**Password Cracking and Hardening (Report)**

**Project Title**: - Password Cracking and Hardening: Analyzing Security Vulnerabilities

**Objective**: - The objective of this project was to investigate the vulnerabilities associated with weak passwords and to implement password cracking techniques using industry-standard tools. By understanding the effectiveness of these methods, I aimed to underscore the importance of robust password policies in enhancing cybersecurity.

**Environment**

Operating System: Kali Linux

Virtualization Software: Oracle VirtualBox

RAM: 2GB

**Tools and Resources**

John the Ripper: An open-source password cracking software used for testing password strength.

Wordlist: rockyou.txt, a widely recognized password list containing common weak passwords.

OpenSSL: Used for generating password hashes.

**Methodology**

**Step 1**: Generate Password Hashes

I created multiple password hashes (MD5, SHA-1, SHA-256) to establish a dataset for testing:

echo -n "password" | openssl dgst -md5 >> md5hash.txt

echo -n "password" | openssl dgst -sha1 >> sha1hash.txt

echo -n "password" | openssl dgst -sha256 >> sha256hash.txt

**Step 2**: Prepare the Wordlist

To ensure a diverse range of passwords for testing, I downloaded the rockyou.txt wordlist:

wget <https://github.com/graphicore/rockyou.txt/releases/download/2020-12-21/rockyou.txt.gz>

gunzip rockyou.txt.gz

**Step 3**: Crack Passwords Using John the Ripper

I utilized John the Ripper to crack the generated hashes:

john --wordlist=~/rockyou.txt md5hash.txt

john --wordlist=~/rockyou.txt sha1hash.txt

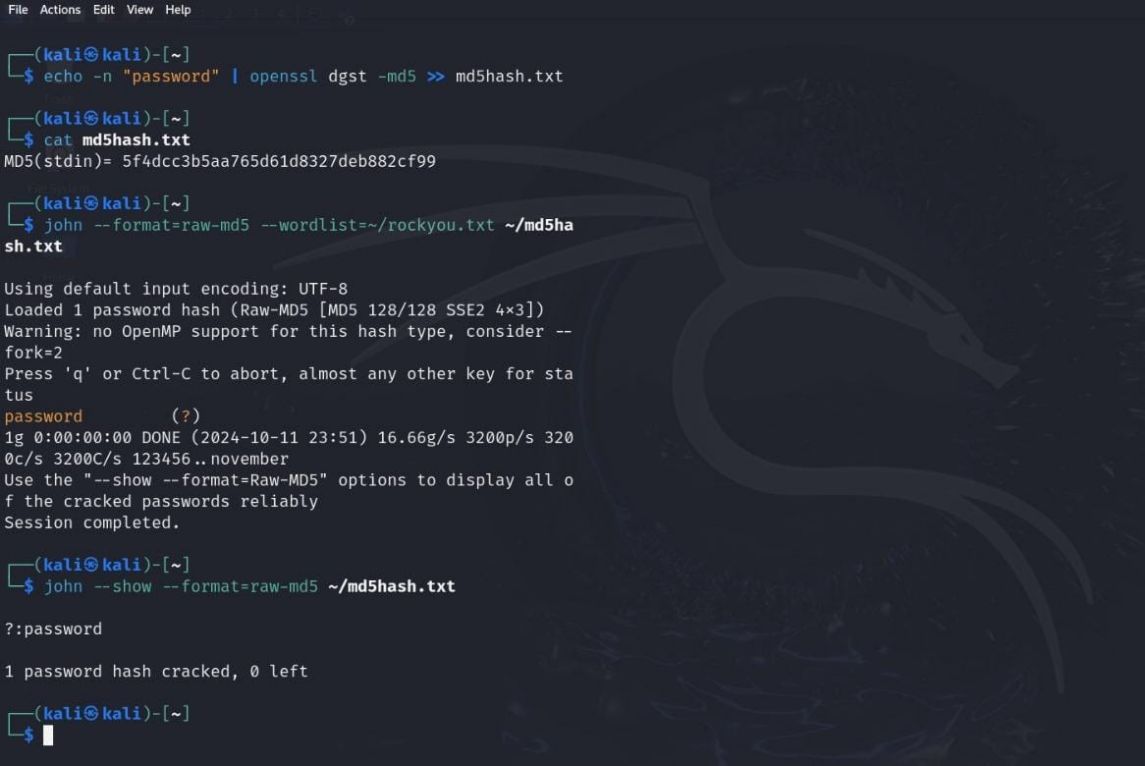
john --wordlist=~/rockyou.txt sha256hash.txt

After the cracking process, I displayed the results:

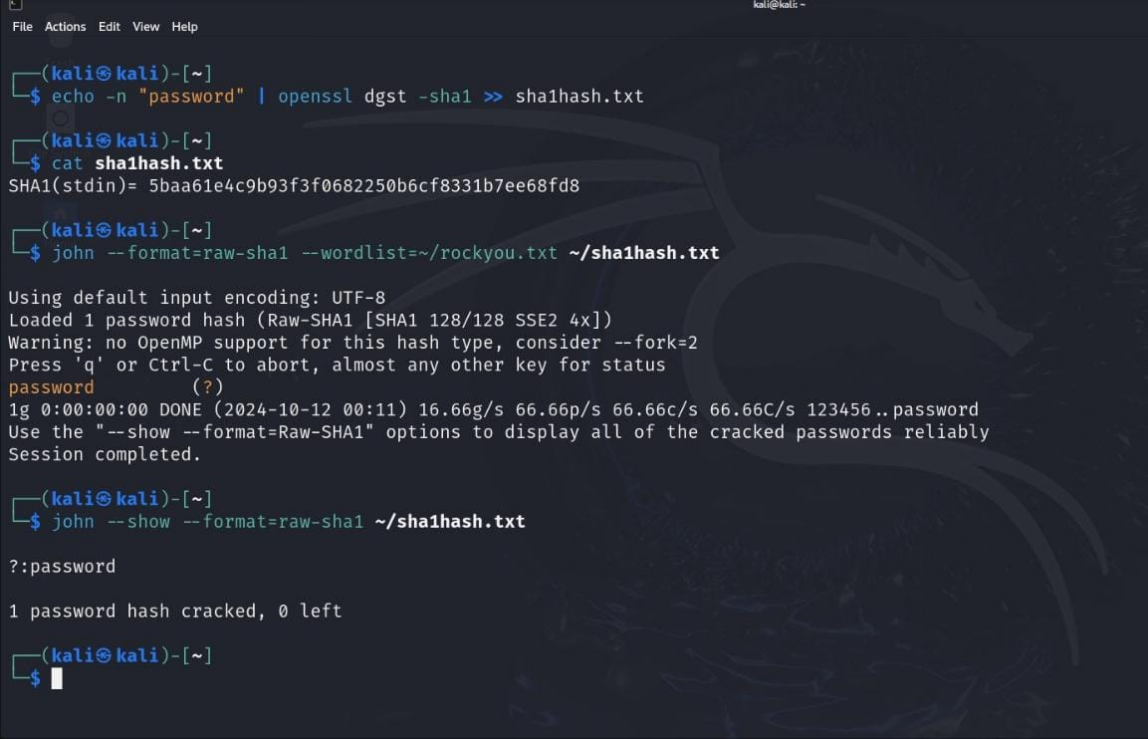
john --show md5hash.txt

john --show sha1hash.txt

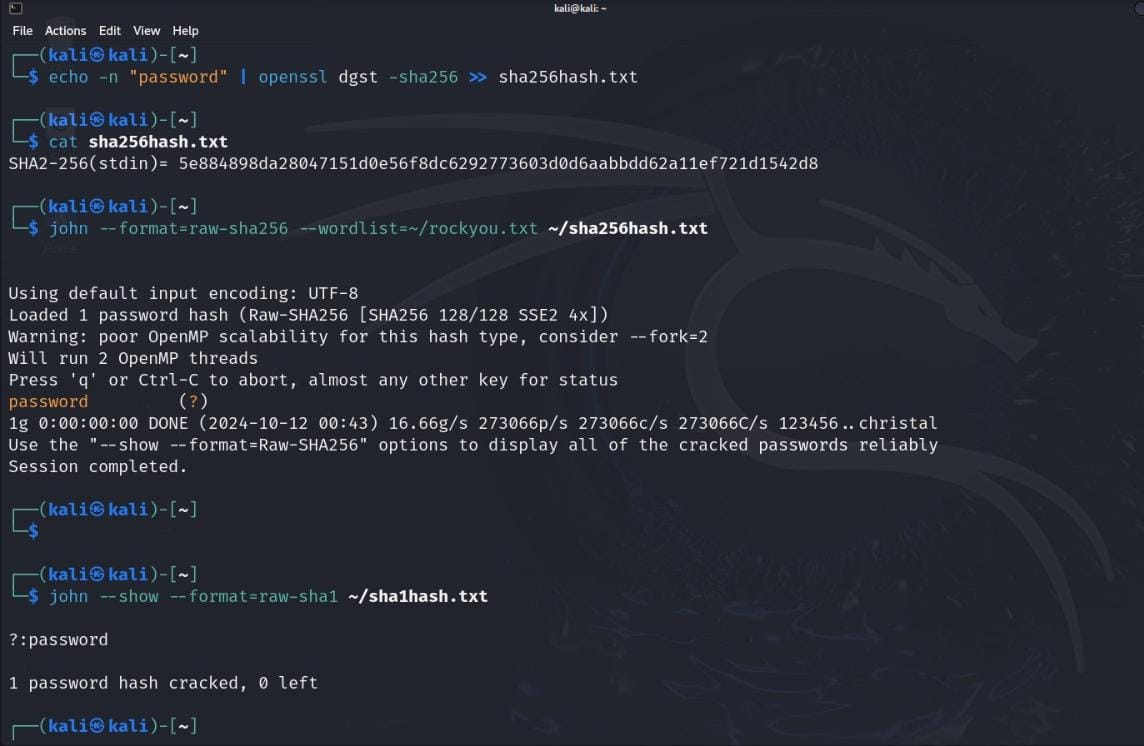
john --show sha256hash.txt



**MD5**



**SHA1**



**SHA256**

**Step 4:** Document Findings

I documented the cracked password and analyzed the effectiveness and speed.

John the Ripper: Quickly cracked the hashes with ease.

**Results**

The project successfully demonstrated the following:

Cracked Hashes:

MD5: password (5f4dcc3b5aa765d61d8327deb882cf99)

SHA-1 and SHA-256 hashes were also tested.

**Insights**: The results reinforced the risks associated with using weak passwords.

**Recommendations**

From the findings, I propose the following best practices for password security:

Adopt Stronger Passwords: Encourage the use of complex passwords with a minimum length of 12 characters, mixing letters, numbers, and special characters.

Educate Users: Implement user training to highlight common password pitfalls and the importance of unique passwords.

Multi-Factor Authentication: Organizations should employ MFA to enhance security beyond just passwords.

Regular Policy Updates: Periodic reviews and updates to password policies should be conducted to ensure ongoing effectiveness.

**Conclusion**

This project provided valuable insights into the vulnerabilities associated with weak passwords and demonstrated the effectiveness of password cracking tool like John the Ripper. By understanding these vulnerabilities, I can advocate for stronger password practices and contribute to enhancing cybersecurity measures.