en cs de sk es

TECH pedia

SISTEMAS DE SEGURIDAD MODERNOS

MIGUEL SORIANO

Título: Sistemas de seguridad modernos
Autor: Miguel Soriano
Publicado por: České vysoké učení technické v Praze
Fakulta elektrotechnická
Dirección de contacto: Technická 2, Praha 6, Czech Republic
Número de teléfono: +420 224352084
Print: (only electronic form)
Número de páginas: 44
Edición: Primera edición, 2017

ISBN 978-80-01-06209-8

TechPedia
European Virtual Learning Platform for
Electrical and Information Engineering

http://www.techpedia.eu

Erasmus+

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea.
Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.

NOTAS EXPLICATIVAS

	Definición
	Interesante
	Nota
	Ejemplo
	Resumen
	Ventajas
	Desventajas

ANOTACIÓN

Este módulo contiene información necesaria para que los estudiantes consigan una orientación básica en el ámbito de la seguridad de la red, incluyendo servicios de seguridad, mecanismos de seguridad, tipos de atacantes, amenazas a la seguridad. Además, conseguirá tener una idea básica de los componentes que debe tener un sistema de seguridad de la red.

OBJETIVOS

Este módulo proporciona una visión general de los sistemas de seguridad modernos. Se divide en seis bloques o capítulos.

El primer capítulo introduce los conceptos de seguridad de red, servicios de seguridad, mecanismos de seguridad,... La segunda es una visión general de las amenazas de seguridad de red, introduciendo los conceptos de virus, gusanos, caballos de Troya; software espía ("spyware") y publicitario ("adware"); ataques de día cero; ataques de denegación de servicio; intercepción y robo de datos; suplantación de identidad...

El tercer capítulo contiene una descripción de algunos de los componentes de un sistema de seguridad de la red (antivirus, cortafuegos, sistemas de detección de intrusiones, VPN,...). El cuarto capítulo presenta otras soluciones para ofrecer seguridad (por ejemplo, métodos de autenticación fuerte, fortalecimiento del sistema operativo, protección de servicios web,...)

Por último, hay un capítulo dedicado a la seguridad móvil. Los teléfonos inteligentes juegan un papel muy importante en las comunicaciones modernas; nadie duda de la importancia de los teléfonos inteligentes en nuestras vidas. La naturaleza de estos dispositivos, que permiten la convivencia en un dispositivo de servicios de telefonía y de transmisión de datos, genera la posibilidad de nuevos tipos de ataques. En este capítulo se muestra cómo un hacker puede aprovecharse de un teléfono inteligente comprometido.

LITERATURA

[1] CVE. A dictionary of publicly known information security vulnerabilities and exposures. http://cve.mitre.org; 2015

[2] W. Cheswick and S. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, 1994. ISBN

[3] E. D. Zwicky, S. Cooper, and D. B. Chapman. *Building Internet Firewalls.* O'Reilly and Associates, 2nd edition, 2000. ISBN.

[4] João Porto De Albuquerque , Paulo Lício De Geus "A Framework for Network Security System Design" .

[5] L. Bilge and T. Dumitraș, “Before we knew it: An empirical study of zero-day attacks in the real world,” in ACM Conference on Computer and Communications Security, Raleigh, NC, 2012, pp. 833–844.

[6] Kim Zetter. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* Crown Publishers, 2014. ISBN: 978-0-7704-3617-9

[7] Adeyinka, O., "Internet Attack Methods and Internet Security Technology,", 2008. AICMS 08. Second Asia International Conference on Modeling & Simulation pp.77-82, ISBN: 978-0-7695-3136-6

[8] Thomas W. Shinder The Best Damn Firewall Book Period (Second Edition), Syngress Publishing Inc. 2007. ISBN: 978-1-59749-218-8

[9] Karen Scarfone, Paul Hoffman. Guidelines on Firewalls and Firewall Policy. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-41, Revision 1. Sept. 2009

[10] Eric Geier “Intro to Next Generation Firewalls” http://www.esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html September, 2011

[11] Cliff, A.: “Password Crackers - Ensuring the Security of Your Password”, Security Focus, Feb. 19, 2001. http://online.securityfocus.com/infocus/1192

Indice

1 Introducción

No hay duda que el mundo está cada vez más interconectado gracias al auge de Internet y de las nuevas tecnologías de la información y comunicación. En los últimos años, empresas orientadas a Internet, o el comercio electrónico, han incrementado notablemente su eficiencia y sus ingresos. Sin embargo, a medida que los usuarios disponen de más aplicaciones que utilizan la red son cada vez más vulnerables frente a una gama mayor de amenazas a la seguridad. Por lo tanto, para combatir esas amenazas y para asegurar que las transacciones de red no se vean comprometidas, es cada vez más relevante disponer de herramientas y mecanismos de seguridad de red no sólo para empresas y entornos militares, sino también para las organizaciones y los usuarios de ordenadores personales.

En el pasado, los hackers eran programadores altamente cualificados que conocían al detalle las aplicaciones y comunicaciones informáticas y de esta manera se aprovechaban de las vulnerabilidades. Hoy en día casi cualquier persona puede convertirse en un hacker gracias a la descarga a través de Internet de determinadas herramientas. Estas herramientas han generado una mayor necesidad de políticas de seguridad dinámicas y seguridad de la red. Muchas organizaciones tratan de clasificar la vulnerabilidad y sus consecuencias: una base de datos de la vulnerabilidad más famosa es la National Vulnerability Database de la corporación MITRE [1].

El ámbito de la seguridad de la red todavía está en una etapa creciente; los incidentes de seguridad están aumentando a un ritmo alarmante cada año. A pesar de los avances significativos en el estado del arte de la red y de la seguridad informática en los últimos años, los sistemas son más vulnerables que nunca. Cada avance tecnológico en el ámbito de la informática puede dar lugar a nuevas amenazas que requieren nuevas soluciones de seguridad. A medida que la complejidad de las amenazas aumenta, también lo hacen las medidas de seguridad necesarias para proteger las redes.

1.1 ¿Qué es la seguridad de red?

La seguridad de la red se refiere a cualquiera actividad diseñada para proteger la red. En concreto, estas actividades protegen la usabilidad, fiabilidad, integridad y seguridad de la red y datos. La seguridad de la red se ha convertido en un requisito para todas las comunicaciones que afectan a negocios, especialmente a aquellos que dependen de Internet.

Los clientes, proveedores y socios de negocios necesitan la protección de toda la información compartida, especialmente la información que se considera sensible, como números de tarjetas de crédito o detalles confidenciales de la empresa.

La seguridad de la red no sólo se refiere a la seguridad en los ordenadores en cada extremo de la comunicación. Cuando se transmiten datos, el canal de comunicación no debe ser vulnerable a los posibles ataques. Un posible hacker podría intentar analizar la información que circula por el canal de comunicación, con el fin de obtener los datos e incluso reinsertar un mensaje falso. Proteger la red es tan importante como proteger los ordenadores y cifrar el mensaje.

La seguridad de la red es un prerrequisito para el buen funcionamiento de cualquier negocio en Internet. Un requisito de seguridad importante es evitar la denegación de servicio; el tiempo de inactividad de la red es costoso para todo tipo de empresas. La seguridad efectiva permite a una empresa agregar nuevos servicios y aplicaciones sin interrumpir el funcionamiento de la red. La salvaguarda de datos es un enfoque proactivo necesario para evitar la interrupción de servicios al cliente, incluso cuando se están produciendo las modificaciones.

Algunos de los beneficios que una empresa obtiene a través de redes seguras son: la confianza del cliente (privacidad de usuario), movilidad (acceso seguro sin que aparezcan virus u otras amenazas), la mejora de la productividad (por ejemplo, menos pérdida de tiempo en tareas no productivas como correo no deseado o antivirus), y economía (el tiempo de inactividad de la red es costoso para todo tipo de empresas).

1.2 ¿Qué es un sistema de seguridad para la red?

Un sistema de seguridad para la red es un conjunto de dispositivos, ya sean hardware o software, que utilizan algoritmos criptográficos y protocolos seguros para proteger los sistemas de información y comunicación de una empresa.

Algunas funciones de estos dispositivos son la supervisión y control del tráfico entrante y saliente a la red, detección de ataques, protección de la infraestructura de red incluyendo el rendimiento del ancho de banda de la red; protección frente al robo de datos, seguridad y continuidad del servicio frente ataques de denegación de servicio,...

A medida que aumentan las necesidades de seguridad de las organizaciones, los sistemas de seguridad de red se vuelven más complejos y los enfoques tradicionales deben ser adaptados, siendo necesaria la incorporación de mecanismos distribuidos para reforzar la seguridad, la gestión de la confianza descentralizada, y el uso ampliamente extendido de técnicas criptográficas (como IPSec y redes privadas virtuales).

Por otra parte, el sistema de seguridad de la red es sólo una pequeña parte (aunque muy importante) de la infraestructura de seguridad de información de una organización y debe ser contemplada junto con la seguridad en otros ámbitos, como son, la seguridad física, la seguridad personal, seguridad en las operaciones, y mecanismos sociales.

1.3 Servicios de seguridad

Un servicio de seguridad es un servicio que garantiza un nivel de seguridad adecuado a los sistemas o a las transferencias de datos. Los servicios de seguridad son implementados mediante los mecanismos de seguridad, de acuerdo con las políticas de seguridad.

Durante más de veinte años, la seguridad de la información incluía como principios básicos de la seguridad de la información, la confidencialidad, integridad y disponibilidad (conocida como la tríada de la CIA). Más tarde, se añadieron otros elementos de seguridad de la información a los tres atributos de seguridad clásicos de la tríada de la CIA. Estos elementos son la autenticación, control de acceso, no repudio, y la privacidad. Sin embargo, esta clasificación es objeto de debate entre los profesionales de la seguridad.

- La confidencialidad se refiere a la protección de la información frente a su divulgación a entidades no autorizadas (organizaciones, personas, máquinas y procesos). El objetivo de este servicio es que nadie pueda leer la información enviada, a excepción de la entidad (o entidades) destinataria previstas. Dicha información incluye no sólo datos, sino también tamaño, existencia, características de comunicación, etc.

- Integridad de datos es la protección de los datos frente a la creación, modificación, supresión, duplicación o la reordenación por parte de entidades no autorizadas (organizaciones, personas, máquinas y procesos). La violación de la integridad siempre tiene su origen en ataques activos.

- Disponibilidad significa garantizar el acceso a la información o recursos a los que un usuario o entidad tiene derecho. Así pues, por ejemplo, un disco estropeado o un ataque de denegación de servicio suponen una violación de la disponibilidad. Asimismo, retrasos superiores a los esperados o establecidos en los niveles de calidad de servicio, puede ser calificados como una violación de la disponibilidad. Un sistema de información que no está disponible cuando se necesita por lo menos es tan malo como la ausencia de sistema.

- El servicio de autenticación se ocupa de asegurar que las identidades de las entidades comunicantes están garantizadas. Los parámetros que permiten la autenticación pueden clasificarse en tres categorías distintas. Esos parámetros típicamente son: algo que uno sabe (conocimiento), algo que uno tiene (posesión), o algo que uno es (inherencia). Los parámetros de conocimiento incluyen cosas que un usuario debe conocer para iniciar la sesión, por ejemplo una contraseña. Los parámetros de posesión incluyen cualquier cosa que un usuario debe tener en su poder para iniciar la sesión, por ejemplo, una tarjeta. Los parámetros de inherencia incluyen las características biológicas que tiene un usuario (por ejemplo, huella dactilar).

- El control de acceso es la protección de los recursos o servicios de información frente al acceso o uso no autorizado por parte de entidades (organizaciones, personas, máquinas y procesos). Es decir, el control de acceso se refiere a la prevención del uso no autorizado de un recurso. Así pues, este servicio controla

quien puede tener acceso a ciertos recursos, en qué condiciones puede acceder, y que se puede hacer en estos accesos (por ejemplo, posibilidad de leer un documento o de modificarlo).

- No repudio es un servicio de seguridad que utiliza evidencias para proporcionar protección contra la denegación por parte de alguna de las entidades participantes en una comunicación de haber participado en toda o parte de esa comunicación.

- Privacidad de los datos es el servicio de seguridad que permite a un individuo mantener el derecho a controlar la información sobre él, cómo se utiliza y quien lo utiliza.

1.4 Mecanismos de seguridad

Los mecanismos de seguridad son procesos que implementan los servicios de seguridad basados en un enfoque hardware, software, físico o administrativo. Dichos mecanismos dan soporte a los servicios de seguridad y ejecutan actividades específicas para la protección contra los ataques o contra los resultados de un ataque.

Los mecanismos de seguridad se dividen en aquellos que se implementan en una capa de protocolo específico y aquellos que no son específicos para una capa de protocolo concreta o servicio de seguridad

Algunos de los mecanismos de seguridad son:

- Cifrado: es un mecanismo destinado a la protección del contenido de un mensaje mediante el uso de algoritmos matemáticos que transforman los datos en una forma que no es legible por usuarios o entidades no autorizadas.
- Firma digital: es un mecanismo que utiliza una transformación criptográfica de un mensaje para probar tanto su origen como su integridad y por tanto, ofreciendo protección contra la falsificación.
- Control de acceso: abarca una variedad de mecanismos que establecen la política de derechos de acceso a los recursos. Este mecanismo requiere la autenticación y posteriormente la autorización para acceder a los recursos que se desee proteger.
- Integridad de datos: abarca una variedad de mecanismos utilizados para asegurar la integridad de un mensaje o de un flujo de datos.
- Intercambio de autenticación: el objetivo de este mecanismo es asegurar la identidad de una entidad mediante un intercambio de información.
- Tráfico de relleno: es un mecanismo que inserta bits en un flujo de datos para impedir que tenga éxito un ataque por análisis de tráfico.
- Control de encaminamiento permite que un mensaje cuando atraviesa una red de telecomunicación siga unos determinados enlaces y permite cambios en las rutas, especialmente cuando se detecta que hay un problema de seguridad. Este mecanismo también afecta a la seguridad perimetral.
- Notarización es un mecanismo que utiliza terceras partes de confianza para garantizar ciertas propiedades en un intercambio de datos.
- Seguridad perimetral es un mecanismo que permite aceptar o bloquear datos procedentes o destinados a un ordenador concreto ubicado fuera de la red local.

1.5 Clasificación de los atacantes

Las amenazas a la seguridad son potencialmente ejecutadas por los atacantes, que generalmente difieren en su capacidad y actividad. A continuación se resume brevemente qué propiedades se enmarcan bajo el nombre de capacidades y cuales en actividades, así como las clases de atacantes resultante de esta combinación.

Capacidad: La capacidad de un atacante normalmente se determina por:

- Coste. Relaciona el coste que un atacante requiere en términos de equipamiento para llevar a cabo un ataque con éxito. Este coste puede variar desde muy barato, (por ejemplo, sólo se requiere un soldador y algunos cables), a prohibitivamente alto, donde se necesita equipos extremadamente complejos y costosos.

- Habilidad. Por lo general, se refiere a los conocimientos que un atacante debe conocer para llevar a cabo un ataque exitoso. Algunos ataques pueden ser realizados por personal sin conocimientos, simplemente copiando un comando, mientras que otros pueden requerir un amplio conocimiento del servicio o protocolo particular de red, o bien una persona entrenada en el uso de algún equipo especial.

- Trazas. Este aspecto está relacionado con las huellas que deja por el atacante cuando realiza una acción ilegítima. Si después del ataque a un equipo, todo queda en el mismo estado que antes del ataque, incluyendo el contenido de la memoria, entonces es más difícil de saber que ha habido un ataque que en otras situaciones. El caso extremo opuesto sería aquel ataque que provoca la destrucción física de un equipamiento.

Actividad. En función de las actividades que se llevan a cabo en un ataque, éste se puede clasificar como pasivo o activo:

- Ataque pasivo. Un ataque pasivo es aquél en que el atacante monitoriza el canal de comunicación sin modificar ni añadir datos. Un atacante pasivo sólo pone en peligro la confidencialidad de los datos. El objetivo del atacante es obtener la información que se está transmitiendo. Estos ataques incluyen análisis de tráfico, monitorización de comunicaciones no protegidas, descifrado de tráfico encriptado y captura de información de autenticación, como passwords.

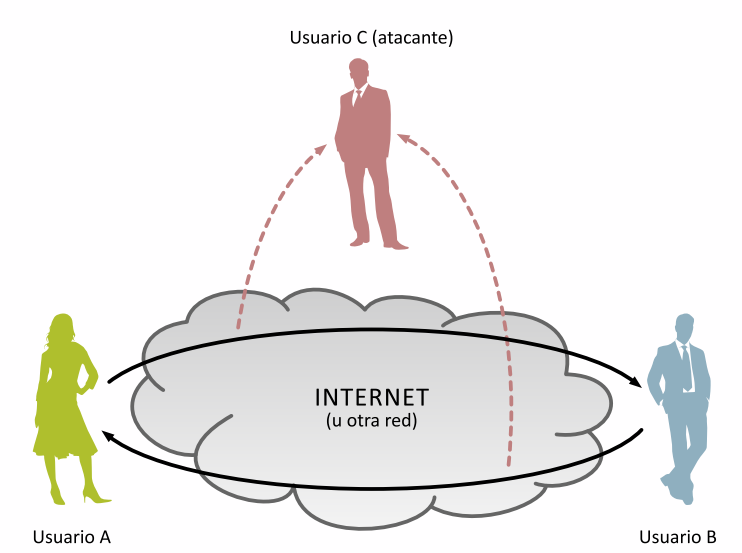

Fig. 1.1 – Ataque pasivo

- Ataque activo. Un ataque activo intenta alterar los recursos del sistema o afectar a su funcionamiento. En este tipo de ataque el adversario intenta borrar, añadir, o modificar los datos transmitidos. Un atacante activo amenaza la integridad de datos y autenticación, así como la confidencialidad. En algunas ocasiones, los ataques pasivos son actividades previas para preparar un ataque activo.

