Vulnerabilidades y ataques en redes

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Introducción

En este módulo, se tratan los aspectos generales de seguridad de una infraestructura de red. En general, estas redes están basadas en la arquitectura de red denominada TCP/IP. Esta arquitectura determina cómo se realiza la comunicación entre los dispositivos interconectados, con lo cual su conocimiento es fundamental para la correcta comprensión de los mecanismos de protección adecuados para alcanzar infraestructuras de redes seguras.

La arquitectura TCP/IP posee características que propician en gran medida las vulnerabilidades asociadas a su funcionamiento. Si bien se trata de una arquitectura que ha probado durante décadas su buen funcionamiento, su diseño responde a necesidades de un contexto muy distinto al que actualmente afrontan las comunicaciones, donde la seguridad no formó parte de su diseño inicial.

Por otro lado, la expansión de Internet ha propiciado nuevos escenarios de aplicación, lo que genera un incremento exponencial del número de equipos conectados a la red. En consecuencia, se ha incrementado también el interés por los ataques, dado que cada vez procesan información más atractiva y se torna necesario el desarrollo de herramientas y mecanismos de protección.

Para más información sobre la Recomendación X.800, consulta: https://goo.gl/0tqrIT

Para más información sobre ITU, consulta: https://goo.gl/uzHtQC

Para más información sobre el Modelo OSI, consulta: https://goo.gl/J5y0ca

Los protocolos que forman parte de la arquitectura TCP/IP poseen vulnerabilidades que pueden ser explotadas en ataques y, al mismo tiempo, condicionan el tipo de mecanismos y herramientas que pueden ser utilizados para dotarlos de seguridad. Es por ello que es condición indispensable para el avance en los conceptos relacionados con la seguridad en redes la compresión de los fundamentos de TCP/IP y los protocolos que implementa en cada una de sus capas.

Este material toma como base la *Recomendación X.800* elaborada por la Unión Internacional de Telecomunicaciones (ITU). Esta recomendación no es una especificación de implementación, sino una descripción de los *servicios de seguridad básicos que pueden ser aplicados* cuando es necesario proteger la comunicación entre sistemas. Asimismo, *define en qué capa* del modelo de interconexión de sistemas abiertos (*OSI*) se puede aplicar cada servicio e incluye los mecanismos que pueden ser implementados para ofrecerlos.

Vulnerabilidades y ataques

La utilización masiva de Internet dio lugar a numerosos avances tecnológicos, especialmente en el campo de las telecomunicaciones, avances que han permitido que los sistemas de información alcancen un enorme grado de conectividad.

En la actualidad, las TIC (tecnologías de la información y las comunicaciones) determinan de manera muy significativa el desarrollo de nuestra sociedad y se tornan indispensables en el entorno de las organizaciones como factor de competitividad.

Es oportuno pensar que estos avances deben ser acompañados en la misma medida con políticas de protección de la información, especialmente en sistemas distribuidos. La seguridad de las redes se enfrenta a un nuevo escenario que contempla varios inconvenientes:

- Aumento de la interconexión de sistemas y redes.
- Crecimiento de la utilización de redes informáticas para la transmisión de información sensible.
- Aumento de la capacidad técnica de un ataque en red. Las noticias sobre ataques a las redes informáticas son cada vez más habituales.

En 1991, como respuesta a estas necesidades de seguridad en las redes informáticas, la Unión Internacional de Telecomunicaciones aprobó la *Recomendación X.800.* Esta recomendación describe los servicios de seguridad básicos que pueden ser aplicados en cada capa del modelo OSI y los mecanismos con los cuales pueden ser implementados.

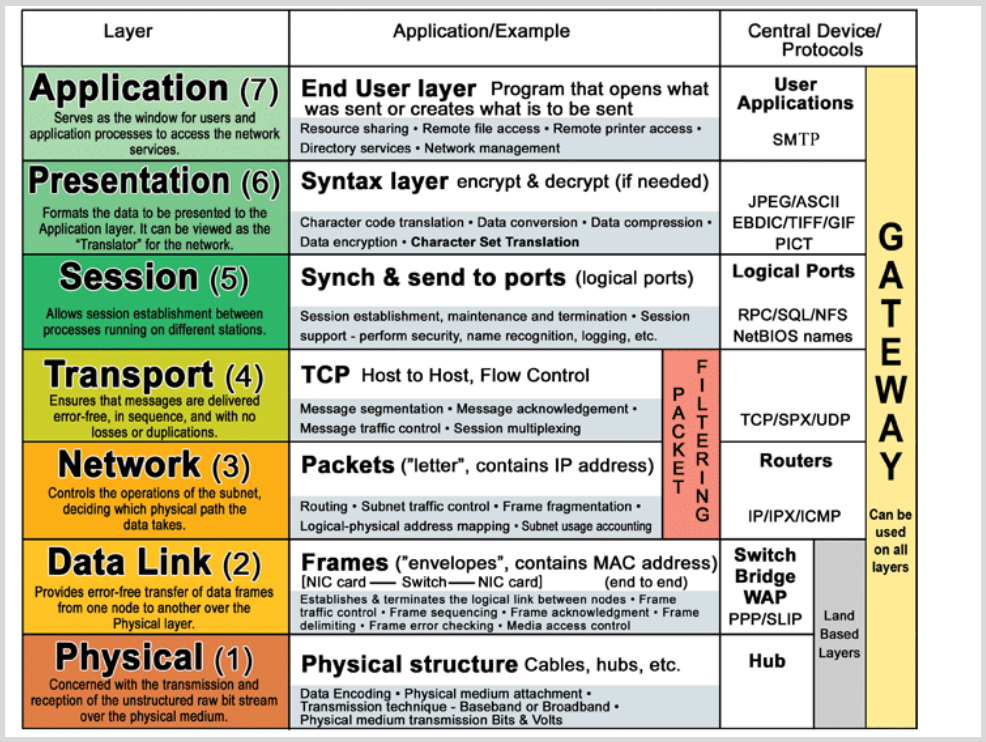
El modelo OSI de seguridad

La Recomendación X.800, conocida como *arquitectura de seguridad OSI* (*open system interconnection*), define una manera sistemática de especificar los requisitos de seguridad con el fin de facilitar la tarea a los responsables de seguridad al momento de definir y realizar el análisis de las necesidades de seguridad de esta, así como la evaluación de los productos y políticas de seguridad que serán aplicadas.

En distintos momentos, deben establecerse controles de seguridad para proteger la información intercambiada entre los procesos de aplicación. Estos controles deben hacer que el costo de obtener o modificar los datos de una manera indebida sea mayor que el valor potencial de esta acción, o

hacer que el tiempo requerido para obtener los datos de una manera indebida sea tan largo que pierdan su valor. (Unión Internacional de Telecomunicaciones [ITU], 1991, p. 3).

Figura 1: Modelo de interconexión de sistemas abiertos (OSI)



Fuente: Cisco, 2017, https://goo.gl/RHy3zX

Como se notará más adelante, tener claros los conceptos relacionados con este modelo, sus capas y los protocolos que operan en cada una de ellas será fundamental para determinar cuáles son sus vulnerabilidades, qué servicios de seguridad se pueden implementar y con cuáles mecanismos.

La arquitectura de seguridad OSI se centra en tres aspectos fundamentales en relación a la seguridad, que se presentan en la siguiente tabla.

Tabla 1: Aspectos centrales de la arquitectura de seguridad OSI

Ataques a la seguridad	Mecanismos de seguridad	Servicios de seguridad
Intento de destruir, exponer, alterar, deshabilitar, robar o conseguir acceso a	Mecanismo implementado con la finalidad de reforzar la seguridad de un	Servicio que garantiza la seguridad adecuada de los sistemas de una organización, así como

una información o servicio en una organización.	sistema que permite prevenir ataques a la seguridad, detectarlos o recuperarse de ellos.	en las comunicaciones que puedan producirse. Están diseñados para mitigar los ataques a la seguridad al hacer uso de mecanismos de seguridad.

