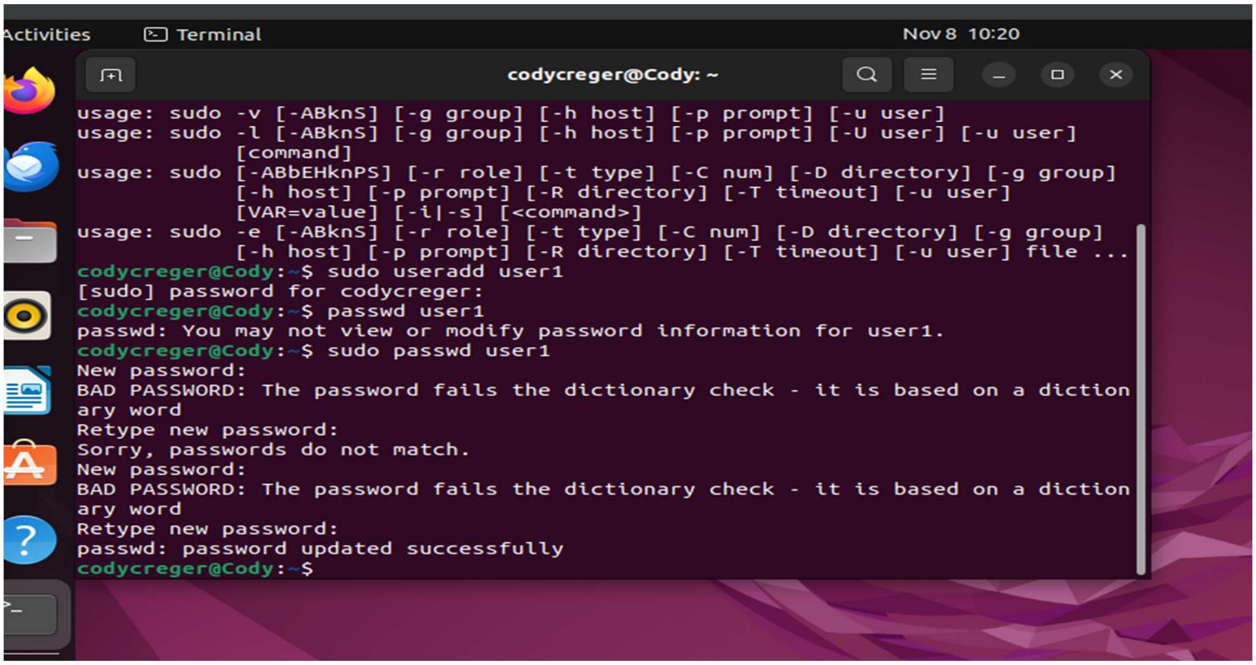
CYSE 270: Linux System for Cybersecurity

The goal of this lab is to test the strength of different passwords.

Task A – Password Cracking

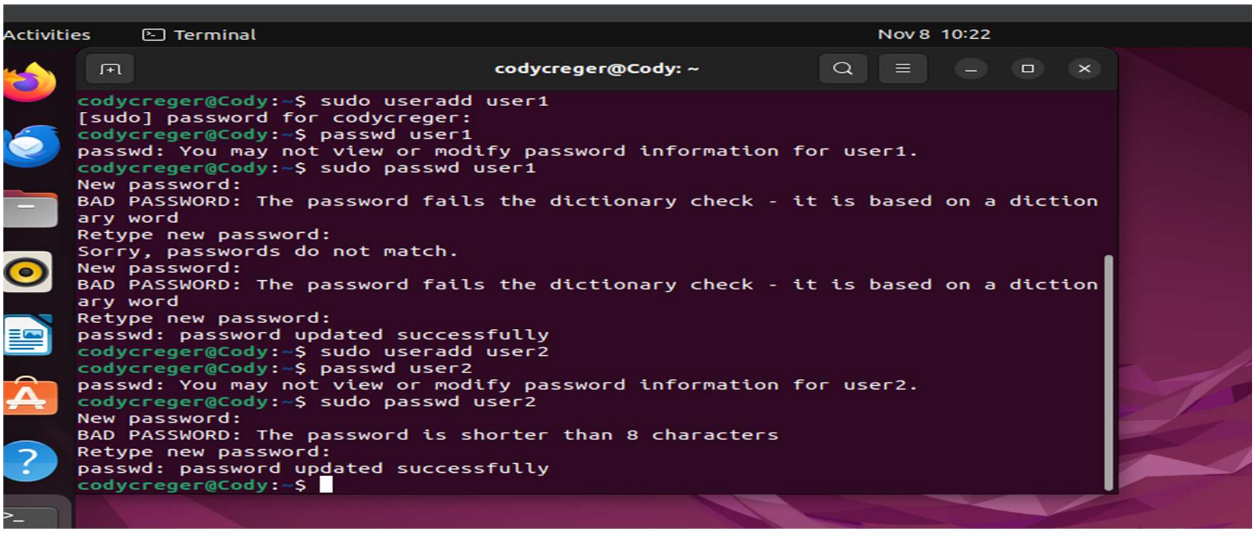
1. Create 6 users in your Linux Terminal, then set the password for each user that meets the following complexity requirement respectively. You should list the passwords created for each user. [6 * 5 = 30 points]