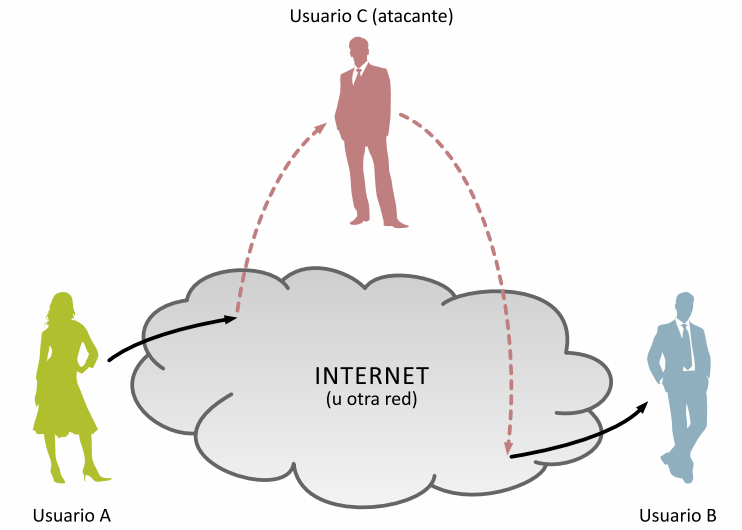

Fig. 1.2 – Ataque activo

Y también como ataques no invasivos, frente a semi-invasivos o invasivos:

- Ataques no invasivos. No manipulan el dispositivo.
- Ataques semi-invasivos. Manipulan a través del empaquetado del dispositivo, pero no establecen contacto eléctrico directo con la superficie del chip.

- Ataques invasivos. En estos casos no hay prácticamente ningún límite a las medidas adoptadas para extraer la información del dispositivo.

Debe tenerse en cuenta que no todos los ataques semi-invasivos o invasivos son ataques activos. Por ejemplo, los ataques semi-invasivos pasivos pueden tratar de capturar datos críticos de la memoria y ataques invasivos pasivo pueden utilizar una estación de sonda para detectar señales de datos valiosos. Ejemplos de ataques pasivos son el análisis de tráfico y monitorización. La mayoría de los ataques, sin embargo, son ataques activos, tales como ataques de enrutamiento, la suplantación de identidad, denegación de servicio, ataques físicos...

Clase. Para conjuntar tanto la capacidad como la actividad, IBM introdujo la siguiente taxonomía de clase de atacantes:

- Clase I (inteligentes y externos). A menudo son personas con muchos conocimientos de seguridad, pero pueden tener un conocimiento insuficiente del sistema que quieren atacar. Pueden tener acceso sólo a equipos moderadamente sofisticados. A menudo tratan de aprovecharse de una debilidad existente en el sistema, en lugar de tratar de buscar nuevas debilidades.

- Clase II (internos y con conocimientos). Tienen formación técnica especializada y experiencia notable. Pueden tener distinto nivel de comprensión de las partes del sistema, pero potencialmente pueden acceder a la mayor parte de equipos. A menudo tienen herramientas e instrumentos altamente sofisticados para el análisis.

- Clase III (organizaciones financiadas). Son capaces de formar equipos de especialistas con conocimientos relacionados y complementarios respaldados por grandes recursos económicos. Son capaces de analizar en profundidad un sistema, diseñar ataques sofisticados, y usar las herramientas de análisis más avanzados. Pueden utilizar atacantes de clase II como parte del equipo de ataque.

1.6 Terminología

Si bien no es posible proporcionar un glosario completo de términos relacionados con la seguridad de redes, se considera interesante describir algunos de los conceptos más habituales en este ámbito:

- Ataque. En el contexto de la seguridad informática / seguridad de red, un ataque es un intento de acceder a los recursos de un equipo informático o de una red sin autorización, o bien eludir las medidas de seguridad que han sido adoptadas.

- Auditoría. Conjunto de acciones que permiten llevar a cabo un seguimiento de eventos relacionados con la seguridad, tales como los accesos al sistema o a la red, acceso a determinados objetos, ...

- Ruptura. Superar las medidas de seguridad con la finalidad de acceder a datos o recursos sin autorización, o conseguir cambiar permisos de determinados recursos o borrar o modificar datos.

- Buffer. Zona de almacenamiento de datos.

- Buffer overflow (desbordamiento de buffer). Una manera de bloquear un sistema poniendo más datos en un buffer que los que dicho buffer es capaz de almacenar.

- Contramedidas. Medidas adoptadas para prevenir o responder a un ataque o código malicioso.

- Cracker. Un hacker que se especializa en descubrir las contraseñas del sistema para tener acceso a los sistemas informáticos sin autorización.

- Ataque de denegación de servicio. Una acción deliberada que consigue que un equipo o red deje de funcionar como se espera (por ejemplo, evitando que los usuarios sean capaces de conectarse a la red).

- Exposición. Medida del grado en que una red o equipo individual es vulnerable a los ataques, sobre la base de sus vulnerabilidades particulares y la duración de tiempo durante el que los intrusos tener la oportunidad de atacar.

- Hacker. Una persona que dedica tiempo en aprender los detalles de los sistemas de los equipos para poner a prueba los límites de sus capacidades e identificar las vulnerabilidades del sistema.

- Código malicioso. Un programa de ordenador o script que realiza una acción que daña intencionadamente a un sistema, o que permite conseguir un propósito no autorizado (por ejemplo, proporciona acceso al sistema a usuarios no autorizados.

- Fiabilidad. Probabilidad de que un sistema o una red lleve a cabo de forma sus actividades previstas de forma satisfactoria durante un período de tiempo específico en condiciones normales de funcionamiento.

- Riesgo. Producto de la probabilidad que una amenaza específica sea capaz de aprovechar una vulnerabilidad del sistema, lo que resulta en daños, pérdida de datos, u otros resultados no deseados por el valor del daño ocasionado por ese ataque potencial.

- Gestión de riesgos. El proceso de identificar, controlar, y, o bien minimizar o bien eliminar por completo los eventos que suponen una amenaza para la fiabilidad del sistema, integridad o confidencialidad de los datos.

- Sniffer. Un programa que captura los datos a medida que viajan a través de una red. También se denomina analizador de paquetes.

- Amenaza. Un peligro potencial de datos o sistemas. Una amenaza puede ser un virus; un hacker, un fenómeno natural, como un tornado; un empleado descontento; un competidor, ...

- Caballo de Troya. Un programa de ordenador que realiza una función deseable, pero contiene código oculto destinado a permitir la captura no autorizada, modificación o destrucción de datos.

- Virus. Software que se introduce en un sistema o red con el fin de realizar una acción no autorizada (desde aparecer un mensaje inofensivo hasta eliminar todos los datos del disco duro)

- Vulnerabilidad. Una debilidad en el hardware o software o incluso en la política de seguridad, que deja un sistema o red expuesta a la amenaza de acceso no autorizado, daño o destrucción de datos.

- Gusano. Un programa que se replica a sí mismo, difundiéndose de una máquina a otra a través de una red.

2 Amenazas a la seguridad de la red

Donde hay una red de telecomunicaciones, hay amenazas a su seguridad. Los tipos de amenazas potenciales a la seguridad de la red están en constante evolución; así pues, todo administrador de una red debe monitorizar constantemente todos los equipos y servicios. El hecho que la seguridad de la red se vea comprometida puede tener consecuencias graves, como la pérdida de privacidad, y el robo de información.

Es importante señalar que no todas las amenazas a la seguridad son malintencionadas. Las amenazas no maliciosas suelen proceder de empleados que no tienen suficiente formación y no son conscientes de las amenazas y vulnerabilidades de seguridad. Según qué tipo de errores y omisiones pueden ocasionar la revelación, pérdida o alteración de datos valiosos. Por otra parte, los desastres naturales también suponen amenazas que no son malintencionadas. En este capítulo, sólo se detallan las amenazas maliciosas a la seguridad.

Las amenazas malintencionadas consisten en ataques desde el interior por parte de usuarios internos descontentos y ataques desde el exterior de la red que sólo buscan dañar y/o interrumpir el correcto funcionamiento de una organización. Los atacantes más peligrosos son generalmente los internos (o los que fueron usuarios internos a la organización en un pasado) puesto que saben que las medidas de seguridad aplicadas.

Las herramientas y métodos de ataque a la red han evolucionado. En el pasado reciente (hace pocos años) un hacker debía tener además de ordenador, un conocimiento sofisticado de redes y de programación para diseñar herramientas rudimentarias y elaborar ataques básicos. Hoy en día, la red de hackers ha mejorado muchísimo sus métodos y herramientas, de forma que para realizar un ataque ya no se requiere el mismo nivel de conocimientos; por lo tanto personas que hace algunos años no hubieran podido ocasionar un delito informático, ahora sí pueden ser capaces de llevarlo a cabo.

La definición de "hacker " ha cambiado con los años. Antes se consideraba que un hacker era una persona que disfrutaba obteniendo los máximos recursos de un sistema al que estaba accediendo, o bien era capaz de acceder a sistemas para los que no tenían autorización o intencionalmente sobrepasaban sus límites en los sistemas para los que no tienen acceso legítimo. Actualmente, el término correcto a utilizar para alguien que rompe un sistema de seguridad informática es “cracker”. Los métodos comunes para acceder a un sistema incluyen averiguar contraseñas, explotar las debilidades de seguridad conocidas, suplantación de identidad en la red y la ingeniería social.

Existe una falta de comunicación entre los desarrolladores de tecnología de seguridad y desarrolladores de redes. Aunque la seguridad es un requisito crítico en las redes emergentes, existe una importante falta de métodos de seguridad que se pueden implementar fácilmente. En contraste con el diseño de red, el diseño de seguridad no está suficientemente maduro. No existe una metodología concreta

consensuada internacionalmente para gestionar la complejidad de los requisitos de seguridad.

Muchas de las amenazas actuales a la seguridad de la red se propagan a través de Internet. Es importante señalar que los terminales móviles inteligentes están conectados a Internet y por lo tanto, su seguridad es un tema absolutamente relevante.

2.1 Malware: virus, gusanos, troyanos y zombis

Software malicioso (malware) es un término genérico que hace referencia a cualquier software dañino instalado en un sistema, diseñado para ejecutar instrucciones no deseadas en un ordenador, sin el consentimiento del usuario. Dicho software puede causar pérdidas o daños en el sistema. Los virus informáticos son una tipología de software malicioso que se difunden entre ordenadores llevando a cabo operaciones que van en detrimento de las prestaciones de los equipos.

La ejecución de malware puede degradar la velocidad de las tareas que un usuario desea realizar en su ordenador y también puede obtener información crítica u obtener acceso no autorizado a un sistema informático. Malware no es lo mismo que software defectuoso, este último es software que tiene un propósito legítimo, pero contiene errores que no fueron detectados antes de su despliegue. De hecho, los virus informáticos son en realidad un subconjunto de la familia de malware, donde también se incluyen los gusanos, troyanos, adware, spyware, rootkits, etc...

De acuerdo con PandaLabs durante 2014, se detectaron más de 75 millones de nuevas muestras de malware, lo cual significa un 34 % del total y es más de dos veces la cantidad de nuevas muestras detectadas en 2013 (que fue de 30 millones). A continuación se presenta una definición de algunos de los tipos de malware más relevantes:

- Los virus son programas que se auto-replican que usan archivos para infectar y propagarse. Cuando se abre un archivo infectado, el virus se activa dentro del sistema.

- Un gusano es similar a un virus, ya que ambos se auto-replican, pero el gusano no requiere un archivo para su propagación. Estos programas fueron utilizados inicialmente con finalidades legítimos en el desempeño de funciones de gestión de red, gracias a su capacidad de auto-réplica, pero esta misma capacidad de multiplicarse rápidamente ha sido explotada por los hackers para crear gusanos maliciosos que aprovechan debilidades del sistema operativo para realizar acciones dañinas. Hay dos tipos principales de gusanos: gusanos de correo masivo y gusanos de red. Los gusanos de correo masivo utilizan el correo electrónico como un medio para infectar otros ordenadores. Los gusanos de red seleccionan un equipo objetivo de ataque y una vez que el gusano tiene acceso al host de destino, se pueden infectar por medio de un troyano o de otra manera.

- Los troyanos aparentan ser software benigno para el usuario, pero, de hecho, llevan a cabo acciones que el usuario del programa desconoce. Básicamente, el troyano se aprovecha de los privilegios y permisos que tiene el usuario en el sistema para realizar cualquier acción requiera dichos permisos. Esto significa que un troyano es especialmente peligroso si el usuario desprevenido que lo instala es un administrador y tiene acceso al sistema de archivos. Un tipo de malware que se propaga por lo general como un troyano es el conocido como ransomware. Este tipo de malware infecta el sistema informático, restringe el acceso a este equipo y exige que el usuario pague un rescate para los operadores del malware para eliminar la restricción.

- Un zombi es un software malicioso que se propaga a través de la red. Después de ser introducido en un sistema informático, aprovechando alguna debilidad, dicho equipo queda infectado y puede ser controlado y administrado a distancia. Cuando varios ordenadores están infectados por el mismo tipo de software malicioso, esto se conoce como red de bots. La botnet puede ser controlada desde un ordenador remoto y forzar a los equipos infectados a llevar a cabo un conjunto de órdenes (habitualmente idénticas en todos estos equipos). Esto permite los ataques DDoS (Distributed Denial of Service, Denegación de Servicio Distribuida).

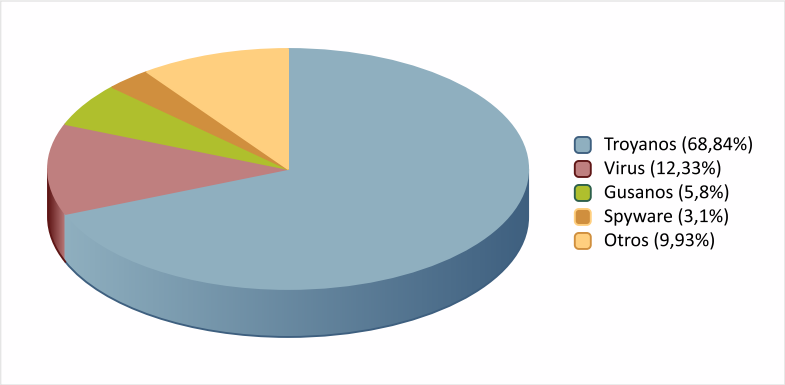

Fig. 2.1 – Tipos de nuevos malware creados durante 2014

2.2 Software espía (spyware) y software con publicidad (adware)

El término adware se refiere al software que muestra publicidad y se muestra al usuario incrustado en otra aplicación.

Adware es considerado como una alternativa legítima que se ofrece a los consumidores que no desean pagar por el software. Hay muchas aplicaciones, juegos o utilidades con soporte publicitario que se distribuyen como adware (o freeware). Hoy en día existe un creciente número de desarrolladores de software que ofrecen sus productos como software patrocinado por publicidad, que no es eliminada a no ser que el usuario pague para registrarse.

En el caso de adware legítimo, los anuncios deben desaparecer cuando el usuario deja de ejecutar el programa, y el usuario siempre tiene la opción de desactivar los anuncios mediante la compra de una clave de registro.

Spyware es un término general usado para describir software instalado en un ordenador a través de Internet, sin el consentimiento del usuario, que lleva a cabo ciertas acciones como publicidad, obtención de información acerca de los hábitos de navegación o modificación de la configuración del equipo.

La información recopilada puede enviarse a través de Internet a un servidor, normalmente como resultado de la utilización de un software desconocido para el usuario y que puede ser capturada para diferentes propósitos. Las tácticas típicas incluyen la entrega de anuncios no solicitados mediante ventanas emergentes, robo de información personal (incluyendo contraseñas a las cuentas en línea o información financiera como números de tarjetas de crédito), seguimiento de la actividad de navegación Web con fines de marketing, y envío de peticiones HTTP a sitios de publicidad.

El software espía puede ser instalado junto con otro software o como resultado de una infección por virus. A veces están diseñados para que sea difícil, no sólo su eliminación sino también su detección. Otros tipos de software espía realizan cambios en el equipo y pueden causar que dichos equipos se ralenticen o se bloqueen.

Los usuarios afectados, con frecuencia, notan un comportamiento no deseado y la degradación del rendimiento del sistema. Una infección de spyware puede crear una actividad significativa no deseada de CPU, uso de disco, y tráfico de red.

Los programas anti-spyware pueden trabajar bien proporcionando protección en tiempo real o bien exploración en franjas horarias establecidas. En el primer caso, se escanean todos los datos entrantes en busca de spyware y se bloquean las amenazas de una manera similar a como operan los antivirus. En el segundo caso

se utilizan exclusivamente para la detección y eliminación de software espía ya instalado en el ordenador.

2.3 Día cero: vulnerabilidades y ataques

Existen diversas, aunque ligeramente diferentes definiciones de vulnerabilidades de día cero. Algunas definiciones se refieren como defectos de software que dejan los usuarios expuestos a ciberataques antes de que esté disponible o sea público, un parche o solución; mientras que otras definen a este término como una vulnerabilidad de seguridad en el mismo día en que la vulnerabilidad se da a conocer públicamente (día cero). En la primera definición, una vulnerabilidad de día cero puede ser desconocida para todo el mundo exceptuando algún atacante; algunos autores se refieren a los ataques a estas vulnerabilidades como 'anterior al día cero'. En otros casos, el proveedor de software puede ser consciente de la vulnerabilidad, pero aún no ha emitido una solución o parche que lo resuelva.

