[FORT]TEMA 6: Mantenimiento

Para mantener un sistema debemos:

1. mantenerlo actualizado
2. mantenernos informados de vulnerabilidades no parcheadas, deshabilitando los servicios que tengan alguna hasta que sean parcheadas
3. Monitorizar el sistema buscando actividades sospechosas.

La información del sistema se guardan en los logs, que guardan todo lo que queremos que guarden. Los Logs no se deben guardar en la propia máquina, ya que si hay una intrusión es muy posible que sean eliminados.

Systemd y los Logs

Systemd es una funcionalidad cada vez más usada que usa “jorunald” o “jorunarl-ctl”, que guarda los logs en /var/logs/journal con un nombre bastante aleatorizado. En esta carpeta se crean archivos “.journal” que contienen el log. Systemd guarda los logs en un archivo binario que solo puede ser analizado con journal-ctl, esto es problemático si una máquina deja de funcionar ya que dificulta su visionado desde el exterior. Por esta razón se recomienda instalar otros sistemas de log:

- Syslogd: se encuentran en
- rsyslog

Syslogd

Podemos ver si usamos syslog con:

```
ps -elf | grep syslog
```

Dentro de los logs tenemos las facility (Quien produce el mensaje de log) y las severity (Como de importante es dicho mensaje de error). En /etc/syslog.conf podenos realizar la configuración de las facility y severity del sistema de logs.

```
*.*; auth,authpriv.nono -/var/log/syslog #Guardamos todo lo relacionado con autenticación en /var/log/syslog

#el -/ significa que debe de enviarse inmediatamente al archivo de log en cuestión sin esperar a que se actualice
```

rsyslog

Se puede configurar en /etc/rsyslog.conf

Rotación de logs

Antiguamente si una máquina pillaba los logs de otra no los podía mandar a una tercera. Ahora, con las versiones modernas de syslogd los logs que vienen de fuera pueden ser reenviados. Para evitar que los archivos de log sean demasiado grandes se pueden configurar para que cada día creen un archivo de log nuevo, manteniendo los anteriores. Podemos ver los logs en /var/log con el comando:

```
ls -l /var/log/ke*
```

Esto se puede hacer con logrotate, que puede ser configurado en logrotate.conf

```
weekly #Cada semana un log nuevo
rotate 4 #Preserva los logs antiguos 4 rotaciones (Tras 4 semanas se borra cada log)
create
include /etc/logrotate.d #Ubicación de configuraciones específicas
```

```
#Archivos a los que se aplica la config
/var/log/syslog
/var/log/mail.log
#Parámetros que se aplican
{
  rotate 4 #Se conservan los logs 4 rotaciones
  weekly #Se crea un archivo nuevo cada semana
}
```

lynis

Hace un análisis de como está un sistema y da pistas de cosas de seguridad mejorables.