Workshop

Dictionary Attacks

Each of these are hashed using a different algorithm, determine the type of hash from the Hashcat Wiki and use a wordlist (eg rockyou) to crack the password.

Practice hashes to crack:

```
edba955d0ea15fdef4f61726ef97e5af507430c0

742929dcb631403d7c1c1efad2ca2700

sha256:600000:WW5SZ2puaW0=:yVQajGrUC8Bkl5vERgJQQf+smvL3YnJpcdiig

$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12

$2y$10$vcrYth5YcCLlZaPDj6PwqOYTw68W1.3WeKlBn70JonsdW/MhFYK4C

b8fd3f41a541a435857a8f3e751cc3a91c174362:d
```

Custom Wordlist Scenarios

1. Employees are allocated a default password which adheres to the following pattern:

   Their first name and last name (first letter of each capitalized), followed by an exclamation point and a randomly generated 4 digit number at the end.
   Example:

   ```
   FirstnameLastname!8008
   ```

You discover a new employee by the name ‘Floyd Wallis’, create a custom wordlist to crack the password:

```
46a326c63dc32b83653e1963486a8bf710b09e60b535f3f02b1b2f19be17(
```

The Floyd Wallis Challenge:

format1: FirstnameLastname[digit][digit][digit][special char]

```
cdd25832c4c7b5ba1f5bd6c9897bbaafc4078f8fca2f0751e2892325ffa68
```

format2: [digit][digit]Firstname[special char]Lastname[digit][digit]

```
b4a77a1dba8e5c7c60e58e64951c0761a9c28f2f
```

Format2: LastnameStudentnumber[digit][special char][digit][special char]

```
b251f42ab5b2040f9f6adf5e8c02deaf67060bf232aba0ef1d2636c0a5cb1
```

2. You are creating a custom wordlist for a man by the name ‘Lars Berghorst’ (a totally fictional and hypothetical character). Some of his interests include:

```
Football (supports Dortmund)
History student (enjoys the crusades)
Map Games
Politics
Mayonnaise
Raw milk
Lives in the Allendale region of the Pennines
Cats
German/ Dutch nationalism
Snus
```

Password must include at least 1 capital letter and 1 special character.

Please email us the lists when completed <3.

```
0a85ee853211b8d9f58bedea202b9ab0
```

This is an AI generated image of what this individual may look like:

DVWA Brute-Force Using HTTP-Get requests

https://medium.com/@hamidullahbayram/using-hydra-on-login-pages-with-a-right-method-dvwa-training-1e85e8d4f5fd

Extra (try at your own risk) :3

Using Burpsuite for Brute Forcing

https://medium.com/@aayanx41/dvwa-brute-force-c2901f630c3d