Es muy difícil descubrir estos ataques; de hecho, a menudo se requieren meses, y a veces años antes de que un desarrollador sea consciente de la vulnerabilidad que ha dado lugar a un ataque concreto.

En cualquier caso, el resultado es el mismo: los usuarios están muy expuestos a los ataques. Como indican L. Bilge y T. Dumitras en [5] "Mientras se desconoce una vulnerabilidad, no puede repararse el software afectado y los productos antivirus no puede detectar el ataque a través del escaneo basado en firmas". Las vulnerabilidades de software pueden ser descubiertas por crackers, compañías de seguridad o investigadores, por los propios proveedores de dicho software, o por los usuarios. Si son descubiertas por un cracker, es muy posible que durante un tiempo exista un mecanismo informático o programa que se aproveche de dicha debilidad y que sea conocido sólo en el mundo de los hackers/crackes, hasta que las compañías de software de seguridad o el proveedor de ese software se den cuenta.

Fig. 2.2 – Período de vulnerabilidad de un ataque día cero.

Los ataques de día cero han permitido a algunos de los ataques más duros de los últimos años. Por ejemplo, la operación Aurora (2009) explotaba una vulnerabilidad de Internet Explorer con más de 20 objetivos, incluyendo Morgan Stanley, Google, Yahoo, Dow Chemical, Adobe Systems, Juniper Networks e incluso software para empresas de seguridad como Symantec

Probablemente, el ataque de día cero más famoso fue Stuxnet (2010). De hecho, el gusano Stuxnet utilizó cuatro ataques de día cero separados para dañar los controladores industriales e interrumpir instalación de enriquecimiento de uranio de Natanz en Irán. Stuxnet fue diseñado para manipular los controladores

industriales lógicos programables (PLCs) realizados por Siemens que controlaban y supervisaban la velocidad de las centrifugadoras. Los atacantes remotos no pudieron acceder directamente a estos dispositivos ya que los equipos no estaban conectados a Internet; lo que hicieron fue diseñar su ataque para que se propagase a través de unidades de disco USB infectados. De esta manera, se infectaron primero ordenadores pertenecientes a cinco empresas externas, que se creía que están conectadas de alguna manera con el programa nuclear. El uso de cuatro vulnerabilidades de día cero fue un hecho único. Por otra parte, Stuxnet también utilizó y se aprovechó de otras vulnerabilidades, lo que muestra la extraordinaria sofisticación y planificación que hubo para hacer este ataque.

2.4 Escaneo y suplantación de identidad

En este contexto, el término escaner se refiere a un programa utilizado por hackers para identificar (a veces, de forma remota) posibles vulnerabilidades de un sistema dado.

Los administradores también utilizan escáneres para detectar y corregir vulnerabilidades en sus sistemas antes de que un intruso las encuentre. Actualmente hay muchos programas de análisis disponibles como software gratuito en Internet.

Un buen programa de escaneo puede localizar a un equipo objetivo en Internet, determinar cuáles son los servicios TCP/IP que se están ejecutando en dicha máquina, e identificar aquellos servicios que tienen alguna vulnerabilidad.

Un ataque de suplantación de identidad es cuando una entidad atacante se hace pasar por otro usuario o dispositivo en una red.

Hay varios tipos diferentes de ataques de suplantación; incluyendo suplantación de e-mail, suplantación de direcciones IP, suplantación ARP, suplantación de servidores DNS…

La suplantación de e-mail supone el envío de mensajes desde una dirección de correo electrónico falsa o falsificar la dirección de correo electrónico de otro usuario. La mayoría de los servidores de correo electrónico tienen características de seguridad para evitar el envío de mensajes de usuarios no autorizados; sin embargo, es posible recibir correo electrónico desde una dirección que no es la dirección real de la persona que envía el mensaje.

En un ataque de suplantación de direcciones IP, un atacante envía paquetes con una dirección IP origen falsa (o "falsificada") con el fin de enmascarar su identidad.

Hay muchas herramientas y procedimientos que las organizaciones pueden emplear para reducir la amenaza de ataques de suplantación. Las medidas comunes que pueden adoptar las organizaciones para la prevención del ataque de suplantación incluyen el filtrado de paquetes, el uso de software de detección de suplantación de identidad y el uso de protocolos criptográficos de red.

2.5 Ataques de denegación de servicio (DoS) y DoS distribuida (DDoS)

Como se detalla en [8] , “los ataques de denegación de servicio son una de las opciones más populares que usan los atacantes en Internet que quieren perturbar las operaciones de una red. A pesar de que no destruyen o roban datos como hacen otros tipos de ataques, el objetivo del atacante DOS es desmantelar la red denegando el servicio a sus usuarios legítimos. Los ataques DoS son fáciles de iniciar ya que hay software fácilmente disponible en sitios web de hackers que permiten que cualquiera pueda lanzar un ataque DOS aunque tenga poca o ninguna experiencia técnica”

En este tipo de ataques, el sistema recibe un número considerable de peticiones de comunicación y no es capaz de establecer la comunicación con todos los solicitantes. Entonces, el sistema consume recursos para completar el establecimiento de conexión. Con el tiempo, el sistema no puede responder a más peticiones de representación sin servicio.

Los ataques de denegación de servicio distribuidos (DDoS) utilizan ordenadores intermedios llamados agentes (que son equipos que tienen una vulnerabilidad y han sido comprometidos), que a menudo están infectadas con un Troyano. Estos sistemas constituyen una botnet y se utilizan para dirigirse a un único sistema provocando un ataque DoS .

La diferencia con un ataque DoS clásico se debe al uso de botnet en DDoS con muchos equipos (pueden ser cientos o incluso miles) y muchas conexiones a Internet, a menudo distribuidos globalmente en DDoS .

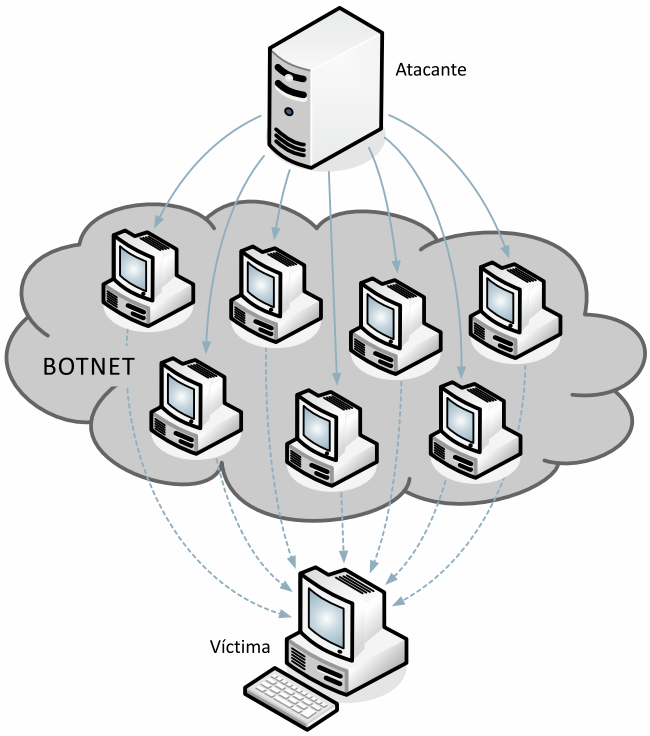

Figure 2.3. Esquema de un ataque DDoS

El atacante activa de forma remota estos programas troyanos, haciendo que los ordenadores intermedios ejecuten al mismo tiempo el ataque. Esto hace que sea imposible detener el ataque bloqueando una única dirección IP o unas cuantas, ya que el ataque procede de ordenadores que pueden estar en cualquier lugar del mundo. Por otra parte y por la misma razón, distribución entre muchísimos terminales ubicados en cualquier lugar, es muy difícil distinguir el tráfico de usuarios legítimos del tráfico de los terminales que realizan el ataque.

Es importante tener en cuenta que los ataques DDoS representan una amenaza a dos niveles. No sólo la red puede ser el blanco de un ataque DOS (ya que se lanzan ataques contra los servidores e impide la entrada y salida de tráfico de la red), sino también a sus ordenadores, ya que podrían ser utilizados como "equipos intermedios de la botnet" para lanzar un ataque DoS contra la otra red o sitio.

Los ataques DDoS se pueden dividir en los ataques basados en volumen, ataques a protocolos y ataques a nivel de aplicación, de acuerdo con el objetivo del ataque. En el primer caso, el objetivo es saturar el ancho de banda de la red, en el segundo recursos de equipos de comunicación intermedio, y en el tercer caso de accidente el servidor de aplicaciones.

