

PRÁCTICA 1 - LECCIÓN 3 : Rocky + RAID1 + LUKS

Estructura del examen.

Examen práctico con un poco de desarrollo teórico que haremos a mano. Tenemos que venir de casa con dos máquinas (ubuntu y rocky) preconfiguradas porque si no no nos da tiempo. Tenemos que configurar el prompt de usuario con usuario, nombre y apellidos, fecha y la hora. Va a pedir cosas que hemos hecho.

Vamos a tener que entregar capturas de pantalla porque las capturas que tenemos hasta el momento no nos permiten copiar y pegar. Podemos usar cualquier programa en el ordenador anfitrión para hacer capturas. Pero VirtualBox tiene un programa propio

Para no pisar la imagen anterior, hacemos una foto

Comando para ver lista de todos los comandos que se han hecho:

1. history
2. El contenido de este comando se guarda en el archivo
3. Para borrar el history:

```
history -c
```

4. Si el history fuera muy largo, podemos paginarlo:

```
history | more
```

Vamos a configurar una máquina Rocky con RAID1 y cifrado. La hipótesis de trabajo es que en el Bash (directorio) vamos a almacenar info protegida, confidencial, de carácter personal.

Como tenemos que añadir un RAID1 tenemos que añadir dos discos más (como estamos en una instantánea de la máquina virtual, cuando recuperemos los cambios iniciales, los dos discos nuevos que hemos añadido se pierden, junto con toda la configuración que hayamos incluido nueva).

1. lsblk
2. mdadm. Nos dará que no está ese comando. Si alguna vez vamos a instalar un paquete y no lo encontramos: `yum provides mdadm` `yum install mdadm`
3. `mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sdc /dev/sdd`
4. Una vez creado, lo añadimos a un grupo de volúmenes distinto. ¿Porqué en uno distinto? Porque tiene espacio de almacenamiento distintos. Creamos el volume group

```
vgcreate raid1 /dev/md0
```

```
vgdisplay raid1
```

5. Ahora creamos un volumen lógico

```
lvcreate -L 10G -n rvar raid1
```

6. Instalar cryptsetup si no estuviera instalado

7. Hacemos:

Para formateo:

```
cryptsetup luksFormat /dev/raid1/rvar --force-password
```

Y ya estaría el disco cifrado. Para poder usar el disco cifrado, lo primero que hay que hacer es abrirlo:

```
cryptsetup luksOpen /dev/raid1/rvar rvar-open (el nombre vaya)
```

<name> ese campo del campo anterior es el nombre que le va a dar al dispositivo abierto.

```
mkfs.xfs /dev/mapper/rvar-open
```

```
o
```

```
mkfs -t xfs ...
```

```
cd /mnt/
```

```
rm -rf rvar/
```

```
mkdir rvar
```

```
mount /dev/mapper/rvar-open /mnt/rvar
```

```
systemctl isolate
```

```
cd /var
```

```
cp -r rvar/*
```

```
cd ..
```

```
cd /etc/
```

nano fstab y editamos:

```
/dev/mapper/rvar-open /var xfs defaults 00
```

```
more crypttab (te lo crea vacío el archivo)
```

```
blkid (da los identificadores únicos de todos los dispositivos)
```

```
cryptsetup luksUUID /dev/raid1/rvar
```

```
cryptsetup luksUUID /dev/raid1/rvar >> crypttab
```

```
nano crypttab
```

```
rvar-open    UUID=...    none
```

```
comprobar que todo está bien
```

```
reboot
```

```
lsblk
```

```
comprobar que está todo montado
```