

Create 6 users in your Linux Terminal, then set the password for each user that meets the following complexity requirement respectively. You should list the passwords created for each user.

- a. For user1, the password should be a simple directory word (all lowercase)

```
(student@kali.example.com)-[~]
└─$ sudo useradd user1

(student@kali.example.com)-[~]
└─$ sudo passwd user1
New password:
Retype new password:
passwd: password updated successfully
```

Password: eternal

- b. For user2, the password should consist of 4 digits

```
(student@kali.example.com)-[~]
└─$ sudo useradd user2

(student@kali.example.com)-[~]
└─$ sudo passwd user2
New password:
Retype new password:
passwd: password updated successfully
```

Password: 1234

- c. For user3, the password should consist of a simple dictionary word of any length characters (all lowercase) + digits

```
(student@kali.example.com)-[~]
└─$ sudo useradd user3

(student@kali.example.com)-[~]
└─$ sudo passwd user3
New password:
Retype new password:
passwd: password updated successfully
```

Password: patch123

- d. For user4, the password should consist of a simple dictionary word characters (all lowercase) + digits + symbols

```
(student@kali.example.com)-[~]
└─$ sudo useradd user4

(student@kali.example.com)-[~]
└─$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully
```

Password: science123!

- e. For user5, the password should consist of a simple dictionary word (all lowercase) + digits

```
(student@kali.example.com)-[~]
└─$ sudo useradd user5

(student@kali.example.com)-[~]
└─$ sudo passwd user5
New password:
Retype new password:
passwd: password updated successfully
```

Password: night987

- f. For user6, the password should consist of a simple dictionary word (with a combination of lower and upper case) + digits + symbols

```
(student@kali.example.com)-[~]
└─$ sudo useradd user6

(student@kali.example.com)-[~]
└─$ sudo passwd user6
New password:
Retype new password:
passwd: password updated successfully
```

Password: Tr0ubl3!

Export above users' hashes into a file named xxx.hash (xxx = MIDAS ID) and use John the Ripper tool to crack their passwords in wordlist mode (use rockyou.txt) Keep your john the ripper cracking for 10 minutes. How many words have been successfully cracked

```

(student@kali.example.com)-[~]
└─$ ls -l
total 136692
drwxr-xr-x 2 student student      4096 Sep 18 21:57 Desktop
drwxr-xr-x 2 student cyseteam     4096 Sep 18 21:57 Documents
drwxr-xr-x 2 student student      4096 Sep 18 21:57 Downloads
drwxr-xr-x 2 student student      4096 Sep 18 21:57 Music
drwxr-xr-x 2 student cyseteam     4096 Sep 18 21:57 Pictures
drwxr-xr-x 2 student student      4096 Sep 18 21:57 Public
drwxr-xr-x 2 student cyseteam     4096 Sep 18 21:57 Templates
drwxr-xr-x 2 student student      4096 Sep 18 21:57 Videos
-rw-r--r-- 1 student cyseteam     5488 Sep 26 21:57 copyright_cyse270
-rwxr-xr-x 1 student cyseteam         0 Oct  8 19:46 display.sh
-rwxr-xr-x 1 student cyseteam         0 Oct  8 19:41 example_file
-rw-rw-r-- 1 Travis travismedia    0 Sep 24 19:42 fruit.txt
-rw-r--r-- 1 student cyseteam         0 Oct  9 23:48 ihenr002.hash
-rw-rw-r-- 1 student      5000         0 Sep 24 19:49 invoice.txt
-rw-r--r-- 1 student cyseteam 139921507 Oct  9 23:21 rockyou.txt
-rw-r----- 1 root      root         2645 Oct  9 23:39 shadow
-rw-r--r-- 1 student cyseteam     2023 Oct  3 19:53 test.txt
drwx----- 1 student cyseteam         0 Oct  9 23:16 thinclient_drives

(student@kali.example.com)-[~]
└─$ sudo cat shadow > ihenr002.hash

```

```

(student@kali.example.com)-[~]
└─$ sudo john --format=crypt ihenr002.hash --wordlist=/home/student/rockyou.txt
Using default input encoding: UTF-8
Loaded 12 password hashes with 12 different salts (crypt, generic crypt(3) [?/64
])
Remaining 9 password hashes with 9 different salts
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha51
2crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1234          (user2)
eternal       (user1)

```