SEGURIDAD DE LA INFORMACIÓN

Edgar Vega Briceño

TIC's

3ciencias

SEGURIDAD DE LA INFORMACIÓN

Edgar Vega Briceño

Editorial Área de Innovación y Desarrollo,S.L.

ÁREA DE INNOVACIÓN Y DESARROLLO, S.L.

C/Alzamora, 17 - 03802 - ALCOY (ALICANTE) info@3ciencias.com

Primera edición: **marzo 2021**

ISBN: **978-84-122093-6-5**

DOI: https://doi.org/10.17993/tics.2021.4

ACERCA DEL AUTOR

El académico Edgar Vega Briceño es Ingeniero en Informática con un posgrado en Administración de la Tecnología de Información y Comunicación por la Universidad Nacional (UNA) de Costa Rica. Es certificado Ethical Hacker por ECCouncil y es certificado instructor de la Academia de Cisco en Seguridad de Redes. Ha fortalecido su formación en países como Estados Unidos, India, España y Uruguay. Cuenta con más de 13 años de experiencia como académico en distintas universidades públicas y privadas de Costa Rica. Ha sido consultor en empresa privadas. Actualmente, es académico en la Universidad Nacional (UNA) a tiempo completo y sus intereses de investigación se inclinan a la ciberseguridad en sociedades hiperconectadas y la transformación digital para el desarrollo sostenible.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

CAPÍTULO I: ¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?

La seguridad de la información es un concepto que se involucra cada vez más en muchos aspectos de nuestra sociedad hiperconectada, en gran parte como resultado de nuestra adopción casi ubicua de la tecnología de información y comunicación. En nuestra vida cotidiana, muchos de nosotros trabajamos con computadoras para nuestros empleadores, jugamos con computadoras en casa, vamos a la escuela en línea, compramos productos de los comerciantes en Internet, llevamos nuestras computadoras portátiles a la cafetería o al centro comercial y revisamos nuestro correo electrónico en distintos lugares, llevamos nuestro teléfonos inteligentes a todos lados y los usamos para verificar nuestros saldos bancarios, monitorear el ejercicio físico con sensores en nuestro cuerpo y así sucesivamente con muchos aspectos de nuestra vida cotidiana.

Aunque la tecnología nos permite ser más productivos y nos permite acceder a una gran cantidad de información con solo un clic del ratón, también conlleva una gran cantidad de problemas de seguridad. Si la información sobre los sistemas utilizados por nuestros empleadores o nuestros bancos se expone a un ciberdelincuente, las consecuencias pueden ser terribles. Podríamos encontrarnos repentinamente desprovistos de fondos, ya que el contenido de nuestra cuenta bancaria se transfiere a un banco en otro país en medio de la noche sin nosotros darnos cuenta. Nuestro empleador podría perder millones de dólares, enfrentar enjuiciamiento legal y sufrir daños a su reputación debido a un problema de configuración del sistema que permite a un atacante obtener acceso a una base de datos que contiene información de la identificación personal o información de propiedad exclusiva. Basta con ver noticias sobre estafas informáticas en canales locales o internacionales, hoy día más frecuentemente que hace cinco, diez o veinte años.

Según la ISO/IEC (2016), la seguridad de la información se podría definir como aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada. Esta definición básicamente significa que debemos proteger nuestros datos y nuestros recursos de infraestructura tecnológica de aquellos quiénes intentarían hacer un mal uso de ellos.

Por otro lado, en un sentido general, seguridad significa proteger nuestros activos. Esto puede significar protegerlos de atacantes que invaden nuestras redes, desastres naturales, condiciones ambientales adversas, cortes de energía, robo o vandalismo u

otros estados indeseables. En última instancia, intentaremos protegernos contra las formas más probables de ataque, en la mejor medida que podamos, dado nuestro contexto.

Cuando miramos qué es exactamente lo que aseguramos, es posible que tengamos una amplia gama de activos potenciales. Podemos considerar elementos físicos que podríamos querer proteger, como aquellos de valor inherente (por ejemplo, reservas de oro de un Banco) o aquellos que tienen valor para nuestro negocio (por ejemplo, computadoras). También podemos tener elementos de naturaleza más etérea, como software, código fuente o datos. En el entorno informático actual, es probable que descubramos que nuestros activos lógicos son al menos tan valiosos, si no más, que nuestros activos físicos. Además, también debemos proteger a las personas que participan en las operaciones de la organización o empresa. Las personas son nuestro activo más valioso, ya que, en general, no podemos hacer negocios sin ellas. Duplicamos nuestros activos físicos y lógicos y guardamos copias de seguridad de ellos en otro lugar para evitar que ocurra una catástrofe, o al menos es lo que se debe realizar.

En nuestros esfuerzos por proteger nuestros activos, también debemos considerar las consecuencias de la seguridad que elegimos implementar. Hay una cita muy conocida que dice: "El único sistema verdaderamente seguro es uno que está apagado, escondido en un bloque de hormigón y sellado en una habitación revestida de plomo con guardias armados", y aun así tengo mis dudas. De hecho, me gusta usar esa frase cuando realizo alguna charla de Seguridad Informática. Aunque ciertamente podríamos decir que un sistema en tal estado podría considerarse razonablemente seguro, seguramente no es utilizable ni productivo. A medida que aumentamos el nivel de seguridad, generalmente disminuimos el nivel de productividad, pero hay que buscar un equilibrio.

Además, al proteger un activo, sistema o entorno, también debemos considerar cómo el nivel de seguridad se relaciona con el valor del artículo que se está asegurando. Podemos, si estamos dispuestos a adaptarnos a la disminución del rendimiento, aplicar niveles muy altos de seguridad a todos los activos de los que somos responsables. Podemos construir una instalación de mil millones de dólares rodeada de cercas de alambre de púas y patrullada por guardias armados y perros de ataque feroces, y que con cuidado coloque nuestro activo en una bóveda herméticamente sellada en el interior, pero eso no tendría mucho sentido. En algunos entornos, sin embargo, estas medidas de seguridad pueden no ser suficientes. En cualquier entorno en el que planeemos establecer niveles elevados de seguridad, también debemos tener

en cuenta el costo de reemplazar nuestros activos si los perdemos, y asegurarnos de establecer niveles razonables de protección para su valor. El costo de la seguridad que implementamos nunca debe superar el valor de lo que protege (Jeong, Lee, y Lim, 2019).

1.1. ¿Cuándo nuestro entorno es seguro?

Definir el punto exacto en el que podemos ser considerados seguros presenta un desafío ¿Estamos seguros si nuestros sistemas están debidamente actualizados? ¿Estamos seguros si usamos contraseñas seguras? ¿Estamos seguros si estamos completamente desconectados de Internet? Desde cierto punto de vista, todas estas preguntas pueden responderse con un "no".

Incluso si nuestros sistemas están debidamente actualizados, siempre habrá nuevos ataques a los que seremos vulnerables. Cuando se utilizan contraseñas seguras, habrá otras vías que un ciberdelincuente puede aprovechar. Cuando estamos desconectados de Internet, se puede acceder físicamente a nuestros sistemas o ser robados si no implementamos seguridad física. En resumen, es muy difícil definir cuándo estamos realmente seguros. Sin embargo, podemos reflexionar sobre la pregunta.

Definir cuándo tenemos un ambiente inseguro es una tarea mucho más sencilla y podemos enumerar rápidamente una serie de elementos que nos pondrían en este estado:

- No actualizar sistemas operativos y aplicaciones.
- Usar contraseñas débiles como "contraseña" o "1234".
- Descarga de programas de Internet de fuentes no seguras.
- Abrir archivos adjuntos de correo electrónico de remitentes desconocidos.
- Usar y desplegar redes inalámbricas sin cifrado.

Podríamos seguir durante algún tiempo haciendo crecer esa lista, pero lo bueno es que una vez que seamos capaces de señalar los aspectos que pueden causar que sea el entorno sea inseguro, podemos tomar medidas para mitigar estos problemas. Este problema es similar a cortar algo por la mitad una y otra vez; siempre quedará una pequeña porción para volver a cortar, aunque es posible que nunca lleguemos a un estado que definitivamente podamos llamar "seguro", pero podemos dar pasos en

la dirección correcta.

Algunas regulaciones internacionales intentan definir qué es seguro, o al menos una serie de reglas que deberíamos tomar para ser "lo suficientemente seguros". Tenemos el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS, por sus siglas en Inglés) para las empresas que procesan pagos con tarjeta de crédito, la Ley de Responsabilidad y Portabilidad del Seguro de Salud de 1996 (HIPAA, por sus siglas en Inglés) para organizaciones que manejan la atención médica y los registros de pacientes, la Administración Federal de Seguridad de la Información Ley (FISMA, por sus siglas en Inglés) que define los estándares de seguridad para las agencias federales en los Estados Unidos. Si estos estándares son efectivos o no, es motivo de mucha discusión, pero seguir los estándares de seguridad definidos para la industria en la que operamos generalmente se considera aconsejable, por no decir obligatorio.

1.2. La triada de confidencialidad, integridad y disponibilidad

Tres de los conceptos principales en seguridad de la información son precisamente la confidencialidad, integridad y disponibilidad, comúnmente conocida como la tríada de la seguridad de la información. La tríada de la CIA, que ha sido utilizada por más de 20 años, brinda un modelo mediante el cual podemos pensar y discutir conceptos de seguridad, y tiende a centrarse mucho en la seguridad de los datos. (Parada *et al.*, 2018).

La confidencialidad es un concepto similar, pero no igual, a la privacidad. La confidencialidad es un componente necesario de la privacidad y se refiere a nuestra capacidad de proteger nuestros datos de aquellos que no están autorizados para verlos. La confidencialidad es un concepto que puede implementarse en muchos niveles de un proceso.

Un ejemplo clásico, si consideramos el caso de una persona que retira dinero de un cajero automático, la persona en cuestión probablemente buscará mantener la confidencialidad del número de identificación personal (PIN) que le permite, en combinación con su tarjeta de cajero automático, extraer dinero. Además, el propietario del cajero automático mantendrá la confidencialidad del número de cuenta, saldo y cualquier otra información necesaria para comunicarse con el banco del que se debitarán los fondos. El banco mantendrá la confidencialidad de la transacción con el cajero automático y la actualización del saldo en la cuenta después de que se hayan retirado los fondos. Si en algún momento de la transacción se compromete la confidencialidad, los resultados podrían ser preocupantes para

la persona, el propietario del cajero automático y el banco titular, lo que podría dar lugar a lo que se conoce como incumplimiento en el campo de la seguridad de la información.

La confidencialidad puede verse comprometida por la pérdida de una computadora portátil que contiene datos confidenciales, una persona que mira por encima del hombro mientras escribimos una contraseña, envío de archivos adjuntos de correo electrónico a la persona equivocada, un atacante que penetra en nuestros sistemas o infraestructura por medio de aplicaciones MITM (Man in The Middle) (Tchernykh *et al.*, 2019).

En cuanto a la integridad se refiere a la capacidad de evitar que nuestros datos se modifiquen de manera no autorizada o indeseable. Esto podría significar el cambio o la eliminación no autorizada de nuestros datos o partes de nuestros datos, o podría significar un cambio o eliminación autorizado, pero no deseable. Para mantener la integridad, no solo necesitamos tener los medios para evitar cambios no autorizados en nuestros datos, sino también la capacidad de revertir los cambios autorizados que deben deshacerse. Podemos ver un buen ejemplo de mecanismos que nos permiten controlar la integridad en los sistemas de archivos de muchos sistemas operativos modernos como Windows y Linux. Con el fin de prevenir cambios no autorizados, tales sistemas a menudo implementan permisos que restringen las acciones que un usuario no autorizado puede realizar en un archivo determinado. Además, algunos de estos sistemas y muchas aplicaciones, como las bases de datos, pueden permitirnos deshacer o revertir cambios que no son deseables. La integridad es particularmente importante cuando discutimos los datos que proporcionan la base para otras decisiones. Si un atacante modificara los datos que contenía los resultados de las pruebas médicas, como un caótico ejemplo, podríamos ver el tratamiento incorrecto prescrito, lo que podría resultar en la muerte del paciente (Zambrano *et al.*, 2017).

Por último, la disponibilidad se refiere a la capacidad de acceder a nuestros datos cuando los necesitamos. La pérdida de disponibilidad puede referirse a una amplia variedad de interrupciones en cualquier parte de la cadena de comunicaciones que nos permite acceder a nuestros datos. Tales problemas pueden ser el resultado de pérdida de energía, problemas del sistema operativo o de la aplicación, ataques a la red de datos, compromiso de un sistema u otros problemas que impidan a los usuarios acceder a su información. Tales problemas son comúnmente causados por los ya conocidos y avanzados ataques de denegación de servicio (DoS) (Wang *et al.*, 2017).

Una vez conocidos esos tres elementos, podemos comenzar a discutir temas de seguridad de la información de una manera muy específica. Por ejemplo, si quisiéramos trasladar discos duros de respaldo en el que tenemos la única copia existente, pero sin cifrar, de algunos de nuestros datos confidenciales almacenados en esas unidades, pero si perdiéramos el envío en el tránsito, tendremos un problema de seguridad. Desde el punto de vista de la confidencialidad, es probable que tengamos un problema ya que nuestros archivos no estaban encriptados y pueden ser fácilmente leídos. Desde el punto de vista de la integridad, suponiendo que pudimos recuperar los discos duros, nuevamente tenemos un problema debido a la falta de cifrado utilizado en nuestros archivos, es decir pudieron ser modificados, alterando su integridad, esto no sería inmediatamente evidente para nosotros pues no tendríamos control sobre las firmas de archivos. En cuanto a la disponibilidad, tenemos un problema a menos que los discos duros se recuperen debido a que no tenemos una copia de seguridad de las unidades. Es decir, estamos frente a un caso totalmente caótico de seguridad de la información que en estos días sería una completa negligencia.

En la última década, esta triada ha sido criticada por algunos especialistas que indican que estos pilares no abarcan en su totalidad los requerimientos básicos que demanda la seguridad de la información en la nueva dinámica de la presente sociedad hiperconectada. Una de esas críticas más notables es de Donn Parker, el cual propuso otros tres pilares que complementan a la triada los cuales son: control, autenticidad y utilidad para formar algo que denominó hexágono Parkeriano.

1.3. Control, autenticidad y utilidad

Control

El control se refiere a la disposición física de los medios en los que se almacenan los datos. Esto nos permite, sin involucrar otros factores como la disponibilidad, discutir nuestra pérdida de datos en su medio físico. En nuestro envío perdido de cintas de respaldo, digamos que algunas de ellas estaban encriptadas y otras no. El principio de posesión nos permitiría describir con mayor precisión el alcance del incidente; las cintas encriptadas en el lote son un problema de posesión, pero no un problema de confidencialidad, y las cintas no encriptadas son un problema en ambos sentidos. Esto es fundamental en el entorno actual, donde los datos pueden estar en varios dispositivos y puede haber numerosas versiones.

Autenticidad

La autenticidad nos permite hablar de la atribución adecuada en cuanto al propietario o creador de los datos en cuestión. Por ejemplo, si enviamos un mensaje de correo electrónico que está alterado de modo que parezca que proviene de una dirección de correo electrónico diferente a aquella desde la que realmente se envió, estaríamos violando la autenticidad del correo electrónico. La autenticidad se puede imponer mediante el uso de firmas digitales. Un concepto muy similar, pero inverso, es el de no repudio. El no repudio impide que alguien realice una acción, como enviar un correo electrónico, y luego negar que lo haya hecho. Esto es fundamental para el comercio electrónico y está definido por las leyes que rigen las transacciones. También discutiremos el no repudio con mayor detalle en el Capítulo 4.

Utilidad

La utilidad se refiere a la utilidad de los datos para nosotros. La utilidad es también el único principio del hexágono Parkeriano que no es necesariamente de naturaleza binaria; podemos tener una variedad de grados de utilidad, dependiendo de los datos y su formato. Este es un concepto algo abstracto, pero resulta útil para discutir ciertas situaciones en el mundo de la seguridad. Por ejemplo, en uno de los ejemplos anteriores, tuvimos un envío de cintas de respaldo, algunas de las cuales estaban encriptadas y otras no. Para un atacante u otra persona no autorizada, las cintas cifradas probablemente serían de muy poca utilidad, ya que los datos no serían legibles. Las cintas sin cifrar serían de mucha mayor utilidad, ya que el atacante o la persona no autorizada podría acceder a los datos.

Sin embargo, este libro se enfoca en la filosofía de los tres pilares ya ampliamente conocidos.

1.4 Ataques y tipos

Podemos enfrentar ataques desde una amplia variedad de enfoques y ángulos. Cuando observamos qué constituye exactamente un ataque, podemos desglosarlo de acuerdo con el tipo de ataque que representa, el riesgo que representa el ataque y los controles que podríamos usar para mitigarlo.

Cuando observamos los tipos de ataques que podríamos enfrentar, generalmente podemos ubicarlos en una de cuatro categorías: intercepción, interrupción, modificación y fabricación.

Interceptación

Los ataques de interceptación permiten que usuarios no autorizados accedan a nuestros datos, aplicaciones o entornos de red, y son principalmente un ataque contra la confidencialidad. La interceptación puede tomar la forma de ver o copiar archivos no autorizados, espiar conversaciones telefónicas o leer correos electrónicos, y puede realizarse contra datos en reposo o en movimiento. Correctamente ejecutados, los ataques de interceptación pueden ser muy difíciles de detectar.

Interrupción

Los ataques de interrupción hacen que nuestros activos se vuelvan inutilizables o no estén disponibles para nuestro uso, de forma temporal o permanente. Los ataques de interrupción a menudo afectan la disponibilidad, pero también pueden ser un ataque a la integridad. En el caso de un ataque de Denegación de Servicios (DoS, por sus siglas en Inglés) en un servidor de correo electrónico, clasificaríamos esto como un ataque de disponibilidad. En el caso de un atacante que manipula los procesos en los que se ejecuta una base de datos para evitar el acceso a los datos que contiene, podríamos considerar esto un ataque de integridad, debido a la posible pérdida o corrupción de datos, o podríamos considerarlo como una combinación de los dos. También podríamos considerar que dicho ataque a la base de datos es un ataque de modificación en lugar de un ataque de interrupción.

Modificación

Los ataques de modificación implican la manipulación de nuestro activo. Tales ataques podrían considerarse principalmente un ataque de integridad, pero también podrían representar un ataque de disponibilidad. Si accedemos a un archivo de manera no autorizada y modificamos los datos que contiene, habremos afectado la integridad de los datos contenidos en el archivo. Sin embargo, si consideramos el caso en el que el archivo en cuestión es un archivo de configuración que gestiona cómo se comporta un servicio en particular, tal vez uno que está actuando como un servidor web, podríamos afectar la disponibilidad de ese servicio al cambiar el contenido del expediente. Si continuamos con este concepto y decimos que la configuración que modificamos en el archivo para nuestro servidor web es una que altera la forma en que el servidor maneja las conexiones encriptadas, incluso podríamos hacer de esto un ataque de confidencialidad.

Fabricación

Los ataques de fabricación implican generar datos, procesos, comunicaciones u

otras actividades similares con un sistema. Los ataques de fabricación afectan principalmente la integridad, pero también podrían considerarse un ataque de disponibilidad. Si generamos información espuria en una base de datos, esto se consideraría un ataque de fabricación. También podríamos generar correo electrónico, que se usa comúnmente como un método para propagar malware, como podríamos encontrar que se usa para propagar un gusano. En el sentido de un ataque de disponibilidad, si generamos suficientes procesos adicionales, tráfico de red, correo electrónico, tráfico web o casi cualquier otra cosa que consuma recursos, potencialmente podemos hacer que el servicio que maneja dicho tráfico no esté disponible para usuarios legítimos del sistema.

1.5. Amenazas, vulnerabilidades y riesgos

Para poder hablar más específicamente sobre los ataques, necesitamos introducir algunos elementos nuevos en nuestra terminología. Cuando observamos la posibilidad de que un ataque en particular nos afecte, podemos hablar de él en términos de amenazas, vulnerabilidades y el riesgo asociado que podría acompañarlos o materializarse.

Amenazas

Cuando hablamos de los tipos de ataques que podríamos encontrar, en la sección de "Ataques", discutimos algunas de las cosas que tienen el potencial de causar daño a nuestros activos. En última instancia, esto es lo que es una amenaza, algo que tiene el potencial de causarnos daño. Las amenazas tienden a ser específicas de ciertos entornos, particularmente en el mundo de la seguridad de la información. Por ejemplo, aunque un virus puede ser problemático en un sistema operativo Windows, es poco probable que el mismo virus tenga algún efecto en un sistema operativo Linux.

Vulnerabilidades

Las vulnerabilidades son debilidades que pueden usarse para dañarnos. En esencia, son agujeros que pueden ser explotados por amenazas para causarnos daño. Una capacidad de vulnerabilidad podría ser un sistema operativo específico o una aplicación que estamos ejecutando, una ubicación física donde hemos elegido ubicar nuestro edificio de oficinas, un centro de datos que se puebla sobre la capacidad de su sistema de aire acondicionado, la falta de respaldo generadores u otros factores.

Riesgo

El riesgo es la probabilidad de que algo malo suceda. Para que podamos tener un riesgo en un entorno particular, necesitamos tener una amenaza y una capacidad de vulnerabilidad que la amenaza específica pueda explotar. Por ejemplo, si tenemos una estructura hecha de madera y la prendemos fuego, tenemos una amenaza (el fuego) y una vulnerabilidad que coincide (la estructura de madera). En este caso, definitivamente tenemos un riesgo.

Del mismo modo, si tenemos la misma amenaza de incendio, pero nuestra estructura está hecha de concreto, ya no tenemos un riesgo creíble, porque nuestra amenaza no tiene una vulnerabilidad que explotar. Podemos argumentar que una llama suficientemente caliente podría dañar el concreto, pero este es un evento mucho menos probable.

A menudo tendremos discusiones similares con respecto al riesgo potencial en entornos informáticos y los posibles ataques, pero poco probables, que podrían ocurrir. En tales casos, la mejor estrategia es pasar nuestro tiempo mitigando los ataques más probables. Si postramos nuestros recursos en tratar de planificar cada posible ataque, por improbable que sea, no tendremos protección donde realmente la necesitamos.

Impacto

Algunas organizaciones, como la Agencia de Seguridad Nacional de los Estados Unidos (NSA, por sus siglas en Inglés), agregan un factor adicional a la ecuación de amenaza / vulnerabilidad / riesgo, en forma de impacto. Si consideramos que el valor del activo amenazado es un factor, esto puede cambiar si vemos un riesgo presente o no. Si revisamos nuestro ejemplo de cinta de respaldo perdida y estipulamos que las cintas de respaldo no cifradas contienen solo nuestra colección de recetas de galletas con chispas de chocolate, es posible que no tengamos ningún riesgo. Los datos expuestos no nos causarían problemas, ya que no contenían nada sensible y podemos hacer copias de seguridad adicionales de los datos de origen. En este caso particular, podríamos decir con seguridad que no tenemos ningún riesgo.

1.6. Controles

Para ayudarnos a mitigar el riesgo, podemos establecer medidas que ayuden a garantizar que se tenga en cuenta un tipo determinado de amenaza. Estas medidas se denominan controles. Los controles se dividen en tres categorías: física, lógica y administrativa.

Físicos

Los controles físicos son aquellos controles que protegen el entorno físico en el que se encuentran nuestros sistemas o donde se almacenan nuestros datos. Dichos controles también controlan el acceso dentro y fuera de dichos entornos. Los controles físicos lógicamente incluyen elementos como cercas, puertas, cerraduras, bolardos, protectores y cámaras, pero también incluyen sistemas que mantienen el entorno físico, como sistemas de calefacción y aire acondicionado, sistemas de extinción de incendios y generadores de energía de respaldo.

Aunque a primera vista, los controles físicos pueden no parecer parte de la seguridad de la información, en realidad son uno de los controles más críticos con los que debemos preocuparnos. Si no somos capaces de proteger físicamente nuestros sistemas y datos, cualquier otro control que podamos implementar será irrelevante. Si un atacante puede acceder físicamente a nuestros sistemas, puede, al menos, robar o destruir el sistema, dejándolo no disponible para nuestro uso en el mejor de los casos. En el peor de los casos, tendrá acceso directo a nuestras aplicaciones y datos y podrá robar nuestra información y recursos, o subvertirlos para su propio uso.

Lógicos

Los controles lógicos, a veces llamados controles técnicos, son aquellos que protegen los sistemas, redes y entornos que procesan, transmiten y almacenan nuestros datos. Los controles lógicos pueden incluir elementos como contraseñas, encriptación, controles de acceso lógico, firewalls y sistemas de detección de intrusos.

Los controles lógicos nos permiten, en un sentido lógico, evitar que se realicen actividades no autorizadas. Si nuestros controles lógicos se implementan correctamente y tienen éxito, un atacante o un usuario no autorizado no puede acceder a nuestras aplicaciones y datos sin subvertir los controles que tenemos implementados.

Administrativos

Los controles administrativos se basan en reglas, leyes, políticas, procedimientos, pautas y otros elementos que son de naturaleza “en papel”. Los controles establecen las reglas sobre cómo esperamos que se comporten los usuarios de nuestro entorno. Según el entorno y el control en cuestión, los controles administrativos pueden representar diferentes niveles de autoridad. Es posible que tengamos una regla simple como “apagar la cafetera al final del día”, con el objetivo de garantizar que no

causamos un problema de seguridad física al quemar nuestro edificio por la noche. También podemos tener un control administrativo más estricto, como uno que requiere que cambiemos nuestra contraseña cada 60 días.

Un concepto importante cuando discutimos los controles administrativos es la capacidad de exigir su cumplimiento. Si no tenemos la autoridad o la capacidad para garantizar que se cumplan nuestros controles, son peores que inútiles, porque crean una falsa sensación de seguridad. Por ejemplo, si creamos una política que dice que nuestros recursos comerciales no pueden, de ninguna manera, ser utilizados para uso personal, debemos ser capaces de hacer cumplir esto. Fuera de un entorno altamente seguro, esta puede ser una tarea difícil. Tendremos que controlar el uso del teléfono y del teléfono móvil, el acceso a la Web, el uso del correo electrónico, las conversaciones de mensajes instantáneos, el software instalado y otras áreas potenciales de abuso. A menos que estemos dispuestos a dedicar una gran cantidad de recursos para monitorear estas y otras áreas, y lidiar con violaciones de nuestra política, rápidamente tendríamos una política que no podríamos hacer cumplir. Una vez que se comprende que no aplicamos nuestras políticas, podemos prepararnos rápidamente para una mala situación.

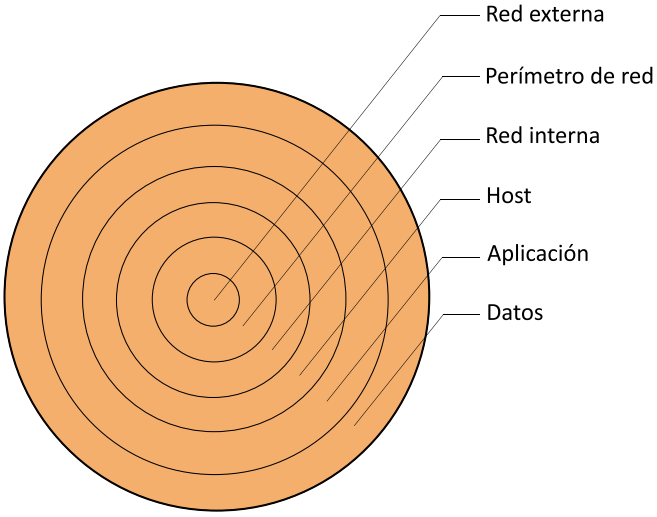
1.7. Defensa en profundidad

La defensa en profundidad es una estrategia común tanto para las maniobras militares como para la seguridad de la información. En ambos sentidos, el concepto básico de defensa en profundidad es formular una defensa multicapa que nos permita montar una defensa exitosa si una o más de nuestras medidas defensivas fallan. Esas capas que queremos establecer para defender nuestros activos desde una perspectiva lógica; al menos, se deberían pretender defensas en los niveles de red externa, perímetro de red, red interna, host, aplicación y datos. Dadas las defensas bien implementadas en cada capa, haremos que sea muy difícil penetrar con éxito profundamente en nuestra red y atacar nuestros activos directamente.

Un concepto importante para tener en cuenta al planificar una estrategia defensiva usando la defensa en profundidad es que no es una solución mágica. No importa cuántas capas coloquemos, o cuántas medidas defensivas coloquemos en cada capa, no podremos mantener a todos los atacantes fuera por un período de tiempo indefinido, ni este es el objetivo final de la defensa en profundidad en una configuración de seguridad de la información. El objetivo es colocar suficientes medidas defensivas entre nuestros activos verdaderamente importantes y el atacante para que ambos notemos que hay un ataque en curso y también nos demos el tiempo suficiente para

tomar medidas más activas para evitar que el ataque tenga éxito.

Figura 1. Defensa en Profundidad.



Fuente: elaboración propia.

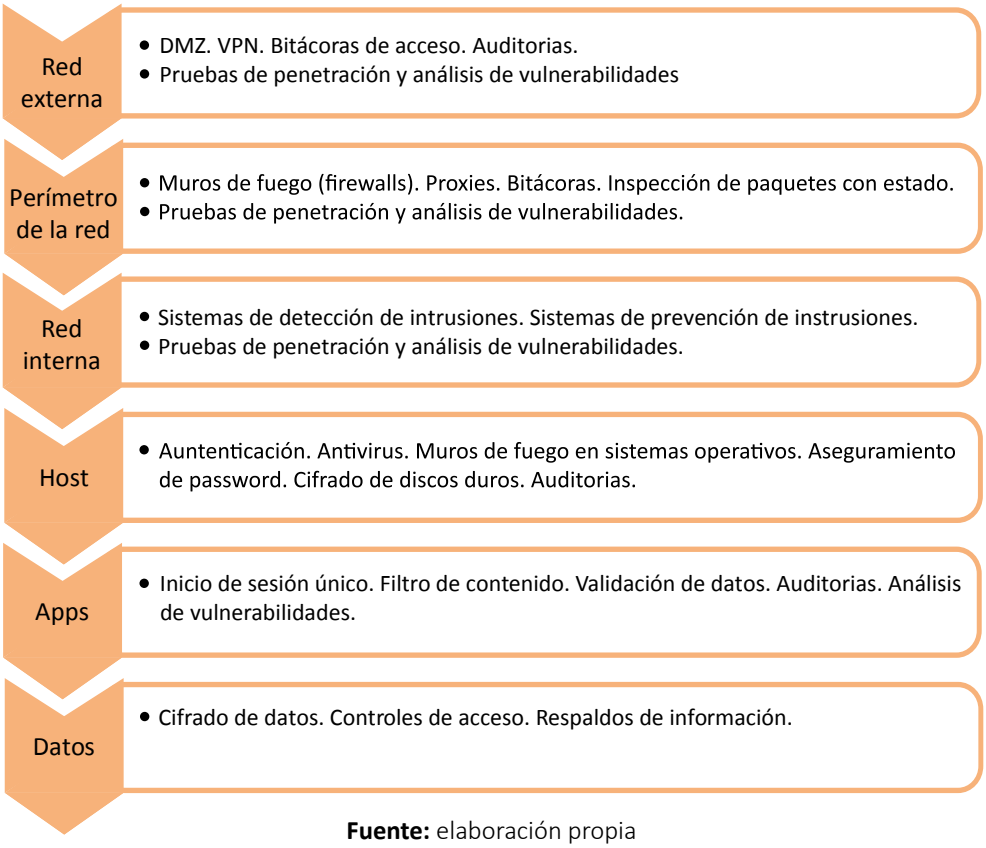
Capas

Cuando miramos las capas que podríamos colocar en nuestra estrategia de defensa en profundidad, probablemente descubriremos que varían dada la situación particular y el entorno que estamos defendiendo. Como discutimos, desde una perspectiva de seguridad de la información estrictamente lógica, nos gustaría ver la red externa, perímetro de red, la red interna, el host, la aplicación y las capas de datos como áreas para colocar nuestras defensas. Podríamos agregar complejidad a nuestro modelo defensivo al incluir otras capas vitales como defensas físicas, políticas, conciencia y capacitación del usuario, y una multitud de otras, pero por el momento nos quedaremos con un ejemplo más simple. A medida que avancemos en el libro, volveremos al concepto de defensa en profundidad mientras discutimos la seguridad para áreas más específicas.

Como podemos ver en la Figura 2, se enumeran algunas de las defensas que podríamos usar para cada una de las capas que discutimos. En algunos casos, vemos una medida defensiva en varias capas, ya que se aplica en más de un área. Un buen ejemplo de esto es la prueba de penetración. La prueba de penetración es un método para encontrar lagunas en nuestra seguridad mediante el uso de algunos de los mismos métodos que usaría un atacante para ingresar (discutiremos esto en mayor

profundidad más adelante), y es una táctica que podríamos querer usar en todas las capas de nuestra defensa. A medida que avancemos en el libro, discutiremos cada una de estas áreas con mayor detalle y las defensas específicas que podríamos querer usar para cada una.

Figura 2: Defensas en cada Capa.



Fuente: elaboración propia

1.8. Resumen

La seguridad de la información es un componente vital para la era en la que los datos de innumerables personas y organizaciones se almacenan en una variedad de sistemas informáticos, a menudo no bajo nuestro control directo. Cuando se discute la seguridad de la información en un sentido general, es importante recordar que la seguridad y la productividad son a menudo conceptos diametralmente opuestos, y que ser capaz de señalar exactamente cuándo estamos seguros es una tarea difícil.

Cuando se discuten problemas o situaciones de seguridad de la información, es útil tener un modelo para hacerlo. Dos modelos potenciales son la tríada de la Seguridad

de la Información compuesta de confidencialidad, integridad y disponibilidad, y el hexágono Parkeriano, compuesta de confidencialidad, integridad, disponibilidad, posesión o control, autenticidad y utilidad.

Cuando observamos las amenazas que podríamos enfrentar, es importante comprender el concepto de riesgo. Solo enfrentamos el riesgo de un ataque cuando hay una amenaza presente y tenemos una vulnerabilidad que esa amenaza en particular puede explotar. Para mitigar el riesgo, utilizamos tres tipos principales de controles: físicos, lógicos y administrativos.

La defensa en profundidad es un concepto particularmente importante en el mundo de la seguridad de la información. Para construir medidas defensivas utilizando este concepto, implementamos múltiples capas de defensa, cada una de las cuales nos brinda una capa adicional de protección. La idea detrás de la defensa en profundidad no es mantener a un atacante permanentemente, sino retrasarlo lo suficiente como para alertarnos del ataque y permitirnos montar una defensa más activa.

1.9. Cuestionario de estudio

1. Explique la diferencia entre una vulnerabilidad y una amenaza.
2. Enumere seis elementos que podrían considerarse controles lógicos.
3. ¿Qué término podríamos usar para describir la utilidad de los datos?
4. ¿Qúe categoría de ataque es un ataque contra la confidencialidad?
5. ¿Cómo sabemos en qué punto podemos considerar nuestro entorno seguro?
6. ¿Usando el concepto de defensa en profundidad, qué capas podríamos usar para asegurar nosotros mismos en contra de que alguien elimine datos confidenciales de nuestra oficina en una unidad flash USB?
7. ¿Según el hexágono de Parker, qué principios se ven afectados si perdemos un envío de cintas de respaldo encriptadas que contienen información personal y de pago para nuestros clientes?
8. Si los servidores web de nuestro entorno se basan en Internet de Microsoft se descubre Information Server (IIS) y un nuevo gusano que ataca los servidores web Apache ¿Qué no tenemos?

9. Si desarrollamos una nueva política para nuestra organización que requiere que usemos contraseñas complejas y generadas automáticamente que son exclusivas de cada sistema y tienen un mínimo de 30 caracteres de longitud, tal como: !Hs4 (j0qO $ & zn1% 2SK38cn ^! Ks620! ¿Qué se verá afectado negativamente?

10. Considerando la tríada de la Seguridad de la Información y el hexágono Parkeriano, ¿cuáles son las ventajas y desventajas de cada modelo?

CAPÍTULO 2: IDENTIFICACIÓN Y AUTENTICACIÓN

Cuando estamos desarrollando medidas de seguridad, ya sea en la escala de un mecanismo específico o de una infraestructura completa, la identificación y la autenticación son conceptos clave. Identificación es la afirmación de lo que alguien o algo es, y autenticación establece si esta afirmación es cierta. Podemos ver que tales procesos tienen lugar diariamente en una amplia variedad de formas. Un ejemplo muy común de una transacción de identificación y autenticación se puede encontrar en el uso de tarjetas de pago que requieren un número de identificación personal (PIN). Cuando deslizamos la tira magnética en la tarjeta, estamos afirmando que somos la persona indicada en la tarjeta. En este punto, hemos dado nuestra identificación, pero nada más. Cuando se nos solicita que ingresemos el PIN asociado con la tarjeta, estamos completando la parte de autenticación de la transacción, con suerte cumpliendo con éxito.

Algunos de los métodos de identificación y autenticación que utilizamos en la vida diaria son particularmente frágiles y dependen en gran medida de la honestidad y diligencia de los involucrados en la transacción. Muchos de estos intercambios que implican la exhibición de tarjetas de identificación, como la compra de artículos restringidos a personas mayores de cierta edad, se basan en la teoría de que la tarjeta de identificación que se muestra es genuina y precisa. También dependemos de que la persona o el sistema que realiza la autenticación sea competente y capaz no solo de realizar el acto de autenticación, sino también de poder detectar actividades falsas o fraudulentas.

Podemos utilizar varios métodos de identificación y autenticación, desde el simple uso de nombres de usuario y contraseñas, hasta tokens de hardware especialmente diseñados que sirven para establecer nuestra identidad de múltiples maneras. Discutiremos varios de estos métodos y cómo se usan a lo largo del capítulo.

2.1. Identificación

La identificación, como mencionamos en la sección anterior, es simplemente una afirmación de quiénes somos. Esto puede incluir quién afirmamos ser como persona, quién afirma que un sistema está a través de la red, quién es la parte de origen de un correo electrónico o transacciones similares. Es importante tener en cuenta que el proceso de identificación no se extiende más allá de este reclamo y no implica ningún tipo de verificación o validación de la identidad que reclamamos. Esa parte del proceso se conoce como autenticación y es una transacción separada (Parra, 2019).

Quien decimos ser es un concepto tenue, en el mejor de los casos. Podemos identificarnos por nuestros nombres completos, versiones abreviadas de nuestros nombres, apodos, números de cuenta, nombres de usuario, tarjetas de identificación, huellas digitales, muestras de ADN y una enorme variedad de otros métodos. Desafortunadamente, con algunas excepciones, tales métodos de identificación no son únicos, e incluso algunos de los métodos de identificación supuestamente únicos, como la huella digital, pueden duplicarse en muchos casos.

Quien afirmamos ser puede, en muchos casos, ser un elemento de información que está sujeto a cambios. Por ejemplo, nuestros nombres pueden cambiar, como en el caso de las mujeres que cambian su apellido al casarse en algunos países, las personas que legalmente cambian su nombre a un nombre completamente diferente, o incluso las personas que simplemente eligen usar un nombre diferente. Además, generalmente podemos cambiar las formas lógicas de identificación con mucha facilidad, como en el caso de números de cuenta, nombres de usuario y similares. Incluso los identificadores físicos, como la altura, el peso, el color de la piel y el color de los ojos se pueden cambiar. Uno de los factores más importantes para tener en cuenta cuando trabajamos con la identificación es que un reclamo de identidad sin fundamento no es información confiable por sí sola.

Verficicación de identidad

La verificación de identidad es un paso más allá de la identificación, pero aún es un paso por debajo de la autenticación, que discutiremos en la siguiente sección. Cuando se nos pide que mostremos una licencia de conducir, cédula de identificación, pasaporte, certificado de nacimiento u otra forma similar de identificación, esto generalmente tiene el propósito de verificar la identidad, no de autenticación. Este es el equivalente aproximado de alguien que reclama la identidad “Juan Pérez”, nos preguntamos si la persona es realmente Juan Pérez, y estamos satisfechos con una respuesta de “Seguro que soy” de la persona (además de un poco de papeleo). Como verificación de identidad, esto es muy inconsistente, en el mejor de los casos.

Podemos llevar el ejemplo un poco más allá y validar la forma de identificación, por ejemplo, un pasaporte, contra una base de datos que contenga una copia adicional de la información que contiene y que coincida con la fotografía y las especificaciones físicas con la persona parada frente a nosotros. Esto puede acercarnos un poco, pero aún no estamos al nivel de seguridad que obtenemos de la autenticación. La verificación de identidad se utiliza no solo en nuestras interacciones personales sino también en los sistemas informáticos. En muchos casos, como cuando enviamos un

correo electrónico, la identidad que proporcionamos se considera verdadera, sin que se tomen medidas adicionales para autenticarnos. Tales brechas en la seguridad contribuyen a la enorme cantidad de tráfico de spam que vemos y que según investigaciones como las de PreciseSecurity.com, los mensajes de spam representan más de la mitad de esa cantidad, representando el 55% del tráfico global de correo electrónico en el año 2019.

Identificación falsa

Como hemos discutido, los métodos de identificación están sujetos a cambios. Como tales, también están sujetos a falsificación. Todos hemos oído hablar de la licencia de conducir fraudulenta de uso común, a menudo utilizada por menores para comprar artículos para los que son demasiado jóvenes para comprar, o para entrar en bares o clubes nocturnos cuando no son mayores de edad para hacerlo. En una nota un poco más siniestra, los delincuentes y terroristas también utilizan estos medios de identificación falsificados para una variedad de tareas de naturaleza nefasta. Ciertos medios principales de identificación, como los certificados de nacimiento, también proporcionan una forma de obtener formas adicionales de identificación, como las del Seguro Social o licencias de conducir, fortaleciendo así una identidad falsa. Esto se ha tipificado en legislación de muchos países como delitos penales.

Este tipo de ataque es desafortunadamente común y fácil de ejecutar. Dada una cantidad mínima de información, generalmente un nombre, dirección y número de Seguro Social son suficientes, es posible hacerse pasar por alguien en un grado suficiente para poder actuar como esa persona en muchos casos. Las víctimas de robo de identidad pueden descubrir que se han realizado líneas de crédito, tarjetas de crédito, préstamos para vehículos, hipotecas de viviendas y otras transacciones utilizando su identidad robada.

Tales crímenes ocurren debido a la falta de requisitos de autenticación para muchas de las actividades en las que participamos. En la mayoría de los casos, la única verificación que se realiza es la verificación de identidad, como discutimos en la sección anterior. Este proceso es un pequeño obstáculo, en el mejor de los casos, y puede evitarse fácilmente utilizando formas de identificación falsificadas. Para rectificar esta situación, necesitamos completar el proceso de identificación y autenticación de las personas involucradas en estas transacciones, para demostrar al menos de manera más concluyente que realmente estamos interactuando con las personas que creemos que somos. En el caso de las personas, este no es un problema técnico insoluble en ninguna medida, pero es más un problema de usuario.

Cuando observamos problemas similares para los sistemas y entornos informáticos, podemos ver muchas de las mismas dificultades. Es totalmente posible enviar un correo electrónico desde una dirección que es diferente de la dirección de envío real, táctica que es utilizada regularmente por los spammers. Podemos ver los mismos problemas en muchos otros sistemas y protocolos que se usan a diario y son parte de la funcionalidad de Internet.

2.2. Autenticación

Según Parra (2019) la autenticación es, en un sentido de seguridad de la información, el conjunto de métodos que utilizamos para establecer un reclamo de identidad como verdadero. Es importante tener en cuenta que la autenticación solo establece si el reclamo de identidad realizado es correcto. La autenticación no infiere ni implica nada sobre lo que la parte autenticada puede hacer; esta es una tarea separada conocida como autorización, la cual discutiremos con mayor detalle en el Capítulo 3, pero lo importante que debemos entender por ahora es que la autenticación debe realizarse primero.

En términos de autenticación, hay varios métodos que podemos usar, y cada categoría se denomina factor. Dentro de cada factor, hay varios métodos posibles que podemos usar. Cuando intentamos autenticar un reclamo de identidad, cuantos más factores usemos, más positivos serán nuestros resultados. Los factores son algo que sabes, algo que eres, algo que tienes, algo que haces y dónde estás.

“Algo que sabes” es un factor de autenticación muy común. Esto puede incluir contraseñas, el número de identificación personal (PIN, por sus siglas en Inglés), frases de contraseña o casi cualquier elemento de información que una persona pueda recordar. Podemos ver una implementación muy común de esto en las contraseñas que usamos para iniciar sesión en nuestras cuentas en las computadoras. Este es un factor débil porque si la información de la que depende el factor está expuesta, esto puede anular la unicidad de nuestro método de autenticación.

“Algo que eres” es un factor basado en los atributos físicos relativamente únicos de un individuo, a menudo referidos como biometría. Este factor puede basarse en atributos simples, como la altura, el peso, el color del cabello o el color de los ojos, pero estos no tienden a ser lo suficientemente únicos como para hacer identificadores muy seguros. Los más utilizados son los identificadores más complejos, como las huellas digitales, los patrones de iris o retina, o las características faciales. Este factor es un poco más fuerte, ya que falsificar o robar una copia de un identificador físico es una tarea algo más difícil, aunque no imposible. Hay dudas sobre si la biometría es

realmente un factor de autenticación, o si realmente solo constituye una verificación. Discutiremos esto nuevamente más adelante en el capítulo cuando cubramos la biometría en mayor profundidad.

Figura 3. Token de Seguridad basado en software.

Fuente: elaboración propia.

"Algo que tiene" es un factor generalmente basado en la posesión física de un elemento o dispositivo, aunque este factor también puede extenderse a algunos conceptos lógicos. Podemos ver estos factores en el uso general en forma de tarjetas de cajero automático, tarjetas de identidad emitidas por el gobierno, o tokens de seguridad basados en software, como se muestra en la Figura 3. Algunas instituciones, como los bancos, también han comenzado a utilizar el acceso a dispositivos lógicos como teléfonos celulares o cuentas de correo electrónico como métodos de autenticación. Este factor puede variar en fuerza dependiendo de la implementación. En el caso de

un token de seguridad, en realidad necesitaríamos robar un dispositivo específico para falsificar el método de autenticación. En el caso de que el acceso a una dirección de correo electrónico se utilice como este tipo de factor, tenemos una medida de resistencia considerablemente menor.

"Algo que haces", a veces considerado una variación de algo que eres, es un factor basado en las acciones o comportamientos de un individuo. Dichos factores pueden incluir el análisis de la marcha del individuo, la medición de múltiples factores en su escritura, el retraso de tiempo entre las pulsaciones de teclas mientras escribe una frase de paso o factores similares. Estos factores presentan un método de autenticación muy fuerte y son muy difíciles de falsificar. Sin embargo, tienen el potencial de rechazar incorrectamente a los usuarios legítimos a una tasa más alta que algunos de los otros factores, lo que resulta en la negación de algunos usuarios que en realidad deberían autenticarse.

"Donde se encuentra" es un factor de autenticación basado en posicionamiento geográfico. Este factor funciona de manera diferente a los otros factores, ya que su método de autenticación depende de la persona que se autentica como físicamente presente en una ubicación o ubicaciones particulares. Podemos ver una implementación algo floja de este factor en el acto de extraer fondos de un cajero automático. Aunque ciertamente esta no es una decisión de diseño debido a razones de seguridad, es cierto que esto solo se puede hacer en ubicaciones geográficas particulares. Este factor, aunque es potencialmente menos útil que algunos de los otros factores, es muy difícil de contrarrestar sin alterar completamente el sistema que realiza la autenticación.

Autenticación multifactorial

Como probablemente estén pensando, la autenticación multifactor utiliza uno o más de los factores que discutimos en la sección anterior. Podemos ver un ejemplo común de autenticación multifactor en el uso de un cajero automático. En este caso, tenemos algo que sabemos, nuestro PIN, y algo que tenemos, nuestra tarjeta de cajero automático. Nuestra tarjeta de cajero automático cumple una doble función como factor de autenticación y como forma de identificación. Podemos ver un ejemplo similar al escribir cheques que se extraen de una cuenta bancaria; en este caso, algo que tenemos, los cheques en sí y algo que hacemos, aplicando nuestra firma a ellos. Aquí, los dos factores involucrados en la redacción de un cheque son bastante débiles, por lo que a veces vemos que se les aplica un tercer factor, una huella digital. También podríamos argumentar que la firma y la huella dactilar no

son, en este caso, en realidad autenticación, sino más bien verificación, un proceso mucho menos robusto que discutimos cuando hablamos de identidad anteriormente en el capítulo.

Dependiendo de los factores particulares seleccionados, podemos ensamblar esquemas de autenticación multifactor más fuertes o débiles en una situación dada. En algunos casos, aunque ciertos métodos pueden ser más difíciles de vencer, no son prácticos de implementar. Por ejemplo, el ADN es un método muy fuerte de autenticación, pero no es práctico para el uso regular. Como discutimos en el Capítulo 1, cuando hablamos de seguridad, debemos tener cuidado de construir una seguridad que sea razonablemente proporcional a lo que estamos protegiendo. Podríamos instalar escáneres de iris en cada terminal de tarjeta de crédito en lugar de que el cliente firme su recibo de la tarjeta de crédito y sin duda mejorar nuestra seguridad, pero esto sería costoso y poco práctico y podría molestar a nuestros clientes.

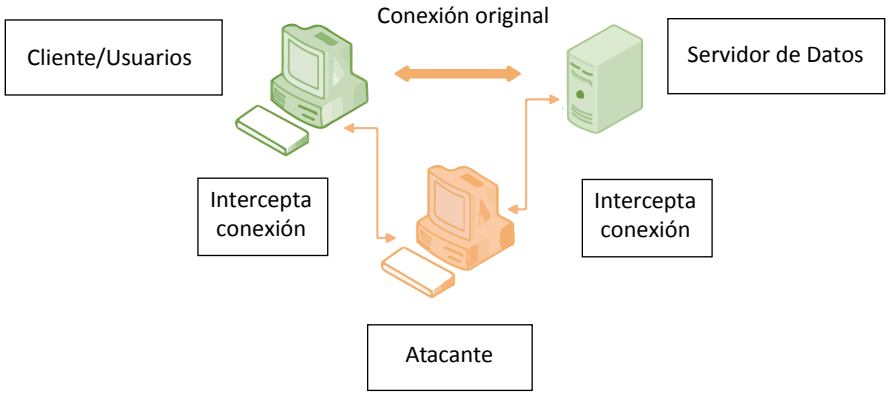
Autenticación mutua

La autenticación mutua se refiere a un mecanismo de autenticación en el que ambas partes se autentican entre sí. En el proceso de autenticación estándar, que es solo de autenticación unidireccional, el cliente se autentica en el servidor para demostrar que es la parte que debe acceder a los recursos que proporciona el servidor. En la autenticación mutua, el cliente no solo se autentica en el servidor, sino que el servidor también se autentica en el cliente. La autenticación mutua a menudo se implementa mediante el uso de certificados digitales, que discutiremos con mayor detalle en el Capítulo 5. Brevemente, tanto el cliente como el servidor tendrían un certificado para autenticar al otro.

En los casos en que no realizamos la autenticación mutua, nos dejamos abiertos a ataques de suplantación de identidad, a menudo denominados ataques de hombre en el medio (MITM, por sus siglas en Inglés). En un ataque de hombre en el medio, el atacante se inserta entre el cliente y el servidor y suplanta el servidor al cliente, y el cliente al servidor, como se muestra en la Figura 4. Esto se hace eludiendo el patrón normal de tráfico, luego interceptando y reenviando el tráfico que normalmente fluiría directamente entre el cliente y el servidor. Esto normalmente es posible porque el atacante solo tiene que subvertir o falsificar la autenticación del cliente al servidor.

Si implementamos la autenticación mutua, esto se convierte en un ataque considerablemente más difícil de llevar a cabo para la parte atacante.

Figura 4. Ataque de hombre en el medio.



Fuente: elaboración propia.

La autenticación mutua también se puede utilizar en combinación con la autenticación multifactor, y esta última generalmente se realiza solo en el lado del cliente. La autenticación multifactorial desde el servidor hasta el cliente no solo sería técnicamente desafiante sino también poco práctico en la mayoría de los entornos actuales. Posiblemente, podríamos implementar la autenticación mutua de múltiples factores en un entorno de seguridad extremadamente alta, pero esto resultaría en una pérdida muy grande de productividad.

Contraseñas

Las contraseñas son familiares para la gran mayoría de nosotros que usamos computadoras y dispositivos móviles regularmente. En combinación con un nombre de usuario, una contraseña generalmente nos permitirá acceder a un sistema informático, una aplicación, nuestro correo electrónico, redes sociales, un teléfono o dispositivos similares. Las contraseñas, aunque solo son un factor de autenticación, pueden, cuando se construyen e implementan adecuadamente, representar un nivel relativamente alto de seguridad.

Cuando describimos una contraseña como fuerte, no proporcionamos una imagen inmediata de lo que estamos discutiendo. Un mejor término descriptivo podría ser complejo para comunicar los conceptos importantes inherentes a la creación de una contraseña. Si construimos una contraseña que contenga letras minúsculas y una longitud de ocho caracteres, podemos usar una utilidad para descifrar contraseñas, que discutiremos más adelante en el Capítulo 10, para descifrar la contraseña en un minuto o dos, dado un valor razonablemente fuerte computadora en la cual ejecutar la herramienta de craqueo. Si usamos la misma contraseña de ocho caracteres,

pero usamos letras mayúsculas y minúsculas, el descifrador de contraseñas tardará alrededor de seis días en romper la contraseña. Si agregamos números a la mezcla, nos llevará un poco más de 25 días descifrar nuestra contraseña. Si utilizamos el método de construcción de contraseña recomendado para crear contraseñas seguras, crearíamos una contraseña que se construyera con letras mayúsculas, minúsculas, números y símbolos, como los signos de puntuación, entonces eso es potencialmente más difícil de recordar, como $ sU y qw!3, tendríamos una contraseña que llevaría más de dos años descifrar con una estación de trabajo promedio.

