Validación de los conocimientos adquiridos: preguntas/respuestas

1. Preguntas

Si cree que sus conocimientos sobre este capítulo son suficientes, conteste a las preguntas siguientes:

Seguridad local

1. ¿Cuáles son los tres principales objetivos de la seguridad informática?

2. ¿Por qué es importante controlar los derechos SUID y SGID de sus binarios?

3. Dé el comando que permite buscar y visualizar la información detallada relativa a los archivos ordinarios en /usr cuyo propietario es root y que dispone del privilegio SUID.

4. Un archivo del paquete rpm bash le resulta raro. El resultado de la verificación RPM indica `.M.....T /bin/bash.` ¿Qué ha ocurrido?

5. ¿Es pertinente forzar a los usuarios a cambiar de contraseña cada semana, sabiendo que la contraseña debe responder a unas reglas estrictas?

6. ¿Cómo comprobar la información de contraseña de cualquier usuario?

   - A - `chage -l user`
   - B - `passwd -l user`
   - C - `grep ^user /etc/shadow`

- D - `passwd -S user`

7 ¿Cuál es el inconveniente principal del funcionamiento por defecto de pwgen para los españoles?

8 Genere seis contraseñas aleatorias de una longitudad de 8 caracteres.

9 El usuario ftponly no debe poder conectarse de manera interactiva. Por lo tanto, ¿qué comando puede teclear para modificar su shell de conexión?

10 ¿Cómo bloquear toda conexión interactiva nueva?

- A - pasando en init 1.
- B - modificando todos los shells en /bin/false.
- C - bloqueando todos los terminales dentro de /etc/securetty.
- D - creando el archivo /etc/nologin.

11 Un "scan" rápido por John The Ripper muestra que éste ha pasado hace apenas unos segundos en determinados logins. ¿Por qué?

12 ¿Cuál es el objetivo de un rootkit?

13 ¿Por qué debería contemplarse la instalación de un antivirus en un servidor que dispone de particiones de archivos?

14 ¿Qué línea de comandos tiene que teclear para actualizar la base de datos de las firmas de virus clamav?

15 ¿Sabía que la simple línea ":(){ :|:& };:" en bash puede provocar la parada de su máquina? Es una «fork bomb»: crea miles de procesos y termina por saturar la máquina. ¿Cómo puede impedir que sus usuarios creen demasiados procesos?

16 ¿Cómo conservar (en el boot) las configuraciones de ulimit?

- A - creando un script lanzado por init.
- B - modificando /etc/security/limits.conf.
- C - modificando el archivo /etc/profile con una serie de ulimit.
- D - modificando el archivo ~/.bashrc de los usuarios y en /etc/skel.

17 Un boletín de seguridad del CERT le informa de un fallo de seguridad de un producto instalado en su puesto. ¿Qué tiene que hacer?

Seguridad de la red

18 ¿Cómo aislar los puertos abiertos y las conexiones activas en su máquina?

19 ¿Para qué sirve el comando **nmap**?

- A - Facilitar una tarjeta de la red.
- B - Probar los puertos remotos de una máquina de la red.
- C - Obtener información de seguridad en una máquina de la red.
- D - Conocer el sistema operativo de una máquina remota.

20 ¿Cómo se puede emplear de manera malintencionada la información devuelta por nmap?

21 El servicio smbd parece ejecutarse en su máquina y, sin embargo, no tiene particiones de Windows. ¿Qué tendría que hacer?

22 ¿Cómo saber si un servicio integra los TCP Wrappers?

23 ¿Cuál es la ruta a los dos archivos de configuración de los TCP Wrappers?

24 Prohíba la conexión al servicio sshd a todo el mundo salvo a la subred 10.17.32.0/22.

25 Si no pudiera contar con NetFilter, ¿cómo prohibiría todo intento de conexión a su máquina?

26 ¿Cómo suprimir todas las reglas de una sola vez?

27 Prohíba toda conexión de la subred 10.17.32.0/22 en su máquina, salvo 10.17.32.5.

28 ¿Cómo impedir cualquier conexión TCP saliente con destino a un servicio ssh (puerto 22)?

29 Su PC dispone de dos tarjetas de red. ¿Cómo prohibir cualquier entrada o salida en la segunda?

30 Su PC, que dispone de dos tarjetas de red, sirve de enrutador. Quiere impedir el encaminamiento del puerto TCP 22. ¿Cómo hacerlo?

2. Resultados

Diríjase a las páginas siguientes para comprobar sus respuestas. Por cada respuesta correcta, sume un punto.

Número de puntos /30

Para este capítulo, su resultado mínimo debe ser de 22 respuestas acertadas (22/30).

Localice los puntos clave que le dieron problemas y repase el capítulo antes de pasar al siguiente:

- ✓ Seguridad local.
- ✓ Seguridad de la red.

3. Respuestas

Seguridad local

1 ¿Cuáles son los tres principales objetivos de la seguridad informática?

La seguridad de conexión, la integridad de los datos y la confidencialidad de los datos.

2 ¿Por qué es importante controlar los derechos SUID y SGID de sus binarios?

Un comando con los derechos SUID asigna los derechos de su propietario al que lo utiliza. Si el comando es un shell o cualquier otro comando peligroso como cat, las consecuencias pueden ser desastrosas.

3 Dé el comando que permite buscar y visualizar la información detallada relativa a los archivos ordinarios en /usr cuyo propietario es root y que dispone del privilegio SUID.

```
find /usr -user root -type f -perm -4000 -ls
```

4 Un archivo del paquete rpm bash le resulta raro. El resultado de la verificación RPM indica `.M.....T /bin /bash.` ¿Qué ha ocurrido?

M indica que se han modificado los permisos del archivo, y T que, la fecha de modificación también. Compruebe los permisos de /bin/bash y, si es necesario, vuelva a colocarlos correctamente (755).

5 ¿Es pertinente forzar a los usuarios a cambiar de contraseña cada semana, sabiendo que la contraseña debe responder a unas reglas estrictas?

No, o más bien, no necesariamente. Si cambia demasiado a menudo, los usuarios la olvidarán o la apuntarán. Obtendrá el efecto inverso de lo que desea.

6 ¿Cómo comprobar la información de contraseña de cualquier usuario?

- A - `chage -l user`
- B - `passwd -l user`
- C - `grep ^user /etc/shadow`
- D - `passwd -S user`

A y D. El resultado de A es más legible.

7 ¿Cuál es el inconveniente principal del funcionamiento por defecto de pwgen para los españoles?

Da los resultados en inglés, menos comprensibles para nosotros.

8 Genere seis contraseñas aleatorias de una longitudad de 8 caracteres.

```
pwgen -s 8 6
```

9 El usuario ftponly no debe poder conectarse de manera interactiva. Por lo tanto, ¿qué comando puede teclear para modificar su shell de conexión?

```
usermod -s /bin/false ftponly
```

10 ¿Cómo bloquear toda conexión interactiva nueva?

- A - pasando en init 1.
- B - modificando todos los shells en /bin/false.
- C - bloqueando todos los terminales dentro de /etc/securetty.
- D - creando el archivo /etc/nologin.

D. El módulo pam_nologin prohibirá cualquier conexión nueva.

11 Un "scan" rápido por John The Ripper muestra que éste ha pasado hace apenas unos segundos en de terminados logins. ¿Por qué?

La contraseña es obvia, es probable que esté relacionada con el nombre del propio login o con una variante. Fuerze a estos usuarios a cambiar su contraseña.

12 ¿Cuál es el objetivo de un rootkit?

El objetivo de un pirata es obtener el mayor número de privilegios posibles en una máquina e instalar en ella ransomwares, criptomineros, bots... Se instala un rootkit en local gracias a cualquier fallo (humano o de software) del sistema con el objetivo de abrir una puerta secreta mucho más accesible.

13 ¿Por qué debería contemplarse la instalación de un antivirus en un servidor que dispone de particiones de archivos?

Porque algunos archivos que contengan virus pueden circular a sus espaldas en las diversas particiones, sobre todo si sus usuarios están con Windows. Los virus específicos de Linux son muy raros.

14 ¿Qué línea de comandos tiene que teclear para actualizar la base de datos de las firmas de virus clamav?

