HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN XUÂN GIANG

NGHIÊN CỨU GIẢI PHÁP BẢO MẬT WEBSITE CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI - 2021

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN XUÂN GIANG

NGHIÊN CỨU GIẢI PHÁP BẢO MẬT WEBSITE CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ

CHUYÊN NGÀNH: HỆ THỐNG THÔNG TIN

MÃ SỐ: 8.48.01.04

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TS. LÊ HỮU LẬP

HÀ NỘI - 2021

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn này là công trình nghiên cứu của cá nhân tôi trong thời gian qua, được thực hiện dưới sự hướng dẫn khoa học của PGS.TS. Lê Hữu Lập. Mọi thông tin, số liệu được sử dụng, phân tích trong luận văn là kết quả nghiên cứu do tôi tự tìm hiểu, tham khảo những tài liệu, bài viết được đăng tải trên những tạp chí khoa học và các trang web được liệt kê trong danh mục tài liệu tham khảo.

Tôi xin hoàn toàn chịu trách nhiệm nếu có sự không trung thực trong thông tin sử dụng trong công trình nghiên cứu này.

Hà nội, ngày tháng năm 2021

Người cam đoan

Nguyễn Xuân Giang

LỜI CẢM ƠN

Được sự đồng ý của Học viện Công nghệ Bưu chính Viễn thông và sự đồng ý của thầy giáo hướng dẫn PGS.TS. Lê Hữu Lập, học viên đã thực hiện đề tài luận văn tốt nghiệp Thạc sĩ: "Nghiên cứu giải pháp bảo mật website cho các doanh nghiệp vừa và nhỏ".

Để hoàn thành luận văn này, học viên xin chân thành cảm ơn các thầy cô giáo đã tận tình hướng dẫn, giảng dạy trong suốt quá trình học tập, nghiên cứu và rèn luyện ở Học viện Công nghệ Bưu chính Viễn thông.

Học viên xin chân thành cảm ơn thầy giáo PGS.TS. Lê Hữu Lập đã tận tình, chu đáo hướng dẫn trong quá trình thực hiện luận văn này.

Học viên đã có nhiều cố gắng để thực hiện luận văn một cách hoàn chỉnh nhất. Tuy nhiên, do còn nhiều hạn chế về kiến thức và kinh nghiệm nên không thể tránh khỏi những thiếu sót nhất định mà học viên chưa thấy được. Học viên rất mong nhận được sự góp ý của quý Thầy, Cô giáo và các bạn đồng nghiệp để luận văn được hoàn chỉnh hơn.

Học viên xin trân trọng cám ơn!

Hà Nội, ngày tháng năm 2021

Học viên

Nguyễn Xuân Giang

MỤC LỤC

DANH MỤC CÁC THUẬT NGỮ VIẾT TẮT

Viết tắt	Tiếng Anh	Tiếng việt
APT	Advanced Persistent Threat	Tấn công có chủ đích
CSRF	Cross Site Request Forgery	Giả mạo yêu cầu trang web liên quan
DDoS	Distribute Denial of Service	Tấn công từ chối dịch vụ phân tán
DMZ	Demilitarized Zone	Vùng nhận dạng
DoS	Denial of Service	Tấn công từ chối dịch vụ
HTTP	Hyper Text Transfer Protocol	Giao thức truyền tải siêu văn bản
HTTPS	HTTP Secure	Giao thức HTTP có bảo mật
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập
IPS	Intrusion Prevention System	Hệ thống ngăn chặn xâm nhập
ISS	Internet Security Systems	Hệ thống bảo mật Internet
NSM	Network System Monitor	Hệ thống giám sát bảo mật mạng
OWASP	Open Web Application Security Project	Dự án mở về bảo mật ứng dụng Web
DRDoS	Distributed Reflection Denial of Service	Tấn công từ chối dịch vụ phản xạ nhiều vùng
SQL	Structured Query Language	Ngôn ngữ truy vấn cấu trúc

