Logs y Auditoría

Autores:

Carolina García Antón

Günther Rodríguez Díaz

Logs y Auditoría

- Contenido:
  - Introducción
  - Archivos
  - Utilidades
    - Lastlog
    - Last
  - Barredores
  - Syslog
  - Logrotate
  - Otras herramientas

Logs y Auditoría - Introducción

- ¿Qué es logging?
  - Cualquier procedimiento por el que un sistema operativo o aplicación graba eventos mientras ocurren y los guarda para un examen posterior.
  - Es un componente esencial de cualquier sistema operativo, al cual se le debe prestar mucha atención.
  - En cuanto a seguridad nos permite mantener un registro de las acciones dañinas de un atacante. Son la evidencia de que “nos han atacado”

Logs y Auditoría - Archivos

- Toda la estructura de archivos de log se encuentra en el directorio: */var/log/*
- Este directorio contiene multitud de archivos que corresponden a distintos servicios que se ejecutan en nuestra máquina y posteriormente imprimen su actividad en el fichero de log correspondiente o incluso en ficheros de log compartidos
- Se pueden ver estos fichero con el típico comando "*tail -f /var/log/nombrefichero*"

Logs y Auditoría – Utilidades

- Puede resultar muy engorroso examinar los archivos de logs directamente y mucho más dificil de detectar anomalías, errores o situaciones extrañas en nuestro sistema, para eso en el sistema existen utilidades que nos presentan esta información de forma más comoda y legible:
  - *lastlog*
  - *last*

Logs y Auditoría - *lastlog*

- Se encarga de imprimir información relativa a los logins de los usuarios de forma que muestra todos los usuarios contenidos en "*/etc/passwd*" y su último login si ha iniciado sesion alguna vez y si no un mensaje "**Never Logged in**". Esta utilidad lee la información del fichero "*/var/log/lastlog*":

Username	*Port*	*From*	*Latest*
root	*tty1*		*Thu Jul 1 12:12:12 2003*
user1	*ttyp0*	*172.16.0.1*	*Thu Jul 1 12:15:00 2003*
user2			***Never Logged in***

Logs y Auditoría - *last*

- Informa del último login de usuarios, pero esta vez mostrando información sólo de los usuarios que han hecho “log in”, dando así información como: usuarios, terminal usado, IP, fecha y hora y duración de sus sesiones. Esta utilidad lee la información del fichero “/var/log/wtmp”:

```
root     tty1                 Thu Jul 1 12:12  Still logged in
user1    ttyp0    172.16.0.1  Thu Jul 1 12:15 – 12:20 (05:00)
```

Logs y Auditoría - Barredores

- A pesar de la existencia de logs del sistema que nos permiten registrar intentos de ataques y sus autores, esto no es infalible y así un buen atacante puede eliminar las pistas de su ataque mediante la utilización de programas llamados barredores o limpiadores. Estos programas básicamente se encargan de borrar las entradas de los ficheros de logs correspondientes, de forma que no queden indicios de su entrada.

Logs y Auditoría - Barredores

- Algunos de estos programas son:
  - Cloak2 (shadowing)
  - Utclean (elimina entradas)
  - SYSLOG Fogger (entradas falsas)
  - Marry (editor)
- Existen formas de evitar que los atacantes borren sus rastros del todo:
  - Copias de seguridad de logs en otras máquinas.
  - Herramientas de logging de terceros.

Logs y Auditoría – Mensajes Kernel y Sistema

- Existen dos demonios que se encargan de manejar los mensajes del kernel y del sistema, estos son:
  - syslogd: Guarda los logs del sistema y de muchos servicios. Guarda el nombre del programa, el tipo de servicio, la prioridad y el mensaje del propio programa.
  - klogd:Guarda los logs propios del kernel para su posterior análisis en caso de error, por ejemplo.
- Ambos escriben sus mensajes en "*/var/log/messages*"

Logs y Auditoría – Syslog.conf

- El syslogd nos permite personalizar los loggings del sistema mediante el fichero de configuración "*/etc/syslog.conf*". Aquí se define todo sobre lo que se quiere hacer log, para esto se definen normas con dos campos:
  - Selector = A qué hacer log.
  - Action = Dónde hacer log.

Logs y Auditoría – Syslog.conf

- Campo Selector:
  - Consta de dos partes: type (facility) y priority.
    - Type:
      - auth
      - authpriv
      - cron
      - daemon
      - kern
      - lpr
      - mail
      - news
      - uucp
    - Priority:
      - alert
      - crit
      - debug
      - emerg
      - err
      - info
      - notice
      - warning

Logs y Auditoría – Syslog.conf

- Campo Action:
  - Especifica a donde deben ir los mensajes, normalmente es un fichero, aunque otras opciones muy interesantes son:
    - Consola
    - Máquina remota
    - Usuarios concretos
    - Todos los usuarios

Logs y Auditoría – Syslog.conf

- Ejemplo de syslog.conf:

```
#kernel
kern.*                                  /dev/console

# The authpriv file goes to a remote host.
authpriv.*                              @otramaquina

# Log all the mail messages in one place.
mail.*                                  /var/log/maillog


# Log cron stuff
cron.*                                  /var/log/cron

# Everybody gets emergency messages
*.emerg                                 *

# Save news errors of level crit and higher in a special file.
uucp,news.crit                          /var/log/spooler
```

Logs y Auditoría – logrotate

- Cuando tenemos un gran sistema linux con muchos usuarios, máquinas, etc, los logs pueden llegar a ser ficheros muy grandes. Para solucionar esto se usa *logrotate* que nos permitirá realizar copias de seguridad de los logs o rotarlos. También permite comprimir y enviar logs.
- Para realizar esto se usa el cron, al cual se le indicará si queremos hacer esto diariamente, semanalmente, etc.

Logs y Auditoría – logrotate

- Algunas opciones interesantes de logrotate:
  - Compress
  - Daily
  - Endscript
  - Mail [dirección de correo]
  - Monthly
  - Nocompress
  - Rotate [n]
  - Size
  - weekly

Logs y Auditoría – logrotate

- Ejemplo:

```
errors pepe@mail.com
    compress
/var/log/messages {
    rotate 5
    weekly
    postrotate
    endscript
}
```

Logs y Auditoría – Otras herramientas

- LogWatch
  - Analiza los logs durante un periodo de tiempo especificado por el usuario y genera informes personalizables y de fácil lectura para el administrador.
- Secure Syslog
  - Herramienta de logging de sistema criptográficamente segura, que permite la auditoría remota de los logs. Así un si un intruso entra conprivilegios de root sigue siendo posible auditar el sistema.

Logs y Auditoría

FIN