■ Password Cracking Demo

Using John the Ripper on Kali Linux

Cybersecurity Class

Objectives

- Understand what password hashes are.
- See how weak passwords are cracked.
- Compare MD5 and SHA-1 cracking.
- Discuss defenses against password cracking.

What is a Hash?

• A one-way function that converts data into a fixed-length string.
• Used to store passwords securely.
• Example (MD5 of 'password'): 5f4dcc3b5aa765d61d8327deb882cf99

Why Crack Passwords?

- To test password strength.
- To understand attacker techniques.
- To highlight why strong passwords + salts are needed.

Tools We Use

- John the Ripper (installed by default in Kali).
- Wordlists (e.g., rockyou.txt, class_wordlist.txt).
- MD5 and SHA-1 hashes prepared for this demo.

Demo: Crack MD5 Hashes

1. Run dictionary attack:

```
john --format=raw-MD5 --wordlist=class_wordlist.txt md5_hashes.txt
```

2. Show cracked passwords:

```
john --show --format=raw-MD5 md5_hashes.txt
```

Demo: Crack SHA-1 Hashes

1. Run dictionary attack:

```
john --format=raw-SHA1 --wordlist=class_wordlist.txt sha1_hashes.txt
```

2. Show cracked passwords:

```
john --show --format=raw-SHA1 sha1_hashes.txt
```

Smarter Cracking with Rules

Try mutating dictionary words:

```
john --format=raw-MD5 --wordlist=class_wordlist.txt --rules=Single
md5_hashes.txt
```

Defenses Against Cracking

- Use long, unique passwords.
- Hash with a salt to prevent rainbow tables.
- Use slow hashing algorithms (bcrypt, Argon2).

- Enforce MFA and account lockouts.

■■ Ethics Reminder

- Only crack hashes you own or have permission to test.
- Demo data in this class is safe to use.
- Unauthorized cracking is illegal and unethical.