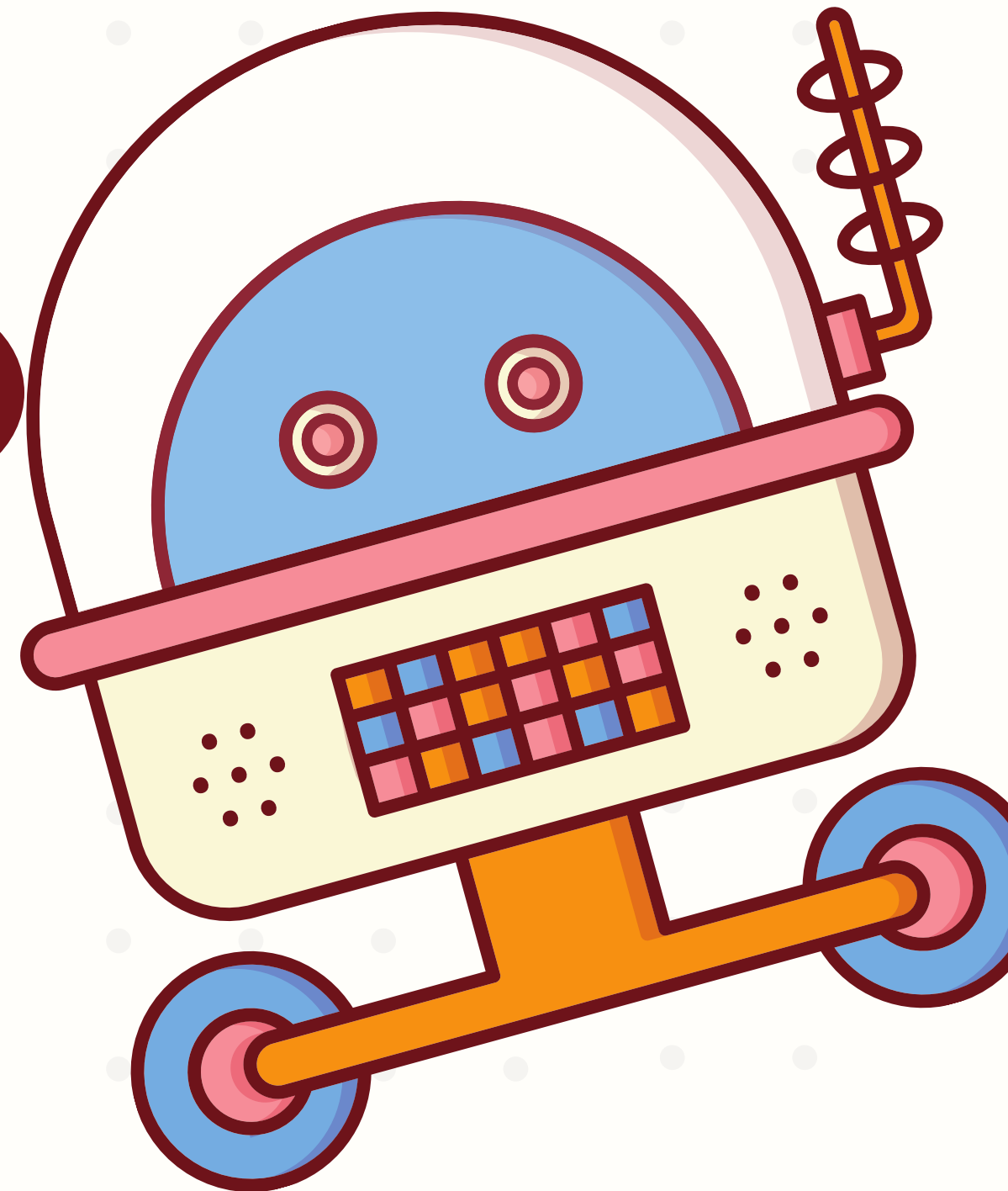