Fuente: elaboración propia.

Ataques a la seguridad

La Recomendación X.800 clasifica los ataques a la seguridad en dos tipos:

- Ataque activo: un ataque activo tiene como objetivo la alteración de los recursos del sistema, por lo que puede afectar a su funcionamiento.
- Ataque pasivo: el objetivo de un ataque pasivo no es alterar la comunicación sino *escuchar* y analizar el tráfico de la red o conseguir acceso al sistema sin afectar a los recursos de él.

Cada uno de estos tipos de ataques presenta distintas variantes.

Tabla 2: Tipos de ataques a la seguridad y sus variantes

Tipo de ataque	Descripción
Activo	Suplantación de identidad
	Repetición
	Modificación
	Interrupción o denegación
Pasivo	Análisis de tráfico
	Intercepción de mensajes

Fuente: elaboración propia.

Servicios de seguridad

En la Recomendación X.800, se describe un servicio de seguridad como: "un servicio proporcionado por una capa de sistemas abiertos comunicantes, que garantiza la seguridad adecuada de los sistemas y de la transferencia de datos" (ITU, 1991, p. 9). Estos servicios se dividen en cinco

categorías y catorce servicios específicos, que se encuentran debidamente abordados y definidos en la citada norma.

Uno de los principales aportes de la Recomendación X.800 es que identifica a estos servicios de seguridad y establecen una relación directa con la capa de la arquitectura OSI en la que pueden ser implementados y por consiguiente los protocolos y servicios que son abarcados.

Para ello, parte desde la identificación de los distintos ataques a la seguridad de las redes asociándolas con el servicio de seguridad que lo mitiga, como se expone en la siguiente tabla.

Tabla 3: Relación entre servicios de seguridad y ataques

Servicios de seguridad	Ataques					
	Intercepción	Análisis de tráfico	Suplantación	Repetición	Modificación	Denegación de Servicio
Autenticación de entidades origen/destino			X			
Autenticación del origen de los datos			X			
Control de acceso			X			
Confidencialidad	X					
Confidencialidad del flujo de tráfico		X				
Integridad de los datos				X	X	X
No repudio						
Disponibilidad						X

Fuente: adaptado de Prodigy, (s.f.), https://goo.gl/ix2yhZ.

Para más información sobre el Centro Criptológico Nacional de España (CCN), consulta: https://www.ccn.cni.es/

Mecanismos de seguridad

Si bien la Recomendación X.800 no presenta una definición para mecanismos de seguridad, es posible extraerla de otros documentos técnicos, en este caso, del *CCN-STIC-401, Guía de seguridad. Glosario y*

abreviaturas, elaborado por el Centro Criptológico Nacional de España, que reúne definiciones y abreviaturas de conceptos relacionados a la seguridad de la información y nuevas tecnologías.

Este documento ofrece la siguiente definición de mecanismo de seguridad: "La lógica o algoritmo que implementa una función relevante de seguridad sea en Hardware o en software. (ITSEC)" (CCN [Centro Cristológico Nacional]-STIC [Servicios de Tecnologías de la Información y las Comunicaciones]-401, 2015, p. 549).

Los mecanismos de seguridad se dividen en dos categorías: unos relacionados específicamente con los servicios de seguridad y otros relacionados con la gestión:

- Mecanismos específicos de seguridad: se pueden incorporar en la capa de protocolo correspondiente para proporcionar algunos de los servicios de seguridad OSI.
- Mecanismos generales de seguridad: mecanismos que no son específicos de ninguna capa de protocolo o servicio de seguridad OSI específico, sino que están relacionados con la gestión de seguridad.

A partir de esta segmentación, define y específica cuáles servicios de seguridad se pueden suministrar con estos mecanismos, relación que se presenta en la siguiente tabla.

Tabla 4: Relación entre servicios de seguridad y mecanismos de seguridad

Servicios de seguridad	Mecanismos de seguridad							
	Cifra-do	Firma digital	Control de acceso	Integridad de los datos	Intercambio de autenticación	Relleno de tráfico	Control de enrutamiento	Notarización
Autenticación de Entidades origen/destino	X	X			X			
Autenticación del origen de los datos	X	X						
Control de acceso			X					
Confidencialidad	X						X	
Confidencialidad del flujo	X					X	X	

de tráfico								
Integridad de los datos	X	X		X				
No repudio		X		X				X
Disponibilidad				X	X			

Fuente: adaptación de ITU, 1991.

Continuando con los aportes de la Recomendación X.800, otro de los aspectos clave que contribuye es la relación entre los servicios de seguridad y las capas del modelo OSI en las que es posible implementarlos. Esta asociación se encuentra ampliamente fundamentada en su "Anexo B", donde se detalla el criterio utilizado para establecer esta relación que se presenta a continuación en la Tabla 5.

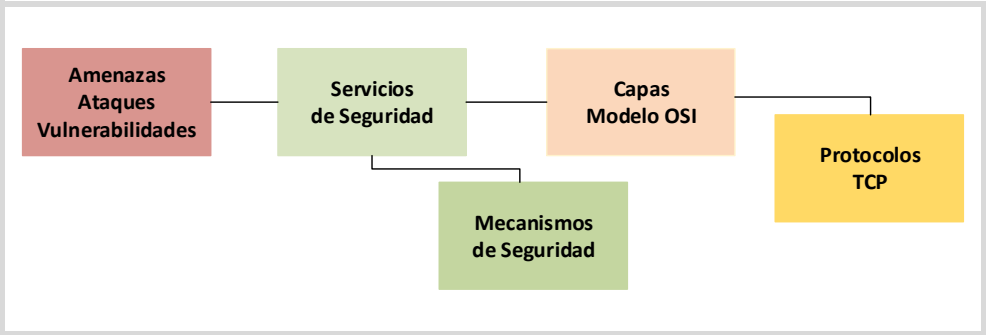
Tabla 5: Relación entre servicios de seguridad y capas del modelo OSI

Servicios de seguridad	Capas del modelo OSI						
	1	2	3	4	5	6	7
Autenticación de Entidades origen/destino			X	X			X
Autenticación del origen de los Datos			X	X			X
Control de acceso			X	X			X
Confidencialidad	X	X	X	X	X		X
Confidencialidad del flujo de tráfico	X	X	X	X	X		X
Integridad de los datos			X	X			X
No repudio							X
Disponibilidad							

Fuente: adaptación de Recomendación X. 800, 1991, p. 28.

A este esquema de relaciones, ampliamente documentado y justificado en la Recomendación X.800 entre ataques a la seguridad, servicios de seguridad, mecanismos de seguridad y capas del modelo OSI, se lo puede representar gráficamente como se muestra a continuación y dejar a la vista su aporte a la seguridad en redes. Es que sea que se parta de un servicio de seguridad, de un protocolo TCP o una capa del modelo OSI, es posible conocer las amenazas involucradas y, en consecuencia, cuáles servicios y mecanismos de seguridad son los apropiados para mitigarlas y viceversa.

Figura 2: Utilidad del Modelo de Seguridad OSI



Fuente: elaboración propia.

En resumen, el desafío de la seguridad en redes es superar las amenazas a las que expone el incremento en la interconexión entre redes y sistemas como producto de un uso cada vez más masivo de Internet como medio, cuya arquitectura inicial no tuvo a la seguridad como una de sus características esenciales.

En este marco, conocer de forma sólida la arquitectura sobre la cual se basan las comunicaciones es fundamental para abordar cualquier problemática de seguridad. El modelo de seguridad OSI presentado, cuya publicación data ya de varios años, sigue siendo válido, pues el modelo OSI sigue vigente, ofrece información elemental para determinar cuáles factores se ven involucrados ante una amenaza y cómo pueden ser contrarrestados.