SSL	Secure Sockets Layer	Lớp Socket bảo mật
TCP	Transmission Control Protocol	Giao thức kiểm soát truyền tin
TLS	Transport Layer Security	Bảo mật lớp vận chuyển
XSS	Cross-Site Scripting	Tấn công thực thi mã script
WAF	Web Application Firewall	Tường lửa ứng dụng web

DANH MỤC HÌNH VẼ

MỞ ĐẦU

Trong thời đại công nghiệp 4.0, vấn đề an ninh mạng ngày càng trở nên nóng bỏng với hàng loạt vụ tấn công nhằm vào các website của các cơ quan nhà nước và doanh nghiệp, đặc biệt là những doanh nghiệp vừa và nhỏ. Theo số liệu của Tổng cục Thống kê, tính đến hết năm 2020, cả nước có khoảng 900 nghìn doanh nghiệp đang hoạt động, trong đó, số lượng doanh nghiệp vừa, nhỏ và siêu nhỏ chiếm 98%. Đây sẽ là mảnh đất màu mỡ cho các hacker tấn công, làm ngừng trệ các dịch vụ dựa trên nền tảng website, gây ảnh hưởng nghiêm trọng đến kinh tế, uy tín và hoạt động điều hành của các cơ quan nhà nước và doanh nghiệp.

Các chuyên gia bảo mật đã liệt kê một số cách mà việc bị tin tặc tấn công có thể gây hại cho các cơ quan nhà nước cũng như các doanh nghiệp như sau [24]:

** Mất lưu lượng truy cập.*

Đây là một vấn đề vô cùng quen thuộc nhưng vẫn chưa bao giờ bớt nghiêm trọng. Cùng với việc các doanh nghiệp tập trung vào nền tảng online của họ để đảm bảo trải nghiệm tiện lợi và kết nối với người dùng hiệu quả, thời gian website ngừng hoạt động có thể tương đương với những tổn thất vô cùng lớn. Do bản chất liên tục được truy cập bởi người dùng, các doanh nghiệp mua sắm trực tuyến đặc biệt cần chú ý trang bị giải pháp giám sát và bảo vệ hợp lý.

Mất lưu lượng truy cập có thể do những lý do khác nhau, điển hình là do bị liệt vào danh sách đen của các bộ máy tìm kiếm do chứa mã độc. Google thực hiện việc này bằng cách hiện dòng chữ "trang web này có thể bị hack" bên cạnh kết quả tìm kiếm kèm với thông báo bảo mật toàn màn hình khi người dùng click vào. Với nhiều website, lượng tiếp cận tự nhiên hầu như đến từ các bộ máy tìm kiếm. Việc bị "chỉ điểm" bởi các bộ máy tìm kiếm sẽ khiến một lượng lớn người dùng rời khỏi website mà họ đang định truy cập.

** Lây lan malware sang máy tính người dùng.*

Với sự bùng nổ của tiền ảo và công nghệ blockchain trong những năm gần đây, cộng đồng mạng đã chứng kiến những biến thể vô cùng mới mẻ đang gia nhập

vào kho malware toàn cầu: malware đào tiền ảo. Loại malware này khi bị chèn vào website sẽ ngầm dùng CPU của người dùng để đào đồng tiền ảo Monero và các loại tiền ảo khác cho tin tặc.

Điều xảy ra tiếp theo là mỗi khi người dùng truy cập website đó, máy tính của họ sẽ đột ngột chậm đi hoặc họ sẽ được trình diệt virus cảnh báo về mã độc tồn tại trên website. Trong trường hợp người đó không có trình duyệt virus trong máy tính, chính website này sẽ chịu trách nhiệm cho việc để lây lan malware sang thiết bị của họ.

** Mất uy tín thương hiệu.*

Đây là vấn đề thật sự lớn. Sau khi tìm hiểu về những vấn đề trên, hẳn chúng ta đã có cái nhìn rõ hơn rằng nếu website không được thực hiện bảo mật một cách hiệu quả, người dùng sẽ nhanh chóng nắm được. Họ sẽ được cảnh báo bởi bộ máy tìm kiếm, các ứng dụng diệt virus và phần mở rộng trình duyệt. Trải nghiệm của họ với website sẽ không hề tích cực.

