CYSE 270: Linux System for Cybersecurity

Assignment: Lab 5 – Password cracking

Danielle Caplinger

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)

   Passwd: welcome

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

   5390

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

   Passwd: umbrella941

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

   Passwd: umbrella!784$

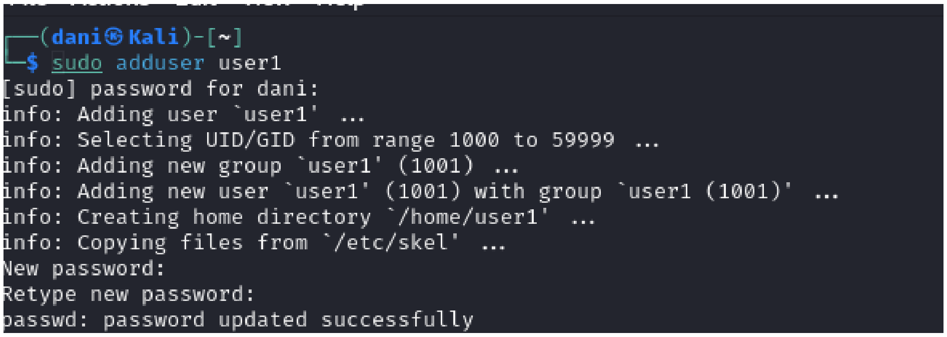
5. For user5, the password should consist of a simple dictionary word (all lowercase) + digits

   Passwd: hats8234

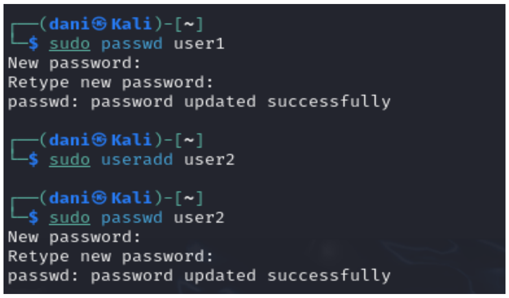
6. For user6, the password should consist of a simple dictionary word (with a combination of lower and upper case) + digits +symbols

   ChEEse!97#

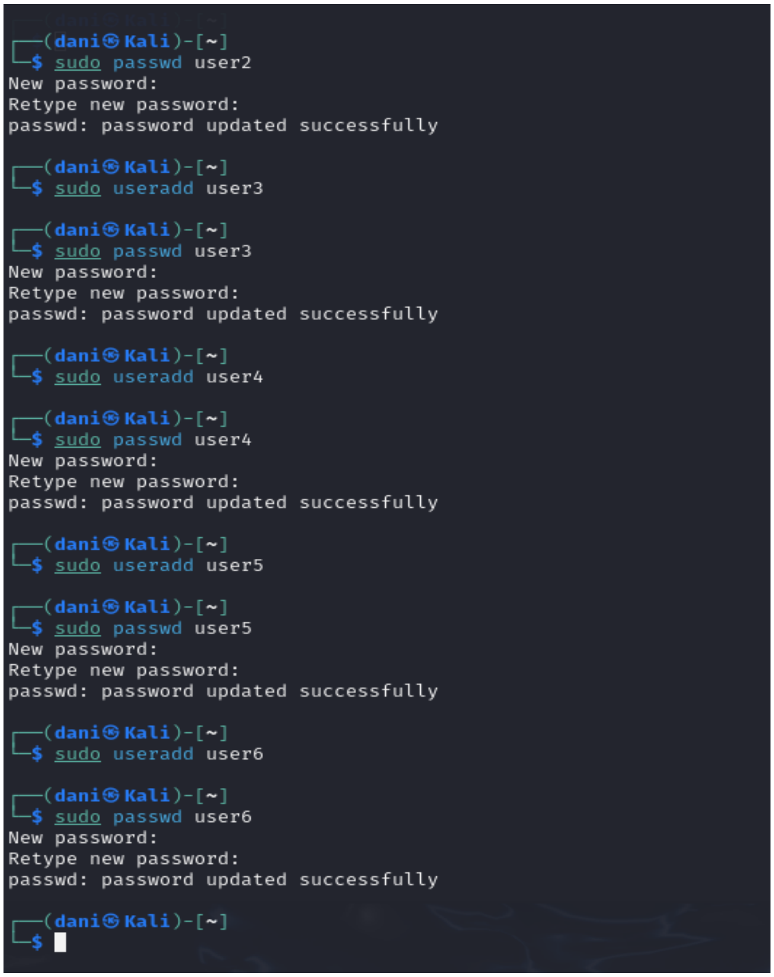
Screenshot for all added users:



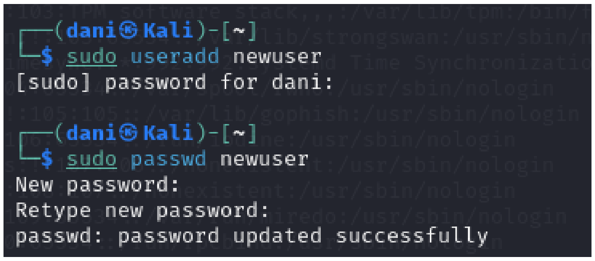
```
┌──(dani㉿Kali)-[~]
└─$ sudo adduser user1
[sudo] password for dani:
info: Adding user `user1' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `user1' (1001) ...
info: Adding new user `user1' (1001) with group `user1 (1001)' ...
info: Creating home directory `/home/user1' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
```



```
┌──(dani㉿Kali)-[~]
└─$ sudo passwd user1
New password:
Retype new password:
passwd: password updated successfully

┌──(dani㉿Kali)-[~]
└─$ sudo useradd user2

┌──(dani㉿Kali)-[~]
└─$ sudo passwd user2
New password:
Retype new password:
passwd: password updated successfully
```

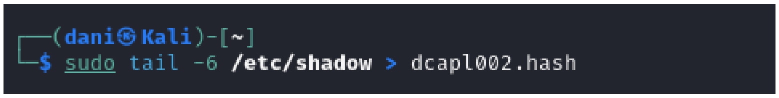


```
┌──(dani㉿Kali)-[~]
└─$ sudo passwd user2
New password:
Retype new password:
passwd: password updated successfully

┌──(dani㉿Kali)-[~]
└─$ sudo useradd user3

┌──(dani㉿Kali)-[~]
└─$ sudo passwd user3
New password:
Retype new password:
passwd: password updated successfully

┌──(dani㉿Kali)-[~]
└─$ sudo useradd user4

┌──(dani㉿Kali)-[~]
└─$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully

┌──(dani㉿Kali)-[~]
└─$ sudo useradd user5

┌──(dani㉿Kali)-[~]
└─$ sudo passwd user5
New password:
Retype new password:
passwd: password updated successfully

┌──(dani㉿Kali)-[~]
└─$ sudo useradd user6

┌──(dani㉿Kali)-[~]
└─$ sudo passwd user6
New password:
Retype new password:
passwd: password updated successfully

┌──(dani㉿Kali)-[~]
└─$ 
```

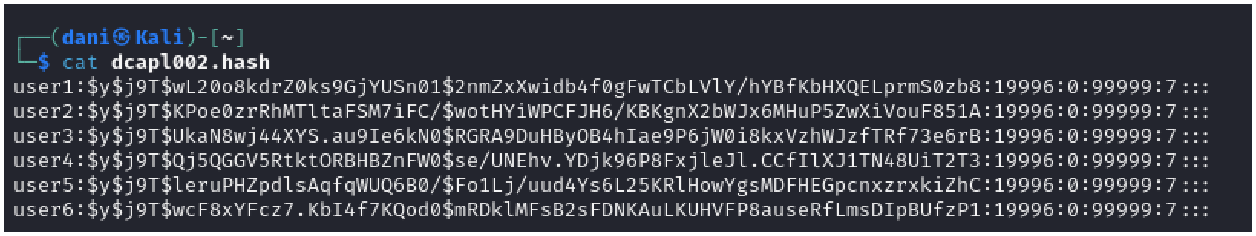


```
┌──(dani㉿Kali)-[~]
└─$ sudo useradd newuser
[sudo] password for dani:

┌──(dani㉿Kali)-[~]
└─$ sudo passwd newuser
New password:
Retype new password:
passwd: password updated successfully
```

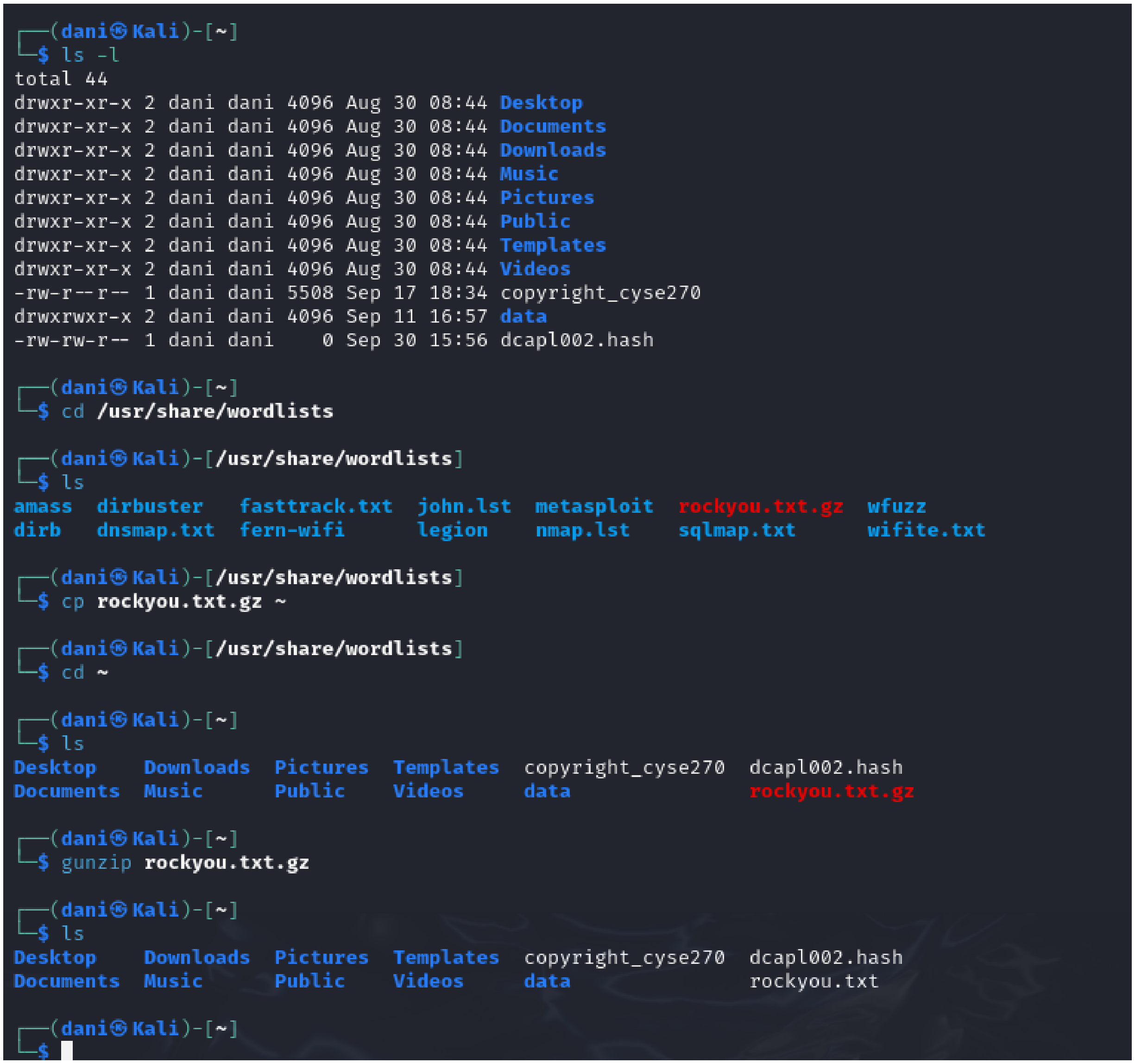
2. Export above users' hashes into a file named xxx.hash (replace xxx with your MIDAS name) and use **John the Ripper** tool to crack their passwords in wordlist mode (use rockyou.txt). **[40 points]** 3. Keep your john the ripper cracking for 10 minutes. How many passwords have been successfully cracked? [30 points]



