



# ACCESS CONTROL



Presented by: **Brahim Ferik**

# ACCESS CONTROL: PASSWORD SECURITY ESSENTIALS

- **Passwords are a fundamental component of access control, serving as a primary authentication method. Strong passwords enhance security by preventing unauthorized access.**



---

# LESSON OBJECTIVES

- ☐ **Understand common vulnerabilities in passwords.**
- ☐ **Learn how attackers exploit weak passwords.**
- ☐ **Develop strategies to create and manage uncrackable passwords.**
- ☐ **Implement advanced authentication layers.**



# TOP MOST COMMON PASSWORDS 2024

TOP 10  
MOST COMMON  
PASSWORDS  
IN 2023

\*\*\*\*\*

- |   |           |    |            |
|---|-----------|----|------------|
| 1 | 123456    | 6  | qwerty123  |
| 2 | 123456789 | 7  | 1q2w3e     |
| 3 | qwerty    | 8  | 12345678   |
| 4 | password  | 9  | 11111      |
| 5 | 12345     | 10 | 1234567890 |



---

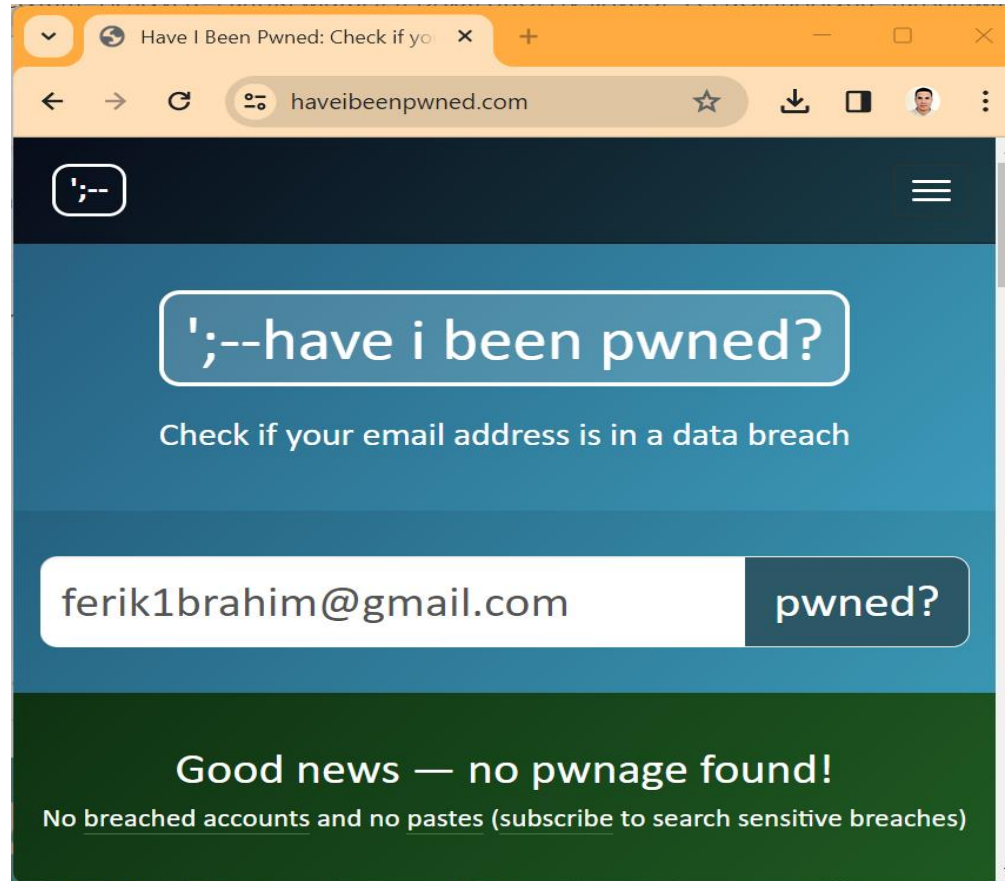
# TOP MOST COMMON PASSWORDS 2024

- ☐ **<https://shorturl.at/CJrUZ>**
- ☐ **<https://shorturl.at/J4U0I>**
- ☐ **<https://shorturl.at/BqWh7>**



# VERIFICATION OF PROTECTION?

haveibeenpwned.com



The screenshot shows a web browser window with the URL 'haveibeenpwned.com'. The page features a dark blue header with a logo and a menu icon. The main content area has a blue background with a white search bar containing the email 'ferik1brahim@gmail.com' and a dark blue button labeled 'pwned?'. Below the search bar, a green banner displays the message 'Good news — no pwnage found!' and 'No breached accounts and no pastes (subscribe to search sensitive breaches)'.



# PASSWORD CRACKING SIMULATION



---

# PASSWORD CRACKING METHODS

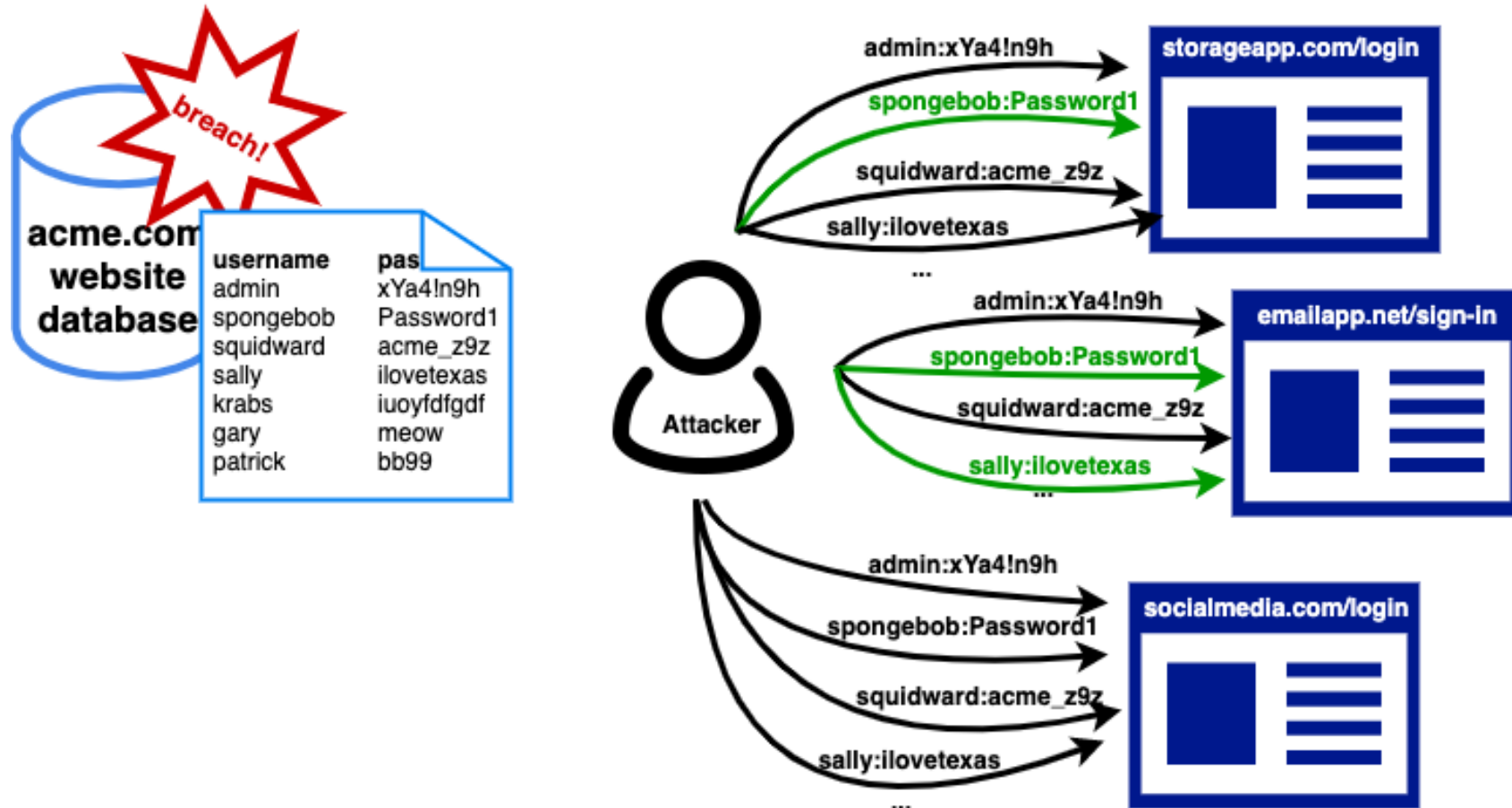
- **Key Techniques**

- ☐ **Dictionary Attacks.**
- ☐ **Combinator Attacks.**
- ☐ **Brute-force Attacks.**
- ☐ **Phishing/Social Engineering.**
- ☐ **Credential Stuffing.**





# PASSWORD CRACKING METHODS



---

# PASSWORD CRACKING METHODS



**HASHCAT**



# PASSWORD CRACKING METHODS

- **Applied Work (rar file)**

- ❑ **rar2john.exe protected.rar**
- ❑ **hashcat.exe -m 13000 -a3 value\_hash ?d?d?d?d**
- ❑ **hashcat.exe --show -m 13000 value\_hash**
- ❑ **<https://shorturl.at/icb1C>**



# PASSWORD CRACKING METHODS

- **Applied Work (Zip file)**

- ❑ **john.exe -list=formats**
- ❑ **zip2john.exe protected.zip>zip.hash**
- ❑ **john.exe zip.hash**



# PASSWORD CRACKING METHODS



# PASSWORD CRACKING METHODS

- **Applied Work (PDF, DOCX, XLSX, ...)**
- ❑ **Practical Exercises.**
- ❑ **Prepare a wordlist containing common passwords.**



---

# HOW TO PREVENT BRUTE FORCE PASSWORD HACKING?

- ☐ **Never use information that can be found online (like names of family members).**
- ☐ **Have as many characters as possible.**
- ☐ **Combine letters, numbers, and symbols.**
- ☐ **Be different for each user account.**
- ☐ **Do not use common patterns.**



---

# HOW TO PREVENT BRUTE FORCE PASSWORD HACKING?

- ☐ **Lockout policy**
- ☐ **Progressive delays**
- ☐ **Captcha**
- ☐ **Requiring strong passwords**
- ☐ **Two-factor authentication**





# CHECK YOUR PASSWORD



Check your  
password



[password.kaspersky.com](https://password.kaspersky.com)



# HOW SECURE IS MY PASSWORD?

## How Secure Is My Password?

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



It would take a computer about

# 7 milliseconds

to crack your password

[www.passwordmonster.com](http://www.passwordmonster.com)

[howsecureismypassword.net](http://howsecureismypassword.net)



---

# PASSWORD GENERATION STRATEGIES

- ☐ **Use of Password Managers**
- ☐ **Passphrases**
- ☐ **Random Character Combinations**
- ☐ **Keyboard Patterns**



