Actividad 2.3: Integridad y Análisis de Logs en EC2

Dario Briongos Garcia

Introducción

Utilizando la instancia EC2 que tenemos a disposición vamos a trabajar conceptos de cifrado e integridad.

Elementos que manejaremos: SHA, logs, seguridad

Instrucciones

1. **Integridad de archivos con SHA - 256**

1.1 Generar el hash SHA-256 del archivo original

Ejecuta en la instancia EC2:

```
sha256sum datos.txt > datos.sha256
```

Con este comando creo el archivo con el hash del fichero original

1.2 Modificar el archivo para simular un ataque

Añade una línea nueva al archivo:

```
echo "Modificación maliciosa" >> datos.txt
```

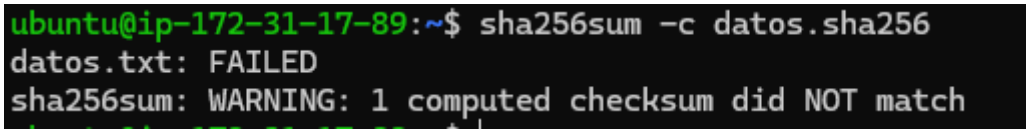
El archivo cambió respecto al original, lo que rompe la integridad.

1.3 Verificación de la integridad del archivo

Comprueba la coincidencia del hash:

```
sha256sum -c datos.sha256
```

Deberías observar un Fallo indicando que el archivo ha cambiado



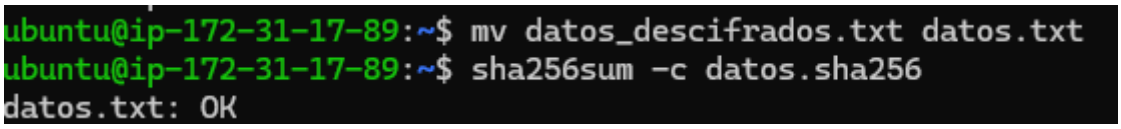
1.4 Restaurar archivo original y verificar

Restituye el archivo original:

```
mv datos_descifrados.txt datos.txt

sha256sum -c datos.sha256
```

Ahora debería funcionar



2. Análisis básico de logs

Como sabemos, los logs nos permiten saber qué ha pasado en el sistema: accesos, comandos, avisos, errores,

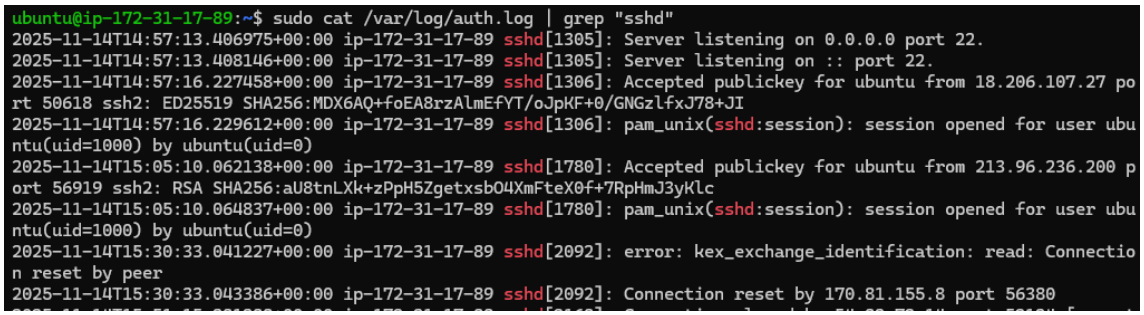
etc.

2.1 Revisar accesos SSH a la instancia

Ubuntu:

```
sudo cat /var/log/auth.log | grep "sshd"
```

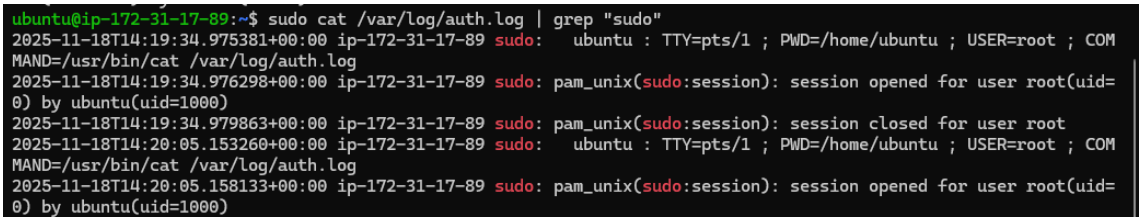
Interpreta IP de origen, Acceso aceptado o rechazado, Hora del evento



