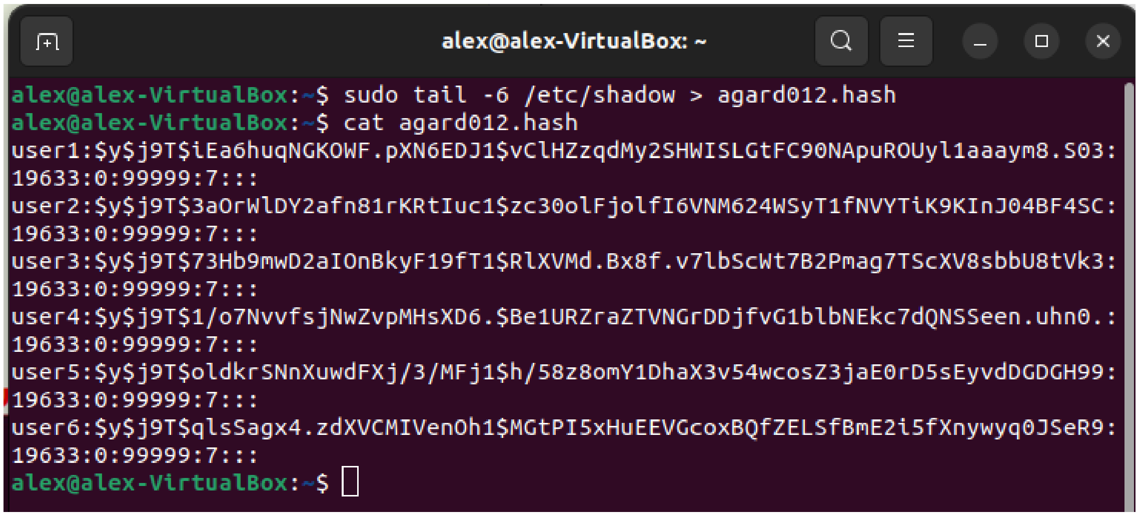
Assignment 5 – CYSE 270

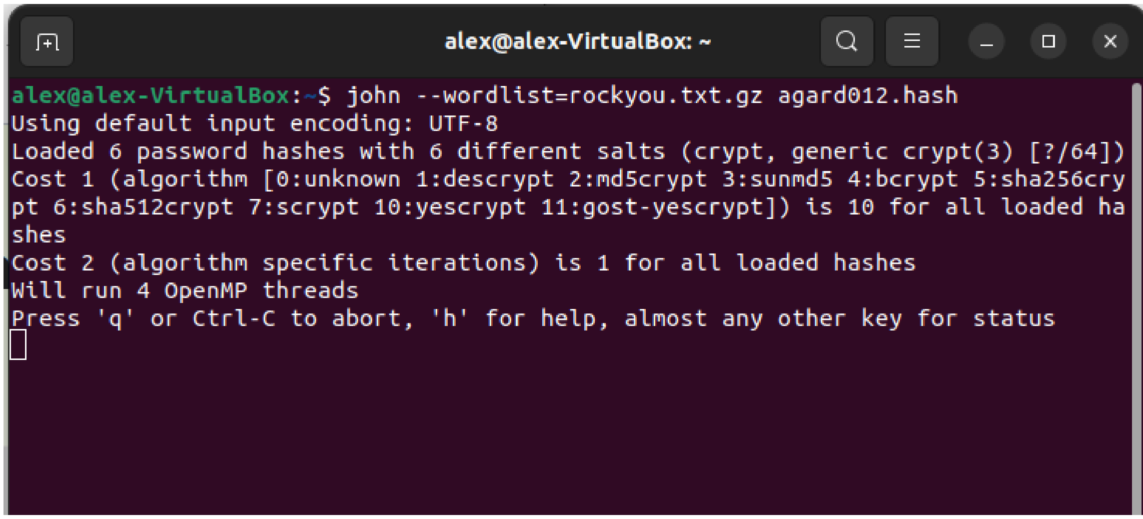
1.Create 6 users in your Linux Terminal, then set the password for each user that meets the following complexity requirement respectively. You should list the passwords created for each user. **I used the sudo useradd "user1" and then created the passwords using sudo passwd**

1. word
2. 1234
3. word1234
4. word1234!
5. words12345
6. WordS123!

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).

