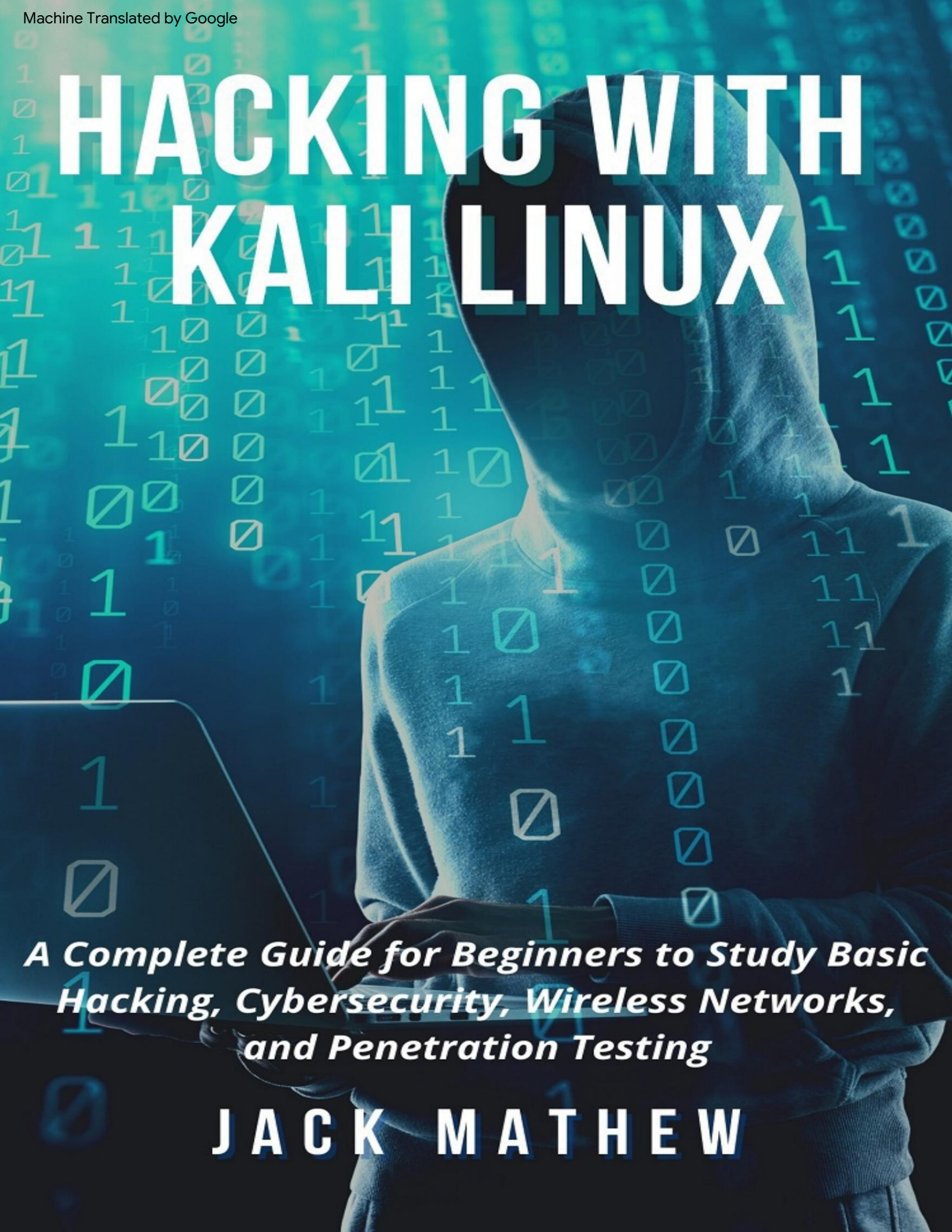
HACKING WITH KALI LINUX



A Complete Guide for Beginners to Study Basic Hacking, Cybersecurity, Wireless Networks, and Penetration Testing

JACK MATHEW

Hackear con Kali Linux

Una guía completa para que los principiantes estudien lo básico
Hacking, Ciberseguridad, Redes Inalámbricas y
Pruebas de penetración

jack mateo

https://t.me/librosdehacking

Tabla de contenido

Introducción

Felicitaciones por comprar Hacking con Kali Linux y gracias por hacerlo.

Las secciones adjuntas examinarán la totalidad de las diversas partes que debemos conocer cuando llegue el momento de trabajar con la piratería y trabajar con Kali Linux para completar todo esto. Hay varios instrumentos que podemos usar con respecto a la piratería, pero uno de los mejores marcos de trabajo que podemos usar para lograr esto es el marco Kali Linux.
Este manual dedicará un poco de esfuerzo para analizar todo eso y familiarizarse con la forma en que podemos hacer que todo funcione.

El comienzo de este manual investigará algunos de los aspectos esenciales de la piratería, las razones por las que tendríamos que invertir algo de energía en intentar piratear y utilizarla para nuestras propias organizaciones, y una mirada decente a la diferencia entre programadores morales, no confiables. programadores, y todo el mundo en el medio.

A partir de ahí, investigaremos un poco sobre la protección en línea y los ataques digitales. Con nuestro mundo avanzado y la forma en que tantas personas están en la web e intentan compartir y examinar datos constantemente, no es de extrañar que los programadores estén tratando de encontrar técnicas que les permitan acceder a las computadoras y las organizaciones. ahí fuera para tomar datos individuales y monetarios en cualquier momento que lo deseen.
Es por eso que dedicaremos un poco de esfuerzo para analizar cómo podemos mantener a nuestras organizaciones libres de cualquier peligro con la protección en línea y, al mismo tiempo, conocer qué tipos de ataques digitales son más probables.

Ahora ha llegado el momento de llevar esto un poco más allá y echar un vistazo a cómo funcionará la piratería. Investigaremos el ciclo de piratería en más sutilezas, mientras también observamos el malware, y cómo eso, y algunos otros tipos de ataques pueden convertirse en lo más importante para ayudarnos a obtener resultados.

En ese momento, ha llegado el momento de continuar con algunas de las cosas que podemos hacer con el marco Kali Linux. Esto a menudo se considera extraordinario en comparación con otros marcos de trabajo de codificación con los que trabajar, y dejaremos de lado el esfuerzo para analizar cuál es el problema aquí y cómo podemos utilizarlo para nuestras necesidades. En esta parte, echaremos un vistazo

en las razones por las que a las personas les gusta trabajar con Linux, cómo instalar Kali Linux, cómo trabajar con Kali en una máquina virtual si esta es la mejor opción para nosotros, e incluso cómo configurar Kali Linux, para que esté preparado para una parte de los asaltos que tenemos que hacer.

Esto es solo el comienzo de lo que podemos hacer con respecto a la piratería. Ya que hemos preparado el escenario y en su mayor parte estamos listos con una parte de esto, ha llegado el momento de ir un poco más allá y echar un vistazo a algunas de las cosas ingeniosas que podemos utilizar Kali Linux para ayudarnos. fuera con Veremos cómo controlar y tratar nuestras organizaciones, la importancia de los cortafuegos, cómo obtener datos de los usuarios cuando los necesitamos, el uso de Kali Linux en algunos de los dispositivos compactos que necesitamos usar e incluso cómo trabajar con MalDuino y Kismet.

Sin embargo, esto no es todo. Vamos a investigar algunos de los medios con los que podemos trabajar cuando llegue el momento de hackear una organización de nuestra elección y recopilar la información que podamos necesitar. Para completar este manual, también vamos a invertir algo de energía analizando cómo podemos eludir un SSHS secreto, cómo piratear los marcos remotos WPA y WPA2, cómo utilizar una parte de los diferentes dispositivos disponibles para garantizar que te mantengas encubierto y que nadie quiera seguir los ataques hasta ti, y cómo podemos utilizar Metasploit para ayudarnos a completar nuestras propias pruebas de ingreso.

Como podemos ver en este manual, hay una gran cantidad de partes que deben convertirse en un factor integral para que podamos terminar realmente el asalto con el que querríamos trabajar. Estas son varias técnicas que pueden hacer los programadores, las personas que acaban de salir del plástico y las personas que han estado en el juego durante bastante tiempo. En el momento en que espera proteger su propia organización o la organización de otra persona, o si desea piratear otra organización, se alegrará de tener estos dispositivos preparados para ayudarlo a completar este trabajo.

Hay un montón de cosas geniales que podemos hacer cuando ha llegado el momento de trabajar en el camino hacia la piratería y tener todo esto listo y todas las configuraciones pueden ser quizás la mejor técnica que puede decidir para asegurar su propia organización. En el momento en que esté listo para estudiar piratería y la totalidad de las herramientas y métodos que podemos utilizar mientras pirateamos junto con el marco Kali Linux, asegúrese de leer este manual para comenzar.

Hay muchos libros sobre este tema en el mercado, ¡gracias de nuevo por elegir este! Se hizo todo lo posible para garantizar que esté lleno de la mayor cantidad de información útil posible; ¡Por favor, disfruta!

Capítulo 1

Definición de Hacking y Tipos de Hackers

El camino hacia la piratería incluye obtener acceso no autorizado a un marco de PC o una colección de marcos de PC. Los programadores obtienen acceso a los marcos descifrando códigos o contraseñas. El método que usan los programadores para obtener el código o la clave secreta se está rompiendo y un programador es alguien que adopta el camino hacia la piratería. Los programadores pueden piratear una cuenta de correo electrónico, una página web de medios basada en la web, un sitio, una organización LAN completa o una reunión de marcos. Eventualmente, es a través de programas de cálculos de claves secretas que los programadores obtienen acceso a una frase secreta.

Para cada una de sus necesidades diarias, las personas y las organizaciones utilizan PC o PC. Para una progresión constante de las aplicaciones y los datos comerciales, algunas asociaciones tienen WAN, organización de territorio amplio, sitio o espacio, o una organización de PC. Por lo tanto, existe una apertura de alto riesgo de estas organizaciones a los programadores al igual que el resto del universo de la piratería.

Propósito de la piratería

Generalmente, el objetivo de ciertos programadores es causar cierto daño económico o de reputación a un elemento, grupo o individuo a través de su

expectativa nociva o criminal. Lo logran mediante la difusión de informes nocivos o inexactos que pueden causar la interrupción del negocio después de que roban sus activos o toman su información clasificada. Las organizaciones pueden terminar en algunas circunstancias socialmente negativas con estos datos engañosos. Además, como propio de la ley, el hacking es un tipo de ciberdelito o ciberdelito. No obstante, las organizaciones legales gubernamentales y las fundaciones certificadas explícitamente participan en otro lado de la piratería a nivel de expertos. En este caso, probablemente evitarán que la gente haga travesuras o contrarresten algunas expectativas inaceptables de los programadores. Además, este tipo de piratería se realiza para asegurar y salvar a los residentes y la sociedad en libertad.

Tipos de piratas informáticos

Es muy fundamental para nosotros separar los destinos y las partes de los programadores conociendo sus tipos para obtener detalles sobre los objetivos sugeridos anteriormente.

hacktivista

Dejar datos desagradables en un sitio que piratean es el punto focal de este tipo de programadores. Lo hacen para difundir mensajes estrictos, sociales y políticos. Además, estos programadores pueden centrarse en diferentes países.

sombrero gris

Este tipo de programadores no tienen intención de engañar cuando acceden a un marco sin aprobación. Se encuentran entre los programadores de tapas de alto contraste. El objetivo de estos programadores es mostrar a los socios del framework partes de sus deficiencias y debilidades.

Hacker ético

El objetivo de este tipo de programadores es eliminar y reconocer las deficiencias sospechosas. Examinan los marcos al obtener acceso como programadores autorizados y percibidos por pasos y también se los conoce como gorra blanca. Algunas cosas que también hacen es recuperar

datos básicos necesarios para fines de seguridad, descifrar códigos hostiles a arreglos sociales o ilegales, y evaluación de debilidades. Son especialistas pagados, afirmados y preparados.

Los programadores morales son las personas solitarias a las que se les permite hacer este tipo de piratería legítimamente. Conocen tipos similares de reglas a seguir como un programador de gorra oscura y utilizarán una parte de pensamientos similares en el camino. Sin embargo, en su mayoría han obtenido el consentimiento para pasar y hacer una parte de estas alternativas, en lugar de intentar hacerlo para obtener su propio beneficio.

Para el programador moral, el objetivo es mantener el marco lo más libre posible de cualquier peligro en el camino. Necesitan asegurar su propia organización o la organización de otra persona que entienda lo que son aquí. Esto hará que sea más fácil para ellos ingresar a la organización sin hacerlo de manera ilegal. Estos programadores utilizarán muchas estrategias similares para sus ataques, como vemos con una parte de otros tipos de programadores. Esto implica que dependerán de las pruebas de ingreso, delineando asaltos, y eso es solo el comienzo. En cualquier caso, lo harán como una forma de ayudarles a determinar dónde están las debilidades del marco en lugar de echar un vistazo a las formas en que puede hacer un mal uso de ellas.

Galleta

Estas son gorras oscuras. Aseguran la sección en sitios u organizaciones de PC de una manera no aprobada y con un objetivo de mala fe. Además, existe una conexión de aumento individual en sus expectativas a través de la infracción de los derechos de garantía para lucrar con asociaciones delictivas, la toma de activos de los saldos financieros en línea, la toma de datos privados autorizados, etc. Hoy en día, estos programadores participan en sus ejercicios de manera oscura y tener un lugar con esta clasificación.

Tipos de piratería

Los peligros que los sitios deben administrar son los peligros más sucesivos absolutos de la piratería. Los programadores participan durante el tiempo que pasan revelando el contenido de un sitio o cambiando con el uso de acceso no autorizado. Las personas o reuniones que están en contra de las asociaciones sociales o políticas más

ocasiones se centran en sus sitios. Asimismo, piratean sitios de datos públicos o legislativos, y esto es completamente normal. Estas son algunas de las técnicas normales de piratería que utilizan en los sitios:

Suplantación de DNS

Aquí y allá, los clientes pueden ignorar la información de la reserva de un área o sitio, y esta estrategia para piratear utiliza esta información de la tienda. En ese momento, dirige la información hacia otro sitio vengativo.

robo de galletas

Las golosinas contienen contraseñas de inicio de sesión, datos secretos, etc., y con el uso de códigos nocivos, los programadores se acercarán al sitio para tomar golosinas. En el momento en que una organización genuina los utilice, los ayudará a brindarle una ayuda superior en general. Sin embargo, almacena una tonelada de datos adicionales sobre usted y su marco, y si el programador puede tomar estas delicias, en realidad querrá utilizarlas de la forma que desee. Esto puede ser peligroso y es una explicación integral de que a menudo es mejor matar y debilitar el uso de golosinas en cualquier caso.

Reparación de interfaz de usuario

Los programadores utilizan esta técnica creando una interfaz de usuario falsa. En consecuencia, los clientes serán coordinados a otro sitio de principio a fin cuando hagan clic para ir a un sitio en particular.

Virus

Cuando los programadores obtienen acceso a un sitio en particular, descargan una infección en los registros del sitio. Sus objetivos son arruinar los activos o datos en dicho sitio. Hay muchos tipos de infecciones con las que podemos juntarnos, y se pueden propagar a través de conexiones de correo electrónico, sitios que han sido socavados y más.

Estas infecciones pueden asumir el control de la PC, cerrar registros, tomar datos y, en cualquier caso, propagarse a una parte de los contactos que usted

tenga en su marco para obtener los datos que los programadores podrían querer tener. Esta es la razón por la que es tan imperativo revisar y tener cuidado con los tipos de sitios que abre, y asegurarse de no acceder a sitios que puedan dañar su PC.

Suplantación de identidad

Utilizan esta técnica para repetir el primer sitio y, por lo tanto, los programadores aprovecharán y abusarán efectivamente de los datos del cliente despistado, como sutilezas de Mastercard, frases secretas de cuenta y, por lo tanto, algunos más.

Por lo general, estos se enviarán por correo electrónico. El correo electrónico aparecerá como si viniera de una fuente genuina, por ejemplo, su banco u otro sitio en el que invierte algo de energía, solicitándole que mire un mensaje o cambie su nombre de usuario y palabra secreta.

Dado que el programador trabaja muy duro para ocultar cosas y hacer que parezcan oficiales, las personas no tardan tanto en ser arrasadas. De hecho, incluso el sitio se verá genuino, por lo que no es difícil tocar las diversas cosas e ingresar los datos. Si alguien sucumbe a esto, el programador puede tomar la totalidad de esa información y usarla para realmente ingresar a su registro que pueda necesitar.

¿Cómo obtienen acceso los piratas informáticos a los sistemas informáticos?

Podemos obtener datos trabajando y hablando con otros a través de la ayuda de algunos héroes en el mundo de la PC que forman organizaciones. Y luego, por una variedad de razones, tenemos algunas personas no muy buenas que causan inconvenientes al usar sus PC para colarse en esas organizaciones. Estos arreglos de personas son programadores y parte de las cosas en las que participan incluyen:

- Cierra un sitio web creando mucho tráfico hacia él
- Obtener información de la tarjeta de crédito
- Obtener contraseñas
- robar secretos

Independientemente de si trastornando lo mismo de siempre o tomando datos para sus

beneficio, los programadores están trabajando constantemente. De vez en cuando, siempre habrá noticias sobre ellos y, en un momento dado, es probable que te estés preguntando qué es exactamente lo que están haciendo los programadores. Continuamente ingresan al marco tomando contraseñas. Para quebrantar la seguridad de una organización, el primer paso para ellos es descubrir una frase secreta. En consecuencia, para que su frase secreta sea difícil de descifrar para cualquiera, es muy útil transformarla de manera consistente. Para que entiendas lo que hacen los programadores cuando las personas los examinan, aquí hay algunos términos clave que probablemente te des cuenta:

- **Caballo de Troya:** este método da la impresión de ser un programa útil y se engaña a los clientes para que hagan clic y lo abran.
  Sin embargo, las PC de dichos clientes pueden sufrir ataques imprevistos que pueden estar en segundo plano o pasar desapercibidos. Dado que estos se colarán en la PC a través de técnicas secretas, por ejemplo, estar en un programa que parece ser genuino, es difícil identificarlos. En cualquier caso, cuando el troyano ingresa al marco, puede abrir pasajes secundarios y otras cosas para ayudar al programador a obtener los datos que necesita.

- **Secuestro de sesión:** este proceso consiste en que los programadores incrustan paquetes de información maliciosa en una transmisión de información real a través de la asociación web.
- **Script kiddie:** estos son programadores simples o jóvenes que actúan como programadores genuinos mientras utilizan los instrumentos de los programadores. Estas personas no pensarán tanto en averiguar cómo hackear. Quieren terminar un asalto, pero en realidad no piensan a menudo en los rudimentos que lo acompañan o los códigos que deben utilizar. En igualdad de condiciones, simplemente tomarán una parte de los instrumentos y proyectos que ahora están disponibles y los utilizarán para cuidarlos. Simplemente necesitan terminar el pirateo y recibir los datos a cambio, sin angustiarse por aprender ninguna de las estrategias en el camino.

- **Root kit:** un intruso puede camuflarse y aumentar su autoridad sobre su sistema utilizando esta disposición de herramientas.
- **Acceso root:** para cualquier programador que trabaje con un framework, el acceso root es el nivel de acceso más elevado. El acceso a la raíz es el más buscado por los programadores genuinos en un marco de PC.

- **Gusano de correo electrónico:** los programadores utilizan un mensaje de correo electrónico de aspecto característico para enviar un pequeño programa o contenido cargado de infección a una víctima despistada.
- **Ataque de denegación de servicio:** los programadores utilizan esta técnica para inundar un sitio con tráfico falso, lo que impide la ubicación de la persona en cuestión o impide que se ocupe de su tráfico normal. Este rechazará al trabajador de una organización específica y puede dificultar que los clientes genuinos accedan al marco de cualquier manera. Esto le permite al programador tener la oportunidad de dejar un troyano o un pasaje secundario o algo diferente en esa organización.
    - **Denegación de servicio distribuida:** esta será algo única ya que utilizará más de una PC para realizar el ataque. En el DoS, el programador simplemente está usando una PC, y el firewall generalmente puede ver esa dirección IP y dejará de permitir la ayuda desde esa dirección. Con el DDoS, el programador está utilizando varias PC para hacer el ciclo, lo que dificulta que el firewall detenga el ataque.
- **Desbordamiento de búfer:** los programadores utilizan esta estrategia abrumando el soporte de la aplicación para transmitir órdenes maliciosas a un marco.
- **Puerta trasera:** los programadores obtienen acceso a un sistema de PC utilizando este camino misterioso. Los engaños, las infecciones y otros tipos de malware pueden ingresar y usar esta opción para ayudarlos a ingresar al sistema y regresar y reenviar tantas veces como deseen. Si está intentando asegurar su propia PC u otro marco, asegúrese de que cuando haya terminado por completo, arregle todo para que no haya pasajes secundarios potenciales para que un programador pase.

Protección contra la piratería

Un peligro diligente que influye constantemente en la seguridad de un país y sus residentes es la piratería. A nivel de la persona, cuando los programadores borran todos los merecidos fondos de reserva monetaria de alguien, puede traer desgracias monetarias indecibles. Asimismo, puede provocar repercusiones de largo recorrido y grandes desgracias monetarias a través del robo de información a nivel jerárquico. Es vital bloquear este terrible peligro y defenderlo.

