Task - 6

Principles of Password

Objective: Understand what makes a password strong and test it against password strength tools.

Tools: Online free password strength checkers

About:

What is a password:

A password is a secret string of characters used to verify a person’s identity and integrity for the system, it helps protect accounts, data , and systems from unauthorized access.

By keeping it private, only the rightful user can gain access without passwords , sensitive could be easily stolen or misused

What do attacker’s do

Most of the times the attackers or hacker try to brute-force the password to gain access to the data or Network

So, keeping a strong password is very much important for protecting Network or data and organizations.

Even a least privileged employ account also matters because , once the attacker gain access to network he can plan many attacks.

There are some rules for the password.

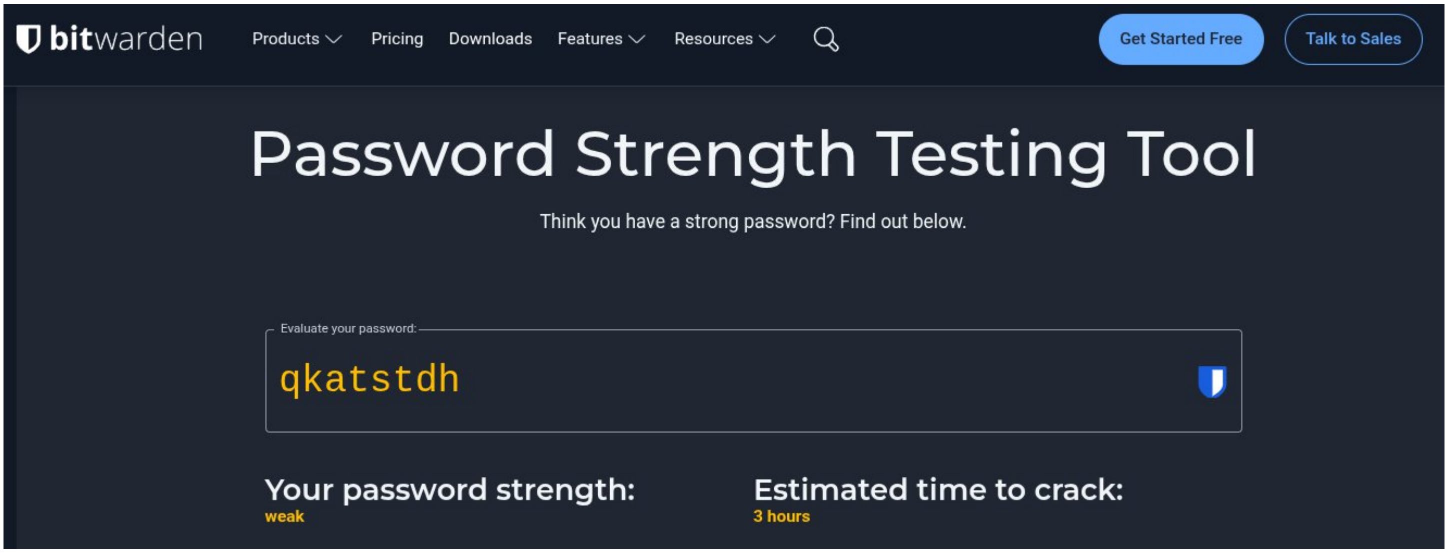
1. The length of the password must be more than 8 characters and recommend 10 characters
2. At least one special character
3. At least one number
4. Combination of uppercase and lowercase letters

Let us see why does these rule matters

Note: Hackers are not going to manually try each and every possibility , they use automated tools to crack passwords.