---

# PASSWORD GENERATION STRATEGIES

## ☐ Example of a Strong Password

**G7#pX9@wZ2!qL**



# PASSWORD GENERATION STRATEGIES

## ❑ Passphrases

### Passwords :

samuel123  
m0nk3y99  
49lakestreet  
Y#Cb3\$D6dZYF

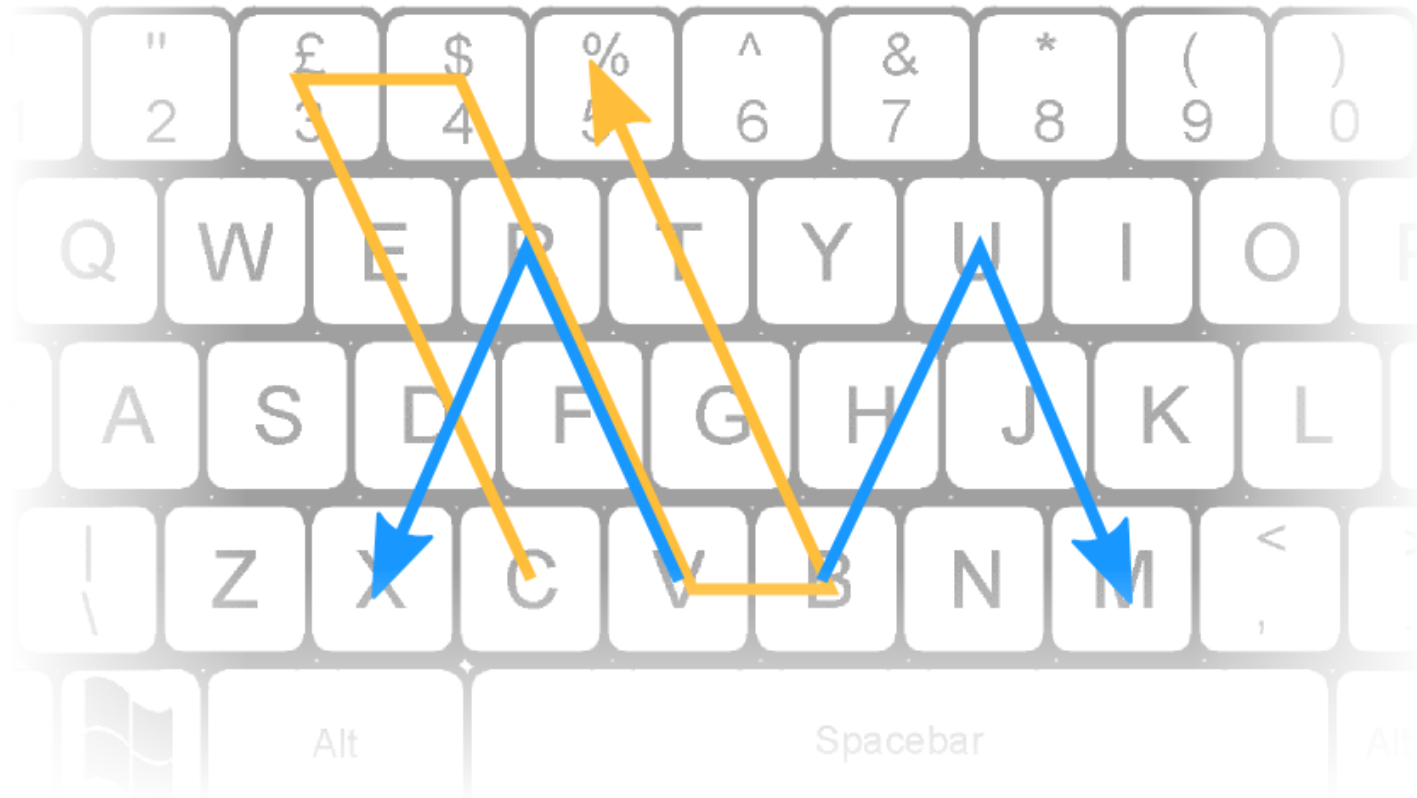
### Pass-phrases :

I love ice-cream!  
Jerry lives in Bugtussle KY  
I can see tham, yall.  
2 be or not 2 be, that is the ?



