G.FARAZ

TOOL NAME:JOHN THE RIPPER

What I learned from the project?

At any circumstances at any situation any password can be cracked by the john the ripper. If the password is very simple and easy to find the dictionary then the password is easily cracked in seconds by the john the ripper tool. But when the password is little bit long than 8 char value then tool takes much longer time to crack the password by entering into the incremental mode and finally the jtr can crack the password By which we can say any password in the world can be cracked.

What can we further improve in these project?

By finding effect ways of cracking password easily without invoking the jtr into the incremental mode. If new methods of cracking password easily can make the jtr much better tool. By which with in a short period of time the jtr can crack the password whose length is greater than 8 char.

What is john the ripper?

This manual page documents briefly the john command. This manual page was written for the Debian GNU/Linux distribution because the original program does not have a manual page. john, better known

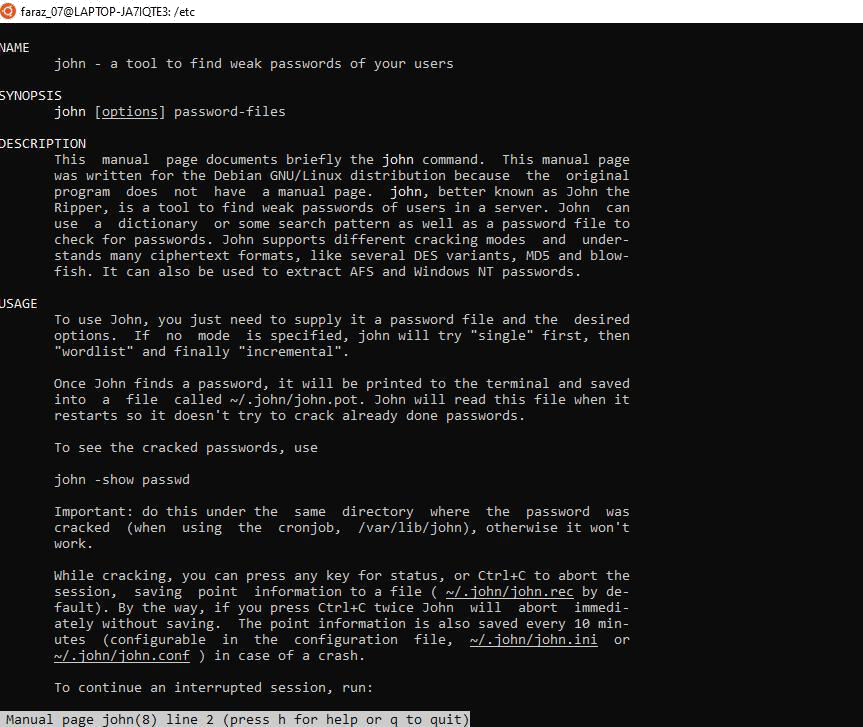
as John the Ripper is a tool to find weak passwords of users in a server. John can use a dictionary or some search patern as well as a password file to check for passwords. John supports different cracking modes and understand many cipher text formats, like several DES variants, MD5 and blowfish. It can also be used to extract AFS and Windows NT passwords.

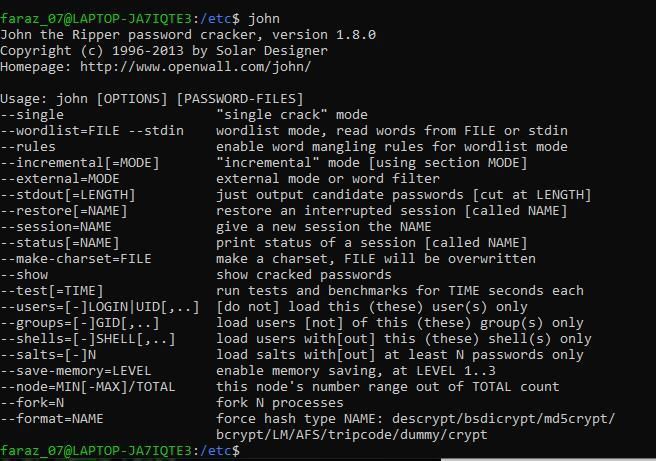
To use John, you just need to supply it a password file and the desired options. If no mode is specified, john

