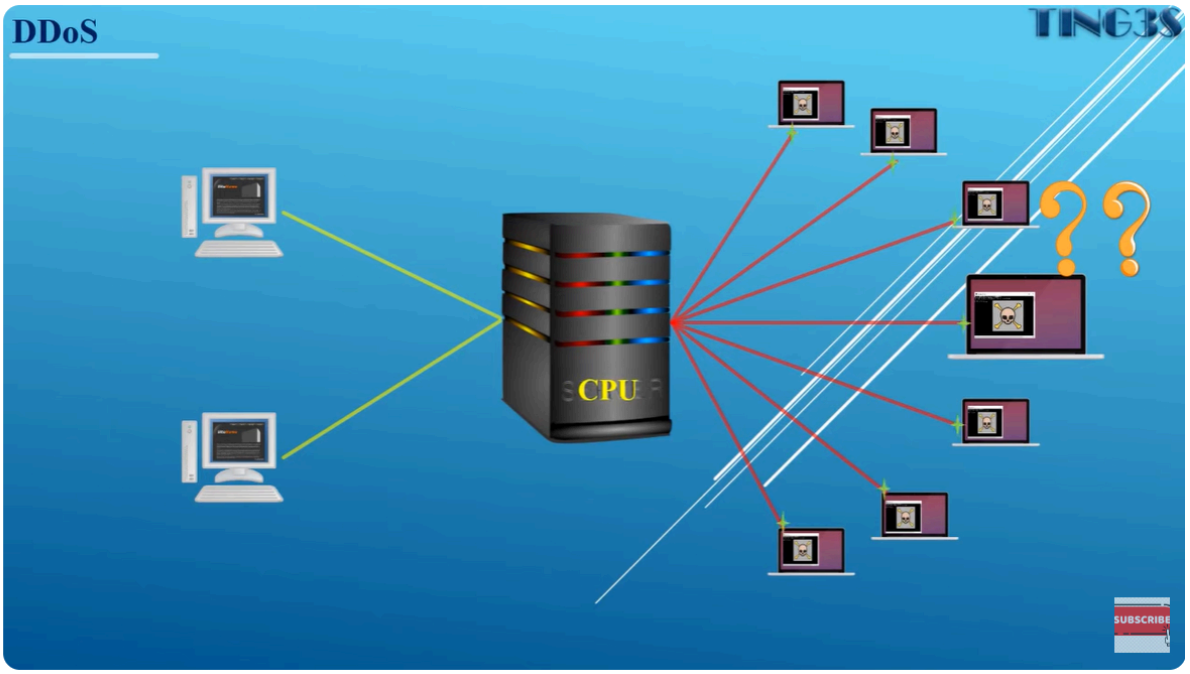
Phần 1 : Tổng quan về DDOS

I . Cơ sở lý thuyết.

1.Khái niệm.

Tấn công từ chối dịch vụ phân tán (Distributed Denial of Service) nhìn ở hai khía cạnh:

- Thứ nhất nó là loại tấn công từ chối dịch vụ -> làm tắc nghẽn băng thông hoặc cạn kiệt tài nguyên , dẫn đến bị gián đoạn hoặc ngừng các dịch vụ .
- Thứ hai là phân tán -> nó huy động rất nhiều các máy khác nhau bị nó chiếm quyền kiểm soát (gọi là các con zombie) tấn công máy nạn nhân.



2.Các giai đoạn tấn công chung.

a.Giai đoạn chuẩn bị :

Chuẩn bị công cụ cho cuộc tấn công ,ban đầu hacker sẽ tiến hành viết các mã độc hoặc các chương trình độc hại , sau đó lừa người dùng có thể là click vào một link quảng cáo nào đấy có chứa các mã độc này,lúc này các máy tính sẽ bị hacker xâm nhập và kiểm soát , thường người dùng sẽ không biết, sau đó cài đặt các automated agents(chương trình tấn công tự động) để gửi các yêu cầu giả mạo. Kết thúc giai đoạn này, hacker sẽ có một attack- network (một mạng các máy tính ma phục vụ cho việc tấn công DDoS).

b. Giai đoạn xác định mục tiêu và thời điểm tấn công:

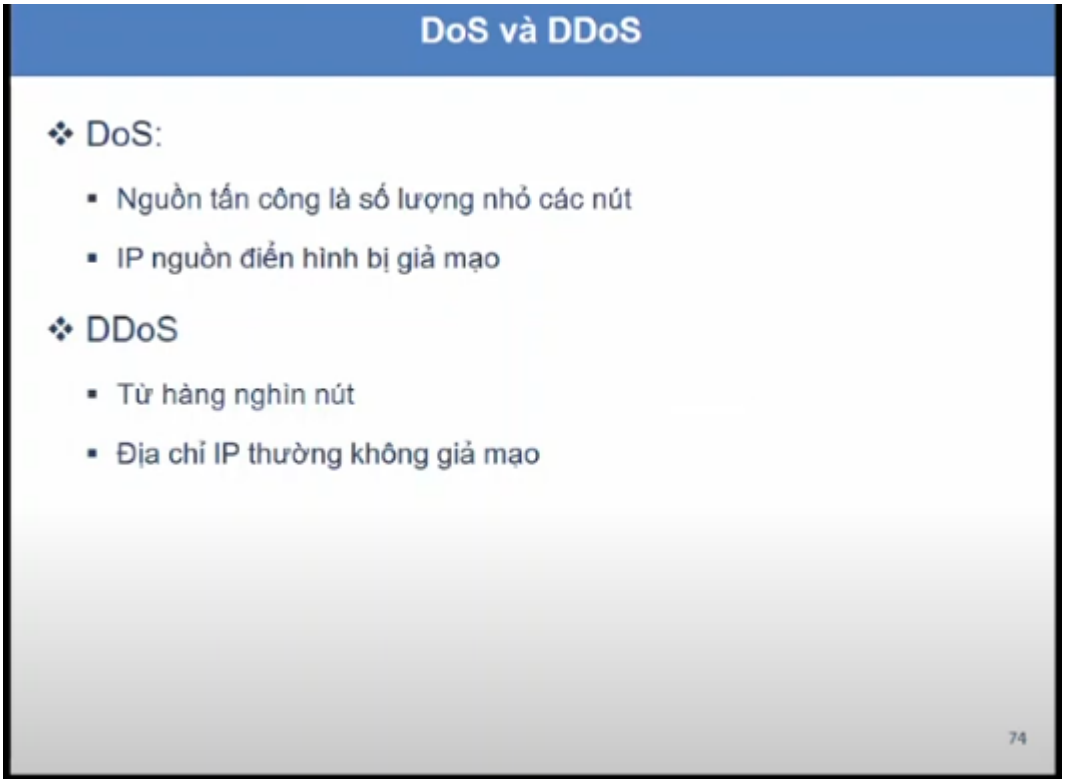
Sau khi xác định được mục tiêu cần tấn công, hacker sẽ điều chỉnh attack-network chuyển hướng tấn công mục tiêu đó .Yếu tố thời điểm sẽ quyết định mức độ thiệt hại của cuộc tấn công. Vì vậy, nó phải được hacker ấn định trước.

Ví dụ : Hacker thường nhằm vào các trang có lưu lượng truy cập cao ví dụ như thương mại điện tử , chọn những thời điểm vàng (sale chẳng hạn) để tấn công làm sập web .

c. Giai đoạn tấn công và xóa dấu vết :

Đúng thời điểm đã định trước, hacker phát động lệnh tấn công từ máy của mình. Toàn bộ attack- network (có thể lên đến hàng ngàn, hàng vạn máy) đồng loạt tấn công mục tiêu, mục tiêu sẽ nhanh chóng bị cạn kiệt băng thông và không thể tiếp tục hoạt động. Sau một khoảng thời gian tấn công, hacker tiến hành xóa dấu vết có thể truy ngược đến mình, việc này đòi hỏi trình độ cao của những hacker chuyên nghiệp.

3.So Sánh Với DOS.