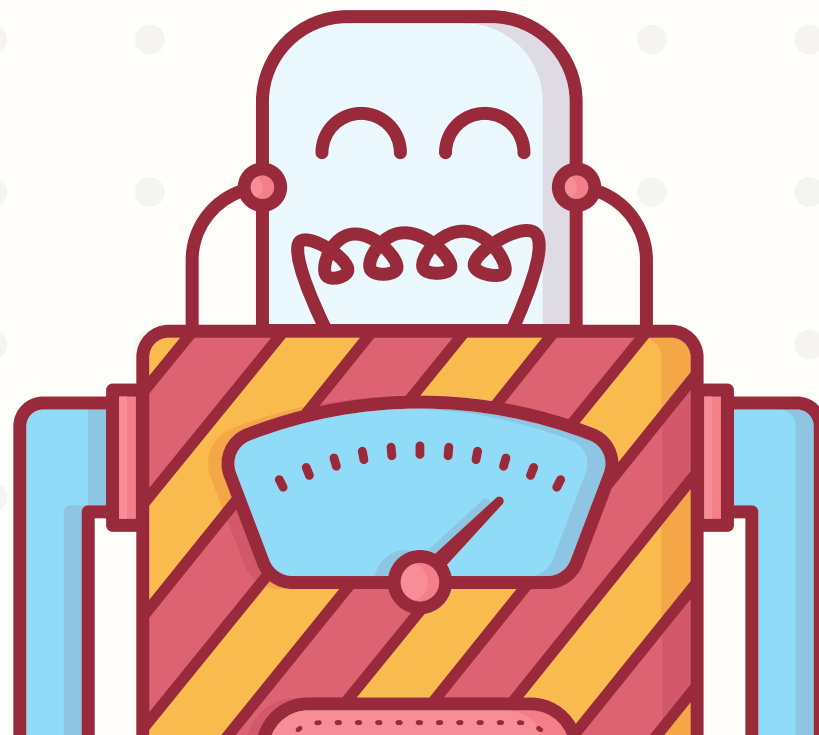
