

QUYẾT ĐỊNH

**Ban hành Phương án chống tấn công từ chối dịch vụ (DoS, DDoS)
trên hệ thống tại Bệnh viện Đa khoa Khánh Hòa**

GIÁM ĐỐC BỆNH VIỆN ĐA KHOA KHÁNH HÒA

Căn cứ Quyết định 578/QĐ-UBND ngày 04/8/2025 của UBND tỉnh Khánh Hòa về việc kiện toàn chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bệnh viện Đa khoa Khánh Hòa;

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015 của Quốc hội;

Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018 của Quốc hội;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông về Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Xét đề nghị của Lãnh đạo Phòng Kế hoạch Tổng hợp Bệnh viện Đa khoa Khánh Hòa.

QUYẾT ĐỊNH:

Điều 1. Ban hành Phương án chống tấn công từ chối dịch vụ (DoS, DDoS) trên hệ thống tại Bệnh viện Đa khoa Khánh Hòa (đính kèm).

Điều 2. Quyết định này có hiệu lực kể từ ngày ký ban hành.

Điều 3. Lãnh đạo các khoa, phòng, trung tâm và các cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận: (VBĐT)

- Như điều 3;

- Lưu: VT, KHTH.

GIÁM ĐỐC



Phan Hữu Chính

PHƯƠNG ÁN CHỐNG TẤN CÔNG TỪ CHỐI DỊCH VỤ (DOS, DDOS) TRÊN HỆ THỐNG

*(Kèm theo Quyết định số 1097/QĐ-BVĐKKH ngày 23/9/2025
của Bệnh viện Đa khoa Khánh Hòa)*

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Xây dựng phương án cảnh báo và chống tấn công xâm nhập từ xa và chống tấn công từ chối dịch vụ (DoS, DDoS) trên hệ thống thông tin quan trọng của Bệnh viện, 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 xâm nhập từ xa và chống tấn công từ chối dịch vụ (DoS, DDoS) đối với các hệ thống máy chủ cung cấp dịch vụ qua Internet của Bệnh viện.
- 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 Bệnh viện.
- 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 và chống tấn công từ chối dịch vụ (DoS, DDoS) trên hệ thống máy chủ, Website của Bệnh viện 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 Bệnh viện để đưa ra các giải pháp hiệu quả nhất nhằm đảm bảo an toàn, an ninh thông tin hệ thống thông tin của Bệnh viện.
- Cơ chế cảnh báo phải kịp thời, hiệu quả cao nhất đối với hệ thống thông tin của Bệnh viện.
- Đưa ra các giải pháp cụ thể để phòng chống các cuộc tấn công xâm nhập từ xa và chống tấn công từ chối dịch vụ (DoS, DDoS) nhằm và hệ thống thông tin của Bệnh viện.

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

- 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 ...) Tài nguyên này 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 là tấn công từ chối dịch vụ phân tán (DDos)

- 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

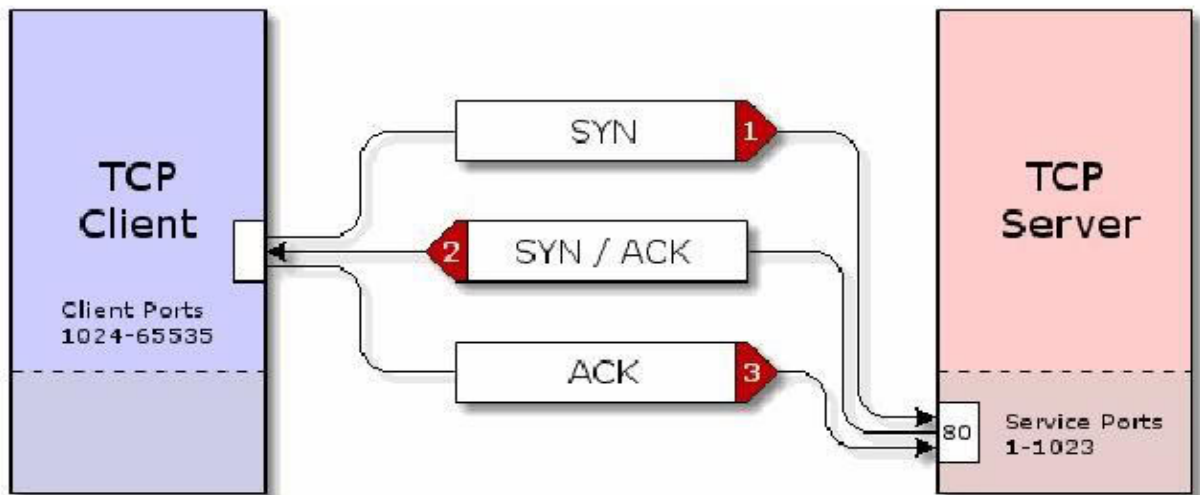
a) Tấn công thông qua kết nối SYN Flood Attack

