente descubres.
Una organización conocida como EC Council (International Council of Electronic Commerce Consultants) es una de las organizaciones más importantes a la hora de regular estos temas. Según ellos, un hacker ético debe mantener privada toda la información obtenida en el trabajo y tratarla como confidencial. Esto se indica en particular para la información personal del cliente, lo que significa que no se le permite transferir, dar, vender, recopilar ni hacer nada de la información del cliente, como el número de seguro social, etc. -dirección de correo, dirección particular, única identificación, nombre, etc. La única forma en que puede proporcionar este tipo de información a un tercero es con un permiso por escrito de su empleador (cliente).

Si bien algunos pueden discutir sobre la distinción entre piratas informáticos y piratas informáticos éticos, la división es bastante simple: los piratas informáticos están separados por sus intenciones. Esto significa que aquellos que planean dañar y usan sus habilidades para acceder a datos sin permiso son etiquetados como sombreros negros, mientras que aquellos que trabajan con el permiso de sus clientes son considerados piratas informáticos de sombrero blanco. Nombrar estas dos categorías de "lo malo" y "lo bueno" puede ser controvertido, por lo que intentaremos seguir estas expresiones de la siguiente manera: • Los sombreros negros generalmente operan fuera de la ley, lo que significa que no tienen permiso del persona llamada "el cliente" para dar su consentimiento a sus actividades.

Por el contrario, los sombreros blancos tienen permiso y permiso de la persona.

llamado "cliente" e incluso mantienen la información que tienen entre el cliente y los sombreros blancos solamente.

Los sombreros grises, por el contrario, entran en ambas áreas y utilizan ambos tipos de acción en diferentes períodos.

Los hacktivistas son una categoría de hackers que no hemos mencionado antes.

Pertenecen al movimiento conocido como Hacktivismo, que se refiere a las acciones que utilizan los hackers para influir en el público en general mediante la promoción de una agenda política particular. Hasta ahora, los hacktivistas han estado involucrados con agencias, grandes empresas y gobiernos.

Código de conducta y ética del hacker Como cualquier otra profesión, el hacking tiene su Código de conducta que establece reglas que pueden ayudar a los clientes (individuos u organizaciones) a evaluar si la persona que interactúa con sus redes y sistemas informáticos es generalmente confiable. La organización que implementó este Código ya ha sido identificada en las secciones anteriores y se conoce como el Consejo de la CE.

Obtener una referencia CEH del Consejo de la CE significa que comprende completamente las expectativas que debe cumplir. Hemos proporcionado algunas partes del código, así que asegúrese de leerlo y familiarizarse con él. • La información que obtenga durante su trabajo profesional debe mantenerse confidencial y privada (especialmente la información personal) • A menos que tenga el permiso de su cliente, no puede dar, transferir ni vender la dirección, el nombre u otra información de identificación única del cliente. • Debe proteger la propiedad intelectual, la suya y la de otros, mediante el uso de habilidades que haya adquirido usted mismo para que todos los beneficios vayan al creador original. • Asegúrese de informar al personal autorizado sobre cualquier peligro que sospeche que pueda provenir de la comunidad de Internet, las transacciones electrónicas u otros indicadores de hardware y software. • Asegúrese de que los servicios que brinde estén dentro de su área de especialización para que trabaje con honestidad y sea consciente de cualquier limitación que pueda ser el resultado de su educación o experiencia. • Solo puede trabajar en proyectos para los que esté calificado y realizar tareas que coincidan con sus habilidades de capacitación, educación y experiencia laboral. • No debe utilizar a sabiendas software que se haya obtenido ilegalmente o que se haya almacenado de forma no ética. • No puede participar en prácticas financieras que puedan considerarse engañosas, como facturación doble, soborno, etc.

• Asegúrese de utilizar la propiedad del cliente correctamente, sin exceder los límites establecidos en su contrato. • Debe revelar un posible conflicto de intereses a todas las partes involucradas, especialmente si ese conflicto no se puede evitar. • Asegúrese de administrar todo el proyecto en el que está trabajando, incluidas las actividades de promoción y divulgación de riesgos.

Capítulo 6: Escanee su sistema

Hay varias formas de escanear su computadora. Sin embargo, es importante comprender que los diferentes escaneos persiguen diferentes tipos de datos y, por lo tanto, producen resultados diferentes. Por lo tanto, debe observar más de cerca el escaneo antes de comenzar dicho proceso. Los escaneos generalmente comparten un tema similar basado en la premisa de que el objetivo es recopilar información sobre uno o más hosts. Pero si profundiza, verá algunas diferencias en el camino. Cada escaneo proporciona una retroalimentación diferente sobre el tipo de datos que obtiene, por lo que cada escaneo es valioso a su manera. Para evitar complicaciones, usamos una categorización simple y decimos que hay tres categorías y todas tienen sus características específicas.

Escaneo de puertos

La primera categoría que mencionaremos es el escaneo de puertos. Este es un proceso de envío cuidadoso de paquetes o mensajes a la computadora a la que se dirige. El propósito de este escaneo es recopilar datos y estas sondas generalmente están conectadas a la cantidad de puertos o tipos menores o iguales a 1024. Si esta técnica se aplica con cuidado, hay muchas cosas que puede aprender sobre las posibilidades de un sistema que usted escanear ofertas para toda la red. Incluso puede encontrar diferencias entre sistemas como controladores de dominio, servidores web, servidores de correo, etc. durante el proceso. Uno de los escáneres de puerta más utilizados se conoce como tarjeta Fyodor. El escaneo de puertos es uno de los tipos de escaneo más utilizados y es común que otras personas asuman que está hablando de escaneo de puertos llamando al término "escanear".

Escaneo de red El

escaneo de red es la segunda categoría de escaneo que mencionaremos. Está especialmente diseñado para encontrar todos los hosts que están 'activos' en una red en particular, lo que significa que este escaneo encontrará todos los hosts que se están ejecutando actualmente en el sistema. Identificará qué sistemas pueden ser el objetivo o encontrará hosts que puedan continuar

exploración. Estos tipos de escaneos también se conocen como barridos de ping y pueden escanear el rango de direcciones IP muy rápidamente y luego determinar si un host está habilitado en la dirección. El ejemplo más común de un escaneo de red es Angry IP, pero se usan muchos más para lograr el mismo objetivo.

Exploración de vulnerabilidades La tercera categoría se conoce como exploración de vulnerabilidades y se utiliza para encontrar todas las debilidades del sistema previsto. La razón más común para usar este tipo de escaneo es si el cliente quiere medidas proactivas, especialmente si hay alguna duda de que alguien pueda atacarlo. El propósito de aquellos que desean un análisis de vulnerabilidades es comprender deliberadamente la situación sobre posibles problemas y actuar sobre ellos lo más rápido posible. Los escaneos de vulnerabilidad clásicos reciben información sobre puntos de acceso, hosts, puertos (especialmente los abiertos); analiza la respuesta de todos los servicios, genera informes y clasifica cualquier amenaza como una función muy importante. Son populares entre las grandes empresas porque se pueden utilizar para encontrar un fácil acceso al sistema.

Los dos escáneres de vulnerabilidades más utilizados son Rapid7 Nexpose y Tenable Nessus. Además, existen en el mercado muchos escáneres especializados y los más conocidos son Nikto, Burp Suite, WebInspect, etc.

Para evitar posibles malentendidos que puedan surgir con un hacker ético, debe saber la diferencia entre pruebas de penetración y vulnerabilidad. En primer lugar, un análisis de vulnerabilidades tiene como objetivo identificar las debilidades de un host o una red, pero no aprovecha las debilidades que encuentra. Por otro lado, las pruebas de penetración van un paso más allá y no solo pueden encontrar las mismas debilidades, sino que también las utilizan con el objetivo de averiguar hasta dónde podría llegar un atacante si las encontrara.

Probablemente te preguntes qué tipo de información genera una prueba de penetración. La respuesta no puede ser fácil; sin embargo, se pueden hacer algunas suposiciones generales. Al escanear un sistema, es muy probable que encuentre muchos conjuntos de datos diferentes. Podemos enumerarlos de la siguiente manera para que sea más fácil para usted: • Hosts en vivo de la red • Arquitectura del sistema • Puertos abiertos y cerrados e información que el host tiene sobre el sistema operativo (o más sistemas) • Procesos en ejecución en el host sistema • Tipo de debilidades del sistema y su nivel • Parches que tiene el sistema de destino • Información sobre la presencia de firewalls

• Enrutadores y sus direcciones, junto con otra información. Si observa
más de cerca, queda claro por qué muchas personas definen el análisis como un tipo de proceso de recopilación de información que pueden utilizar los atacantes reales. Si es lo suficientemente creativo y competente, puede realizar un escaneo exitoso.
Sin embargo, si se encuentra con un obstáculo mientras escanea, sus habilidades deberían entrar y ver cuál será su próximo movimiento. Tenga en cuenta que una vez que haya recopilado la información, llevará algún tiempo analizarla, y eso también depende de qué tan bueno sea para leer los resultados que le dio el escaneo. Cuanto más conocimiento tenga, más fácil será descifrar los resultados.

Verificación del sistema

en vivo Comencemos por encontrar los objetivos que investigaría e investigaría. Tenga en cuenta que aunque haya obtenido información sobre el rango de IP o IP propiedad de su cliente (individuo u organización), esto no significa que cada una de esas direcciones IP tenga un host conectado. Lo primero que debe hacer si desea lograr un progreso significativo es averiguar qué "pulsos" son reales y cuáles no y, por lo tanto, qué direcciones IP tienen hosts. La pregunta es, ¿cómo va a verificar si hay sistemas activos en el entorno al que se dirige? La respuesta es bastante simple. Esto puede hacerse de muchas maneras.

Aún así, los más utilizados son el escaneo de puertos, la marcación de guerra, el ping y el wardriving. Cada una de estas técnicas tiene su propio valor porque todas proporcionan cierta información que es exclusiva de sus diseños. Una vez que los conozca, comprenderá cómo funcionan y qué diferencias tienen, y será más fácil implementar el que más necesita para una prueba de penetración.

