**CSC 312 Cybersecurity LAB 02 Points: 20**

For this assignment, you need to use a computer. I assume you have access to a Microsoft Windows based personal computer. Some parts of the assignment require downloading and installing new software but does not necessarily need administrative privileges. However, some software will require installation on C: drive under Program Files and hence you need access to a computer with **administrative privileges**.

1. **John the Ripper and Password Cracking**

We will use a popular password cracking software and identify passwords in a UNIX style password file provided by me.

***Important note:*** **Do not attempt to crack passwords from any other file, other than the ones on your own computer, if you do not have permission to do so. Do not attempt to crack passwords on systems that do not belong to you.**

1. If password cracking and unauthorized access to computer systems can lead to criminal charges, why are tools like these made available? Give one ethical use of a password cracking software.

Using password cracking software to regain access to one’s own passwords if lost. (Or acting as a trusted party for someone else

1. Use any browser to access **http://www.openwall.com/john/** and select **1.9.0-jumbo-1 64-bit (Windows binaries,** [7z, 22 MB](https://www.openwall.com/john/k/john-1.9.0-jumbo-1-win64.7z)**)**. Copy the downloaded **john-1.9.0-jumbo-1-win64.7z** file to the folder **C:\Software**.
2. Now that we have downloaded a Zip file that includes an executable file, we want to be sure that it does not have any virus content and has not been tampered with. Scan the file with any virus scanning software you have access to. If there is any virus content, immediately delete the file.

To verify that the file has not been tampered with check its SHA1 hash. Open a command window and type the following command:

Command used to check for the hash:

certutil -hashfile "C:\Software\"john-1.9.0-jumbo-1-win64.7z"" SHA1

Ensure that it reads as below (where 8 hex digits have been deleted). If not, discard the file and start all over.

**af a9 -- -- 70 ab cd 9e 74 21 3d d4 0b 1c e5 92 99 db -- --**

Provide the missing digits: 93c8

1. Right-click the **john-1.9.0-jumbo-1-win64.7z** file and choose Extract All. It will create a folder named **john-1.9.0-jumbo-1-win64**. For convenience, rename the folder to ***Ripper***.
2. Download the **passwd1.txt** file I have posted on Blackboard and copy it into the **P:\Software\Ripper** folder.
3. Now you are ready to crack the password file. If you wish to understand all the options, read the files **C:\Software\Ripper\README.txt, EXAMPLES.txt, and FAQ.txt** under the folder **C:\Software\Ripper\doc**.
4. Open a command window and type the command: **cd C:\Software\Ripper**
5. If valid password files are specified but no options are given, John will go through the default selection of cracking modes with their default settings. Launch the Ripper program on **passwd1.txt** file by typing the command: **run\john passwd1.txt**
6. While some of the easy passwords will be cracked within seconds, others may take several hours or may be even days. Run the program sufficiently long, until you crack at least 8-9 passwords, if not all.
7. To stop execution, type **Control-C** in the command prompt window. Finally, you may type **run\john –-show passwd1.txt** to display all the cracked passwords.

**List of cracked passwords**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Username** | **Plaintext password** | **Order in which cracked** |
| 1. | **root** | w1zard | 8 |
| 2. | **john** | wizard | 3 |
| 3. | **tom** | tomkatz | 1 |
| 4. | **helena** | helena | 2 |
| 5. | **kristi** | letmein | 4 |
| 6. | **lisa** | 12345678 | 7 |
| 7. | **steve** | abc123 | 6 |
| 8. | **arlette** | phoenix9 | 5 |
| 9. | **kathy** | sk8board | 9 |
| 10. | **doug** | crabcola | 10 |

1. **Cracking Linux Passwords with John and Johnny on Kali**
2. Open a terminal window On Kali. Kali uses **/etc/passwd** and **/etc/shadow** files to keep track of user credentials. An inspection of **/etc/shadow** shows that for all but one account login is prevented with an **\*** or **!** placed in the second field.

The only account that permits login is: kali

1. Add an account for yourself, so you do not have to login as **kali** all the time.

Create a sudo user account and home directory with bash as a default login shell using your Brockport login. Then set the account password as pa$$w0rd.

Command used to create the account: sudo adduser etay1

Command used to set the account password: I actually didn’t have to use this command it automatically prompted me to set a password but sudo passwd username

1. Add an account for yourself with your first name as the username and with bash as a default login shell. This account is not included in the **sudo** group.

Command used: sudo useradd elijah -m -s /bin/bash elijah

Add a password and set your password as **qwertyui**

Command used: sudo passwd elijah

1. Type the following two commands to check the **/etc/passwd** and **/etc/shadow** files.

**tail –n 2 /etc/passwd /etc/shadow**

1. In order to crack the password information, we need to add the hashed password information **/etc/shadow** to the **/etc/passwd** file. Use ***unshadow*** command to unshadow and combine both files, and pipe the result to a new file named passwd.txt (save passwd.txt under Documents folder).

Note: if you don’t know how to use the unshadow command to combine shadow and passwd files, search the internet.

Command used for unshadowing:

sudo unshadow /etc/passwd /etc/shadow > ~/Documents/passwd.txt

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Move to the **Documents** directory. Display **passwd.txt** and see what it contains. Since we are only interested in kali account and the last two lines that were added by us, you may edit the **passwd.txt** file, remove all other lines and keep only the tree accounts (kali, Your Brockport id and your first name accounts), and save the edited file as **crack.hash**.

You will be left with exactly three lines in **crack.hash**.

You may check this by typing the command: **wc –l crack.hash**

1. We are ready to crack the passwords in **crack.hash**.

Type the command: **john --format=crypt crack.hash**

1. Abort execution after five minutes. At this stage only one hash remains to be cracked.

Remaining hash to be cracked corresponds to the account: etay1

1. Johnny provides a GUI for the John the Ripper password cracking tool. Download Johnny by typing the following command:

sudo apt install johnny

***Notes:***

* Before installing johnny double check that Khali is connected to the internet.
* If you face a problem, states the following

*“Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease Temporary failure resolving 'http.kali.org'”*

In */etc/apt/sources.list*, for the following line

deb http://http.kali.org/kali kali-rolling main non-free contrib

add ***s*** for http

deb https://http.kali.org/kali kali-rolling main non-free contrib

1. After successfully installing Johnny, open the application. Open the password file **crack.hash**. You should see the three lines of the password file. Uncheck the lines corresponding to the accounts for which the passwords have already been determined and displayed, leaving only one line checked.
2. At this stage, pretend as a hacker who is trying to guess the password, perhaps knowing some personal information about the account holder ­– car driven, spouse or children’s names, favorite sports team, etc. Press **Guess password** and enter the guess. The application would check that and would respond if that is indeed correct. Keep trying various possibilities and eventually enter **pa$$w0rd** as a guess, at which stage Johnny will accept it. (There is no requirement to answer this question; simply explore the graphical user interface to discover its functionality.)
3. Return to the command window and type the command: **john –-show crack.hash**

Show the output below:

kali:kali:1000:1000:,,,:/home/kali:/usr/bin/zsh

2 password hash cracked, 0 left