

Số: 548/QĐ-BVMDL

Cà Mau, ngày 26 tháng 06 năm 2025

QUYẾT ĐỊNH

**Ban hành các quy trình, Phương án, Kịch bản phòng ngừa khắc phục sự cố
gây mất an toàn thông tin tại Bệnh viện Mắt – Da liễu tỉnh Cà Mau**

GIÁM ĐỐC BỆNH VIỆN MẮT – DA LIỄU TỈNH CÀ MAU

Căn cứ Luật giao dịch điện tử số 20/2023/QH15 ngày 22/06/2023;

Căn cứ Luật Công nghệ thông tin 67/2006/QH11 ngày 29/06/2006;

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

*Căn cứ Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ về
Ngăn chặn xung đột thông tin trên mạng;*

*Căn cứ Nghị định số 85/2016/ NĐ-CP ngày 01/07/2016 của Chính phủ về
đảm bảo an toàn hệ thống thông tin theo cấp độ;*

*Căn cứ thông tư số 03/2017/TT-BTTTT ngày 24/04/2017 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/NNĐ-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 20/2017/TT-BTTTT ngày 12/09/2017 của Bộ Thông tin
và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên
toàn quốc;*

*Căn cứ Nghị định số 137/2024/NĐ-CP ngày 23/10/2024 của Chính Phủ
Quy định về giao dịch điện tử của cơ quan nhà nước và hệ thống thông tin phục
vụ giao dịch điện tử;*

*Căn cứ quyết định số 4159/QĐ-BYT, ngày 13/10/2014 của Bộ Y tế về Ban
hành quy định về đảm bảo an toàn thông tin Y tế điện tử tại các đơn vị trong
ngành Y tế;*

*Căn cứ Thông tư số 54/TT-BYT ngày 29/12/2017 của Bộ Y tế về việc Ban
hành Bộ tiêu chí ứng dụng công nghệ thông tin tại các cơ sở khám bệnh, chữa
bệnh;*

*Căn cứ Thông tư 13/2025/TT-BYT ngày 06 tháng 06 năm 2025 của Bộ y tế
Vv Hướng dẫn triển khai hồ sơ bệnh án điện tử;*

Căn cứ Văn bản số 365/TTYTQG-GPQLCL ngày 06 tháng 06 năm 2025 của Trung tâm thông tin y tế Quốc Gia về Hướng dẫn yêu cầu kỹ thuật triển khai phần mềm hồ sơ bệnh án điện tử;

Xét đề nghị của Trưởng phòng Kế hoạch – Tổng hợp.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này các Quy trình, Phương án, Kịch bản phòng ngừa khắc phục sự cố gây mất an toàn thông tin tại bệnh viện Mắt – Da liễu tỉnh Cà Mau, cụ thể như sau:

1.1. Kịch bản phòng ngừa khắc phục sự cố hệ thống tại Bệnh viện Mắt – Da liễu tỉnh Cà Mau (có kịch bản kèm theo);

1.2. Quy trình sao lưu và phục hồi dữ liệu tại Bệnh viện Mắt – Da liễu tỉnh Cà Mau (có quy trình kèm theo);

1.3. Phương án cảnh báo và phòng chống tấn công có chủ đích đối với các hệ thống cung cấp dịch vụ qua internet của tại Bệnh viện Mắt – Da liễu tỉnh Cà Mau (có phương án kèm theo);

1.4. Phương án chống tấn công xâm nhập từ xa (DOS, DDOS) cơ chế chống tấn công từ chối dịch vụ trên hệ thống của tại Bệnh viện Mắt – Da liễu tỉnh Cà Mau (có phương án kèm theo);

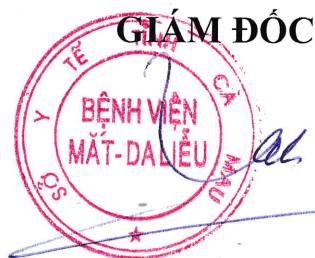
Điều 2. Các quy trình, phương án, kịch bản này được áp dụng cho tất cả nhân viên trong toàn bệnh viện.

Điều 3. Tổ CNTT Phòng Kế hoạch – Tổng hợp, các khoa, phòng, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này.

Quyết định có hiệu lực kể từ ngày ký./.

Nơi nhận:

- Như Điều 3;
- Lưu: VT, KHTH.






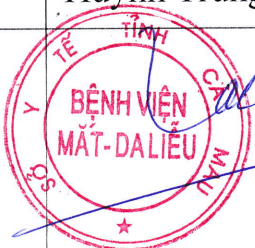
Huỳnh Trung Lâm

SỞ Y TẾ TỈNH CÀ MAU
BỆNH VIỆN MẮT – DA LIỄU

KỊCH BẢN
PHÒNG NGỪA KHẮC PHỤC SỰ
CÔNG HỆ THỐNG

KỊCH BẢN
PHÒNG NGỪA KHÁC PHỤC SỰ CỐ HỆ THỐNG

*(Ban hành theo Quyết định số 54B/QĐ- BVMDL ngày 26/06/2025
của Bệnh viện Mắt- Da liễu Cà Mau)*

	Người lập	Người xem xét	Người phê duyệt
Họ tên	Lê Minh Nhựt	Trần Kim Thanh	Huỳnh Trung Lâm
Ký tên			 
Chức vụ	Tổ trưởng CNTT	Trưởng phòng Kế hoạch – Tổng hợp	Giám đốc
Ngày	26/06/2025	26/06/2025	26/06/2025

KỊCH BẢN PHÒNG NGỪA KHẮC PHỤC SỰ CỐ HỆ THỐNG

1. MỤC ĐÍCH, YÊU CẦU

1.1. Mục đích

Bảo đảm an toàn thông tin mạng của Bệnh viện Mắt – Da liễu tỉnh Cà Mau, trong đó tập trung an toàn thông tin cho các 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 giải pháp ứng phó khi gặp sự cố mất an toàn thông tin mạng.

Nâng cao năng lực, hiệu quả hoạt động của Tổ Công nghệ thông tin ứng cứu sự cố an toàn thông tin mạng, nội bộ, gắn kết với các đơn vị cung cấp phần mềm, hợp tác, kết nối chặt chẽ, điều phối kịp thời, phối hợp đồng bộ, hiệu quả của các lực lượng để ứng cứu sự cố mạng, chống tấn công mạng.

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 bảo đảm an toàn thông tin mạng.

1.2 Yêu cầu

- Phải khảo sát, đánh giá các nguy cơ, sự cố an toàn thông tin mạng của hệ thống thông tin đưa ra phương án đối phó, ứng cứu sự cố phù hợp, kịp thời

- Phương án đối phó, ứng cứu sự cố an toàn thông tin mạng phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi sự cố xảy ra.

2. NHIỆM VỤ TRIỂN KHAI

2.1. Đánh giá các nguy cơ, sự cố an toàn thông tin mạng:

Đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá; dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố (bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).

2.2. Phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể

Đối với mỗi hệ thống thông tin cần xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng. Trong phương án đối phó, ứng cứu phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được

tính chất, mức độ nghiêm trọng của sự cố khi sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố cần đảm bảo các nội dung sau:

2.2.1. *Phương pháp, cách thức để xác định nhanh chóng, kịp thời nguyên nhân, nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp.*

- Sự cố do bị tấn công mạng;
- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật do hoặc do lỗi đường điện, đường truyền, hosting, ...;
- Sự cố do lỗi của người quản trị, vận hành hệ thống;
- Sự cố do liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn, ...

2.2.2. *Phương án đối phó, ứng cứu, khắc phục sự cố đối với một hoặc nhiều tình huống sau:*

STT	Tình huống	Cách phòng ngừa
I. Tình huống sự cố do bị tấn công mạng		
1	Tấn công từ chối dịch vụ: Là một loại hình tấn công nhằm ngăn chặn những người dùng hợp lệ được sử dụng một dịch vụ nào đó, Các cuộc tấn công có thể được thực hiện nhằm vào bất kì một thiết bị mạng nào bao gồm là tấn công vào các thiết bị định tuyến, web, thư điện tử và hệ thống DNS, ...	<ul style="list-style-type: none"> - Cài đặt và duy trì phần mềm chống virus. - Cài đặt tường lửa và cấu hình nó để giới hạn lưu lượng đến và đi từ máy tính của bạn. - Làm theo các hướng dẫn thực hành an toàn về phân phối địa chỉ email. - Dùng các bộ lọc email để giúp bạn quản lý lưu lượng không mong muốn. - Nâng cao ý thức của người sử dụng khi tham gia vào hệ thống thông tin trung tâm. - Ban hành quy chế đảm bảo an toàn an ninh thông tin trong toàn trung tâm.
2	Tấn công giả mạo: Là một hành vi giả mạo các ý nhằm lấy được các thông tin nhạy cảm như tên người dùng, mật khẩu và các chi tiết thẻ tín dụng bằng cách giả dạng thành một chủ thể tin cậy trong một giao dịch điện tử.	<ul style="list-style-type: none"> - Tập huấn, tuyên truyền nâng cao nhận thức về công nghệ thông tin cho cán bộ nhân viên trung tâm về phát hiện các tình huống giả mạo. - Triển khai một bộ lọc SPAM để phát hiện virus, người gửi trống cho toàn bộ hệ thống mail cũng như các hệ thống công nghệ thông tin của trung tâm.

STT	Tình huống	Cách phòng ngừa
	Các giao dịch thường dùng để đánh lừa những người ít dùng ít đa nghi là các giao dịch có vẻ xuất phát từ các website xã hội phổ biến, các trung tâm chi trả trực tuyến hoặc các quản trị mạng.	<ul style="list-style-type: none"> - Giữ tất cả các hệ thống hiện tại với các bản vá lỗi bảo mật và cập nhật mới nhất. Cài đặt một giải pháp chống virus, lên lịch cập nhật chữ ký, và theo dõi trạng thái chống virus trên tất cả các thiết bị. - Thực hiện chế độ mã hóa tất cả thông tin nhạy cảm, quan trọng của trung tâm để lưu trữ an toàn.
3	Tấn công sử dụng mã độc: Một khái niệm chung dùng để chỉ các phần mềm độc hại được viết với mục đích có thể lây lan phát tán (hoặc không lây lan, phát tán) trên hệ thống máy tính và internet, nhằm thực hiện các hành vi bất hợp pháp nhằm vào người dùng cá nhân, cơ quan, tổ chức. Thực hiện các hành vi chuộc lợi cá nhân, kinh tế, chính trị hoặc đơn giản là để thỏa mãn ý tưởng và sở thích của người viết.	<ul style="list-style-type: none"> - Luôn luôn cài đặt, cập nhật và sử dụng một phần mềm diệt virus có bản quyền để bảo vệ các máy tính. - Xây dựng chính sách với các thiết bị PnP. - Thiết lập quy tắc đối xử với các file. - Truy cập web an toàn. - Cập nhật máy tính, phần mềm. - Thành lập tổ chức xử lý các sự cố về công nghệ thông tin để kịp thời phối hợp xử lý khi phát hiện mã độc.
4	Tấn công truy cập trái phép, chiếm quyền điều khiển: Truy cập vào dữ liệu, chiếm đoạt quyền truy cập và leo theo đặc quyền.	<ul style="list-style-type: none"> - Với kiểu tấn công vào mật khẩu: Đặt mật khẩu mạnh. Không sử dụng mật khẩu ở dạng bản rõ cả khi lưu trữ hoặc truyền trên mạng. <p>Trong các khuyến nghị về chính sách an ninh mạng, đều yêu cầu phải ghi lại nhật ký hệ thống. Bằng cách xem xét các bản ghi nhật ký, admin có thể biết được các thông tin và số lần truy cập không thành công. Nếu phát hiện từ một địa chỉ IP có số lần truy cập không thành công vượt quá giới hạn cho phép thì đây rất có thể là do tấn công vào mật khẩu. Ví dụ về việc phân tích nhật ký hệ thống, để phát hiện tấn công mật khẩu. Để xử lý, admin cần cấu hình giới hạn về số lần đăng nhập, ví dụ trong bài viết này.</p>


STT	Tình huống	Cách phòng ngừa
		<p>- Với kiểu tấn công lợi dụng sự tin cậy, admin cần giảm thiểu việc cấu hình trust giữa các hệ thống, Ví dụ, khi bạn dùng trình duyệt IE trên máy chủ windows Server, mỗi khi bạn vào một website thì IE đều hỏi bạn xem có trust cái site đó không.</p> <p>- Với kiểu tấn công MITM: vì kẻ đứng giữa cần nhân bản dữ liệu mà hãm chặn bắt, do vậy sẽ tiêu tốn nhiều băng thông. Admin cần có công cụ giám sát băng thông để phát hiện ra việc này. Ví dụ về các phần mềm giám sát hoặc phần mềm giám sát băng thông.</p> <p>- Với kiểu tấn công tràn bộ đệm, bạn cần có công cụ giám sát trạng thái của các tiến trình đang chạy trong hệ thống, ví dụ 2 công cụ Event Viewer kết hợp với Performance Monitor trên Windows.</p>
5	Tấn công thay đổi giao diện.	- Xem những thông tin nhật ký, file log của máy chủ và truy tìm xem, hacker đã làm gì và làm như thế nào trên hệ thống của mình.
6	Tấn công mã hóa phần mềm, dữ liệu, thiết bị.	<p>- Cài đặt và duy trì phần mềm chống virus.</p> <p>- Công cụ chống phần mềm độc hại.</p>
7	Tấn công phá hoại thông tin, dữ liệu, phần mềm.	<p>- Cài đặt và duy trì phần mềm chống virus.</p> <p>- Công cụ chống phần mềm độc hại.</p>
8	<p>Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu.</p> <p>Tấn công tổng hợp sử dụng kết hợp nhiều hình thức.</p>	<p>- Cập nhật máy tính, phần mềm.</p> <p>- Cài đặt và duy trì phần mềm chống virus trên các máy tính.</p> <p>- Công cụ chống phần mềm độc hại.</p>
II. Tình huống sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật		
1	Sự cố nguồn điện.	<p>- Sử dụng bộ lưu điện UPS.</p> <p>- Sử dụng nguồn điện dự phòng.</p>

STT	Tình huống	Cách phòng ngừa
2	Sự cố đường kết nối Internet.	- Sử dụng nhiều đường kết nối internet của nhiều nhà cung cấp dịch vụ.
3	Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin.	- Sao lưu hệ thống hằng ngày. - Lưu trữ dự phòng ở nhiều nơi.
4	Sự cố liên quan đến quá tải hệ thống.	- Kiểm tra hệ thống thường xuyên. - Nâng cấp hệ thống để phù hợp với từng giai đoạn của trung tâm.
III. Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống		
1	Lỗi trong cập nhật, thay đổi, cấu hình phần cứng. Lỗi trong cập nhật, thay đổi, cấu hình phần mềm. Lỗi liên quan đến chính sách và thủ tục an toàn thông tin. Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc. Lỗi khách liên quan đến người quản trị, vận hành hệ thống.	- Backup dự phòng trước khi cập nhật, thay đổi cấu trúc hệ thống.
IV. Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn, ...		
1	Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn, ...	Trung tâm thuê hệ thống lưu trữ dự phòng tại các trung tâm dữ liệu đạt tiêu chuẩn do Bộ TTTT công bố để lưu các bản sao dữ liệu.

SỞ Y TẾ TỈNH CÀ MAU
BỆNH VIỆN MẮT – DA LIỄU

**QUY TRÌNH
SAO LƯU VÀ PHỤC HỒI DỮ LIỆU**

QUY TRÌNH
SAO LƯU VÀ PHỤC HỒI DỮ LIỆU
TẠI BỆNH VIỆN MẮT – DA LIỄU TỈNH CÀ MAU
(Ban hành theo Quyết định số 54b/ QĐ- BVMDL ngày 26/06/2025
của Bệnh viện Mắt Da liễu Cà Mau)

	Người lập	Người xem xét	Người phê duyệt
Họ tên	Lê Minh Nhựt	Trần Kim Thanh	Huỳnh Trung Lâm
Ký tên			
Chức vụ	Tổ trưởng CNTT	Trưởng phòng Kế hoạch – Tổng hợp	Giám đốc
Ngày	26/06/2025	26/06/2025	26/06/2025

GIẢI PHÁP SAO LƯU – PHỤC HỒI HỆ THỐNG TẠI BỆNH VIỆN MẮT – DA LIỄU TỈNH CÀ MAU

1. SAO LƯU DỮ LIỆU

1.1 Hệ thống HIS, LIS, EMR

Các hệ thống Quản lý khám chữa bệnh (HIS), Quản lý trả kết quả xét nghiệm tự động (LIS), Quản lý bệnh án điện tử (EMR) chạy trên Cloud của Tập đoàn VNPT. Do đó quy trình sao lưu hệ thống tuân thủ các chính sách (SLA) của Tập đoàn VNPT. Cụ thể như sau:

- Phần ứng dụng (App) đều có các bản lưu trữ dự phòng đặt tại các Trung tâm lưu trữ từ xa của Tập đoàn VNPT. Các bản App được lưu trữ tối thiểu 05 phiên bản (version) gần nhất. Thực hiện sao lưu khi có sự thay đổi.
- Phần Cơ sở dữ liệu (DB - database): Được sao lưu định kỳ hàng ngày. Theo quy định mỗi tuần 1 lần sẽ sao lưu toàn bộ cơ sở dữ liệu (Full backup) và hàng ngày sao lưu phần thay đổi (Incremental backup).

1.2 Hệ thống PACS

Hệ thống lưu trữ và truyền tải dữ liệu hình ảnh y khoa (PACS) chạy trên Cloud của Tập đoàn VNPT.

- Phần ứng dụng (App) đều có các bản lưu trữ dự phòng đặt tại các Trung tâm lưu trữ từ xa của Tập đoàn VNPT. Các bản App được lưu trữ 03 tháng gần nhất. Thực hiện sao lưu khi có sự thay đổi.
- Phần Cơ sở dữ liệu (DB - database):
 - Dữ liệu được sao lưu đồng bộ từ DB chính sang DB dự phòng theo thời gian thực (replicate master-slave realtime).
 - Thứ 6 hàng tuần: thực hiện sao lưu bản Full.
 - Thời gian lưu đối với các dữ liệu sao lưu: 01 tháng.

2. PHỤC HỒI HỆ THỐNG KHI CÓ SỰ CỐ

Các bước thực hiện như sau:

1. Xác định hệ thống bị ảnh hưởng: HIS, LIS, EMR, PACS, ...
2. Xác định máy chủ ứng dụng (App) hay hay dữ liệu bị ảnh hưởng.
3. Xác định các nguồn lưu trữ dữ liệu tương ứng với các loại dữ liệu
4. Đơn vị tự thực hiện hoặc thông báo đơn vị cung cấp hệ thống (VNPTIT) để thực hiện phương án khôi phục dữ liệu




- a. Các bước phục hồi đối với hệ thống HIS, LIS, EMR:
 - 1. Khôi phục máy chủ bị sự cố.
 - 2. Restore dữ liệu sao lưu tương ứng với hệ thống bị sự cố từ phiên bản mới nhất (App/DB).
 - 3. Restore file cấu hình sau lưu gần nhất tương ứng.
 - 4. Khởi tạo hệ thống.
 - 5. Kiểm tra các chức năng, dữ liệu để đảm bảo gần nhất.
 - 6. Thông báo với người dùng để truy cập sử dụng.
- b. Đối với hệ thống PACS
 - 1. Phục hồi máy chủ bị sự cố.
 - 2. Restore dữ liệu sao lưu tương ứng với hệ thống bị sự cố từ phiên bản mới nhất (App/DB).
 - 3. Restore file cấu hình sau lưu gần nhất tương ứng.
 - 4. Phục hồi từ backup local: NAS, Server backup.
 - 5. Khởi tạo hệ thống.
 - 6. Kiểm tra các chức năng, dữ liệu để đảm bảo gần nhất.
 - 7. Thông báo với người dùng để truy cập sử dụng.

SỞ Y TẾ TỈNH CÀ MAU
BỆNH VIỆN MẮT – DA LIỄU

PHƯƠNG ÁN
CẢNH BÁO VÀ CHỐNG TẤN CÔNG CÓ CHỦ ĐÍCH ĐỐI
VỚI CÁC HỆ THỐNG CUNG CẤP DỊCH VỤ QUA
INTERNET CỦA BỆNH VIỆN MẮT – DA LIỄU
TỈNH CÀ MAU

PHƯƠNG ÁN
CẢNH BÁO VÀ CHỐNG TẤN CÔNG CÓ CHỦ ĐÍCH ĐỐI VỚI
CÁC HỆ THỐNG CUNG CẤP DỊCH VỤ QUA INTERNET
CỦA BỆNH VIỆN MẮT – DA LIỄU TỈNH CÀ MAU

*Ban hành theo Quyết định số 54B/ QĐ- BVMDL ngày 26/06/2025
của Bệnh viện Mắt Da liễu Cà Mau)*

	Người lập	Người xem xét	Người phê duyệt
Họ tên	Lê Minh Nhứt	Trần Kim Thanh	Huỳnh Trung Lâm
Ký tên			 
Chức vụ	Tổ trưởng CNTT	Trưởng phòng Kế hoạch – Tổng hợp	Giám đốc
Ngày	26/06/2025	26/06/2025	26/06/2025

PHƯƠNG ÁN CẢNH BÁO VÀ CHỐNG TẤN CÔNG CÓ CHỦ ĐÍCH ĐỐI VỚI CÁC HỆ THỐNG CUNG CẤP DỊCH VỤ QUA INTERNET CỦA BỆNH VIỆN MẮT – ĐA LIỄU TỈNH CÀ MAU

I. MỤC ĐÍCH YÊU CẦU

1. Mục đích:

Xây dựng phương án cảnh báo và chống tấn công có chủ đích để bảo đảm an toàn thông tin mạng của đơn vị, trong đó tập trung an toàn thông tin cho các hệ thống thông tin quan trọng của đơn vị, có khả năng thích ứng một số 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 tấn công có chủ đích đối với các hệ thống cung cấp dịch vụ qua internet của trung tâm.

Nâng cao năng lực, hiệu quả hoạt động của Tổ Công nghệ thông tin – Phòng Kế hoạch – Tổng hợp (KHTH) ứng cứu sự cố an toàn thông tin mạng nội bộ, gắn kết với các đơn vị cung cấp phần mềm, hợp tác, kết nối chặt chẽ, điều phối kịp thời, phối hợp đồng bộ, hiệu quả của các lực lượng để ứng cứu sự cố mạng, chống tấn công mạng.

Nâng cao nhân lực cho cán bộ, nhân viên, người lao động đơn vị khi tham gia khai thác, sử dụng các hệ thống thông tin của đơn vị.

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 bảo đảm an toàn thông tin mạng.

2. Yêu cầu:

- Phải khảo sát, đánh giá hiện trạng hạ tầng công nghệ thông tin tại đơn vị để đưa ra các giải pháp hiệu quả nhất nhằm đảm bảo an toàn thông tin hệ thống thông tin của đơn vị.

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

- Đưa ra các giải pháp cụ thể để phòng chống các cuộc tấn công có chủ đích nhắm vào hệ thống thông tin của đơn vị.

II. MỘT SỐ KHÁI NIỆM CƠ BẢN VỀ TẤN CÔNG CÓ CHỦ ĐÍCH

1. Khái niệm về tấn công có chủ đích:

Tấn công có chủ đích APT (Advanced Persistent Threat) được dùng để chỉ kiểu tấn công dai dẳng có chủ đích vào một thực thể. Kẻ tấn công có thể được hỗ trợ bởi một tổ chức, cá nhân nào đó nhằm tìm kiếm thông tin của một tổ chức, các nhân khác.

2. Mục đích của tấn công có chủ đích:

- + Thu thập thông tin tình báo có tính chất thù địch.
- + Đánh cắp dữ liệu và bán lại bí mật kinh doanh cho các đối thủ.
- + Làm mất uy tín của cơ quan tổ chức, đơn vị.
- + Phá hoại, gây bất ổn hạ tầng công nghệ thông tin, viễn thông.

3. Các phương thức tấn công có chủ đích:

- + Tấn công bị động (Passive attack).
- + Tấn công rải rác (Distributed attack).
- + Tấn công nội bộ (Insider attack).
- + Tấn công Phishing.
- + Các cuộc tấn công của không tặc (Hijack attack).
- + Tấn công mật khẩu (Password attack).
- + Khai thác lỗ hổng tấn công (Exploit attack).
- + Lỗi tràn bộ đệm (Buffer overflow).
- + Tấn công từ chối dịch vụ (Denial of service attack).
- + Tấn công theo kiểu Man-in-the-Middle Attack.
- + Tấn công phá mã khóa (Compromised-key Attack).
- + Tấn công trực tiếp.
- + Nghe trộm.
- + Giả mạo địa chỉ.
- + Vô hiệu hóa các chức năng của hệ thống.
- + Lỗi của người quản trị hệ thống.
- + Tấn công vào yếu tố con người.

III. CÁC GIẢI PHÁP PHÒNG NGỪA TẤN CÔNG CÓ CHỦ ĐÍCH

Tấn công APT (Advanced Persistent Threat) là hình thức tấn công mạng có mục tiêu cụ thể do tin tặc chọn, sử dụng các công nghệ tiên tiến và kỹ thuật lừa đảo để đột nhập mạng mục tiêu và dai dẳng tập trung vào mục tiêu đó trong nhiều tuần, nhiều tháng hoặc nhiều năm cho đến khi cuộc tấn công diễn ra thành công (hoặc bị chặn đứng). Một khi vào được trong mạng, tin tặc cố giấu mình để không bị phát hiện trong khi sử dụng một số loại phần mềm độc hại (malware) để đánh cắp thông tin quan trọng. Các cuộc tấn công ATP được tổ chức chặt chẽ, có nguồn

lực tài chính và công nghệ dồi dào. Tuy có thể sử dụng các công cụ đột nhập thông thường, nhưng thường thì các cuộc tấn công ATP sử dụng phần mềm tùy biến tinh vi khó bị hệ thống bảo mật phát hiện. Từ những đánh giá mức độ nguy hiểm của tấn công APT, để phòng ngừa tấn công có chủ đích và hệ thống thông tin, Bệnh viện Mắt – Da liễu Tỉnh Cà Mau đã triển khai các giải pháp cụ thể sau:

1. Triển khai phòng thủ theo chiều sâu:

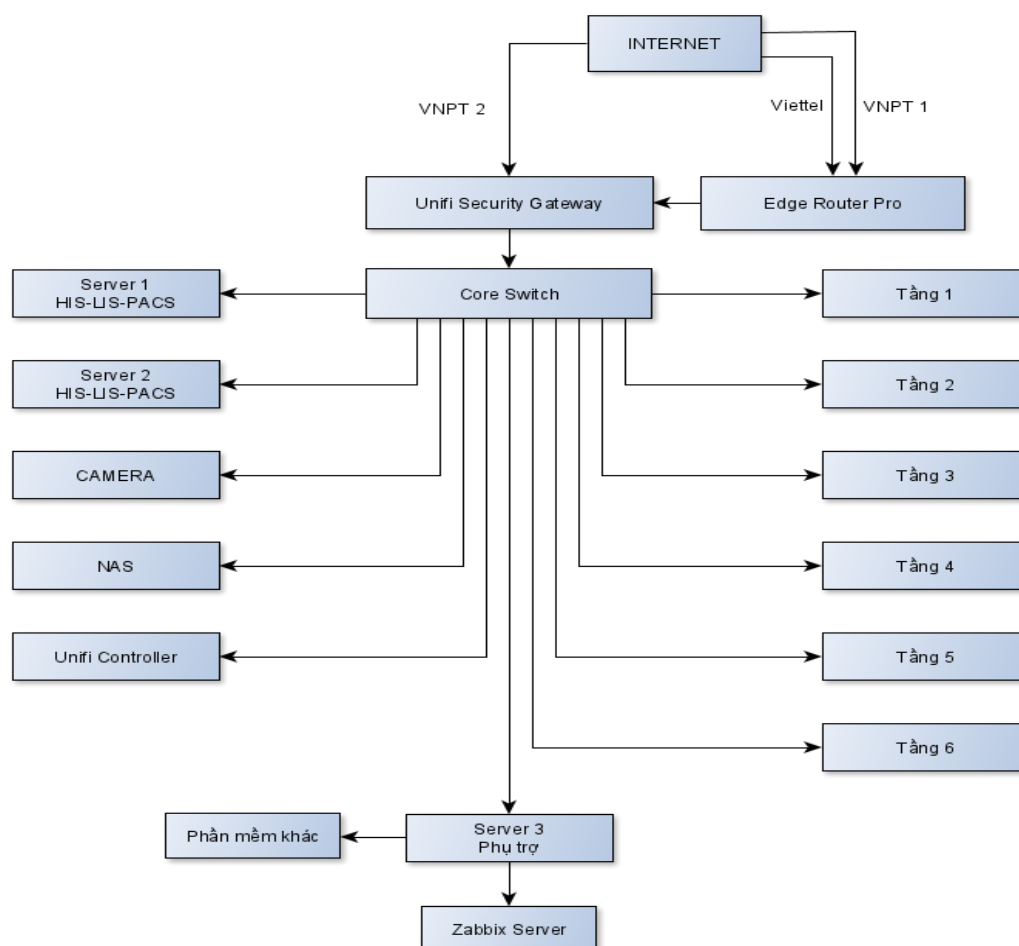
Hệ thống hạ tầng công nghệ thông tin của trung tâm được bảo vệ theo chiều sâu, phân thành nhiều tầng và tách thành nhiều lớp khác nhau. Mỗi tầng và lớp đó sẽ được thực hiện các chính sách bảo mật hay ngăn chặn khác nhau. Một khác cũng là để phòng ngừa khi một tầng hay một lớp nào đó bị xâm nhập thì xâm nhập trái phép đó chỉ bó hẹp trong tầng hoặc lớp đó thôi và không thể ảnh hưởng sang các tầng lớp khác.

Phòng thủ theo chiều sâu hay bảo mật theo lớp không thể thiếu trong chiến lược an ninh mạng, đây là một trong những phương pháp tốt nhất để ngăn chặn cuộc tấn công mạng ATP. Nó có nghĩa kiểm soát các điểm ra vào mạng, sử dụng tường lửa thế hệ mới, triển khai các hệ thống phát hiện/ngăn chặn xâm nhập (IDS/IPS) hệ thống giám sát thông tin và sự cố bảo mật (SIEM), bổ sung hệ thống quản lý lỗ hổng, sử dụng phương thức xác thực quản lý danh tính chắc chắn, cập nhật các bản vá và bảo mật và thực hiện bảo vệ đầu cuối.

1.1. Giải pháp về quy hoạch thiết kế hạ tầng:

Bệnh viện Mắt – Da liễu Tỉnh Cà Mau đã triển khai thiết kế, quy hoạch hệ thống mạng nội bộ hiện đại kết nối thông suốt đến các phòng, khoa trong toàn bệnh viện đáp ứng đầy đủ nhu cầu khai thác sử dụng của trung tâm, đặc biệt chú trọng đến vấn đề an toàn an ninh thông tin của hệ thống:

a. Thiết kế cơ sở hạ tầng theo mô hình tổng thể:



b. Kiến trúc hệ thống mạng trung tâm:

Kiến trúc mạng trung tâm được thiết kế theo mô hình đa tầng phân cấp chuẩn (3 lớp: core layer, distribbution layer, access layer) và sử dụng công cụ mạng tiên tiến như dịch vụ Backup, VLAN, ... nhằm đảm bảo tính sẵn sàng, tính phân quyền tăng tốc đường truyền, ... Hệ thống mạng LAN của trung tâm là hệ thống có đường truyền băng thông cao và có thể kết nối với hệ thống khác để thành hệ thống mạng WAN đáp ứng nhu cầu sử dụng của trung tâm. Hệ thống mạng thiết kế tuân thủ nguyên tắc mạng khách và mạng nội bộ.

Hệ thống mạng công nghệ thông tin trung tâm đã triển khai các giải pháp đảm bảo an toàn, bảo mật hệ thống và các dữ liệu nhạy cảm của trung tâm, cụ thể như sau:

- Lắp đặt trang thiết bị hệ thống firewall chuyên dụng;
- Triển khai hệ thống VPN server cho phép người dùng có thể truy cập vào hệ thống của trung tâm thông qua kết nối VPN đảm bảo an toàn và bảo mật;
- Triển khai hệ thống Gateway kết nối internet (Bảo vệ và kiểm soát kết nối từ bên ngoài vào và từ bên trong ra ngoài internet)

1.2. Giải pháp ngăn chặn phát hiện tấn công có chủ đích:

1.2.1. Thiết lập cơ chế bảo mật hệ thống:

Để đảm bảo cơ chế bảo mật nhằm ngăn chặn phát hiện các cuộc tấn công có chủ đích vào hệ thống mạng thông tin. Hệ thống mạng của trung tâm được tổ chức thành nhiều nhóm mạng tách biệt như:

- + Lớp mạng bên ngoài (Outside network) các giao tiếp giữa hệ thống mạng trung tâm và bên ngoài đều được kết nối với các thiết bị router chuyên dụng có khả năng lọc gói tin, ánh xạ địa chỉ IP, ... tạo ra một cấp tường lửa (Firewall) cho hệ thống.

- + Các máy tính bên ngoài chỉ được truy cập thông tin của trung tâm trên các server dịch vụ được thiết lập trong một thiết bị mạng khác. Nhằm đảm bảo tính an toàn cho các database server chính trong hệ thống.

- + Lớp trong (Inside network): các giao tiếp giữa các máy tính và các Server database của trung tâm đều phải qua thiết bị Routing switch trung tâm cũng được bảo vệ bằng kỹ thuật firewall (tích hợp sẵn trong thiết bị) tạo nên một vành đai an toàn bảo vệ dữ liệu của hệ thống. Ngoài ra giữa các khu vực kết nối có thiết lập các VLAN tách biệt đảm bảo an toàn cho hệ thống.

- + Backbone của hệ thống được đầu nối tập trung về một thiết bị Routing switch layer 3 tạo thành một core network.

Hệ thống đã triển khai hệ thống Firewall đảm bảo an toàn cho hệ thống (Unifi security Gateway) sẽ áp dụng chính sách bảo mật hệ thống:

- + Lọc gói (Packet Filtering) đây là phương pháp ứng dụng phổ biến nhất. Firewall này nhận gói tin từ Internet, kiểm tra thông tin về địa chỉ IP trong phần tiêu đề gói tin và đối chiếu với danh sách cho phép truy cập để xác định xem gói tin đó được chấp nhận hay từ chối.

- + Kiểm tra trạng thái sâu (Deep packet Inspection): Đây là giải pháp Firewall lọc gói cấp cao nó kiểm tra cả tiêu đề và thông tin gói tin để xác định chi tiết hơn ngoài thông tin về địa chỉ nguồn và địa chỉ đích. Đây là cách đảm bảo tất cả các phiên truyền thông tin được khởi tạo bởi máy tính đích và diễn ra chỉ với những nguồn đã biết và tin cậy. Biện pháp này giúp tăng cường khả năng chống các hành động tấn công quét công.

1.2.2. Hệ thống chống virus:

Để cải thiện tốc độ xử lý của tường lửa, thông thường không cấu hình kích hoạt tính năng lọc cao cấp của tường lửa (tường lửa ở các vị trí phải xử lý lưu lượng lớn). Khi đó các chương trình quét virus được cài đặt nhằm phát hiện và ngăn chặn các đoạn mã độc, các chương trình gián điệp, các email có tệp tin virus đính kèm.

Tại Bệnh viện Mắt – Da liễu Tỉnh Cà Mau đã triển khai cài đặt phần mềm diệt virus Windows Security cho tất cả các máy trạm tại các khoa, phòng trong toàn viện để phòng chống ngăn chặn các đoạn mã độc, virus phát tán trong hệ thống của trung tâm.

2. Triển khai hệ thống giám sát phát hiện và chống xâm nhập:

Giám sát chặt chẽ việc kiểm soát an ninh giúp nhận diện các dấu hiệu cảnh báo sớm của một cuộc tấn công APT, thường xuất hiện dưới dạng file log và lưu lượng dữ liệu bất thường, hay các hoạt động bất thường khác. Việc giám sát tất cả các lưu lượng ra vào mạng, lưu lượng nội bộ và tất cả các thiết bị truy cập mạng là hết sức quan trọng. việc giám sát liên tục không chỉ giúp phát hiện hoạt động đáng ngờ sớm nhất có thể mà còn làm giảm khả năng các cuộc xâm nhập leo thang hoặc kéo dài. Kết quả giám sát còn có thể dùng làm chứng chỉ pháp lý nếu cuộc tấn công xảy ra.

