Automatización de Auditorías de Seguridad con Bash

Hace poco me propuse realizar un proyecto para automatizar auditorías de seguridad en un sistema Linux. Usando Bash, logré crear un script que permite verificar el estado de parches, el firewall, usuarios inactivos, y generar un reporte final. Aquí relato mi experiencia y los pasos que seguí para lograrlo.

Objetivo del Proyecto

Desarrollar un script que pudiera realizar las siguientes tareas de forma automática:

1.Verificar si el sistema tiene parches de seguridad pendientes.

2.Comprobar la configuración del firewall (UFW).

3.Identificar cuentas inactivas o con privilegios de root que podrían representar un riesgo.

4.Generar un reporte consolidado con la información recolectada.

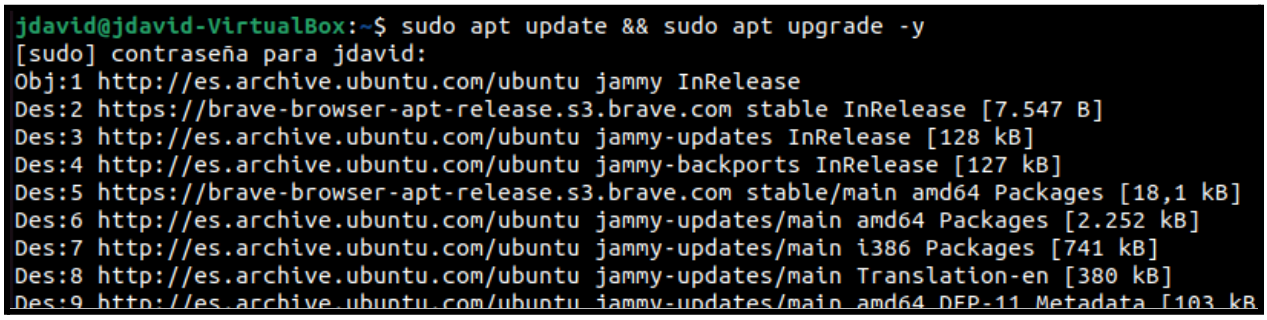
Decidí usar Bash, ya que es ideal para tareas de administración en sistemas Linux como Ubuntu o Kali.

Creación del Script

Paso 1: Configuración del Entorno

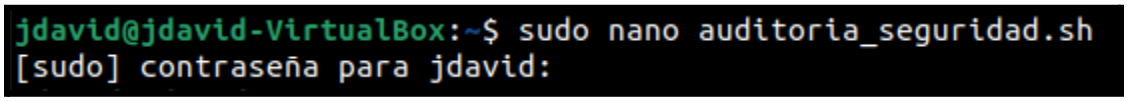
Primero, abrí la terminal y actualicé el sistema:

`sudo apt update && sudo apt upgrade -y`



Luego creé un nuevo archivo en mi directorio de trabajo para escribir el script:

`nano auditoria_seguridad.sh`



Paso 2: Escribí el Código

Añadí las siguientes líneas al archivo para que el script cubriera cada objetivo definido:

```
  GNU nano 6.2
#!/bin/bash
# Archivo de reporte
REPORTE="reporte_auditoria_$(date +%Y%m%d).txt"
echo "=================================" > $REPORTE
echo "    REPORTE DE AUDITORÍA DE SEGURIDAD    " >> $REPORTE
echo "Fecha: $(date)" >> $REPORTE
echo "=================================" >> $REPORTE
echo "" >> $REPORTE
# 1. Verificar Actualizaciones y Parches de Seguridad
echo "[1] Verificando actualizaciones del sistema..." | tee -a $REPORTE
sudo apt-get update > /dev/null
sudo apt-get -s upgrade | grep "Inst" >> $REPORTE 2>/dev/null
echo "Actualizaciones pendientes listadas." | tee -a $REPORTE
echo "" >> $REPORTE
# 2. Comprobar configuración de Firewall (UFW)
echo "[2] Verificando configuración de firewall (UFW)..." | tee -a $REPORTE
if sudo ufw status | grep -q "active"; then
    echo "Firewall está habilitado." >> $REPORTE
    sudo ufw status verbose >> $REPORTE
else
    echo "¡Firewall NO está habilitado!" >> $REPORTE
fi
echo "" >> $REPORTE
# 3. Detectar cuentas de usuario con acceso root
echo "[3] Revisando cuentas con privilegios de root..." | tee -a $REPORTE
awk -F: '($3 == 0) {print $1}' /etc/passwd >> $REPORTE
echo "Cuentas con UID=0 listadas." >> $REPORTE
echo "" >> $REPORTE
# 4. Detectar usuarios inactivos
echo "[4] Buscando usuarios inactivos..." | tee -a $REPORTE
lastlog | grep "Never logged in" >> $REPORTE
echo "Usuarios inactivos listados." >> $REPORTE
echo "" >> $REPORTE
# 5. Escaneo básico de puertos abiertos
echo "[5] Escaneo básico de puertos abiertos..." | tee -a $REPORTE
sudo netstat -tuln | grep LISTEN >> $REPORTE
echo "Puertos abiertos listados." >> $REPORTE
echo "" >> $REPORTE
echo "============================" >> $REPORTE
echo "Auditoría finalizada. Revisa el archivo: $REPORTE" | tee -a $REPORTE
```

Paso 3: Permisos y Ejecución

Guardé el archivo y luego le di permisos de ejecución:

`chmod +x auditoria_seguridad.sh`

```
jdavid@jdavid-VirtualBox:~$ sudo chmod +x auditoria_seguridad.sh
jdavid@jdavid-VirtualBox:~$
```

Lo ejecuté con permisos de root para asegurar que pudiera acceder a toda la información necesaria:

`sudo ./auditoria_seguridad.sh`

```
jdavid@jdavid-VirtualBox:~$ sudo ./auditoria_seguridad.sh
[1] Verificando actualizaciones del sistema...
Actualizaciones pendientes listadas.
[2] Verificando configuración de firewall (UFW)...
[3] Revisando cuentas con privilegios de root...
[4] Buscando usuarios inactivos...
[5] Escaneo básico de puertos abiertos...
Auditoría finalizada. Revisa el archivo: reporte_auditoria_20241220.txt
jdavid@jdavid-VirtualBox:~$
```

Revisión del Resultado

El script generó un archivo de reporte en el mismo directorio llamado algo como:

cat reporte_auditoria_20241220.txt.

```
jdavid@jdavid-VirtualBox:~$ cat reporte_auditoria_20241220.txt
==================================
    REPORTE DE AUDITORÍA DE SEGURIDAD
Fecha: vie 20 dic 2024 17:05:40 CET
==================================

[1] Verificando actualizaciones del sistema...
Actualizaciones pendientes listadas.

[2] Verificando configuración de firewall (UFW)...
¡Firewall NO está habilitado!

[3] Revisando cuentas con privilegios de root...
root
Cuentas con UID=0 listadas.

[4] Buscando usuarios inactivos...
Usuarios inactivos listados.

[5] Escaneo básico de puertos abiertos...
Puertos abiertos listados.

============================
Auditoría finalizada. Revisa el archivo: reporte_auditoria_20241220.txt
```

Al abrirlo con cat o nano, pude ver un resumen detallado:

1.Actualizaciones pendientes: Una lista de paquetes que necesitan ser actualizados, identificando posibles parches críticos.

2.Firewall: Confirmó si el firewall estaba habilitado y mostró detalles sobre las reglas configuradas.

3.Cuentas con UID 0: Identificó si había usuarios con privilegios de root, lo cual es crucial para la seguridad.

4.Usuarios inactivos: Listó cuentas que nunca habían iniciado sesión.

5.Puertos abiertos: Un mapeo de los servicios escuchando en la máquina.