Hay un montón de cosas que puede hacer para asegurarse de que puede proteger su propia organización contra otro programador. Configurar esto bien y ser cauteloso acerca de cómo actuará su propia organización será esencial para mantener alejados a los programadores. Una parte de los diversos avances que puede realizar para prepararse para cualquier programador que desee ingresar a su organización incluirá:

1. Tenga cuidado con los mensajes que utiliza. Muchos de los ataques que investigaremos en este manual se ejecutarán con la ayuda del correo electrónico. Esto no es correcto constantemente. Sin embargo, si eres cauteloso con una parte de los mensajes que abres, especialmente las conexiones, entonces puedes evitar muchos de estos ataques de un programador.
2. Elija algunas contraseñas sólidas que sean más diligentes para descifrar o superar con un ataque de poder de bestia. Elija contraseñas largas, utilice una combinación de letras, números e imágenes, y otras que no se relacionarán con usted o simplemente para especular todo. Numerosos programadores comenzarán intentando asaltar sus contraseñas ya que esta es una parte endeble de su seguridad. Puede arreglar esto con la ayuda de una palabra secreta sólida.
3. Realice una prueba de infiltración para buscar una parte de las debilidades que se encuentran en el marco. Investigaremos cómo trabajar con pruebas de infiltración, más adelante, sin embargo, este es un método extraordinario para determinar qué aplicaciones puede intentar usar el programador para ingresar a su organización. Hacer uno por ti mismo te ayudará a mantenerlo seguro.
4. Cambie las contraseñas constantemente. En el momento en que cambias el

frase secreta constantemente, es mucho más difícil para el programador pensar en lo que es o utilizar una parte de diferentes estrategias para superar la ruptura de claves secretas con la ayuda de la frase secreta.

5. No ofrecer datos de la organización a ninguna otra persona. Cualquier dato significativo y delicado sobre su organización debe mantenerse en secreto y encubierto. Cuantas más personas piensen en su organización, más probable es que los datos salgan a la luz y que un programador quiera usarlos.
6. Considere codificar los datos que envía a otros en su intercambios Esto hace que sea difícil para cualquier persona que no tenga la clave correcta leer detenidamente los datos que está enviando, independientemente de si se capturan.
7. Elija una convención de seguridad sólida para proteger su organización. Asegúrese de no estar trabajando con la opción WEP, ya que esta suele ser más fácil de superar para un programador. Si bien WPA y WPA2 siguen siendo opciones indefensas contra un asalto, están mucho más conectadas a tierra y pueden mantenerlo más seguro en el camino.

8. Utilice malware enemigo y contra la programación de infecciones. Esto hará que sea más difícil para cualquiera de los ataques que el programador está intentando enviar a su enfoque para pasar.
9. Asegúrese de actualizar su producto y trabajar marco con la frecuencia que sea necesaria. Estas actualizaciones ayudarán a eliminar una parte de las debilidades que se encuentran en el marco de trabajo que usa y otra programación, por lo que hacer la actualización hará que sea más difícil para un programador acceder a su marco.

Como debería ser obvio, habrá un montón de alternativas con las que puede trabajar cuando llegue el momento de asegurarse de que su PC contraste con una parte de los hacks que vienen en su dirección. Asegúrese de trabajar con una parte de estas opciones, y encontrará que es significativamente más difícil para un programador acceder a su marco y usarlo para su propio beneficio.
ruta.

Capitulo 2

La seguridad cibernética

El acto de proteger la información, las organizaciones, los marcos electrónicos, los teléfonos móviles, los trabajadores y las computadoras de ataques vengativos es la seguridad de la red. Además, se refieren a ella como seguridad de datos electrónicos o seguridad de innovación de datos. Las clasificaciones básicas pueden encontrar un camino en los términos como una variedad de configuraciones, desde portátiles hasta procesamiento comercial.

- El factor de seguridad de red más excéntrico es la capacitación del cliente final. En el momento en que las personas se olvidan de seguir los ensayos de seguridad sólidos, coincidentemente pueden familiarizar una infección con un marco generalmente seguro. De esta manera, es muy fundamental para la seguridad de cualquier asociación enseñar a sus representantes a no conectar unidades USB no identificadas y borrar conexiones de correo electrónico dudosas.

- Por cualquier motivo de pérdida de información o de actividades, la forma en que una asociación reacciona ante un incidente de seguridad en la red es la congruencia empresarial y la recuperación de la calamidad. Además, para que la asociación vuelva a un límite de trabajo similar al que tenía antes del evento, los ciclos que dirigen cómo la asociación restablece sus datos y actividad son los métodos de recuperación de catástrofes.
  Si bien la asociación se esfuerza por funcionar sin patrimonio explícito, la asociación tiene un arreglo con el que cuenta, que es la congruencia empresarial.

- Las opciones y técnicas para asegurar y cuidar los recursos de información son la seguridad operativa. Esta interacción incorpora los ejercicios que determinan dónde y cómo se puede compartir o guardar la información y los consentimientos de los clientes al llegar a una organización.

- En el momento en que la información está en camino o lejos, la protección y la honestidad de la información están garantizadas por la seguridad de los datos.
- Que los dispositivos y la programación estén libres de peligros es el punto central de la seguridad de las aplicaciones. A pesar de que está destinado a proteger la información, una aplicación socavada podría dar

admisión a la información. Antes de la disposición de un dispositivo o programa, la etapa de planificación es el comienzo de una seguridad fructífera.

- Independientemente de si un ataque puede provenir de un malware empresarial o estar enfocado en los agresores, el acto de obtener una red de PC de los intrusos es la seguridad de la organización.

Escala de amenazas cibernéticas

Constantemente, el gobierno de los EE. UU. gasta alrededor de $ 19 mil millones en protección en línea. En cualquier caso, la velocidad a la que se desarrollan los ataques digitales es muy rápida. Según NIST, el Instituto Nacional de Estándares y Tecnología, se recomienda la observación continua de todos los activos electrónicos para ayudar en el reconocimiento temprano y combatir la expansión del código vengativo. La seguridad de la red contrarresta tres peligros de superposición y son:

1. Para razonar pavor o frenesí, el ciberterror espera subvertir la electrónica marcos
2. La mayoría de las veces, la recopilación de datos de inspiración política está relacionada con ataques digitales. 3. Con fines de lucro o para causar disturbios, las reuniones o los artistas individuales pueden apuntar a marcos a través del delito cibernético.

Ransomware, troyanos, spyware, gusanos e infecciones son algunas de las estrategias habituales que utilizan los agresores para controlar organizaciones o PC. Para la recopilación de información secreta, utilizan troyanos y software espía y para dañar o auto imitar sistemas o registros. Usan gusanos o infecciones. Todos los datos del cliente están codificados por ransomware, que se mantiene firme para tener la oportunidad de hacerlo, y para el uso para obtener acceso a sus datos codificados, habrá solicitudes de instalación. Una descarga de aspecto real puede contener una carga útil de malware y la utilizan junto con una conexión de correo electrónico espontánea para propagar código nocivo.

Independientemente del tamaño, todas las empresas tienen algo razonable la protección de la red. Últimamente, el gobierno, el dinero, el montaje y la atención médica son algunas de las empresas que registraron la mayoría de los ataques cibernéticos. Dado que estas empresas recopilan información clínica y monetaria, algunas de estas áreas son más interesantes para los ciberdelincuentes. En cualquier caso, también pueden enfocarse en todas las organizaciones que utilizan redes para ataques de clientes, secretos corporativos

actividades e información del cliente.

Más que antes, el mundo depende de la innovación. Por lo tanto, hay una inundación en la creación de información computarizada. Hoy en día, los gobiernos y las organizaciones utilizan las PC para almacenar gran parte de esa información, y la envían entre organizaciones a diferentes PC. Hay debilidad en los dispositivos y sus marcos ocultos que sabotean los destinos y la fuerza de una asociación cuando se usan incorrectamente. Para cualquier negocio, puede haber un alcance de pulverizar resultados con una penetración de datos. A través de la falta de confianza del cómplice y del comprador, y la ruptura de la información puede desenredar la posición de una organización. Una organización puede perder el control debido a la deficiencia de información esencial, por ejemplo, innovación con licencia o documentos de origen. Además, debido a la rebeldía con las normas de seguridad de la información, los ingresos corporativos pueden verse afectados por la penetración de la información. Unos 3,6 millones de dólares es el gasto normal que una ruptura de noticias puede costarle a una asociación influenciada. Es muy básico para las asociaciones llevar a cabo y recibir un enfoque sólido de seguridad de la red con rupturas de información prominentes que se destaquen como verdaderamente de interés periodístico.

Avance de la Ciberseguridad

El punto focal de la protección de red convencional está en la ejecución de esfuerzos de protección alrededor de un borde caracterizado. BYOD, Traiga su propio dispositivo y los teletrabajadores son las nuevas actividades de habilitación que han consumido la superficie de ataque, han reducido la visibilidad del movimiento digital y han roto el límite. Hoy, a pesar de los niveles récord de gasto en seguridad, hay un rápido aumento en los descansos. El énfasis está en la protección en línea impulsada por humanos para una asociación mundial. Es otra metodología que, en lugar de un gran número de peligros en desarrollo, se centra en cambios en la conducta del cliente. Donde reside la información, la seguridad de la red impulsada por humanos amplía los controles de seguridad en todos los marcos y brinda información sobre la forma en que un cliente final coopera con la información en cualquier caso, cuando la asociación no está a cargo únicamente. Eventualmente, para reducir los tiempos de identificación y examen de los peligros, así como para enfocar y sacar a la luz los peligros más reales, esta metodología pretende distinguir las peculiaridades de la conducta.

Protección del usuario final

De todos modos, ¿cuáles son los esfuerzos de seguridad que brinda la protección en línea a los marcos y clientes? En primer lugar, para codificar registros, mensajes y otra información imprescindible, la protección de la red depende de las convenciones criptográficas. Este procedimiento no solo protege contra robos o accidentes, sino que también protege los datos en el camino. Del mismo modo, la programación de seguridad del cliente final verifica la PC en busca de bits de código malicioso, aísla este código y luego lo borra del sistema. Para el código malicioso encubierto en MBR, Master Boot Record con un plan específico para borrar o codificar datos del disco duro de las PC, los proyectos de seguridad también pueden eliminarlos después de haberlos identificado. También hay un énfasis en la ubicación continua de malware por medio de convenciones de seguridad electrónica.

Para que algunos evalúen la conducta de un programa y su código para protegerse contra troyanos e infecciones que cambian de forma con cada ejecución, tanto malware transformativo como polimórfico, utilizan el examen social y la heurística. Desde la organización de un cliente, los proyectos de seguridad pueden restringir los proyectos posiblemente perniciosos a una bolsa de aire virtual para descubrir cómo identificar con mayor probabilidad nuevas contaminaciones y diseccionar su comportamiento. Además, a medida que los especialistas en protección de redes identifican mejores enfoques para combatir nuevos peligros, los programas de seguridad continúan desarrollando nuevas salvaguardias.

Capítulo 3

Tipos de ataques cibernéticos

Con el uso de algunos procedimientos para aniquilar, modificar o tomar datos o marcos de información, cualquier actividad enfocada en hostil que se centre cerca de casa, dispositivos de PC, bases o marcos de datos de PC es un ataque cibernético. De inmediato, aquí hay una parte de los ciberataques básicos de hoy:

Ataque de cumpleaños

La realización de los ataques de cumpleaños se basa en cálculos hash que las personas utilizan para afirmar la respetabilidad de una marca avanzada, programación o mensaje. Un MD de longitud fija, resumen de mensaje, que está libre de la longitud del mensaje de información, se crea mediante un mensaje de trabajo hash preparado. El mensaje tiene los atributos de este MD en particular. La probabilidad de descubrir dos mensajes irregulares es la referencia para el asalto de cumpleaños, que, cuando se maneja con un trabajo hash, produce un MD similar. El agresor puede suplantar con seguridad el mensaje del cliente con el suyo si el agresor determina un MD similar para el mensaje que tiene el cliente.

Además, independientemente de que miren los MD, el beneficiario no reconocerá la sustitución.

Ataque de espionaje

Los agresores capturan el tráfico de la organización para que se produzca el asalto de espionaje. Para algunos datos secretos que un cliente puede estar enviando absurdamente, por ejemplo, números y contraseñas de Mastercard, un agresor puede adquirir esa información escuchando. Hay dos tipos de agresores fisgones, y son dinámicos y separados:

- Espionaje activo: mediante el envío de consultas a los transmisores, los agresores se enmascararán a sí mismos y a las unidades dispuestas mientras sustraen efectivamente los datos. Llaman a esta interacción alterar, filtrar o probar.

- Escuchas pasivas: cuando los agresores sintonizan el mensaje

transmisión en la organización, reconocerán los datos.

Además, dado que liderar el espionaje latente antes de los ataques dinámicos requiere que el agresor adquiera información sobre las unidades bien dispuestas, es muy importante que detectar los dinámicos para identificar los ataques de espionaje no involucrados. Para prepararse para escuchar, la mejor contramedida es el cifrado de la información.

XSS, ataque de secuencias de comandos entre sitios

Para ejecutar aplicaciones o contenidos programables en el navegador de Internet de la persona en cuestión, son los activos web externos los que utilizan los ataques XSS. Básicamente, el agresor utilizará JavaScript pernicioso al infundir una carga útil en la base de información de un sitio. Utilizando la carga útil del agresor como un componente del cuerpo HTML, el sitio comunicará la página al programa de la víctima para ejecutar el contenido nocivo cuando la víctima demande una página del sitio. Por ejemplo, el agresor puede utilizar la golosina del trabajador del agresor después de retirarla para capturar el encuentro cuando envía esta golosina a la persona en cuestión. Cuando usan XSS para abusar de una mayor debilidad, puede haber los resultados más riesgosos.

Los agresores pueden manejar y acceder a la máquina de la víctima de forma remota, recopilar datos a medida que encuentran la red, capturar capturas de pantalla o registrar pulsaciones de teclas, así como recibir premios a través de estas debilidades. Dado que existe una amplia ayuda para JavaScript en la web, generalmente es el más manipulado, mientras que, dentro de Flash, ActiveX y VBScript, pueden explotar XSS.

Los ingenieros pueden desinfectar la información cuando los clientes en una demanda HTTP antes de reflejarla para protegerse contra ataques XSS. Además, antes de repetir cualquier cosa al cliente, es crucial asegurarse de que toda la información se obtenga, se tamice y se apruebe, incluidas las estimaciones de los límites de las preguntas durante las búsquedas. Caracteres extraordinarios como >, <,/, y ?, los espacios se pueden cambiar a su propia URL codificada como HTML. Los clientes pueden tener la opción de paralizar el contenido del lado del cliente.

Ataque de inyección SQL

Para los sitios basados en información, un problema básico es la infusión de SQL.
La interacción ocurre cuando, de cliente a trabajador, un

evildoer ejecuta una consulta SQL a la base de información a través de la información de información. Para ejecutar órdenes SQL predefinidas, es factible incorporar órdenes SQL en la contribución del plano de información, por ejemplo, en lugar de la frase secreta o el inicio de sesión. Del conjunto de datos, la información delicada puede ser mal utilizada por una infusión de SQL efectiva. Asimismo, puede dar órdenes al marco de trabajo, recuperar la sustancia de un documento determinado, ejecutar actividades de organización como el cierre de la base de datos y ajustar (borrar, actualizar o agregar) la información del conjunto de datos. Por ejemplo, el registro de un cliente puede ser mencionado por una estructura web en un sitio, y luego para extraer los datos de la cuenta asociada utilizando SQL dinámico, enviarlo a la base de datos. La interacción puede dejar una apertura para los agresores en cualquier caso, cuando esto funciona para los clientes que están ingresando adecuadamente su número de registro.

No hay una calificación particular entre los planos de información y control con la debilidad de este tipo de ataque de protección de red.
En consecuencia, si un sitio usa SQL dinámico, las infusiones de SQL pueden funcionar en su mayor parte. Además, debido a la frecuencia de las interfaces utilitarias más establecidas, la infusión de SQL es muy común con las aplicaciones ASP y PHP. Además, debido a la accesibilidad de la naturaleza de la interfaz automática, las infusiones SQL más inciertas y mal utilizadas son ASP.NET y J2EE. En su base de datos, aplique el modelo de consentimiento de privilegios mínimos para protegerse de los ataques de infusión de SQL. Es crucial no incorporar ningún SQL poderoso mientras se aferra al ciclo y las preguntas definidas para las articulaciones preparadas. Además, para prevenir ataques de infusión, necesitará una base de datos sólida para el código ejecutado. Asimismo, a nivel de aplicación, es fundamental aprobar la información de entrada contra una lista blanca.

Ataque de contraseña

Obtener contraseñas suele ser el método de ataque básico y exitoso, ya que para verificar a los usuarios en un marco de datos, las contraseñas son el sistema más comúnmente utilizado. A través de la especulación interna y externa, el acceso a un conjunto de datos de palabras secretas, el uso de diseño social, la obtención de contraseñas decodificadas al olfatear la asociación con la organización o el control del área de trabajo de una persona, los agresores pueden acceder a la palabra secreta de una persona. En ese momento, pueden utilizar un preciso o irregular

manera de ejecutar la última metodología.

- Utilizando el asalto de referencia de palabra, los esfuerzos de asalto para acceder a la organización o PC de un cliente utilizando una referencia de palabra de contraseñas regulares. Los agresores pueden analizar los resultados después de aplicar un cifrado similar a una referencia de palabra clave secreta comúnmente utilizada mientras duplican un documento codificado que contiene las contraseñas.

- Los atacantes pueden confiar en que una clave secreta funcionará después de utilizar una forma irregular de tratar con varias contraseñas supuestas.
  Este ciclo se llama potencia bruta. La interacción en general será inteligente para los agresores cuando utilicen actividades de ocio, cargo, trabajo, nombre y términos similares de la persona para descifrar contraseñas identificadas con la persona.

Una estrategia de bloqueo de registro que bloqueará su registro después de algunos esfuerzos de palabras secretas no válidas es todo lo necesario para protegerse del poder animal y los ataques de referencia de palabras.

Ataque en coche

El método generalizado para propagar malware son los ataques de descargas no autorizadas. En una de las páginas, los agresores tendrán contenido vengativo plantado en código PHP o HTTP. Con esto plantado, el contenido podría desviar a la víctima a un sitio restringido por los programadores o podría introducir malware directamente en la PC del visitante. Cuando un topógrafo visita una ventana emergente o un mensaje de correo electrónico o cuando visita un sitio, pueden ocurrir descargas ocultas. Puede contaminarse con un ataque desde un vehículo sin importar si no abre una conexión de correo electrónico maliciosa o presiona un botón de descarga. Para que pueda potenciar el asalto, es posible que no necesite hacer nada, lo que hace que el asalto desde un vehículo no sea lo mismo que otros tipos de ataques de protección de red. Debido a la ausencia de actualizaciones o actualizaciones ineficaces, una descarga oculta puede explotar un navegador de Internet, un marco de trabajo o una aplicación que contenía imperfecciones de seguridad.

Es posible que deba mantenerse alejado de los sitios que podrían contener código nocivo y mantener sus marcos de trabajo o programas con visión de futuro para monitorearse contra los ataques de vehículos en movimiento. Aunque esos sitios son responsables de

piratería, intente adherirse a las configuraciones regionales que usa con regularidad. Además, borre constantemente aplicaciones o proyectos inútiles de su dispositivo. Los ataques desde vehículos pueden abusar de una mayor debilidad en su sistema cuando tiene más módulos.

Ataques de Phishing y Spear Phishing

La razón de un ataque de phishing es impactar a los clientes para lograr algo u obtener información personal mediante el envío de un correo electrónico que parece provenir de fuentes confidenciales. Este tipo de asalto utiliza astucia especializada y diseño social. El malware se puede apilar en su PC a través de una conexión de correo electrónico. Además, puede ser engañado para que entregue sus propios datos o luego descargue nuevamente el malware a través de una conexión a un sitio mal concebido. Una acción de phishing muy enfocada es el skewer phishing.
Se introduce un toque de exploración en los objetivos por parte del agresor, tras lo cual se elaboran mensajes significativos e individuales. Lance phishing parece, según todos los informes, ser muy difícil de reconocer, y protegerse contra él también puede ser más entusiasta. El simulacro de correo electrónico es quizás la metodología más sencilla que usan los programadores para dirigir un ataque de phishing. Hacen que el correo electrónico parezca que proviene de una persona real como su cómplice o los ejecutivos, ya que han tergiversado los datos en el segmento "De" del correo electrónico. Asimismo, la clonación de sitios es otra técnica que utilizan los estafadores para implantar validez a su historia. Lo engañarán para que ingrese calificaciones de inicio de sesión o datos realmente reconocibles, PII.

Aquí hay algunas estrategias en las que puede participar para eliminar el peligro del phishing:

- **Sandboxing:** puede utilizar un clima de sandbox para probar la sustancia del correo electrónico, tocando las conexiones dentro del correo electrónico o registrando la acción al abrir la conexión . **Análisis de encabezado**
- **de correo electrónico:** cómo llegó un correo electrónico a su ubicación es la razón de los encabezados de correo electrónico. Como se expresa en el correo electrónico, debe haber una similitud en el área de los límites "Return-Path" y "Respuesta a".
- **Al pasar el cursor sobre los enlaces:** no intente hacer clic cuando

mueva el mouse sobre la conexión. Sabrá a dónde lo llevará realmente cuando pase el mouse sobre la conexión, y para traducir la URL, debe aplicar un razonamiento básico.

- **Pensamiento crítico:** dado que tiene otros 200 mensajes no iniciados en su bandeja de entrada o está concentrado u ocupado, considerará que un correo electrónico es un artículo genuino. Necesitará un momento para investigar el correo electrónico.

MitM, ataque de hombre en el medio

En el caso de que un programador se plante entre un trabajador y los intercambios, se está produciendo un ataque de MitM. Una parte de los tipos de asalto del hombre en el centro incluyen: **Repetición**

Los agresores pueden imitar a uno de los miembros bloqueando y guardando mensajes antiguos y tratar de enviarlos más tarde; posteriormente, se está produciendo un asalto de repetición. Puede utilizar una cadena que cambie más tarde o un número arbitrario para contrarrestar qué nonce o las marcas de tiempo de la reunión para contrarrestarlo fácilmente.

Suplantación de IP

La ridiculización de IP ocurre cuando un marco le da acceso al agresor, imaginando que está hablando con un elemento conocido y confiable. Un host objetivo obtiene un host conocido y confiable del agresor quien, en lugar de su propia dirección IP de origen, envía un paquete con dicha fuente IP. Es factible que el anfitrión objetivo haga un seguimiento después de tolerar el paquete.

Secuestro de sesión

Entre el trabajador de la organización y un cliente de confianza, los agresores pueden capturar una reunión en este tipo de ataque MitM. Si bien la condena del trabajador es la de la correspondencia con el cliente a medida que se procede a la reunión, habrá una sustitución de la dirección IP del PC agresor por la del cliente confiado. Por ejemplo, la interacción del asalto puede ir

por lo tanto:

1. Existe una asociación por parte del cliente a un trabajador.
2. El control del cliente es adquirido por el PC del agresor.
3. La PC del agresor desvincula al cliente del trabajador.
4. El agresor utiliza su dirección IP para suplantar la de la dirección IP del cliente, de esta manera, ridiculizando las cantidades de arreglo del cliente.
5. Hay un discurso persistente por parte del PC del agresor con el trabajador, y la convicción del trabajador es que la correspondencia efectivamente procede con el cliente.

Para contrarrestar todos los ataques de MitM a partir de ahora, no hay ningún plan o innovación única para hacer la magia. En general, la protección viable contra los ataques de MitM es la afirmación y el cifrado computarizados, que garantizan la respetabilidad y la privacidad de los intercambios. En cualquier caso, ese cifrado probablemente no ayudará con la forma en que los agresores infundirán un ataque de hombre en el centro. Por ejemplo, la clave pública de un hombre llamado Greg podría ser bloqueada por un agresor y, en consecuencia, reemplaza esa clave como su clave. En ese momento, cualquiera podría utilizar accidentalmente la clave pública subtitulada por el agresor, pensando que está enviando un mensaje codificado a Greg. En consecuencia, el agresor puede leer detenidamente la directiva esperada para Greg y luego utiliza la clave codificada de Greg real para enviar el mensaje a Greg, y Greg nunca verá que el mensaje ha sido socavado. Asimismo, antes de enviar el mensaje a Greg, el agresor puede cambiar el mensaje. Eventualmente, dado el asalto de MitM, Greg aceptará que sus datos están seguros ya que está utilizando encriptación.

Actualmente, ¿cómo reconocería la responsabilidad de la clave pública entre ellos? Abordar un problema como este impulsa el avance de las capacidades de hash y los especialistas en autenticación. El procedimiento adjunto se puede usar cuando alguien necesita estar seguro de que un agresor no verá un mensaje que necesita enviar a Greg y que el mensaje seguramente provendrá de ese mensaje sin alteración por parte de un agresor:

1. La clave asimétrica será codificada por el individuo después de haberla creado con su propia clave pública.
2. Luego, el individuo avanzará la clave simétrica codificada para

Greg.

3. Después de eso, el individuo firmará cuidadosamente una capacidad hash de la mensaje que han procesado.
4. Luego, con el uso de la clave simétrica, la persona codificará el mensaje hash marcado y su mensaje y luego lo enviará todo a Greg.

5. Dado que solo Greg tiene la clave privada para descifrar el cifrado, Greg realmente querrá obtener la clave simétrica de la persona.

6. Dado que tiene la clave simétrica, el individuo solitario que puede descifrar el hash marcado simétrico y el mensaje codificado es Greg.

7. Y debido a que Greg puede contrastar el hash del mensaje recibido y marcó cuidadosamente uno y puede registrar el hash del mensaje recibido, Greg puede afirmar que el mensaje no ha sido ajustado.
8. Dado que solo la persona puede firmar el hash para que se confirme con la clave pública de la persona, Greg también puede demostrarse a sí mismo que la persona fue el remitente.

DoS, denegación de servicio y denegación distribuida de DDoS Ataques de servicio

Cuando los activos de un marco no pueden reaccionar a las demandas de soporte, significa que la negativa del ataque de la administración ha dominado dicho marco. Sin embargo, el atacante controla la programación maligna que ha contaminado en muchas otras máquinas host, el ataque de un DDoS también afecta los activos de un sistema. Los agresores no obtienen beneficio directo por la desautorización de la administración, en absoluto como los ataques que crearon para aumentar u obtener acceso. Los ataques DoS cumplen una parte de los atacantes. Sea como fuere, podría haber suficientes beneficios reales para los agresores si los activos atacados tienen un lugar con un competidor comercial.

Del mismo modo, para que los atacantes envíen otro tipo de ataque, generalmente provocarán ataques DoS para desconectar un sistema. Aquí hay una parte de los diferentes tipos de ataques DDoS y DoS:

botnets

Para que los programadores lleven a cabo ataques DDoS, pueden doblar una gran cantidad de marcos con malware utilizando botnets. Además, para realizar los ataques contra los marcos objetivos, utilizan estos bots o marcos zombis. En la mayoría de las ocasiones, estos superarán el límite de manejo y la capacidad de transferencia de datos del marco objetivo. Además, dado que las áreas de las redes de bots varían mucho, es posible que sea difícil seguir estos ataques DDoS. La moderación de las botnets puede surgir a través de:

- Utilizando el tamizado de apertura oscura. Antes de ingresar a una red segura, elimina el tráfico molesto. Se necesita el host del Protocolo de puerta de enlace fronteriza para avanzar en la dirección de actualizaciones a los conmutadores de ISP en caso de reconocer un ataque DDoS. En el siguiente rebote, la interfaz null0 hará que todo el tráfico se dirija directamente a los trabajadores de urgencias.

- Para denegar el tráfico de direcciones de caricatura, utilizando el tamizado RFC3704, cuya organización de origen correcta puede seguirse para ese tráfico. Por ejemplo, desde las direcciones de la lista bogon, los paquetes se eliminarán mediante la separación RFC3704.

Ping de ataque mortal

El ping de ataques mortales utiliza un tamaño de IP por encima del límite de 65 535 bytes para hacer ping a un sistema objetivo utilizando paquetes de IP. El paquete de IP es dividido por los agresores ya que no se permiten paquetes de IP de este tamaño. En ese momento, pueden ocurrir otros accidentes, así como inundaciones de apoyo cuando el marco objetivo vuelve a ensamblar el paquete. En el momento en que utiliza un firewall, puede bloquear el ataque del ping de la muerte ya que los paquetes de IP que se han dividido se verificarán para determinar el tamaño más grande.

Ataque de pitufo

Los asaltantes sumergen a una organización objetiva en el tráfico con el ICMP al igual que el uso de IP satirizando con este ataque. Los atacantes se enfocan en la transmisión de direcciones IP con la utilización de demandas de reverberación ICMP. En esa capacidad, la causa de estas demandas de ICMP proviene de la ubicación de una víctima parodiada. Por ejemplo, para que los agresores comuniquen la dirección 10.255.255.255, el agresor parodiaría una ICMP

demanda de reverberación de 10.0.0.10 si la dirección de siniestro propuesta es 10.0.0.10. Todas las direcciones IP en el alcance recibirán esta solicitud y dominaría a la organización ya que todas las reacciones regresan a 10.0.0.10. Esta estrategia no solo puede generar una gran cantidad de bloqueo organizacional, sino que también puede robotizarse, ya que muy bien puede ser repetible. Es posible que deba paralizar las transmisiones coordinadas por IP en los conmutadores para proteger sus dispositivos de este ataque. En ese momento, querrá asegurar la demanda de transmisión de reverberación ICMP en los dispositivos de la organización. Además, para evitar que reaccionen a los paquetes ICMP de las direcciones de transmisión, otra alternativa es diseñar los marcos finales.

Ataque de lágrima

Los agresores utilizan esta estrategia para equilibrar campos en sucesivos paquetes de Protocolo de Internet haciendo que la fractura y la longitud se cubran entre sí en la parte atacada. Aunque se quedará corto, durante el ciclo, habrá un esfuerzo por parte del sistema atacado para reproducir paquetes. En ese punto, el marco colapsará a largo plazo debido al desorden. Es posible que deba bloquear los puertos 445 y 139 a medida que debilita SMBv2 para protegerse contra este ataque DoS en caso de que no tenga parches.

Ataque de inundación TCP SYN

Es durante un apretón de manos de instauración de una reunión de TCP cuando los asaltantes hacen un uso indebido del espacio de la cuna que utilizan este asalto. La pequeña línea de medida del marco objetivo se verá desbordada con demandas colectivas del dispositivo de los asaltantes. En todo caso, cuando el marco objetivo responde a esas solicitudes, no reacciona. Y teniendo en cuenta que pendiente de la reacción del dispositivo del agresor, el ciclo hará que se rompa el marco objetivo. Por último, cuando la línea de asociación se completa, hace que el marco quede inutilizable o se bloquee.

Para que pueda contrarrestar los ataques de inundación TCP SYN, aquí hay algunos elementos que se pueden evitar:

- En conexiones abiertas, reduzca el tiempo de espera y aumente el tamaño de la cola de conexión

- Para detener los paquetes SYN entrantes, coloque los servidores detrás de un firewall configurado

Capítulo 4

Tipos de malware

La programación indeseable que alguien introduce en su marco sin su consentimiento es el significado exacto de la programación perniciosa. Puede haber una conexión real de este producto con la proliferación y el código, lo que implica que, a través de Internet, puede reproducirse a sí mismo o introducir aplicaciones valiosas. Un par de tipos básicos de malware incluyen:

software espía

Utilizan software espía para recopilar las tendencias de lectura de los clientes, su PC y sus datos. Además, sin su conocimiento, el spyware rastrea todo lo que hace y un cliente distante obtiene esa información. Del mismo modo, el spyware puede introducir o descargar proyectos maliciosos de Internet. Cuando introduce otra aplicación gratuita, el spyware suele ser un programa diferente que se instala accidentalmente y su funcionamiento es muy similar al del adware.

publicidad

Las organizaciones utilizan adware, una aplicación de producto con fines de promoción. En el momento en que se ejecute cualquier programa, se realizará una presentación de las normas de publicidad. Mientras examina cualquier sitio, puede descargar adware en consecuencia a su PC. En la pantalla de tu PC, a través de una barra o un resorte, puedes verlo.

Secuestro de datos

Este tipo de malware toma medidas para borrar o distribuir la información de la víctima después de bloquearla, a menos que haya una cuota de pago por parte de la persona en cuestión. El malware más desarrollado utiliza la estrategia de chantaje criptoviral. Hacer esto codificará los documentos de la persona en cuestión y sin la clave de decodificación, hace que sea prácticamente difícil de recuperar. Suele ser muy difícil para una persona capacitada cambiar el bloqueo del sistema con el uso de algún ransomware de PC simple.

Cuentagotas

Para el establecimiento de infecciones en las PC, utilizan un programa llamado cuentagotas. La programación de filtrado de infecciones no puede distinguir un cuentagotas ya que no está influenciado por código maligno en algunos ejemplos. Además, para el programa de infección que habita en un sistema socavado, un cuentagotas puede interactuar con Internet y descargar actualizaciones.

gusanos

Los gusanos proliferan en PC y organizaciones como proyectos independientes y, dado que no tienen conexión con un archivo host, se diferencian de las infecciones.
Utilizan la conexión de correo electrónico para propagar gusanos y se activa cuando abre el programa. Además de realizar actividades nocivas, el gusano también puede enviar una copia de sí mismo a todos los contactos de la dirección de correo electrónico de una computadora contaminada. En ese momento, puede haber una oportunidad de renunciar a los ataques de la administración contra los centros de la organización cuando un gusano se propaga por la web y sobrecarga a los trabajadores de correo electrónico.

Bombas Lógicas

Se agrega a una aplicación una especie de programación vengativa, que es una bomba de razonamiento. Un evento en particular lo desencadena como una fecha y hora en particular o una condición coherente.

troyanos

Por lo general, los troyanos tienen una capacidad vengativa y están encubiertos en un programa útil. Dado que los troyanos no imitan, este importante atributo los aísla de las infecciones. Del mismo modo, los agresores pueden hacer un mal uso del acceso indirecto creado por un troyano para enviar ataques a un sistema. Por ejemplo, para que los programadores puedan realizar un ataque después de utilizarlo para conectarse, pueden programar un troyano para abrir un puerto de número alto.

Virus sigilosos

Para que las infecciones de secreto se cubran, asumen el control sobre los elementos de un marco. El informe del producto es el de no infectado ya que han socavado la ubicación del malware. Cambian la hora y la fecha del último ajuste del documento y disfrazan cualquier expansión en el tamaño de un registro contaminado.

Virus polimórficos

Cuando las infecciones difieren en los patrones de decodificación y encriptación, utilizan este ciclo para ocultarse. De esta manera, en un principio, decodificado por un programa de descifrado es un motor de cambio asociado y el codificado

infección. Una región de código será contaminada posteriormente por la infección codificada. En ese momento, habrá un avance de otra rutina de decodificación por parte del motor de cambio. Usando un cálculo relacionado con el nuevo estándar de decodificación, una copia de la infección y el motor de transformación serán luego codificados por la infección. El nuevo código luego tendrá una conexión del paquete de infección codificado y cambiará el motor. En consecuencia, la interacción sigue repitiendo lo mismo. Es muy precario distinguir tales infecciones. No obstante, debido a los pocos cambios en su código fuente, tienen un grado de entropía importante. Para una identificación rápida, puede utilizar Process Hacker.

Infecciones del sistema o del registro de arranque

Las placas duras darán un registro de un registro de arranque por la infección adjunta al arranque experto. Para que pueda propagarse a otras PC y placas, observará el área de arranque y cargará la infección en la memoria cuando inicie el sistema.

Infectores de archivos

Este tipo de infecciones se asocian con código ejecutable como registros .exe. A medida que se acumula el código, se introducirá la infección. Además, con la creación de un archivo de infección con un nombre similar, que es una extensión .exe, otra forma de virus de archivo se conectará con el archivo. Por lo tanto, el código de infección se ejecutará cuando se abra el documento.

Virus de macros

Las que quedan contaminadas por estas infecciones son aplicaciones como Excel o Microsoft Word. Las infecciones a gran escala se agregan a la agrupación de instancias de una aplicación. Antes de mover el control a la aplicación, la infección ejecuta instrucciones cuando se abre la aplicación. En el marco de la PC, habrá una replicación de la infección antes de que se una a otros códigos.

Capítulo 5

Cómo funciona el proceso de piratería

El derrame de datos del marco es la utilización esencial de la piratería en el pasado. Actualmente hay un significado tenue asociado con el truco en los nuevos años, la cortesía de algunos jugadores sinvergüenzas. Por otra parte, para que estén seguros de las deficiencias y cualidades de sus marcos, los programadores son utilizados por diferentes organizaciones para hacer esto. Obtienen una gran compensación a través de una confianza positiva que construyen, y conocen el punto en el que deben detenerse. En este sentido, de inmediato, ¿qué tal si hacemos un salto profundo en el arte de la piratería?

Fase de preparación

Aquí se necesita profundamente un lenguaje de programación. Aunque verá algunas reglas fundamentales, no debe limitarse a un idioma en particular. La resistencia es muy requerida en esta etapa ya que puede requerir cierta inversión para dominar el lenguaje de programación.

- Es obligatorio conocer la construcción informática de bajo nivel. Aunque hay algunos factores, su procesador ve solo este lenguaje. Además, cuando no sabe cómo reunirse, es posible que no sea concebible abusar de un programa.

- También deberá realizar secuencias de comandos de slam. El control de los marcos de Linux/Unix se completará fácilmente, incluida la realización de la mayor parte del trabajo para usted a través de la composición.
contenido.
- Dado que PHP es lo que utilizan la mayoría de las aplicaciones web, debe intentar aprender PHP y, en este campo, una decisión sensata para usted es Perl.

- También puede automatizar algunas tareas con lenguajes de secuencias de comandos de nivel increíble y significativo como Ruby y Python.
- Los dialectos que utilizaron en la construcción de Windows y Linux son C++ y C. en particular; instruye cómo funciona la memoria y reúne el lenguaje.

En ese punto, su objetivo debe estar en la imagen. Esta interacción se denomina identificación, que es la forma en que acumulará datos esenciales sobre su objetivo. Tendrás menos sobresaltos cuando te enteres de tu objetivo antes de tiempo.

Actualmente, el camino hacia la piratería puede comenzar. Para sus pedidos, ponga en uso un terminal *nix. Para clientes de Windows, un *nix ayudará a copiar a través de Cygwin. Nmap no necesita molestarse con Cygwin ya que se ejecuta en Windows y utiliza WinPCap. En cualquier caso, debido a la ausencia de archivos adjuntos en bruto, Nmap no funciona bien en los marcos de Windows.
Además, debido a su adaptabilidad, BSD y Linux deberían estar en su lista de contemplaciones. Además, hay algunas herramientas preintroducidas con algunas transmisiones de Linux. Por otra parte, en la Tienda Windows, puede encontrar un terminal * nix en Windows 10 Fall Creators Updates o posterior y, por cortesía del Subsistema Linux de Windows, Windows puede copiar la línea de orden de Linux.

Actualmente, el primer paso es obtener su marco. Para que usted se dé suficiente seguridad a sí mismo, necesita ver muy bien todos los procedimientos regulares. Necesitas la aprobación de tu objetivo para que asaltes cuando comiences con lo básico.
Puede hacer esto utilizando máquinas virtuales para configurar su centro de investigación, solicitar el consentimiento escrito de su objetivo o incluso atacar a su organización. Tropezará con dificultades si intenta atacar a una organización porque es ilícita, independientemente de su contenido.

El camino hacia la prueba de su objetivo es la siguiente etapa. ¿Puedes llegar al marco lejano? Si bien es lo que usan la mayoría de los sistemas operativos, la consecuencia de usar la utilidad ping para asegurarse de que su objetivo esté vivo puede no ser muy concreta. Los jefes nerviosos de los marcos pueden apagarlo sin mucho esfuerzo, ya que depende de la convención ICMP. En ese punto, debe caracterizar el sistema operativo. En el momento en que espera ejecutar una salida de puerto, intente Nmap o POF. Para que puedas hacer tu arreglo de actividad; ejecutar la salida de los puertos le revelará el tipo de interruptor o firewall que está utilizando su objetivo y verá los puertos que están abiertos en el sistema operativo y la máquina. En ese momento, puede utilizar el cambio -0 para iniciar la identificación del sistema operativo en Nmap.

En este punto, habría encontrado un puerto abierto o fuera del marco.
En la mayoría de las ocasiones, existe una garantía sólida para puertos específicos como HTTP

(80) y FTP (20).

- La prueba de un shell protegido, SSH, la administración que se ejecuta en el objetivo es un puerto 22 abierto, y esto puede ser un poder bestial de vez en cuando.
- Es concebible que su objetivo no haya podido recordar otros puertos UDP y TCP, incluidos algunos puertos UDP abiertos para juegos LAN y Telnet.

El siguiente ciclo es la verificación después de que lo más probable es que rompas la frase secreta. El poder animal es uno de los pocos métodos que puedes usar para descifrar una frase secreta. Puede probar cada palabra secreta potencial que contiene una referencia de palabra predefinida de la programación de poder animal.

- En la mayoría de los casos, encontrar su camino hacia un marco será, en general, mucho más fácil incluso sin descifrar la clave secreta. Para
- transferirlo al sitio protegido, puede ir a un establecimiento de prueba TCP o obtener una tableta establecida. En ese momento, hará que la palabra secreta aparezca en su intermediario cuando se abra la dirección IP. Puede que no sea una buena idea intentar iniciar sesión en una máquina remota
- utilizando todas las palabras secretas imaginables. Si bien puede requerir algo de inversión para terminar, podría ensuciar los registros del sistema y los sistemas de detección de interrupciones pueden identificarlo sin ningún problema. Debe comprender que solo si el hash de la palabra secreta está en su cuenta, la ruptura de la palabra secreta puede ser una estrategia decente.
- Como es muchas veces más rápido, otro procesador es el método más actualizado que utiliza el Tarjeta de diseños Puede obtener soporte de velocidad monstruosa cortando los cálculos MD5 y el mal uso de las deficiencias de la mayoría de los cálculos hash puede mejorar fundamentalmente la velocidad de
- ruptura ya que son en gran medida frágiles. El poder de la bestia puede tomar mucho tiempo ya que los clientes están utilizando contraseñas sólidas. . No
- obstante, las estrategias de tracción animal han mejorado

-

con algunas mejoras significativas

La ventaja de un súper cliente es lo que necesita obtener ahora. Si se trata de un marco de Windows que está intentando romper, necesitará ventajas de administrador, y si su objetivo es una máquina * nix, las ventajas raíz son todo lo que necesita.

- No podrá acceder a todos los aspectos más destacados de una asociación a la que tenga acceso. Sea como fuere, puede hacer todo si tiene la cuenta de raíz, director o supercliente. Pero se ha ajustado, la cuenta
- de administrador cae como algo normal para los conmutadores, y es el presidente que representa a Windows. Es posible que necesite un grado particular de verificación para que pueda obtener la mayor cantidad de datos
- ya que todos han sido garantizados. Necesitará ventajas de supercliente para ver todos los documentos en una PC. En los sistemas operativos BSD y Linux, los clientes raíz obtienen ventajas comparativas como cuenta de cliente

En la actualidad, es posible que deba participar en varias acrobacias. En la mayoría de las ocasiones, es posible que deba aumentar su nivel de aprobación haciendo un volcado de memoria para poder infundir código o ejecutar una tarea a un nivel más elevado haciendo una inundación de cuna para adquirir el estado de supercliente.

- Puede hacer esto encontrando o componiendo un programa incierto que pueda ejecutar en su máquina
- Si la programación desordenada tiene establecido el bit setuid, esto ocurrirá en marcos similares a Unix y, por lo tanto, es como un supercliente que se ejecutará el programa.

Es posible que necesite tener acceso indirecto creado en esta etapa. En general, será ideal que pueda regresar cuando haya adquirido la admisión total a un marco. Puede pasar de forma secundaria a ciertas administraciones de marco fundamentales como el trabajador SSH. Sin embargo, durante la siguiente revisión del marco, es posible que se elimine su pasaje secundario. En ese momento, la disposición es acceder indirectamente al compilador real, por lo que tiene una forma potencial de regresar a través de cada programación agregada. También,

sus huellas deben ser cubiertas. El supervisor del marco no debe pensar en la compensación del marco. Nunca haga más registros de los necesarios ni implemente una mejora en el sitio. Del mismo modo, no tienes que hacer más clientes. Haz actividades rápidas. Asegúrese de que su misteriosa palabra secreta esté codificada cada vez que repare un trabajador como SSHD. Aunque sin contener datos significativos, el trabajador debe darles acceso si alguien intenta iniciar sesión con esta clave secreta.

