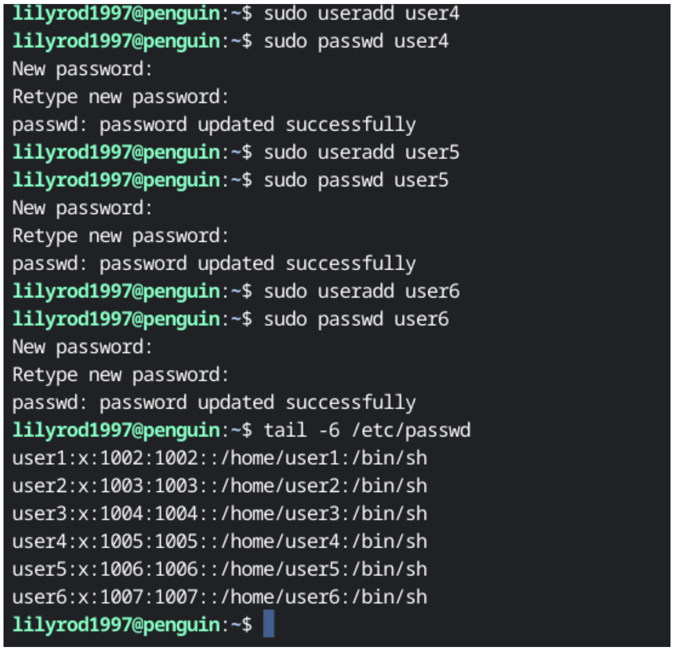
Lilibeth Rodriguez Sanchez

Assignment 5 Password Cracking

Task A: Password Cracking

Step 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.

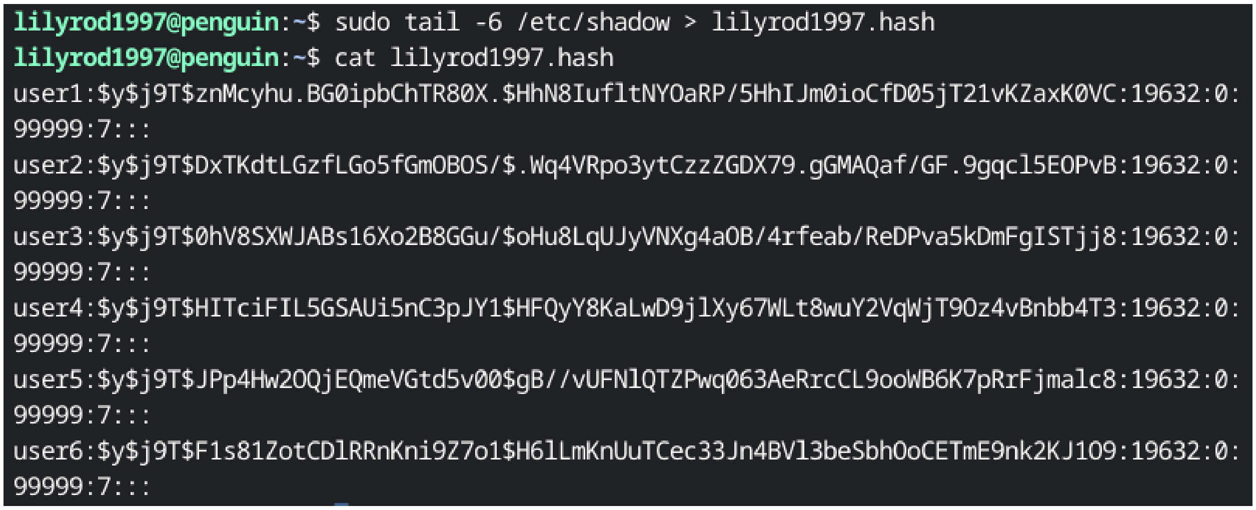


```
lilyrod1997@penguin:~$ sudo useradd user4
lilyrod1997@penguin:~$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully
lilyrod1997@penguin:~$ sudo useradd user5
lilyrod1997@penguin:~$ sudo passwd user5
New password:
Retype new password:
passwd: password updated successfully
lilyrod1997@penguin:~$ sudo useradd user6
lilyrod1997@penguin:~$ sudo passwd user6
New password:
Retype new password:
passwd: password updated successfully
lilyrod1997@penguin:~$ tail -6 /etc/passwd
user1:x:1002:1002::/home/user1:/bin/sh
user2:x:1003:1003::/home/user2:/bin/sh
user3:x:1004:1004::/home/user3:/bin/sh
user4:x:1005:1005::/home/user4:/bin/sh
user5:x:1006:1006::/home/user5:/bin/sh
user6:x:1007:1007::/home/user6:/bin/sh
lilyrod1997@penguin:~$
```