Claro, esto no es todo. En la actualidad, se conocen diversos ataques a la seguridad de las redes como el *IP spoofing*, *DNS spoofing*, *SMTP spoofing*, *man in the middle*, *DDoS* y *cross site scripting*, los cuales se abordan de forma detallada en la bibliografía básica y aquí no han sido mencionados. Esto se debe a que, en el fondo, estos ataques se basan en vulnerabilidades presentes en protocolos que operan en las distintas capas del modelo OSI, con lo cual, si se es capaz de identificar los protocolos o capas afectadas, el modelo de seguridad OSI permitirá asociar el servicio y mecanismo de seguridad adecuado para brindar protección.

Por último, se debe tener en cuenta el avance de la migración en curso del protocolo IPV4 al protocolo IPV6, cuyo principal objetivo es extender la capacidad de asignación de direcciones en el espacio DNS. Esta nueva versión del protocolo IP afecta en cierto grado al modelo OSI, pues incorpora nuevas características como IPSec que resuelven en gran medida las vulnerabilidades de su anterior versión.

Referencias

CCN [Centro Criptologico Nacional]-STIC [Servicios de Tecnologías de la Información y las Comunicaciones]-401. (2015). *Guía de seguridad. Glosario y abreviaturas*. Recuperado de https://www.ccn-cert.cni.es/guias/glosario-de-terminos-ccn-stic-401.html

Cisco. (2017). *An OSI Model for cloud*. Recuperado de https://blogs.cisco.com/cloud/an-osi-model-for-cloud

Gómez Vieites, A. (2011). *Enciclopedia de la Seguridad Informática* (2° ed.). Madrid, España: Ra-Ma.

Unión Internacional de Telecomunicaciones (ITU). (1991). *Recomendación X.800*. Arquitectura de Seguridad para la Interconexión de Sistemas Abiertos para Aplicaciones del CCIT. Recuperado de https://www.itu.int/rec/T-REC-X.800-199103-I/es

Seguridad en servicios de red

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Introducción

La lectura del presente material es meramente complementaria a la bibliografía básica. Las definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha bibliografía.

Un servicio de red es una aplicación que se ejecuta a través de un protocolo de alguna capa del Modelo OSI, capaz de proveer almacenamiento, manipulación, presentación, comunicación de datos u otra funcionalidad e implementado a través de una arquitectura cliente-servidor o punto a punto.

Cada servicio es implementado por un *componente servidor* que se ejecuta en uno o más equipos y es accedido a través de la red por medio de un *componente cliente* que se ejecuta en un equipo o dispositivo remoto.

Tabla 1: Ejemplos de servicios de red por capas del Modelo OSI

Capa Modelo OSI	Protocolo	Servicio
7. Aplicación	FTP	Transferencia de archivos
6. Presentación	TLS	Compresión de archivos
5. Sesión	RPC	Llamada a procedimientos remotos
4. Transporte	TCP	Control de transmisión
3. Red	IPSec	Seguridad para protocolo IP
2. Enlace de datos	ARP	Resolución de direcciones
1. Física	Wi-Fi	Conexión inalámbrica

Fuente: elaboración propia.

Desde el punto de vista de la seguridad, asegurar la confidencialidad, integridad y disponibilidad de los servicios de red es fundamental; en definitiva, estos son los responsables de gestionar el flujo de información a través de la infraestructura tecnológica hacia adentro y fuera de la organización.

En materia de estándares, la serie ISO/IEC 27033 "Tecnologías de Información, Técnicas de Seguridad, Seguridad en Redes" ofrece un conjunto de guías útiles para diseñar e implementar redes seguras y ello implica servicios de red seguros.

También la norma ISO/IEC 27001 "Sistemas de Seguridad de la Información", e ISO/IEC 27002 "Código de Buenas Prácticas para la Gestión

de la Seguridad de la información", hacen mención a la gestión segura de los servicios de red y brindan directrices en tal sentido.

Seguridad en servicios de red

Luego de la breve introducción a los servicios de red, su relevancia en materia de seguridad y los recursos disponibles para alcanzar servicios de red seguros, se presenta a continuación una revisión de algunos de los servicios de red más comunes y un breve análisis de las vulnerabilidades que estos poseen, las que comprometen la seguridad entorno de red en el que se ejecutan.

El servicio FTP

FTP (File Transfer Protocol, puerto 21 TCP)[1] es un protocolo de transferencia de archivos. A través de este protocolo un equipo cliente se conecta a un equipo remoto que hace de servidor para enviar archivos locales o descargar archivos almacenados en ese servidor.

Una de las vulnerabilidades de este protocolo es que está diseñado para ofrecer una óptima velocidad en la conexión, pero no para ofrecer una máxima seguridad; el intercambio de información, desde la autenticación del usuario en el servidor hasta la transferencia de cualquier archivo, se efectua en texto claro, permitiendo a un atacante capturar ese tráfico y obtener así un acceso válido al servidor. Además, si el atacante es capaz de capturar y reproducir los archivos transferidos evidencia una amenaza a la privacidad de los datos del usuario.

Debido a estas debilidades del protocolo FTP, se debe concientizar en el uso de alternativas seguras como SCP y SFTP, que vienen integradas al paquete SSH (Secure SHell). Estos protocolos permiten transferir archivos cifrando el tráfico.

La conexión FTP debe ser limitada de forma exclusiva a los usuarios que lo necesiten. A modo de ejemplo, el usuario root no debería utilizar este servicio, dado que generalmente trabaja en consola.

[1] Para más información sobre File Transfer Protocol (FTP), consulte: https://goo.gl/M8AHV4

El servicio FTP anónimo

Los vulnerabilidades del servicio FTP son exponenciales cuando se debe implementar un servidor de FTP anónimo; es común que estos servicios se convierten en servidores de imágenes sensibles o de distribución indebida de programas protegidos por Licencias comerciales.

Uno de los ataques mas frecuentes a los servidores FTP es la denegación de servicio provocando el consumo masivo del espacio disponible para la carga de archivos; para mitigar este ataque, se debe situar el directorio ~ftp/ en una partición distinta al resto del sistema de archivos, donde sólo se encuentre ese directorio; algunos servidores limitan directamente la cantidad de archivos que se pueden cargar en una misma sesión.

Otro tipo de denegación de servicio que sufren los servidores FTP anónimos tiene que ver con el consumo excesivo de recursos de procesamiento (CPU), tornando al servicio incapaz de responder a las peticiones que se le generan, esto es frecuente en servidores que permiten al descarga de directorios enteros empeaqueatos o comprimidos como un único archivo.

El servicio TELNET

El protocolo TELNET (Telecommunication Network, puerto TCP 23)[2] ofrece la capacidad de utilizar un equipo como si se tratara de una terminal virtual de otra a través de la red. Crea un canal virtual de comunicación similar, aunque inseguro, al que se utilizaría estando en una terminal física conectada a un servidor. Esta comunicación, al establecerse en modo texto, permite hacer uso de las capacidades del equipo sin la necesidad de desplazarse hasta la ubicación física de ese servidor.

Hasta tiempos recientes, TELNET era uno de los servicios que se mantenían habilitados por defecto; con las nuevas prácticas de configuración segura, este protocolo pasó a formar parte de las listas de servicios que deben ser inhabilitados, reduciendo de esta manera las posibilidades de conexión remota insegura. Dado que TELNET no cifra la comunicación, un atacante con un analizador de red (sniffer) es capaz de capturar las credenciales del usuario utilizadas en la conexión.

Las soluciones alternativas mas utilizadas para conexiones remotas son las aplicaciones basadas en el SSH o SSL-Telnet, que ademas de implementar

[2] Para mas información sobre Telecommunication Network (Telnet), consulte: https://goo.gl/DcGkAR

mecanismos de autenticación mas robutos, cifran el tráfico en ambos extermos.