2.1. Quản lý danh sách điều khiển truy xuất, an toàn cổng thiết bị, lọc địa chỉ mạng:

**** Danh sách điều khiển truy xuất:***

Danh sách truy nhập là gồm các luật cho phép hay ngăn chặn các gói tin sau khi tham chiếu vào thông tin trong tiêu đề của gói tin để giới hạn các người dùng có thể truy xuất vào các hệ thống nội bộ, ...

**** Bảo mật cổng của thiết bị, lọc địa chỉ vật lý của thiết bị mạng:***

Ở các điểm truy cập mạng công cộng, việc mở rộng LAN của người dùng; việc truy xuất vào các máy chủ nội bộ cần được kiểm soát.

Các giải pháp như cấu hình bảo mật cổng của thiết bị, quản lý địa chỉ vật lý là giải pháp cực kỳ an ninh và hiệu quả trong trường hợp này.

- Cấu hình bảo mật cổng của thiết bị trên các switch nhằm đảm bảo không thể mở rộng LAN khi chưa có sự đồng ý của người quản trị hệ thống, nếu vi phạm điều đó, port trên switch đó sẽ chuyển về trạng thái cấm hoặc trạng thái ngừng hoạt động.

- Địa chỉ vật lý là địa chỉ được cài đặt sẵn từ nhà sản xuất. về nguyên tắc tất cả các máy tính trên mạng sẽ không trùng nhau về địa chỉ này. Sự kiểm soát theo địa chỉ này là rất cụ thể tới từng máy tính trong mạng, trừ khi người dùng có quyền cài đặt phần mềm và làm giả địa chỉ này ở máy tính đó, hoặc là mở máy tính rồi thay thế card giao tiếp mạng mới.

2.2. Một số giải pháp khác:

2.2.1. Xây dựng hệ thống cập nhật sửa lỗi tập trung:

Công đoạn đầu tiên của hacker khi tiến hành tấn công có chủ đích là khảo sát hệ thống đích để tìm ra các lỗi của hệ điều hành, của các ví dụ, của các ứng dụng khi chúng chưa được cập nhật trên website của nhà cung cấp.

Thực trạng ở các cơ quan, đơn vị nói chung, tại Bệnh viện Mắt – Da liễu Tỉnh Cà Mau nói riêng cho thấy việc sử dụng các sản phẩm phần mềm hầu như ít cập nhật các bản vá lỗi, có chăng cũng đang riêng lẻ trên các máy tính cá nhân, đó chính là cơ hội cho hacker dùng các công cụ khai thác lỗ hổng bảo mật. Để cập nhật bản vá lỗi cho tất cả các máy khách trong toàn bộ hệ thống qua internet mất thời gian và tốn nhiều băng thông đường truyền và không thống nhất.

Đơn vị triển khai giải pháp xây dựng hệ thống tự động cập nhật từ nhà cung cấp trên Internet về máy chủ rồi từ máy chủ này, triển khai cho tất cả các máy khách trong toàn mạng, mặt khác các cán bộ kỹ thuật thường xuyên theo dõi để cập nhật kịp thời những bản vá trên các hệ điều hành đảm bảo hệ thống máy chủ máy trạm luôn được an toàn.

Hệ thống WSUS (Windows Server Update Services) của Microsoft không những cập nhật bản vá lỗi cho tất cả các sản phẩm khác của hãng bao gồm Internet Explorer, SQL server, Office, Mail; máy chủ Web.

2.2.2. Ghi nhật ký, theo dõi, giám sát hệ thống:

a. Ghi nhật ký:

Giải pháp ghi lại các phiên bản kết nối, các phiên bản đăng nhập của người dùng, các tiến trình hoạt động sẽ giúp quản trị mạng có thể tìm lại dấu vết người dùng, hacker và các lỗi gây ra cho hệ thống trước đó. Các máy chủ Web, máy chủ ứng dụng khác đã được kích hoạt tính năng ghi nhật ký, việc quản lý lưu trữ các thông tin này là rất cần thiết. Chính vì triển khai hệ thống ghi nhật ký tập trung lại một máy chủ chuyên dụng khác là rất hiệu quả. Hệ thống sẽ giúp chúng ta ghi các cảnh báo, thông báo từ các thiết bị cứng như: tường lửa, router, switch, từ các máy chủ web, database và các hệ thống khác.

b. Theo dõi, giám sát:

Theo dõi, giám sát là công việc thường xuyên và quan trọng của nhà quản trị mạng chuyên nghiệp, đó chính là công việc phòng chống hiệu quả trước khi sự cố xuất hiện. Theo dõi, giám sát có thể:

- Phát hiện trên hệ thống mạng có nhiều virus phát tán.
- Giám sát các máy trính trong mạng LAN và trên môi trường Internet.
- Theo dõi hiệu năng hoạt động các phần cứng của máy chủ để tiến hành nâng cấp, bảo trì, bảo dưỡng.

- Phát hiện các công cụ nghe lén mật khẩu, quét các lỗi của hệ thống và các ứng dụng.

- Thống kê số lượng các kết nối, các session cũng như các lưu lượng bất thường trên hệ thống mạng.

2.2.3. Giải pháp mã hóa dữ liệu và đường truyền:

Dữ liệu trên máy chủ, máy tính cá nhân của trung tâm đã được mã hóa nội dung trước khi đưa vào lưu trữ và cả khi đi trên đường truyền.

- Tại các máy chủ và máy tính có thể lưu trữ dữ liệu quan trọng, có dữ liệu cần chia sẻ; tại các thiết bị lưu trữ cần thiết phải tiến hành mã hóa nội dung, điều đó đảm bảo rằng nếu có thể mất thiết bị lưu trữ, máy tính, người tấn công cũng không thể giải mã được dữ liệu.

- Giải pháp Ipsec sẽ được triển khai tại các hệ thống máy chủ và người dùng cũng như các thiết bị mạng phải được cấu hình.

3. Sử dụng dịch vụ đánh giá, phân tích mối đe dọa:

Từ các giải pháp đã đưa ra ở trên để phòng chống tấn công có chủ đích; Tổ công nghệ thông tin trung tâm thường xuyên theo dõi giám sát tình hình hoạt động của hệ thống mạng, máy chủ, máy trạm cũng như các thiết bị khác để từ đó đưa ra các phân tích, đánh giá về các mối đe dọa tấn công vào hệ thống của trung tâm, từ đó lập kế hoạch xử lý các tình huống cụ thể để phòng chống các tấn công có chủ đích vào hệ thống.

4. Đào tạo nâng cao nhận thức bảo mật người sử dụng

Việc đào tạo nâng cao nhận thức về đảm bảo an toàn an ninh thông tin nói chung và nhận thức về bảo mật trong ứng dụng công nghệ thông tin nói riêng là việc làm hết sức cần thiết từng bước nâng cao nhận thức cho người sử dụng. Làm cho người sử dụng thấu hiểu về các rủi ro của việc nhấn vào những liên kết không rõ ràng trong email và nhận biết những kỹ thuật lừa đảo sẽ biến họ thành những đối tác trong cuộc chiến chống lại các mối đe dọa bảo mật, giúp bảo vệ mạng dữ liệu mà họ nắm giữ.

Thông qua việc đào tạo này sẽ trang bị cho cán bộ nhân viên tại trung tâm hiểu được chính sách của trung tâm, cũng như những hiệu quả của cán bộ nhân viên nếu một sự cố an ninh mạng xảy ra do hành động của họ. Từ đó đưa ra các cơ chế, quy chế trong việc vận hành khai thác sử dụng hệ thống công nghệ thông tin của trung tâm, để tất cả cán bộ nhân viên trung tâm có ý thức về an toàn an ninh thông tin trong quá trình làm việc tại trung tâm.

5. Lập kế hoạch ứng phương án phòng chống tấn công có chủ đích đối với hệ thống thông tin tại trung tâm:

Dù nỗ lực hết mình và trang thiết bị những công nghệ đắt tiền thì việc bảo mật của trung tâm vẫn đứng trước nguy cơ bị vi phạm ở điểm nào đó. Vậy cần phải xây dựng một kế hoạch ứng phó sự cố hữu hiệu có thể dập tắt cuộc tấn công, giảm thiểu thiệt hại và chặn bớt rò rỉ dữ liệu, giảm thiểu tổn hại uy tín thương hiệu của đơn vị, cụ thể tại Bệnh viện Mắt – Da liễu tỉnh Cà Mau triển khai các quy chế, cơ chế cảnh báo, phương án phòng ngừa các sự cố về công nghệ thông tin tại trung tâm. Từ các phương án này tổ công nghệ thông tin lập các kế hoạch phân công cụ thể cho từng thành viên trong đơn vị triển khai thực hiện đảm bảo an toàn an ninh cho hệ thống thông tin của trung tâm

6. Một số phương án cụ thể về phòng ngừa đối phó với tấn công có chủ đích:

STT	Tình huống	Các phòng ngừa
Tình huống sự cố do bị tấn công mạng		
1	Tấn công Phishing (hay tấn công giả mạo): là hình thức tấn công mạng phổ biến khi kẻ tấn công làm giả Website của một đơn vị uy tín để lừa đảo người dùng nhập thông tin.	<ul style="list-style-type: none"> - Kiểm tra kỹ các email, tin nhắn, đường link website trước khi thực hiện nhập thông tin. - Cài đặt các phần mềm cảnh báo, quét mã độc cho website. - Cảnh giác với website sử dụng HTTP (kém an toàn) thay vì HTTPS (an toàn hơn).
2	Tấn công mạng từ bên trong: tin tặc có thể cài phần mềm gián điệp vào máy tính cá nhân của các thành viên trong công ty, hoặc lấy được tài khoản và mật khẩu của nhân viên sau đó thực hiện hành vi tấn công của mình.	<ul style="list-style-type: none"> - Hạn chế sử dụng mạng wifi công cộng bởi chúng có thể khiến thiết bị nhiễm mã độc. - Đặt mật khẩu phức tạp để tránh các cuộc tấn công Password. - Bật tính năng xác thực 2 lớp qua tin nhắn.
3	Tấn công gián tiếp: Tin tặc có thể tấn công một đối tượng thông qua việc tấn công một đối tác của đối tượng đó. Điển hình là tấn công chuỗi cung ứng.	<ul style="list-style-type: none"> - Sử dụng Firewall và các chương trình diệt virus, Malware. - Luôn kiểm tra dữ liệu vào – ra. - Lựa chọn các sản phẩm ứng dụng có nguồn gốc rõ ràng đảm bảo độ tin cậy.



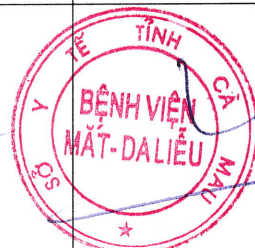

STT	Tình huống	Các phòng ngừa
4	Tấn công theo tệp đính kèm: File đính kèm email, tệp đính kèm tin nhắn facebook là những công cụ tấn công mạng phổ biến của tin tặc. sau khi người dùng click vào tệp đính kèm sẽ lập tức dính virus, gây nhiều hậu quả nghiêm trọng.	<ul style="list-style-type: none"> - Người sử dụng email: luôn kiểm tra người gửi, không download các tệp tin không rõ nguồn gốc. - Với mạng xã hội và các dịch vụ khác: khuyến cáo người sử dụng tải file đính kèm không rõ nguồn gốc.
5	Tấn công truy cập trái phép, chiếm quyền điều khiển: truy cập vào dữ liệu, chiếm đoạt truy cập và leo thang đặc quyền.	<ul style="list-style-type: none"> - Với kiểu tấn công vào mật khẩu: <ul style="list-style-type: none"> + Đặt mật khẩu mạnh. Không sử dụng mật khẩu ở bản rõ cả khi lưu trữ hoặc truyền trên mạng. + Trong các khuyến nghị về chính sách an ninh mạng, đều yêu cầu phải ghi lại nhật ký hệ thống. bằng cách xem xét các bản ghi nhật ký. Admin có thể biết được các thông tin về số lần truy cập không thành công. Nếu phát hiện từ một địa chỉ IP có số lần truy cập không thành công vượt quá giới hạn cho phép thì đây rất có thể là do tấn công vào mật khẩu. ví dụ về việc phân tích nhật ký hệ thống để phát hiện về số lần đăng nhập, ví dụ trong bài viết này. - Với kiểu tấn công lợi dụng sự tin cậy, admin cần giảm thiểu việc cấu hình giữa các hệ thống. ví dụ, khi bạn dùng trình duyệt IE trên máy chủ windows server, mỗi khi bạn vào một website thì máy chủ Ie đều hỏi bạn xem có trust cái site đó không. Bạn hãy cân nhắc kỹ trước khi đưa website đó vào danh mục Trust bởi vì nếu máy chủ web đó bị khống chế bởi hacker thì bạn sẽ gặp nguy cơ, ... - Với kiểu tấn công MITM: vì kẻ đứng giữa cần nhân bản giữ liệu mà hãm chặn bắt, do vậy sẽ tiêu tốn nhiều băng thông. Admin cần có công cụ giám sát băng thông để phát hiện ra việc này.

STT	Tình huống	Các phòng ngừa
		<p>Ví dụ về các phần mềm giám sát hoặc phần mềm giám sát băng thông.</p> <ul style="list-style-type: none"> - Với kiểu tấn công tràn bộ đệm, ban đầu cần có công cụ giám sát trạng thái của các tiến trình đang chạy trong hệ thống, ví dụ hai công cụ Event Viewer Viewer kết hợp với PERformance monitor trên windows.
6.	Tấn công thay đổi giao diện.	<ul style="list-style-type: none"> - Xem những thông tin nhật ký, file log của máy chủ và truy tìm xem hacker đã làm gì và làm như thế nào trên hệ thống của mình.
7	Tấn công mã hóa phần mềm, dữ liệu thiết bị	<ul style="list-style-type: none"> - Cài đặt duy trì phần mềm chống virus. - Công cụ chống phần mềm độc hại.
8	Tấn công phá hoại thông tin, dữ liệu phần mềm.	<ul style="list-style-type: none"> - Cài đặt và duy trì phần mềm virus. - Công cụ chống phần mềm độc hại.
9	<p>Tấn công nghe trộm, gián điệp lấy cắp thông tin, dữ liệu.</p> <p>Tấn công tổng hợp sử dụng kết hợp nhiều hình thức.</p> <p>Các hình thức tấn công mạng.</p>	<ul style="list-style-type: none"> - Cập nhật máy tính, phần mềm. - Cài đặt và duy trì phần mềm virus. - Công cụ chống phần mềm độc hại.
10	Tấn công vào con người: kẻ tấn công có thể liên lạc với người quản trị hệ thống tạo nên một hộp thoại đăng nhập sau đó yêu cầu người dùng thay đổi mật khẩu, thay đổi cấu hình hệ thống. phương thức tấn công mạng này rất khó tìm ra giải pháp ngăn chặn triệt để ngoài giáo dục con người.	<ul style="list-style-type: none"> - Nâng cao nhận thức, kiến thức khi sử dụng internet và các dịch vụ online. - Một số hình thức, phương thức tấn công vào hệ thống mạng, máy tính khác như: thông qua usb, đĩa CD, địa chỉ IP, server, qua đầu vào của máy in, ...

SỞ Y TẾ TỈNH CÀ MAU
BỆNH VIỆN MẮT – DA LIỄU

PHƯƠNG ÁN
CHỐNG TẤN CÔNG XÂM NHẬP TỪ XA (DOS, DDOS)
CƠ CHẾ CHỐNG TẤN CÔNG TỪ CHỐI DỊCH VỤ TRÊN HỆ
THỐNG CỦA BỆNH VIỆN MẮT – DA LIỄU TỈNH CÀ MAU

PHƯƠNG ÁN
CHỐNG TẤN CÔNG XÂM NHẬP TỪ XA (DOS, DDOS)
CƠ CHẾ CHỐNG TẤN CÔNG TỪ CHỐI DỊCH VỤ TRÊN HỆ
THỐNG CỦA BỆNH VIỆN MẮT – DA LIỄU TỈNH CÀ MAU
(Ban hành theo Quyết định số 54B/QĐ- BVMDL ngày 26/06/2025
của Bệnh viện Mắt Da liễu Cà Mau)

	Người lập	Người xem xét	Người phê duyệt
Họ tên	Lê Minh Nhựt	Trần Kim Thanh	Huỳnh Trung Lâm
Ký tên		 	
Chức vụ	Tổ trưởng CNTT	Trưởng phòng Kế hoạch – Tổng hợp	Giám đốc
Ngày	26/06/2025	26/06/2025	26/06/2025

PHƯƠNG ÁN CHỐNG TẤN CÔNG XÂM NHẬP TỪ XA (DOS, DDOS) CƠ CHẾ CHỐNG TẤN CÔNG TỪ CHỐI DỊCH VỤ TRÊN HỆ THỐNG CỦA BỆNH VIỆN MẮT – DA LIỄU TỈNH CÀ MAU

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 xa (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 thống 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, bất 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.

