Tấn công offline có phạm vị tương đối hạn chế, hiệu suất thấp. Bởi đây là dạng đánh cắp tài khoản đơn giản nhất, không yêu cầu trình độ cao và cũng không tốn bất kỳ chi phí nào. Nếu bạn để lộ pass hay lưu ở dạng không mã hóa trong tập tin thì các hacker có thể dễ dàng đánh cắp được. Có tới 50% vụ đánh cắp tài khoản do gần gũi với nạn nhân nên có thể tiếp cận tài sản của họ.

Tấn công offline cũng không đòi hỏi thủ phạm phải có tay nghề quá cao chỉ đơn giản là chúng sử dụng mật khẩu, tài khoản của người dùng do sơ hở trong việc khởi tạo thông tin bảo mật của họ hoặc chúng đã biết mật khẩu từ trước.

Thông qua nghiên cứu các vụ việc xảy ra, các chuyên gia cho biết kẻ tấn công offline chủ yếu là những người thân lân cận bạn và đã nhắm đến bạn trong một khoảng thời gian dài trước đó.

Insider attack: Đây là kiểu tấn công, đánh cắp mật khẩu trong nội bộ. Thực chất đây là hành vi của những người trong nội bộ công ty. Do bất đồng hoặc là gián điệp được công ty khác cài vào với mục đích phá hoại hệ thống an ninh mạng của toàn công ty. Họ có thể nghe trộm hoặc đánh cắp thông tin mật khẩu để truy cập vào những nguồn thông tin bí mật, quan trọng, và đánh cắp chúng với mục đích phi pháp.

assword attack (tấn công trực tiếp mật khẩu) : Các dạng tấn công này, chủ yếu sử dụng hệ thống mật khẩu được lưu sẵn trong máy hoặc kho password, hacker sẽ phá bảo an hệ thống và truy cập vào nguồn mật khẩu này.

**Dictionary attack:** Một kiểu tấn công lợi dụng thực tế rằng mọi người có xu hướng sử dụng các từ phổ biến và password ngắn, cũng như có liên quan tới thông tin cá nhân, gia đình... Hay những công ty, tổ chức thường đặt password theo một format xác định. Từ đó chúng tạo ra một từ điển password để tăng tỉ lệ tìm ra password đúng.

**. Key logger attack:** Trước khi bị 'dính' vào kiểu tấn công này, người dùng thường đã bị 'dính' một tấn công nào đó khác, như bị lây nhiễm trojan hay bị mở backdoor, dính Keylog... Qua đó hacker có được thông tin về tổ hợp phím mà người dùng đã sử dụng.

**Social engineering attacks:** Tấn công kỹ nghệ xã hội sử dụng kiến thức và cách thức tiếp cận liên quan tới tâm lý học hành vi, như giả mạo (Phishing / Spear phishing), khơi gợi tính tò mò hoặc tham lam ( Baiting )...

Cách phòng tránh:

Tốt hơn hết, bạn không nên sử dụng mật khẩu mặc định hoặc các dạng mật khẩu sử dụng các số, chữ thông thường. Hãy đan xen các ký tự đặc biệt trong mật khẩu máy tính, tài liệu của bạn.

Ngoài ra, việc sử dụng mật khẩu là những cái tên hoặc con số gợi nhớ cũng dễ khiến hacker hoặc những kẻ phá hoại xung quanh bạn nắm được. Bạn nên đặt mật khẩu chứa trên 21 ký tự và thay đổi mật khẩu thường xuyên. Thông thường, sau 48 ngày bạn nên đổi mật khẩu một lần, nhất là đối với các công ty lớn, chứa nhiều dữ liệu quan trọng, càng đổi thường xuyên càng tốt.

1. để lộ pass hay lưu ở dạng không mã hóa trong tập tin, sơ hở trong việc khởi tạo thông tin bảo mật của họ

theo thống kê có tới 50% vụ đánh cắp tài khoản do những người thân lân cận, gần gũi với nạn nhân và đã nhắm đến nạn nhân trong một khoảng thời gian dài trước đó.