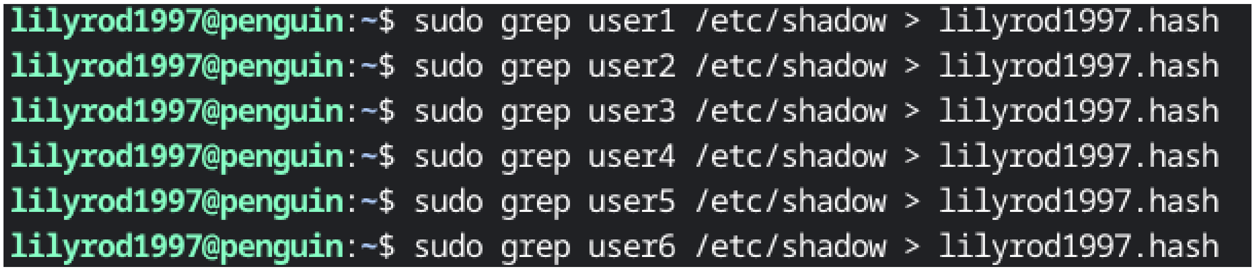
I used the command “sudo useradd user1” in order to add the new user into the system. After that I used “sudo passwd user1” in order to create the password as described in the instructions. I then used the command “ tail -6 /etc/passwd” just to verify that the users were created. Below are the usernames and passwords that were created based on the instructions per each user.

User1 : cow
User2: love
User3: cow123
User4: cow123@
User5: lovely123!
User6: Cat123#

Step 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).

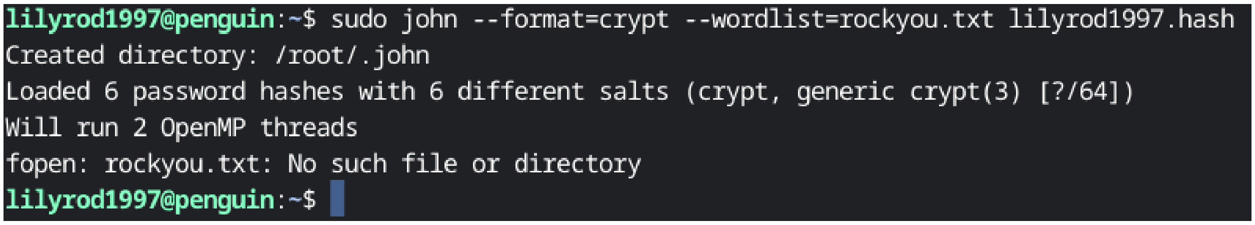


```
lilyrod1997@penguin:~$ sudo tail -6 /etc/shadow > lilyrod1997.hash
lilyrod1997@penguin:~$ cat lilyrod1997.hash
user1:$y$j9T$znMcyhu.BG0ipbChTR80X.$HhN8IufltNYOaRP/5HhIJm0ioCfD05jT21vKZaxK0VC:19632:0:
99999:7:::
user2:$y$j9T$DxTKdtLGzfLGo5fGmOBOS/$.Wq4VRpo3ytCzzZGDX79.gGMAQaf/GF.9gqcl5EOPvB:19632:0:
99999:7:::
user3:$y$j9T$0hV8SXWJABs16Xo2B8GGu/$oHu8LqUJyVNXg4aOB/4rfeab/ReDPva5kDmFgISTjj8:19632:0:
99999:7:::
user4:$y$j9T$HITciFIL5GSAUi5nC3pJY1$HFQyY8KaLwD9jlXy67WLt8wuY2VqWjT9Oz4vBnbb4T3:19632:0:
99999:7:::
user5:$y$j9T$JPp4Hw2OQjEQmeVGtd5v00$gB//vUFNlQTZPwq063AeRrcCL9ooWB6K7pRrFjmalc8:19632:0:
99999:7:::
user6:$y$j9T$F1s81ZotCDlRRnKni9Z7o1$H6lLmKnUuTCec33Jn4BVl3beSbhOoCETmE9nk2KJ1O9:19632:0:
99999:7:::
```



```
lilyrod1997@penguin:~$ sudo grep user1 /etc/shadow > lilyrod1997.hash
lilyrod1997@penguin:~$ sudo grep user2 /etc/shadow > lilyrod1997.hash
lilyrod1997@penguin:~$ sudo grep user3 /etc/shadow > lilyrod1997.hash
lilyrod1997@penguin:~$ sudo grep user4 /etc/shadow > lilyrod1997.hash
lilyrod1997@penguin:~$ sudo grep user5 /etc/shadow > lilyrod1997.hash
lilyrod1997@penguin:~$ sudo grep user6 /etc/shadow > lilyrod1997.hash
```

