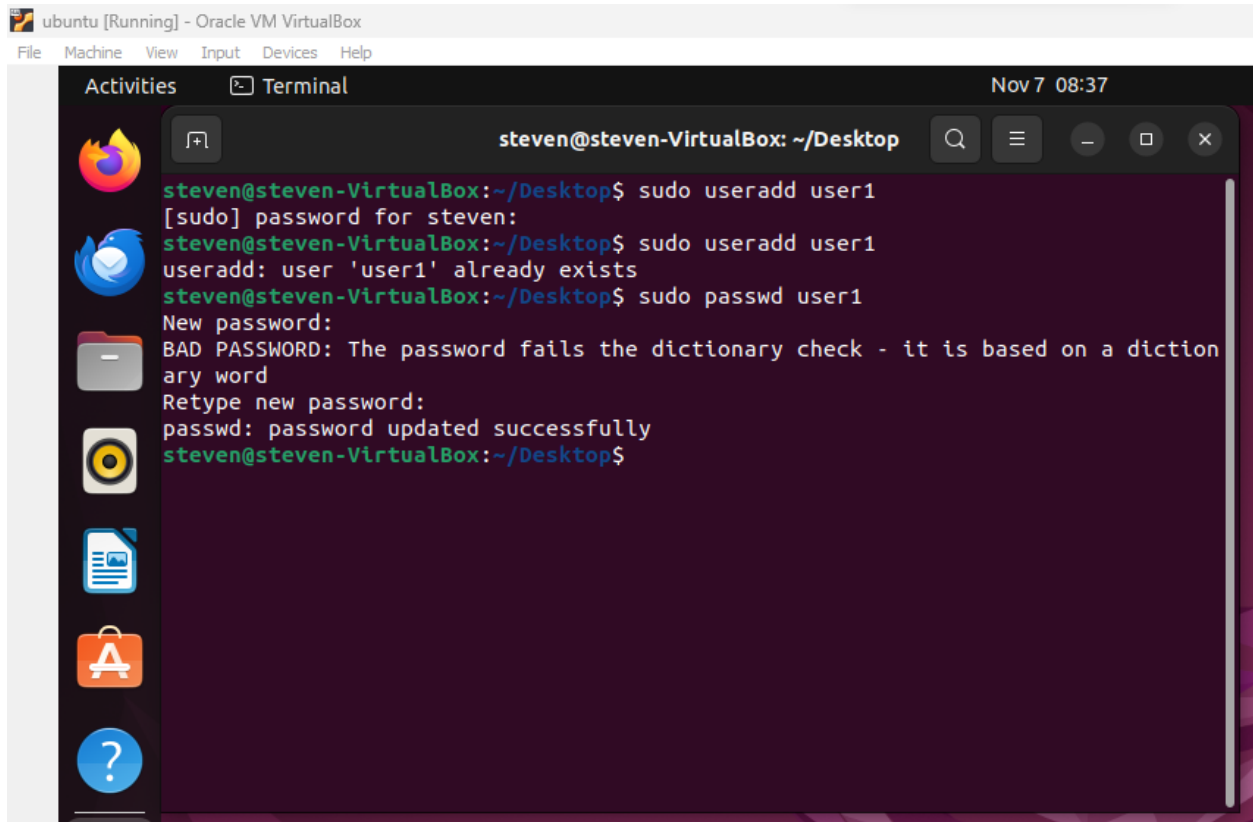


Task A – Password Cracking

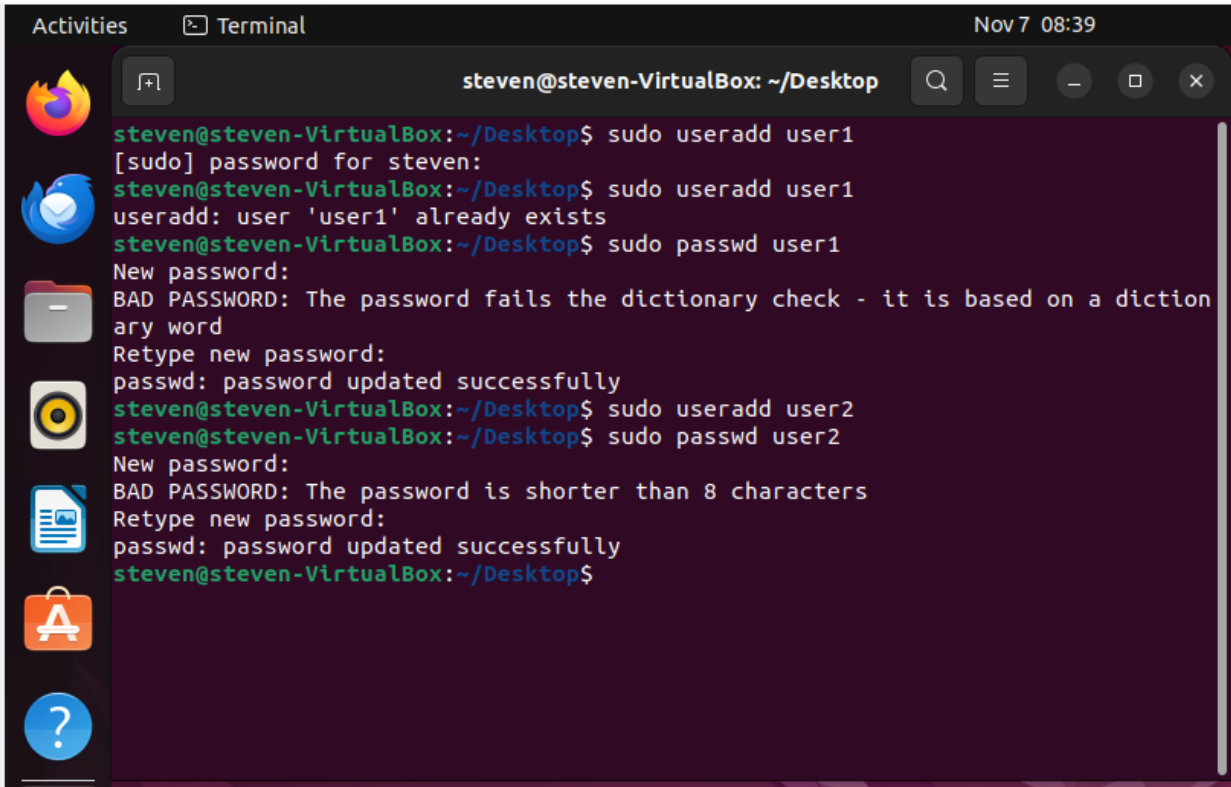
1. Create 6 users in your Linux Terminal, then set the password for each user that meets the following complexity requirement respectively. You should list the passwords created for each user. [6 * 5 = 30 points]

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



```
ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Nov 7 08:37
steven@steven-VirtualBox: ~/Desktop
steven@steven-VirtualBox:~/Desktop$ sudo useradd user1
[sudo] password for steven:
steven@steven-VirtualBox:~/Desktop$ sudo useradd user1
useradd: user 'user1' already exists
steven@steven-VirtualBox:~/Desktop$ sudo passwd user1
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$
```

2. For user2, the password should consist of 4-character digits **(2345)**



```
steven@steven-VirtualBox: ~/Desktop
steven@steven-VirtualBox:~/Desktop$ sudo useradd user1
[sudo] password for steven:
steven@steven-VirtualBox:~/Desktop$ sudo useradd user1
useradd: user 'user1' already exists
steven@steven-VirtualBox:~/Desktop$ sudo passwd user1
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$ sudo useradd user2
steven@steven-VirtualBox:~/Desktop$ sudo passwd user2
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$
```

3. For user3, the password should consist of a simple dictionary word of any length (all lowercase) + digits (capital123)

```
ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Nov 7 08:40
steven@steven-VirtualBox: ~/Desktop
steven@steven-VirtualBox:~/Desktop$ sudo useradd user1
[sudo] password for steven:
steven@steven-VirtualBox:~/Desktop$ sudo useradd user1
useradd: user 'user1' already exists
steven@steven-VirtualBox:~/Desktop$ sudo passwd user1
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$ sudo useradd user2
steven@steven-VirtualBox:~/Desktop$ sudo passwd user2
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$ sudo useradd user3
steven@steven-VirtualBox:~/Desktop$ sudo passwd user3
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$
```

4. For user4, the password should consist of a simple dictionary word (all lowercase) + digits +symbols
(final123!)

```
ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Nov 7 08:42
steven@steven-VirtualBox: ~/Desktop

Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$ sudo useradd user2
steven@steven-VirtualBox:~/Desktop$ sudo passwd user2
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$ sudo useradd user3
steven@steven-VirtualBox:~/Desktop$ sudo passwd user3
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$ sudo useradd user4
steven@steven-VirtualBox:~/Desktop$ sudo passwd user4
New password:
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$
```