1. The length of the password must be more than 8 characters and recommend 10 characters

   See the Simple 8 characters password only lower case takes 3 hours



Password Strength Testing Tool

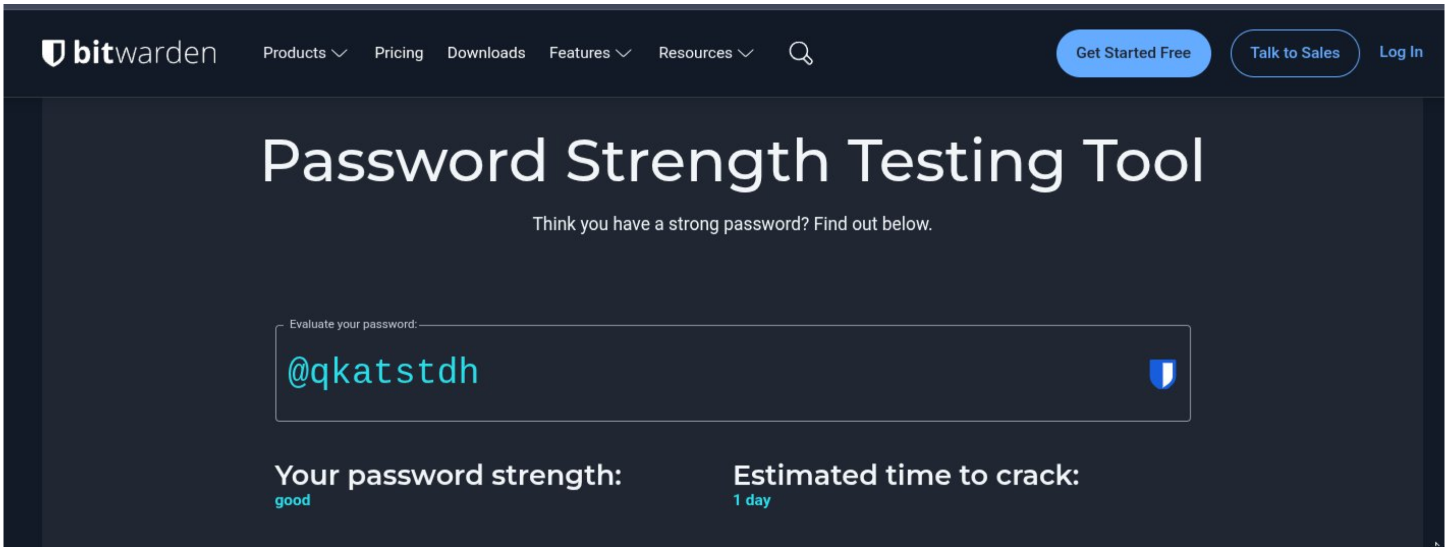
Think you have a strong password? Find out below.

Evaluate your password: qkatstdh

Your password strength: weak

Estimated time to crack: 3 hours

2. At least one special character, and include the first rule also



Password Strength Testing Tool

Think you have a strong password? Find out below.