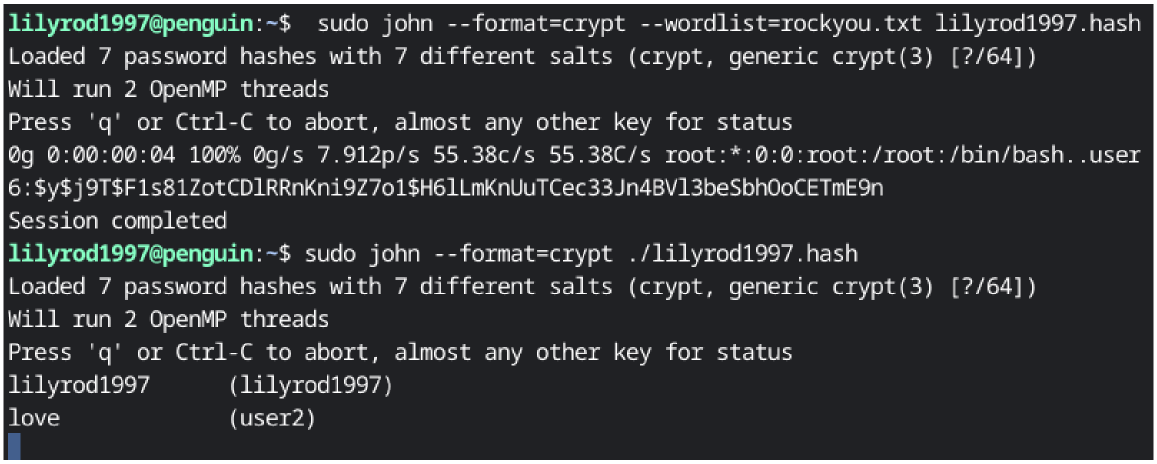
For this step I used “sudo grep user1 /etc/shadow > lilyrod1997.hash” command in order to export each user individually but then I noticed that it didnt show all users at once when using “cat lilyrod1997.hash” command therefore, I used “ sudo tail -6 /etc/shadow > lily.rod1997.hash” in order to export all last 6 users at once into lilyrod1997.hash. I then used “ cat lilyrod1997.hash” and confirmed that all users were exported.



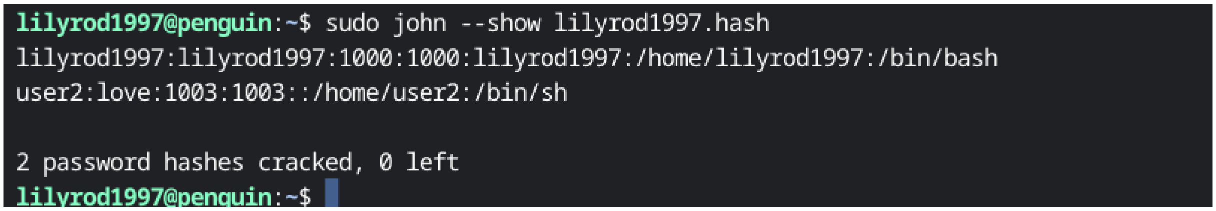
```
lilyrod1997@penguin:~$ sudo john --format=crypt --wordlist=rockyou.txt lilyrod1997.hash
Created directory: /root/.john
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Will run 2 OpenMP threads
fopen: rockyou.txt: No such file or directory
lilyrod1997@penguin:~$
```

In order to use John the ripper tool to crack the password in wordlist mode I used the command “ sudo john –format=crypt –wordlist=rockyou.txt lilyrod1997.hash” command and it appeared that 6 password hashes were loaded

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



```
lilyrod1997@penguin:~$  sudo john --format=crypt --wordlist=rockyou.txt lilyrod1997.hash
Loaded 7 password hashes with 7 different salts (crypt, generic crypt(3) [?/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:04 100% 0g/s 7.912p/s 55.38c/s 55.38C/s root:*:0:0:root:/root:/bin/bash..user
6:$y$j9T$F1s81ZotCDlRRnKni9Z7o1$H6lLmKnUuTCec33Jn4BVl3beSbhOoCETmE9n
Session completed
lilyrod1997@penguin:~$ sudo john --format=crypt ./lilyrod1997.hash
Loaded 7 password hashes with 7 different salts (crypt, generic crypt(3) [?/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
lilyrod1997      (lilyrod1997)
love             (user2)
```



```
lilyrod1997@penguin:~$ sudo john --show lilyrod1997.hash
lilyrod1997:lilyrod1997:1000:1000:lilyrod1997:/home/lilyrod1997:/bin/bash
user2:love:1003:1003::/home/user2:/bin/sh

2 password hashes cracked, 0 left
lilyrod1997@penguin:~$
```

I used the command “sudo john –format=crypt –wordlist=rockyou.txt lilyrod1997.hash and it loaded The password but wasnt able to crack them. So that is why I then used the command “ sudo john –format=crypt ./lilyrod1997.hash and that is when I was able to run John the ripper for 10 minutes And was able to crack 2 passwords. 1 of the passwords was one that I used for the users that I Created. In those 10 minutes none of the other users were loaded. I then used “sudo john –show Lilyrod1997.hash to show me the username and passwords that I was able to crack in those 10 Minutes.

Extra Credit: