

CFGM. Seguridad Informática

Unidad 6

Seguridad activa en redes

The McGraw-Hill Companies

CONTENIDOS

- 1. Seguridad en la conexión a redes no fiables**
- 2. Protocolos seguros**
- 3. Seguridad en redes cableadas**
- 4. Seguridad en redes inalámbricas**
- 5. Seguridad WEP**
- 6. Seguridad WPA**

1. Seguridad en la conexión a redes no fiables

Ningún dispositivo, por sencillo que sea, está libre de sufrir un ataque, por lo que es muy importante minimizar las posibilidades de que esto ocurra. Existen diversas herramientas que nos permitirán proteger los equipos de la red, como los cortafuegos y los proxys, y las técnicas y herramientas que abordaremos a lo largo de esta unidad.

1.1. Spyware en tu ordenador

Un spyware es un pequeño programa que se instala en nuestro equipo con el objetivo de espiar nuestros movimientos por la red y robar nuestros datos, de modo que a través de él puede obtenerse información como nuestro correo electrónico y contraseña, la dirección IP de nuestro equipo, nuestro teléfono, páginas buscadas y visitadas, así como cuánto tiempo se pasa en ellas, u otros datos igualmente importantes como las descargas realizadas, las compras que hacemos por Internet e incluso el número de tu tarjeta. A medida que recopilan esta información la envían a empresas de publicidad de Internet para comercializar con nuestros datos.

1. Seguridad en la conexión a redes no fiables

1.1. Spyware en tu ordenador

Este tipo de software se instala sin que tengamos conocimiento de ello y trabaja en segundo plano, de modo que no nos damos cuenta de su presencia, aunque existen una serie de indicios que pueden alertarnos de que están ahí:

- Cambian las páginas de inicio o búsqueda del navegador.
- Se abren pop-ups por todos lados, incluso aunque no estemos conectados ni tengamos abierto nuestro navegador, llenando la pantalla.
- Aparecen barras de búsquedas de sitios como Hotbar, etc., que no podemos eliminar.
- Falsos mensajes de alerta en la barra de Windows (al lado del reloj) de supuestas infecciones que no podemos eliminar.
- Cuando navegamos por Internet hay veces que no se llega a mostrar la página Web que queremos abrir, ya que el tráfico de red va cada vez más lento.



2. Protocolos seguros

2.1. Protocolo HTTPS

El protocolo HTTPS es la alternativa segura al uso de HTTP. Sus siglas corresponden a Hypertext Transfer Protocol Secure, es decir, protocolo seguro de transferencia de hipertexto y se emplea para conexiones a páginas Web en las que hay que proteger los datos que se intercambian con los servidores.

Podemos verlo de manera habitual cuando accedemos a las páginas Web de tiendas en línea, servicios donde sea necesario enviar datos personales o contraseñas ó entidades bancarias, como se muestra en la Figura.



2. Protocolos seguros

2.2. Protocolo SSH

El protocolo Secure Shell (intérprete de órdenes seguro, SSH) nos permite acceder a equipos remotos a través de una red y copiar datos que residen en ellos de forma segura, utilizándose como alternativa al uso de Telnet.

Su forma de trabajar es similar a la de Telnet, pero incorpora técnicas de cifrado que protegen la información que viaja por la red, de modo que un sniffer no pueda hacerse con el usuario y la contraseña usados en la conexión, ni otros datos que se intercambian.

3. Seguridad en redes cableadas

3.1. Red privada virtual (VPN)

¿Qué es una VPN?

Una VPN o Red privada virtual es, básicamente, una red virtual que se crea dentro de otra red, habitualmente Internet.

¿Cómo funciona una VPN?

Las VPN se basan en establecer un túnel entre los dos extremos de la conexión y usar sistemas de encriptación y autenticación para asegurar la confidencialidad e integridad de los datos que se transmiten.

Instalación y configuración de una VPN

Cuando implementemos una VPN, será necesario realizar la instalación y configuración de dos partes bien diferenciadas, el servidor y el cliente.

3. Seguridad en redes cableadas

3.2. Detección de intrusos

Detectar intrusiones es una tarea muy compleja para la que se ha ido desarrollando un software específico denominado Sistema de Detección de Intrusiones, IDS.

Existen varias herramientas interesantes de detección de intrusos pero su uso es bastante complejo, algunos ejemplos más representativos son Tripwire Enterprise y Snort:

- Tripwire Enterprise, que permite detectar las acciones en la red que no se ajustan a la política de seguridad de la empresa, e informar de aquellos que necesitan especial atención.
- Snort, que es una aplicación de código abierto que permite tanto la detección de intrusión como su prevención.