Capítulo 6

Por qué los piratas informáticos usan Linux

Hay algunos aspectos destacados excepcionales en el marco de trabajo de Linux que lo hacen más abrumador que otros sistemas operativos. Con Unix como su forma anterior, el arreglo de trabajo de Linux es de código abierto. Paso a paso, hay una rápida mejora en la utilización de Linux. Además, a diferencia de usar otros sistemas operativos como Mac o Windows, a los programadores les gusta usar Linux debido a las ventajas adicionales que el sistema operativo Linux tiene sobre otros. El sistema operativo de Linux tiene características sorprendentes y extraordinarias que lo hacen más dominante que otros marcos, aunque sus sistemas operativos son más fáciles de entender.

Por qué los hackers prefieren el sistema operativo Linux

Para su prueba, y porque necesitan sacar dinero de sus límites comunes de piratería, los programadores ingresan a las organizaciones de PC o marcos de PC independientes. Además, para probar sus habilidades, los programadores requerirán el marco de trabajo, que ofrece la seguridad más extrema.
Por lo tanto, Linux parece, a todas luces, ser la opción más ideal para los programadores, ya que les hace más seguro en la totalidad de sus ejercicios.
Para bibliotecas y aplicaciones de Linux, hoy en día han compuesto una gran cantidad de líneas de código. Esta interacción ha permitido que se incorpore a emprendimientos muy diferentes ya que se hace de una manera asombrosamente mesurada. Por ejemplo, puede utilizar una parte de una biblioteca como un código de control de la organización, incluso si le permite rastrear la organización para verificar la ejecución proactiva. Además, la seguridad de la red se puede piratear sin esfuerzo.

Como es adaptable, los programadores tienen la oportunidad de jugar todos sus ejercicios elegantes utilizando el gimnasio de la jungla de Linux. Del mismo modo, es muy sencillo para los programadores comprender, aprender y usar Linux, ya que pueden utilizar sus estrategias de prueba iniciales para saber si hay incertidumbre. Linux es muy seguro porque cuando surgen problemas, los programadores pueden solucionarlos, ya que pueden echar un vistazo a cada línea del código de Linux. También puede ser utilizado en cualquier momento por cualquier cliente que lo maneje y no solo por unos pocos desarrolladores que trabajan en algunas asociaciones corporativas. Aquí hay una parte de las ventajas de Linux sobre otros:

Fácil de usar

La convicción general es que Linux es solo para programadores y desarrolladores y, en general, esa será la fantasía general. No obstante, este sencillo está lejos de ser una realidad. Fácilmente tendrá una comprensión básica de Linux si lo ha estado utilizando durante bastante tiempo. No es equivalente a la disposición de trabajo de Windows. A fin de cuentas, puede ser muy precario cuando hacemos el cambio a un sistema operativo alternativo. Descubrirá que Linux es fácil de entender y más útil que Windows.

Menos consumo de RAM

Linux quema menos utilidad de manejo y RAM al igual que requiere menos

espacio para círculo ya que es muy ligero. En consecuencia, puede tener otros marcos de trabajo, por ejemplo, Windows y OS X introducidos con él.

Linux es el futuro

Para empezar, Android depende de Linux, y la decisión de los trabajadores web es el sistema operativo Linux por su calidez, adaptabilidad y solidez.

Sin requisitos para los conductores

No necesita preocuparse por los controladores discretos antes de poder utilizar Linux. Dentro de la pieza de Linux, rastreará cada uno de los controladores importantes que necesitará cuando introduzca Linux. Posteriormente, para introducir drivers para equipos, ya no necesitarás CDs.

Tomar en serio la privacidad

Por todas partes en Internet, numerosas personas están discutiendo sobre Windows 10 y el tema de la seguridad. Por lo general, su información es recopilada por Windows 10. Sin embargo, no hay ningún caso en que alguien recopile datos e información sobre usted para fines financieros cuando utiliza el sistema operativo Linux.

Las herramientas de piratería a menudo se escriben para Linux

Nmap y Metasploit, una parte de los dispositivos de piratería más conocidos, están adaptados para Windows. No obstante, Linux tiene mejores herramientas y, de una manera mucho mejor, supervisa la memoria y no todas las funciones se transfieren de Linux.

Varios lenguajes de programación cuentan con el soporte de Linux

La mayoría de los dialectos de programación tienen abundante ayuda de Linux. En Linux, funcionan perfectamente Perl, Python, Ruby, PHP, Java y C++/C. Es poderoso y básico cuando necesita utilizar Linux para cualquiera de los dialectos de secuencias de comandos.

Menos vulnerable

Hay tanta debilidad en básicamente todos los marcos de trabajo disponibles excepto Linux. Linux tiene menos debilidades y se enorgullece de ser el marco de trabajo más seguro.

Bajo costo

En general, se sabe que Linux es un marco de trabajo de código abierto, por lo tanto, puede obtenerlo en línea de forma gratuita al igual que instalar y usar la aplicación sin reservas.

Flexibilidad

Puede utilizar Linux para áreas de trabajo de élite y aplicaciones de trabajo, al igual que los marcos implantados.

Mantenimiento

Es muy simple mantener el arreglo de trabajo de Linux. Puede introducir todos los productos sin esfuerzo. Es mucho más fácil buscar su producto ya que cada versión de Linux tiene su almacén de programación central.

Portátil y ligero

Desde casi cualquier dispersión de Linux que necesiten, las unidades y placas de arranque en vivo modificadas están ahí para que los programadores las creen. Dado que los activos que quema son muy inferiores, se apresura a introducirlos. La forma en que consume menos activos hace que Linux sea liviano.

Interfaz de línea de comandos

Windows y Mac no tienen la interfaz de línea de orden sólida, profundamente integrada y diseñada de manera única que Linux se jacta de tener. Otros clientes y programadores de Linux tendrán control sobre su marco con un acceso más notable.

multitarea

Todo simultáneamente, puede utilizar Linux, ya que así es como está planeado. Por ejemplo, sus diferentes trabajos no encontrarán ningún tipo de interrupción con una gran posición de impresión detrás de escena. Además, sus ciclos esenciales no se alterarán incluso con algunos trabajos realizados simultáneamente.

Amigable con la Red

Linux tiene éxito en la supervisión de la red, ya que ofrece algunas órdenes y bibliotecas que los programadores usan para probar las infiltraciones de la red.
Posteriormente, como marco de trabajo de código abierto, el grupo que se suma a él lo hace como una organización tan absurda. Además, más que otros marcos de trabajo, Linux hace que el refuerzo de la red sea más rápido como un marco de trabajo confiable.

Estabilidad

En el momento en que necesita mantener los niveles de ejecución, el único sistema operativo que no necesita reiniciarse ocasionalmente es Linux. Del mismo modo, la razón de los derrames de memoria no puede retroceder ni hacer que se congele también. Durante mucho tiempo, puede seguir utilizando este marco de trabajo.

Dado que los programadores pueden desarrollar sus capacidades de piratería y probar sus habilidades en este marco de trabajo, se decide por Linux como su decisión más ideal. Los proyectos de arreglo y la instalación son fáciles de usar, y algunas dispersiones de Linux tienen dispositivos que hacen que la instalación de más programación sea muy fácil de entender.

Capítulo 7

Instalación y actualizaciones de Kali Linux

Un marco de trabajo centrado en la seguridad es quizás lo más fundamental que debe tener cuando busca una profesión en seguridad de datos. Puede realizar eficazmente tareas prolongadas y tediosas con la ayuda de un marco de trabajo razonable. A partir de ahora, los marcos de trabajo de Linux son en realidad innumerables. No obstante, quizás la opción más ideal sea Kali Linux. los expertos en protección en línea lo utilizan para evaluar la seguridad de la red, la piratería moral y las pruebas de infiltración.

Kali Linux será uno de los nombres principales a los que se hará referencia con respecto a las apropiaciones hostiles de Linux, la piratería y las pruebas de infiltración. Hay algunas tareas de seguridad de datos como otras herramientas de piratería de línea de pedido que Linux viene preempaquetado, como seguridad de aplicaciones, criminología informática, seguridad de red y pruebas de acceso. En un nivel muy básico, cuando te esfuerzas por participar en la piratería moral, el arreglo de trabajo de Linux es un arreglo extremo.

Instalación de KaliLinux

El camino hacia la introducción de Kali Linux puede ser muy básico, y las opciones de instalación son varias. Los métodos por los que se inclina la gran mayoría son:

1. Usar el marco de trabajo para el arranque doble de Kali Linux 2. Con programas de virtualización como VirtualBox o VMware 3. Instalación de la placa dura para Kali Linux 4. Hacer una unidad USB de arranque de Kali Linux mientras se presenta Kali linux

El énfasis estará en utilizar la programación de virtualización para introducir Kali Linux incluso cuando hay algunas opciones disponibles. Para que pueda realizar una prueba de acceso completa utilizando todas las herramientas que necesita, puede configurar su máquina siguiendo estos pasos.

Requisitos para la instalación

- Soporte USB / unidad de DVD-CD
- Mientras se trabaja con VirtualBox o VMware, la recomendación es de alrededor de 4 GB

- La recomendación para su disco duro es un espacio libre mínimo de 20 GB

El proceso de instalación

Paso 1: instalación de VMware:

Inicialmente, una especie de programación de virtualización es fundamental para ejecutar Kali Linux. Para algunas personas, existe una inclinación por VMware de todos modos, cuando pueden utilizar VirtualBox de Oracle como una característica de algunas alternativas que pueden revisar. Desde su organizador de aplicaciones, envíe VMware cuando haya terminado con la instalación.

Paso 2: descarga de Kali Linux y verificación de integridad de la imagen:

Puede elegir el que mejor se adapte a sus necesidades cuando vaya a la página de descarga de la autoridad para descargar Kali Linux. Además, hay algunos números hexadecimales en la página de descarga. No hay nada tan significativo en ellos. Además, para las tareas que se identifican con seguridad es el objetivo de Kali Linux. En esa capacidad, se requiere excepcionalmente la verificación de la honestidad de la imagen descargada. Se debe verificar la marca única SHA 256 del documento y hacer un examen con el que ve en el sitio web donde realiza la descarga.

Paso 3: lanzamiento de una nueva máquina virtual:

Presionará el botón 'crear otra máquina virtual' cuando llegue a la página de inicio de VMware Workstation Pro. Antes de configurar los detalles de la máquina virtual, probablemente eligió el marco de trabajo del visitante después de elegir el archivo iso de Kali Linux. Elija la máquina virtual Kali Linux para iniciar la máquina virtual, y tocará el botón verde con el grabado 'encendido'. ¡Verás cómo se enciende la máquina!

El proceso de instalación

En el menú de GRUB, recibirá instrucciones para elegir su sistema favorito de la instalación cuando la máquina esté llena de combustible. Antes de continuar, elija el establecimiento gráfico. Será llevado a otra página donde se le pedirá que elija su formato para la consola, el área de su país y el idioma que desee. En ese momento, el cargador tendrá la configuración relacionada de su organización diseñada después de la introducción de segmentos adicionales cuando haya terminado con los datos locales. En ese momento, para esta instalación, el instalador generará una ubicación y un nombre de host. Antes de proceder con el establecimiento, debe proporcionar datos adecuados sobre el clima. Tendrá que continuar cuando haya establecido una palabra secreta para la máquina Kali Linux. Una nota importante aquí: ¡asegúrese de mantener su clave secreta con cuidado! En ese momento, el instalador activará la configuración de su región de tiempo después de que probablemente configure su palabra secreta. En la parcelación de la placa, se detendrá. Desde el segmento circular, el instalador le dará cuatro decisiones. La opción 'guiada - utilizar todo el círculo' es la más simple de todas. Para opciones de configuración más granulares, los clientes experimentados deben utilizar la estrategia de distribución 'manual'. Si eres otro cliente, la propuesta es recoger todos los documentos cuando estés recogiendo la placa divisoria y puedes tocar 'continuar'. Luego, en la máquina host, todos los cambios que necesita hacer podrían afirmarse. Debe tener cuidado aquí, ya que puede eliminar los datos del círculo si continúa.

De esta forma, la interacción de establecimiento de registro se realizará por parte del instalador cuando confirme las progresiones en la parcela. Como este ciclo puede requerir algunos minutos, el establecimiento se realizará de forma natural. Si desea adquirir futuras actualizaciones y programación, el sistema le solicitará la configuración de un espejo de la organización cuando se publiquen los registros básicos. Si desea utilizar los almacenes de Kali, asegúrese de tener esta función habilitada.
En ese momento, se organizarán los documentos conectados del administrador del paquete. Luego, el cargador de arranque de GRUB es lo siguiente que se le pedirá que presente. Elija 'sí' y, dado que será necesario para iniciar Kali, elegirá el dispositivo para escribir los datos importantes para el cargador de inicio en el disco duro. Para completar el establecimiento, presione el botón 'continuar' cuando haya finalizado el establecimiento de GRUB en la placa. En ese punto, se introducirán documentos explícitos para la última etapa. En este punto, apóyate porque tu excursión de investigar Kali Linux ha terminado recientemente.

comenzó desde que introdujo efectivamente a Kali.

Actualizando Kali Linux

La lista de registros del paquete es el paso inicial de una actualización para su marco Kali Linux. Ingresará el pedido adjunto cuando abra la terminal; $ sudo able update Como alternativa, para todos los paquetes planificados para la actualización, puede mostrarlos.

Tiene la oportunidad de revisar todos los paquetes sin demora con el uso de poder introducir PACKAGE-NAME solo como una actualización de paquete individual en esta etapa. Actualmente, ha revisado por completo su Kali Linux.

Capítulo 8

Instalación de Kali Linux en una máquina virtual

Con el equipo incomparable que tiene actualmente, puede ejecutar marcos de trabajo únicos de varias maneras. Además, algunas de las alternativas disponibles para usted son discos duros, USB y DVD. En esta parte, la suposición será que para que pueda ejecutar su Kali Linux, no tiene una PC dedicada y, después de todo, usaremos una PC virtual o un clima virtualizado para ejecutarlo. Lo más probable es que haya introducido una caja virtual en su PC para que comencemos la interacción. Además, en caso de que no lo tenga en su sistema, puede descargarlo cuando visita el sitio oficial de VirtualBox. Para el equipo que usaremos para presentar Kali Linux, este producto copiará este equipo.

En general, se da cuenta de que, excepto si se acerca a la programación, tiende a ser muy precario descargar dicha programación. De esta forma, descargará la imagen ISO de Kali Linux desde su página de autoridad. Además, en caso de que necesite realizar un seguimiento mientras refleja eso, el tipo de

el Kali Linux KDE de 64 bits es lo que usaremos. El tamaño de su descarga es de alrededor de 3,2 GB, y la descarga puede llevar algún tiempo.
En ese momento tendrá el. Imagen ISO montada en la máquina virtual cuando la haya administrado. Si tiene el objetivo de utilizarlo en otra máquina, puede copiarlo en un USB o DVD de arranque. Sea como fuere, es posible que tengas que considerar ciertas contemplaciones. En ese momento, puede abrir VirtualBox cuando se descarga la imagen.

Ahora, presionará el botón 'nuevo' para crear otra máquina virtual, que es lo principal que hará. En ese momento, en el marco operativo normal, debe indicar la presencia de los documentos de los registros de ayuda de esta máquina actual. Puede elegir Linux para el tipo, ya que Kali está construido sobre Linux. Además, para el formulario, Ubuntu de 64 dígitos será su decisión. Aunque para preparar a Kali para la acción en VirtualBox, es una configuración predeterminada ideal para nosotros. No hay garantía de que funcionará impecablemente al indicar la variante y el tipo. En ese punto, el resumen de la medida de memoria que necesitamos será el siguiente. Puede optar por 2 GB, ya que incluso 1 GB lo hará en cualquier caso. Por otra parte, puede sentirse libre de darle todo lo que necesite si tiene suficiente memoria.

La disposición del disco duro es el siguiente paso aquí, que VirtualBox le preguntará. Puede decidir utilizar uno actual o hacer uno. Para no ir de un lado a otro entre varios emuladores, puedes elegir Imagen de disco de VirtualBox después de elegir el tipo de documento del disco duro. Si está utilizando VMware, por ejemplo, una alternativa más apropiada será VHD.
A partir de ese momento, su designación de capacidad en el disco duro real es la siguiente alternativa para elegir. En ese momento, puede elegir una asignación dinámica. Entonces, la medida de asignación para esta máquina es lo que elegirá actualmente. Debería considerar verificar cuánta memoria tiene accesible antes de continuar con esta actividad. El lugar que necesita para guardar sus placas virtuales se puede determinar dentro de VirtualBox.
Luego puede aprobar y presionar el botón 'hacer'. Sin embargo, ese no es el final del ciclo. Para que estemos seguros de que podemos obtenerlos, es posible que debamos jugar con la configuración básica. Para futuras referencias, tendrá la oportunidad de manejar el clima virtual y esto es muy fundamental. Es posible que deba leer más sobre el tema de la configuración de la máquina virtual, ya que es un punto amplio.

También puede continuar con la configuración del marco ya que, durante el

ciclo de creación, has cubierto algunas cosas. Si no tiene una unidad de disquete, puede eliminar el disquete en el marco.
Puede incitar a VirtualBox a buscar cualquier medio en el reproductor de DVD primero en la solicitud de arranque. Es valioso darse cuenta de que en la introducción subyacente, esa es la base de nuestra imagen de Kali. Si es importante, es posible que también deba verlo más tarde, pero puede tener 2 MB para la memoria base.
De acuerdo con la imagen de arriba, asegúrese de reflejar los aspectos más destacados de todo incluido. En ese punto, puede ayudar a la memoria de la imagen hasta alrededor de 128 MB cuando continúa con 'Mostrar'. Además, si quieres volverte loco con gráficos explícitos, puedes habilitar el aumento de velocidad 3D. Puede correr el riesgo de consumir algo de hardware y no le dé una memoria de video irrazonable si está ejecutando un equipo antiguo. A partir de ese momento, puede hacer quizás la configuración más esencial, que es verificar la capacidad. Asegúrese de que el archivo de imagen que ha descargado de la página de autoridad de Kali Linux esté destacando la unidad de CD-ROM vacía. Además, para que usted tenga la opción de elegirlo. documento ISO, puede lograrlo tocando el símbolo del círculo debajo de ascribes.

Actualmente, se acepta que ha montado la imagen del CD-ROM ya que la unidad se dirige a la. imagen ISO. Puede dejar la casilla de verificación DVD/CD en vivo como predeterminada y no marcarla. Debe centrarse en la disposición principal comprobando la configuración de la organización. Algunos de ellos son:

- Redes genéricas
- Redes solo de host
- Redes internas
- Redes en puente
- redes NAT
- Traducción de direcciones de red, NAT
- no adjunto

Puede ir a la página de autoridad de VirtualBox para conocer todos los modos. Además, dado que su conexión web está conectada, este modo predeterminado podría ser suficiente si todo lo que necesita hacer es ver el correo electrónico dentro del visitante, descargar registros y navegar por la web. Por lo que vale para los novatos, puede, por el momento, usar NAT. En el momento en que envía la máquina, todo debería funcionar de maravilla si está conectado a través de un enlace Ethernet. Sin una tarjeta de interfaz, es posible que no funcione para usted

llega a la web si no tienes una asociación cableada. En ese momento, solo necesita presionar el botón 'comenzar' para ejecutar el sistema operativo si se refiere a ejecutar Kali en un clima virtual.

Capítulo 9

Cómo organizar Kali Linux

Kali 2.0 fue lanzado por Offensive Security luego de diez años de desarrollo. Es más, de todas las descargas de Kali/Backtrack, la más sencilla de usar con diferencia es Kali 2.0. Hay algunos aspectos destacados nuevos con el nuevo Kali si está acostumbrado al primer Kali. Sin embargo, ¡no hay nada mejor que esto! Han suavizado y rediseñado totalmente los menús con un símbolo de apoyo que aborda gran parte de los aparatos.

Aquí hay algunas cosas nuevas sobre Kali 2.0:

- Screencasting incorporado
- Notificaciones de escritorio
- Para una carga más rápida de Metasploit, hay un Ruby 2.0 nativo
- Nuevas categorías y menús

- Nueva interfaz de usuario

Han suavizado muy bien el Kali 2.0 y lo han contrastado con anteriores adaptaciones de Backtrack/Kali; el diseño fluye muy bien. como se esparce sucinta y claramente, la vibra es la de tener todo fácilmente disponible. Para armar tu Kali, puedes seguir los caminos que lo acompañan mientras inspeccionamos una porción de sus partes.

Descripción general del escritorio

Una vez más, todo lo que necesita está disponible en el área de trabajo, que se siente y se ve muy bien.

Servidor web Apache

A partir de ahora, parece que han eliminado el trabajador web de Apache para reinicie, inicie y evite los símbolos de administración de Kali 2.0. De hecho, usted Es posible que deba utilizar el pedido a continuación en caso de que necesite Comience desde un breve terminal:

- Para reiniciar, puede usar apache2 restart o "servicio apache2 restart"
- Para detener, puede usar " /etc/init.d/apache2 stop" o "servicio apache2 stop"
- Para empezar – puede usar "/etc/init.d/apache2 start" o "servicio apache2 start"

Verá el cambio de Kali 1 con respecto a la página web predeterminada como ahora podrá utilizar el servidor web de Kali. Actualmente, situado en un sobre llamado HTTP, también hay un nivel más para el sitio raíz. En eso capacidad, en lugar del antiguo registro "/var/www/", ahora podrá suelte los sobres o páginas de su sitio en el catálogo "/var/www/HTML/" cuando utiliza el trabajador de Apache.

Proyección de pantalla

Ahora podrá utilizar screencasting porque hay un resaltado de screencasting implícito en Kali 2.o. Puede registrar continuamente las actividades de sus pruebas de seguridad.

Menú de lugares

Dentro de su Kali, tiene conexiones a diferentes áreas contenidas en el menú Lugares.

espacios de trabajo

También hay espacios de trabajo en las versiones anteriores de Backtrack/Linux.
Workspace son las pantallas de área de trabajo adicionales que puede usar si no tiene la menor idea sobre el área de trabajo. Para cada una de las ventanas que ha abierto, puede obtener un esquema de ellas utilizando la 'clave misma'. Además, puede abrir el menú del espacio de trabajo si tiene una pantalla táctil. Entre los espacios de trabajo, tendrá la capacidad de reubicar proyectos en ejecución explícitos.