Điều gì sẽ xảy ra nếu dữ liệu của các cơ quan, các doanh nghiệp, bị mất vào tay tin tặc? Uy tín của những đơn vị này sẽ bị ảnh hưởng nghiêm trọng. Còn nếu chúng ta không may trở thành nạn nhân của một vụ lộ thông tin nhạy cảm - như thông tin thanh toán - xử lý rủi ro sẽ vô cùng khó khăn và tốn kém.

** Tốn kém chi phí.*

Chốt lại, tổn thất của mỗi hệ quả của việc bị hack website có thể được đo bằng những khoản phí tổn. Phí dọn sạch malware và phục hồi dữ liệu mới chỉ là bước đầu. Các chiến dịch marketing sẽ phải bị hủy bỏ. Nguồn lực và thời gian sẽ bị lãng phí. Lợi nhuận sẽ sa sút nghiêm trọng. Khách hàng sẽ rời bỏ dịch vụ. Tổng chi phí dành cho các cuộc tấn công mạng trên toàn cầu đã đạt tới con số 100 tỉ đô la Mỹ.

Như đã nói ở trên, tin tặc có động lực về lợi nhuận khi thực hiện hack website. Với động lực đó, có thể khẳng định tội phạm mạng sẽ còn tăng trưởng theo cấp số nhân trong thời gian tới.

Thực tế cho thấy việc bảo mật website ở những doanh nghiệp vừa và nhỏ hiện nay đang tồn tại những yếu kém, vấn đề an toàn bảo mật chưa được quan tâm đúng mức. Có rất nhiều lí do khiến cho tình trạng bảo mật website còn yếu

kém ở Việt Nam nói chung và các doanh nghiệp vừa vả nhỏ nói riêng. Dưới đây là một số lí do chính:

Thứ nhất: nguồn nhân lực công nghệ thông tin mỏng, đặc biệt là chưa có hoặc rất ít đơn vị có chuyên viên bảo mật phụ trách riêng

Thứ hai: Sự nhận thức hạn chế về an toàn bảo mật của người sử dụng

Thứ ba: Chỉ coi trọng việc đăng tin và truy cập được đến website, chưa coi trọng việc phát hiện và phòng ngừa điểm yếu của website

Thứ tư: không rà quét thường xuyên các lỗ hổng bảo mật của website và hạ tầng công nghệ thông tin của đơn vị

Thứ năm: Không cập nhật thường xuyên các bản vá lỗi cho website, cho hệ thống thông tin của đơn vị

Vì vậy, vấn đề nghiên cứu các giải pháp bảo mật website có tính cấp thiết, có ý nghĩa khoa học và thực tiễn. Từ nhu cầu phát triển, đòi hỏi các cơ quan, tổ chức, doanh nghiệp phải có biện pháp đảm bảo an toàn cho website của mình.

Từ những lý do trên và đặc thù công việc quản lý nhà nước tại Sở Thông tin và Truyền thông Hà Nội, học viên đã chọn đề tài **"Nghiên cứu giải pháp bảo mật website cho các doanh nghiệp vừa và nhỏ"** cho luận văn tốt nghiệp trình độ đào tạo thạc sĩ.

1. Mục đích nghiên cứu:

Mục đích chính của luận văn là nghiên cứu các giải pháp bảo mật website và đánh giá mức độ bảo mật của một website bất kỳ.

2. Đối tượng và phạm vi nghiên cứu:

- Đối tượng nghiên cứu của luận văn là các ứng dụng website và các vấn đề liên quan đến bảo mật website.

- Phạm vi nghiên cứu của luận văn là: các giải pháp bảo mật website và đánh giá mức độ bảo mật của một website bất kỳ.

3. Phương pháp nghiên cứu:

- Về mặt lý thuyết: Thu thập, khảo sát, phân tích các tài liệu và thông tin có liên quan đến các bảo mật website.

- Về mặt thực nghiệm: Khảo sát thực tế và đánh giá mức độ bảo mật của một website bất kỳ.

Bố cục của luận văn gồm 3 chương chính với các nội dung sau:

Chương 1: Tổng quan bảo mật Website

Nội dung của Chương 1 là tìm hiểu các lỗi bảo mật và các phương thức tấn công website của hacker.

Chương 2: Các giải pháp đảm bảo an toàn thông tin của Website

Nội dung của Chương 2 luận văn tập trung nghiên cứu các giải pháp đảm bảo an toàn thông tin của website, trong đó đi sâu vào biện pháp tấn công từ chối dịch vụ.

Chương 3: Đánh giá mức độ bảo mật website của Sở Thông tin và Truyền thông Hà Nội

Chương 3 của luận văn tiến hành đánh giá mức độ bảo mật website Sở Thông tin và Truyền thông Hà Nội và đưa ra các giải pháp nâng cao bảo mật.

CHƯƠNG 1. TỔNG QUAN VỀ BẢO MẬT WEBSITE

Nội dung của Chương 1 sẽ tìm hiểu các lỗi bảo mật và các phương thức tấn công website của hacker.

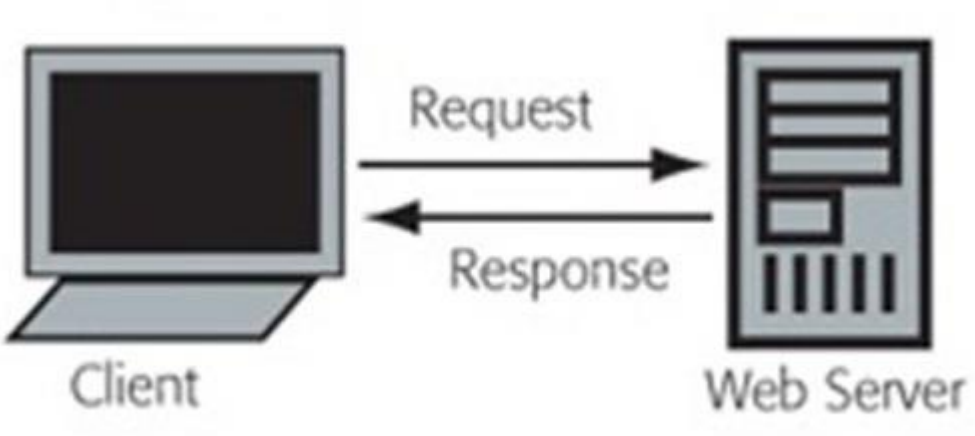
1.1. Một số loại website phổ biến

Có nhiều tiêu chí để phân loại website, để phân loại một cách tổng quan, chính xác và đầy đủ, học viên sẽ tập trung vào các tiêu chí như cấu trúc website, chức năng, quyền sở hữu và tính bảo mật.