Marcación de

guerra La marcación de guerra es una forma antigua pero conveniente de escanear el sistema. Prácticamente no cambió desde la década de 1980 y la razón por la que todavía se usa hoy en día es porque ha demostrado ser una de las herramientas más confiables y útiles para recopilar información. En la práctica, esta técnica es bastante simple en comparación con otras formas de escaneo. La marcación de guerra funciona según el principio de marcar un bloque con diferentes números de teléfono mientras se usan módems estándar. Una vez que el escaneo ha marcado los números, puede determinar las ubicaciones de los sistemas a los que también está conectado su módem y aceptar esas conexiones. A primera vista, puede parecer un mecanismo anticuado, pero es más que útil en múltiples niveles.
Lo que es más importante, los módems todavía se usan ampliamente porque son asequibles y tienen buenas líneas telefónicas que están básicamente en todas partes.
Una de las razones por las que los módems todavía se usan hoy en día es que respaldan la

tecnologías existentes. Entonces, si fallan otras opciones de conectividad, las líneas telefónicas están disponibles para evitar cortes importantes. Para las empresas, es una buena oferta porque es asequible y brinda algún tipo de seguridad en caso de que suceda algo realmente grande.

Entonces, la siguiente pregunta es qué sucede cuando encuentras un módem. Primero, debe estar familiarizado con los dispositivos que a menudo están conectados a módems en la actualidad. Por ejemplo, las PBX (Private Branch Exchanges) a menudo están vinculadas a modos no digitales. Estos tipos de módems son buenos para diferentes tipos de travesuras de un atacante. Sin embargo, algunos módems tienen cortafuegos o máquinas de fax, enrutadores, etc. Entonces, cuando los atacantes obtienen acceso a través de un firewall, el entorno del dispositivo no está protegido por mucho tiempo. Los puntos de pivote deben tenerse en cuenta al abrir el sistema. Los puntos de pivote son sistemas que están comprometidos y luego se utilizan para atacar otros sistemas, lo que hace que su entorno sea inseguro. A lo largo de los años, se han creado muchos programas como programas de marcación de guerra. Los más conocidos son: v Tone Loc, un programa basado en la búsqueda de tonos de marcación eligiendo números aleatorios que estén al alcance de un atacante. Este programa también puede buscar la frecuencia portadora de un módem. Se requiere la entrada con códigos de área y rangos de números a los que un atacante quiere llamar.

PhoneSweep de Niksun, un programa que representa una de las pocas opciones comercialmente disponibles en el mercado.

THC-SCAN ADOS, un programa basado en marcar números de teléfono con módems y busca una frecuencia portadora de ese módem.

Silbido

Otra herramienta de escaneo comúnmente utilizada es ping. Ping se utiliza para determinar la conectividad de una red determinando si el host remoto está activo o inactivo. Si bien es una característica bastante simple, sigue siendo muy eficiente para el proceso de escaneo inicial. Ping se basa en mensajes del Protocolo de mensajes de control de Internet (ICMP), por lo que este tipo de exploración también se conoce como exploración ICMP. Es simple. Un sistema envía un eco (en este caso, un eco ICMP) a otro sistema y, si está activo, responderá enviando otro eco ICMP como respuesta. Cuando el sistema inicial recibe esta respuesta, confirma que el objetivo está activo o activo.

Ping no solo le dice si el objetivo está vivo, sino que también obtiene información sobre la velocidad de los paquetes objetivo y los datos TTL (tiempo de vida). Para usar ping en Windows, simplemente ingrese el siguiente mensaje: ping o ping. Las versiones de Linux usan el mismo comando, pero el comando hace ping constantemente al objetivo a menos que

presionas ctrl + c para detener el proceso.
Si bien puede usar ping para acceder a nombres de host y direcciones IP, le recomendamos que haga ping por dirección IP en lugar de la técnica del nombre de host, ya que el nombre de host inactivo puede significar un problema de DNS en lugar de un sistema no disponible. Tenga en cuenta que si tiene un sistema de ping, lo hará y no recibirá ninguna respuesta, aunque sabe que el sistema de destino está funcionando, es posible que el sistema de destino tenga un servicio de ping deshabilitado. Si eso es cierto, no recibirá ninguna respuesta de ese tipo de sistema.

Consultar puertos y su estado

Cuando localice los sistemas activos de la red, el siguiente paso es volver a mirar los hosts. El objetivo es determinar si tienen puertos abiertos o no.
En general, acérquese a cualquier host en vivo que haya encontrado antes y examine los puertos para determinar si alguno de ellos está abierto. Sin embargo, en esta etapa solo puede ver si hay puertas abiertas o cerradas, pero no hay nada que pueda hacer al respecto porque esa función avanzada se encuentra en algunas secciones más avanzadas.

Recuerde que conocer las puertas y los escaneos de puertas es una de las habilidades esenciales para la piratería ética y cuando investigue diferentes tipos de escaneos de puertas, sabrá en qué situaciones prefiere uno sobre el otro. Presta atención a los detalles, porque al final del día, estudiar es la mejor manera de mejorar tus habilidades.

Capítulo 7: Pruebas de penetración

Las pruebas de penetración, también conocidas como pruebas de penetración, son una de las principales actividades de los hackers éticos. Una prueba de penetración también se conoce como ataque de sombrero blanco porque la realiza un hacker de sombrero blanco para ayudar al propietario del sistema. Es un proceso de detección de vulnerabilidades en aplicaciones, redes y sistemas que podrían ser explotados por usuarios maliciosos que intentan ingresar al sistema. El proceso se puede realizar manualmente, pero también se puede automatizar utilizando otras aplicaciones. Independientemente de cómo lo haga, el objetivo del proceso siempre sigue siendo el mismo. Primero, recopile tanta información sobre el objetivo como sea posible antes de comenzar la prueba. Esto se reduce a encontrar puntos de acceso y tratar de ingresar al sistema, además de recopilar los hallazgos en un documento.

No importa cómo enfoque el proceso, el objetivo siempre es el mismo: encontrar debilidades en la seguridad de un sistema. Esto se suele hacer de forma digital, pero también puede ser en la parte física de la seguridad informática. Como sabes, hay

son métodos de piratería que utilizan el personal para ingresar al sistema. Las pruebas de penetración se pueden usar para probar cuántos empleados conocen la política de seguridad y qué tan rápido una organización puede reconocer una amenaza.
Después de identificar las debilidades explotables de un sistema, el hacker ético notifica a los administradores de sistemas de red y TI de la organización. En base a esto, estos expertos pueden tomar medidas para ayudar a proteger sus sistemas y desplegar los recursos necesarios.

El propósito de las pruebas de penetración El propósito principal de una prueba de penetración es averiguar si el sistema contiene vulnerabilidades que pueden explotarse para desestabilizar la seguridad del sistema, para ver si la seguridad está a la altura y para probar qué tan bien saben los empleados de una empresa. los problemas de seguridad. Esto se hace para determinar cómo se vería afectada la organización por una posible intrusión y cómo se pueden remediar las vulnerabilidades.

Esto también puede conducir a que se descubran errores en la política de seguridad de una empresa. Por ejemplo, algunas empresas tienen muchas políticas con respecto a la detección y prevención de un ataque de piratería, pero no saben cómo eliminar al hacker.

Responsabilidades de las pruebas de penetración en la nube En algunas redes, puede encontrar diferentes combinaciones de sistemas locales y sistemas en la nube. Esto significa que las responsabilidades de las pruebas de penetración varían entre las diferentes redes.
Ya hemos mencionado la importancia de los informes en las pruebas de penetración.
Por lo general, brindarán a la empresa una gran cantidad de información útil sobre su sistema de seguridad y los ayudarán a priorizar las mejoras del sistema de seguridad que habían planeado. Estos informes brindan a los desarrolladores de aplicaciones el incentivo para crear aplicaciones más seguras. Al comprender cómo los piratas informáticos ingresan a sus aplicaciones, los desarrolladores pueden educarlos más sobre cómo hacer que sus proyectos futuros sean más seguros para que vulnerabilidades similares nunca vuelvan a aparecer.

¿Con qué frecuencia debe realizar pruebas de penetración?

Por lo general, las empresas hacen esto regularmente. Esto generalmente se hace una vez al año. Cuanto más a menudo realizan pruebas de penetración, más eficiente se vuelve el trabajo de seguridad y administración de TI. Además de las pruebas de penetración que se realizan regularmente, las empresas también lo hacen cuando: - La empresa agrega una nueva infraestructura o aplicación a su sistema - La empresa realiza cambios importantes en su sistema - La empresa agrega nuevas oficinas en una ubicación diferente - La empresa está agregando nuevos parches de seguridad

- La empresa cambia su política de seguridad Sin
embargo, debe tener en cuenta que las pruebas de penetración no son las mismas para todas las empresas. El funcionamiento de la prueba de penetración depende de muchos factores, como: • ¿Qué tamaño tiene la empresa? Cuanto mayor sea la presencia de una empresa, más probable es que sea atacada por un pirata informático porque tienen más enfoques de ataque y pagos más jugosos. • ¿Cuánto dinero puede dar la empresa para las pruebas de penetración? Las empresas más pequeñas no siempre pueden permitirse realizarlas anualmente, porque el proceso puede costar bastante dinero. Solo las empresas más lucrativas lo hacen anualmente, mientras que las más pequeñas lo hacen cada dos años.

¿Que dice la ley? En algunas industrias, existen leyes que obligan a las empresas a realizar tareas de seguridad. • Algunas empresas tienen su infraestructura en la nube. En ocasiones estas empresas no pueden realizar sus propias pruebas de penetración y la responsabilidad recae en el propio proveedor.

Cada empresa tiene diferentes necesidades cuando se trata de pruebas de penetración. Esta es la razón por la cual los hackers de sombrero blanco deben ser muy flexibles cuando se trata de pruebas de penetración, porque sus esfuerzos serán más eficientes si las pruebas de penetración que realizan se adaptan a la empresa para la que trabajan. Después de cada prueba de penetración, se recomienda realizar una serie de pruebas de seguimiento para garantizar que los resultados se anoten en las pruebas de penetración que aún no se han realizado.
venir.

Herramientas de prueba de

penetración Las pruebas de penetración se pueden automatizar debido a la cantidad de herramientas disponibles en la actualidad. Los pentesters suelen utilizar estas herramientas para escanear rápidamente el sistema en busca de vulnerabilidades comunes. Se utilizan para escanear código para encontrar componentes maliciosos que pueden usarse para romper el sistema. Encuentran vulnerabilidades en el sistema examinando técnicas de encriptación y valores codificados.