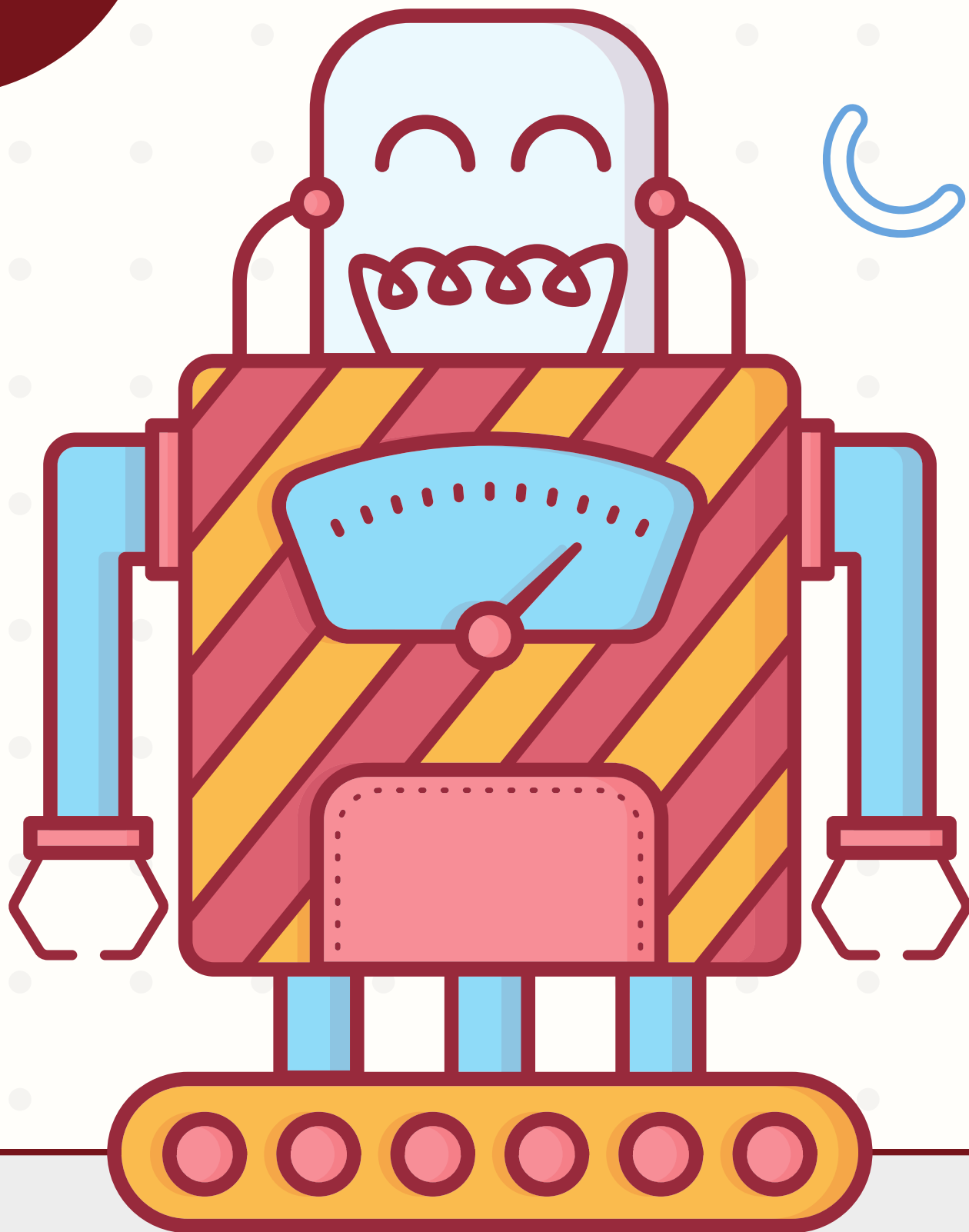


