

UNTANGLING USERS

Becoming the root with su

In this challenge, we need to use `su` to switch our user to `root`. `su` asks for the root password which in this case is `hack-the-planet`. After becoming `root` user, the flag can be read using `cat /flag` and it is

```
pwn.college{Uc4CnLabI_F-UfSevHjQ0TO3wQe.dVTN0UDL3YjN0czW}
```

Other users with su

In this challenge, we need to switch to the user `zardus` instead. This can be done with `su zardus` and the password is `dont-hack-me`. Now `/challenge/run` gives the flag: `pwn.college{ok1rWXs56pgTeYKA5UCZYBt3pHt.dZTN0UDL3YjN0czW}`

Cracking passwords

A leak of `/etc/shadow` exists in `/challenge/shadow-leak`. It can be cracked using `john /challenge/shadow-leak` which gives the following output:

```
Created directory: /home/hacker/.john
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:11 0% 2/3 0g/s 257.7p/s 257.7c/s 257.7C/s 123456
0g 0:00:00:12 0% 2/3 0g/s 259.3p/s 259.3c/s 259.3C/s lacrosse..pumpkin
0g 0:00:00:16 0% 2/3 0g/s 265.4p/s 265.4c/s 265.4C/s deedee..grizzly
0g 0:00:00:20 1% 2/3 0g/s 269.3p/s 269.3c/s 269.3C/s ncc1701d..1022
aardvark (zardus)
1g 0:00:00:21 100% 2/3 0.04636g/s 269.9p/s 269.9c/s 269.9C/s Johnson..buzz
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Now you can use the password `aardvark` with `su zardus /challenge/run` gives the flag:

```
pwn.college{wbnRUeEVK6Iyf3Wwz3kxOvmx_F9.ddTN0UDL3YjN0czW}
```

Using sudo

We cannot run `cat /flag` since we do not have superuser permission.

Since we have `sudo` permission, `sudo cat /flag` works and gives the flag: `pwn.college{IywhJmTTg9bXLreExGlwjq_033y.dhTN0UDL3YjN0czW}`