Brute Force Attacks

- **Brute Force Password Attack**: A brute force attack involves systematically guessing every possible combination of letters, numbers, and special characters until the correct password is discovered. This method iterates through all potential combinations, starting from the simplest to the most complex.

- **Protection Against Brute Force Attacks**: To safeguard against brute force attacks, one effective method is implementing timeouts. This security measure locks out users after a certain number of failed login attempts, forcing them to wait before they can try entering passwords again, thus significantly slowing down the rate of attempted breaches.

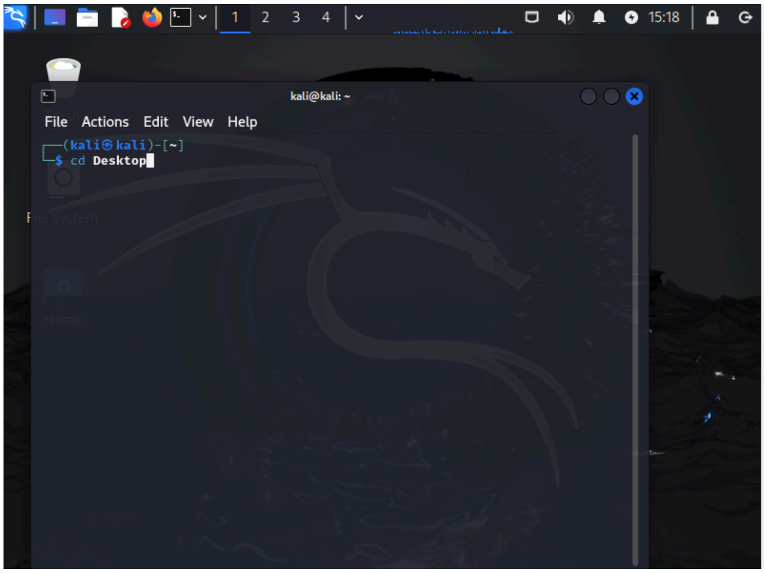
Equipment and Software Needed

- Kali Linux operating system
- John the Ripper password cracking tool installed

Step 1: Prepare the Environment

1. Open Terminal:
   - Press `Ctrl+Alt+T` to open a new terminal window on your Kali Linux desktop.
2. Create a Password Hash File:
   - Navigate to your desktop or a working directory:

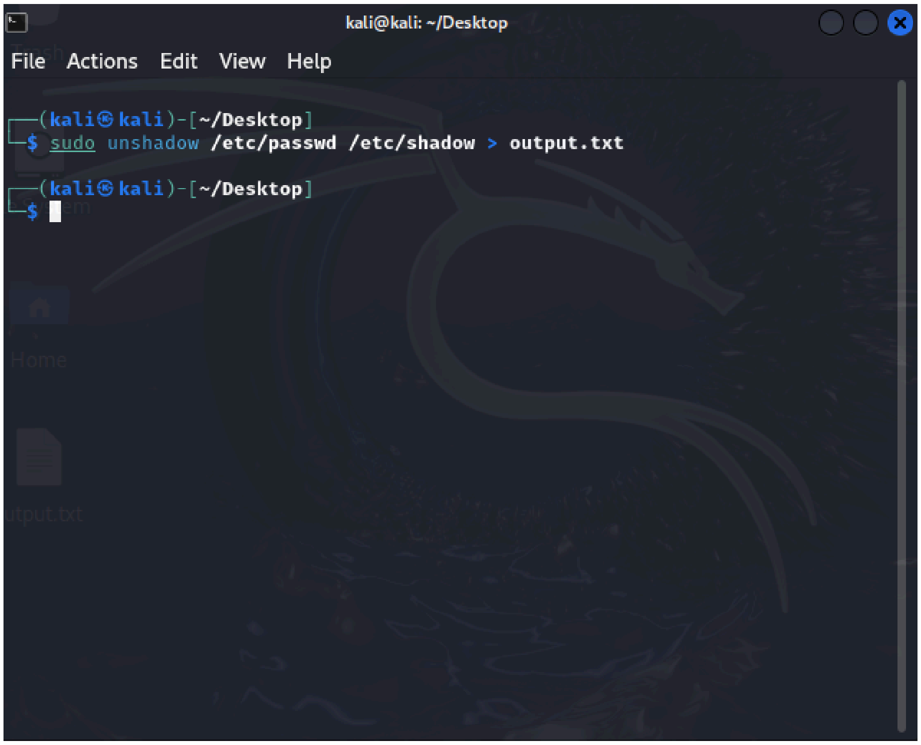
cd ~/Desktop



```
┌──(kali㉿kali)-[~]
└─$ cd Desktop
```