El tipo de descifrado de contraseñas que estamos discutiendo aquí se denomina craqueo por fuerza bruta. Esto implica probar todas las combinaciones posibles de caracteres de los que la contraseña podría estar compuesta, en secuencia, hasta que los intentemos todos. Dado un poderoso sistema en el cual ejecutar el cracker y una contraseña mal construida, este puede ser un medio muy efectivo para recuperar contraseñas.

Según Flores *et al.* (2019), además de construir contraseñas seguras, también debemos tener cuidado de practicar una buena higiene de contraseñas. Un problema con las contraseñas seguras es que pueden ser difíciles de recordar. Esto podría alentarnos a tomar medidas para recordar nuestras contraseñas, como escribirlas y publicarlas en un lugar útil, tal vez bajo nuestro teclado o en nuestro monitor. Esto, por supuesto, anula por completo el propósito de tener una contraseña si alguien viene a husmear en nuestro escritorio.

Otro problema de contraseña es la sincronización manual de contraseñas, en resumen, usar la misma contraseña en todas partes. Si usamos la misma contraseña para nuestro correo electrónico, para nuestro inicio de sesión en el trabajo, para nuestras redes sociales y en cualquier otro lugar, estamos colocando la seguridad de todas nuestras cuentas con cada propietario del sistema donde usamos la misma contraseña. Si alguno de ellos está comprometido y su contraseña está expuesta, tenemos un problema grave. Todo lo que un atacante debe hacer es buscar nuestro nombre de cuenta en Internet para encontrar algunos de los lugares donde se usa el mismo nombre y comenzar a probar nuestra contraseña predeterminada. Cuando el atacante ingresa a nuestra cuenta de correo electrónico, el juego ha terminado con éxito a favor del atacante.

Biometría

Cuando se discute la biometría, debemos considerar qué es exactamente cuando la usamos como factor de autenticación. Como discutimos en la sección de

"Identificación" al comienzo del capítulo, existe una diferencia entre la autenticación y la verificación. Cuando completamos una transacción de autenticación con un identificador biométrico, esencialmente le pedimos al usuario que proporcione evidencia que él o ella es quien dice ser; esto es, por definición, verificación y no autenticación. Aunque algunos identificadores biométricos pueden ser más difíciles de falsificar que otros, esto solo se debe a las limitaciones de la tecnología actual. En algún momento en el futuro, necesitaremos desarrollar características biométricas más robustas para medir, o dejar de usar la biometría como mecanismo de autenticación.

Dicho esto, podemos usar sistemas biométricos de dos maneras diferentes. Podemos usarlos para verificar el reclamo de identidad que alguien ha presentado, como discutimos anteriormente, o podemos revertir el proceso y usar la biometría como método de identificación. Este proceso es comúnmente utilizado por las agencias de aplicación de la ley para identificar al propietario de las huellas dactilares que se han dejado en varios objetos, y puede ser un esfuerzo que consume mucho tiempo, teniendo en cuenta el gran tamaño de las bibliotecas de huellas dactilares en poder de dichas organizaciones. También vemos un uso similar en la comparación de muestras de ADN tomadas de sospechosos en crímenes en comparación con la evidencia física recuperada de la escena del crimen.

Para usar un sistema biométrico de cualquier manera, necesitamos llevar al usuario a través del proceso de inscripción. La inscripción implica registrar la característica biométrica elegida del usuario, por ejemplo, hacer una copia de una huella digital, y registrar la característica en el sistema. El procesamiento de la característica también puede incluir la anotación de ciertas partes de la imagen, dependiendo de la característica en cuestión, para usarlas en el sistema en el futuro.

Los factores biométricos se definen por siete características: universalidad, unicidad, permanencia, colectabilidad, rendimiento, aceptabilidad y elusión.

Según Jain (2011), se definen cada de una ellas, a saber:

1. La *universalidad* estipula que deberíamos poder encontrar nuestra característica biométrica elegida en la mayoría de las personas que esperamos inscribir en el sistema. Por ejemplo, aunque podríamos usar una cicatriz como identificador, no podemos garantizar que todos tengan una cicatriz. Incluso si elegimos una característica muy común, como una huella digital, debemos tener en cuenta que algunas personas pueden no tener un dedo índice en su mano

derecha y estar preparados para compensar esto.

2. La *unicidad* es una medida de cuán única es una característica particular entre los individuos. Por ejemplo, si elegimos usar la altura o el peso como un identificador biométrico, tendríamos una muy buena posibilidad de encontrar varias personas en cualquier grupo dado que son de la misma altura o peso. Podemos seleccionar características con un mayor grado de unicidad, como el ADN o los patrones de iris, pero siempre existe la posibilidad de duplicación, ya sea intencional o no.

3. La *permanencia* muestra cuán bien una característica particular resiste el cambio con el tiempo y con el avance de la edad. Si elegimos un factor que puede variar fácilmente, como la altura, el peso o la geometría de la mano, eventualmente nos encontraremos en la posición de no poder autenticar a un usuario legítimo. En cambio, podemos usar factores como las huellas dactilares que, aunque pueden modificarse, es poco probable que se modifiquen sin una acción deliberada.

4. La *colectabilidad* mide cuán fácil es adquirir una característica con la que luego podamos autenticar a un usuario. La biometría más utilizada, como las huellas digitales, es relativamente fácil de colectar, y esta es una de las razones por las que se usan comúnmente. Si elegimos una característica que es más difícil de adquirir, como una huella, el usuario deberá quitarse el zapato y el calcetín para inscribirse (y autenticarse nuevamente más tarde), lo cual es considerablemente más problemático que tomar una huella digital.

5. El *rendimiento* es un conjunto de métricas que juzgan qué tan bien funciona un sistema dado. Dichos factores incluyen velocidad, precisión y tasa de error. Discutiremos el rendimiento de los sistemas biométricos con mayor detalle más adelante en esta sección.

6. La *aceptabilidad* es una medida de cuán aceptable es la característica particular para los usuarios del sistema. En general, los sistemas que son lentos, difíciles de usar o incómodos de usar tienen menos probabilidades de ser aceptables para el usuario. Es probable que los sistemas que requieren que los usuarios se quiten la ropa,

toquen dispositivos que otras personas hayan usado repetidamente o que proporcionen tejidos o fluidos corporales probablemente no gozarán de un alto grado de aceptabilidad.

7. La *elusión* describe la facilidad con que un sistema puede ser engañado por un identificador biométrico falsificado. El ejemplo clásico de un ataque de elusión contra la huella digital como identificador biométrico se encuentra en el "dedo gomoso". En este tipo de ataque, se levanta una huella digital de una superficie, potencialmente de forma encubierta, y se usa para crear un molde con el cual el atacante puede proyectar una imagen positiva de la huella digital en gelatina. Algunos sistemas biométricos tienen características diseñadas específicamente para vencer tales ataques midiendo la temperatura de la piel, el pulso, la respuesta pupilar y una serie de otros elementos.

Hay varios problemas comunes a los sistemas biométricos. Como mencionamos cuando discutimos la elusión, algunos identificadores biométricos se pueden falsificar fácilmente. Dado un identificador falsificado, enfrentamos un problema; no podemos revocar tal característica.

Aunque podemos eliminar el identificador particular del sistema y ya no permitimos que se use para autenticar a un usuario, en algunos casos esto no es práctico. Si miramos las huellas digitales como un ejemplo, encontramos un identificador de uso tan común que alguien que usa falsamente nuestras huellas digitales podría causarnos grandes problemas. Aunque actualmente podemos pasar a una biometría más fuerte que, en la actualidad, no se puede copiar fácilmente, como un patrón de iris, tales esfuerzos no quedarán fuera del alcance de los atacantes para siempre.

También nos enfrentamos a posibles problemas de privacidad en el uso de la biometría, tanto como propietarios de dichos sistemas y como usuarios de ellos. Cuando estamos inscritos en un sistema biométrico, esencialmente estamos regalando una copia de cualquier identificador elegido, ya sea una huella dactilar, un patrón de iris, una muestra de ADN u otro. Una vez que dicho elemento se ha ingresado en un sistema informático, tenemos poco control, si es que lo tenemos, sobre lo que se hace con el material. Podemos esperar que una vez que ya no estemos asociados con la institución en cuestión, dichos materiales serían destruidos, pero realmente no tenemos forma de garantizar que esto realmente haya tenido lugar. Particularmente en el caso del muestreo de ADN, las repercusiones de la entrega de

material genético podrían ser un problema que se cierne sobre nuestras cabezas por el resto de nuestras vidas.

Tokens físicos

Un token de físico estándar es un dispositivo pequeño, generalmente en el formato general de una tarjeta de crédito o llavero. Los tokens más simples se ven idénticos a una unidad flash USB y contienen una pequeña cantidad de almacenamiento con un certificado o identificador único. Algunos incorporan pantallas LCD, como se muestra en la Figura 5, teclados para ingresar contraseñas, lectores biométricos, dispositivos inalámbricos y funciones adicionales para mejorar la seguridad.

Muchos tokens físicos contienen un reloj interno que, en combinación con el identificador único del dispositivo, un PIN o contraseña de entrada, y potencialmente otros factores, se utilizan para generar un código, que generalmente se muestra en la pantalla del token. Este código cambia regularmente, normalmente cada 30 segundos. La infraestructura utilizada para realizar un seguimiento de dichos tokens puede predecir, para un dispositivo determinado, cuál será la salida adecuada en un momento dado, pudiéndose usar esa salida para autenticar al usuario.

Figura 5. Token físico para acceso bancario.

Fuente: elaboración propia.

En el caso de tokens más complejos que incluyen la capacidad de ingresar un PIN o leer una huella digital, la seguridad del dispositivo se mejora considerablemente. Para que un atacante utilice un dispositivo multifactor robado, el atacante no solo necesitaría el token físico en sí, sino que también tendría que subvertir la infraestructura que estaba sincronizada con la salida de información del dispositivo o extraer algo que usted saber y / o algo que usted es factor (es) del propietario legítimo del dispositivo.

2.3. Resumen

La identificación es una afirmación de la identidad de una parte en particular. Puede ser una persona, proceso, sistema u otra entidad. La identificación es solo una afirmación de identidad y no implica que esta afirmación sea correcta, ni ningún privilegio que pueda estar asociado con la identidad, si se demuestra que es cierta.

La autenticación es el proceso que utilizamos para validar si el reclamo de identidad es correcto. Es importante tener en cuenta que la autenticación y la verificación no son lo mismo y que la verificación es una prueba mucho más débil desde una perspectiva de seguridad.

Cuando realizamos la autenticación, podemos usar varios factores. Los factores principales son algo que sabes, algo que eres, algo que tienes, algo que haces y dónde estás. Cuando usamos un mecanismo de autenticación que incluye más de un factor, esto se conoce como autenticación multifactor. El uso de múltiples factores nos da un mecanismo de autenticación mucho más fuerte de lo que podríamos tener.

2.4. Cuestionario de estudio

1. ¿Cuál es la diferencia entre verificación y autenticación de un ¿identidad?
2. ¿Cómo medimos la velocidad a la que no podemos autenticar legítimamente usuarios en un sistema biométrico?
3. ¿Cómo llamamos al proceso en el que el cliente se autentica en el servidor y el servidor se autentica con el cliente?
4. ¿Se describiría una clave como qué tipo de factor de autenticación?
5. ¿Qué factor biométrico describe qué tan bien una característica resiste el cambio? ¿Tiempo extraordinario?
6. Si estamos utilizando una tarjeta de identidad como base para nuestro esquema de autenticación ¿Qué pasos podríamos agregar al proceso para permitirnos pasar a la autenticación multifactor?
7. Si estamos utilizando una contraseña de 8 caracteres que contiene solo caracteres en minúsculas ¿Aumentar la longitud a 10 caracteres representaría un aumento significativo en la fuerza?
8. Mencione tres razones por las cuales una tarjeta de identidad por sí

sola podría no ser ideal Método de autenticación.

9. ¿Qué factores podríamos usar al implementar un esquema de autenticación multifactor para los usuarios que inician sesión en estaciones de trabajo que se encuentran en un entorno seguro y son utilizados por más de una persona?

10. Si estamos desarrollando un sistema de autenticación multifactorial para un entorno en el que podríamos encontrar un número de usuarios discapacitados o lesionados mayor que el promedio, como un hospital ¿Qué factores de autenticación podríamos usar o evitar? ¿Por qué?

CAPÍTULO III: AUTORIZACIÓN

Una vez que hayamos recibido un reclamo de identidad y hayamos establecido si ese reclamo es válido, como discutimos en el Capítulo 2, pasamos a lo que una instancia autenticada tiene permitido hacer y si le permitiremos o negaremos el acceso a nuestros recursos. Podemos lograr esto con dos conceptos principales: autorización y control de acceso. La autorización nos permite especificar dónde se debe permitir o denegar el acceso a la parte, y el control de acceso nos permite administrar este acceso a un nivel muy granular.

Los controles de acceso se pueden construir de varias maneras. Podemos basar los controles de acceso en atributos físicos, conjuntos de reglas, listas de individuos o sistemas, o factores más complejos. El tipo particular de control de acceso a menudo depende del entorno en el que se va a utilizar. Podemos encontrar controles de acceso más simples implementados en muchas aplicaciones y sistemas operativos, mientras que se pueden implementar configuraciones multinivel más complejas en entornos militares o gubernamentales. En tales casos, la importancia de lo que controlamos el acceso puede dictar que hagamos un seguimiento de lo que nuestros usuarios tienen acceso a través de varios niveles de sensibilidad (Arana, 2013).

Cuando discutimos los conceptos de control de acceso, podemos referirnos a ellos en un sentido puramente lógico o físico o, más comúnmente, como una combinación de ambos. En términos de sistemas de control de acceso, es importante comprender que, cuando se trata de entornos informáticos, lo lógico y lo físico a menudo están estrechamente relacionados. Los sistemas de control de acceso lógico, incluso aquellos que no tienen un componente físico inmediatamente obvio, aún dependen del sistema físico.

Del mismo modo, muchos, pero no todos, los controles de acceso físico como las puertas especializadas tienen algún tipo de componente lógico. A menudo, los sistemas que controlan nuestro acceso a las instalaciones y dentro de ellas dependen igualmente de las redes, los sistemas informáticos y otros componentes similares. En muchos sentidos, la seguridad de la información y la seguridad física están estrechamente relacionadas entre sí.

3.1. Autorización

La autorización es el siguiente paso dado después de haber completado la identificación y autenticación, como se muestra en la Figura 6. La autorización nos permite determinar, una vez que hemos autenticado a la parte en cuestión,

exactamente qué se les permite hacer. Normalmente implementamos la autorización mediante el uso de controles de acceso, que discutiremos más adelante en este capítulo.

Principio de menor privilegio

Cuando estamos determinando qué acceso proporcionaremos a las partes a las que les hemos proporcionado acceso autorizado, hay un concepto importante que debemos tener en cuenta, llamado el principio del privilegio mínimo. El principio del privilegio mínimo dicta que solo debemos permitir el mínimo acceso a una parte, esto podría ser una persona, cuenta de usuario o proceso, para permitirle realizar la funcionalidad necesaria. Por ejemplo, alguien que trabaja en un departamento de ventas no debería necesitar acceso a los datos de nuestro sistema interno de recursos humanos para hacer su trabajo. La violación del principio del privilegio mínimo es el corazón de muchos de los problemas de seguridad que enfrentamos hoy.

Una de las formas más comunes en las que encontramos que el principio de menor privilegio implementado de manera inadecuada es en los permisos que otorgamos a las cuentas de usuario del Sistema Operativo, más comúnmente violadas por los usuarios y administradores de los sistemas operativos de Microsoft. En los sistemas operativos de Microsoft, a menudo encontramos que los usuarios ocasionales, que realizan tareas como crear documentos en procesadores de texto e intercambiar correo electrónico, están configurados con acceso administrativo, lo que les permite llevar a cabo cualquier tarea. Como consecuencia de esto, cada vez que el usuario privilegiado abre un archivo adjunto de correo electrónico que contiene malware o se encuentra con un sitio web que empuja el código de ataque a la computadora cliente, estos ataques tienen un dominio libre en el sistema porque están actuando como el usuario, quien, a su vez, está dotado de capacidades administrativas que permitirían por ejemplo detener el antivirus o instalar programas que comprometan el sistema operativo.

Figura 6. Secuencia lógica de autorización.

Fuente: elaboración propia.

Podemos ver el mismo problema en los servicios o procesos que se ejecutan a un nivel más privilegiado de lo que necesitan para llevar a cabo sus funciones. Si tenemos un servicio que ejecuta un servidor web, por ejemplo, este servicio solo necesita el permiso suficiente para acceder a los archivos y scripts que pertenecen directamente al contenido web que sirve, y nada más. Si permitimos que el servicio web acceda a archivos adicionales en el sistema de archivos, un atacante podría leer o alterar estos archivos para obtener acceso no autorizado a información más confidencial de la que normalmente haríamos pública, lo que le da al atacante un camino para atacar más profundamente sistema.

Al seguir cuidadosamente el principio de privilegio mínimo al configurar sistemas, asignar permisos para cuentas y planificar nuestra seguridad, podemos eliminar algunas de las herramientas de acceso más fácil que los atacantes pueden usar contra nosotros. Esta es una medida de seguridad muy simple que podemos implementar, y es muy efectiva.

3.2. Control de acceso

Cuando observamos los controles de acceso, tenemos cuatro tareas básicas que podríamos querer llevar a cabo: permitir el acceso, denegar el acceso, limitar el acceso y revocar el acceso. Entre estas cuatro acciones, podemos describir la mayoría de los problemas o situaciones de control de acceso.

Permitir el acceso nos permite dar a una parte en particular, o partes, acceso a un recurso dado. Por ejemplo, podríamos querer darle acceso a un usuario en particular a un archivo, o podríamos querer que un grupo completo de personas acceda a todos los archivos en un directorio dado. También podríamos estar refiriéndonos al acceso en un sentido físico, al darles a nuestros empleados acceso a nuestras instalaciones mediante el uso de una llave o credencial.

Negar el acceso es lo opuesto diametral de otorgar acceso. Cuando denegamos el acceso, estamos impidiendo el acceso de una parte determinada al recurso en cuestión. Podríamos estar negando el acceso a una persona en particular que intente iniciar sesión en una máquina según la hora del día, o podríamos negar que personas no autorizadas ingresen al vestíbulo de nuestro edificio más allá del horario comercial. Muchos sistemas de control de acceso están configurados para denegar de forma predeterminada, y los usuarios autorizados solo tienen acceso permitido.

Limitar el acceso se refiere a permitir cierto acceso a nuestro recurso, pero solo hasta cierto punto. Esto es muy importante cuando utilizamos aplicaciones que pueden

estar expuestas a entornos propensos a ataques, como vemos con los navegadores web utilizados en Internet. En tales casos, podríamos ver que la aplicación se ejecuta en un entorno limitado para limitar lo que se puede hacer fuera del contexto de la aplicación. En un sentido físico, podemos ver el concepto de limitaciones de control de acceso en los diferentes niveles de claves que podríamos ver en las cerraduras de un edificio. Es posible que tengamos una llave maestra que puede abrir cualquier puerta del edificio, una llave intermedia que puede abrir solo unas pocas puertas y una llave de bajo nivel que puede abrir solo una puerta.

La revocación del acceso es una idea muy importante en el control de acceso. Es vital que una vez que le hayamos otorgado a una parte acceso a un recurso, podamos quitar ese acceso nuevamente. Si, por ejemplo, despidiéramos a un empleado, desearíamos revocar cualquier acceso que pudieran tener a plataformas y servicios de la organización. Queremos eliminar el acceso a su cuenta de correo electrónico, no permitir que se conecten a nuestra red privada virtual (VPN), desactivar su credencial para que ya no puedan ingresar a la instalación y revocar otros accesos que puedan tener. Particularmente cuando trabajamos con recursos orientados a la computadora de alguna manera, puede ser vital poder revocar el acceso a un recurso dado muy rápidamente, además debemos recordar que un empleado descontento ha sido motivo de muchos incidentes de seguridad internos.

Cuando buscamos implementar controles de acceso, hay dos métodos principales que podríamos usar: listas y capacidades de control de acceso. Cada uno de estos tiene aspectos positivos y negativos, y las formas en que podemos llevar a cabo las cuatro tareas básicas que cubrimos anteriormente variarán según el método que elijamos para nuestra implementación de control de acceso.

3.3. Listas de control de acceso

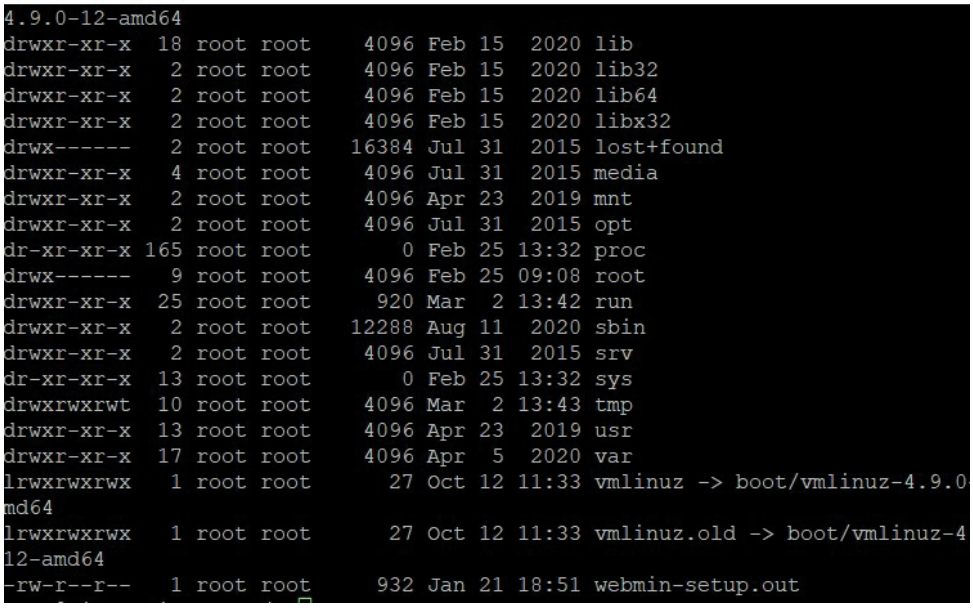
Las listas de control de acceso (ACL, por sus siglas en Inglés), son una opción muy común de implementación de control de acceso. Las ACL generalmente se usan para controlar el acceso en los sistemas de archivos en los que se ejecutan nuestros sistemas operativos y para controlar el flujo de tráfico en las redes a las que están conectados nuestros sistemas (Costas, 2014).

Cuando se construyen ACL, generalmente se construyen específicamente para un determinado recurso, y contienen los identificadores de la parte a la que se le permite acceder al recurso en cuestión y lo que la parte puede hacer en relación con el recurso. En un ejemplo muy simple, al usuario Kilo Mike se le permite el acceso a un determinado recurso de red o de software, mientras que al usuario Rodrigo se

le niega específicamente el acceso. Esto puede parecer un concepto muy simplista, pero en el contexto de implementaciones de ACL más grandes, como las que se usan en los sistemas de archivos, las ACL pueden volverse bastante complejas.

En el caso de los sistemas de archivos, un archivo o directorio también pueden tener varias ACL configuradas. En sistemas operativos tipo UNIX, por ejemplo, podemos ver listas de acceso separadas para un archivo dado, en forma de usuario, grupo y otro. Podemos otorgar a un usuario individual permisos de lectura, escritura y ejecución, un grupo de usuarios diferentes permisos de lectura, escritura y ejecución, y un conjunto diferente de permisos de lectura, escritura y ejecución para cualquier persona que no sea un individuo o grupo Ya he cubierto. Estos tres conjuntos de permisos se mostrarán como rwxrwxrwx, con el primero rwx conjunto que representa el usuario, el segundo el grupo y el tercero otro, como se muestra en la Figura 7.

Figura 7. Permisos de archivos y directorios en sistema operativo Linux.



Fuente: elaboración propia.

Mediante el uso de tales conjuntos de permisos de archivos, podemos, de manera simple, controlar el acceso a los sistemas operativos y aplicaciones que utilizan nuestro sistema de archivos. Aunque solo analizamos los permisos del sistema de archivos basados en Unix, la mayoría de los sistemas de archivos utilizan un conjunto de permisos muy similares, si no idéntico.

También podemos elegir usar direcciones IP como base para el filtrado en nuestra

ACL. Podemos implementar dicho filtrado basado en direcciones individuales o en un rango completo de direcciones IP, sin embargo, al igual que las direcciones las direcciones IP pueden falsificarse y no son exclusivas de una interfaz de red particular. Además, las direcciones IP emitidas por los proveedores de servicios de Internet (ISP, por sus siglas en Inglés) están sujetas a cambios frecuentes, lo que hace que las direcciones IP sean la única base para filtrar una perspectiva inestable, en el mejor de los casos.

También podemos filtrar por el puerto que se utiliza para comunicarse a través de la red. Muchos servicios y aplicaciones comunes usan puertos específicos para comunicarse a través de redes. Por ejemplo, FTP usa los puertos 20 y 21 para transferir archivos, el Protocolo de acceso a mensajes de Internet (IMAP, por sus siglas en Inglés) usa el puerto 143 para administrar el correo electrónico, "Secure Shell" (SSH) usa el puerto 22 para administrar conexiones remotas a los sistemas y muchos más: 65535 puertos en todo tanto para el protocolo TCP como UDP. Podemos controlar el uso de muchas aplicaciones en la red al permitir o denegar el tráfico que se origina o se envía a cualquier puerto que nos interese administrar. Al igual que las direcciones MAC e IP, los puertos específicos que se utilizan para las aplicaciones son una convención, no una regla absoluta. Podemos, con relativa facilidad, cambiar los puertos que las aplicaciones usan a diferentes puertos por completo.

Es probable que el uso de atributos individuales para construir ACL presente una variedad de problemas, incluido el hecho de que nuestro atributo no garantiza que sea único, como una dirección IP, o que sea fácil de modificar, como una dirección MAC. Cuando usamos varios atributos en combinación, comenzamos a llegar a una técnica más segura. Una combinación muy utilizada es la de la dirección IP y el puerto, que generalmente se denomina socket. De esta manera, podemos permitir o denegar el tráfico de red desde una o más direcciones IP utilizando una o más aplicaciones en nuestra red de manera funcional.