1. For user1, the puser1assword should be a simple dictionary word (all lowercase) PW=seahorse



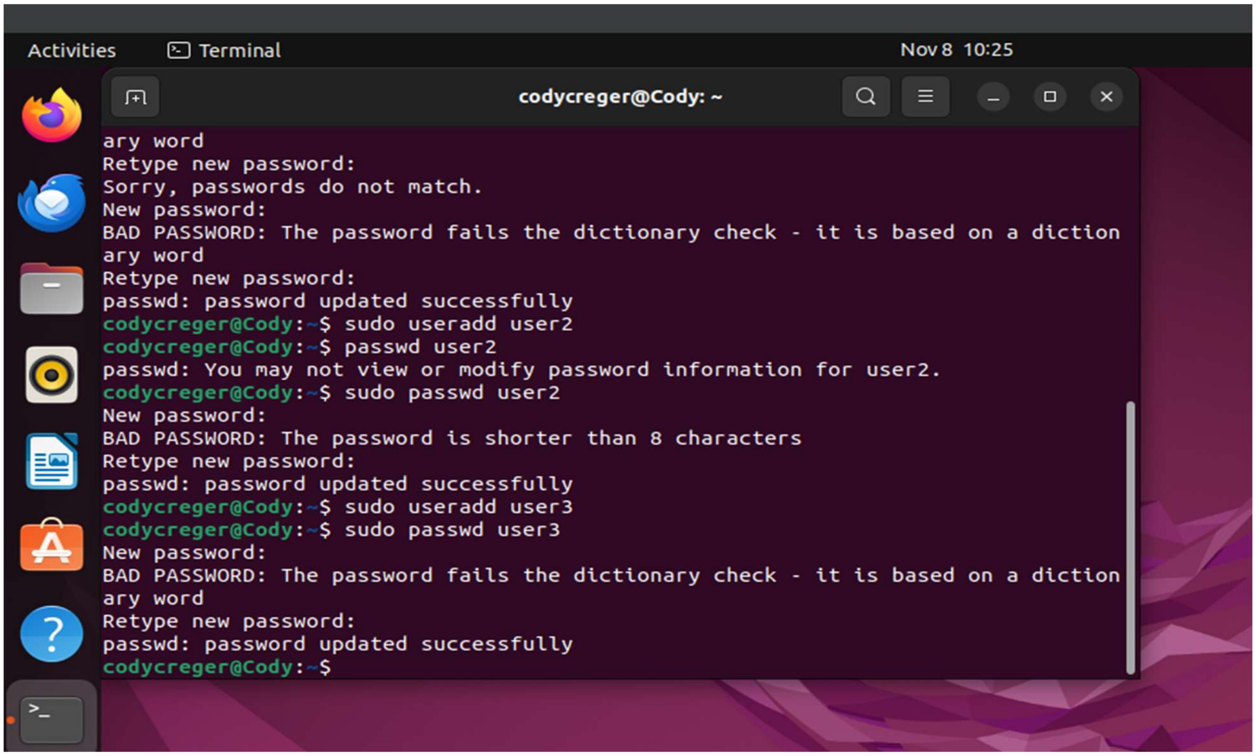
```
usage: sudo -v [-ABknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-ABknS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
            [command]
usage: sudo [-ABbEHknPS] [-r role] [-t type] [-C num] [-D directory] [-g group]
            [-h host] [-p prompt] [-R directory] [-T timeout] [-u user]
            [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-ABknS] [-r role] [-t type] [-C num] [-D directory] [-g group]
            [-h host] [-p prompt] [-R directory] [-T timeout] [-u user] file ...
codycreger@Cody:~$ sudo useradd user1
[sudo] password for codycreger:
codycreger@Cody:~$ passwd user1
passwd: You may not view or modify password information for user1.
codycreger@Cody:~$ sudo passwd user1
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:
BAD PASSWORD: The password fails the dictionary check - it is based on a diction
ary word
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$
```

