Unidad IV

Técnicas y herramientas para protección y monitoreo de servidores

4.1. Protocolo SNMP.

El **Protocolo Simple de Administración de Red** o **SNMP** (del inglés ***Simple Network Management Protocol***) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2).

SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria.

4.2. Corta fuegos físicos y lógicos.

Los *firewalls* o cortafuegos son una de las herramientas básicas de la seguridad informática. Permiten controlar las conexiones de red que acepta o emite un dispositivo, ya sean conexiones a través de Internet o de otro sistema.
Existen infinidad de variantes de cortafuegos (dedicados, de tipo *appliance*, gestionados, etc.). Este artículo se centrará exclusivamente en los cortafuegos personales (también conocidos como firewalls) y cómo sacarles el mayor provecho.
Los cortafuegos personales son habitualmente programas que, o bien están integrados en el sistema operativo, o bien son aplicaciones de terceros que pueden ser instaladas en ellos.

4.3. Sniffers.

En informática, un **analizador de paquetes** es un programa de captura de las tramas de una red de computadoras.

Es algo común que, por topología de red y necesidad material, el medio de transmisión (cable coaxial, cable de par trenzado, fibra óptica, etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguir

esto el analizador pone la tarjeta de red en un estado conocido como "modo promiscuo" en el cual en la capa de enlace de datos no son descartadas las tramas no destinadas a la dirección MAC de la tarjeta; de esta manera se puede capturar (*sniff*, "olfatear") todo el tráfico que viaja por la red.

Los analizadores de paquetes tienen diversos usos, como monitorear redes para detectar y analizar fallos, o para realizar ingeniería inversa en protocolos de red. También es habitual su uso para fines maliciosos, como robar contraseñas, interceptar correos electrónicos, espiar conversaciones de chat, etc.

4.4. Correo no deseado.

Debe saber que una vez que los alumnos son dados de alta en la plataforma, se envía automáticamente un correo electrónico en el que se incluyen los datos necesarios para acceder a esta. Cuando recibimos una devolución de un correo electrónico nos ponemos en contacto con la persona en cuestión a través de teléfono o de email para informarle de ello. Si el correo no nos es devuelto, debe entenderse que ha sido entregado correctamente, por lo que podemos saber si usted no ha leído nuestro mensaje. En cualquier caso, NO es tan frecuente que un correo electrónico se pierda, ya que, el protocolo que utiliza este tipo de servicio web es bastante seguro.

Debido a la gran cantidad de correos de publicidad que se reciben diariamente en estos servidores, algunos servidores de correo electrónico como Hotmail, Gmail o Yahoo cuentan con un servicio anti-spam (anti correo no deseado) que en ocasiones NO funciona correctamente. Se trata de un herramienta que se activa automáticamente por lo que debería controlarla para evitar perder correos que sean de su interés. De hecho, los mensajes que sean derivados a esa carpeta se eliminarán automáticamente a los pocos días de su recepción.

A continuación le mostramos cómo acceder a esa carpeta y cómo recuperar los mensajes que hayan sido erróneamente detectados como spam.

4.5. Comprobación de integridad de archivos y directorios.

En los sistemas de archivos tradicionales, el método de escritura de datos es intrínsecamente vulnerable a errores imprevistos que generan incoherencias en el sistema. Debido a que un sistema de archivos tradicional no es transaccional, puede haber bloques sin referenciar, recuentos de vínculos erróneos u otras estructuras de sistema de archivos no coherentes. La adición de diarios soluciona

algunos de estos problemas, pero puede presentar otros problemas si el registro no se puede invertir. La existencia de datos incoherentes en el disco de una configuración ZFS sólo puede ser debida a un error de hardware·(en cuyo caso, la agrupación debería haber sido redundante) o porque hay un error en el software de ZFS.

La utilidad fsck soluciona problemas conocidos específicos de sistemas de archivos UFS. Casi todos los problemas de agrupación de almacenamiento ZFS suelen estar relacionados con errores de hardware o fallos de alimentación. Muchos se pueden evitar utilizando agrupaciones redundantes. Si una agrupación se ha dañado por un error de hardware o un fallo de alimentación.

Si la agrupación no es redundante, siempre existe el riesgo de que los daños en el sistema de archivos lleguen a hacer que parte o todos los datos queden inaccesibles.

4.6. Analizadores de puertos.

Un "**analizador de red**" (también llamado *rastreador de puertos*) es un dispositivo que permite "supervisar" el tráfico de red, es decir, capturar la información que circula por la red.

En una red no conmutada, los datos se envían a todos los equipos de la red. Pero en uso normal, los equipos ignoran los paquetes que se les envían. Así, al usar la interfaz de red en un modo específico (en general llamado *modo promiscuo*), es posible supervisar todo el tráfico que pasa a través de una tarjeta de red (una tarjeta de red Ethernet, una tarjeta de red inalámbrica, etc.).

4.7. Monitoreo de red.

El término **Monitoreo de red** describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a losadministradores de redes mediante correo electrónico, pager u otras alarmas. Es un subconjunto de funciones de la administración de redes.

4.8. Herramientas de auditoría de red:

4.8.1. Pruebas de penetración,

La prueba de penetración permite conocer el impacto real de un ataque informático. Durante la prueba de penetración se intentan explotar las vulnerabilidades descubiertas con el objetivo de demostrar el impacto que podría tener en la organización.

A diferencia de la auditoría de vulnerabilidades, la prueba depenetración se enfoca en que tanto impacto puede tener un ataque en la organización y no en que activos podrían ser vulnerables. No se reporta un listado de activos vulnerables y sus vulnerabilidades, se reporta un listado de las actividades más peligrosas para el negocio que podría realizar un atacante real.

Websec lleva a cabo todas sus pruebas de penetración manualmente. Nuestros expertos en seguridad las hacen a mano para garantizar que se realicen de forma segura y eficaz. En Websec utilizamos técnicas de Black Box, White Box y Grey Box (nivel de información proporcionada por el cliente), para asegurar el resultado preciso del análisis.

4.8.2. Hackeo ético.

La **ética hacker** es una nueva ética surgida de y aplicada a las comunidades virtuales o cibercomunidades, aunque no exclusivamente.

La expresión se suele atribuir al periodista Steven Levy en su ensayo seminal *Hackers: Heroes of the Computer Revolution*, publicado en 1984, dónde describe y enuncia con detalle losprincipios morales que surgieron a finales de los años cincuenta en el Laboratorio de Inteligencia Artificial del MIT y, en general, en la cultura de los aficionados a la informática de los años sesenta y setenta. Aquellos principios --que se resumen en el acceso libre a la información y en que la informática puede mejorar la calidad de vida de las personas-- han constituido la base de la mayor parte de definiciones que se han elaborado posteriormente. Uno de sus mentores actuales ha sido el finlandés Pekka Himanen.