Secure System Design: Threats and Countermeasures
CS392

Name: Arunika Yadav

Roll No. :1601CS56

Date: 26th Mar 2019 **Assignment 5**
Submission Filename: assign5.pdf **Due Date: 30th Mar 2019 Full Marks 40**

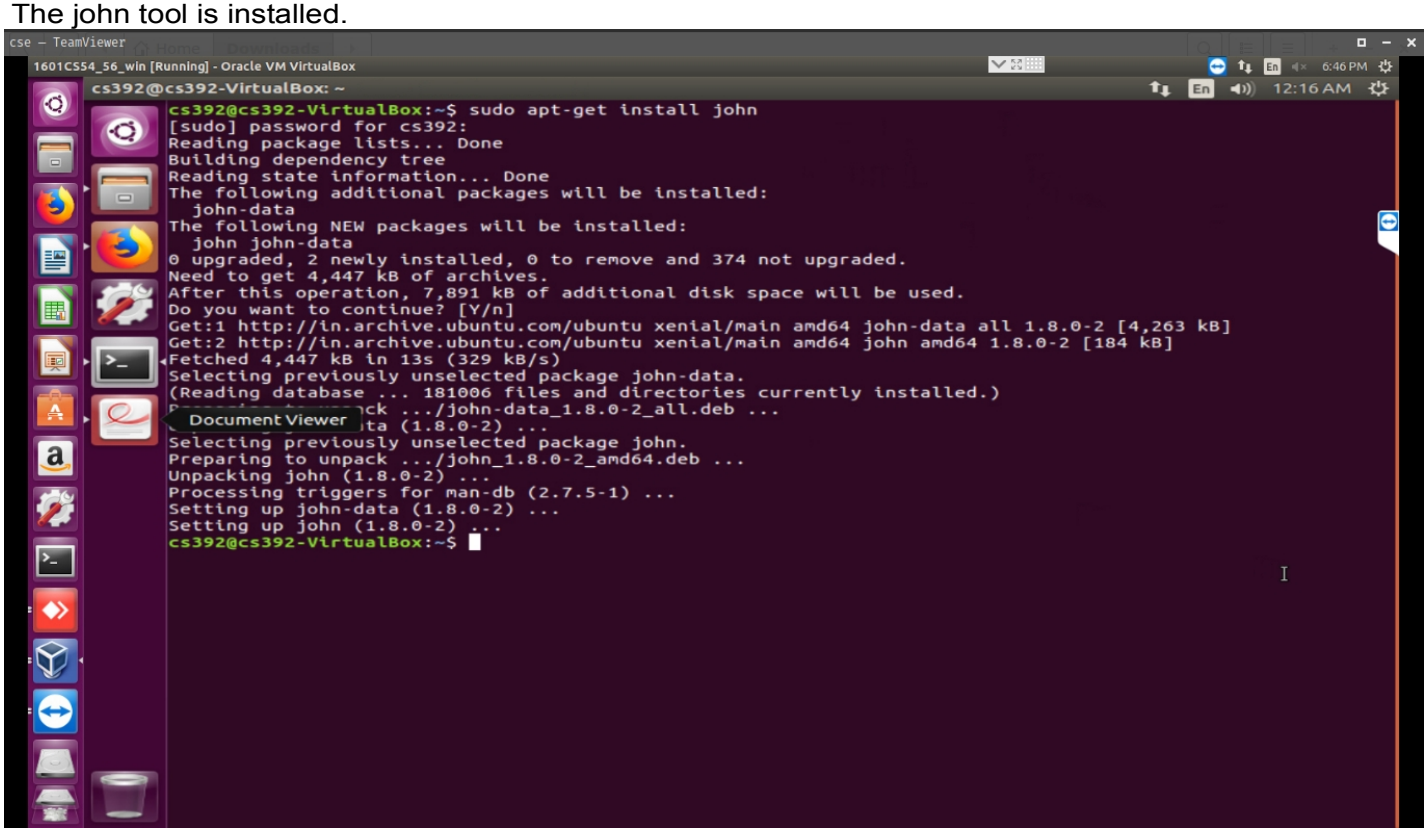
1 Assignment Overview

The learning objective of this assignment is for students to gain the first-hand experience on using password cracking tool to check for the weak passwords. A system administrator needs to be careful that users should not use easy to crack passwords.

