

Dealing With Slack Space



- Anti-Forensics

Encrypting all temp folders and logs with a random password on boot

What?



When you use a sudo command it gets logged in the auth log file.

So if you are trying to do something like get into a hidden filesystem that has special properties like a seed for the pass the logs would allow them to find that information...

Here is a line from my logs...

```
Sep  2 10:31:24 KensLinux sudo: kenthefurry : TTY=pts/0 ; PWD=/tmp0 ;  
USER=root ; COMMAND=/sbin/losetup /dev/loop3 CD.iso
```

```
Sep  2 10:31:39 KensLinux sudo: kenthefurry : TTY=pts/0 ; PWD=/tmp0 ;  
USER=root ; COMMAND=/sbin/cryptsetup create One /dev/loop3 -d  
/dev/urandom
```

What?



That is bad because anything that can help an examiner nail you roll of quarters is not something you want to leave out in the open, let alone easily searchable on your harddrive.

That log line alone would tell PWD=the current directory the command was used in and the CD.iso with no exact location tells it is PWD+CD.iso so the CD.iso is located in /tmp0/CD.iso.

Tutorial





First things first, we need to take care of the temp files. The easiest way to do this is to create a 10G or so data file and use it as a disk to hold all of our tmp files and logs in.

To do this lets open a Terminal (Ctrl+Alt+T), and now to make things easier we will log into the root account.

```
sudo su
```

Now we need to make a folder to hold the data file, I would make the folder in the root folder / and add a period in front of it so you don't see the folder normally.

```
cd /
```

```
mkdir .Private
```

Now lets make the data file.

```
dd if=/dev/zero of=TMP bs=1M count=10240
```



Now we need to fill that file with random data.

```
losetup /dev/loop3 TMP
cryptsetup create One /dev/loop3 -d /dev/urandom
badblocks -swt random /dev/mapper/One
cryptsetup remove One
losetup /dev/loop3 -d
losetup /dev/loop3 /dev/null
```

Now we need to make a crypttab entry so we can make sure the cryptdisks will work.

```
nano /etc/crypttab
```

Add this line...

```
TMP /.Private/TMP /dev/urandom cipher=aes-cbc-essiv:sha256,hash=sha256,tmp
```

- Now reboot so we can make sure it will create the disk correctly; re-open a terminal and re-sudo su.

Now lets see if TMP is in the mapper file

```
ls /dev/mapper/
```

- In there there should be TMP among the list.



Now that we know the disk will be made on boot we need to mount it to the tmp folder.

So lets edit the fstab file.

```
nano /etc/fstab
```

add these lines...

```
/dev/mapper/TMP /tmp etc2 defaults 0 0
```

```
/tmp /var/tmp none bind 0 0
```

```
/tmp /var/log none bind 0 0
```

Now reboot, your boot will be a little bit slower but it will work.

Check your mount

```
mount
```

You should see all the right mount files.

Dealing With Slack Space



The End

By KenTheFurry

Email: KenTheFurry@gmail.com

GPG: 068ACDD2