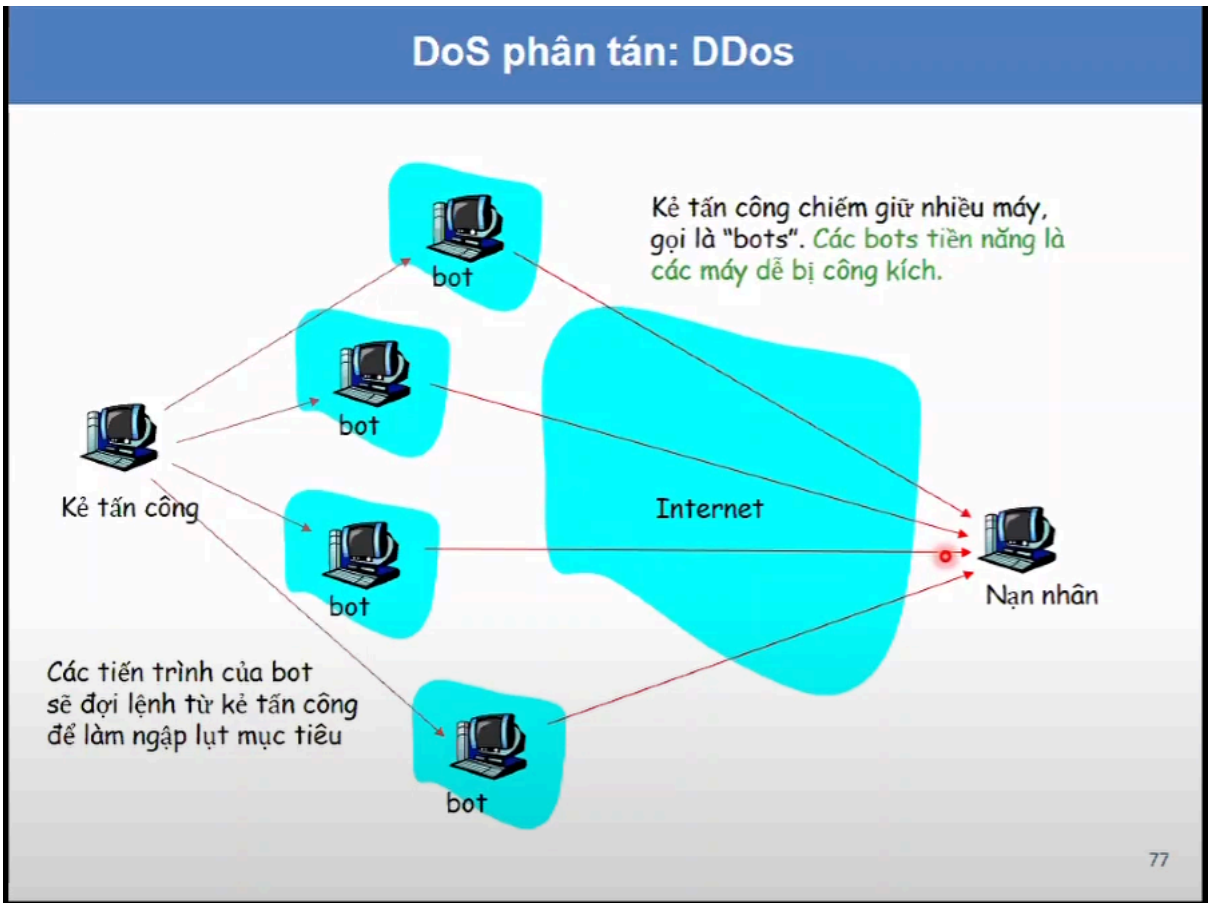
Bởi vì DDos đã lợi dụng được mạng máy tính ma nên nó cũng không cần phải giả mạo địa chỉ làm gì , vì chính những máy tính ma này là máy tính có IP hợp pháp , nhưng nó bị các hacker lợi dụng . Và ta cũng không thể nào ngăn chặn được IP này vì có quá nhiều nút , khi chặn một IP sẽ vô hình dung chặn đường truyền những người dùng hợp pháp khác , ví dụ như trường mình có khoảng 20 cái IP public ra ngoài , dùng chung cho tất cả các máy , hay nhà chúng ta có khoảng 10 cái máy dùng chung 1 IP public ra ngoài ,nhưng nếu 1 trong số đó bị nhiễm mã độc , chặn IP này sẽ làm chặn đến máy khác làm ảnh hưởng đến lưu lượng truy cập hệ thống , cho nên rất khó ngăn chặn kiểu tấn công này.

