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. [6 * 5 = 30 points].

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

2. For user2, the password should consist of 4 digits.(6798)

3. For user3, the password should consist of a simple dictionary word of any length characters (all lowercase) + digits.(guy68)

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

5. For user5, the password should consist of a simple dictionary word (all lowercase) + digits.(frown69)

6. For user6, the password should consist of a simple dictionary word (with a combination of lower and upper case) + digits + symbols. (LoveS89!@)

```
┌──(damis001㉿kali)-[~]
└─$ sudo useradd Jessi

┌──(damis001㉿kali)-[~]
└─$ sudo passwd Jessi
New password:
Retype new password:
passwd: password updated successfully
```

```
┌──(damis001㉿kali)-[~]
└─$ sudo useradd Bill

┌──(damis001㉿kali)-[~]
└─$ sudo passwd Bill
New password:
Retype new password:
passwd: password updated successfully
```

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

```
┌──(damis001㉿kali)-[~]
└─$ sudo cp /etc/shadow /home/damis001/
```

```
┌──(damis001㉿kali)-[~]
└─$ sudo cat shadow > damis001.hash
```

3) Keep your john the ripper cracking for 10 minutes. How many passwords have been successfully cracked? [30 points. 0 passwords cracked

```
┌──(damis001㉿kali)-[~]
└─$ sudo john --format=crypt damis001.hash --wordlist=/home/damis001/rockyo
u.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?
/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:
sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
fopen: /home/damis001/rockyou.txt: No such file or directory
```