Minimización automática de ventanas

De vez en cuando, algunas ventanas desaparecen o se limitan automáticamente, que es otra cosa en el nuevo Kali 2.0. En la barra de favoritos, a un lado del símbolo relacionado, verá un círculo blanco cuando una ventana está limitada. La ventana principal de la terminal aparecerá si hace clic una vez en el símbolo de la terminal, y ambas ventanas limitadas de la terminal volverán cuando haga clic dos veces.
Del mismo modo, para ver ventanas limitadas, puede presionar "Alt-tab". Luego, para ver ventanas adicionales, puede salir corriendo cuando tenga presionada la "pestaña alternativa".

Herramientas de línea de comandos

Es en el índice "/usr/share que tienen la mayoría de los dispositivos introducidos. En el momento en que escribes los nombres de estos dispositivos en una terminal, puedes ejecutar estos dispositivos y otros dispositivos en el menú. Para que te acostumbres usted mismo con el catálogo de ofertas y el marco del menú, es posible que necesite

para tomar un par de segundos en eso.

Menú de aplicaciones

En el menú Aplicación, verá el área de un resumen de las mejores opciones básicas del programa. También, por tipo, hay un diseño inteligente de los instrumentos. Por ejemplo, si desea ver las herramientas de prueba de aplicaciones web más reconocidas, simplemente debe tocar el elemento del menú Análisis de aplicaciones web. Verá un resumen de la totalidad de los dispositivos para una clasificación particular. Es por el hecho de que las mejores herramientas aparecen en el marco del menú, y en Kali, no todas las herramientas están disponibles. Básicamente, accesible en la disposición del menú de Kali es solo una parte insignificante de los dispositivos introducidos y es solo desde la línea de pedido que la mayor parte de los dispositivos están accesibles.

Barra de favoritos

En el lado izquierdo del área de trabajo, verá una "barra más querida" ajustable en el nuevo Kali. Con esto, puede ingresar rápidamente a la actividad, ya que puede obtener las aplicaciones que utiliza con mayor frecuencia con esta lista de menú. A través de las condiciones necesarias, puede iniciar el dispositivo direccionado en consecuencia con solo un tic. Por ejemplo, antes de enviar Metasploit, si quiere asegurarse de haber creado la base de datos predeterminada, puede reiniciar la programación del conjunto de datos tocando el botón de Metasploit. En ese momento, puede ver diferentes aplicaciones en la parte inferior de la barra de selección superior tocando "mostrar aplicaciones". En sobres, puede orquestar los proyectos por tipo. También puede usar la barra de seguimiento escribiendo lo que necesita si no ve la aplicación que está buscando.

Capítulo 10

Escaneado (nmap, massscan, hping3) y Gestión Redes (Wireshark)

En el transcurso de las pruebas de acceso, Nmap es un identificador de host fundamental y un instrumento de verificación de la organización planificado en la red. En su mayoría, usan Nmap como un escáner de seguridad y un localizador de debilidades, lo que lo convierte en una utilidad increíble al igual que su uso para identificar y acumular datos. Dado que puede ejecutarse en algunos marcos de trabajo distintivos como Mac, BSD, Linux y Windows, esto convierte a Nmap en un dispositivo multipropósito. Usan Nmap para algunos propósitos sorprendentes que incluyen:

- Asegurando agujeros y detectando la vulnerabilidad, como scripts nmap
- Detección del sistema operativo, versión de software y dirección de hardware
- Funciona para el descubrimiento de servicios, es decir, detectar la versión y el software en el puerto respectivo
- enumeración y descubrimiento de puertos; detectar puertos que están abiertos en el host
- Descubrimiento de host; detectar el host en vivo en la red

Como un dispositivo típico, se puede acceder a Nmap tanto para la interfaz de usuario gráfica como para la interfaz de línea de pedido. Además, para realizar el examen, Nmap utiliza algunas estrategias, algunas de las cuales son el filtrado de bob de FTP, la verificación de identidad de cambio de TCP, la verificación de asociado de TCP (), y algunas más.

Uso efectivo de nmap

Dado que tenemos una distinción entre un filtrado de desarrollo y un análisis básico y sencillo, el sistema objetivo tiene una gran dependencia en el uso de Nmap. Para que podamos obtener el resultado correcto al pasar por alto la programación preventiva/de detección de interrupciones y el firewall, es necesario utilizar estrategias avanzadas. Verá algunos modelos debajo de algunas órdenes fundamentales de su uso:

En el marco objetivo, si planea examinar un puerto en particular, por ejemplo, filtrando solo en la PC objetivo Telnet, FTP y HTTP, entonces necesitará un límite pertinente para utilizar el orden del mapa. Del mismo modo, debe llamar al documento en el límite de la barra si los acuerdos de propiedad intelectual que desea bloquear están contenidos en un registro que tiene. Otra situación es que, dado que en general será peligroso para usted, es posible que deba prohibir las entregas de IP explícitas si necesita filtrar toda la subred. En consecuencia, utilice el límite de restricción cuando utilice el orden del mapa. Debe agregar un límite de SL a la orden si desea ver el resumen completo de los hosts que está verificando.

Enumeración de una gran cantidad de hosts con Massscan

Desde hace algún tiempo, el escaneo masivo ha estado cerca, y de un lado al otro del planeta, los pentesters lo están utilizando. En un segundo, Masscan puede comunicar hasta 10 millones de paquetes como aparato de vigilancia. Massscan utiliza una pila de IP/TCP personalizada y transmisión no simultánea con varias reuniones y transmisión de paquetes que utilizan varias cadenas.

Puede identificar rápidamente una gran cantidad de hosts utilizando el escaneo masivo. Básicamente, el escaneo masivo puede verificar toda la web en tan solo 6 minutos, según el creador de la herramienta. Además, debido al alto ritmo de su transmisión, también utilizan el escaneo masivo para las pruebas de estrés. Para que cualquiera logre esas altas tasas, requerirá controladores únicos como NIC y PF_RING. Dado que colabora con el uso de un estilo similar de Nmap, esta parte lo convierte en un dispositivo ventajoso.

Funciones de escaneo masivo

- Pila de IP/TCP personalizada
- Escaneo básico de vulnerabilidades, como el acaparamiento de banners de heartbleed
- Opción de destino de estilo Nmap y especificación Salida de estilo Nmap
- Escaneo ultrarrápido de puertos: hasta 10 millones de paquetes por segundo en transmisión (requiere controladores PF_RING y NIC compatible)

Usos de Masscan

- Escaneo aleatorio de conocimiento o enumeración divertida de Internet
- Enumeración de varias subredes dentro de una organización
  Enumeración de un gran número de hosts
- Para el mapeo de la red, se puede usar massscan como la primera herramienta de reconocimiento

Hping3 como generador de paquetes y herramienta de escaneo de red

Como analizador gratuito y generador de paquetes para la convención IP/TCP para la difusión de Antirez, la esperanza es un instrumento de filtrado de organizaciones. Para la seguridad de la red, hping3 es un tipo de analizador, y para las pruebas de seguridad y la inspección de organizaciones y firewalls, es uno de los verdaderos instrumentos.
También lo usan para el abuso de la estrategia de filtrado de barrido inactivo, que actualmente tiene su ejecución en el escáner de seguridad Nmap. Como agente de análisis/construcción de paquetes IP/TCP, se organiza una línea de pedido en el aparato de control de la organización esperando. En cualquier caso, cuando la esperanza puede lograr más que enviar demandas de reverberación ICMP, el ping(8)

El orden de Unix impulsó la interfaz. Sus aspectos destacados incluyen la capacidad de enviar registros entre un canal cubierto, la propiedad de un modo de ruta de seguimiento y el respaldo para las convenciones RAW-IP, ICMP, UDP y TCP. En el pasado, solo usaban la esperanza como un aparato de verificación de la organización. De todos modos, unos grupos lo utilizan en unos hábitos para probar cuentas y redes.

Algunos de los usos de la herramienta de escaneo de red hping

- Herramienta de escaneo de red
- Usando la interfaz Tk, es fácil usar las utilidades de red
  Prototipos de sistemas IDS
- Investigación de seguridad y redes en caso de emular comportamiento complicado
- de IP/TCP
- El concepto explota la prueba
- Pruebas de cortafuegos automatizadas
- Escriba aplicaciones reales relacionadas con la seguridad y las pruebas de IP/TCP
- Aprender IP/TCP

- Investigación de redes
- Explotación de vulnerabilidades identificadas de pilas IP/TCP Test IDSes
- Probar las reglas de cortafuegos
- Realice el escaneo inactivo (con una interfaz de usuario fácil de implementar en nmap)
- Uso de la herramienta de escaneo de red de utilidades estándar para sondear/ hacer ping/rastrear hosts detrás de un firewall que bloquea los intentos
- Los estudiantes que aprenden IP/TCP también pueden obtener conocimientos adecuados a través de hping
- Auditoría de pilas de IP/TCP
- Adivinanzas remotas de tiempo de actividad
- Toma de huellas dactilares remotas del sistema operativo
- Traceroute avanzado, bajo todos los protocolos soportados Ruta manual MTU descubrimiento
- Uso de fragmentación, TOS y diferentes protocolos para pruebas de red
- Escaneo avanzado de puertos
- Pruebas de cortafuegos

Asegurar y monitorear su red con Wireshark

El alijo de herramientas para un experto en seguridad empresarial es posiblemente el activo más increíble conocido como Wireshark al que la gente también se refirió antes como Ethereal. A través de una variedad de niveles, desde bits que incluyen un solo paquete hasta datos sobre la asociación, Wireshark puede inspeccionar los detalles del tráfico mientras mira dentro de la organización como un analizador de paquetes de la organización. Wireshark puede investigar problemas de seguridad en la organización de un dispositivo y diseccionar eventos de seguridad a través de su revisión de profundidad y adaptabilidad. Como es gratis, ¡el costo de Wireshark también es increíble!

Instalación de Wireshark

Es casi tan básico como ABC presentar Wireshark. Para Mac OS X o Windows, puede descargar los formularios dobles. Del mismo modo, para la mayoría de los tipos de Unix/Linux, existe la accesibilidad de Wireshark a través del estándar

programación de marcos de circulación. Además, en otros marcos de trabajo, el código fuente es accesible para su establecimiento. Para el formulario de Windows, el grupo que creó Wireshark lo construyó sobre la biblioteca de captura de paquetes de WinPcap. Además, si no dispone de WinPcap correctamente en su establecimiento y está utilizando Windows, es posible que lo tenga instalado para ejecutarlo. Aquí hay una advertencia: antes de ejecutar el instalador de Wireshark, puede utilizar la interacción manual para eliminar una forma obsoleta de WinPcap a través de "Agregar o quitar programas" en el tablero de control. El ciclo de establecimiento es algo muy similar a la agrupación basada en asistente que utiliza dos indicaciones principales: al inicio, le preguntará si espera iniciar el filtro de paquetes de WinPcap Netgroup, la administración de NPF y si necesita instalar WinPcap. . Para que pueda atrapar paquetes, puede elegir la opción anterior que le permitirá incluso si no tiene ventajas de cabeza. Son solo los presidentes los que realmente querrán ejecutar Wireshift que tengan esta asistencia habilitada.

Capítulo 11

cortafuegos

A la luz de un montón de reglas de seguridad, cuando espera obstaculizar o permitir paquetes de datos mientras se activa la pantalla y se acerca el tráfico de la empresa, un dispositivo de seguridad de la empresa que puede utilizar es un firewall. Para que un firewall obstruya el tráfico pernicioso como los programadores y las infecciones, debe establecer un límite entre el tráfico que se aproxima y la organización interna de fuentes externas. Puede mejorar la asociación de la seguridad de la PC como Internet o LAN cuando utiliza dispositivos como firewalls. Una pieza vital de la estructura de seguridad de largo alcance de su organización es el firewall.
Con el uso de un separador de código que revisa cada paquete de información individual a medida que aparece, el firewall está a ambos lados, tanto de entrada como de salida del sistema, para decidir si puede permitir que se bloquee o pase, un firewall desconecta por completo su PC desde Internet.

En el momento en que otorga poder granular sobre los tipos de ciclos de marco y capacidades que se acercan a los activos de administración de sistemas, también puede actualizar la seguridad a través de la capacidad de los firewalls. Para que deniegue o permita el tráfico, existen algunas condiciones de host y marcas que utilizan estos cortafuegos. Puede trabajar, organizar e instalar cortafuegos de forma moderadamente eficaz en cualquier caso, cuando suenen complejos. La convicción de ciertos individuos es que cuando tienen instalado un firewall, el tráfico que pasa por la sección de organización estará controlado. No obstante, un cortafuegos basado en hardware puede ser adecuado para usted. En su PC, puede ejecutarlos, incorporando su uso con Internet Connection Firewall, ICF. En un nivel muy básico, existe una similitud en la capacidad de los dos cortafuegos; para detener la interrupción y ofrecer un procedimiento sólido de estrategia de control de acceso. En pocas palabras, en lo que respecta a la autorización de la estrategia de control de acceso, un firewall es un marco que protege su PC.

Funciones de los cortafuegos

- En esencia, estas son algunas de las funciones básicas de los cortafuegos:
- Actuar como intermediario
- Reportar y registrar eventos
- Controlar y administrar el tráfico de red
- Validar acceso
- Defender los recursos

La definición de cortafuegos personal

En el ámbito del procesamiento seguro, es muy fundamental que comprenda su necesidad de un firewall. Además, dado que ayuda a nuestra comprensión de cómo un firewall puede abordar esos requisitos, debemos comprender los objetivos de la seguridad de los datos.

La necesidad de un cortafuegos personal

Electrónicamente, conectará su PC a una organización expansiva en las horas de acceso rápido a Internet. Tendrás un seguro o control restringido salvo que hayas introducido un cortafuegos individual. Hay algunas desventajas en cualquier asociación rápida, un promedio de cualquier otra cosa. De paso,

el mismo elemento que hace una asociación con un rápido indefenso es la misma explicación que lo hace atractivo. De alguna manera, podría estar saliendo abierto y abierto con su asociación con la web rápida. Algunos de los aspectos más destacados de las asociaciones web de alta velocidad incluyen:

- Asociación dinámica consistente: esta es la forma en que cuando su La PC está asociada con la web sin falta, es débil Acceso rápido: esto significa que tiende a ser muy rápido para que los intrusos entren en su PC

- Una IP ordinaria: será más fácil para un intruso descubrir su PC una y otra vez después de haberlo encontrado.

Uso de un cortafuegos personal para la defensa

En comparación con una conexión estándar de 56 Kbps, ahora es obvio para usted cómo, cuando está en línea en una conexión web de alta velocidad, está indefenso. Actualmente, el peligro que presenta este tipo de asociación es conocido por ustedes, y cómo pueden protegerse contra él es lo que necesitan saber. Aquí hay una parte de las explicaciones indispensables detrás de un firewall individual:

- Sin duda, puede crear estrategias de seguridad que se adapten a sus requisitos particulares, ya que la mayoría de los firewalls cercanos a su hogar son excepcionalmente configurables.
- En el momento en que el programa de su PC intenta interactuar con Internet, desea que lo mantengan informado
- La organización doméstica que diriges espera que la mantengas desconectada de la web.
- Utiliza una red Wi-Fi pública cuando se conecta a Internet en una terminal aérea, restaurante o parque
- Con una asociación de banda ancha 'constantemente encendida', navega por Internet en casa

Tipos de cortafuegos

Aunque los dos son razonables, puede tener firewalls como equipo o programación. Con aplicaciones y números de puerto, puede dirigir el tráfico

mediante el establecimiento de un programa de firewall de producto en su PC mientras puede introducir el tipo de firewall de equipo entre el pasaje y su organización. El tipo de firewall más conocido es el paquete que separa los firewalls, y si no se coordinan con un conjunto de reglas de seguridad de instalación, evitan que los paquetes pasen después de haberlos inspeccionado. La motivación detrás de estos tipos de firewall es desglosar el objetivo y la fuente de los paquetes para las direcciones IP. De esta manera, se confiará en ingresar a la organización si los paquetes coinciden con los de una regla 'permitida' en el firewall.

Sin estado y con estado son las dos clasificaciones de los cortafuegos de filtrado de paquetes. Los que son objetivos obvios para los programadores son los cortafuegos sin estado, ya que deben configurarse mediante la inspección de paquetes de forma autónoma entre sí. Por otra parte, los cortafuegos con estado en general serán significativamente más seguros porque recopilan datos sobre paquetes pasados recientemente. Aunque los cortafuegos de separación de paquetes finalmente ofrecen una protección muy básica y, en general, serán muy deficientes, en realidad pueden ser convincentes. Por ejemplo, para ellos decidir el impacto hostil de la aplicación a la que está llegando la sustancia de las solicitudes puede ser muy difícil para ellos. De esta manera, no habrá posibilidad de que el firewall sepa cuándo podría haber un borrado de un conjunto de datos de una fuente errónea mal interpretada si permite una solicitud perniciosa. Los que están preparados para identificar tales peligros son los cortafuegos intermediarios y de última generación.

SMLI, cortafuegos de inspección multicapa con estado

Si bien estos firewalls los comparan con paquetes confidenciales, canalizan paquetes en las capas de aplicación, transporte y organización.
Del mismo modo, si pasan la capa de forma independiente, SMLI solo les permite pasar después de analizar todo el paquete, lo cual es común en los firewalls NGFW. Garantizan la capacidad de todos los intercambios iniciados que ocurren solo con fuentes confiables, ya que deciden el estado de la correspondencia y observan los paquetes.

NAT, cortafuegos de traducción de direcciones de red

Estos cortafuegos mantienen cubiertas las direcciones IP individuales cuando utilizan una dirección IP única para interactuar con la web al permitir que algunos dispositivos con

direcciones de organismos autónomos. A fin de cuentas, ofrecen una protección más notable contra los ataques, ya que los agresores no pueden detectar sutilezas específicas cuando verifican las direcciones IP de una organización. Estos cortafuegos se establecen entre el tráfico externo y una reunión de PC con cortafuegos intermediarios que tienen similitudes con los cortafuegos NAT.

Cortafuegos de proxy

Según el grado de uso, estos cortafuegos tienen la organización separada. Están plantados entre dos marcos finales, a los que no les gustan los cortafuegos básicos. El cortafuegos debe recibir una solicitud del cliente y utilizar un montón de seguridad para la evaluación y, a partir de ese momento, mantenerlo bloqueado o dar su consentimiento. Básicamente, las convenciones de la capa 7, como FTP y HTTP, se observan como cortafuegos sustitutos y, para que reconozcan el tráfico dañino, utilizan paquetes profundos y revisiones con estado.

NGFW, cortafuegos de próxima generación

Estos cortafuegos combinan una funcionalidad adicional con la innovación de los cortafuegos convencionales como un enemigo de la infección, marcos de contraataque de interrupciones, análisis de tráfico codificado y mucho más. Básicamente, cuenta con la incorporación de DPI, investigación parcelaria profunda. Es dentro del paquete real que la revisión profunda del paquete inspecciona la información mientras echa un vistazo a los encabezados del paquete es lo que los cortafuegos esenciales solo buscan. Con este ciclo, los clientes pueden detener, clasificar y reconocer paquetes con información maliciosa.

Capítulo 12

Obtención de información del usuario: Maltego, Scraping, Shodan/Censys.io

Maltego descubre cómo se asocian los datos entre sí como una aplicación científica y de código abierto. La conexión entre algunos tipos de datos puede ayudar a distinguir la relación oscura al igual que brinda una imagen superior de sus conexiones. Cuando utilice maltego, encontrará conexiones y conexiones de personas, como compañeros compartidos, perfiles sociales, sitios y organizaciones con las conexiones de datos acumuladas. Es posible que deba recopilar la asociación entre los cuadrados netos, los nombres de DNS y las ubicaciones si planea acumular información sobre cualquier base.

Arquitectura de Maltego

Los trabajadores de semillas obtienen la solicitud del cliente de maltego a través de HTTPS en un diseño XML. En ese momento, son los trabajadores de TAS los que recibirán la solicitud del trabajador de semillas antes de que la organización profesional reciba la solicitud. El cliente maltego recibirá en ese momento los efectos de la solicitud. Para mayor seguridad, es posible que deba considerar tener sus trabajadores TAS. A partir de ahora, los módulos básico y experto son los dos tipos de maltego, y la accesibilidad de los módulos son los dos contrastes significativos entre los dos trabajadores. CTAS es lo que tiene el trabajador esencial mientras que en el trabajador experto, verá PTTAS, SQLTAS y CTAS.

Desde dentro de maltego, puede realizar algunas tareas relacionadas con pentesting con PTTAS, incluido el arrebatamiento estándar, el barrido de puertos, etc. Del mismo modo, es factible acceder al conjunto de datos SQL para TAS a través de SQLTAS. También puede obtener resultados después de realizar varias consultas SQL utilizando este módulo. Postgress, Oracle, DB2, MSSQL y MySQL son algunos de los tipos compatibles. En ese punto, accesibles abiertamente son los cambios que se contienen en el TAS empresarial.

Lanzamiento de Maltego

Para que cualquiera pueda comenzar maltego, debe ir a las aplicaciones y buscar

retractarse. A partir de ese momento, obtendrá la recopilación de datos y luego la revisión de la organización, donde luego verá la investigación de DNS. Desde ese punto, entrarás en maltego. Se le pedirá que registre su artículo si lo encuentra de manera interesante. Es posible que deba incluir su dirección de correo electrónico y clave secreta si ha registrado un registro a partir de ahora. Actualizará los cambios cuando haya aprobado su inicio de sesión.

Haga clic en la pestaña 'examinar' después de las actualizaciones de los cambios y del rango; puedes elegir tu elección ideal. En el rango, verá dos clasificaciones significativas, que están cerca de casa y marco. Además, se pueden incluir diferentes sustancias en la gama, por ejemplo, el elemento Shodan. Con la guía de su bandera, puede descubrir interruptores específicos, interruptores, trabajadores, etc. a través de un rastreador web como Shodan.

