

task6

passwords

A terminal window with a dark blue background and a faint keyboard graphic. The prompt is (root@kali)-[/home/kali]. The user runs 'rm pass.txt' and then 'cat > pass.txt'. A red box highlights the output of the cat command, which lists five passwords: R@!q8vNm3Z#7Lw, G7@xL#29qRmZ, BlueSky99!, 12345678, and password1. The user then presses Ctrl-C (^C) and the prompt returns with a cursor.

```
(root@kali)-[/home/kali]
# rm pass.txt

(root@kali)-[/home/kali]
# cat > pass.txt
R@!q8vNm3Z#7Lw
G7@xL#29qRmZ
BlueSky99!
12345678
password1
^C

(root@kali)-[/home/kali]
#
```

we can generate passwords by crunch tool

password is R@!q8vNm3Z#7Lw

WhatsApptask.pdfTutodude DashboardPassword complexityPassword Checker &How Secure Is My P...A Detailed Guide on

security.org/how-secure-is-my-password/

GmailYouTubeMapsNewsTranslateADbug bounty

We may earn compensation from some providers below. [Learn More](#)

Our videos have over 10 million views on [See Our Channel >](#)

Home SecuritySmart HomeDigital SecurityAbout Us

How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

.....

It would take a computer about

2 hundred million years

to crack your password

Entries are 100% secure and not stored in any way or shared with anyone. Period.

Passwords are the bloodline of da

Protect Your Personal Information

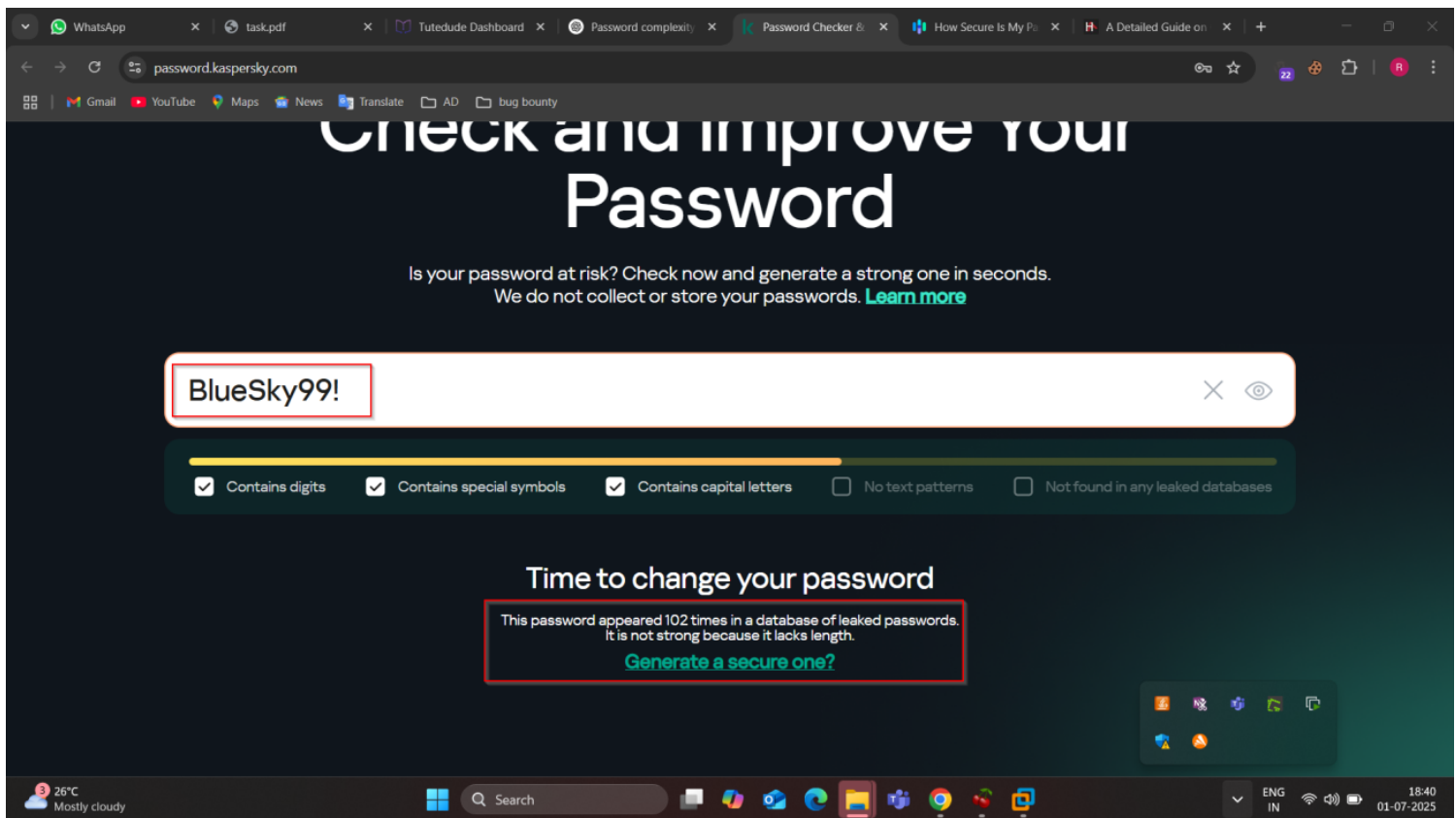
e U.S. shows that less than half of

26°C Mostly cloudy

Search

ENG IN

18:37 01-07-2025



Step 5: Identify Best Practices for Strong Passwords

Best Practices Checklist:

- Minimum 12–16 characters
- Use random combinations
- Avoid personal info
- Don't reuse passwords
- Use password managers

Step 6: Write Tips Learned from the Evaluation

Sample Tips:

- Length is as important as complexity.
- A mix of unrelated words and symbols works better.
- Passwords like `MyDog2023!` may feel secure but are guessable.
- Password managers can auto-generate very secure passwords

Step 7: Research Common Password Attacks

Common Attacks:

Attack Type	Description
Brute Force	Tries all combinations until success.

Attack Type	Description
Dictionary Attack	Tries words from a known wordlist.
Credential Stuffing	Uses previously leaked passwords.
Phishing	Tricks user into giving password.