OLD DOMINION UNIVERSITY

CYSE 270 LINUX SYSTEM FOR CYBERSECURITY

Assignment #5 Password Cracking

John Wilson

01179411

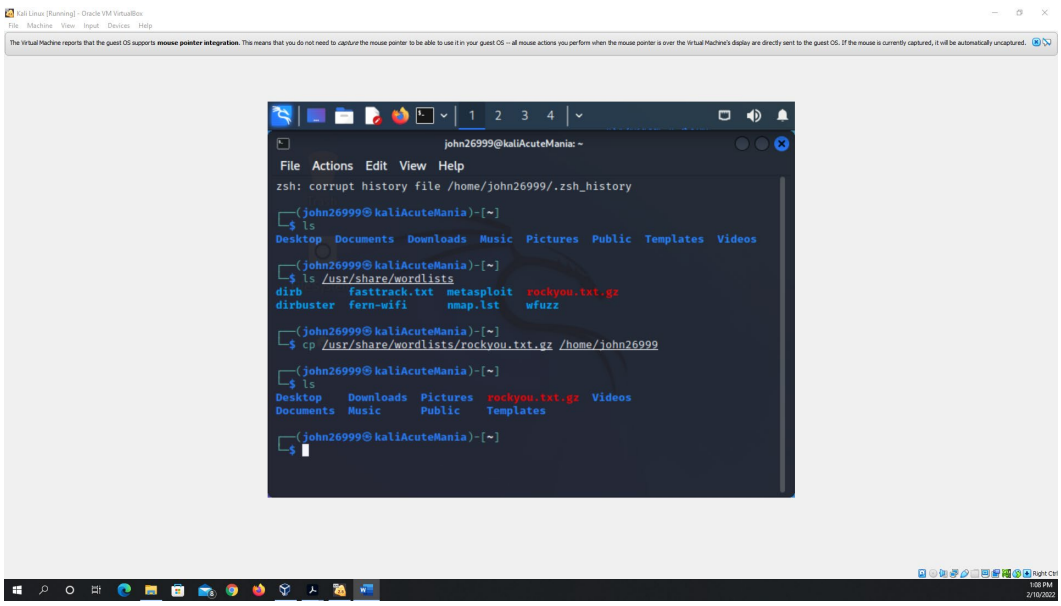
Below is the snippet of a sample lab report.

TASK A

PASSWORD CRACKING

JOHN THE RIPPER PREPERATION PRIOR TO EXECUTING ASSIGNMENT

1) Have to locate the rockyou.txt.gz file, copy the file into the users home directory, and then unzip the file. This is so you can use the file to crack passwords and below are the steps.



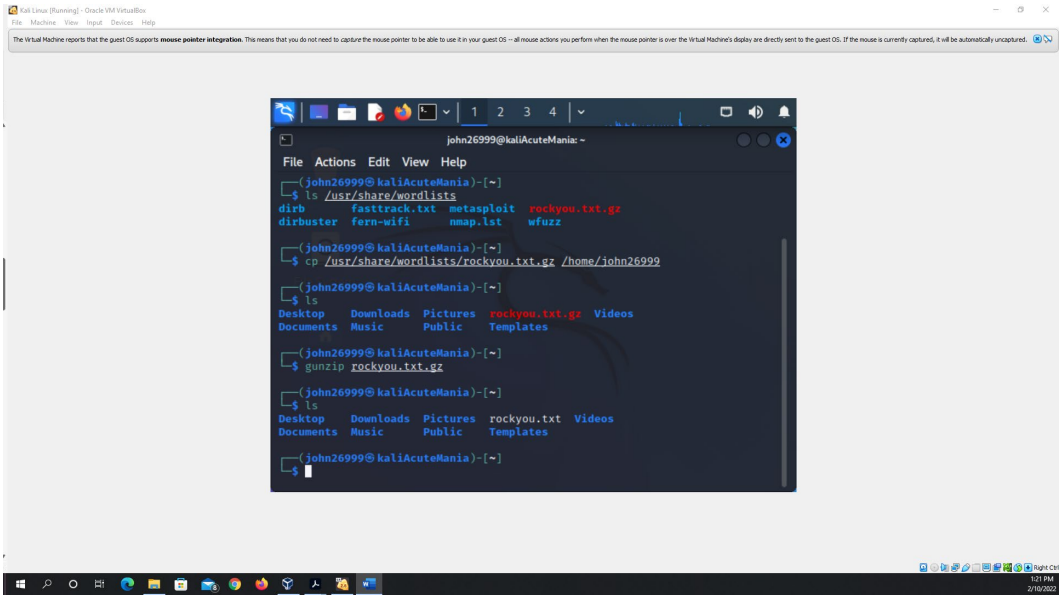


Figure 1 Screenshots of JWILS082 Computer screen for John the Ripper preperation

Above is the screen shot using the commands “ls” to show that nothing called rickyou.txt.gz or rockyou.txt is in the home directory.