For this experiment, you can use *John The Ripper* [1] tool, also known as john. This tool uses a dictionary or a search pattern to check for passwords. To install this tool, you may use the folwoing command

$sudo apt-get install john

The john tool is installed.



Now, use *su* command and change to root. After then, create a folder named *test*. Change its permission to 777 by using *chmod* command.

User changed to root and test folder created and its permissions are changed.

```
cs392@cs392-VirtualBox:~$ su root
Password:
root@cs392-VirtualBox:/home/cs392# mkdir test
root@cs392-VirtualBox:/home/cs392# ls -al test
total 8
drwxr-xr-x  2 root  root  4096 Mar 29 00:32 .
drwxr-xr-x 26 cs392 cs392 4096 Mar 29 00:32 ..
root@cs392-VirtualBox:/home/cs392# ls -al | grep test
drwxrwxr-x 11 cs392 cs392      4096 Mar 14 14:59 oftest
drwxr-xr-x  2 root  root       4096 Mar 29 00:32 test
root@cs392-VirtualBox:/home/cs392# chmod test 777
chmod: invalid mode: 'test'
Try 'chmod --help' for more information.
root@cs392-VirtualBox:/home/cs392# chmod 777 test
root@cs392-VirtualBox:/home/cs392# ls -al | grep test
drwxrwxr-x 11 cs392 cs392      4096 Mar 14 14:59 oftest
drwxrwxrwx  2 root  root       4096 Mar 29 00:32 test
root@cs392-VirtualBox:/home/cs392#
```

Now, goto *test* folder and get a *wordlist* dictionary. You can use the following command to get a dictionary of *wordlist*.

#wget http://scrapmaker.com/data/wordlists/dictionaries/rockyou.txt

Once the *wordlist* file is downloaded then you can add user using *adduser* command and create an account for a new user. Let's create an account with username alice and password alice. You can check */etc/shadow* file to check the entry of that new user's account. The password of that new user is now stored using salted hash function. Now, we can use john to find whether the password can be cracked or not. If it is available in the *wordlist* file then it should show the corresponding password against the username. For this following command can be used-

