



# Defensa

## Shasum

```
shasum Born2beroot.vdi | diff - signature.txt
```

### ¿Qué hace este comando?

1. `shasum Born2beroot.vdi` : genera el hash actual del archivo `.vdi` .
2. `diff - signature.txt` : compara la salida del hash actual ( significa "leer desde `stdin`" ) con el contenido guardado en `signature.txt` .

### ¿Qué resultado esperar?

- **Si no hay diferencias**, no se muestra salida → el archivo no ha sido modificado.
- **Si hay diferencias**, `diff` mostrará las líneas que no coinciden → el archivo ha cambiado.

## Evaluación de Defensa Born2BeRoot

## **Preguntas de evaluación**

### **¿Por qué elegí Debian?**

Es más fácil de instalar y configurar, por lo tanto, es mejor para servidores personales.

### **¿Cuál es la diferencia entre Debian y CentOS?**

Debian es mucho más fácil de actualizar que CentOS cuando se lanza una nueva versión. Debian es más amigable para el usuario y es compatible con muchas bibliotecas, sistemas de archivos y arquitecturas. También ofrece más opciones de personalización. Si eres una empresa más grande, CentOS ofrece más características empresariales y excelente soporte para software empresarial.

# CENTOS VS DEBIAN



Supported by the Red Hat community.

CentOS has a large market due to its user-friendly nature.

CentOS does not come with multiple architecture support.

New updates and upgrades usually take time, thus making it stable.

It is better to install a new CentOS version rather than go for upgrading the older version. This task is cumbersome.

CentOS has a complicated GUI.

CentOS uses YUM as its package manager.

CentOS has limited packages.



Supported by Debian individuals.

Debian lacks market presence due to its terminal end usage.

Debian has multiple architecture support as compared to other distributions.

It has a release cycle of 2 years, thus giving it enough time to fix bugs.

Debian can be easily upgraded from one stable version to another.

Debian comes with user-friendly applications and GUI.

Debian uses apt-get as its package manager.

Debian has a vast amount of packages in its default repository to do something.

---

## ¿Qué es una Máquina Virtual (VM)?

Es un recurso que usa software en lugar de una computadora física para ejecutar programas o aplicaciones. Cada VM tiene su propio sistema operativo y funciona de manera independiente, por lo que puedes tener más de una VM por máquina. Se puede usar para probar aplicaciones en un entorno separado y seguro. Funciona usando software que simula hardware virtual y se ejecuta sobre una máquina anfitriona (host).

---

## ¿Cuál es la diferencia entre aptitude y APT (Advanced Packaging Tool)?

- **Aptitude** es un gestor de paquetes de alto nivel, mientras que **APT** es de más bajo nivel y puede ser usado por gestores de nivel superior.
  - Aptitude es más inteligente: eliminará automáticamente paquetes no usados o sugerirá la instalación de dependencias.
  - APT solo hace lo que se le indica explícitamente desde la línea de comandos.
- 

## ¿Qué es AppArmor?

Es un sistema de seguridad para Linux que proporciona **Control de Acceso Obligatorio (MAC)**. Permite al administrador del sistema restringir las acciones que los procesos pueden realizar. Está incluido por defecto en Debian. Ejecuta `aa-status` para verificar si está activo.

---

## Reglas de Contraseñas

Para las reglas de contraseñas, se usa una biblioteca de verificación de calidad de contraseñas, y hay dos archivos involucrados:

- `common-password`: establece reglas como uso de mayúsculas, minúsculas, caracteres duplicados, etc.
- `login.defs`: almacena reglas de expiración de contraseñas (por ejemplo, 30 días).

Puedes editarlos con:

```
sudo nano /etc/login.defs  
sudo nano /etc/pam.d/common-password
```

## ¿Qué es LVM?

**Gestor de Volúmenes Lógicos (Logical Volume Manager)** – Nos permite manipular fácilmente las particiones o volúmenes lógicos de un dispositivo de almacenamiento.

## UFW (Uncomplicated Firewall)

UFW es una interfaz para modificar el firewall del dispositivo sin comprometer la seguridad.

Se usa para configurar qué puertos permitir para conexiones y cuáles cerrar. Es útil junto con SSH, ya que puedes definir un puerto específico para su uso.

## ¿Qué es SSH?

SSH o **Secure Shell** es un mecanismo de autenticación entre un cliente y un host.

Usa técnicas de cifrado para que toda la comunicación esté encriptada.

Un usuario en Mac o Linux puede usar SSH desde la terminal para trabajar en su servidor de forma remota.

## ¿Qué es Cron?

**Cron** o un **cron job** es una utilidad de línea de comandos para programar comandos o scripts a intervalos específicos o en una hora determinada cada día.

Es útil, por ejemplo, si quieras que tu servidor se reinicie automáticamente a cierta hora cada día.

- `cd /usr/local/bin` – Para mostrar el script `monitoring.sh`
- `sudo crontab -u root -e` – Para editar los cron jobs
- Cambia el script a:

```
*1 * * * * sleep 30s && [ruta_del_script]
```

Esto lo ejecuta **cada 30 segundos**.

Elimina la línea para dejar de ejecutar el script.

## Comandos de Evaluación para UFW, Grupo, Host, Isblk y SSH

- `sudo ufw status`  
👉 Muestra el estado del firewall (UFW).
- `sudo systemctl status ssh`  
👉 Muestra el estado del servicio SSH (si está activo o no).
- `getent group sudo`  
👉 Verifica si el grupo **sudo** existe y qué usuarios pertenecen a él.
- `getent group user42`  
👉 Verifica si el grupo **user42** existe y qué usuarios pertenecen a él.
- `sudo adduser eval`  
👉 Crea un nuevo usuario con el nombre especificado.
- `sudo groupadd evaluacion`  
👉 Crea un nuevo grupo con el nombre especificado.
- `sudo usermod -aG evaluacion eval`  
👉 Añade un usuario a un grupo (sin quitarlo de otros grupos).
- `sudo chage -l nombre_usuario`  
👉 Muestra las reglas de expiración de contraseña del usuario.
- `hostnamectl`  
👉 Muestra el nombre actual del host (hostname) y otra info del sistema.
- `sudo hostnamectl set-hostname eval42`  
👉 Cambia el nombre del host actual al nuevo.
- **Reinicia tu máquina virtual**  
👉 Necesario para que el nuevo hostname se aplique completamente.

- `sudo nano /etc/hosts`  
👉 Edita el archivo `/etc/hosts` y cambia el nombre del host actual por el nuevo (importante para coherencia interna del sistema).
- `lsblk`  
👉 Muestra las particiones de disco (muy útil para ver si `lvm` está activo).
- `dpkg -l | grep sudo`  
👉 Verifica que el paquete `sudo` está instalado
- `cd /var/log/sudo/`  
👉 Vamos al directorio donde tiene que estar `sudo.log`
- `sudo cat sudo.log`  
👉 Vemos el contenido de `sudo.log`
- `sudo cat /etc/sudoers`  
👉 Vemos el archivo en el que esta configurado el `sudo.log`
- `sudo ufw status numbered`  
👉 Muestra las reglas del firewall con número de índice.
- `sudo ufw allow 8080`  
👉 Permite el acceso al puerto especificado en el firewall.
- `sudo ufw delete "número_de_regla"`  
👉 Elimina una regla del firewall según su número (ver con `status numbered`).
- `ssh jdacal-a@127.0.0.1 -p 2323`  
👉 Conéctate por SSH usando el puerto 2323 para verificar que SSH funciona correctamente en ese puerto.
- `sudo crontab -u root -e`  
👉 Ver el crontab y la regla de ejecución.
- `sudo nano /usr/local/bin/monitoring.sh`  
👉 Para revisar el script de monitoring.
- `sudo visudo`  
👉 Reglas de sudoers.