Solución 2.3: Montado de un sistema de ficheros con chroot

Descripción de la tarea

En esta práctica se va a hacer uso de una máquina base con debian, la cual va a contar con un usuario y contraseña. La idea es hacer uso de la imagen .iso de otra distribución para poder recuperar el usuario y contraseña en cuestión.

Pasos de la tarea

1. Realiza una instalación desde cero de una máquina virtual con sistema operativo debian y en ella tiene que existir un usuario cuyo nombre sea tu nombre personal.
2. En ajustes de VirtualBox, en la parte de almacenamiento se tendrá que añadir la imagen de otro sistema operativo, en esta práctica se hará uso de una imagen de Kali Linux. Además, hay que tener en cuenta que en el orden de arranque tiene que figurar previamente la opción óptica sobre disco duro.
3. Arrancamos la máquina virtual y debería cargarse como sistema operativo el propio de Kali Linux.
4. En terminal se realizarán los siguientes pasos:
    1. Cambiar a castellano el teclado.

```
┌──(kali㉿kali)-[~]
└─$ setxkbmap es
```

2. Acceder a la consola de root como administrador a través de los permisos configurados con el comando sudo (`/etc/sudoers`, visudo).

```
┌──(kali㉿kali)-[~]
└─$ sudo su -
┌──(root㉿kali)-[~]
└─# whoami
root
```

3. Mostrar el sistema de ficheros montado, es decir, los que está a usar y podemos utilizar en este sistema operativo live debian.

```
┌──(root㉿kali)-[~]
└─# mount
```

4. Lista la tabla de particiones del disco `/dev/sda`.

```
┌──(root㉿kali)-[~]
└─# fdisk -l /dev/sda
Disk /dev/sda: 50 GiB, 53687091200 bytes, 104857600 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x3aa9977a

Device     Boot     Start       End   Sectors  Size Id Type
/dev/sda1  *         2048 102856703 102854656   49G 83 Linux
/dev/sda2       102858750 104855551   1996802  975M  5 Extended
/dev/sda5       102858752 104855551   1996800  975M 82 Linux swap / Solaris
```

5. Crea el directorio `/mnt/recuperar`.

```
┌──(root㉿kali)-[~]
└─# mkdir /mnt/recuperar && ls -l /mnt
total 0
drwxr-xr-x 2 root root 40 May  2 15:55 recuperar
```

6. Monta la partición 1 del disco duro `/dev/sda` en el directorio del sistema operativo creado en el paso anterior `/mnt/recuperar` en la máquina live. Con la opción *-t auto* solicitamos al comando mount la autodetección del sistema de ficheros montado. Podemos ver este sistema de ficheros con el comando *lsblk -f*.

```
┌──(root㉿kali)-[~]
└─# mount -t auto /dev/sda1 /mnt/recuperar
┌──(root㉿kali)-[~]
└─# df -Th | grep sda1
/dev/sda1      ext4       48G  5.3G   41G  12% /mnt/recuperar
```

Nota: El parámetro `-t auto` le indica al sistema que detecte automáticamente el tipo de sistema de archivos (ext4, NTFS, FAT32, etc.) que tiene la partición /dev/sda1.

7. Monta el directorio `/dev` dentro de la ruta `/mnt/recuperar/dev` para poder tener acceso a todos los dispositivos reconocidos por la distribución live.

```
┌──(root㉿kali)-[~]
└─# mount --bind /dev /mnt/recuperar/dev
```

Nota: Es importante tener en cuenta que *--bind* permite hacer uso del mismo sistema de ficheros en dos lugares diferentes. Por ejemplo, `/dev` puede ser empleado en `/dev` y `/mnt/recuperar/dev`.

8. Monta el directorio `/proc` dentro de `/mnt/recuperar/proc` para poder tener acceso a los procesos del sistema y kernel de kali linux gracias a la distribución live.

```
┌──(root㉿kali)-[~]
└─# mount --bind /proc /mnt/recuperar/proc
```

9. Monta el directorio `/sys` dentro de `/mnt/recuperar/sys` para poder tener acceso al hardware y kernel de kali linux gracias a la distribución live.

```
┌──(root㉿kali)-[~]
└─# mount --bind /sys /mnt/recuperar/sys
```

10. Creamos una jaula mediante el comando *chroot*. Con este comando creamos una jaula, es decir, un entorno cerrado para la distribución Linux que vamos a recuperar, de tal modo que, una vez dentro de la jaula, sólo existe ésta. Por este motivo, al modificar el directirio `/` a `/mnt/recuperar` sólo existe la distribución Linux instalada en el disco duro /dev/sda que queremos recuperar, ya no estamos trabajando en la Live sino en el propio sistema Debian.

```
┌──(root㉿kali)-[~]
└─# chroot /mnt/recuperar /bin/bash
root@kali:/# passwd usuario
New password:
Retype new password:
passwd: password updated successfully
root@kali:/# exit
exit

┌──(root㉿kali)-[~]
└─#
```

11. Desmonta los directorios anteriormente montados para la recuperación del sistema, es decir, `/mnt/recuperar/dev`, `/mnt/recuperar/proc`, `/mnt/recuperar/sys` y `/mnt/recuperar`.

```
┌──(root㉿kali)-[~]
└─# umount /mnt/recuperar/dev /mnt/recuperar/proc /mnt/recuperar/sys
/mnt/recuperar
```

12. Apaga la máquina, en configuración elimina la .iso de la live y accede al sistema nuevamente.

```
┌──(root㉿kali)-[~]
└─# init 0
```