

PDF Password Cracking with pdfrip



ATTACKS

John the Ripper – Perl Module

Pdfrip - Windows

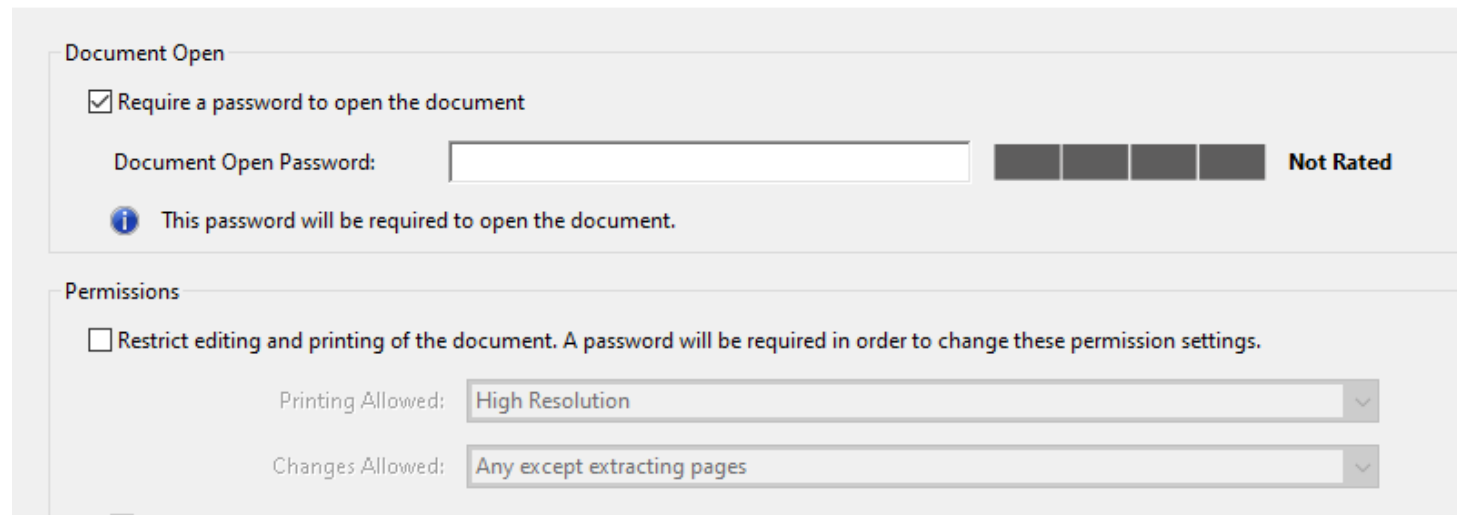
Crack PDF passwords with pdfrip on Windows

Step- 1

❖ Prepare a password protected Pdf file

Go to properties and in the Security tab, you can apply a password

Password Security - Settings



The screenshot shows the 'Password Security - Settings' dialog box. It is divided into two main sections: 'Document Open' and 'Permissions'. In the 'Document Open' section, the checkbox 'Require a password to open the document' is checked. Below it, there is a text input field for the 'Document Open Password' which is currently empty, followed by a password strength indicator showing four dark grey squares and the text 'Not Rated'. An information icon (i) is present next to the text 'This password will be required to open the document.' In the 'Permissions' section, the checkbox 'Restrict editing and printing of the document. A password will be required in order to change these permission settings.' is unchecked. Below this, there are two dropdown menus: 'Printing Allowed:' set to 'High Resolution' and 'Changes Allowed:' set to 'Any except extracting pages'.

Step- 1

- ❖ Download and install pdfrip from official GitHub repository

<https://github.com/mufeedvh/pdfrip/releases>



The screenshot shows the 'Assets' section of a GitHub release. It contains a table with five rows. The first row, 'pdfrip.exe', is highlighted with a red box. The other rows are 'pdfrip_amd64', 'pdfrip_darwin', 'Source code (zip)', and 'Source code (tar.gz)'. Each row lists the asset name, its size in MB, and the release date (11 Feb 2022).

Asset Name	Size	Release Date
pdfrip.exe	1.77 MB	11 Feb 2022
pdfrip_amd64	2.17 MB	11 Feb 2022
pdfrip_darwin	1.91 MB	11 Feb 2022
Source code (zip)		11 Feb 2022
Source code (tar.gz)		11 Feb 2022

Step- 2

- ❖ Download and extract the rockyou dictionary in pdfrip folder

<https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt>

- ❖ Copy the target file to the pdfrip folder as well

Step- 3

- ❖ Open the command terminal in the same folder.
- ❖ Run the following command to crack the password with the dictionary attack

```
>Pdfrip.exe crackme.pdf -w rockyou.txt
```

Here :

- Crackme.pdf is the password-protected file
- rockyou.txt is the dictionary file



DEMO



THANKS