Task 4: The Key Under the Mat - Basic Password Cracking

Name :- Rushikesh Sanjay Kumavat

INTERN ID:- SN1000726

DOMAIN:- Cyber Security

Aim :-

To understand password security by cracking a hashed password using John the Ripper and a dictionary attack.

OBJECTIVE :-

- Generate a password hash
- Store it in a file
- Use John the Ripper with rockyou wordlist
- Crack the password
- Analyze the weakness of weak passwords

Tools Used :-

- Kali Linux
- Metasploitable 2
- John the Ripper

Procedure :-

Step 1: Generate Password Hash

Command used:

➔ openssl passwd -1 password123

Output:

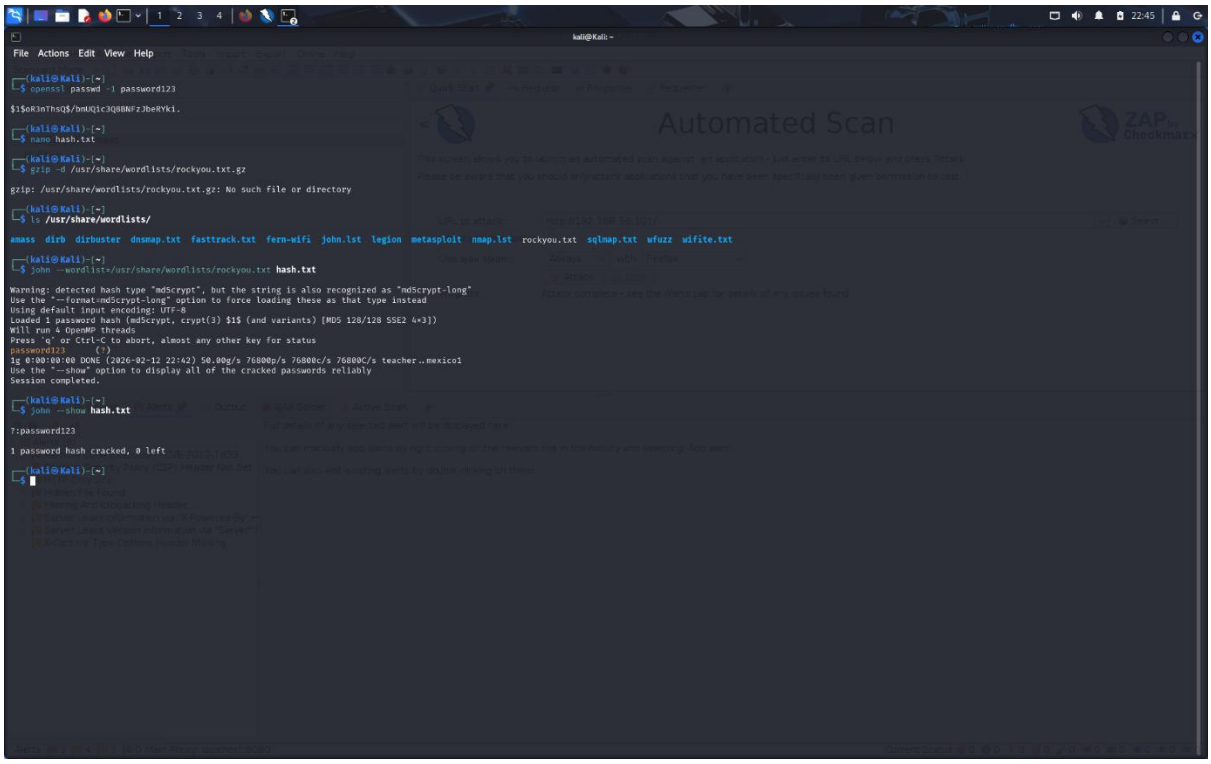
➔ 1oR3nThsQ$/bmUQic3Q8BNFzJbeRYki.

Step 2: Save Hash in File

Command:

➔ nano hash.txt

Paste the hash and save.



Step 3: Verify Wordlist Location

Command:

➔ ls /usr/share/wordlists/

Confirmed:

➔ rockyou.txt

Step 4: Perform Dictionary Attack

Command:

➔ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

John loaded hash type:

➔ md5crypt

Password Cracked:

➔ password123

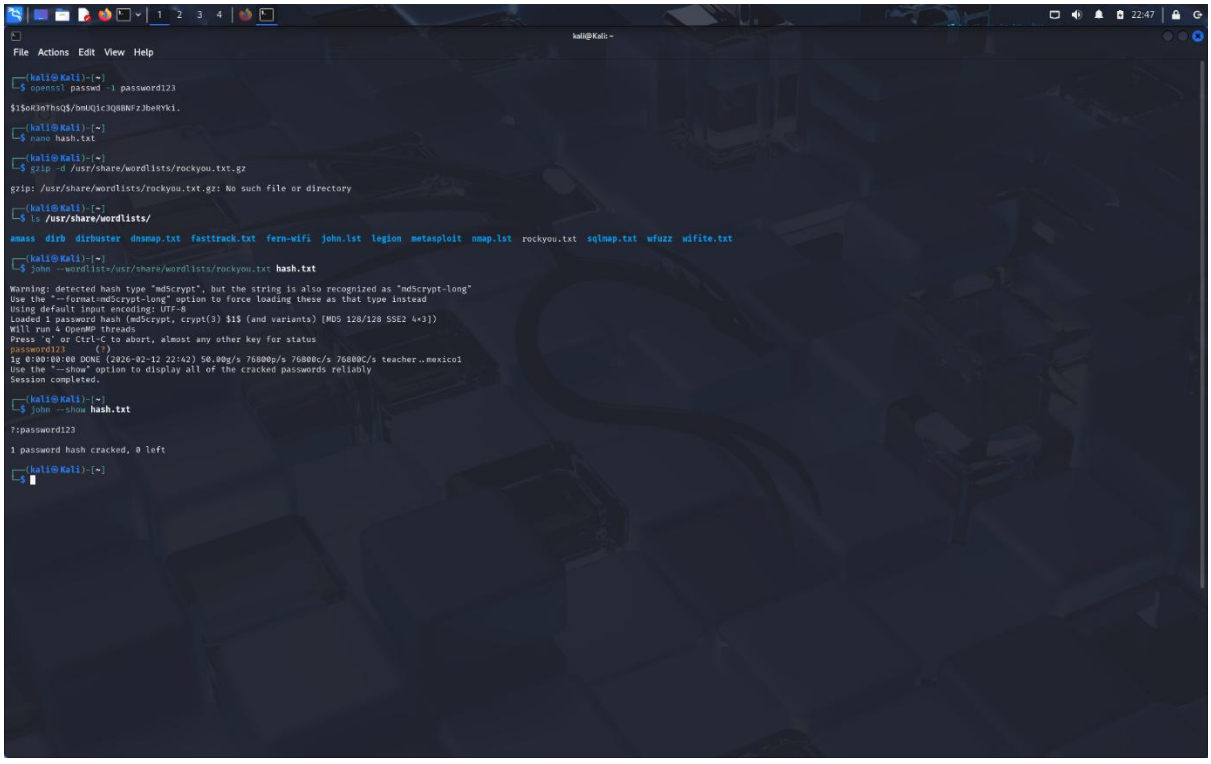
Step 5: Display Cracked Password

Command:

➔ john --show hash.txt

Output:

➔ password123



RESULT :-

The password hash was successfully cracked using a dictionary attack.
The original password was:

➔ password123

CONCLUSION :-

This task demonstrates:

- Weak passwords can be cracked quickly
- Dictionary attacks are very effective
- Proper password policies are necessary
- Hashing alone is not enough without strong passwords