I used the command “ls /usr/share/wordlists” to show where the file rockyou.txt.gz is located.

I used the command “cp /usr/share/wordlists/rockyou.txt.gz /home/john26999” to copy the file rockyoou.txt.gz and move it to the users home directory.

I then used the command “ls” to show that the file rockyou.txt.gz was successfully copied and placed in th users home directory.

I then used the command “gunzip rockyou.txt.gz” to uncompress the file in the users home directory.

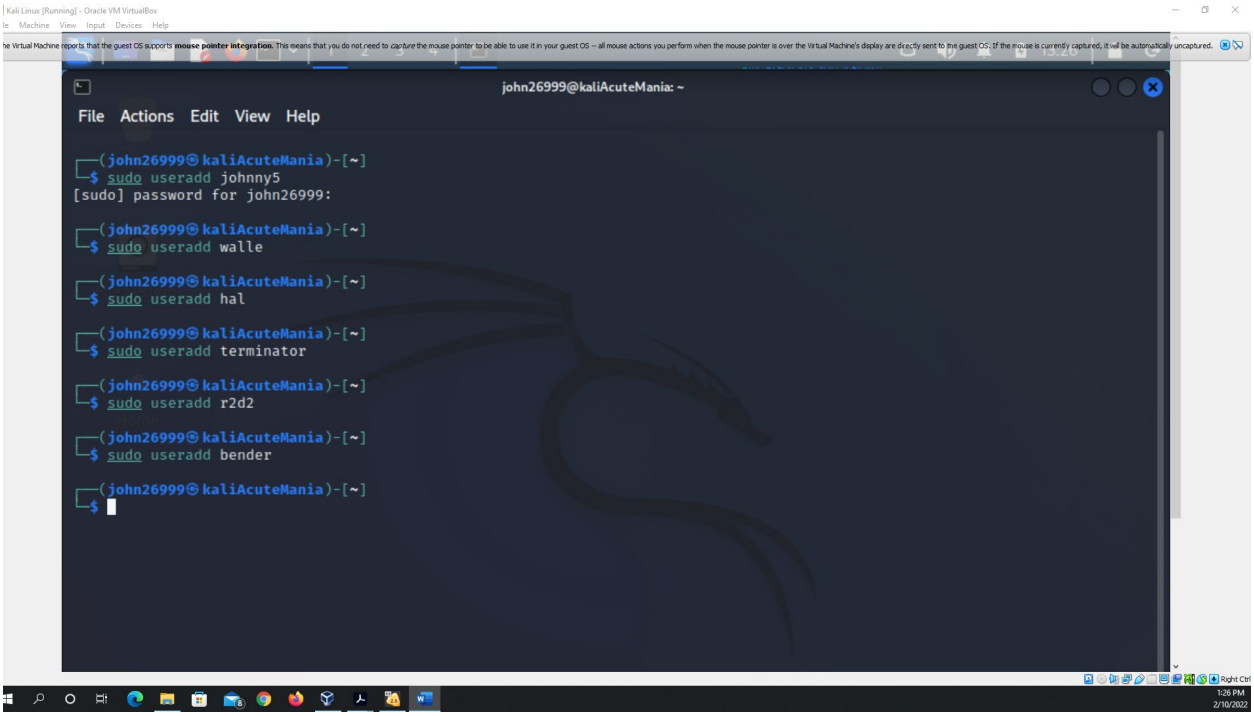
Then I used the command “ls” to show the file rockyou.txt.gz was successfully uncompressed to rockyou.txt in the users home directory.