Estrategias de prueba de penetración

Cada vez que un hacker de sombrero blanco se acerca a una prueba de penetración, siempre debe determinar el alcance en el que operará. Esto generalmente le dice al evaluador a qué partes del sistema acceder, así como qué herramientas y técnicas usar mientras trabaja. Esto ayuda a asignar recursos y mano de obra de manera más eficiente mientras se realiza una prueba de penetración.
Si un probador de penetración contratado por la empresa obtiene acceso al sistema porque encontró la contraseña de un empleado a simple vista, le dice al equipo de seguridad que faltan las prácticas de seguridad del empleado y muestra dónde se pueden mejorar.

hay que hacer.

Hay muchas estrategias que los evaluadores de penetración utilizan con relativa frecuencia: • Pruebas dirigidas El equipo de TI de la empresa suele ser responsable de las pruebas dirigidas. Para ello trabajan en conjunto con los probadores de penetración. Este enfoque también se conoce como el enfoque de "luces encendidas" porque todos tienen acceso a los resultados y el rendimiento de esta prueba. • Pruebas externas Las pruebas externas se realizan para encontrar puntos débiles en las partes del sistema que son visibles desde el exterior. Esto incluye cortafuegos, servidores web, servidores de correo electrónico y nombres de dominio. El propósito de este tipo de prueba de penetración es averiguar si esa parte del sistema se puede utilizar para acceder a las partes más profundas del sistema y hasta dónde puede llegar el hacker durante ese ataque. • Pruebas internas Un ataque que se ejecuta durante las pruebas internas comienza detrás del firewall y lo realiza un usuario con derechos de acceso estándar. Esto generalmente se hace para ver hasta qué punto un empleado de la empresa puede causar daños con intenciones maliciosas. • Pruebas ciegas Pruebas ciegas tiene este nombre porque la información disponible para el probador es muy limitada porque se creó para determinar qué tipo de ruta recorrería rápidamente un verdadero atacante. Estos probadores se utilizan para imitar un ataque total real que una persona malintencionada cometería desde fuera de la empresa y no reciben casi nada más que el nombre de la empresa que los contrata. Este tipo de pruebas pueden tomar bastante tiempo debido al tiempo que el pirata informático necesita para encontrar dónde puede acceder al sistema, lo que lo convierte en un centavo. • Doble ciego Este es un paso adelante en la prueba ciega. La prueba doble ciego es un tipo de prueba en la que solo unas pocas personas dentro de la organización saben que se está realizando la prueba. A los empleados no se les dice dónde o cuándo tendrá lugar el ataque o quién lo llevará a cabo. Este tipo de prueba es muy útil porque proporciona una visión muy útil del seguimiento de la seguridad de la organización, así como de la eficiencia con la que los empleados realizan los procedimientos instruidos. • Prueba de caja negra Esta prueba de penetración requiere que el evaluador no tenga información sobre el objetivo. Es otra variante de la prueba a ciegas. Se le indica al probador que se comporte

como un atacante real y debe encontrar su propio punto de entrada y deducir qué técnicas y herramientas usar para la tarea. • Prueba de caja blanca Las pruebas de caja blanca les brindan a los evaluadores una buena comprensión de la información importante sobre el sistema de la empresa que contrataron para atacar. Esta información puede ir desde las direcciones IP hasta el código fuente y los diagramas de infraestructura. La información facilitada puede ser flexible en función de las necesidades de la empresa.

Es importante que cualquier equipo de pruebas de penetración use diferentes tipos de pruebas para encontrar cualquier debilidad que pueda encontrar. Esto, a su vez, les indica qué tipos de ataques pueden causar más daño al sistema.

El uso de diferentes estrategias de pruebas de penetración ayuda a los equipos de pruebas de penetración a centrarse en los sistemas que desean y comprender los tipos de ataques que son más amenazantes.

Pruebas de penetración de aplicaciones basadas en la nube

Como mencioné anteriormente, con el crecimiento del almacenamiento en la nube, muchas empresas han trasladado su infraestructura del almacenamiento local al almacenamiento en la nube. Debido a la forma en que funcionaba la nube, los hackers de sombrero blanco tuvieron que desarrollar nuevas técnicas y descubrir algunos ángulos nuevos e interesantes al abordar las pruebas de penetración. El problema con las aplicaciones que se ejecutan en la nube es el hecho de que existen varios obstáculos cuando se trata de pruebas de penetración. Cuando desee verificar la seguridad de la aplicación, pueden surgir problemas tanto legales como técnicos.

Así es como, como principiante, puede abordar la piratería de sombrero blanco en la nube.

Paso 1: asegúrese de comprender cómo funciona la política del proveedor de la nube Como sabemos, existen nubes públicas y privadas. Hoy nos centraremos en el lado público, ya que tienen sus propias políticas en lo que respecta a las pruebas de penetración. Un hacker de sombrero blanco siempre debe esperar la confirmación del proveedor antes de realizar la prueba. Esto impone muchas limitaciones a lo que se puede hacer como parte del proceso. Para ser precisos, cuando desea probar una aplicación que se ejecuta en una nube pública, debe investigar mucho sobre qué técnicas recomienda y permite el proveedor. Si no sigue los procedimientos establecidos por el proveedor, puede tener muchos problemas. Por ejemplo, su prueba a veces puede parecer un ataque real, lo que puede llevar a que su cuenta se cierre de forma permanente.

Cada desviación en una nube es notada por el proveedor, que está constantemente buscando desviaciones. A veces alguien te llamará para comprobar lo que está

pasando Sin embargo, lo más frecuente es que se enfrente a una serie de procedimientos automatizados que cierran el sistema si sus acciones se consideran un ataque.
Esto puede conducir a varias cosas malas, como el hecho de que todos sus sistemas y datos almacenados en la nube se desconecten y tenga que explicarle muchas cosas a su proveedor antes de que lo vuelvan a poner en línea.
Otra cosa que puede pasar si haces tus pruebas de penetración de forma irresponsable es que te arriesgues a influir en otros usuarios. Siempre puede cargar los recursos utilizados por otros usuarios durante las pruebas de penetración. Este es un problema con las nubes públicas, ya que siempre hay varios usuarios activos, por lo que no se puede asignar todo el sistema a un solo usuario. Esto también puede generar indignación con el proveedor. Es posible que lo llamen de una manera no tan amigable o simplemente cierren su cuenta.
Para resumir, hay reglas cuando quieres husmear en las nubes públicas. Debe tener en cuenta los requisitos legales junto con todos los procedimientos y políticas que el proveedor le indique. Si no haces esto, tendrás algunos dolores de cabeza.

Paso 2: venga con un plan Cuando
desee realizar una prueba de penetración en una nube, debe enviar un plan. En su plan, debe cubrir lo siguiente: • Aplicación(es): familiarizarse con las API y las interfaces de usuario • Acceso a datos: comprender cómo responderán los datos a la prueba Acceso a la red: comprender cómo el sistema protege los datos y la aplicación Virtualización: Asegúrese de medir cómo las máquinas virtuales manejan su carga de trabajo • Cumplimiento: Conozca las regulaciones y leyes que debe observar al realizar la prueba de penetración. • Automatización: seleccione qué herramientas desea usar mientras realiza las pruebas de penetración. • Enfoque: vea qué administradores involucrará en la prueba de penetración. Hay ventajas en no notificar a los administradores. Esto proporciona información sobre cómo reaccionarían los administradores durante un ataque real. Este enfoque es muy criticado por la mayoría de los administradores.

Si trabaja en equipo, planifique el enfoque con el resto del equipo y asegúrese de que todos sigan cada parte del plan. Todo el equipo debe asegurarse de que no se desvíe de él, ya que esto podría hacer que todos sus esfuerzos se desperdicien porque el administrador eliminó su acceso al sistema.

Paso 3: Elige qué herramientas usarás

El mercado le ofrece muchas herramientas que se pueden utilizar en las pruebas de penetración. En el pasado, las pruebas de lápiz en la nube se realizaban con herramientas locales. Recientemente, sin embargo, se han creado muchas herramientas que se utilizan específicamente para probar bolígrafos en la nube y demostrarán ser una opción más económica. Otra ventaja de estas herramientas es el hecho de que dejan una pequeña huella de hardware.
Lo que necesita saber acerca de estas herramientas es el hecho de que simulan ataques reales. Hay muchos procesos automatizados que pueden detectar vulnerabilidades en un sistema. Los piratas informáticos han realizado actividades automatizadas, como adivinar contraseñas y buscar API para ingresar a un sistema. Es su trabajo simular estas actividades.

A veces, estas herramientas no pueden hacer todo lo que necesita que hagan. Su último recurso suele ser escribir su propio sistema de penetración. Esto siempre debe evitarse tanto como sea posible, ya que puede traerte un poco de vuelta.

Paso 4: Observa la respuesta

Al realizar una prueba de penetración, debe prestar mucha atención a: • Respuesta humana: cuando se trata de pruebas de penetración en la nube, siempre realice un seguimiento de cómo los administradores y los usuarios responderán a su prueba. Muchos apagarán el sistema inmediatamente para evitar daños al sistema.
Otros administradores primero intentan diagnosticar la situación para identificar la amenaza y la solución a algo similar. También debe vigilar de cerca cómo responde la gente a su proveedor de atención al cliente. • Respuesta automática: lo primero que debe observar es cómo responderá el sistema a su prueba de penetración. El sistema de té lo reconocerá y le responderá. Estas respuestas pueden variar desde bloquear una dirección IP hasta apagar todo el sistema. De cualquier manera, debe alertar a los administradores responsables de las aplicaciones y la seguridad para ver qué acciones han tomado y qué ha sucedido en sus áreas.

Ambas respuestas deben estar documentadas. Una vez que documente y considere sus hallazgos, finalmente verá dónde están las debilidades del sistema y qué tan seguro es el sistema.

Paso 5: busque y elimine vulnerabilidades El producto final de las pruebas de penetración es una lista de vulnerabilidades que anotó el equipo. Puede haber muchos problemas, mientras que a veces hay pocos o ninguno.
Si no encuentra uno, es posible que deba realizar otra prueba para volver a evaluar los resultados de la anterior.
Las vulnerabilidades que puede encontrar en las pruebas de penetración de aplicaciones en la nube generalmente se ven así:

Acceso a los datos de la aplicación permitido con la API xxxxx. • Acceso a la API otorgado después de 20 intentos. • Generador de contraseñas detectado al acceder a una aplicación. • El cifrado no cumple con la normativa.

