

LinkedIn: [Kelvin Kimotho](#)

# Magikarp Ground Mission



Easy

General Skills

picoCTF 2021

AUTHOR: SYREAL

## Description

Do you know how to move between directories and read files in the shell? Start the container, `ssh` to it, and then `ls` once connected to begin. Login via `ssh` as `ctf-player` with the password, `a13b7f9d`

### CHALLENGE

### ENDPOINTS

SSH

```
ssh ctf-player@venus.picoctf.net  
-p 51205
```

This challenge launches an instance on demand.

Its current status is:

**RUNNING**

Instance Time Remaining:

**59:27**

Restart  
Instance

### Hints

1

Finding a cheatsheet for bash would be really helpful!

## Solution

I accessed the given machine via ssh from my kali machine.

```
(kali@kali)~[~/Desktop]
$ sudo ssh ctf-player@venus.picoctf.net -p 51205
The authenticity of host 'venus.picoctf.net' (3.131.124.143):51205 can't be established.
ED25519 key fingerprint is SHA256:P1f6h9SBfSVnJbm2AKhphfHhGEyAeTh1b/rN/AwKs24.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'venus.picoctf.net':51205 (ED25519) to the list of known hosts.
ctf-player@venus.picoctf.net's password:
Permission denied, please try again.
ctf-player@venus.picoctf.net's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1041-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ctf-player@pico-chall$
```

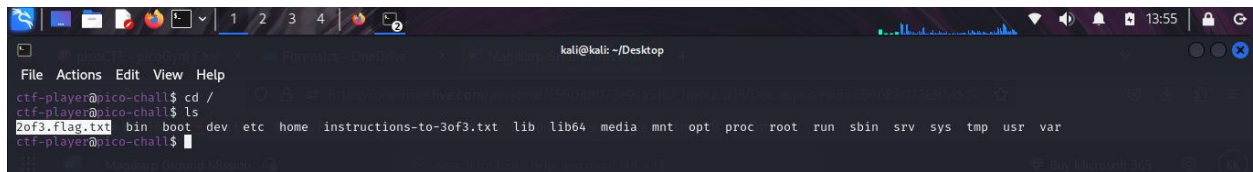
After a successful login, I began navigating the file system using commands like `cd` to navigate directories, `ls` to list files in directories, etc.

```
ctf-player@pico-chall$ ls
1of3.flag.txt  instructions-to-2of3.txt
ctf-player@pico-chall$
```

I found two text files and used `cat` command to view their contents. Using `cat` command I viewed their contents, One had a fragment of the flag 'picoCTF{xxsh\_' and the other one had instruction to find the missing fragment.

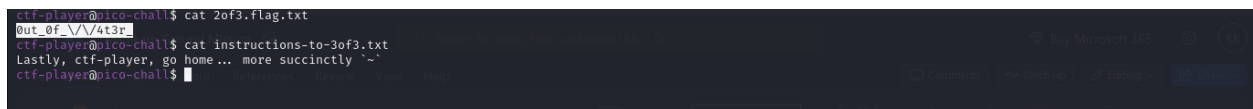
```
ctf-player@pico-chall$ cat 1of3.flag.txt
picoCTF{xxsh_
ctf-player@pico-chall$ cat instructions-to-2of3.txt
1of3.flag.txt
ctf-player@pico-chall$ cat instructions-to-2of3.txt
Next, go to the root of all things, more succinctly '/'
ctf-player@pico-chall$
```

I used `cd` command to move to the root directory '`cd /`' then `ls` command listing all the files in there. I discovered to user created text files.

A terminal window on a Kali Linux desktop. The prompt is ctf-player@pico-chall. The user has run 'cd /' and 'ls', showing a list of system directories. The file 2of3.flag.txt is highlighted in the terminal output.

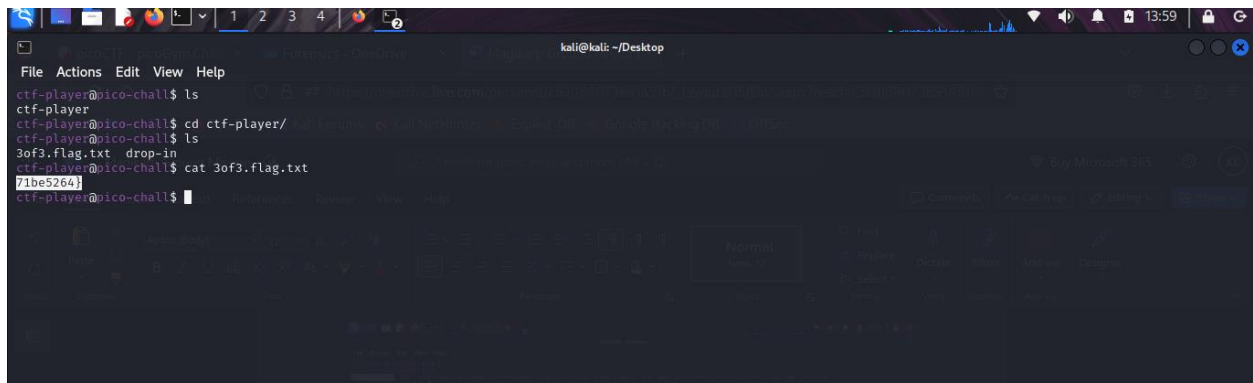
```
ctf-player@pico-chall$ cd /
ctf-player@pico-chall$ ls
2of3.flag.txt  bin  boot  dev  etc  home  instructions-to-3of3.txt  lib  lib64  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
ctf-player@pico-chall$
```

One had the second flag fragment ' **Out\_Of\_//4t3r\_** ' while the other gave me instruction to find the last flag fragment.

A terminal window showing the user running 'cat 2of3.flag.txt' and 'cat instructions-to-3of3.txt'. The output shows the flag fragment 'Out\_Of\_//4t3r\_' and a message to go home.

```
ctf-player@pico-chall$ cat 2of3.flag.txt
Out_Of_//4t3r_
ctf-player@pico-chall$ cat instructions-to-3of3.txt
Lastly, ctf-player, go home... more succinctly '~'
ctf-player@pico-chall$
```

I navigated to home directory where i found the last flag fragment ' **71be5264}**'.

A terminal window showing the user navigating to their home directory and listing files. The file 71be5264 is highlighted. Below the terminal, a file explorer window shows the contents of the home directory, including the file 71be5264.

```
ctf-player@pico-chall$ ls
ctf-player
ctf-player@pico-chall$ cd ctf-player/
ctf-player@pico-chall$ ls
3of3.flag.txt  drop-in
ctf-player@pico-chall$ cat 3of3.flag.txt
71be5264}
ctf-player@pico-chall$
```

I combined the flag fragments and this was the final flag  
**picoCTF{xxsh\_out\_Of\_//4t3r\_71be5264}**.