También podemos construir ACL para filtrar en una amplia variedad de otras cosas. En algunos casos, es posible que queramos monitorear el tráfico que pasa por nuestra red para permitir o denegar el tráfico en función de criterios más específicos, como el contenido de un paquete individual o una serie de paquetes relacionados. Usando tales técnicas, podemos filtrar el tráfico relacionado con los ataques, o el tráfico que simplemente no es deseable para nosotros, como el relacionado con las redes de intercambio de archivos entre pares comúnmente utilizadas para compartir ilegalmente canciones, videos y software con derechos de autor.

3.4. Métodos para el control de acceso

Los controles de acceso son los medios por los cuales implementamos la autorización y denegamos o permitimos el acceso a las partes, en función de los recursos a los que hemos determinado que se les debe permitir el acceso. Aunque el término puede parecer muy técnico y orientado en la dirección de instalaciones informáticas de alta seguridad, los controles de acceso son algo con lo que tratamos a diario.

Cuando cerramos o desbloqueamos las puertas de nuestra casa, estamos usando una forma de control de acceso físico, basado en las llaves (algo que tiene) que usamos.

Cuando arrancamos nuestro automóvil, también es probable que usemos una llave. Para algunos automóviles más nuevos, nuestra clave puede incluso incluir una capa adicional de seguridad al agregar etiquetas de identificación por radiofrecuencia (RFID, por sus siglas en Inglés), identificadores similares a certificados almacenados en la clave y otras tecnologías de seguridad.

Al llegar a nuestro lugar de empleo, podríamos usar una tarjeta (algo que tiene) para ingresar al edificio, una vez más, un control de acceso físico.

Cuando nos sentamos frente a nuestra computadora en el trabajo y escribimos nuestra contraseña (algo que usted sabe), estamos autenticando y utilizando un sistema de control de acceso lógico para acceder a los recursos a los que se nos ha otorgado la misión. Dependiendo de los entornos por los que pasamos en el trabajo, ir a la escuela y realizar otras actividades que componen nuestro día, podemos tener más o menos exposición a los controles de acceso, pero la mayoría de nosotros vemos implementaciones múltiples como estas en un regularmente.

Control de acceso discrecional

El control de acceso discrecional (DAC, por sus siglas en Inglés) es un modelo de control de acceso basado en el acceso determinado por el propietario del recurso en cuestión. El propietario del recurso puede decidir quién tiene y quién no tiene acceso, y exactamente qué acceso tiene permitido tener. En los sistemas operativos de Microsoft, podemos ver DAC implementado. Si decidimos crear un recurso compartido de red, por ejemplo, podemos decidir a quién queremos permitir el acceso.

Control de acceso obligatorio

El control de acceso obligatorio (MAC, por sus siglas en Inglés) es un modelo de control de acceso en el que el propietario del recurso no puede decidir quién

accede a él, sino que el acceso lo decide un grupo o individuo que tiene la autoridad para establecer el acceso a los recursos. A menudo podemos encontrar MAC implementado en organizaciones gubernamentales, donde el acceso a un recurso determinado está en gran medida dictado por la etiqueta de sensibilidad aplicada (secreto, alto secreto, etc.), por el nivel de información confidencial que el individuo tiene permitido acceder (tal vez solo secreto), y si el individuo realmente necesita acceder al recurso, como discutimos cuando hablamos sobre el principio de privilegio mínimo al principio de este capítulo.

Control de acceso basado en roles

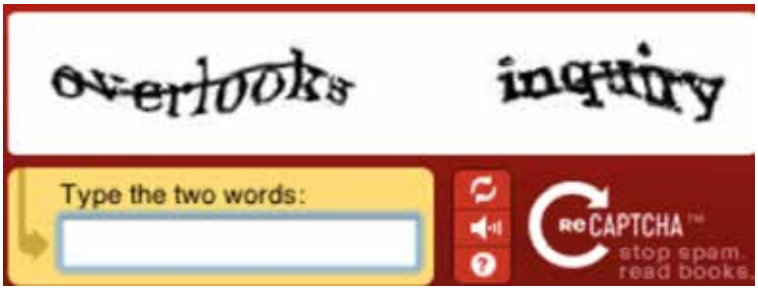
El control de acceso basado en roles (RBAC, por sus siglas en Inglés) es un modelo de control de acceso que, similar al MAC, funciona en los controles de acceso establecidos por una autoridad responsable de hacerlo, en lugar de por el propietario del recurso. La diferencia entre RBAC y MAC es que el control de acceso en RBAC se basa en el rol que desempeña el individuo al que se le otorga acceso. Por ejemplo, si tenemos un empleado cuya única función es ingresar datos en una aplicación en particular, a través de RBAC solo permitiríamos al empleado acceder a esa aplicación, independientemente de la sensibilidad o falta de sensibilidad de cualquier otro recurso que pueda potencialmente acceso. Si tenemos un empleado con una función más compleja (servicio al cliente para una aplicación minorista en línea, tal vez), la función del empleado puede requerir que tenga acceso a información sobre el estado de pago e información de los clientes, el estado del envío, pedidos anteriores y devoluciones, para poder ayudar a dichos clientes. En este caso, RBAC le otorgaría un acceso considerablemente mayor. Podemos ver RBAC implementado en muchas aplicaciones a gran escala que están orientadas a ventas o servicio al cliente.

Control de acceso basado en atributos

El control de acceso basado en atributos (ABAC, por sus siglas en Inglés) se basa lógicamente en atributos. Estos pueden ser los atributos de una persona en particular, de un recurso o de un entorno. Los atributos del sujeto son los de un individuo en particular. Podríamos elegir cualquier número de atributos, como el clásico control de acceso “debe alto para montarse”, que existe para evitar que personas muy altas monten en juegos de parques de atracciones ya que podrían ser perjudiciales para ellos. Otro ejemplo muy común se puede ver en el uso de un Captcha, como se muestra en la Figura 8. Los captchas se utilizan para controlar el acceso, en función de si la parte en el otro extremo puede pasar una prueba que, en teoría, es demasiado difícil de completar para una máquina, lo que demuestra

que la parte es humana. Captcha o, más propiamente, CAPTCHA, significa Prueba de Turing pública completamente automatizada para distinguir entre humanos y computadoras (Moradi y Keyvanpour, 2015).

Figura 8. Captcha común.



Fuente: elaboración propia.

Los atributos son aquellos que se relacionan con un recurso en particular, como un sistema operativo o una aplicación. A menudo vemos que esto ocurre, aunque generalmente por razones técnicas y no por razones de seguridad, cuando encontramos software que solo se ejecuta en un sistema operativo en particular, o sitios web que solo funcionan con ciertos navegadores. Podríamos aplicar este tipo de control de acceso como medida de seguridad al requerir el uso de software específico o protocolos particulares para la comunicación.

Los atributos ambientales se pueden usar para habilitar los controles de acceso que funcionan según las condiciones ambientales. Comúnmente usamos el atributo de tiempo para controlar el acceso, tanto en sentido físico como lógico, en función del tiempo transcurrido o la hora del día. Los controles de acceso en los edificios a menudo se configuran para permitir solo el acceso durante ciertas horas del día, como durante las horas de negocios. También vemos límites de tiempo establecidos en las conexiones VPN, lo que obliga al usuario a volver a conectarse cada 24 horas. Esto a menudo se hace para evitar que los usuarios mantengan dicha conexión ejecutándose después de que se haya eliminado su autorización para usarla. A menudo podemos encontrar ABAC implementado en sistemas de infraestructura como aquellos en entornos de red o telecomunicaciones.

Control de acceso multinivel

Los modelos de control de acceso multinivel se utilizan cuando los modelos de control de acceso más simples que acabamos de comentar no se consideran lo

suficientemente sólidos como para proteger la información a la que controlamos el acceso. Dichos controles de acceso son utilizados ampliamente por organizaciones militares y gubernamentales, o aquellos que a menudo manejan datos de naturaleza muy sensible. Podríamos ver modelos de seguridad multinivel utilizados para proteger una variedad de datos, desde secretos nucleares hasta información de los sistemas que gestionan información de salud de ciudadanos.

Control de acceso físico

Muchos de los métodos de control de acceso que hemos discutido a lo largo del capítulo pueden aplicarse a la seguridad física, así como a la seguridad lógica. Cuando se trate Con los controles de acceso físico, a menudo nos preocupa en gran medida controlar el acceso de personas y vehículos.

El control de acceso para individuos a menudo gira en torno a controlar el movimiento dentro y fuera de los edificios o instalaciones. Podemos ver ejemplos simples de tales controles en los edificios de muchas organizaciones en forma de insignias que moderan la apertura de puertas dentro o dentro de las instalaciones (algo que tiene, del Capítulo 2). Dichas insignias generalmente se configuran en una ACL que permite o niega su uso para ciertas puertas y regula la hora del día en que se pueden usar.

Uno de los problemas más comunes con los controles de acceso físico es el de seguir de cerca. El seguimiento de cola ocurre cuando nos autenticamos en la medida de control de acceso físico, como usar una tarjeta, y luego otra persona nos sigue directamente sin autenticarse.

Un ejemplo mucho más complejo de este tipo de control de acceso con el que muchas personas están familiarizadas es el sistema de seguridad en uso en muchos aeropuertos. Particularmente después de los ataques terroristas del 11 de septiembre del 2001 en los Estados Unidos, hemos visto aumentar el nivel de seguridad en los aeropuertos, en gran parte orientado en la dirección de los controles de acceso. Una vez que ingresamos al sistema de seguridad del aeropuerto, debemos presentar una tarjeta de embarque e identificación (algo que tiene, dos veces). Por lo general, pasamos por una serie de pasos para asegurarnos de no llevar ningún dispositivo peligroso, una forma de control de acceso basado en atributos. Luego procedemos a nuestra puerta y, una vez más, presentamos nuestra tarjeta de embarque para subir al avión. Dichos procesos pueden variar ligeramente según el país en el que viajamos.

3.5. Resumen

La autorización es un paso clave en el proceso en el que trabajamos para permitir que las entidades accedan a los recursos, a saber, identificación, autenticación y autorización, en ese orden. Implementamos la autorización mediante el uso de controles de acceso, más específicamente mediante el uso de listas y capacidades de control de acceso, aunque estas últimas a menudo no se implementan por completo en la mayoría de los sistemas operativos comunes en uso en la actualidad.

Los detalles del control de acceso se definen a través de los diversos modelos que utilizamos al armar tales sistemas. A menudo vemos el uso del acceso más simple modelos de control tales como control de acceso discrecional, control de acceso obligatorio, control de acceso basado en roles y control de acceso basado en atributos en nuestra vida diaria

Los conceptos de control de acceso en general se aplican en gran medida a las áreas lógicas y físicas, pero vemos algunas aplicaciones especializadas cuando se observa específicamente el control de acceso físico. Aquí tenemos varios conjuntos de controles de acceso que se aplican para garantizar que las personas y los vehículos no puedan entrar o entrar en áreas donde no están autorizados. Podemos ver ejemplos de dichos controles en nuestra vida diaria en edificios de oficinas, áreas de estacionamiento e instalaciones de alta seguridad en general.

3.6. Cuestionario de estudio

1. Discuta la diferencia entre autorización y control de acceso.
2. ¿Contra qué protege el modelo Clark-Wilson?
3. ¿Por qué el control de acceso basado en la dirección MAC de los sistemas en nuestra red no representa una fuerte seguridad?
4. ¿Qué debe tener lugar primero, autorización o autenticación?
5. ¿Cuáles son las diferencias entre MAC y DAC en términos de acceso?
6. Investigue modelos de control de acceso multi nivel.
7. Dado un archivo que contiene datos confidenciales y que reside en un sistema operativo Linux, con los permisos para rw-rw-rw podría causar un problema potencial de seguridad, si es así ¿Cuáles pilares de la tríada de la CIA podrían verse afectadas?
8. ¿Qué tipo de control de acceso se usaría en el caso en que deseamos

evitar que los usuarios inicien sesión en sus cuentas después del horario comercial?

9. ¿Cuáles son algunas de las diferencias entre las listas y capacidades de control de acceso?

CAPÍTULO IV: RESPONSABILIDAD Y AUDITORIAS

Cuando hemos superado con éxito el proceso de identificación, autenticación y autorización, o incluso mientras todavía estamos en el proceso, debemos realizar un seguimiento de las actividades que han tenido lugar, es decir se debe garantizar la trazabilidad. A pesar de que podríamos haber permitido que la parte tenga acceso a nuestros recursos, aún debemos asegurarnos de que se comporten de acuerdo con las reglas en lo que respecta a las políticas de seguridad, la conducta empresarial, la ética, el acoso sexual, entre otros.

Actualmente, garantizar que se cumpla con las reglas establecidas en entorno digital-empresarial para su uso se ha convertido en una tarea vital. Ahora almacenamos una gran cantidad de información en forma digital, incluidos datos médicos, información financiera, procedimientos legales, secretos comerciales, datos crudos de investigaciones, entre otra variedad de información. Si no establecemos y seguimos reglas estrictas para el acceso a datos confidenciales almacenados de esta manera, podemos sufrir pérdidas comerciales, robo de propiedad intelectual, robo de identidad, fraude y muchos otros delitos. Algunos tipos de datos, médicos y financieros, por ejemplo, a menudo gozan de protección por ley en varios países y los delitos se encuentran tipificados ya en la legislación de muchos países.

Las auditorías se realizan para garantizar que se cumpla con las leyes, políticas y otros cuerpos de control administrativo aplicables. Podemos auditar una variedad de actividades, incluido el cumplimiento de la política, la arquitectura de seguridad adecuada, la configuración de la aplicación, el comportamiento personal u otras actividades o configuraciones (Fernández y Casas, 2017).

4.1. Responsabilidad

La responsabilidad tiene un papel muy importante pues nos proporciona los medios para dar trazabilidad a las actividades en nuestro entorno hasta su origen. Además, nos proporciona una serie de capacidades, cuando se implementan adecuadamente, que pueden ser de gran utilidad para llevar a cabo los negocios diarios de seguridad y tecnología de la información en nuestras organizaciones. En particular, las organizaciones necesitan mantener cuidadosamente la responsabilidad para garantizar que se cumplen con las leyes o regulaciones asociadas con los tipos de datos que manejan, o la industria en la que operan.

La responsabilidad depende de que la identificación, la autenticación y el control de acceso que estén presentes para que podamos saber con quién está asociada una

transacción determinada y qué permisos se usaron para permitirles llevarla a cabo. Dada la supervisión y el registro adecuados, a menudo podemos hacer exactamente esto y determinar, en muy poco tiempo, los detalles de la situación en cuestión.

En algunos sentidos el monitoreo excesivo de personas, lugares y cosas puede indicar un ambiente poco saludable y además hay que tener cuidado con la legislación vigente en temas de privacidad y protección de datos de la persona. También podemos ir demasiado lejos en la otra dirección. Si no tenemos suficientes controles para disuadir o prevenir aquellos que violen las reglas y abusen de los recursos a los que tienen acceso, también podemos terminar en un mal lugar.

Aunque la violación puede no ser inmediatamente visible para aquellos fuera de la organización, o nunca visible, para el caso, todavía somos responsables de cumplir con las leyes que rigen las violaciones en nuestra ubicación y con las leyes que rigen el manejo de los datos con los que hacemos negocios. En el caso de que no nos comportemos adecuadamente en relación con estas leyes, es posible que podamos continuar con los negocios como de costumbre por un período de tiempo, pero eventualmente seremos descubiertos y las repercusiones en lo personal, comercial y los sentidos legales serán mucho mayores por no haber manejado la situación adecuadamente en primer lugar.

La implementación de la responsabilidad a menudo trae consigo una serie de características útiles desde una perspectiva de seguridad. Cuando implementamos el monitoreo y el registro en nuestros sistemas y redes, podemos usar esta información para mantener una postura de seguridad más alta de lo que podríamos lograr de otra manera. Específicamente, las herramientas que nos permiten la rendición de cuentas también permiten no repudiar, disuadir a quienes abusarían de nuestros recursos, ayudarnos a detectar y prevenir intrusiones y ayudarnos a preparar materiales para procedimientos legales (Tejada, 2019).

No repudio

El no repudio se refiere a una situación en la que existe evidencia suficiente para evitar que un individuo niegue con éxito que él o ella ha hecho una declaración o ha tomado una acción. En la configuración de seguridad de la información, esto puede ser logrado en una variedad de formas. Es posible que podamos presentar pruebas de la actividad directamente desde los registros del sistema o de la red, o recuperar dicha prueba mediante el uso de un examen forense digital del sistema o dispositivos involucrados. También podemos establecer la no repudio mediante el uso de tecnologías de cifrado, más específicamente mediante el uso de funciones

hash que se pueden usar para firmar digitalmente una comunicación o un archivo. Discutiremos tales métodos con una extensión considerablemente mayor en el Capítulo 5 cuando veamos el cifrado. Un ejemplo de esto podría ser un sistema que firma digitalmente cada correo electrónico que se envía desde él, lo que hace inútil cualquier negación que pueda tener lugar con respecto al envío del mensaje en cuestión (Zambrano y Valencia, 2017).

Disuasión

La responsabilidad también puede ser un gran elemento de disuasión contra el mal comportamiento en nuestros entornos. Si los que monitoreamos están al tanto de este hecho, y se les ha comunicado que habrá sanciones por actuar en contra de las reglas, estas personas pueden pensarlo dos veces antes de desviarse de las líneas.

La clave para la disuasión radica en dejar que aquellos que queremos disuadir sepan que serán responsables de sus acciones. Esto se lleva a cabo típicamente a través de la auditoría y monitoreo, los cuales discutiremos en la sección "Auditoría" de este capítulo. Si no lo aclaramos, nuestro elemento disuasorio perderá la mayor parte de su fuerza.

Por ejemplo, si, como parte de nuestras actividades de monitoreo, realizamos un seguimiento de los tiempos de acceso de la tarjeta de ingreso para cuando nuestros empleados entran y salen de nuestras instalaciones, podemos validar esta actividad contra los tiempos que han enviado en su control de ingreso (algunas empresas utilizan esto hoy día) para cada semana, para evitar que nuestros empleados falsifiquen su tarjeta de tiempo y defrauden a la empresa por un pago adicional y no merecido. Si bien esto puede parecer una especie de abuso para algunos, tales métodos a menudo se usan en áreas con un gran número de empleados que trabajan turnos específicos, como los que tienen mesas de ayuda de soporte técnico o centros de llamadas.

Detección y prevención de intrusiones

Una de las motivaciones detrás del registro y monitoreo en nuestros entornos es detectar y prevenir intrusiones tanto en el sentido lógico como físico. Si implementamos alertas basadas en actividades inusuales en nuestros entornos y verificamos la información que hemos registrado regularmente, tenemos muchas más posibilidades de detectar ataques en curso y prevenir aquellos para los que podemos ver los precursores. Particularmente en el ámbito lógico donde los ataques pueden tener lugar en fracciones de segundo, también sería prudente implementar

herramientas automatizadas para llevar a cabo tales tareas. Podemos dividir dichos sistemas en dos categorías principales: sistemas de detección de intrusos (IDS, por sus siglas en Inglés) y sistemas de prevención de intrusos (IPS, por sus siglas en Inglés). Un IDS se utiliza estrictamente como una herramienta de monitoreo y alerta, solo notificándonos que un ataque o actividad indeseable está teniendo lugar. Un IPS, que a menudo funciona a partir de la información enviada por el IDS, en realidad puede tomar medidas en función de lo que sucede en el entorno. En respuesta a un ataque a través de la red, un IPS puede rechazar el tráfico desde la fuente del ataque. Discutiremos IDS e IPS con mayor detalle en capítulos siguientes.

Admisibilidad de registros

Cuando buscamos introducir registros en entornos legales, a menudo es mucho más fácil hacerlo y aceptarlos cuando se producen a partir de un sistema de seguimiento regulado y consistente. Por ejemplo, si buscamos presentar evidencia forense digital que hemos reunido para su uso en un caso judicial, la evidencia probablemente no será admisible a la corte a menos que podamos proporcionar una cadena de custodia sólida y documentada para dicha evidencia. Necesitamos poder mostrar dónde estuvo la evidencia en todo momento, cómo pasó exactamente de una persona a otra, cómo se protegió mientras estaba almacenada, entre otros aspectos (Urbina, 2016).

Con suerte, nuestros métodos de responsabilidad para la recopilación de evidencia, si se siguen adecuadamente, nos permitirán mostrar esta cadena de custodia ininterrumpida. Si no podemos demostrar esto, nuestras pruebas probablemente solo se tomarán como rumores, en el mejor de los casos, debilitarán considerablemente nuestro caso y quizás nos colocarán en el lado perdedor en la corte.

¿Cómo logramos la responsabilidad?

Como hemos discutido, podemos intentar garantizar la rendición de cuentas estableciendo las reglas y garantizando que se cumplan. Si bien es bueno darle una regla a alguien y pedirle que la cumpla, a menudo tendremos que tomar medidas adicionales para asegurarnos de que esto se esté cumpliendo. Podemos ver exactamente ese mecanismo en funcionamiento en el mundo de la aplicación de la ley. El área geográfica en la que vivimos ha establecido ciertas leyes para que su población las cumpla. A menudo, podemos encontrar leyes que rigen el robo, el daño a terceros, la operación segura de vehículos, el tratamiento de los datos personales y muchos más. Luego tenemos policías que garantizan el cumplimiento de estas leyes, tanto de forma reactiva como proactiva. En el mundo de la seguridad

de la información, a menudo utilizamos las herramientas tecnológicas para llevar a cabo tareas similares.

4.2. Auditoria

Una de las principales formas en que podemos garantizar la responsabilidad a través de medios digitales es asegurando que tengamos registros precisos de quién hizo qué y cuándo lo hicieron. En casi cualquier entorno, desde el nivel más bajo de tecnología hasta el más alto, la responsabilidad se logra en gran medida mediante el uso de auditorías de alguna variedad. Auditamos por una de varias razones. La auditoría nos proporciona los datos con los que podemos implementar la responsabilidad. Si no tenemos la capacidad de evaluar nuestras actividades durante un período de tiempo, no tenemos la capacidad de facilitar la responsabilidad a gran escala. Particularmente en organizaciones más grandes, nuestra capacidad de auditoría equivale directamente a nuestra capacidad de responsabilizar a cualquier persona por cualquier cosa (Tejada, 2019).

También podemos estar obligados por requisitos contractuales o normativos que nos obligan a estar sujetos a auditorías de algún modo recurrente. En muchos casos, dichas auditorías son realizadas por terceros independientes, certificados y autorizados para realizar dicha tarea. Los buenos ejemplos de tales auditorías financieras-contables, que existen para garantizar que las empresas reporten honestamente sus resultados financieros.

¿Qué auditamos?

Cuando realizamos una auditoría, hay una serie de elementos que podemos examinar, principalmente centrados en el cumplimiento de las leyes y políticas relevantes. En el mundo de la seguridad de la información, tendemos a ver el acceso desde los sistemas como un enfoque principal, pero a menudo también lo extendemos a otros campos, como la seguridad física.

Las contraseñas son un elemento auditado comúnmente, ya que deberíamos establecer una política para dictar cómo se construyen y usan. Como discutimos en la sección “Autenticación” en el Capítulo 2, si no nos ocupamos de construir contraseñas de manera segura, un atacante puede descifrarlas fácilmente. También deberíamos preocuparnos por la frecuencia con la que se cambian las contraseñas. Si tenemos una contraseña que cae en manos de alguien que no debería tenerla, queremos cambiar la contraseña en un intervalo relativamente frecuente para garantizar que esta persona no tenga acceso permanente. En muchos casos, la comprobación de la

seguridad de la contraseña y la gestión de los cambios de contraseña se realizan de forma automática mediante funciones dentro de un sistema operativo o mediante utilidades diseñadas para hacerlo.

La licencia de software es otro tema de auditoría común. Particularmente en los sistemas propiedad de la organización para la cual trabajamos, asegurar que todo nuestro software tenga la licencia adecuada es una tarea importante. Si una agencia externa nos auditara y se descubriera que ejecutamos grandes cantidades de software sin licencia, las sanciones financieras podrían ser severas. A menudo es mejor si podemos encontrar y corregir tales asuntos nosotros mismos antes de recibir una notificación de una empresa externa.

El uso de Internet es un elemento auditado muy comúnmente en las organizaciones, a menudo centrado en gran medida en nuestras actividades en la Web, aunque puede incluir mensajes instantáneos, correo electrónico, transferencias de archivos u otras transacciones. En muchos casos, las organizaciones han configurado servidores proxy para que todo ese tráfico se canalice a través de unas pocas puertas de enlace para permitir el registro, el escaneo y el posible filtrado de dicho tráfico. Dichas herramientas nos pueden dar la capacidad de examinar cómo se están utilizando exactamente esos recursos y de tomar medidas si se están utilizando de forma incorrecta.

Muchas organizaciones, como hemos mencionado a lo largo de este capítulo, manejan datos de naturaleza sensible. Particularmente en el caso de los datos que la ley exige que se protejan, siendo los datos médicos un buen ejemplo, debemos tomar medidas para asegurarnos de que estamos cumpliendo con las medidas de seguridad que debemos tener vigentes. En particular, a menudo estamos obligados a garantizar que los accesos a dichos datos se realicen de manera autorizada, que se cumplan los requisitos de retención de datos durante un período de tiempo y que los datos se destruyan de forma segura cuando ya no sean necesarios. Tales datos a menudo se alojan en una variedad de bases de datos, la mayoría de las cuales tienen instalaciones integradas para controlar y monitorear el acceso a un nivel muy granular.

Inicio sesión

Las bitácoras nos dan un historial de las actividades que han tenido lugar en el entorno que se registra. Por lo general, generamos registros bitácoras de forma automatizada en los sistemas operativos y hacemos un seguimiento de las actividades que tienen lugar en la mayoría de los equipos de computación, redes y telecomunicaciones,

así como en la mayoría de los dispositivos que pueden considerarse remotamente incorporados o conectados un ordenador. El registro es una herramienta reactiva, ya que nos permite ver el registro de lo que sucedió después de que haya tenido lugar. Para reaccionar de inmediato a algo que está sucediendo, necesitaríamos usar una herramienta más similar a un IDS / IPS.

Los mecanismos de registro a menudo son configurables y se pueden configurar para registrar cualquier cosa, desde eventos críticos, lo cual es típico, hasta cada acción realizada por el sistema o el software, que generalmente solo se realiza para solucionar problemas cuando vemos un problema. A menudo encontraremos eventos como errores de software, fallas de hardware, usuarios que inician o cierran sesión, acceso a recursos y tareas que requieren mayores privilegios en la mayoría de los registros, según la configuración de registro y el sistema en cuestión.