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



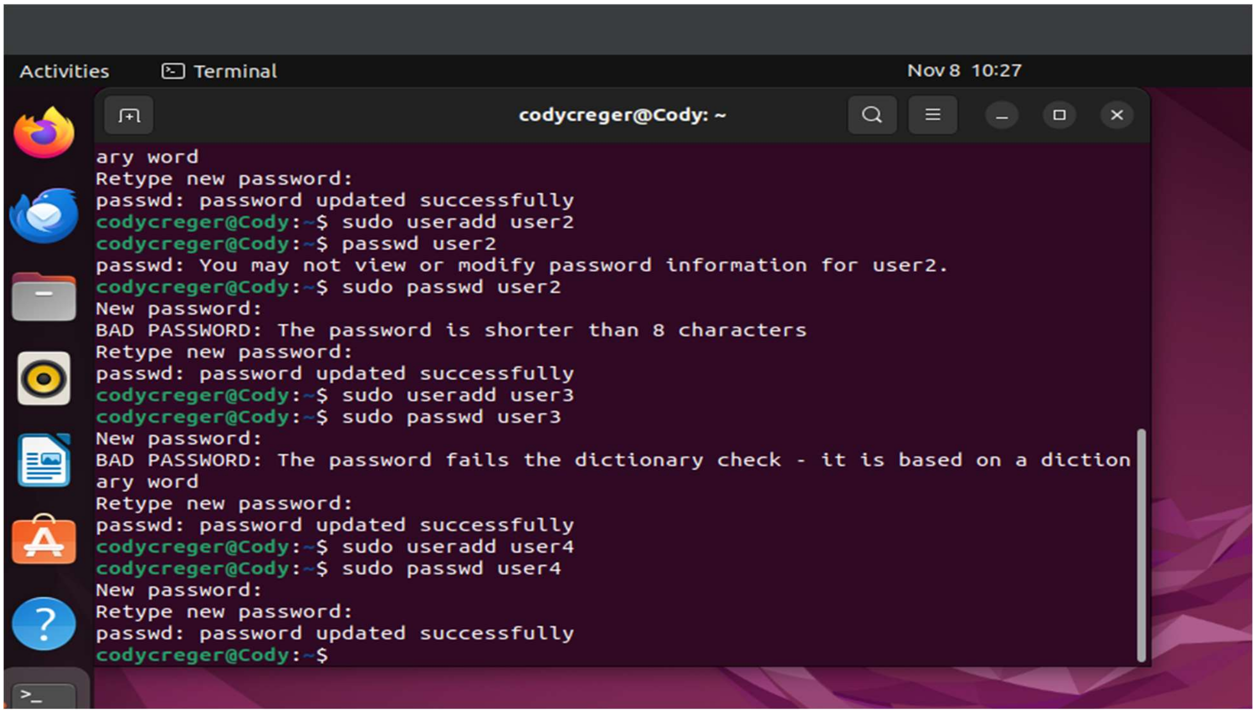
```
codycreger@Cody:~$ sudo useradd user1
[sudo] password for codycreger:
codycreger@Cody:~$ passwd user1
passwd: You may not view or modify password information for user1.
codycreger@Cody:~$ sudo passwd user1
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a diction
ary word
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a diction
ary word
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$ sudo useradd user2
codycreger@Cody:~$ passwd user2
passwd: You may not view or modify password information for user2.
codycreger@Cody:~$ sudo passwd user2
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$
```