3. Seguridad en redes cableadas

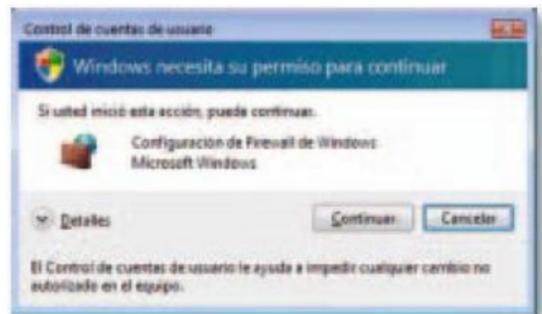
3.3. Arranque de servicios

Un servicio de un sistema operativo es una pequeña aplicación que corre en segundo plano y da soporte a este, para permitirnos tener funcionalidades como, por ejemplo, el uso del protocolo SSH, que ya conoces.

Servicios en Windows Vista

En su búsqueda por evitar que se ejecuten automáticamente servicios no deseados, Windows Vista incorpora el UAC, control de cuentas de usuario.

Con la utilidad UAC activada será necesario autorizar específicamente cada acción o cambio de configuración que realicemos, como activar el firewall de Windows.



Podemos desactivarlo desde el Panel de control > Centro de Seguridad. La opción correspondiente se localiza dentro de las Opciones de Configuración Adicional.

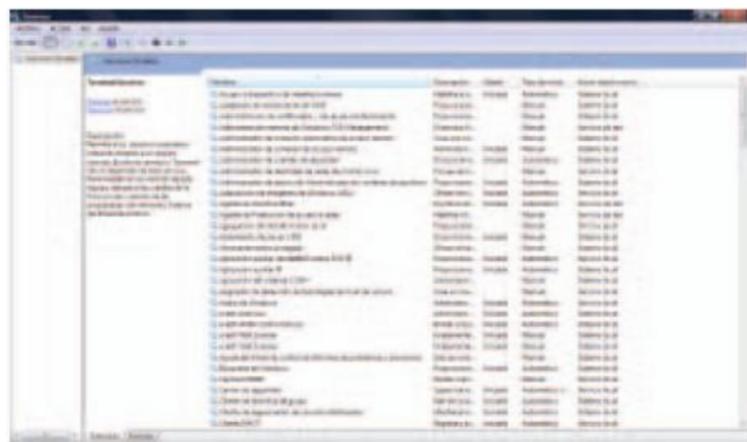
Para acceder a los servicios instalados en el sistema operativo debemos abrir, en el panel de control, las herramientas administrativas.

3. Seguridad en redes cableadas

3.3. Arranque de servicios

□ Servicios en Windows Vista

La lista de servicios de Windows Vista es mayor que la que ofrecía Windows XP y se prevé muy similar a la de Windows 7, ya que varios de ellos se han dividido para dotarnos de mayor control. Si hacemos clic con el ratón sobre el nombre del servicio vemos también una pequeña descripción del mismo.



Dentro de estos servicios encontramos algunos que pueden suponer un riesgo para la seguridad de nuestro equipo si no se inician en un entorno controlado, u otros servicios peligrosos, por lo que puede ser conveniente desactivarlos.

6 Seguridad activa en redes

3. Seguridad en redes cableadas

3.3. Arranque de servicios

□ Servicios en Ubuntu

El manejo de servicios en Linux, denominados habitualmente demonios, es parte esencial de la administración de este tipo de sistemas.

Ubuntu 9.04 ha minimizado el tiempo de arranque del sistema operativo, en parte cargando un menor número de servicios al inicio, lo que, además, facilita la administración.

Podemos acceder a los servicios instalados desde el entorno gráfico del sistema operativo, pulsando sobre Sistema y seleccionado **Administración**, donde está la opción servicios que ves en la Figura. Desde aquí podemos activar y desactivar servicios con un solo clic.

Las verdaderas posibilidades para controlar los servicios están en el uso de la línea de comandos. Los servicios instalados en el sistema se encuentran en la carpeta /etc/init.d pueden arrancarse, pararse, etc., con el uso de cuatro modificadores:

- **start**: arrancamos el servicio
- **stop**: paramos el servicio
- **restart**: reiniciamos el servicio
- **status**: nos informa del estado del servicio.