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

3. Các cách thức tấn công:

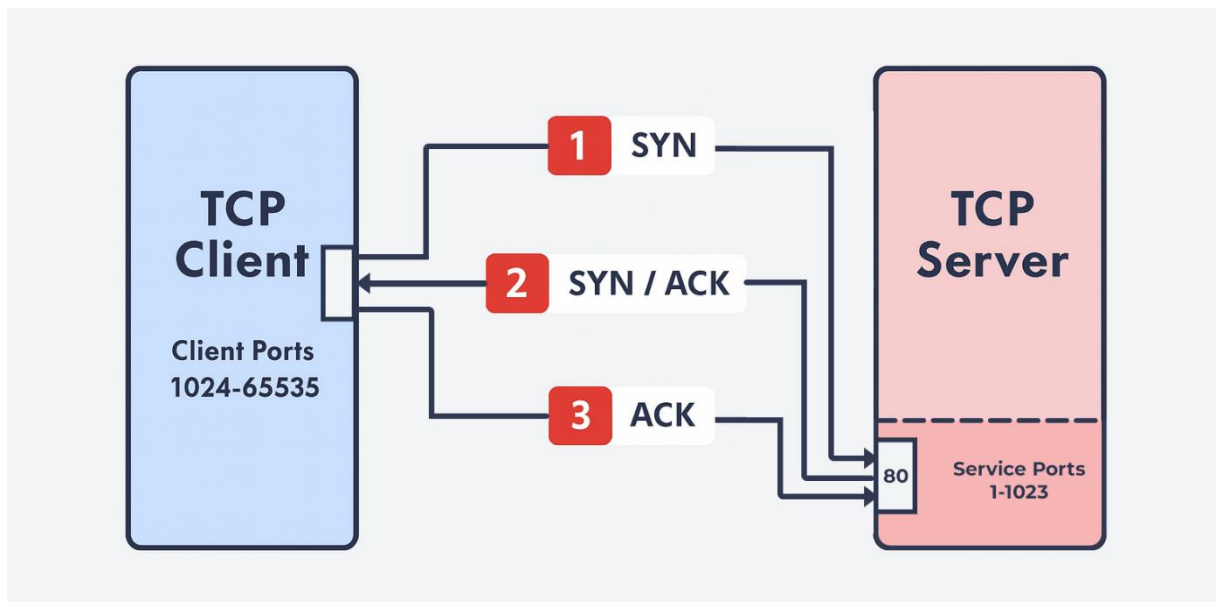
3.1. Tấn công thông qua kết nối SYN Flood Attack:

- 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.

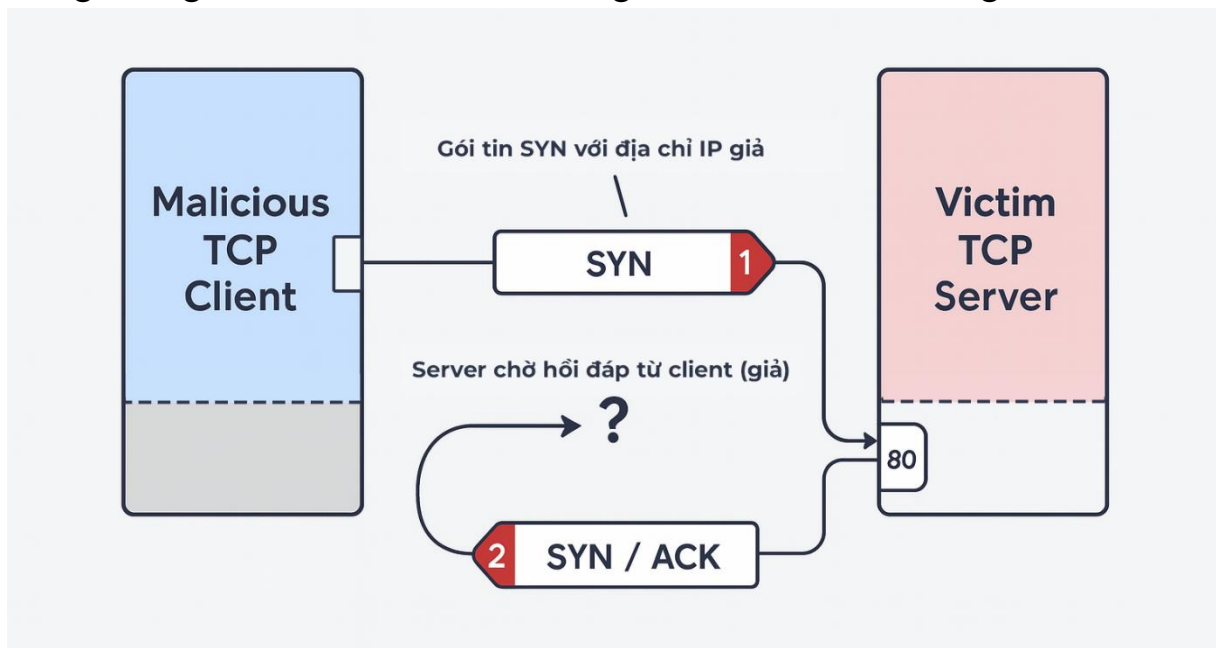
- + Bước 2: Khi nhận được gói tin này, server sẽ gửi lại gói tin SYN/ACK để thông báo cho client biết là nó đã nhận được yêu cầu kết nối và chuẩn bị tài nguyên cho việc yêu cầu này. Server sẽ giành một phần tài nguyên hệ thống như bộ nhớ đệm (cache) để nhận và truyền dữ liệu. Ngoài ra, các thông tin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



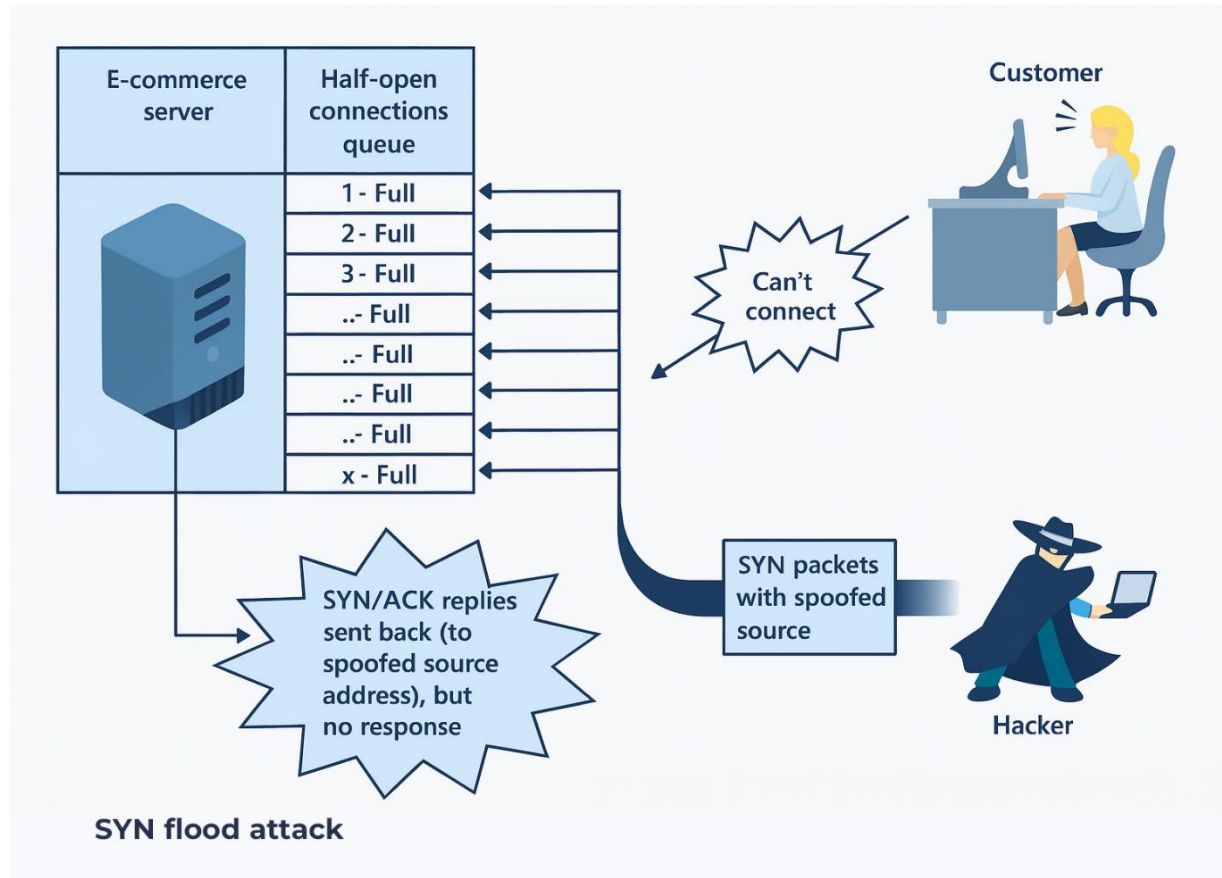
- Do TCP là thủ tục tin cậy trong việc giao nhận (end-to-end) nên trong lần bắt tay thứ hai, server gửi các gói tin SYN/ACK trả lời lại client mà không nhận lại được hồi âm của client để thực hiện kết nối thì nó vẫn bảo lưu nguồn tài nguyên chuẩn bị kết nối đó và lặp lại việc gửi gói tin SYN/ACK cho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



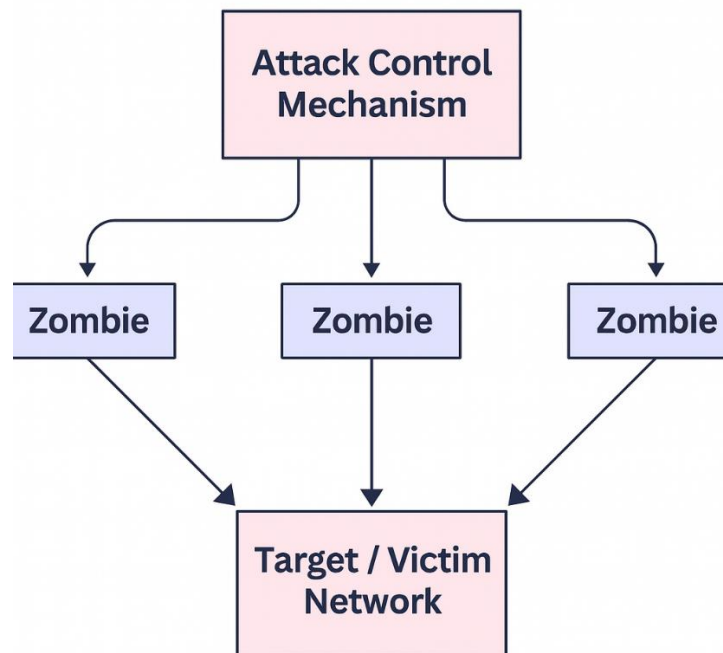
- Nếu quá trình đó kéo dài, server sẽ nhanh chóng trở nên quá tải, dẫn đến tình trạng crash (treo) nên các yêu cầu hợp lệ sẽ bị từ chối không thể đáp ứng được. Có thể hình dung quá trình này cũng giống hư khi máy tính cá nhân (PC) hay bị “treo” khi mở cùng lúc quá nhiều chương trình cùng lúc vậy.