3. For user3, the password should consist of a simple dictionary word of any length (all lowercase) + digits PW=seahorse123



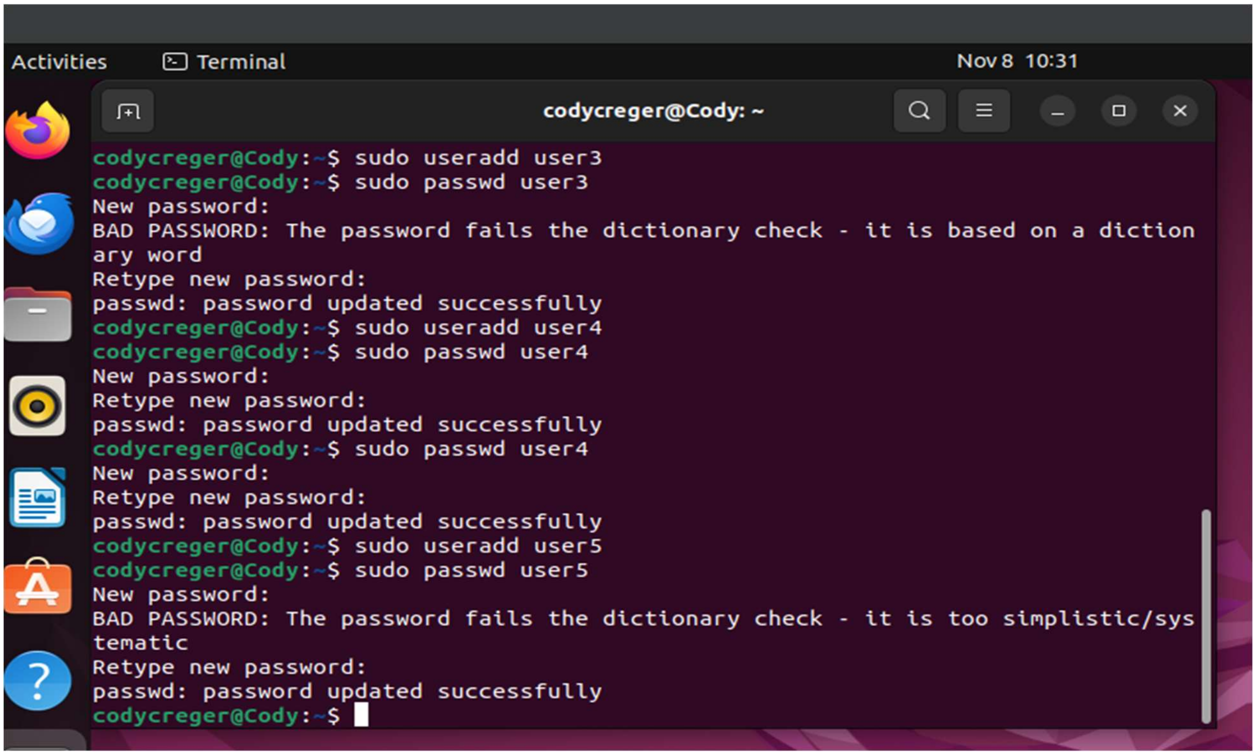
```
ary word
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a diction
ary word
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$ sudo useradd user2
codycreger@Cody:~$ passwd user2
passwd: You may not view or modify password information for user2.
codycreger@Cody:~$ sudo passwd user2
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$ sudo useradd user3
codycreger@Cody:~$ 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
codycreger@Cody:~$
```

4. For user4, the password should consist of a simple dictionary word (all lowercase) + digits +symbols PW= seahorse123!



```
ary word
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$ sudo useradd user2
codycreger@Cody:~$ passwd user2
passwd: You may not view or modify password information for user2.
codycreger@Cody:~$ sudo passwd user2
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$ sudo useradd user3
codycreger@Cody:~$ 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
codycreger@Cody:~$ sudo useradd user4
codycreger@Cody:~$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$
```