El servicio SMTP

El servicio SMTP (Simple Mail Transfer Protocol, puerto 25 TCP)[3] es ampliamente utilizado para la transferencia de correo electrónico entre equipos; los equipos que intervienen en la comunicación pueden ubicarse en el mismo espacio físico o en lugares remotos.

Las medidas de seguridad mas comunes se basan en realizar consultas inversas al servidor DNS para asegurar de que sólo los equipos registrados envían mensajes; otra práctica común es bloquear el reenvío de mensajes a direcciones que no pertenzcan al dominio local.

Servidores Web

Los servidores web (HTTP, puerto 80, 8080 TPC)[4], es, por excelencia, el servicio más utilizadas por los usuarios de Internet. Los problemas de seguridad relacionados con este HTTP se dividen en tres grupos, en función de los datos a los que se pueden ver comprometidos:

- **Seguridad en el servidor.** Se debe garantizar que la información almacenada en el equipo servidor no pueda ser modificada de forma no autorizada; la información debe permanecer disponible y accedida únicamente por usuarios autorizados.

- **Seguridad en la red.** Cuando un usuario se conecta a un servidor web se produce un intercambio de información entre ambos; se debe garantizar la integridad de los datos transmitidos durante esta comunicación; además se debe garantizar la confidencialidad durante dicha comunicación. Esto cobra especial relevancia cuando se trata de sitios de comercio electrónico y durante el intercambio de datos de tarjetas de crédito.

- **Seguridad en el cliente.** Se debe garantizar al usuario que lo que descarga de un servidor está libre de amenazas y no afectará a la seguridad de su equipo; hechos como este pueden afectar a la imagen de la empresa provocando pérdida de credibilidad y de potenciales clientes.

[3] Para más información sobre Simple Mail Transfer Protocol (SMTP), consulte: https://goo.gl/msrgpy
[4] Para más información sobre Hypertext Transfer Protocol (HTTP), consulte: https://goo.gl/rWazHm

Dotar de seguridad al servidor conlleva, además de las practicas genericas para una estación de trabajo, medidas excepcionales dedicadas al servidor web y su entorno de trabajo. Estas medidas son propias para cada programa servidor. No obstante, y para cualquier software de servidor utilizado (Apache, IIS...), se debe adoptar la siguiente premisa: reducir al mínimo las cuentas de usuario en estos servidores y limitar los servicios ofrecidos por éste aplicando el criterio de separación de tareas; si bien es habitual que un servidor dedicado a cualquier tarea con una cantidad elevada de usuarios brinde también el serivicio web, es recomendable que este servicio se aloje en un servidor dedicado a esa tarea.

Los servidores web se ven afectados también por los errores de programación en las aplicaciones web que hospedan, con lo cual, es fundamental implementar prácticas de programación segura para reducir estos riesgos.

Otra medida de seguridad fundamental es ejecutar el servidor bajo la identidad de un usuario con privilegios mínimos para que todo funcione de forma adecuada con privilegios suficientes, pero nunca como super usuario.
Para garantizar la seguridad de los datos que circulan entre un cliente y el servidor es necesario cifrar dichos datos a través de la implementación de protocolos seguros como SSL/TLS.

Por otro lado, desde un enfoque de usuario, un servidor es seguro si protege la información que recibe y envía hacia él, manteniendo su privacidad, y si no lo conduce a descargas de programas maliciosos (generalmente virus) en su equipo; si sucede lo contrario, la compañía responsable de las páginas se enfrenta a una importante pérdida de imagen, además de los posibles problemas judiciales, de cara a sus usuarios: supóngase que se divulgue en los medios un fallo de seguridad en la versión electrónica de cierto banco; será difícil que todos sus usuarios sigan manteniendo la suficiente confianza en él como para mantener allí su dinero.

SNMP

El protocolo simple de administración de red (puerto 161 TCP)[5] facilita el intercambio de información entre dispositivos presentes en la red (agentes) y es posible reunir información sobre estos (administrador) y utilizarla con fines de gestión.

[5] Para más información acerca del Protocolo Simple de Administración de Red (SNMP), consulta: https://goo.gl/C2TtrW

Este protocolo ampliamente utilizado ha presentado una serie de vulnerabilidades a lo largo de sus versiones, lo que da lugar a ejecución remota de códigos, ataques de denegación de servicios, entre otros.

En la actualidad, su versión SNMP v3 ha resuelto en gran medida estas vulnerabilidades, aunque su configuración se ha vuelto un tanto compleja. No obstante esto, es la versión recomendada.

En resumen, los servicios de red son los que hacen posible en gran medida el funcionamiento de una red, con lo cual dotarlos de seguridad es una tarea elemental para asegurar la confidencialidad, integridad y disponibilidad de dichos servicios y el flujo de información que procesan. Cada servicio tiene su propia particularidad, opera en una capa del Modelo OSI específica y, por lo tanto, es válido recurrir al Modelo OSI de Seguridad, Recomendación X.800 para adoptar los servicios y mecanismos de seguridad adecuados para alcanzar servicios de red seguros.

Las normativas estándares comentadas son también un recurso útil que sirve de guía para gestionar estos servicios de manera formal y basada en buenas prácticas y procesos de mejora continua.

Se debe tener presente que cualquier acción de protección de estos servicios debe estar basada en análisis y gestión de riesgos con el objetivo de que los esfuerzos y recursos utilizados estén dirigidos a aquellos servicios de red que expongan amenazas reales para la organización.

Por último, de forma análoga a lo que sucede entre criptografía y criptoanálisis, donde la segunda estudia formas de vulnerar a la primera en lo que hace a los servicios de red, sucede algo similar con las técnicas de escaneo de vulnerabilidades. Existen herramientas que se encargan de identificar los servicios desplegados en la red para someterlos a análisis de vulnerabilidades, utilizando para ello bases de datos de patrones y firmas actualizadas. Estas herramientas brindan como salida reportes de diagnósticos útiles para conocer el estado de seguridad de dichos servicios y recomendaciones de medidas de seguridad cuando estos presenten vulnerabilidades conocidas.

Referencias

Gómez Vieites, A. (2011). *Enciclopedia de la Seguridad Informática* (2.ª ed.). Madrid, España: Ra-Ma.

ISO/IEC 27001. (2013a). [Tecnologías de información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información. Requerimientos]. Suiza: ISO (Organización Internacional de Estandarización). Recuperada de https://www.iso.org/standard/54534.html

ISO/IEC 27002. (2013b). [Tecnologías de información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información]. Suiza: ISO. Recuperada de https://www.iso.org/standard/54533.html

ISO/IEC 27033-2. (2013c). [Tecnologías de información. Técnicas de seguridad. Seguridad en Redes. Parte 2. Guía para el diseño e implementación de seguridad en Redes]. Suiza: ISO. Recuperada de https://www.iso.org/standard/51581.html?browse=tc

Seguridad en redes inalámbricas

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Introducción

La lectura del presente material es meramente complementaria a la bibliografía básica. Las definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha bibliografía.

En esta lectura, se presenta una breve revisión de las redes inalámbricas que cumplen con la familia de estándares 802.11[1], conocidas como redes Wi-Fi (*wireless fidelity*), y los aspectos más relevantes en materia de seguridad.

El uso de este tipo de redes se ha extendido de manera exponencial tanto para usos hogareños como organizacionales y es cierto que una implementación sin características solidas de seguridad es un recurso cada vez mas utilizado por atacantes que se valen de estos puntos de acceso para inyectar en la red, tanto interna del punto de acceso, como externa accedida a través de éste, todo tipo de ataques.

En el marco de una investigación forense, que se realice con posterioridad al hecho cometido, la dirección IP que se toma como uno de los elementos de prueba es la que tiene asignada el punto de acceso vulnerable, por ende, el principal responsable será el propietario de ese activo.