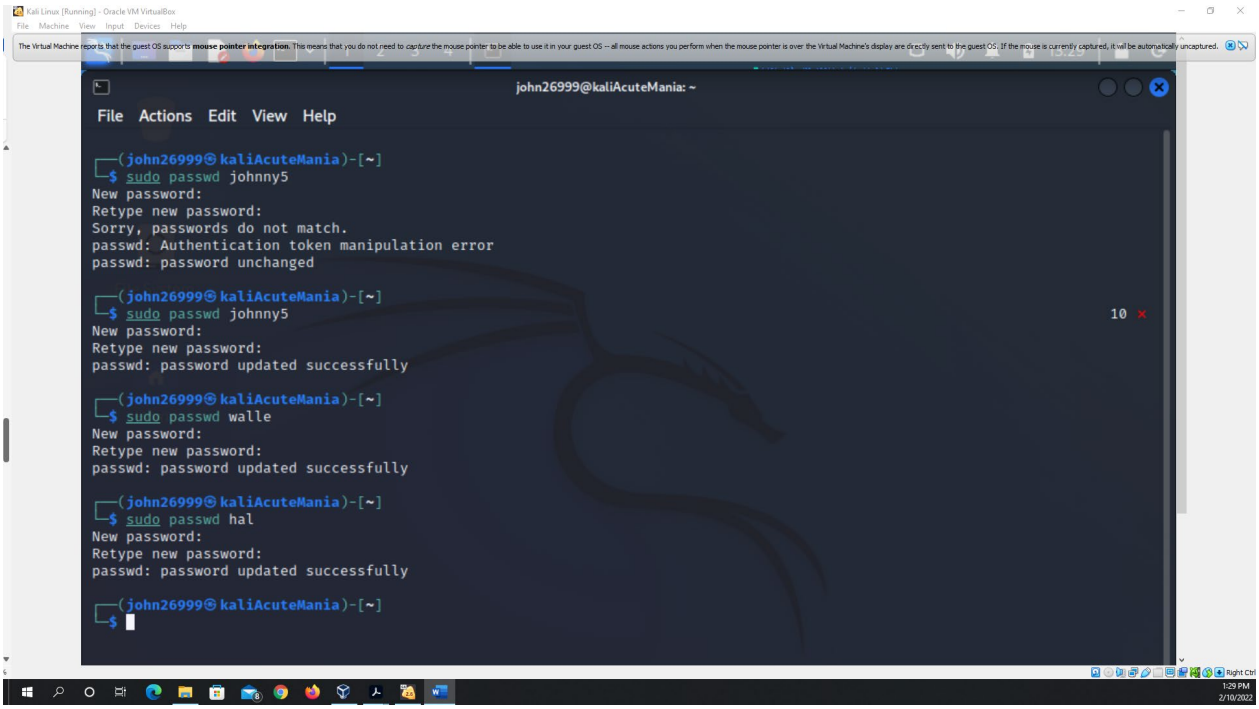
Now we being the assignment.

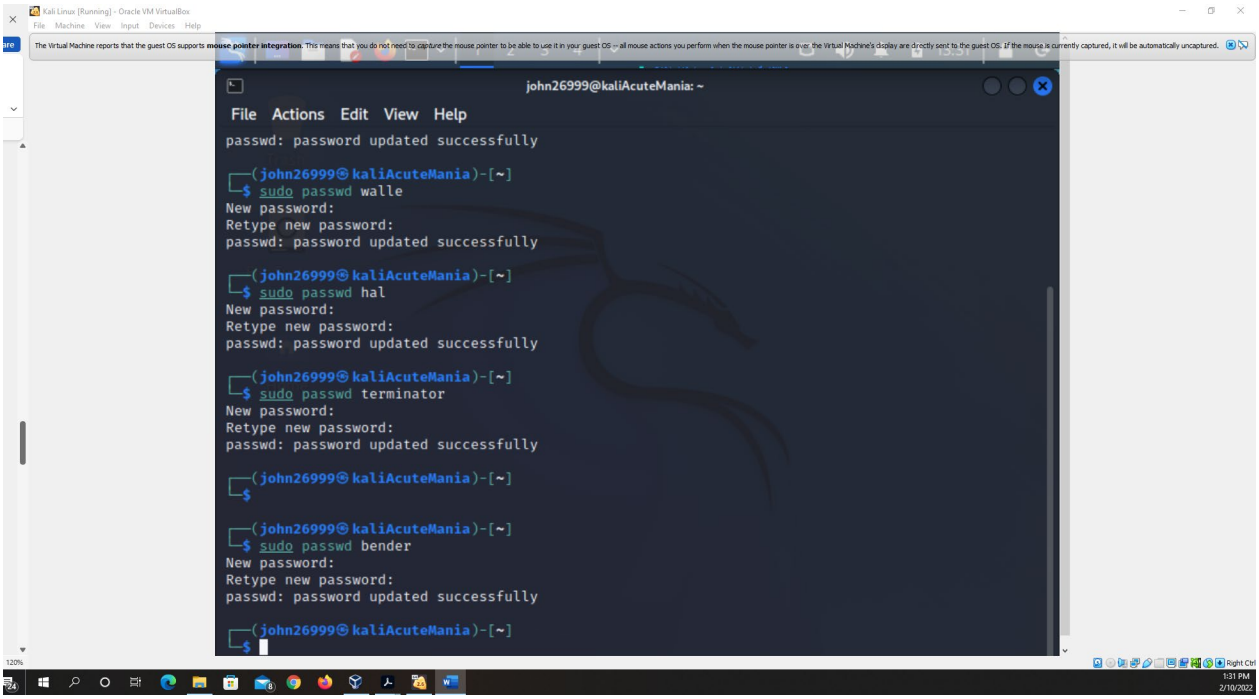
1) Create 6 users in your Linux system, then assign each user a password that meets the following complexity requirement respectively. You should list the passwords created for each user. [6 * 5 = 30 points]

    1. A simple dictionary word (all lowercase)
    2. 4-character digits
    3. A simple dictionary word (all lowercase) + digits
    4. A simple dictionary word (all lowercase) + digits +symbols
    5. A simple dictionary word (all lowercase) + digits
    6. A simple dictionary word (w. a mix of lower and upper case) + digits +symbols

Remember, do not use the passwords for your real-world accounts.




Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine's display are directly sent to the guest OS. If the mouse is currently captured, it will be automatically uncaptured.
john26999@kaliAcuteMania: ~
File Actions Edit View Help
(john26999㉿kaliAcuteMania)-[~]
$ sudo passwd johnny5
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
(john26999㉿kaliAcuteMania)-[~]
$ sudo passwd johnny5
New password:
Retype new password:
passwd: password updated successfully
(john26999㉿kaliAcuteMania)-[~]
$ sudo passwd walle
New password:
Retype new password:
passwd: password updated successfully
(john26999㉿kaliAcuteMania)-[~]
$ sudo passwd hal
New password:
Retype new password:
passwd: password updated successfully
(john26999㉿kaliAcuteMania)-[~]
$
10
Right Ctrl
1:29 PM
2/10/2022


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine's display are directly sent to the guest OS. If the mouse is currently captured, it will be automatically uncaptured.
john26999@kaliAcuteMania: ~
File Actions Edit View Help
passwd: password updated successfully
(john26999㉿kaliAcuteMania)-[~]
$ sudo passwd walle
New password:
Retype new password:
passwd: password updated successfully
(john26999㉿kaliAcuteMania)-[~]
$ sudo passwd hal
New password:
Retype new password:
passwd: password updated successfully
(john26999㉿kaliAcuteMania)-[~]
$ sudo passwd terminator
New password:
Retype new password:
passwd: password updated successfully
(john26999㉿kaliAcuteMania)-[~]
$
(john26999㉿kaliAcuteMania)-[~]
$ sudo passwd bender
New password:
Retype new password:
passwd: password updated successfully
(john26999㉿kaliAcuteMania)-[~]
$
120%
Right Ctrl
1:31 PM
2/10/2022