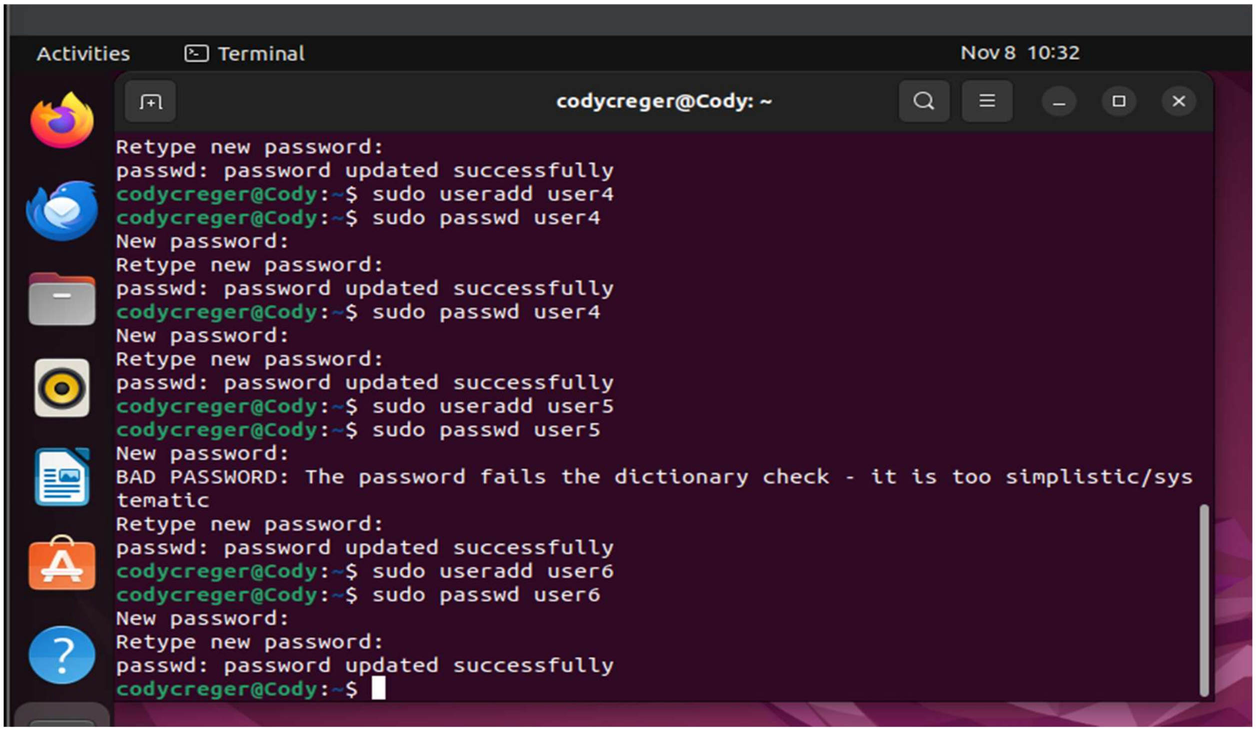
5. For user5, the password should consist of a simple dictionary word (all lowercase) + digits. PW=seahorse12345



```
codycreger@Cody:~$ sudo useradd user3
codycreger@Cody:~$ 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
codycreger@Cody:~$ sudo useradd user4
codycreger@Cody:~$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$ sudo useradd user5
codycreger@Cody:~$ sudo passwd user5
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/sys
tematic
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$
```