Los problemas casi siempre diferirán según la aplicación que esté probando y el tipo de prueba que haya realizado.
No olvides que hay varias capas para probar. Todos los componentes, como la red, el sistema de almacenamiento, la base de datos, etc., se prueban por separado. Los problemas, a su vez, también se informan por separado. Siempre debe realizar una prueba con todas las capas juntas para ver cómo interactúan. Siempre es aconsejable informar lo que sucedió en cada capa.

Debe mantener a su proveedor de la nube involucrado en cada paso del camino para evitar cualquier política o problema legal que pueda surgir de su prueba de penetración. Esto también lo ayuda a determinar qué enfoque es óptimo y cómo debe aplicarse a las diferentes aplicaciones. La mayoría de los proveedores tienen mejores prácticas que brindan los resultados más precisos en sus redes.

Consejos generales sobre Cloud Pen Testing Otra cosa a tener en cuenta es quién está en el equipo de penetración. Si hace esto internamente, siempre debe asumir que no se ha encontrado todo.
Los equipos de prueba que provienen de la empresa suelen dejar cierto margen para la supervisión. Saben demasiado sobre las aplicaciones desde el principio y siempre pueden pasar por alto cosas que creen que no vale la pena mirar. Los hackers de sombrero blanco son el método más seguro, aunque un poco más caro. Buscarán en su sistema de manera más eficiente y detallada.

Siempre consulte con su proveedor para ver qué prácticas son más eficientes, qué aplicaciones probar y los requisitos que se deben cumplir con la prueba de penetración.
El uso de enfoques probados suele ser una buena manera de comenzar.
Las pruebas de penetración son ahora más importantes que nunca. Es la única forma de asegurarse de que las cosas que tiene en la nube sean lo más seguras posible para acomodar a la mayor cantidad de usuarios posible.
Las pruebas de penetración no son una opción en estos días. Es la única forma de demostrar que sus aplicaciones y datos basados en la nube son lo suficientemente seguros como para permitir el máximo acceso de los usuarios con un riesgo mínimo.

¿Cómo se pueden comparar la seguridad local y la seguridad en la nube?

Esta es una gran pregunta para muchas personas. Las personas a menudo descartan la nube e inmediatamente asumen que almacenar sus datos en servidores dentro de una oficina es la opción más segura. Este suele ser el caso porque usted posee el hardware y

software cuando almacena sus datos en la ubicación. Sin embargo, esto puede ser una desventaja porque algunos de los mejores proveedores de la nube pueden brindarle mucha seguridad que es posible que no obtenga en el acto.

Para ser claros, el sistema en la nube es impresionante porque fue creado para brindar una durabilidad del 99,99 por ciento y hacer que todo lo disponible esté siempre disponible.

Este tipo de disponibilidad no se puede replicar localmente debido a las limitaciones del hardware y el software disponibles para usted. Recrear estos resultados requeriría una gran inversión y un gran número de personas.

Antes de decidir rápidamente qué opción elegir, hay muchas cosas que considerar. Debe considerar su presupuesto y el tamaño de su equipo de seguridad. Si parece que falta su respuesta, recuerde que los proveedores de la nube tienen grandes equipos que manejarán estas cosas por usted y tienen sistemas automatizados que protegen constantemente el sistema.

Para resumir, las empresas de la nube han invertido mucho tiempo y dinero en la creación de sus sistemas y eso los hace mucho más confiables.

Capítulo 8: Herramientas de seguridad más comunes El mercado de herramientas de seguridad es tan grande como el campo mismo. Separar los cientos de herramientas diferentes ayuda a dividirlas en diferentes categorías.

La primera categoría son los administradores de eventos. Estas herramientas responden a eventos que ocurren en las redes que monitorea. Analizan los registros en sus sistemas para detectar estos eventos.

Otra herramienta útil son los rastreadores de paquetes que le permiten decodificar paquetes mientras investiga el tráfico para escanear su carga. Los rastreadores de paquetes se utilizan cuando profundiza en los eventos de seguridad que ocurren.

Los sistemas de detección y prevención de intrusiones son otra categoría útil de herramientas. Pueden parecer cortafuegos y antivirus, pero difieren mucho en su función. Cuando se trata de este software, siempre debe considerarlo como un perímetro alrededor de su red que está ahí para detectar actividades ilícitas.

Por supuesto, no todas las herramientas se pueden categorizar por lo específicas que son en lo que respecta a su función y diseño. Sin embargo, pueden ser muy útiles para muchas situaciones diferentes.

Es muy difícil determinar qué herramientas son mejores que otras en diferentes categorías debido a los diferentes propósitos que pueden tener. La mayoría de las herramientas de las que estamos hablando son muy diferentes entre sí y nunca puedes

decir que uno es absolutamente mejor que el otro. Esto significa que es difícil seleccionar herramientas para cada trabajo diferente, pero aquí hay algunas herramientas de uso común que siempre debe tener en cuenta al realizar un trabajo.

SolarWinds Log and Event Manager Es posible que nunca haya oído hablar de SolarWinds, pero debe escuchar con atención ahora. Esta empresa ha creado una gran cantidad de útiles herramientas de gestión durante varios años. En el mercado de colectores y analizadores NetFlow, NetFlow Traffic Analyzer de SolarWinds es una herramienta popular. Otra gran herramienta que SolarWinds nos ha brindado es Network Performance Monitor, que es una de las mejores del mercado para herramientas de monitoreo de redes SNMP. En resumen, lo que necesita saber sobre SolarWinds es que ofrecen una amplia variedad de herramientas gratuitas que puede usar para diferentes tareas y que pueden cumplir muchos roles diferentes que puede estar tratando de cumplir usted mismo. Los administradores de redes y sistemas a menudo agradecen a SolarWinds por ser una gran fuente de herramientas útiles.

Captura de pantalla de SolarWinds Log and Event Manager Hablando de SolarWinds, es difícil ignorar algunas de sus piezas de software más importantes. Si está buscando herramientas de seguridad de red, querrá consultar el LEM, abreviatura de Log and Event Manager. Esta es una opción fácil si está buscando un sistema de seguridad y gestión de eventos que sea muy fácil de usar para principiantes. Esta es la herramienta con la que desea comenzar. En el mercado SIEM de nivel de entrada, esta es posiblemente la opción más competitiva. Cuando se trata de SolarWinds, puede esperar obtener todo lo que tendría cada sistema base y algo más. SolarWinds LEM tiene una excelente función de administración de registros y funciona con un motor impresionante.

El LEM también le ofrece impresionantes funciones de respuesta. Detecta amenazas en tiempo real y es muy confiable en lo que hace. La herramienta funciona muy bien cuando intenta protegerse de las vulnerabilidades y amenazas de día cero que no conoce, ya que no se basa en la creación de firmas. Comportamiento es lo que busca esta herramienta. Rara vez necesita actualizarlo. Uno de los mejores activos del LEM es el tablero. El sistema es muy simple y agiliza el trabajo de encontrar anomalías y reportarlas.

Si desea comprar el LEM de SolarWinds, debe estar dispuesto a pagar $ 4,585. Si no está seguro de la compra, siempre existe la prueba de 30 días que ofrece la compañía.

Administrador de configuración de red de SolarWinds

El LEM no es la única pieza impresionante de software que SolarWinds puede

presumir. Tienen varias otras herramientas que se centran en la seguridad de la red. Uno es su administrador de configuración de red, que se usa para monitorear su equipo y garantizar que todo esté configurado según ciertos estándares.
Lo que hace por su seguridad es que detecta cambios no autorizados en su sistema. Esto es útil porque estos cambios pueden ser una buena señal de un próximo ataque.

La función principal de este software es ayudarlo a recuperarse restaurando su sistema a las últimas configuraciones autorizadas. También resalta los cambios y guarda la información en un archivo de configuración. Otra cosa con la que te ayuda es el cumplimiento. Le ayuda a pasar auditorías debido a los informes estandarizados que crea en el trabajo.

El Network Configuration Manager tiene un precio de 2.895 dólares. El precio puede cambiar según los nodos administrados que seleccione. Este software, al igual que el anterior, viene con una prueba de 30 días si no estás seguro de querer comprarlo.

Rastreador de dispositivos de usuario de SolarWinds

Esta es otra de las grandes herramientas que ofrece SolarWinds. Es una gran herramienta que todo aquel que trabaje en seguridad informática debería tener. Realiza un seguimiento de los dispositivos de punto final y los usuarios para mejorar su seguridad. Puede usarlo para identificar qué puertos se están utilizando y cuáles están disponibles.
Esta herramienta es excelente en situaciones en las que espera un ataque con un objetivo específico. Las herramientas lo ayudan a identificar al usuario con actividad sospechosa.
Las búsquedas realizadas a través de este software se basan en nombre de usuario, direcciones IP/MAC y nombres de host. La búsqueda puede ser un poco más profunda e incluso llegar a escanear conexiones anteriores del sospechoso.
El precio inicial del User Device Tracker comienza en US $ 1,895. Cambia nuevamente según la cantidad de puertos que el sistema tiene que rastrear. Al igual que los programas anteriores, también viene con un período de prueba de 30 días.

Wireshark

Hablando de Wireshark, sería un insulto decir que es solo una herramienta de seguridad. Esta herramienta es muy popular y se utiliza. Es aclamado como uno de los mejores paquetes de captura y análisis. Esta herramienta se utiliza para analizar a fondo el tráfico de la red. Puede capturar y descifrar cualquier paquete para que pueda inspeccionar los datos que contiene.

Wireshark ha construido una gran reputación. Debido a la calidad del servicio que ofrece, se ha convertido prácticamente en el estándar para las demás herramientas del mercado. La competencia siempre trata de emularlo en la medida de lo posible. Muchos administradores utilizan Wireshark para comprobar las grabaciones obtenidas a través de

otro software. Esto se ha hecho tantas veces que las versiones más nuevas del software le permiten ejecutar un archivo de captura al configurar que ya tiene que pasar por el tráfico de inmediato. Donde la herramienta sobresale más son los filtros que vienen con ella. Son una gran adición, ya que lo ayudan a identificar los datos exactos que son relevantes para usted.

Es difícil acostumbrarse al software. Hay cursos que duran varios días y dan instrucciones de cómo usarlos. Sin embargo, vale la pena aprender a usar Wireshark. Es una herramienta extremadamente valiosa para cualquier administrador. La herramienta es gratuita y se puede utilizar en la mayoría de los sistemas operativos.
Puedes conseguir uno tú mismo en el sitio web oficial.

