

# Project Report

## Password Cracking->John The Ripper

### By- Abhinav Lather

#### John The Ripper Tool

John the Ripper is an Open Source password security auditing and password recovery tool available for many operating systems. **John the Ripper jumbo** supports hundreds of hash and cipher types, including for: user passwords of Unix flavors (Linux, \*BSD, Solaris, AIX, QNX, etc.), macOS, Windows, "web apps" (e.g., WordPress), groupware (e.g., Notes/Domino), and database servers (SQL, LDAP, etc.); network traffic captures (Windows network authentication, WiFi WPA-PSK, etc.)

->What is hashing a password?

Password hashing is the practice of algorithmically turning a password into ciphertext, or an irreversibly obfuscated version of itself, as a means of blocking against the threat of password breaches.

Some algorithms for Hashing are:-

- SHA-1
- SHA-256
- MD5
- AES

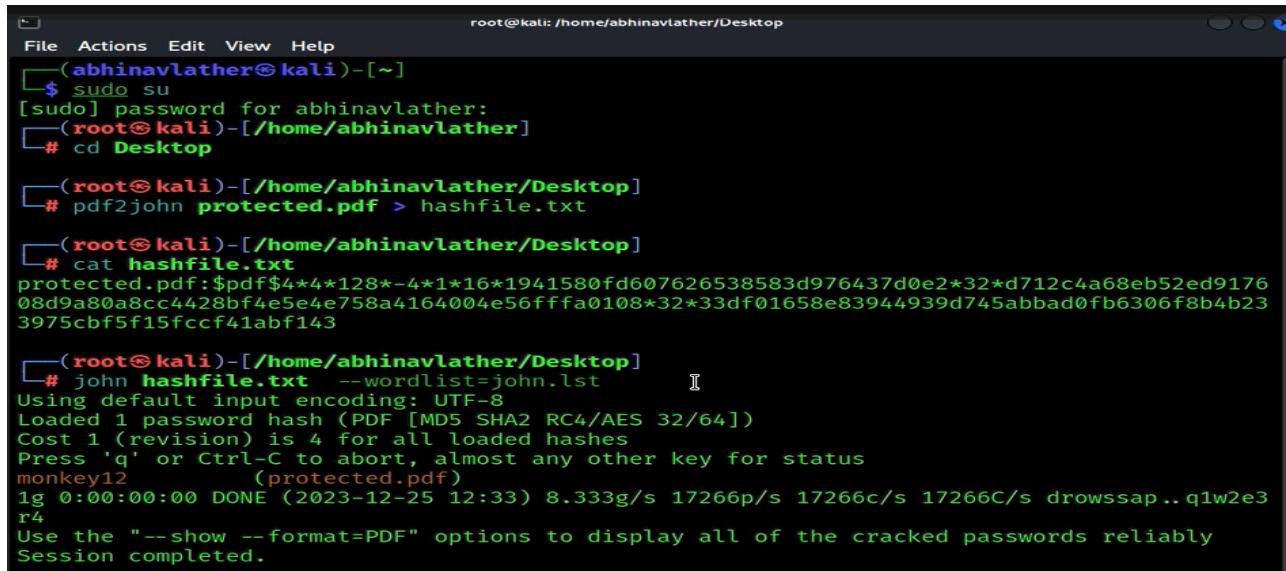
Passwords are stored in a hashed form so that they are not easy to read.

Commands used for cracking the password

1. pdf2john filename.pdf > hashfilename.txt

2. john hashfilename.txt --wordlist='file containing list of passwords'

## Screenshots




```
root@kali: /home/abhinavlather/Desktop
File Actions Edit View Help
(abhinavlather@kali)-[~]
$ sudo su
[sudo] password for abhinavlather:
(root@kali)-[/home/abhinavlather]
# cd Desktop

(root@kali)-[/home/abhinavlather/Desktop]
# pdf2john protected.pdf > hashfile.txt

(root@kali)-[/home/abhinavlather/Desktop]
# cat hashfile.txt
protected.pdf:$pdf$4*4*128*-4*1*16*1941580fd607626538583d976437d0e2*32*d712c4a68eb52ed9176
08d9a80a8cc4428bf4e5e4e758a4164004e56ffa0108*32*33df01658e83944939d745abbad0fb6306f8b4b23
3975cbf5f15fccf41abf143

(root@kali)-[/home/abhinavlather/Desktop]
# john hashfile.txt --wordlist=john.lst
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
Cost 1 (revision) is 4 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
monkey12 (protected.pdf)
1g 0:00:00:00 DONE (2023-12-25 12:33) 8.333g/s 17266p/s 17266c/s 17266C/s drowssap..q1w2e3
r4
Use the "--show --format=PDF" options to display all of the cracked passwords reliably
Session completed.
```



```
Media Player
john.lst [Read-Only]
~/Desktop
Save
1419 fishie
1420 flight
1421 florida1
1422 flowerpot
1423 forward
1424 freddie
1425 freebird
1426 freeman
1427 frisco
1428 fritz
1429 froggie
1430 froggies
1431 frogs
1432 fucku
1433 future
1434 gabby
1435 games
1436 garcia
1437 gaston
1438 gateway
1439 george1
1440 georgia
1441 german
1442 germany1
1443 getout
1444 ghost
1445 gibson
1446 giselle
1447 gmoney
1448 goblin
1449 gobblue
1450 gollum
1451 grandma
1452 gremlin
1453 grizzly
1454 grumpy
1455 guess
Plain Text Tab Width: 8 Ln 1, Col 1 INS
```