II. Các dạng tấn công.

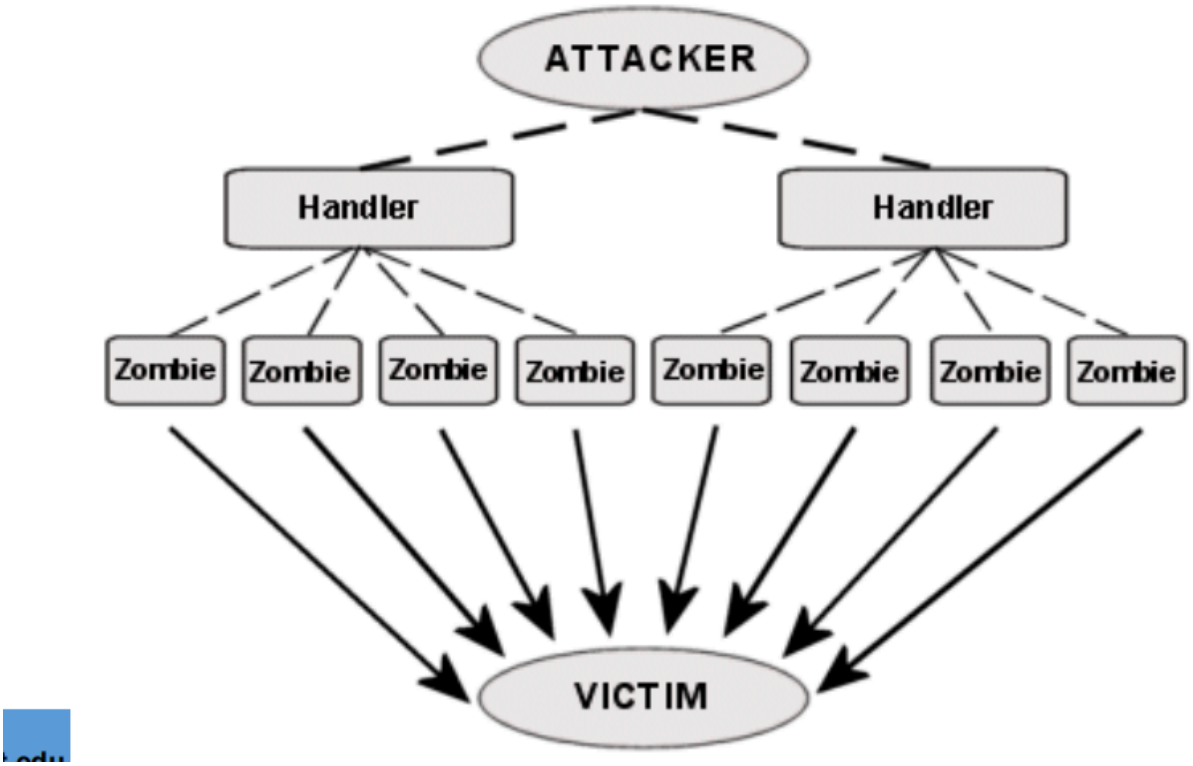
1.Theo kiến trúc tấn công.

a. Tấn công DDOS trực tiếp.

ĐƯA hai ảnh này vào slide thôi



Architecture of a DDoS Attack

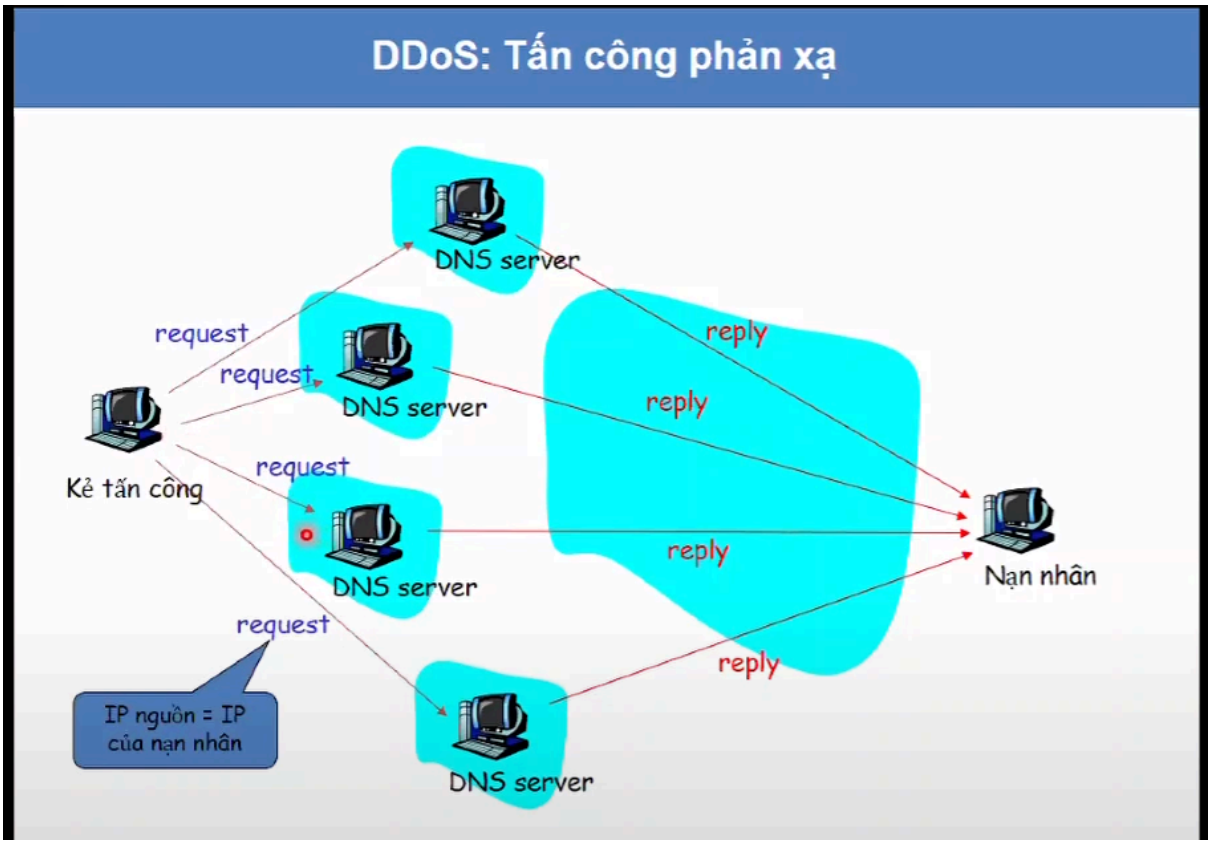


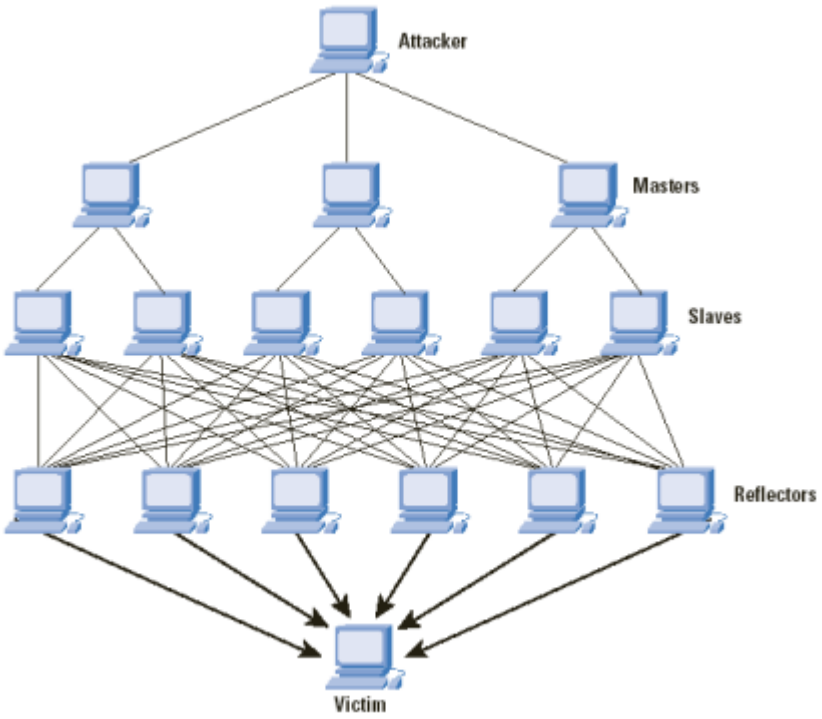
- Như đã nói ở các giai đoạn tấn công chung , kẻ tấn công sẽ dùng các mã độc để lừa người dùng kick vào và chiếm quyền điều khiển, tạo nên mạng máy tính ma (botnet/ zombie) , sau đó cài đặt các chương trình tấn công , spam tự động để gửi các yêu cầu giải mạo đến máy nạn nhân, lượng yêu cầu giả mạo này rất lớn và từ nhiều nguồn nên rất khó đối phó.

- Điều quan trọng ở đây là nó sẽ dùng các handler là kênh giao tiếp trung gian giữa kẻ tấn công và các botnet , chúng sử dụng các dịch vụ như HTTP(http request/ response) để gửi lệnh tấn công đến các botnet hoặc nhận dữ liệu từ botnet về kẻ tấn công

b. Tấn công DDOS gián tiếp/ phản xạ (Reflective).

Chỉ đưa hai ảnh vào thôi





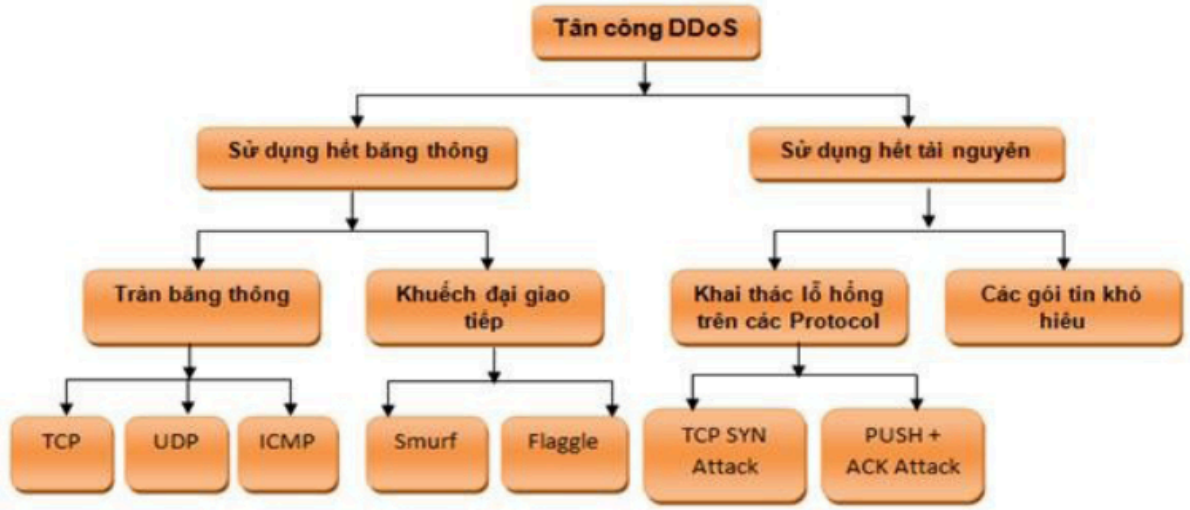
- Về cơ bản thì những tầng bên trên tương tự như tấn công trực tiếp , có điều đến tầng Reflectors , các con zombies (tầng slaves) sẽ gửi yêu cầu request đến tầng Reflectors (các máy này đang hoạt động bình thường và chưa bị mất quyền kiểm soát) . sau đó các Reflectors sẽ Response các phản hồi quay ngược trở lại , mấu chốt là các Slaves này sẽ Fake cái địa chỉ IP này về IP của nạn nhân , và tất cả các response này sẽ tập trung dồn về máy nạn nhân.

- Các Reflectors này thường là một server có hệ thống rất lớn (DNS SERVER) bị lợi dụng để làm máy nạn nhân cạn kiệt tài nguyên hoặc băng thông , những máy này vẫn chưa bị các hacker xâm nhập và điều khiển.

- Loại tấn công này khó ngăn chặn hơn so với ban đầu rất nhiều bởi tính phân tầng phức tạp.

2. Theo mục đích tấn công.

cho ảnh này vào thôi



a.Tấn công làm tắc nghẽn băng thông :

- Mục tiêu: Mục đích chính của tấn công DDoS là làm cho dịch vụ trực tuyến không thể truy cập được bằng cách làm đầy băng thông của mạng hoặc làm quá tải các máy chủ.

- Phương pháp: Trong một cuộc tấn công DDoS, một lượng lớn các yêu cầu được gửi đến một máy chủ hoặc một hệ thống mạng từ các máy tính hoặc thiết bị đang được kiểm soát bởi kẻ tấn công. Điều này tạo ra một lượng lớn lưu lượng mạng hoặc các yêu cầu đối với máy chủ, làm cho nó không thể xử lý tất cả các yêu cầu từ người dùng hợp lệ, dẫn đến việc dịch vụ trở nên không khả dụng cho người dùng chính thức.

- Ví dụ :Tấn công DDoS nhằm vào một trang web bán lẻ lớn.Kẻ tấn công sử dụng một mạng lưới botnet để gửi một lượng lớn yêu cầu truy cập đến trang web đó từ hàng nghìn hoặc thậm chí hàng triệu máy tính zombie. Các yêu cầu này có thể là các yêu cầu HTTP(gửi/ nhận) .Bằng cách làm đầy băng thông của máy chủ hoặc hạ tầng mạng, trang web sẽ trở nên không thể truy cập được cho người dùng bình thường.

b.Tấn công làm cạn kiệt tài nguyên.

- Mục tiêu: Mục tiêu của tấn công tắc nghẽn tài nguyên là làm cho tài nguyên của một hệ thống bị cạn kiệt hoặc làm quá tải, thường là tài nguyên hệ thống như CPU, bộ nhớ, hoặc các tài nguyên khác.

- Phương pháp: Trong tấn công tắc nghẽn tài nguyên, kẻ tấn công tập trung vào việc sử dụng hoặc làm cạn kiệt tài nguyên quan trọng của một hệ thống bằng cách gửi yêu cầu hoặc thực hiện các hành động mà tiêu tốn nhiều tài nguyên.

- Ví dụ ,tấn công tắc nghẽn CPU nhằm vào một dịch vụ trực tuyến quan trọng, kẻ tấn công tạo ra một chương trình độc hại hoặc sử dụng các công cụ tự động để tạo ra một lượng lớn yêu cầu đến dịch vụ mục tiêu, mỗi yêu cầu yêu cầu một lượng tính toán đáng kể. Ví dụ, trong một tấn công tắc nghẽn CPU, kẻ tấn công có thể gửi các

yêu cầu phức tạp yêu cầu xử lý tính toán nhiều từ các hệ thống như máy chủ hoặc ứng dụng web. Do việc tài nguyên CPU bị cạn kiệt, dịch vụ sẽ trở nên chậm hoặc không thể truy cập được cho người dùng bình thường.

III . Phòng chống DDos .

Cần kết hợp nhiều phương pháp và sự phối hợp của nhiều bên , ví dụ như bên máy nạn nhân và các botnet .

- Không để hệ thống trở thành bot:
  - + Nâng cấp router, tường lửa để lọc các yêu cầu điều khiển của kẻ tấn công
  - + Cập nhật bản vá
  - + Phần mềm quét virus , phát hiện bất thường
  - + Hệ thống ngăn chặn xâm nhập trái phép
- Đối với máy nạn nhân :
  - + Sử dụng hệ thống giám sát phát hiện DDos.
  - + Sử dụng tường lửa để chặn cổng dịch vụ bị tấn công.
  - + Dự phòng tài nguyên lớn (tăng băng thông , nâng ram , cpu)
  - + Giới hạn gói tin truyền đến (ví dụ có cái trò khi đăng nhập ấy , ta chỉ được đăng nhập bao nhiêu lần trên bao nhiêu phút , sau đó phải chờ bao lâu mới được đăng nhập lại , hoặc thậm chí nhiều quá sẽ bị chặn , mục đích để chống các trường hợp gửi quá nhiều yêu cầu trong 1 thời gian làm tắc nghẽn băng thông)