# BRUTE FORCE

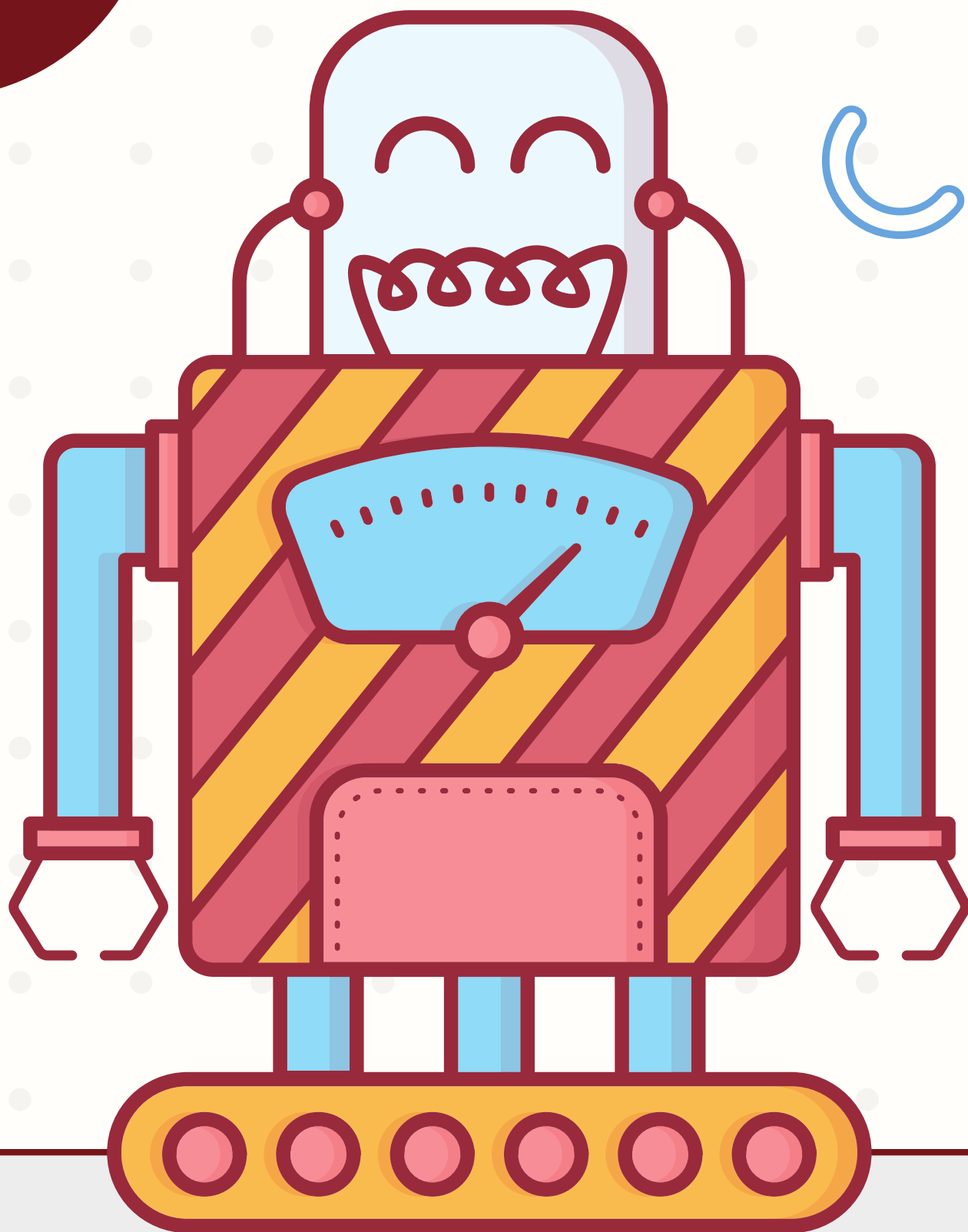
Oleh: Kelompok 3



# PENGERTIAN

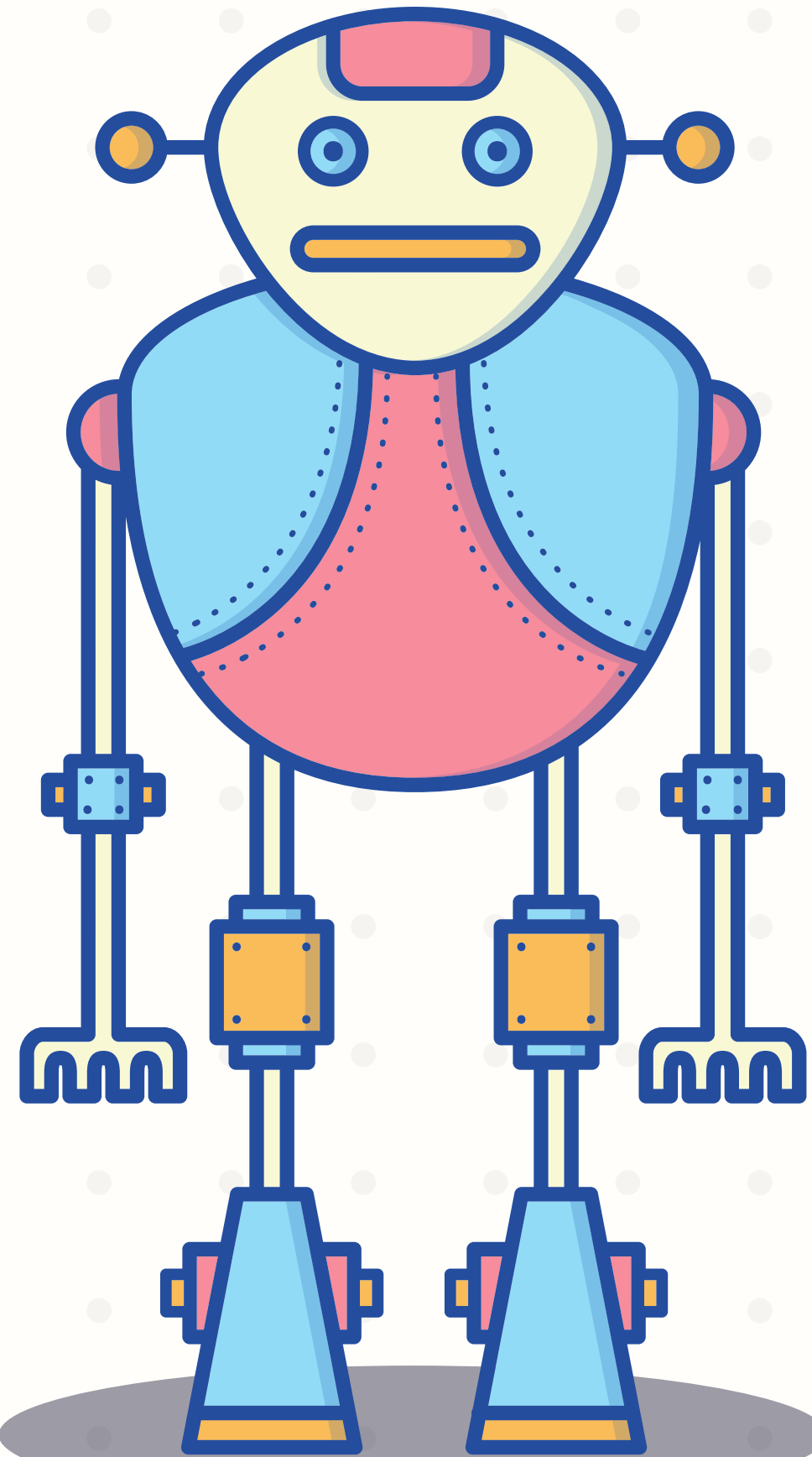


Brute force adalah metode penyelesaian masalah yang mencoba semua kemungkinan solusi untuk menemukan solusi yang benar. Dalam kata lain brute force adalah metode paling sederhana untuk mengakses situs atau server (atau apa pun yang dilindungi kata sandi).



# CIRI CIRI

- Sederhana & Mudah diimplementasikan
- Memeriksa semua kemungkinan
- Tidak efisien
- Menggunakan banyak waktu & memori
- Tidak memerlukan ilmu khusus
- Deterministik



