Password cracking lab

Aim:

A hands-on lab to demonstrate password cracking using John the Ripper, Hashcat, and rockyou.txt wordlist to understand how attackers exploit weak passwords.

Procedure:

- We create hashes using SHA-512 with OpenSSL.
- Crack the hashes using both John the Ripper and Hashcat.
- Use the famous rockyou.txt dictionary to crack the hashes.
- Validate GPU support with hashcat -I.
- Compare tools based on performance and flexibility.

Execution:

→ Create Hashed Passwords Using SHA-512:

simulate how passwords are stored by creating hashed values using OpenSSL.

```
echo -n "password123" | openssl passwd -6 -stdin
```

```
$6$randomsalt$k9yuexWlD1aZ9ROZjmGHW3...etc
```

```
echo -n "qwerty" | openssl passwd -6 -stdin
```

Repeat this for any number of passwords you want to crack.

→ Save the derived hashes to a file:

```
nano hashes.txt
```

Paste your generated hashes one per line, for example:

```
$6$xyz123$CtAvmQH1WBQX84Z8B9uZj2W5Hgq...

$6$xyz123$Lqp7k9TLjYJRAFnvFjGgWiCqM…
```

Save with `Ctrl+O`, then exit with `Ctrl+X`.

→ Unzip the famous Wordlist file for cracking

```
gunzip /usr/share/wordlists/rockyou.txt.gz
```

The default dictionary is compressed. First, unzip it, This will make it available for cracking.

→ Crack Passwords with John the Ripper

Run John the Ripper with the wordlist and the hashes:

```
john --wordlist=/usr/share/wordlists/pass.txt hashes.txt
```

To verify cracked passwords after processing:

```
john --show hashes.txt
```

Note: John uses CPU only and is effective for many Unix-style password formats.

→ Crack Passwords with Hashcat:

First, ensure the hash type is correct. For SHA-512 crypt, Hashcat uses mode 1800.

```
hashcat -m 1800 -a 0 -o cracked.txt hashes.txt /usr/share/wordlists/rockyou.txt
```

```
cat cracked.txt
```

```
$6$xyz123$hashvalue:password123
```

→ Identify Hash Type:

```
hashid [your_hash]
```

This will try to identify the algorithm (e.g., SHA-512 Crypt, MD5, etc.).

→ Specify Format in John:

Sometimes John doesn’t auto-detect format. Force it like this:

```
john --format=sha512crypt hashes.txt
```

Use this when dealing with SHA-512 hashes from Linux shadow files.

→ Check GPU Support in Hashcat

Check if your system and GPU support Hashcat cracking:

```
hashcat -I

Platform ID #1

  Name: NVIDIA GeForce GTX 1650

  Version: OpenCL 1.2 CUDA
```

“Using a GPU dramatically improves performance with Hashcat.”

→ Comparison of John vs Hashcat

Feature	John the Ripper	Hashcat
Usage	CPU only	GPU supported
Cracking Speed	Medium	Very Fast
Hashing Support	Broad	Very Broad
Format Detection	Automatic + Manual	Manual preferred
Ideal	Password Auditing, Unix	Large-scale hash cracking