TRUNG TÂM Y TẾ MỸ HÀO

PHƯƠNG ÁN
CHỐNG TẤN CÔNG XÂM NHẬP TỪ XA (DOS, DDOS)
CƠ CHẾ CHỐNG TẤN CÔNG TỪ CHỐI DỊCH VỤ
TRÊN HỆ THỐNG CỦA TRUNG TÂM Y TẾ MỸ HÀO

TRUNG TÂM Y TẾ MỸ HÀO

PHƯƠNG ÁN
CHỐNG TẤN CÔNG XÂM NHẬP TỪ XA (DOS, DDOS) CƠ CHẾ CHỐNG TẤN CÔNG TỪ CHỐI DỊCH VỤ TRÊN HỆ THỐNG CỦA TRUNG TÂM Y TẾ MỸ HÀO

	Người lập	Người xem xét	Người phê duyệt
Họ tên	**Phạm Việt Đức**	**Lê Thị Mai**	**Bùi Quang Trọng**
Ký tên	Đức		
Chức vụ	Nhân viên CNTT	Trưởng phòng Kế hoạch – Nghiệp vụ - Điều dưỡng	Giám đốc
Ngày	18/8/2025	18/8/2025	18/8/2025

Số: 7../QĐ-TTYT Ngày ban hành: 18/8/2025

Đường Hào, tháng 8/2025

PHƯƠNG ÁN CHỐNG TẤN CÔNG XÂM NHẬP TỪ XA (DOS, DDOS) CƠ CHẾ CHỐNG TẤN CÔNG TỪ CHỐI DỊCH VỤ TRÊN HỆ THỐNG CỦA TRUNG TÂM Y TẾ MỸ HÀO

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích:

- Xây dựng phương án cảnh báo và chống tấn công xâm nhập từ xa (DoS, DDoS) và chống tấn công từ chối dịch vụ trên hệ thống thông tin quan trọng của trung tâm, có khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin mạng.

- Đề ra các cơ chế, cảnh báo và phòng ngừa chống tấn công tấn công xâm nhập từ xã (DoS, DDoS) và chống tấn công từ chối dịch vụ đối với các hệ thống máy chủ cung cấp dịch vụ qua Internet của trung tâm.

- Nâng cao năng lực, hiệu quả hoạt động của công nghệ thông tin trong việc ứng cứu sự cố an toàn thông tin trong toàn trung tâm.

- Bảo đảm các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả phương án ứng cứu sự cố tấn công xâm nhập từ xa (DoS, DDoS) và chống tấn công từ chối dịch vụ trên hệ thống máy chủ, Website của trung tâm đảm bảo tuyệt đối an toàn hoạt động liên tục của hệ thống thông tin.

2. Yêu cầu:

- Phải khảo sát, đánh giá hiện trạng hạ tầng công nghệ thông tin đặc biệt là các máy chủ cung cấp dịch vụ, hệ thống Website, phần mềm ứng dụng tại trung tâm để đưa ra các giải pháp hiệu quả nhất nhằm đảm bảo an toàn, an ninh thông tin hệ thống thông tin của trung tâm.

- Cơ chế cảnh báo phải kịp thời, hiệu quả cao nhất đối với hệ thống thông tin của trung tâm.

- Đưa ra các giải pháp cụ thể để phòng chống các cuộc tấn công xâm nhập từ xa (DoS, DDoS) và chống tấn công từ chối dịch vụ nhằm và hệ thông thông tin của trung tâm.

II. KHÁI NIỆM, PHÂN LOẠI VÀ CÁCH THỨC TẤN CÔNG

1. Khái niệm về tấn công DoS, DDoS:

- Tấn công bằng từ chối dịch vụ DoS (Denial of Service) có thể mô tả như hành động ngăn cản những người dùng hợp pháp khả năng truy cập và sử dụng vào một dịch vụ nào đó.

- Nó bao gồm: làm tràn ngập mạng, mất kết nối với dịch vụ, ... mà mục đích cuối cùng là máy chủ (Server) không thể đáp ứng được các yêu cầu sử dụng dịch vụ từ các máy trạm (Client).

2. Phân loại:

Có 2 loại

- Loại 1: Dựa theo đặc điểm của hệ thống bị tấn công: gây quá tải khiến hệ thống mất khả năng phục vụ.

+ Tin tặc gửi rất nhiều yêu cầu dịch vụ, bắt chước như người dùng thực sự yêu cầu đối với hệ thống.

+ Để giải quyết yêu cầu, hệ thống phải tốn tài nguyên (CPU, bộ nhớ, đường truyền, ...). Mà tài nguyên này thì là hữu hạn. Do đó hệ thống sẽ không còn tài nguyên để phục vụ các yêu cầu sau.

+ Hình thức chủ yếu của kiểu này tấn công từ chối dịch vụ phân tán.

- Loại 2 : Làm cho hệ thống bị treo, tê liệt do tấn công vào đặc điểm của hệ thống hoặc lỗi về an toàn thông tin.

+ Tin tặc lợi dụng kẽ hở an toàn thông tin của hệ thống để gửi các yêu cầu hoặc các gói tin không hợp lệ (không đúng theo tiêu chuẩn) một cách cố ý, khiến cho hệ thống bị tấn công khi nhận được yêu cầu hay gói tin này, xử lý không đúng hoặc không theo trình tự đã được thiết kế, dẫn đến sự sụp đổ của chính hệ thống đó.

+ Điển hình là kiểu tấn công Ping of Death hoặc SYN Flood.