1.1.1. Phân loại theo cấu trúc website

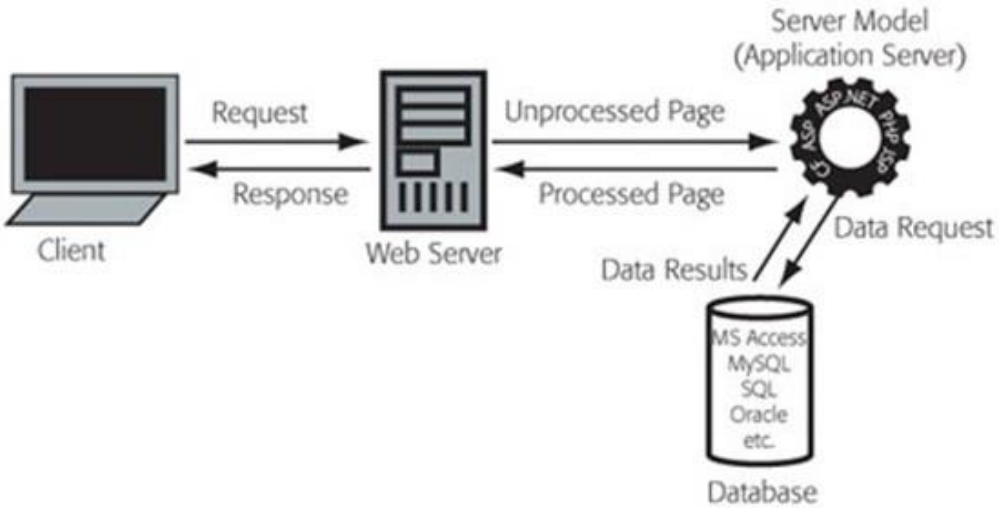
Phân loại website theo cấu trúc cũng có thể hiểu là dạng dữ liệu, cách vận hành của trang web. Hiện nay có 02 loại cấu trúc web bao gồm [5][6]:

Website tĩnh (static website): Website tĩnh ở đây được hiểu theo nghĩa là dữ liệu website không được thay đổi thường xuyên. Loại website này được lập trình dựa trên nền tảng HTML, CSS và Javascript. Nếu muốn thay đổi nội dụng trên website, quản trị viên phải sửa đổi trực tiếp trên mã lệnh và chỉ những người am hiểu về ngôn ngữ lập trình mới có thể thực hiện thao tác này. Chính vì thế mà website tĩnh hiện nay không được sử dụng phổ biến.



Hình 1.1 Phương thức hoạt động của website tĩnh

Website động (dynamic website): Hầu hết các website hiện nay đều thuộc cấu trúc website động. Khác với website tĩnh, website động luôn luôn có thông tin mới do các thông tin này được cập nhật thường xuyền bởi các quản trị viên. Các thông tin mới này được lưu vào cơ sở dữ liệu của website và đưa ra sử dụng dựa theo yêu cầu của người dùng. Hiện nay có nhiều ngôn ngữ lập trình được sử dụng để lập trình các website động như HTML, CSS, Javascript, PHP hay ASP.NET…



Hình 1.2 Phương thức hoạt động của website động

1.1.2. Phân loại theo chức năng

1.1.2.1. Trang website thương mại điện tử

Website thương mại điện tử là một trang web mà mọi người có thể trực tiếp mua sản phẩm từ đó. Hầu hết các thương hiệu sản phẩm lớn và nhiều thương hiệu nhỏ hơn đều có một trang web này. Bất kỳ trang web nào có giỏ hàng và cần cung cấp thông tin thanh toán để mua hàng đều thuộc loại thương mại điện tử. Một số ví dụ điển hình như shopee.vn, tiki.vn, lazada.vn…

1.1.2.2. Website landing page giới thiệu sản phẩm

Khác với trang website thương mại điện tử, một trang landing page giới thiệu sản phẩm đơn giản chỉ cung cấp thông tin về một loại sản phẩm, dịch vụ nào đó của doanh nghiệp.

Trang web thường được tạo nhanh chóng và cấu trúc đơn giản với chỉ một mục tiêu là cung cấp thông tin cho người xem website. Thường được sử dụng khi doanh nghiệp ra mắt sản phẩm hoặc dịch vụ mới.

1.1.2.3. Trang website giải trí

Đây là dạng website cung cấp nội dung phục vụ cho một nhu cầu giải trí cụ thể nào đó, chẳng hạn như: nghe nhạc, xem phim hay chơi game. Ngày càng có nhiều trang web giải trí khác nhau ra đời, nhằm phục vụ cho nhu cầu thư giãn, giải trí của người dùng và mục đích kinh doanh của chủ sở hữu.

1.1.2.4. Website tin tức

Đây là loại website cung cấp thông tin văn hóa, chính trị, xã hội, sức khỏe, giáo dục… cho độc giả. Chủ sở hữu của dạng website này thường là các cơ quan Nhà nước, hiệp hội, tổ chức, tòa soạn được cấp phép.

