1. Tìm hiểu về DoS

1.1 DoS là gì?

Đây là một thuật ngữ công nghệ, viết tắt của Denial of Service, có nghĩa là từ chối dịch vụ. Tấn công từ chối dịch vụ là một hình thức tấn công mạng nhằm làm cho một hệ thống (hoặc máy chủ) trở nên không khả dụng bằng cách gửi một lượng lớn yêu cầu vượt quá khả năng xử lý của hệ thống đó. Tin tặc thực hiện DoS bằng cách gửi các yêu cầu đến hệ thống mục tiêu, tạo áp lực lớn lên tài nguyên như băng thông, CPU, hoặc bộ nhớ. Điều này dẫn đến việc hệ thống không thể phản hồi yêu cầu từ người dùng, gây ra sự chậm trễ hoặc ngừng hoạt động hoàn toàn.

Trong một cuộc tấn công DoS, tin tặc thường sử dụng nhiều phương pháp lên hệ thống mục tiêu, bao gồm một số phương pháp phổ biến sau:

1.1.1 Ping Floods: Tin tặc gửi một lượng lớn gói tin ping tới một máy chủ, làm cho máy chủ phải xử lý và phản hồi một cách không hiệu quả.

1.1.2 SYN Floods: Tin tặc gửi các yêu cầu kết nối TCP mà không hoàn thành việc thiết lập kết nối, chiếm hết tài nguyên kết nối TCP của máy chủ.

1.1.3 HTTP Floods: Gửi một lượng lớn yêu cầu HTTP đến một máy chủ web, gây ra hiện tượng quá tải và khiến cho máy chủ không thể phản hồi các yêu cầu từ người dùng hợp pháp.

1.1.4 Smurf Attacks: Tin tặc gửi gói tin ICMP (Internet Control Message Protocol) với địa chỉ nguồn được làm giả, khiến cho các máy chủ trong mạng phản hồi tới một địa chỉ không tồn tại, tạo ra một lượng lớn thông tin phản hồi không mong muốn.

Sau khi bị tấn công DoS, hệ thống sẽ trở nên không còn khả dụng, gây thiệt hại nghiêm trọng đến hoạt động kinh doanh và uy tín của tổ chức hoặc doanh nghiệp bị tấn công.

1.2 Mục đích của các cuộc tấn công DoS

Đối tượng tấn công của DoS luôn rất đa dạng, nhưng chủ yếu đều tập trung vào hệ thống máy chủ của các tổ chức, doanh nghiệp hay Chính phủ. Mục đích của DoS thường sẽ như sau:

1.2.1 Gây gián đoạn và làm giảm hiệu suất: Cuộc tấn công DoS đều làm cho hệ thống hay dịch vụ trở nên không thể sử dụng được đối với người dùng. Việc này gây ra sự gián đoạn, chậm trễ và ngừng hoạt động, làm suy giảm hiệu suất của hệ thống bị tấn công.

1.2.2 Đe doạ tiền chuộc: Tin tặc thực hiện tấn công DoS để đe dọa và ép doanh nghiệp phải trả tiền để khôi phục hoạt động bình thường của hệ thống.

1.2.3 **Tác động đến hoạt động kinh doanh và uy tín:** Các trang web thương mại điện tử, dịch vụ giao dịch trực tuyến, hay các tổ chức kinh doanh trực tuyến đều có thể trở thành đối tượng của DoS, làm ảnh hưởng nghiêm trọng đến doanh số bán hàng và uy tín của họ.

1.2.4 Tấn công hệ thống Chính phủ hoặc tổ chức lớn: Đối với các tổ chức Chính phủ, DoS có thể được sử dụng như một phương tiện chiến tranh mạng để làm quá tải hệ thống của đối thủ.

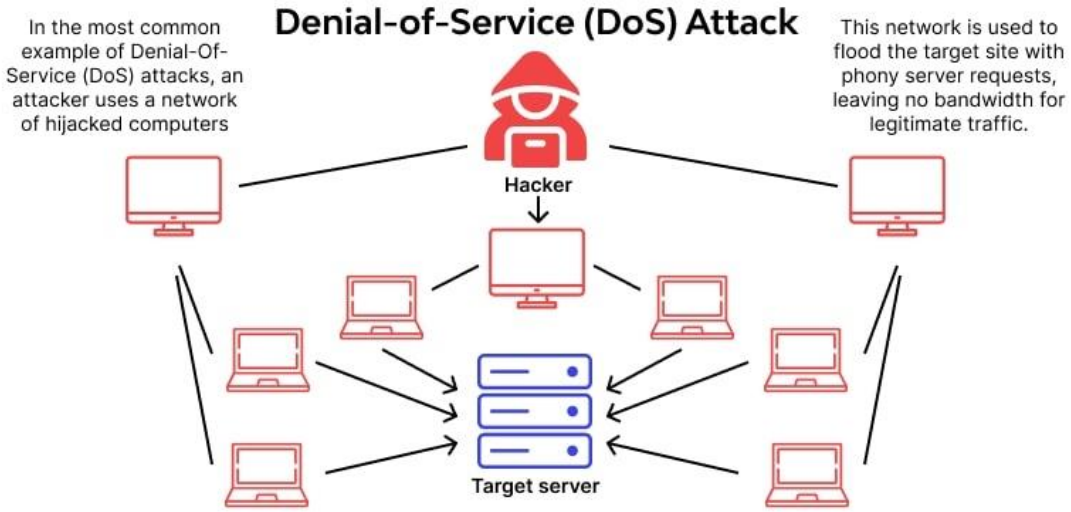
1.2.5 Tạo điều kiện cho các hành động khác: Cuộc tấn công DoS thường tạo cơ hội cho tin tặc thực hiện các hành động xấu khác như xâm nhập vào hệ thống, lợi dụng sự chậm trễ để truy cập thông tin quan trọng, thậm chí là xoá đi dữ liệu.

1.2.6 Thử nghiệm và nghiên cứu: Một số cá nhân có thể tiến hành các cuộc tấn công DoS như một cách thử nghiệm, để hiểu rõ hơn về cách thức hoạt động của hệ thống, kiểm tra tính ổn định và xác định các lỗ hổng bảo mật.

Vì những lí do trên, tin tặc đã thực hiện tấn công từ chối dịch vụ - DoS, và gây ra nhiều ảnh hưởng nghiêm trọng đến hoạt động hay độ uy tín của các tổ chức, doanh nghiệp chịu sự tấn công này.

1.3 Cách hoạt động của DoS

Bước đầu tiên của cuộc tấn công DoS là lựa chọn mục tiêu, thường là máy chủ hoặc dịch vụ trực tuyến. Sau đó, tin tặc sẽ sử dụng các phương tiện như botnet (một mạng các máy tính bị nhiễm malware) để tạo ra lưu lượng truy cập giả mạo đến mục tiêu.



Quá trình tấn công diễn ra khi tin tặc gửi liên tục lưu lượng truy cập giả mạo đến hệ thống hoặc máy chủ. Khi lưu lượng truy cập giả mạo đổ vào hệ thống, nó tạo ra tình trạng quá tải, khiến cho hệ thống không thể xử lý được và dịch vụ trở nên không khả dụng. Tình trạng quá tải này có thể kéo dài từ vài giây đến nhiều ngày liền. Khi cuộc tấn công kết thúc, dịch vụ trực tuyến có thể được khôi phục, nhưng sẽ để lại hậu quả nghiêm trọng đối với doanh nghiệp, tổ chức chịu cuộc tấn công từ chối dịch vụ này.

1.4 Tác hại của DoS

Tác hại của tấn công từ chối dịch vụ DoS là rất lớn và có tác động đáng kể đến các tổ chức và hệ thống mạng:

1.4.1 Sập hệ thống và máy chủ: Cuộc tấn công DoS có thể làm sập hoặc làm gián đoạn hoạt động của hệ thống và máy chủ, dẫn đến việc người dùng không thể truy cập vào dịch vụ hoặc tài nguyên.

1.4.2 Thiệt hại tài chính: Các doanh nghiệp chịu ảnh hưởng từ tấn công DoS thường phải tiêu tốn nhiều chi phí để khắc phục sự cố và nâng cấp bảo mật của hệ thống.

1.4.3 **Gián đoạn hoạt động kinh doanh:** DoS gây ra mất kết nối mạng, dẫn đến gián đoạn hoạt động kinh doanh, làm suy giảm hiệu suất làm việc của nhân viên và gây ra nhiều rủi ro liên quan đến việc thực hiện các công việc.

1.4.4 Mất uy tín với khách hàng: Việc không thể truy cập vào website hay dịch vụ trực tuyến có thể làm giảm uy tín của doanh nghiệp trong mắt khách hàng. Nếu sự cố kéo dài, có thể làm doanh nghiệp mất đi lượng khách của mình.

1.4.5 Hình thành lỗ hổng bảo mật: Sau khi bị tấn công, việc tập trung vào việc khôi phục lại trang web và dịch vụ sẽ được ưu tiên. Trong quá trình khôi phục này, hệ thống bảo mật thường bị tạm ngừng hoạt động và các lỗ hổng bảo mật chưa được vá kịp thời, tạo điều kiện thuận lợi cho hacker quay lại tấn công trang web với các phương thức khác.

1.4.6 Thất thoát doanh thu và dữ liệu: Ngoài thiệt hại tài chính trực tiếp, DoS cũng có thể dẫn đến mất mát tiền bạc do không thể thực hiện các giao dịch kinh doanh quan trọng, và còn có thể làm mất các dữ liệu quan trọng của tổ chức.

Nhìn chung, bất kỳ ai cũng đều có thể trở thành nạn nhân của cuộc tấn công từ chối dịch vụ DoS hay DDoS – tấn công từ chối dịch vụ phân tán, và để có thể bảo vệ được hệ thống của mình, các tổ chức hay doanh nghiệp cần phải thực hiện những biện pháp bảo mật hiệu quả, giúp giảm thiểu tối đa tác hại từ DoS.

2. Phân biệt DoS và DDoS

Bên cạnh DoS thì DDoS cũng chính là một hình thức tấn công mạng nguy hiểm mà bạn nên lưu ý tới. Về cơ bản, DoS và DDoS đều là những hình thức tấn công dịch vụ, nhưng DDoS khác ở điểm nó có thể được phân tán từ nhiều dải IP khác nhau, khiến người bị tấn công khó phát hiện để ngăn chặn. Để có thể phân biệt được hai thuật ngữ trên, bạn có thể theo dõi bảng dưới đây:

Đặc điểm	**DoS**	**DDoS**
Tên	Tấn công từ chối dịch vụ.	Tấn công từ chối dịch vụ phân tán.
Số lượng hệ thống tấn công	Chỉ sử dụng một hệ thống để nhắm vào mục tiêu cụ thể.	Sử dụng nhiều hệ thống hoặc một mạng lưới các thiết bị đã bị nhiễm malware để tấn công mục tiêu.
Vị trí gửi gói dữ liệu	Gửi gói tin tới mục tiêu từ một nguồn duy nhất.	Gửi gói tin từ nhiều nguồn khác nhau, có thể từ hàng trăm hoặc thậm chí hàng ngàn địa chỉ IP khác nhau.
Số lượng thiết bị tấn công	Chỉ một thiết bị duy nhất.	Có nhiều thiết bị đồng thời tham gia vào cuộc tấn công.
Tốc độ tấn công	Tốc độ tấn công thấp hơn so với DDoS do tập trung từ một nguồn duy nhất.	Có tốc độ tấn công cao hơn do sử dụng nhiều nguồn tấn công cùng một lúc.
Khả năng bị ngăn chặn	Có thể dễ dàng hơn để phát hiện và ngăn chặn.	Khó khăn hơn để ngăn chặn vì sự phân tán của nhiều nguồn tấn công khác nhau.
Khă năng bị theo dõi	Dễ theo dõi hơn vì số lượng hệ thống tham gia ít hơn.	Khó để theo dõi và xác định nguồn tấn công vì được phân tán từ nhiều nguồn.
Lưu lượng truy cập đến mạng mục tiêu	Gửi lưu lượng truy cập nhất định đến mạng của mục tiêu.	Gửi lưu lượng truy cập lớn đến mạng mục tiêu, gây quá tải và làm ngừng hoạt động hệ thống.
Phương pháp tấn công điển hình	1. Tấn công tràn bộ đệm 2. Tấn công Ping of Death hoặc ICMP flood	1. Tấn công amplification (khuếch đại)

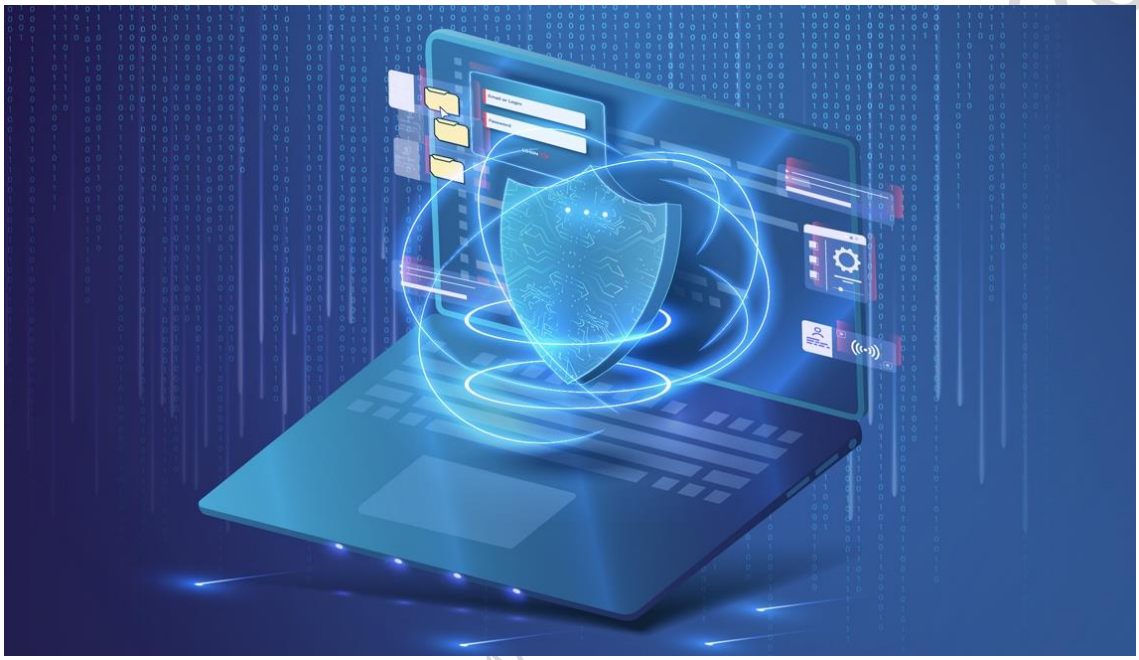
	3. Tấn công Teardrop Attack.	2. Phân mảnh dữ liệu (Fragmentation Attack) 3. Khai thác lỗ hổng trong ứng dụng (Application Layer Attack).

3. Giải pháp phòng chống DoS và DDoS

Sau khi đã tìm hiểu qua tác hại của DoS là gì, cách thức hoạt động của hình thức tấn công từ chối dịch vụ này và phân biệt DoS với DDoS, tiếp theo hãy cùng tham khảo qua một số phương pháp giúp phòng chống tấn công mạng DoS và DDoS:

3.1 Cài đặt và duy trì phần mềm diệt virus

Đảm bảo cài đặt và duy trì phần mềm diệt virus hiện đại để ngăn chặn vi-rút và phần mềm độc hại truyền qua mạng, từ đó giảm thiểu nguy cơ bị lợi dụng để thực hiện các cuộc tấn công.



3.2 Cài đặt tường lửa và cấu hình hạn chế truy cập

Sử dụng tường lửa và cấu hình nó để giới hạn lưu lượng truy cập vào và ra từ máy tính của bạn.

Thiết lập các quy tắc tường lửa chặt chẽ để từ chối hoặc hạn chế lưu lượng truy cập không mong muốn.

3.3 Thực hiện biện pháp bảo mật cho địa chỉ email và bộ lọc thư điện tử

3.3.1 Áp dụng biện pháp bảo mật để không phân phối địa chỉ email một cách rộng rãi, tránh việc tiếp nhận các email từ nguồn không xác định hoặc không tin cậy.

3.3.2 Sử dụng các bộ lọc thư điện tử để quản lý lưu lượng truy cập không mong muốn và ngăn chặn email chứa các đính kèm hay nội dung độc hại.

Về cơ bản, để ngăn chặn toàn bộ DoS và DDoS là điều không thể, nhưng việc thực hiện các phương pháp trên cũng sẽ làm giảm bớt một phần tác hại từ các cuộc tấn công từ chối dịch vụ.