2.2 Ver quién ha usado sudo

```
sudo cat /var/log/auth.log | grep "sudo"
```

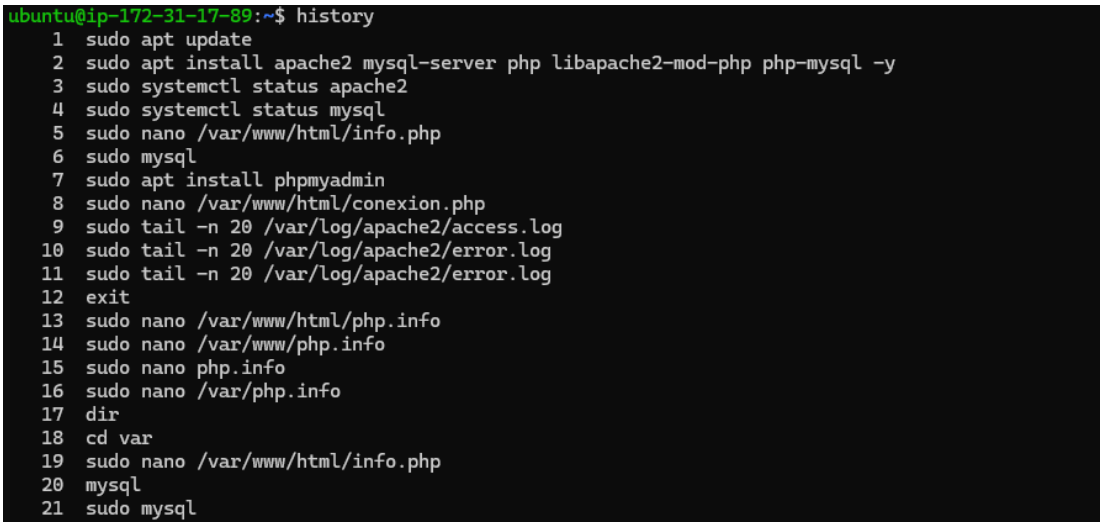
nos aparecen los intentos de uso de sudo, mostrando qué usuario lo ejecutó y cuándo.



2.3 Consultar el historial de comandos

Útil para auditar acciones.

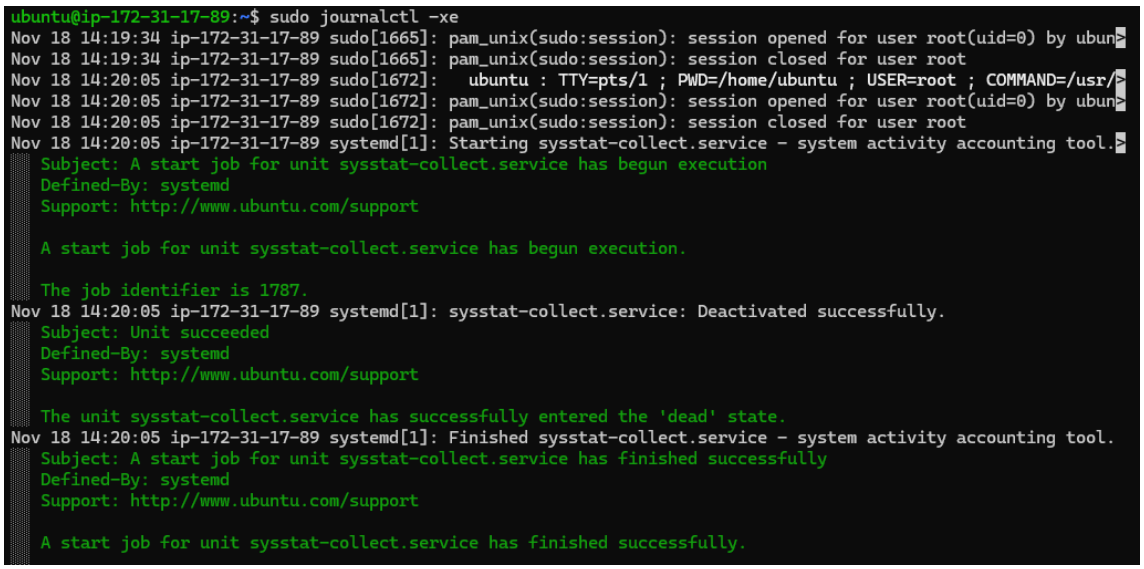
```
History
```



2.4 Ver logs del sistema

Este comando es para ver eventos recientes del sistema: errores, avisos y procesos en ejecución.

```
sudo journalctl -xe
```



2.5 Buscar modificaciones sospechosas del archivo

Ubuntu:

```
sudo grep "datos.txt" /var/log/syslog
```

comprobé si había registros relacionados con el archivo, lo que ayuda a detectar accesos o cambios no autorizados.

3. Cuestiones

1. ¿Qué diferencia existe entre cifrar un archivo y generar su hash?

   Cifrar es transformar el archivo en un formato que no se pueda leer pero si tienes la clave puedes revertir el efecto y Hash genera una huella única para verificar integridad.

2. ¿Qué ocurre si un atacante modifica un archivo cifrado?

   Que el archivo ya no podrá descifrarse correctamente o te dará algún error porque el contenido cifrado cambia.

3. ¿Por qué no se puede revertir un hash?

Porque solo produce una huella sin información suficiente para reconstruir el original.

4. ¿Dónde se encuentran los logs principales de un sistema Linux?

En /var/log/, por ejemplo: auth.log, syslog, dmesg, entre otros.

5. ¿Qué información aportan los logs de SSH y sudo?

SSH: IP de origen, hora, si el acceso fue aceptado o rechazado.

Sudo: qué usuario ejecutó comandos con privilegios y cuándo.

6. Explica por qué revisar logs ayuda a detectar actividad sospechosa.

Porque muestra accesos, errores y modificaciones que nos permiten identificar uso indebido.

7. ¿Qué servicio de AWS permite centralizar logs de múltiples EC2?

CloudWatch Logs permite monitorizar varias instancias EC2 desde un único panel.