1.1.2.5. Mạng xã hội

Mạng xã hội là dạng website cho phép mỗi cá nhân và doanh nghiệp tạo ra một không gian mạng riêng cho chính mình bằng cách tạo tài khoản. Mỗi tài khoản sẽ có thể đăng tải thông tin, viết nhật ký, chia sẻ bất cứ điều gì mà mình quan tâm trên trang cá nhân. Phần lớn người dùng mạng xã hội là để phục vụ cho nhu cầu giải trí, kết nối, liên lạc với bạn bè. Những trang mạng xã hội phổ biến nhất hiện nay như: Facebook, Twitter, Instagram, Tumblr, Youtube, Zalo,….

1.1.2.6. Website diễn đàn

Website diễn đàn là những trang web tập trung những người có cùng chung một sở thích, công việc, tư tưởng. Mỗi tài khoản sẽ chia sẻ thông tin, quan điểm của mình về những vấn đề xung quanh lĩnh vực của diễn đàn. Khác với mạng xã hội, diễn đàn mang tính đóng hơn và tập trung vào một lĩnh vực duy nhất.

1.1.2.7. Website rao vặt

Website này cung cấp một nền tảng cho phép khách hàng đăng tin về sản phẩm muốn mua, bán. Khác biệt với các website thương mại điện tử là sẽ không có giao dịch trên website rao vặt, mà những giao dịch sẽ được thực hiện trực tiếp khi người xem hàng và người bán hàng đạt được thỏa thuận.

1.1.2.8. Website cổng thông tin điện tử của tổ chức nhà nước, chính phủ, trường học, bệnh viện

Là những website đại diện cho một tổ chức thuộc nhà nước như các sở, cục, vụ, bộ, với mục đích hoạt động là cung cấp thông tin chính thống cho người dân về hoạt động của tổ chức nhà nước. Những website này thường được đăng ký tên miền gov. Những website của tổ chức giáo dục như các trường học thường được đăng ký tên miền edu.

1.1.3. Phân loại theo quyền sở hữu

Website doanh nghiệp: là trang web đại diện cho một doanh nghiệp cụ thể. Website được tạo ra với mục đích giới thiệu doanh nghiệp, cập nhật thông tin hoạt động, quảng bá sản phẩm dịch vụ và còn rất nhiều chức năng khác. Tất cả các đơn vị đều có nhu cầu quảng bá hình ảnh của mình nên website doanh nghiệp được xem là một phần không thể thiếu đối với các công ty hiện nay. Ví dụ website của công ty sữa Vinamilk: https://www.vinamilk.com.vn

Website cá nhân: Khác với trang web doanh nghiệp, website cá nhân chỉ thuộc quyền sở hữu của một người nào đó. Loại website này chỉ phổ biến với người của công chúng, những người cần quảng bá hình ảnh cá nhân để phục vụ cho mục đích thương mại hay công việc. Chẳng hạn như: chính trị gia, ca sĩ, nhà thiết kế, nhà văn, nhà thuyết giảng…

1.1.4. Phân loại theo tính bảo mật

Tất cả các website được công bố trên không gian mạng internet đều cần được bảo mật, nhưng tùy vào chức năng và mục đích hoạt động mà yêu cầu mức độ bảo mật cũng khác nhau. Chúng ta có thể phân loại các website theo cấp độ bảo mật như sau:

1.1.4.1. Website cần tính bảo mật thấp

Những trang web được liệt kê vào phân loại này thường là những website tĩnh hoặc các landing page, chỉ có mục đích cung cấp thông tin về sản phẩm, dịch vụ của doanh nghiệp.

Những trang web dạng này thường không khắt khe về tính bảo mật vì những thông tin cung cấp không mang tính chất nhạy cảm.

1.1.4.2. Website cần tính bảo mật trung bình

Những trang web ở loại này thường là những website chỉ cung cấp thông tin giải trí, tin tức thông thường như trang thông tin điện tử tổng hợp hoặc blog cá nhân.

Những thông tin cần bảo mật ở những website này chỉ là những thông tin về hình ảnh, bài viết của chính website.

1.1.4.3. Website cần tính bảo mật cao

Đây thường là những website cung cấp các dịch vụ như mua bán hàng hóa, cung cấp thông tin cá nhân, doanh nghiệp. Có thể liệt kê các website thương mại điện tử, các diễn đàn, mạng xã hội nhỏ.

Những thông tin của khách hàng như thông tin cá nhân, thông tin thanh toán, hình ảnh cá nhân đều mang tính chất nhạy cảm do đó những trang web này cần tính bảo mật cao. Đảm bảo không để rò rỉ thông tin quan trọng, tạo cơ hội cho hacker tấn công gây thiệt hại cho khách hàng và doanh nghiệp.

1.1.4.4. Website cần tính bảo mật rất cao

Những website yêu cầu tính bảo mật rất cao thường là những website thuộc các tổ chức chính phủ, nhà nước. Những thông tin là phát ngôn của tổ chức nhà nước nếu bị tin tặc tấn công gây sai lệch sẽ gây ra những hậu quả vô cùng nghiêm trọng.

Bên cạnh đó những mạng xã hội với lượng người dùng rất lớn như facebook, twitter, youtube, zalo cũng là những website cần tính bảo mật rất cao. Vì lượng thông tin cá nhân rất lớn lên đến hàng triệu, hàng tỉ thông tin cá nhân. Nếu bị tin tặc tấn công và lợi dụng cũng sẽ gây ra những thiệt hại vô cùng lớn.

1.2. Tình hình tấn công website trên thế giới và Việt Nam [11][13][14][15]

Trong 9 tháng đầu năm 2020, báo cáo mới được công bố đã ghi nhận xu hướng tích cực của an ninh website trên toàn cầu. Cụ thể, hệ thống CyStack

Attack Map ghi nhận 343.365 vụ tấn công vào website, giảm 24,7% so với cùng kỳ năm trước.

Dấu hiệu tích cực còn thể hiện ở xu hướng giảm dần theo thời gian của các cuộc tấn công website trong năm 2020. Số cuộc tấn công website trong quý II/2020 và quý III/2020 giảm lần lượt 17,1% và 38,8% so với cùng kỳ năm 2019.

Cũng theo báo cáo, châu Á đang là điểm nóng thứ hai, chỉ sau Mỹ khi xét tới số vụ tấn công website với 113.913 vụ, tương đương 33,2% tổng số vụ tấn công trên toàn cầu.

Như vậy, trong 9 tháng đầu năm 2020, châu Á đi ngược lại xu hướng giảm của thế giới khi số vụ tấn công website tăng 4,1% so với cùng kỳ năm 2019.

Thống kê cho thấy, trong số các quốc gia tại châu Á, Thổ Nhĩ Kỳ là nước có số vụ tấn công website gia tăng mạnh nhất trong 3 quý đầu năm 2020 với 56.903 vụ, tăng 31,7% so với cùng kỳ năm trước. Thổ Nhĩ Kỳ cũng tăng một thứ hạng trên bảng xếp hạng Top 15 quốc gia bị tấn công website nhiều nhất trên thế giới, xếp ở vị trí thứ 2.

Tại Việt Nam, các hệ thống mạng và website bị tấn công theo chiều hướng gia tăng hàng năm, không chỉ về số lượng mà các phương pháp tấn công cũng liên tục được hoàn thiện:

- Năm 2019: Theo thống kê của của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), trong năm 2019, trung tâm đã ghi nhận 6.219 sự cố tấn công mạng vào các trang web của Việt Nam. Trong đó có 2.155 sự cố tấn công lừa đảo (Phishing), 3.824 trường hợp sự cố tấn công thay đổi giao diện (Deface) và 240 sự cố website bị nhiễm mã độc (Malware). So với cùng kỳ năm 2018, tổng số sự cố tấn công tăng 104%. Cụ thể, từng loại tấn công tăng giảm như sau: Phishing tăng 141%, deface tăng 109%, riêng malware giảm 26,57%. Bên cạnh đó, hàng ngày có khoảng gần 100.000 địa chỉ mạng của Việt Nam truy vấn hoặc kết nối mạng lưới máy tính ma (botnet).