6 Seguridad activa en redes

4. Seguridad en redes inalámbricas

Las ventajas y los inconvenientes que proporcionan las redes inalámbricas son:

VENTAJAS	INCONVENIENTES
Movilidad: nos permite conectarnos desde cualquier punto (dentro del alcance de la red inalámbrica).	Menor rendimiento: el ancho de banda es mucho menor.
Escalabilidad: podemos añadir equipos fácilmente y con un coste reducido.	Seguridad: cualquiera que esté en el alcance de la red puede aprovechar una vulnerabilidad para colarse en la red o descifrar los mensajes.
Flexibilidad: permite colocar un equipo en cualquier punto (no es necesaria una toma de red).	Interferencias: la red es mucho más sensible a interferencias.

Existen varios tipos de conexiones inalámbricas: Bluetooth, Wifi (puedes ver una adaptador Wifi en la primera Figura), 3G (puedes ver un adaptador 3G en la segunda figura).



6 Seguridad activa en redes

4. Seguridad en redes inalámbricas

4.1. Tecnologías Wifi

El estándar IEEE 802.11 define los dos primeros niveles de la capa OSI para las redes de área local inalámbricas (WLAN). Los protocolos estándar que permiten la comunicación inalámbrica son:

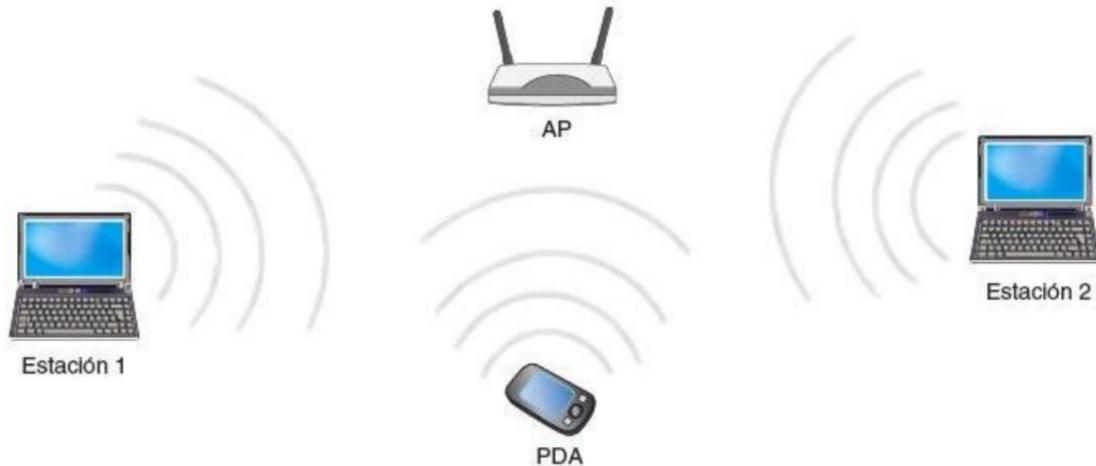
Protocolo	Frecuencia	Alcance aproximado	Velocidad	Otros
802.11a	5GHz	50 metros	54 Mbit/s	Sufre menos interferencias porque no es la banda de los teléfonos móviles y otros electrodomésticos, sin embargo es mucho más sensible a los obstáculos.
802.11b	2,4GHz	100 metros	11Mbit/s	La frecuencia de 2,4 es menos sensible a los obstáculos, pero en esta frecuencia trabajan muchos electrodomésticos que provocan interferencias.
802.11g	2,4GHz	100 metros	54Mbit/s	Las interferencias sufridas son las mismas que en 802.11b
802.11 n	2,4GHz y 5GHz	100 metros	600 Mbps	Aunque el estándar se publicó de forma definitiva en Septiembre de 2009, ya existían anteriormente dispositivos que cumplían un borrador del estándar llamado 802.11 draft n. Los dispositivos de este tipo son compatibles con todos los protocolos anteriores

6 Seguridad activa en redes

4. Seguridad en redes inalámbricas

4.2. Conceptos de redes Wifi

Aunque como ya estudiaste en el módulo Redes Locales también existe la topología ad-hoc, lo más habitual es la topología infraestructura en la que existe un punto de acceso que es el encargado de gestionar el proceso de comunicación entre todas las estaciones Wifi.



En primer lugar para que un cliente pueda comunicarse con la red tiene que estar asociado al punto de acceso y para poderse asociar tiene que pasar un proceso de autenticación. Una vez pasado este proceso, la estación quedará asociada al punto de acceso y podrá comunicarse con este y a través de él con otros equipos.

6 Seguridad activa en redes

4. Seguridad en redes inalámbricas

4.3. Seguridad Wifi

Lo que habitualmente queremos es controlar quien se conecta a nuestra red. Para ello podemos aplicar varias medidas de seguridad, que se pueden agrupar según el nivel en el que aplican:

Nivel físico: En este nivel podemos intentar controlar la señal producida por los puntos de acceso y las interferencias recibidas. A través de la utilización de diferentes antenas podemos intentar conseguir que la señal salga lo menos posible de los límites deseados.

Nivel de enlace: En el nivel de enlace hay mucha variedad de medidas que podemos tomar para conseguir este objetivo:

- Controlar el acceso a través de una contraseña común para todos los clientes.
- Controlar el acceso a través de una característica del cliente, como por ejemplo la dirección MAC o un nombre de usuario y contraseña.

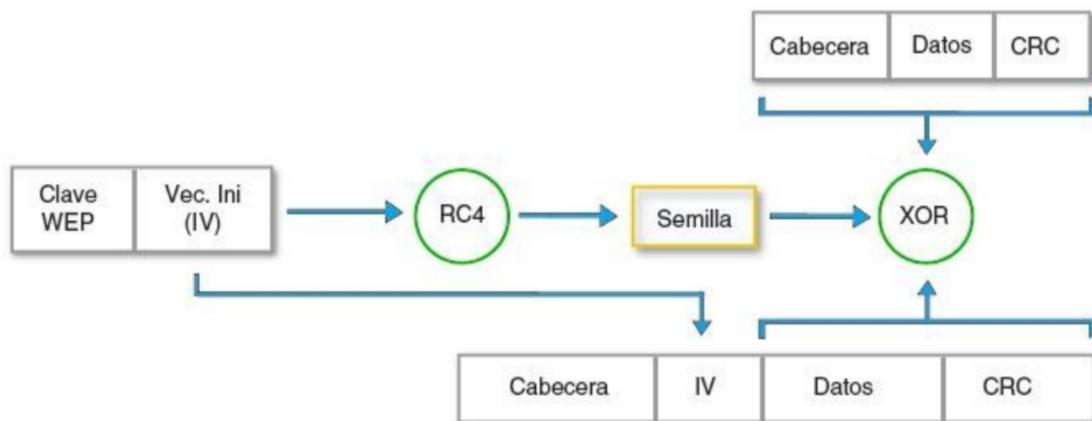
6 Seguridad activa en redes

5. Seguridad WEP

WEP (Wired Equivalent Privacy) es el sistema de cifrado estándar que se utilizó inicialmente para el cifrado del protocolo 802.11. Intenta dar a las redes inalámbricas la seguridad que se tiene en las redes cableadas.

WEP utiliza un algoritmo llamado RC4 para a partir de la clave WEP y de un vector de inicialización de 24 bits (también llamado IV), generar una secuencia aleatoria, llamada semilla, la cual utilizará para cifrar la comunicación con el punto de acceso. Puedes ver un esquema del algoritmo en la Figura.

El resultado es una trama en la que la cabecera y el vector de inicialización van sin cifrar y tanto los datos como el CRC van cifrados.



5. Seguridad WEP

Existen dos métodos a través de los cuales un usuario puede autenticarse con un punto de acceso WEP:

- **Abierta (open):** La estación puede autenticarse sin necesidad de utilizar la clave WEP, simplemente con solicitar la asociación, el punto de acceso dará por asociada a la estación. Después de este proceso de autenticación la estación solo podrá comunicarse con el punto de acceso si conoce la clave WEP utilizada para encriptar la comunicación.
- **Clave compartida (shared key):** Cuando una estación envía una solicitud de asociación al punto de acceso, este envía un texto sin cifrar a la estación, llamado «desafío». El punto de acceso solo asociará a las estaciones que devuelvan correctamente cifrado con la clave WEP dicho texto.

Aunque pueda parecer más seguro shared key, no lo es, porque cualquier estación inalámbrica podría atrapar tanto el paquete de desafío como el mismo paquete cifrado y con esta información asociarse correctamente con el punto de acceso y iniciar un ataque a nuestro punto de acceso. Se recomienda el método de autenticación abierto.