Por lo general, los registros solo están disponibles para que los administradores del sistema los revisen y, por lo general, los usuarios del sistema no los pueden modificar, tal vez con la excepción de escribirles. Es muy importante tener en cuenta que recopilar registros sin revisarlos es una tarea bastante inútil. Si nunca revisamos el contenido de los registros, bien podríamos no haberlos recopilado en primer lugar. Es importante que programemos una revisión periódica de nuestros registros para detectar cualquier contenido inusual en su contenido.

También se nos puede pedir que analicemos el contenido de los registros en relación con un incidente o situación en particular. Este tipo de actividades a menudo recae en el personal de seguridad en el caso de investigaciones, incidentes y verificaciones de cumplimiento. En estos casos, esto puede ser una tarea difícil si el período de tiempo en cuestión es mayor que unos pocos días. Incluso buscar el contenido de un registro relativamente simple, como el generado por un servidor proxy web, puede significar examinar enormes cantidades de datos de uno o más servidores. En tales casos, los scripts personalizados o incluso una herramienta como grep pueden ser invaluables para realizar tales tareas en un período de tiempo razonable.

Monitoreo

El monitoreo es un subconjunto de la auditoría y tiende a enfocarse en observar información sobre el ambiente que se está monitoreando para descubrir condiciones indeseables como fallas, escasez de recursos, problemas de seguridad y tendencias que pueden indicar la llegada de tales condiciones. El monitoreo es en gran medida una actividad reactiva, con acciones tomadas en función de los datos recopilados, generalmente de registros generados por varios dispositivos. Aunque podríamos

considerar que la parte del análisis de tendencias de la tala es una actividad proactiva, todavía estamos reaccionando a las circunstancias actuales para evitar condiciones peores que las que vemos en la actualidad (Fernández y Casas, 2017).

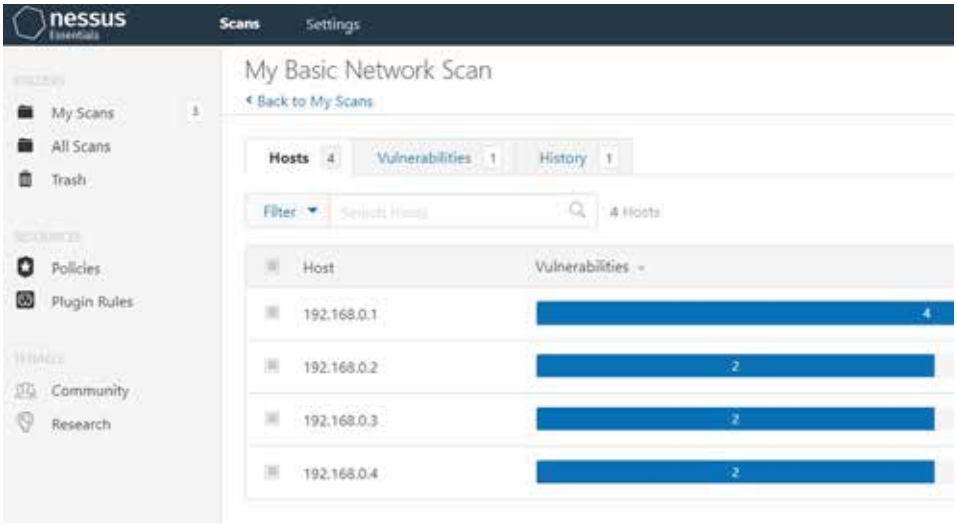
Cuando realizamos el monitoreo, generalmente observamos elementos de datos específicos que hemos recopilado, como el uso de recursos en las computadoras, la latencia de la red, tipos particulares de ataques que ocurren repetidamente contra servidores con interfaces de red que están expuestos a Internet, el tráfico que pasa a través de nuestro sistema físico. controles de acceso en momentos inusuales del día, y así sucesivamente. En reacción a tal actividad que ocurre en niveles superiores a lo que normalmente esperamos, llamado nivel de recorte, nuestro sistema de monitoreo podría estar configurado para enviar una alerta a un administrador del sistema o personal de seguridad física, o podría desencadenar una acción más directa para mitigar el problemas como dejar caer el tráfico desde una dirección IP particular, cambiar a un sistema de respaldo para un servidor crítico, convocar a funcionarios encargados de hacer cumplir la ley u otras tareas similares.

Evaluaciones

En algunos casos, nuestras auditorías pueden tomar una ruta más activa para determinar si todo es como debería ser y si cumple con las leyes, regulaciones o políticas relevantes. En tales casos, podemos encontrar útil examinar cuidadosamente nuestros entornos en busca de vulnerabilidades. Podemos adoptar dos enfoques principales para tales actividades: evaluaciones de vulnerabilidad y pruebas de penetración. Si bien estos términos se usan indistintamente, en realidad son dos conjuntos distintos de actividades.

Las evaluaciones de vulnerabilidad generalmente implican el uso de herramientas de escaneo de vulnerabilidades, como Nessus, tal y como se muestra en la Figura 9, que permite detectar vulnerabilidades. Dichas herramientas generalmente funcionan escaneando los sistemas de destino para descubrir qué puertos están abiertos en ellos y luego interrogando cada puerto abierto para averiguar exactamente qué servicio está escuchando en el puerto en cuestión. Dada esta información, la herramienta de evaluación de vulnerabilidad puede consultar su base de datos de información de vulnerabilidad para determinar si puede haber alguna vulnerabilidad presente. Aunque las bases de datos de tales herramientas tienden a ser bastante exhaustivas, los ataques más nuevos o aquellos que los atacantes usan con moderación a menudo se les escapan (Vega, 2020).

Figura 9. Interfaz web de Nessus Essentials.



Fuente: elaboración propia.

Como un método más activo para encontrar agujeros de seguridad, es posible que también deseemos realizar pruebas de penetración. Las pruebas de penetración, aunque pueden utilizar la evaluación de vulnerabilidades como punto de partida, llevan el proceso varios pasos más allá. Cuando realizamos una prueba de penetración, imitamos, lo más cerca posible, las técnicas que usaría un atacante real. Podemos intentar recopilar información adicional sobre el entorno objetivo de los usuarios u otros sistemas cercanos, explotar fallas de seguridad en aplicaciones basadas en la Web o bases de datos conectadas a la Web, realizar ataques a través de vulnerabilidades sin parches en aplicaciones o sistemas operativos, o métodos similares.

El objetivo final en la realización de evaluaciones de cualquier tipo es encontrar y corregir vulnerabilidades antes de que lo hagan los atacantes. Si podemos hacerlo con éxito y de forma recurrente, aumentaremos considerablemente nuestra postura de seguridad y tendremos muchas más posibilidades de resistir los ataques. Al igual que con cualquier medida de seguridad que podamos implementar, las evaluaciones de seguridad de la información son solo un componente único en nuestra estrategia defensiva global y transversal en el modelo de seguridad en profundidad.

4.3. Resumen

Cuando permitimos que otros accedan a los recursos en los que se basan nuestros negocios, o información personal de naturaleza sensible, necesitamos

responsabilizarlos por lo que hacen con los recursos o la información. La responsabilidad y la rendición de cuentas puede ser un requisito para las organizaciones, dependiendo de los datos que manejen y de la industria en la que operan.

La auditoría es el proceso por el que pasamos para garantizar que nuestro entorno cumpla con las leyes, normativa, estándares internacionales, reglamentos y políticas que lo vinculan. La auditoría también es el mecanismo a través del cual podemos implementar la responsabilidad. Podemos llevar a cabo una variedad de tareas en nombre de la auditoría, incluido el registro, el monitoreo, las evaluaciones y similares.

Con el fin de respaldar las actividades de auditoría, rendición de cuentas y monitoreo, a menudo realizamos registros en muchos de los dispositivos de nuestro entorno. Dichos registros a menudo son generados por software, dispositivos informáticos y otro hardware conectado a las computadoras. Los registros generados por los dispositivos pueden ser de naturaleza muy general y contener solo una cantidad limitada de información, o pueden ser muy específicos y contener grandes cantidades de información altamente detallada.

En función de los datos que recopilamos de los sistemas, también podemos realizar monitoreos en nuestros entornos organizacionales. El monitoreo nos permite tomar medidas sobre las actividades en el período posterior a su ocurrencia, que puede ir desde la identificación de tendencias en el funcionamiento de nuestros sistemas hasta la toma de medidas para bloquear los ataques muy rápidamente después de que se hayan identificado por primera vez.

4.4. Cuestionario de estudio

1. ¿ Cuál es el beneficio de iniciar sesión?
2. Discuta la diferencia entre autenticación y responsabilidad.
3. Describa detalladamente el no repudio.
4. Nombre cinco elementos que deseáramos auditar en nuestro entorno.
5. ¿Por qué es importante la responsabilidad cuando se trata con datos sensibles?
6. ¿Por qué podría ser una buena idea auditar nuestro software instalado?

7. Cuando se trata de cuestiones legales o regulatorias ¿Por qué necesitamos responsabilidad?
8. ¿Cuál es la diferencia entre evaluación de vulnerabilidad y pruebas de penetración?
9. ¿Qué impacto puede tener la responsabilidad en la admisibilidad de la evidencia en casos judiciales?
10. Dado un entorno de TI que contiene servidores que manejan datos confidenciales del cliente, algunos de los cuales están expuestos a Internet ¿Querríamos realizar una evaluación de vulnerabilidad, una prueba de penetración o ambas? ¿Por qué?

CAPÍTULO V: SEGURIDAD FÍSICA

La seguridad física se ocupa en gran medida de la protección de tres categorías principales de activos: personas, equipos y datos. Nuestra principal preocupación, por supuesto, es proteger a las personas. Las personas son considerablemente más difíciles de reemplazar que los equipos o los datos, particularmente cuando tienen experiencia en su campo particular y están familiarizados con los procesos y tareas que realizan.

El siguiente en orden de prioridad de protección son nuestros datos. Si lo hemos planeado y preparado con suficiente antelación, deberíamos poder proteger fácilmente nuestros datos de cualquier desastre que no sea de escala global. Si no nos preparamos para tal problema, podemos perder fácilmente nuestros datos de forma permanente.

Por último, protegemos nuestro equipo y las instalaciones que lo albergan. Esto puede parecer un conjunto muy importante de objetos a los que podríamos querer asignarles un mayor nivel de prioridad al planificar nuestras medidas de seguridad física, sin embargo, este generalmente no es el caso, fuera de algunas situaciones, la mayoría de las cuales en realidad giran en torno a mantener a las personas seguras. En el mundo de la tecnología, gran parte del hardware que utilizamos es relativamente genérico y fácil de reemplazar. Incluso si estamos utilizando equipos más especializados, a menudo podemos reemplazarlo en cuestión de días o semanas.

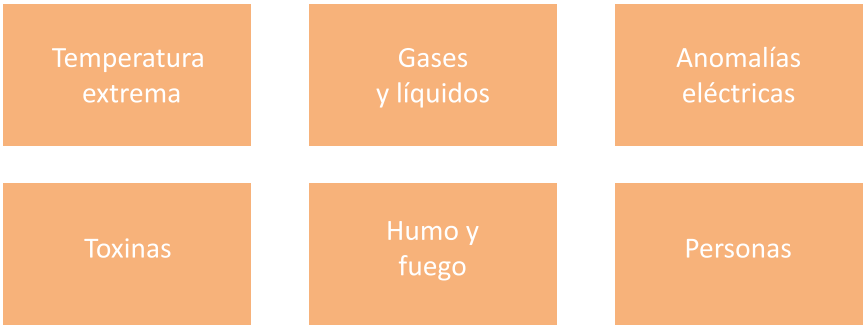
Es importante indicar que, aunque discutiremos la protección de personas, datos y equipos como conceptos separados en este capítulo, en realidad están estrechamente integrados. Por lo general, no podemos y no debemos desarrollar planes de seguridad que protejan cualquiera de estas categorías de forma aislada de las demás.

En muchas organizaciones más grandes, la protección de personas, datos y equipos está cubierta por un conjunto de políticas y procedimientos que se denominan colectivamente planificación de continuidad de negocio (BCP, por sus siglas en Inglés) y planificación de recuperación de desastres (DRP, por sus siglas en Inglés). BCP se refiere específicamente a los planes que implementamos para garantizar que las funciones comerciales críticas puedan continuar en un estado de emergencia. DRP cubre los planes que implementamos para prepararnos ante un desastre potencial, y qué haremos exactamente durante y después de un desastre en particular.

Las amenazas que enfrentamos cuando nos preocupa la seguridad física generalmente

se dividen en algunas categorías principales, como se enumeran aquí y se muestran en la Figura 10:

Figura 10. Categorías principales de amenazas físicas.

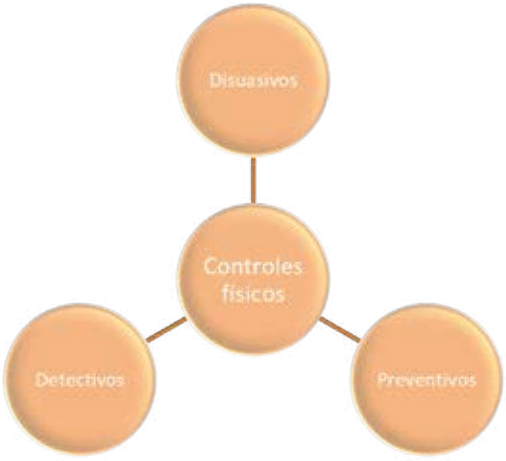


Fuente: elaboración propia.

5.1. Controles de seguridad física

Los controles de seguridad física son los dispositivos, sistemas, personas y otros métodos que implementamos para garantizar nuestra seguridad en un entorno físico. Hay tres tipos principales de controles físicos: disuasivos, detectives y preventivos, como se muestra en la Figura 11. Cada uno tiene un enfoque diferente, pero ninguno es completamente distinto y está separado de los demás, como veremos más adelante. Además, estos controles funcionan mejor cuando se usan en concierto. Cualquiera de ellos no es suficiente para garantizar nuestra seguridad física en la mayoría de las situaciones.

Figura 11. Tipos de controles de seguridad física.



Fuente: elaboración propia.

Disuasivos

Los controles de disuasión están diseñados para desalentar a aquellos que buscan violar nuestros controles de seguridad de hacerlo. Se puede considerar una variedad de controles para ser un elemento disuasivo, incluidos, como discutimos anteriormente en esta sección, varios que se superponen con las otras categorías. En el sentido de controles detectivos puros, podemos señalar elementos específicos que pretenden indicar que otros controles pueden estar en su lugar.

Ejemplos de esto incluyen letreros en lugares públicos que indican que el hay cámaras de seguridad en el sitio y los letreros con logotipos de compañías de alarmas que podemos encontrar en áreas residenciales. Los signos en sí mismos no hacen nada para evitar que las personas actúen de manera indeseable, pero señalan que puede haber consecuencias por hacerlo. Estas medidas, si bien no se suman directamente a lo que podríamos considerar seguridad física, ayudan a mantener honestas a las personas honestas.

También podemos ver que las medidas de seguridad en las otras categorías tienen doble función como elementos disuasivos. Si tenemos medidas de seguridad obvias en el lugar que son visibles para aquellos que quieran violar nuestra seguridad, como guardias, perros, áreas bien iluminadas, cercas y otras medidas similares, nuestro posible criminal podría decidir que somos demasiado difíciles.

Detectivos

Los controles detectivos sirven para detectar e informar eventos indeseables que están ocurriendo. El ejemplo clásico de un control de este tipo se puede encontrar en alarmas antirrobo y sistemas de detección de movimientos. Tales sistemas típicamente monitorean en busca de indicadores de actividad no autorizada, tales como puertas o ventanas que se abren, vidrios rotos, movimiento y cambios de temperatura, y también pueden estar en su lugar para monitorear condiciones ambientales no deseadas como inundaciones, humo y fuego, cortes eléctricos, exceso de dióxido de carbono en el aire, y así sucesivamente.

También podemos ver sistemas detectivos en forma de guardias humanos o animales, ya sea que estén patrullando físicamente un área o monitoreando de segunda mano mediante el uso de tecnología como los sistemas de cámaras. Este tipo de monitoreo tiene puntos buenos y malos, ya que un ser vivo puede estar técnicamente menos enfocado que un sistema electrónico, pero tiene el potencial de distraerse y deberá ser relevado para las comidas, los descansos en el baño y otras actividades similares.

Además, podemos escalar tales guardias desde el guardia de seguridad desarmado más humilde hasta las fuerzas de seguridad altamente capacitadas y bien armadas, según sea apropiado para la situación. Como es cierto para la mayoría de las implementaciones que involucran seguridad, el principio de defensa en profundidad, como discutimos en el Capítulo 1, se aplica aquí.

Preventivos

Los controles preventivos se utilizan para evitar físicamente que entidades no autorizadas infrinjan nuestra seguridad física. Un excelente ejemplo de seguridad preventiva se puede encontrar en la simple cerradura mecánica. Las cerraduras son casi omnipresentes para asegurar varias instalaciones contra la entrada no autorizada, incluidas empresas, residencias y otros lugares. Además de las cerraduras, también podemos ver controles preventivos en forma de cercas altas, bolardos (los postes pintados de colores brillantes y rellenos de cemento que se colocan para evitar que los vehículos ingresen a los edificios) y, una vez más, los guardias y los perros. También podemos ver controles preventivos enfocados específicamente en personas, vehículos u otras áreas particulares de preocupación, dependiendo del entorno en cuestión.

¿Cómo usamos los controles de acceso físico?

Los controles preventivos son generalmente el núcleo de nuestros esfuerzos de seguridad y, en algunos casos, pueden ser la única iniciativa de seguridad física que se encuentre en funcionamiento. Podemos ver esto comúnmente en residencias, donde hay cerraduras en las puertas, pero no hay sistemas de alarma ni ninguna otra medida que pueda disuadir a un delincuente de ingresar sin autorización.

En las instalaciones comerciales, es mucho más probable que veamos implementados los tres tipos de controles, en forma de cerraduras, sistemas de alarma y letreros que indican la presencia de los sistemas de alarma. Siguiendo los principios de defensa en profundidad, cuantas más capas apliquemos para la seguridad física, mejor estaremos.

Otra consideración importante en la implementación de la seguridad física es solo establecer una seguridad que sea razonablemente consistente con el valor de lo que estamos protegiendo. Si tenemos un almacén vacío, no tiene sentido instalar cerraduras de alta seguridad, sistemas de alarma y guardias armados. Del mismo modo, si tenemos una casa llena de computadoras y dispositivos electrónicos caros, no tiene sentido equiparla con cerraduras baratas y renunciar por completo a un

sistema de alarma.

5.2. Protegiendo a las personas

La principal preocupación de la seguridad física es proteger a las personas de las que depende nuestro negocio y a las personas cercanas a nosotros. Si bien implementamos medidas de seguridad y sistemas de respaldo para garantizar que nuestras instalaciones, equipos y datos permanezcan en condiciones funcionales, si perdemos a las personas de las que dependemos para trabajar con los equipos y los datos, tenemos un problema bastante difícil de resolver. En muchos casos, podemos restaurar nuestros datos de las copias de seguridad, podemos construir nuevas instalaciones si se destruyen o dañan, y podemos comprar nuevos equipos; pero reemplazar a personas con experiencia más allá de la una o dos a la vez que encontramos con una rotación normal es difícil, si no imposible, dentro de un período de tiempo razonable.

Preocupaciones físicas para las personas

Como las personas son bastante frágiles en comparación con los equipos, pueden ser susceptibles a casi todo el alcance de las amenazas que discutimos al comienzo de este capítulo. Las temperaturas extremas, o incluso temperaturas no tan extremas, pueden hacer que una persona se sienta muy incómoda, en el mejor de los casos. En el caso de líquidos, gases o toxinas, la ausencia, presencia o proporciones incorrectas de una variedad de ellos puede ser perjudicial para las personas.

Del mismo modo la falta de un gas como el oxígeno, o demasiado, puede ser mortal para las personas muy rápidamente. Aunque podemos ver muy claramente de dónde proviene el daño de una toxina que se introduce en un ambiente, es posible que ya existan varias sustancias comunes, pero que no son tóxicas en las cantidades o mezclas en las que se usan comúnmente. Podríamos ver que ciertas sustancias químicas son beneficiosas cuando se usan para filtrar el agua en nuestras instalaciones, pero lo mismo podría no ser cierto si se cambian las proporciones o mezclas químicas (De la Rocha *et al.*, 2017).

Cualquier variedad de organismos vivos puede ser peligrosa para las personas, desde animales más grandes, hasta insectos, hasta mohos, hongos u otros organismos microscópicos casi invisibles. Las personas pueden sufrir el contacto con organismos vivos de varias maneras, desde ser mordidos o picados por varios bichos, hasta desarrollar problemas respiratorios por inhalar moho.

El movimiento puede ser muy perjudicial para las personas, particularmente

cuando dicho movimiento es el resultado de un terremoto, deslizamiento de tierra, avalancha, problemas estructurales del edificio u otros problemas similares. En la mayoría de los casos, tales amenazas pueden ser muy dañinas y difíciles de proteger.

Las anomalías energéticas son, por supuesto, muy peligrosas para las personas. Podríamos encontrar equipos con blindaje o aislamiento mal mantenido, o fallas mecánicas y / o eléctricas que podrían exponer a las personas a microondas, electricidad, ondas de radio, luz infrarroja, radiación u otras emisiones dañinas. Los resultados de tales exposiciones pueden ser inmediatamente obvios, en el caso de una descarga eléctrica, o pueden ser a largo plazo, en el caso de exposición a la radiación.

Las personas, por supuesto, son una de las amenazas más severas contra otras personas. Hay una cantidad infinitamente variable de formas en que otras personas pueden causarnos problemas mientras planificamos la seguridad de los nuestros. Podríamos encontrar disturbios civiles como una posibilidad real en ciertas partes del mundo. Podríamos encontrar ataques de ingeniería social, en un esfuerzo por extraer información de nuestro personal o para obtener acceso no autorizado a instalaciones o datos a través de ellos. Nuestra gente podría ser atacada físicamente en un estacionamiento oscuro, o sometida a otras circunstancias similares.

El humo y el fuego también pueden ser muy peligrosos para las personas en el sentido de quemaduras, inhalación de humo, problemas de temperatura y otros problemas similares. Particularmente en el caso de grandes instalaciones, el humo y el fuego pueden hacer que el diseño físico del área sea muy confuso o impasible, y puede hacer que sea muy difícil para nuestro personal caminar hacia la seguridad. También podemos ver el problema compuesto por suministros, infraestructura o el tejido del edificio en sí mismo, reaccionando de manera desfavorable y liberando toxinas, colapsando o produciendo las amenazas que hemos discutido en esta sección.

La seguridad

Como mencionamos al principio del capítulo, la seguridad de las personas es la principal preocupación en nuestra lista cuando planificamos la seguridad física. La seguridad de las personas está por encima de cualquier otra preocupación y debe priorizarse por encima de guardar equipos o datos, incluso cuando tales acciones causen daños directos a dichos elementos.

Podríamos encontrar un ejemplo de esto en los sistemas de extinción de incendios que se usan en algunos centros de datos. En muchos casos, los químicos, gases o

líquidos que se usan para extinguir incendios en tales ambientes son muy dañinos para las personas y pueden matarlos si se usan en dicho ambiente. Por esta razón, los sistemas de extinción de incendios a menudo están equipados con una anulación de seguridad que puede evitar que se implementen si hay personas en el área. Si evitáramos que el sistema de supresión extinguiera el incendio porque sabíamos que una persona todavía estaba en el centro de datos, podríamos perder todo el equipo en el centro de datos y potencialmente datos que no podríamos reemplazar. Esta seguiría siendo la elección correcta con la vida humana en juego.

Del mismo modo, si estamos en una instalación donde se está produciendo una emergencia, nuestra prioridad debe ser la evacuación de la instalación, no la seguridad del equipo.

5.3. Protegiendo datos

En segundo lugar solo a la seguridad de nuestro personal está la seguridad de nuestros datos. Uno de nuestros principales medios para proteger los datos es el uso del cifrado. Aunque esta es una solución razonablemente segura, ciertos ataques pueden dejarlo inútil, como los que rompen el algoritmo de cifrado en sí mismo o usan otros medios para obtener las claves de cifrado. Siguiendo el concepto de defensa en profundidad que cubrimos en el Capítulo 1, otra capa de seguridad que debemos garantizar es el elemento físico. Si mantenemos nuestros medios de almacenamiento físicos físicamente seguros contra los atacantes, las condiciones ambientales desfavorables u otras amenazas que puedan dañarlos, nos colocamos en una base de seguridad considerablemente más sólida.

Tal como lo indica Cadena (2017), dependiendo del tipo de medio físico en el que se almacenan nuestros datos, cualquier cantidad de condiciones físicas adversas puede ser problemática o perjudicial para su integridad. Dichos medios a menudo son sensibles a la temperatura, la humedad, los campos magnéticos, la electricidad, el impacto y más, y cada tipo de medio tiene sus puntos fuertes y débiles particulares.

Los medios magnéticos, ya sea que nos refiramos a discos duros de cualquier tipo, cintas, memorias flash u otros, generalmente implican una variedad de movimientos y sensibilidad magnética. La combinación de sensibilidad magnética y partes móviles a menudo hace que dichos medios de almacenamiento sean frágiles de una forma u otra. En la mayoría de los casos, los campos magnéticos fuertes pueden dañar la integridad de los datos almacenados en medios magnéticos, con medios fuera de la carcasa metálica, como cintas magnéticas, que son aún más sensibles a dicha interrupción. Además, sacudir dichos medios mientras está en movimiento,

generalmente mientras se leen o escriben, puede tener una variedad de efectos no deseados, que a menudo dejan los medios inutilizables.

Los medios flash, que se refieren a la categoría general de medios que almacenan datos en chips de memoria no volátiles, en realidad son bastante resistentes. Si podemos evitar los impactos que podrían aplastar directamente los chips en los que se almacenan los datos y no los exponemos a descargas eléctricas, generalmente resistirán condiciones que muchos otros tipos de medios no soportarán. No son terriblemente sensibles a los rangos de temperatura por debajo de lo que realmente destruiría la carcasa, y a menudo sobrevivirán una breve inmersión en líquido, si se secan adecuadamente después. Algunas unidades flash están diseñadas específicamente para sobrevivir a condiciones extremas que normalmente destruirían dichos medios, para aquellos que podrían considerar tales condiciones como un problema potencial.

Los medios ópticos, como los CD, DVD o Blue Ray, son bastante frágiles, como pueden atestiguar aquellos con niños pequeños. Incluso pequeños rasguños en la superficie del medio pueden dejarlo inutilizable. También es muy sensible a la temperatura, está construido en gran parte de plástico y papel de aluminio delgado. Fuera de un entorno protegido, como una bóveda de almacenamiento de medios construida con fines específicos, cualquiera de una variedad de amenazas puede destruir los datos en dichos medios.

Un factor adicional que puede causar preocupación cuando se trata de medios de almacenamiento durante un período prolongado es la obsolescencia técnica. El tipo de medios de almacenamiento, software, interfaces y otros factores pueden afectar nuestra capacidad para leer los datos almacenados. Por ejemplo, ya es muy difícil encontrar unidades lectoras de disquetes.

Disponibilidad

Como lo afirma Costas-Santos (2014), una de nuestras mayores preocupaciones cuando discutimos la protección de datos es garantizar que los datos estén disponibles para nosotros cuando necesitamos acceder a ellos. La disponibilidad de nuestros datos a menudo depende de que tanto nuestro equipo como nuestras instalaciones permanezcan en condiciones de funcionamiento, como discutimos anteriormente, y los medios en los que se almacenan nuestros datos están en condiciones de funcionamiento. Cualquiera de las preocupaciones físicas que discutimos anteriormente puede hacer que nuestros datos sean inaccesibles, en el sentido de poder leerlos desde los medios en los que están almacenados.

Aunque estamos discutiendo específicamente el acceso a los datos aquí, y hablamos sobre algunos de los posibles problemas de hardware al acceder a ciertos tipos de medios anteriores, también hay un componente de infraestructura y equipo bastante sustancial para considerar al discutir la disponibilidad. No solo podemos experimentar problemas al leer los datos de los medios, sino que también podemos tener problemas para llegar a donde se almacenan los datos. Si estamos experimentando una interrupción, ya sea que esté relacionada con la red, la energía, los sistemas informáticos u otros componentes, en cualquier punto entre nuestra ubicación y una ubicación de datos remota, es posible que no podamos acceder a nuestros datos de forma remota. Hoy en día, muchas empresas operan a nivel mundial y es posible que la pérdida de la capacidad de acceder a los datos de forma remota, incluso temporalmente, sea un problema bastante grave.

Datos residuales

Cuando consideramos la idea de mantener los datos seguros, no solo necesitamos tener los datos disponibles cuando necesitamos acceder a ellos, sino que también debemos poder hacer que los datos sean inaccesibles cuando ya no se necesiten. En algunos casos, esta necesidad es relativamente obvia; por ejemplo, es posible que no pasemos por alto la necesidad de triturar una pila de papel que contenga datos confidenciales antes de desecharla. Pero los datos almacenados en medios electrónicos pueden no presentarse tan claramente a todos los que puedan estar manejándolos o eliminándolos.

En muchos casos, podemos encontrar datos almacenados en varios dispositivos relacionados con la informática, como computadoras, dispositivos de medios portátiles, unidades flash, cintas de respaldo, medios de DVD o Blu-ray y artículos similares. Esperaríamos que las personas relativamente expertas en informática se den cuenta de que los medios o dispositivos pueden contener algunos datos confidenciales, y que deberían borrar los datos antes de deshacerse de ellos. Por desgracia, este no es siempre el caso.

Además de los dispositivos que obviamente contienen almacenamiento y pueden contener datos potencialmente sensibles, hay una variedad de otros lugares en los que podemos encontrar datos almacenados. Aunque puede que no parezcan inmediatamente dispositivos informáticos, una amplia variedad de equipos de oficina, como fotocopiadoras, impresoras y máquinas de fax, pueden contener almacenamiento interno volátil o no volátil, a menudo en forma de disco duro. En dichos medios de almacenamiento, a menudo podemos encontrar copias de los

documentos que han sido procesados por la unidad, para incluir datos comerciales confidenciales. Cuando estos tipos de dispositivos se retiran del servicio o se envían para su reparación, es posible que no siempre pensemos en eliminar los datos del medio de almacenamiento y, como tal, podemos estar exponiendo datos que normalmente no queremos que se hagan públicos.

Copias de seguridad

Para garantizar que podamos mantener la disponibilidad de nuestros datos, es probable que deseemos mantener copias de seguridad. No solo necesitamos hacer una copia de seguridad de los datos en sí, pero también necesitamos mantener copias de seguridad de los equipos y la infraestructura que se utilizan para proporcionar acceso a los datos.

Podemos realizar copias de seguridad de datos de varias maneras. Podemos utilizar arreglos redundantes de discos económicos (RAID, por sus siglas en Inglés) en una variedad de configuraciones para garantizar que no perdamos datos de fallas de hardware en discos individuales, podemos replicar datos de una máquina a otra a través de una red, exportar todo a la nube o podemos hacer copias de datos en medios de almacenamiento de respaldo, como DVD o cintas magnéticas.

5.4. Asegurando el acceso

Cuando hablamos de asegurar el acceso a nuestro equipo o nuestras instalaciones, volvemos nuevamente al concepto de defensa en profundidad. Hay múltiples áreas, dentro y fuera, donde es posible que deseemos colocar una variedad de medidas de seguridad, dependiendo del contexto. Una instalación militar puede tener el nivel más alto de seguridad disponible, mientras que una pequeña tienda minorista en un supermercado puede tener el nivel más bajo.

A menudo podemos ver medidas para asegurar el acceso físico implementadas en el perímetro de la propiedad en la que se encuentran varias instalaciones. Algunas veces, al menos veremos medidas mínimas para garantizar que el tráfico de vehículos esté controlado y no entre en lugares indeseables. Dichas medidas pueden adoptar la forma de paisajismo de seguridad. Por ejemplo, podemos ver árboles, grandes rocas, grandes maceteros de cemento y similares colocados frente a los edificios o al lado de las entradas para evitar la entrada de vehículos. En instalaciones más seguras, podríamos ver cercas, barreras de concreto y otras medidas más obvias. Dichos controles están generalmente establecidos como elementos de disuasión, y también pueden ser de naturaleza preventiva.

En la instalación en sí, probablemente veremos una variedad de cerraduras, ya sean mecánicas o electrónicas con credenciales de acceso, en las puertas que ingresan al edificio. Un arreglo típico para edificios no públicos es que la entrada principal del edificio se desbloquee durante el horario comercial y un guardia de seguridad o recepcionista estacionado dentro. En instalaciones más seguras, es probable que veamos todas las puertas cerradas en todo momento y que se requiera una tarjeta de identificación o una llave para ingresar al edificio. Por lo general, una vez dentro del edificio, los visitantes tendrán acceso limitado al área del lobby y, tal vez sala de reuniones y baños, mientras que aquellos autorizados a ingresar al resto del edificio usarán una llave o tarjeta de accesos para acceder.

Una vez dentro de la instalación, veremos una variedad de controles de acceso físico, dependiendo del trabajo y los procesos que se llevan a cabo. Podemos ver controles de acceso en puertas internas o pisos individuales del edificio para evitar que los visitantes o personas no autorizadas accedan libremente a toda la instalación. En el caso de que existan salas de computadoras o centros de datos, el acceso a ellos estará restringido a aquellos que específicamente necesiten ingresar a ellos por razones de negocios. También podemos encontrar controles de acceso físico más complejos en tales áreas, como los sistemas biométricos.

5.5. Resumen

Los controles de seguridad física, que incluyen medidas disuasivas, de detección y preventivas, son los medios que implementamos para mitigar los riesgos de seguridad física. Los elementos disuasivos tienen como objetivo desalentar a aquellos que podrían violar nuestra seguridad, las medidas de detección nos alertan o nos permiten detectar cuándo tenemos una intrusión potencial, y los controles preventivos realmente evitan que se produzcan intrusiones. Por separado, ninguno de estos controles es una solución completa, pero juntos pueden ponernos en una posición mucho más sólida para la seguridad física.

Proteger a las personas es la principal preocupación al planificar nuestra seguridad física. Aunque los datos y el equipo generalmente se pueden reemplazar, cuando se toman las precauciones adecuadas, las personas pueden ser muy difíciles de reemplazar. Las personas son criaturas frágiles, y uno de los mejores pasos que podemos dar cuando nos enfrentamos a una situación en la que podrían verse perjudicados es sacarlos de la situación peligrosa. Además, podemos implementar una variedad de controles administrativos para mantenerlos seguros en sus entornos de trabajo.

La protección de datos, solo superada por la protección de nuestra gente, es una actividad muy crítica en nuestro mundo de negocios basados en tecnología. Una de nuestras principales preocupaciones con los datos es garantizar su disponibilidad cuando sea necesario, y otra es garantizar que podamos eliminarlos por completo cuando ya no deseamos conservarlos. Uno de nuestros principales métodos para garantizar la disponibilidad es realizar copias de seguridad, ya sea mediante el uso de RAID para proteger contra fallas de los medios de almacenamiento, copias de seguridad en medios extraíbles como DVD o cintas magnéticas o exportar todo a un Centro de Datos externo.

La protección de nuestro equipo, aunque es la más baja de las tres categorías en nuestra lista de prioridades, sigue siendo una tarea vital. Cuando seleccionamos el sitio para nuestras instalaciones, debemos tener en cuenta las amenazas que podrían ser relevantes para la ubicación y tomar medidas para mitigarlas. También debemos tomar las medidas necesarias para asegurar el acceso fuera, hacia y dentro de nuestras instalaciones. Tenemos que proteger nuestro equipo no solo de aquellos que se entrometen desde el exterior, sino también de aquellos que tienen acceso legítimo a la instalación, pero no a ciertas áreas dentro de ella. No omitimos mencionar que necesitamos mantener las condiciones ambientales apropiadas para que nuestros equipos funcionen, principalmente energía, temperatura y humedad.

5.6. Cuestionario de estudio

1. Mencione las tres preocupaciones principales para la seguridad física, en orden de importancia.
2. Nombra las tres categorías principales en las que típicamente nos preocupa la seguridad física.
3. ¿Por qué podríamos querer usar RAID?.
4. ¿Cuál es la principal preocupación relacionada con la seguridad física?
5. ¿Qué tipo de control de acceso físico podríamos implementar para bloquear el acceso a un vehículo?
6. Dé tres ejemplos de un control físico que constituya un elemento disuasivo.
7. Dé un ejemplo de cómo un organismo vivo podría constituir una amenaza para nuestro equipo.

8. ¿Qué categoría de control físico podría incluir un candado?
9. ¿Qué son los datos residuales y por qué es una preocupación al proteger la seguridad donde nuestros datos?
10. ¿Cuál es nuestra herramienta principal para proteger a las personas?

CAPÍTULO VI: SEGURIDAD EN LA RED

En el mundo de la seguridad de la red, podemos enfrentarnos a una serie de amenazas de atacantes, configuraciones incorrectas de la infraestructura o dispositivos habilitados para la red, o incluso de simples interrupciones. A pesar de que la red depende de la mayoría del mundo, la pérdida de conectividad de red y la pérdida de los servicios que brindan dichas redes pueden ser sofocantes, en el mejor de los casos, y potencialmente devastadoras para las empresas.

Podemos buscar una variedad de vías para proteger nuestras redes y recursos de red contra la variedad de amenazas que podríamos enfrentar. Podemos agregar seguridad en forma de diseño de red al diseñar nuestras redes de una manera que las haga inherentemente más seguras y resistentes a ataques o contratiempos técnicos. También podemos implementar una variedad de dispositivos en los límites (seguridad perimetral) y dentro de nuestras redes para aumentar nuestro nivel de seguridad, como firewalls y sistemas de detección de intrusos (IDS, por sus siglas en Inglés).

6.1. Seguridad en el diseño de redes

El diseño adecuado de la red nos proporciona una de las principales herramientas que tenemos para protegernos de la variedad de amenazas de red que podríamos enfrentar. Con una red bien diseñada, podemos evitar algunos ataques por completo, mitigar otros y, cuando no podemos hacer nada más, fracasar de manera elegante.

La segmentación de la red puede contribuir en gran medida a reducir el impacto de tales ataques. Cuando segmentamos una red, la dividimos en múltiples redes más pequeñas, cada una actuando como su propia red pequeña llamada subred. Podemos controlar el flujo de tráfico entre subredes, permitiendo o rechazando el tráfico en función de una variedad de factores, o incluso bloqueando el flujo de tráfico por completo si es necesario. Las redes segmentadas adecuadamente pueden aumentar el rendimiento de la red al contener cierto tráfico a las partes de la red que realmente necesitan verlo, y pueden ayudar a localizar problemas técnicos de la red. Además, la segmentación de la red puede evitar que el tráfico no autorizado de la red o los ataques lleguen a partes de la red a las que preferiríamos evitar el acceso, además de facilitar considerablemente la tarea de monitorear el tráfico de la red (Pawar y Anuradha, 2015).

Otro factor de diseño que puede ser de ayuda en el nombre de asegurar nuestras redes es canalizar el tráfico de la red a través de ciertos puntos donde podemos

inspeccionar, filtrar y controlar el tráfico, a menudo conocidos como puntos de estrangulamiento. Los puntos de estrangulamiento pueden ser los enrutadores que mueven el tráfico de una subred a otra, los firewalls o servidores proxy que controlan el tráfico que se mueve dentro o fuera de nuestras redes o partes de nuestras redes, o los servidores proxy de aplicaciones que filtran el tráfico para aplicaciones particulares como el tráfico web o de correo electrónico. Discutiremos algunos de estos dispositivos con mayor detalle en la siguiente sección de este capítulo.

La redundancia en el diseño de la red puede ser otro factor importante para ayudar a mitigar los problemas en nuestras redes. Ciertos problemas o ataques técnicos pueden hacer que partes inutilizables de nuestras redes, dispositivos de infraestructura de red, dispositivos fronterizos como cortafuegos u otros componentes que contribuyen a la funcionalidad de nuestras redes. Un buen diseño de red incluye redundancia planificada para dispositivos que fallan, se pierde la conectividad o se ataca hasta el punto de que se vuelven inútiles o perdemos el control de ellos. Por ejemplo, si uno de nuestros dispositivos fronterizos está siendo sometido a un ataque de denegación de servicios distribuido (DDoS, por sus siglas en Ingés), hay algunos pasos que podemos tomar para mitigar el ataque. Sin embargo, podemos cambiar a una conexión diferente a Internet o enrutar el tráfico a través de un dispositivo diferente hasta que podamos llegar a una solución a más largo plazo.

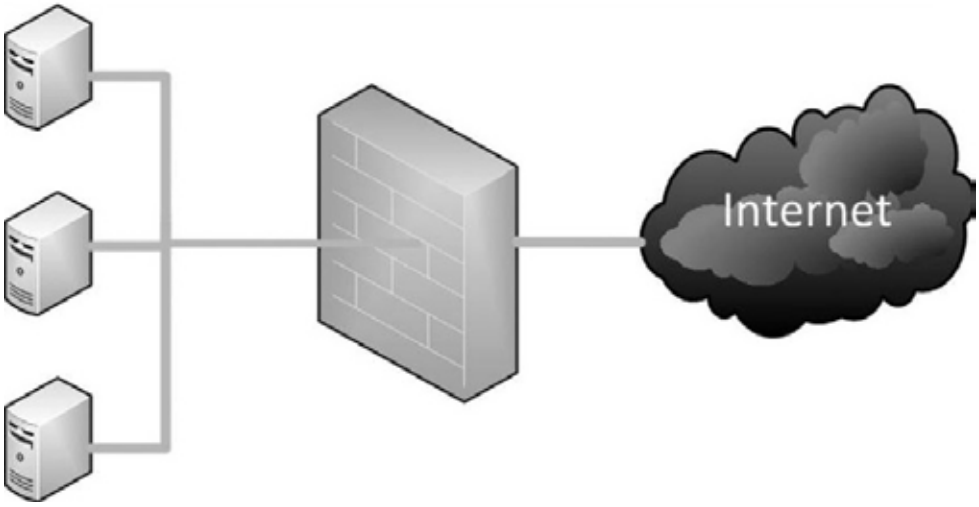
Muros de fuego o firewalls

Un firewall es un mecanismo para mantener el control sobre el tráfico que fluye dentro y fuera de nuestras redes. El concepto y las primeras implementaciones de las tecnologías de cortafuegos se remontan a finales de los años ochenta y principios de los noventa, estos equipos generalmente se colocan en una red donde vemos un cambio en el nivel de confianza, por ejemplo, una red de acceso público en un aeropuerto y una red para el uso de las computadoras del departamento de Migración y Extranjería. Es posible que veamos un firewall en el límite entre nuestra red interna e Internet, como se muestra en la Figura 12. También podemos ver un firewall instalado en nuestra red interna para evitar el acceso a tráfico de red de naturaleza delicada por aquellos que no tienen razón para hacerlo.

Muchos de los firewalls en uso hoy en día se basan en el concepto de examinar los paquetes que ingresan a través de la red. Ese análisis determina qué debe permitirse entrar o salir. Si el tráfico está permitido o bloqueado puede basarse en una variedad de factores y depende en gran medida de la complejidad del cortafuegos. Por ejemplo, podríamos permitir o no permitir el tráfico en función del protocolo que se

utilice, permitiendo que pase el tráfico web y de correo electrónico, pero bloqueando todo lo demás.

Figura 12. Topografía de red con muro de fuego.



Fuente: elaboración propia.

Filtrado de paquetes

El filtrado de paquetes es una de las tecnologías de firewall más antiguas y simples. El filtrado de paquetes analiza el contenido de cada paquete en el tráfico individualmente y realiza una determinación general, en función de las direcciones IP de origen y destino, el número de puerto y el protocolo que se utiliza, de si se permitirá el paso del tráfico. Dado que cada paquete se examina individualmente y no en concierto con el resto de los paquetes que comprenden el contenido del tráfico, es posible desviar los ataques a través de este tipo de firewall

Inspección de paquetes con estado

Los firewalls de inspección de paquetes con estado (generalmente conocidos como firewalls con estado) funcionan según el mismo principio general que los firewalls de filtrado de paquetes, pero pueden realizar un seguimiento del tráfico a nivel granular. Mientras que un firewall de filtrado de paquetes solo examina un paquete individual fuera de contexto, un firewall con estado puede vigilar el tráfico a través de una conexión determinada, generalmente definida por las direcciones IP de origen y destino, los puertos que se utilizan y la red ya existente tráfico. Un firewall con estado utiliza lo que se llama una tabla de estado para realizar un seguimiento del estado de la conexión y solo permitirá el tráfico que sea parte de una conexión nueva

o ya establecida. La mayoría de los firewalls con estado también pueden funcionar como un firewall de filtrado de paquetes, combinando a menudo las dos formas de filtrado.

Inspección profunda de paquetes

Los firewalls de inspección profunda de paquetes agregan otra capa de inteligencia a nuestras capacidades de firewall. Los firewalls de inspección profunda de paquetes son capaces de analizar el contenido real del tráfico que fluye a través de ellos. Aunque los cortafuegos de filtrado de paquetes y los cortafuegos con estado solo pueden mirar la estructura del tráfico de la red para filtrar los ataques y el contenido no deseado, los cortafuegos de inspección profunda de paquetes pueden volver a ensamblar el contenido del tráfico para ver lo que se entregará a la aplicación para la que está destinada en última instancia.

Para usar una analogía, si enviamos un paquete a través de uno de los transportistas de paquetería comunes, el transportista observará el tamaño y la forma del paquete, cuánto pesa, cómo está envuelto y las direcciones de envío y destino. En general, esto es lo que pueden hacer los firewalls de filtro de paquetes y los firewalls con estado. Ahora, si el transportista de paquetes hiciera todo esto, además de abrir el paquete e inspeccionar su contenido, luego juzgar si el paquete pudiera enviarse en función de su contenido, esto estaría mucho más en línea con la inspección profunda.

Aunque esta tecnología es muy prometedora para bloquear una gran cantidad de los ataques que podríamos ver, también se plantea la cuestión de la privacidad. En teoría, alguien en control de un dispositivo de inspección profunda de paquetes podría leer cada uno de nuestros mensajes de correo electrónico, ver cada página web exactamente como la vimos y escuchar fácilmente nuestras conversaciones de mensajería instantánea.

Servidores proxy

Los servidores proxy son, en última instancia, una variante especializada de un firewall. Estos servidores proporcionan características de seguridad y rendimiento, generalmente para una aplicación particular, como el correo o la navegación web. Los servidores proxy pueden servir como un punto de estrangulamiento (discutido anteriormente en el capítulo) para permitirnos filtrar el tráfico en busca de ataques o contenido no deseado, como malware o acceso a sitios web que alojan contenido para adultos o ilegal. También nos permiten registrar el tráfico que los atraviesa para una inspección posterior, y sirven para proporcionar una capa de seguridad para los

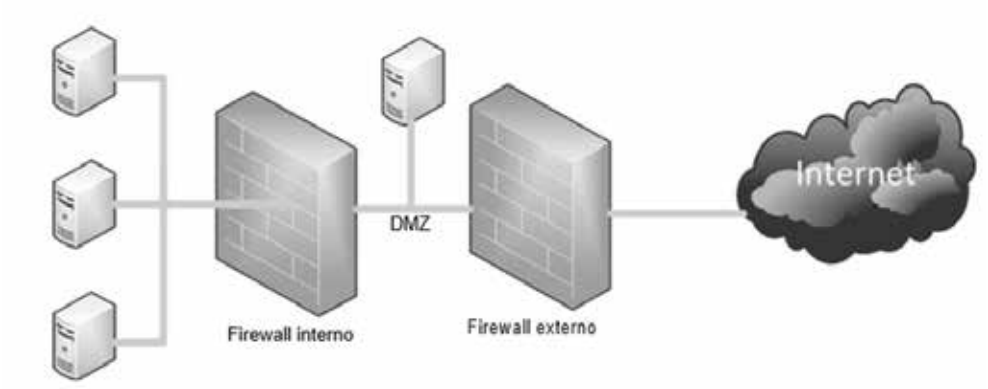
dispositivos detrás de ellos, al servir como una fuente única para las solicitudes.

Los servidores proxy son casi omnipresentes en el mundo de muchas empresas, en gran parte debido a la capacidad de filtrado que proporcionan. Muchas compañías confían en ellos para evitar que las grandes cantidades de spam que fluyen a través del correo electrónico lleguen a sus usuarios y disminuyan la productividad. También vemos que se usan para filtrar el tráfico web en dichos entornos a fin de evitar que los empleados visiten sitios web que puedan tener material cuestionable, y para filtrar el tráfico que podría indicar la presencia de malware.

Zonas desmilitarizadas

Una zona desmilitarizada (DMZ, por sus siglas en Inglés), es generalmente una combinación de una característica de diseño de red y un dispositivo de protección como un firewall. Como discutimos anteriormente en la sección "Seguridad en el diseño de redes", a menudo podemos aumentar el nivel de seguridad en nuestras redes al segmentarlas adecuadamente. Cuando observamos sistemas que necesitan estar expuestos a redes externas como Internet para funcionar, como servidores de correo y servidores web, debemos garantizar su seguridad y la seguridad de los dispositivos en la red detrás de ellos. A menudo podemos hacer esto poniendo una capa de protección entre el dispositivo, como nuestro servidor de correo e Internet, y entre el resto de nuestra red y el dispositivo, como se muestra en la Figura 13.

Figura 13. Esquema de una DMZ.



Fuente: elaboración propia.

El esquema permite solo el tráfico que necesita llegar al servidor de correo que se encuentra en la DMZ desde Internet habilitando solamente los puertos de comunicación 143 y 25, por ejemplo, que corresponden al protocolo de acceso a mensajes de Internet (IMAP, por sus siglas en Inglés) y al de transferencia simple de

mensajes (SMTP, por sus siglas en Inglés), respectivamente.

6.2. Detección de intrusiones en la red

Los Sistemas de Detección de Intrusos (IDS, por sus siglas en Inglés) monitorean las redes, los hosts o las aplicaciones a las que están conectados para actividades no autorizadas. Existen varios tipos de IDS: los sistemas de detección de intrusos basados en el host (HIDS, por sus siglas en Inglés), los sistemas de detección de intrusos basados en el protocolo de aplicación (APIDS, por sus siglas en Inglés) y los sistemas de detección de intrusos basados en la red (NIDS, por sus siglas en Inglés). Nos centraremos en los NIDS en este capítulo, volviendo a los HIDS y APIDS más adelante en otro capítulo.

Los NIDS normalmente se conectarán a la red en un lugar donde puedan monitorear el tráfico constante, pero deben colocarse con cuidado para que no se sobrecarguen. Colocar un NIDS detrás de otro dispositivo de filtrado, como un firewall, puede ayudar a eliminar parte del tráfico con falsos positivos para disminuir la cantidad de datos que el NIDS necesita inspeccionar. Como los NIDS necesitan examinar una gran cantidad de tráfico en una red típica, generalmente solo pueden hacer una inspección relativamente superficial para determinar si la situación en la red es normal o no. Debido a esto, un NIDS puede pasar por alto algunos tipos de ataques, particularmente aquellos diseñados específicamente para pasar por tales inspecciones. Los ataques de creación de paquetes implican paquetes de tráfico muy específicamente diseñados que llevan ataques o código malicioso (Javaid *et al.*, 2016).

Métodos para detección de intrusiones

Según Hodo *et al.* (2016), los IDS a menudo se clasifican por la forma en que detectan los ataques. En general, se dividen en dos categorías principales: detección basada en firmas y detección basada en anomalías. Los IDS basados en firmas funcionan de manera muy similar a la mayoría de los sistemas antivirus pues mantienen una base de datos de las firmas que pueden indicar un tipo particular de ataque y comparan el tráfico entrante con esas firmas. En general, este método funciona bien, excepto cuando encontramos un ataque que es nuevo o que se ha construido específicamente para no coincidir con las firmas de ataque existentes. Uno de los grandes inconvenientes de este método es que muchos sistemas basados en firmas dependen únicamente de su base de datos de firmas para detectar ataques. Si no tenemos una firma para el ataque, es posible que no la veamos en absoluto. Además de esto, el atacante que crea el tráfico puede tener acceso a las mismas

herramientas IDS que estamos utilizando, y puede probar el ataque contra ellos para evitar específicamente nuestras medidas de seguridad.

El otro método principal de detección de IDS es la detección basada en anomalías, el cual generalmente funciona tomando una línea de base del tráfico normal y la actividad que tiene lugar en la red. Pueden medir el estado actual del tráfico en la red contra esta línea de base para detectar patrones que no están presentes en el tráfico normalmente.

Dichos métodos pueden funcionar muy bien cuando buscamos detectar nuevos ataques o ataques que se han ensamblado deliberadamente para evadir a los IDS. Por otro lado, también podemos ver un mayor número de falsos positivos basados en anomalías que los basados en firmas. Si el tráfico en la red cambia de lo que estaba presente cuando tomamos nuestra línea de base, el IDS puede ver esto como indicativo de un ataque, y lo mismo ocurre con la actividad legítima que causa patrones de tráfico inusuales o picos en el tráfico.

Por supuesto, podemos establecer un IDS que nos brinde algunas de las ventajas de cada tipo de detección y utilizar los métodos basados en la firma y en la anomalía en un solo IDS, una clase de configuración híbrida lo que nos permitirá mucha más flexibilidad en la detección de ataques, aunque quizás a expensas de operar un poco más lentamente y causar un retraso en la detección.

