ÍNDICE

Tema 2

La seguridad en los elementos físicos existentes en una red

1. Introducción, orientaciones para el estudio y objetivos
2. Los sistemas de cableado o inalámbricos
3. Repetidores, *hubs* y conmutadores (*switches*)
4. Encaminadores (*routers*)
5. Los servidores y otras máquinas
6. Conocimientos y competencias adquiridas
7. Bibliografía
8. Palabras clave
9. Ejercicios resueltos
10. Ejercicios de autoevaluación

1. INTRODUCCIÓN, ORIENTACIONES PARA EL ESTUDIO Y OBJETIVOS

Todas las redes están compuestas por una serie de dispositivos físicos, **máquinas**, que tienen una mayor o menor capacidad de control mediante programación *software*, pero no dejan de ser máquinas, con una misión concreta en la red. Es radicalmente importante considerar sus posibles inseguridades, teniendo en cuenta que, en cierto sentido, son las piezas básicas del sistema. Esas máquinas, además, se comunican entre sí utilizando uno o varios **medios de transmisión**, habitualmente **cables** de una tecnología determinada, unos más susceptibles que otros a determinados problemas de seguridad. Hoy en día, además, cada vez son más las redes que, enteramente o en parte, se comunican mediante **sistemas inalámbricos**, que exhiben sus problemas particulares desde el punto de vista de la seguridad.

Tanto los medios de transmisión como las distintas máquinas son susceptibles de ataques contra su seguridad, desde dos puntos de vista:

- Ataques físicos a su seguridad, en los que se busca la destrucción parcial o total del dispositivo concreto y, como consecuencia, la inhabilitación, total o parcial, de la red en la que prestan sus servicios.

- Ataques «lógicos» a su seguridad, en los que, buscando los mismos objetivos que los anteriores, no se dispone de un acceso físico y, como consecuencia, no se pueden realizar o, aun disponiendo de acceso físico, no es el método preferido para el ataque.

Aunque no se vaya a desarrollarlos, hay que considerar los ataques físicos, es decir, los ataques en los que los dispositivos resultan dañados físicamente. Estos ataques son relativamente fáciles de evitar, disponiendo de

una buena política de seguridad física, que evite el acceso físico a tales sistemas por parte de personal no autorizado.

Centrándose en los ataques lógicos, hay que entender cada una de las responsabilidades de los elementos *hardware* típicos de una red y cada una de sus posibles inseguridades, para considerarlas de cara a la política de seguridad.

Así pues, primero hay que identificar los elementos que se tienen que considerar:

- Canales de comunicación y cableados típicos: par trenzado, fibra óptica, sin olvidarse de considerar la comunicación inalámbrica.
- Repetidores.
- *Hubs* o concentradores.
- Conmutadores.
- Encaminadores.
- Máquinas utilizadas por los usuarios, especialmente servidores.

Para su estudio posterior ayudará el recordar los niveles OSI que deben implementar muchos de estos dispositivos. Se incluye la figura 2.1, como recordatorio de cada una de las funciones que realizan. No obstante, se examinan con más detalle en los siguientes apartados.

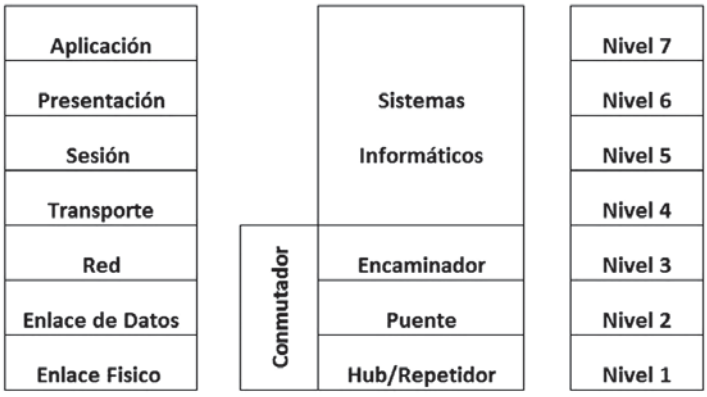

Figura 2.1. Niveles OSI de dispositivos en sistemas de comunicaciones.