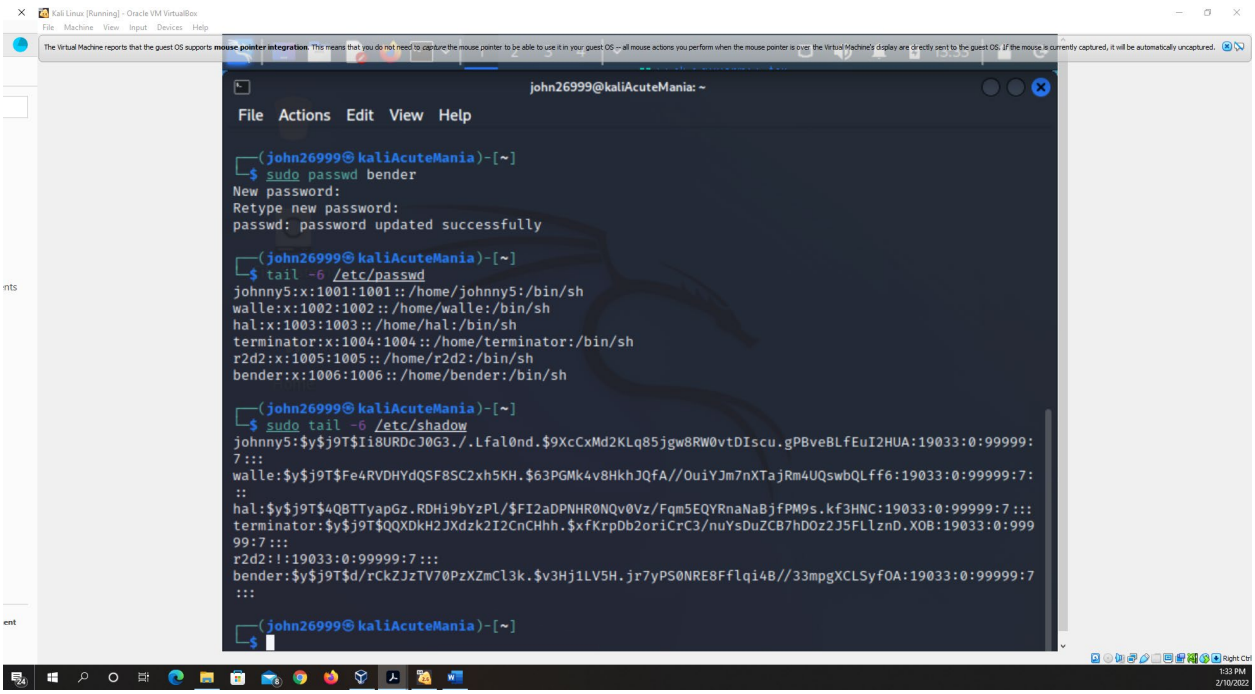


Figure 2 Screenshots of JWILS082 Computer screen for step 1

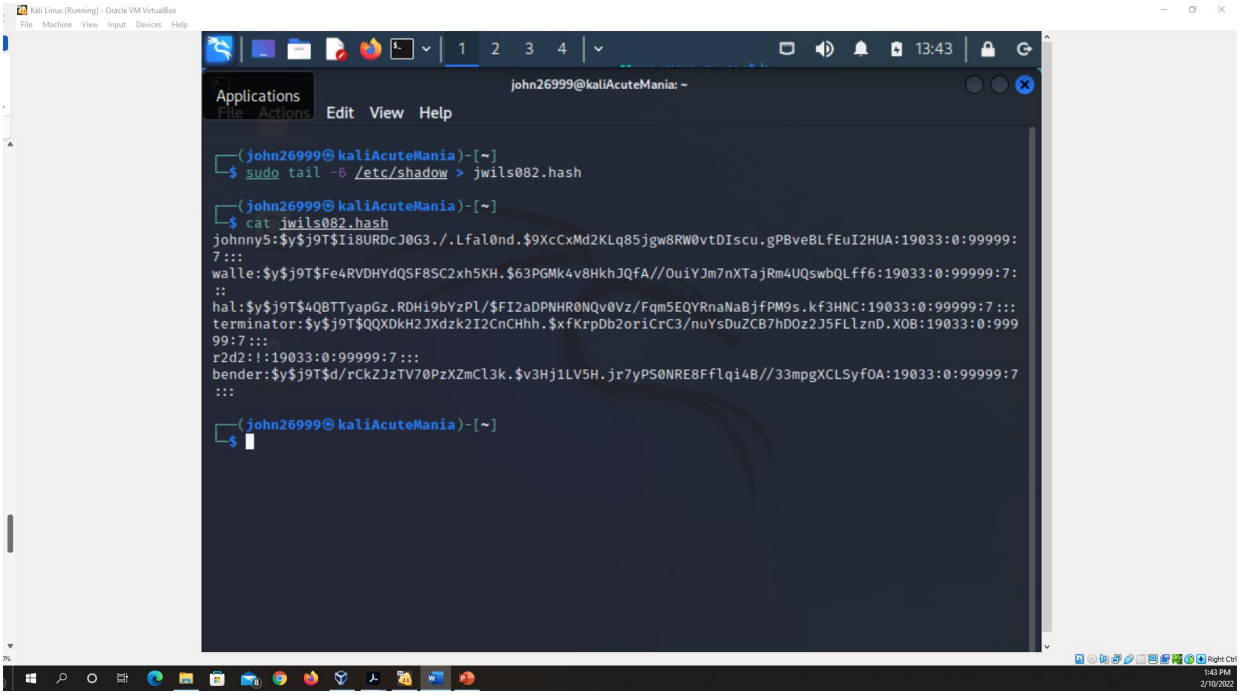
Above are the screen shots using the command “sudo useradd xxxxx (sidenote – xxxxx is replaced as a username)” six times to create six different user so that I can crack the passwords. “sudo” is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “useradd” is the command that adds a new user to the system. “xxxxx” is th useradded. For this step I added the users johnny5, walle, hal, terminator, r2d2, bender (robot names in pop culture).