# PASSWORD GENERATION STRATEGIES

## ❑ Keyboard Patterns



---

# **PASSWORD POLICIES FOR LOCAL WINDOWS ACCOUNTS - DEMO**

☐ **Password Policy**

☐ **Account Lockout Policy**



---

# WINDOWS USER MANAGEMENT

## ☐ The Syntax of the Command

**net user ?**

## ☐ View All Users on the System

**net user**





# WINDOWS USER MANAGEMENT

- ❑ Adding a User without a Password

**net user username /add**

- ❑ Set Password

**net user username password**

- ❑ Set Password with Confirm

**net user username \***

- ❑ Deleting a Specific User

**net user username /delete**

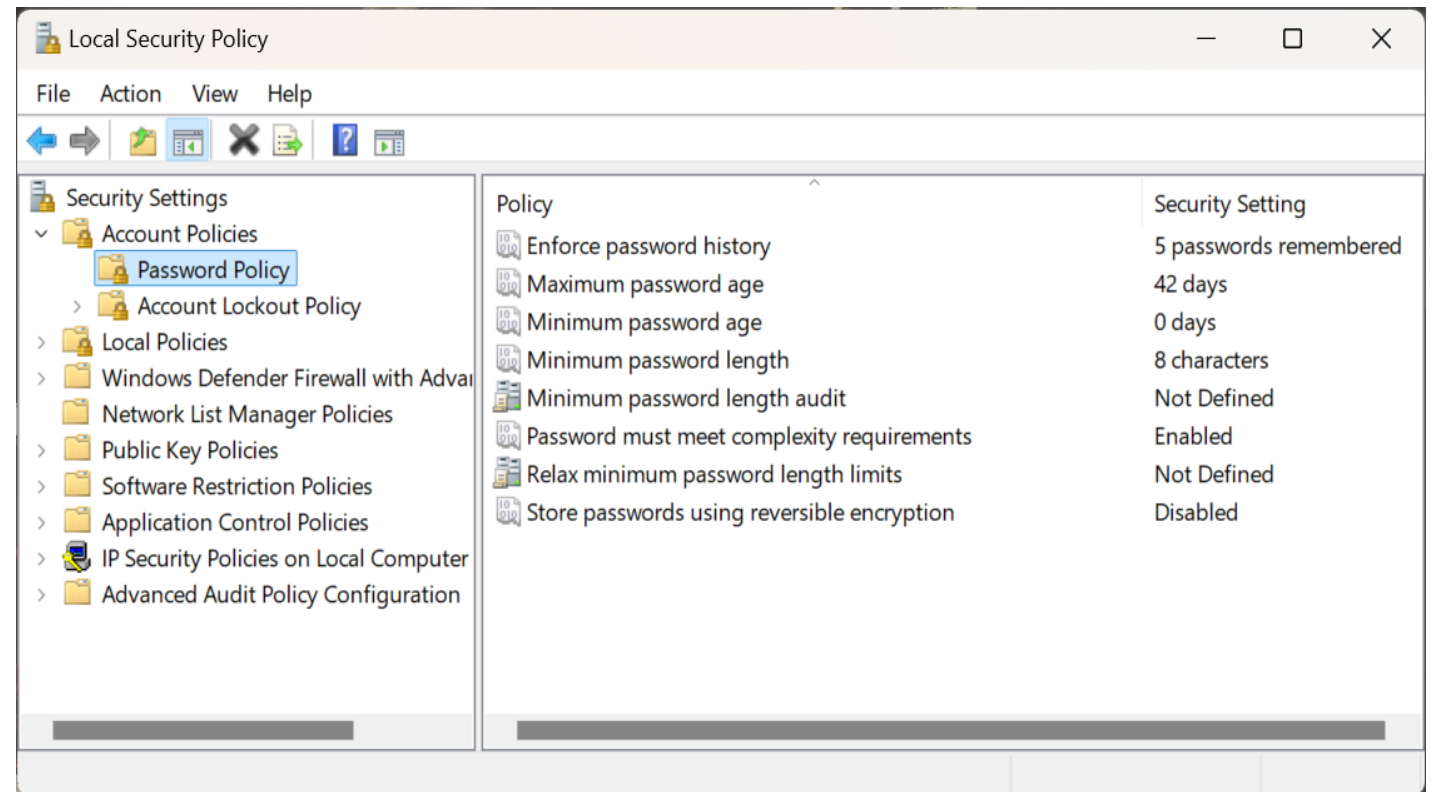


# PASSWORD POLICIES

❑ **Search Local Security Policy**

❑ **Win + R : secpol.msc**

❑ **secpol.msc CMD**



---

# PASSWORD POLICIES FOR LOCAL WINDOWS ACCOUNTS

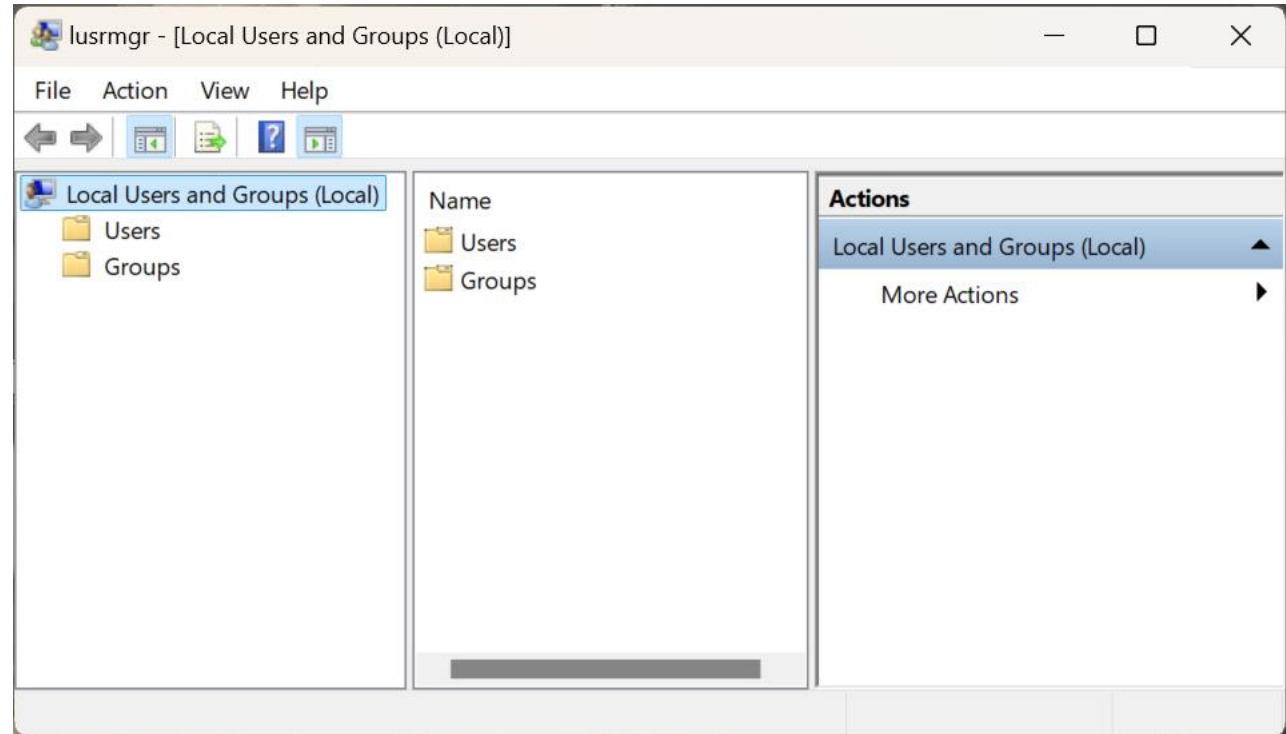
- ☐ **Enforce password history (3 passwords)**
- ☐ **Maximum password age (90 days)**
- ☐ **Minimum password length (8)**
- ☐ **Password must meet complexity requirements (Enable)**



