PASSWORD CRACKING WITH JTR

CYBERSECURITY & ETHICAL HACKING PROJECT TASKS

www.networkwalks.com

network Walks

WEEK 3 | PROJECT MODULE 1

PASSWORD CRACKING WITH JTR

Background

John the Ripper (JTR) is a popular password cracking tool used by security professionals to test how strong passwords are. It started as a tool for Unix systems but now works on Windows, Linux, and Mac. It can check many types of password hashes and also unlock password protected files like PDF, ZIP, and Office documents.

Johnny is the graphical version of John the Ripper. It gives a simple point and click screen, so beginners can use JTR without typing long commands. Both tools are widely used in security testing and learning labs to understand password safety.

In this lab task you will use JTR John and JTR Johnny to recover the password of a protected PDF file. This exercise helps you learn how password cracking works and why it is important to use strong passwords for protection.

Task

Crack the password of attached PDF file (My Locked PDF1.pdf) using JTR JOHN and JTR JOHNNY tools on your Windows PC.

Related Info:

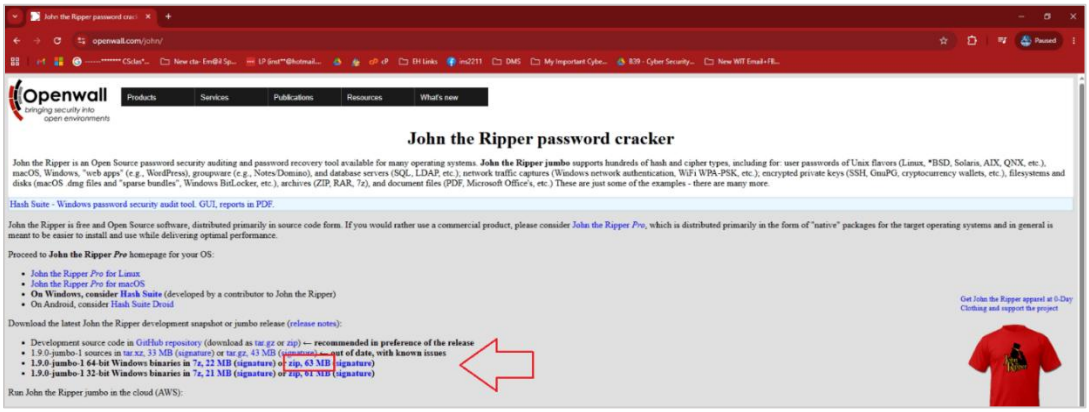
Note: If you are using Kali Linux then you can open JTR (John The Ripper) directly because it comes pre-installed in Kali Linux

Solution

STEP 1

Download John the Ripper from official website on your windows PC:

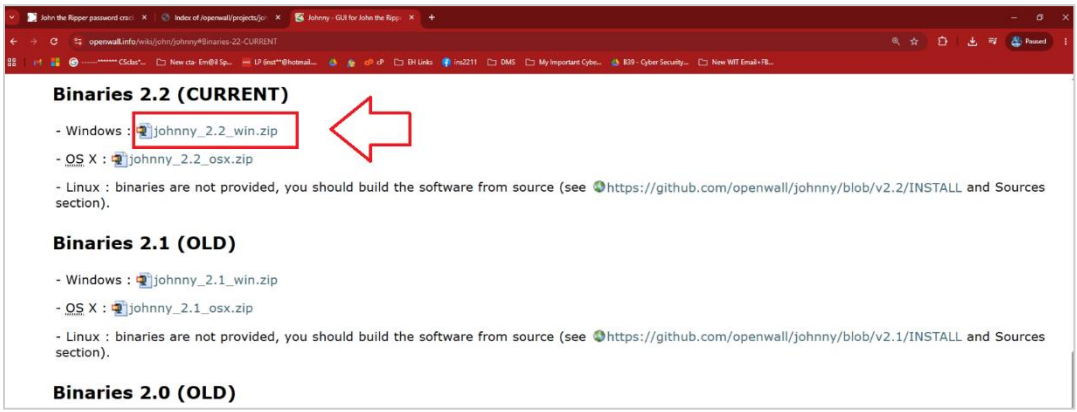
https://www.openwall.com/john/
or https://distro.ibiblio.org/openwall/projects/john/1.9.0/
or you can download from Google Drive:
https://drive.google.com/drive/u/1/folders/1aHtgOh7U9mQhkN8VHU7ctTyaDg5KbuJx



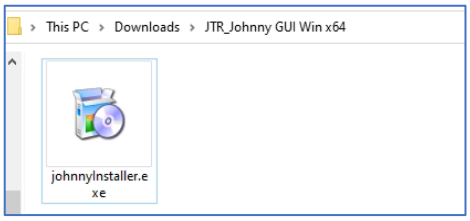
STEP 2

Download Johnny GUI from official website:

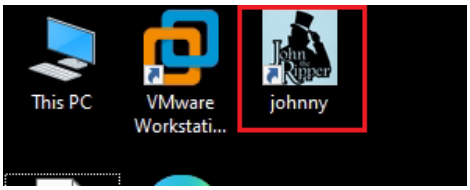
https://openwall.info/wiki/john/johnny
or you can download from Google Drive:
https://drive.google.com/drive/u/1/folders/1aHtgOh7U9mQhkN8VHU7ctTyaDg5KbuJx



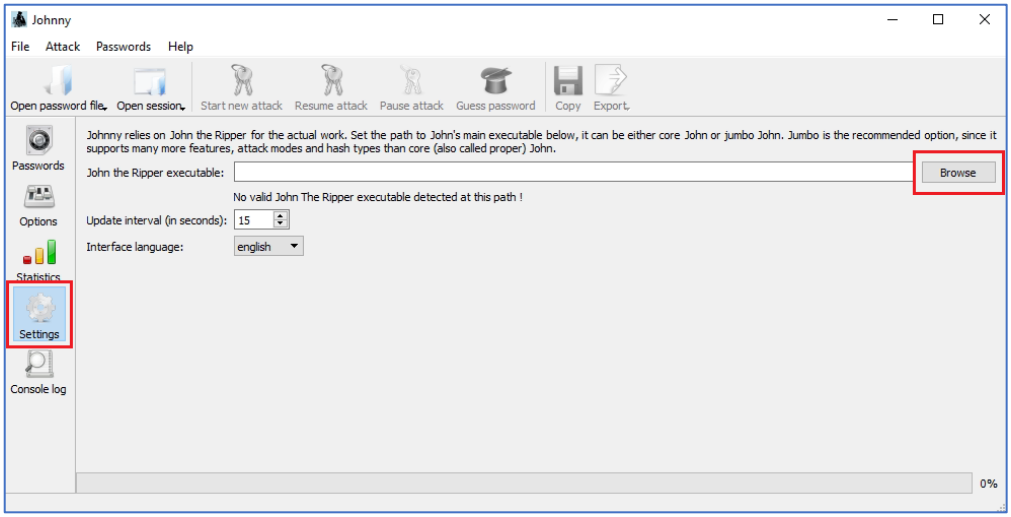
Run the setup file & install Johnny as shown in below:



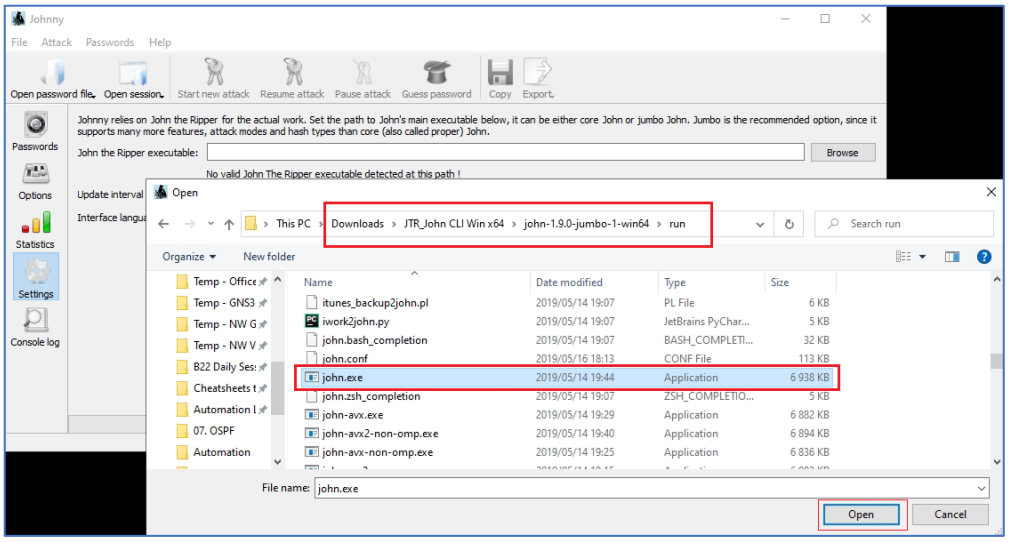
After installation, open Johnny:



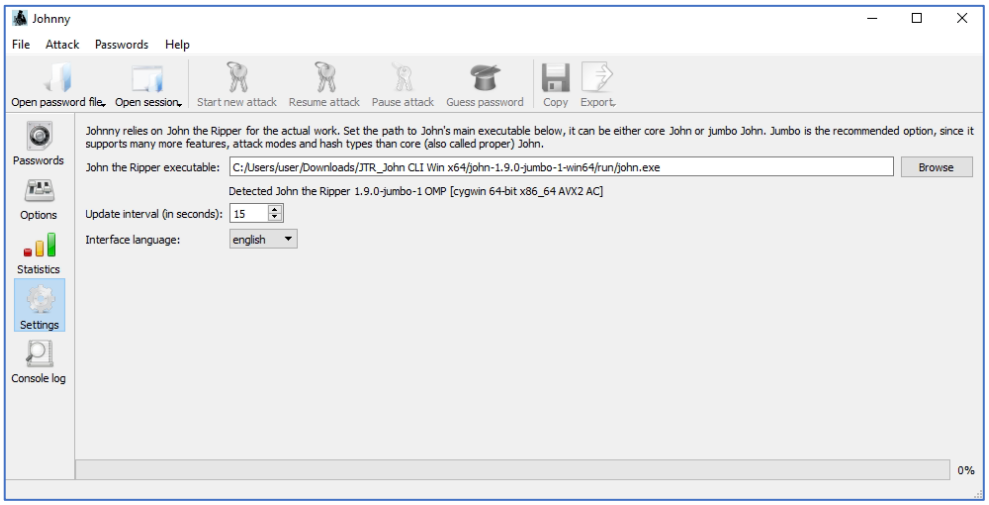
Click on settings & browse:



Select John.exe:



**john.exe file is located in the run folder as shown in this screenshot.*



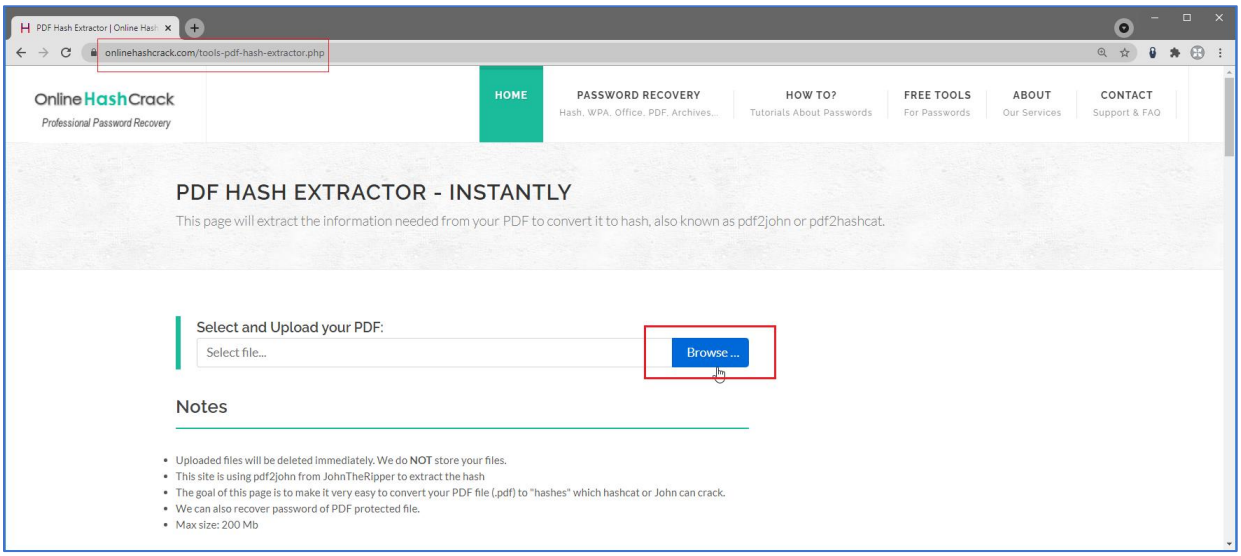
STEP 3

Follow below steps to crack the password.