Web Scraping con Python

¿Qué tal si aceptamos que necesita extraer rápidamente una gran cantidad de información de los sitios lo más rápido posible, cómo podría lograr este logro sin obtener su información yendo a cada sitio a la vez? A fin de cuentas, la respuesta corta es web scratching. Para que lo que planee hacer sea más rápido y simple, es posible que deba generar rascado web. Si necesita recopilar información de sitios y cuando el volumen es enorme, puede utilizar web scratching. Sea como fuere, ¿qué puede incitar a alguien a querer recopilar datos masivos de los lugares? Es fundamental hablar de la aplicación web scratching para que entendamos la explicación:

- Bolsas de **trabajo:** algunas sutilezas de los sitios sobre entrevistas, oportunidades de empleo, etc., a las que los clientes sin duda pueden acceder ya que se registra en un solo lugar.
- **Desarrollo e investigación:** recopilan temperatura, datos generales, información, etc. de los sitios, que son una gran cantidad de datos mediante el rascado web, y utilizan el resultado para I + D o para completar revisiones después de examinarlo.

- **Raspado de redes sociales:** descubrir qué se está moviendo mediante la recopilación de información de sitios de medios basados en la web como Twitter a través del raspado web.
- **Recopilación de direcciones de correo electrónico:** el web scratching es utilizado por algunas asociaciones que utilizan publicidad por correo electrónico para enviar mensajes masivos después de recopilarlos.
- **Comparación de precios:** para el análisis de los precios de los artículos, las administraciones como ParseHub utilizan el web scratching para recopilar información de destinos de compras basados en la web.

La extracción de una enorme cantidad de datos de los sitios es un procedimiento de web scratching. La información del sitio no está organizada, y para tenerla en una estructura organizada, esta información no estructurada se recopila mediante web scratching para hacer el trabajo. El código de composición, las API y las administraciones en línea son algunas de las diversas formas de eliminar sitios. Ciertos sitios permiten el web scratching, mientras que otros no lo permiten si necesitamos movernos a su lado legítimo. Es posible que deba echar un vistazo al documento "robots.txt" del sitio para saber si dicho sitio permite el rascado web o no.

Shodan y Censys

Es en el Internet de las Cosas que estamos viviendo actualmente. Comenzando desde las cámaras de vigilancia vial y los marcos de administración de señales de tráfico hasta los conmutadores WiFi domésticos, las cosas que están asociadas con Internet están constantemente en nuestra experiencia. Además, es tanto en la web como en esta realidad actual donde podemos descubrir a cada uno de ellos ya que tienen una asociación.
Con la ayuda de Google para encontrar la información que busca en la web, también puede rastrear estos dispositivos asociados con algunos rastreadores web poco comunes.

¡Qué tal si invitamos a Shodan y Censys!

Dado que ha estado presente durante alrededor de 7 años, para Internet de las cosas, el jefe, al igual que el rastreador web principal, es shodan. La motivación detrás del nombre provino de una conciencia creada por el hombre excepcionalmente miserable llamada Shodan, que era System Shock, el principal enemigo de la configuración de juegos de PC. A pesar de que tiene la capacidad de destruir el daño, Shodan en realidad no es tan incansable. Sea como fuere, necesitarás saber

cómo funciona el índice web antes de pasar a las terribles noticias.

Shodan es comúnmente como alguien que golpea cada entrada que ve mientras deambula por el área. Sea como fuere, existe el mundo entero en lugar de una ciudad o golpeando cada dirección IPv4. Esta persona tendrá algunos datos y se los ofrecerá si obtiene información sobre una parte específica del área o un tipo particular de entradas. El individuo le revelaría la cantidad de entradas, las personas que responden a estas entradas y sus expresiones. Además, sobre esos Internet de las cosas, puede obtener sus datos de shodan, que incluye si hay una interfaz web que pueda utilizar, su tipo y cómo se llaman. Aunque, por lo general, es modesto, debe aceptar que use shodan porque no es totalmente gratuito.

Además de que no hay cerraduras en ciertas entradas, es posible que no descubras nada tan extraño en golpear ciertas entradas. Además, para que los alborotadores entren, puede que no sea factible para nadie. Algunos marcos que utilizan contraseñas e inicios de sesión predeterminados, incluidas cámaras IP y conmutadores desprotegidos, son las representaciones de estas entradas en el ámbito de Internet de las cosas. Se verá a sí mismo adquiriendo acceso total a la clave secreta e iniciar sesión cuando haya descubierto cómo solucionarlo después de ingresar a su interfaz web. Además, dado que puede descubrir fácilmente estos datos predeterminados sobre contraseñas e inicios de sesión en el sitio de los fabricantes, todo es en este punto, no es ciencia avanzada. Además, si cuenta con la ayuda de una cámara IP, puede manejar e incluso ver todo si se trata de una cámara IP. Además, puede modificar la configuración si se trata de un interruptor. Incluso puede usar una voz alarmante para conversar con el niño indefenso si se trata de una pantalla infantil. Todo está a la altura de los principios de vuestra ética.

Capítulo 13

Kali Linux en dispositivos portátiles como Raspberry Pi

Sin embargo, tiende a ser lo suficientemente divertido como para poner a prueba organizaciones, parodiar registros o descifrar contraseñas WiFi. En cualquier caso, es posible que necesite un aparato efectivamente versátil si espera llevar el espectáculo fuera de casa. Por lo tanto, aquí vienen Raspberry Pi y Kali Linux. Planificaron Kali Linux para pruebas de infiltración de red como marco de trabajo. Para que pueda probar las debilidades de Bluetooth, las organizaciones de parodia, la ruptura de contraseñas WiFi y muchas cosas diferentes, tiene la oportunidad de ejecutarlo en su PC. Debe saber que puede ser acusado de un delito legal y ser capturado por ignorar la Ley de Seguridad Informática en caso de que ingrese a redes protegidas que utilizan esta información. Simplemente puede utilizar esta información para jugar con las redes que controla, para su aprendizaje o, esencialmente, para usarla de manera excelente. Ahora, dado que hemos hablado mucho sobre Kali Linux, y por no repetir todo lo que ha leído anteriormente, nuestra atención se centrará en cómo construiremos nuestra Raspberry Pi y la versión que utilizaremos. Por lo tanto, ¡debemos completarlo!

Para que pueda utilizar Raspberry Pi, no necesitan mucha fuerza para que pueda utilizarlos como una pequeña PC estimada en términos de crédito. Tendrá un dispositivo de prueba de marco súper compacto que puede llevar fácilmente a donde quiera que vaya con la combinación de Kali Linux y Raspberry Pi.

Lo escencial

- Para realizar la instalación inicial, necesitará una PC. Obtenga una
- consola remota pequeña y compacta con un panel táctil que puede contener un lado de un pequeño saco. Por lo general, será muy útil si
- lleva la Raspberry Pi con usted. De esta forma, una carcasa está bien pero discrecional. Una nueva forma de resaltar esta pantalla es fundamental pero con Raspberry Pi 2 o versiones más recientes; no
- encaja al ras Una tarjeta SD de 8 GB Una tarjeta Wi-Fi Aprobarás un par de baterías externas de 5V que utilizan una parte USB que funcionaba para teléfonos móviles. Por lo tanto, necesita un paquete de
- batería
-

- Modelo 2 o B/B+ de Raspberry Pi. Aunque para presentar Raspberry Pi 2, necesitará algunos avances adicionales; Es posible que deba utilizar el Modelo B + si no desea pasar por esos medios.

Paso 1: Instalación de Kali en la Raspberry Pi

Para Raspberry Pi, descargar e instalar el trabajo de pantalla táctil para Kali Linux será lo principal que debe hacer. La interacción de establecimiento es muy regular de presentar algún otro marco de trabajo para Raspberry Pi. Aquí hay un enfoque rápido:

Instalación de Kali en la tarjeta SD de Windows

1. Para su equipo, debe descargar Kali Linux Frambuesa Pi. Puede obtener el formulario Pi 2 para Raspberry Pi 2 y la variante TFT para el modelo B/B++. En su interior, desbloqueará el registro img. Debes observar aquí porque, para Raspberry Pi, debes descargar la versión estándar de Kali Linux si no estás utilizando la pantalla táctil.
2. Debes tener la solicitud (.registro ejecutivo) desabrochada dentro después de descargar Win32DiskImager.
3. Con el uso de un lector de tarjetas, en ese momento tendrá su tarjeta SD integrada en la PC con Windows.
4. Luego, tocará dos veces la aplicación, Win32DiskImager.exe que ha descargado recientemente.
5. En la parte superior derecha del gadget, tocará el menú desplegable para elegir entre el resumen si la aplicación no reconoce naturalmente su tarjeta SD.
6. El documento .img de Raspbian que tienes recientemente descargado se puede descubrir cuando hace clic en el símbolo del sobre del registro desde el área de la imagen de la aplicación.
7. Win32DiskImager hará algo asombroso mientras te sientas cómodo después de haber tocado el botón 'redactar'. Puede incrustar su tarjeta en su Raspberry Pi después de haber disparado de forma segura su tarjeta SD cuando termine.

Instalación de Kali en OS X Tarjeta SD

1. Para que puedas trabajar con él en tu equipo, primero deberás tener descargada la imagen Kali Linux Raspberry Pi. Tomará una versión Pi 2 para Raspberry Pi 2 y un formulario TFT para el modelo B/B++. La versión estándar de Kali Linux para Raspberry Pi es fundamental para descargar si es la pantalla que está utilizando.

2. Para su versión actual de OS X, tenga la versión adecuada
   Adaptación elegida al desabrochar la aplicación después de haber descargado el fabricante de la tarjeta RPi-sd.
3. Con el uso de un lector de tarjetas, incruste su tarjeta SD en su Mac.

4. Luego, puede abrir el desarrollador de su tarjeta RPi-sd. Habrá un momento breve para que elijas una imagen de Raspbian. El registro que ha tenido descargado antes es todo lo que debe elegir.

5. Luego, otro breve le preguntará sobre la asociación de su tarjeta SD.
   Todo lo que necesita es tocar 'continuar' ya que está asociado cuando lo incrustó antes. En ese momento, se le presentarán las alternativas para las tarjetas SD. Se verificará y no verá nada más en la lista si acaba de tener uno incrustado. Ajuste bien la tarjeta que necesita utilizar si no es así.

6. Luego, ingresarás la frase secreta para la organización y presionarás ingresar.
7. Si hay alguna descarga de la tarjeta SD, verás una más breve. Dado que para que la aplicación reproduzca un duplicado inmediato, debe desmontarse; no hay nada extraño en ello. En el Finder, para que su tarjeta SD ya no esté accesible, debe tocarla dos veces. Una expresión de alerta aquí: NUNCA lo elimine de su puerto USB. Puede hacer clic en continuar cuando esté seguro.
8. La preparación de su tarjeta SD terminará con la tarjeta RPi-sd fabricante. En ese momento, puede incrustarlo en su unidad Raspberry Pi después de haberlo lanzado de forma segura.

Paso 2: la conexión de la pantalla

La pantalla táctil funciona a la perfección con la información/rendimiento universalmente útil que tiene Raspberry Pi. Percibirás cómo funciona esto en un mundo perfecto porque, en la esquina, está la disposición de pines en tu Raspberry Pi. Acceda a la presentación de Raspberry Pi.

Paso 3: tener todo enchufado e iniciar

En esta etapa, debe conectar todo a través del espectáculo agredido.
Tenga su conector Wi-Fi conectado a los puertos USB. A partir de ese momento, conecte el Pi a su grupo de baterías. Aquí, puede encontrar un ciclo engorroso y moderado para el inicio. Si requiere alguna inversión, no se congele. Para empezar, antes del ciclo de inicio del arranque, durante un rato, verá una pantalla blanca. Por último, una pantalla de inicio de sesión le dará la bienvenida. Para que su pantalla funcione, es posible que deba trabajar con algún tipo de arreglo si está utilizando una Raspberry Pi 2. Básicamente, es posible que deba pasar al siguiente nivel si es el B + que estás utilizando. En su mayor parte, para que la pantalla funcione, es posible que se requieran algunos pasos para la Raspberry Pi 2 actual. Una pantalla blanca y trágica lo invitará cuando la inicie al principio. No obstante, conseguir que la pantalla funcione no es excesivamente complicado.

Sorprendentemente, es posible que una conexión Pi no necesite una pantalla HDMI o, a través de esta parte, es posible que necesite acceso SSH. Luego, para iniciar su Pi, simplemente asocie ambos.

Paso 4: habilite Wi-Fi al iniciar sesión

Para que pueda utilizar las herramientas dentro de Kali Linux, deberá habilitar la tarjeta Wi-Fi al iniciar sesión. Raspberry Pi percibirá su tarjeta Wi-Fi de forma natural. En cualquier caso, es fundamental entrar en tu organización. La interfaz de usuario de Kali Linux debe controlarse en cualquier caso.
Finalmente, debe cambiar la frase secreta de su dispositivo antes de participar en cualquier otra cosa. Si no lo hace, su dispositivo puede ser bloqueado por otra persona con habilidades de piratería.

capitulo 14

malduino

MalDuino tiene la capacidad de infusión de consola como un dispositivo USB controlado por Arduino. A una velocidad sobrehumana, MalDuino actuará como un compositor, las órdenes de la consola cuando lo enciendes. El cielo es el límite con MalDuino, ya que puedes ajustar el fondo del área de trabajo o adquirir una concha de converse. Además, MalDuino puede funcionar admirablemente para tramposos, especialistas y analizadores de infiltración. La mejor experiencia BadUSB es todo lo que MalDuino pretende dar.
Además, utilizando bibliotecas de código abierto, es a través del IDE de Arduino que han modificado a MalDuino con respecto a la programación. Puede cambiar el contenido escrito en DuckyScript al código que comprenderá MalDuino. Para que ellos lo programen básicamente como, lo harían con un Arduino; Esto hace que sea factible para los aficionados maestros de Arduino programarlo de la misma manera que lo hace agradable para principiantes. Las dos versiones de MalDuino son Lite y Elite.

Élite

Puede elegir el contenido que desea ejecutar desde la tarjeta, ya que esta versión tiene cuatro interruptores DIP y un lector de tarjeta Micro-SD, y es mucho más grande. Del mismo modo, puede programar el contenido de infusión de pulsaciones de teclas que guarda la tarjeta Micro-SD aparte de consumir el firmware una sola vez. Este ciclo se opone a la versión Lite, que, si desea ejecutar un contenido alternativo, debe ser rayado. Puede soltar, reutilizar o reconstruir cada uno de estos aspectos destacados porque es directamente desde el Arduino que modificaron los dos MalDuinos. A pesar de que puede tener un par de pines con los que jugar, puede comprar uno y realmente le gusta utilizarlo como un Arduino estándar. Se le incitará a participar en el esfuerzo de subvención del grupo, especialmente con la oportunidad que ofrece.

Un poquito

La versión Lite contiene un cambio separado del conector USB, y esta forma es diminuta. Puede elegir entre programación y modo de ejecución con

la capacidad del interruptor y la señal de que el contenido ha completado el proceso de pasar por un LED. Con una cantidad de espacio muy considerable para la mayoría del contenido, en sus 32 KB de memoria disponible localmente, Lite almacena contenido. Puede utilizar el convertidor de contenido para cambiar el contenido a un código compatible con malduino, ya que puede utilizar un procesador de textos para redactar el contenido. En ese momento, con el IDE de Arduino, también puede transferir contenido. Utilizando el interruptor en la parte posterior, puede cambiar el Lite al modo preparado después de haber desconectado el MalDuino Lite. En ese momento, ¡puedes comenzar a utilizarlo!

El hardware

El cuerpo principal de la forma Elite mide alrededor de 4,6 cm x 1,1 cm, generalmente 1,8 x 0,43 pulgadas, por lo que puede utilizar una carcasa antigua. Para la tarjeta Micro-SD y los interruptores DIP, es posible que deba cortar algunas aberturas para ellos. Es posible que reconozca que el firmware con el que se envía es probablemente una especie de prueba de control de calidad para las zambullidas después de practicar un poco de RTFM y jugar con los interruptores. Dependiendo de qué interruptores estén encendidos, estos puntos destacados hacen que el rendimiento de MalDuino sea el número 1 a 4.

La puesta en marcha

Su Arduino IDE no solo debe ser presentado, sino también con visión de futuro cuando necesite configurar el MalDuino. Dado que modificaron el Elite como un "Sparkfun Pro Micro" que funciona a 8 MHz y 3,3 V, se espera que introduzca los bloques Sparkfun y abra el administrador de la placa. En ese momento, la entrada en línea del Malduino Script Converter es su próximo punto culminante, ya que existen tantas funciones que funcionan como:

- Para importar al IDE, genera automáticamente el proyecto Arduino
- Tendrá la libertad de seleccionar el idioma de la distribución de su teclado
- Entre la versión Elite y Lite, puede convertir scripts a través de él.

Solo necesita tener el MalDuino rayado una vez y luego guardarlo nuevo

contenidos que utilizan la tarjeta Micro-SD cuando está en actividad normal, ya que anula el contenido para descargar el proyecto o crea contenido sencillo para la adaptación de Elite.

El software

Para ejecutar una orden, una ruta alternativa rápida será la combinación de ALT-F2 ya que está ejecutando Linux. Por lo tanto, puede guardar un registro en 1111.txt después de escribirlo en un documento. Entonces, para un registro que se compara con el nuevo interruptor de inmersión Express, la búsqueda estará en Elite para la tarjeta Micro-SD si enciende los interruptores de inmersión 4 y 2. Por lo tanto, habrá un esfuerzo por parte del producto para analizar el contenido y encontrar el archivo con el nombre 0101.txt, es decir, no la doble representación de los números 4 y 2 sino en la solicitud de cambio de inmersión 1,2,3 y 4 En ese momento, habrá un destello rápido del LED rojo cuando termine. Es concebible que el comando único que funcione exactamente sea el combo ALT-F2, y básicamente todos los comandos funcionaron. De esta manera, no obtendrá ninguna ventana de orden de ejecución sin ALT-F2.

Protegiéndose de MalDuino

Como dispositivos de infusión de pulsaciones de teclas, MalDuino es un grupo más extenso de dispositivos USB, denominados BadUSB. Tienen la capacidad de hacer algunos tipos de cosas clandestinas al explotar la contribución de la consola como un método confidencial para interactuar con una PC. Sin embargo, ¿cuáles son simplemente las acciones que puede tomar para monitorearse contra MalDuino? Puede aliviar o protegerse de los peligros de los ataques de BadUSB de las siguientes 3 formas diferentes:

Bloqueo de derechos de administrador

No hace ninguna diferencia si está preocupado por el asalto de BadUSB o no; hacer esto puede ser muy valioso. Si necesita realizar cambios en el nivel de administrador, solo debe indicar sí o no para realizar cambios que requieran derechos de administrador en Windows 10. Independientemente de si la persona es el administrador, verá que no lo es. correcto y sin sentido darle a alguien ese grado de control. Antes de ocuparse de las llaves del palacio, puede cambiar esto con un cambio de nivel de bóveda para hacer que el sistema operativo requiera la contraseña de su administrador.

Caza de patos

Este procedimiento es pertinente en Windows. Hay una pequeña aplicación en GitHub que puede ejecutarse como una medida de paso secundaria. La velocidad a la que se componen sus claves es lo que filtra constantemente. En el momento en que reconoce velocidades de composición sorprendentes, bloqueará todos los HID. Sin embargo, una parte de los primeros pocos caracteres de un enlace casi seguro puede atravesarse y ese es su único inconveniente.

Protección Física

Es solo un arreglo general, y es muy importante no permitir que dispositivos no aprobados se conecten a su sistema. Puede poner recursos en algunos dispositivos de bloqueo de puertos para impedir realmente el acceso a los puertos USB. Es posible que deba mirar más a fondo debido a la base básica. De cualquier manera, puede prevenir cualquier ataque usándolo cuando está al aire libre.

Capítulo 15

kismet

Como sistema de ubicación de interrupción remota, un kismet es un dispositivo de protección, rastreador, buscador de dispositivos y organización remota. Si bien las capacidades de kismet son incompatibles con los equipos, por ejemplo, RTLSDR, así como algunos equipos de captura específicos, también funciona con ciertas interfaces de radio, Bluetooth e interfaces Wi-Fi caracterizadas por productos. Algo y bajo la estructura WSL, kismet también funciona con Windows pero funciona de maravilla con OS X y Linux. Kismet funciona con interfaces Bluetooth y Wi-Fi, al igual que otros dispositivos de equipos en Linux. Las interfaces Wi-Fi implícitas le permiten funcionar en OS X y trabajar con botones remotos en Windows 10.

Ver las actividades del usuario de Wi-Fi usando Kismet

Con una línea directa de la vista y un cable de radio Wi-Fi direccional, es posible identificar las señales de Wi-Fi que pasan por las paredes de su hogar, incluso con sus paredes de seguridad. Las personas pueden dominar una gran cantidad de información a partir de estos datos, como los fabricantes de dispositivos cercanos, los movimientos de los ocupantes y la organización que usan en un momento dado. Para objetivos fijos, utilizar kismet en una circunstancia determinada puede generar datos más matizados. Por lo tanto, es ideal para mostrar conexiones entre dispositivos a largo plazo en lugar de simplemente buscar el pasaje. El atractivo proviene de las estrategias de percepción de señales cuando espiamos a los clientes que utilizan kismet, por lo que es a través de las señales que transmite que deseamos descubrir lo que no podemos ver. Aquí, Wi-Fi son las cosas que estamos manejando y los dispositivos que alguien posee, el movimiento humano, los dispositivos asociados y los interruptores son las cosas que estamos tratando de ver. Hacer esto va mucho a tu mente creativa.

Estará más dispuesto a apagar su Wi-Fi en dispositivos no utilizados y cambiar a una organización con cable si puede asegurarse de que alguien pueda ver si estaba usando su PC o su PlayStation y si estaba en su casa. Utilizando una organización remota, usan kismet para verificar

cada canal Wi-Fi accesible en silencio colocándolo en modo de pantalla para paquetes remotos para que haga algo increíble. Puede ver carcasas de señales robotizadas como estos paquetes que los puntos de acceso remotos pueden comunicar varias veces en un segundo. Además, las carcasas de prueba aún no asociadas y los paquetes de información se intercambian desde los dispositivos asociados. Kismet puede imaginar la acción de los dispositivos relacionados con organizaciones específicas al igual que las propias organizaciones.