Teclee `freshclam` *simplemente.*

15 ¿Sabía que la simple línea ":(){ :|:& };:" en bash puede provocar la parada de su máquina? Es una «fork bomb»: crea miles de procesos y termina por saturar la máquina. ¿Cómo puede impedir que sus usuarios creen demasiados procesos?

ulimit permite modificar el número de proceso por usuario con el parámetro -u; `ulimit -u 1024` *coloca el límite a 1024 procesos por usuario.*

16 ¿Cómo conservar (en el boot) las configuraciones de ulimit?

- A - creando un script iniciado por init.
- B - modificando /etc/security/limits.conf.
- C - modificando el archivo /etc/profile con una serie de ulimit.

- D - modificando el archivo ~/.bashrc de los usuarios y en /etc/skel.

B. Son los módulos PAM los que se encargarán de modificar el entorno del usuario a su conexión.

17 Un boletín de seguridad del CERT le informa de un fallo de seguridad de un producto instalado en su puesto. ¿Qué tiene que hacer?

Compruebe en el sitio de su distribución si la alerta le corresponde. Si es así, y según el nivel de criticidad y las reglas de su empresa, actualice su distribución.

Seguridad de la red

18 ¿Cómo aislar los puertos abiertos y las conexiones activas en su máquina?

Con el comando netstat ya tratado: `netstat -a -A inet`

19 ¿Para qué sirve el comando **nmap**?

- A - Facilitar una tarjeta de la red.
- B - Probar los puertos remotos de una máquina de la red.
- C - Obtener información de seguridad en una máquina de la red.

D - Conocer el sistema operativo de una máquina remota.

B, C y D. nmap es una verdadera navaja suiza de la seguridad de red.

20

¿Cómo se puede emplear de manera malintencionada la información devuelta por nmap?

Además de la presencia de numerosos puertos abiertos, nmap intenta detectar el nombre del servicio asociado y su versión. De ahí, a través de los boletines de seguridad, se puede intentar encontrar y luego aprovechar un fallo. Si un servicio no está encriptado, por ejemplo telnet, es más sencillo: basta con colocar un «sniffer» (wireshark, por ejemplo) para visualizar el tráfico de forma transparente.

21

El servicio smbd parece ejecutarse en su máquina y, sin embargo, no tiene particiones de Windows. ¿Qué tendría que hacer?

Suprima este servicio al arrancar y párelo. De manera general, suprima todos los servicios inútiles y reactívelos en caso de necesidad.

22

¿Cómo saber si un servicio integra los TCP Wrappers?

Se compila la librearía de manera estática dentro del binario. Mire la cadena «host_access» en el programa con el comando strings.

23 ¿Cuál es la ruta a los dos archivos de configuración de los TCP Wrappers?

/etc/hosts.allow y /etc/hosts.deny.

24 Prohíba la conexión al servicio sshd a todo el mundo salvo a la subred 10.17.32.0/22.

En /etc/hosts.deny escriba sshd `:ALL`*. En /etc/hosts.allow escriba* `sshd :10.17.32.0/255.255.252.0`*.*

25 Si no pudiera contar con NetFilter, ¿cómo prohibiría todo intento de conexión a su máquina?

Modifique la regla por defecto en entrada: `iptables -P INPUT DROP`

26 ¿Cómo suprimir todas las reglas de una sola vez?

Con el parámetro -F: `iptables -F`

27 Prohíba toda conexión de la subred 10.17.32.0/22 en su máquina, salvo 10.17.32.5.

```
iptables -A INPUT -s 10.17.32.0/22 ! 10.17.32.5 -j DROP
```

28

¿Cómo impedir cualquier conexión TCP saliente con destino a un servicio ssh (puerto 22)?

```
iptables -A OUTPUT -p tcp -dport 22
```

29

Su PC dispone de dos tarjetas de red. ¿Cómo prohibir cualquier entrada o salida en la segunda?

Con dos reglas iptables: `iptables -A INPUT -i eth0 -j DROP` *.*
Para la segunda, sustituya INPUT por OUTPUT.

30

Su PC, que dispone de dos tarjetas de red, sirve de enrutador. Quiere impedir el encaminamiento del puerto TCP 22. ¿Cómo hacerlo?

```
iptables -A FORWARD -i eth0 -o eth1 -p tcp -dport 22 -j DROP
```