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

(hat123)

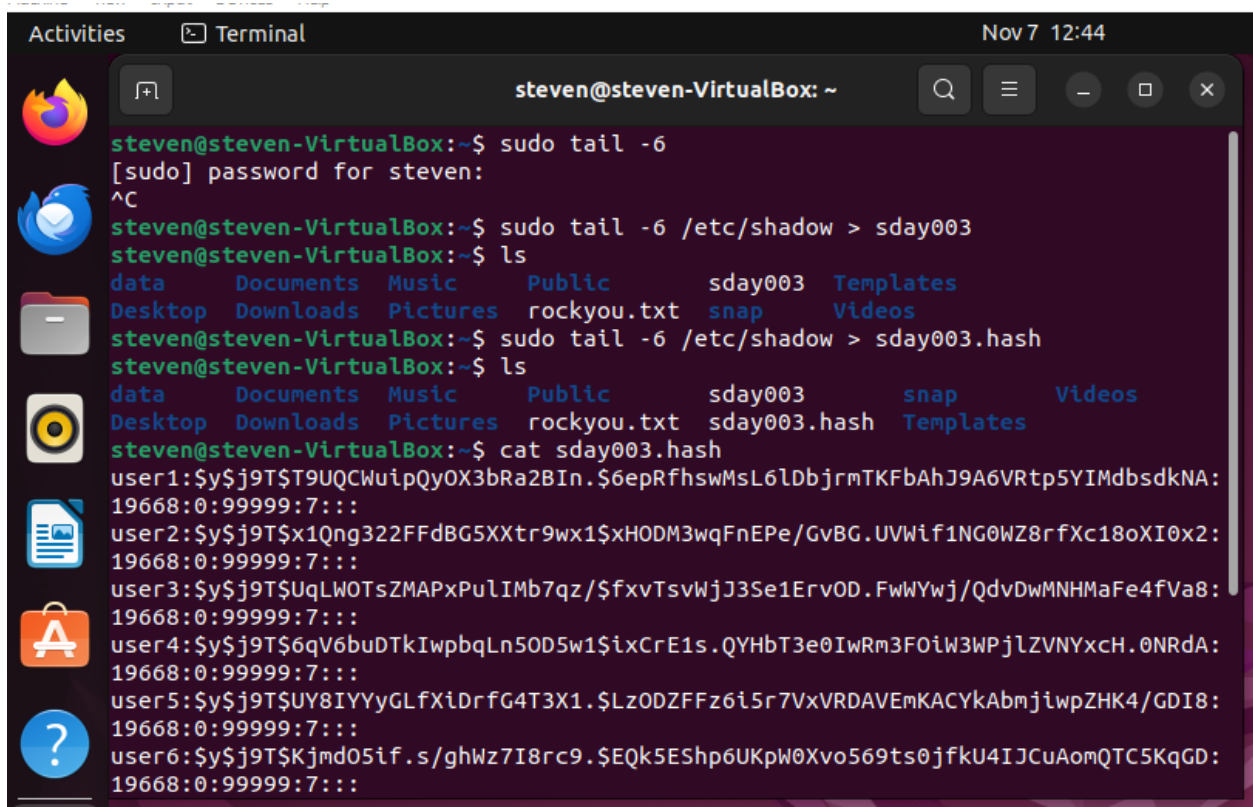
```
ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Nov 7 08:44
steven@steven-VirtualBox: ~/Desktop
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$ sudo useradd user3
steven@steven-VirtualBox:~/Desktop$ sudo passwd user3
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$ sudo useradd user4
steven@steven-VirtualBox:~/Desktop$ sudo passwd user4
New password:
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$ sudo useradd users5
steven@steven-VirtualBox:~/Desktop$ sudo passwd users5
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$
```