2. LOS SISTEMAS DE CABLEADO O INALÁMBRICOS

En las comunicaciones digitales, una diferencia de potencial (o voltaje, si se prefiere) implica un 1 binario y otra (o la ausencia de alguna) marca el 0 binario. Como se sabe, este formato simple hace bastante resistente al «ruido» a las comunicaciones digitales, pero, a su vez, implica un cierto inconveniente, que consiste en la necesidad de transmitir 8 de tales elementos binarios para cada carácter. Cuando se considera un circuito eléctrico, como por ejemplo una red *Ethernet* que usa cables de **par trenzado**, el estado del voltaje está constantemente cambiando para transmitir información, lo que introduce la primera inseguridad: la **interferencia electromagnética**.

La interferencia electromagnética es producida por circuitos de corriente alterna, los que existen en las comunicaciones analógicas y digitales. Si se pudiera «ver» a los electrones en el cable, se podría observar que, al cambiar el voltaje y fluir la corriente por el cable, los electrones tienden a «colocarse» sobre todo en la superficie del cable, mientras que el punto central del cable no mostraría «movimiento» electrónico. Si se incrementa la potencia, se empieza a radiar energía, con un ángulo de 90º al flujo de corriente. Lo verdaderamente importante es que esta radiación está en relación directa con la señal en el cable. Además, si se hace mayor la frecuencia o el voltaje, crece también la cantidad de energía radiada.

Esta radiación electromagnética puede medirse y obtener, a partir de ella, la señal que está viajando por el cable. De hecho, hace muchos años que se dispone de dispositivos para tal medición, que se conectan alrededor del cable, para medir la señal que viaja por el conductor central. Una vez registrados los «pulsos» digitales, simplemente hay que convertirlos de formato binario a un formato más entendible.

Una solución obvia, pero no por ello comúnmente desplegada, es usar cables apantallados, de los que se dispone también hace tiempo, pero que son más caros y presentan otros problemas de montaje que no son objeto de este libro. Estos cables no solo protegen la información que viaja a través del medio de transmisión frente a «escuchas» indeseadas, sino que además la protegen contra interferencias que puedan distorsionarla hasta el punto de inhabilitarla.

Una forma alternativa de medir el peligro al que se está expuesto con este tipo de problemas es mirar la gran cantidad de dinero que gastan

los ejércitos en disponer de lo que, en su jerga, se denomina **productos TEMPEST**, que empiezan por cables apantallados, pero pueden ser conmutadores (o cualquier dispositivo) apantallados y que pueden llegar a habitaciones, o incluso edificios enteros, apantalladas.

Otra solución, que se puede usar completa o parcialmente, dependiendo de la necesidad y del presupuesto es usar cable de **fibra óptica** que, además de permitir en muchas ocasiones una mayor velocidad de transmisión, es completamente inmune a las interferencias citadas, pues la transmisión se basa en señales de luz.

Otro aspecto importante a tener en cuenta (al que se volverá en breve) es que en los segmentos de red en que no existan conmutadores y no se tenga un control muy exhaustivo de quién está conectado con un equipo al segmento, se corre el riesgo de que alguien esté usando un **analizador de protocolos** (o «***sniffer***»), que permite «ver» el tráfico de cualquier equipo a cualquier otro equipo, aprovechando la capacidad de casi cualquier tarjeta de red *Ethernet* de trabajar en modo «promiscuo». Hasta hace unos años, no era fácil disponer de un «***sniffer***», pero, hoy en día, existes muchas herramientas gratuitas (diseñadas para gestión, no para ataques de red) que permiten capturar el tráfico que viaja por la red y aprovechar los conocimientos de IP de cada uno, para obtener, realmente, mucha información.

Se puede también usar transmisión sin cable, mediante **lasers o infrarrojos**. El principal inconveniente es la facilidad de cortar el servicio, interrumpiendo la señal.

Aunque se analizarán detalladamente los problemas específicos que supone el uso de comunicaciones y redes inalámbricas o «*wireless*» en el tema 18, conviene hacer una introducción de los problemas que presenta este tipo de tecnología de comunicación.

Se puede definir una red inalámbrica (WLAN - *Wireless LocalArea Network*) como un sistema flexible de comunicación de datos, que suele implementarse como extensión, o alternativa a una red de área local (LAN - *Local Area Network*) tradicional, dentro de un edificio o entre varios edificios (modelo campus).

Las WLANS usan señales electromagnéticas de radio para comunicar información de un punto a otro, sin necesidad de ningún cable.