6. For user6, the password should consist of a simple dictionary word (with a combination of

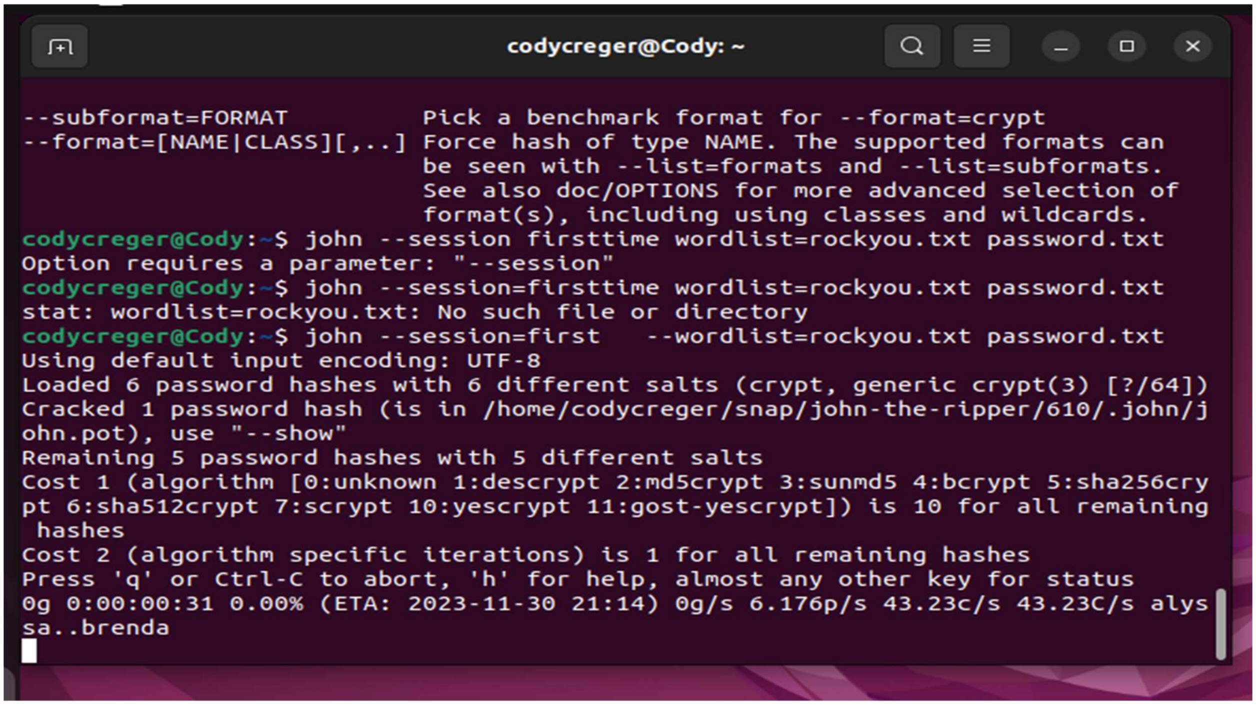
lower and upper case) + digits +symbols PW=SEahorse123!



```
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$ sudo useradd user4
codycreger@Cody:~$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$ sudo useradd user5
codycreger@Cody:~$ sudo passwd user5
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/sys
tematic
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$ sudo useradd user6
codycreger@Cody:~$ sudo passwd user6
New password:
Retype new password:
passwd: password updated successfully
codycreger@Cody:~$
```

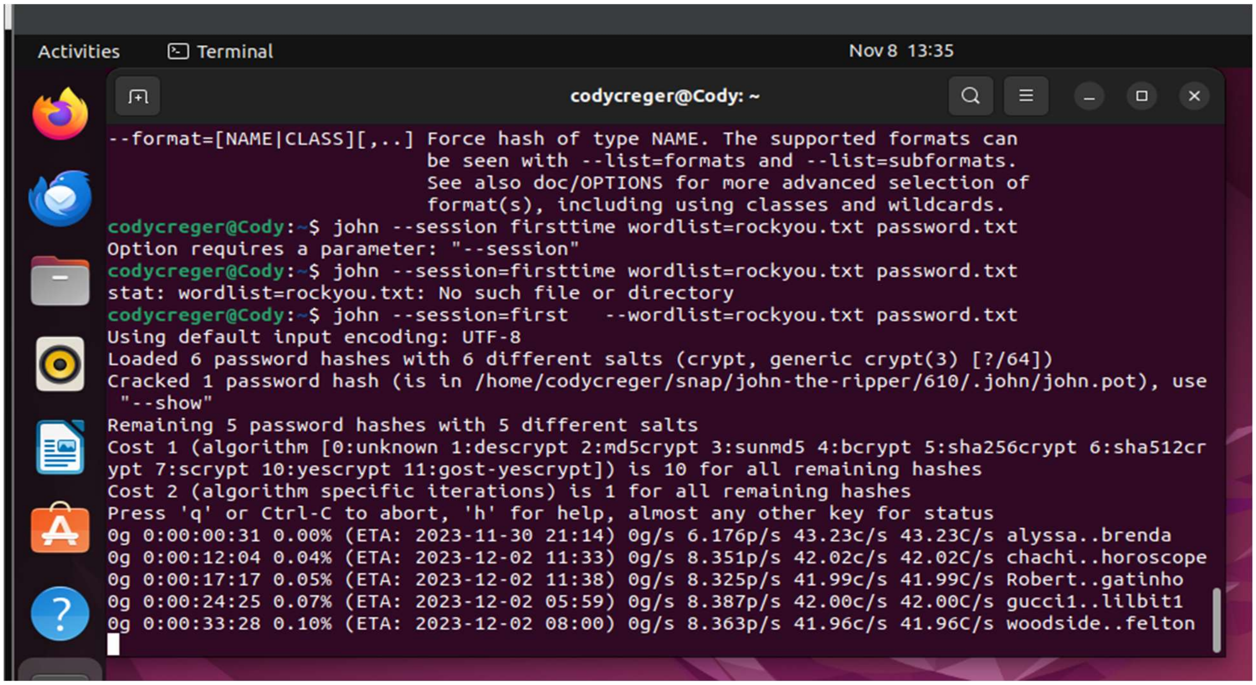
Remember, do not use the passwords for your real-world accounts.