# SEJARAH

- . Sejarah awal
- . Era komputer awal
- . Penggunaan modern

# SKENARIO BRUTE FORCE

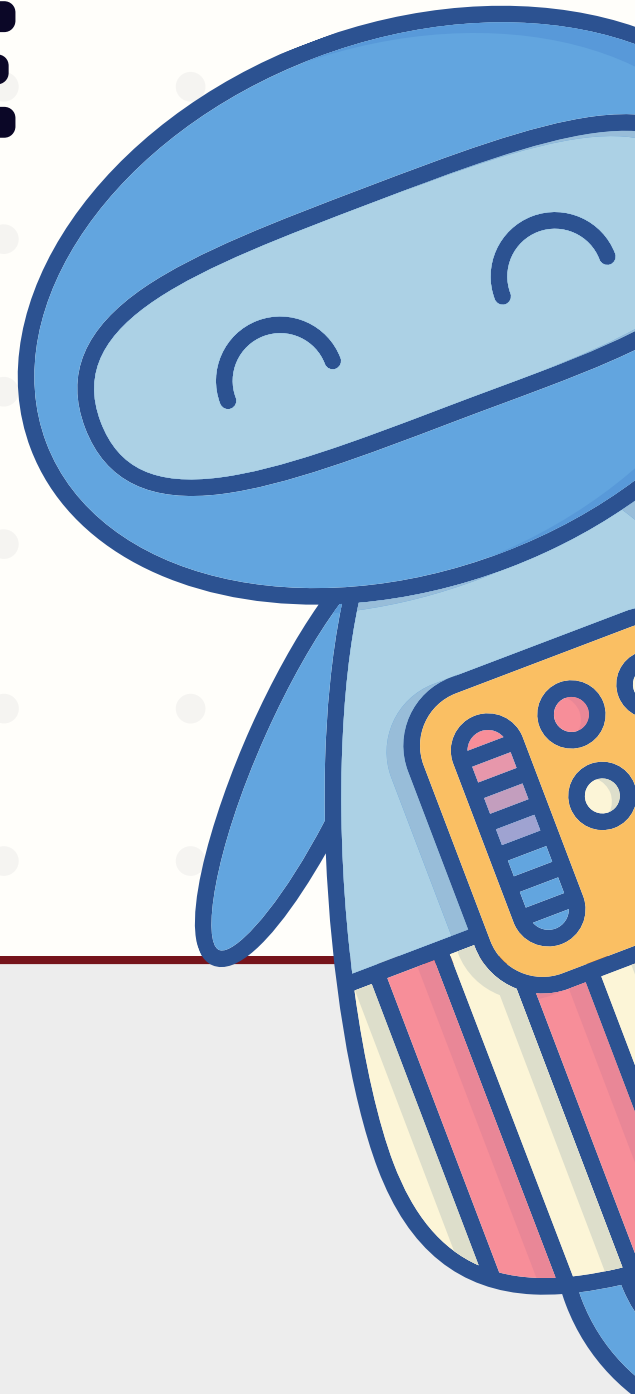
**1. PEMECAHAN KATA  
SANDI**

**2. PENENCARIAN  
STRING**

**3. MUTASI DAN  
KOMBINASI**

**4. PENYELESAIAN  
TEKA TEKI**

# CONTOH CODE BRUTE FORCE DI PYTHON



```
import itertools
import string

def brute_force_password(target):
    chars = string.ascii_lowercase
    for length in range(1,
len(target) + 1):
        for attempt in
itertools.product(chars,
repeat=length):
            if ''.join(attempt) ==
target:
                return
''.join(attempt)
            return None

password = "abc"
found_password =
brute_force_password(password)
print(f"Password found:
{found_password}")
```

# CARA PENGGUNAAN BRUTE FORCE

## 1. MENDEFINISIKAN MASALAH

Tentukan masalah yang ingin di selesaikan. Misalnya, apakah Anda mencari solusi optimal dari kombinasi tertentu, atau memecahkan sebuah teka-teki?

## 2. TENTUKAN KEMUNGKINAN SOLUSI

Tentukan semua kemungkinan solusi yang mungkin. Misalnya, jika Anda mencari kata sandi, ruang solusinya bisa berupa semua kombinasi karakter yang mungkin.

## 3. BUAT ALGORITMA

# LANJUTAN...

## **4. IMPLEMEN TASI**

Pelaksanaan atau penerapan untuk mencapai suatu tujuan.

## **5. EVALUASI SETIAP SOLUSI**

Untuk mempertimbangkan baik buruknya hasil kerja.

## **6. RUN/ MENAMPILKAN HASIL**

Menampilkan hasil kerja.





# TOOLS UNTUK MELANCARKAN BRUTE FORCE ATTACK



01

Hydra: tools populer untuk melakukan brute force attack pada protokol autentikasi yang umum seperti SSH, FTP, HTTP, dan sebagainya.

02

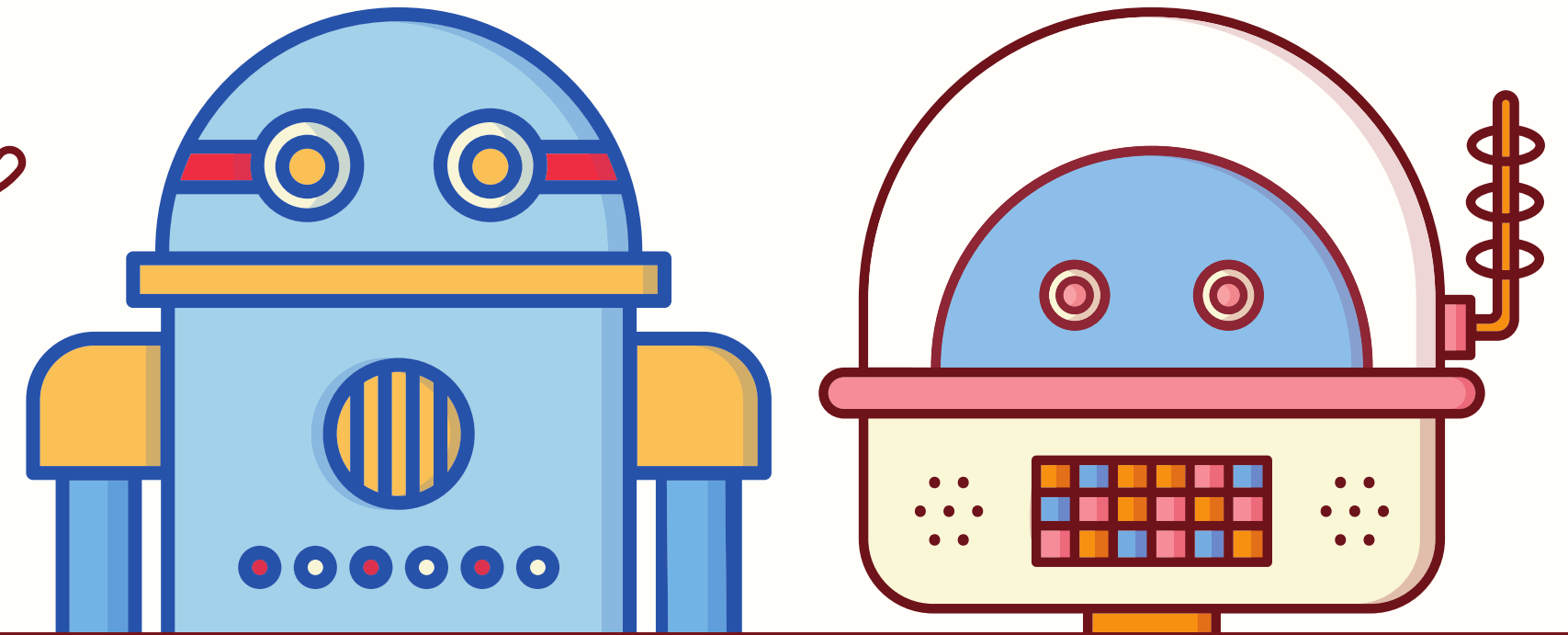
Medusa: Tools untuk menyerang berbagai protokol autentikasi seperti SSH, Telnet, FTP, HTTP, dan sebagainya.

03

John the Ripper: Tools open-source untuk menguji kelemahan password dengan melakukan brute force attack dan serangan kamus.



# LANJUTAN...



## TUJUAN SERANGAN BRUTE FORCE

Pencurian informasi pribadi seperti kata sandi, frasa sandi, dan informasi lain yang digunakan untuk mengakses akun online dan sumber daya jaringan. Menyamar sebagai pengguna untuk mengirim tautan phishing atau menyebarkan konten

## CARA MENGHINDARI SERANGAN BRUTE FORCE

1. Buat Kombinasi Password yang Rumit
  2. Mengatur Limit Login
  3. Gunakan Captcha
  4. Manfaatkan Two Factor Authentication
  5. Mengganti URL Login WordPress
  6. Menggunakan CloudFlare
  7. Memantau Log WordPress Anda
- 