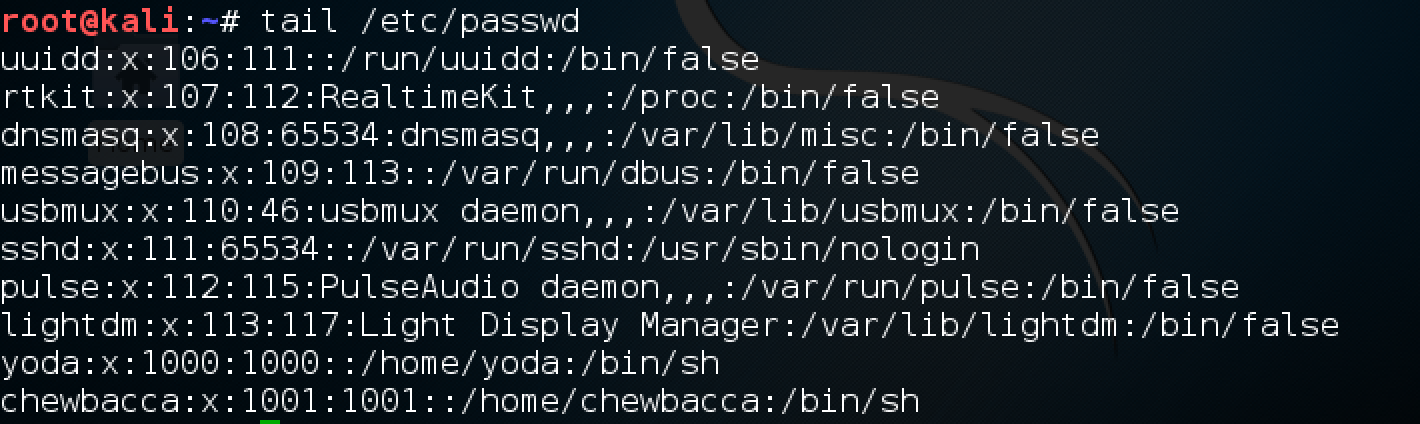
CSCI 345 Lab 3

Brandi Durham and Andrew Miller

1. ls -l /etc/passwd

-rw-r--r-- 1 root root 1721 Aug 30 2016 /etc/passwd

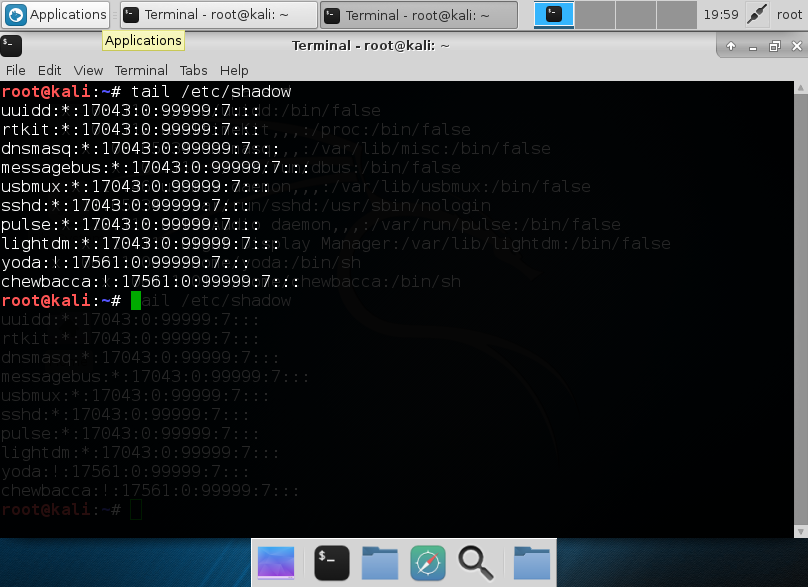
First ‘-’ means it is not a directory, ‘re-’ means the owner has permission to read and write to the file, the ‘r--’ means that the group only has permission to read and the last if for other/world who only has permission to read.

2) 

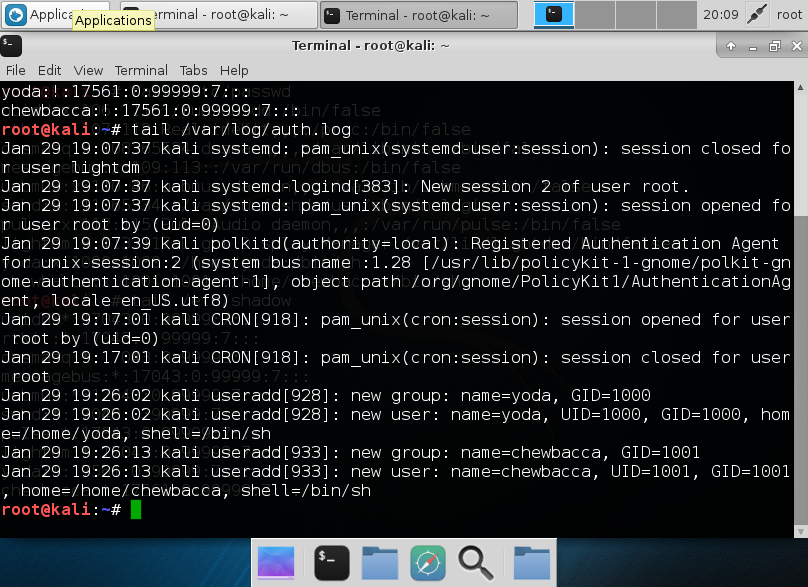
The file shows user name, encrypted password, user ID number, user’s group ID number, full name of the user, user home directory, login shell.