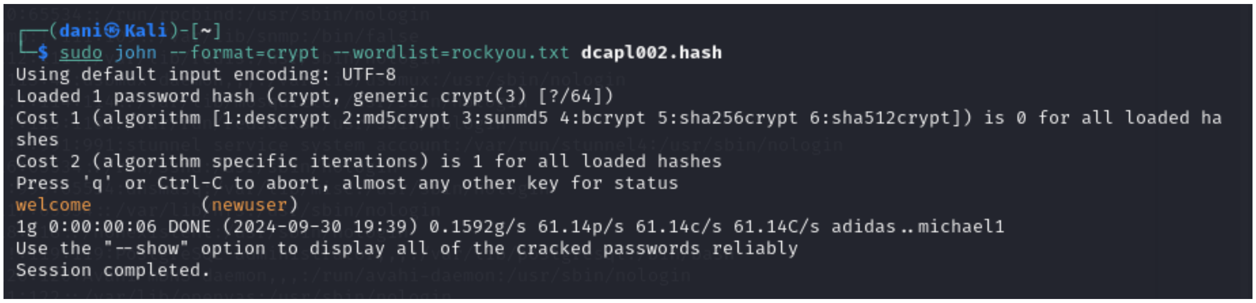
```
┌──(dani㉿Kali)-[~]
└─$ sudo tail -6 /etc/shadow > dcapl002.hash
```



