Level01

Due to the lack of any content in the `level01` user's home directory we proceed to doing a bit of basic enumeration and we can observe that the `/etc/passwd` file contains a **hashed password**.

```
level01@SnowCrash:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
... SNIP ...
flag00:x:3000:3000::/home/flag/flag00:/bin/bash
flag01:42hDRfypTqqnw:3001:3001::/home/flag/flag01:/bin/bash
flag02:x:3002:3002::/home/flag/flag02:/bin/bash
... SNIP ...
```

/etc/passwd file

The `/etc/passwd` file is a critical file on a unix system. It is world readable by default and stores important information of the users on each line. These lines contain **7 fields** separated by a `:` wich are the following:

- **Username**
- **Password**
- **User ID (UID)**
- **Group ID (GID)**
- **User ID Info (GECOS)**
- **Home directory**
- **Login shell**

The password field stores the password of the user. The `x` character indicates the password is stored in `/etc/shadow` file in the encrypted format. Many years ago, the password hash was stored in the `/etc/password` file wich leads to a major vulnerability if readable by unprivileged users.

Crack the hash with John

It is possible to use a tool for password cracking. **John the ripper** is one of them and can conduct a **wordlist attack** (among others) against our hashed password. For a basic usage, we simply need to supply a wordlist with the `-w=<wordlist>` option and hashed password in a file to `john`.

```
┌──(kali㉿kali)-[~]
└─$ echo 42hDRfypTqqnw > level01.txt
┌──(kali㉿kali)-[~]
```

```
└─$ john -w=/usr/share/wordlists/rockyou.txt level01.txt
Using default input encoding: UTF-8
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 256/256 AVX2])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
abcdefg          (?)
1g 0:00:00:00 DONE (2023-01-03 08:41) 20.00g/s 245760p/s 245760c/s 245760C/s
123456..frenchie
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

The password found is `abcdefg` and lets us login as the `flag01` user to launch the `getflag` command.

```
level01@SnowCrash:~$ su flag01
Password:
Don't forget to launch getflag !
flag01@SnowCrash:~$ getflag
Check flag.Here is your token : f2av5il02puano7naaf6adaaf
```