Nessus Professional Entre las soluciones para identificar malware, problemas y vulnerabilidades, Nessus Professional es una de las más utilizadas. Millones de profesionales usan Nessus Professional debido a la vista externa que les ofrece. También le brinda una gran perspectiva sobre cómo mejorar la seguridad de su sistema.
Nessus Professional ofrece una de las coberturas más amplias cuando se trata de amenazas. Utiliza mucha inteligencia impresionante y es muy fácil de usar. El software también se actualiza con bastante frecuencia, lo que significa que nunca tendrá problemas con problemas nunca antes vistos. Tiene un paquete bastante completo cuando se trata de escaneo de vulnerabilidades.
Si desea utilizar los servicios de Nessus Professional, debe pagar $ 2,190 por año. Si no está seguro de la inversión, puede utilizar el período de prueba de 7 días.

oler

Entre los IDS de código abierto, Snort se destaca entre los mejores. Este sistema de detección de intrusos se creó en 1998. Se convirtió en propiedad del sistema Cisco en 2013. Snort ingresó al Salón de la Fama del Código Abierto en 2009. Esto significa que ha sido reconocido como uno de los mejores software de código abierto de la historia.
Esto dice mucho.
Hay tres modos en el snort: sniffer, registrador de paquetes y detección de intrusos en la red. El modo sniffer es el modo básico y la función principal es leer paquetes de red y mostrar su contenido. El registrador de paquetes es bastante similar, excepto que los paquetes escaneados se registran en el disco. El modo más interesante es el modo de detección de intrusos. Analiza el tráfico de acuerdo con las instrucciones de una regla establecida por usted. Según el tipo de amenaza que haya encontrado, puede pasar por diferentes líneas de acción.

Snort puede encontrar muchos tipos diferentes de grietas en el sistema que podrían ser un

señal de un posible ataque que puede tener lugar en el futuro. Snort tiene un sitio web donde puedes descargarlo.

Volcado de

TCP Si alguna vez estuvo interesado en saber qué rastreador de paquetes fue el primero, no busque más allá de Tcpdump. La primera versión del software fue en 1987. Desde entonces, se ha actualizado y mantenido periódicamente. Sin embargo, el núcleo del software siempre se ha mantenido igual. La mayoría de los sistemas similares a Unix vienen con un volcado de TCP preinstalado porque es la herramienta predeterminada para esos sistemas operativos.

La forma estándar de trabajar para el volcado de TCP es capturar el tráfico en los vertederos en la pantalla. Puede notar que esto es bastante similar al modo sniffer del que hablamos anteriormente. Los volcados se pueden canalizar para capturar archivos específicos para su posterior análisis, de forma similar al modo de registrador de empaquetadores. Wireshark generalmente se usa junto con el volcado de TCP.

La mayor fortaleza del volcado de TCP es el hecho de que captura fácilmente los filtros y usa varios comandos de Unix para hacer el trabajo mucho más corto y fácil. Si tiene un buen conocimiento de los sistemas similares a Unix, manejar el tráfico y capturar las partes específicas que le interesan no será un problema.

kismet

Se puede decir mucho sobre Kismet. Es un sistema de detección de robo, rastreador de paquetes y detector de red en uno. La función preferida es cuando se trabaja en una LAN. Funciona con la mayoría de las tarjetas inalámbricas y puede atravesar muchos tipos diferentes de tráfico. Esta herramienta es compatible con Linux, OS X, OpenBSD, NetBSD y FreeBSD. Kismet tiene un soporte muy limitado para los sistemas Windows porque muy pocos adaptadores de red admiten el modo de monitoreo de Kismet.

Este software tiene la licencia Gnu GPL. La forma en que se diferencia de otros detectores de redes inalámbricas radica en que el trabajo se realiza de forma pasiva. No utiliza paquetes registrables, sino que detecta directamente la presencia de puntos de acceso. También hace conexiones entre ellos. De las herramientas de código abierto para el monitoreo de redes inalámbricas, esta es la más utilizada.

Nikto

Nikto es otra pieza excelente de software de código abierto. Es uno de los escáneres de servidores web más populares. Su función principal es ejecutar servidores web a través de una gran cantidad de pruebas para encontrar rastros de miles de programas diferentes que pueden amenazar su seguridad. Puede funcionar con diferentes versiones de muchos servidores diferentes. Comprueba las configuraciones del servidor y busca anomalías en el sistema.

Nikto está diseñado para la velocidad en lugar del sigilo. Probará un servidor web lo antes posible, pero su paso aparecerá en los archivos de registro y será detectado por los sistemas de detección y prevención de intrusos.
Nikto tiene licencia GNU GPL. Se puede descargar desde GitHub desde casa.

OpenVAS

OpenVAS, también conocido como Open Vulnerability Assessment System, es un conjunto de herramientas que proporciona muchos análisis completos de vulnerabilidades. La mayoría de los componentes del sistema son de código abierto y el software es completamente gratuito.
OpenVAS tiene dos componentes principales. La primera parte del software es el escáner. Como su nombre lo indica, es responsable de escanear las computadoras.
El gerente es la segunda parte. El administrador funciona como un controlador para el escáner y trabaja con los resultados de los escaneos. La base de datos de pruebas de vulnerabilidad de red es un componente adicional que puede agregar al software para hacerlo más eficiente. Puede descargar el software desde dos software: Greenborne Security Feed y Greenborne Community Feed. Este último es gratuito mientras que el primero es de pago.

OSSEC

OSSEC significa Open Source SECurity. Es un programa basado en host que se utiliza para la detección de intrusos. Este tipo de sistema de detección se diferencia de sus homólogos basados en red en que el propio host ejecuta el programa. Trend Micro es propietaria de OSSEC. En términos de seguridad informática, este nombre tiene bastante peso.
El uso principal de este software es en software similar a Unix, donde el trabajo se dedica a la configuración y el escaneo de archivos. También ve algún uso en los sistemas Windows donde vigila el registro. La herramienta le avisa a través de la consola o del correo electrónico cuando se detecta algo sospechoso.
OSSEC tiene un inconveniente relativamente importante, al igual que cualquier otro IDS basado en host. Debe instalar una nueva copia en cada dispositivo que desee proteger. Esto se ve algo mitigado por el hecho de que la información se puede dirigir a una consola centralizada.

OSSEC también tiene licencia GNU GPL. Si desea utilizarlo, puede descargarlo del sitio web.

OSSEC también se distribuye bajo la licencia GNU GPL y se puede descargar desde su propio sitio web.

Nexponer

Nexpose es otra herramienta común. Fue creado por Rapid7 y se utiliza para gestionar vulnerabilidades. Hace todo lo que puede hacer un administrador de vulnerabilidades. Eso

cumple con el llamado ciclo de vida del gestor de vulnerabilidades. Esto significa que el software maneja todas las fases involucradas en el proceso.
Cuando se trata de las características con las que viene, es un todo completo. El software tiene muchas funciones interesantes, como la opción de escaneo virtual y la detección dinámica. Puede escanear muchos tipos diferentes de entornos y puede manejar una cantidad de direcciones IP. Es un software en desarrollo y está en constante crecimiento.

Hay dos versiones del producto que puede obtener. Hay una edición comunitaria que tiene muchas menos funciones que las versiones comerciales completas, los precios comienzan en $ 2,000 al año. Si tiene alguna pregunta sobre el software o desea descargar Nexpose, visite el sitio web oficial.

GFI LanGuard GFI

LanGuard es aclamado como una excelente herramienta de seguridad de TI para empresas. Esta herramienta fue creada para ayudarlo con el escaneo de red y la aplicación automática de parches. También le ayuda a cumplir con los estándares de cumplimiento. Este software es compatible con la mayoría de los sistemas operativos.
GFI LanGuard tiene un tablero muy intuitivo que también ayuda a identificar virus.
También funciona con navegadores web. Otro punto fuerte del software es el hecho de que funciona con una amplia variedad de dispositivos.
Si está buscando GFI LanGuard, encontrará que hay muchas opciones diferentes cuando se trata de características adicionales. El precio es flexible y se renueva anualmente. Si no está seguro de comprar el software, puede probar primero la versión de prueba.

Herramientas de seguridad para la nube

Como mencioné anteriormente, la nube se ha convertido en una opción popular cuando se trata de almacenar software y datos porque es un método muy eficiente y seguro para mantener seguros sus objetos de valor digitales. La nube tiene costos más bajos, escalabilidad más fácil y movilidad adicional. Estas perspectivas están impulsando a muchas empresas a mover sus datos de las instalaciones a la nube. Esto, a su vez, hizo que los piratas informáticos se inclinaran cada vez más a idear nuevos métodos de sistemas de ataque para descifrar las nubes. Esta es la razón por la que muchos proveedores como Dropbox y Evernote le brindan muchas políticas diferentes que poco a poco se están apoderando del mundo de los negocios.
Sin embargo, la nube tiene sus propios defectos. Ha habido problemas con respecto a la privacidad de los datos y la residencia. Por supuesto, estos problemas no son suficientes para que la gente abandone la nube. Esta es la razón por la cual la importancia de la seguridad relacionada con la nube ha aumentado, ya que los usuarios y proveedores siempre están tratando de encontrar formas de mitigar algunos de los riesgos.

Si desea poner su negocio en la nube, hay algunas herramientas que siempre debe tener en cuenta cuando desee mantener sus datos seguros. Sin embargo, antes de comenzar a hablar de ello, primero debe saber qué es Shadow IT.

El término Shadow IT se refiere a todos los sistemas o servicios utilizados en los datos de la organización sin la aprobación de la organización. Shadow IT no es nada nuevo, pero comenzó a convertirse en un problema creciente debido al aumento de la popularidad de la nube.

Esto hace que sea más difícil para las empresas mantener sus datos seguros porque las políticas son más difíciles de implementar.

Tres de las siguientes cinco herramientas están destinadas a reducir los riesgos de seguridad que puede encontrar al trabajar con la computación en la nube.

Bitglass

Bitglass aún no está completo y aún se encuentra en la fase beta. Protege los datos de su empresa. Bitglass se puede utilizar tanto en ordenadores como en dispositivos móviles. Su objetivo es mantener la visibilidad de sus datos y reducir el riesgo de que esos datos se pierdan en el dispositivo o en la propia nube.

Bitglass cubre diferentes tipos de seguridad debido a la cantidad combinada en este paquete. Si hablamos de lo que puede hacer por las aplicaciones en la nube, Bitglass puede hacer varias cosas. Puede detectar el uso de las aplicaciones y cifrar los datos que ha subido a la nube.