Seguridad en redes inalámbricas

Con la evolución de Internet y de las redes surgió la necesidad de crear una tecnología inalámbrica capaz de asegurar la compatibilidad de equipos fabricados por distintos proveedores. Con el objetivo de lograr esa compatibilidad, se creó, en 1999, la Wireless Ethernet Compatibility Alliance (WECA), actualmente llamada Wi-Fi Alliance[2] y conformada por un grupo de empresas fabricantes de dispositivos inalámbricos.

En el año 2000, WECA certificó la norma IEEE 802.11b, con la marca WiFi. A partir de allí todos los equipos con el sello WiFi pueden interactuar entre ellos con independencia del fabricante. Desde su creación, la familia de estándares 802.11 ha ido evolucionando y mejorando aspectos como el rango y velocidad de transferencia de información, entre otros. (Villarroel, 2017)

La norma que define el estándar IEEE 802.11 se diseñó de manera que se mantuviera una completa compatibilidad con los servicios de redes locales (Ethernet). La principal diferencia que existe entre la norma 802.11 y la norma 802.3 (Ethernet) es la forma en que los paquetes son transmitidos, el resto no presenta cambios (Villarroel, 2017).

[1] Para más información sobre la familia de estándares 802.11, consulta: https://goo.gl/eyQYjx
[2] Para más información sobre Wi-Fi Alliance, consulte: http://www.wi-fi.org/

En la actualidad, este tipo de red se encuentra disponible prácticamente en todos los ámbitos de la sociedad, campus universitarios, centros de investigación, aeropuertos, zonas públicas de esparcimiento, domicilios, organizaciones, entre otros, por lo que es necesario implementar medidas de control para limitar accesos no deseados a estas redes y asegurar la disponibilidad del servicio.

Tabla 1: Evolución de la seguridad en redes inalámbricas

1997	2001	2003	2004 → actualidad
WEP	**802.1X EAP**	**WPA**	**802.11i /WPA2**
- Cifrado básico. - Autenticación débil. - Claves estáticas. - No escalable. - Filtrado MAC y SSID-Cloacking utilizados como complemento WEP.	- Claves dinámicas. - Cifrado mejorado. - Autenticación de usuarios. - 802.1X EAP (LEAP, PEAP). - RADIUS.	- Estandarizado. - Cifrado mejorado. - Autenticación de usuarios sólida (LEAP, PEAP, PEAP-FAST).	- Cifrado AES. - Autenticación. - Gestión dinámica de claves.

Fuente: adaptación de Certificaction Kits, 2012.

Protocolo de autenticación WEP

Para prevenir accesos no autorizados, se diseñó el protocolo Wired Equivalent Privacy (WEP)[3]. Este protocolo utiliza un cifrado de clave simétrica de manera que, para acceder a la red, el usuario debe conocer esta clave. A pesar de que el estándar IEEE 802.11 soportaba el cifrado desde su creación, las primeras versiones no lo incluían, con lo cual era muy fácil conectarse a una red Wi-Fi cualquiera con el consecuente riesgo que supone para el propietario de la red.

Por otro lado, se encontraron importantes fallos de seguridad en este protocolo que permiten a un atacante descifrar el tráfico al basarse en un análisis estadístico de este o manipular los puntos de acceso. Este es un

[3] Para más información sobre Wired Equivalent Privacy (WEP), consulta: https://tools.ietf.org/html/rfc5418

problema grave principalmente en lugares en los que la clave WEP de acceso no se cambia con frecuencia. Los principales errores en el diseño del protocolo WEP son los siguientes:

- uso de una única clave estática que comparten los usuarios;
- el vector de inicialización utilizado es de 24 bits, lo que provoca colisiones en puntos de acceso muy concurridos;
- uso de un control de integridad lineal, como es CRC-32;
- uso del algoritmo de cifrado RC4.

Con el análisis de las debilidades del protocolo, surgieron numerosos ataques que terminaron en el desarrollo de dos herramientas de dominio público como Airsnort[4] o WEPCrack[5], las que permiten analizar el tráfico y obtener la clave en redes inalámbricas con seguridad WEP.

Protocolo de autenticación WPA

La necesidad de mejorar el protocolo WEP era evidente, por lo que, en octubre de 2002, la Wi-Fi Alliance aprobó el uso del Temporal Key Integrity Protocol (TKIP)[6] bajo el nombre de Wi-Fi Protected Access (WPA)[7].

Este protocolo TKIP incluye mecanismos para mejorar el cifrado de datos en las redes inalámbricas. WPA utiliza TKIP, que usa el mismo algoritmo de cifrado que WEP (RC4), pero construye claves de una forma distinta (Serrano Flores, 2011).

El protocolo TKIP implementa una clave temporal de 128 bits que deben conocer los usuarios para poder conectarse a los puntos de acceso. Para crear la clave que cifrará los datos, esta clave temporal se combina con la dirección MAC del dispositivo del usuario y, a continuación, se añade un vector de inicialización de 16 bytes (Serrano Flores, 2011).

La principal diferencia de WPA respecto a WEP es que las claves temporales cambian, en promedio, a cada 10.000 paquetes enviados, lo que conlleva una mejora significativa a la seguridad de la red (Serrano Flores, 2011).

[4] Para más información sobre Airsnort, consulta: https://sourceforge.net/projects/airsnort/
[5] Para más información sobre WEPCrack, consulta: http://wepcrack.sourceforge.net/
[6] Para más información sobre Temportal Key Integrity Protocol (TKIP), consulta: http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf
[7] Para más información sobre de Wi-Fi Protected Access (WPA), consulta: http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf

En la actualidad, la nueva generación de dispositivos incluye el uso del algoritmo de cifrado AES, implementación que es parte de la evolución del protocolo WPA2[8].

Ataques a las redes inalámbricas

A continuación, se presenta una breve revisión de algunas de las principales amenazas a las que se encuentran expuestas las redes inalámbricas Wi-Fi. Para profundizar estos conceptos, se recomienda recurrir a la bibliografía básica, la que aborda estos contenidos de forma ampliada.

Warchalking

El Warchalking es una práctica que consiste en dibujar símbolos en paredes o pisos para indicar la existencia de puntos de acceso desprotegidos que permitan el acceso inalámbrico a redes y /o a Internet. Luego todos podrán ver desde el exterior que en ese lugar hay nodos abiertos sin ningún tipo de protección (Vieites, 2011).

WarDriving

El Wardriving se realiza desde un vehículo con el cual se recorren diversas calles y con un GPS y un plano de la ciudad, se marcan los puntos desprotegidos (Vieites, 2011).