- Được xem là một trong những kiểu tấn công DoS kinh điển nhất. Lợi dụng điểm yếu của thủ tục TCP/IP khi “bắt tay ba chiều”, mỗi khi client (máy khách) muốn thực hiện kết nối (connection) với server (máy chủ) thì phải thực hiện việc bắt tay ba chiều (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.

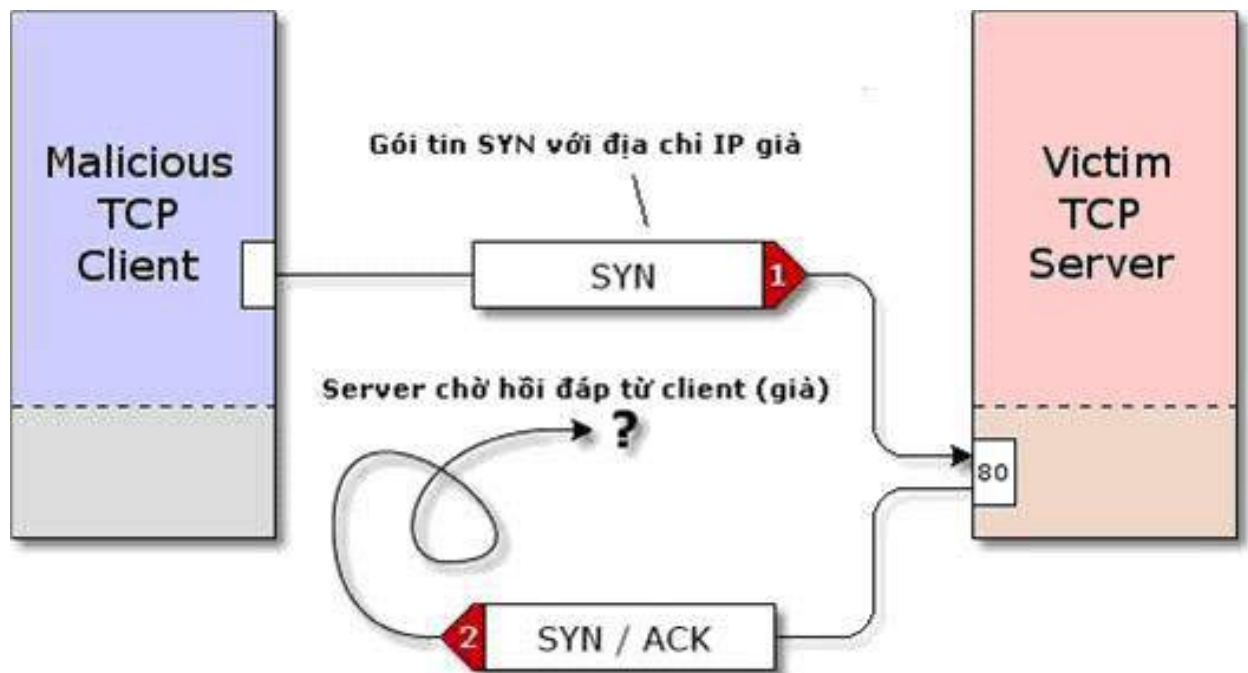
+ Bước 3: Cuối cùng, client hoàn tất việc bắt tay ba chiều bằng cách hồi âm lại gói tin chứa ACK cho server và tiến hành kết nối.



Hình 1. Cơ chế tấn công thông qua kết nối SYN Flood Attack

- 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 server vẫn bảo lưu nguồn tài nguyên chuẩn bị kết nối đó và lặp lại việc gửi gói tin SYN/ACK cho client đến khi nào nhận được hồi đáp của máy client.

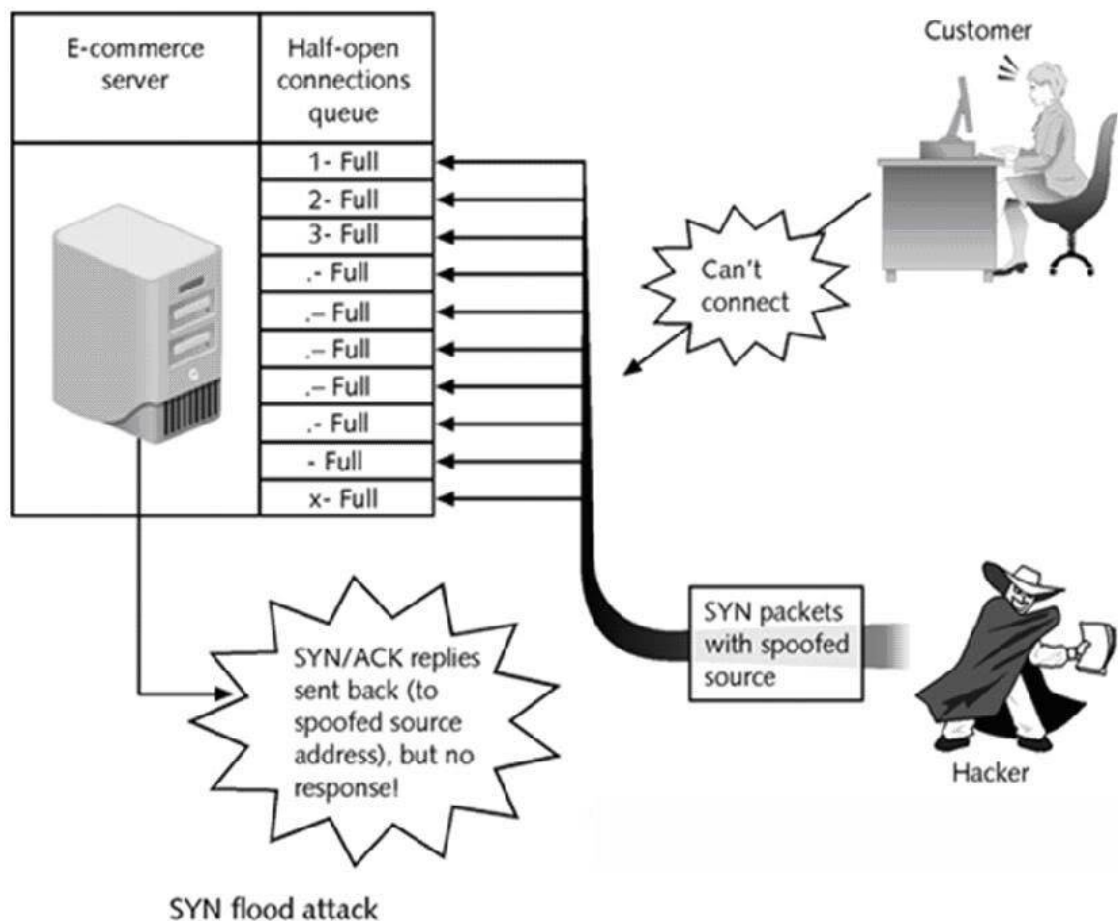
- Trong trường hợp nhiều client không hồi đáp trong khi server vẫn tiếp tục lặp lại việc gửi gói tin để chờ kết nối sẽ khiến server nhanh chóng cạn kiệt tài nguyên! Các hacker tấn công sẽ tìm cách để đạt đến giới hạn này.



Hình 2. Giả mạo client

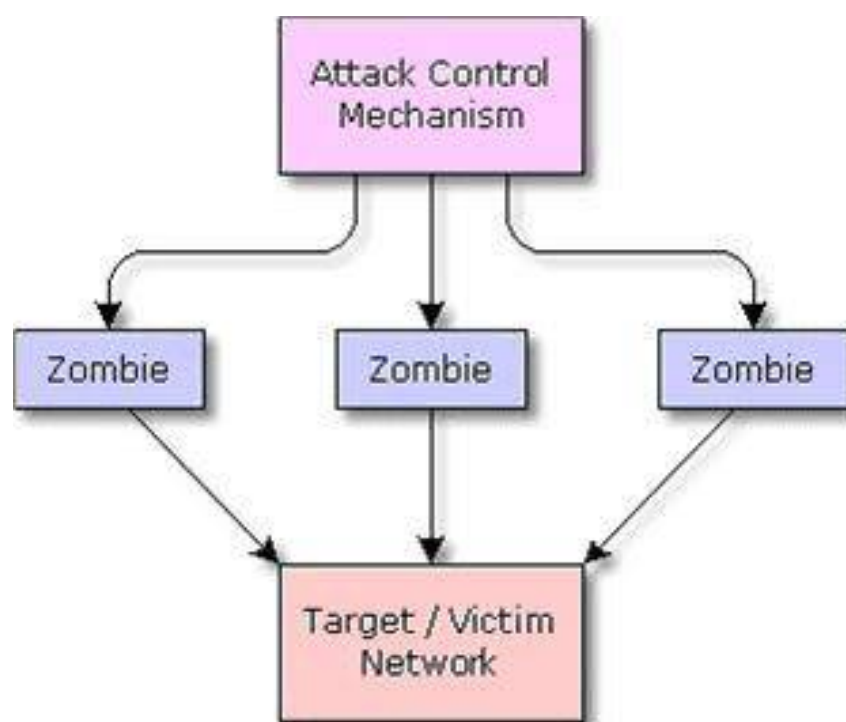
- Nếu quá trình đó kéo dài, server sẽ nhanh chóng trở nên quá tải, dẫn đến tình trạng crash (treo) nên các yêu cầu hợp lệ sẽ bị từ chối không thể đáp ứng được.

- 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 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.



Hình 3. Cơ chế giữ các connection luôn mở

- Nếu như kẻ tấn công tiếp tục gửi nhiều gói tin SYN đến server thì cuối cùng server sẽ không thể tiếp nhận thêm kết nối nào nữa, dù đó là các yêu cầu kết nối hợp lệ. Việc không thể phục vụ kết nối mới cũng đồng nghĩa với việc máy chủ không tồn tại. Việc này gây ngưng trệ hoạt động của hệ thống.



Hình 4. Mô hình cơ chế điều hành mạng lưới botnet

b) Lợi dụng tài nguyên của nạn nhân để tấn công

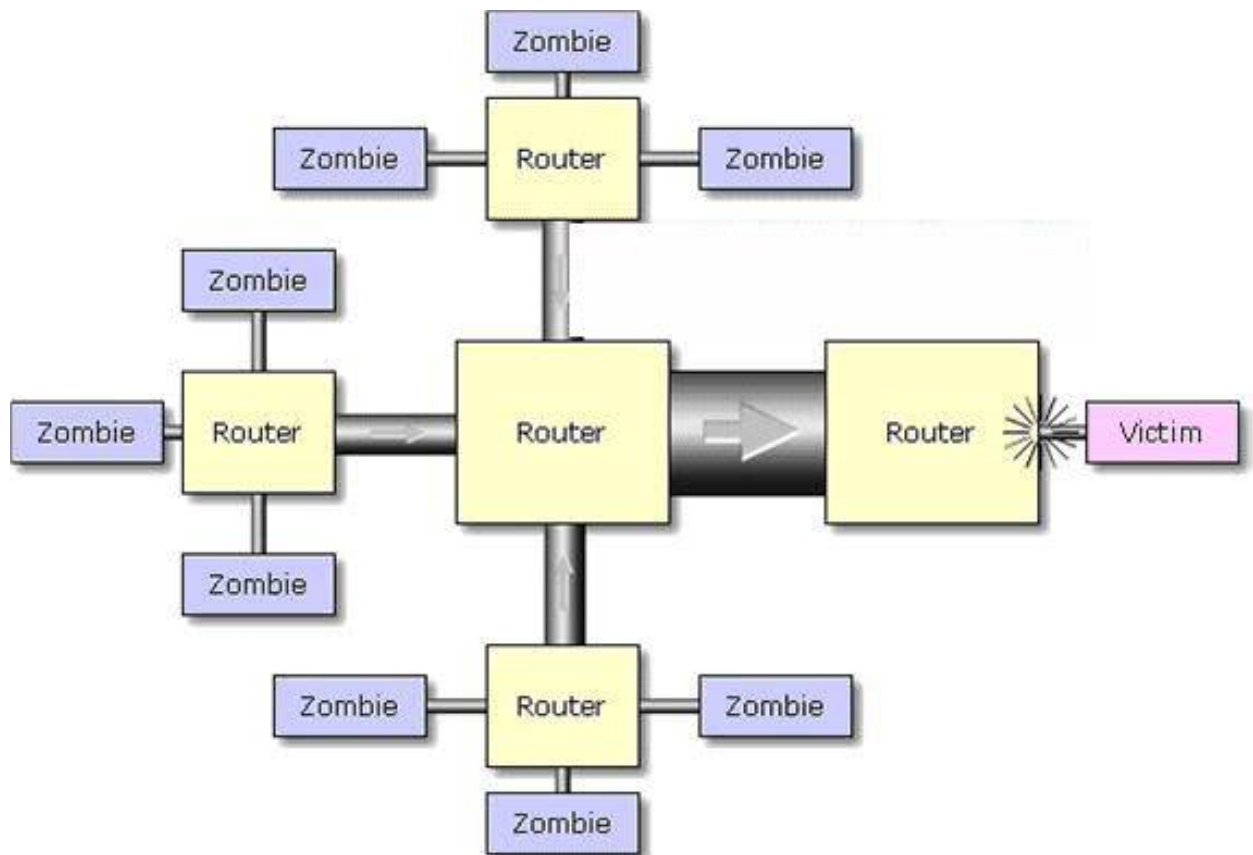
- Land Attack
 - + Tương tự như SYN flood
 - + Nhưng hacker sử dụng chính IP của mục tiêu cần tấn công để dùng làm địa chỉ IP nguồn trong gói tin.
 - + Đẩy mục tiêu vào một vòng lặp vô tận khi cố gắng thiết lập kết nối với chính nó.
- UDP flood
 - + Hacker gửi gói tin UDP echo với địa chỉ IP nguồn là 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.

c) Sử dụng Băng thông

DDoS (Distributed Denial of Service)

- 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 kẻ tấn công sẽ 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.

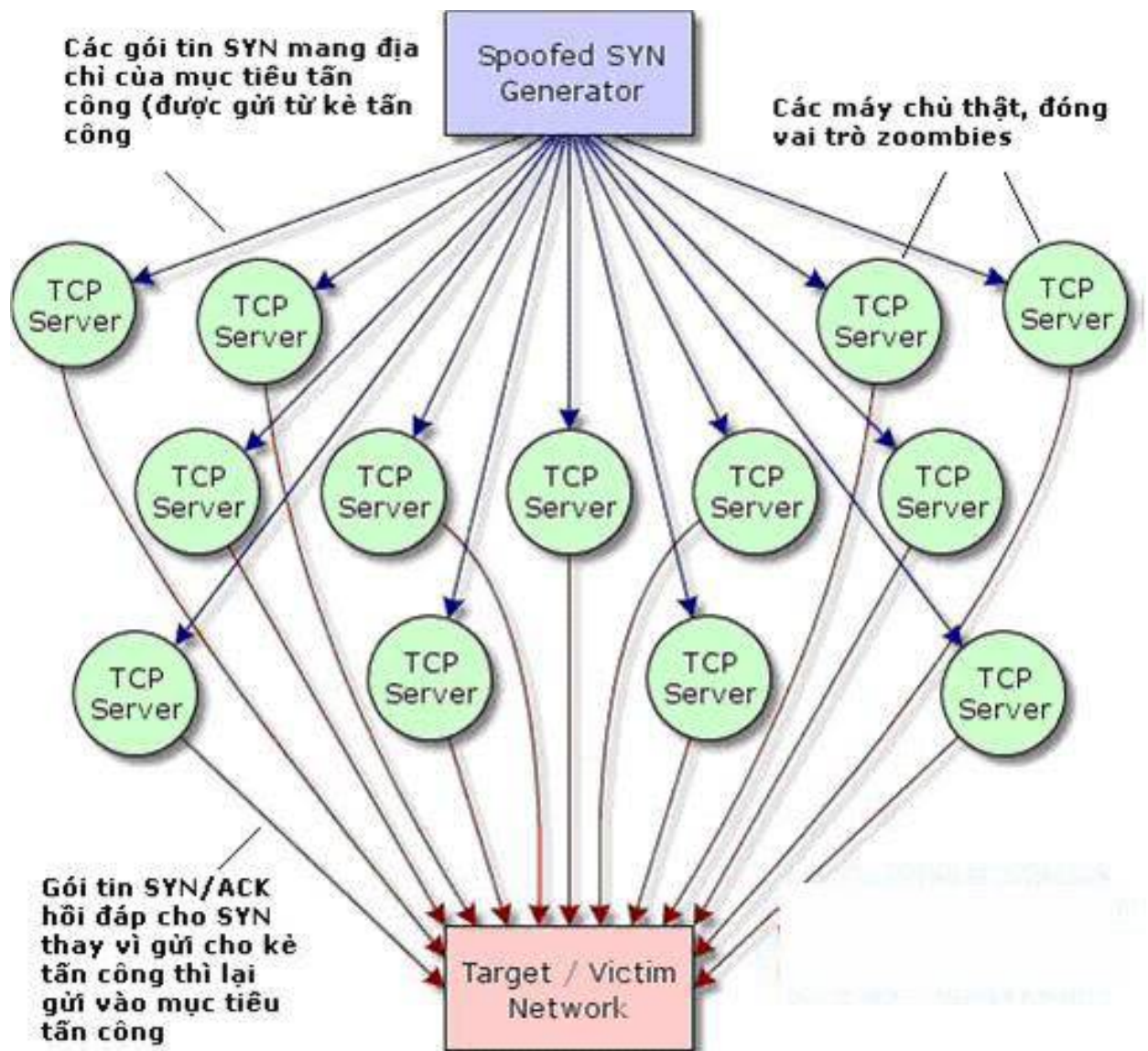


Hình 5. Cơ chế tấn công DDOS

- 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.

d) Sử dụng tài nguyên khác

- Smurf Attack



Hình 6. Cơ chế tấn công Smurf Attack

- + Kiểu tấn công này cần một hệ thống rất quan trọng là mạng khuếch 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 “vất 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)

- Về cơ bản, DRDoS là sự phối hợp giữa 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 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, Microsoft... 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 zombies 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.

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 niệm giả mạo địa chỉ IP sẽ không còn tồn tại.

- MIB statistics

Trong Management Information Base của router 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 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 trong thể bị động. 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 các gói tin IP từ các nguồn không tin cậy là hữu hiệu nhất.

- Mô hình hệ thống mạng của Bệnh viện 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, 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.

- Dừng 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.

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

1. Tối thiểu hóa số lượng Agent

- Từ phía người dùng: đề phòng để không để bị lợi dụng trở thành máy tính tấn công các hệ thống khác. Nhân viên phải nghiêm túc thực hiện các quá trình bảo mật trên máy tính, không click vào các đường link lạ, tránh bị các phần mềm độc hại âm thầm cài đặt và chạy mã độc trên máy của mình

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 Agent, nên triệt tiêu được một Handler cũng có nghĩa là loại bỏ một lượng đáng kể các Agent trong Attack Network.

3. 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.

- 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 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 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.

4. 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.

- 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.