Otra gran ventaja de Bitglass es el hecho de que puede rastrear sus datos sin importar dónde se encuentren en Internet. Esto significa que tiene una vista de los datos sin importar a dónde vayan y en manos de quién estén. También reduce un gran riesgo cuando se trata de datos comprometidos debido a la pérdida del dispositivo. Bitglass tiene la capacidad de borrar un dispositivo con sus datos sin necesidad de realizar pasos adicionales.

Skyhigh Networks Skylight

Networks utiliza registros de firewalls y servidores proxy que ya existen para analizar y proteger sus aplicaciones en la nube. Realiza un seguimiento del uso de las aplicaciones de fuentes autorizadas y no autorizadas.

Puede ajustar la evaluación de riesgos para garantizar que los resultados sean los que desea ver sobre su sistema, sin información adicional innecesaria.

Otra gran ventaja de Skyhigh es la detección de inconsistencias en su sistema y violaciones de datos.

La última característica notable de Skyhigh Networks es que tiene seguridad de 3 clics. Esto significa que la política se puede aplicar en toda la nube y brindarle acceso directo a las aplicaciones sin usar agentes de dispositivos o VPN. En

Además, puede usar Skyhigh para cifrar y proteger datos.

NetsCheap Nets

Goedkoop está especialmente diseñado para dar sombra a TI. Puede monitorear aplicaciones en la nube y detectar anomalías en su red. Supervisa una amplia gama de actividades diferentes en su red y le proporciona informes completos sobre sus análisis y la información recopilada.

Le ayuda a hacer preguntas comerciales y de seguridad para descubrir vulnerabilidades en su sistema.

Otra gran característica de Nets Goedkoop es la aplicación de políticas que le permiten vigilar a sus empleados mientras interactúan con las aplicaciones en la nube, mientras detiene cualquier actividad que pueda considerar no deseada. Permite al trabajador aumentar su productividad sin comprometer su seguridad.

CipherCloud

CipherCloud tiene como objetivo cifrar y tokenizar sus datos para proteger su nube.
A diferencia de las pocas herramientas anteriores, no se enfoca en TI en la sombra. Más bien, hace que las áreas conocidas de la nube sean lo más seguras posible.
CipherCloud es bastante específico debido al hecho de que los datos que carga se cifran durante la carga y se descifran durante la descarga. Su red corporativa conserva las claves de cifrado utilizadas durante el proceso. Esto significa que cualquier usuario no autorizado simplemente obtiene un lote de texto ilegible en lugar de datos útiles.

CipherCloud también puede detectar malware y evitar la pérdida de datos. Hay varias compilaciones para CipherCloud que están específicamente especializadas para ayudar a sistemas específicos, mientras que hay varias que funcionan con cualquier aplicación en la nube.

Okta

Okta es bastante único entre estas cinco soluciones de aplicaciones en la nube. El objetivo de Okta es garantizar que haya un SSO seguro, abreviatura de Single Sign-On, para todas las aplicaciones que posee su empresa. Okta puede comunicarse con las aplicaciones más utilizadas que encuentras en la mayoría de las empresas.
Okta tiene muchas funciones útiles que agradecerás, como la compatibilidad con dispositivos móviles y la autenticación multifactor.

El software le proporciona registros de auditoría detallados, lo que significa que puede realizar un seguimiento del acceso de sus usuarios a sus aplicaciones en la nube. Otra gran ventaja es el panel de control central desde el cual puede administrar las políticas de acceso en todo el sistema. También le da la opción de administración basada en roles.

Pruebas de penetración en la nube desde el punto de vista del cliente

vista

Cuando se trata de pruebas de penetración en el sitio, generalmente asume que posee todos los componentes y que todas las pruebas que realiza están bajo su supervisión y con su aprobación. Las pruebas de penetración funcionan de forma ligeramente diferente en la nube. El principal inconveniente de la nube es que los consumidores y los proveedores comparten la responsabilidad en lo que respecta a la seguridad informática. Ambos grupos son elegibles para realizar pruebas de penetración en las aplicaciones en la nube. Hay dos cosas a tener en cuenta cuando desee realizar pruebas de penetración en la nube.
Lo primero que debes considerar es si eres un consumidor o un proveedor. El otro factor es el modelo de servicio que seleccionó.

Las responsabilidades de los consumidores y proveedores.

Los proveedores de la nube tienen una amplia variedad de opciones cuando se trata de pruebas de penetración, incluso las más brutales, como las pruebas DDoS y las pruebas de equipo rojo. Hay mucha competencia cuando se trata del mercado de servicios en la nube. Hay muchos gigantes que brindan un excelente servicio y la necesidad de mejorar es cada vez más abrumadora.
Los usuarios de la nube están cada vez más interesados en la ciberseguridad. A menudo se comunican con sus proveedores para involucrarse más en el proceso de seguridad y las pruebas de penetración.
Los propios consumidores tienen un acceso mucho más limitado a las aplicaciones y pruebas de penetración en la nube. Estas restricciones dependen en gran medida del modelo que utilice su proveedor de servicios en la nube.

Pruebas de penetración Depende del modelo de servicio en la nube

Existen tres modelos diferentes de servicio en la nube: SaaS (software como servicio), PaaS (plataforma como servicio) e IaaS (infraestructura como servicio). Estos tres modelos difieren entre sí en la división de responsabilidades entre proveedor y consumidor cuando se trata de capas de nube.

Para comprender estos modelos, primero debe conocer las ocho capas de una nube: • Instalaciones (edificios). • Red (tanto física como virtual). • Computadoras y almacenamiento (especialmente almacenamiento de archivos y hardware proporcionado por la CPU). • Hipervisor (El hipervisor se utiliza en entornos virtualizados. La tarea del hipervisor es gestionar la asignación de recursos entre las máquinas del sistema).

Sistema operativo (SO) y máquina virtual (VM) (estos dos se consideran

ser la misma capa debido a que cuando se trata de entornos no virtualizados, la ejecución del hardware de almacenamiento está cubierta por el sistema operativo, mientras que en entornos virtualizados (entornos en los que la VM se encarga de esta tarea). . • Pila de soluciones (utiliza bases de datos y lenguajes de programación). • Aplicación (esta capa está compuesta por las aplicaciones utilizadas por los usuarios). • Interfaz de programa de aplicación (API) o interfaz gráfica de usuario (GUI) (los consumidores y clientes utilizan esta capa para comunicarse con el sistema).

Lo que puede hacer con las aplicaciones y las pruebas de penetración depende directamente del tipo de control que tenga sobre las capas. Los diferentes tipos de modelos le brindan diferentes grados de control sobre las capas.

modelo IaaS

El modelo IaaS es específico en el sentido de que el control del sistema operativo y la máquina virtual, así como los niveles superiores de la nube, recae en el usuario. El proveedor es responsable de la conectividad del hardware y la red. Esto significa que los consumidores pueden realizar pruebas de penetración en la API/GUI, la aplicación, la pila de soluciones y las capas de VM.

Modelo PaaS

En el modelo PaaS, el proveedor proporciona todo el software y hardware necesarios para ejecutar una aplicación, mientras que el consumidor solo implementa la aplicación. Este modelo le da al consumidor menos capas con las que lidiar: la API/GUI y las capas de aplicación para ser precisos.

modelo SaaS

El modelo SaaS es similar al PaaS, lo que permite que el consumidor pruebe las capas y lo que proporciona el proveedor. El alcance de las pruebas se limita a la capa API/GUI. Sin embargo, algunos proveedores que utilizan este modelo permiten a sus usuarios ejecutar sus propias aplicaciones independientemente del sistema. Estas aplicaciones pueden ser probadas por el consumidor cuando lo desee.

Cosas para recordar como cliente de Cloud Penetration Pruebas

Hay dos reglas de oro cuando se trata de pruebas de penetración en la nube:

- Pregunta siempre a tu proveedor si quieres realizarte una prueba
- Realice pruebas de penetración solo en las capas que administra

La mayoría de los proveedores tienen ciertos requisitos que deben cumplirse antes de darle acceso a sus sistemas. Por lo general, encontrará esta información en el

sitio web del proveedor. Si crea o prueba una prueba de penetración no autorizada sin cumplir con los requisitos, su cuenta se cerrará porque el proveedor también debe garantizar la seguridad de los otros usuarios para que no puedan correr riesgos con actividades sospechosas.

El trabajo de un proveedor no es fácil. Siempre tienen tantas cosas en qué pensar y equilibrar. Siempre deben asegurarse de que los datos de sus clientes estén seguros, pero sin dañar los intereses del cliente debido a las políticas de seguridad que el proveedor podría implementar. El proveedor no es todopoderoso, por lo que las pruebas de penetración que pueden hacer deben hacerse dentro de su propio dominio. Es bueno que ningún proveedor de la nube pueda acceder a sus datos sin su permiso, por lo que puede estar seguro de que su privacidad está segura.

Capítulo 9: ¿Qué necesito saber?

¿Cómo consigues un trabajo? ¿Qué formación y experiencia necesitas?

Decir que el hacking ético es un trabajo como cualquier otro sería muy erróneo. No requiere ningún tipo de diploma o certificación. El conocimiento y la experiencia son lo único que importa en esta industria. No importa cuántos diplomas tengas, lo más importante es tu ingenio y saber hacer. Los certificados son fáciles de obtener una vez que se ha probado a sí mismo.

¿Necesita certificaciones o licencias?

No necesitas certificados para ser un hacker ético. Sin embargo, es bueno tenerlos ya que confirman tu habilidad en el campo. Hay muchas certificaciones diferentes cuyo valor depende del trabajo al que aspiras. Debe hacer su investigación cuando esté buscando una certificación. Las habilidades más valiosas que puedes tener en esta área de trabajo, además del conocimiento en sí mismo, son la perseverancia, las habilidades de comunicación y la resolución de problemas.

La naturaleza del trabajo ¿Qué hay detrás de la superficie de la pista? ¿Qué haces usualmente?