1. .Sở hở trong việc sử dụng hệ thống mật khẩu được lưu sẵn trong máy hoặc kho password
2. mọi người có xu hướng sử dụng các từ phổ biến và password ngắn, cũng như có liên quan tới thông tin cá nhân, gia đình... Hay những công ty, tổ chức thường đặt password theo một format xác định
3. do tính tò mò hoặc tham lam

-**MD5** (viết tắt của từ**Message- Digest algorithm 5**, giải thuật tiêu hóa tin 5) là một hàm băm mật mã theo chuẩn RFC 1321, có giá trị hash dài 128bit.

-Bạn có thể hình dung, bạn có 2 bộ dữ liệu và cần so sánh xem chúng có hoàn toàn giống nhau không, nếu không có MD5, bạn sẽ phải so sánh dữ liệu thô của 2 bộ dữ liệu đó. MD5 không làm vậy, nó tạo ra một checksum trên 2 bộ dữ liệu rồi so sánh checksum này để quyết định xem 2 bộ dữ liệu có giống nhau không.

-checksum: là tổng kiểm tra, \_là 1 giá trị đc tạo ra từ thuật toán hàm băm mật mã , thuật toán này có thể chạy trên 1 đoạn dl, như 1 tệp riêng lẻ, hay mất khẩu.

Vd: [Microsoft File Checksum Integrity Verifier](https://vi.eyewated.com/cach-tai-xuong-va-cai-djat-trinh-kiem-tra-tinh-toan-ven-cua-tep-kiem-tra-fciv/) [(FCIV)](https://vi.eyewated.com/cach-tai-xuong-va-cai-djat-trinh-kiem-tra-tinh-toan-ven-cua-tep-kiem-tra-fciv/)

-> hack cơ đã làm gì.? Sd hàm rainbow( bảng cầu vồng) là một danh ѕách chứa các giá trị haѕh có ѕố lượng mật khẩu ứng ᴠới ѕố lượng ký tự nào đó. Sử dụngRainboᴡ Table, bạn có thể lấу một cách đơn giản giá trị haѕh được trích rút từ máу tính mục tiêu ᴠà thực hiện một tìm kiếm. Khi giá trị haѕh được tìm thấу trong bảng, bạn ѕẽ có mật khẩu.

-Backdoor (cửa hậu) trong phần mềm hay hệ thống máy tính thường là một cổng không được thông báo rộng rãi, cho phép người quản trị xâm nhập hệ thống để tìm nguyên nhân gây lỗi hoặc bảo dưỡng. Ngoài ra nó cũng dùng để chỉ cổng bí mật mà hacker và gián điệp dùng để truy cập bất hợp pháp.

-Backdoor trong thuật ngữ khoa học máy tính là cách kẻ xâm nhập có thể truy cập vào hệ thống mà không cần thông qua tuyến đường đã được bảo mật. Vì hệ thống bảo mật của máy tính không thể nhìn thấy các backdoor nên nạn nhân có thể không nhận ra máy tính của mình đã xuất hiện lỗ hổng nguy hiểm này.

Hash là đưa 1 gtrij đầu vào -> 1 gtri đầu ra, nhưng gtri đầu ra kb gtri đầu vào

-brute-force: sd hàm hash\_salt

A drawing of a house

Description automatically generated with low confidence

-**SQL Injection** là một kỹ thuật lợi dụng những lỗ hổng về câu truy vấn của các ứng dụng. Được thực hiện bằng cách chèn thêm một đoạn [SQL](https://topdev.vn/blog/sql-la-gi/) để làm sai lệnh đi câu truy vấn ban đầu, từ đó có thể khai thác dữ liệu từ database. **SQL injection** có thể cho phép những kẻ tấn công thực hiện các thao tác như một người quản trị web, trên cơ sở dữ liệu của ứng dụng.

SQL (Structured Query Language)

Ví dụ, trong form đăng nhập, người dùng nhập dữ liệu,