**Practical 6: Password Cracking and Attacks**

**Objectives**: By the end of this practical exercise, students should be able to:

* ~~Setup and use virtual machines.~~
* ~~Know the usage of integrity check program such as FCIV.~~
* Store passwords in Safe Document.
* Install password cracking program.
* Use rainbow tables to crack hashed passwords.
* Understand the importance of strong passwords.

**Instructions:** Write your answers in the spaces provided.

Please also down the Practical 6 from BrightSpace.

Practical 6 is using Windows XP, and you may want to explore it.

Important : Disable Windows defender

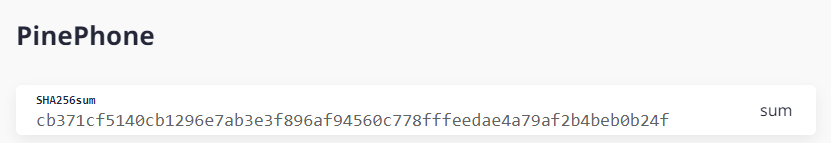
## Windows Certutil

## Using certutil to hash files.

## <https://www.mcbsys.com/blog/2017/03/use-certutil-to-get-file-hash/>

* + 1. Download PinePhone; <https://www.kali.org/get-kali/#kali-mobile>

You may download any files you like provided there is CRC checksum for the file; Hashing.

* + 1. **Take Noted of the file checksum; SHA256sum --cb371cf5140cb1296e7ab3e3f896af94560c778fffeedae4a79af2b4beb0b24f**
    2. ****
    3. Go to your folder where PinePhone is downloaded.
    4. C:\Users\admin\Downloads>certutil -hashfile nethunterpro-2023.2-pinephone-phosh.img.tar.xz sha256
    5. Note down the hash value produced by the “certutil” command line tool.

C:\Users\admin\Downloads>certutil -hashfile nethunterpro-2023.4-pinephone-phosh.img.tar.xz sha256

SHA256 hash of nethunterpro-2023.4-pinephone-phosh.img.tar.xz:

8004ce925753d8e502af631dcd8d93d16dbedc60e87eb910b3a4d1e8c520840c

CertUtil: -hashfile command completed successfully.

* + 1. Now, compare it with the integrity check value on Question A2
    2. What is your observation?

The file has been tampered with and it’s a different hash

* + 1. What is your conclusion?

I learned how to check if the file has been tampered with, and how it works

<https://www.okta.com/identity-101/hashing-algorithms/>

MD5: 72b003ba1a806c3f94026568ad5c5933

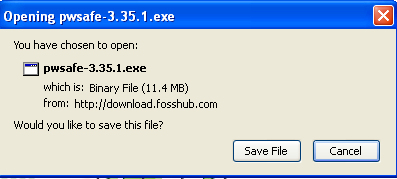
SHA-256: f6bf870a2a5bb6d26ddbeda8e903f3867f729785a36f89bfae896776777d50af

## Store Passwords in Safe Document

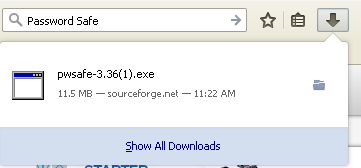
Note: Because of the difficulty in remembering strong passwords, you can store all password list in a single “strong” encrypted document.

* + 1. Google **pwsafe,** download and install.

The version you see below may be different from yours.



When the file is downloaded, click on the downloaded file to install it.





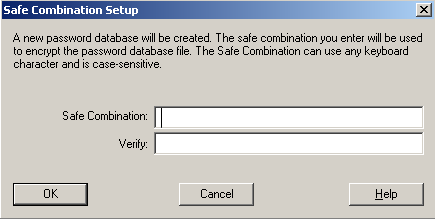
Click on “Run” button and follow the instructions to install this program on your computer with default settings.

Double-click the Password Safe desktop icon to start Password Safe.

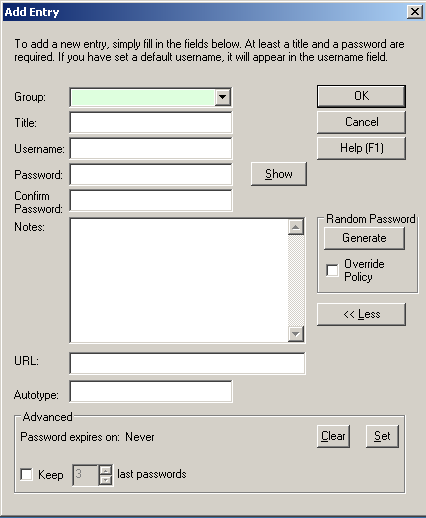


Click **Create new database**. Save it using a filename of your choice.

Enter a strong password for **Safe Combination**. The password must have upper and lowercase letters and at least one digit or character of punctuation. Re-entering of password is under **Verify**. Click **OK**.



Now you can add your passwords to the database. Click **Edit** and **Add Entry**. Fill in the blanks for title, username and password for accounts that you use regularly. **Group** and **Notes** are optional entries. Note that the password may appear in clear text when you enter it. Click **OK.**

Try to create an entry for your personal email, bank accounts, etc.

Note: As you may have downloaded a later version of Password Safe, the user interface may not look exactly like the one shown here.

Click **File** and then click **Exit**.

Start **Password Safe** again. Enter your safe combination.

Double-click the entry you have created. Your password is now added to the Windows Clipboard. You can paste the password into the **Password** line whenever you access the account to which it corresponds. The password will be cleared from the Clipboard when Password Safe is closed.

You may try to paste the password into the password field of your account (for e.g. your personal email account, bank account etc.).

Close the Password Safe.

# Part III

## A. Use Rainbow Tables for Cracking Hashed Password

Although brute force and dictionary attacks were once the primary tools to crack an encrypted password, today rainbow tables are more frequently used. In this exercise, you will download and install Ophcrack, an open-source password cracker program that uses rainbow tables.

<https://en.wikipedia.org/wiki/Rainbow_table>

A rainbow table is a precomputed table for caching the outputs of a cryptographic hash function, usually for cracking password hashes. Passwords are typically stored not in plain text form, but as hash values. If such a database of hashed passwords falls into the hands of an attacker, they can use a precomputed rainbow table to recover the plaintext passwords.

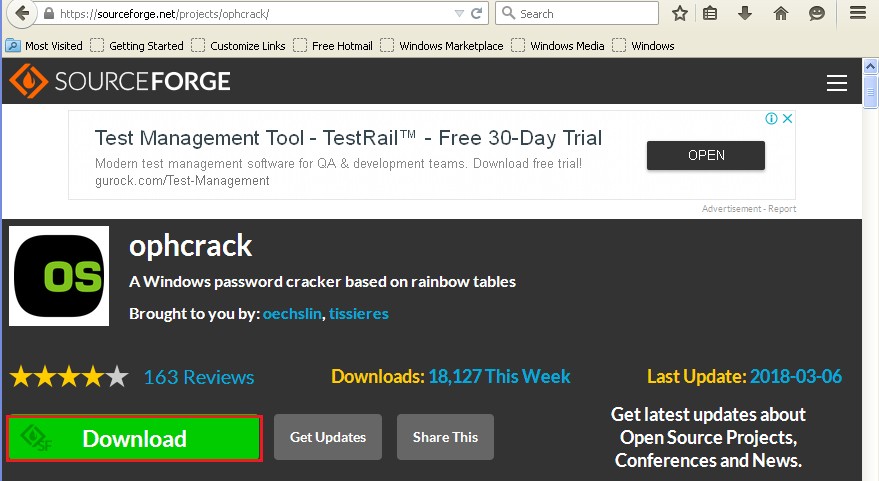
Note: **This program should never be used to attempt to crack the password of a valid account.**

1. Open your FireFox web browser and enter the URL

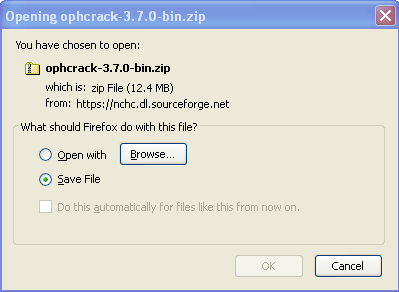
[**http://sourceforge.net/projects/ophcrack/**](http://sourceforge.net/projects/ophcrack/)

Note: The location of content on the Internet such as this program may change without warning. If you are no longer able to access the program through the above URL, then use a search engine like Google ([www.google.com](http://www.google.com/)) and search for “Ophcrack”.

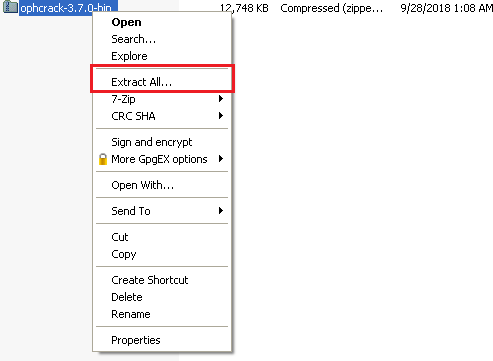
## \*\*\* You may need to turn off your anti-virus software running this on your host machine. You should not face any problems downloading/executing Ophcrack, perform the steps in virtualised environment \*\*\*



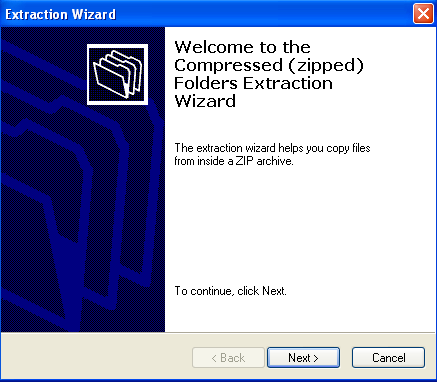
1. Click to download the Ophcrack password crack program and save the compressed file ophcrack-3.7.0-bin.zip in the Documents download area.



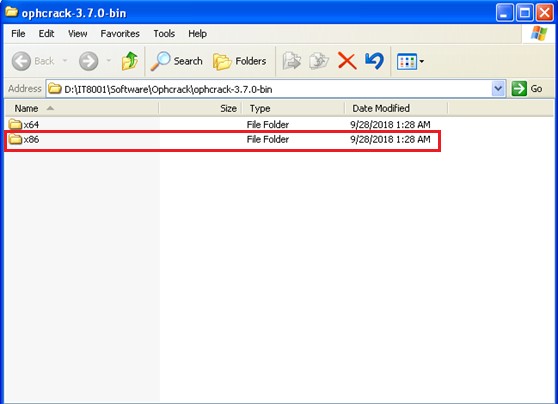
1. When the file is downloaded, unzip the file by right clicking and select extract all to extract all the files.



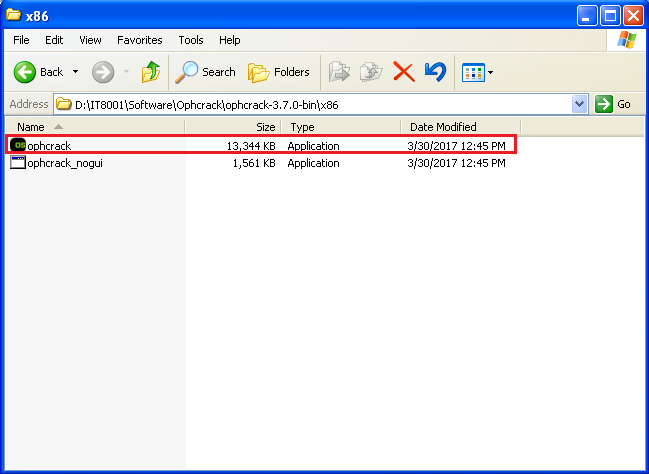
1. Click next to extract the files.



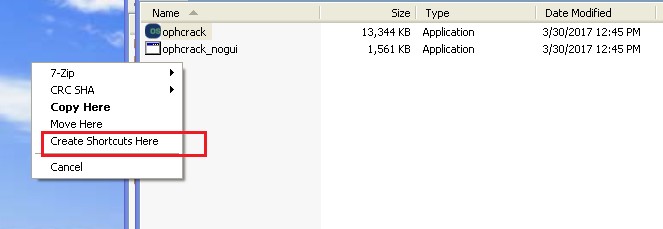
1. Two binaries would be extracted in two folders – x64 and x86. Click on the x86 folder to open it. (The x64 folder is for Ophcrack in a 64-bit environment)



1. Right click on the ophcrack application and drag it to the desktop.



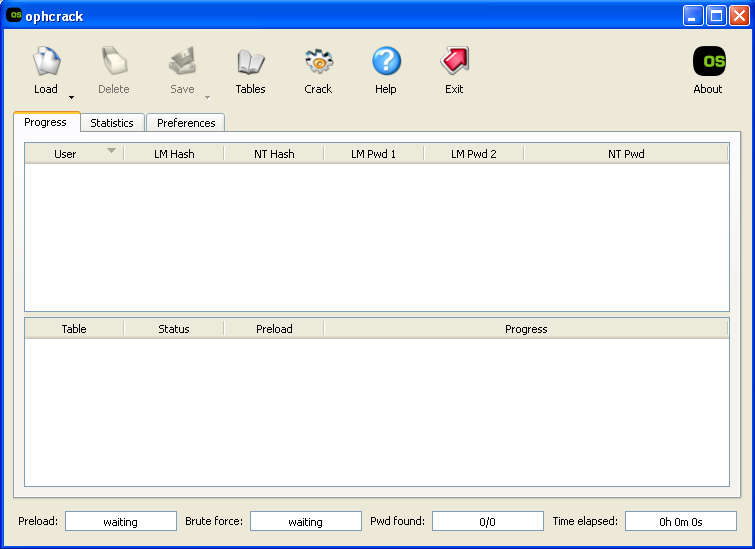
1. Select Create Shortcuts here to create a link. This will facilitate opening the program.



1. You should have an icon shutcut to Ophcrack on the desktop.



1. Click on the ophcrack icon to start the program.



You will be able to select different rainbow tables that you want to use. Please note that the rainbow tables are very big and may take you more than one hour to download, depending on your connection speed. We will select two rainbow tables which would be used later.

1. Go to <https://sourceforge.net/projects/ophcrack/files/tables/>  Rainbow Tables to download two zipped files for the following rainbow tables:
   * tables\_xp\_free\_small
   * tables\_vista\_free

Copy the two zipped files containing the above tables to your Windows XP VM, and unzipped them to two respective folders.

1. Try to crack these eight passwords listed below. Copy one entire line at a time to the clipboard and submit it to **Ophcrack**.

1:1009:1aa818381e4e281baad3b435b51404ee:5f18a8499cdd4f43d89424ad39ce9af7::: 2:1010:52af70e5a826c9c1aad3b435b51404ee:1399c76929f41a9e7557e02c3993748c:::

3:1011:2cd59457353d8649aad3b435b51404ee:cbb19245d2baa671749236af72493285:::

4:1012:1feb990b23c293a2aad3b435b51404ee:4f351f502f1aee79a331bbcb40c9500f::: 5:1013:22858418fe80dbecaad3b435b51404ee:577030bb1a8b6c42c8eaa1eac5137447::: 6:1014:0b9c5cab5e9c5de1aad3b435b51404ee:a00aa4b31f99caa9260484fefbaceadb::: 7:1015:0182bd0bd4444bf8aad3b435b51404ee:328727b81ca05805a68ef26acb252039:::

8:1016:0182bd0bd4444bf8a0859a0c248642f8:dd046a504430737c964078609b30f301:::

Write down each answer in the spaces provided.

A screenshot of a computer

Description automatically generated

LM - The LM hash is used for storing passwords. It is disabled in W7 and above. However, LM is enabled in memory if the password is less than 15 characters. That's why all recommendations for admin accounts are 15+ chars. LM is old, based on MD4 and easy to crack. The reason is that Windows domains require speed, but that also makes for shit security.

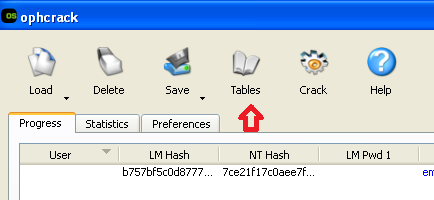
NT - The NT hash calculates the hash based on the entire password the user entered. The LM hash splits the password into two 7-character chunks, padding as necessary.

NTLM - The NTLM hash is used for local authentication on hosts in the domain. It is a combination of the LM and NT hash as seen above.

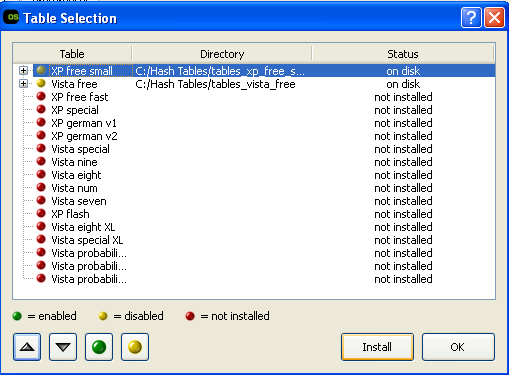
NetNTLMv1/2 - Hash for authentication on the network (SMB). Sometimes called NTLMv2, but don't get confused; it is not the same as an NTLM hash.