3. Các cách thức tấn công:

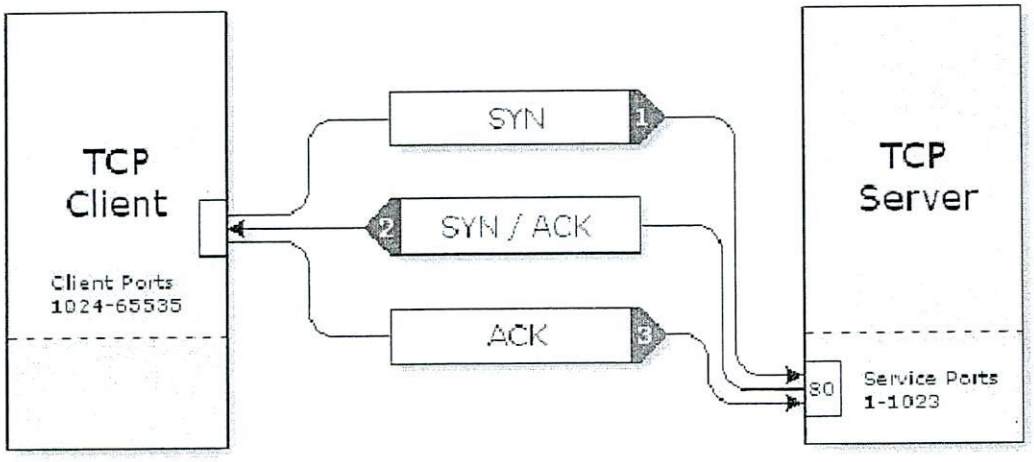
3.1. Tấn công thông qua kết nối SYN Flood Attack:

- Được xem là một trong những kiểu tấn công DoS kinh điển nhất. Lợi dụng sơ hở của thủ tục TCP khi "bắt tay ba chiều", mỗi khi client (máy khách) muốn thực hiện kết nối (connection) với server (máy chủ) thì nó thực hiện việc bắt tay ba lần (three – ways handshake) thông qua các gói tin (packet).

+ Bước 1: Client (máy khách) sẽ gửi các gói tin (packet chứa SYN=1) đến máy chủ để yêu cầu kết nối.

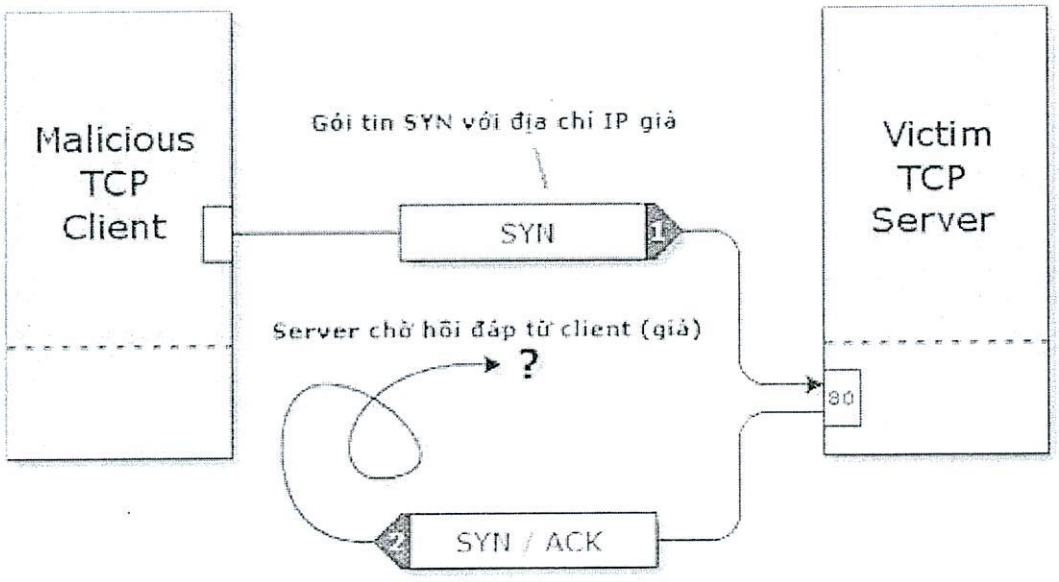
+ Bước 2: Khi nhận được gói tin này, server sẽ gửi lại gói tin SYN/ACK để thông báo cho client biết là nó đã nhận được yêu cầu kết nối và chuẩn bị tài nguyên cho việc yêu cầu này. Server sẽ giành một phần tài nguyên hệ thống như bộ nhớ đệm (cache) để nhận và truyền dữ liệu. Ngoài ra, các thông tin khác của client như địa chỉ IP và cổng (port) cũng được ghi nhận.

+ Bước 3: Cuối cùng, client hoàn tất việc bắt tay ba lần bằng cách hồi âm lại gói tin chứa ACK cho server và tiến hành kết nối.



- Do TCP là thủ tục tin cậy trong việc giao nhận (end-to-end) nên trong lần bắt tay thứ hai,server gửi các gói tin SYN/ACK trả lời lại client mà không nhận lại được hồi âm của client để thực hiện kết nối thì nó vẫn bảo lưu nguồn tài nguyên chuẩn bị kết nối đó và lập lại việc gửi gói tin SYN/ACK cho client đến khi nào nhận được hồi đáp của máy client.

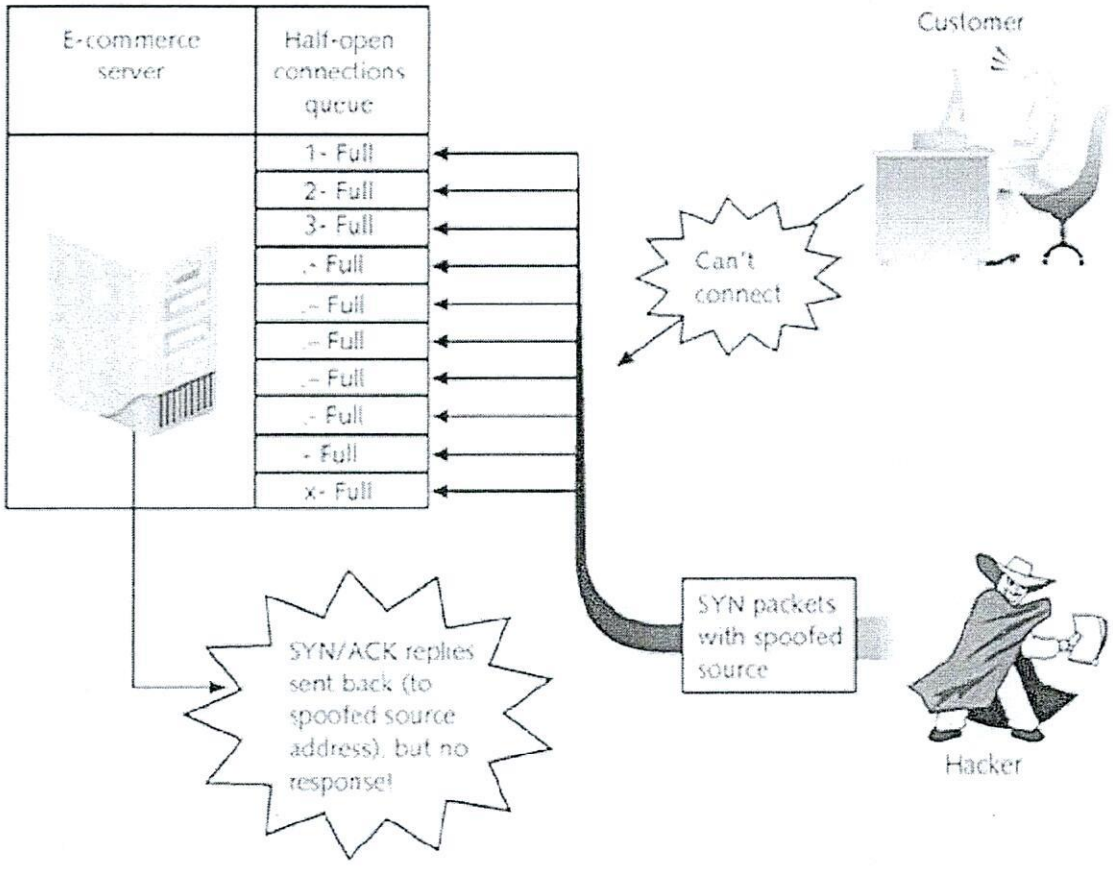
- Điểm mấu chốt là ở đây là làm cho client không hồi đáp cho Server. Và có hàng nhiều, nhiều client như thế trong khi server vẫn "ngây thơ" lặp lại việc gửi packet đó và giành tài nguyên để chờ "người về" trong lúc tài nguyên của hệ thống là có giới hạn! Các hacker tấn công sẽ tìm cách để đạt đến giới hạn đó.



- Nếu quá trình đó kéo dài, server sẽ nhanh chóng trở nên quá tải, dẫn đến tình trạng crash (treo) nên các yêu cầu hợp lệ sẽ bị từ chối không thể đáp ứng được. Có thể hình dung quá trình này cũng giống hư khi máy tính cá nhân (PC) hay bị "treo" khi mở cùng lúc quá nhiều chương trình cùng lúc vậy.

- Thông thường, để giả địa chỉ IP gói tin, các hacker có thể dùng Raw Sockets (không phải gói tin TCP hay UDP) để làm giả mạo hay ghi đè giả lên IP gốc của gói tin. Khi một gói tin SYN với IP giả mạo được gửi đến server, nó cũng như bao gói tin khác, vẫn hợp lệ đối với server và server sẽ cấp vùng tài nguyên cho đường truyền này, đồng thời ghi nhận toàn bộ thông tin và gửi gói SYN/ACK

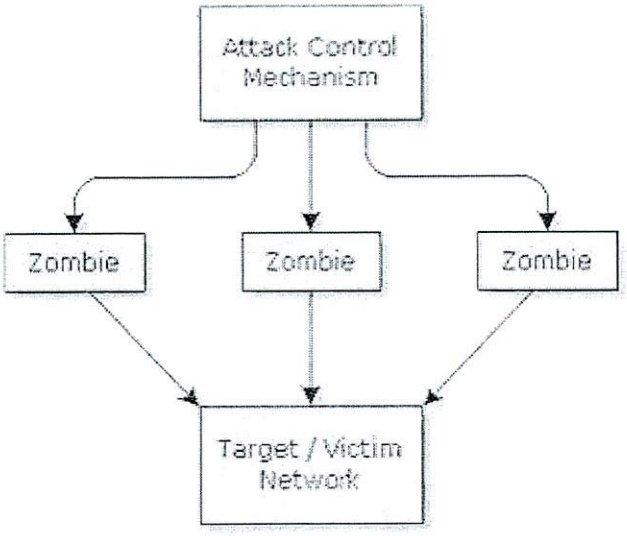
ngược lại cho Client. Vì địa chỉ IP của client là giả mạo nên sẽ không có client nào nhận được SYN/ACK packet này để hồi đáp cho máy chủ. Sau một thời gian không nhận được gói tin ACK từ client, server nghĩ rằng gói tin bị thất lạc nên lại tiếp tục gửi tiếp SYN/ACK, cứ như thế, các kết nối (connections) tiếp tục mở.



SYN flood attack

- Nếu như kẻ tấn công tiếp tục gửi nhiều gói tin SYN đến server thì cuối cùng server đã không thể tiếp nhận thêm kết nối nào nữa, dù đó là các yêu cầu kết nối hợp lệ. Việc không thể phục nữa cũng đồng nghĩa với việc máy chủ không tồn tại. Việc này cũng đồng nghĩa với xảy ra nhiều tổn thất do ngưng trệ hoạt động, đặc biệt là trong các giao dịch thương mại điện tử trực tuyến.