Lo que podemos obtener de Wi-Fi

De todos modos, ¿cómo lidiaríamos con la circunstancia actual? Puede continuar investigando información matizada sobre una organización que necesita observar cuando la haya reconocido. Es posible que deba buscar sutilezas, por ejemplo, la asociación de organización del equipo y el hardware de alguien o una asociación. En realidad, querrá saber el tipo de arreglo para ciertos dispositivos y el reconocimiento de otros tipos de arreglo para la marca única. No solo las estaciones de trabajo y los teléfonos móviles son sencillos para usted, sino que también verá la acuicultura asociada o las impresoras 3D con una configuración como esta.

Actualmente, el tipo de persona que eres tiene mucha confianza en la utilidad de esta información. Es útil para un delincuente que necesita encontrar dispositivos costosos husmeando en todas las casas a distancia. Al utilizar un asalto fijo, puede apuntar a uno o mantenerse alejado de uno por completo porque kismet puede reconocer las cámaras de vigilancia remota. Además, cuando no hay nadie en la casa, definitivamente podemos interpretarlo, ya que es muy factible para nosotros ver cuándo los dispositivos de los usuarios usan información, desaparecen y aparecen. Asimismo, con la utilización de la información de la señal Wi-Fi, los programadores pueden consolidar la información del GPS al desplazarse por un área. Haciendo esto, cada dirección de la organización remota será factible para los programadores cuando armen una guía. Básicamente, como ahora hay organizaciones planificadas por Google y Wigle Wifi, podría haber presencia de esta información. En las áreas, para la ubicación de movimientos remotos dudosos, las personas también pueden usarlo como vigilancia local.

Herramientas esenciales

Hay algunas cosas que deben aferrarse a esta guía. Necesitará kismet para ejecutar un marco de Linux, y para el examen, necesitará

también requieren un conector de organización remota que sea compatible con Kali.
Aquí, la versión más establecida que es constante es lo que examinaremos, aunque las tarjetas remotas únicas como macOS pueden ejecutarse en el nuevo tipo de kismet. Si desea ejecutarlo en Raspberry Pi, kismet funcionará completamente en una instalación Kali-Pi como una máquina virtual.

Paso 1: instalación de kismet:

El archivo git debe pasar por un ciclo de clonación antes del establecimiento de kismet en Kali Linux. No tendrá que preocuparse por ninguna condición que dependa del tipo de sistema de trabajo que esté utilizando.
No obstante, el resumen algo más largo de las condiciones para kismet podría haberse introducido para el buen funcionamiento de kismet.
Dado que debe clasificar, iniciar sesión, desentrañar y reconocer innumerables datos remotos, son muy necesarios. Del mismo modo, debe introducir montones de bibliotecas ya que controlará una tarjeta remota. En ese momento, debe tener el establecimiento diseñado explorando el registro de kismet. Para su circulación en el marco de trabajo particular, esta interacción tendrá el establecimiento dispuesto. En ese punto, podrá realizar el establecimiento después del cumplimiento de ese ciclo. Utilizará la opción suidinstall para finalizar la instalación ejecutando el siguiente documento con ella. En ese momento, presentará kismet. Después del establecimiento, debe recibir paquetes como cliente no root agregándose al grupo de kismet.

Asegúrese de que su nombre de usuario genuino se sustituya en el espacio por "su nombre de usuario".

Paso 2: ponga en modo monitor su tarjeta inalámbrica:

Con la configuración USB, conectará su tarjeta de organización remota a la máquina virtual o su PC. Los pedidos ifconfig o IP a se pueden utilizar para descubrir su tarjeta. Puede utilizar "wlan0" o "wlan1" para nombrar su tarjeta.
A continuación, podrá colocar su consideración en un modo de pantalla después de nombrarlo. Hacia el final del nombre de la tarjeta, verá un

"mon" como se le cambia el nombre con esta interacción. Además, para enviar kismet, utilizará este nombre.

Paso 3: lanza kismet:

Es fácil comenzar a utilizar kismet. Para su tarjeta que ha colocado en modo de pantalla remota, asegúrese de poner el término después de la – c, ya que para determinar la fuente que capta, kismet utiliza la – c. En ese momento, kismet comenzará a recibir paquetes después de encenderse. En ese momento, puede volver al menú y realizar algunas personalizaciones.

Algunos dispositivos Wi-Fi que puedes distinguir cerca aparecerán ante ti cuando inicies kismet. Si está utilizando 5 GHz, 2,4 GHz o ambos, tendrá una diferencia en la cantidad de dispositivos que puede identificar.

capitulo 16

Omitir un SSH oculto

Ahora tenemos que dedicar un poco de esfuerzo para intentar atravesar y eludir uno de los inicios de sesión de SSH. Haremos esto agregando nuestra propia clave.

a un trabajador distante y luego obtener la entrada que necesitamos. Entonces, si necesitamos revisar y organizar las claves SSH para que podamos iniciar sesión de manera rápida y productiva sin una palabra secreta, podemos hacerlo con una sola orden. Este será un ciclo sencillo de atravesar.

El SSH se conocerá como Secure Shell, y será una convención de organización criptográfica que será valiosa para ayudarnos a trabajar los beneficios de la organización de manera segura en una organización inestable. Las aplicaciones normales que veremos con esta incorporarán opciones como iniciar sesión con la línea de pedido y ejecución remota de pedidos, sin embargo, es posible que cualquier servicio que desee utilizar se obtenga con la convención SSH.

La fase inicial de este ciclo es asegurarnos de que hemos tenido la opción de ejecutar el generador de claves para crear las claves. Suponiendo que haya producido efectivamente una parte de estas claves, podemos evitar estos medios. El código que podemos usar para este está debajo

ssh-keygen-t rsa

En ese punto, podemos pasar y utilizar esta orden específica para presionar la tecla para que se asocie con el trabajador remoto. Esto será algo que podemos ajustar para coordinar con el nombre de cliente del trabajador y el nombre de host de su trabajador también. De hecho, querremos revisar y utilizar el código a continuación para que esto funcione.

gato ~/.ssh/ id_rsa.pub | ssh usuario@nombre de host 'cat >> .ssh/ authorized_keys'

La primera vez que dupliquemos estas claves, tendremos que ingresar la clave secreta para ayudar al programa a preparar la instalación y listo. Sin embargo, después de esa primera vez, deberíamos tener la opción de iniciar sesión sin requerir una palabra secreta o incluso utilizar rsync o SCP sin ingresar la palabra secreta por ningún tramo de la imaginación. Puede probar esto con el pedido adjunto:

ssh usuario@nombre de host

Sin duda va a ser significativamente más fácil de pasar en comparación con

componer en clave secreta constantemente.

Nd, eso es todo lo que necesitamos hacer. Invertirá algo de energía ayudándonos a ingresar al SSH y hará que sea más fácil para nosotros acceder a esto sin esperar utilizar una clave secreta cada vez que hagamos el trabajo. Completar esto puede ser difícil, y usted tiene que saber la palabra secreta la primera vez, sin embargo, si puede llegar a esto, y realmente querrá ingresar a la organización en cualquier momento que desee.

capitulo 17

Omitir una autenticación de dirección Mac y Autenticación abierta

Otra cosa que podemos hacer con respecto a la piratería es eludir la autenticación de direcciones Mac para ingresar a la organización que necesitamos utilizar.
Este será un elemento que encontraremos con las tendencias de Mac que nos permitirá acceder al sistema y usarlo de la forma que queramos. Esto garantizará que podamos ingresar a nuestra organización cuando no esté funcionando bien o en otra alternativa que queramos utilizar, por ejemplo, piratear otra PC. ¿Qué tal si investigamos cómo funcionará esto?

La dirección de Control de acceso a medios, o la dirección MAC, resultará intrigante porque puede reconocer en particular todos los centros que aparecerán en una organización. Aparecerá como seis conjuntos de dígitos hexadecimales, que pueden incorporar del 0 al 9, y la totalidad de las letras de la A a la F, que se aislarán mediante carreras o dos puntos.

Esta dirección MAC generalmente estará relacionada con el conector de la organización o un dispositivo que los convierte en capacidades de red. A la luz de esta explicación, se hará referencia en general como la ubicación real. Los primeros tres conjuntos de estos dígitos en la ubicación se conocerán como el Identificador único de la organización, y debemos hacer un esfuerzo para analizarlos, ya que nos ayudan a distinguir la organización que

vendió o fabricó el aparato. En ese momento, los últimos tres conjuntos de dígitos que aparecerán serán los números específicos que solo van a ese dispositivo y parecerán el número crónico de toda la interacción.

Teniendo esto en cuenta, invertiremos algo de energía en analizar y analizar algunos de los medios que debemos usar para evitar que la dirección MAC se separe en una parte de nuestras organizaciones remotas. El paso inicial con el que debemos trabajar es pensar que vamos a trabajar con un conmutador que tenga configurado el filtrado MAC en cualquier caso. Podemos decir que nuestra dirección MAC será AA-BB-OO-11-22. Este puede aparecer cuando estamos utilizando la separación de MAC en nuestra propia organización remota.

En ese punto, ha llegado el momento de seguir adelante. Podemos iniciar sesión en la máquina que estamos usando para Kali Linux y luego poner ese conector Wi-Fi en el modo que le permite detectar lo que sucede a su alrededor.
Esto se terminará con el airman-ng y debería ser posible con el pedido básico en nuestra terminal a continuación:

Airmon-ng inicio wlan ()

Actualmente, es posible que una parte de los ciclos con Kali Linux cuando haga esto nos muestre algunos errores. En caso de que termine con ciertos problemas o un mensaje de error aquí, en ese momento, debe eliminar la interacción en este programa que, según todos los informes, tiene el problema.
Puede hacer esto con el orden a continuación:

matar [pid]

Ahora ha llegado el momento de atravesar y despachar otra pieza de este ciclo, que es el Airodum-ng. Esto nos ayudará a encontrar la organización remota con la que necesitamos trabajar e incluso nos ayudará a ver qué clientes están asociados en toda esta interacción. El orden que podemos usar para que funcione es el siguiente: *airodump-ng –c [canal] –bssid [dirección MAC del enrutador de destino] –i wlan0mon*

Esto debería mostrarnos un resumen completo de los usuarios asociados con este dispositivo en la parte inferior de nuestra terminal. En ese punto, el

El siguiente segmento enumerará las ubicaciones MAC de la multitud de usuarios asociados que realmente queremos parodiar en este momento para validar ese arreglo remoto para que podamos hacer lo que queramos en él.

Lo único que debe tener en cuenta a partir de ahora es que solo obtendrá un resumen de esta progresión si realmente hay alguien que esté asociado con la organización remota que estamos observando. Suponiendo que no tenga a nadie asociado actualmente con el dispositivo, no obtendrá un resumen ahora.

Actualmente es la oportunidad ideal para que pasemos a la siguiente etapa. Después de haber tenido la opción de revisar y encontrar la dirección MAC que desea utilizar, ha llegado el momento de recorrer el camino hacia el uso de la solicitud rin de MacChange para parodiar la dirección MAC con la que queremos trabajar. Invertiremos nuestra energía en ridiculizar la dirección MAC de su conector remoto, sin embargo, lo principal que debemos hacer aquí antes de comenzar, debemos desactivar la interfaz de verificación conocida como wlan0mon y wlan0. Esto nos permitirá realizar una parte de las progresiones que necesitamos a la dirección MAC. Podemos hacer esto con el orden adjunto para simplificar un poco las cosas:

Airmon-ng deja de wlan0mon

En el momento en que finaliza ese ciclo, podemos desactivar la interfaz remota cuya dirección MAC debemos parodiar en el siguiente orden:

Ifconfig wlan0 abajo

En ese momento, esto nos presentará el MacChanger. Podemos utilizar este aparato para cambiar la dirección MAC. El código que podemos hacer con este estará debajo:

macchanger - m [Nueva dirección MAC] wlan0

Y luego, tenemos que revisar y traer la totalidad de esa copia de seguridad. Recuerde, un par de pasos anteriores, revisamos y cerramos el marco con el objetivo de que pudiéramos cambiar el nuestro y obtener esta alternativa. En cualquier caso, ahora tenemos que pasar y presentar

todo copia de seguridad una vez más. El código con el que podemos trabajar aquí incluirá:

Ifconfig wlan0 arriba

Dado que hemos tenido la opción de cambiar la dirección MAC que está en nuestro conector remoto a una dirección MAC registrada en blanco que la otra organización permitirá, podemos intentar validar con la organización y ver si esto funcionó y si es posible. que podemos asociar con la interacción también.

Es más, eso es todo para completar esto. Recuerde que esta interacción puede tomar un poco de tiempo si no encuentra a alguien que esté directamente en la organización en primer lugar. Es posible que deba tener cierta persistencia con este para asegurarse de que funcionará de la manera que desee y para garantizar que realmente pueda rastrear la dirección MAC correcta que funcionará con ese conmutador.

Sin embargo, siempre que haya tenido la opción de pasar y cambiar su dirección MAC para que funcione admirablemente con una de las otras alternativas que tienen un lugar con esa organización remota para que usted también pueda continuar. Esta es una interacción sencilla que estará lista para ayudarnos a aprender el ciclo y cómo podemos funcionar para ingresar a la organización que querríamos en el camino.

capitulo 18

Hackear WPA y WPA2

El universo de las organizaciones remotas será extraordinario para muchos clientes. Agrega una tonelada de seguridad a las organizaciones del pasado, y será esencial para ayudarnos a trabajar con nuestra organización remota mientras se mueve y sin estar conectado a su enlace constantemente. Las alternativas WPA y WPA2 serán probablemente las mejores en lo que respecta a la protección de sus datos, pero es posible que los programadores accedan a ellas si son pacientes, y están preparadas y asumen el trabajo difícil. Esa es la razón por la que invertiremos algo de energía en esta sección dando un vistazo a los avances que son importantes para piratear estas dos organizaciones remotas.

Lo principal que tenemos que investigar es preparar nuestro asalto. Inicialmente, debemos tener una comprensión superior de cuándo podemos piratear legalmente una organización de Wi-Fi. En muchas áreas, el único momento en que puede piratear legalmente una parte de estas organizaciones es el punto en el que la organización tiene un lugar con usted, o si tiene un lugar con alguien que nos ha dado su consentimiento para piratear la organización. para que puedas comprobarlo y asegurarte de que está protegido de un programador. Hackear redes que no cumplen con los estándares que están arriba, entonces el ciclo de hacking es ilegal y muy bien puede ser conocido como un delito grave en caso de que quede atrapado en la manifestación.

Dado que esto está muy lejos, es la oportunidad ideal para que revisemos y descarguemos la imagen circular de Kali Linux. Este será uno de los aparatos favoritos para trabajar cuando llegue el momento de piratear estas organizaciones. Puede descargar la imagen de la institución, también llamada ISO, utilizando los avances adjuntos:

1. El paso inicial con el que trabajaremos es ir a https://www.kali.org/downloads/en el navegador de Internet de sus requisitos.
2. Haga clic en HTTP cerca de cualquiera de las formas de esto que desee. para utilizar.
3. Espere a que termine el registro con el ciclo de descarga.

A partir de aquí, debemos tener la opción de unirnos a un glimmer roll over a la PC con la que estamos trabajando. La unidad Blaze que estamos utilizando debe acompañar a 4 gigabytes de la sala o más para completar esta interacción.

En ese momento, podemos hacer que la unidad Blaze sea de arranque. Complete el resto de los medios que debe hacer para instalar el marco Kali Linux y configurarlo todo en su propia PC.

En el momento en que el marco Kali Linux está configurado y preparado, ha llegado el momento de comenzar el truco real que necesitamos lograr. Podemos hacer esto abriendo la terminal para Kali Linux en su PC. Puede descubrir y tocar este símbolo de la aplicación Terminal, que se parecerá a un cuadro negro que tiene un ">_" blanco. También puede tocar o Alt, Ctrl, T para abrir este terminal.

Este es el momento en el que deberá presentar Aircrack para ayudar con el asalto. Puede escribir el orden que se encuentra debajo para ayudarlo a resolver este caso único:

sudo apt-get install aircrack-ng En

el momento en que aparezca el informe para este, deberá ingresar la palabra secreta. Puede escribir la clave secreta que usa para iniciar sesión en esa PC en cualquier caso. En ese punto, presione el botón Enter. Esto asegurará que el acceso raíz estará habilitado para cualquiera de las diferentes órdenes que desee tener la opción de ejecutar en la Terminal. Si elige a partir de ahora abrir otra ventana para una Terminal, lo cual es concebible, recuerde que es posible que deba pasar y ejecutar el pedido con el prefijo sudo o decidir ingresar la palabra secreta en el marco nuevamente para obtener los mejores resultados. .

Este es el lugar donde estaremos listos para presentar el programa Aircrack-ng del que hablábamos anteriormente. Cuando se le solicite, debe presionar Y, luego esperar hasta que el programa tenga la oportunidad de completar el proceso de instalación en general. Una vez que se realiza este establecimiento, ha llegado el momento de encender el aire acondicionado. escriba el orden para hacer esto y luego presione enter para continuar.

En ese momento, es la mejor oportunidad para que revisemos y descubramos el nombre de la pantalla que queremos usar. Encontrará esto en algún lugar del segmento de interfaz. Suponiendo que está intentando hacer este ataque a su propia organización, se llamará wlan0. suponiendo que

No vea el nombre de la pantalla de ninguna manera, sepa que su tarjeta particular para Wi-Fi no admitirá este tipo de observación por ningún tramo de la imaginación.

Actualmente es la oportunidad ideal para transitar e iniciar el camino hacia la observación de nuestra organización. Puede hacer esto con el pedido adjunto debajo y, en ese momento, presione Entrar cuando haya terminado.

Airmon-ng inicia wlan0.

Asegúrese de presionar el nombre correcto de la organización que desea examinar. Si está haciendo el suyo propio, incluiría el archivo wlan0. En cualquier caso, suponiendo que está intentando controlar el control remoto de otra PC, debe implementar ciertas mejoras para lidiar con esto y asegurarse de que realmente está tratando con la organización única que desea.

En ese punto, necesitamos revisar y habilitar una interfaz de modo de pantalla con esto. Cuando lo encontremos, podemos ingresar el pedido adjunto para ayudarnos a configurarlo:

Iwconfig

Actualmente, pueden aparecer varios ciclos diferentes, y es posible que algunos de ellos nos devuelvan errores. Suponiendo que esto ocurra, necesitaremos asesinar cualquiera de los ciclos que nos devuelvan errores. Esto sucederá regularmente cuando la tarjeta Wi-Fi tenga problemas con una parte de los servicios en ejecución en su PC. Puede sacrificar estos ciclos cuando los complete y utilice el orden a continuación:

Airmon-ng comprobar matar

Mientras estamos aquí, necesitamos auditar el nombre de la interfaz de pantalla. La mayor parte del tiempo, el nombre será bastante básico, como mon0 o wlan0mon. También debemos asegurarnos de decirle a la PC que ha llegado el momento de escuchar algunos de los interruptores cercanos. Para obtener un resumen de los interruptores que terminan estando en un alcance similar al suyo, puede ingresar el orden a continuación:

Airodump-ng mon0

Haz que sustituyas el mon0 con la parte correcta. Necesitamos que se complete como el nombre de la interfaz de pantalla que utilizamos en el avance anterior, o esto no funcionará de la manera que desearíamos.

Como está mirando cerca, debemos asegurarnos de que estamos mirando aquí. Deberíamos tener la opción de descubrir el interruptor que más nos gustaría hackear. Hacia el final de cada línea de texto que viene en su dirección, verá un nombre. Debe echar un vistazo a esto para localizar el que tiene un lugar con la organización que más le gustaría piratear todo el tiempo.

Durante esta interacción, debemos asegurarnos de que estamos trabajando con el interruptor correcto y de que estamos eligiendo uno que acompañe a la seguridad WPA o WPA2 que se le agrega. Si ve uno de estos a la izquierda del nombre de la organización, en ese punto, ha llegado el momento de continuar.
Algo más, esta no será una organización que puedas piratear en el camino.

Este es el lugar donde estaremos listos para tomar nota de la dirección MAC y el número de canal del conmutador con el que necesitamos trabajar. Estos serán los fragmentos de datos que deberíamos ver a la izquierda del nombre de la organización. La dirección MAC será la línea de números que encontraremos en el extremo izquierdo de la mitad de la línea del interruptor. Por otra parte, el canal será alguno o similar que se encuentra a un lado de la etiqueta que tienes para el WPA o WPA2.

En esta parte, estaremos listos para filtrar la red elegida hasta que veamos un apretón de manos. Esto sucederá cuando una cosa interactúe con una organización, o cuando la PC pueda asociarse con un interruptor. Ingrese el código a continuación para asegurarse de que estamos reemplazando los segmentos que son vitales para el pedido con los datos de la organización: *Airodum-ng -c channel – bssid MAC -w / root/ Desktop/ mon0*

En este, habrá un par de cosas que ocurrirán. En primer lugar, podemos suplantar el canal con el número de canal que teníamos la opción de descubrir en el otro avance.

En ese momento, necesitamos reemplazar MAC con la dirección MAC que planeamos usar o espiar aquí.

Recuerde que también debemos revisar y reemplazar el mon0 con el nombre de la interfaz con la que necesita trabajar.

Una vez que todo está configurado, simplemente observamos durante un buen rato para ver si aparece el apretón de manos. Cuando ves una línea que tiene la etiqueta de protocolo de enlace WPA, además, le sigue una dirección MAC que aparece en el punto más alto de tu pantalla a la derecha, en ese punto ha llegado el momento de continuar. También es posible que avancemos en esto y no nos quedemos todo el tiempo, es factible para nosotros restringir un apretón de manos usando el ataque mortal antes de continuar con esta parte.

En el momento en que llegue el momento de pasar y obtener ese apretón de manos, en ese momento querrá ingresar a la organización y ver qué está sucediendo, siempre que la otra persona no tenga la seguridad legítima en su organización. alrededor de entonces. Luego puede recorrer una parte de las convenciones de seguridad que están allí, y esto le permite mirar alrededor, leer y cambiar una parte de los paquetes que aparecen, por lo tanto, mucho más. Necesita trabajar con un par de aparatos para que esto funcione, sin embargo, puede ser una estrategia efectiva para completar el truco que desea lograr.

capitulo 19

Seguro y Anónimo Usando Tor, Cadenas de proxy y VPN

Habrá algunas circunstancias en las que es posible que desee ponerse de acuerdo y hacer una parte del trabajo que necesita, sin que otros tengan la opción de seguir a dónde se dirige. Ser seguro y desconocido en línea es algo en lo que muchas personas se enfocan en su trabajo y, en algunos casos, es difícil asegurarse de que puede llegar a este punto y mantener ese misterio.
Es por eso que invertiremos algo de energía en echar un vistazo a las diversas técnicas que podemos usar para protegernos encubiertos y cuando estamos en la web.

que es tor

Pinnacle será una convención para la organización web que se ha planificado para anonimizar la información que se transfiere a través de ella. El uso de este producto hará que sea, en cualquier caso, difícil, si es posible, que los espías entren en la organización y vean el historial de búsqueda de sus publicaciones en los medios basados en la web, el correo web y cualquier otro movimiento en línea que intente hacer. También encontrarán que es difícil saber de qué país eres, simplemente investigando tu dirección IP. Esto puede ser útil para muchas personas que necesitan estar en la web.

En el momento en que ejecuta esta ayuda, una parte de las autoridades de información más importantes, como Google Ads y otras opciones, no pasarán ni realizarán una parte del análisis de tráfico que necesitan, y no pasarán y reunir alguna información sobre las propensiones que está haciendo en la web. Esto también hace que sea más difícil para los programadores sospechar de esos datos también.

La red Tor es intrigante porque pasará por los trabajadores de miles de voluntarios que se encuentran en todo el mundo. La información que utilice se empaquetará en paquetes que se codificarán cuando ingresen a esta organización. En ese momento, a diferencia de lo que vemos con nuestras asociaciones web convencionales, Tor podrá eliminar una parte del encabezado del paquete, que será esencial para el acceso a los datos que se pueden utilizar para ayudarnos con aprender cosas sobre el remitente, por ejemplo, el marco de trabajo desde donde se envió inicialmente este mensaje.

Por fin, Tor estará listo para codificar el resto de los datos que usamos para llamar a la cubierta del paquete. Esto es algo que las asociaciones habituales que usamos con la web no utilizarán. En ese punto, nuestros paquetes de información, que están codificados y modificados, serán dirigidos a través de un gran número de estos trabajadores voluntarios, conocidos como transferencias, mientras avanza hacia el objetivo final. La forma indirecta en que estos paquetes irán en esta organización hará que sea más difícil de seguir.

Cada uno de los elementos de transferencia descifrará apenas lo suficiente de esa capa para saber de qué transferencia proviene la información y qué transferencia necesita para enviar ese paquete a la red. La transferencia está lista para volver a envolverla en otra cubierta antes de enviarla una vez más.

Si bien esta estrategia no es 100% precisa constantemente, tendrá la opción de

mantenga sus datos significativamente más seguros de lo que veremos con las asociaciones estándar con la web. La forma en que codificamos la información que usamos, y que podemos trabajar con ella de una manera que depende de las transferencias en lugar de enviarla solo en cada lugar, puede hacer que trabajar con ella sea significativamente más simple y seguro.

Uso de cadenas de proxy

Otra alternativa con la que podemos trabajar aquí para garantizar que nuestros datos permanezcan libres de cualquier daño en el camino es trabajar con estas cadenas intermediarias. Estos harán mucho más difícil que el programador nos descubra y lo que estamos haciendo. Utilizará una máquina intermediaria cuya dirección IP será la que quede en el otro marco, en lugar de la nuestra. Además, el marco Proxy está configurado para que todo esto funcione.

El ancla intermedia se utilizará para ayudarnos a tolerar nuestro propio tráfico y, luego, lo llevaremos al objetivo que debería conseguirlo. El intermediario invertirá energía registrando todo el tráfico que queramos enviar de una u otra manera, pero afortunadamente si alguien quisiera revisar este registro, tendría que obtener una orden judicial o una citación. para hacerlo, y esto hace que sea más difícil para nosotros entrar en la otra organización sin que nadie nos descubra.

Si podemos tomar una parte de nuestras habilidades de codificación y unir más de uno de estos intermediarios en una cadena, será mucho más difícil para la otra PC reconocer la primera dirección IP con la que queremos trabajar. . Por otra parte, si se descubre que uno de los intermediarios está fuera del ámbito de la persona en cuestión, en ese momento, será realmente imposible que cualquier tráfico realmente regrese a nuestra propia dirección IP.

Afortunadamente, en caso de que desee permanecer encubierto con la ayuda de intermediarios, tanto BackTrack como Kali con Linux tendrán algunas herramientas excelentes que lo ayudarán a realizar esta interacción, y esto se conoce como una cadena intermedia. Depende de usted decidir si esta es la opción correcta para mantenerse discreto y encubierto.

VPN

Otro instrumento con el que podemos trabajar cuando llega el momento de proteger nuestra organización es la VPN. Esto representará una red privada virtual,

y te permitirá un acercamiento para realizar una asociación segura con otra organización a través de la web. Estas pueden ser una alternativa increíble para usar en momentos en los que querríamos llegar a sitios que están limitados según su ubicación, para ayudarlo a leer la acción de otros que lo ven, y más.

Estas VPN son realmente famosas, pero no se utilizarán en general por la primera razón para lo que fueron diseñadas. Inicialmente se crearon para ayudar a conectar una red de negocios o permitirle una forma de acceder a una red de negocios cuando estamos en casa.

Para que esto sea lo más sencillo posible, la VPN podrá asociar su PC, tableta o teléfono móvil a otra PC u otro trabajador en algún lugar de la web, y podrá navegar en la web con esa conexión con elementos de seguridad. Por lo tanto, si ve que este trabajador se encuentra en otro país, parecerá que realmente está por allí y nos permite recuperar datos y servicios a los que normalmente no podríamos acceder en ningún tramo del mundo. imaginación.

Hay un montón de formas increíbles en las que podemos beneficiarnos con respecto a la eliminación de la VPN. Estos incluirán:

1. Nos ayudará a eludir una parte de las limitaciones en el lugar con respecto a los sitios o una parte del video y el sonido en tiempo real a la que querríamos acercarnos más.
2. Puede facilitar la transmisión de una parte del contenido que queremos en Hulu y Netflix.
3. Hará que sea más fácil protegerse de disminuciones como escabullirse o problemas con los puntos focales de Wi-Fi, por lo que es más diligente para un programador obtener el acceso que necesita.
4. Nos ayudará a adquirir, al menos, un poco de anonimato cuando estamos en la web y realmente podemos ocultar nuestra área real de los demás.
5. Hace que sea más fácil protegerse de iniciar sesión cuando está descargando torrents.

Es normal que las personas trabajen con VPN y otros servicios cuando quieran eludir algunas de las limitaciones geográficas para ver los programas y películas que deseen en varios países o incluso para

ayudar con torrents. Sin embargo, esto puede ser particularmente valioso cuando es posible que desee piratear, ya que hace que sea más difícil para otros encontrarlo y determinar de dónde provienen la totalidad de los ataques en cualquier caso.

capitulo 20

Suplantación de IP

El siguiente tema en el que debemos invertir un poco de energía aquí es la posibilidad de satirizar IP. Esta será una interacción en la que podemos hacer paquetes para el Protocolo de Internet que tendrán direcciones de origen ajustadas en ellos, ya sea para ayudarnos a encubrir el carácter de la persona que envía los datos, para ayudarnos a imitar otra disposición de PC y en algunos casos para ambos. Esta suele ser la estrategia que utilizará un programador cuando quiera ejecutar un ataque DDoS contra su dispositivo objetivo o el sistema que lo rodea.

Enviar y aceptar estos paquetes será una de las estrategias fundamentales que impartirán estas PC y dispositivos organizados, y será en cierto modo la premisa de cómo funcionará la web avanzada. Estos paquetes de IP acompañarán un encabezado, que luego será seguido por el cuerpo del paquete y contendrá una parte de los datos importantes sobre la dirección, como la dirección de origen. En un paquete típico, uno con el que el programador no ha jugado, la dirección IP de origen solo será la ubicación de quién envió el paquete. Sin embargo, si el programador ha tenido la opción de parodiar el paquete, la ubicación se creará después de todo.

La ridiculización de la propiedad intelectual se parecerá mucho a un agresor que lleva un paquete a

alguien con alguna ubicación inaceptable para regresar perforado. En caso de que la persona que recibió el paquete quiera evitar que el remitente transmita este paquete, bloquear todos los paquetes que provienen de esa dirección no servirá de mucho porque la dirección de devolución también se puede cambiar.

Junto con una idea similar aquí, si el destinatario quisiera tener la opción de reaccionar a la dirección de retorno que ve en el paquete, su paquete de reacción no se dirigirá directamente al remitente genuino. En igualdad de condiciones, irá a cualquier dirección IP que el programador tomó para utilizar.
La capacidad de parodiar las ubicaciones de los paquetes será quizás la mayor debilidad que veremos con estos ataques DDoS.

Por ejemplo, el ataque DDoS dependerá de la caricatura para dominar un objetivo con tráfico mientras cubre el carácter de la fuente que lo acompaña. Esto hará que sea más difícil trabajar con cualquier esfuerzo de alivio si la dirección IP de la fuente es falsa y se aleatoriza en una premisa persistente, será mucho más difícil ocultar las solicitudes que son malévolas. La caricatura de IP, por lo tanto, hará que sea realmente difícil para los grupos de seguridad de la red y la autorización legal encontrar quién está causando el asalto.

Del mismo modo, descubriremos que la burla también se utilizará para ayudarnos a adoptar la apariencia de otro dispositivo cuando queramos. Entonces, las reacciones que acompañan a esto se enviarán al dispositivo en el que nos estamos enfocando en lugar de a nosotros. Algunos ataques, incluidos los ataques volumétricos como la intensificación de DNS, dependerán de este tipo de debilidad. La capacidad que tenemos para cambiar la IP de origen será una pieza importante del plan que veremos con la convención TCP/IP, lo que implica que debemos estar estresados continuamente sobre lo que está pasando aquí.

Aparte de los ataques DDoS que discutimos anteriormente, la burla se terminará con todo el punto de esconderse y afirmar ser otro dispositivo. Esto le permitirá al programador entrar y evadir la confirmación y acceder o capturar la reunión de otro cliente. El programador entonces está listo para seguir el camino para hacer lo que quiera con esta organización, lo que le permitirá causar algún daño y atacar a la organización, sin que nadie tenga la opción de anexarlo.

capitulo 21

Pruebas de penetración con Metasploit

Lo último que investigaremos es cómo lidiar con una prueba de infiltración y cómo podemos utilizar el marco Metasploit para ayudarnos a completar esto. La prueba de acceso, o una prueba de penetración, será un ciclo que incluye atacar una parte de los marcos de datos de la misma manera que un agresor lo haría con su marco. Esto nos ayuda a descubrir una parte de las debilidades en el marco y cerrarlas antes de que el programador pueda llegar a ellas.

La marca distintiva que encontraremos con las pruebas de penetración es que no se dañará el marco, y el propietario de ese marco dará el consentimiento vital antes de comenzar. La debilidad que veremos se caracterizará por una deficiencia en la seguridad que existirá en una parte de nuestro marco que le dará una sección destacada al programador para que la use para comenzar su ataque. Hay varios puntos donde aparecerán estas debilidades, como errores en el plan, errores, y eso es solo la punta del iceberg.

Probablemente, la sección más conocida se centra en estos ataques y los lugares donde debemos mirar antes de que un programador pueda llegar a ellos incluye los programas, la infusión de SQL, Blaze, ActiveX y el diseño social.

Debido a las diversas situaciones que pueden causar un asalto, se requerirán distintos tipos de pruebas de infiltración. Los tres tipos de pruebas que podemos examinar pueden incorporar pruebas de caja blanca, caja negra y caja oscura. En el momento en que comenzamos con una parte de la prueba de descubrimiento, en ese momento, ninguno de los datos sobre ese marco se devolverá a la persona que está realizando la prueba. Será obligación de nuestro analizador recopilar los datos correctos sobre el marco que deben asaltar.

En ese momento, podemos continuar con la prueba de caja blanca. Esto ayuda, ya que proporcionará datos completos sobre el marco objetivo todo el tiempo. Esto será valioso porque nos ayuda a ver una parte de los efectos que pueden ocurrir con un ataque interno a la organización.

Y luego, por fin, tenemos el asalto a la caja tenue. Este será el lugar donde el analizador obtendrá una parte de los datos sobre este marco, pero no

hasta el último trozo de ella. Estas pruebas serán las más valiosas para ayudarnos a comprender mejor lo que puede ocurrir y el efecto principal de uno de estos ataques externos.

En este sentido, necesitamos trabajar en las cuatro fases que sucederán cuando trabajemos con las pruebas de entrada y la interacción de Metasploit. El primer paso en el que nos concentraremos es organizar la prueba que debemos utilizar. El objetivo de esto es ayudarnos a reconocer el grado y sorprendentemente el sistema que necesitamos usar para hacer esta prueba. El alcance de esta prueba será educado por las estrategias y normas actualmente ensayadas.

La segunda etapa con la que podremos trabajar se conocerá como revelación. Habrá tres cosas que podemos hacer aquí. El primero es reunir una parte de los datos del marco y una parte de la información que contiene.
Esto se conocerá como toma de huellas dactilares. En ese punto, llegamos a la siguiente acción y que se conoce como verificar y examinar sorprendentemente los puertos del sistema. Por último, la tercera acción nos ayudará a reconocer las debilidades que tendrá el marco.

La tercera fase de esta prueba será sobre el asalto. Esta etapa estará lista para ayudarnos a reconocer las aventuras por las debilidades. Un esfuerzo será un programa de PC que tiene el objetivo de usar la debilidad para obtener la admisión fundamental a ese marco en términos generales. Una vez que el programador pueda obtener este acceso, la carga útil será el producto que lo ayudará a supervisar ese sistema socavado. La aventura se realizará para ayudar a transportar la carga útil con la que estamos trabajando aquí.

Y después, terminamos con la cuarta etapa. Con frecuencia, este puede descuidarse, pero suponiendo que esté haciendo este ciclo para otra persona, deberá concentrarse en él para cuidarlo. Esta etapa se conocerá como anunciar. El objetivo que veremos con esta etapa es que nos ayude a hacer un informe detallado de una parte de las debilidades reconocidas del marco, el efecto que tienen en nuestro negocio y una parte de los arreglos fundamentales.

Aunque habrá una gran cantidad de varios dispositivos que pueden ayudar con este ciclo, Metasploit será uno de los dispositivos más utilizados. Es por eso que invertiremos algo de energía en ver cómo hacer este tipo de interacción, cómo trabajar con pruebas de infiltración y cómo se puede terminar con Metasploit.

Para empezar, debemos entender que Metasploit será un sistema que ha sido coordinado en módulos. El tipo principal será hacer el esfuerzo.
Estos tipos de módulos están planificados de manera que puedan explotar cualquier deficiencia que se encuentre en un marco. Estas serán cosas como la infusión de código, los esfuerzos de aplicación y la inundación de la cuna.

En ese momento, habrá una parte de los módulos auxiliares. Estos serán los que desarrollarán ciertas actividades, pero estas actividades no están configuradas para explotar una parte de las deficiencias del marco. Por ejemplo, pueden ser cosas como ayuda para jurar y filtrar.

El tercer tipo de módulo que se descubre en este marco son los módulos posteriores al abuso. Estos también son significativos porque su centro principal nos ayudará con datos de eventos sociales en una parte de los marcos objetivos.

Por último, descubriremos los módulos de carga útil. Estos serán los módulos que podrán subsanar una carencia de la que se ha abusado de manera efectiva. La carga útil nos ayudará a controlar el marco del que pudimos abusar en el camino. Con esta carga útil, es más sencillo abrir el meterpreter para ayudar a trabajar con los registros DLL.

Así que ahora, debemos hacer una pausa por un minuto para descargar este marco y prepararlo para la acción. Lo revisaremos y lo haremos con la instalación de Windows aquí, pero puede revisar y hacer cambios y hacer una parte del trabajo que desee para prevenir otros problemas en el camino también, y funcionará de esta manera en diferentes marcos . Solo tienes que ir al sitio de Metasploit y luego hacer clic en que quieres hacer la instalación de Windows.

Desde aquí, deberá descargar el instalador y, luego, aparecerán algunas indicaciones que lo ayudarán a completar esta instalación. Para ayudar a afirmar que el establecimiento fue un éxito, debe comenzar la orden brevemente, asegurándose de que usted es el jefe, y luego use la orden de "commanmsfvenom.bat - help". Si obtiene un rendimiento, entonces esto le mostrará que funcionó, y debería enumerar la totalidad de las diversas opciones que están disponibles para que las use desde esta sección.

Hay un par de opciones con las que podemos trabajar aquí. Por ejemplo, en caso de que queramos tener la opción de desglosar el

la totalidad de los payloads que son accesibles, tendríamos la opción de trabajar con el orden de "msfvenom.bat - list payloads". Este puede ser un resumen considerable, pero en realidad nos muestra lo que está disponible aquí.

Si desea continuar y activar la seguridad que está disponible con Metasploit, debe utilizar el orden de msfconsole.bat. Luego puede acceder al soporte de MSF, que será el dispositivo que podemos usar para la línea de pedido que funcionará con este programa.

Lo siguiente en el resumen en el que podemos concentrarnos es que debemos enumerar la totalidad de los esfuerzos a los que tenemos acceso con la ayuda de la búsqueda de ayuda del pedido. Si necesitamos revisar y buscar una aventura en particular, debe utilizar el número, la etapa o el nombre de CVE.

Supongamos que necesitamos tener la opción de enumerar la totalidad de las aventuras que ocurrieron en la época de 2018. Para hacer esto, tendríamos que dibujar el orden de "buscar cve: 2018" y esto debería profundizar en la totalidad de las piezas que necesitamos.

Para recorrer este ciclo y luego recopilar parte de la información sobre el esfuerzo realizado, debemos pasar la url de ese esfuerzo y asegurarnos de que esté en el orden de la información. El código con el que podemos trabajar para que esto funcione incorpora:

Explotar/ multi/ navegador/ java_jre17_exec.

Una vez que podemos echar un vistazo al resumen y luego podemos rastrear una aventura intrigante que queremos usar, ha llegado el momento de usar el orden que usamos anteriormente. Después de emitir la orden que necesitamos para trabajar con esa aventura en particular, es posible que establezcamos una parte de las alternativas que necesitamos usar con la orden establecida. Esto podría ser algo así como configurar el puerto de vecindario y el host cercano. Las órdenes que podemos utilizar para que éste suceda incorporarán las siguientes:

establecer SRVHOST 0.0.0.0

establecer SRVHOST 8080

En caso de que desee tener la opción de revisar y verificar los factores que estamos listos para establecer, tendríamos que trabajar con el pedido, mostrar opciones para completarlo. En el momento en que la aventura que nos

está trabajando tiene más de un objetivo, podemos establecer un objetivo particular determinando una ID para el orden objetivo establecido. Una parte de los enfoques accesibles con los que necesitaremos trabajar se registrará con la ayuda del orden de los objetivos de visualización.

Trabajar con el programa Metasploit hará que sea significativamente más sencillo para nosotros realizar y completar una de nuestras propias pruebas de infiltración. Esto hará que sea más fácil para nosotros avanzar y ganar competencia con un toque más sobre nuestro marco, y determinar dónde aparecerán las debilidades más reconocidas y cómo podemos cerrarlas y mantener alejados a los programadores.

Conclusión

Gracias por llegar hasta el final de Hacking con Kali Linux, esperemos que haya sido informativo y pueda brindarle todas las herramientas que necesita para lograr sus objetivos, sean cuales sean.

El siguiente paso es llegar a estar donde podamos pasar un poco de tiempo aprendiendo más sobre el mundo de la piratería y cómo podemos utilizarlo para algunas de nuestras propias necesidades. Ya sea que esté buscando proteger su propia red y asegurarse de que un pirata informático no pueda ingresar al sistema, o si está más interesado en

pirateando otra red y tomando la información (que, como comentamos, es ilegal), puede utilizar muchas de las técnicas y otros métodos que se encuentran en esta guía.

Hay muchas partes diferentes que se unen cuando intentamos trabajar con piratería, y Kali Linux será un gran recurso para ayudarnos a superar algunas de estas piraterías y garantizará que podamos hacer todo esto. Pasamos un tiempo analizando cómo configurar el sistema Kali Linux para que esté listo para funcionar y ayudarnos con todo el pirateo que queremos hacer en el camino.

Además de poder trabajar con el sistema Kali Linux para realizar parte de nuestra piratería, también debemos dedicar un tiempo a observar algunas de las otras técnicas de piratería que podemos usar. Vamos a pasar algún tiempo viendo cómo hacer una prueba de penetración, algunos de los ataques de intermediarios, ataques de denegación de servicio, cómo acceder a algunas de las redes inalámbricas y la importancia de una prueba de penetración.

Luego nos tomamos un tiempo para ver las diferentes partes que pueden ayudarnos a mantener seguras nuestras redes. Por ejemplo, con la ayuda de un buen firewall y el uso de pruebas de penetración, e incluso VPN y otras opciones como esta para mantener su anonimato cuando está en línea, podrá hacer que sea un poco más difícil para el hacker encontrarlo. , y esto hace que sea mucho más fácil para usted mantener toda esa información lo más segura posible.

Muchas partes vienen al mundo de la piratería, y debemos aprender algunos de los métodos y técnicas que vienen con esto para mantener las cosas organizadas y mantener alejados a los piratas informáticos. Cuando esté listo para aprender un poco más sobre la piratería y cómo puede funcionar para algunas de nuestras necesidades, asegúrese de consultar esta guía para ayudarlo a comenzar.