#john --wordlist=rockyou.txt /etc/shadow

John comes with a word list that it uses by default. This is quite good, but to crack more and more secure passwords, you then need a word list with more words. Hence the rockyou.txt is downloaded and the user alice is added.

```
root@cs392-VirtualBox: /home/cs392/test
chmod: invalid mode: 'test'
Try 'chmod --help' for more information.
root@cs392-VirtualBox:/home/cs392# chmod 777 test
root@cs392-VirtualBox:/home/cs392# ls -al | grep test
drwxrwxr-x 11 cs392 cs392      4096 Mar 14 14:59 oftest
drwxrwxrwx  2 root  root       4096 Mar 29 00:32 test
root@cs392-VirtualBox:/home/cs392# cd test
root@cs392-VirtualBox:/home/cs392/test# wget http://scrapmaker.com/data/wordlists/dictionaries/rockyou.tx
t
--2019-03-29 00:36:03--  http://scrapmaker.com/data/wordlists/dictionaries/rockyou.txt
Resolving scrapmaker.com (scrapmaker.com)... 192.254.232.166
Connecting to scrapmaker.com (scrapmaker.com)|192.254.232.166|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.scrapmaker.com/data/wordlists/dictionaries/rockyou.txt [following]
--2019-03-29 00:36:05--  https://www.scrapmaker.com/data/wordlists/dictionaries/rockyou.txt
Resolving www.scrapmaker.com (www.scrapmaker.com)... 192.254.232.166
Connecting to www.scrapmaker.com (www.scrapmaker.com)|192.254.232.166|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 139921497 (133M) [text/plain]
Saving to: 'rockyou.txt'

rockyou.txt                 100%[===================================>] 133.44M  2.84MB/s    in 42s

2019-03-29 00:36:49 (3.21 MB/s) - 'rockyou.txt' saved [139921497/139921497]

root@cs392-VirtualBox:/home/cs392/test# adduser alice
Adding user `alice' ...
Adding new group `alice' (1001) ...
Adding new user `alice' (1001) with group `alice' ...
Creating home directory `/home/alice' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for alice
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
root@cs392-VirtualBox:/home/cs392/test#
```

```
whoopsie:*:16911:0:99999:7:::
avahi-autoipd:*:16911:0:99999:7:::
avahi:*:16911:0:99999:7:::
dnsmasq:*:16911:0:99999:7:::
colord:*:16911:0:99999:7:::
speech-dispatcher:!:16911:0:99999:7:::
hplip:*:16911:0:99999:7:::
kernoops:*:16911:0:99999:7:::
pulse:*:16911:0:99999:7:::
rtkit:*:16911:0:99999:7:::
saned:*:16911:0:99999:7:::
usbmux:*:16911:0:99999:7:::
cs392:$6$gsiHltNB$IfsAmIl29dPZ5tLHs95kKnJ4QZNBMBYVgcSm0JyzhjipggPAeoFEUYgRVeg5fcqVaIWnwJ7a5aAgxcGJ22AcJ0:
17918:0:99999:7:::
sshd:*:17969:0:99999:7:::
alice:$6$G3apUe0U$42qIrXdFgtU4KimkIdSRkz81dPmrAXwLByjANi1qpcLNbPYlc9HqHnlhipHJqrijNMIhM/FjaJL8yXQVOsWAZ1:
17983:0:99999:7:::
root@cs392-VirtualBox:/home/cs392/test#
```

The command to find the password for the user alice is run with the rockyou.txt being used as the default dictionary.

```
alice:$6$G3apUe0U$42qIrXdFgtU4KimkIdSRkz81dPmrAXwLByjANi1qpcLNbPYlc9HqHnlhipHJqrijNMIhM/FjaJL8yXQVOsWAZ1:
17983:0:99999:7:::
root@cs392-VirtualBox:/home/cs392/test# john --wordlist=rockyou.txt /etc/shadow
Created directory: /root/.john
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
computer         (root)
computer         (cs392)
```

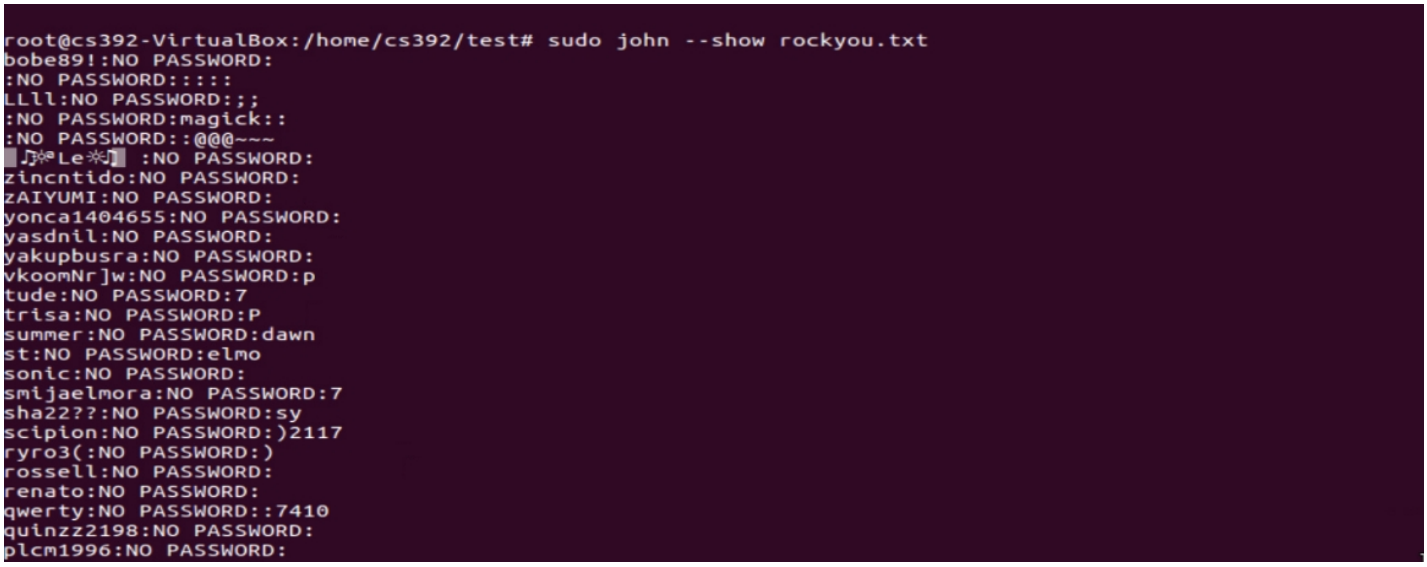
The john tool is able to crack 3 passwords in 6 seconds as is seen in the output below. The password for the user alice is found and displayed against her name. All the hashes in the /etc/shadow files are compared with the hashes generated by the john tool from the passwords in the wordlist. It tries this password on all hashes in our file so the more usernames we give it the more chances that it will be cracked. John has the ability to take a wordlist and mangle the words in it to try variations of that word. It will add numbers to the end of the word and try replacing letters with numbers and adding other random symbols.

```
root@cs392-VirtualBox: /home/cs392/test
www-data:*:16911:0:99999:7:::
backup:*:16911:0:99999:7:::
list:*:16911:0:99999:7:::
irc:*:16911:0:99999:7:::
gnats:*:16911:0:99999:7:::
nobody:*:16911:0:99999:7:::
systemd-timesync:*:16911:0:99999:7:::
systemd-network:*:16911:0:99999:7:::
systemd-resolve:*:16911:0:99999:7:::
systemd-bus-proxy:*:16911:0:99999:7:::
syslog:*:16911:0:99999:7:::
_apt:*:16911:0:99999:7:::
messagebus:*:16911:0:99999:7:::
uuidd:*:16911:0:99999:7:::
lightdm:*:16911:0:99999:7:::
whoopsie:*:16911:0:99999:7:::
avahi-autoipd:*:16911:0:99999:7:::
avahi:*:16911:0:99999:7:::
dnsmasq:*:16911:0:99999:7:::
colord:*:16911:0:99999:7:::
speech-dispatcher:!:16911:0:99999:7:::
hplip:*:16911:0:99999:7:::
kernoops:*:16911:0:99999:7:::
pulse:*:16911:0:99999:7:::
rtkit:*:16911:0:99999:7:::
saned:*:16911:0:99999:7:::
usbmux:*:16911:0:99999:7:::
cs392:$6$gsiHltNB$IfsAmIl29dPZ5tLHs95kKnJ4QZNBMBYVgcSm0JyzhjipggPAeoFEUYgRVeg5fcqVaIWnwJ7a5aAgxcGJ22AcJ0:
17918:0:99999:7:::
sshd:*:17969:0:99999:7:::
alice:$6$G3apUe0U$42qIrXdFgtU4KimkIdSRkz81dPmrAXwLByjANi1qpcLNbPYlc9HqHnlhipHJqrijNMIhM/FjaJL8yXQVOsWAZ1:
17983:0:99999:7:::
root@cs392-VirtualBox:/home/cs392/test# john --wordlist=rockyou.txt /etc/shadow
Created directory: /root/.john
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
computer         (root)
computer         (cs392)
alice            (alice)
3g 0:00:00:06 100% 0.4457g/s 399.4p/s 427.9c/s 427.9C/s star123..nugget
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@cs392-VirtualBox:/home/cs392/test#
```

This will try to explore all the hashed entries of */etc/shadow* with specified *rockyou wordlist*. Please note that it is a time taking task. If no *wordlist* is specified then system will use the default *wordlist*. Also, if you want to check the already cracked passwords from a password file then the following command can be used

$sudo john --show passwordFilename

The above command is used to see the number of passwords cracked by the rockyou.txt dictionary when used by the john tool.



```
root@cs392-VirtualBox:/home/cs392/test# sudo john --show rockyou.txt
bobe89!:NO PASSWORD:
:NO PASSWORD:::::
LLll:NO PASSWORD:;;
:NO PASSWORD:magick::
:NO PASSWORD::@@@~~~
[illegible] :NO PASSWORD:
zincntido:NO PASSWORD:
zAIYUMI:NO PASSWORD:
yonca1404655:NO PASSWORD:
yasdnil:NO PASSWORD:
yakupbusra:NO PASSWORD:
vkoomNr]w:NO PASSWORD:p
tude:NO PASSWORD:7
trisa:NO PASSWORD:P
summer:NO PASSWORD:dawn
st:NO PASSWORD:elmo
sonic:NO PASSWORD:
smijaelmora:NO PASSWORD:7
sha22??:NO PASSWORD:sy
scipion:NO PASSWORD:)2117
ryro3(:NO PASSWORD:)
rossell:NO PASSWORD:
renato:NO PASSWORD:
qwerty:NO PASSWORD::7410
quinzz2198:NO PASSWORD:
plcm1996:NO PASSWORD:
```

