**Bài 2.1**

1. **Phân biệt **Dictionary attack** và **Brute-force attack.****

|  |  |  |
| --- | --- | --- |
| **Tiêu chí** | **Tấn công từ điển (Dictionary attack)** | **Tấn công vét cạn (Brute-force attack)** |
| **Cách thức** | Hacker dùng một danh sách sẵn có các mật khẩu phổ biến (dictionary wordlist) để thử lần lượt. | Hacker thử tất cả các khả năng có thể (chữ, số, ký tự đặc biệt) cho đến khi tìm được mật khẩu đúng. |
| **Hiệu quả** | Nhanh hơn vì chỉ thử những mật khẩu có khả năng cao (dựa trên thói quen người dùng). | Chậm hơn nhiều vì phải kiểm tra mọi khả năng có thể. |
| **Khả năng thành công** | Phụ thuộc vào việc người dùng đặt mật khẩu có nằm trong danh sách từ điển hay không. | Gần như chắc chắn thành công nếu đủ thời gian và tài nguyên (nhưng rất tốn kém). |
| **Ví dụ** | Thử các mật khẩu như 123456, password, admin, qwerty... | Thử tất cả các tổ hợp từ a, aa, ab, abc, a1b2c3!... cho đến khi tìm được. |

1. **Ví dụ về phòng chống trên **máy chủ****
   1. **Đối phó với **Dictionary attack****

**- **Biện pháp**:** Yêu cầu mật khẩu mạnh.

+ Bắt buộc mật khẩu phải có độ dài tối thiểu (ví dụ 10–12 ký tự).

+ Yêu cầu kết hợp chữ hoa, chữ thường, số, ký tự đặc biệt.

+ Kiểm tra mật khẩu không nằm trong danh sách mật khẩu phổ biến (banned password list).

**- Ví dụ cụ thể:** Trong hệ thống đăng ký, khi người dùng đặt mật khẩu 123456, server sẽ trả về lỗi:

"Mật khẩu quá phổ biến, vui lòng chọn mật khẩu mạnh hơn."

Điều này giúp vô hiệu hóa hầu hết dictionary attack.

* 1. **Đối phó với **Brute-force attack****

**- **Biện pháp**:** Giới hạn số lần đăng nhập sai.

+ Khóa tài khoản tạm thời sau 5 lần đăng nhập sai liên tiếp.

+ Thêm cơ chế **CAPTCHA** khi nghi ngờ hành vi tự động.

+ Dùng **rate limiting** (giới hạn tần suất request từ một IP).

****- Ví dụ cụ thể:**** Nếu hacker thử 10 lần đăng nhập sai trong 1 phút, server sẽ:

+ Khóa tài khoản trong 15 phút, **hoặc**

+ Bắt buộc người dùng giải CAPTCHA để tiếp tục.

Điều này khiến brute-force trở nên cực kỳ tốn thời gian, gần như không khả thi.