Table of Contents

Audit

¿Tiene traviesos duendecillos que modifican archivos sin permiso?

¿El unicornio rosado invisible se “comio un archivo” y le cambió el password al jefecito?

Existe una manera de descubrir estos fenómenos, de denunciar a esas maldosas deidades.

El sistema Audit de Linux provee una vía para registrar información relevante a la seguridad del sistema. Se basa en reglas preconfiguradas, Audit genera logs para registrar toda la información posible sobre los eventos que ocurren en el sistema. Esta información es crucial para determinar quien es el infractor de alguna política de seguridad. No obstante Audit no proporciona seguridad adicional, una herramienta mas adecuada es SELinux.

Audit proporciona registros de eventos para:

- Fecha y hora, tipo y resultado de un evento.
- Etiquetas de sensibilidad de sujetos y objetos.
- Asociación de un evento con la identidad del usuario que accionó el evento
- Modificaciones de las configuraciones de Audit y el acceso a los archivos de log.
- Usos de mecanismos de autenticación, como SSH, Kerberos y otros.
- Cambios en bases de datos de confianza, como /etc/passwd
- Intentos de importar o exportar información hacia o desde el sistema.
- Incluir o excluir eventos basados en la identidad del usuario, etiquetas de sujeto y objeto, y otros atributos.

El sistema Audit consta de dos partes, a saber las aplicaciones y utilidades de espacio de usuario y el procesamiento de llamadas del sistema del lado del kernel.

Reglas

```
sudo auditctl -w /etc/hosts -p wa -k hosts_changes
sudo auditctl -w /etc/hosts.allow -p wa -k hosts_allow_changes
sudo auditctl -w /etc/hosts.deny -p wa -k hosts_deny_changes
sudo auditctl -w /etc/passwd -p wa -k passwd_changes
sudo auditctl -w /etc/group -p wa -k group_changes
sudo auditctl -w /etc/hostname -p wa -k hostname_changes
sudo auditctl -w /etc/crontab -p wa -k crontab_changes
sudo auditctl -w /etc/anacrontab -p wa -k anacrontab_changes
sudo auditctl -w /etc/resolv.conf -p wa -k resolv_changes
sudo auditctl -w /etc/rsyslog.conf -p wa -k rsyslog_changes
sudo auditctl -w /etc/rsyslog.d -p wa -k rsyslog_d_changes
sudo auditctl -w /etc/cron.d -p wa -k cron_d_changes
sudo auditctl -w /etc/cron.daily/ -p wa -k cron_daily_changes
sudo auditctl -w /etc/cron.hourly/  -p wa -k cron_hourly_changes
sudo auditctl -w /etc/cron.monthly/  -p wa -k cron_monthly_changes
sudo auditctl -w /etc/cron.weekly/  -p wa -k cron_weekly_changes
sudo auditctl -w /etc/modprobe.d/  -p wa -k modprobe_d_changes
sudo auditctl -w /etc/audit/ -p wa -k audit_changes
```

```
sudo auditctl -w /etc/audit/rules.d/ -p wa -k audit_rules_d_changes
```

Hacer las reglas anteriores persistentes:

```
sudo auditctl  -l > /etc/audit/rules.d/gbm.rules
```

Redireccionar registros de audit a syslog

El formato del audit es complicado de digerir, la mayoría de aplicaciones saben leer syslog, pero no audit, con los siguientes pasos puede redirigir los eventos de audit a syslog, de manera que puedan ser consumidos por medio de este protocolo.

Configure audisp **/etc/audisp/plugins.d/**:

```
active = yes
direction = out
path = builtin_syslog
type = builtin
args = LOG_LOCAL6
format = string
```

Configure rsyslog **/etc/rsyslog.d/audit.conf**:

```
local6.*    /var/log/audit.log
```

Reinicie los servicios:

```
service auditd restart
systemctl restart rsyslog
```

Referencias

- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/chap-system_auditing.html
- http://security.blogoverflow.com/2013/01/a-brief-introduction-to-auditd/