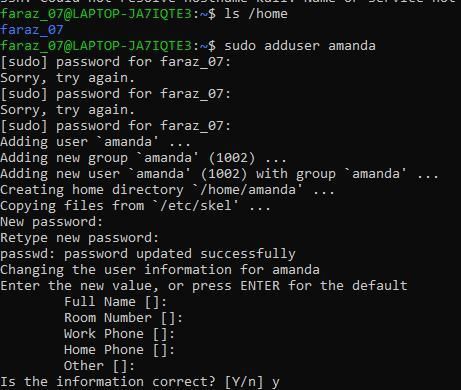
will try "single" first, then "wordlist" and finally "incremental". Once John finds a password, it will be printed to the terminal and saved into a file called ~/.john/john.pot.

John will read this file when it restarts so it doesn't try to crack already done passwords.

To see the cracked passwords, use: john -show passwd

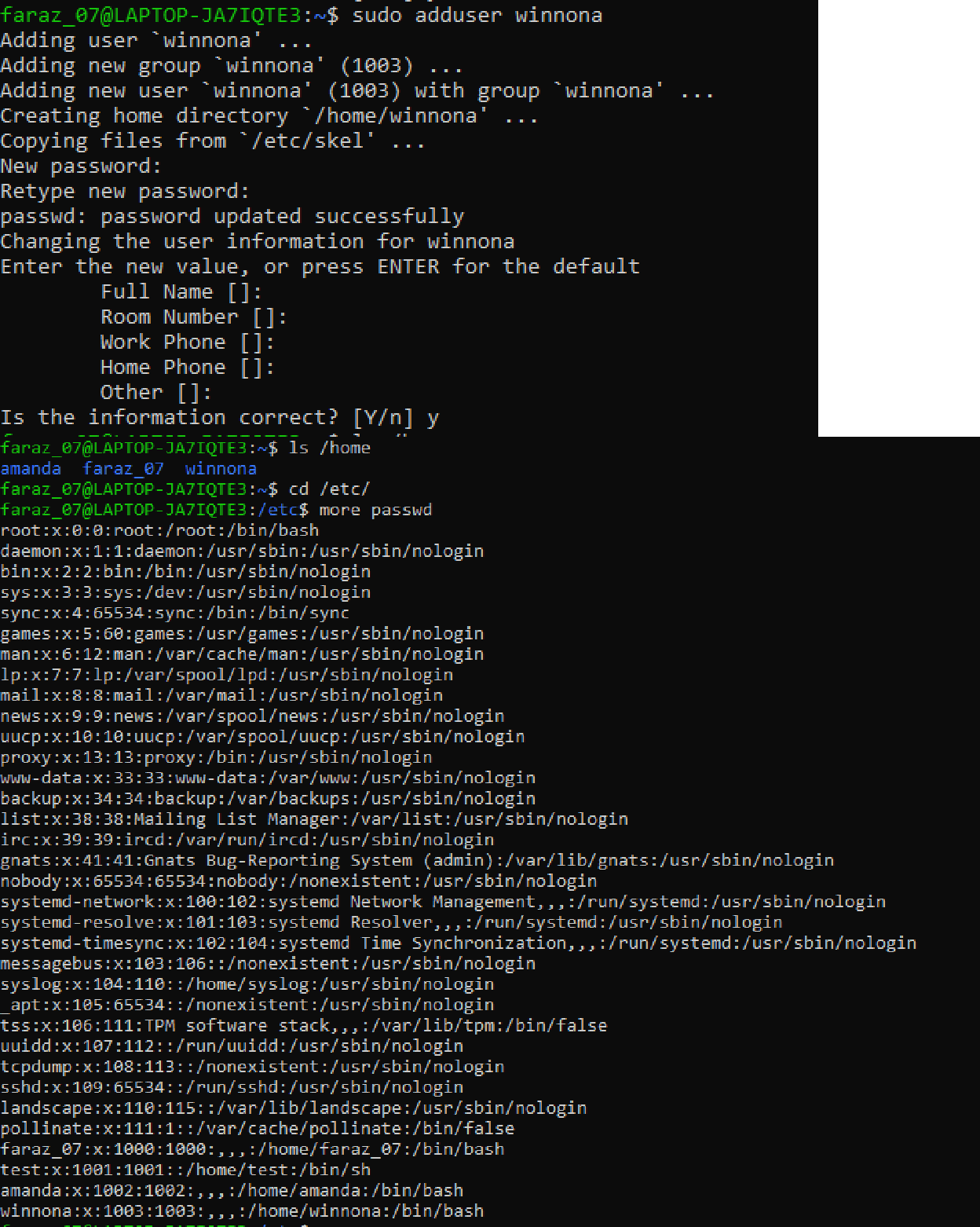




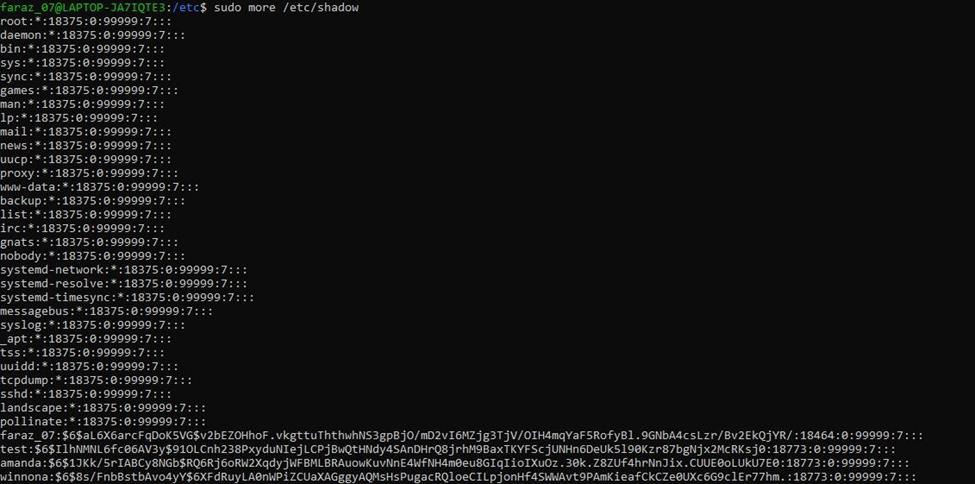


The password is going to be stored in the hash form because to protect the user from the third party attacks in the above picture you notice that the password is being asked before entering the person into the database of the system. so, for protecting the system from the third attackers the system hash the password.

