

Bash básico para SOC

1. Objetivo. – Crear un script para recopilar y mostrar información relevante del sistema, incluyendo intentos fallidos de autenticación, usuarios con privilegios elevados y servicios activos, con el fin de apoyar tareas básicas de monitoreo.

2. Herramientas. - Para este laboratorio se utilizaron:

- Oracle VirtualBox.
- Cliente Ubuntu (máquina virtual)

3. Configuración

3.1 Preparación del entorno y creación de script

En primer lugar, se creó una carpeta destinada a almacenar el script de monitoreo. Posteriormente, se desarrolló el script utilizando el editor nano en Linux, dentro de este script se introdujeron distintos comandos orientados a tareas básicas de monitoreo, tales como intentos fallidos de login, identificación de usuarios con UID 0 (privilegios root) y la enumeración de servicios activos en el sistema. (ver Figura 1)



```
maincruf@maincruf-VirtualBox: ~/lab_linux_4_bash_soc
GNU nano 7.2 soc_monitor.sh *
#!/bin/bash

echo "=====
echo " SCRIPT BASICO DE MONITOREO SOC
echo "=====
echo ""
echo " Intentos fallidos de login:"
echo "-----"

grep "Failed password" /var/log/auth.log | tail -n 5

echo ""
echo " Usuarios con UID 0 (privilegios root):"
echo "-----"

awk -F: '$3 == 0 {print $1}' /etc/passwd

echo ""
echo " Servicios activos en el sistema:"
echo "-----"

systemctl list-units --type=service --state=running | head -n 10

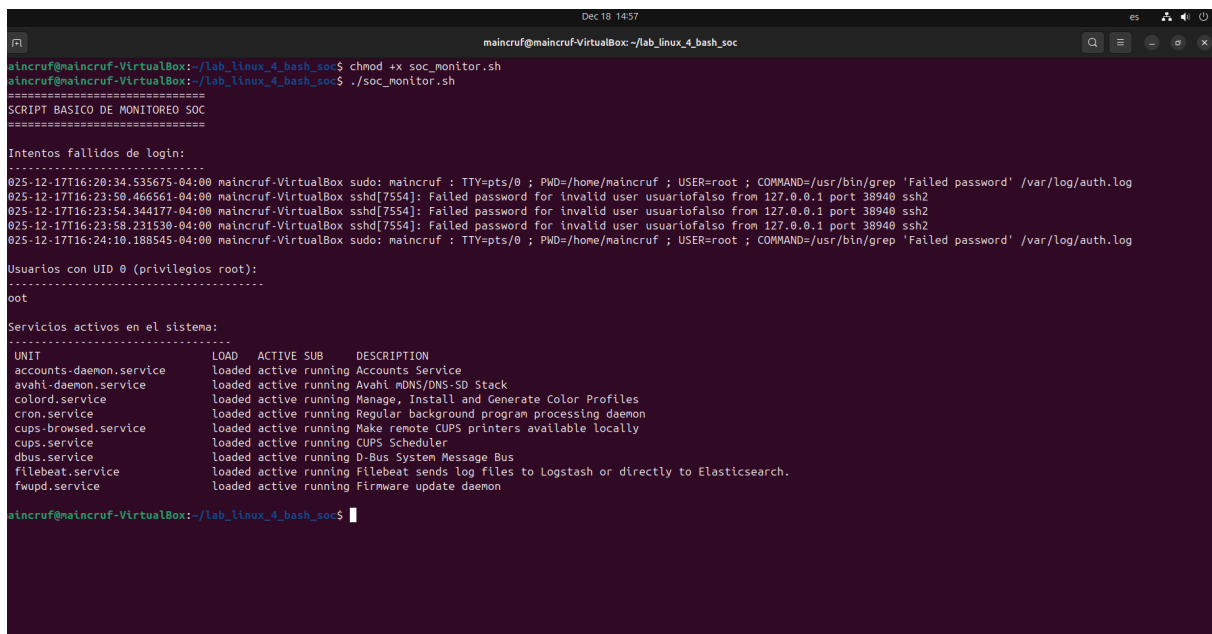
echo ""
```

Figura 1. Creación de script de monitoreo.

4. Verificación Técnica

4.1 Permisos y ejecución de script de monitoreo

Se modificaron los permisos del script para permitir su correcta ejecución. Durante la ejecución, el script mostró los registros de autenticación y servicios activos del sistema. Además, no se identificaron usuarios con privilegios elevados como usuarios root. Con base en los resultados obtenidos, se concluyó que el script funcionó de manera correcta y cumplió con los objetivos. (Ver figura 2)



```
Dec 18 14:57
maincruf@maincruf-VirtualBox: ~/lab_linux_4_bash_soc

maincruf@maincruf-VirtualBox:~/lab_linux_4_bash_soc$ chmod +x soc_monitor.sh
maincruf@maincruf-VirtualBox:~/lab_linux_4_bash_soc$ ./soc_monitor.sh

=====
SCRIPT BASICO DE MONITOREO SOC
=====

Intentos fallidos de login:
-----
025-12-17T16:20:34.535675-04:00 maincruf-VirtualBox sudo: maincruf : TTY=pts/0 ; PWD=/home/maincruf ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
025-12-17T16:23:50.466561-04:00 maincruf-VirtualBox sshd[7554]: Failed password for invalid user usuariofalso from 127.0.0.1 port 38940 ssh2
025-12-17T16:23:54.344177-04:00 maincruf-VirtualBox sshd[7554]: Failed password for invalid user usuariofalso from 127.0.0.1 port 38940 ssh2
025-12-17T16:23:58.231530-04:00 maincruf-VirtualBox sshd[7554]: Failed password for invalid user usuariofalso from 127.0.0.1 port 38940 ssh2
025-12-17T16:24:10.188545-04:00 maincruf-VirtualBox sudo: maincruf : TTY=pts/0 ; PWD=/home/maincruf ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log

Usuarios con UID 0 (privilegios root):
-----
root

Servicios activos en el sistema:
-----
UNIT                                LOAD    ACTIVE SUB    DESCRIPTION
accounts-daemon.service            loaded active running Accounts Service
avahi-daemon.service               loaded active running Avahi mDNS/DNS-SD Stack
colord.service                     loaded active running Manage, Install and Generate Color Profiles
cron.service                       loaded active running Regular background program processing daemon
cups-browsed.service               loaded active running Make remote CUPS printers available locally
cups.service                       loaded active running CUPS Scheduler
dbus.service                       loaded active running D-Bus System Message Bus
filebeat.service                   loaded active running Filebeat sends log files to Logstash or directly to Elasticsearch.
fwupd.service                      loaded active running Firmware update daemon

maincruf@maincruf-VirtualBox:~/lab_linux_4_bash_soc$
```

Figura 2. Resultado de la ejecución de script de monitoreo.