Las ondas de radio son conocidas, en este marco, como portadoras de radio, ya que su única función es llevar energía al receptor remoto. Los datos que se transmiten se superponen sobre la portadora, lo que se conoce como modulación de la portadora por la información que se transmite. Esta operación hace que la señal de radio ocupe más de una frecuencia. Puede haber varias portadoras de radio en el mismo espacio a la vez, sin interferir entre sí, si se transmite en diferentes frecuencias de radio. Para extraer los datos, el receptor de radio selecciona una frecuencia de radio, a la vez que rechaza todo el resto de señales de radio, de otras frecuencias.

En una configuración típica (como la de la figura 2.2) un dispositivo transmisor/receptor, denominado «punto de acceso», conecta los dispositivos inalámbricos a la red de cable. Tal dispositivo recibe, almacena y transmite los datos entre la WLAN y la red cableada. Un único punto de acceso puede soportar un grupo pequeño de usuarios y funcionar en un rango de entre 100 m y 1 km, dependiendo de la tecnología concreta. El punto de acceso (o la antena conectada a él) suele estar montada en alto. Los usuarios acceden a la WLAN a través de adaptadores WLAN específicos, normalmente implementados como tarjetas del dispositivo.

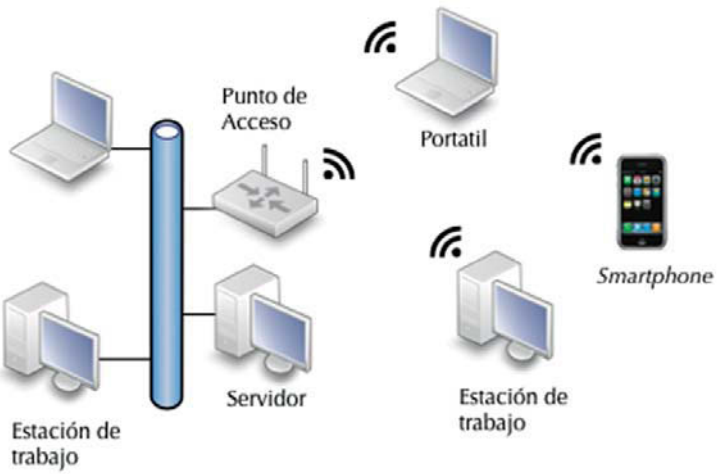

Figura 2.2. Red con dispositivos inalámbricos.

Las comunicaciones inalámbricas siguen el estándar 802.11 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Dicho estándar dispone en estos momentos de 4 versiones (a/b/g/n), cada una de las cuales deter-

mina la velocidad de transmisión, la técnica de modulación utilizada, así como la compatibilidad o no con otras versiones. En estos momentos, la velocidad de transmisión de las redes inalámbricas está entre los 11 Mbps y los 100 Mbps.

Los problemas de seguridad de las WLAN están divididos en los problemas de los dispositivos físicos y en las señales de radio transmitidas. Es evidente que, con una correcta elección del receptor de radio, se puede obtener cualquier transmisión de este tipo de tecnología. En este caso, la seguridad se apoya, especialmente, en las técnicas de acceso a los puntos de acceso, en la criptografía utilizada en emisores y receptores y en su posible configuración y uso. Como se verá en los temas sobre criptografía, una cosa es disponer de una herramienta adecuada y otra muy distinta es usarla correctamente. Baste decir, solo a modo de idea, que muchas redes WLAN han sido atacadas con éxito (esto quiere decir que se ha obtenido toda la información que fluía por ellas) porque o bien la criptografía que se podía usar no se usaba (caso muy habitual) o bien estaba configurada con un algoritmo criptográfico débil, una selección de clave pobre, un cambio de clave muy infrecuente o una combinación de todos estos factores.

3. REPETIDORES, *HUBS* Y CONMUTADORES (O *SWITCHES*)

Hay que recordar (figura 2.1) que un **repetidor** no es más que un amplificador de la señal, con dos puertos. Solo implementa funciones del nivel 1 de OSI. Se usan, simplemente, para extender la distancia máxima para la que un cable funciona correctamente. El repetidor recibe la señal en uno de sus puertos, la amplifica (si lleva «ruido» también) y la transmite por el otro puerto. Se puede pensar en romperlo, pero es difícilmente «atacable», por no tener nada realmente configurable.

Los ***hubs*** (o concentradores) son, en esencia, repetidores multipuerto que soportan cables de par trenzado en una topología de estrella. Cada nodo se comunica con el *hub*, que, a su vez, amplifica la señal y la transmite por cada uno de los puertos. Los *hubs* funcionan en el nivel eléctrico, es decir, otra vez el nivel 1 de OSI. El funcionamiento de los *hubs* los hace especialmente susceptibles a los ataques de tipo monitorización mediante «*sniffers*». Un atacante conectado a cualquiera de los puertos del *hub* reci-

birá copia de todos los paquetes que este reciba desde cualquiera de las estaciones conectadas al mismo.