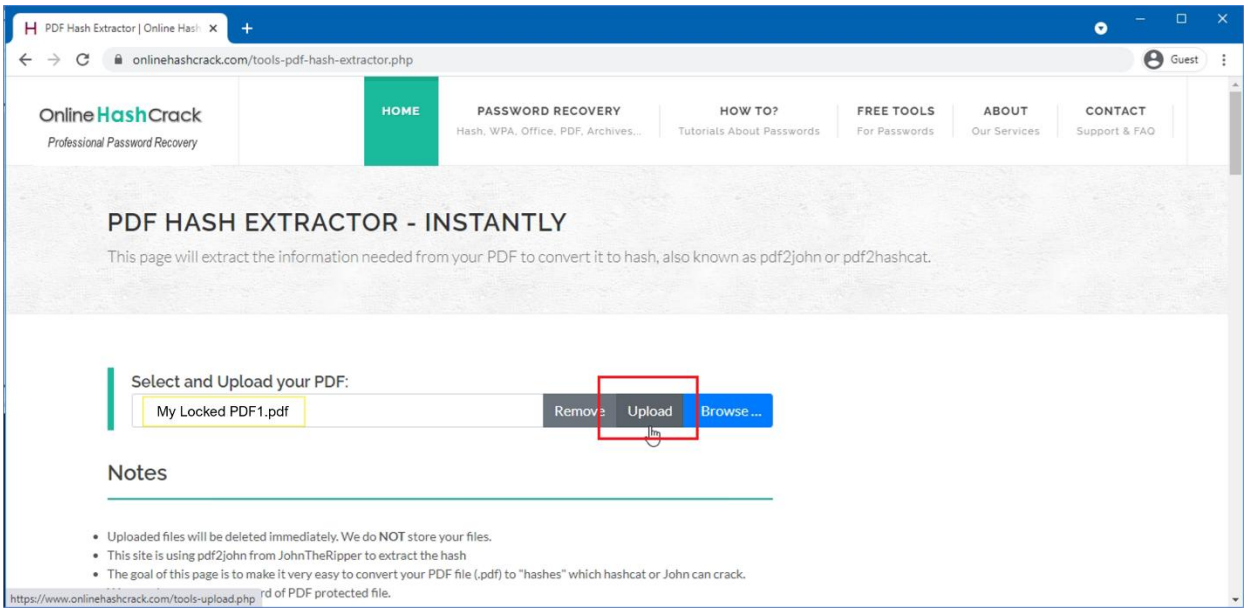
Download the encrypted PDF file to your PC:

Open the hash website & upload your pdf file to find its hash:

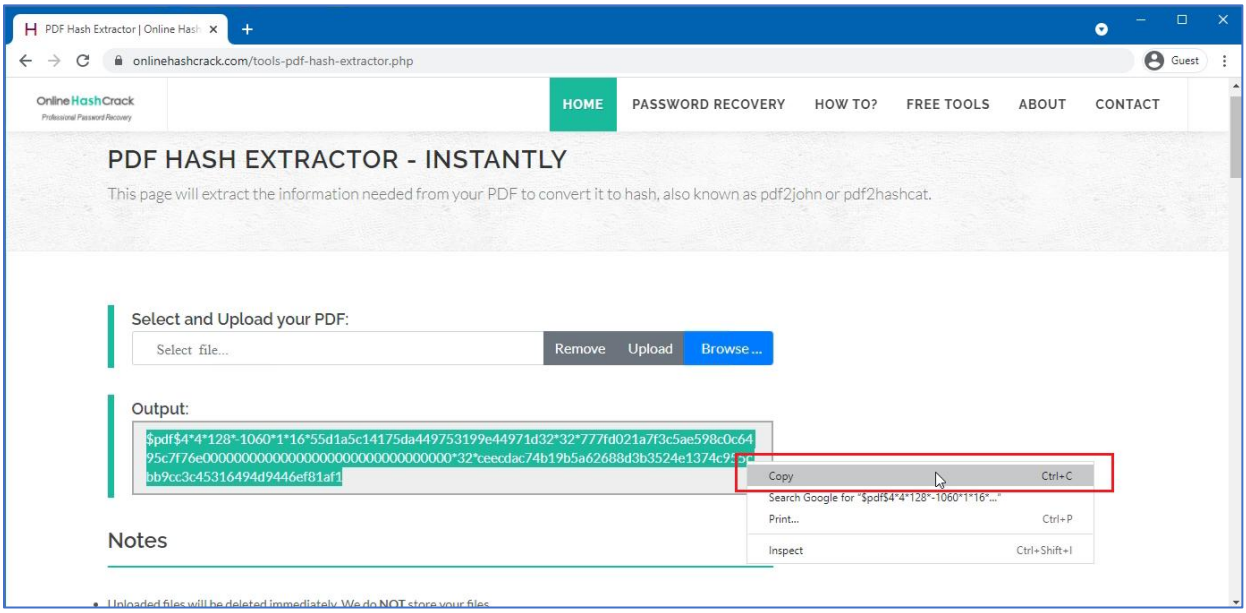
https://www.onlinehashcrack.com/tools-pdf-hash-extractor.php



Browse the PDF file & click on Upload:

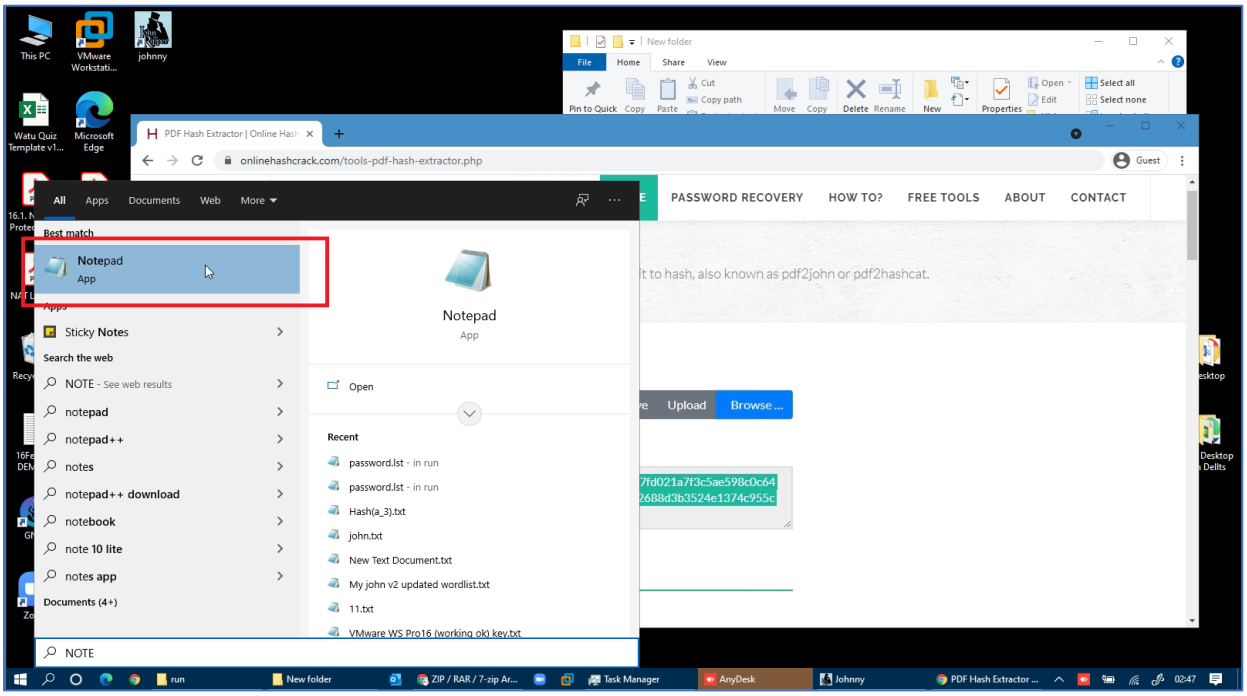


Select & copy the hash value:

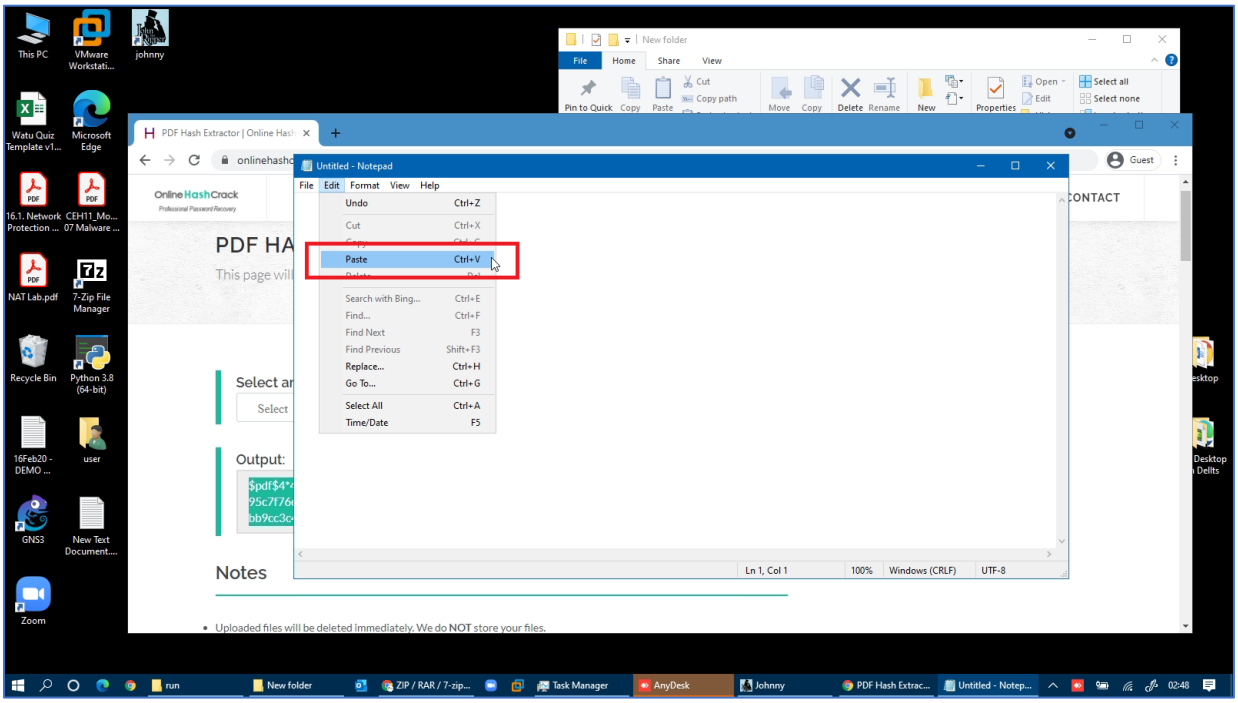


***Note:** If your hash contains extra characters like b' in the start then make sure to remove those when saving in txt file (hash value should be in the format shown in above screenshot i.e. starting with pdf....).

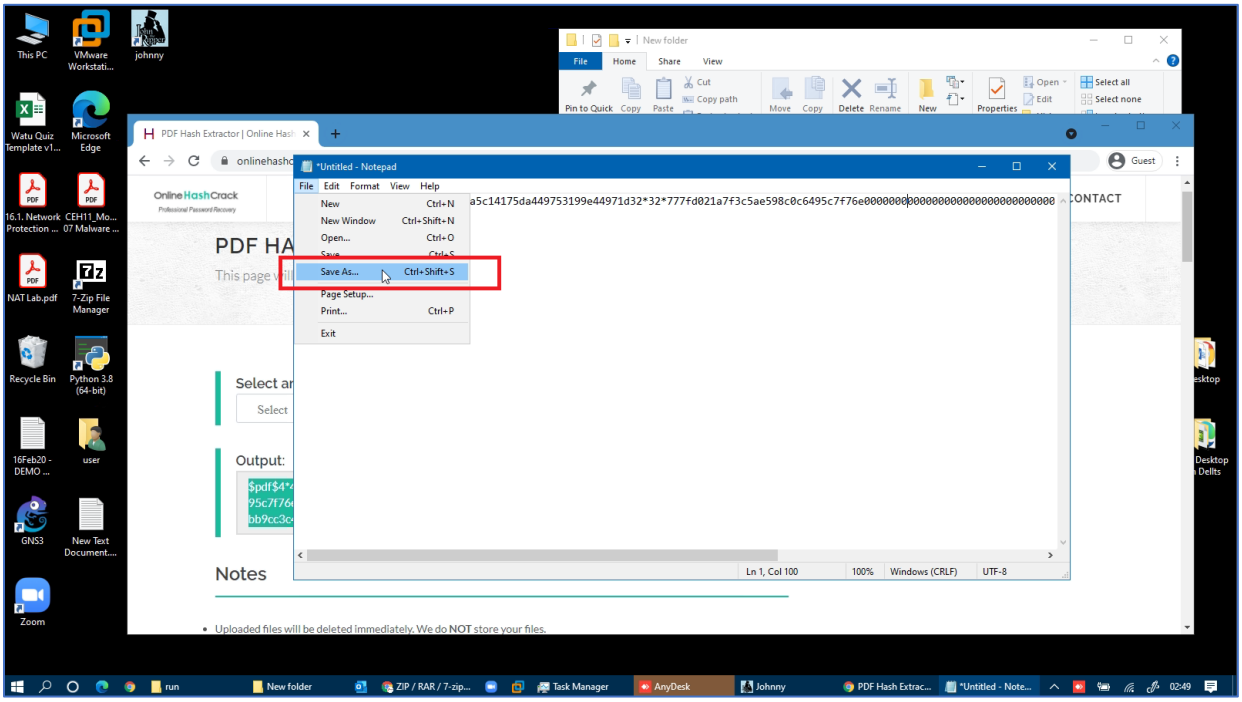
Open notepad:



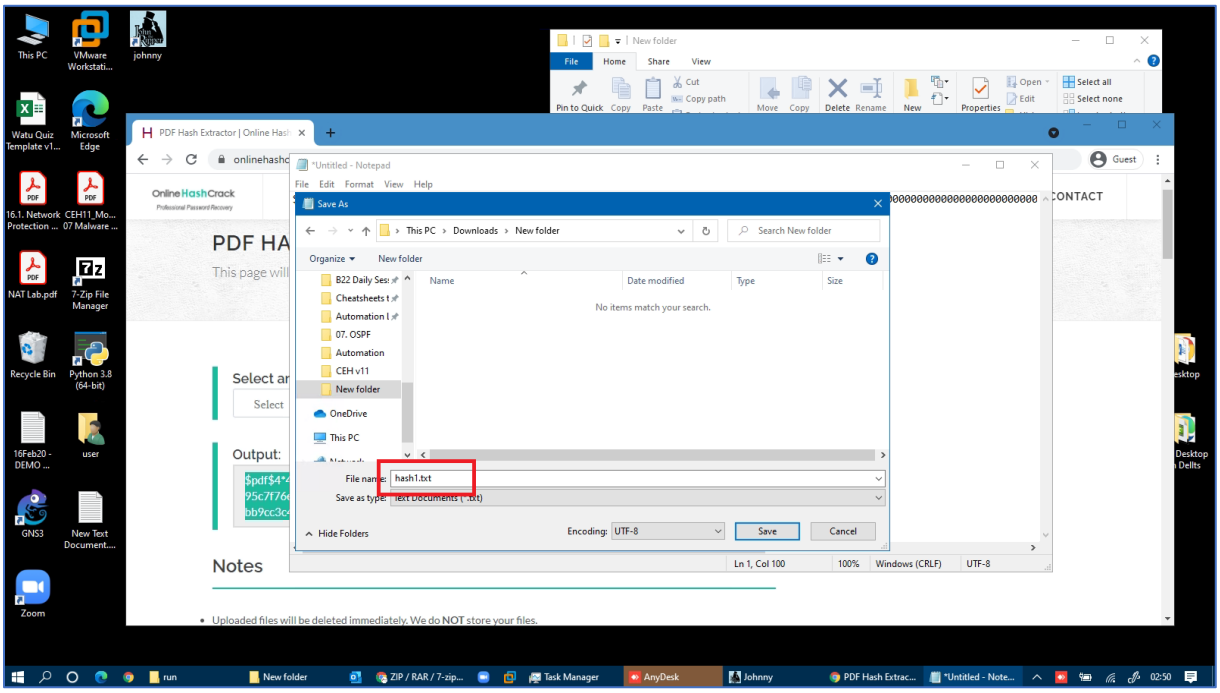
Paste the hash value inside notepad:



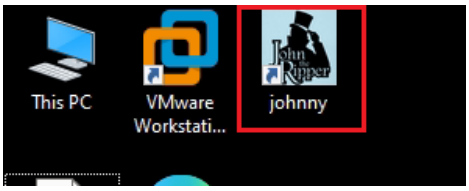
Save as text file:



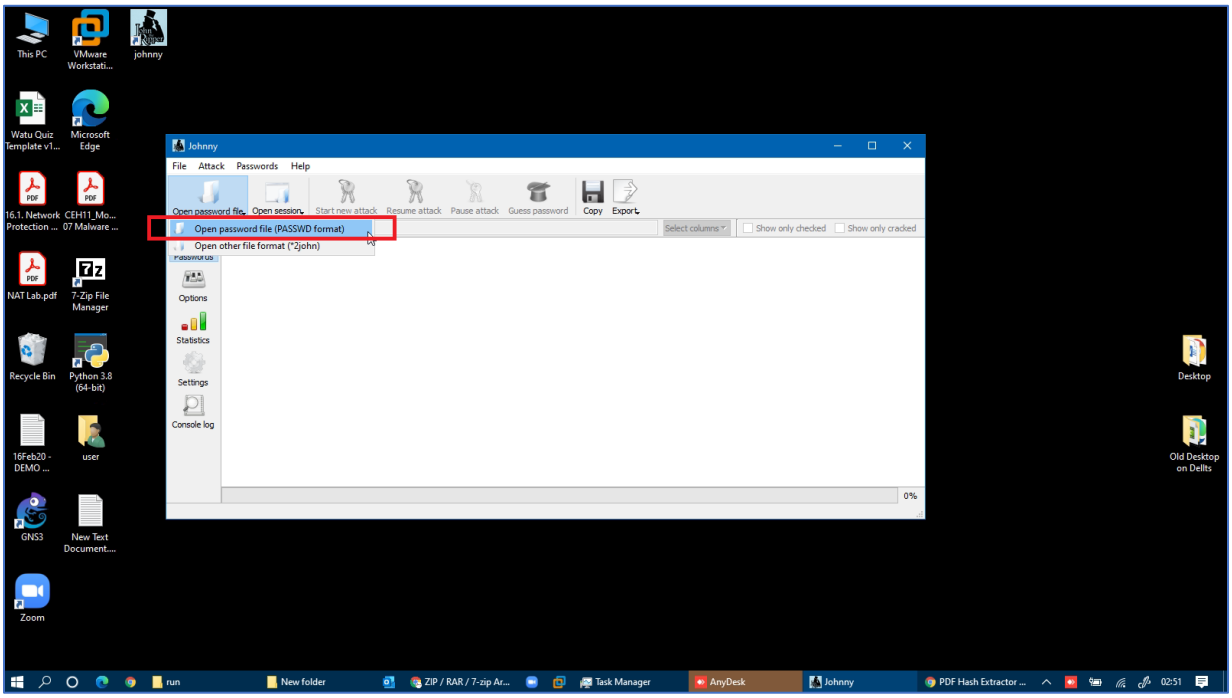
Save the file with name *hash1.txt:*



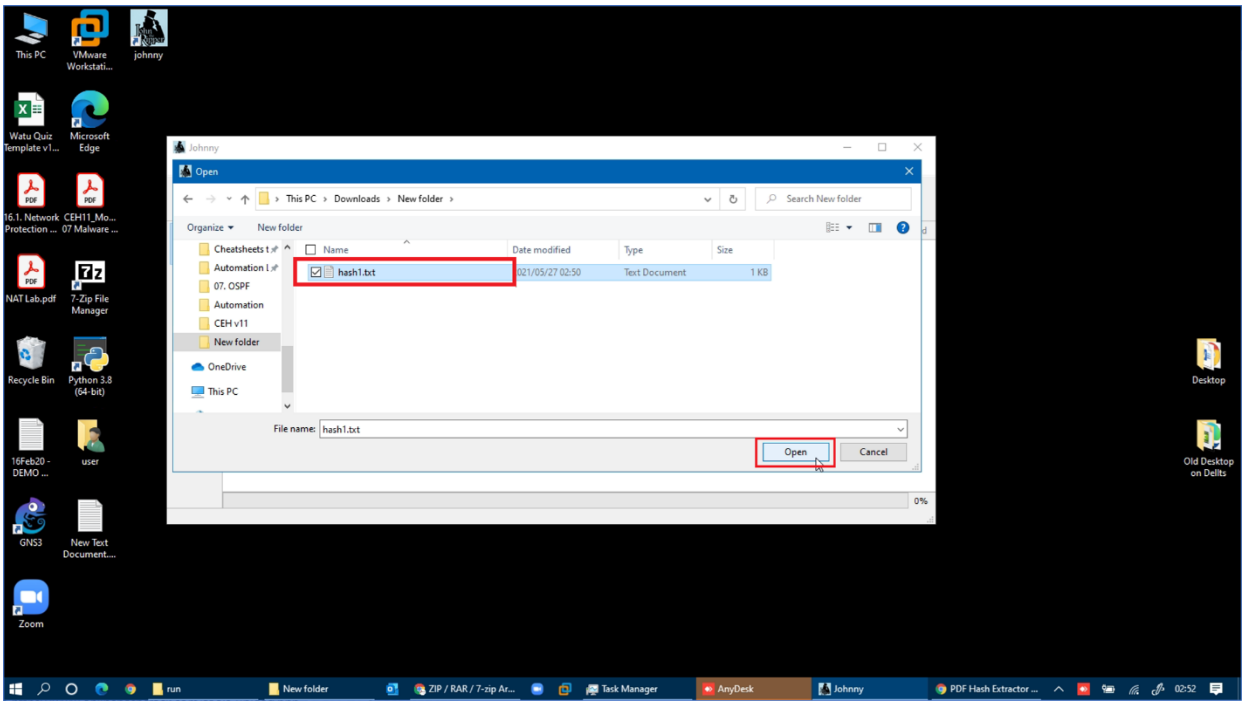
Open Johnny again:



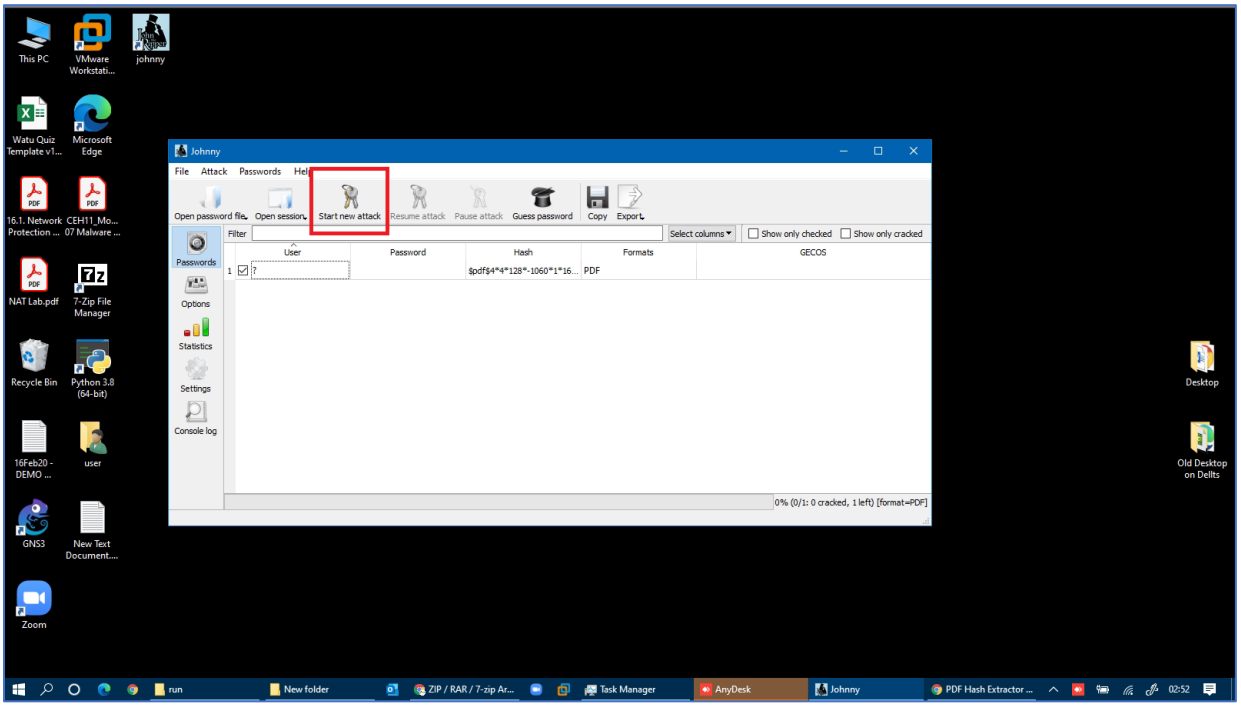
Click on '*Open password file*':