2.6 Ataques de ingeniería social

Se define ingeniería social (en este entorno) como la obtención de información confidencial por medio de la interacción humana.

El tipo de información que un atacante quiere conseguir puede ser variable, pero cuando el objetivo es un individuo, los atacantes suelen tratar de engañar a las víctimas con el fin de obtener sus contraseñas, información bancaria, o acceder a su ordenador para instalar software malicioso.

A diferencia de otros tipos de ataques, la ingeniería social no se refiere a una manipulación tecnológica aprovechando las vulnerabilidades de hardware o software y no requiere habilidades técnicas. En cambio, este tipo de ataque explota las debilidades humanas - falta de cuidado o el deseo de ser cooperativo - para acceder a las credenciales de red de un usuario legítimo. Los talentos que son más útiles al intruso que utiliza esta técnica son los llamados “don de gentes”, como tener una personalidad encantadora, o persuasiva, o un mando de autoridad.

Muchos profesionales de seguridad consideran que el eslabón más débil de la cadena de seguridad es el ser humano. Algunos ataques comunes de ingeniería social incluyen correo electrónico de un “amigo” que contiene un enlace o un archivo para descargar (con software malicioso incrustado), o solicitud de ayuda ...

3 Componentes de un sistema de seguridad en la red

Para disminuir la vulnerabilidad de un ordenador en una red hay muchas soluciones y tecnologías disponibles. Las organizaciones tienen una extensa selección de tecnologías, que van desde paquetes de software antivirus, equipos de seguridad de red dedicada tales como firewalls y sistemas de detección de intrusos, para proporcionar protección a todas las áreas de la red

Es importante señalar que no hay una solución única que proteja a un sistema de una variedad de amenazas. Un sistema de seguridad de la red por lo general se compone de muchos componentes. Lo ideal sería que todos los componentes trabajasen juntos, de forma que si uno falla los otros puedan seguir protegiendo frente a ataques, mejorando así de la seguridad. Estos componentes pueden ser hardware y/o software. El software debe ser actualizado constantemente para ofrecer protección frente a amenazas emergentes.

Actualmente, las organizaciones utilizan combinaciones de firewalls, IDS, cifrado y mecanismos de autenticación para crear “intranets” conectadas a Internet, pero al mismo tiempo protegidas. Una Intranet es una red informática privada que utiliza protocolos de Internet. Las Intranets difieren de las “extranets” en que las primeras generalmente se restringen a los empleados de la organización, mientras que a las extranets pueden acceder por lo general clientes, proveedores, u otras entidades autorizadas.

3.1 Antivirus y antispyware

Viruses, gusanos y caballos de Troya son ejemplos de software malicioso, también llamado malware. El software antivirus o anti-virus se usa para prevenir, detectar y eliminar el malware, incluyendo pero sin limitarse a los virus informáticos, gusanos, troyanos, spyware y adware. Para ser eficaz, el software antivirus debe ser actualizado periódicamente - de lo contrario no será capaz de ofrecer protección contra nuevos virus.

La industria antivirus se apoya en una amplia red de usuarios que proporcionan alertas de nuevos virus, de manera que los mecanismos preventivos y correctivos pueden ser desarrollados y distribuidos rápidamente. Todos los meses se generan miles de nuevos virus, por lo tanto, es esencial que la base de datos de virus se mantenga actualizada. La base de datos de virus es el registro que tiene el software antivirus que ayuda a identificar los virus conocidos cuando intentan atacar. Los proveedores de software antivirus de buena reputación publican las últimas actualizaciones en sus sitios web, y permiten la actualización automática del software de los equipos de los usuarios. La política de seguridad de la red debe estipular que todos los equipos de la red se mantienen actualizados y, a ser posible, están protegidos por el mismo paquete antivirus para minimizar los costos de mantenimiento y de actualización. También es esencial actualizar regularmente el software en sí mismo.

Independientemente de lo útil que sea el software antivirus, su uso a veces puede tener desventajas. El software antivirus puede disminuir las prestaciones o rendimiento de un equipo. Los usuarios inexpertos pueden también tener problemas para entender las instrucciones y decisiones que el software antivirus les presenta. Una decisión incorrecta puede conducir a un fallo de seguridad.

La erradicación de un virus es el término que se utiliza para la limpieza de un ordenador. Hay varios métodos de erradicación: eliminar el código que se corresponde con el virus en el archivo infectado; eliminar el archivo infectado o poner en cuarentena dicho archivo infectado, es decir, trasladarlo a un lugar donde no se puede ejecutar. Típicamente, se emplean las siguientes estrategias.

Detección basada en firmas consiste en la búsqueda de patrones conocidos en un código ejecutable. Los virus se reproducen infectando las "aplicaciones host" lo que significa que se copia una porción de código ejecutable en un programa existente. Los virus están programados para no infectar el mismo archivo varias veces con el fin de tener la certeza que funcionan según lo previsto. Para ello, se incluyen una serie de bytes en la aplicación para comprobar si ya ha sido infectada, esto se denomina firma de virus. Dicha firma es única para cada virus. Los programas antivirus intentan detectar la presencia de esta firma para decidir si el archivo está infectado o no. Este método se denomina detección basada en firmas y es el método más antiguo utilizado por el software antivirus.

Sin embargo, este método no puede detectar virus cuyas firmas no han sido archivadas por los editores del software antivirus. Además, los programadores de virus a menudo utilizan técnicas de camuflaje para dificultar la detección de las firmas. Para contrarrestar estas amenazas, se utiliza el enfoque heurístico.

Un tipo de enfoque heurístico son las firmas genéricas que pueden identificar virus nuevos o variantes de los virus existentes a partir del conocimiento de código malicioso conocido o ligeras variaciones de dicho código. El método heurístico analiza el comportamiento de las aplicaciones con el objetivo de detectar actividad similar a la de un virus conocido.

Por lo tanto, este tipo de programa antivirus puede detectar virus, aun cuando la base de datos antivirus no estén actualizadas.

Sin embargo, en estos esquemas podemos encontrarnos con falsas alarmas, es decir, que el antivirus identifique a un software totalmente correcto como malicioso.

3.2 Cortafuegos (Firewall)

Un cortafuegos es un mecanismo de control de la frontera, o defensa del perímetro. El propósito de un cortafuegos es evitar el acceso no autorizado, hacia o desde una red, al bloquear el tráfico procedente del exterior o interior de esta red

Todos los mensajes que entran o salen de la red interna a través del firewall son examinados para verificar si cumplen las normas de seguridad especificadas en las reglas del firewall, bloqueando aquellos que no satisfacen los criterios de seguridad establecidos. Los firewalls pueden ser implementados tanto en hardware como en software, o una combinación de ambos [8].

Parte de las políticas de seguridad de una organización quedan reflejadas en las reglas de los cortafuegos que establecen la restricción de acceso a recursos de red específicos. En la analogía de la seguridad física, un cortafuegos es el equivalente a una puerta de bloqueo, en una puerta de perímetro o en una puerta de una habitación en el interior del edificio, que permite que sólo puedan entrar los usuarios autorizados (aquellos que disponen de una llave o tarjeta de acceso). La tecnología de cortafuegos también está disponible en versiones apropiadas para redes domésticas u ordenadores personales. El cortafuegos crea una capa protectora entre la red y el mundo exterior. En efecto, el cortafuegos se ubica normalmente en el punto de entrada a la red, de modo que puede analizar los datos y recibir y transmitir aquellos paquetes autorizados sin retraso significativo. Asimismo, tiene filtros incorporados que impiden que aquello que se considera no autorizado o potencialmente peligroso entre en el sistema. Por otra parte, los cortafuegos proporcionan una importante función de auditoría; a menudo, proporcionan resúmenes al administrador de red acerca de qué tipo / volumen de tráfico se ha procesado a través de él, incluyendo intentos de intrusión

El NIST (National Institute of Standards and Technology), clasifica los cortafuegos en tres categorías básicas [9]: filtrado de paquetes, inspección de estado y proxys. Estas tres categorías, sin embargo, no son mutuamente excluyentes; la mayoría de los cortafuegos modernos tienen una mezcla de capacidades que hacen que puedan estar clasificados en más de una.

Los cortafuegos de filtrado de paquetes son esencialmente dispositivos de encaminamiento que utilizan funcionalidades de control de acceso para las direcciones del sistema y las sesiones de comunicaciones; también pueden filtrar el tráfico de la red en base a ciertas características. Normalmente se despliegan dentro de las infraestructuras de red TCP / IP. Sus principales puntos fuertes son la velocidad y la flexibilidad y la debilidad más relevante es su incapacidad para evitar ataques que emplean vulnerabilidades específicas de la aplicación (ya que no examinan los datos de la capa superior) .

