UJAR TECH SOLUTION

NAME: Rithik varma

INTERN ID: UTS1103

TASK 8

Exploring the CIA Triad in Real-World Scenarios:

Understand and practically identify how to identify, prepare, and crack password hashes using John the Ripper (JTR), one of the most popular password-cracking tools.

PRACTICAL DESCRIPTION

Problem:- *Explore a Linux machine How password hashing works, How attackers exploit weak password storage , Hands-on experience with real-world cracking tools, Understanding the importance of password strength and salting*

Key Concepts of Cracking Password Hashes with (JtR):

1. John the Ripper:-

John the Ripper (JtR) is a password-cracking tool used by security professionals (and attackers) to recover plaintext passwords from their hashed values. It is widely used in penetration testing to test the strength of stored passwords.

2. Hashes:-

A hash is the output of a one-way cryptographic function (e.g., MD5, SHA1, SHA256). Systems store hashed passwords instead of plaintext. If hashes are weak, attackers can attempt to crack them using tools like John the Ripper.

3. How John the Ripper Works:-

John the Ripper cracks hashes using different attack modes:
Dictionary Attack – Tries words from a list (e.g., rockyou.txt).

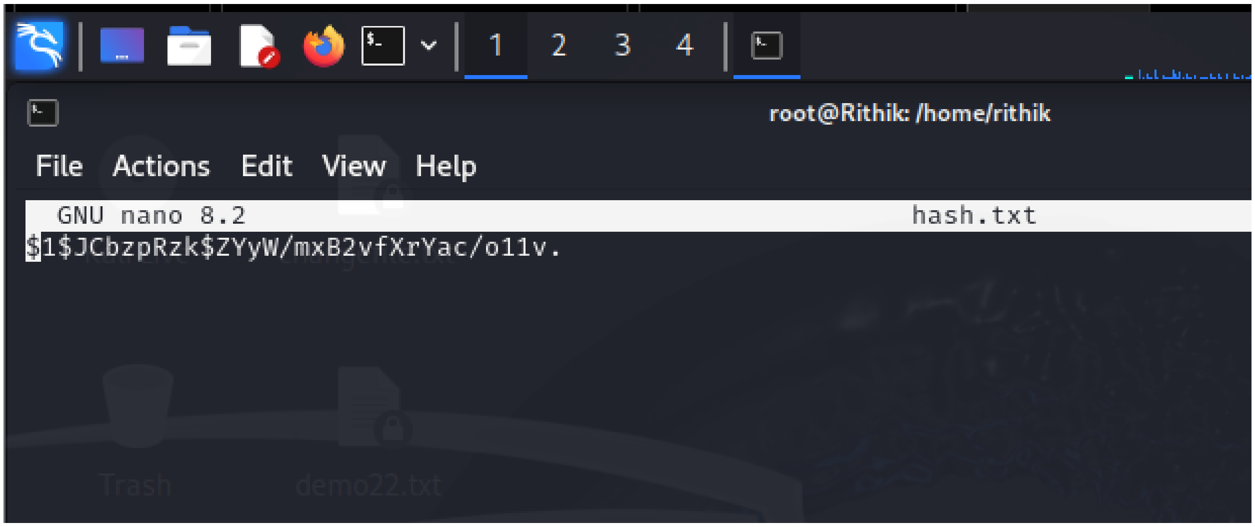
Brute Force Attack – Tries every possible character combination.

Hybrid Attack – Mixes dictionary + brute force (adds numbers/symbols to words).

Incremental Mode – Tries all possible passwords up to a certain length.