# ❑ Computer Management > System Tools > Local Users and Groups.

❑ Win + R : lusrmgr.msc

❑ lusrmgr.msc CMD

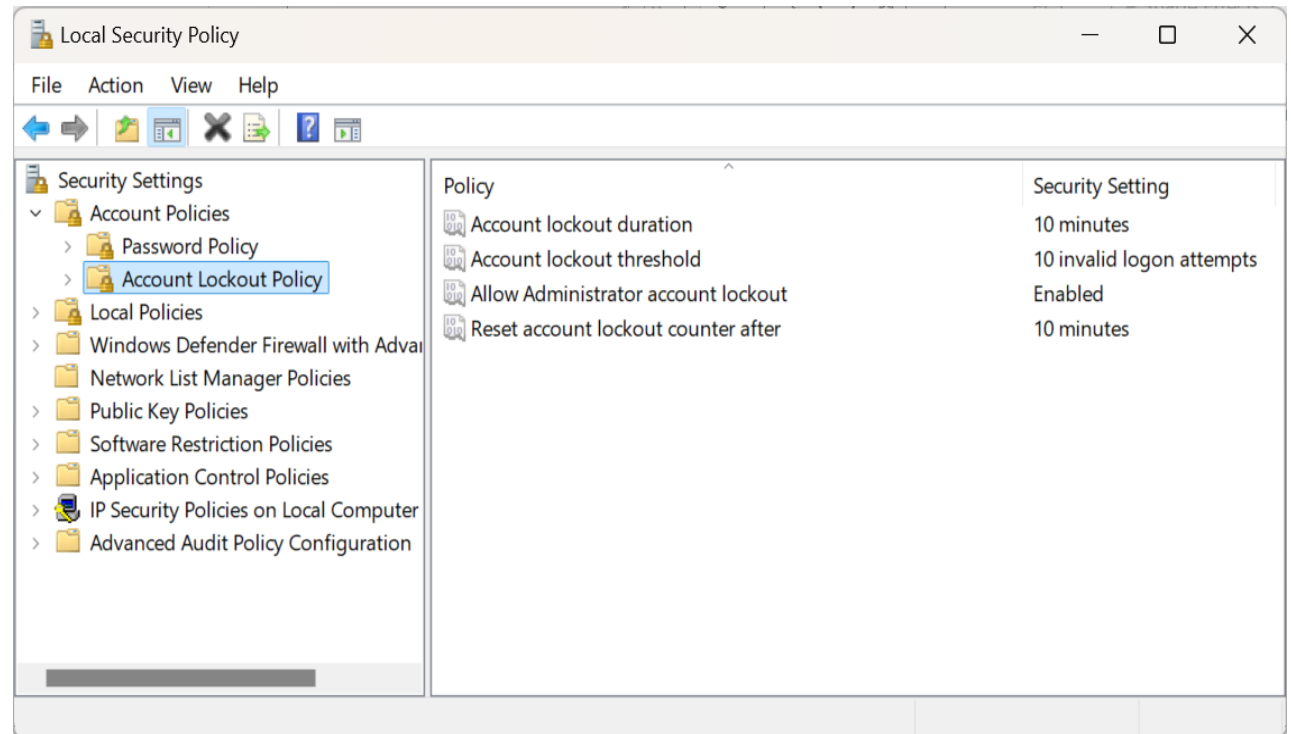


# ACCOUNT LOCKOUT POLICY

❑ **Search Local Security Policy**

❑ **Win + R : secpol.msc**

❑ **secpol.msc CMD**



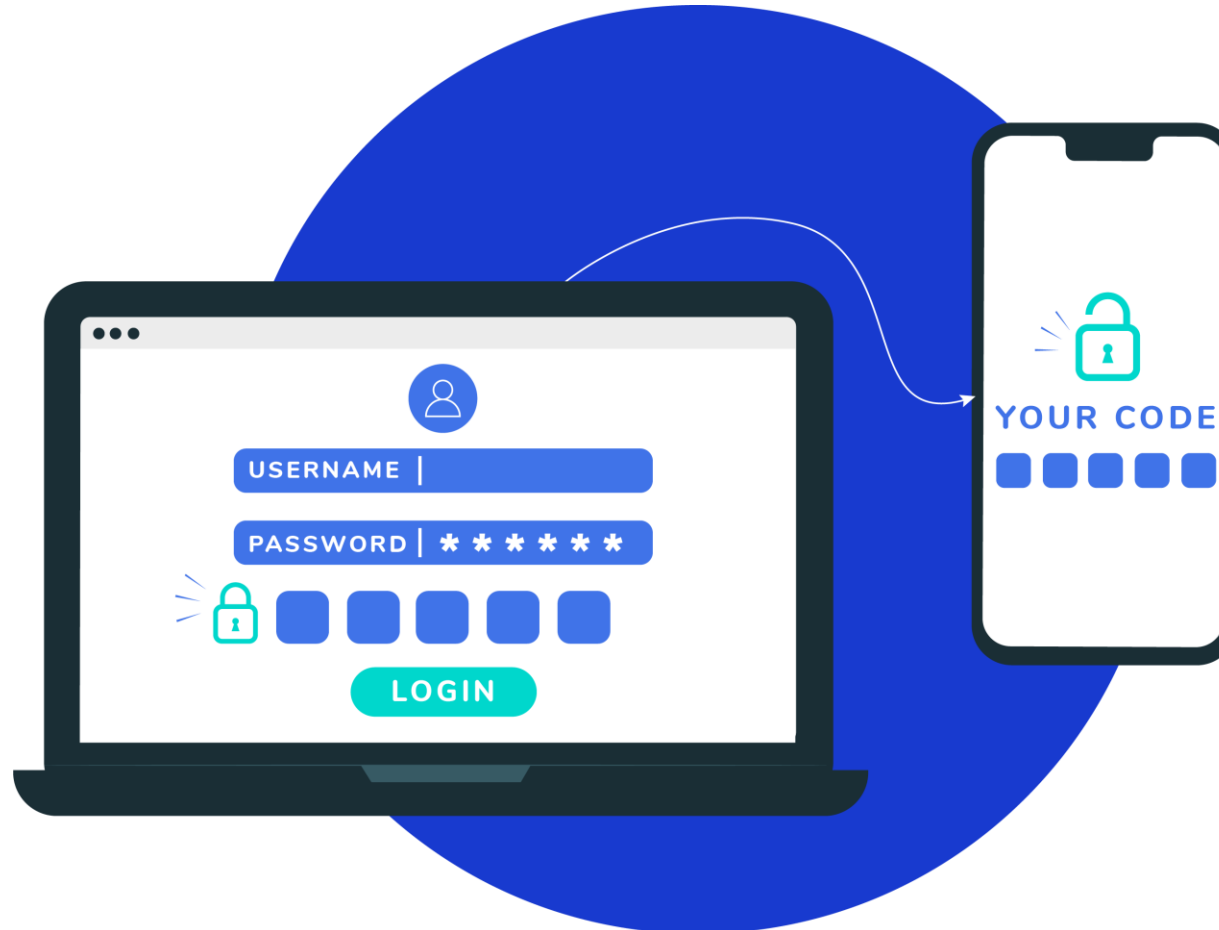
---

# ACCOUNT LOCKOUT POLICY

- ☐ **Account lockout threshold: 3 invalid logon attempts.**
- ☐ **Account lockout duration: 15 minutes.**
- ☐ **Reset account lockout counter after: 5 minutes.**



# ENABLE TWO-FACTOR AUTHENTICATION (2FA)



---

# ENABLE TWO-FACTOR AUTHENTICATION (2FA)



**Google Authenticator**



**Microsoft Authenticator**



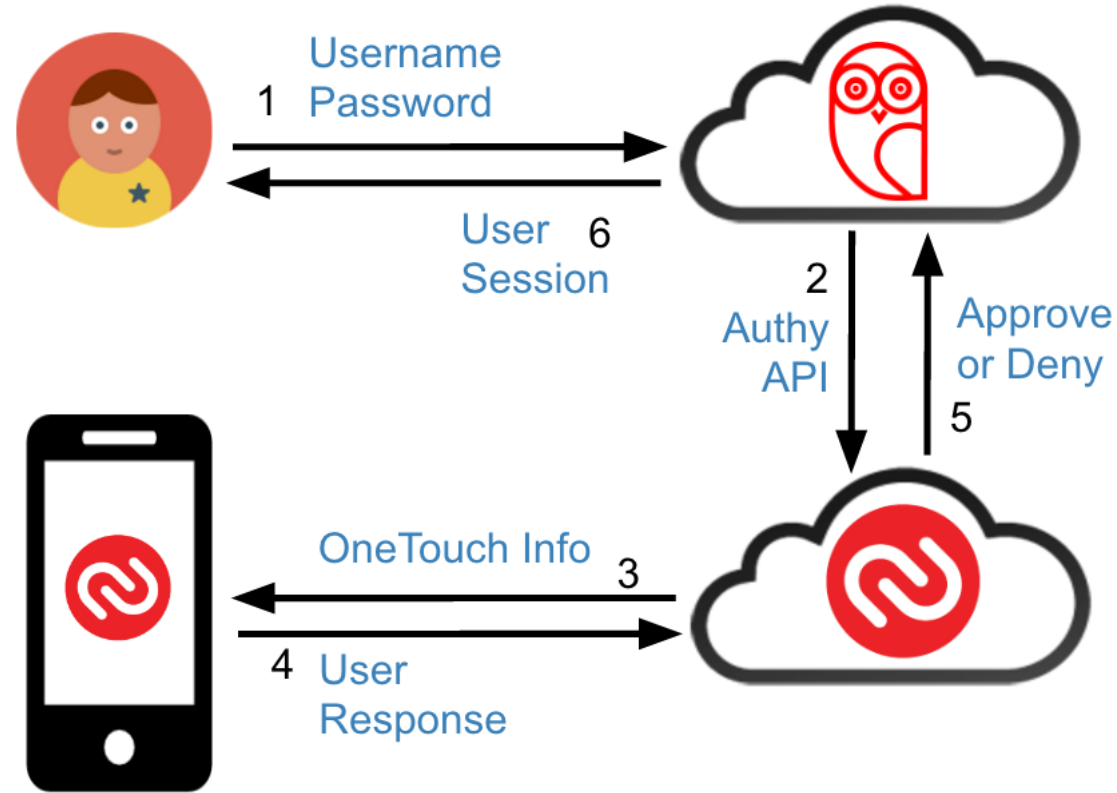


---

