

Cracking ZIP File Passwords with John the Ripper: A Practical Demonstration

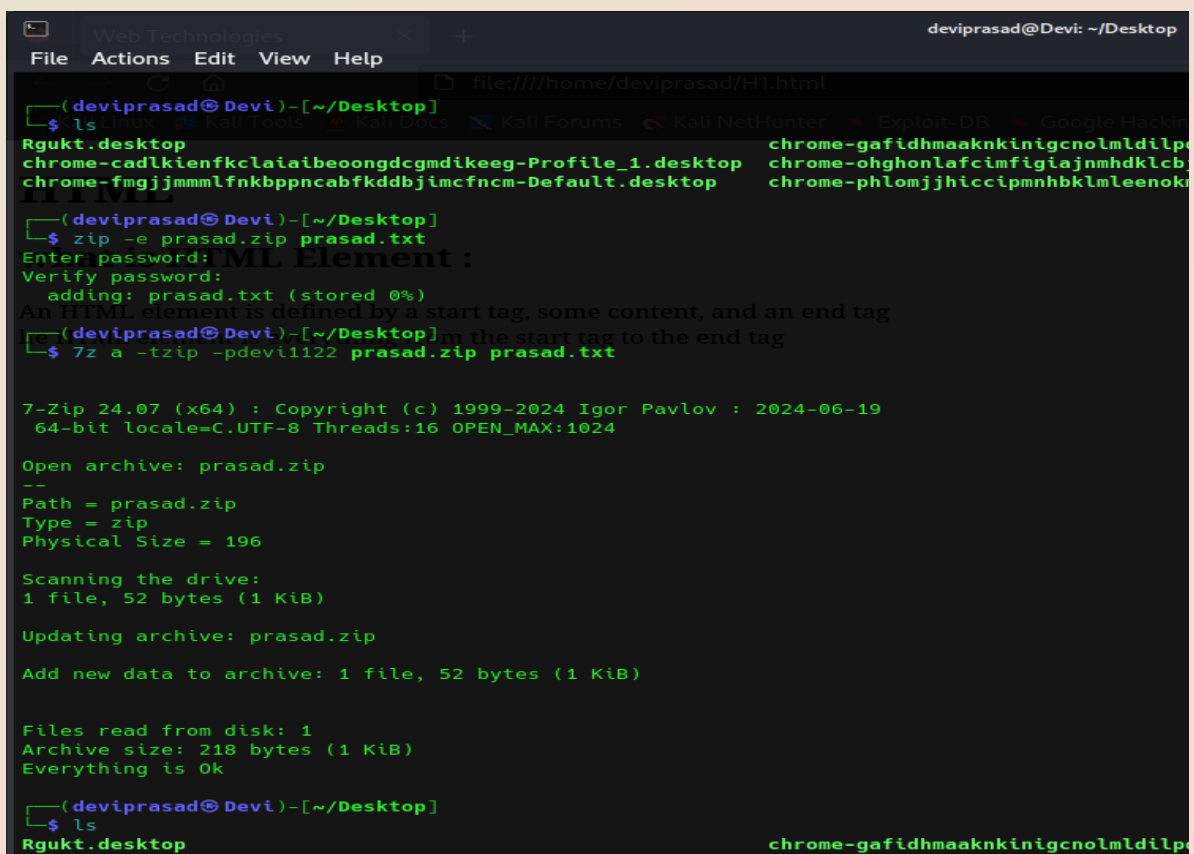
INTRODUCTION: I Have recently cracked password of a zip file using john the ripper and I want to demonstrate how I find the unknown password of my protected zip file.

OBJECTIVE: The main purpose of using this john ripper tool is to recover the forgotten passwords ethically

TOOLS USED: John the ripper
A secured zip file
zip2john

STEPS INVOLVED:

STEP1: At first I have created a zip file and protected it with a password then a password will be required to access or unzip the zip file everytime I need.



```
(deviprasad@Devi)~[~/Desktop]
$ ls
Rgukt.desktop  chrome-cadlkienfkclaiabeoongdcgmdikeeg-Profile_1.desktop  chrome-gafidhmaaknkinigcnoImldilp
chrome-fmgjjmmmlfnkbpncabfkddbilmcfncm-Default.desktop  chrome-ohghonlafclmfigiajnmhdklcb
chrome-phlomjjhiccipmnhbklmleenok

HTML
(deviprasad@Devi)~[~/Desktop]
$ zip -e prasad.zip prasad.txt
Enter password: ML Element :
Verify password:
adding: prasad.txt (stored 0%)
An HTML element is defined by a start tag, some content, and an end tag
(deviprasad@Devi)~[~/Desktop]
$ 7z a -tzip -pdevi1122 prasad.zip prasad.txt

7-Zip 24.07 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-06-19
64-bit locale=C.UTF-8 Threads:16 OPEN_MAX:1024

Open archive: prasad.zip
--
Path = prasad.zip
Type = zip
Physical Size = 196

Scanning the drive:
1 file, 52 bytes (1 KiB)

Updating archive: prasad.zip

Add new data to archive: 1 file, 52 bytes (1 KiB)

Files read from disk: 1
Archive size: 218 bytes (1 KiB)
Everything is Ok

(deviprasad@Devi)~[~/Desktop]
$ ls
Rgukt.desktop  chrome-gafidhmaaknkinigcnoImldilp
```

