Zombie

Writeup by Speer
Category: Miscellaneous

Author: JohnHammond

Description

Oh, shoot, I could have sworn there was a flag here. Maybe it's still alive out there?

Upon connecting to the remote host it appears empty. There are no obvious files to interact with. I run `ps axo` as I suspect the challenge title is referencing zombie processes.

```
user@zombie:~$ ps axo
PID   USER     TIME   COMMAND
    1 root       0:00 /usr/sbin/sshd -D -e
    8 root       0:00 sshd: user [priv]
   10 user       0:00 sshd: user@pts/0
   11 user       0:00 {.user-entrypoin} /bin/bash /home/user/.user-entrypoint.sh
   12 user       0:00 tail -f /home/user/flag.txt
   14 user       0:00 bash -i
   17 user       0:00 ps axo
```

I take a look at the `.user-entrypoint.sh` file to see what is happening when I connect:

```bash
user@zombie:~$ cat .user-entrypoint.sh
#!/bin/bash

nohup tail -f /home/user/flag.txt >/dev/null 2>&1 & # disown

rm -f /home/user/flag.txt 2>&1 >/dev/null

bash -i
```

I read up on `nohup` https://en.wikipedia.org/wiki/Nohup

I also checked out the `/proc` of the command

```bash
user@zombie:~$ cat /proc/12/status
Name: tail
Umask:  0022
State:  S (sleeping)
...
```

I looked at the `fd` folder which holds the file descriptors for the process. It contains symbolic links to I/O of the process and also the specific files/resources that are open with that process.

```
 user@zombie:/proc/11/fd$ ls -la
total 0
dr-x------    2 user     user            0 Jun 19 02:51 .
dr-xr-xr-x    9 user     user            0 Jun 19 02:51 ..
lr-x------    1 user     user           64 Jun 19 02:51 0 ->
/dev/null
l-wx------    1 user     user           64 Jun 19 02:51 1 ->
/dev/null
l-wx------    1 user     user           64 Jun 19 02:51 2 ->
/dev/null
lr-x------    1 user     user           64 Jun 19 02:51 3 ->
/home/user/flag.txt (deleted)

user@zombie:/proc/11/fd$ cat 3
flag{6387e800943b0b468c2622ff858bf744}
```