Análisis del tráfico y sustracción de información confidencial

- Un tercero no autorizado intercepta de forma no autorizada las señales de radio intercambiadas entre una estación inalámbrica y un punto de acceso, lo que compromete la confidencialidad de la información. (Valero Sánchez, 2010, http://tejo.unizar.es/wifi.pdf)
- Interceptar la comunicación de forma no autorizada es un ataque pasivo dado que, quien realiza esta intercepción, puede capturar un mensaje sin alterar los datos, el emisor y el receptor del mensaje no advierten la intrusión, con lo cual no se toman medidas para evitarlo. (Valero Sánchez, 2010, http://tejo.unizar.es/wifi.pdf)

[8] Para más información sobre Wi-Fi Protected Access v.2 (WPA2), consulta: http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf

Conexión no autorizada a la red inalámbrica

- Un intruso se introduce en el sistema de una red WLAN al suplantar la identidad de un usuario autorizado. Una vez ingresado a la red, el intruso puede vulnerar la confidencialidad e integridad del tráfico de la red. Esto constituye un ejemplo de ataque activo. (Valero Sánchez, 2010, http://tejo.unizar.es/wifi.pdf)
- Una variante de los accesos no autorizados es el caso de los atacantes que engañan a las estaciones inalámbricas al instalar un punto de acceso ilegal alternativo y capturar claves secretas y claves de inicio de sesión. (Valero Sánchez, 2010, http://tejo.unizar.es/wifi.pdf)

Interferencias electromagnéticas

- Las interferencias de radio pueden degradar seriamente el ancho de banda (la tasa de transferencia de datos). Estas interferencias suponen un ataque de denegación de servicios (DoS). (Valero Sánchez, 2010, http://tejo.unizar.es/wifi.pdf)
- En muchos casos, las interferencias son accidentales, pero también pueden ser intencionadas. Si un atacante dispone de un transmisor potente, puede generar una señal de radio lo suficientemente fuerte como para cancelar las señales más débiles e interrumpir las comunicaciones. (Valero Sánchez, 2010, http://tejo.unizar.es/wifi.pdf)

Amenazas físicas

Una WLAN utiliza una serie de componentes físicos, incluyendo los puntos de acceso, cables, antenas, adaptadores inalámbricos y *software*. Los daños sufridos por cualquiera de estos componentes podrían reducir la intensidad de las señales, limitar el área de cobertura o reducir el ancho de banda, lo que pone en riesgo la capacidad de los usuarios para acceder a los datos y a los servicios de información. (Valero Sánchez, 2010, http://tejo.unizar.es/wifi.pdf)

En resumen, como sucede en el ámbito de toda nueva tecnología, las redes inalámbricas, principalmente las tratadas en este material, 802.11 Wi-Fi, han ido evolucionando sus características de seguridad con el tiempo.

A pesar de ello, existen diversos factores que afectan a la seguridad de estas redes que van más allá de los métodos de autenticación que aseguran la confidencialidad en integridad de la información y que tienen

que ver con la disponibilidad del servicio. Por ejemplo, las interferencias y las pérdidas de señal siguen siendo una vulnerabilidad presente y que se deben tener considerar al momento de diseñar e implementar redes de este tipo.

En materia de normativas estándares, ISO/IEC 27033-6, "Tecnologías de Información, Técnicas de Seguridad, Seguridad en Redes. Parte 6: Asegurando el acceso a Redes Inalámbricas IP", ofrece un marco formal para un tratamiento seguro de redes inalámbricas.

También ISO/IEC 27001, "Tecnologías de Información, Técnicas de Seguridad, Sistema de gestión de la seguridad de la información, Requerimientos", e ISO/IEC 27002 "Tecnologías de información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información", brindan requerimientos y directrices que sirven de guía para la gestión de redes inalámbricas.

Referencias

Certification Kits LLC. (2012). Evolution of Wireless LAN Security (Traducción propia). Recuperado de https://www.certificationkits.com/cisco-certification/cisco-ccna-640-802-exam-certification-guide/cisco-ccna-wireless-part-iii/

Gómez Vieites, A. (2011). *Enciclopedia de la Seguridad Informática* (2.ª ed.). Madrid, España: Ra-Ma.

ISO/IEC 27001. (2013a). [Tecnologías de información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información. Requerimientos]. Suiza: ISO (Organización Internacional de Estandarización). Recuperada de https://www.iso.org/standard/54534.html.

ISO/IEC 27002. (2013b). [Tecnologías de información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información]. Suiza: ISO. Recuperada de https://www.iso.org/standard/54533.html.

ISO/IEC 27033-6. (2016). [Tecnologías de información. Técnicas de seguridad. Seguridad en Redes. Parte 6. Asegurando el acceso a Redes Inalámbricas IP]. Suiza: ISO. Recuperada de https://www.iso.org/standard/51585.html

Valero Sánchez, J. A.(2010). *Curso de redes Inalámbricas*. Zaragoza, España: Universidad de Zaragoza. Recuperado de: http://tejo.unizar.es/wifi.pdf)

Mecanismos de prevención y protección

Seguridad Informática

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Introducción

La lectura del presente material es meramente complementaria a la bibliografía básica. Las definiciones teóricas de los conceptos aquí expuestos deben ser tomadas de dicha bibliografía.

En este material, se abordan los distintos mecanismos de prevención y protección de la infraestructura de red de una organización. El objetivo de estos mecanismos es proteger la información interna y a la vez permitir que la organización pueda seguir comunicándose con redes de niveles de seguridad más bajos, como puede ser Internet.

Es importante tener en presente que no existe una única herramienta que brinde una protección generalizada de la red. Por el contrario, dotar de seguridad a una red supone diseñar una estrategia que integre una serie de soluciones que en conjunto contribuyan en la cobertura de la superficie de ataque que expone la organización.

Mecanismos de prevención y protección

El componente que delimita la red interna de la red externa es el cortafuegos (*firewall*). Se sitúa entre la red local e Internet con el fin de filtrar el tráfico no autorizado proveniente del exterior hacia la red interna y funciona sobre la capa de red de TCP/IP.

Los cortafuegos implementan una política de seguridad que define los servicios y accesos permitidos en términos de configuración de red. Las funcionalidades básicas de un cortafuegos son las siguientes:

- bloqueo de tráfico no deseado;
- redirección de tráfico a sistemas internos;
- ocultación de sistemas vulnerables;
- control de tráfico hacia y desde la red privada;
- ocultación de información: nombres de sistemas, topología de red, etcétera;
- sistema de autenticación más robusto.

En cuanto a los tipos de cortafuegos existentes, la forma más común de clasificarlos es al basarse en los niveles de la pila TCP/IP en los que operan y en la complejidad del filtrado implementado por el cortafuegos.

- Router *de filtrado de paquetes*. Este tipo de cortafuegos filtra los paquetes en función de los principales campos de la cabecera IP y TCP e ignora el resto de los campos y datos del paquete correspondiente. En la actualidad, son muy raros de encontrar implantados en los sistemas. Existen cortafuegos de filtrado de paquetes más avanzados que incorporan una tabla de estado que le permite hacer un seguimiento de

las conexiones abiertas y manejar así características especiales de ciertos protocolos.

- *Pasarelas a nivel de aplicación.* También conocido como *proxy*, este tipo de cortafuegos actúa de intermediario en todas las transacciones que lo atraviesan, modificando partes de los campos de datos según la política de seguridad definida.
- *Pasarelas a nivel de circuito.* Este tipo de cortafuegos redirige las tramas una vez que se ha comprobado que la conexión ha sido establecida.

Router de filtrado de paquetes

Los cortafuegos de filtrado funcionan básicamente descartando o aceptando paquetes en función de una serie de reglas definidas por el administrador de la red. Las reglas comprueban cierta información contenida en los paquetes como dirección IP de origen/destino, número de puerto de origen/destino, tipo de protocolo de transporte usado (UDP o TCP), interfaz por la que llega el paquete, tamaño del paquete, entre otros.

Figura 1: *Router* de filtrado de paquetes

Fuente: elaboración propia.

Existen dos criterios de implementación de las reglas de filtrado basados en las políticas predeterminadas por el *router*:

- *Política restrictiva.* Todo el tráfico que no esté permitido explícitamente en las reglas de filtrado será descartado.
- *Política permisiva.* Todo el tráfico que no esté prohibido explícitamente en las reglas de filtrado será aceptado.

La elección de la política por defecto depende de varios factores: en función del número de *hosts* externos que puedan acceder a la red, el número de servicios abiertos, etcétera. Una política restrictiva puede llegar a ser complicada de mantener, ya que es necesario indicar explícitamente en las reglas de filtrado qué paquetes deben ser aceptados. No obstante,

esta es la opción más segura. Por otro lado, *una política permisiva facilita el uso de la red a los usuarios,* pero el nivel de seguridad proporcionado es bajo.

