Install libre office

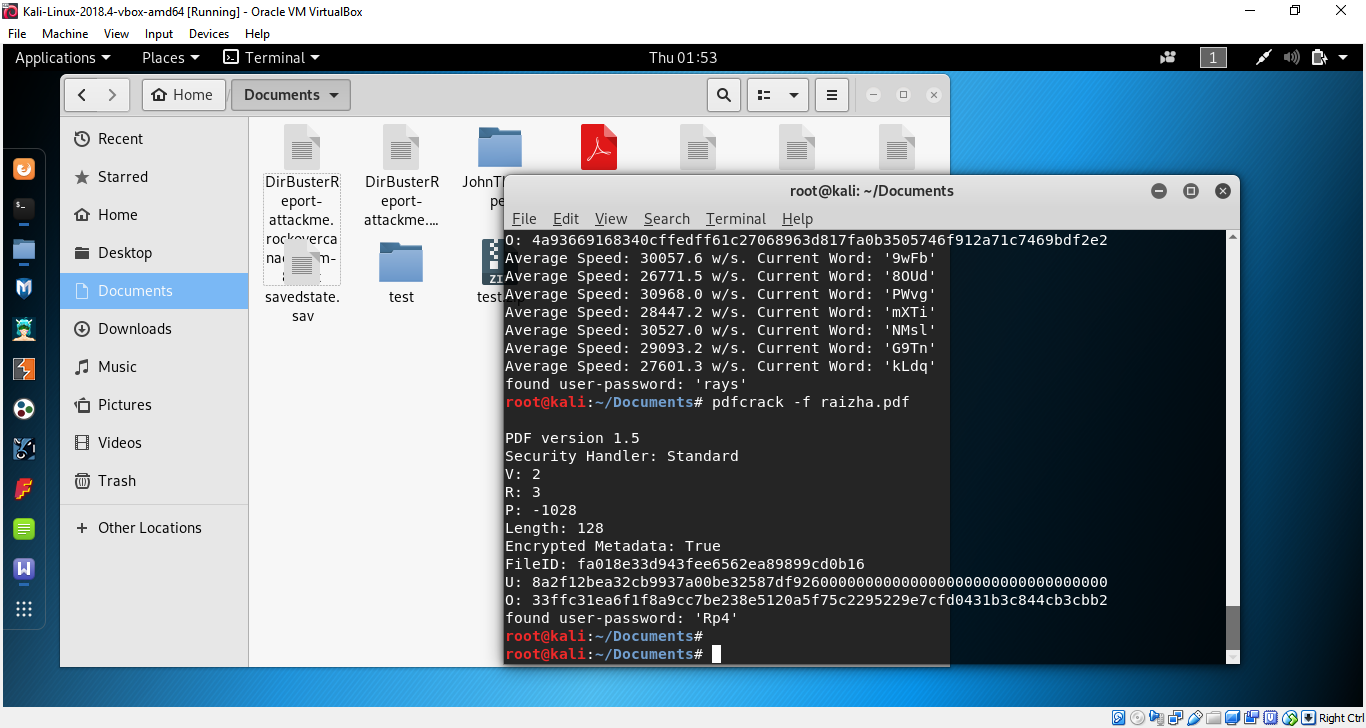
1. Enter into root with “sudo -I” if you have not done so already
2. **Sudo apt-get install libreoffice**

You choose the “File/Export to PDF” option and navigate to the “Security” tab. There you will find the “Set Passwords” buttons that will let you set a password for opening the file, or/and a password for editing permission. After setting the passwords, you can click the “Export” button and you are done.

This is a brute force attack

Pdfcrack

1. Install pdf crack
   1. **Sudo apt-get install pdfcrack**
2. Change your directory to the folder of the pdf you wish to crack
3. The base command is
   1. **Pdfcrack -f filename.extension (raizha.pdf)**



Typically I have found that 4 letters of any characters takes about 2-4 minutes. I am unsure for longer passwords.

*This format included uppercase, lowercase and number characters*

To perform PDFcrack with a dictionary

1. Enter the command
   1. **Pdfcrack -f (location of file) -w (location of dictionary)**
      1. Example
         1. Pdfcrack -f /root/Documents/rise.hash -w /usr/share/wordlists/rockyou.txt

How do I speed up password cracking?

1. You can use the following options. Try passing characters as follows:
   1. $ pdfcrack -f file.pdf -c abcdef123
2. Use the characters abcdef123 as charset to recover the password. In this example, stop when reaching 10 as password length:
   1. $ pdfcrack -f file.pdf -m 10
3. You can also skip trying passwords shorter than 8:
   1. $ pdfcrack -f file.pdf -n 8

Using JohnTheRipper

* Slower with BruteForce attack (using John)
* Faster with wordlist, Dictionary, attack
  + *Tested length up to “mitochondria” and it cracked it in 6 seconds*
  + *Though it had to be spelt in all lower cases.*

1. Install JohnTheRipper
   1. *I don’t know where the already installed JohnTheRipper folder is located, so essentially I have moved it*
   2. Change to the directory that you want to install the folder
   3. Enter the command
      1. **Git clone** [**https://github.com/magnumripper/JohnTheRipper.git**](https://github.com/magnumripper/JohnTheRipper.git)
2. Change the directory to your new JohnTheRipper folder
   1. Example:
      1. Cd Documents/JohnTheRipper
      2. Cd run

*You can do* ***ls*** *to confirm if there is the* ***pdf2john.pl*** *script*

*This format did numbers and lowercase letters*

1. Create the hash file
   1. Enter the command
      1. **./pdf2john.pl (location of pdf) > (location of hash)**
      2. Example
         1. ./pdf2john.pl /root/Documents/raizha.pdf > /root/Documents/rise.hash

To recreate the hash, you need to create another password for the file. Recreating the hash or txt file does not work from my experiments

1. Change directory to the folder of your hash file
2. Enter the command to crack
   1. **John –format=pdf rise.hash**
3. OR enter the command with wordlist
   1. **John –wordlist=(location of word list) (location of hash)**
   2. Example
      1. John –wordlist=/usr/share/wordlists/rockyou.txt ~/Documents/rise.hash
4. The terminal should then output the password for you

<https://www.howtoforge.com/tutorial/linux-pdf-password/>

<https://www.quora.com/How-can-you-install-LibreOffice-in-Kali-or-any-other-Linux-operating-system>

<https://www.cyberciti.biz/tips/linux-howto-crack-recover-pdf-file-password.html>

<https://www.youtube.com/watch?v=_K-EvuQt_2s>

<https://netlockit.wordpress.com/2017/11/03/cracking-password-protected-pdf-files-with-john-the-ripper/>