La Tabla 1, adoptada de [9] muestra un ejemplo de conjunto de reglas de un cortafuegos de filtrado de paquetes

	Dirección origen	Puerto origen	Dirección Destino	Puerto	Acción	Descripción
1	Cualquiera	Cualquiera	192.168.1.0	> 1023	Permitir	Regla para permitir conexiones de retorno a subred interna
2	192.168.1.1	Cualquiera	Cualquiera	Cualquiera	Denegar	Evitar que haya conexiones directamente desde el cortafuegos
3	Cualquiera	Cualquiera	192.168.1.1	Cualquiera	Denegar	Evitar que usuarios externos puedan conectarse directamente al cortafuegos.
4	192.168.1.0	Cualquiera	Cualquiera	Cualquiera	Permitir	Los usuarios internos pueden acceder a servidores externos.
5	Cualquiera	Cualquiera	192.168.1.2	SMTP	Permitir	Permitir que lleguen e-mails al sistema procedentes de usuarios externos
6	Cualquiera	Cualquiera	192.168.1.3	HTTP	Permitir	Permitir a usuarios externos accede a servidores WWW
7	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Denegar	Cualquier acción no permitida anteriormente es denegada explícitamente.

Los cortafuegos de inspección de estado, también conocidos como filtrado dinámico de paquetes, se basan en la supervisión del estado de las conexiones activas para determinar qué paquetes de red pueden pasar a través del firewall. Estos cortafuegos analizan los paquetes en las capas inferiores a la de aplicación. Mediante el registro de información de sesión, como direcciones IP y números de puerto, un cortafuegos de inspección de estado puede adoptar un criterio de seguridad mucho más estricto gracias al análisis de ciertos valores de las cabeceras de protocolos que permite controlar el estado de cada conexión durante un período de tiempo. Se realiza un seguimiento de los paquetes salientes que solicitan tipos específicos de paquetes entrantes y sólo se permite que pasen a través del cortafuegos aquellos paquetes entrantes que constituyen una respuesta adecuada a otros previos. El cortafuegos analiza cada nuevo paquete teniendo en cuenta su tabla de estado para determinar si el estado del paquete contradice su estado esperado. Los cortafuegos de inspección de estado tradicionales no inspeccionan el campo de datos de los paquetes de red y no tienen la capacidad de para distinguir un tipo de tráfico web de otro (aplicaciones legítimas y los ataques).

Los cortafuegos proxy o cortafuegos de pasarela de aplicaciones, son una incorporación bastante reciente a entornos de seguridad convencionales. Los cortafuegos proxy combinan la tecnología de inspección de estado con la capacidad de realizar inspecciones con cierta profundidad a nivel de aplicación. Esta capacidad permite el análisis de protocolos en la capa de aplicación como HTTP y FTP y controlar el tráfico para analizar el comportamiento de la actividad del protocolo e identificar desviaciones o posibles signos de ataque respecto a comportamientos normales o benignos. Esto permite que un cortafuegos permita o deniegue el acceso en función de cómo se ejecuta una aplicación en la red.

Los cortafuegos de próxima generación (NGFW) son una plataforma de red integrada que combina un firewall tradicional con otras funcionalidades de filtrado de dispositivos de red tales como cortafuegos proxy utilizando inspección profunda de paquetes (DPI), un sistema de prevención de intrusiones (IPS) y otras técnicas tales como filtrado web, gestión de QoS/ancho de banda, inspección del antivirus e integración de terceros servicios (por ejemplo, Active Directory) [10] . De hecho, básicamente constituyen una solución de administración unificada de amenazas (UTM). El principal inconveniente de NGFW es que por lo general tienden a utilizar los motores internos separados para llevar a cabo funciones de seguridad individuales y en consecuencia, un paquete puede ser examinado varias veces por diferentes motores para determinar si se debe permitir que se transmita a la red. Ese enfoque de turno rotativo añade latencia lo que puede afectar al rendimiento de la red.

3.3 Sistemas de detección de intrusión (IDS)

Un sistema de detección de intrusiones (IDS) es una herramienta de seguridad de red que ofrece protección adicional ayudando a prevenir intrusiones en ordenadores , mediante la supervisión del tráfico de la red. Trabajan en base a firmas y al uso de análisis heurístico para identificar patrones sospechosos que podrían indicar un ataque a un sistema o red.

Los sistemas IDS pueden ser dispositivos de software o hardware utilizados para detectar un ataque. Son utilizados para controlar la conexión y así determinar si se han lanzado ataques. Algunos sistemas IDS solo monitorizan y dan la alerta de un ataque, mientras que otros tratan de bloquearlo. En la analogía en el mundo tangible, un IDS es equivalente a una cámara de vídeo y un sensor de movimiento; pueden detectar actividad no autorizada o sospechosa y trabajan con sistemas automatizados de respuesta, tales como guardias de vigilancia, para detener la actividad.

Un IDS difiere de un cortafuegos en que estos últimos limitan el acceso entre redes con el fin de evitar la entrada y no señalizan los ataques desde el interior de la red . El IDS evalúa una acción sospechosa de intrusión una vez que ha tenido lugar y establece una alarma . Por otra parte, el IDS observan los ataques que se originan desde el interior de una red.

Los IDS realizan una evaluación de vulnerabilidades (a veces se denomina exploración), que es una tecnología desarrollada para evaluar la seguridad de un sistema informático o red. Las funciones de detección de intrusos incluyen la supervisión y el análisis de actividades tanto del usuario como del sistema, análisis y posibles vulnerabilidades de las configuraciones del sistema, evaluación del sistema e integridad de ficheros, análisis de los patrones de actividad anormales y seguimiento de violaciones a las políticas de usuario . Hay varias formas de clasificar un IDS

- Detección de mal uso y detección de anomalías
    - Detección de mal uso: el IDS analiza la información que recopila y la compara con grandes bases de datos de firmas de ataques. Esencialmente, el IDS busca un ataque específico que ya se ha documentado. La técnica de detección de intrusos basada en firma de ataque consiste en la búsqueda de "firmas" (secuencias de acciones típicas de un ataque) en todas las comunicaciones que pasan por la red. Igual que ocurre con los sistemas de detección de virus, la calidad del software de detección depende de la base de datos de firmas de ataque utilizada, por lo que se necesita una actualización frecuente de esta base de datos.
    - Detección de anomalías: el administrador del sistema define el estado normal de tráfico de la red, protocolos y tamaños típicos de los intercambios. El detector de anomalías compara el estado en cada momento con el estado normal y a partir de las diferencias se buscan anomalías de comportamiento, que pueden ser debidas a algún ataque.

- Basados en red o basados en equipos
    - Basados en red, (NIDS, Network-based system): se analizan las comunicaciones que se intercambian por la red. El NIDS puede detectar mensajes maliciosos diseñados de forma que las reglas de filtrado de un firewall no lo detecten.
    - Basados en equipo (HIDS, Host-based system): el IDS analiza toda la actividad en cada equipo individual.

3.4 Redes privadas virtuales (VPN Virtual Private Network)

Una red privada virtual (VPN) es una tecnología de red que hace que sea posible utilizar una red pública como Internet para la comunicación privada gracias a la creación de una conexión segura (cifrada) .

Las VPN a menudo se utilizan para permitir que los usuarios remotos puedan conectarse de forma segura a una red privada, y de esta manera, permitir la extensión de intranets. En otras palabras, una VPN permite el envío de datos entre dos ordenadores que utilizan la infraestructura de enrutamiento proporcionada por una red interna compartida o pública (como Internet) de manera que emula las propiedades de una conexión privada punto a punto. La conexión segura se muestra al usuario como una comunicación de red privada, a pesar de que esta comunicación se lleva a cabo a través de una interconexión de redes públicas, de ahí el nombre de la red privada virtual

Hay varias motivaciones para la construcción de redes privadas virtuales, pero un aspecto común es el requisito de “virtualizar” una parte de las comunicaciones, en otras palabras, que una parte de las comunicaciones de una organización sea esencialmente “invisible” para observadores externos, aprovechando al mismo tiempo la eficiencia de una infraestructura de comunicaciones común. Los usos comunes de las VPN son: el acceso remoto seguro a los recursos corporativos a través de Internet y conexión de redes remotas a través de Internet. Una solución VPN debe proporcionar los siguientes servicios de seguridad:

- Autenticación de usuario. La VPN restringe el acceso sólo a usuarios autorizados; por lo tanto, la identidad debe ser verificada. Por otra parte, las VPN deben proporcionar registros de auditoría.
- Cifrado de datos. Los datos que se intercambian a través de la red pública deben ser “incomprensibles” para los usuarios no autorizados.
- Gestión de claves. Antes del cifrado de datos, se requiere que los usuarios configuren aspectos vinculados a la conexión criptográfica (algoritmos , claves , ...)

4 Soluciones de seguridad en red

Una red es tan fuerte como su punto más débil. Además de utilizar los componentes descritos en la sección anterior, a continuación se detallan un conjunto de acciones que los usuarios y/o administradores de red deben poner en práctica con el fin de mejorar la seguridad del sistema.