The user is added with command sudo adduser amanda . We are going to add another user into the system.



In the linux system the user name and password are stored in the etc directory file name called passwd. You can view the command in the above picture.



In the new version of the linux the password are stored in a different file called shadow file You view the password by using the command:-/etc sudo more/etc shadow.

Understanding /etc/shadow file fields/format

Basically, the /etc/shadow file stores secure user account information. All fields are separated by a colon

(:) symbol. It contains one entry per line for each user listed in [/etc/passwd file.](https://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/) Generally, shadow file entry looks as follows (click to enlarge image):

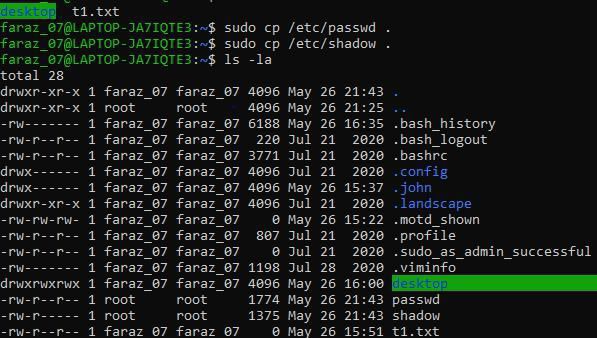
(Fig.01: /etc/shadow file fields)

