



Prince Sultan University
College of Computer and Information Sciences
CYS401 – Fundamentals of Cybersecurity

Practical 3: John the Ripper Password Cracking Tool in Kali Linux –
(Cracking .zip/.rar file password,
Cracking User Password
Cracking MS Office Documents Password)

***Disclaimer:** All the labs in this course are prepared for educational purposes. we can't harm anyone all the commands are done within our own system and network.*

Instructions:

- a. The assignment must be done individually.
- b. The assignment is of 10 marks. You'll have to demonstrate the assignment on your PC OR submit a report. For each assignment, there will be an assessment.
- c. The assignment should preferably be done on a laptop.
- d. Required Tools: Kali- Linux, John the Ripper.

Introduction:

What is John the Ripper Used for?

JtR is primarily a password cracker used during pentesting exercises that can help IT staff spot weak passwords and poor password policies.

JtR also includes its own wordlists of common passwords for 20+ languages. These wordlists provide JtR with thousands of possible passwords from which it can generate the corresponding hash values to make a high-value guess of the target password. Since most people choose easy-to-remember passwords, JtR is often very effective even with its out-of-the-box wordlists of passwords.

Lab Details:

In this lab we will use John the Ripper tool in Kali Linux to crack password for different type of files.

- Decrypt the user password
- .zip/ .rar file
- User passwords (if they are very weak and commonly use words)
- Password protected word document.

Steps:

Cracking password for .zip file:

1. On your windows machine, create a filename.zip file on desktop and set password for that file (Choose easy password).
2. Login to Kali Linux.
3. Drag and drop the .zip file in kali Linux machine.
4. Open JtR: go to application-> password attacks->john the ripper.
5. In kali terminal, type "cd Desktop/"
6. Type "zip2john filename.zip" (You will see the password in encrypted form)
7. Now we will export it to a text file. Type "zip2john filename.zip > pass.txt"
8. Read the file "cat pass.txt"
9. Now start cracking the password. Type "John -format=zip pass.txt" (you will see the password)
10. You can try the alphanumeric password, but it will take little bit more time for cracking.

Cracking User Password:

1. First create new user in kali machine. Type "sudo adduser Abeera".
2. To check type "cat /etc/passwd"
3. Assign password to Abeera. "passwd Abeera".
4. Now we will crack user password using JtR (in Kali, user password stored in shadow file). Type "john /etc/shadow" (it will give you pass for all the users including root)

Cracking password for .docx file:

1. To crack word document, you need JtR python script that decrypt password.
2. Create word file and put password on it. Drag it to kali machine
3. Open browser and type link
<https://raw.githubusercontent.com/magnumripper/JohnTheRipper/bleeding-jumbo/run/office2john.py>
4. Open terminal. Type "wget https://raw.githubusercontent.com/magnumripper/JohnTheRipper/bleeding-jumbo/run/office2john.py" (start cloning). Type "ls" to check the file (office2john.py)
5. Give execute permission to office2john.py to execute word document. Type "chmod +x office2john.py"
6. Export it to text file. Type "python office2john.py /home/Desktop/filename.docx > /home/Desktop/hash.txt"
7. "cd Desktop" -> cat hash.txt (to check the password)
8. cd ..
9. Crack using JtR. Type "john /home/kali/Desktop/hash.txt"
10. You will see the password. (It will take time based on the complexity of password).
11. Try the same method for .ppt, .xlsx etc.

***** Password Cracked 😊 *****

	<pre> Session Actions Edit View Help (shoug@kali)-[~] \$ cd ~ echo "this is my secret file" > secret.txt zip -P 1234 test.zip secret.txt adding: secret.txt (stored 0%) (shoug@kali)-[~] \$ zip2john test.zip > pass.txt cat pass.txt Created directory: /home/shoug/.john ver 1.0 efh 5455 efh 7875 test.zip/secret.txt PKZIP Encr: 2b chk, TS_chk, cmplen=35, decmplen=23, crc=9EEF1168 ts=29AB cs=29ab type=0 test.zip/secret.txt:\$pkzip\$1*2*2*0*23*17*9eef116b*0*44*0*23*29ab*b8b841451e28ffe463e8226cae6ec1a6 4772c849385a899e786ccd78d2e7204a0092dd*\$/pkzip\$:secret.txt:test.zip::test.zip (shoug@kali)-[~] \$ john pass.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 1234 (test.zip/secret.txt) 1g 0:00:00:00 DONE 2/3 (2026-10-17 05:14) 25.00g/s 1172Kp/s 1172Kc/s 1172KC/s 123456..ferrises Use the "--show" option to display all of the cracked passwords reliably Session completed. (shoug@kali)-[~] \$ john --show pass.txt test.zip/secret.txt:1234:secret.txt:test.zip::test.zip 1 password hash cracked, 0 left (shoug@kali)-[~] \$ </pre>	
	<pre> Session Actions Edit View Help (shoug@kali)-[~] \$ grep abeera ~/shadow.txt > abeera.txt (shoug@kali)-[~] \$ sudo rm -f /root/.john/john.pot [sudo] password for shoug: (shoug@kali)-[~] \$ sudo john --format=crypt abeera.txt Using default input encoding: UTF-8 Loaded 1 password hash (crypt, generic crypt(3) [??/64]) Cost 1 (algorithm [1:descrypt 2:md5crypt 3:summd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes Cost 2 (algorithm specific iterations) is 1 for all loaded hashes 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 123 (abeera) 1g 0:00:00:06 DONE 2/3 (2026-10-17 05:37) 0.1582g/s 163.2p/s 163.2c/s 163.2C/s 123456..pepper Use the "--show" option to display all of the cracked passwords reliably Session completed. (shoug@kali)-[~] \$ sudo john --show --format=crypt abeera.txt abeera:123:1001:1001:::/home/abeera:/bin/bash 1 password hash cracked, 0 left (shoug@kali)-[~] \$ </pre>	
	<pre> (shoug@kali)-[~] \$ office2john secret.docx > hash.txt cat hash.txt. john hash.txt john --show hash.txt cat: hash.txt.: No such file or directory Using default input encoding: UTF-8 Loaded 1 password hash (Office, 2007/2010/2013 [SHA1 128/128 ASIMD 4x / SHA512 128/128 ASIMD 2x AES]) Cost 1 (MS Office version) is 2013 for all loaded hashes Cost 2 (iteration count) is 100000 for all loaded hashes Will run 4 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status 0g 0:00:01:05 70.55% 1/3 (ETA: 05:43:18) 0g/s 117.1p/s 117.1c/s 117.1C/s 1dsecret.docx1..1docxsecret! Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst hello123 (secret.docx) 1g 0:00:01:56 DONE 2/3 (2026-10-17 05:43) 0.008585g/s 116.9p/s 116.9c/s 116.9C/s harriet..hilda Use the "--show" option to display all of the cracked passwords reliably Session completed. secret.docx:hello123 1 password hash cracked, 0 left </pre>	