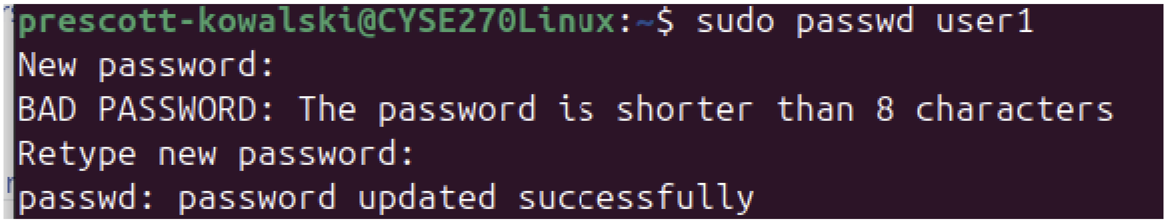
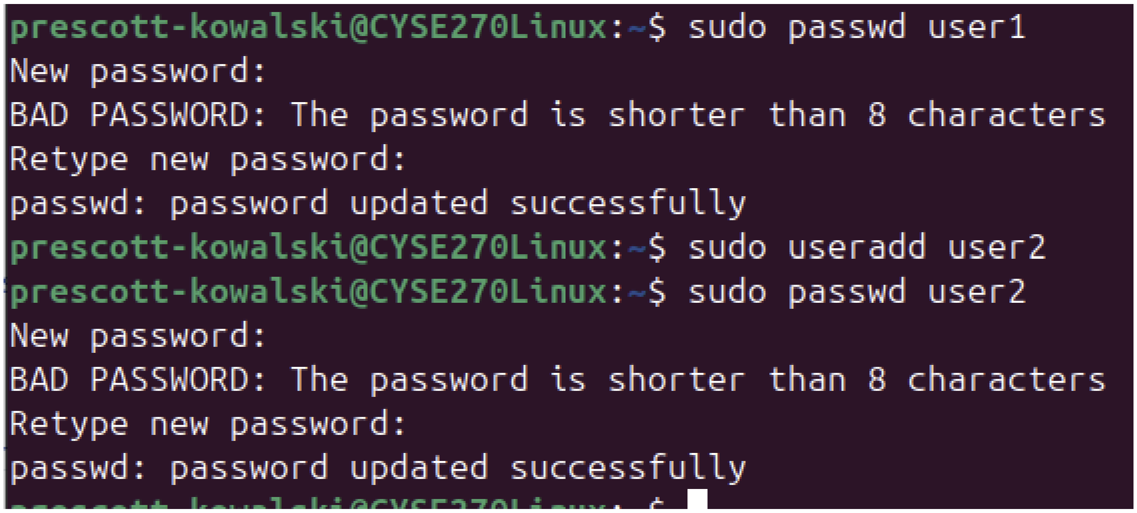
Prescott Kowalski
CYSE 270: Linux System for Cybersecurity
The goal of this lab is to test the strength of different passwords.
Task A – Password Cracking
1. Create 6 users in your Linux Terminal, then set the password for each user that meets the following complexity requirement respectively. You should list the passwords created for each user. [6 * 5 = 30 points].
1. For user1, the password should be a simple dictionary word (all lowercase)
apple



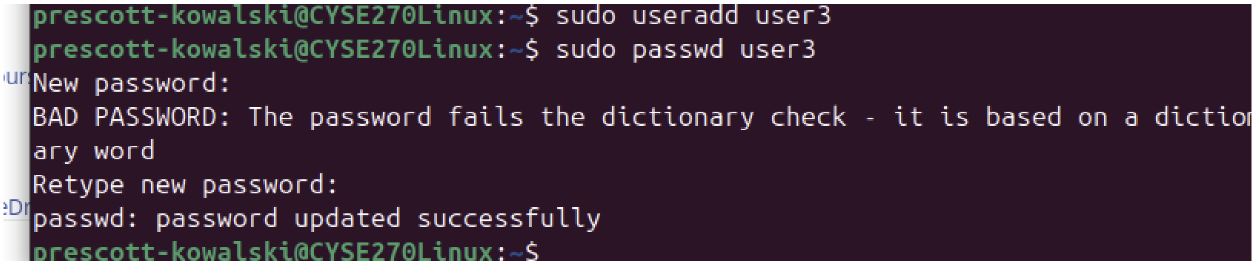
```
prescott-kowalski@CYSE270Linux:~$ sudo passwd user1
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
```

2. For user2, the password should consist of 4 digits.
1234



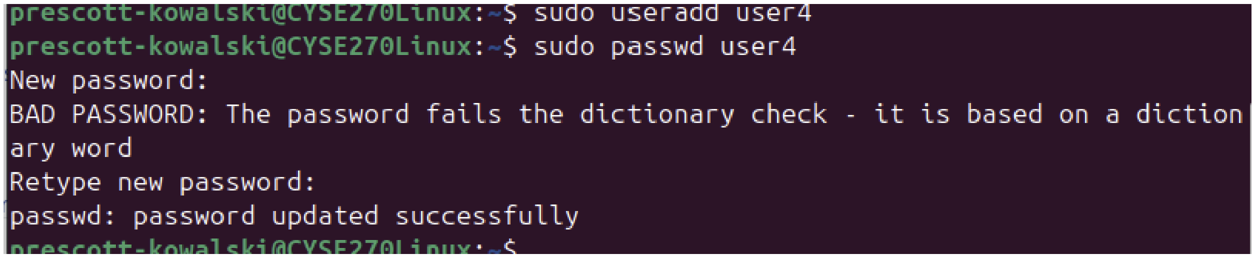
```
prescott-kowalski@CYSE270Linux:~$ sudo passwd user1
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
prescott-kowalski@CYSE270Linux:~$ sudo useradd user2
prescott-kowalski@CYSE270Linux:~$ sudo passwd user2
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
prescott-kowalski@CYSE270Linux:~$
```

3. For user3, the password should consist of a simple dictionary word of any length characters (all lowercase) + digits.
banana42



```
prescott-kowalski@CYSE270Linux:~$ sudo useradd user3
prescott-kowalski@CYSE270Linux:~$ 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
prescott-kowalski@CYSE270Linux:~$
```

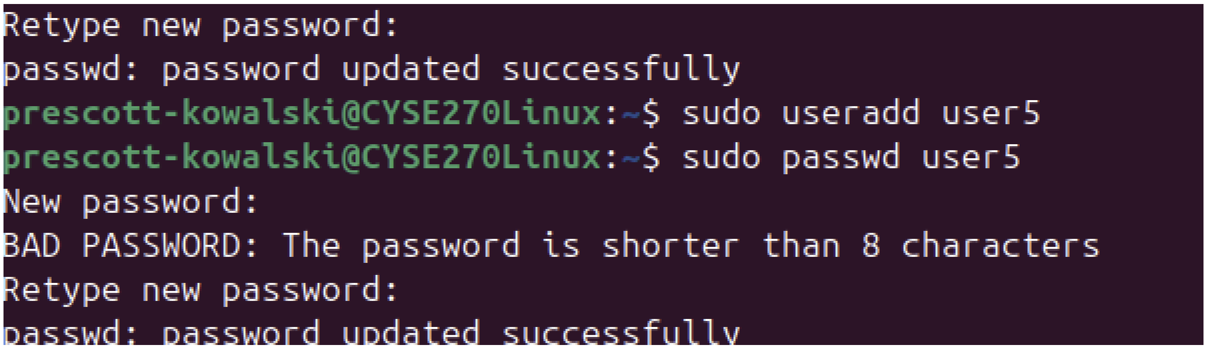
4. For user4, the password should consist of a simple dictionary word characters (all lowercase) + digits + symbols.
orange99!



```
prescott-kowalski@CYSE270Linux:~$ sudo useradd user4
prescott-kowalski@CYSE270Linux:~$ sudo passwd user4
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
prescott-kowalski@CYSE270Linux:~$
```

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

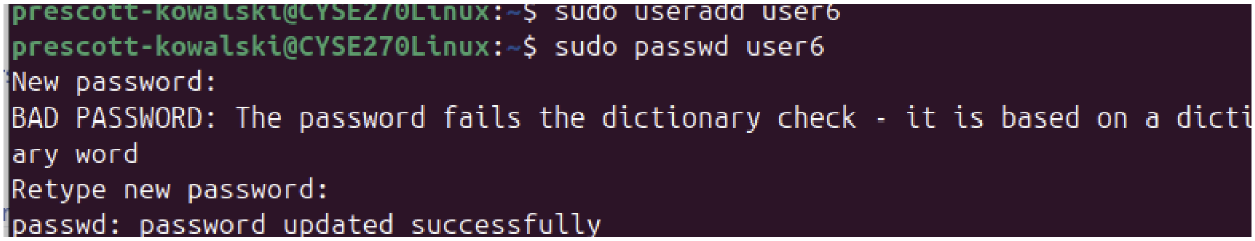
grape77



```
Retype new password:
passwd: password updated successfully
prescott-kowalski@CYSE270Linux:~$ sudo useradd user5
prescott-kowalski@CYSE270Linux:~$ sudo passwd user5
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
```

