Task A - Password Cracking

1. 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.

1. For user1, the password should be a simple dictionary word (all lowercase)

```
giancarlo@giancarlo-VirtualBox:~$ sudo useradd user1
[sudo] password for giancarlo:
useradd: user 'user1' already exists
giancarlo@giancarlo-VirtualBox:~$ sudo passwd user1
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a diction
ary word
Retype new password:
passwd: password updated successfully
giancarlo@giancarlo-VirtualBox:~$
```

Password: lower

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

```
giancarlo@giancarlo-VirtualBox:~$ sudo useradd user2
giancarlo@giancarlo-VirtualBox:~$ sudo passwd user2
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: password updated successfully
giancarlo@giancarlo-VirtualBox:~$
```

Password: 0000

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

```
giancarlo@giancarlo-VirtualBox:~$ sudo useradd user3
giancarlo@giancarlo-VirtualBox:~$ sudo passwd user3
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a diction
ary word
Retype new password:
passwd: password updated successfully
giancarlo@giancarlo-VirtualBox:~$
```

Password: lowercase333

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

```
giancarlo@giancarlo-VirtualBox:~$ sudo useradd user4
giancarlo@giancarlo-VirtualBox:~$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully
giancarlo@giancarlo-VirtualBox:~$
```

Password: car000!$

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

```
giancarlo@giancarlo-VirtualBox:~$ sudo passwd user5
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a diction
ary word
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a diction
ary word
Retype new password:
passwd: password updated successfully
giancarlo@giancarlo-VirtualBox:~$
```

Password: password123

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

```
giancarlo@giancarlo-VirtualBox:~$ sudo useradd user6
giancarlo@giancarlo-VirtualBox:~$ sudo passwd user6
New password:
Retype new password:
passwd: password updated successfully
giancarlo@giancarlo-VirtualBox:~$
```

Password: DictionarY369!$

2. Export above users' hashes into a file named xxx.hash (replace xxx with your MIDAS) and use John the Ripper tool to crack their passwords in wordlist mode (use rockyou.txt). [40 points]

```
giancarlo@giancarlo-VirtualBox:~$ sudo nano /etc/pam.d/common-password
giancarlo@giancarlo-VirtualBox:~$ sudo passwd user1
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
giancarlo@giancarlo-VirtualBox:~$ sudo tail -1 /etc/shadow > goble001.hash
giancarlo@giancarlo-VirtualBox:~$ cat goble001.hash
user6:$y$j9T$ojPUF/jIvlr2pxg4s4RNA.$bzlFGV2cKxwCxHjCf5oOM9ki57u9gf/qIY/3w6Lwx38:19661:0:99999:7:::
giancarlo@giancarlo-VirtualBox:~$ john --wordlist=rockyou.txt goble001.hash
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [0:unknown 1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt 7:scrypt 10:yescrypt 11:gost-yesc
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Crash recovery file is locked (maybe use "--session"): /home/giancarlo/snap/john-the-ripper/610/.john/john.rec
giancarlo@giancarlo-VirtualBox:~$ john --show goble001.hash
0 password hashes cracked, 1 left
```

3. Keep your john the ripper cracking for 10 minutes. How many passwords have been successfully cracked?

Extra credit (10 points):
Find and use the proper format in John the ripper to crack the following MD5 hash. Show your steps and results.

- 5f4dcc3b5aa765d61d8327deb882cf99
- 63a9f0ea7bb98050796b649e85481845