1. **Username** : It is your login name.
2. **Password** : It is your encrypted password. The password should be minimum 8-12 characters long including special characters, digits, lower case alphabetic and more. Usually password format is set to $id$salt$hashed, The $id is the algorithm used On GNU/Linux as follows:
   1. **$1$** is MD5
   2. **$2a$** is Blowfish
   3. **$2y$** is Blowfish

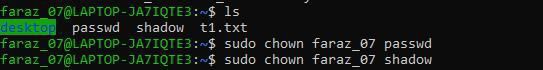
4. **$5$** is SHA-256

5. **$6$** is SHA-512

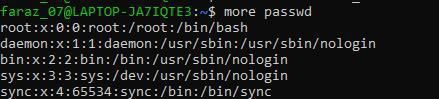
1. **Last password change (lastchanged)** : Days since Jan 1, 1970 that password was last changed

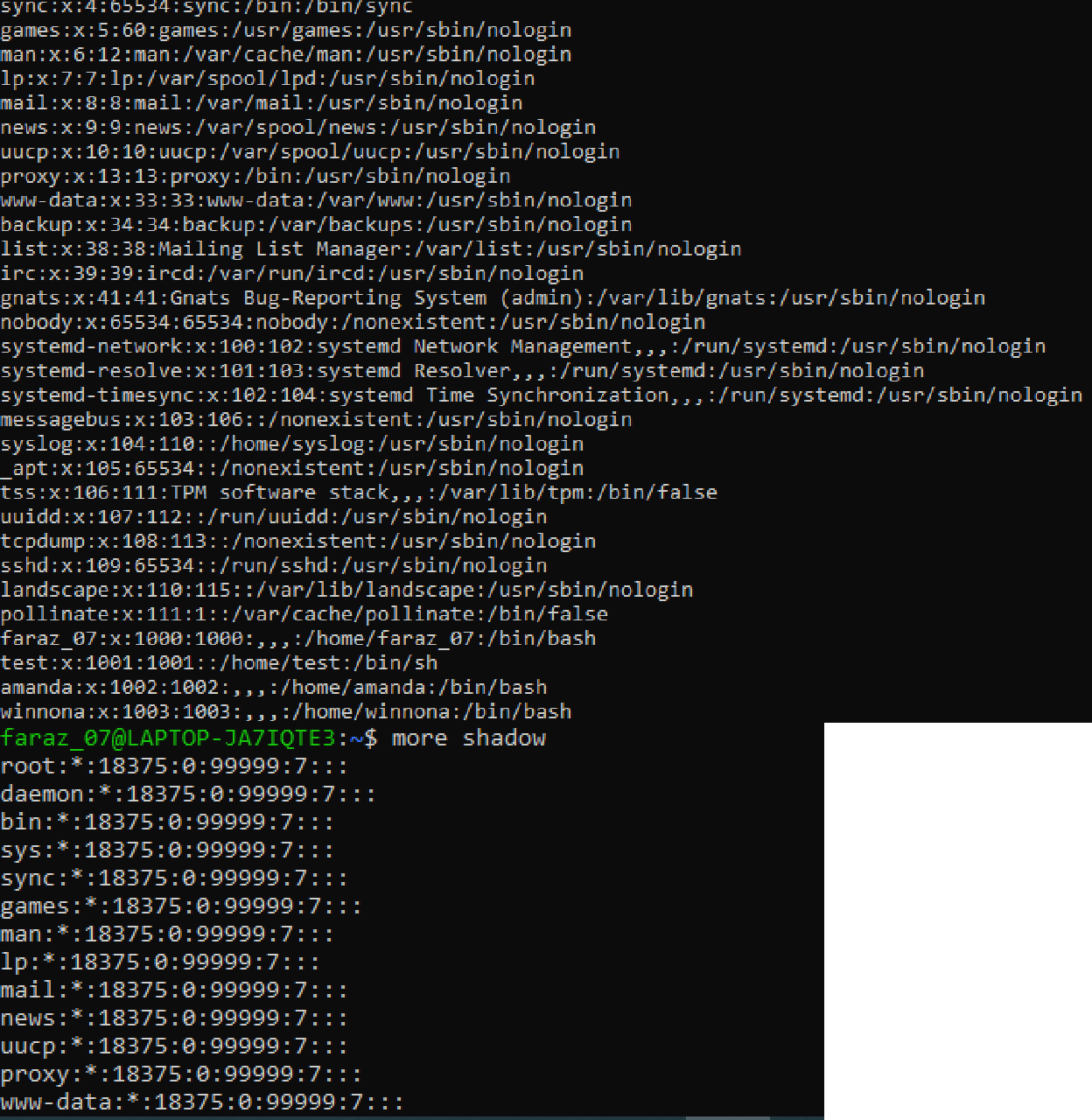


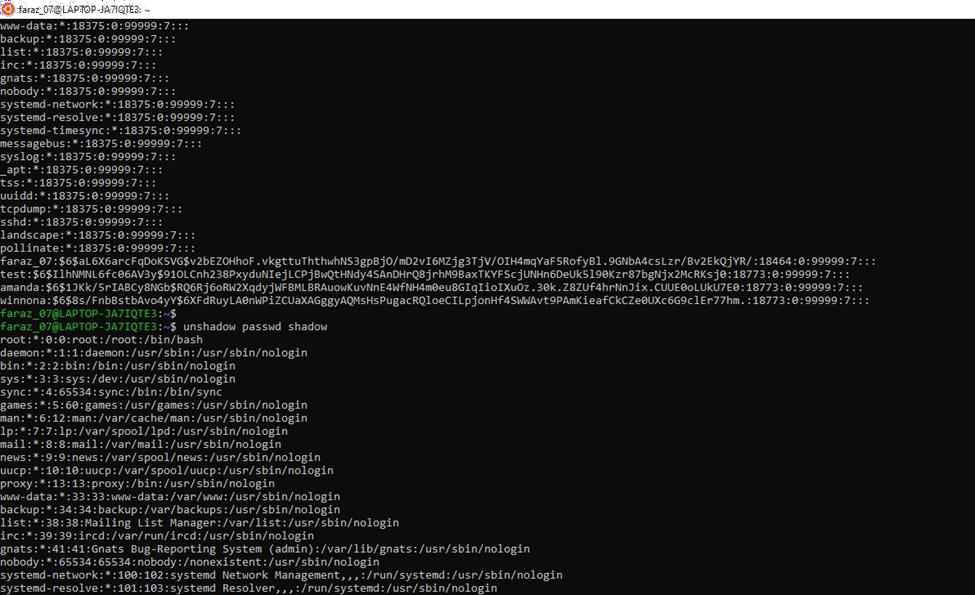
We copy the files of password and the shadow file.



