chroot to other linux drive from img

┌──(root NaruZKurai)-[~]
└─# mmls flag_drive.img

```
mmls flag_drive.img
```

```
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0000206847   0000204800   Linux (0x83)
003:  000:001   0000206848   0000411647   0000204800   Linux Swap / Solaris x86 (0x82)
004:  000:002   0000411648   0000819199   0000407552   Linux (0x83)
```

┌──(root NaruZKurai)-[~]
└─#

```
sudo mkdir /mnt/flag_drive
```

```
sudo mount -o loop,offset=$((2048*512)) flag_drive.img /mnt/flag_drive #Linux (0x83) is after offset 2047 *512 bytes  so 2048
```

```
sudo mount -t proc /proc /mnt/flag_drive/proc
```

```
sudo mount -o bind /sys /mnt/flag_drive/sys
```

```
sudo mount -o bind /dev /mnt/flag_drive/dev
```

```
sudo chroot /mnt/flag_drive #possibly need to add /bin/bash or /bin/sh or depending on the operating system fish or ash or whatever else that system uses. look in /bin/ to see what shell it uses
```

#and just coz im hella forgetfull

```
find / -type f -name "*words*" 2>/dev/null
```

#im serious super forgetfull

```
grep -R "picoCTF{" / 2>/dev/null
```

Revision #6
Created 2024-05-08 20:08:14 UTC by naruzkurai
Updated 2024-05-09 03:21:21 UTC by naruzkurai