# ENABLE TWO-FACTOR AUTHENTICATION (2FA)



# ENABLE TWO-FACTOR AUTHENTICATION (2FA)



# PASSWORD MANAGEMENT TOOLS

- **Local vs. Cloud Managers**

- ☐ **Local (Offline): KeePass, Bitwarden**

- ☐ **Cloud-Based: 1Password, LastPass**



Keepass



bitwarden



# USE A PASSWORD MANAGER

LastPass \*\*\*\*



Keepass



---

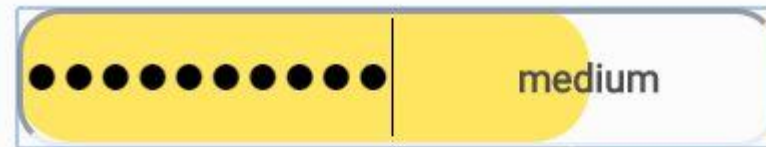
# **APPLIED PROGRAMMING TASKS: EXPLORING PASSWORD SECURITY ESSENTIALS**

- A. Develop a Password Strength Verification Tool.**
- B. Build a Secure Password Generator.**
- C. Implement Two-Factor Authentication.**
- D. Analyze Breached Passwords.**
- E. Passphrase Password Generator.**



# APPLIED PROGRAMMING TASKS: EXPLORING PASSWORD SECURITY ESSENTIALS

## A. Develop a Password Strength Verification Tool.



Show Password

Password must include:

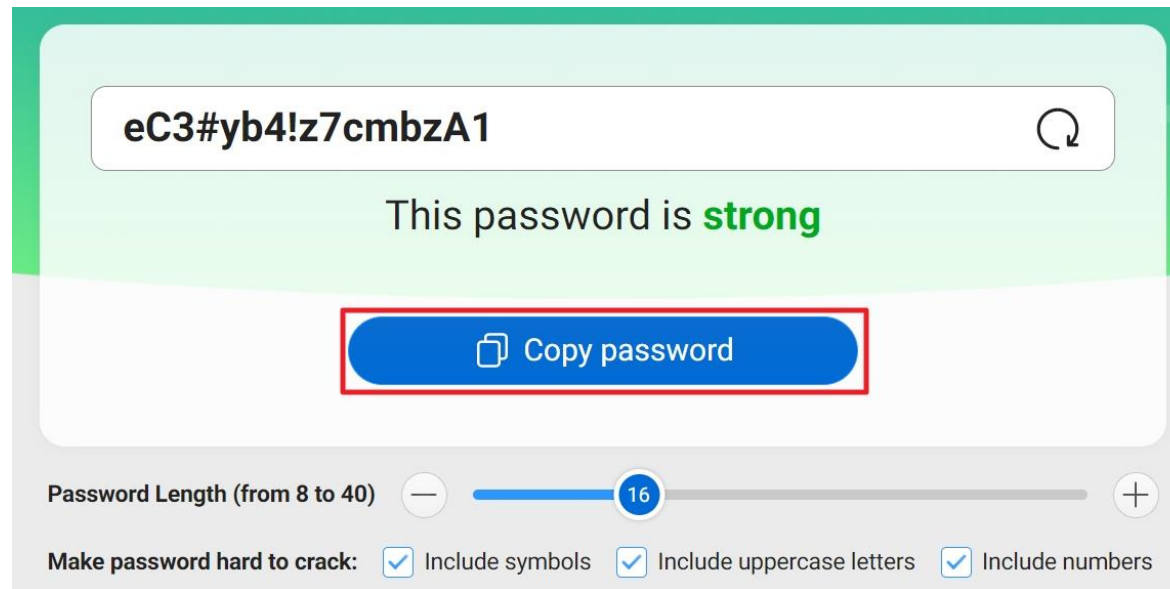
- ✓ 8-20 Characters
- ✗ At least one capital letter
- ✓ At least one number
- ✓ No spaces

Show Password



# APPLIED PROGRAMMING TASKS: EXPLORING PASSWORD SECURITY ESSENTIALS

## B. Build a Secure Password Generator.



The image shows a user interface for a password generator. At the top, a text box displays the generated password "eC3#yb4!z7cmbzA1" with a refresh icon to its right. Below the text box, a green banner states "This password is **strong**". Underneath the banner is a blue button with a copy icon and the text "Copy password", which is highlighted by a red rectangular border. At the bottom, there is a slider for "Password Length (from 8 to 40)" with a value of 16. Below the slider, the text "Make password hard to crack:" is followed by three checked checkboxes: "Include symbols", "Include uppercase letters", and "Include numbers".



# APPLIED PROGRAMMING TASKS: EXPLORING PASSWORD SECURITY ESSENTIALS

## C. Implement Two-Factor Authentication.

Two-factor Authentication

Please enter the authentication code.

The authentication code has been sent to email: example@yeastar.com.

