Observaciones relativas a la seguridad

La seguridad es una preocupación constante para la gestión de los sistemas modernos y particularmente para los accesos de red. Las distribuciones Linux activan por defecto numerosos mecanismos de protección, como los módulos PAM, el firewall (`iptables`, `firewalld`, etc.) o SELinux.

Estas protecciones indispensables en producción pueden perturbar seriamente sus comprobaciones. Si constata que, a pesar de todos sus esfuerzos, la configuración de sus servicios de red no funciona correctamente, con síntomas bastante diversos, desactive temporalmente algunas de las protecciones del sistema. Si haciendo una nueva comprobación, todo funciona correctamente, tendrá que identificar con precisión el problema para adaptar su configuración funcional y la configuración de seguridad.

Esta desactivación temporal de la capa de seguridad debe estar reservada a un entorno de pruebas, ¡nunca en producción!

1. iptables

Por defecto, en la mayoría de las distribuciones, `iptables` no autoriza ninguna conexión entrante excepto SSH. Para comprobar su configuración, puede usar el comando `iptables -L`.

Ejemplo

```
iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
```

```
ACCEPT     icmp --  anywhere       anywhere
ACCEPT     all  --  anywhere       anywhere
ACCEPT     tcp  --  anywhere       anywhere       state NEW tcp dpt:ssh
REJECT     all  --  anywhere       anywhere       reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source          destination
REJECT     all  --  anywhere       anywhere       reject-with icmp-host-prohibited
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
```

`iptables` está activado y filtra los accesos.

Si `iptables` está instalado como servicio, administrado por un script `init System V` o por `systemd`, podemos desactivarlo temporalmente usando los comandos `service` o `systemctl`.

Ejemplo

```
service iptables stop
service iptables stop
Redirecting to /bin/systemctl stop iptables.service
[root@beta ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source          destination

Chain FORWARD (policy ACCEPT)
target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
```

Si `iptables` no ha sido instalado como servicio, podemos desactivar sus controles con los comandos siguientes:

```
iptables -F
iptables -X
iptables -t nat -F
iptables -t mangle -F
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
```

2. firewalld

Este servicio está gestionado por `systemd`. Podemos desactivarlo (temporalmente) y reactivarlo usando el comando `systemctl`:

```
systemctl stop|start firewalld
```

3. SELinux

SELinux (*Security Enhanced Linux*) es un componente del núcleo especializado en la seguridad. Es muy potente y permite, por ejemplo, limitar los derechos de un proceso superusuario.

Su configuración es compleja y produce efectos a veces desconcertantes. Algunos servicios dejan de funcionar correctamente, con mensajes de error más o menos claros y, a veces, sin ninguna relación con la seguridad.

Se puede desactivar temporalmente SELinux, para asegurarse de que el problema "sin solución" no es provocado por este último.

Ejemplo

Comprobar la configuración de SELinux:

```
sestatus
SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   enforcing
Mode from config file:          enforcing
Policy version:                 24
Policy from config file:        targeted
```

`SELinux` está en modo reforzado.

Desactivar temporalmente SELinux:

```
setenforce 0
sestatus
SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   permissive
Mode from config file:          enforcing
Policy version:                 24
Policy from config file:        targeted
```

SELinux está en modo permisivo.