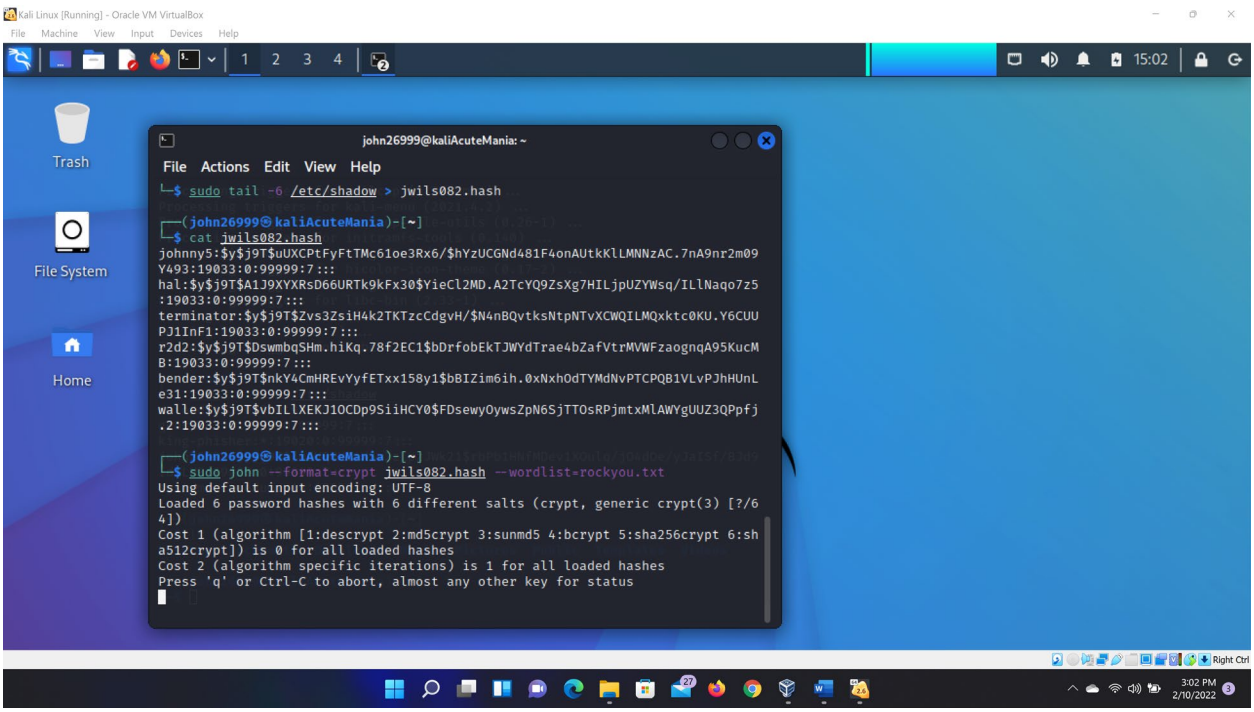
The second are screenshots placing passwords as instructed in step 1 by using the command “sudo passwd xxxxx (sidenote – xxxxx is replaced as a username)” six times to assign a password for each user. The list of usernames and passwords used are listed below.

a. johnny5: media
b. walle: 1234
c. hal: f1our07
d. terminator: sky34%
e. r2d2: starwars57
f. bender: FuTuRe234*&

The other screenshot I used the command “sudo tail -6 /etc/passwd” to show that the users were created. “sudo” is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “tail” is the command that displays the bottom part of the file data. “-6” is the command that shows exactly the last 6 lines. “/etc/passwd” to show the primary group membership.

2) Export above users' hash into a file named xxx.hash (replace xxx with your MIDAS ID) and use John the Ripper to crack their passwords in wordlist mode (use rockyou.txt). [40 points]





Had to change computers as the other one kept freezing on me so this is on my other laptop. Computers can be challenging.

Figure 3 Screenshot of JWILS082 Computer screen for step 2

Above is the screen shot using the command “sudo tail -6 /etc/shadow > jwils082.hash” that export six users (johnny5, walle, hal, terminator, r2d2, and bender) in to the file jwils082.hash that is located in my home directory. “sudo” is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “tail” is the command that displays the bottom part of the file data. “-6” is the command that shows exactly the last 6 lines. “/etc/shadow” is the absolute path to where the file group is located in the etc directory. “>” is the command to copy and redirect the information towards another file. “jwils082.hash” is the file where the hash information went.

I used the command “cat jwils082.hash” to prove the information was successfully copied to the file. “cat” is the command that reads data from a file and gives the output on the screen. “jwils082.hash” is the file the information is located.

On the third screenshot, I opened the john the ripper terminal in Kali Linux and issued the command “sudo john --format=crypt jwils082.hash --wordlist=rockyou.txt”. “sudo” is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “john” is the command to use the john the ripper software. “--format” picks a benchmade format for “--format=crypt”. “jwils082.hash” is the file the hash information is located. “--wordlist=rockyou.txt” is the command that says to read words from the file rockyou.txt.”

And then we wait for the program to run for at least ten minutes. But because I have multiple classes I will do homework from another class while I wait in hopes that it works.

3) Keep your john the ripper cracking for at least 10 minutes. How many passwords have been successfully cracked? [30 points]