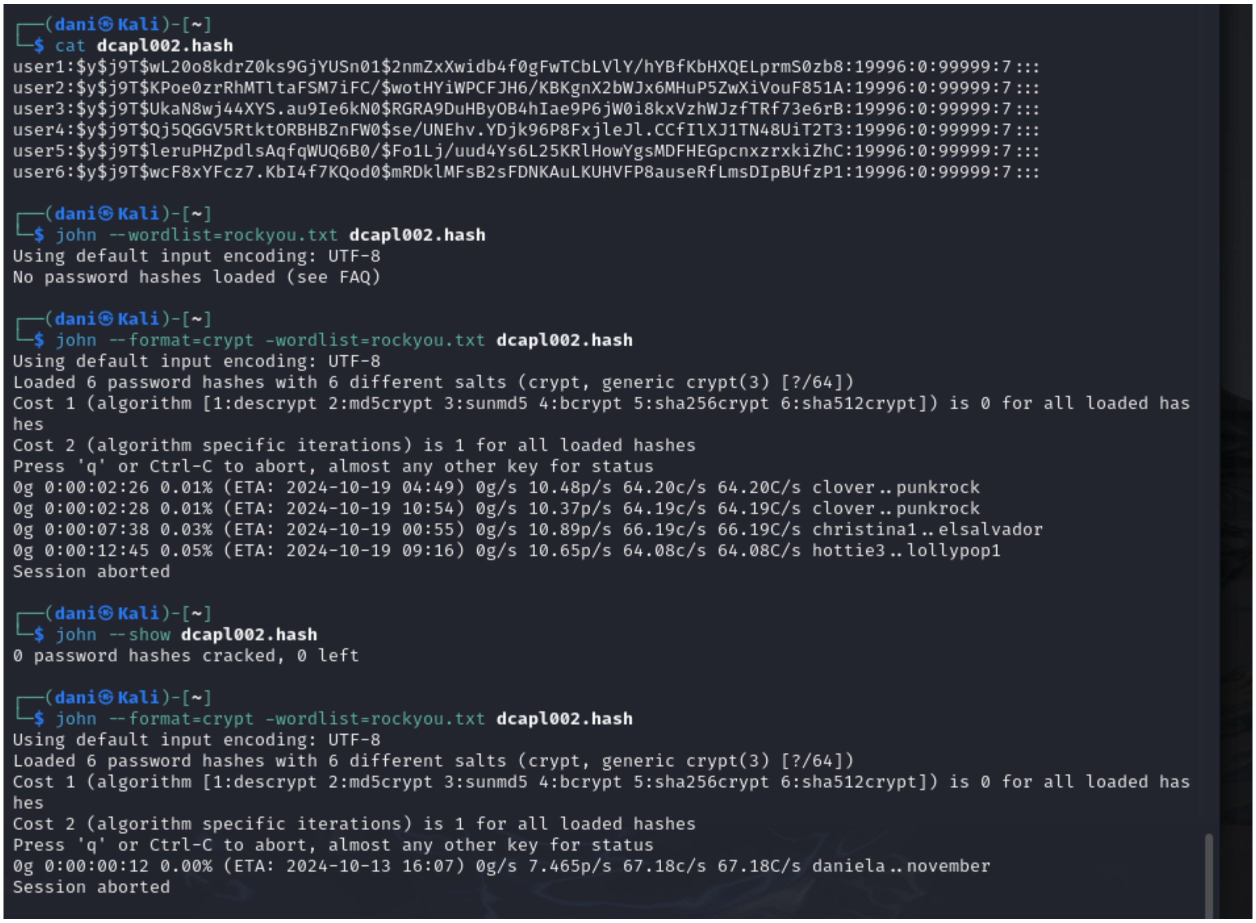
```
┌──(dani㉿Kali)-[~]
└─$ cat dcapl002.hash
user1:$y$j9T$wL20o8kdrZ0ks9GjYUSn01$2nmZxXwidb4f0gFwTCbLVlY/hYBfKbHXQELprmS0zb8:19996:0:99999:7:::
user2:$y$j9T$KPoe0zrRhMTltaFSM7iFC/$wotHYiWPCFJH6/KBKgnX2bWJx6MHuP5ZwXiVouF851A:19996:0:99999:7:::
user3:$y$j9T$UkaN8wj44XYS.au9Ie6kN0$RGRA9DuHByOB4hIae9P6jW0i8kxVzhWJzfTRf73e6rB:19996:0:99999:7:::
user4:$y$j9T$Qj5QGGV5RtktORBHBZnFW0$se/UNEhv.YDjk96P8FxjleJl.CCfIlXJ1TN48UiT2T3:19996:0:99999:7:::
user5:$y$j9T$leruPHZpdlsAqfqWUQ6B0/$Fo1Lj/uud4Ys6L25KRlHowYgsMDFHEGpcnxzrxkiZhC:19996:0:99999:7:::
user6:$y$j9T$wcF8xYFcz7.KbI4f7KQod0$mRDklMFsB2sFDNKAuLKUHVFP8auseRfLmsDIpBUfzP1:19996:0:99999:7:::
```



```
┌──(dani㉿Kali)-[~]
└─$ ls -l
total 44
drwxr-xr-x 2 dani dani 4096 Aug 30 08:44 Desktop
drwxr-xr-x 2 dani dani 4096 Aug 30 08:44 Documents
drwxr-xr-x 2 dani dani 4096 Aug 30 08:44 Downloads
drwxr-xr-x 2 dani dani 4096 Aug 30 08:44 Music
drwxr-xr-x 2 dani dani 4096 Aug 30 08:44 Pictures
drwxr-xr-x 2 dani dani 4096 Aug 30 08:44 Public
drwxr-xr-x 2 dani dani 4096 Aug 30 08:44 Templates
drwxr-xr-x 2 dani dani 4096 Aug 30 08:44 Videos
-rw-r--r-- 1 dani dani 5508 Sep 17 18:34 copyright_cyse270
drwxrwxr-x 2 dani dani 4096 Sep 11 16:57 data
-rw-rw-r-- 1 dani dani    0 Sep 30 15:56 dcapl002.hash

┌──(dani㉿Kali)-[~]
└─$ cd /usr/share/wordlists

┌──(dani㉿Kali)-[/usr/share/wordlists]
└─$ ls
amass  dirbuster    fasttrack.txt  john.lst  metasploit  rockyou.txt.gz  wfuzz
dirb   dnsmap.txt   fern-wifi      legion    nmap.lst    sqlmap.txt      wifite.txt

┌──(dani㉿Kali)-[/usr/share/wordlists]