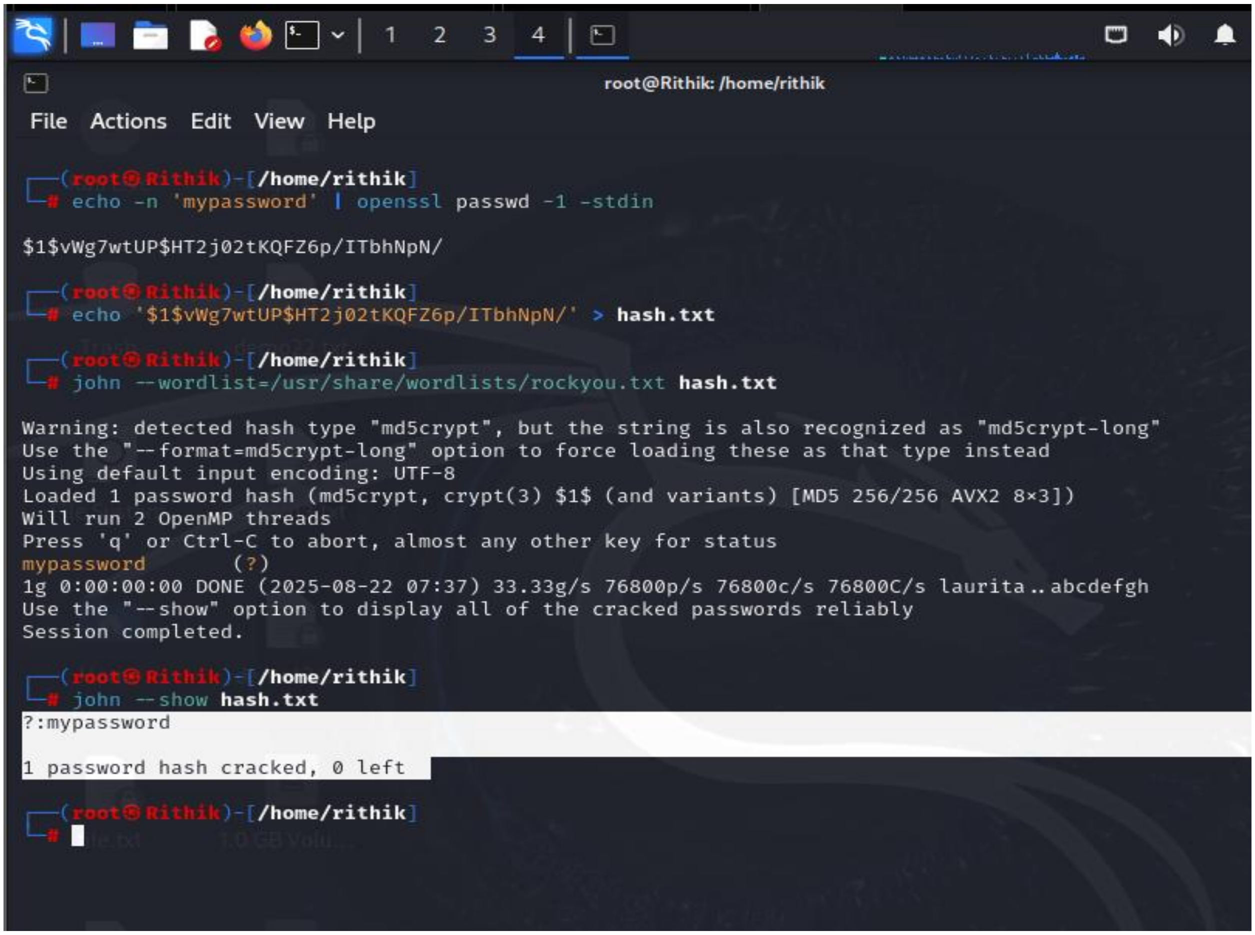
Practical of Crack Hashes with JtR Using Kali Linux:

Creating nano file to store hash password of name (hash.txt).



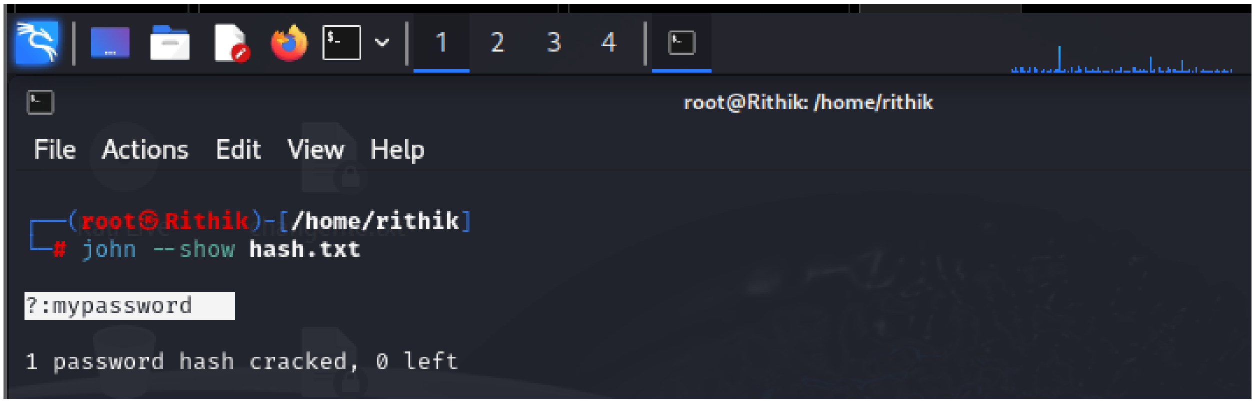
```
  GNU nano 8.2                                          hash.txt
$1$JCbzpRzk$ZYyW/mxB2vfXrYac/o11v.
```

Hear we have converted word into hasha codeusing(echo -n 'mypassword' | openssl passwd -1 -stdin)



```
┌──(root㉿Rithik)-[/home/rithik]
└─# echo -n 'mypassword' | openssl passwd -1 -stdin

$1$vWg7wtUP$HT2j02tKQFZ6p/ITbhNpN/

┌──(root㉿Rithik)-[/home/rithik]
└─# echo '$1$vWg7wtUP$HT2j02tKQFZ6p/ITbhNpN/' > hash.txt

┌──(root㉿Rithik)-[/home/rithik]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
mypassword       (?)
1g 0:00:00:00 DONE (2025-08-22 07:37) 33.33g/s 76800p/s 76800c/s 76800C/s laurita..abcdefgh
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿Rithik)-[/home/rithik]
└─# john --show hash.txt
?:mypassword

1 password hash cracked, 0 left

┌──(root㉿Rithik)-[/home/rithik]
└─# 
```

In above image we have used word list john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt



```
┌──(root㉿Rithik)-[/home/rithik]
└─# john --show hash.txt

?:mypassword

1 password hash cracked, 0 left
```

At end we aske to show cracked password using (john --show hash.txt)

Conclusion:-

John the Ripper demonstrates how easily weak passwords can be cracked from hashes.

To improve security, organizations should:

- *Enforce strong password policies*
- *Use modern salted hashing algorithms (bcrypt, scrypt, Argon2)*
- *Implement multi-factor authentication (MFA)*