Combine the passwd and shadow files to output the hashes into a text file:

sudo unshadow /etc/passwd /etc/shadow > output.txt



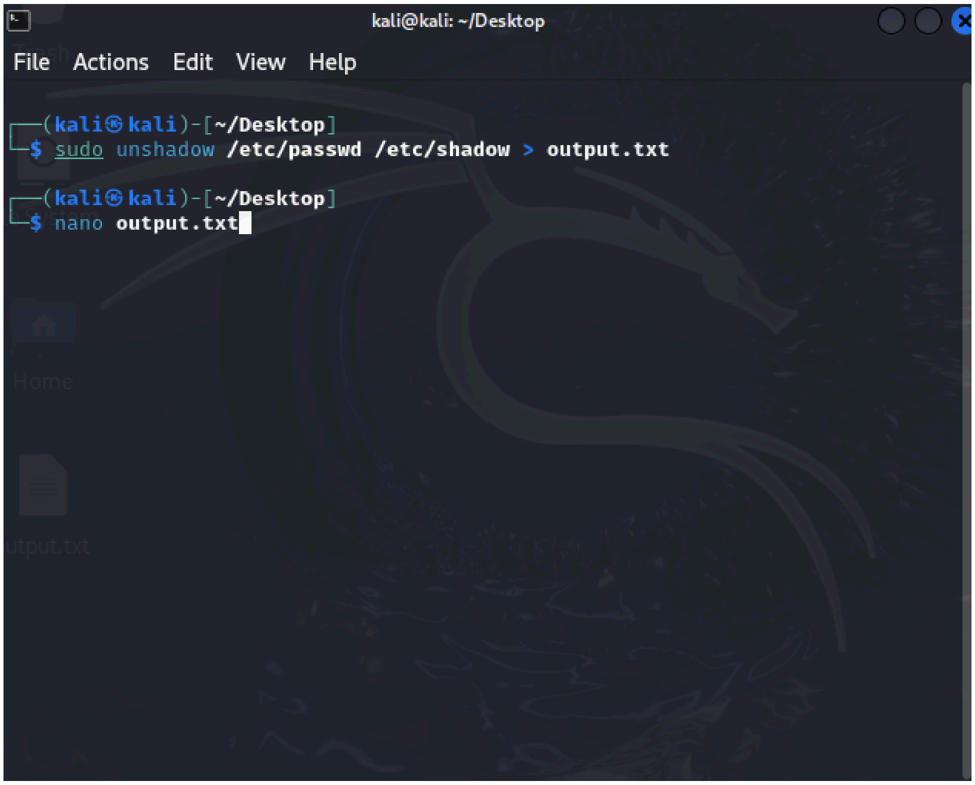
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo unshadow /etc/passwd /etc/shadow > output.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Enter your sudo password when prompted.

