Password Cracking

By: Isaac

How do hackers get your password?

1. Large lists of passwords are leaked from hacked organizations
2. Passwords are not in plaintext/English but in random gibberish
3. Hackers need to revert the passwords back to plaintext

How does password cracking work?

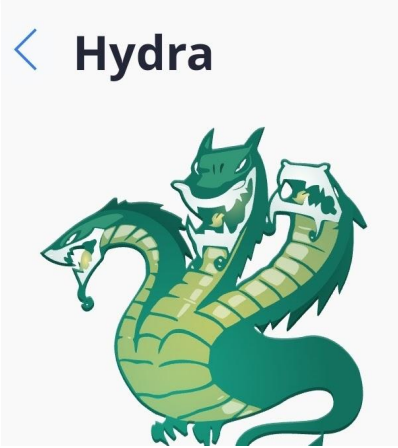
1. Figure out password characteristics(password length, letters or numbers, special characters)
2. Perform brute force attack based on password characteristics

Password leaks

1. Leaked passwords from organizations are usually encrypted with something called a hash
2. Hash types include:
    a. MD5
    b. SHA-1
    c. SHA-2
    d. MD5
3. If you know the hash type, you can crack the password!

Password cracking libraries

- Hydra
- John the Ripper
- hashcat
- Rainbowcrack



Time to crack passwords!

1. Figure out hash type
2. Use online password cracking websites to crack the password!

Challenge:

Two encrypted passwords have been recovered from a leaked password list. Decode the password and find the real value!

Password #1: 6c44e5cd17f0019c64b042e4a745412a

Password #2: def7de584a38613baf9925b263963a788b1acd62

Reflection

- Hashes cannot be “decrypted” because they are intended to be one-way only
- Hashes can only be cracked by matching it up with online databases
- Databases are made of password leak lists including the rockyou password list

Thank you for coming!

Next meeting will be next Monday!