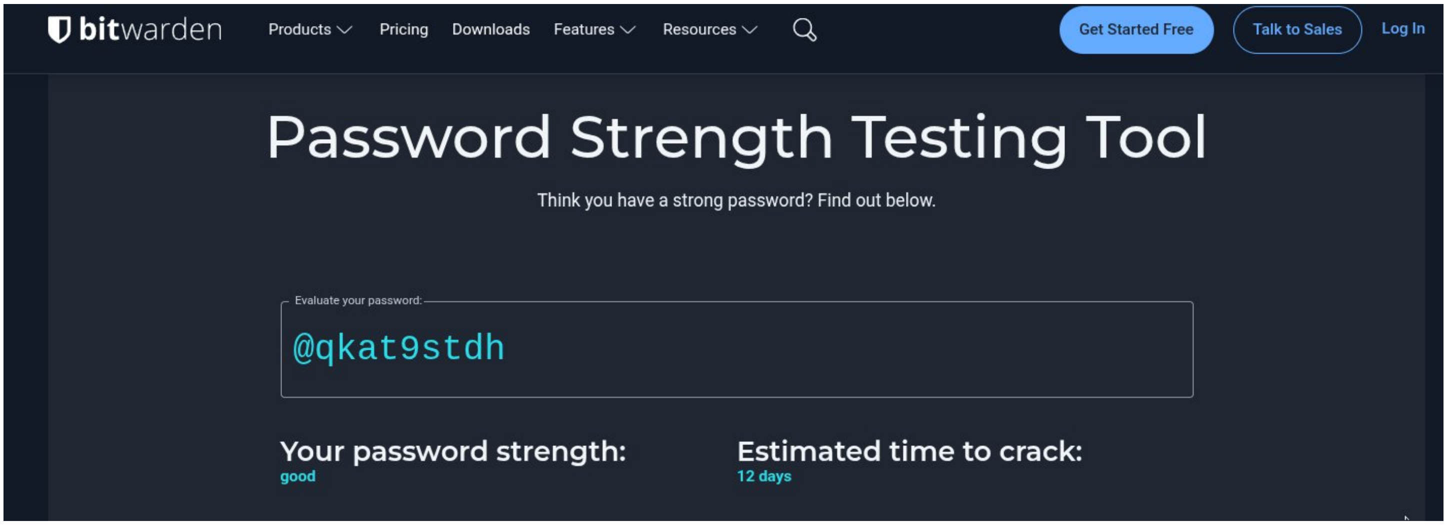
Evaluate your password: @qkatstdh

Your password strength: good

Estimated time to crack: 1 day

See we added just a ‘@’ symbol at starting , for a normal computer it takes 1 day to crack with brute-force attack.

3. Including rule 1 &2, now implement rule 3, at least one number



Password Strength Testing Tool

Think you have a strong password? Find out below.

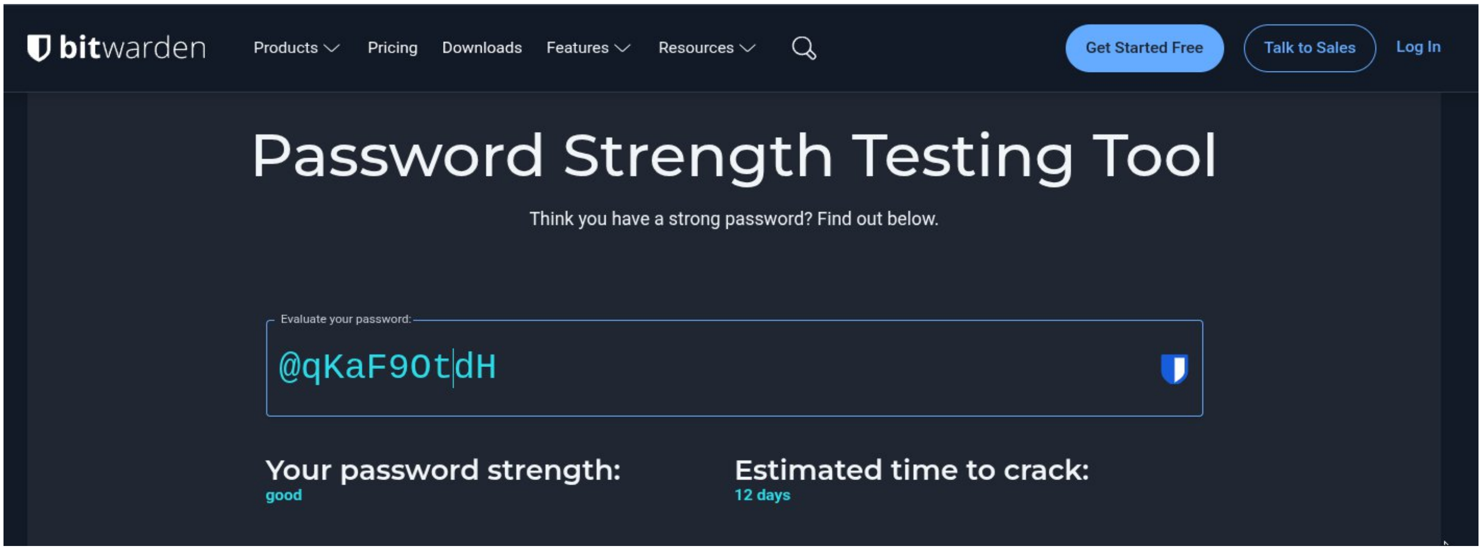
Evaluate your password: @qkat9stdh

Your password strength: good

Estimated time to crack: 12 days

By adding a number it takes 12 days to crack

4. Combination of uppercase and lowercase letters



Password Strength Testing Tool

Think you have a strong password? Find out below.