Hasta hace pocos años, se disponía de **puentes** (o «***bridges***») como segmentadores de datos. No se va a hablar de ellos aquí pues, prácticamente, han desaparecido, siendo sustituidos por dispositivos, combinación de *hub* y puente, que se denominan **conmutadores (*switches*)**.

Comparados con los anteriores, los conmutadores son muy «inteligentes». Implementan (figura 2.1) hasta el nivel 2 de OSI, por lo menos, aunque hay que señalar que existen también los llamados «conmutadores de nivel 3», cuyas funcionalidades coinciden con las de los encaminadores que se verán en el siguiente epígrafe. Esto quiere decir que, en sus funciones básicas, son capaces de «aprender» las direcciones MAC de cada nodo conectado a cada uno de sus puertos, crear una tabla de direcciones y gestionar el tráfico con respecto a ella. En concreto, un mensaje que vaya a una estación concreta, viajará por el cable que una el conmutador y la citada estación, y solo por ese cable, evitando, así, los ataques de tipo monitorización con ***sniffers***, citados en el apartado anterior.

Otra técnica típica de los conmutadores, y que colabora para una mayor seguridad, es la de permitir el establecimiento de las redes de área local virtuales (o **VLANs**).

Las VLANs son grupos de ordenadores relacionados lógicamente entre sí por un número de grupo (número de VLAN) y configurados por el administrador del conmutador, gracias al *software* de configuración, residente en el sistema operativo del conmutador. Concretamente, se configuran los puertos de cada conmutador, asociándolos a una o más VLANs. Esto conduce a una mayor segmentación lógica de los equipos, a la vez que permite organizar mejor las máquinas por tareas o por departamentos.

Desafortunadamente, siempre que hay más posibilidades de configuración, hay más posibilidades de ataques. Hay que recordar del tema 1 que, si hay un sistema operativo, habrá ***bugs***, algunos de ellos harán posible atacar el conmutador y, como consecuencia, la red. ¿Cómo?

Hay 2 métodos para acceder al conmutador para administrarlo:

- A través de la consola, una conexión local y directa al conmutador.
- Remotamente, ya sea por telnet, ssh o http.

De manera general, un conmutador tiene un sistema operativo y un juego de cuentas de usuario, de las cuales una de ellas se usa como la cuenta de administración.

Si se accede al conmutador mediante la consola, únicamente hay que conocer la información de la contraseña asociada a esa cuenta. Desde el punto de vista de seguridad, hay que tener el **acceso físico al conmutador** (o, al menos, a los más importantes) suficientemente asegurado y la contraseña de acceso debe de ser distinta de la que proporcione, por defecto, el proveedor del conmutador. Tal contraseña, además, habrá que cambiarla con una cierta periodicidad y no publicarla. Todos los detalles de cómo hacerlo deberían de formar parte de la política de seguridad.

La otra forma de acceder al conmutador, suponiendo que se conoce la contraseña de la cuenta, es basándose en un protocolo de una aplicación IP. Esto tiene una consecuencia inmediata que se debe resaltar: **un conmutador** debe implementar *al menos* el nivel 2 de OSI, pero, sólo con el fin de poder gestionarlo de manera remota, de hecho **implementa todos los niveles OSI**, tiene una dirección IP y es administrable mediante IP.

Habitualmente, los conmutadores tienen, además, unas listas de direcciones IP desde las cuales está permitido acceder al conmutador, por ejemplo los conmutadores *Catalyst* de *Cisco Systems*. Tal lista, obviamente, debe estar cuidadosamente configurada con las direcciones IP de los equipos de uso habitual de los posibles administradores del conmutador, pero que lo deba estar no quiere decir que lo esté. Al no ser obligatoria tal configuración, en prácticamente todos los modelos se puede dejar la lista vacía, significando que se puede acceder desde cualquier dirección IP, con el riesgo que esto entraña.

Una vez se tiene un equipo desde el cual acceder, este se puede acceder mediante **telnet**, siempre que la dirección IP desde la cual se haga esté en la lista de direcciones permitidas. El uso de telnet tiene posibles efectos desagradables. Como se repetirá en el tema 3, telnet es una aplicación que no encripta el nombre de usuario ni la contraseña que se usa para el acceso. Como consecuencia, cualquiera con un acceso «promiscuo» y un analizador de protocolos podría obtener tal información y usarla posteriormente para conectarse, o intentarlo, al conmutador.