1. So far you are just using the **brute force** method to crack the passwords. You will not be able to crack all the eight listed passwords with the brute force method. You need to make use of rainbow tables to crack strong passwords.

Select **Tables**.



Select the table to load and install (e.g. XP Free Small table), and click on “Install” button.



Then browse to the folder where the table is located. Click on to enable the table, or  to disable the table. When you are done with loading an installing the tables click **OK**.

1. Crack the eight passwords again, this time using the rainbow tables.
2. Based on what you have seen, is there a pattern to what type of passwords are more secure?

Some passwords wont be cracked as the password is not inside the password list

1. Close all windows when finished.

# Part IV

## A. Windows Password Cracking

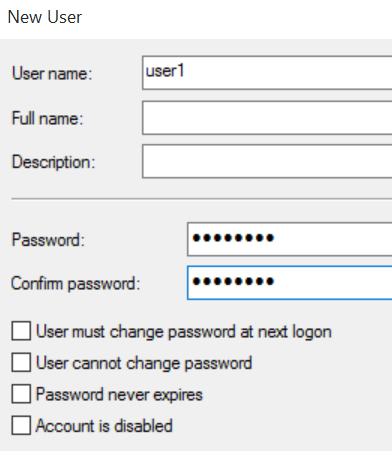
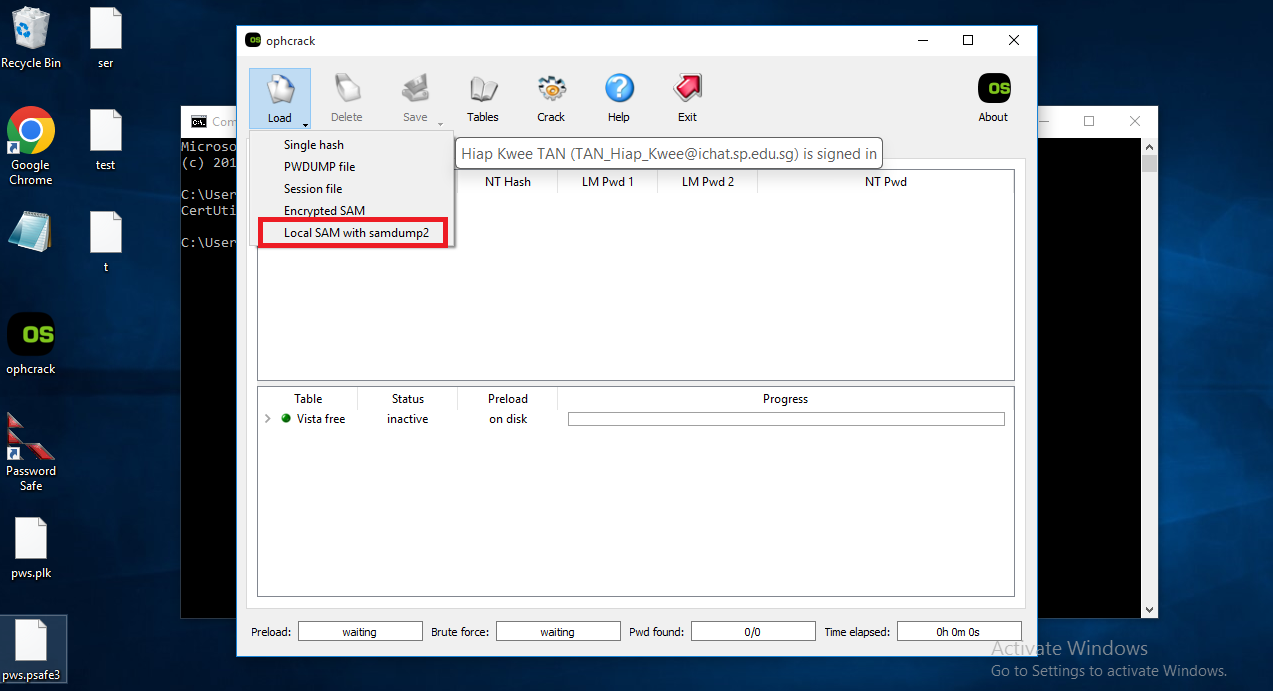
Ophcrack is an open source Windows password cracker that uses rainbow tables. It may not work with anti-virus software which flag it as a Trojan.