6.3. Protegiendo el tráfico de red

Además de proteger nuestras redes de intrusiones, también debemos observar el tráfico que fluye sobre ellas. En línea con el concepto de defensa en profundidad que vimos en el primer capítulo, queremos establecer tantas capas de seguridad como sea razonable para el valor de lo que estamos asegurando. Incluso cuando estamos en un entorno que consideramos seguro, podemos estar sujetos a una variedad de ataques, y sería una negligencia no implementar protecciones preventivas.

Datos interceptados

Una de las mayores preocupaciones cuando enviamos datos confidenciales a través de una red es que los datos sean interceptados por alguien que pueda usarlos incorrectamente. Dadas las numerosas redes disponibles en la actualidad en oficinas, hoteles, cafeterías, restaurantes y otros lugares, la oportunidad de exponer accidentalmente los datos a un atacante es muy alta.

Cuando enviamos datos a través de redes que no son seguras ni confiables, un

atacante puede obtener una gran cantidad de información de lo que enviamos. Si usamos aplicaciones o protocolos que no cifran lo que se envía a través de la red, podemos terminar dando nuestras credenciales de inicio de sesión, números de tarjeta de crédito, información bancaria y otros datos a cualquier persona que esté husmeando el tráfico.

Los datos pueden ser interceptados desde redes cableadas e inalámbricas, a menudo con muy poco esfuerzo, dependiendo del diseño de la red. Discutiremos algunas de las herramientas que se pueden usar para realizar dicha intercepción más adelante en este capítulo.

Exposición inalámbrica

Las redes inalámbricas, en particular, son uno de los principales riesgos de seguridad cuando consideramos los lugares donde nuestros datos podrían estar expuestos. El acceso gratuito a Internet inalámbrico se proporciona comúnmente hoy en varios lugares. Aunque puede ser bueno poder obtener acceso a la red de forma gratuita, muchas personas no entienden el riesgo de seguridad que acompaña a dicho servicio. En general, estas redes se configuran sin contraseña y sin encriptación de ningún tipo, lo que normalmente se implementa para proteger la confidencialidad de los datos en tráfico fluyendo por la red. Incluso en los casos en que se requiere una contraseña para acceder a la red, como podríamos encontrar en un hotel, si todos los demás en el hotel también están en la red, pueden ver nuestros datos.

Aunque tales redes inseguras son un problema de seguridad, no son insalvables. Discutiremos una de las herramientas que podríamos usar para asegurar tales conexiones en la siguiente sección.

Redes privadas virtuales

El uso de redes privadas virtuales (VPN, por sus siglas en Inglés) pueden proporcionarnos una solución para enviar tráfico confidencial a través de redes no seguras. Una conexión VPN, a menudo denominada túnel, es una conexión cifrada entre dos puntos. Esto generalmente se logra mediante el uso de una aplicación de cliente VPN en un extremo de la conexión, y un dispositivo llamado concentrador VPN en el otro extremo. El cliente utiliza el software para autenticarse en el concentrador VPN, generalmente a través de Internet, y después de que se ha establecido la conexión, todo el tráfico intercambiado desde la interfaz de red conectada a la VPN fluye a través del túnel VPN encriptado, es decir, si un atacante captura datos difícilmente va a poder leerlos (Harmening, 2017).

Las VPN a menudo se usan para permitir que los trabajadores remotos se conecten a los recursos internos de una organización. Cuando se establece dicha conexión, el dispositivo conectado puede actuar como si estuviera conectado directamente a la red interna de la organización que aloja la conexión. Esto puede ser muy útil ya que nos permite habilitar un mayor acceso para un trabajador remoto de lo que normalmente podríamos hacer de manera segura cuando el trabajador está fuera de los límites de nuestra red.

Además de permitirnos acceder a los recursos internos de nuestra organización, las VPN también se pueden usar para proteger o anonimizar el tráfico que enviamos a través de conexiones no confiables. Las compañías como StrongVPN venden sus servicios al público exactamente para tales fines, lo que nos permite proteger el contenido de nuestro tráfico de los registros de nuestros proveedores de servicios de Internet (ISP, por sus siglas en Inglés) o ser rastreados por otros en la misma red, para ocultar nuestra ubicación geográfica y evitar el bloqueo orientado a la ubicación.

Dichos servicios también son populares entre aquellos que participan en servicios de intercambio de archivos en redes punto a punto, conocidas como P2P. Los ISP y las organizaciones como “Motion Picture Association of America (MPAA)” y “Recording Industry Association of America (RIAA)” señalan dicha actividad como frecuente para infringir los derechos de autor. Las VPN pueden permitir que tanto el tráfico como las direcciones IP reales de aquellos que participan en tales actividades permanezcan ocultas de aquellos que las buscarían.

6.4. Seguridad en redes inalámbricas

Como discutimos anteriormente en este capítulo, las redes inalámbricas no seguras transmiten libremente nuestros datos para que cualquiera con la tecnología apropiada (y de fácil acceso hoy día) los intercepte y pueda leerlos. Recordemos también que las tecnologías de redes inalámbricas hoy día han superado por mucho las distancias y cobertura, lo que significa que cada vez más se amplía el rango de posibilidad de captura de tráfico en zonas alrededor del equipo que difunda una red inalámbrica.

Además de los problemas con nuestro tráfico potencialmente escuchado, también existe el posible problema de que los dispositivos inalámbricos se conecten sin nuestro conocimiento. En particular, los puntos de acceso inalámbrico que se conectan a nuestra red sin autorización, comúnmente conocidos como puntos de acceso no autorizados, pueden presentar un problema de seguridad grave.

Por ejemplo, si trabajamos en un área donde la conexión inalámbrica estaba prohibida, podríamos encontrar que una persona ingeniosa decidió traer un punto de acceso propio e instalarlo debajo de su escritorio, para proporcionar acceso inalámbrico en una zona de fumadores al aire libre cercana. Aunque esto podría no haberse hecho con malas intenciones en mente, esta simple acción puede haber invalidado todo el conjunto de medidas de seguridad de red cuidadosamente planificadas que hemos implementado.

Si el punto de acceso no autorizado en nuestro ejemplo se configuró con poca o ninguna seguridad, nuestro amigo que ha instalado puntos de acceso bien intencionado habría proporcionado a cualquier persona dentro del alcance del punto de acceso una ruta fácil directamente a nuestra red, evitando cualquier seguridad fronteriza que podamos tener en su lugar. Existe la posibilidad de que un IDS de red pueda recoger la actividad desde el punto de acceso no autorizado, pero no hay garantía de esto. La solución simple para encontrar dicho equipo malicioso es documentar cuidadosamente los dispositivos legítimos que forman parte de la infraestructura de la red inalámbrica, y buscar regularmente dispositivos adicionales utilizando una herramienta como Kismet, la cual discutiremos más adelante en este capítulo.

Para los dispositivos legítimos y autorizados en nuestra red, nuestro método principal para proteger el tráfico que fluye a través de ellos es el uso de cifrado. El cifrado utilizado por los dispositivos inalámbricos 802.11, el más común de la familia de redes inalámbricos, se divide en tres categorías principales: Privacidad equivalente a cableado (WEP, por sus siglas en Inglés), acceso Wi-Fi protegido (WPA, por sus siglas en Inglés) y acceso Wi-Fi protegido versión 2 (WPA2). De estos, WPA2 es el más actual y ofrece la seguridad inherente más sólida.

Protocolos seguros

Una de las formas más simples y fáciles de proteger nuestros datos es usar protocolos seguros. Muchos de los protocolos más comunes y antiguos, como el Protocolo de transferencia de archivos (FTP, por sus siglas en Inglés) para transferir archivos, Telnet para interactuar con máquinas remotas, el Protocolo de oficina de correos (POP, por sus siglas en Inglés) para recuperar correo electrónico y una gran cantidad de otros, manejan datos en de manera insegura. Dichos protocolos a menudo envían información confidencial, como inicios de sesión y contraseñas, en texto sin formato a través de la red. Cualquier persona que escuche en la red con un “sniffer” (programa husmeador) colocado correctamente puede recoger el tráfico de dichos

protocolos y recoger fácilmente la información confidencial del tráfico que envían.

Muchos protocolos inseguros tienen equivalentes seguros, por ejemplo, en lugar de operar a través de la línea de comando con Telnet, podemos usar Secure Shell (SSH), y en lugar de transferir archivos con FTP, podemos usar el Protocolo de transferencia segura de archivos (SFTP, por sus siglas en Inglés), que también se basa en SSH.

SSH es un protocolo muy útil para proteger las comunicaciones, ya que podemos enviar muchos tipos de tráfico a través de él. Se puede usar para transferencias de archivos y acceso a terminales, como mencionamos, y para proteger el tráfico en una variedad de otras situaciones, como cuando se conecta a un escritorio remoto, se comunica a través de una VPN, se montan sistemas de archivos remotos y cualquier otra cantidad Tareas. El cifrado utilizado por SSH es RSA, un algoritmo de cifrado de clave pública.

6.5. Herramientas de seguridad de red

Podemos utilizar una amplia variedad de herramientas para mejorar la seguridad de nuestra red. Muchas de estas herramientas son las mismas que usan los atacantes que penetran en nuestras redes, y esta es una de las principales razones por las que son útiles en nuestra labor de proteger. Podemos usar las mismas herramientas que usan los atacantes para penetrar nuestras defensas y así ponerlas a prueba para mejorarlas. Al usar tales herramientas para localizar vulnerabilidades de seguridad que podemos reparar para mantener a los atacantes alejados.

La clave para usar una estrategia de evaluación de este tipo es realizar evaluaciones minuciosas y regulares con la suficiente frecuencia como para que podamos encontrar los agujeros antes de que lo hagan los atacantes. Si solo realizamos tales pruebas, comúnmente conocidas como pruebas de penetración, de forma ocasional y superficial, es probable que no captemos todos los problemas presentes en nuestro entorno. Además, a medida que los diversos dispositivos de hardware de red y el software que se ejecuta en ellos se actualizan, agregan o eliminan con el tiempo, las vulnerabilidades presentes en nuestro entorno también cambiarán. También es importante tener en cuenta que la gran mayoría de las herramientas que podríamos usar solo serán capaces de encontrar problemas conocidos. Los ataques o vulnerabilidades nuevos o no publicados, comúnmente conocidos como ataques de día cero, aún pueden sorprendernos cuando surgen y causar serios dolores de cabeza (Vega, 2020).

Como discutimos anteriormente en el capítulo, los atacantes que acceden a un

dispositivo inalámbrico pueden potencialmente pasar por alto todas nuestras medidas de seguridad cuidadosamente planificadas. Peor aún, si no tomamos medidas para garantizar que los dispositivos inalámbricos no autorizados, como los puntos de acceso no autorizados, no se instalen en nuestra red, podríamos estar permitiendo un gran agujero en la seguridad de nuestra red y nunca lo sabremos.

Podemos usar varias herramientas para detectar dispositivos inalámbricos y una de las herramientas más conocidas para detectar tales dispositivos se llama Kismet, que se ejecuta en Linux y se puede encontrar en la distribución de Kali Linux. Kismet se usa comúnmente para detectar puntos de acceso inalámbrico y puede encontrarlos incluso cuando se han hecho intentos para hacerlo difícil. Existe un software similar, llamado NetStumbler, para Windows, aunque no tiene un conjunto de características tan completo como Kismet.

Además de detectar dispositivos inalámbricos, algunas herramientas pueden permitirnos romper las diferentes variedades de cifrado que se utilizan en dichas redes. Existen muchas herramientas para tales propósitos, pero algunas de las más comunes para descifrar WEP, WPA y WPA2 incluyen coWPAtty y Aircrack-NG.

Escáneres

Los escáneres son uno de los pilares de la industria de pruebas y evaluaciones de seguridad. Generalmente podemos dividirlos en dos categorías principales: escáneres de puertos y escáneres de vulnerabilidad. Hay cierta superposición entre los dos, dependiendo de la herramienta particular de la que estemos hablando.

Uno de los escáneres de puertos más famosos que podríamos querer usar es una herramienta gratuita llamada Nmap, abreviatura de mapeador de red. Aunque Nmap generalmente se conoce como un escáner de puertos, en realidad es más que eso. Aunque Nmap puede realizar escaneos de puertos, también puede buscar hosts en una red, identificar los sistemas operativos que esos hosts están ejecutando, detectar las versiones de los servicios que se ejecutan en cualquier puerto abierto y mucho más (Calderon, 2017).

En su mayor parte, en términos de seguridad de red, los escáneres son los más útiles cuando se utilizan como herramienta para descubrir las redes y sistemas que se encuentran en nuestro entorno. Analizaremos algunos de los usos de los escáneres que son más específicos para la seguridad del sistema operativo en el Capítulo 7.

Sniffers de paquetes

Un analizador de red o protocolo, también conocido como sniffer de paquetes, o simplemente sniffer, es una herramienta que puede interceptar el tráfico en una red, comúnmente conocido como sniffing. Básicamente equivale a escuchar cualquier tráfico que pueda ver la interfaz de red de nuestra computadora o dispositivo, ya sea que lo hayamos recibido o no donde normalmente el adaptador de red debe establecerse en modo promiscuo. A continuación algunas aplicaciones de este tipo:

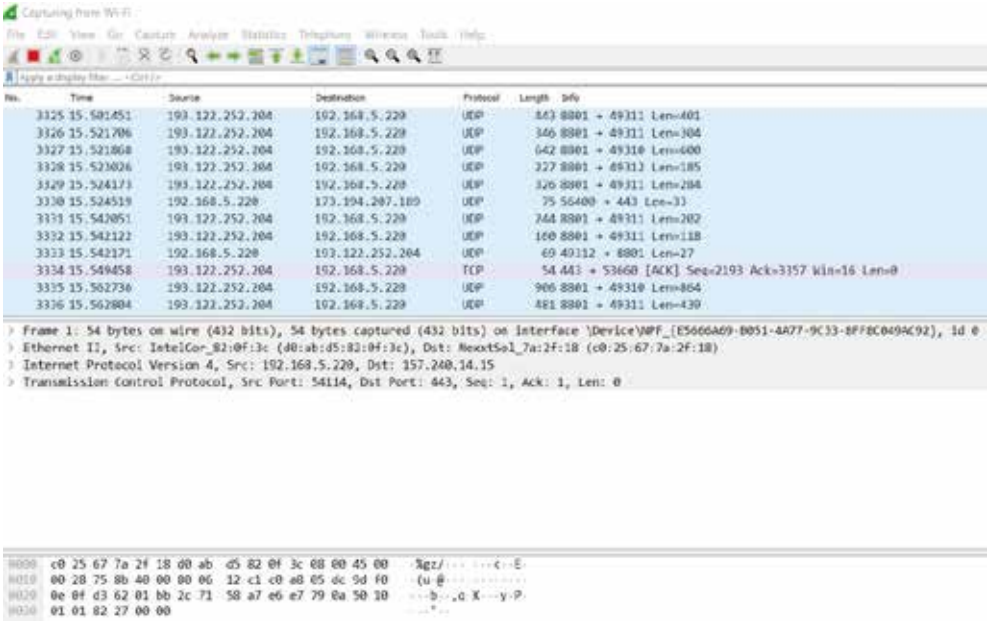
Tcpdump es una herramienta clásica y ha existido desde fines de la década de 1980. Tcpdump es una herramienta de línea de comandos que nos permite monitorear las actividades de la red a la que estamos conectados, y tiene solo algunas otras características clave como el filtrado del tráfico. Tcpdump solo se ejecuta en sistemas operativos tipo UNIX, pero también existe una versión para Windows, llamada WinDump.

Wireshark, anteriormente conocido como Ethereal, es un sniffer con todas las funciones que es capaz de interceptar el tráfico de una amplia variedad de redes cableadas e inalámbricas. Tiene una interfaz gráfica, que se muestra en la Figura 14, incluye un gran número de herramientas de filtrado, clasificación y análisis, y además es uno de los rastreadores más populares en el mercado hoy en día incluso para evaluaciones de seguridad.

Kismet, tal y como lo discutimos anteriormente, también es un sniffer especializado. Aunque muchos de los otros rastreadores son independientes de los medios de red, en su mayor parte, Kismet solo rastreará desde redes inalámbricas. Debido a este enfoque muy específico, puede proporcionarnos un conjunto de herramientas mucho más específico.

También podemos ver rastreadores de paquetes en forma de hardware, como el analizador de red portátil OptiView de Fluke Networks. Aunque definitivamente podemos beneficiarnos de analizadores portátiles bien equipados como este, a menudo tienden a ser muy caros y van mucho más allá del presupuesto promedio.

Figura 14. Interfaz de Wireshark.



Fuente: elaboración propia.

Honeypots

Los Honeypots son una herramienta algo controvertida en el arsenal de aquellos que podemos usar para mejorar la seguridad de nuestra red. Un Honeypot puede detectar, monitorear y, a veces, alterar las actividades de un atacante. Los Honeypots están configurados para mostrar deliberadamente vulnerabilidades o configuraciones que harían el sistema atractivo para un atacante, es decir un objetivo de ataque. Este podría ser un servicio intencionalmente vulnerable, un sistema operativo desactualizado y sin parches, un recurso compartido de red llamado "documentos de alta importancia" u otros elementos similares que podrían servir como cebo para un atacante. Claro está, se requieren destrezas para evitar que el atacante descubra que es una trampa.

Una de las cosas interesantes sobre los Honeypots es que las vulnerabilidades o los datos que se dejan fuera para atraer al atacante son completamente falsos. En realidad, los Honeypots están configurados para mostrar estos elementos para que podamos atrapar a los atacantes y monitorear lo que están haciendo en el sistema sin su conocimiento. Esto podría hacerse en un esfuerzo por proporcionar un sistema de alerta temprana para una corporación, como un método para investigar qué métodos están usando los atacantes o como un objetivo intencional para monitorear

las actividades del malware en la naturaleza.

También podemos expandir los Honeypots en estructuras más grandes mediante la instalación de varios sistemas de este tipo en una red, a menudo denominada red trampa o Honeynets las cuales pueden permitirnos configurar múltiples Honeypots con diferentes configuraciones y vulnerabilidades, generalmente con algún tipo de panel de control centralizado para monitorear todos los Honeypots en la red. Las Honeynets pueden ser particularmente útil para el monitoreo a gran escala de la actividad de malware, ya que podemos emular una variedad de diferentes sistemas operativos y vulnerabilidades (Anirudh *et al.,* 2017).

Herramientas para análisis de Firewalls

En nuestro kit de herramientas de red, también podemos encontrar útil incluir aquellas que puedan mapear la topología y ayudar a localizar vulnerabilidades en nuestros firewalls. Hping3 es una herramienta conocida y útil para tales esfuerzos. Es capaz de construir paquetes de Protocolo de mensajes de control de Internet (ICMP, por sus siglas en Inglés) especialmente diseñados para evadir algunas de las medidas normales que se implementan para evitar que veamos los dispositivos que están detrás de un firewall. También podemos hacer un script de las actividades de Hping3 para probar las respuestas de los firewalls y los IDS, de modo que podamos tener una idea de las reglas con las que están operando.

También podemos usar una variedad de otras herramientas que hemos discutido en esta sección para probar la seguridad de nuestros firewalls. Podemos usar escáneres de puertos y vulnerabilidades para mirarlos desde el exterior con el fin de encontrar cualquier puerto que esté inesperadamente abierto, o cualquier servicio que se ejecute en nuestros puertos abiertos y que sea vulnerable a ataques conocidos. También podemos usar rastreadores para examinar el tráfico que ingresa y sale de los firewalls, suponiendo que podamos implementar dicha herramienta en una ubicación de red que nos permita ver el tráfico.

Seguridad de red en el mundo real

Hoy podemos ver el uso de la seguridad de la red en casi todo el mundo. En las empresas y en las organizaciones, podemos ver esfuerzos concertados para diseñar redes seguras, incluida la implementación de firewalls e IDS. Dependiendo de la industria a la que nos estamos refiriendo, nuestro negocio puede depender completamente del éxito de tales medidas para mantenernos seguros. Si observamos empresas centradas en la red, como Amazon o Salesforce, la gran mayoría de sus

negocios se realiza directamente a través de Internet. Si no tuvieran medidas de seguridad rígidas y no las evaluaran continuamente para encontrar debilidades, sus negocios fracasarían rápidamente.

En el back-end de tales organizaciones, también podemos encontrar una variedad de medidas de seguridad que se implementan para mantener seguro el tráfico y las actividades de sus empleados y usuarios. El uso comercial de las conexiones VPN es muy común, ya que esto permite a los empleados que trabajan desde su casa o en el camino utilizar los recursos internos de la red de forma remota. También podemos ver el uso de protocolos seguros cuando aquellos que están fuera de los firewalls corporativos se comunican con servidores expuestos externamente para intercambiar correos electrónicos, enviar archivos, comunicarse por mensajería instantánea, entre otros.

Como mencionamos, tales compañías también necesitan evaluar constantemente sus propias medidas de seguridad. Podemos utilizar una serie de herramientas para hacerlo desde una perspectiva de red, incluidas las pocas que discutimos en este capítulo y muchas más, también es importante comprender que tales herramientas a menudo no se ajustan claramente a las líneas de seguridad de red, seguridad del sistema operativo y seguridad de las aplicaciones, sino que a menudo abarcan uno o más, si no todos, de estos aspectos. Esto refleja la necesidad de garantizar la seguridad en todas estas formas y que estas categorías se superpongan en gran medida.

6.6. Resumen

Cuando protegemos nuestras redes, lo hacemos desde una variedad de ángulos diferentes, utilizamos un diseño de red seguro para garantizar que nuestras redes estén segmentadas correctamente, que tengamos los puntos de estrangulamiento adecuados para permitir la supervisión y el control del tráfico, y que seamos redundantes donde se necesita redundancia. También implementamos dispositivos de seguridad como cortafuegos e IDS para protegernos tanto dentro como fuera de nuestras redes.

Además de proteger las redes en sí, también debemos buscar proteger el tráfico de nuestra red. Debido a la naturaleza de nuestras redes, ya sean cableadas o inalámbricas, a menudo es posible espiar el tráfico que circula por ellas. Para proteger nuestro tráfico, podemos usar VPN para asegurar nuestras conexiones cuando usamos redes no confiables, podemos usar medidas de seguridad específicas para redes inalámbricas cuando necesitamos usarlas, y podemos hacer uso de protocolos

seguros como Una medida de seguridad general.

En nuestros esfuerzos por brindar seguridad a nuestra red, podemos usar una variedad de herramientas de seguridad. Cuando se trata de redes inalámbricas, podemos usar herramientas que se adapten específicamente a tales tareas, como Kismet o NetStumbler. También podemos escuchar el tráfico de la red con herramientas como Wireshark o Tcpdump, buscar dispositivos en nuestras redes con herramientas como Nmap y probar nuestros firewalls con hping3 y otras utilidades similares. También podemos colocar dispositivos llamados honeypots en nuestras redes específicamente para atraer la atención de los atacantes con el fin de estudiarlos y sus herramientas y alertarnos de su presencia.

6.7. Cuestionario de estudio

1. ¿Para qué podríamos usar la herramienta Kismet?
2. Explique el concepto de segmentación.
3. Si necesitáramos una herramienta de línea de comandos que pudiera detectar el tráfico de la red, ¿cuál herramienta podríamos utilizar y por qué?
4. ¿Cuáles son los tres tipos principales de encriptación inalámbrica?
5. ¿Cuál herramienta podríamos usar para buscar dispositivos en una red?
6. ¿Por qué usaríamos un honeypot?
7. Explique la diferencia entre la firma y la detección de anomalías en los sistemas de detección de intrusiones.
8. ¿Qué usaríamos si necesitáramos enviar datos confidenciales a través de un sitio no confiable?
9. ¿Cuál sería el objetivo de utilizar DMZ en nuestras redes empresariales?
10. ¿Cuál es la diferencia entre un firewall con estado y un firewall de inspección profunda de paquetes?

CAPÍTULO VII: SEGURIDAD DEL SISTEMA OPERATIVO

Cuando buscamos proteger nuestros datos, procesos y aplicaciones contra ciberataques, entonces una de las áreas más importantes en las que podemos encontrar debilidades es en el sistema operativo que alberga todo lo antes mencionado. Si no nos ocupamos de proteger nuestros sistemas operativos, realmente no tenemos ninguna base que pueda sustentar una seguridad razonablemente sólida.

Hay varias maneras de mitigar las diversas amenazas y vulnerabilidades que podríamos enfrentar desde la perspectiva del sistema operativo. Una de las categorías más fáciles que podemos señalar es el fortalecimiento del sistema operativo. Podemos usar esta técnica cuando estamos configurando hosts que podrían enfrentar una acción hostil para disminuir el número de puertas a través de las cuales un atacante podría llegar a nosotros.

También podemos agregar herramientas y aplicaciones a nuestro sistema operativo que están diseñadas para combatir algunas de las técnicas que los atacantes podrían usar contra nosotros. El más común y obvio de estos es el uso de herramientas anti-malware, que discutiremos más adelante en este capítulo y que nos protegen de la amplia variedad de códigos maliciosos a los que nuestro sistema operativo podría estar expuesto, especialmente si mantiene conexión a Internet de forma constante. En la misma clase general de software, también podemos buscar firewalls de software y sistemas de detección de intrusos basados en host.

También podemos utilizar la gran cantidad de herramientas de seguridad que están disponibles para ayudarnos a detectar áreas potencialmente vulnerables en nuestros hosts. Podríamos usar tales herramientas para encontrar servicios que no sabíamos que se estaban ejecutando, localizar servicios de red que se sabe que contienen fallas explotables y, en general, inspeccionar nuestros sistemas operativos desde el registro hasta las tareas en ejecución de forma integral.

Mediante la combinación de todos estos esfuerzos, una vez más para volver al concepto de defensa en profundidad, podemos mitigar muchos de los problemas de seguridad que podemos encontrar en los hosts de los que somos responsables (Costas, 2014).

Fortalecimiento del Sistema Operativo

Cuando nos referimos al fortalecimiento del sistema operativo uno de los principales objetivos es reducir la cantidad de vías disponibles a través de las cuales nuestro sistema operativo podría ser atacado. Existen áreas que deben ser analizadas y

que se conocen como superficie de ataque. Cuanto mayor sea nuestra superficie de ataque, mayores serán las posibilidades de que un atacante penetre con éxito nuestras$ defensas. Cada área en la que estamos potencialmente inseguros se suma a nuestra superficie de ataque, y cada área en la que hemos aplicado medidas de seguridad, la disminuye.

Hay seis formas principales con las que podemos disminuir nuestra superficie de ataque:

☑ Eliminar software innecesario.

☑ Eliminar o desactivar servicios no esenciales.

☑ Hacer modificaciones a cuentas comunes.

☑ Aplicando el principio de menor privilegio.

☑ Aplicar actualizaciones de software de manera oportuna.

☑ Hacer uso de las funciones de registro y auditoría.

Claro está, Siempre debemos tener mucho cuidado al realizar cambios en la configuración del sistema operativo, las herramientas y el software. Algunos de los cambios que podríamos hacer podrían tener efectos no deseados en la forma en que funciona nuestro sistema operativo, y una máquina en producción no es el lugar para aprender esto a través de la experiencia. Siempre es una buena idea investigar los cambios cuidadosamente antes de hacerlos y probarlos en un ambiente controlado con máquinas virtuales, por ejemplo.

