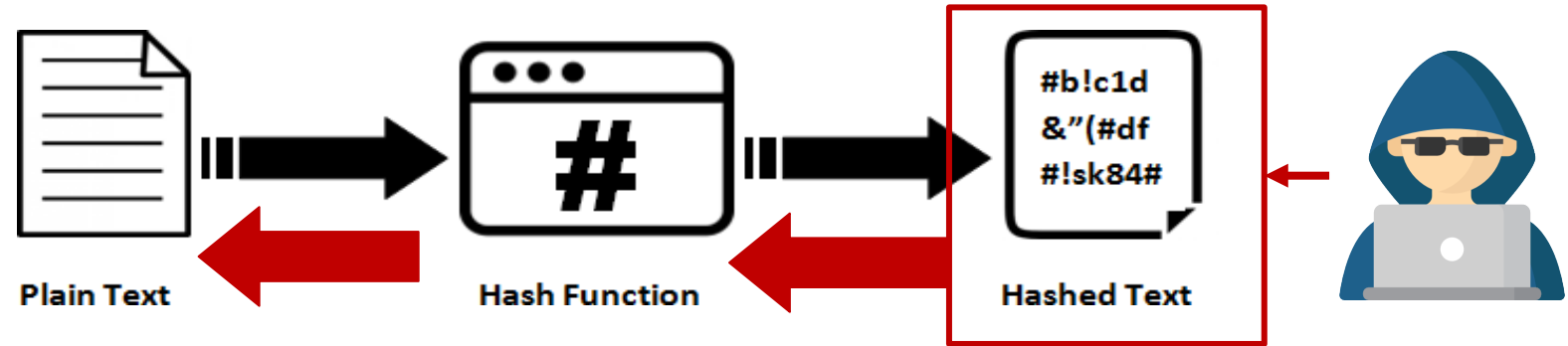


# OFFLINE GUESSING ATTACK(\$)

## Offline Guessing Attack

An attack where the attacker obtains the hashed passwords, and attempts to guess the passwords.



- This is a plausible threat, due to:
  - many incidents of **stolen (hashed) passwords** as a consequence of **hacks on servers** or **sniffing traffic**
  - usage of the **same passwords across different** accounts; so **compromise of a password for one account affects other accounts**.

**Recap:** In Unix, password hashes are stored in `/etc/passwd`, but in modern Unix/Linux systems it is in the *shadow* file in `/etc/shadow`.

# PASSWORD-RELATED INCIDENTS

## SingHealth cyber attack a result of human lapses, IT system weaknesses: COI report

By CYNTHIA CHOO



Reuters file photo

The SingHealth cyber attack happened because of lapses by employees and vulnerabilities with the system.

Published 10 JANUARY, 2019 UPDATED 10 JANUARY, 2019

85 Shares



SINGAPORE — The SingHealth cyber attack happened because of lapses by employees and vulnerabilities with the system. Ultimately, the breach into the public healthcare group's database was preventable even though the attacker was skilled.

These were the key findings in a report released on Thursday (Jan 10) by

**Vulnerabilities and weaknesses in the SingHealth network and SCM system contributed to the attacker's success in obtaining and taking the data**

- The SCM database, which is legally owned by SingHealth, functioned on an open network that was linked to the Citrix servers of Singapore General Hospital (SGH), which resulted in a critical vulnerability the attacker exploited.
- It was found that there was a lack of monitoring of the SCM database for unusual queries and access. For one, there was no existing control to detect or block bulk queries being made to the database. For another, the Citrix servers of SGH were not monitored for real-time analysis and alerts of vulnerabilities and issues arising from these servers.
- The Citrix servers were not adequately secured against unauthorised access. Notably, the process requiring 2-factor authentication (2FA) for administrator access was not enforced as the exclusive means of logging in as an administrator. This allowed the attacker to access the server through other routes that did not require 2FA.
- Another weakness which may have been exploited by the attacker included **weak administrator account passwords**. This was among others discovered during a test but the remediation process undertaken by IHiS was mismanaged and inadequate, and a number of **vulnerabilities remained** at the time of the cyber attack.

# PASSWORD-RELATED INCIDENTS



29  
Oct 13

## Adobe Breach Impacted At Least 38 Million Users



The recent data breach at **Adobe** that exposed user account information and prompted a flurry of password reset emails impacted at least 38 million users, the company now says. It also appears that the already massive source code leak at Adobe is broadening to include the company's **Photoshop** family of graphical design products.

AnonNews - Everything Anonymous  
(F4Q) (RC) (Forum) (44000) (44000) (44000)

## 6.46 million LinkedIn passwords leaked online

**Summary:** More than 6.4 million LinkedIn passwords have leaked to the Web after an apparent hack. Though some login details are encrypted, all users are advised to change their passwords.

By [Zack Whittaker](#) for [Between the Lines](#) | June 6, 2012 -- 05:46 GMT (13:46 SGT)



A vulnerability in Starbucks' mobile app could be putting coffee drinkers' information—including their usernames, email addresses and passwords—at risk.



# BRUTE FORCE ATTACK



MATCH

- Brute force guessing attack against passwords tries to guess password by enumerating all passwords and their hashes in sequence, and check whether they match the target hashes.
- A measure **against brute force attack** is to **increase the space of possible passwords**, e.g., longer passwords, allowing more varieties of symbols (alphabets, numerals, signs).

**Password policy is an important means to increase difficulties of brute force attack**

# PASSWORD ENTROPY-measured by $2^k$

$\rightarrow c$ $\downarrow n$	26 (lowercase)	36 (lowercase alphanumeric)	62 (mixed case alphanumeric)	95 (keyboard characters)
5	23.5	25.9	29.8	32.9
6	28.2	31.0	35.7	39.4
7	32.9	36.2	41.7	46.0
8	37.6	41.4	47.6	52.6
9	42.3	46.5	53.6	59.1
10	47.0	51.7	59.5	65.7

**Table 10.1:** Bitsize of password space for various character combinations. The number of  $n$ -character passwords, given  $c$  choices per character, is  $c^n$ . The table gives the base-2 logarithm of this number of possible passwords.

Source: Menezes et al. Handbook of Applied Cryptography.

At present, software password crackers can crack up to 16 million pswd/sec per pc.  
Write a program to calculate how long it will take to bruteforce  
passwords for each entry.