6. For user6, the password should consist of a simple dictionary word (with a combination of lower and upper case) + digits +symbols (TrAnSfOrM4444!)

```
steven@steven-VirtualBox: ~/Desktop
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$ sudo useradd user5
steven@steven-VirtualBox:~/Desktop$ sudo passwd user5
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
steven@steven-VirtualBox:~/Desktop$ sudo useradd user6
steven@steven-VirtualBox:~/Desktop$ sudo passwd user6
New password:
BAD PASSWORD: No password supplied
Retype new password:
No password has been supplied.
passwd: Authentication token manipulation error
passwd: password unchanged
steven@steven-VirtualBox:~/Desktop$ sudo passwd user6
New password:
Retype new password:
passwd: password updated successfully
```

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

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]



```
Activities Terminal Nov 7 12:44
steven@steven-VirtualBox: ~
steven@steven-VirtualBox:~$ sudo tail -6
[sudo] password for steven:
^C
steven@steven-VirtualBox:~$ sudo tail -6 /etc/shadow > sday003
steven@steven-VirtualBox:~$ ls
data Documents Music Public sday003 Templates
Desktop Downloads Pictures rockyou.txt snap Videos
steven@steven-VirtualBox:~$ sudo tail -6 /etc/shadow > sday003.hash
steven@steven-VirtualBox:~$ ls
data Documents Music Public sday003 snap Videos
Desktop Downloads Pictures rockyou.txt sday003.hash Templates
steven@steven-VirtualBox:~$ cat sday003.hash
user1:$y$j9T$T9UQCWuipQyOX3bRa2BIn.$6epRfhswMsL6lDbjrnTKFbAhJ9A6VRtp5YIMdbSDKNA:
19668:0:99999:7:::
user2:$y$j9T$x1Qng322FFdBG5XXtr9wx1$xHODM3wqFnEpe/GvBG.UVWif1NG0WZ8rfXc18oXI0x2:
19668:0:99999:7:::
user3:$y$j9T$UqLWOTsZMAPxPulIMb7qz/$fxvTsvWjJ3Se1ErvOD.FwWYwj/QdvDwMNHMaFe4fVa8:
19668:0:99999:7:::
user4:$y$j9T$6qV6buDTkIwpbqLn50D5w1$ixCrE1s.QYHbT3e0IwRm3F0iW3WPjLZVNYxch.0NRdA:
19668:0:99999:7:::
user5:$y$j9T$UY8IYYyGLfxiDrfg4T3X1.$Lz0DZFFz6i5r7VxVRDAVEmKACYkAbmjiwpZHK4/GDI8:
19668:0:99999:7:::
user6:$y$j9T$Kjmd05if.s/ghWz7I8rc9.$EQk5EShp6UKpW0Xvo569ts0jfkU4IJCuAomQTC5KqGD:
19668:0:99999:7:::
```

```
Activities Terminal Nov 7 12:50
steven@steven-VirtualBox: ~
0g 0:00:03:19 0.02% (ETA: 2023-11-19 17:06) 0g/s 16.33p/s 98.94c/s 98.94C/s aluc
ard..hottie101
Session aborted
steven@steven-VirtualBox:~$ john --wordlist=rockyou.txt sday003.hash --show
Invalid options combination: "--show"
steven@steven-VirtualBox:~$ john --wordlist=rockyou.txt sday003.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:descript 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 3 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
0g 0:00:00:36 0.00% (ETA: 2023-11-18 16:10) 0g/s 15.72p/s 107.5c/s 107.5C/s evel
yn..kelly
Session aborted
steven@steven-VirtualBox:~$ john --format=crypt --wordlist=rockyou.txt sday003.h
ash
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:descript 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 3 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? None

```
Activities Terminal Nov 7 13:12
steven@steven-VirtualBox: ~
0g 0:00:03:19 0.02% (ETA: 2023-11-19 17:06) 0g/s 16.33p/s 98.94c/s 98.94C/s aluc
ard..hottie101
Session aborted
steven@steven-VirtualBox:~$ john --wordlist=rockyou.txt sday003.hash --show
Invalid options combination: "--show"
steven@steven-VirtualBox:~$ john --wordlist=rockyou.txt sday003.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 3 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
0g 0:00:00:36 0.00% (ETA: 2023-11-18 16:10) 0g/s 15.72p/s 107.5c/s 107.5C/s evel
yn..kelly
Session aborted
steven@steven-VirtualBox:~$ john --format=crypt --wordlist=rockyou.txt sday003.h
ash
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 3 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
```

[30 points] 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.

These are hard and couldn't figure them out. Would love a walk through to understand this information.

5f4dcc3b5aa765d61d8327deb882cf99

63a9f0ea7bb98050796b649e85481845