Password cracking can be resource-intensive. If you are able to, you may want to increase the virtual memory of your Win10 VM to 4GB.

Note: **This program should never be used to attempt to crack the password of a valid account.**

In Win10 VM:

First create a few users with passwords to crack.

1. In the bottom left corner, right-click on the Windows icon, and choose “Computer Management”.
2. In the left pane, expand “Local Users and Groups”.
3. Right-click on Users and choose New User.
4. Create a new user with Username “user1” and a simple password “password”. Uncheck the box “User must change password at next login”.
5. Click Create.
6. Create another user with User name “user2” and simple password “bubble”. (or you can select another password value)
7. Create another user with User name “user3” and not-so-simple password “bluebubble”. (or you can select another password value)
8. Open the file, Ophcrack as Administrator; Right click the file, and “Run as administrator”.
9. 
10. Under Load menu, click on “Load SAM with samdump2”.

It will dump your current SAM file.

**If step 10 fails, proceed to the below steps, a to e Only.**

a. Create a new folder, and copy Mimikatz.exe, mimidrv.sys and mimilib.sys to it.

b. Right click, mimikatz.exe, and “Run as Administrator”.

c. Type the command in RED.

d. Copy the NTLM hash of the username you one to crack to Ophcrack; for this case, I am cracking admin password.

e. Then proceed to crack the password using Ophcrack.

mimikatz # privilege::debug

Privilege '20' OK

mimikatz # sekurlsa::logonpasswords full

Authentication Id : 0 ; 614370 (00000000:00095fe2)

Session : Interactive from 1

User Name : admin

Domain : DESKTOP-A6FC7NP

Logon Server : DESKTOP-A6FC7NP

Logon Time : 1/7/2024 6:20:56 PM

SID : S-1-5-21-4200824037-223962120-302892357-1001

msv :

[00000003] Primary

\* Username : admin

\* Domain : DESKTOP-A6FC7NP

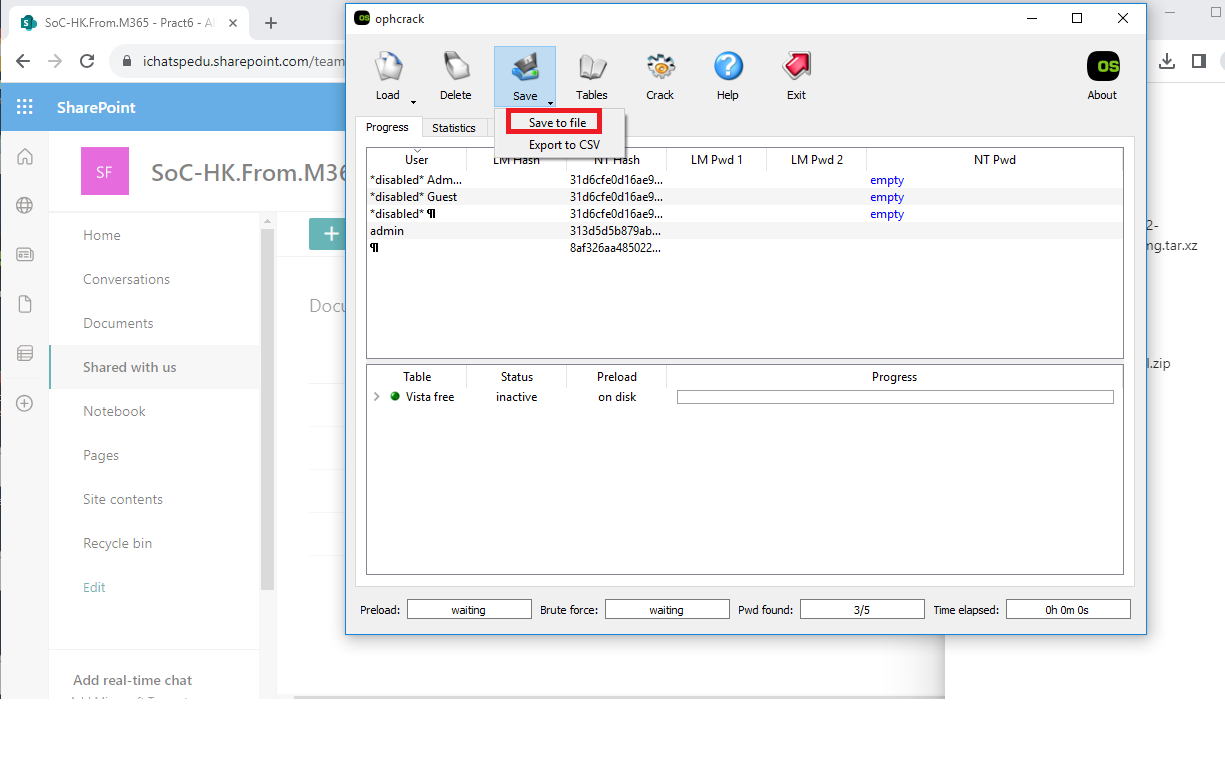
\* NTLM : 313d5d5b879ab0b9b3bbb2bb4ec9c697