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

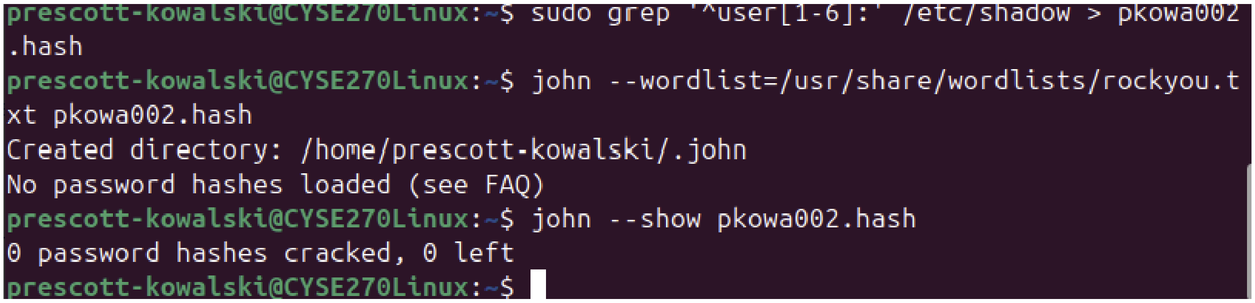
Strawberry88@



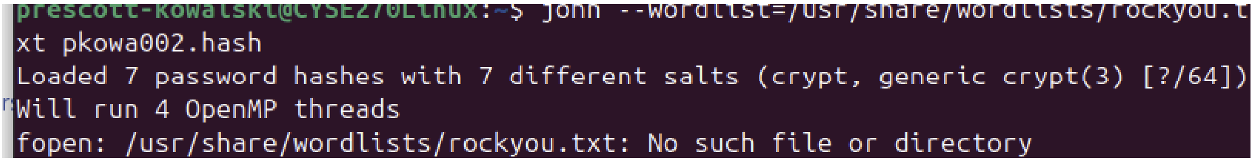
```
prescott-kowalski@CYSE270Linux:~$ sudo useradd user6
prescott-kowalski@CYSE270Linux:~$ sudo passwd user6
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dicti
ary word
Retype new password:
passwd: password updated successfully
```

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 name) and use John the Ripper tool to crack their passwords in wordlist mode (use rockyou.txt). [40 points]



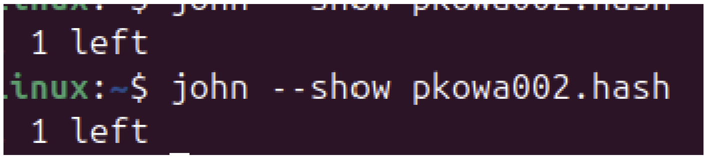
```
prescott-kowalski@CYSE270Linux:~$ sudo grep '^user[1-6]:' /etc/shadow > pkowa002
.hash
prescott-kowalski@CYSE270Linux:~$ john --wordlist=/usr/share/wordlists/rockyou.t
xt pkowa002.hash
Created directory: /home/prescott-kowalski/.john
No password hashes loaded (see FAQ)
prescott-kowalski@CYSE270Linux:~$ john --show pkowa002.hash
0 password hashes cracked, 0 left
prescott-kowalski@CYSE270Linux:~$
```



```
prescott-kowalski@CYSE270Linux:~$ john --wordlist=/usr/share/wordlists/rockyou.t
xt pkowa002.hash
Loaded 7 password hashes with 7 different salts (crypt, generic crypt(3) [?/64])
Will run 4 OpenMP threads
fopen: /usr/share/wordlists/rockyou.txt: No such file or directory
```

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

All of them but user 6



```
.inux:~$ john --show pkowa002.hash
 1 left
.inux:~$ john --show pkowa002.hash
 1 left
```

CYSE 270: Linux System for Cybersecurity

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.

a. 5f4dcc3b5aa765d61d8327deb882cf99 **Password**

Did the steps but my John started acting up so I used hashcat. Jumbo john wouldn't install

sudo apt install build-essential git libssl-dev zlib1g-dev yasm
git clone https://github.com/openwall/john.git
cd john/src
make -s clean && make -sj$(nproc)
Installing all apps after submitting

b. 63a9f0ea7bb98050796b649e85481845 **Root**

Fun learning experience, waiting on updates. Excited for extra credit future weeks. Forgot to install many apps prior. Snap shotted this vm before I updated and installed everything