6 Seguridad activa en redes

6. Seguridad WPA

Los estándares WPA y WPA2 se centran en asegurar el proceso de autenticación y el cifrado de las comunicaciones. En ambos estándares se proponen dos soluciones para la autenticación, una empresarial y otra para pequeñas empresas y hogares:

- **WPA Empresarial:** Requiere de la utilización de un servidor RADIUS independiente para gestionar la autenticación de los usuarios a través de un nombre de usuario y contraseña.
- **WPA Personal:** Utiliza un método de autenticación que requiere compartir una clave entre todas las estaciones de la red. Es más apropiado para pequeñas empresas y hogares porque no requiere de la utilización de un servidor RADIUS.

6.1. Seguridad WPA personal

Existen dos tipos de encriptación en WPA:

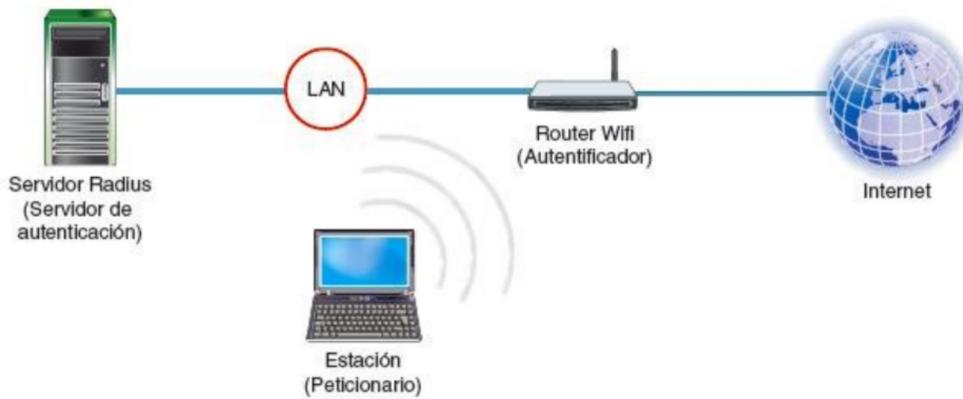
- **TKIP (Protocolo de integridad de clave temporal):** Es un protocolo que partiendo de una clave (que no es la precompartida) compartida entre el punto de acceso y todas las estaciones, genera nuevas claves diferentes por cada cliente y renovables cada cierto tiempo. Para ello mezcla la clave original con la dirección MAC y con un vector de inicialización. De esta forma cada estación utiliza una clave independiente para encriptar la comunicación.
- **AES (cifrado avanzada estándar):** Es un algoritmo más robusto y complejo que TKIP. Es preferible utilizar AES que TKIP, por ser este mas avanzado y seguro. Como inconveniente requiere hardware más potente.

6 Seguridad activa en redes

6. Seguridad WPA

6.2. Seguridad WPA empresarial

La estructura necesaria para poder utilizar la arquitectura WPA empresarial es la que se muestra en la Figura.



Utilizando la seguridad WPA empresarial se aumenta la seguridad y la flexibilidad, ya que podemos modificar la contraseña de un usuario o cancelarlo sin que esto afecte al resto. Esto supone una notable mejora con respecto a WPA-PSK en redes con muchos usuarios.

6 Seguridad activa en redes

7. Recomendaciones de seguridad en WLAN

1. Asegurar la administración del punto de acceso (AP), punto de control de las comunicaciones de todos los usuarios, crítico en la red, cambiando la contraseña por defecto.
2. Actualizar el firmware disponible para mejorar sus prestaciones de seguridad
3. Aumentar la seguridad de los datos transmitidos: encriptación WEP o WPA/WPA2 o servidor Radius, y cambiando las claves regularmente
4. Realizar una administración y monitorización minuciosa, lo que implica una administración más compleja pero más segura:
 - Cambiar el SSID por defecto y desactivar el broadcasting de SSID. Los clientes deberán conocer el nombre del SSID
 - Desactivar el servidor DHCP, y asignar manualmente las IP en clientes
 - Cambiar las direcciones IP del punto de acceso y el rango de la red por defecto
 - Filtrado de conexiones permitidas mediante direcciones MAC
 - Número máximo de dispositivos que pueden conectarse
 - Analizar periódicamente los usuarios conectados verificando si son autorizados o no
5. Desconexión del AP cuando no se use

Créditos

Autores del libro del alumno

César Seoane Ruano, Ana Belén Saiz Herrero,

Emilio Fernández Álvarez, Laura Fernández Aranda

Edición

Estudio177.com, Laura García Olaya