Tareas de seguridad

Debido a la interconexión cada vez más grande de las redes privadas y públicas, la seguridad se ha convertido en una preocupación mayor de los administradores del sistema. Existen diferentes herramientas que permiten seguir y diagnosticar las alertas de seguridad.

1. Comandos de prueba y de vigilancia

Existen diferentes comandos que permiten efectuar pruebas de accesibilidad en los servidores de red, para encontrar posibles fallos de seguridad.

Estos comandos están detallados en el capítulo Configuración de red de este libro.

a. El comando nc

El comando `ncat` o `nc` (*netcat*) es una herramienta multiusos, que permite establecer comunicaciones a través de sockets, locales o en red, en TCP y en UDP, en IPv4 o IPv6, como cliente o servidor, especificando un puerto de escucha.

Con todas sus opciones, este comando permite comprobar los diferentes tipos de comunicación, en particular a través de la red.

El comando `nc` reemplaza al comando tradicional `telnet`. Este ya no se encuentra generalmente en las distribuciones recientes, para disuadir de su uso en relación con un servidor `telnet`, lo que provoca un problema de seguridad (contraseña del usuario transmitida sin cifrar por la red).

b. El comando nmap

El comando `nmap` (*Network Mapper*), que se encuentra en el paquete `nmap`, es una herramienta potente de exploración de una red y de auditoría de seguridad. Permite determinar las máquinas activas en la red y los servicios de red disponibles en esas máquinas.

El comando puede ofrecer en particular una tabla de los puertos de cada máquina de destino, con su estado (abierto, cerrado o filtrado por un firewall). Este comando puede opcionalmente buscar y mostrar información más detallada: sistema operativo y aplicación a la escucha en cada puerto, incluyendo los números de la versión.

El uso de este comando tiene que hacerse con prudencia y respetando las obligaciones legales, porque comprobar los puertos abiertos de una máquina, sin autorización, se puede considerar como una tentativa de intrusión y ser objeto de procedimientos penales.

2. Los sistemas IDS (Intrusion Detection System)

Los firewalls filtran generalmente los paquetes en función de sus direcciones IP y/o de los números de puertos utilizados. Esta protección se puede esquivar con aplicaciones malintencionadas, que usan puertos bien conocidos abiertos (como el puerto TCP 80 para HTTP) para sus propias conexiones.

Para asegurar un control más elaborado, hacen falta aplicaciones especializadas, capaces de analizar el tráfico a nivel de aplicación para detectar una actividad sospechosa. Estos programas se llaman sistemas de detección de intrusión o IDS (*Intrusion Detection System*).

a. Técnicas de análisis

Para identificar los tráficos malintencionados, los IDS disponen de tres técnicas:

- Detección de anomalías: se basa en la detección de eventos anormales, síntomas de actividades sospechosas. Por ejemplo, un gran volumen de mensajes ICMP puede indicar que hay sistemas que son víctimas o están en el origen (involuntario) de un ataque por denegación de servicio.
- El análisis del protocolo: busca el tráfico que utiliza un protocolo incorrecto o desviado de su uso habitual.
- El análisis de firmas de ataques: permite identificar ataques o actividades malintencionadas referenciadas. Es la técnica más eficaz y menos susceptible de producir falsos positivos, porque gestiona ataques o intrusiones conocidas.

b. Fuentes de información

Numerosos organismos, asociaciones y empresas mantienen sitios en Internet dedicados a las amenazas de seguridad y emiten alertas en cuanto un nuevo ataque aparece. Es importante conocerlos y asegurar una vigilancia tecnológica permanente sobre todo lo concerniente a la seguridad.

Entre estos organismos, podemos señalar:

`Bugtraq`	Lista de difusión dedicada a las vulnerabilidades, su explotación y su corrección.
`CERT`	*Computer Emergency Response Team*. Este organismo estudia las vulnerabilidades, efectúa investigaciones para reforzar la seguridad de red y propone servicios vinculados a la seguridad.
`CIAC`	*Computer Incident Advisory Capability*. Organismo de vigilancia y de investigación de seguridad, gestionado por el *U.S. Department Of Energy*.

3. Fail2Ban

Fail2Ban es un programa de vigilancia y de bloqueo de intrusiones Su principio es analizar

los archivos del registro del sistema y de diferentes servicios de red (SSH, FTP, HTTP, SMTP, etc.), para buscar eventos que correspondan a las tentativas de intrusión. De esta manera puede determinar el origen de esos ataques y modificar temporalmente las reglas del firewall para prohibir esas direcciones.

Su archivo de configuración principal, `/etc/fail2ban/jail.conf`, contiene la configuración para vigilar muchos servicios, se actualiza automáticamente.

El nombre del archivo (carcel, en español) evoca la prohibición de las direcciones IP sospechosas, con una duración más o menos larga.

4. Snort

Snort es el más conocido de los IDS open source. Vigila el tráfico de red basándose en un motor de análisis y un conjunto de reglas.

a. Los componentes

El programa Snort está compuesto por un daemon y por archivos de configuración generalmente localizados en `/etc/snort`. El archivo de configuración principal es `snort.conf`. Las reglas aplicadas están situadas en los archivos del subdirectorio `rules`.

El comando `oinkmaster` asegura la actualización de las reglas, según el archivo de configuración `/etc/oinkmaster.conf`.

b. Gestión de las fuentes de información

Los archivos de reglas de Snort tienen que descargarse desde la página web del editor.

Los archivos están declarados en el archivo de configuración `oinkmaster.conf`, según el formato siguiente:

```
url = http://www.snort.org/snort-rules/archivo_reglas
```

Donde `archivo_reglas` especifica un archivo de reglas con formato `tar.gz`.

La descarga para la actualización de las reglas tiene que ser programada a intervalos regulares, usando para ello el servicio `cron` por ejemplo, planificando el comando `oinkmaster`.

Sintaxis

```
oinkmaster -o DirReglas
```

`DirReglas` es el directorio que contiene los archivos de reglas funcionamiento, por defecto, `/etc/snort/rules`.

Los archivos de reglas tienen que estar configurados en el archivo `snort.conf` con el parámetro `include`, esto es el caso para los archivos por defecto del editor.

c. Gestión de las alertas

Cuando Snort detecta un tráfico sospechoso, registra un evento en el archivo de registros a través del daemon de registro de eventos (`rsyslogd` o `syslogd`) local o remoto, y almacena una copia del paquete en un archivo con formato `libpcap` usado por `tcpdump` (se puede analizar con diferentes herramientas, como Wireshark).

También puede estar configurado para almacenar información en una base de datos (Oracle, MySQL, PostGreSQL…).

Ejemplo

Configuración para el uso de un daemon de registro de eventos remoto.

```
output alert_syslog: host=192.168.0.60, LOG_ALERT
```

5. OpenVAS

OpenVAS (*Open Vulnerability Assessment Scanner*) es una version open source del escáner de vulnerabilidades Nessus. El programa es una suite de software que propone un servidor y clientes.

a. El servidor OpenVAS

El servidor OpenVAS escanea y analiza los hosts de redes en busca de vulnerabilidades conocidas, usando para ello NVT (*Network Vulnerability Tests*).

b. Los clientes OpenVAS

Los clientes OpenVAS son módulos de software que funcionan en línea de comandos o con una interfaz gráfica. Permiten efectuar análisis de seguridad a los hosts de la red y transmitir los resultados al servidor.

c. Base de datos de vulnerabilidades

OpenVAS mantiene actualizada una fuente pública de vulnerabilidades, OpenVAS NVT Feed. Esta permite que los servidores estén informados de las últimas vulnerabilidades conocidas. Hay más de 50 000 NVT.