

ÍNDICE

INTRODUCCIÓN	13
--------------------	----

UNIDAD DIDÁCTICA 1

CAPÍTULO 1. Descripción del problema de la seguridad en las comunicaciones y en la información. Tipos de ataques	19
--	----

1.1. Introducción	23
1.2. Las preguntas que deben hacerse para definir el problema	25
1.3. Soluciones aparentemente perfectas y soluciones razonables ..	31
1.4. Conclusiones.....	35
1.5. Evaluación	36

CAPÍTULO 2. La seguridad en los elementos físicos existentes en una red	39
---	----

2.1. Introducción	43
2.2. Los sistemas de cableado o inalámbricos	44
2.3. Repetidores, <i>hubs</i> y conmutadores (o <i>switches</i>)	47
2.4. Encaminadores	52
2.5. Los servidores y otras máquinas.....	54
2.6. Conclusiones.....	55
2.7. Evaluación	56

CAPÍTULO 3. La seguridad en los elementos <i>software</i> existentes en una red	59
---	----

3.1. Introducción	63
3.2. Los sistemas operativos de estaciones y servidores.....	65

3.3. Los protocolos y aplicaciones IP.....	68
3.4. Mejoras de seguridad con IPv6.....	73
3.5. Criterios de evaluación de seguridad.....	74
3.6. Conclusiones.....	79
3.7. Evaluación.....	80
CAPÍTULO 4. Métodos de ataque a equipos y redes.....	83
4.1. Introducción.....	87
4.2. Taxonomía de los tipos de ataques.....	88
4.3. Ataques orientados a la obtención de información sobre el objetivo.....	90
4.4. Ataques orientados a la obtención no autorizada de información confidencial, basados en la mala administración de sistemas.....	93
4.5. Ataques orientados a la obtención no autorizada de información confidencial, basados en vulnerabilidades del <i>software</i>	100
4.6. Ataques de tipo denegación de servicio (DOS).....	106
4.7. Ataques «creativos».....	110
4.8. Conclusiones.....	113
4.9. Evaluación.....	114
CAPÍTULO 5. Defensas básicas ante ataques.....	117
5.1. Introducción.....	121
5.2. Controles de acceso físico a sistemas.....	122
5.3. Controles de acceso lógico a sistemas.....	124
5.4. Otros controles simples de acceso a la información.....	132
5.5. Conclusiones.....	134
5.6. Evaluación.....	136
CAPÍTULO 6. La política de seguridad como respuesta razonable a los problemas de seguridad en las comunicaciones y en la información.....	139
6.1. Introducción.....	143
6.2. ¿Qué es una política de seguridad?.....	144
6.3. Aspectos físicos de la política de seguridad.....	150
6.4. Aspectos lógicos de la política de seguridad.....	153
6.5. Aspectos humanos y organizativos de la política de seguridad.....	157
6.6. Aspectos legales de la política de seguridad.....	159
6.7. Conclusiones.....	162
6.8. Evaluación.....	163

UNIDAD DIDÁCTICA 2

CAPÍTULO 7. Introducción: métodos no criptográficos en la implantación de la política de seguridad	167
7.1. Introducción	171
7.2. Herramientas que implementan la política de seguridad	172
7.3. Otros elementos típicos a tener en cuenta	175
7.4. Evaluación	176
CAPÍTULO 8. Los cortafuegos (<i>firewalls</i>) y sus aplicaciones como elemento básico de una política de seguridad de redes	179
8.1. Introducción	183
8.2. Los filtros de paquetes	186
8.3. Los <i>gateways</i> de aplicación o servidores <i>proxy</i>	193
8.4. ¿Qué se puede mejorar?	195
8.5. Conclusiones	198
8.6. Evaluación	199
CAPÍTULO 9. Tecnología de última generación en cortafuegos	201
9.1. Introducción	205
9.2. Caso práctico: el modelo <i>Cisco PIX Firewall</i>	209
9.3. Caso práctico: el modelo <i>Checkpoint Firewall-1</i>	219
9.4. La confusión reinante	221
9.5. Conclusiones	222
9.6. Evaluación	223
CAPÍTULO 10. Herramientas de análisis de vulnerabilidades para la auditoría de seguridad en las comunicaciones	225
10.1. Introducción	229
10.2. Caso práctico: el modelo <i>Cisco Secure Scanner</i>	232
10.3. Caso práctico: los programas de <i>Internet Security Systems</i> ...	234
10.4. Conclusiones	237
10.5. Evaluación	238
CAPÍTULO 11. Herramientas de detección de intrusiones para la monitorización de la seguridad en las comunicaciones	241
11.1. Introducción	245
11.2. Caso práctico: los sistemas <i>Cisco Secure IDS</i>	249
11.3. Caso práctico: los sistemas <i>Real Secure</i> de ISS	255
11.4. ¿Qué son los <i>Honey pots</i> ?	258
11.5. Conclusiones	260
11.6. Evaluación	261