El uso de *routers* de filtrado de paquetes es muy simple, pero tiene algunas desventajas:

- no suelen disponer de un *log* donde registrar el tráfico de manera que el administrador de la red pueda saber si está sufriendo un ataque;
- no evita ataques a nivel de capa de aplicación;
- pueden ser evadidos mediante ataques de suplantación de identidad, modificando la dirección IP del origen (*IP spoofing*);
- pueden presentar agujeros de seguridad si el administrador de red no realiza una correcta configuración de las reglas de filtrado.

Pasarela a nivel de aplicación

Una pasarela a nivel de aplicación, también llamada *proxy*, actúa de intermediaria en todas las transacciones que la atraviesan. Los usuarios contactan con la pasarela que ofrecerá servicios *proxy* para unas determinadas aplicaciones (Telnet, HTTP, FTP, IMAP, POP, entre otras). Este proceso es transparente al usuario, ya que tiene la impresión de comunicarse directamente con la máquina destino.

Figura 2: Pasarela de nivel de aplicación. *Proxy*

Fuente: elaboración propia.

Este tipo de pasarelas suelen ser más seguras que los *routers* de filtrado de paquetes, ya que no hay que incluir reglas a nivel de red que indiquen todo el tráfico permitido. Solo es necesario indicar las aplicaciones admitidas.

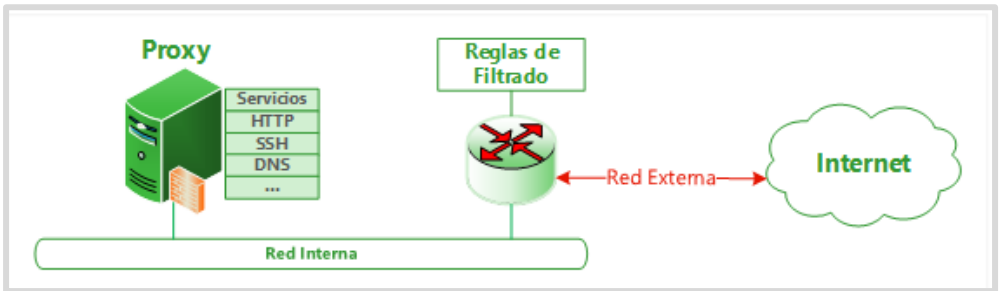
Las pasarelas a nivel de aplicación permiten además la autenticación de los usuarios que pretenden conectarse a los servicios. También es muy sencillo mantener un *log* en el que se registra el tráfico entrante.

La principal debilidad de este tipo de cortafuegos es la posibilidad de una caída del *proxy* en entornos con mucha demanda, ya que supone un procesamiento extra en cada conexión que podría sobrecargar el sistema. Otra desventaja surge de la necesidad de que el *proxy* requiera soporte específico para las distintas aplicaciones.

Normalmente existe soporte para las aplicaciones más comunes, pero los problemas surgen a la hora de adoptar nuevas tecnologías.

En la práctica, es habitual encontrar topologías de defensa que incluyen tanto una pasarela a nivel de aplicación como un *router* de filtrado de paquetes para una mayor seguridad del sistema.

Figura 3: Topología de defensa. *Router* de filtrado combinado con *proxy*



Fuente: elaboración propia.

Pasarela a nivel de circuito

Las pasarelas a nivel de circuito pueden ser consideradas un híbrido entre los *routers* de filtrado de paquetes y las pasarelas a nivel de aplicación. En primer lugar, el usuario debe establecer una conexión con la pasarela, al igual que en las pasarelas a nivel de aplicación. Una vez establecida la conexión, la pasarela se comporta como un *router* de filtrado de tráfico y redirige las tramas entre ambos extremos sin analizar el contenido de estos a nivel de aplicación.

La principal ventaja de este tipo de cortafuegos es que, una vez realizada la autenticación del usuario, no hay necesidad de examinar el contenido de los paquetes, únicamente las cabeceras, lo que reduce la carga del sistema.

Sistemas de detección de intrusiones

El mejor complemento para la seguridad perimetral son los mecanismos de detección de intrusiones (*IDS*).

Un sistema de detección de intrusiones permite detectar actividades incorrectas, inapropiadas o anómalas en un sistema. Los sistemas de detección de intrusiones pueden trabajar en conjunto con un cortafuegos para incrementar el nivel de seguridad, lo que da lugar a los sistemas de prevención de intrusiones.

El IDS incorpora un analizador de paquetes de la red (*sniffer*) con los que el núcleo del IDS puede obtener información sobre el tráfico que circula por la red. Mediante el análisis del tráfico capturado, el IDS detecta anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

Este tipo de sistemas permite la detección de ataques de exploración de la red o del sistema (sistema operativo de los equipos, versiones de *software*, *hosts* activos, escáner de vulnerabilidades, topología de la red, etc.), ataques de denegación de servicio (DoS o DDoS) o ataques de acceso a sistemas.

Sistemas de prevención de intrusiones

Es un caso especial de IDS que incorpora un cortafuegos que permite el filtrado del tráfico.

Por lo general, se presentan integrados al IDS y la funcionalidad de IPS puede ser activada o desactivada.

Switch de nivel de aplicación

Normalmente un *switch* trabaja en la capa dos del modelo OSI, pero, debido a la necesidad de trabajar con grandes anchos de banda, cada vez son más comunes los conmutadores de nivel de aplicación, capa siete del modelo OSI.

Estos dispositivos analizan la información de aplicación (DNS, HTTP, FTP, etc.) para realizar tareas de balanceo de carga entre varios servidores. Algunos conmutadores incorporan capacidades que proporcionan protección frente a ataques de denegación de servicio (DoS o DDoS).

Cortafuegos/IDS de aplicación

Al igual que los *switches* a nivel de aplicación, estos sistemas trabajan con la capa siete del modelo OSI. Estas herramientas se pueden instalar sobre el sistema final a proteger y, además de permitir el análisis del tráfico de la red, pueden analizar elementos como la gestión de la memoria, llamadas al sistema o intentos de conexión de una aplicación.

Para funcionar, el cortafuegos necesita que el administrador defina unos perfiles en los que se realiza una fase de entrenamiento que permite establecer un modelo de comportamiento normal de las aplicaciones y se definen unas políticas de seguridad. Todas las acciones que no estén definidas en el perfil se considerarán un intento de intrusión y serán bloqueadas por el sistema.

Conmutador híbrido

Este dispositivo *hardware* puede ser considerado un híbrido entre los *switches* de nivel de aplicación y los cortafuegos/IDS de aplicación, ya que se instalan de la misma manera que los primeros, pero funcionan a través de la definición de políticas de seguridad como los segundos.

Estos dispositivos tienen la ventaja de que pueden ser configurados mediante la importación de datos obtenidos mediante un escáner de vulnerabilidades ejecutado sobre el sistema a proteger. Puede utilizarse en conjunto con un *switch* de nivel de aplicación que le redirija únicamente el tráfico malicioso para reducir la carga de trabajo.

Escáneres de vulnerabilidades

Se trata de herramientas que permiten realizar un conjunto de pruebas sobre un sistema o red para encontrar las debilidades o fallos de seguridad de estos.

Los escáneres de vulnerabilidades son herramientas de seguridad muy útiles que deben utilizarse como complemento de otros sistemas de prevención.

Algunas de sus ventajas son que reducen de manera eficaz los fallos de seguridad más frecuentes en un sistema y que permiten detectar cambios en las configuraciones de los sistemas.

Mientras que las principales desventajas de estas herramientas tienen que ver con que solo son capaces de detectar fallos de seguridad durante los lapsos de tiempo en los que se ejecuta y que solo pueden encontrar las vulnerabilidades que contengan en su base de datos, por lo que esta debe actualizarse constantemente para incluir nuevas amenazas.

Sistemas trampa

Los sistemas trampa presentan como característica novedosa respecto a los sistemas tradicionales que buscan atraer al atacante en lugar de evitarlo.