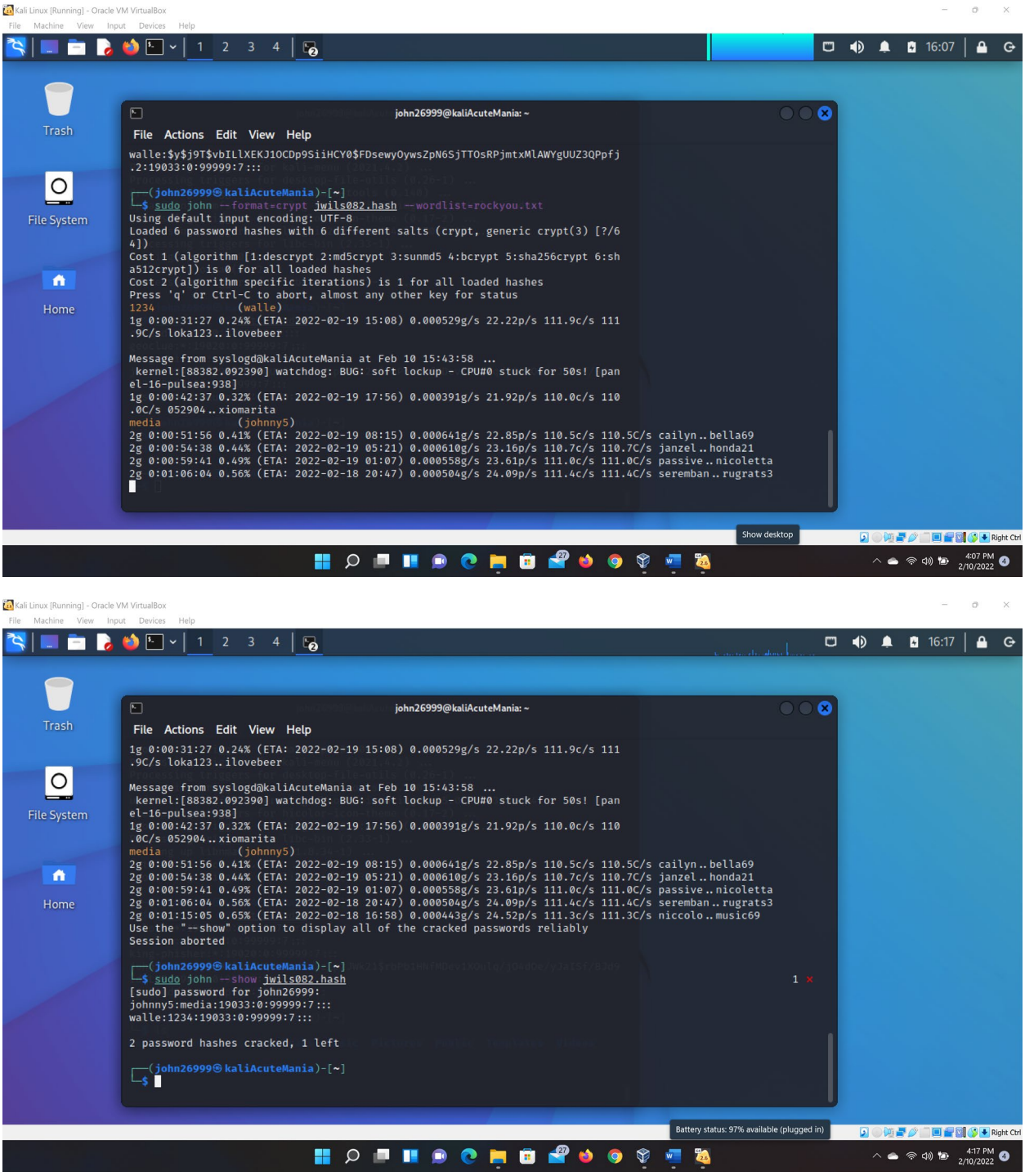


Figure 4 Screenshot of JWILS082 Computer screen for step 3

Above is the screen shot that illustrates the passwords successfully cracked. As you can see the program has only been able to crack two of the passwords in over 60 minutes time. So either my computer is slow or I set the passwords to be more challenging than the exercise is supposed to be. Either way, what I

noticed from this exercise is that it can take a long time to run the program and the more complicated you make the passwords (by combining numbers and letters; or numbers, letters, and symbols; or uppercase and lowercase letters, numers and symbols) makes it more difficult to crack. So complicated passwords do help in keeping bad actors from using bruteforce attacks.

I also ran the command “sudo john –show jwils082.hash” to show the passwords that were cracked. “sudo” is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “john” is the command to use the john the ripper software. “--show” is the command that displays the passwords cracked. “jwils082.hash” is the file where the hash information is located.