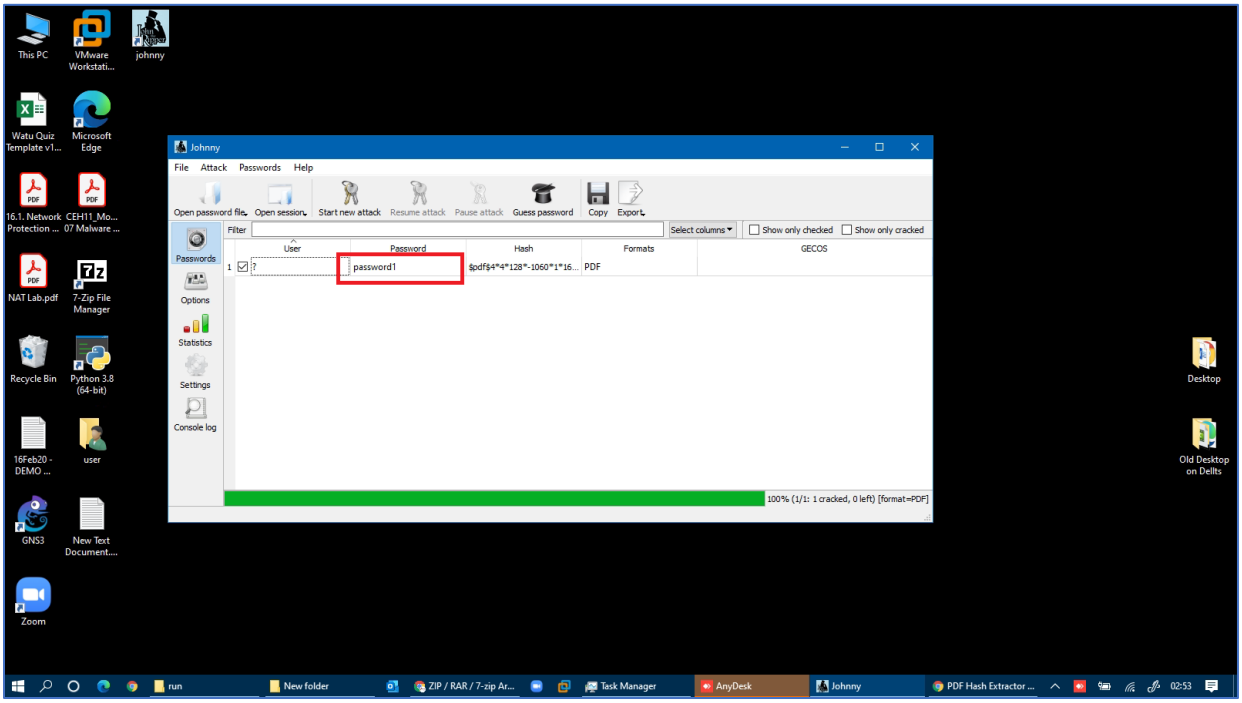
Browse to the *hash1.txt* file that you have just saved & click on Open:



Click on *'Start new attack':*

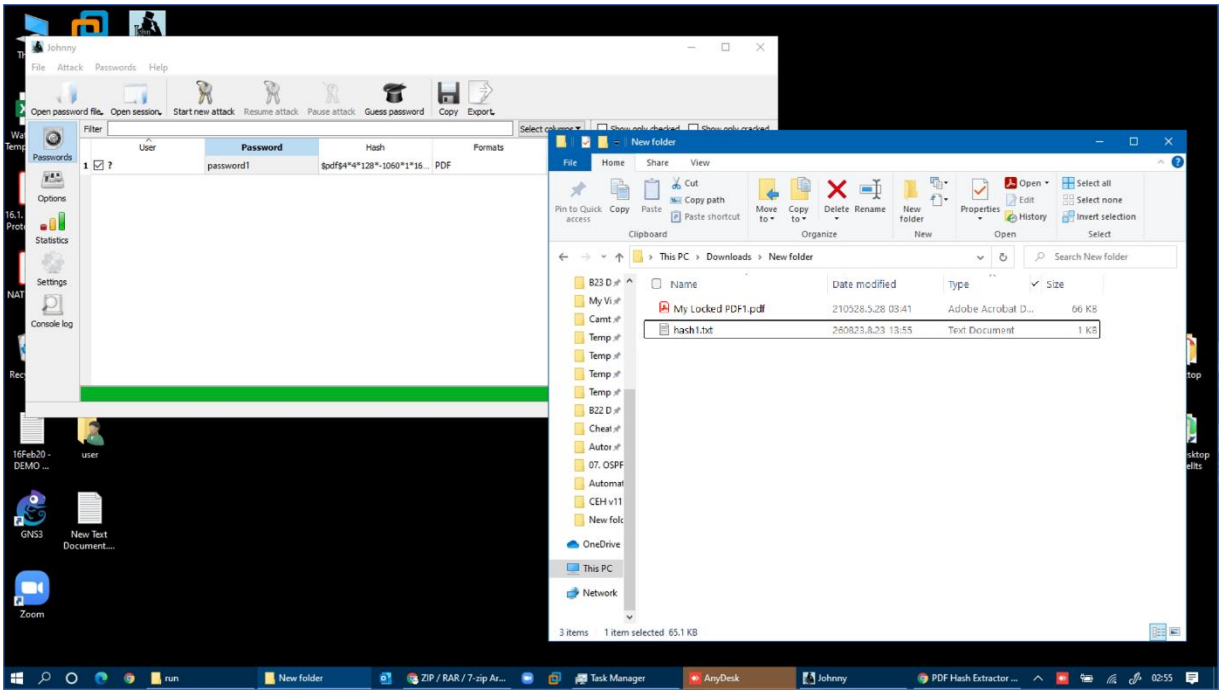


Your PDF file password will be cracked (it might take some time depending on your computer speed & password complexity):