Step 2: Edit the Hash File

1. Open the Hash File:
   - View the contents of the `output.txt` file to locate the password hash for the Kali user

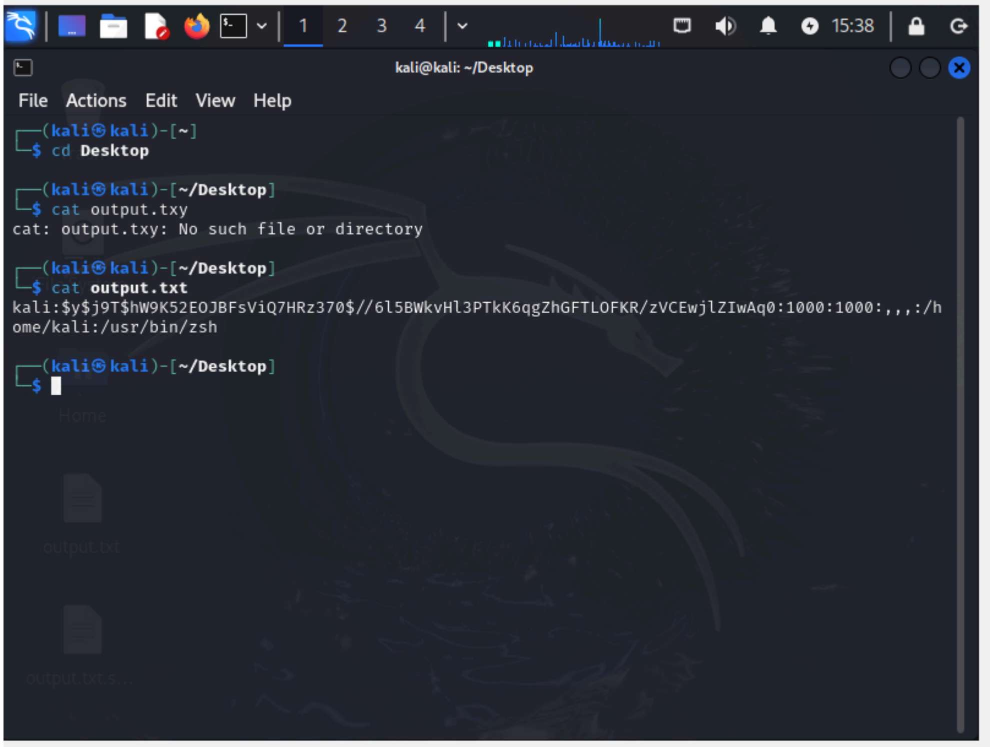
nano output.txt



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo unshadow /etc/passwd /etc/shadow > output.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ nano output.txt
```

Remove all entries except for the one corresponding to the Kali user, which should include a username followed by an encrypted password.

1. Save and Close the File:
   - Press `Ctrl+X` to exit, press `Y` to save changes, and then `Enter` to confirm.

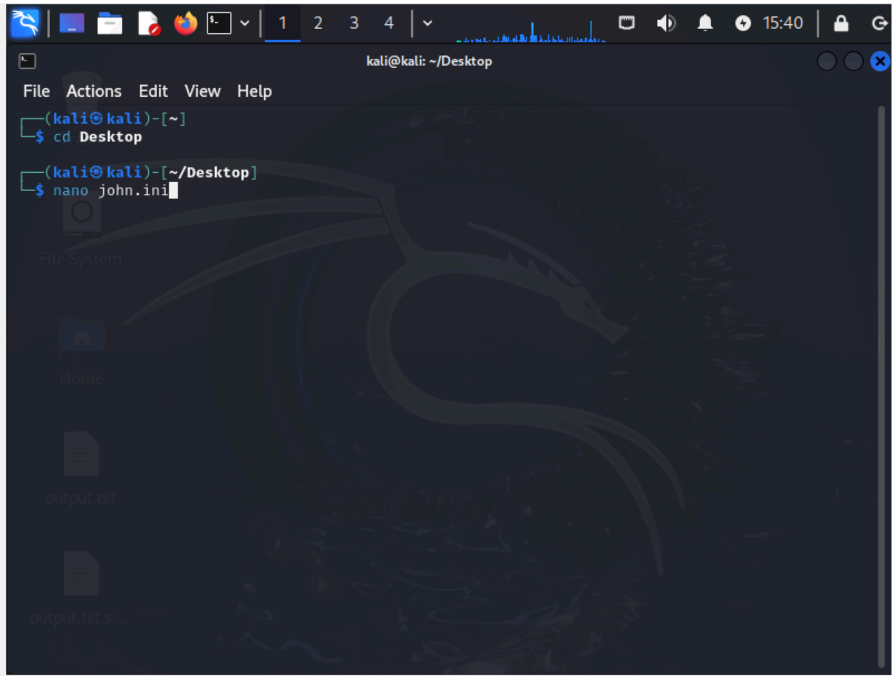


```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ cat output.txy
cat: output.txy: No such file or directory

┌──(kali㉿kali)-[~/Desktop]
└─$ cat output.txt
kali:$y$j9T$hW9K52EOJBFsViQ7HRz370$//6l5BWkvHl3PTkK6qgZhGFTLOFKR/zVCEwjlZIwAq0:1000:1000:,,,:/h
ome/kali:/usr/bin/zsh

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

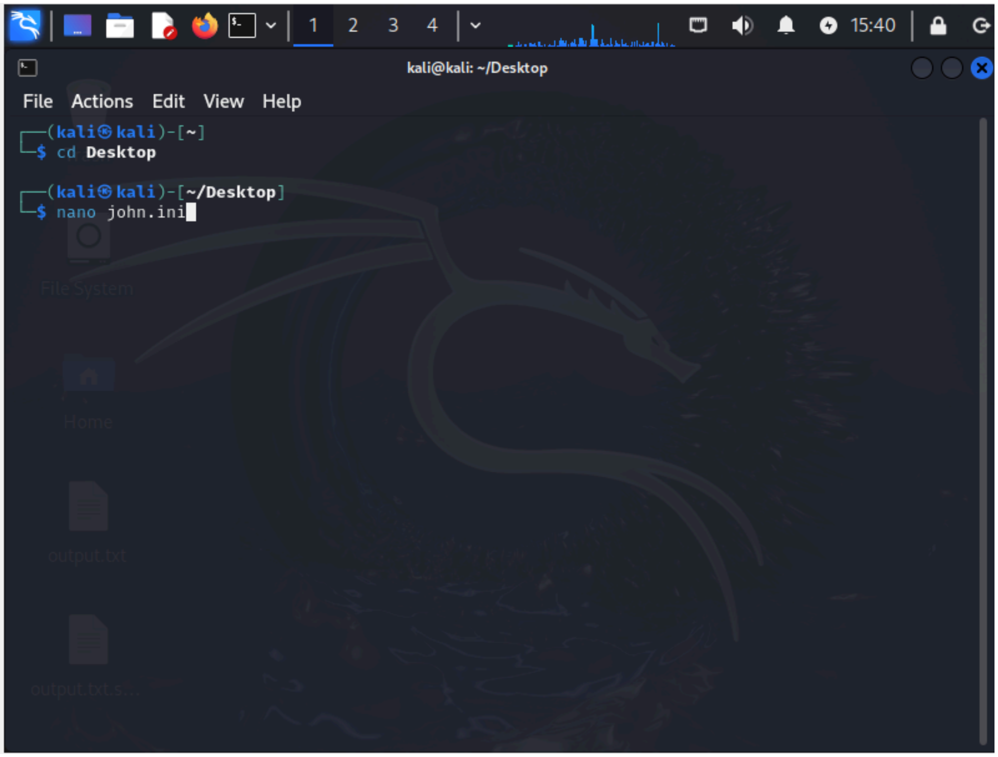
Step 3: Configure John the Ripper

1. Create a Custom John the Ripper Configuration File:
   - Open a new configuration file named `john.ini`:

     nano john.ini



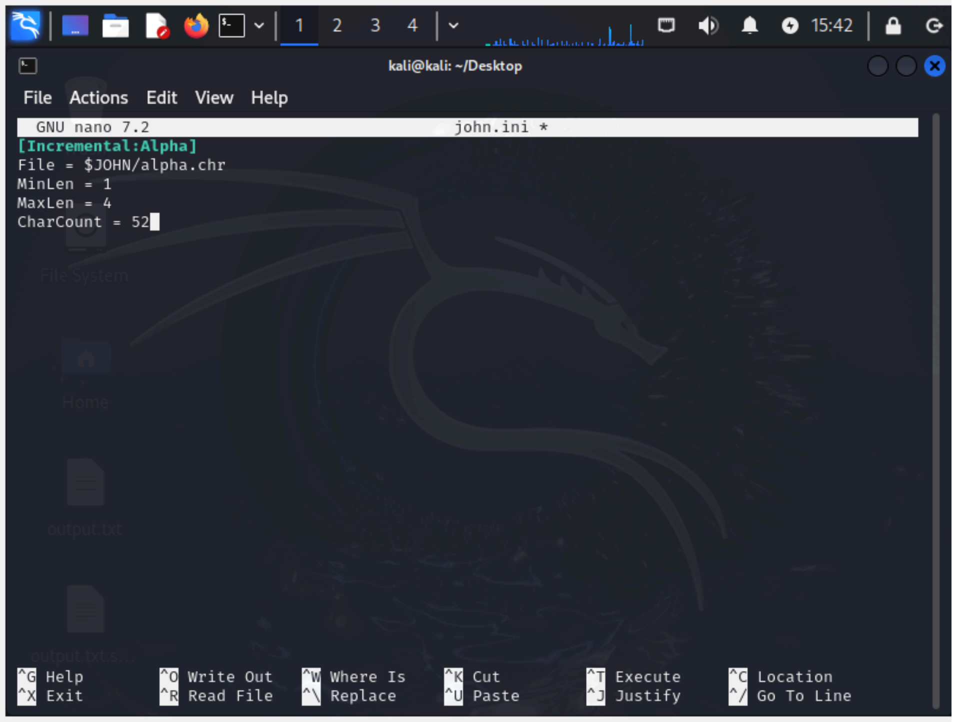
```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ nano john.ini
```



```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ nano john.ini
```

Configure the file for a brute force attack with specific parameters:

```
[Incremental:Alpha]
File = $JOHN/alpha.chr
MinLen = 1
MaxLen = 4
CharCount = 52
```



```
  GNU nano 7.2                           john.ini *
[Incremental:Alpha]
File = $JOHN/alpha.chr
MinLen = 1
MaxLen = 4
CharCount = 52
```

This configuration sets the attack to only use alphabetic characters and limits the password length to 4 characters for a quick demonstration.