Evaluate your password: @qKaF90tdH

Your password strength: good

Estimated time to crack: 12 days

It also takes 12 days to crack

These rules are good but there are one more rule which specifically should not do

Note: In any password should not use data of birth, years, pet names, parents names, mobile numbers, vehical names, place or area names in the passwords

Ex:

Rocky@2010

Priya#1987

Bullet_5678

Delhi$2002

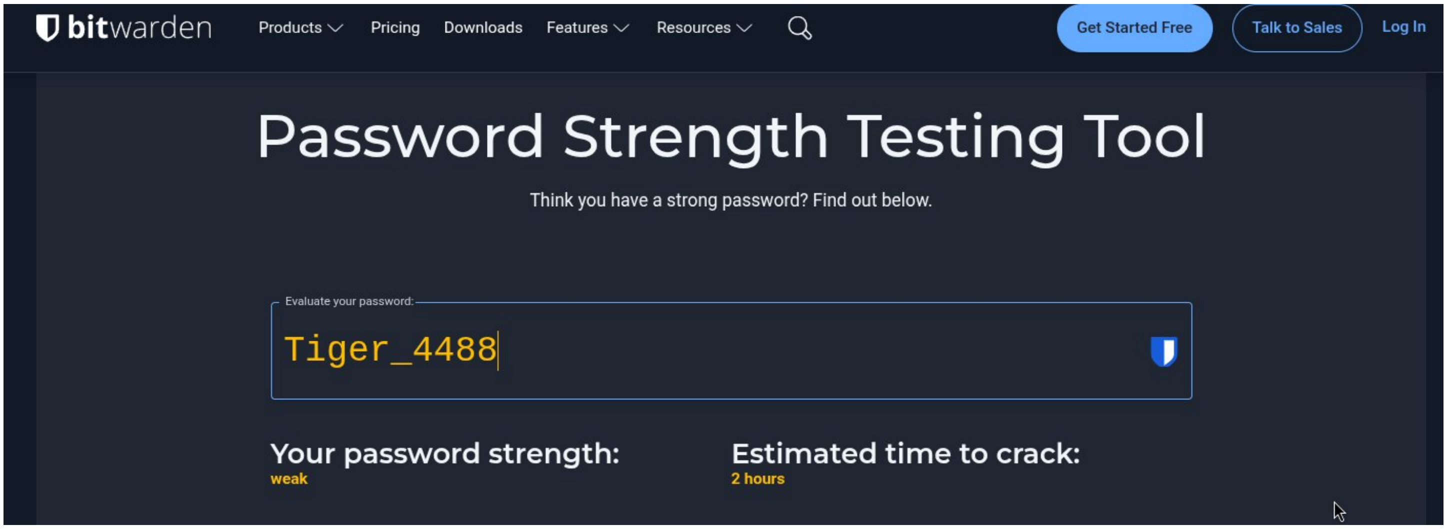
Shadow!9920

Honda#7865

Mumbai@1999

Tiger_4488

See the result of this password: Tiger_4488



Password Strength Testing Tool

Think you have a strong password? Find out below.

Evaluate your password:

Tiger_4488

Your password strength:
weak

Estimated time to crack:
2 hours

It follows all the rules numbers , special characters more than 8 , characters and uppercase and lower case letters

But it’s too easy to them to get these kind of details , and with one information you may leak other’s also

Summary:

Password complexity directly increases security by making guessing attacks much harder. Longer passwords exponentially raise the total possible combinations, slowing brute-force attacks. Including uppercase, lowercase, numbers, and special characters expands the character set, making each position harder to guess. Avoiding personal information prevents attackers from using social engineering or dictionary-based guesses, forcing them to attempt full-scale, time-consuming cracking methods.