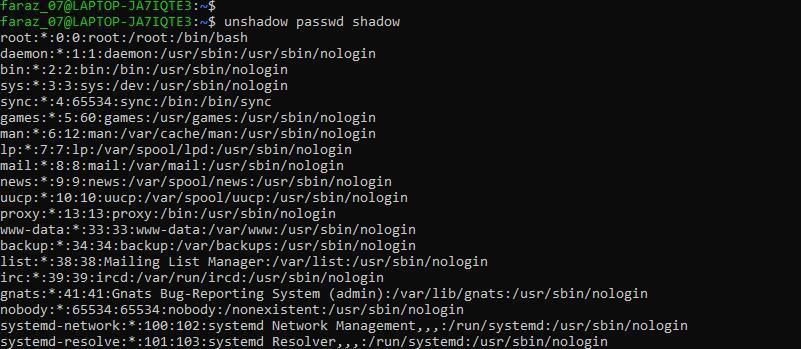
We change the

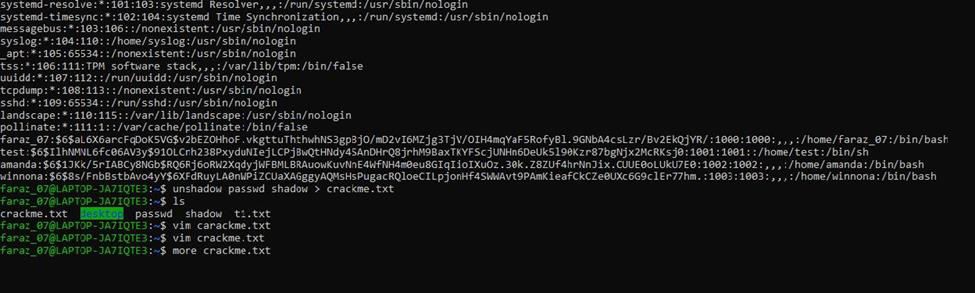


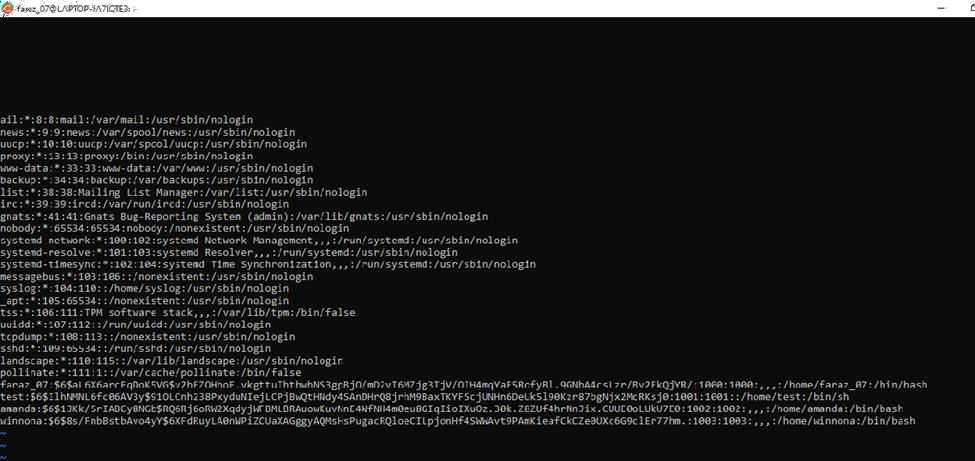




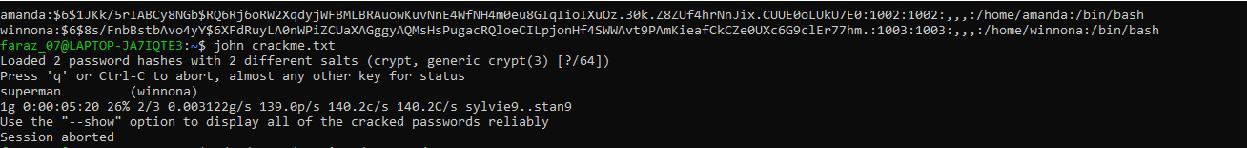
For combine the passwd and shadow file we use the unshadow tool in john the ripper which combines both these shadow file and passwd file.







After doing the above step we delete all the unwanted data in the file and save the file with the last two user which we are entered into the system.



After doing the last step we crack the password of the user by using the command :- john filename

.With these the password of the user is going to be cracked and displayed. In the process of cracking the password the john the ripper uses the

After finishing the combinations of two files the output of those files are saved into a separate file called the crackme.txt.

To use John, you just need to supply it a password file and the desired options. If no mode is specified, john will try "single" first, then "wordlist" and finally "incremental**”**.

For terminating the session press ctrl c .