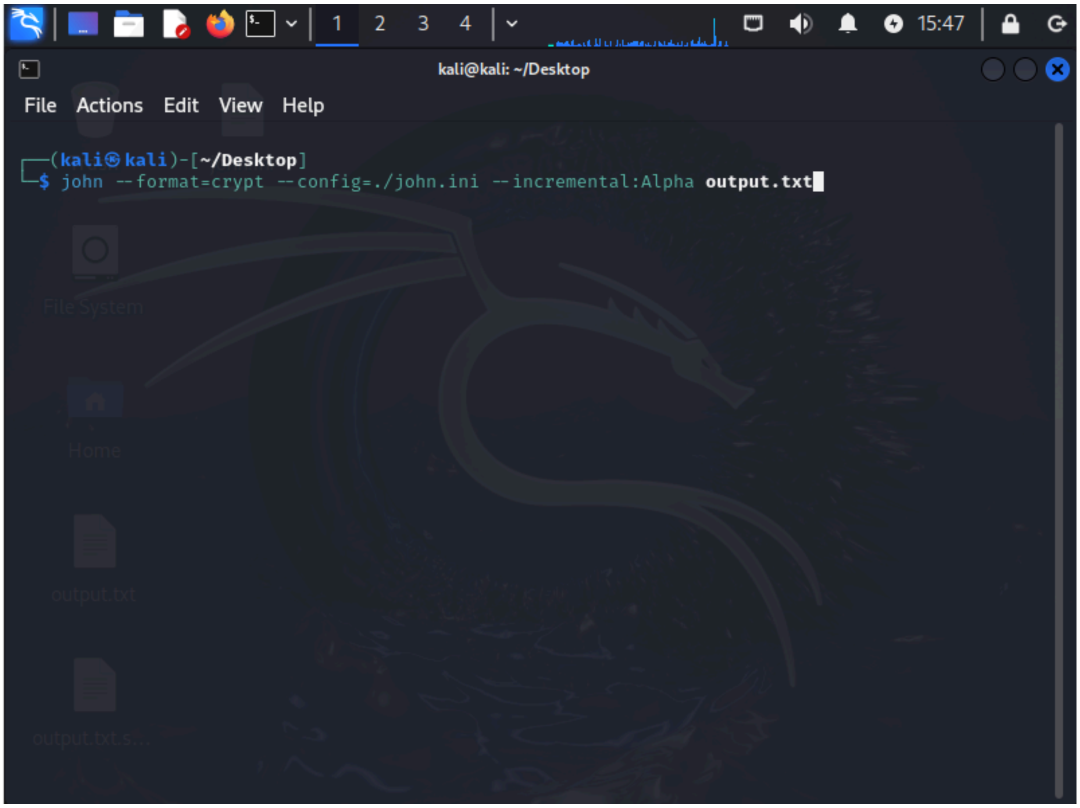
2. Save and Close the Configuration File:
   - Press `Ctrl+X`, then `Y` to save, and `Enter` to confirm.

2.

Step 4: Run the Brute Force Attack

1. Execute John the Ripper:
   - Start the brute force attack using the custom configuration

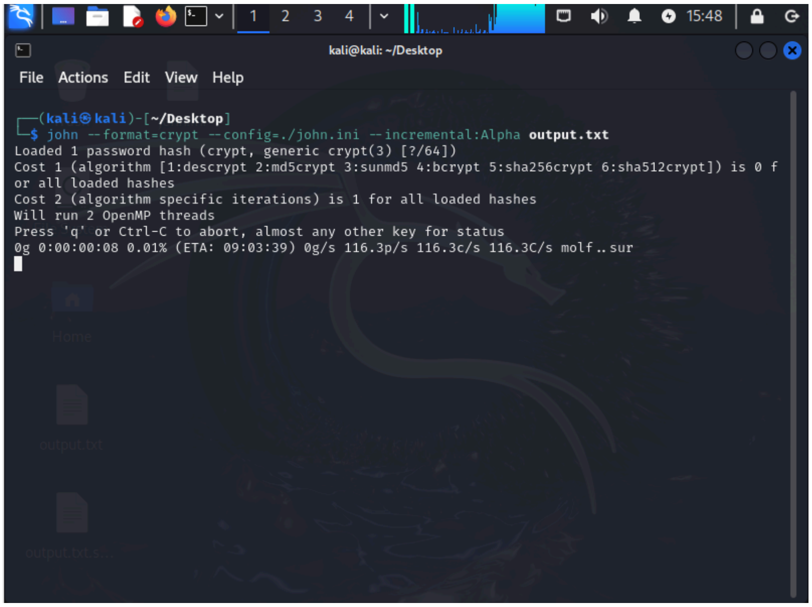
```
john --format=crypt --config=./john.ini --incremental:Alpha output.txt
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=crypt --config=./john.ini --incremental:Alpha output.txt
```

