level01

In the first level, we unearthed clues for level01:

```
level00@SnowCrash:~$ cat /etc/passwd/
...
flag01:42hDRfypTqqnw:3001:3001::/home/flag/flag01:/bin/bash
...
```

We gave a shot at using the hash as a key, but obviously it wasn't that simple. Digging around for hash cracking tools, we bumped into "John the Ripper".
Funny enough, in the previous level, our flag was chilling inside a file named "john" - talk about a nudge in the right direction, right? :-)
After giving John a try, we figured out it's a DES hash. Good thing John's got a built-in dictionary with many common passwords.

```
level01@SnowCrash:~$ echo 42hDRfypTqqnw > hash.txt

level01@SnowCrash:~$ john hash.txt
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 128/128 SSE2-16])
No password hashes left to crack (see FAQ)
```

John cracked the password instantly, yet the terminal displayed no result.
The decrypted password is stored in a separate file.

```
level01@SnowCrash:~$ cat ~/.john/john.pot
42hDRfypTqqnw:abcdefg

level01@SnowCrash:~$ su flag01
Password: abcdefg
Don't forget to launch getflag !

flag01@SnowCrash:~$ getflag
Check flag.Here is your token : f2av5il02puano7naaf6adaaf

flag01@SnowCrash:~$ su level02
Password: f2av5il02puano7naaf6adaaf

level02@SnowCrash:~$
```