\* SHA1 : 2c51df2937a28743c55d2cf90c69b8e8c03d3f0e

[00010000] CredentialKeys

\* NTLM : 313d5d5b879ab0b9b3bbb2bb4ec9c697

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_END\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

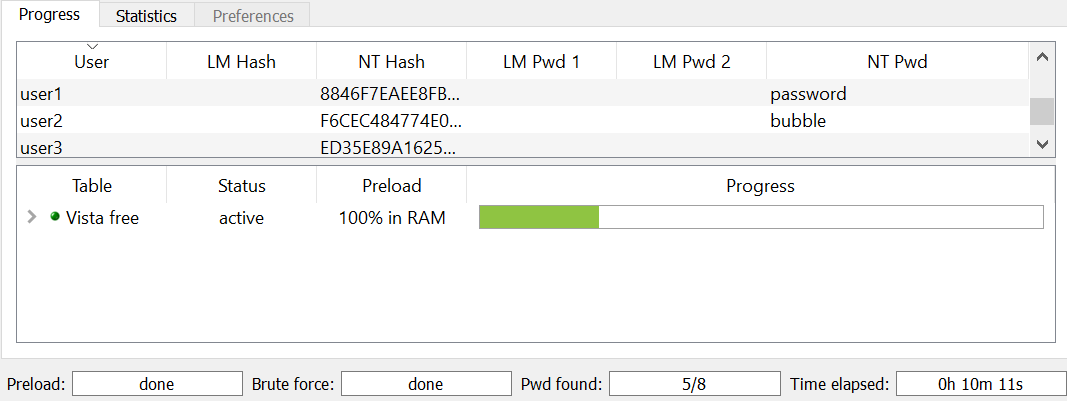


Under Save menu, click “Save to file”. Name the file;ntt.txt, and upload the file to your Kali VM.

You can use scp or any tools you have learnt in term 1.

1. Click Crack to start the password cracking. It may take a while to crack even the simple passwords.
2. You do not have to wait for all the passwords to be cracked, you can click Stop and exit Ophcrack.

With bigger rainbow tables, there is a higher chance that the passwords (if they are not complex) can be cracked.



## B. Using John the Ripper password cracker

In Kali VM:

1. Create a user with the simple password “service”.

sudo useradd –m user1

sudo passwd user1

1. In a terminal, run John the Ripper to crack the passwords in the current Linux shadow file.

sudo john /etc/shadow

You may get a message that there are no password hashes that John the Ripper can crack.

1. Run the following command to use John the Ripper with the crypt format to crack the hashed passwords; sudo john --list=formats | grep crypt

sudo john --format=crypt /etc/shadow

1. The passwords that are cracked will be displayed.
2. A directory called .john is created in the /root directory. The passwords that are cracked successfully are listed in a file john.pot in this directory. View the cracked passwords.

sudo cat /root/.john/john.pot

1. To view the cracked passwords again using John the Ripper command

sudo john –-show /etc/shadow

1. View the contents of the password list available in the john the ripper directory. This password list is tried when John the Ripper is used without any options. How many words are there in the default password.list?

less /usr/share/john/password.lst

wc –l /usr/share/john/password.lst

1. View the other word lists available in Kali. How many words are there in these word lists?

sudo find / -name \*wordlist\*

Some wordlists can be found in the directory /usr/share/wordlists.

