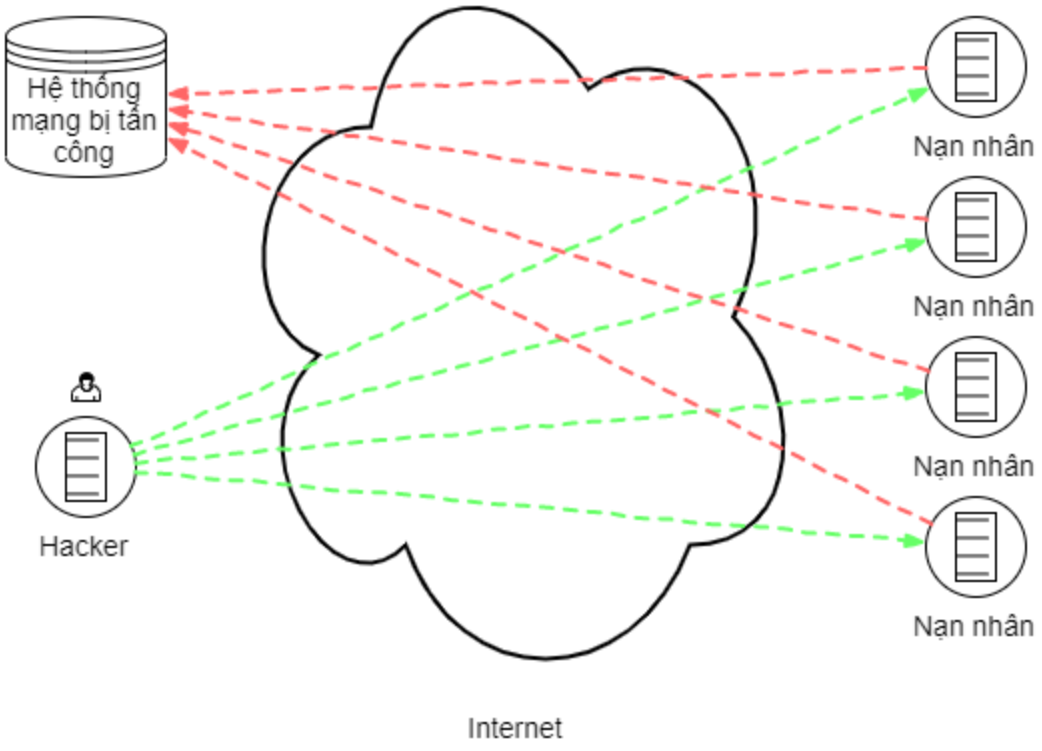
Báo cáo An ninh mạng LTU15 - đề tài 10: tấn công ddos

I. Định nghĩa

1. 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.

2. 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:

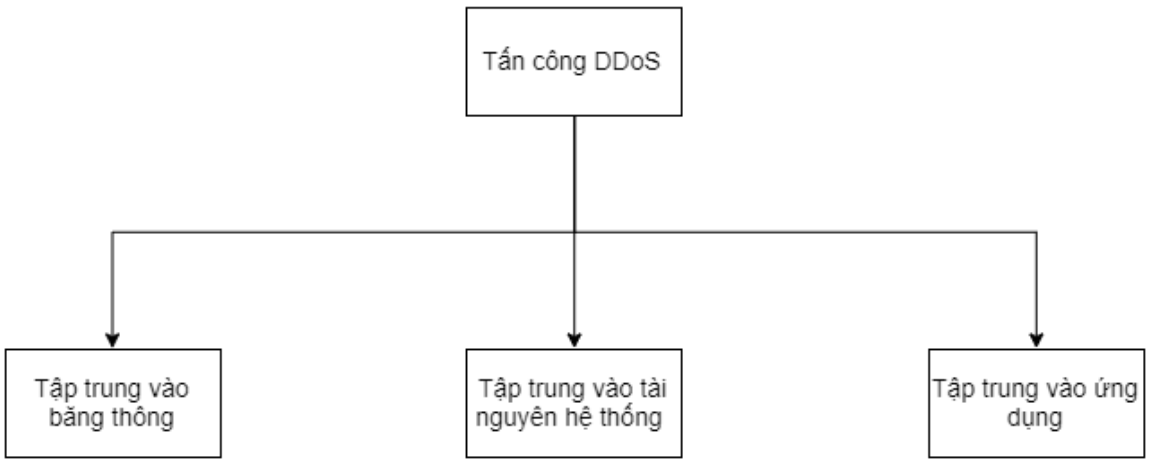


Hình 1: Mô hình DDoS

3. Một vài cuộc tấn công DDoS nổi tiếng:
   - GITHUB: 1.35 TB/s. Vào ngày 28/2/2018, nền tảng Github - một nền tảng phổ biến để lưu trữ code của lập trình viên - đã bị tấn công với lưu lượng truy cập lên tới 1,35 TB/s.
   - Occupy Central Hongkong: 500 GB/s. Vụ tấn công này xảy ra năm 2014, với mục tiêu là hệ thống bỏ phiếu online của cuộc Cách Mạng Dù tại Hồng Kông. Được ghi nhận đỉnh điểm lưu lượng truy cập lên tới 500 GB/s, kéo dài tới hơn 15 phút và lặp lại mỗi vài giờ. Các gói tin được nguỵ trang với lưu lượng hợp lệ được gửi từ không chỉ một hay hai botnet mà năm botnet.
   - CloudFlare: 400 GB/s. Cũng vào năm 2014, hệ thống cung cấp dịch vụ bảo mật mạng và phân phối nội dung CloudFlare bị tấn công bởi một kỹ thuật gọi là "reflection - phản xạ". Kẻ tấn công sử dụng một loạt địa chỉ nguồn giả mạo để gửi số lượng lớn các yêu cầu tới máy chủ NTP (Network Time Protocol) và có khả năng phản xạ và khuếch đại gói phản hồi. Một máy tính bị hack với băng thông 1Gbps có thể phản xạ và khuếch đại lên tới 200Gbps.
   - United States Banks: 60GB/s. Năm 2012, không chỉ một hay hai mà là cả 6 ngân hàng thuộc hệ thống Ngân hàng Hoa Kỳ đã bị tấn công bởi một chuỗi liên tiếp các cuộc tấn công DDoS. Kẻ tấn công đã sử dụng hàng trăm máy chủ bị nhiễm mã độc để gửi số lượng cực lớn các gói tin gây quá tải, lên tới 60GB/s.

4. 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: