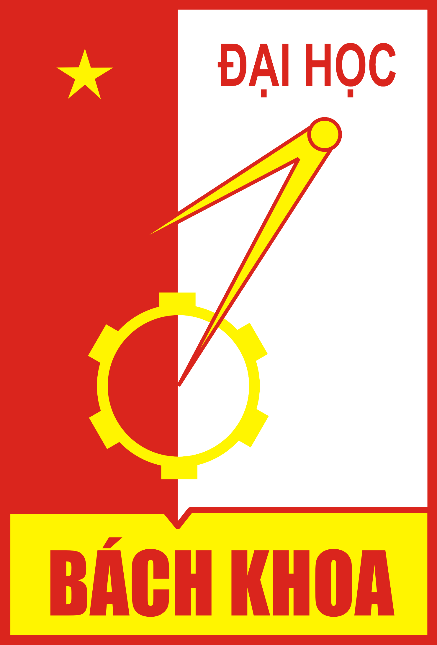
**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**Viện Công nghệ Thông tin và Truyền thông**



**BÁO CÁO BÀI TẬP LỚN**

Môn học**: An ninh mạng**

Đề tài: **10 - Tìm hiểu tấn công DoS/DDos trong mạng và**

**cách thức phòng chống.**

Giảng viên hướng dẫn: **ThS.** **Bùi Trọng Tùng**

Lớp: **LTU15**

Nhóm: **6**

Thành viên: Nguyễn Đức Thiên - MSSV 20168806

Vũ Hoàng Đức Hiếu - MSSV 20168199

Nguyễn Hoàng Nhung - MSSV 20168399

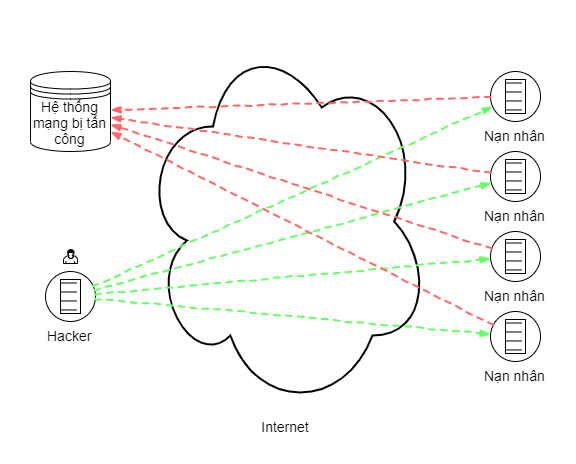
1. Định nghĩa
2. Tấn công từ chối dịch vụ.

* Tấn công từ chối dịch vụ, Denial of Service attack viết tắt là DoS hoặc DoS attack.
* DoS là một dạng tấn công mạng mà mục tiêu chính là làm cho hệ thống bị tấn công không thể phản hồi lại các yêu cầu truy cập vào một tài nguyên hệ thống.
* Một cuộc tấn công DoS nhằm mục đích ngăn chặn đối với người dung hợp lệ được cấp quyền hoặc uỷ quyền truy cập vào tài nguyên hệ thống, hoặc trì hoãn các hoạt động, chức năng của hệ thống.
* Kẻ tấn công DoS sẽ nỗ lực để làm cho tài nguyên hệ thống không có sẵn cho người dùng, thông thường mục tiêu sẽ là các máy chủ server web cấu hình cao, nơi cuộc tấn công sẽ khiến cho người dùng không thể truy cập trang web mong muốn.

1. Hệ thống phân tán Tấn công từ chối dịch vụ.

* Hệ phân tán Tấn công từ chối dịch vụ, Distributed Denial of Service attack được viết tắt là DDoS hoặc DDoS attack.
* Sự tấn công DoS từ nhiều máy tính hoặc một hệ thống khác với mục tiêu là một hệ thống mạng hoặc server web, gây ra một lưu lượng truy cập lớn hơn sức tải của hệ thống mạng, đến mức làm nghẽn các hoạt động của người dùng hợp lệ được gọi là một cuộc tấn công DDoS
* Kẻ tấn công có thể sử dụng bất kỳ máy tính nào khác bằng việc lợi dụng các lỗ hổng bảo mật hoặc điểm yếu trên máy tính, từ đó chiếm quyền kiểm soát. Sau đó kẻ tấn công có thể bắt máy tính của bạn phải gửi hàng loạt yêu cầu truy cập, hoặc dữ liệu lớn, tới mục tiêu ở đây là một hệ thống mạng hoặc server web khác.
* Cuộc tấn công được thêm từ "Distributed - Phân tán" bởi vì nó không thực hiện từ một máy tính nào mà được "phân tán" ra các máy tính bị chiếm quyền kiểm soát. Mỗi máy tính bị chiếm quyền kiểm soát được gọi là 1 máy bot và hệ thống các máy này được gọi là botnet.

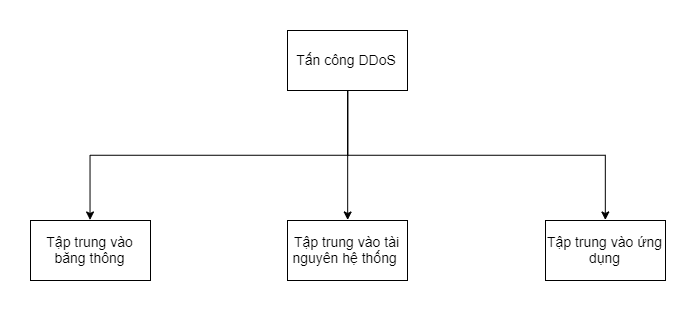
Sơ đồ hệ thống botnet:



Hình 1: Mô hình DDoS

2. Phân loại DoS và DDoS.

Có rất nhiều cách thức và phương pháp để phân loại DoS cũng như DDos. Trong đó thường được sử dụng và biết đến nhất là phân loại DDoS theo mục tiêu của cuộc tấn công. Có 3 mục tiêu chính thường bị kẻ tấn công nhắm tới là băng thông, tài nguyên hệ thống và tầng ứng dụng.



Hình 2: Phân loại DDoS theo mục tiêu

4.1 Tấn công tập trung vào băng thông:

- Loại tấn công này tạo ra tắc nghẽn bằng cách cố gắng tiêu thụ hết tất cả băng thông mạng có sẵn giữa mục tiêu và Internet. Một lượng lớn dữ liệu được gửi đến bằng cách khuếch đại hoặc tạo lưu lượng lớn bằng botnet.

Cũng gọi tấn công thể tích. Loại tấn công này cố gắng tạo ra tắc nghẽn bằng cách tiêu thụ tất cả băng thông có sẵn giữa mục tiêu và Internet lớn hơn (Dung lượng trung bình băng thông của liên kết mạng kết nối với máy chủ). Một lượng lớn dữ liệu được gửi đến mục tiêu bằng cách sử dụng một hình thức khuếch đại hoặc một phương tiện khác để tạo lưu lượng lớn, chẳng hạn như các yêu cầu từ botnet.

Thông thường, băng thông máy chủ nhỏ hơn băng thông ISP (nhà cung cấp dịch vụ Internet). Vì vậy, luôn luôn có thể liên kết máy chủ thành công, nó dẫn đến dịch vụ không tồn tại cho (một số) người dùng hợp pháp.

      Trong tấn công thể tích, kiểu tấn công phổ biến nhất là lũ lụt. Có một số ví dụ: