Guía de estudio - Monitoreo y auditoría de SSH

¡Hola! Te damos la bienvenida a esta nueva guía de estudio.

¿En qué consiste esta guía?

El monitoreo y la auditoría de las conexiones SSH son componentes esenciales para la seguridad de los sistemas remotos. Vigilar quién intenta acceder y detectar patrones sospechosos permiten identificar ataques de fuerza bruta, accesos no autorizados y otros incidentes de seguridad.

En esta guía, se explorarán dos herramientas fundamentales para este propósito: Fail2Ban y Logwatch. Estas herramientas permiten, respectivamente, bloquear automáticamente direcciones IP maliciosas y generar informes detallados sobre los eventos registrados en los logs del sistema.

¡Vamos con todo!

Tabla de contenidos

¡Comencemos!

Herramientas clave para el monitoreo y la auditoría de SSH

Importancia del monitoreo en SSH

- **Detección temprana:** Permite identificar intentos de acceso indebido, ataques de fuerza bruta y comportamientos anómalos.
- **Prevención de incidentes:** Al bloquear automáticamente IPs sospechosas, se reducen significativamente los riesgos de intrusiones.
- **Auditoría y análisis:** Generar informes periódicos ayuda a revisar el historial de conexiones, facilitando auditorías y la mejora continua de la seguridad.

Herramientas destacadas

- **Fail2Ban:** Se encarga de analizar los archivos de log (como `/var/log/auth.log`), detectando patrones de ataques y bloqueando las IPs infractoras mediante reglas de firewall.
- **Logwatch:** Ofrece resúmenes diarios o periódicos de los logs del sistema, enfocándose en actividades relevantes (como las conexiones SSH), permitiendo a los administradores tener una visión global de lo ocurrido.

Uso de Fail2Ban para proteger y monitorear SSH

¿Qué es Fail2Ban?

Fail2Ban es una herramienta que escanea los logs en busca de patrones que indiquen intentos de acceso fallidos o comportamientos maliciosos. Cuando detecta una actividad sospechosa, automáticamente agrega una regla en el firewall para bloquear la dirección IP por un tiempo determinado.

Instalación y configuración básica

Instalación: En sistemas basados en Debian/Ubuntu/Red Hat - Rocky Linux:

```
sudo apt-get update
sudo apt-get install fail2ban

sudo dnf update -y
sudo dnf install fail2ban -y
fail2ban-client --version
```

Configuración inicial:

Crea una copia del archivo de configuración por defecto:

```
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

Edita el archivo `/etc/fail2ban/jail.local:`

```
sudo nano /etc/fail2ban/jail.local
```

Ubica la sección `[sshd]` y asegúrate de que las siguientes directivas estén habilitadas:

```
[sshd]
enabled  = true
port     = ssh
filter   = sshd
logpath  = /var/log/auth.log
maxretry = 5
```

- *Esto indica que después de 5 intentos fallidos se bloqueará la IP que realice dichos intentos.*

Reinicia Fail2Ban para aplicar los cambios:

```
sudo systemctl restart fail2ban
```

Actividad guiada: Configurar un Jail personalizado para SSH

1. **Iniciar la máquina virtual con Rocky Linux.**
2. **Instalar Fail2Ban**

```
sudo dnf install fail2ban -y
```

3. **Editar la configuración:**

Abre el archivo de configuración de Fail2Ban:

```
sudo nano /etc/fail2ban/jail.local
```

4. **Modificar parámetros:**

Ajusta el parámetro `maxretry` a un valor que consideres adecuado, por ejemplo, 3:

```
maxretry = 3
```

Define el tiempo de baneo, agregando:

```
bantime = 3600
```

- *Esto bloquea la IP durante 1 hora después de 3 intentos fallidos.*

Guarda los cambios y reinicia el servicio:

```
sudo systemctl restart fail2ban
```

Verifica el estado:

```
sudo fail2ban-client status sshd
```

Uso de Logwatch para la auditoría de conexiones SSH

¿Qué es Logwatch?

Logwatch es una herramienta de análisis de logs que genera informes detallados de los eventos registrados en el sistema. Se utiliza para resumir la actividad del día, facilitando la revisión de eventos críticos como conexiones SSH, errores y accesos denegados.

Instalación y configuración básica

Instalación:
En sistemas basados en Debian/Ubuntu/Red Hat - Rocky Linux:

```
sudo apt-get update
sudo apt-get install logwatch

sudo dnf install logwatch -y
```

Generar un Informe de SSH:

Para obtener un informe detallado de las actividades de SSH del día:

```
sudo logwatch --detail high --service sshd --range today --mailto
tu_correo@dominio.com --format text
```

- Este comando enviará un correo (si el sistema está configurado para enviar emails) o mostrará el informe en la terminal.

Configuración automática:

- La configuración de Logwatch se encuentra en `/usr/share/logwatch/default.conf/logwatch.conf` y `/etc/logwatch/conf/logwatch.conf`.
- Puedes editar estos archivos para ajustar el rango de fechas, el formato y la dirección de envío de los informes.

¡Manos a la obra! - Configurar informes diarios de actividad SSH

Configura Logwatch para informes diarios:

Abre el archivo de configuración:

```
sudo nano /etc/logwatch/conf/logwatch.conf
```

Asegúrate de definir la opción de rango de fecha como `yesterday` o `today` y configura el correo de destino:

```
MailTo = tu_correo@dominio.com
Range = yesterday
Detail = High
```

Ejecuta manualmente Logwatch:

```
sudo logwatch --detail high --service sshd --range yesterday --format
text
```

Verifica la recepción del informe:

- Confirma que el correo o el informe generado contenga los eventos relacionados con SSH, tales como intentos de conexión exitosos y fallidos.

Organizador de comandos y configuraciones

Herramienta	Comando/Configuración	Descripción
Fail2Ban	`sudo apt-get install fail2ban`	Instala Fail2Ban en sistemas Debian/Ubuntu.
	`sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local`	Crea un archivo de configuración local.
	En `[sshd]: enabled = true, port = ssh, logpath = /var/log/auth.log, maxretry = 3, bantime = 3600`	Configura el jail para monitorear y bloquear intentos fallidos.
	`sudo fail2ban-client status sshd`	Verifica el estado del jail SSH.
Logwatch	`sudo apt-get install logwatch`	Instala Logwatch.
	`sudo logwatch --detail high --service sshd --range today --mailto correo@dominio.com --format text`	Genera un informe detallado de SSH.
	Editar `/etc/logwatch/conf/logwatch.conf: MailTo, Range, Detail`	Configura Logwatch para informes diarios automáticos.

Tabla 01. Resumen.
Fuente: ADL.

Reflexiona:

- ¿Por qué es fundamental monitorear las conexiones SSH y qué riesgos se pueden mitigar con estas herramientas?
- ¿Cómo pueden ajustarse los parámetros de Fail2Ban para equilibrar la seguridad y evitar bloqueos de usuarios legítimos?
- ¿De qué manera los informes generados por Logwatch pueden ayudar en una auditoría de seguridad y en la identificación de patrones sospechosos?
- ¿Qué ventajas ofrece utilizar tanto Fail2Ban como Logwatch en conjunto para proteger y

auditar los accesos SSH?

El monitoreo y la auditoría son pilares esenciales en la gestión de la seguridad en sistemas que utilizan SSH. Herramientas como Fail2Ban y Logwatch no solo ayudan a prevenir y mitigar ataques mediante la detección y bloqueo automático de IPs maliciosas, sino que también proporcionan informes detallados que facilitan la auditoría y el análisis de la actividad en el sistema. Al implementar estas soluciones y ajustar sus configuraciones de acuerdo con las necesidades específicas de tu entorno, podrás mantener un control riguroso sobre el acceso a tus servidores, elevando significativamente el nivel de seguridad.