STEP2:After setting up a password for the zip file I have extracted the hash from the zip file using the command **zip2john**.

```
(deviprasad@Devi)-[~/Desktop]
$ zip2john prasad.zip > prasad.txt
ver 2.0 prasad.zip/prasad.txt PKZIP Encr: cmplen=64, decmplen=52, crc=1339F7DB ts=62DA cs=1339 type=0
what is HTML Element :
(deviprasad@Devi)-[~/Desktop]
$ ls
Rgukt.desktop chrome-gafidhmaaknkinigcnolmldilpdlfpa-Profile_1.desktop chrome.desktop
chrome-cadlkienfkclaiabeoongdcgmdikeeg-Profile_1.desktop chrome-ohghonlafcinfigiajnmhdklcbjlbfa-Profile_1.desktop prasad.txt
chrome-fmgjjmmmlfknkbpncabfkdbjmcfcnc-Default.desktop chrome-phlomjjhiccpnmhbkmlenokmcfmcg-Profile_1.desktop prasad.zip
(deviprasad@Devi)-[~/Desktop]
$ cat prasad.txt
prasad.zip/prasad.txt:$pkzip$1*1*2*0*40*34*1339f7db*0*28*0*40*1339*701ac5b8c431beddfe5c3b
b765195a03bc248e5881e86ec956ecd43f078d6e260e486ee0ae03f2ba5686454c73dd3031905
d277cbb00d3795f3949ceb8de7bc0*$/pkzip$prasad.txt:prasad.zip:prasad.zip
```

STEP3:Then a text file created **prasad.txt** , using **cat** command I can see the hash of the zip file shown in the above image

The hash of the zip file:

prasad.zip/prasad.txt:

**\$pkzip\$1*1*2*0*40*34*1339f7db*0*28*0*40*1339*701ac5b8c431beddfe5c3b
b765195a03bc248e5881e86ec956ecd43f078d6e260e486ee0ae03f2ba5686454c73
dd3031905d277cbb00d3795f3949ceb8de7bc0*\$/
pkzip\$:prasad.txt:prasad.zip:prasad.zip**

STEP4: After this step I used **john** tool to crack the password of the zip file , I used **john prasad.txt** command .

```
(deviprasad@Devi)-[~/Desktop]
$ john prasad.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
devi1122 (prasad.zip/prasad.txt)
1g 0:00:00:32 DONE 3/3 (2024-12-31 12:19) 0.03082g/s 10517Kp/s 10517Kc/s 10517KC/s devis151..devenz06
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(deviprasad@Devi)-[~/Desktop]
$ unzip prasad.zip
Archive:  prasad.zip
[prasad.zip] prasad.txt password:
replace prasad.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: █
```

STEP5:Here is my password **devi1122** shown in the above terminal image then I tried to unzip my zip file(**prasad.zip**) and tried with the password cracked using john ripper , then it worked.



Insights Gained from the Cracking Process:

Weak Passwords are Vulnerable: The cracked password emphasized how easily weak or common passwords can be broken, especially those found in popular dictionaries.

Importance of Strong Passwords: The demonstration highlighted the need for complex, unique passwords that are not easily guessable or included in common dictionaries.

John the Ripper's Versatility: The tool's ability to support various attack methods (e.g., dictionary and brute-force) makes it a valuable resource for password auditing and security testing.

Optimization Techniques: Adjusting rules and attack strategies can significantly reduce the time and computational resources needed for cracking.

Summary of the Demonstration: This demonstration showcased the use of John the Ripper to crack the password of a secured ZIP file. By extracting the hash and performing a dictionary attack, the password was successfully cracked, highlighting the vulnerability of weak or commonly used passwords. The process reinforced the importance of using strong, complex passwords and demonstrated John the Ripper's capabilities as a powerful password-auditing tool.

-Deviprasad