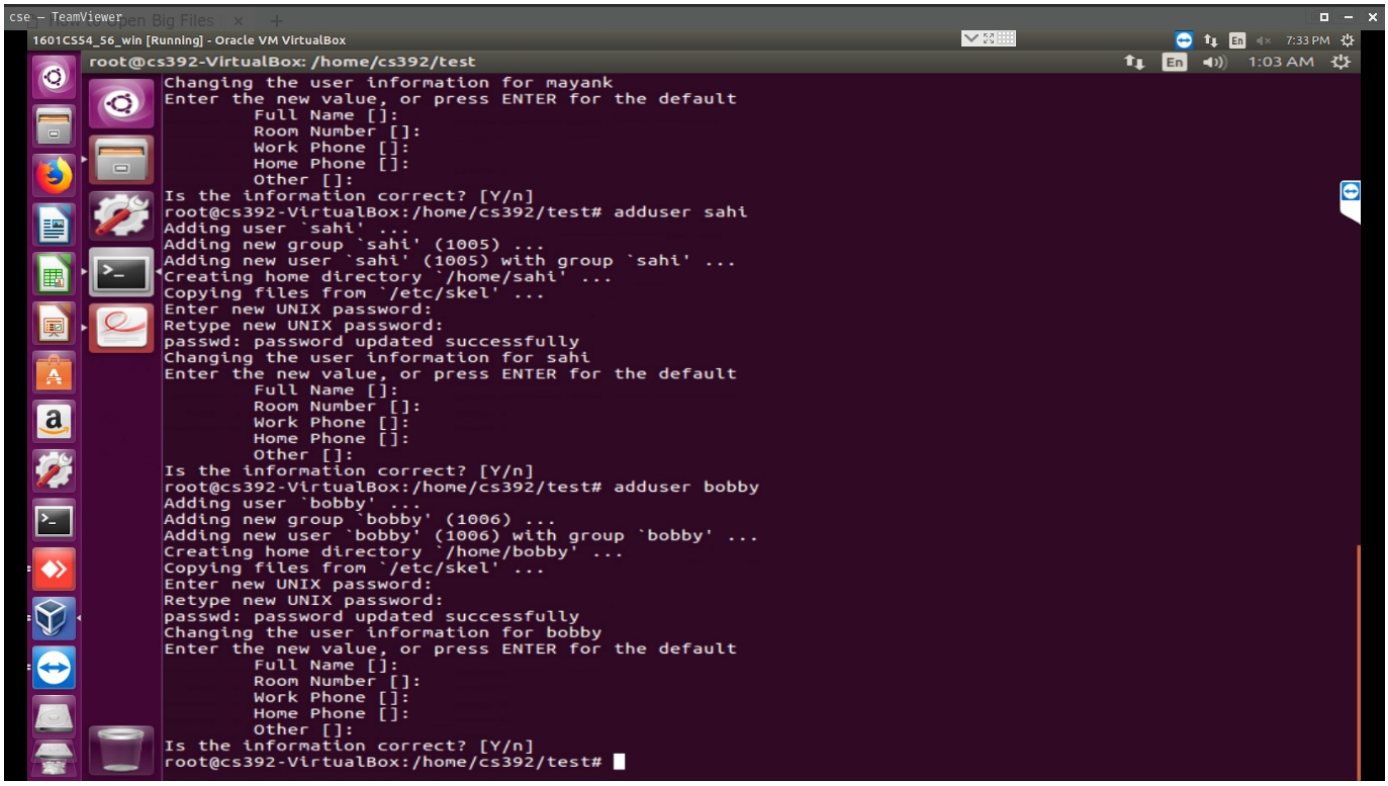
```
01793480473:NO PASSWORD::
.lcl:NO PASSWORD:
.:NO PASSWORD:vermilion2::.
.:NO PASSWORD:tay::.
.:NO PASSWORD:tamcara::.
.:NO PASSWORD:skate::.
.:NO PASSWORD:sharney::
.:NO PASSWORD:lol::.
.:NO PASSWORD:liz5::.
.:NO PASSWORD:Hello
.:NO PASSWORD:C..R..E..E..D.::
.:NO PASSWORD:Arakun::.
.:NO PASSWORD:.thedock.::.
..:NO PASSWORD:puddles::..
..:NO PASSWORD:porqueami::..
..:NO PASSWORD:mali:;..
..:NO PASSWORD:laura::..
..:NO PASSWORD:Marissa::..
...:NO PASSWORD::[blt]:::...
...:NO PASSWORD::
'wsn:NO PASSWORD:

182 password hashes crac[illegible]2
root@cs392-VirtualBox:/h[illegible]cs[illegible]te
```

Now, add 5 users as per followings-

- **Add two users and their passwords will be chosen from the *rockyou wordlist* file.**
- **Add one user with password as the reverse of the *username*.**
- **Add one user with password as the 123 extension of the *username*. So if the *username* is *bob* then password will be**
  bob123
- **Add one user with randomly generated strong password**

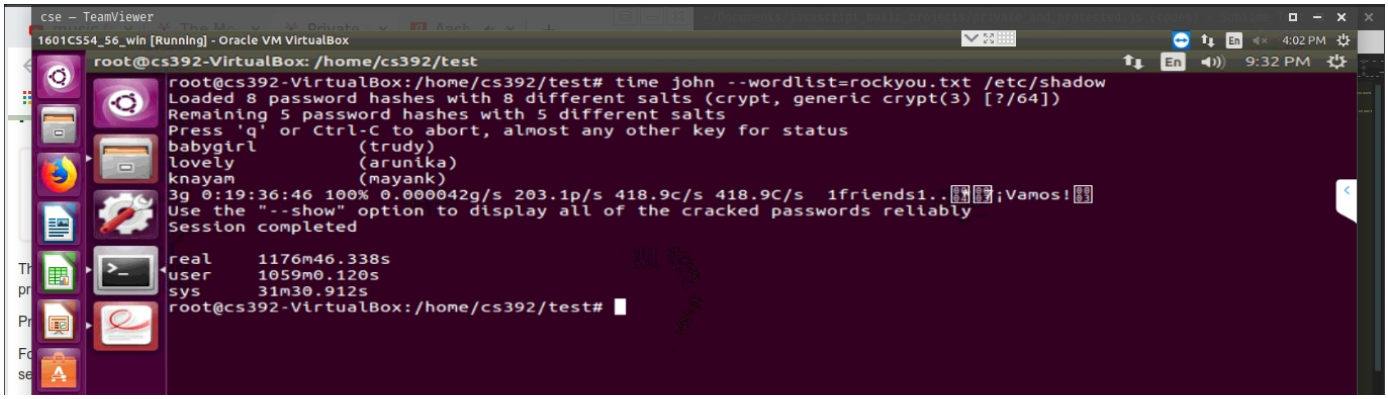
Now your task is to crack the passwords using john tool. Report whether you can crack all the passwords and also the time needed to crack them. To check time requirement, you can use the *time* command.

The 5 users are added as given above with the password criteria.



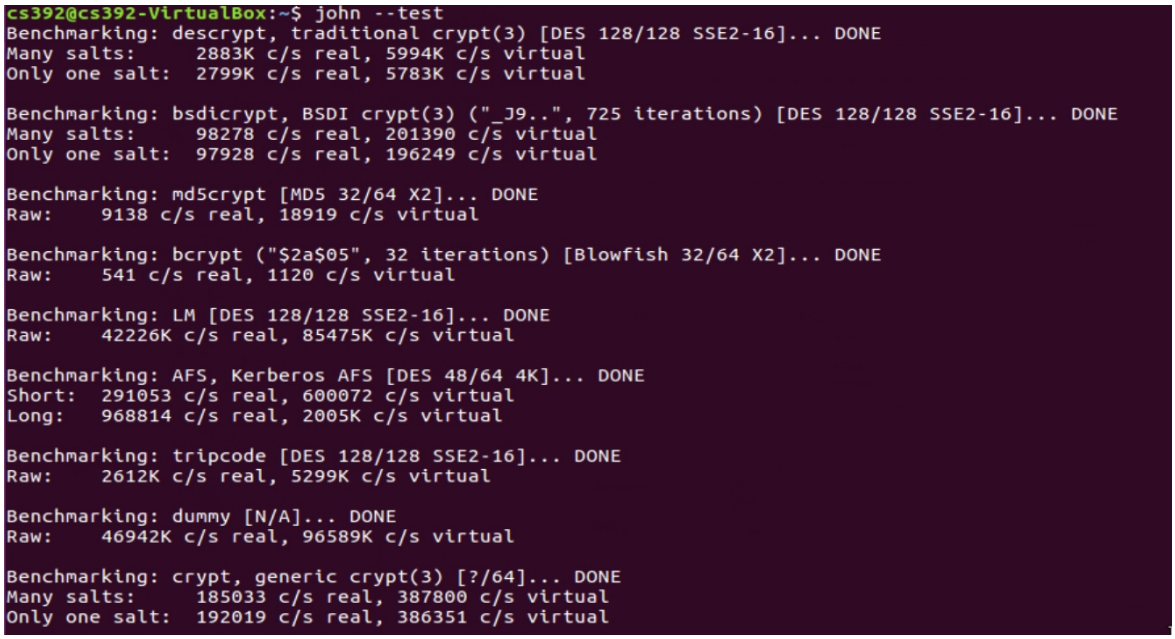
The same is shown by displaying the contents of the /*etc*/shadow file:

The status of the john tool is as shown below:

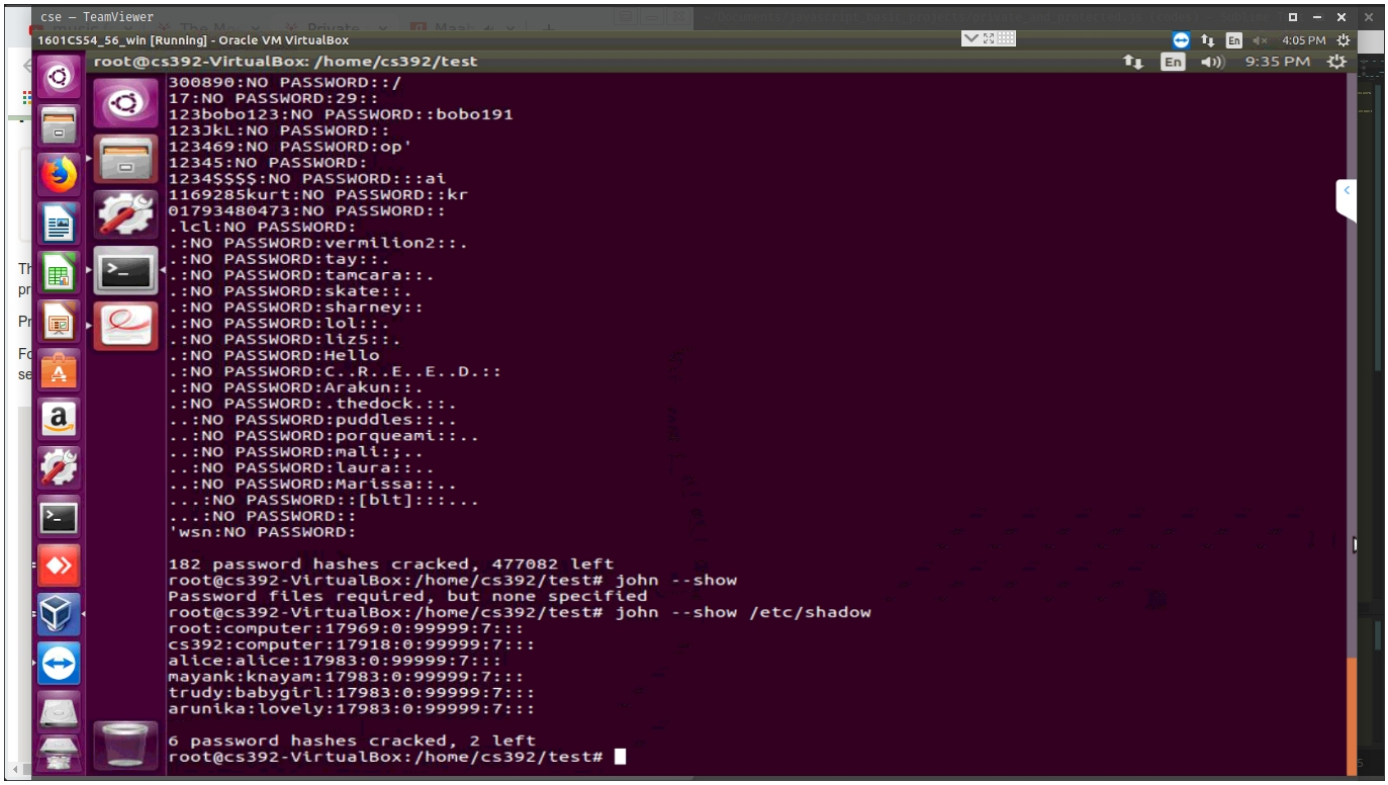


It took a little over **19 hours** to break 3 passwords out of the 5 kinds of passwords that were entered. The passwords which could not be cracked, were not able to be found by the john tool using the reverse hashing technique and hence not cracked.

The speed (combinations/second) at which the different hashing algorithms hash the password are given as follows:



Also the time taken to crack the passwords depends upon the position of the password in the dictionary. Also the passwords of the user sahi(sahi123) and of bobby(b1Fc9by) could not be cracked by the john tool.



The total number of passwords that were cracked using the /etc/shadow file are shown using the command john --show /etc/shadow. The 2 passwords which could not be cracked and the 6 passwords which could be cracked is shown above.

2 Submission

You need to submit a detailed report to describe what you have done and what you have observed; you also need to provide explanation to the observations that are interesting or surprising. Attach supporting snapshots wherever possible.