- Đây không phải là kiểu tấn công bằng đường truyền cao, bởi vì chỉ cần một máy tính nối internet qua ngã dial-up đơn giản cũng có thể tấn công kiểu này (tất nhiên sẽ lâu hơn chút).



3.2. Lợi dụng tài nguyên của nạn nhân để tấn công:

Land Attack

+ Tương tự như SYN flood.

+ Nhưng hacker sử dụng chính IP của mục tiêu cần tấn công để dùng làm địa chỉ IP nguồn trong gói tin.

+ Đẩy mục tiêu vào một vòng lặp vô tận khi cố gắng thiết lập kết nối với chính nó.

UDP flood

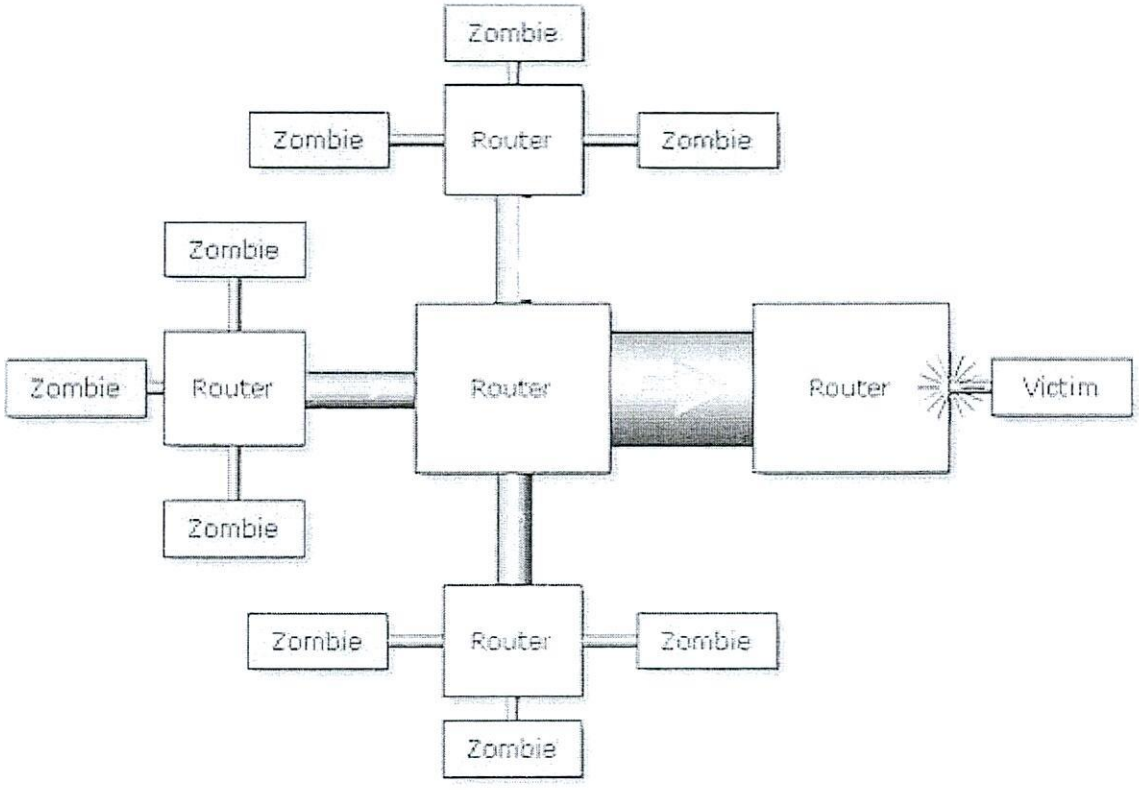
+ Hacker gửi gói tin UDP echo với địa chỉ IP nguồn là cổng loopback của chính mục tiêu cần tấn công hoặc của một máy tính trong cùng mạng.

+ Với mục tiêu sử dụng cổng UDP echo (port 7) để thiết lập việc gửi và nhận các gói tin echo trên 2 máy tính (hoặc giữa mục tiêu với chính nó nếu mục tiêu có cấu hình cổng loopback), khiến cho 2 máy tính này dần dần sử dụng hết băng thông của chúng, và cản trở hoạt động chia sẻ tài nguyên mạng của các máy tính khác trong mạng.

3.3. Sử dụng Băng Thông:

DDoS (Distributed Denial of Service)

- Xuất hiện vào mùa thu 1999, so với tấn công DoS cổ điển, sức mạnh của DDoS cao hơn gấp nhiều lần. Hầu hết các cuộc tấn công DDoS nhằm vào việc chiếm dụng băng thông (bandwidth) gây nghẽn mạch hệ thống dẫn đến hệ thống ngưng hoạt động. Để thực hiện thì kẻ tấn công tìm cách chiếm dụng và điều khiển nhiều máy tính/mạng máy tính trung gian (đóng vai trò zombie) từ nhiều nơi để đồng loạt gửi ào ạt các gói tin (packet) với số lượng rất lớn nhằm chiếm dụng tài nguyên và làm tràn ngập đường truyền của một mục tiêu xác định nào đó.

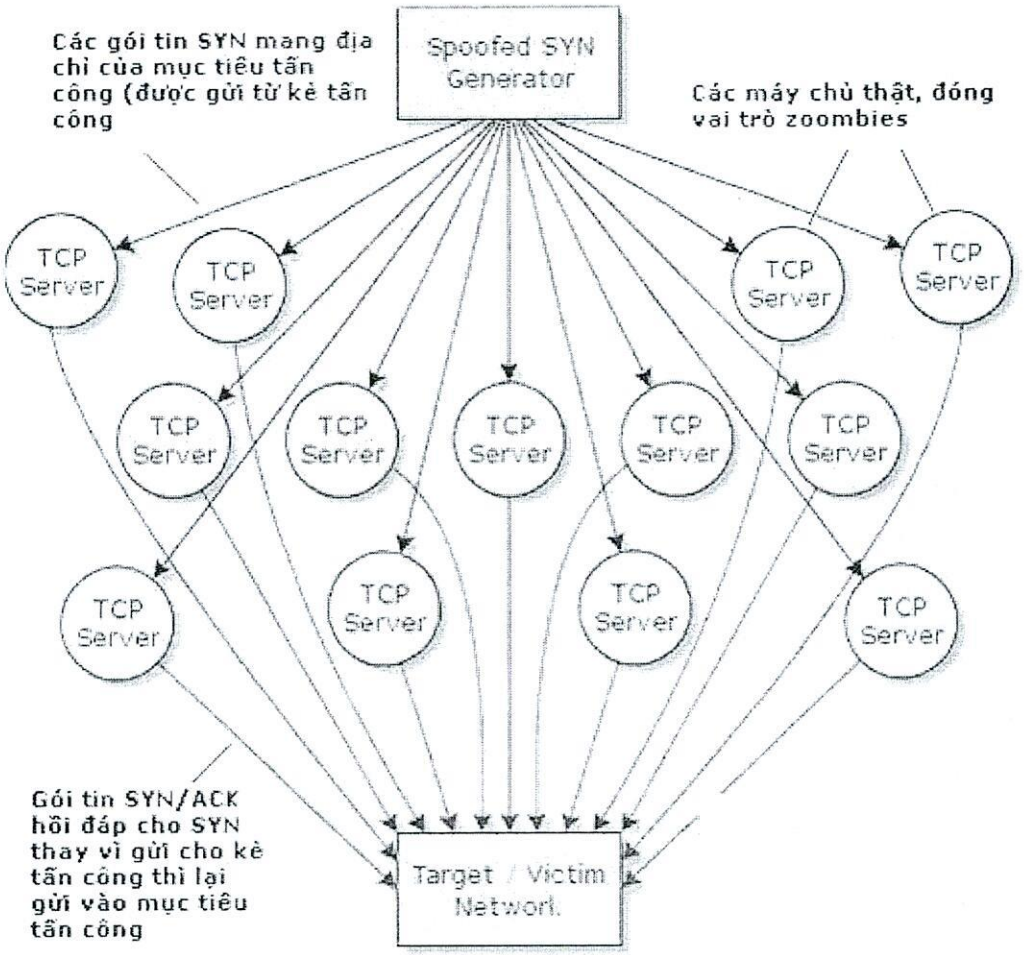


- Nói nôm na là nó giống như tình trạng kẹt xe vào giờ cao điểm vậy. Ví dụ rõ nhất là sự "cộng hưởng" trong lần truy cập điểm thi đại học vừa qua khi có quá nhiều máy tính yêu cầu truy cập cùng lúc làm dung lượng đường truyền hiện tại của máy chủ không tài nào đáp ứng nổi.

- Hiện nay, đã xuất hiện dạng virus/worm có khả năng thực hiện các cuộc tấn công DDoS. Khi bị lây nhiễm vào các máy khác, chúng sẽ tự động gửi các yêu cầu phục vụ đến một mục tiêu xác định nào đó vào thời điểm xác định để chiếm dụng băng thông hoặc tài nguyên hệ thống máy chủ. Trường hợp của MyDoom là ví dụ tiêu biểu cho kiểu này.

3.4. Sử dụng tài nguyên khác:

Smurf Attack



+ Kiểu tấn công này cần một hệ thống rất quan trọng là mạng khuyếch đại.

+ Hacker dùng địa chỉ của máy tính cần tấn công để gửi gói tin ICMP echo cho toàn bộ mạng (broadcast).

+ Các máy tính trong mạng sẽ đồng loạt gửi gói tin ICMP reply cho máy tính mà hacker muốn tấn công.

+ Kết quả là máy tính này sẽ không thể xử lý kịp thời một lượng lớn thông tin và dẫn tới bị treo máy.

Tear Drop

+ Trong mạng chuyển mạch gói, dữ liệu được chia thành nhiều gói tin nhỏ, mỗi gói tin có một giá trị offset riêng và có thể truyền đi theo nhiều con đường khác nhau để tới đích. Tại đích, nhờ vào giá trị offset của từng gói tin mà dữ liệu lại được kết hợp lại như ban đầu.

+ Lợi dụng điều này, hacker có thể tạo ra nhiều gói tin có giá trị offset trùng lặp nhau gửi đến mục tiêu muốn tấn công.

+ Kết quả là máy tính đích không thể sắp xếp được những gói tin này và dẫn tới bị treo máy vì bị "vắt kiệt" khả năng xử lý.

+ Phá hoại hoặc chỉnh sửa thông tin cấu hình.

+ Lợi dụng việc cấu hình thiếu an toàn như việc không xác thực thông tin trong việc gửi/nhận bản tin cập nhật (update) của router, ... mà kẻ tấn công sẽ thay đổi trực tiếp hoặc từ xa các thông tin quan trọng này.

+ Khiến cho những người dùng hợp pháp không thể sử dụng dịch vụ.

+ Phá hoại hoặc chỉnh sửa phần cứng.

+ Lợi dụng quyền hạn của chính bản thân kẻ tấn công đối với các thiết bị trong hệ thống mạng để tiếp cận phá hoại các thiết bị phần cứng như router, switch, ...

+ Ngoài ra còn có kiểu tấn công từ chối dịch vụ phản xạ nhiều vùng DRDoS (Distributed Reflection Denial of Service)

- Xuất hiện vào đầu năm 2002, là kiểu tấn công mới nhất, mạnh nhất trong họ DoS. Nếu được thực hiện bởi kẻ tấn công có tay nghề thì nó có thể hạ gục bất cứ hệ thống nào trên thế giới trong phút chốc.

- Mục tiêu chính của DDDoS là chiếm đoạt toàn bộ băng thông của máy chủ, tức là làm tắc nghẽn hoàn toàn đường kết nối từ máy chủ vào xương sống của Internet và tiêu hao tài nguyên máy chủ. Trong suốt quá trình máy chủ bị tấn công bằng DrDoS, không một máy khách nào có thể kết nối được vào máy chủ đó. Tất cả các dịch vụ chạy trên nền TCP/IP như DNS, HTTP, FTP, POP3, ... đều bị vô hiệu hóa.

- Về cơ bản, DRDoS là sự phối hợp giữa hai kiểu DoS và DDoS. Nó có kiểu tấn công SYN với một máy tính đơn, vừa có sự kết hợp giữa nhiều máy tính để chiếm dụng băng thông như kiểu DDoS. Kẻ tấn công thực hiện bằng cách giả mạo địa chỉ của server mục tiêu rồi gửi yêu cầu SYN đến các server lớn như Yahoo, Micorosoft, ... chẳng hạn để các server này gửi các gói tin SYN/ACK đến server mục tiêu. Các server lớn, đường truyền mạnh đó đã vô tình đóng vai trò zoombies cho kẻ tấn công như trong DDoS.

Quá trình gửi cứ lặp lại liên tục với nhiều địa chỉ IP giả từ kẻ tấn công, với nhiều server lớn tham gia nên server mục tiêu nhanh chóng bị quá tải, bandwidth bị chiếm dụng bởi server lớn. Tính "nghệ thuật" là ở chỗ chỉ cần với một máy tính với modem 56kbps, một hacker lành nghề có thể đánh bại bất cứ máy chủ nào trong giây lát mà không cần chiếm đoạt bất cứ máy nào để làm phương tiện thực hiện tấn công

4. Phát hiện dấu hiệu của một cuộc tấn công:

Agress Filtering:

Kỹ thuật này kiểm tra xem một packet có đủ tiêu chuẩn ra khỏi một subnet hay không dựa trên cơ sở gateway của một subnet luôn biết được địa chỉ IP của các máy thuộc subnet. Các packet từ bên trong subnet gửi ra ngoài với địa chỉ nguồn không hợp lệ sẽ bị giữ lại để điều tra nguyên nhân. Nếu kỹ thuật này được áp dụng trên tất cả các subnet của internet thì khái nhiệm giả mạo địa chỉ IP sẽ không còn tồn tại.

MIB statistics:

Trong Management Information Base (SNMP) của route luôn có thông tin thống kê về sự biến thiên trạng thái của mạng. Nếu ta giám sát chặt chẽ các thống kê của Protocol ICMP, UDP và TCP ta sẽ có khả năng phát hiện được thời điểm bắt đầu của cuộc tấn công để tạo "quỹ thời gian vàng" cho việc xử lý tình huống.

5. Cách phòng chống tổng quát:

Nhìn chung, tấn công từ chối dịch vụ không quá khó thực hiện, nhưng rất khó phòng chống do tính bất ngờ và thường là phòng chống trong thế bị động khi sự việc đã rồi. Việc đối phó bằng cách tăng cường "phần cứng" cũng là giải pháp tốt, nhưng thường xuyên theo dõi để phát hiện và ngăn chặn kịp thời cái gói tin IP từ các nguồn không tin cậy là hữu hiệu nhất.

- Mô hình hệ thống mạng của trung tâm đã được thiết kế, xây dựng hợp lý, luôn có phương án dự phòng trong hệ thống tránh phụ thuộc lẫn nhau quá mức. Bởi vậy khi một bộ phận gặp sự cố sẽ không làm ảnh hưởng tới toàn bộ hệ thống.

- Hệ thống máy chủ đã được thiết lập mật khẩu mạnh (strong password) để bảo vệ các thiết bị mạng và các nguồn tài nguyên quan trọng khác.

- Đã triển khai thiết lập các mức xác thực đối với người sử dụng cũng như các nguồn tin trên mạng. Đặc biệt, nên thiết lập chế độ xác thực khi cập nhật các thông tin định tuyến giữa các router.

- Xây dựng hệ thống lọc thông tin trên router, firewall... và hệ thống bảo vệ chống lại SYN flood.

- Chỉ kích hoạt các dịch vụ cần thiết, tạm thời vô hiệu hoá và dừng các dịch vụ chưa có yêu cầu hoặc không sử dụng.

- Xây dựng hệ thống định mức, giới hạn cho người sử dụng, nhằm mục đích ngăn ngừa trường hợp người sử dụng ác ý muốn lợi dụng các tài nguyên trên server để tấn công chính server hoặc mạng và server khác.

- Liên tục cập nhật, nghiên cứu, kiểm tra để phát hiện các lỗ hổng bảo mật và có biện pháp khắc phục kịp thời.

- Sử dụng các biện pháp kiểm tra hoạt động của hệ thống một cách liên tục để phát hiện ngay những hành động bất bình thường.

- Xây dựng và triển khai hệ thống dự phòng.

- Khi bạn phát hiện máy chủ mình bị tấn công hãy nhanh chóng truy tìm địa chỉ IP đó và cấm không cho gửi dữ liệu đến máy chủ.

- Dùng tính năng lọc dữ liệu của router/firewall để loại bỏ các packet không mong muốn, giảm lượng lưu thông trên mạng và tải của máy chủ.

- Nếu bị tấn công do lỗi của phần mềm hay thiết bị thì nhanh chóng cập nhật các bản sửa lỗi cho hệ thống đó hoặc thay thế.

- Dùng một số cơ chế, công cụ, phần mềm để chống lại TCP SYN Flooding. Tắt các dịch vụ khác nếu có trên máy chủ để giảm tải và có thể đáp ứng tốt hơn.

Nếu được có thể nâng cấp các thiết bị phần cứng để nâng cao khả năng đáp ứng của hệ thống hay sử dụng thêm các máy chủ cùng tính năng khác để phân chia tải.

6. Chi tiết phòng chống DDoS:

- Có rất nhiều giải pháp và ý tưởng được đưa ra nhằm đối phó với các cuộc tấn công kiểu DDoS. Tuy nhiên không có giải pháp và ý tưởng nào là giải quyết trọn vẹn bài toán Anti-DDoS. Các hình thái khác nhau của DDoS liên tục xuất hiện theo thời gian song song với các giải pháp đối phó, tuy nhiên cuộc đua vẫn tuân theo quy luật tất yếu của bảo mật máy tính: "Hacker luôn đi trước giới bảo mật một bước".

- Có ba giai đoạn chính trong quá trình Anti-DDoS:

+ Giai đoạn ngăn ngừa: tối thiểu hóa lượng Agent, tìm và vô hiệu hóa các Handler.

+ Giai đoạn đối đầu với cuộc tấn công: Phát hiện và ngăn chặn cuộc tấn công, làm suy giảm và dừng cuộc tấn công, chuyển hướng cuộc tấn công.

+ Giai đoạn sau khi cuộc tấn công xảy ra: thu thập chứng cứ và rút kinh nghiệm.

III. CÁC GIẢI PHÁP PHÒNG NGỪA TẤN CÔNG DOS, DDOS

1. Tối thiểu hóa số lượng Agent:

- Từ phía User: một phương pháp rất tốt để năng ngừa tấn công DDoS là từng internet user sẽ tự đề phòng không để bị lợi dụng tấn công hệ thống khác. Muốn đạt được điều này thì ý thức và kỹ thuật phòng chống phải được phổ biến rộng rãi cho các internet user. Attack-Network sẽ không bao giờ hình thành nếu không có user nào bị lợi dụng trở thành Agent. Các user phải liên tục thực hiện các quá trình bảo mật trên máy vi tính của mình. Họ phải tự kiểm tra sự hiện diện của Agent trên máy của mình, điều này là rất khó khăn đối với user thông thường.

- Một số giải pháp tích hợp sẵn khả năng ngăn ngừa việc cài đặt code nguy hiểm vào hardware và software của từng hệ thống. Về phía user họ nên cài đặt và cập nhật liên tục các software như antivirus, anti_trojan và server patch của hệ điều hành.

- Từ phía ISP: Thay đổi cách tính tiền dịch vụ truy cập theo dung lượng sẽ làm cho user lưu ý đến những gì họ gửi, như vậy về mặt ý thức sẽ tăng cường phát hiện DDoS Agent sẽ tự nâng cao ở mỗi User.

2. Tìm và vô hiệu hóa các Handler:

- Một nhân tố vô cùng quan trọng trong attack-network là Handler, nếu có thể phát hiện và vô hiệu hóa Handler thì khả năng Anti-DDoS thành công là rất cao. Bằng cách theo dõi các giao tiếp giữa Handler và Client hay Handler và Agent ta có thể phát hiện ra vị trí của Handler. Do một Handler quản lý nhiều, nên triệt tiêu được một Handler cũng có nghĩa là loại bỏ một lượng đáng kể các Agent trong Attack Network.

3. Phát hiện dấu hiệu của một cuộc tấn công:

Agress Filtering:

Kỹ thuật này kiểm tra xem một packet có đủ tiêu chuẩn ra khỏi một subnet hay không dựa trên cơ sở gateway của một subnet luôn biết được địa chỉ IP của các máy thuộc subnet. Các packet từ bên trong subnet gửi ra ngoài với địa chỉ nguồn không hợp lệ sẽ bị giữ lại để điều tra nguyên nhân. Nếu kỹ thuật này được áp dụng trên tất cả các subnet của internet thì khái nhiệm giả mạo địa chỉ IP sẽ không còn tồn tại.

MIB statistics:

- Trong Management Information Base (SNMP) của route luôn có thông tin thống kê về sự biến thiên trạng thái của mạng. Nếu ta giám sát chặt chẽ các thống kê của Protocol ICMP, UDP và TCP ta sẽ có khả năng phát hiện được thời điểm bắt đầu của cuộc tấn công để tạo "quỹ thời gian vàng" cho việc xử lý tình huống.

4. Làm suy giảm hay dừng cuộc tấn công:

Load balancing:

Thiết lập kiến trúc cân bằng tải cho các server trọng điểm sẽ làm gia tăng thời gian chống chọi của hệ thống với cuộc tấn công DDoS. Tuy nhiên, điều này không có ý nghĩa lắm về mặt thực tiễn vì quy mô của cuộc tấn công là không có giới hạn.

Throttling:

Thiết lập cơ chế điều tiết trên router, quy định một khoảng tải hợp lý mà server bên trong có thể xử lý được. Phương pháp này cũng có thể được dùng để ngăn chặn khả năng DDoS traffic không cho user truy cập dịch vụ. Hạn chế của kỹ thuật này là không phân biệt được giữa các loại traffic, đôi khi làm dịch vụ bị gián đoạn với user, DDoS traffic vẫn có thể xâm nhập vào mạng dịch vụ nhưng với số lượng hữu hạn.

Drop request:

Thiết lập cơ chế drop request nếu nó vi phạm một số quy định như: thời gian delay kéo dài, tốn nhiều tài nguyên để xử lý, gây deadlock. Kỹ thuật này triệt tiêu khả năng làm cạn kiệt năng lực hệ thống, tuy nhiên nó cũng giới hạn một số hoạt động thông thường của hệ thống, cần cân nhắc khi sử dụng.

5. Chuyển hướng của cuộc tấn công:

Honeyspots:

- Một kỹ thuật đang được nghiên cứu là Honeyspots. Honeyspots là một hệ thống được thiết kế nhằm đánh lừa attacker tấn công vào khi xâm nhập hệ thống mà không chú ý đến hệ thống quan trọng thực sự.

- Honeyspots không chỉ đóng vai trò "Lê Lai cứu chúa" mà còn rất hiệu quả trong việc phát hiện và xử lý xâm nhập, vì trên Honeyspots đã thiết lập sẵn các cơ chế giám sát và báo động.

- Ngoài ra Honeyspots còn có giá trị trong việc học hỏi và rút kinh nghiệm từ Attacker, do Honeyspots ghi nhận khá chi tiết mọi động thái của attacker trên hệ thống. Nếu attacker bị đánh lừa và cài đặt Agent hay Handler lên Honeyspots thì khả năng bị triệt tiêu toàn bộ attack-network là rất cao.

6. Giai đoạn sau tấn công:

Traffic Pattern Analysis:

Nếu dữ liệu về thống kê biến thiên lượng traffic theo thời gian đã được lưu lại thì sẽ được đưa ra phân tích. Quá trình phân tích này rất có ích cho việc tinh chỉnh lại các hệ thống Load Balancing và Throttling. Ngoài ra các dữ liệu này còn giúp Quản trị mạng điều chỉnh lại các quy tắc kiểm soát traffic ra vào mạng của mình.

Packet Traceback:

Bằng cách dùng kỹ thuật Traceback ta có thể truy ngược lại vị trí của Attacker (ít nhất là subnet của attacker). Từ kỹ thuật Traceback ta phát triển thêm khả năng Block Traceback từ attacker khá hữu hiệu, gần đây đã có một kỹ thuật Traceback khá hiệu quả có thể truy tìm nguồn gốc của cuộc tấn công dưới 15 phút, đó là kỹ thuật XXX.

Bevent Logs:

Bằng cách phân tích file log sau cuộc tấn công, quản trị mạng có thể tìm ra nhiều manh mối và chứng cứ quan trọng.

7. Cách thức phòng chống tấn công DoS, DDoS:

TT	Tình huống	Cách phòng tránh
1	Tấn công gây nghẽn mạng (UDP flood và ping flood).	Tăng băng thông, sử dụng các hệ thống cân bằng tải, chuyển hướng cuộc tấn công, dùng cơ chế mạo danh IP hoặc chuyển lượng truy cập sang một nhà cung cấp dịch vụ chống DDoS.
2	Tấn công chuyển hướng. Mục đích: Gây tốn tài nguyên bằng cách giả mạo IP nguồn để các máy chủ mục tiêu phản hồi về máu chủ nạn nhân, từ đó tạo ra các cuộc tấn công với quy mô lớn, đặc biệt là hệ thống có khả năng khuếch đại. Phương thức: Gửi IP mạo danh đến nhiều máy tính để nhận lại lượng phản hồi về địa chỉ đích giả mạo được định sẵn, khi đó nạn	

TT	Tình huống	Cách phòng tránh
	nhân cũng sẽ không biết được nguồn thực sự tấn công mình.	
3	Tấn công Smurf và Fraggle.	Thiết lập lại router để đảm bảo không ai có thể lợi dụng tính năng phát đi IP của thiết bị.
4	Tấn công SYN flood (TCP). Mục đích: Gây cạn tài nguyên máy chủ và chặn việc nhân các yêu cầu kết nối mới. Phương thức: Lợi dụng quá trình " bắt tay" 3 chặng TCP: gửi đi yêu cầu SYN đến máy chủ và được phản hồi bằng một gói SYN-ACK, tuy nhiên không gửi lại gói ACK khiến cho tài nguyên máy chủ bị sử dụng hết vào việc đợi gói ACK gửi về.	Sử dụng bộ lọc, tăng backlog, giảm SYN-RECEIVED Timer, SYN caching, tường lửa, …
5	(HTTP) flood (Web Spidering).	Chỉ cho phép các bot được tin cậy như của Google quét trang.
6	Tấn công PUSH và ACK.	Tương tự như tấn công SYN flood.
7	Tấn công tại chỗ: Mục đích: Crash hệ thống. Phương thức: các gói IP được tạo sao cho địa chỉ nguồn và số cổng nguồn chính là địa chỉ đích và số cổng đích, khiến cho đối tượng tự phản hồi lại chính gói của mình.	
8	Tấn công khuếch đại DNS: Mục tiêu: Làm quá tải đối tượng bằng phản hồi từ các bộ giải mã DNS. Phương thức: Mạo danh địa chỉ IP của máy bị tấn công để gửi yêu cầu đến nhiều bộ giải mã DNS. Các bộ giả mã hồi đáp về IP của máy bị tấn công với kích thước gói dữ liệu có thể lớn hơn kích thước yêu cầu tới 50 lần.	Các kĩ thuật chống mạo danh, hệ thống cân bằng tải và chuyển hướng lưu lượng về các máy chủ khác.

TT	Tình huống	Cách phòng tránh
9	Tấn công lớp thứ 7: Mục tiêu: Nhắm vào 1 tính năng cụ thể của 1 ứng dụng web. Phương thức: Một ví dụ là khi các máy chủ website liên tục mở các thread mới cho mỗi yêu cầu kết nối và mỗi kết nối lại mới lại gây tiêu tốn tài nguyên máy chủ. Đến một thời điểm nào đó, máy chủ sẽ không còn có thể nhận kết nối mới và bắt đầu từ chối dịch vụ với người truy cập.	Tăng dung lượng, sử dụng các giải pháp điện toán đám mây, tối ưu hiệu năng của máy chủ web và dùng front-end proxy.