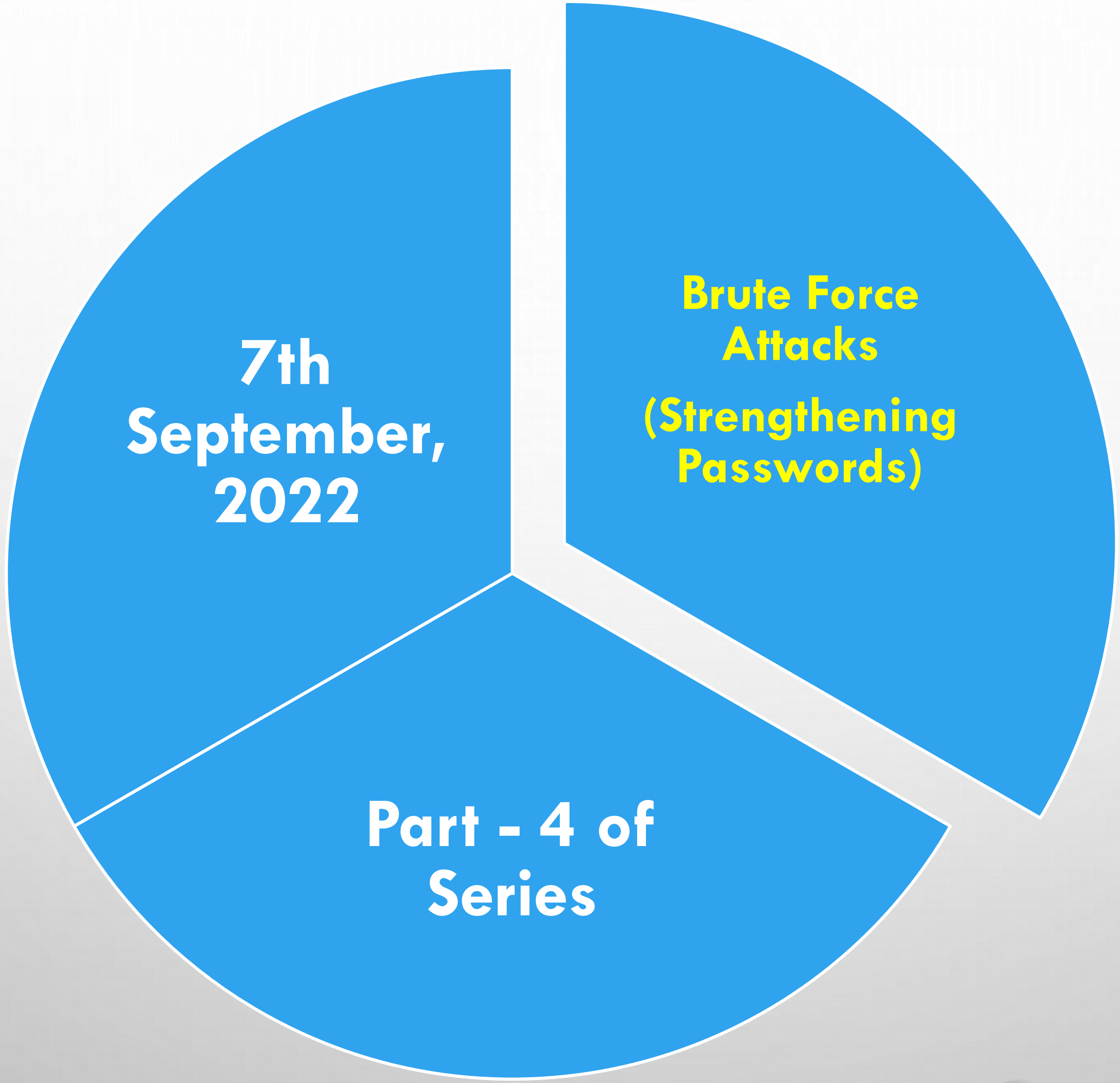
CELEBRATION OF CYBER JAAGROOKTA (AWARENESS) DIWAS (CJD)

(ON THE FIRST WEDNESDAY OF EVERY MONTH

COMMENCING APRIL,2022 ONWARDS)

Central Mine Planning & Design Institute Ltd.
RANCHI



7th September, 2022

Brute Force Attacks

(Strengthening Passwords)

Part - 4 of Series

BRUTE FORCE ATTACKS

Know a Brute Force Attack

A trial-and-error method to guess login info, keys, or make an unauthorized access.

Simply put, the hackers try all possible combinations in order to guess correctly.

Since ‘brute force’ is used to try and gain entry to systems, the attacks are known as Brute Force Attacks.

Though it’s an old method, but it's still very effective primarily thriving on callousness of the users.

Depending on the complexity of the password, cracking it can take anywhere from just a few seconds to many years.

Types of Brute Force Attacks

There are various types of Brute Force Attacks like:

- Simple Brute Force Attacks
- Dictionary Attacks
- Hybrid Brute Force Attacks etc.

But, the most common is a simple brute force attack which uses automation and scripts to guess passwords. Typical brute force attacks make a large number of guesses every second.

Simple brute force attacks: Logical guess regarding credentials — usually through multiple guesses. Extremely simple passwords are more prone to this*.*

Dictionary attacks: Hackers use unabridged dictionaries and augment words with special characters and numerals.

Hybrid brute force attacks: A blend of outside tools along with logical guesses. May also mix dictionary and brute force attacks. Usually used to crack combo passwords that mix common words with other characters.

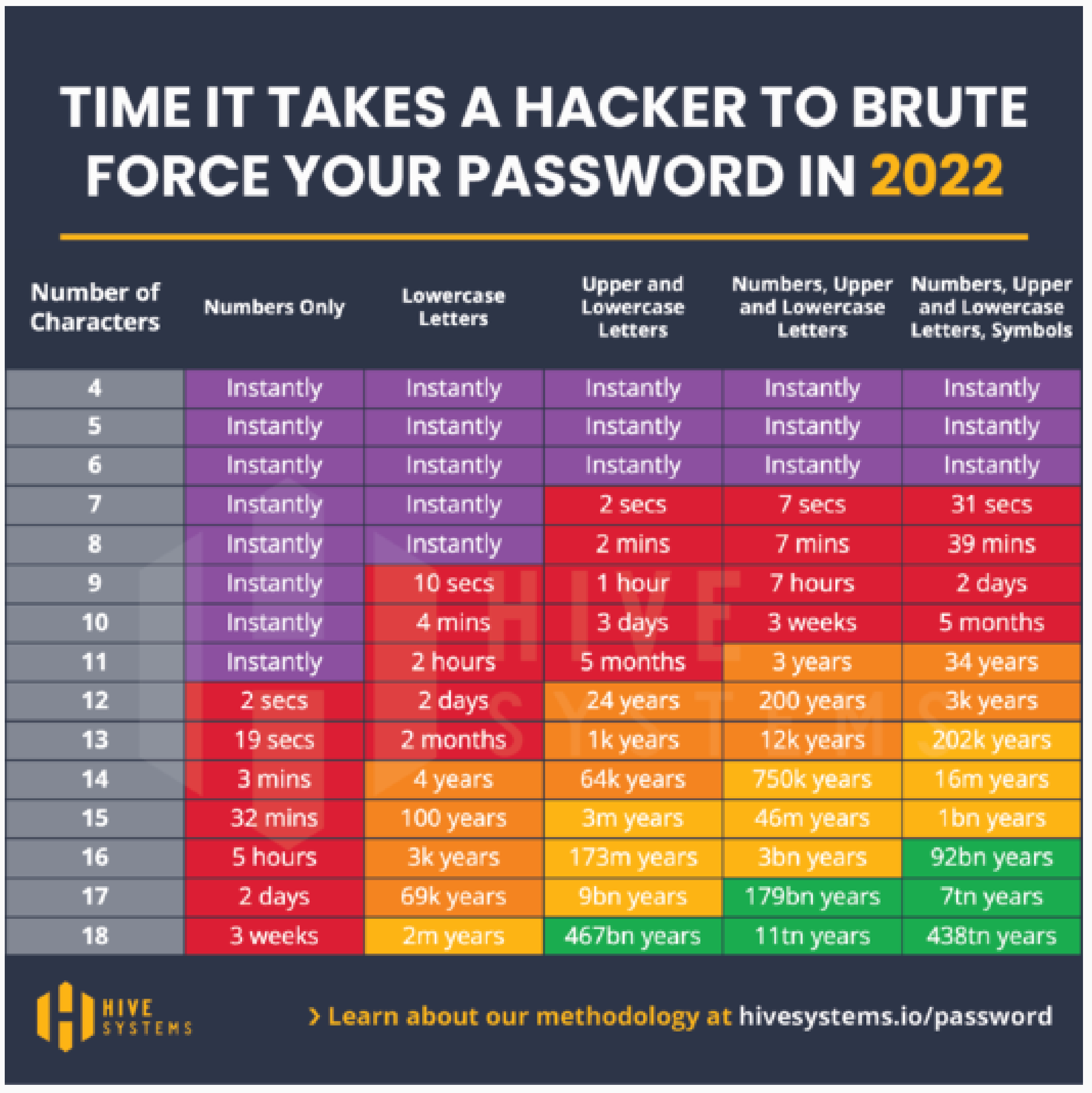
STRENGTHEN PASSWORDS AGAINST BRUTE FORCE ATTACKS

Strengthening Passwords Against Brute Force Attacks

As a user, one needs to appreciate the fact that the first and probably the best defence against brute force attacks is creating strong passwords.

Brute force attacks need time to crack credentials. So, if the hackers find out that it takes too long to crack credentials, they lose patience and drop the idea of cracking that device.

So, make sure that your password is not easy to crack in terms of time.



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

> Learn about our methodology at hivesystems.io/password

Therefore, to be practically safe as on date, your password needs to be of:

at least 11 characters with numbers, Upper and Lower case letters and symbols

You may note that in the year 2021, a password of 10 characters with numbers, Upper and Lower case letters and symbols was estimated to have taken **5 years** to get cracked with the available technology then.

The same would take **5 months** now in the year 2022.

A strong password is essential when it comes to your digital security, and you need a unique one for each of the various types of digital activities.

Weak passwords can most likely lead to data compromise. **Be Warned**.

Even though Brute Force Attacks are based on a very old technology, they continue to thrive because:

- they are relatively simple to perform
- the lack of preventive strategies for the targets

The journey continues...........