└─$ cp rockyou.txt.gz ~

┌──(dani㉿Kali)-[/usr/share/wordlists]
└─$ cd ~

┌──(dani㉿Kali)-[~]
└─$ ls
Desktop    Downloads  Pictures  Templates  copyright_cyse270  dcapl002.hash
Documents  Music      Public    Videos     data               rockyou.txt.gz

┌──(dani㉿Kali)-[~]
└─$ gunzip rockyou.txt.gz

┌──(dani㉿Kali)-[~]
└─$ ls
Desktop    Downloads  Pictures  Templates  copyright_cyse270  dcapl002.hash
Documents  Music      Public    Videos     data               rockyou.txt

┌──(dani㉿Kali)-[~]
└─$ 
```



```
┌──(dani㉿Kali)-[~]
└─$ sudo john --format=crypt --wordlist=rockyou.txt dcapl002.hash
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded ha
shes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
welcome          (newuser)
1g 0:00:00:06 DONE (2024-09-30 19:39) 0.1592g/s 61.14p/s 61.14c/s 61.14C/s adidas..michael1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



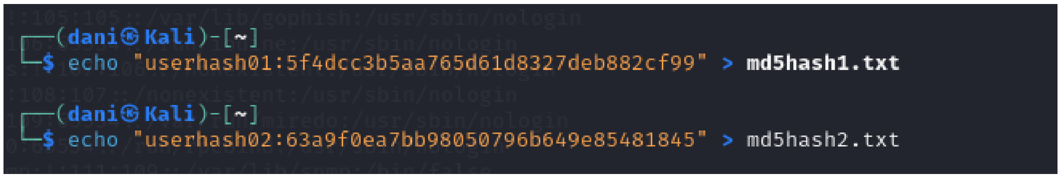
```
┌──(dani㉿Kali)-[~]
└─$ cat dcapl002.hash
user1:$y$j9T$wL20o8kdrZ0ks9GjYUSn01$2nmZxXwidb4f0gFwTCbLVlY/hYBfKbHXQELprmS0zb8:19996:0:99999:7:::
user2:$y$j9T$KPoe0zrRhMTltaFSM7iFC/$wotHYiWPCFJH6/KBKgnX2bWJx6MHuP5ZwXiVouF851A:19996:0:99999:7:::
user3:$y$j9T$UkaN8wj44XYS.au9Ie6kN0$RGRA9DuHByOB4hIae9P6jW0i8kxVzhWJzfTRf73e6rB:19996:0:99999:7:::
user4:$y$j9T$Qj5QGGV5RtktORBHBZnFW0$se/UNEhv.YDjk96P8FxjleJl.CCfIlXJ1TN48UiT2T3:19996:0:99999:7:::
user5:$y$j9T$leruPHZpdlsAqfqWUQ6B0/$Fo1Lj/uud4Ys6L25KRlHowYgsMDFHEGpcnxzrxkiZhC:19996:0:99999:7:::
user6:$y$j9T$wcF8xYFcz7.KbI4f7KQod0$mRDklMFsB2sFDNKAuLKUHVFP8auseRfLmsDIpBUfzP1:19996:0:99999:7:::