3) Why is there a “!” in place of a password for the new users?

If the user ID has a password then the field will have an !, else it will have an \*.



4) What information does this log give you about the new users?

Gives username, user ID, and group ID, default shell and time of creation. 

5) Why are the two hashes different even though the passwords are the same?

The could have used a salt in addition to the password using other information such as time of creation or username or user ID.

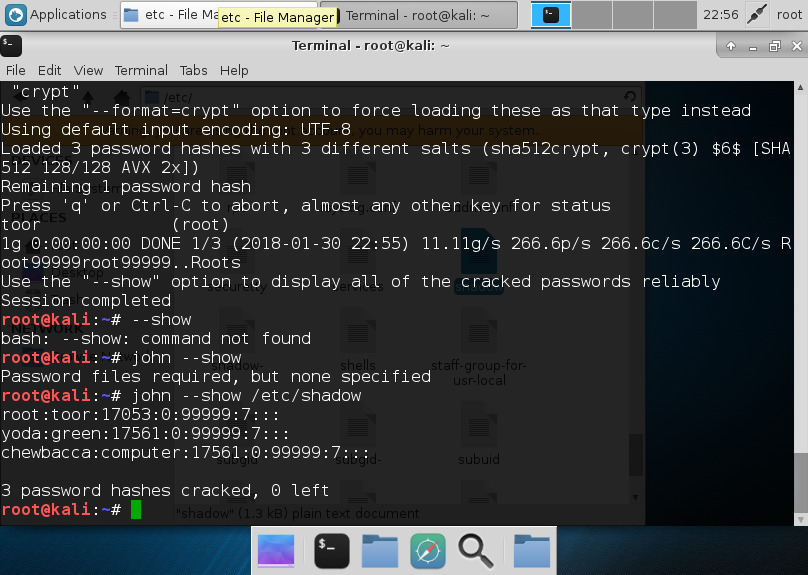
6) Command that will crack the /etc/shadow file :

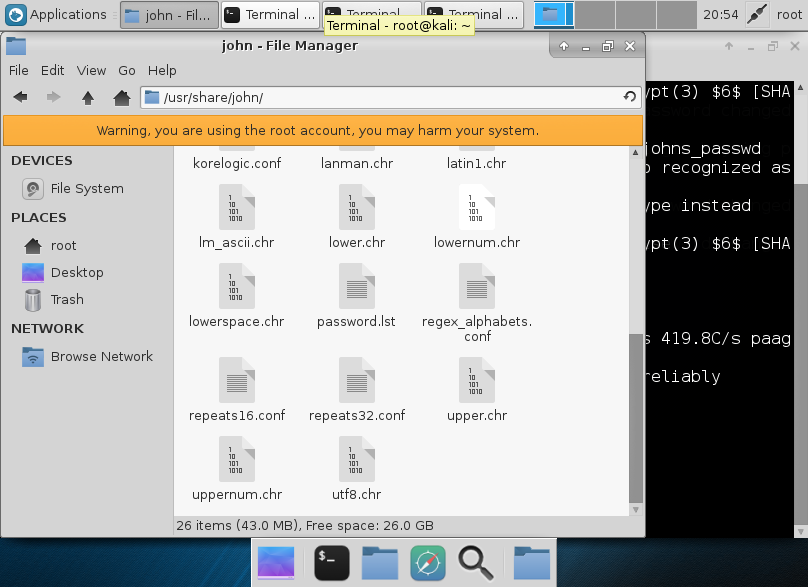
john --show /etc/shadow (not using wordlist)

john --wordlist=/user/share/dict/words /etc/shadow (using wordlist)

6) Where are the passwords stored?

/.john/john.pot





Part 2)

Cracked Passwords:

leiah:$6$YBpYViFc$rfxV4nNJPOSBRROBziOZQDsa392w9uovyHuYVGtcf7VwY8zMhj54eWQFrqYwPPgCBdP5uo/DGmFQVEXJMcFTd.:3arth

yoda:$6$XjyNY9NT$gyBbFoLwVxmJDxYYDstklFPArvw6qgIsWSjw5ykLHT6OirweY5fpRHC6Cco8VWJL1CYYLrCCi4/aXdgSx6FFr.:m3rcury

chewbacca:$6$EAcKJ0CM$VxbXXxKEKQUV00RzFGLBmgJ9dI9npFiTrpsv.3Yj.XCU7aHfDyf3jpMgy0y/JKSEwWv47q6oLLi/REulMusoG0:5un

skywalker:$6$iJQrBFC8$MEmk9HXCMg9B/Vz.wdqYb7Q997c4ojbFX2bfU.ujjeBMu3Mh.mkKcRGq.9iGjpx47IG9nOFauBxNHiXXnIBxL/:uranu5

Cracked using substitution rules then I checked using a more comprehensive known good ruleset for john/hashcat published by: Unix-Ninja