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]



```
--subformat=FORMAT         Pick a benchmark format for --format=crypt
--format=[NAME|CLASS][,..] Force hash of type NAME. The supported formats can
                           be seen with --list=formats and --list=subformats.
                           See also doc/OPTIONS for more advanced selection of
                           format(s), including using classes and wildcards.
codycreger@Cody:~$ john --session firsttime wordlist=rockyou.txt password.txt
Option requires a parameter: "--session"
codycreger@Cody:~$ john --session=firsttime wordlist=rockyou.txt password.txt
stat: wordlist=rockyou.txt: No such file or directory
codycreger@Cody:~$ john --session=first   --wordlist=rockyou.txt password.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cracked 1 password hash (is in /home/codycreger/snap/john-the-ripper/610/.john/j
ohn.pot), use "--show"
Remaining 5 password hashes with 5 different salts
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 remaining
 hashes
Cost 2 (algorithm specific iterations) is 1 for all remaining hashes
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
0g 0:00:00:31 0.00% (ETA: 2023-11-30 21:14) 0g/s 6.176p/s 43.23c/s 43.23C/s alys
sa..brenda
```

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



```
--format=[NAME|CLASS][,..] Force hash of type NAME. The supported formats can
                           be seen with --list=formats and --list=subformats.
                           See also doc/OPTIONS for more advanced selection of
                           format(s), including using classes and wildcards.
codycreger@Cody:~$ john --session firsttime wordlist=rockyou.txt password.txt
Option requires a parameter: "--session"
codycreger@Cody:~$ john --session=firsttime wordlist=rockyou.txt password.txt
stat: wordlist=rockyou.txt: No such file or directory
codycreger@Cody:~$ john --session=first   --wordlist=rockyou.txt password.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cracked 1 password hash (is in /home/codycreger/snap/john-the-ripper/610/.john/john.pot), use
 "--show"
Remaining 5 password hashes with 5 different salts
Cost 1 (algorithm [0:unknown 1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512cr
ypt 7:scrypt 10:yescrypt 11:gost-yescrypt]) is 10 for all remaining hashes
Cost 2 (algorithm specific iterations) is 1 for all remaining hashes
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
0g 0:00:00:31 0.00% (ETA: 2023-11-30 21:14) 0g/s 6.176p/s 43.23c/s 43.23C/s alyssa..brenda
0g 0:00:12:04 0.04% (ETA: 2023-12-02 11:33) 0g/s 8.351p/s 42.02c/s 42.02C/s chachi..horoscope
0g 0:00:17:17 0.05% (ETA: 2023-12-02 11:38) 0g/s 8.325p/s 41.99c/s 41.99C/s Robert..gatinho
0g 0:00:24:25 0.07% (ETA: 2023-12-02 05:59) 0g/s 8.387p/s 42.00c/s 42.00C/s gucci1..lilbit1
0g 0:00:33:28 0.10% (ETA: 2023-12-02 08:00) 0g/s 8.363p/s 41.96c/s 41.96C/s woodside..felton
```

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
- 63a9f0ea7bb98050796b649e85481845