1. Create two more users, this time with the passwords “backstreet” and “blueflowers”. These passwords are not in the default password.lst.
2. Run John the Ripper to crack the passwords in the Linux shadow file. When it can’t find the password in the password.lst, it will start to try all possible character combinations as passwords (brute force)

sudo john --format=crypt /etc/shadow

1. While John the Ripper is running, you can usually press Enter to see the status.
2. If you do not wish to wait for John the Ripper to crack the password, use Control-C to stop.
3. We will now run John the Ripper with another password list called “rockyou.txt”. It is currently located in /usr/share/wordlists in compressed mode, so we will uncompress it.

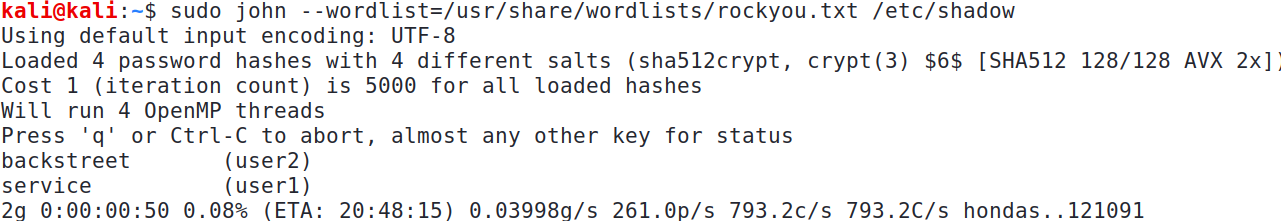
sudo gunzip /usr/share/wordlists/rockyou.txt.gz

1. Try running John the Ripper with the password list rockyou.txt. Enter the command in a single line.

sudo john --wordlist=/usr/share/wordlists/rockyou.txt --format=crypt /etc/shadow

<https://www.cyberciti.biz/faq/understanding-etcshadow-file/>

1. While John the Ripper is running, you can usually press Enter or other keys to see the status.



John the Ripper is trying the passwords in this range from the wordlist

1. If pressing the keys does not show the status, a workaround is to use the kill command to send a USR1 signal to the John the Ripper process.

First, in another terminal, run the ps command to find the Process ID of the John the Ripper process.

sudo ps –ef | grep john

Then use the kill command to send a USR1 signal to the John the Ripper process.

sudo kill –s USR1 *ProcessID* (replace *ProcessID* with ProcessID of john)

View the status in the terminal running John the Ripper.

John the Ripper can also crack Windows passwords.

└─$ sudo john --format=nt ntt.txt

## C. Using Hydra to crack network passwords

In web-server2 VM:

1. Create a new user with the simple password “peanut”.

useradd –m student01

passwd student01

In Kali VM:

1. Type “man hydra” to view the manual page for Hydra.
2. Run Hydra to crack the user student01’s SSH password on web-server2 VM with a password list. (check that the SSH service is still running)

Change to your web-server2 IP

Change to the user whose password you want to crack

hydra 192.168.10.100 ssh –l student01 –P /usr/share/wordlists/rockyou.txt –V –t 10

1. Hydra will try the values contained in the password list, ten at a time.

In web-server2 VM:

1. Such online password attacks can be easily detected. View the logfile /var/log/secure. You will see the many password attempts being logged.

Hydra can also be used to crack Web login forms.

Besides Hydra, Ncrack and Medusa can also be used to crack network passwords.

## D. Using fcrackzip to crack password protected zip files

In Kali VM:

1. Download the “fcrackzip.zip” file from the earlier links under “Files-for-Topic9”. You can also download from <http://http.kali.org> or install using the “apt-get install” command.
2. Extract the fcrackzip.zip.
3. Run the following command to install fcrackzip.

sudo dpkg -i fcrackzip\_1.0-10\_amd64.deb

1. Download the sample password-protected “files.zip” from Brightspace or the earlier links under “Files-for-Topic9”.
2. Try to unzip the file. A password is required to extract its contents.

unzip files.zip

1. In a terminal, type “man fcrackzip” to view the manual page for the fcrackzip command.
2. Run the following command to try fcrackzip with the dictionary list “rockyou.txt”

fcrackzip --dictionary –p /usr/share/wordlists/rockyou.txt files.zip

1. Fcrackzip will find a list of possible passwords. Try out the possible passwords and see which of them can extract the contents of “files.zip”.
2. Run fcrackzip with the -u option to try out all the possible passwords and see which of them can extract the contents of “files.zip”.

fcrackzip --dictionary –p /usr/share/wordlists/rockyou.txt –u files.zip

End of Practical 6