- *Honeypot*. Es un *software* o conjunto de ordenadores cuyo objetivo es atraer atacantes al simular ser sistemas débiles y vulnerables a ataques. Estos sistemas están diseñados para captar la atención del atacante y así poder recopilar información sobre sus métodos y actividades. Para que el sistema sea efectivo, el atacante no debe notar en ningún momento que está siendo engañado o monitorizado.
  Honeypot suele situarse detrás de un cortafuegos, aunque es posible situarlo delante.
- *Honeynet*. Una *honeynet* es un tipo especial de *honeypot* que actúa sobre una red entera, diseñada para ser atacada y recabar más información sobre posibles atacantes. Se usan equipos reales con sistemas operativos reales que corren aplicaciones reales. Este tipo de *honeypots* se usan principalmente para la investigación de nuevas técnicas de ataque y para comprobar el *modus operandi* de los intrusos.

Padded cell

Este tipo de sistemas funciona conjuntamente con otros sistemas IDS. Cuando el sistema IDS detecta tráfico malicioso, lo redirige hacia el sistema *padded cell*. Un sistema *padded cell* simula un entorno real que atraiga a los atacantes y en el que no puedan causar daño.

Al igual que *honeypot* y *honeynet*, los sistemas *padded cell* son utilizados para comprender los métodos de ataque de los intrusos.

Para instalar en un entorno real un sistema *padded cell*, puede utilizarse un sistema *bait and switch*. *Bait and switch* utiliza el IDS Snort[1] para detectar los ataques y se instala en un sistema que tenga al menos tres interfaces de

[1] Para más información sobre Snort, consulta: https://www.snort.org

red de manera que, cuando detecta tráfico malicioso, lo redirecciona hacia el sistema *padded cell* sin que el atacante se dé cuenta.

Verificador de integridad de archivos

Es una herramienta que puede usarse como complemento de un sistema de detección de intrusiones. Utiliza funciones criptográficas de tipo resumen (*hash*) o código de verificación (*checksum*) para calcular los valores correspondientes y compararlos con valores de referencia con la intención de encontrar diferencias en los archivos.

Los intrusos pueden modificar o borrar archivos que pueden revelar su actividad y eliminar las huellas que hayan podido dejar. También podrían dejar una puerta trasera por la cual volver a acceder al sistema.

Este tipo de sistemas solo pueden detectar intrusiones si el atacante ha modificado algún contenido o archivo ejecutable.

Topologías de defensa y zonas desmilitarizadas

Una topología de defensa puede estar conformada por un dispositivo o un conjunto de dispositivos que estarán configurados de manera que el tráfico que pase a través de ellos pueda ser limitado, cifrado o descifrado.

La planificación de una arquitectura de seguridad no es trivial, sino que es una tarea delicada que debe fundamentarse en una *política de seguridad* definida por la corporación, determinar los responsables y beneficiarios de los servicios, ubicar el cortafuegos en un lugar adecuado y controlar y mantener el correcto funcionamiento de este, así como de las políticas de seguridad implementadas. (Portillo, 2009, https://goo.gl/2ttXmd).

Arquitecturas simples

Una arquitectura simple es aquella en la que se sitúa el *firewall* o el control de seguridad en la conexión entre la red interna y el medio inseguro al que está conectado (Internet).

Esta arquitectura cuenta con un equipo al que se lo denomina *bastión*. Se trata de un equipo que posee una fuerte protección, ya que estará expuesto a sufrir ataques desde el exterior. Se sitúa entre la red exterior y la red interna.

El bastión con interfaz dual es el intermediario entre la red interna y el exterior, por lo que es el punto crítico de la topología. Si el atacante logra vulnerar al *firewall*, la red interna quedará expuesta y, por lo tanto, podrá ser atacada.

Arquitecturas de defensa en profundidad

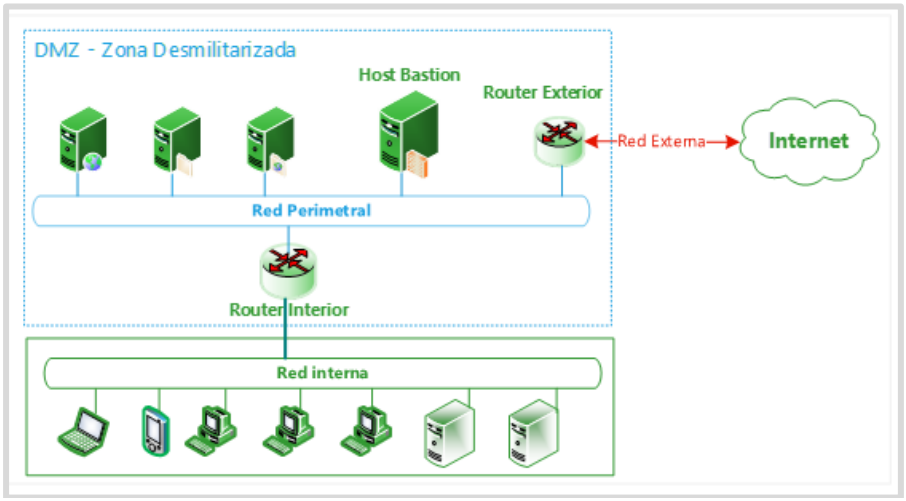
Es frecuente conectar el cortafuegos a una tercera red, conocida como *zona desmilitarizada* (DMZ), en la que se ubican los servidores que deben permanecer accesibles desde la red exterior, como un servidor web, servidor de correos, servidor de acceso remoto, entre otros.

En este tipo de arquitecturas, se pueden diferenciar dos zonas en la red interna: la DMZ o *perimeter network* y la *internal network* o zona de red interior. A esta última zona, los paquetes llegan ya filtrados desde la zona desmilitarizada.

Esta arquitectura permite mantener segura la red interna a pesar de que un atacante haya logrado infiltrarse en la DMZ.

El concepto de *defensa en profundidad* proviene del ámbito militar y refiere a la acción de anteponer una serie de barreras para proteger al objetivo. En este caso, el objetivo que se defenderá será la información de la organización alojada en la red interna.

Figura 4: Arquitectura de defensa en profundidad



Fuente: elaboración propia.

Como conclusión, no existe una solución única que permita proteger por sí sola a toda la infraestructura de tecnología de la organización.

Se trata de una actividad compleja y dinámica que requiere del diseño de una estrategia de seguridad basada en la política de seguridad de la organización y, oportunamente, en análisis y gestión de riesgos para enfocar las acciones de protección tanto en relación a las vulnerabilidades propias de las tecnologías involucradas, como también en relación a los riesgos propios del segmento de negocio en la cual opera la organización.

La seguridad tiene un componente económico y un componente técnico.

En relación al componente económico, las acciones de protección deben estar alineadas con la capacidad de recursos que la organización disponga para invertir en seguridad. Por otro lado, el activo que se protege debe poseer un valor superior a la suma de los esfuerzos desplegados para protegerlo.

En cuanto al componente técnico, una seguridad excesiva puede afectar a la disponibilidad de los servicios que operan en la red, con lo cual se torna inadecuada. Se debe encontrar un punto de equilibrio en el cual los servicios puedan operar bajo un entorno con las medidas de seguridad apropiadas y suficientes.

Por otro lado, es oportuno poner en contexto el factor humano y la necesidad de formación en materia de seguridad y concientización de usos responsables de los activos y la información. Si en el contexto de la organización este factor no es abordado en el marco de un sistema de gestión de seguridad de la información, por más avanzadas que sean las tecnologías de prevención y protección que se implementen, estas no podrán hacer frente a las amenazas que escapen a su contexto de control.

Referencias

Gómez Vieites, A. (2011). *Enciclopedia de la Seguridad Informática* (2.ª ed.). Madrid, España: Ra-Ma.