Eliminar todo el software innecesario

Cada pieza de software instalada en nuestro sistema operativo se agrega a nuestra superficie de ataque. Algunos programas pueden tener un efecto mucho mayor que otros, pero todos suman. Si realmente estamos buscando fortalecer nuestro sistema operativo, debemos analizar detenidamente el software que debería instalarse en él y tomar medidas para asegurarnos de que estamos trabajando con lo necesario.

Si estamos preparando un servidor web, por ejemplo, deberíamos tener el software del servidor web, las bibliotecas o los intérpretes de código necesarios para admitir el servidor web y las utilidades que se ocupan de la administración y el mantenimiento del sistema operativo, como software de respaldo, herramientas de acceso remoto, entre otros. Realmente no tenemos ninguna razón para instalar nada más si el sistema realmente va a funcionar únicamente como un servidor web.

Nuestros problemas comienzan a surgir cuando vemos otro software instalado en el host, a menudo con las mejores intenciones. Por ejemplo, supongamos que uno de nuestros desarrolladores inicia sesión de forma remota y necesita realizar un cambio en una página web sobre la marcha, por lo que instalan el software de desarrollo web que necesitan. Luego, deben evaluar los cambios, por lo que instalan su navegador web favorito y los complementos multimedia asociados, como Adobe Flash (si todavía anda por ahí) y Acrobat Reader, así como un reproductor de video para probar el contenido del video. En muy poco tiempo, no solo tenemos software que no debería estar allí, sino que el software se desactualiza rápidamente, porque no está instalado "oficialmente" por lo que no está dentro de los planes de actualización y mantenimiento. En este punto, tenemos un problema de seguridad relativamente serio en un host con conexión a Internet.

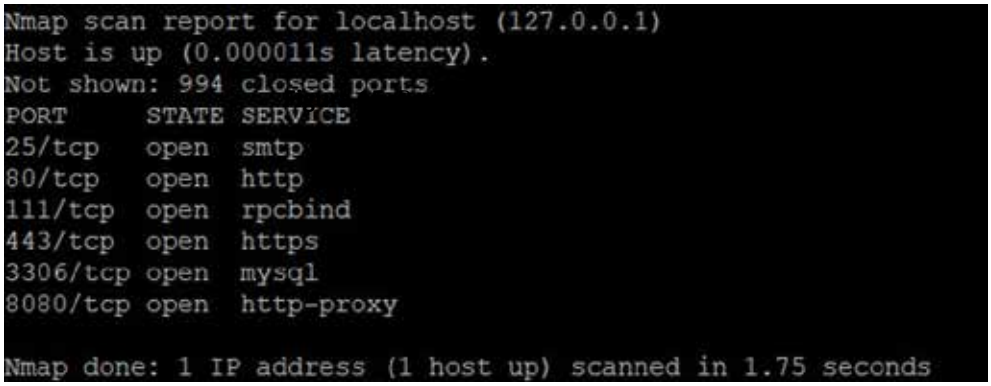
Eliminar todos los servicios no esenciales

En la misma línea que eliminar software innecesario, también deberíamos eliminar o deshabilitar servicios no esenciales. Muchos sistemas operativos se envían con una amplia variedad de servicios activados para compartir información a través de la red, localizar otros dispositivos, sincronizar la hora, permitir el acceso y la transferencia de archivos y realizar otras tareas. También podemos encontrar que los servicios han sido instalados por diversas aplicaciones para proporcionar las herramientas y los recursos de los que depende para funcionar.

Desactivar los servicios operativos puede ser un ejercicio de experimentación y frustración ya que en muchos casos, dichos servicios no se nombran de una manera que indique su función real y rastrear lo que cada uno de ellos está haciendo puede requerir un poco de investigación. Una de las mejores cosas que hacer primero cuando buscamos ubicar estos servicios extraños es determinar los puertos de red en los que el sistema realmente está escuchando las conexiones de red. Muchos sistemas operativos tienen utilidades integradas que nos permitirán hacer esto, como netstat en los sistemas operativos de Microsoft, pero también podemos usar Nmap para tales tareas.

Como discutimos en el capítulo 6, Nmap puede permitirnos descubrir los dispositivos en nuestras redes, pero también puede permitirnos determinar en qué puertos de red está escuchando un sistema determinado. Si ejecutamos el siguiente comando Nmap: nmap dirección_IP, veremos resultados similares a los que se muestran en la Figura 15.

Figura 15. Resultado de escaneo Nmap.



Fuente: elaboración propia.

En este caso, podemos señalar inmediatamente varios servicios comunes que se ejecutan en el destino, entre ellos:

Puerto 25: servicio para envío de correo electrónico a través del protocolo SMTP.

Puerto 80: servicio para el protocolo de transferencia de hipertexto (HTTP), que ofrecer contenido web, es decir un servidor web.

Puerto 443: servicio para el protocolo de transferencia de hipertexto seguro (HTTPS), que funciona para habilitar sitios y aplicaciones web protegidas con Secure Sockets Layer (SSL) y / o Transport Layer Security (TLS).

Puerto 3306: servicio para la ejecución de un servidor gestor de base de datos llamado MySQL.

También hay otros puertos abiertos que ejecutan varios servicios. Podemos utilizar esta información como punto de partida para cerrar servicios no deseados.

Alterar cuentas predeterminadas

Una debilidad común en muchos sistemas operativos es el uso de cuentas conocidas como estándar. En muchos sistemas operativos, podemos encontrar el equivalente de una cuenta de invitado y una cuenta de administrador. También podemos encontrar una variedad de otros, incluidos aquellos destinados al uso de personal de soporte, para permitir que los servicios o utilidades operen, y una gran cantidad de otros, que varían ampliamente según el proveedor del sistema operativo, la versión, entre otros. Dichas cuentas se denominan comúnmente cuentas predeterminadas.

En algunos casos, las cuentas predeterminadas pueden venir equipadas con permisos

excesivamente liberales para regular las acciones que se les permite llevar a cabo, lo que puede causar muchos problemas cuando los utiliza un atacante informado. También podemos encontrar que las cuentas predeterminadas se configuran con una contraseña particular o sin contraseña. Si permitimos que esas cuentas permanezcan en el sistema con su configuración predeterminada, es posible que dejemos las puertas proverbiales que protegen el acceso a nuestro sistema de manera abierta para que los atacantes puedan simplemente entrar y sentirse como en casa.

Las medidas típicas que tomaríamos para mitigar tales riesgos de seguridad son generalmente muy simples de llevar a cabo. Primero debemos decidir si las cuentas son necesarias, y deshabilitar o eliminar las que no usaremos. En el caso de las cuentas de invitados, las cuentas de soporte y otras de naturaleza similar, a menudo podemos desactivar las cuentas de forma rápida y fácil o eliminarlas por completo sin causarnos problemas. En el caso de las cuentas administrativas, a menudo con nombres como administrador, administrador o root, es posible que no podamos eliminarlas del sistema de manera segura o que el sistema operativo nos impida hacerlo. Sin embargo, en la mayoría de los casos, se puede cambiar el nombre de esas cuentas para confundir a los atacantes que podrían intentar hacer uso de ellas. Por último, no debemos dejar ninguna cuenta con una contraseña predeterminada, sin importar su estado.

Aplicar el principio de menor privilegio

Como discutimos en el Capítulo 3, el principio del privilegio mínimo dicta que solo le permitimos a una parte el permiso mínimo absoluto necesario para llevar a cabo su función. Dependiendo del sistema operativo en cuestión, podemos encontrar esta idea puesta en práctica en mayor o menor medida. En casi cualquier sistema operativo moderno, podemos encontrar las tareas que un usuario en particular puede llevar a cabo separadas en aquellas que requieren privilegios administrativos y aquellas que no.

En general, los usuarios normales del sistema operativo pueden leer y escribir archivos, y tal vez ejecutar scripts o programas, pero están limitados a hacerlo dentro de una determinada porción restringida del sistema de archivos. Por lo general, los usuarios normales no pueden realizar tareas como modificar la forma en que funciona el hardware, realizar cambios en los archivos de los que depende el sistema operativo, instalar software que pueda cambiar o afectar todo el sistema operativo. Dichas actividades están generalmente restringidas a aquellos usuarios a los que se les permite el acceso administrativo.

En la mayoría de los sistemas operativos similares a UNIX y Linux, a menudo podemos ver tales roles estrictamente aplicados. Aunque sería posible para el administrador de dicho sistema permitir que todos los usuarios actúen con los privilegios de un administrador, esto generalmente no es la convención y el acceso administrativo o "raíz" a menudo se protege cuidadosamente. En los sistemas operativos de Microsoft, a menudo podemos encontrar exactamente lo contrario para ser verdad. En un sistema operativo Windows, podemos encontrar que la mayoría de los usuarios autorizados para iniciar sesión directamente en el sistema operativo tienen derechos administrativos. Aunque no hay razones técnicas para tales diferencias comunes en los privilegios otorgados a las cuentas de usuario entre los dos sistemas operativos, generalmente existe una diferencia en la mentalidad de los usuarios y administradores que configuran dichas cuentas.

Cuando permitimos que el usuario promedio del sistema funcione regularmente con privilegios administrativos, quedamos a merced de una amplia gama de problemas de seguridad. Si el usuario ejecuta un archivo o aplicación infectado con malware, lo hace como administrador y ese programa tiene mucha más libertad para alterar el sistema operativo y otro software instalado en el host. Si un atacante compromete la cuenta de un usuario y se le han otorgado derechos administrativos a esa cuenta, ahora le hemos dado las claves de todo el sistema directamente al atacante. Casi cualquier tipo de ataque que podamos discutir, lanzado desde casi cualquier fuente, tendrá un impacto considerablemente mayor cuando se permita el acceso a los derechos administrativos en un host.

Si, en cambio, limitamos los privilegios en nuestros sistemas al mínimo necesario para permitir a nuestros usuarios realizar sus tareas requeridas, vamos a mitigar muchos problemas de seguridad. En muchos casos, los ataques fallarán por completo cuando un atacante intente ejecutarlos desde una cuenta de usuario que se ejecute con un conjunto limitado de permisos. Esta es una medida de seguridad muy barata y fácil que podemos implementar, y es fácil de implementar.

Realizar actualizaciones

Las actualizaciones periódicas y oportunas de nuestros sistemas operativos y aplicaciones son fundamentales para mantener una seguridad sólida. Los nuevos ataques se publican regularmente, y si no aplicamos los parches de seguridad lanzados por los proveedores que fabrican nuestros sistemas operativos y aplicaciones, es probable que seamos víctimas muy rápidamente de una gran cantidad de ataques conocidos.

Podemos considerar los diversos elementos de malware que se propagan a través de Internet en cualquier momento como un excelente ejemplo de esta idea. Muchas piezas de malware pueden propagarse explotando vulnerabilidades conocidas que los proveedores de software han reparado hace mucho tiempo. Aunque vale la pena ser prudente cuando planea instalar actualizaciones de software y probarlas a fondo antes de hacerlo, generalmente no es prudente retrasar este proceso por mucho tiempo.

Uno de los momentos más cruciales para garantizar que hayamos parcheado correctamente un sistema es directamente después de que hayamos terminado de instalarlo. Si conectamos un sistema recién instalado y completamente sin parchear a nuestra red, podemos verlo atacado y comprometido en muy poco tiempo, incluso en redes internas. La mejor práctica comúnmente considerada en tal situación es descargar los parches en medios extraíbles y usar estos medios para parchear el sistema antes de conectarlo a una red.

Activar registro y auditoría

Por último, pero no menos importante, debemos configurar y activar las funciones de registro y auditoría apropiadas para nuestro sistema operativo. Aunque los detalles sobre cómo configuramos dichos servicios pueden variar ligeramente según el sistema operativo en cuestión y el uso que se le dé al sistema, generalmente necesitamos poder mantener un registro preciso y completo de lo importante procesos y actividades que tienen lugar en nuestros sistemas operativos. En general, queremos registrar eventos importantes, como el ejercicio de privilegios administrativos, los usuarios que inician y cierran sesión en el sistema, o que no inician sesión, los cambios realizados en el sistema operativo y una serie de actividades similares que tienen lugar durante la operación diaria.

Dependiendo del entorno en el que colocaremos el sistema, es posible que también deseemos incluir características adicionales para complementar las herramientas integradas en el sistema operativo para estos fines. Es posible que queramos instalar una variedad de herramientas de monitoreo que vigilan la funcionalidad del sistema y nos alertan sobre problemas con el sistema en sí o anomalías que pueden aparecer en los diversos registros del sistema o de la aplicación. Es posible que también deseemos instalar una arquitectura de registro adicional para monitorear las actividades de múltiples máquinas, o simplemente permitir que se mantengan copias remotas duplicadas de registros fuera del sistema para ayudar a garantizar que tengamos un registro inalterado de las actividades. eso podría haber tenido lugar

en el sistema. También es importante tener en cuenta que la revisión de los registros es una parte vital del proceso. Si recopilamos registros pero nunca los revisamos, es mejor que no los recopilemos en absoluto, pues sería inútil.

Protección contra malware

Una gran preocupación en la actualidad es el número alucinante y la variedad de malware presente en las redes, sistemas y dispositivos de almacenamiento en todo el mundo. Usando tales herramientas, los atacantes pueden deshabilitar sistemas, robar datos, realizar ataques de ingeniería social, chantajear a los usuarios, reunir inteligencia y realizar una serie de otros ataques.

Un buen ejemplo de un elemento de malware particularmente complejo e impactante para examinar es el conocido Emotet, diseñado para registrar datos personales y robar datos financieros (SophosLabs Research Team, 2019).

Herramientas antimalware

La mayoría de las aplicaciones antimalware detectan amenazas de la misma manera que lo hacen los IDS que discutimos en el capítulo 6: ya sea haciendo coincidir una firma o detectando actividades anómalas que tienen lugar. Las herramientas antimalware tienden a depender más de las firmas que de la detección de anomalías, que en el campo antimalware generalmente se denomina heurística. Las firmas de malware generalmente son actualizadas por el proveedor de la aplicación al menos una vez al día y pueden actualizarse con mayor frecuencia si eso fuera necesario.

Las herramientas antimalware generalmente detectan el malware de una de las dos formas principales: detectando la presencia o el tráfico indicativo de malware en tiempo real, o realizando análisis de los archivos y procesos que ya están en el sistema. Cuando se encuentra malware, las respuestas de la herramienta antimalware pueden incluir eliminar cualquier proceso asociado y eliminar los archivos, eliminar los procesos y poner en cuarentena los archivos para que no puedan ejecutarse pero que no se eliminen, o simplemente dejar lo que sea que haya sido detectado, aunque solo dejar los archivos intactos no es una respuesta típica, pero puede ser necesario ya que las herramientas antimalware a veces detectan herramientas de seguridad y otros archivos que no son malware, que es posible que no queramos eliminar.

Podemos encontrar herramientas antimalware implementadas en sistemas operativos de host y en una variedad de servidores, de forma habitual para entornos empresariales, con el fin de protegerlos contra actividad de malware. También podemos encontrar dichas herramientas instaladas en servidores proxy para filtrar

el malware del tráfico entrante y saliente. Esto es muy común en el caso de los servidores proxy para correo electrónico, ya que muchos elementos de malware usan el correo electrónico como método de propagación. En el caso de que dicha herramienta detecte malware, podemos ver que el correo electrónico se rechaza por completo, o simplemente podemos ver el malware eliminado del cuerpo del mensaje o del archivo adjunto.

7.1. Muros de fuego de software y detección de intrusos de host

Además de las herramientas que podemos usar en la red para detectar y filtrar tráfico no deseado, como firewalls e IDS, podemos agregar otra capa de seguridad a nivel de host implementando un conjunto de herramientas muy similar aquí. Aunque a menudo podemos encontrar firewalls e IDS implementados a nivel de red en forma de dispositivos diseñados específicamente, las funciones reales que realizan generalmente se llevan a cabo a través de software especializado residente en los dispositivos. Se puede instalar un software similar directamente en los hosts que residen en nuestras redes.

Muros de fuego de software

Los firewalls de software configurados adecuadamente son una capa adicional de seguridad muy útil que podemos agregar a los hosts que residen en nuestras redes. Dichos cortafuegos generalmente contienen un subconjunto de las características que podríamos encontrar en un dispositivo de cortafuegos grande, pero a menudo son capaces de un filtrado de paquetes muy similar y una inspección de paquetes con estado. A menudo encontramos los conjuntos de reglas de tales aplicaciones expresados en términos de aplicaciones y puertos particulares permitidos para enviar y recibir tráfico en las diversas interfaces de red que existen en el host. Dichos softwares pueden ir desde las versiones relativamente simples que están integradas y se envían con sistemas operativos comunes, como Windows y Mac OS X, hasta versiones grandes destinadas a su uso en redes corporativas que incluyen monitoreo centralizado y la capacidad de mucho más reglas complejas y opciones de gestión.

Detección de intrusiones en el host

Los sistemas de detección de intrusos basados en el host (HIDS, por sus siglas en Inglés) se utilizan para analizar las actividades en o dirigidas a la interfaz de red de un host en particular. Tienen muchas de las mismas ventajas que tienen los sistemas de detección de intrusos basados en red (NIDS, por sus siglas en Inglés) pero con un alcance de operación considerablemente reducido. Al igual que con los firewalls

de software, dichas herramientas pueden variar desde versiones simples para el consumidor hasta versiones comerciales mucho más complejas que permiten un monitoreo y administración centralizados.

Una falla potencial con los HIDS administrados centralizadamente es que, para que el software informe un ataque al mecanismo de administración en tiempo real, la información debe comunicarse a través de la red. Si el host en cuestión está siendo atacado activamente a través de la misma red sobre la que informaríamos, es posible que no podamos hacerlo. Podemos intentar mitigar estos problemas enviando una baliza regular desde el dispositivo al mecanismo de administración, lo que nos permite asumir un problema si dejamos de ver múltiples dispositivos inesperadamente, pero esto podría no ser un enfoque completo.

Herramientas de seguridad del sistema operativo

Como discutimos en nuestra cobertura de las herramientas que podríamos usar para evaluar la seguridad de nuestra red en el Capítulo 6, también se pueden usar varias herramientas iguales o similares para evaluar la seguridad de nuestros hosts. Podemos usar escáneres para examinar cómo interactúan nuestros hosts con el resto de los dispositivos en la red, herramientas de evaluación de vulnerabilidad para ayudar a señalar áreas particulares donde podemos encontrar aplicaciones o servicios que pueden estar abiertos a ataques, y herramientas de escalada de privilegios para obtener acceso no autorizado a nuestros sistemas y varios marcos de explotación para permitirnos acceder a una amplia gama de herramientas y ataques que podrían ser utilizados por aquellos que intentan subvertir nuestra seguridad. Las herramientas que discutiremos en esta sección no se parecen a una lista exhaustiva, pero tocaremos algunos de los aspectos más destacados.

Escáneres

Podemos usar una gran cantidad de herramientas de escaneo para ayudar a detectar varios defectos de seguridad cuando estamos mirando hosts. Aunque discutimos esto en el Capítulo 6 desde una perspectiva de red, tales herramientas también se pueden usar para mejorar la seguridad de nuestros hosts. Podemos buscar puertos abiertos y versiones de servicios que se estén ejecutando, examinar etiquetas mostradas por los servicios para obtener información, examinar la información que muestran nuestros sistemas en la red y realizar una gran cantidad de tareas similares.

Anteriormente en este capítulo, cuando estábamos discutiendo el fortalecimiento, vimos un ejemplo muy simple de usar Nmap para mirar un dispositivo a través de

la red para descubrir los puertos que tenían servicios que los escuchaban. Nmap en realidad tiene un conjunto de funcionalidades muy amplio y amplio y puede brindarnos mucha más información si se lo solicitamos. Le podemos pedir a Nmap que también busque las versiones particulares de los servicios y aplicaciones que encontró y que también intente identificar el sistema operativo que se ejecuta en el dispositivo. Además, también existe la herramienta Nessus para realizar evaluaciones de seguridad.

7.2. Resumen

Una de las principales técnicas que podemos utilizar en nuestros esfuerzos para asegurar los sistemas operativos de los que somos responsables es el fortalecimiento o el hardening como se conoce en Inglés. Las tareas principales, cuando buscamos fortalecer un sistema operativo, son eliminar todo el software innecesario, eliminar todos los servicios no esenciales, alterar las cuentas predeterminadas en el sistema, utilizar el principio de privilegio mínimo, aplicar actualizaciones al software de manera apropiada y registro y auditoría de conductos.

También podemos aplicar varias capas adicionales de seguridad a nuestros sistemas operativos en forma de software adicional. Podemos instalar herramientas antimalware en un esfuerzo por detectar, prevenir y eliminar el malware cuando lo encontremos. Podemos utilizar la tecnología de firewall directamente en nuestros hosts para filtrar el tráfico no deseado a medida que entra o sale de nuestras interfaces de red. También podemos instalar HIDS para detectar ataques a medida que nos llegan a través de la red.

En nuestros esfuerzos por proteger nuestros sistemas operativos, podemos utilizar una variedad de herramientas para encontrar las fallas de seguridad que puedan estar presentes. Hay varias herramientas de escaneo disponibles, siendo Nmap una de las más conocidas. También podemos utilizar herramientas de evaluación de vulnerabilidades para localizar fallas de seguridad específicas en nuestros servicios o software habilitado para redes, como Nessus.

7.3. Cuestionario de estudio

1. ¿Qué es un vector para la propagación de malware?
2. ¿Cuál es la diferencia entre un escáner de puertos y una herramienta de evaluación de vulnerabilidad?
3. Explique el concepto de una superficie de ataque.

4. ¿Por qué podríamos querer un firewall en nuestro host si ya existe uno en la red?
5. ¿Qué es el fortalecimiento del sistema operativo?
6. ¿Qué hace la protección del espacio ejecutable por nosotros?
7. ¿Cómo se aplica el principio de privilegio mínimo al sistema operativo?

REFERENCIAS BIBLIOGRÁFICAS

Anirudh, M., Thileeban, S. A., y Nallathambi, D. J. (2017). Use of honeypots for mitigating DoS attacks targeted on IoT networks. In *2017 International conference on computer, communication and signal processing (ICCCSP)* (pp. 1-4). IEEE.

Arana, J. R., Villa, L. A., y Polanco, O. (2013). Implementación del control de acceso a la red mediante los protocolos de autenticación, autorización y auditoría. *Ingeniería y Competitividad, 15*(1), 127-137.

Cadena, R. (2017). ¿Por qué desconfiar de los dispositivos de almacenamiento digital? 3c Tecnología: *glosas de innovación aplicadas a la pyme, 6*(1), 35-46.

Calderon, P. (2017). *Nmap: Network Exploration and Security Auditing Cookbook.* Packt Publishing Ltd.

Chilán-Santana, E. I., y Pionce-Pico, W. F. (2017). Apuntes teóricos introductorios sobre la seguridad de la información. *Dominio de las Ciencias, 3*(4), 284-295.

Costas, J. (2014). *Seguridad informática.* RA-MA, SA.

De la Rocha, B., García, A., y Allende, H. (2017). Pulso Oxímetros: Conociendo el Nivel de Oxígeno en la Sangre. FINGUACH. *Revista de Investigación Científica y Tecnológica de la Facultad de Ingeniería de la Universidad Autónoma de Chihuahua, 4*(13), 10-11.

Fernández, D., y Casas, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias, 3*(3), 157-173.

Flores, J., Guarda, T., y Molina, L. (2019). Seguridad Informática en el Uso de los Nuevos Equipos Tecnológicos. *Revista Ibérica de Sistemas e Tecnologias de Informação,* (E17), 32-38.

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., y Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. *Polo del conocimiento, 2*(12), 145-155.

Fournaris, A. P., y Keramidas, G. (2014). From hardware security tokens to trusted computing and trusted systems. In *System-level design methodologies for telecommunication* (pp. 99-117). Springer, Cham.

Harmening, J. T. (2017). Virtual private networks. In *Computer and Information*

Security Handbook (pp. 843-856). Morgan Kaufmann.

Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., y Atkinson, R. (2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. In *2016 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1-6). IEEE.

Huang, X., Xiang, Y., Bertino, E., Zhou, J., y Xu, L. (2014). Robust multi-factor authentication for fragile communications. *IEEE Transactions on Dependable and Secure Computing, 11*(6), 568-581.

ISO/IEC 27000. (2016). Information technology–Security techniques–Information security management systems–Overview and vocabulary. https://www.iso.org/standard/66435.html

Jain, A. K., Ross, A. A., y Nandakumar, K. (2011). *Introduction to biometrics.* Springer Science & Business Media.

Javaid, A., Niyaz, Q., Sun, W., y Alam, M. (2016). A deep learning approach for network intrusion detection system. In *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)* (pp. 21-26).

Jeong, C. Y., Lee, S. Y. T., y Lim, J. H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management, 56*(5), 681-695.

Morales, Y. J., y Torres, C. O. (2009). Correlación digital de imágenes comprimidas por transformada wavelet. *Bistua: Revista de la Facultad de Ciencias Básicas, 7*(1), 1-5.

Moradi, M., y Keyvanpour, M. (2015). CAPTCHA and its Alternatives: A Review. *Security and Communication Networks, 8*(12), 2135-2156.

Parra, M., y Guillén, E. (2019). Servicios de autenticación y autorización orientados a internet de las cosas. *Telemática, 17*(2), 42-51. https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/302

Parada, D., Flórez, A., y Gómez, U. (2018). Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas. *Información tecnológica, 29*(1), 27-38.

Pawar, M., y Anuradha, J. (2015). Network security and types of attacks in network. *Procedia Computer Science, 48,* 503-506.

Seaman J. (2020). PCI DSS Applicability. En *PCI DSS.* Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-5808-8_7

Solarte, F., Rosero, E., y del Carmen, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL, 28*(5).

SophosLabs Research Team. (2019). Emotet exposed: looking inside highly destructive malware. *Network Security, 2019*(6), 6-11.

Tchernykh, A., Schwiegelsohn, U., Talbi, E. G., y Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science, 36,* 100581.

Tejada, E. (2019). *Auditoría de seguridad informática. IFCT0109.* IC Editorial.

Urbina, G. (2016). *Introducción a la seguridad informática.* Grupo editorial PATRIA.

Vega, E. (2020). *Planificación y ejecución de evaluaciones de seguridad informática desde un enfoque de ethical hacking.* Editorial 3Ciencias.

Wang, Q., Dunlap, T., Cho, Y., y Qu, G. (2017, April). DoS attacks and countermeasures on network devices. In *2017 26th Wireless and Optical Communication Conference (WOCC)* (pp. 1-6). IEEE.

Zambrano, S., y Valencia, D. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias, 3*(3), 676-688.

TIC's

3ciencias