\* \* \* \* \*

Resend available in 119 seconds

☐ Trusted Device

Cancel LOG IN

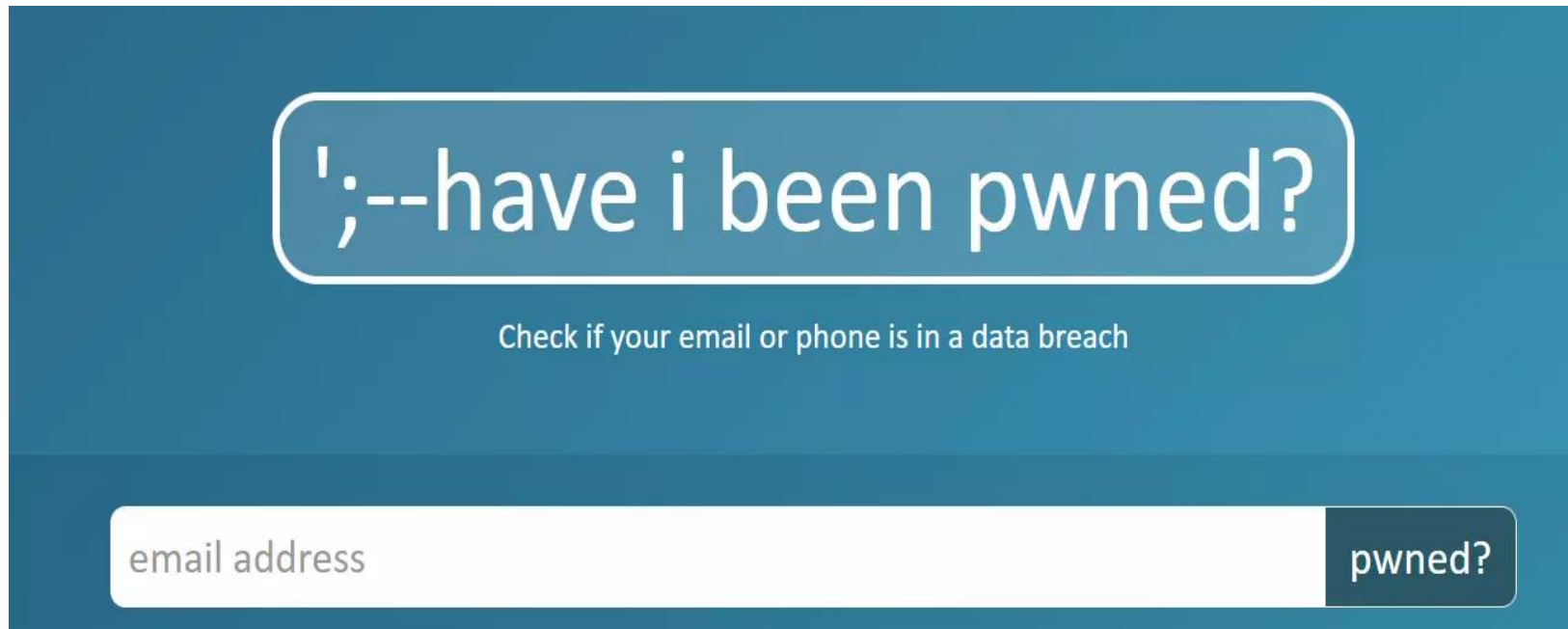
\* \* \* \* \*





# APPLIED PROGRAMMING TASKS: EXPLORING PASSWORD SECURITY ESSENTIALS

## D. Analyze Breached Passwords.



';--have i been pwned?

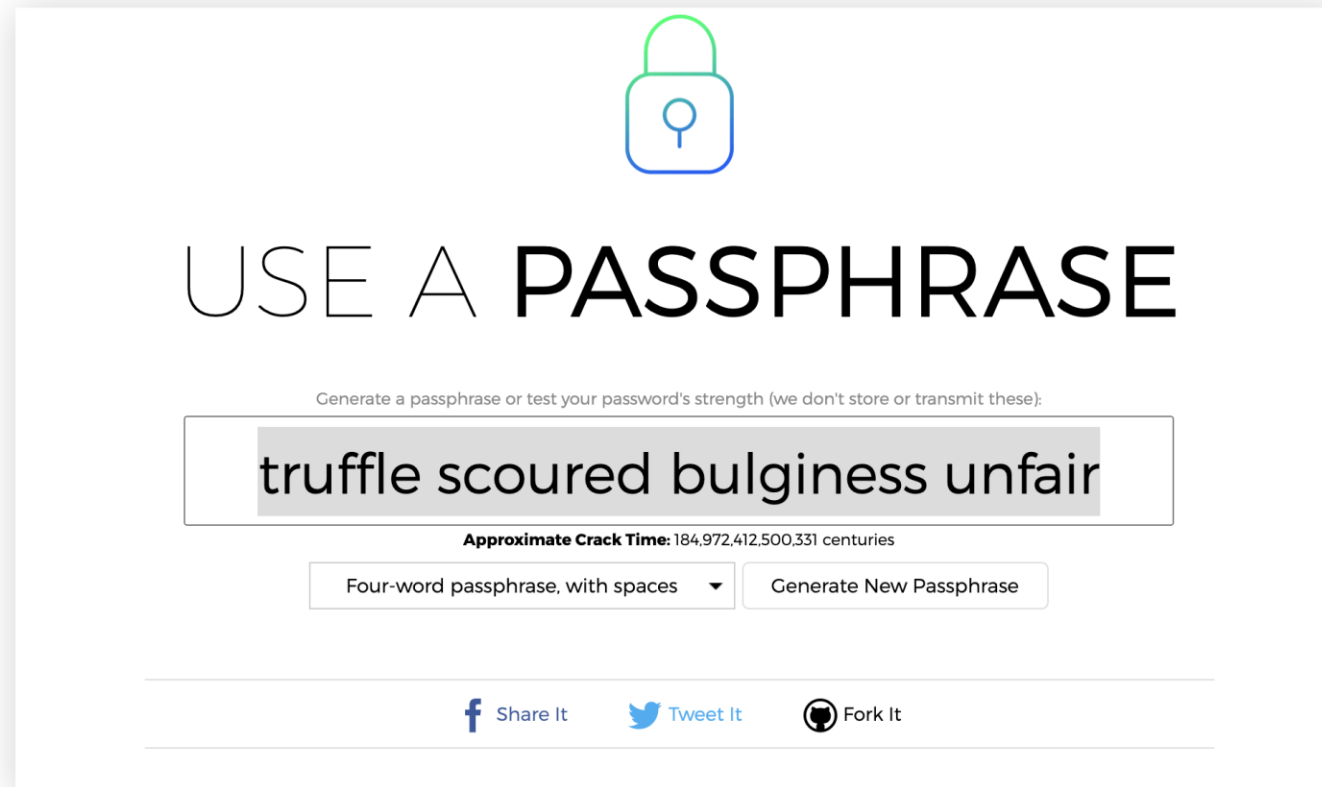
Check if your email or phone is in a data breach

email address pwned?



# APPLIED PROGRAMMING TASKS: EXPLORING PASSWORD SECURITY ESSENTIALS

## E. Passphrase Password Generator.



The image shows a web interface for a passphrase generator. At the top center is a green padlock icon. Below it, the text "USE A PASSPHRASE" is displayed in a large, black, sans-serif font. Underneath this text is a smaller line of gray text: "Generate a passphrase or test your password's strength (we don't store or transmit these):". Below this is a text box containing the generated passphrase "truffle scoured bulginess unfair". Under the text box, the "Approximate Crack Time" is shown as "184,972,412,500,331 centuries". Below the crack time is a dropdown menu set to "Four-word passphrase, with spaces" and a button labeled "Generate New Passphrase". At the bottom of the interface are three social media sharing options: "Share It" with a Facebook icon, "Tweet It" with a Twitter icon, and "Fork It" with a GitHub icon.

USE A PASSPHRASE

Generate a passphrase or test your password's strength (we don't store or transmit these):

truffle scoured bulginess unfair

Approximate Crack Time: 184,972,412,500,331 centuries

Four-word passphrase, with spaces ▼ Generate New Passphrase

[Share It](#) [Tweet It](#) [Fork It](#)