John the Ripper will now attempt to crack the password, iterating through possible combinations based on the settings defined in `john.ini`.

2. Monitor the Progress:
   - Press `Enter` periodically to see the current status and attempts of the password cracking process.

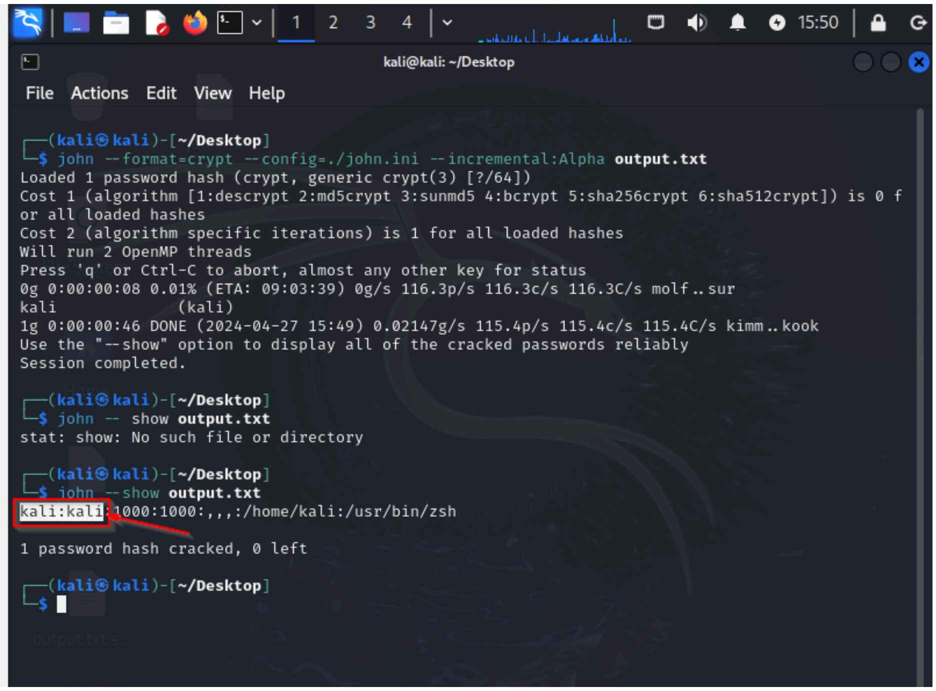


```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=crypt --config=./john.ini --incremental:Alpha output.txt
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 f
or all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:08 0.01% (ETA: 09:03:39) 0g/s 116.3p/s 116.3c/s 116.3C/s molf..sur
```

Step 5: Retrieve the Cracked Password

1. View the Results:
    - Once John completes the cracking process, view the cracked password

john --show output.txt



```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=crypt --config=./john.ini --incremental:Alpha output.txt
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 f
or all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:08 0.01% (ETA: 09:03:39) 0g/s 116.3p/s 116.3c/s 116.3C/s molf..sur
kali             (kali)
1g 0:00:00:46 DONE (2024-04-27 15:49) 0.02147g/s 115.4p/s 115.4c/s 115.4C/s kimm..kook
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$ john -- show output.txt
stat: show: No such file or directory

┌──(kali㉿kali)-[~/Desktop]
└─$ john --show output.txt
kali:kali:1000:1000:,,,:/home/kali:/usr/bin/zsh

1 password hash cracked, 0 left

┌──(kali㉿kali)-[~/Desktop]
└─$
```

The output will display the username and the cracked password.

Conclusion

This guide demonstrates a practical example of setting up and running a brute force password attack using John the Ripper on Kali Linux, highlighting the process of preparing password hashes, configuring the attack parameters, and executing the attack to crack a simple password efficiently. This method illustrates both the potential vulnerabilities in weak passwords and the importance of using complex, secure passwords to protect user accounts.