Hacer este trabajo le dará acceso a algunos sistemas muy vulnerables. Una vez que esté en él, notará cuánto daño puede causar un ataque bien ubicado al sistema y a la empresa misma. Verá las conexiones que no deberían tener, los programas a parchear, si el software y el hardware se están utilizando correctamente y si las contraseñas almacenadas en el sistema son seguras. Cada red es solo una masa de sistemas interconectados que son más fáciles de descifrar de lo que parece al principio. Esto es especialmente importante con las redes que cuidan su dinero o información personal. Una cosa importante a tener en cuenta es

qué tan informado estás. Las redes sociales son un gran lugar para descubrir nuevas noticias antes de que aparezcan en otros medios.
La mayor parte del tiempo que dedica a este trabajo se dedica a investigar redes, eliminar vulnerabilidades potenciales, documentar los hallazgos e informar a sus clientes sobre ellos. A veces sientes que estás de vuelta en la escuela debido a la enorme cantidad de informes que haces como hacker. Los informes deben ser informativos y concisos, ya que esta es la única información que su cliente tiene en sus sistemas.

Es importante que el cliente participe en cada paso. Aunque el proceso es muy abierto, el cliente puede perderse en todas las complejidades del proceso debido al conocimiento técnico requerido para comprenderlas.

¿Cuáles son las suposiciones generales que la gente hace sobre el trabajo?

La gente suele asociar la palabra "hacker" con personas malintencionadas que se dedican a actividades ilegales. Sin embargo, como he dicho muchas veces, esto no es cierto.
Los piratas informáticos son personas a las que les gusta investigar cómo se pueden usar nuevas herramientas y software para resolver problemas y abrir nuevas rutas de ataque. Las personas malintencionadas que usan su conocimiento para dañar a las personas o robar dinero e información no son piratas informáticos. Estos individuos son solo criminales y nada más. La comunidad de hackers odia identificarse como "hackers éticos" debido a la reputación que les han dado los delincuentes. El término "cracker" siempre fue una posibilidad cuando se trataba de piratas informáticos criminales, pero a menudo se pasa por alto.
A algunas personas les gusta observar el proceso de hackeo y verlo como el logro de un mago. Por el contrario, la piratería es un proceso bien pensado que tiene como objetivo atravesar sistemáticamente un sistema para mejorar una red o un sistema.
A pesar de lo que algunas personas piensan, los piratas informáticos no son más que personas que tienen una buena comprensión de cómo funcionan los sistemas. Las computadoras siempre solo harán lo que se les dice y nada más.
Otra suposición errónea que a la gente le gusta hacer es que todas las pruebas que realiza un sombrero blanco son las mismas. Desafortunadamente, este campo apenas se explora y las pruebas de penetración son un término relativamente desconocido para la mayoría de las personas. Hay muchas pruebas de penetración diferentes, cada una de las cuales tiene un requisito de habilidad diferente.

¿Cuántas horas al día trabajas?

La cantidad de tiempo que necesita dedicar cada día a trabajar duro depende del tipo de actividad en la que participe. Si una empresa de alto nivel lo contrata para realizar una prueba de penetración, tendrá que trabajar de 8 a 10 horas al día. Cada tarea

puede tomar hasta 10 semanas. Si solo observa las vulnerabilidades en el sistema o la red, la cantidad de tiempo que dedicará a ellas depende de usted.
Si recibe una llamada de una empresa para ayudarlos a recuperarse de una brecha de seguridad, sus horas pueden dispararse. Las noches enteras no son nada fuera de lo común para la gente de esta industria. Detener un ataque para dañar aún más el sistema no es una tarea fácil, especialmente porque es su responsabilidad administrar el daño y ayudar a la empresa a volver a la acción.

¿Hay algún consejo o atajo que pueda ayudarlo a ponerse a trabajar?

Asegúrate de estar siempre al día con las noticias. Siempre surgen nuevos métodos y es posible que encuentre a alguien que haya encontrado una manera más fácil de hacer algo que le interese. Mantenga siempre un registro de sus hazañas y la información que ha recopilado para realizar un seguimiento de lo que ha hecho. Al hacer esto, puede evitar sentirse mal por perder el tiempo o no ver la solución a tiempo.

Recuerde siempre que no existe tal cosa como demasiada comunicación. Nunca se ha despedido a un hacker porque un cliente haya dado demasiada información sobre el sistema. Rara vez encontrará un cliente que le indique que proporcione menos información. En general, los clientes están ansiosos por estar informados sobre lo que sucede en su sistema, sin importar cuán minúsculo sea, y apreciarán el trabajo que realiza para comunicar esa información de una manera comprensible.

¿Puedes hacer cosas para diferenciarte del resto de los sombreros blancos?

Las empresas tienen la idea errónea de que el trabajo de un hacker ético es simplemente escanear el sistema para encontrar una vulnerabilidad y que nada está mal.
Sin embargo, eso no es verdad. El trabajo de un hacker de sombrero blanco es mucho más extenso y profundo. Siempre intentarán averiguar por qué el programa es vulnerable y cómo esa vulnerabilidad podría ser explotada por una persona malintencionada, así como la cantidad real de daño que puede causar un hacker de sombrero negro exitoso.
Encontrar vulnerabilidades en una red es bastante fácil. La mayor parte del trabajo que tiene que hacer un hacker proviene de analizar qué significa la vulnerabilidad para el sistema. Es posible que desee saber qué puede y quiere hacer el hacker al usar esa vulnerabilidad y cómo la vulnerabilidad afecta a otras partes del sistema. También puede ayudarlo a descubrir cómo un pirata informático criminal ingresa al sistema, evitando que un ataque similar sea efectivo.

¿Qué pasa con el trabajo es el peor y cómo lidiar con él?

Hay pocas cosas que pueden rechazarlo, como clientes específicos. A veces puede ser contratado por personas que no están realmente interesadas en lo que sucede en su sistema y solo buscan hacerlo. Otro tipo de cliente que causará mucho estrés es el tipo indiferente. Algunas empresas no siempre están contentas de contratar a un hacker de sombrero blanco para que les ayude, pensando que reparar el daño dejado por el hacker siempre será mucho más barato que contratar a un profesional para que les ayude. ayudar a mejorar la seguridad de sus redes. Por otro lado, los clientes más reacios pueden contratar a un hacker de sombrero blanco simplemente por temor a que su sistema se vea comprometido. Esto se puede comparar con cuando su automóvil comienza a hacer ruidos extraños. Acude a un mecánico lo antes posible para ver si algo anda mal.

Algunos clientes pueden estar preocupados de que los servicios de un hacker de sombrero blanco puedan costar un centavo. Esta no siempre es la única preocupación, ya que las personas que buscan servicios a menudo son personas que confían en sus habilidades de TI como trabajo. Si descubre muchas vulnerabilidades y problemas, puede hacer que la persona quede mal.

Lo mejor que se puede hacer en tales situaciones es seguir con el buen trabajo. Haz siempre lo mejor que puedas y asegúrate de informar todo lo que encuentres, así como lo que puede significar para la red. Recuerde que usted mismo no es responsable de proteger el sistema. Esa responsabilidad recae en el propio cliente. Lo mejor que se puede hacer es esperar que ellos mismos lo hagan bien.

¿Dónde está el placer en el trabajo? ¿Qué lo hace tan atractivo?

Es difícil determinar exactamente qué es lo mejor del trabajo. Algunas personas están muy contentas de estar haciendo algo que sería ilegal si la situación fuera diferente. La gente a menudo bromea sobre cómo piensa como un criminal después de un tiempo. Esto es cierto en la mayoría de los casos y puede ser una forma divertida de abordar el trabajo.
Hay mucha gente interesante en el sector. Siempre te divertirás intercambiando conocimientos e historias del trabajo con ellos, y posiblemente también haciendo nuevos amigos.

Sin embargo, lo que te da más satisfacción en el trabajo es el hecho de que tienes un gran impacto en la vida de alguien. Usted los ayuda no solo a sentirse más seguros, sino también a estar más seguros. Influyes en la vida de alguien de una manera muy buena y puede ser muy gratificante en sí mismo. Para ser honesto, los salarios también son bastante buenos.

Clientes y consejos generales ¿Hay algo que quieras que tus clientes sepan antes de buscar tu ayuda?

Hay varias cosas que los clientes a menudo tienen que considerar. Lo primero, y quizás lo más importante que hay que recordar acerca de los hackers de sombrero blanco, es el hecho de que no son superhéroes. No pueden resolver todos sus problemas simplemente sumergiéndose. A veces, los clientes piensan que una vez que ingrese a su sistema, lo hará completamente seguro y podrán trabajar sin preocupaciones.

Sin embargo, esto es una ilusión.

Si bien a muchos hackers de sombrero blanco les gustaría que funcionara de esa manera, la realidad es un poco más difícil de digerir. Es importante que cada cliente sea realista. Depende de ellos decidir qué partes del sistema son más importantes y qué tipos de riesgos son aceptables cuando se trata de protegerlos. Es imposible crear un sistema completamente impenetrable. Siempre hay una vulnerabilidad que no puedes ver o una nueva técnica que posiblemente no podrías explicar. Esto significa que el trabajo de un hacker de sombrero blanco no termina cuando encuentra la manera de prevenir un posible ataque. Siempre deben evaluar la situación para ver qué se puede hacer para evitar que un ataque exitoso se salga de control.

Nadie puede protegerse de una amenaza que no sabe que existe.

Por lo tanto, hay algunos pasos que puede seguir para ayudar al pirata informático que contrató a asegurarse de que hizo todo lo posible para mantener su sistema seguro. Antes de que un pirata informático realice una prueba de penetración, proporciónele siempre la mayor cantidad posible de información importante sobre el sistema.

La prueba de penetración está diseñada para encontrar una parte de su sistema que sea vulnerable a un ataque y para mostrar cuánto puede afectar al sistema mismo.

A nadie le gusta que su dinero se haya ido o que falte su información personal confidencial, por lo que siempre debe actuar con rapidez para resolver la vulnerabilidad una vez que el hacker la descubra.

Algo que todos los clientes deben saber es que la prueba de penetración es la parte fácil. Aprender de sus errores y administrar su negocio de una manera más segura es la parte difícil.

¿Cuánto puedes ganar con este trabajo?

Bueno, lo primero que debe tener en cuenta es que sus expectativas generalmente se cumplirán siempre que sean razonables. La segunda cosa que vale la pena señalar es que la piratería es similar a otros trabajos cuando se trata de cuánto trabajo duro se recompensa. Si trabajas lo suficientemente duro y te vuelves lo suficientemente bueno, ganas un centavo. Si usted

quiere trabajar por una gran cantidad inmediatamente después de obtener una certificación o un amplio conocimiento en el campo, puede comenzar usted mismo. Las empresas pueden ser bastante brutales cuando se trata de la cantidad de trabajo que te hacen. Es posible que tenga que viajar mucho y trabajar muchas horas. Algunos hackers suelen decir que dormir es un lujo en este momento. Si se esfuerza por mantener una cantidad significativa de dinero en su bolsillo mientras trabaja de manera saludable, es posible que necesite obtener años de experiencia en TI y seguridad informática.