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

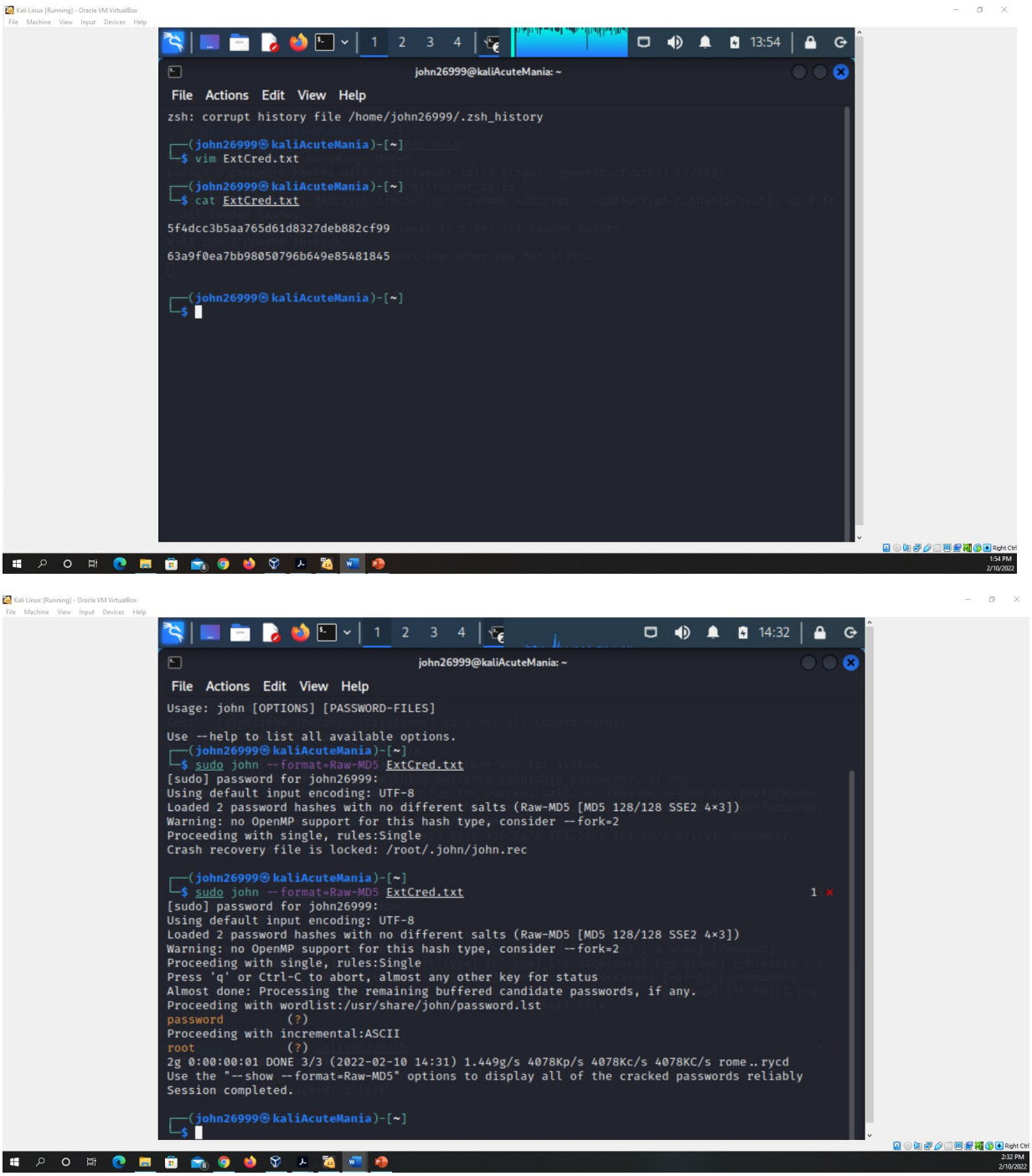


Figure 4 (Extra credit) Screenshot of JWILS082 Computer screen for step 4 (Extra credit)

Frrst had to open VIM to rewrite the numbers and then save them to the file “ExtCred.txt.”

Used the command “cat /home/ExtCred.txt” to prove the information is in the file I placed it.

Above is the screen shot of the commands “sudo john --format-Raw=Md5 ExtCred.txt” that begins the cracking of the hashed passwords. “sudo” is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “--format-Raw=Md5” is the command that tells john the ripper program to crack the hash lines in a file. “ExtCredit.txt” is the file with the two hashes copied

“sudo john --show --format-Raw=Md5 ExtCred.txt” is the command to show the cracked passwords in the screen. “sudo” is the command that allows you to run programs with the security privileges of another user (otherwise known as a super user). “--show–format-Raw=Md5” is the command that tells john the ripper program to crack the hash in a file. “ExtCredit.txt” is the file with the two hashes copied.

You can now see the hashes were hacked successfully. And below are the results:

- 5f4dcc3b5aa765d61d8327deb882cf99 = password
- 63a9f0ea7bb98050796b649e85481845 = root

Sources

Cracking Passwords Using John the Ripper. (n.d.). WonderHowTo. Retrieved February 9, 2022, from https://null-byte.wonderhowto.com/forum/cracking-passwords-using-john-ripper-0181420/

Robertz25. (2021, January 20). *TryHackMe | John The Ripper Writeup*. Medium. https://halloper123.medium.com/tryhackme-john-the-ripper-writeup-edbef564bf38\