- 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.



- 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

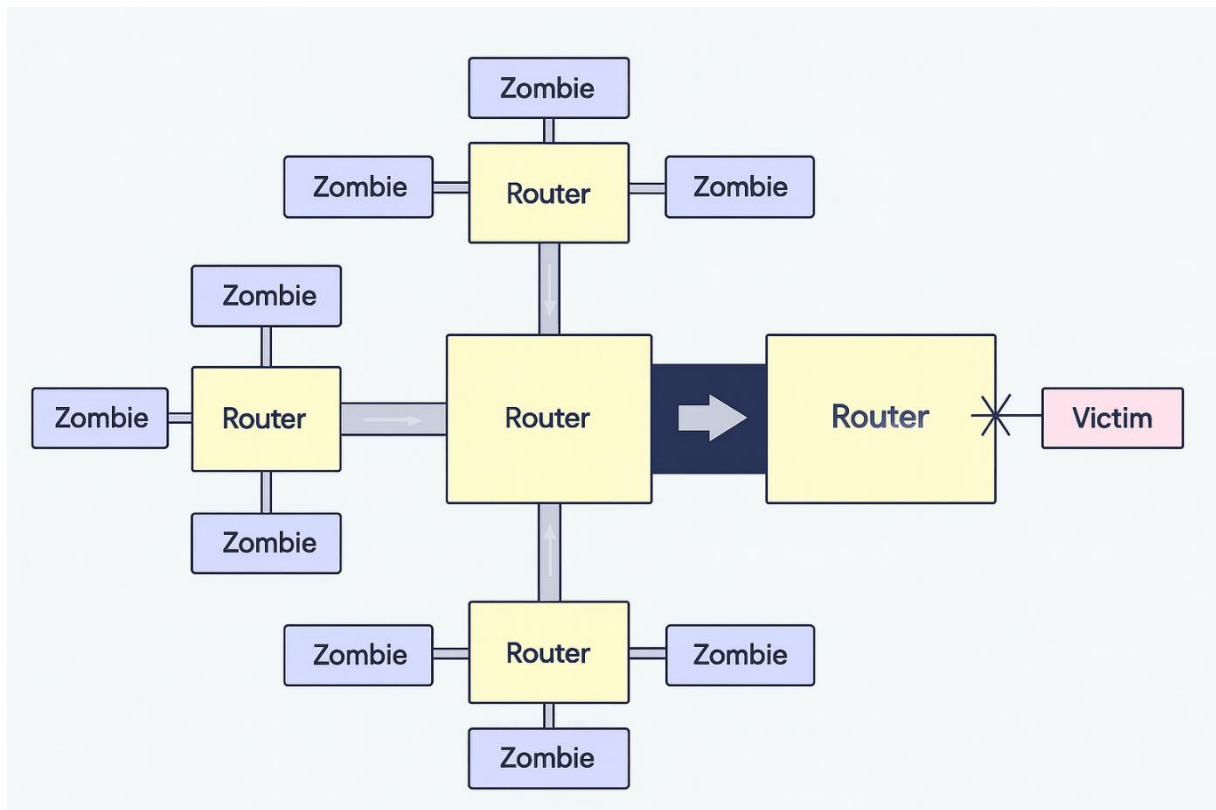
- + Hacker gửi gói tin UDP echo với địa chỉ IP nguồn là cổng loopback của chính mục tiêu cần tấn công hoặc của một máy tính trong cùng mạng.
- + Với mục tiêu sử dụng cổng UDP echo (port 7) để thiết lập việc gửi và nhận các gói tin echo trên 2 máy tính (hoặc giữa mục tiêu với chính nó nếu mục tiêu có 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.

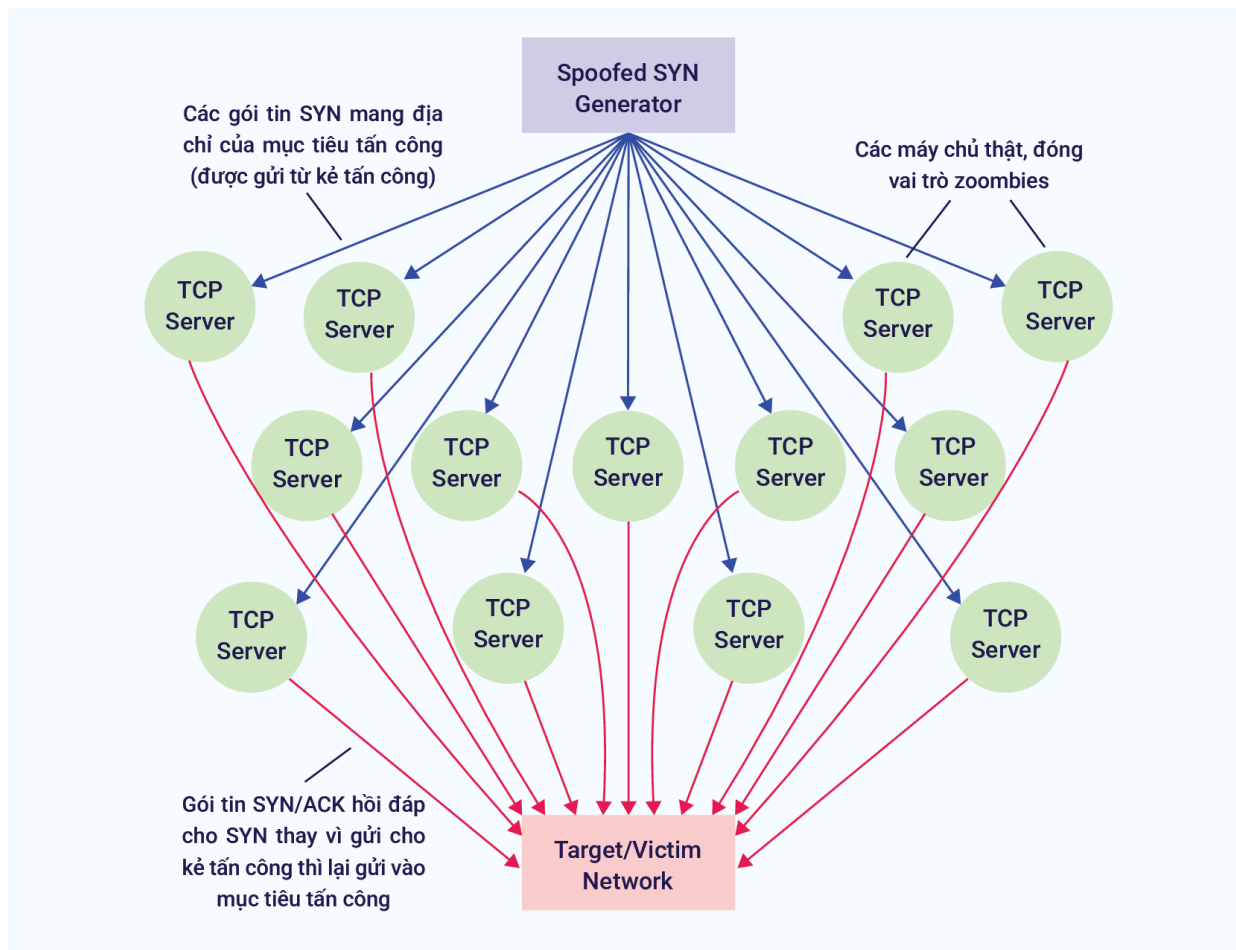


- Nói nôm na là nó giống như tình trạng kẹt xe vào giờ cao điểm vậy. Ví dụ rõ nhất là sự “cộng hưởng” trong lần truy cập điểm thi đại học vừa qua khi có quá nhiều máy tính yêu cầu truy cập cùng lúc làm dung lượng đường truyền hiện tại của máy chủ không tài nào đáp ứng nổi.

- 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 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)

- 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, Microsoft, ... 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 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. 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 niệm 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 “phản 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 ngăn 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 niệm 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:

Honeypots:

- Một kỹ thuật đang được nghiên cứu là Honeypots. Honeypots 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.

- Honeypots 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 Honeypots đã thiết lập sẵn các cơ chế giám sát và báo động.

- Ngoài ra Honeypots còn có giá trị trong việc học hỏi và rút kinh nghiệm từ Attacker, do Honeypots 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 Honeypots 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:

STT	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 tổn tài nguyên bằng cách giả mạo IP nguồn để các máy chủ mục tiêu phản hồi về máy 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 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 nhận 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.

STT	Tình huống	Cách phòng tránh
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.
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.