CAPÍTULO 12. Diseño seguro de redes. Concepto de alta disponibilidad y diseños redundante	263
12.1. Introducción	267
12.2. Diseño de soluciones de alta disponibilidad	269
12.3. Los problemas de infraestructura y soluciones	271
12.4. Los problemas en el nivel 2 de OSI y soluciones.....	273
12.5. Los problemas en el nivel 3 de OSI y soluciones.....	274
12.6. Consideraciones para el resto de los niveles OSI	275
12.7. Consideraciones para el almacenamiento en red: SAN (<i>Storage Area Networks</i>).....	276
12.8. Consideraciones para los dispositivos de seguridad.....	278
12.9. Conclusiones.....	280
12.10. Evaluación.....	281

UNIDAD DIDÁCTICA 3

CAPÍTULO 13. Introducción a la criptografía como herramienta de obtención de una mayor seguridad en las comunicaciones.....	285
13.1. Introducción	289
13.2. Elementos básicos de cualquier método criptográfico	292
13.3. Distintos niveles criptográficos en el <i>software</i> de redes y sistemas.....	297
13.4. Tipos de ataques a sistemas criptográficos	300
13.5. Conclusiones.....	301
13.6. Evaluación	302
CAPÍTULO 14. Métodos criptográficos: sistemas de clave privada, sistemas de clave pública y sistemas de una sola vía (<i>one-way hash</i>)	305
14.1. Introducción	309
14.2. Algoritmos de clave privada o de criptografía simétrica	311
14.3. Funciones de una sola vía	316
14.4. Algoritmos de clave pública o de criptografía asimétrica.....	321
14.5. Conclusiones.....	329
14.6. Evaluación	332
CAPÍTULO 15. Certificación, autenticación e integridad de la información. Firma digital y PKI.....	335
15.1. Introducción	339
15.2. Autenticación, integridad y no repudio.....	340
15.3. Los sistemas de firma digital	346
15.4. La necesidad de certificación. El estándar X.509 y las autoridades de certificación	349

15.5. Los modelos de infraestructura de clave pública o PKI	353
15.6. Problemas de seguridad de las firmas digitales y de las PKI .	361
15.7. Conclusiones.....	364
15.8. Evaluación	365
CAPÍTULO 16. Protocolos criptográficos: SSL, PGP, IPSec y otros.....	367
16.1. Introducción.....	371
16.2. Los protocolos de seguridad y comercio electrónico: SSL y SET.....	373
16.3. Protocolos de <i>tunneling</i> de IP: PPTP y L2TP	382
16.4. Los protocolos IPSec	384
16.5. Los protocolos de correo electrónico seguro: PGP y S/MIME	391
16.6. Conclusiones.....	398
16.7. Evaluación	399
CAPÍTULO 17. Redes privadas virtuales	401
17.1. Introducción.....	405
17.2. Caracterización de las redes privadas virtuales	407
17.3. Ventajas e inconvenientes de las redes privadas virtuales	409
17.4. Arquitecturas de redes privadas virtuales	414
17.5. Diseño y planificación de redes privadas virtuales.....	416
17.6. Problemas de rendimiento, mantenimiento y seguridad	420
17.7. Conclusiones.....	423
17.8. Evaluación	424
CAPÍTULO 18. El comercio electrónico. Seguridad en las transacciones comerciales.....	427
18.1. Introducción.....	431
18.2. Tipos de comercio electrónico	433
18.3. Ventajas del comercio electrónico	434
18.4. La LSSICE y cómo afecta al comercio electrónico en España	435
18.5. Datos sobre el comercio electrónico en España	438
18.6. Asuntos pendientes	441
18.7. Conclusiones.....	446
18.8. Evaluación	447
Comentario bibliográfico.....	449
Índice de acrónimos.....	453
Soluciones a las preguntas de evaluación	465

2.1. INTRODUCCIÓN

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 un 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 *hardwares* 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.