¿Cómo progresas en esta área?

Bueno, esta pregunta es interesante. Por lo general, depende de la persona de la que estemos hablando. Obtendrá nuevos conocimientos todos los días, independientemente del área clave en la que trabaje. Si bien estas habilidades generalmente difieren de una línea de trabajo a otra, adquirir experiencia es la clave para progresar. Si bien puede hacerlo bien con los exámenes y obtener buenos certificados, esto puede ayudarlo, pero lo más importante que puede tener es la habilidad mientras trabaja.

Hay otra manera de sobresalir entre las personas con las que trabaja.

Las conferencias se llevan a cabo anualmente. Si realiza una investigación interesante y demuestra su utilidad, su nombre puede ganar un poco de peso para dar vueltas. Cuanto más participe en estas conferencias, más probable será que se mencione su nombre.

¿Qué tienden a ser sobrevalorados o infravalorados los clientes?

En la mayoría de los casos, los clientes no ven lo valiosos que son para el proceso en sí. Les gusta pensar que un buen hacker es todo lo que necesitas para mantener alejadas a las personas malas. Sin embargo, esto no es cierto ya que el cliente tiene que hacer la mayor parte del trabajo para protegerse. La gente también tiende a poner excusas sobre por qué nunca serán pirateados. Les gusta decir que su empresa es demasiado pequeña o que no tienen ninguna información valiosa que nadie quiera. Todo esto cambia bastante rápido una vez que sus sistemas son realmente pirateados.

Otro error común que cometen las empresas es cuando se comparan con otras empresas. Algunas conversaciones en la sala de juntas a menudo se reducen a esto. Sienten que están desperdiciando dinero si gastan más en seguridad que cualquier otra empresa similar.

Sin embargo, lo que la gente suele sobrestimar son los estándares de cumplimiento. A la gente le gusta pensar que si cumple con estos estándares, su sistema es completamente seguro y no puede haber nada malo cuando un pirata informático intenta ingresar. Lo que necesita saber sobre los estándares de cumplimiento es que no son representativos del rendimiento necesario para mantener su sistema seguro. Son un esbozo aproximado del mínimo indispensable para no ser multado. Para estar realmente seguro, tienes que ir por

millas e ir más allá de lo que prescriben los estándares de cumplimiento.

¿Qué es lo más importante para recordar?

Tienes que poner tu corazón y alma en ello. Este es un mercado que continúa creciendo y está hambriento de personas interesadas en jugar con los sistemas y ver qué los está aprovechando y cómo pueden seguir haciéndolo.
Asegúrate de disfrutar el proceso de aprendizaje. Si parece que es difícil aprender las habilidades que ha conocido una y otra vez, entonces algunas de las partes menos glamorosas del trabajo definitivamente lo aburrirán. Sin embargo, nunca debes dejar de esperar. Es fácil encontrar un trabajo específico que sea divertido para ti y te haga sentir realizado.

Conclusión La piratería

de sombrero blanco no es algo nuevo. De hecho, ha estado aquí durante mucho tiempo, ya sea con diferentes nombres o sin ningún nombre. Ha habido mucha controversia en torno a la piratería de sombrero blanco durante mucho tiempo. Dado que el delito cibernético se ha convertido en una práctica común entre los delincuentes, la palabra 'hacker' ha ido adquiriendo una reputación maliciosa. Debido a la medida en que la tecnología informática ha evolucionado en un tiempo relativamente corto, tiene sentido que la información se mueva de una forma física a una forma digital. Hay muchas organizaciones criminales que valoran la información por encima de todo, por lo que tiene sentido que siempre encuentren nuevas formas de invadir los sistemas. Esto significa que es más importante que nunca tener sistemas seguros. Los datos valiosos como las contraseñas que usamos todos los días es algo muy valioso y debemos protegerlo.

La piratería de sombrero blanco surgió como una solución no tan obvia para encontrar nuevas formas de proteger nuestros sistemas. Piensa en un sistema como si fuera humano. Cuando alguien se enferma, su cuerpo se debilita y sufre algún daño. Sin embargo, si el cuerpo supera la enfermedad a largo plazo, será más resistente a la enfermedad en el futuro. Lo mismo ocurre con las lesiones. Si se rompe un hueso en un lugar varias veces durante un período de tiempo, el nuevo tejido que reemplazará el daño será más resistente que nunca. La piratería de sombrero blanco funciona con un principio similar. Para garantizar que su sistema sea seguro, debe eliminar tantas vulnerabilidades como sea posible. Es difícil decir dónde están estas vulnerabilidades si no se explotan. Sin embargo, realmente no puede esperar a que ocurra un ataque para descubrir la vulnerabilidad y esperar lo mejor. Una vez que un hacker malintencionado invade su sistema, no se sabe qué tan lejos llegará o qué hará. Aún así, era necesario tener un método que ayudara

Las organizaciones mantienen sus sistemas actualizados con las últimas herramientas y técnicas de piratería para crear contramedidas.

La piratería de sombrero blanco es la única forma real de hacer esto. Hacer que el sistema sea menos vulnerable a un ataque de piratas informáticos es exponerlo al peligro. Esto no es algo que esperaría que alguien hiciera porque es un proceso extremadamente preciso y delicado. Los profesionales que contrate para hacer esto por usted deben ser meticulosos en su trabajo y tener amplios conocimientos de informática.
El problema con un hacker de sombrero blanco es que muchas personas lo asocian automáticamente con personas malintencionadas que realizan las mismas actividades que usted, pero por diferentes motivos. Sin embargo, llamar a un hacker no se considera algo malo en todas partes. Las personas en la industria de TI tienen mucho respeto por los hackers de sombrero blanco certificados porque significa que son personas con una gran cantidad de conocimiento en el campo y usan ese conocimiento para hacer el bien a otras personas. Las personas que miran a los sombreros blancos como si fueran delincuentes generalmente no saben qué hacen realmente los sombreros blancos y solo se enfocan en la parte de hacker del título. Esta es principalmente la razón por la que los sombreros blancos no muestran la vocación y la prefieren a sus currículums.

Sin embargo, los hackers de sombrero blanco son una fuerza para el bien. Usan los mismos métodos que los crackers, pero lo hacen con el permiso del propietario del sistema que están pirateando y lo hacen para mejorar la seguridad del sistema. El punto es que son lo opuesto a los hackers de sombrero negro porque hacen su trabajo mucho más difícil.

El área de piratería de sombreros blancos está creciendo rápidamente. Esto se debe en gran parte a la cantidad de ciberdelincuencia que ha crecido en las últimas décadas, por lo que siempre hay empresas que buscan un buen hacker de sombrero blanco. Están dispuestos a pagar una gran cantidad de dinero, pero le ahorrarán tiempo y energía, ya que es más que un trabajo de tiempo completo. Afortunadamente, trabajar independientemente como hacker de sombrero blanco siempre es una opción. Este camino es un poco más lento pero lo llevará a resultados más favorables. Como dije antes, el trabajo solo requiere conocimiento y experiencia, por lo que el trabajo duro es clave para el éxito. Si puede demostrar su valía en el campo, rara vez tendrá las manos libres. Puede obtener varios certificados para demostrar su experiencia en el campo, pero nuevamente, esto no es necesario porque todo lo que tiene que hacer para conseguir un buen trabajo es demostrar su valía ante el empleador. Entonces es viento en popa.

El trabajo puede no ser para todos. A veces puede estar atrapado haciendo lo mismo durante un período prolongado de tiempo y eso simplemente no es interesante para

algunas personas. Por otro lado, encontrará el trabajo extremadamente interesante si disfruta aprendiendo cosas nuevas porque constantemente se descubren nuevos métodos. El trabajo requiere mucha flexibilidad porque nada de lo que haces se hace exactamente en el libro de texto. Por lo general, solo piensa como un cracker para ingresar al sistema, pero antes de eso, hay una etapa en la que debe recopilar cuidadosamente datos sobre el sistema. La parte divertida comienza cuando realmente puedes profundizar en el sistema. Fisgoneará para encontrar algunas debilidades y luego seguirá un plan de pirateo para determinar qué tipo de daño puede causar un usuario malicioso a partir de ese momento. Durante todo esto tendrás que hacer lo que tanta gente teme: hacer informes.

Los informes son el resultado principal de las pruebas de penetración porque son el vínculo directo entre el empleador y el hacker. Los informes brindan una descripción general de cuáles son las vulnerabilidades, cómo se pueden explotar y cómo se pueden remediar. Un cliente necesita esta información para determinar qué hacer más tarde para garantizar que una persona malintencionada nunca haga un uso indebido de la vulnerabilidad.

Debido a que es un campo relativamente nuevo, la piratería representa una gran promesa para los creadores y exploradores. Las personas más conocidas en la comunidad son aquellas que desarrollan herramientas y métodos que ayudan a los hackers de sombrero blanco a trabajar de manera más eficiente. Hacer una de estas herramientas requiere mucho dinero y tiempo, por lo que esta es una tarea solo para los más valientes y hábiles.

Recuerda siempre que no importa lo que te digan los medios, no todos los hackers son malos. Hay quienes usan sus conocimientos técnicos para aprovecharse de otras personas en su propio beneficio, pero los esfuerzos de sombrero blanco se empeñan en detener esto. Hay muchas personas capacitadas en la industria cuyos nombres hablan por sí mismos.

Hoy en día, la piratería informática se ha convertido en una necesidad si desea que sus sistemas permanezcan seguros. Contratar a un hacker de sombrero blanco a veces puede ahorrarle bastante dinero, pero vale la pena si tiene datos confidenciales o secretos que no quiere que le roben o destruyan.

Algunas personas subestiman la importancia de la seguridad informática y dicen cosas como: "No me pasa a mí porque no tengo datos útiles" o "La posibilidad es demasiado pequeña". Estas personas se dan cuenta del error cuando ya es demasiado tarde y ya han sido hackeadas. Siempre debes estar pendiente de la seguridad de tu computadora, porque nunca sabes qué puede pasar y cuándo puedes ser atacado.

Recuerde siempre mantenerse seguro mientras hace cualquier cosa con su sistema. Es posible que sus datos no sean valiosos para un pirata informático, pero son valiosos para usted y para usted.

no debería perderlo.