4.1 Uso de mecanismos de autenticación seguros

Muchas organizaciones requieren el uso de métodos de autenticación robusta, especialmente aquellas que incluyen transacciones en línea que engloban servicios de pago. Existen varias definiciones de autenticación robusta. Algunos autores se refieren a ella como método de autenticación con la combinación de diversos mecanismos que requieren el uso de soluciones de dos o más de las tres categorías de factores (conocimiento, posesión e inherencia), tal como se ha mencionado en la sección 1.3. Otros autores (A. J. Menezes , P. C. van Oorschot y S. A. Vanstone) consideran en [11] que los mecanismos de autenticación robusta requieren un protocolo de desafío- respuesta criptográfico ... En cualquier caso, un protocolo de autenticación robusto no se puede lograr con la transmisión de contraseñas .

Es importante tener en cuenta que la fiabilidad de la autenticación depende no sólo del número de factores implicados, sino también de la forma en que se implementan. En cada categoría, las decisiones tomadas por las reglas de autenticación afectan en gran medida a la seguridad de cada factor. El uso de reglas de contraseña pobres (o incluso la ausencia de estas reglas), por ejemplo, pueden dar lugar a la creación de contraseñas como “secreto”, “Juan”, o “invitado”, lo que contradice por completo el valor de usar una contraseña. Las mejores prácticas incluyen el uso de contraseñas inherentemente fuertes que se actualizan periódicamente. El hecho que en algunas ocasiones haya una cierta laxitud en las normas e implementaciones de seguridad genera una mayor debilidad del sistema; alternativamente, normas más estrictas pueden dar una mayor seguridad en cada uno de los factores, y por lo tanto, una mayor seguridad global en los sistemas de autenticación de múltiples factores.

En el caso de la utilización de contraseñas, es esencial la creación de una política de contraseñas calidad para evitar que se pueda adivinar. La aparición de herramientas informáticas para “crackear” contraseñas ha hecho que sea mucho más fácil para los atacantes poder “adivinarlas”. Existen numerosas herramientas de descubrimiento de contraseñas disponibles que cualquier persona puede utilizar. Desafortunadamente el usuario medio tiende más a que la contraseña sea fácil de recordar que difícil de adivinar.

El “crackeo” de contraseñas es un proceso que consiste en averiguar contraseñas con el fin que un usuario no autorizado o atacante pueda conseguir acceder a un sistema o cuenta. Las contraseñas pueden ser crackeadas en una variedad de maneras diferentes. El más simple es el uso de una lista de palabras o diccionario para romper la contraseña por fuerza bruta. Estos programas comparan las listas de palabras o combinación de caracteres con la contraseña hasta que encuentran una coincidencia. Por lo tanto, es obvio que las contraseñas no deben ser las palabras del diccionario, nombres propios o palabras extranjeras.

Un administrador de red puede utilizar las herramientas de crackeo de contraseñas para garantizar que los usuarios están utilizando contraseñas seguras, y notificar a los usuarios cuyas contraseñas no son suficientemente seguras. Otra forma en que los intrusos pueden usar para descubrir las contraseñas es a través de la ingeniería social. Muchos usuarios crean contraseñas que contienen información personal y,

por lo tanto, pueden ser adivinadas fácilmente si se conoce una mínima cantidad de información sobre ellos. Por lo tanto, las contraseñas no deben contener información personal. Muchos usuarios almacenan las diferentes contraseñas que utilizan en archivos de ordenador. En tal caso, es necesario cifrar estos archivos. De hecho, esta recomendación es útil no sólo para los archivos de contraseñas, sino también para todos los archivos que contienen información crítica.

4.2 Fortalecimiento del sistema operativo

El fortalecimiento del sistema operativo es el hecho de configurar un sistema operativo de forma segura, actualizándolo, creando reglas y políticas para ayudar a gestionar el sistema de una manera segura y eliminar aplicaciones y servicios innecesarios.

El fortalecimiento del sistema operativo normalmente se lleva a cabo mediante la eliminación del ordenador de todos los programas y utilidades de software no esenciales, la aplicación de los parches más recientes, la eliminación de archivos no utilizados, el bloqueo de cuentas de usuario que no utilizan el sistema,… Aunque estos programas no esenciales pueden ofrecer características útiles para el usuario, deben ser eliminados si también proporcionan una "puerta trasera" de acceso al sistema.

A pesar de que son importantes, la eliminación de aplicaciones, inhabilitar servicios, establecer parches, y la instalación de los "service packs" no son las únicas formas de robustecer un sistema operativo. Los privilegios de administración deben utilizarse con moderación, y deben aplicarse las políticas requeridas para hacer cumplir las normas de la organización.

Hay listas de control de fortalecimiento disponibles que los administradores pueden seguir para los sistemas operativos más populares. Aunque que los sistemas operativos Macintosh y Windows pueden ser fortalecidos, esta tarea se realiza con mayor frecuencia en máquinas Windows, ya que en muchos casos su seguridad puede verse comprometida.

4.3 Seguridad física

Garantizar un entorno de red físicamente seguro es el primer paso en el control de acceso a los datos sensibles y al sistema de archivos, pero es sólo una parte de un buen plan de seguridad. Esto es actualmente más cierto que en el pasado, ya que hay más formas de acceder a las redes que antaño. Una red de tamaño medio o grande puede tener varios puntos de acceso, servidores VPN y una conexión dedicada a Internet a tiempo completo. Incluso una pequeña red es probable que esté conectada a Internet una gran parte del tiempo.

Los atacantes virtuales nunca están en contacto físico con los ordenadores o la red que atacan. Pueden acceder a la red desde el otro lado de la calle o del otro lado del mundo. Pero pueden hacer tanto daño como el ladrón que irrumpe en la sede de la empresa para robar o destruir los datos - y son mucho más difíciles de atrapar. Llevar a cabo un control de acceso físico al "perímetro externo" significa:

a) Control de acceso físico a los servidores

b) Control de acceso físico a los terminales conectados a la red.

c) Control de acceso físico a los dispositivos de red

d) Control de acceso físico al cableado de red

e) Ser consciente de las consideraciones de seguridad en la red inalámbrica.

f) Ser consciente de las consideraciones de seguridad en los ordenadores portátiles.

g) Ser consciente de los riesgos de seguridad derivados de permitir que se puedan imprimir ciertos datos.

h) Ser consciente de los riesgos de seguridad derivados de posibles pérdidas de discos duros externos, CDs …

5 Seguridad en móviles

Los dispositivos móviles están reemplazando rápidamente o complementando a la computadora personal en el hogar y en el lugar de trabajo. El rápido crecimiento de los teléfonos inteligentes y el uso de tabletas en los últimos años han llevado al inevitable aumento de ataques a estos dispositivos por los ciberdelincuentes. Por otra parte, algunos mercados de distribución de aplicaciones no suficientemente regulados aumentan los problemas relacionados con el malware en estos dispositivos. Los creadores de malware móvil saben que la mejor manera de infectar tantos dispositivos como sea posible es atacar a los mercados de distribución de aplicaciones.

Hay muchas maneras diferentes de que un hacker puede beneficiarse de un dispositivo móvil comprometido. Algunas de estas han sido adoptadas desde el PC tradicional, como ransomware, botnet y robo de datos. Sin embargo, también aparecen nuevos tipos de ataque debido a la naturaleza de los dispositivos móviles. Asimismo, su gran portabilidad los hace vulnerables a pérdidas físicas y posible robo de datos si el dispositivo no está bien protegido.

La adopción continua de aplicaciones emergentes para la comunicación personal y de negocios amplía la posibilidad de ataque e intentos de filtración de datos, sobre todo mediante estafas de ingeniería social. La libreta de direcciones y el grafo de relaciones sociales es un tesoro para los atacantes. El control de aplicaciones web y móviles para usuarios de negocios ayudará a mitigar este riesgo.

Hoy en día, la evolución de la banca móvil plantea un riesgo potencial aún mayor para los usuarios. Los dispositivos móviles de gran capacidad ya están en el punto de mira de programas maliciosos diseñado para robar datos y dinero, ya que hacen permiten que usuarios realizar transacciones financieras en movimiento de forma sencilla. Por lo tanto, un principio básico de la banca móvil segura es la protección del smartphone de malware y keyloggers.

Los expertos en seguridad han estado advirtiendo de la amenaza de malware móvil desde hace años. El hecho de que todavía no se haya materializado un ataque importante (o no se haya publicitado) ha disminuido la credibilidad de las afirmaciones; sin embargo, no se debe bajar la guardia. El gran volumen de dispositivos móviles, y la prevalencia de las nuevas amenazas de malware móviles sólo aumentan la probabilidad que suceda un importante ataque de malware móvil.

Como dijo Mark Bermingham, director de marketing global en Kaspersky Lab, “A medida que los consumidores y las empresas utilizan los dispositivos móviles para un mayor porcentaje de sus actividades diarias, los cibercriminales se orientan a realizar nuevos ataques en las plataformas de Android y en la de dispositivos IOS”