En los modelos más modernos, se va imponiendo la sustitución del protocolo telnet por el protocolo **ssh** (de «***s****ecure****sh****ell*»). Su uso desde el punto

de vista del administrador es idéntico al de telnet, pero todo el tráfico resulta encriptado, haciendo mucho más segura la comunicación.

Otra forma de acceso remoto para gestión a un conmutador, cada vez más empleado, es mediante **http**. Su funcionamiento es sencillo de entender: se implementa un servidor http en el conmutador, que, a su vez, da acceso a una aplicación típica web, que es la que sirve para administrar el conmutador remotamente. Basta con introducir en un navegador web la URL (*Uniform Resource Locator*) que identifica al conmutador, normalmente su dirección IP, por ejemplo,

http://dirección-IP-conmutador/

para obtener la ventana con la petición de identificación. Si uno conoce, como antes, el nombre de usuario y la contraseña, podrá acceder a la configuración del conmutador.

Este procedimiento se puede refinar, usando **https**, una variación del protocolo http, que trabaja con **SSL** (*Secure Socket Layer*), protocolo criptográfico (del que se hablará en el tema 16) que, bien configurado, permite exigir un certificado digital correspondiente al equipo desde el cual se realiza la conexión.

Además, se puede establecer que la identificación y autenticación (aspectos de seguridad de los que se hablará mucho más en otros temas del libro) no se haga en el conmutador, es decir, se puede pedir que la prueba de que uno es quien dice ser (en términos de cuenta de usuario) se realice en un sistema distinto, que trabaje con un **protocolo AAA** (***Authentication***, ***Authorization, Accounting***), como RADIUS o TACACS/+.

No hay que asustarse por la gran cantidad de términos, muchos de ellos probablemente desconocidos por el lector, que se han mencionado. Muchos de estos términos se aclaran en otras secciones del libro. Su aparición aquí es para resaltar lo importante que se ha vuelto el asegurar el correcto acceso a los conmutadores en una red, entre otras cosas porque son elementos presentes en prácticamente cualquier red que se plantee.

En un acceso permitido, o sea, siendo quien se debe ser, ¿qué pasos de seguridad hay que cumplir para acceder?

1. Hay que conocer el nombre y contraseña correctos.
2. Hay que estar usando una dirección IP correcta.

3. Como consecuencia, para SSL, hay que tener un certificado digital correcto. Como se verá en el tema 16, esto tiene muchas más connotaciones de gestión y de seguridad, pero, por ahora, se supone que se dispone de uno correcto.
4. Hay que conocer la dirección IP correcta del conmutador para abrir la sesión Web.
5. Una vez en la ventana, se teclea el nombre y la contraseña, que será contrastado contra un servidor de autenticación, usando, por ejemplo, el protocolo RADIUS.
6. Ya se está dentro. Ahora, hay que saber cómo configurarlo.

Parece difícil colarse… pero, hay que recordar: cuanto más complejo es un sistema, más difícil es asegurarlo. Revisando la anterior lista punto a punto otra vez:

1. ¿Se ha modificado periódicamente la contraseña?
2. ¿Hay una lista de direcciones IP autorizadas bien configurada, o está vacía?
3. ¿La versión de SSL no tiene «agujeros» de seguridad, como por ejemplo los descritos en http://unaaldia.hispasec.com/2013/02/multiples-vulnerabilidades-en-la.html?
4. ¿Hay una sola o varias direcciones IP en el conmutador?
5. ¿Está activo el servidor AAA?, si no, ¿se dispone de un servidor alternativo de «*backup*»?, o ¿se está preparado para tener que acceder solo en local?
6. Éste no es un punto menor. Con el auge de las herramientas gráficas, cada vez es más fácil configurar mal un conmutador, si no se conoce bien el entorno, porque nadie se lo ha enseñado. Muchos problemas de seguridad tienen su causa en el desconocimiento, no mal intencionado, que deja desconfigurado, o mal configurado, el sistema operativo del conmutador.

Y, por último, ¿se ha tenido en cuenta, en todos los puntos de seguridad, los ataques que, para tener éxito, no necesitan de un acceso al conmutador? Hay que recordar del tema 1 los ataques de denegación de servicio