

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
```

```
ubuntu@ip-172-31-17-89:~$ 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
```

```
ubuntu@ip-172-31-17-89:~$ 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

```
ubuntu@ip-172-31-17-89:~$ sha256sum -c datos.sha256
datos.txt: FAILED
sha256sum: WARNING: 1 computed checksum did NOT match
```

1.4 Restaurar archivo original y verificar

Restituye el archivo original:

```
mv datos_descifrados.txt datos.txt
```

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

Ahora debería funcionar

```
ubuntu@ip-172-31-17-89:~$ mv datos_descifrados.txt datos.txt
ubuntu@ip-172-31-17-89:~$ sha256sum -c datos.sha256
datos.txt: OK
```

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

```
ubuntu@ip-172-31-17-89:~$ sudo cat /var/log/auth.log | grep "sshd"
2025-11-14T14:57:13.406975+00:00 ip-172-31-17-89 sshd[1305]: Server listening on 0.0.0.0 port 22.
2025-11-14T14:57:13.408146+00:00 ip-172-31-17-89 sshd[1305]: Server listening on :: port 22.
2025-11-14T14:57:16.227458+00:00 ip-172-31-17-89 sshd[1306]: Accepted publickey for ubuntu from 18.206.107.27 port 50618 ssh2: ED25519 SHA256:MDX6AQ+foEA8rzAlmEfYT/oJpKF+0/GNGzlfXJ78+JI
2025-11-14T14:57:16.229612+00:00 ip-172-31-17-89 sshd[1306]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
2025-11-14T15:05:10.062138+00:00 ip-172-31-17-89 sshd[1780]: Accepted publickey for ubuntu from 213.96.236.200 port 56919 ssh2: RSA SHA256:aU8tnLXk+zPpH5Zgetxsb04XmFteX0f+7RpHmJ3yKlc
2025-11-14T15:05:10.064837+00:00 ip-172-31-17-89 sshd[1780]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
2025-11-14T15:30:33.041227+00:00 ip-172-31-17-89 sshd[2092]: error: kex_exchange_identification: read: Connection reset by peer
2025-11-14T15:30:33.043386+00:00 ip-172-31-17-89 sshd[2092]: Connection reset by 170.81.155.8 port 56380
```

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.

```
ubuntu@ip-172-31-17-89:~$ sudo cat /var/log/auth.log | grep "sudo"
2025-11-18T14:19:34.975381+00:00 ip-172-31-17-89 sudo:      ubuntu : TTY=pts/1 ; PWD=/home/ubuntu ; USER=root ; COM
MAND=/usr/bin/cat /var/log/auth.log
2025-11-18T14:19:34.976298+00:00 ip-172-31-17-89 sudo: pam_unix(sudo:session): session opened for user root(uid=
0) by ubuntu(uid=1000)
2025-11-18T14:19:34.979863+00:00 ip-172-31-17-89 sudo: pam_unix(sudo:session): session closed for user root
2025-11-18T14:20:05.153260+00:00 ip-172-31-17-89 sudo:      ubuntu : TTY=pts/1 ; PWD=/home/ubuntu ; USER=root ; COM
MAND=/usr/bin/cat /var/log/auth.log
2025-11-18T14:20:05.158133+00:00 ip-172-31-17-89 sudo: pam_unix(sudo:session): session opened for user root(uid=
0) by ubuntu(uid=1000)
```

2.3 Consultar el historial de comandos

Útil para auditar acciones.

```
History
```

```
ubuntu@ip-172-31-17-89:~$ history
 1 sudo apt update
 2 sudo apt install apache2 mysql-server php libapache2-mod-php php-mysql -y
 3 sudo systemctl status apache2
 4 sudo systemctl status mysql
 5 sudo nano /var/www/html/info.php
 6 sudo mysql
 7 sudo apt install phpmyadmin
 8 sudo nano /var/www/html/conexion.php
 9 sudo tail -n 20 /var/log/apache2/access.log
10 sudo tail -n 20 /var/log/apache2/error.log
11 sudo tail -n 20 /var/log/apache2/error.log
12 exit
13 sudo nano /var/www/html/php.info
14 sudo nano /var/www/php.info
15 sudo nano php.info
16 sudo nano /var/php.info
17 dir
18 cd var
19 sudo nano /var/www/html/info.php
20 mysql
21 sudo mysql
```

2.4 Ver logs del sistema

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

```
sudo journalctl -xe
```

```
ubuntu@ip-172-31-17-89:~$ sudo journalctl -xe
Nov 18 14:19:34 ip-172-31-17-89 sudo[1665]: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu
Nov 18 14:19:34 ip-172-31-17-89 sudo[1665]: pam_unix(sudo:session): session closed for user root
Nov 18 14:20:05 ip-172-31-17-89 sudo[1672]: ubuntu : TTY=pts/1 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/
Nov 18 14:20:05 ip-172-31-17-89 sudo[1672]: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu
Nov 18 14:20:05 ip-172-31-17-89 sudo[1672]: pam_unix(sudo:session): session closed for user root
Nov 18 14:20:05 ip-172-31-17-89 systemd[1]: Starting sysstat-collect.service - system activity accounting tool.
Subject: A start job for unit sysstat-collect.service has begun execution
Defined-By: systemd
Support: http://www.ubuntu.com/support

A start job for unit sysstat-collect.service has begun execution.

The job identifier is 1787.
Nov 18 14:20:05 ip-172-31-17-89 systemd[1]: sysstat-collect.service: Deactivated successfully.
Subject: Unit succeeded
Defined-By: systemd
Support: http://www.ubuntu.com/support

The unit sysstat-collect.service has successfully entered the 'dead' state.
Nov 18 14:20:05 ip-172-31-17-89 systemd[1]: Finished sysstat-collect.service - system activity accounting tool.
Subject: A start job for unit sysstat-collect.service has finished successfully
Defined-By: systemd
Support: http://www.ubuntu.com/support

A start job for unit sysstat-collect.service has finished successfully.
```

2.5 Buscar modificaciones sospechosas del archivo

Ubuntu:

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

```
ubuntu@ip-172-31-17-89:~$ sudo grep "datos.txt" /var/log/syslog
ubuntu@ip-172-31-17-89:~$ |
```

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.