

Module:- SECURITY CONCEPT (John The Ripper)

Name:-Prithviraj Nikam

John The Ripper

John The Ripper (JtR) is one of the most popular password cracking tools available in most Penetration testing Linux distributions like Kali Linux, Parrot OS, etc. The tool has been used in most Cyber demos, and one of the most popular was when it was used by the Varonis Incident Response Team. John The Ripper password cracking utility brags of a user-friendly command-line interface and the ability to detect most password hash types.

Password Cracking With John the Ripper (JtR)

Password cracking with JtR is an iterative process. A word is selected from the wordlist, hashed with the same hash algorithm used to hash the password, and the resulting hash is compared with the password hash. If they match, then the word picked from the wordlist is the original password. If they don't match, JtR will pick another word to repeat the same process until a match is found. And as you guessed it! This process can take some time if the password used was complex. John the Ripper supports most encryption technologies found in UNIX and Windows systems.

Modes of Password Cracking

JtR supports 3 main modes of password cracking:

- **Single Mode Crack:** JtR tries to use usernames found on the GECOS field and test them as possible passwords. GECOS is a field of each record in the **/etc/passwd** file on UNIX systems.
- **Wordlist mode:** JtR tries all the password combinations in a wordlist file.
- **Incremental mode (aka Brute-Force attack):** JtR tries all character combinations to crack the password.

Step-1:- First, you have to set password and protect any file. Then you can check the file

cd Downloads

ls

```
prithvi@kali: ~ x prithvi@kali: ~/Downloads x
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetH
(prithvi@kali)-[~]
$ cd Downloads

(prithvi@kali)-[~/Downloads]
$ ls
Android_protected.pdf  Nessus-10.4.1-debian9_amd64.deb  open
Google
Choose an account
```

Step-2:- get the password hash

To get the password hash to be cracked, we need to enter the command:

pdf2john Android_protected.pdf
Protected File name

```
(prithvi@kali)-[~/Downloads]
$ pdf2john Android_protected.pdf
Android_protected.pdf:$pdf$2*3*128*-4*1*16*e759c96322fb9748bb06ab822a710e99*
32*c32493e05fe1a02c81f3d29fd6debc3d28bf4e5e4e758a4164004e56fffa0108*32*09bb0
b88f5eeb18f87b82246a416c481a0877462a4cb401676f49569404c7a0a
Signed out
Prithvi Nikam
prithvi@gmail.com
```

Step-3:-put the password hash in a text file

Type the following command :

```
# pdf2john Android_protected.pdf > prithvihash.txt
```

Protected File name

Followed by:

```
# john prithvihash.txt
```

```
(prithvi@kali)-[~/Downloads]
$ pdf2john Android_protected.pdf > prithvihash.txt

(prithvi@kali)-[~/Downloads]
$ john prithvihash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
Cost 1 (revision) is 3 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed f
or performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123 (Android_protected.pdf)
1g 0:00:00:00 DONE 2/3 (2023-02-01 19:02) 1.886g/s 40094p/s 40094c/s 40094C/
s summer..123
Use the "--show --format=PDF" options to display all of the cracked password
s reliably
Session completed.

(prithvi@kali)-[~/Downloads]
$
```

Step-4:- Also used to “--show” for password showing

```
# sudo john prithvihash.txt - - show
```

```
(prithvi@kali)-[/usr/share/wordlists]
$ sudo john prithvihash.txt --show
Android_protected.pdf:123

1 password hash cracked, 0 left

(prithvi@kali)-[/usr/share/wordlists]
$
```

Step-5:- Now go to wordlist extract the **rockyou.txt.gz** File

#cd /usr/share/wordlists/

#sudo gunzip rockyou.txt.gz

```
(prithvi@kali)-[~]
$ cd /usr/share/wordlists/

(prithvi@kali)-[/usr/share/wordlists]
$ ls
amass  dirb  dirbuster  fasttrack.txt  fern-wifi  john.lst  legion  metasplo

(prithvi@kali)-[/usr/share/wordlists]
$ sudo gunzip rockyou.txt.gz
[sudo] password for prithvi:

(prithvi@kali)-[/usr/share/wordlists]
$ ls
amass  dirb  dirbuster  fasttrack.txt  fern-wifi  john.lst  legion  metasplo

(prithvi@kali)-[/usr/share/wordlists]
$
```

Step-6:- Now copy the **prithvihash.txt** to **/usr/share/wordlists/**

cp prithvihash.txt /usr/share/wordlists/

```

(prithvi@kali)-[~]
$ cd Downloads

(prithvi@kali)-[~/Downloads]
$ ls
Android_protected.pdf      opencti-master.zip  rockyou.txt
Nessus-10.4.1-debian9_amd64.deb  prithvihash.txt
opencti-master             prithvi.txt

(prithvi@kali)-[~/Downloads]
$ cp prithvihash.txt /usr/share/wordlists/
cp: cannot create regular file '/usr/share/wordlists/prithvihash.txt': Permission denied

(prithvi@kali)-[~/Downloads]
$ sudo cp prithvihash.txt /usr/share/wordlists/
[sudo] password for prithvi:

(prithvi@kali)-[~/Downloads]
$ cd /usr/share/wordlists/

(prithvi@kali)-[/usr/share/wordlists]
$ ls
amass      fasttrack.txt  john.lst      nmap.lst      sqlmap.txt
dirb       fern-wifi     legion        prithvihash.txt  wfuzz
dirbuster  hacker.txt    metasploit    rockyou.txt    wifite.txt

```

Step-7:- Sometimes you may need to customize or create your own wordlist or use a different wordlist the command follows the following format

john --wordlist= /usr/share/wordlists/rockyou.txt --format=PDF prithvihash.txt

sudo john prithvihash.txt --show

```

(prithvi@kali)-[/usr/share/wordlists]
$ john --wordlist= /usr/share/wordlists/rockyou.txt --format=PDF prithvihash.txt
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
No password hashes left to crack (see FAQ)

(prithvi@kali)-[/usr/share/wordlists]
$ sudo john prithvihash.txt --show
Android_protected.pdf:123

1 password hash cracked, 0 left

```