Posiblemente para su estudio posterior ayudará el recordar los niveles OSI que deben implementar muchos de estos dispositivos, razón por la cual se incluye la figura 2.1, como recordatorio de cada una de las funciones que realizan. No obstante, hay que examinarlos con más detalle en los siguientes apartados.

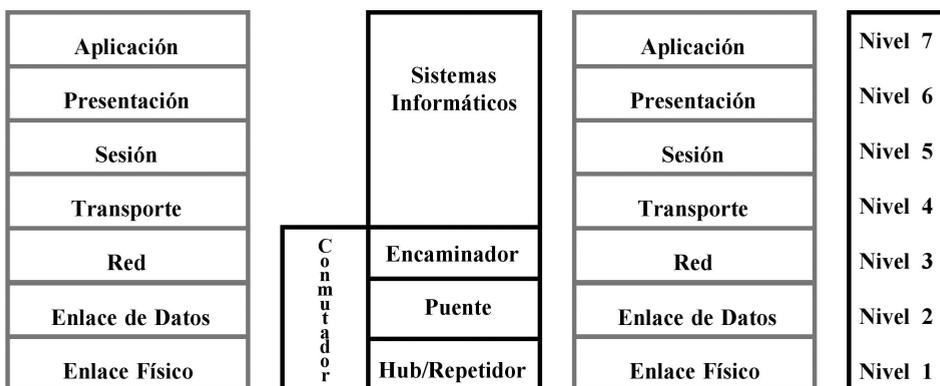


FIGURA 2.1. Niveles OSI de dispositivos en sistemas de comunicaciones.

2.2. 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 la 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 90° 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.

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 este 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, es fácil y barato hacerse con uno realmente sofisticado (diseñado para gestión, no para ataques de red) y aprovechar los conocimientos de IP de cada uno, para obtener, realmente, mucha información.

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

Finalmente, hay que dedicar un rato a hablar de lo que se denomina, hoy en día, **comunicaciones** (y redes) **inalámbricas** (del inglés «*wireless*», sin cables).

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

Las WLANS usan señales electromagnéticas (de radio o infrarrojo) 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 alrededor de 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 de PC.

El estándar más seguido hoy en día para estas comunicaciones es el grupo IEEE 802.X, en concreto el 802.11 para redes entre 1 y 2 Mbps y el 802.11 HR, a 11 Mbps.

Hasta aquí, una breve introducción (o repaso). Los problemas de seguridad están divididos, para las WLAN, en los dispositivos físicos y en las señales de radio. 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 capítulos sobre criptografía, una cosa es disponer de una herramienta estupenda 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.

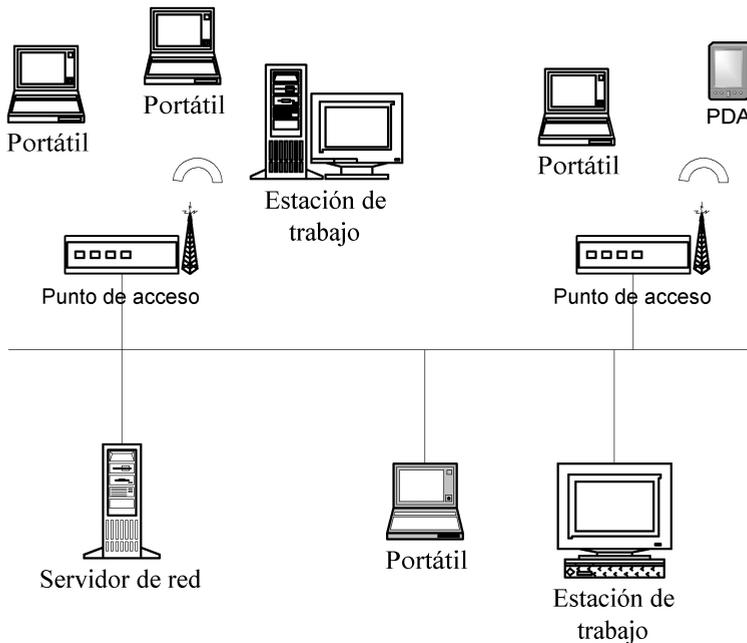


FIGURA 2.2. Red con dispositivos inalámbricos.

A modo de final de sección, se ha visto que la simple selección de cuál va a ser el medio de transmisión, en cada parte de la red, debería tenerse en cuenta en los factores a los que se ha referido previamente en este apartado.

2.3. 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