┌──(dani㉿Kali)-[~]
└─$ john --wordlist=rockyou.txt dcapl002.hash
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

┌──(dani㉿Kali)-[~]
└─$ john --format=crypt -wordlist=rockyou.txt dcapl002.hash
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded has
hes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:02:26 0.01% (ETA: 2024-10-19 04:49) 0g/s 10.48p/s 64.20c/s 64.20C/s clover..punkrock
0g 0:00:02:28 0.01% (ETA: 2024-10-19 10:54) 0g/s 10.37p/s 64.19c/s 64.19C/s clover..punkrock
0g 0:00:07:38 0.03% (ETA: 2024-10-19 00:55) 0g/s 10.89p/s 66.19c/s 66.19C/s christina1..elsalvador
0g 0:00:12:45 0.05% (ETA: 2024-10-19 09:16) 0g/s 10.65p/s 64.08c/s 64.08C/s hottie3..lollypop1
Session aborted

┌──(dani㉿Kali)-[~]
└─$ john --show dcapl002.hash
0 password hashes cracked, 0 left

┌──(dani㉿Kali)-[~]
└─$ john --format=crypt -wordlist=rockyou.txt dcapl002.hash
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded has
hes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:12 0.00% (ETA: 2024-10-13 16:07) 0g/s 7.465p/s 67.18c/s 67.18C/s daniela..november
Session aborted
```

John the ripper was able to crack the "newuser" user's password with a password of "welcome" in under a minute. In ten minutes, John the ripper was not able to crack any of the others.

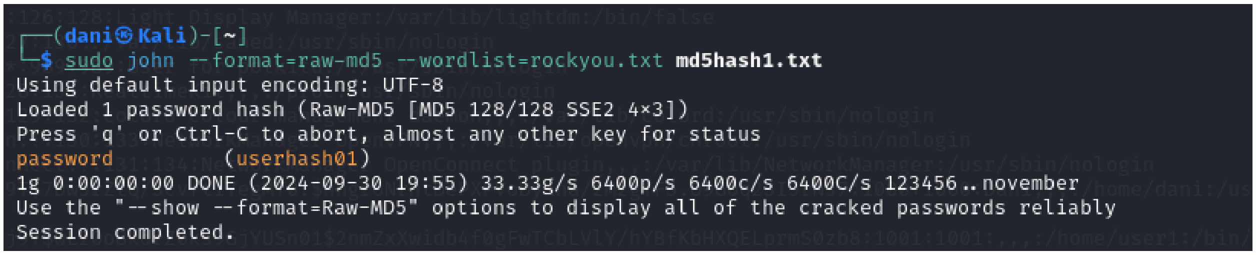
Extra credit (10 points):

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

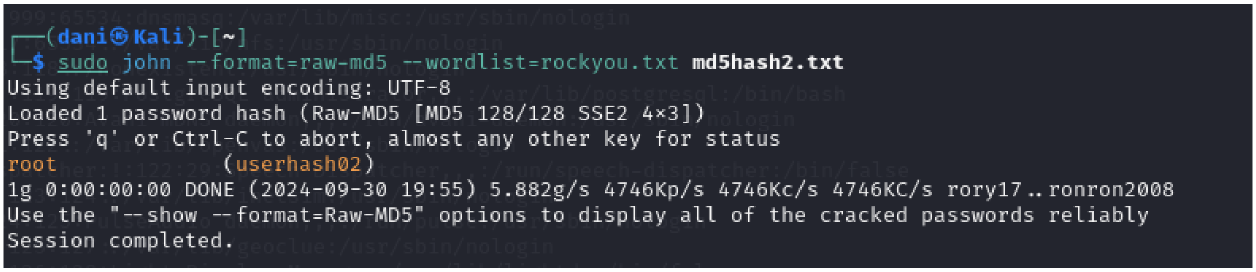
- 5f4dcc3b5aa765d61d8327deb882cf99
- 63a9f0ea7bb98050796b649e85481845



```
┌──(dani㉿Kali)-[~]
└─$ echo "userhash01:5f4dcc3b5aa765d61d8327deb882cf99" > md5hash1.txt

┌──(dani㉿Kali)-[~]
└─$ echo "userhash02:63a9f0ea7bb98050796b649e85481845" > md5hash2.txt
```



```
┌──(dani㉿Kali)-[~]
└─$ sudo john --format=raw-md5 --wordlist=rockyou.txt md5hash1.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (userhash01)
1g 0:00:00:00 DONE (2024-09-30 19:55) 33.33g/s 6400p/s 6400c/s 6400C/s 123456..november
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```



```
┌──(dani㉿Kali)-[~]
└─$ sudo john --format=raw-md5 --wordlist=rockyou.txt md5hash2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
root             (userhash02)
1g 0:00:00:00 DONE (2024-09-30 19:55) 5.882g/s 4746Kp/s 4746Kc/s 4746KC/s rory17..ronron2008
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```