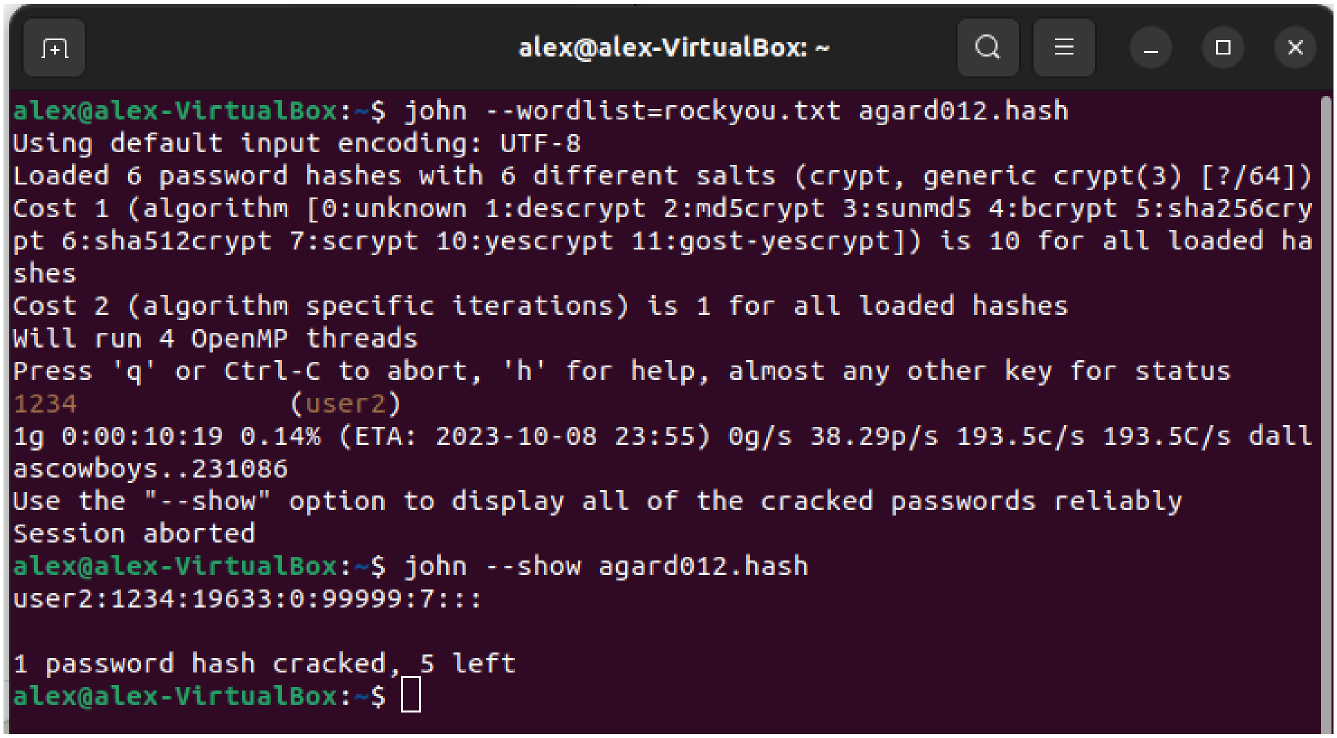


```
alex@alex-VirtualBox:~$ sudo tail -6 /etc/shadow > agard012.hash
alex@alex-VirtualBox:~$ cat agard012.hash
user1:$y$j9T$iEa6huqNGKOWF.pXN6EDJ1$vClHZzqdMy2SHWISLGtFC90NApuROUyl1aaaym8.S03:
19633:0:99999:7:::
user2:$y$j9T$3aOrWlDY2afn81rKRtIuc1$zc30olFjolfI6VNM624WSyT1fNVYTiK9KInJ04BF4SC:
19633:0:99999:7:::
user3:$y$j9T$73Hb9mwD2aIOnBkyF19fT1$RlXVMd.Bx8f.v7lbScWt7B2Pmag7TScXV8sbbU8tVk3:
19633:0:99999:7:::
user4:$y$j9T$1/o7NvvfsjNwZvpMHsXD6.$Be1URZraZTVNGrDDjfvG1blbNEkc7dQNSSeen.uhn0.:
19633:0:99999:7:::
user5:$y$j9T$oldkrSNnXuwdFXj/3/MFj1$h/58z8omY1DhaX3v54wcosZ3jaE0rD5sEyvdDGDGH99:
19633:0:99999:7:::
user6:$y$j9T$qlsSagx4.zdXVCMIVenOh1$MGtPI5xHuEEVGcoxBQfZELSfBmE2i5fXnywyq0JSeR9:
19633:0:99999:7:::
alex@alex-VirtualBox:~$
```



```
alex@alex-VirtualBox:~$ john --wordlist=rockyou.txt.gz agard012.hash
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [0:unknown 1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256cry
pt 6:sha512crypt 7:scrypt 10:yescrypt 11:gost-yescrypt]) is 10 for all loaded ha
shes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
```

3. Keep your john the ripper cracking for 10 minutes. How many passwords have been successfully cracked? **1**



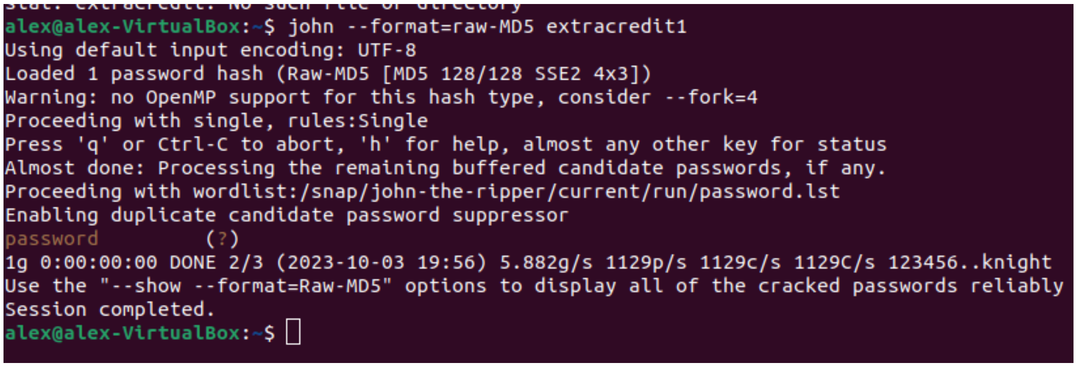
```
alex@alex-VirtualBox:~$ john --wordlist=rockyou.txt agard012.hash
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [0:unknown 1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256cry
pt 6:sha512crypt 7:scrypt 10:yescrypt 11:gost-yescrypt]) is 10 for all loaded ha
shes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
1234             (user2)
1g 0:00:10:19 0.14% (ETA: 2023-10-08 23:55) 0g/s 38.29p/s 193.5c/s 193.5C/s dall
ascowboys..231086
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
alex@alex-VirtualBox:~$ john --show agard012.hash
user2:1234:19633:0:99999:7:::

1 password hash cracked, 5 left
alex@alex-VirtualBox:~$ 
```

4. Find and use the proper format in John the ripper to crack the following MD5 hash. Show your steps and results.

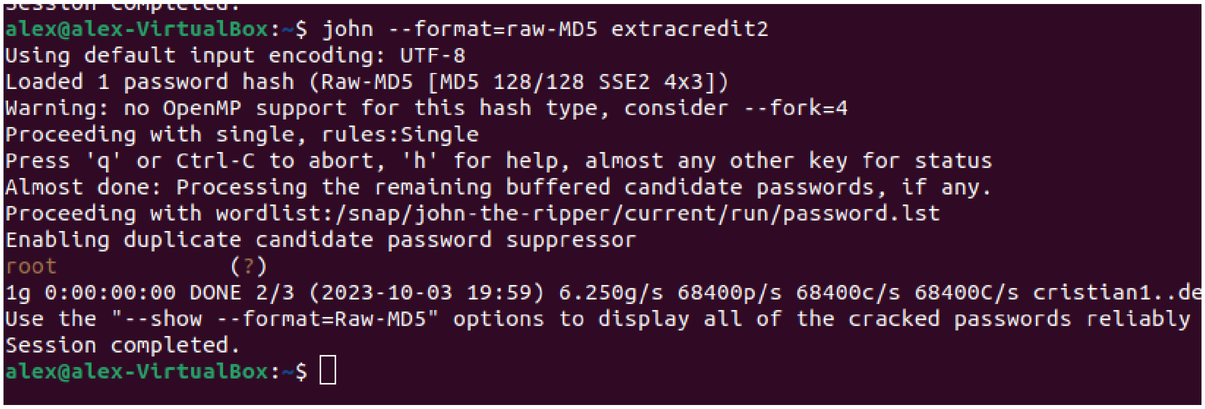
Begin by moving to a text file

Next use the command john –format=raw-MD5 filename

Gives us password and root



```
stat: extracredit: No such file or directory
alex@alex-VirtualBox:~$ john --format=raw-MD5 extracredit1
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/snap/john-the-ripper/current/run/password.lst
Enabling duplicate candidate password suppressor
password         (?)
1g 0:00:00:00 DONE 2/3 (2023-10-03 19:56) 5.882g/s 1129p/s 1129c/s 1129C/s 123456..knight
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
alex@alex-VirtualBox:~$ 
```



```
Session completed.
alex@alex-VirtualBox:~$ john --format=raw-MD5 extracredit2
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/snap/john-the-ripper/current/run/password.lst
Enabling duplicate candidate password suppressor
root             (?)
1g 0:00:00:00 DONE 2/3 (2023-10-03 19:59) 6.250g/s 68400p/s 68400c/s 68400C/s cristian1..de
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
alex@alex-VirtualBox:~$ 
```