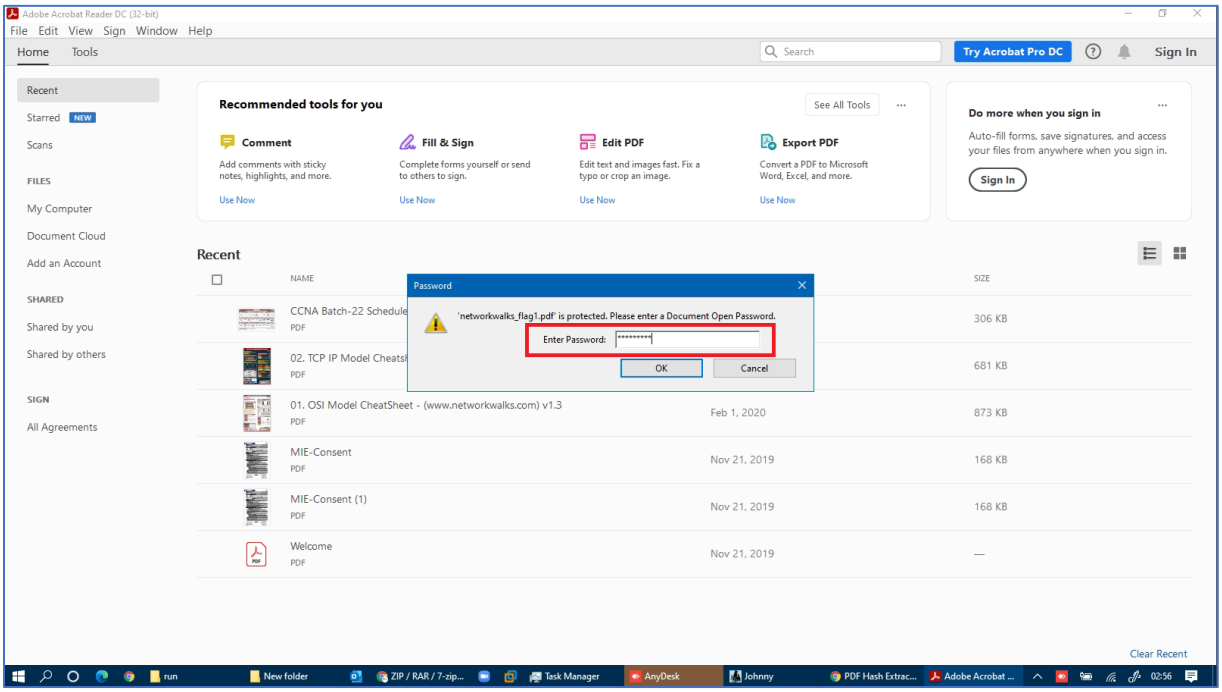


Now you can use this password to open your PDF file.

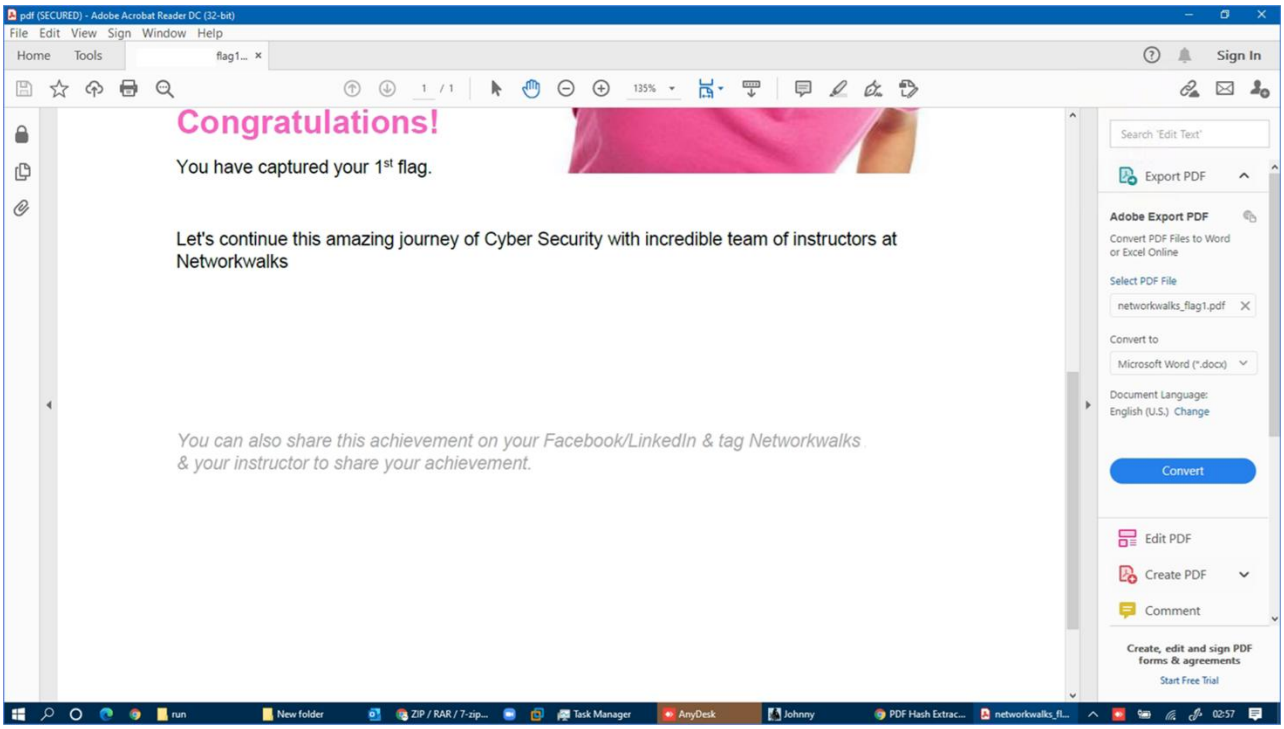
Open the encrypted PDF:



Enter *password1* (which you have just cracked):



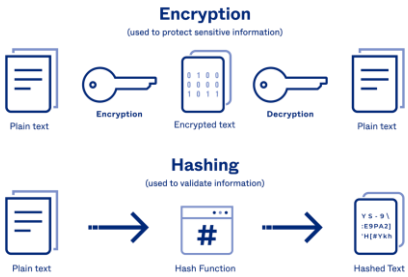
Your PDF file will open.


pdf (SECURED) - Adobe Acrobat Reader DC (32-bit)
File Edit View Sign Window Help
Home Tools
Sign In
Congratulations!
You have captured your 1st flag.
Let's continue this amazing journey of Cyber Security with incredible team of instructors at Networkwalks
You can also share this achievement on your Facebook/LinkedIn & tag Networkwalks & your instructor to share your achievement.
Export PDF
Adobe Export PDF
Convert PDF Files to Word or Excel Online
Select PDF File
networkwalks_flag1.pdf
Convert to
Microsoft Word (*.docx)
Document Language: English (U.S.) Change
Convert
Edit PDF
Create PDF
Comment
Create, edit and sign PDF forms & agreements
Start Free Trial

-End-

Extra References & tips

Encryption is a two-way function; what is encrypted can be decrypted with the proper key. Hashing, however, is a one-way function that scrambles plain text to produce a unique message digest, as shown in below.



DO YOU KNOW?

2026 - South Africa - MTN Group's 2025 breach escalated in 2026, over 5,700 customers affected in Ghana alone and criminal investigations opened across multiple countries

2025 - Namibia - Telecom Namibia refused to pay ransom, attackers leaked billing data of senior government officials, exposing personal records of thousands of subscribers

2025 - Senegal - National tax authority ransomware attack threatened to erase and leak fiscal records covering millions of citizens and businesses

2024 - Uganda - Hackers broke into the Bank of Uganda and stole $16.8 million (one of Africa's largest ever banking cyber heists)

2024 - Nigeria - Fintech giant Flutterwave was hacked and ~$7 million silently diverted from customer accounts

2024 - South Africa's Cell C breach exposed 2TB of data from 7.7 million customers, including ID numbers and banking details

2024 - Kenya's Urban Roads Authority (KURA) suffered a major data breach exposing sensitive government infrastructure data

2024 - Cameroon's National electricity provider ENEO was cyberattacked, suspending power management applications nationwide