1. Create 6 users in your Linux system, then assign each user a password that meets the following
complexity requirement respectively. You should list the passwords created for each user. [6 * 5 = 30
points]
1. A simple dictionary word (all lowercase) **coke - car**
2. 4-character digits pepsi - 1234
3. A simple dictionary word (all lowercase) + digits **beer - happy156**
4. A simple dictionary word (all lowercase) + digits +symbols **accounting12!**
5. A simple dictionary word (all lowercase) + digits jasper **RUN15**
6. A simple dictionary word (w. a mix of lower and upper case) + digits +symbols level6 - **TeachER12#$**

Sudo useradd -m to create an account
Sudo passwd account name to set a password for account

```
└─$ sudo tail -6 /etc/shadow
coke:$y$j9T$gYSsEtHb.DEK1OjffPdyd1$hxXAnI12jlVEB6oP.bFhadvxoercjpOs94aqJSG7KM.:19403:0:99999:7:::
pepsi:$y$j9T$NHC3E2f5N1pc2k2gBn4E7/$fN9EsWdZVJFImjaNdtemhLmBHWLhqRBjlkeEchc8wU8:19403:0:99999:7::
:
beer:$y$j9T$TX/NBFCTt8AlwxKof/ntE/$ZNIZUUk8eTfKk8jJPlNviNGpVCHwAbX3bQDnBxjhqt9:19403:0:99999:7:::
catdog:$y$j9T$dTYNRG6YoVpBKLQXcgdlB0$7F7m5MIXKvfwgft/2Ckk0D6Y0CLFkZcaaPZLFqy7e.3:19403:0:99999:7:
::
jasper:$y$j9T$W4aCK9b5sI1/lF3us5X8/.$fd7NKp/WfBxU7BEVEVe83VozDWjFrOuIWlyGhhgw7P3:19403:0:99999:7:
::
level6:$y$j9T$R0Qmp31bJNxHqTpqteaSf1$ENsqhA8l2WdQKN.5zkeP7/3LAdNlYeRqgpmH6qi5o1A:19403:0:99999:7:
::
```

Remember, do not use the passwords for your real-world accounts.

2. Export above users' hash into a file named xxx.hash (replace xxx with your MIDAS ID) and use John the Ripper to crack their passwords in wordlist mode (use rockyou.txt). [40 points]
Copied the user and password from the screenshot above to bpear003.hash by highlighting and pasting it into the document.
Used sudo john --format=crypt bpear003.hash --wordlist=rockyou.txt
To have john try to crack the passwords in the hashfilek
3. Keep your john the ripper cracking for at least 10 minutes. How many passwords have been successfully cracked? [30 points]

```
┌──(brandon㉿PearsonKali)-[~]
└─$ sudo john --format=crypt bpear003.hash --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
```

After 10 minutes it was only able to crack the pepsi account password 1234. It cracked that password right away pretty much.
I left the computer going for a while it fell asleep so don't have the screenshot of the password being cracked.

Extra credit (10 points):

1. Find and use the proper format in John the ripper to crack the following MD5 hash. Show your
steps and results.
• 5f4dcc3b5aa765d61d8327deb882cf99 password
• 63a9f0ea7bb98050796b649e85481845 root

Type the hashes into a file using vi editor
Then used john --format=raw=md5 to crack the password
Had to do it twice bc didn't type the hash in correctly for the second hash.

```
┌──(brandon㉿PearsonKali)-[~]
└─$ sudo john --format=raw-md5 extracredit.txt --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
1g 0:00:00:00 DONE (2023-02-14 21:08) 33.33g/s 12800p/s 12800c/s 12800C/s 123456..michael1
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

```
┌──(brandon㉿PearsonKali)-[~]
└─$ sudo john --format=raw-md5 --wordlist=rockyou.txt extracredit.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
root             (?)
1g 0:00:00:00 DONE (2023-02-14 21:11) 16.66g/s 13452Kp/s 13452Kc/s 13452KC/s rory17..ronald918
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```