- Năm 2020: Đại dịch Covid-19 bùng phát, hàng loạt doanh nghiệp, cơ quan, tổ chức chuyển sang làm việc từ xa. Các phần mềm làm việc trực tuyến được tìm kiếm và download rầm rộ. Nhiều đơn vị buộc phải mở hệ thống ra internet để nhân

viên có thể truy cập và làm việc từ xa… Điều này tạo môi trường cho kẻ xấu khai thác lỗ hổng, tấn công, đánh cắp thông tin.

Trong năm qua, hàng loạt vụ tấn công mạng quy mô lớn diễn ra trên toàn cầu, điển hình như vụ việc nhà máy của Foxconn bị tin tặc tấn công, bị đòi 34 triệu USD tiền chuộc dữ liệu; hay 267 triệu thông tin người dùng Facebook được rao bán; Intel bị tin tặc tấn công, gây rò rỉ 20 GB dữ liệu bí mật… Mới đây nhất, T-Mobile, một trong những nhà mạng lớn nhất của Mỹ cũng đã trở thành nạn nhân tiếp theo của hacker. Theo quan sát của Tập đoàn công nghệ BKAV, tại Việt Nam, nhiều trang thương mại điện tử lớn, một số nền tảng giao hàng trực tuyến có nhiều người sử dụng, đã bị xâm nhập và đánh cắp dữ liệu.

Theo báo cáo an ninh mạng website trong 9 tháng đầu năm 2020 do Công ty an toàn thông tin CyStack công bố (Là báo cáo thống kê và phân tích tình hình tấn công website trên toàn thế giới, báo cáo an ninh website được CyStack thực hiện định kỳ hàng quý. Dữ liệu trong báo cáo này được trích xuất từ hệ thống CyStack Attack Map do CyStack nghiên cứu và phát triển), hệ thống đã ghi nhận 343.365 vụ tấn công vào website trên toàn thế giới. Trong đó, châu Á đang là điểm nóng thứ hai, chỉ sau Mỹ với 113.913 vụ tấn công website, tương đương 33,2% tổng số vụ tấn công trên toàn cầu, tăng 4,1% so với cùng kỳ năm 2019.

Trong năm 2020, nhờ thực hiện nhiều biện pháp phòng chống tấn công mạng, Việt Nam đã cải thiện đáng kể tình hình an ninh website so với năm 2019. Cụ thể, số cuộc tấn công trong ba quý đầu năm 2020 đã giảm 64,8% so với cùng kỳ năm 2019, từ 8418 về mức 3041 vụ. Tổng kết 9 tháng đầu năm 2020, Việt Nam đứng thứ 18 trên bản đồ tấn công website toàn cầu. Xét trong 5 quý gần nhất, Việt Nam đã cải thiện đáng kể an ninh mạng website, đặc biệt là quý I/2020 với chỉ 838 vụ và xếp thứ 19 trên thế giới. Số lượng cuộc tấn công website tại Việt Nam tăng nhẹ trong quý II và quý III lần lượt là 27,3% và 7,5% so với quý trước đó.

1.3. Các lỗi bảo mật phổ biến của ứng dụng web và nguy cơ mất an toàn thông tin của các doanh nghiệp

Các lỗ hổng bảo mật thường bắt nguồn từ các ứng dụng web, và hầu hết các nhà quản trị chưa có cái nhìn tổng quan về bảo mật ứng dụng web. Đây là lý do dẫn

tới số lượng các cuộc tấn công trên mạng ngày càng nhiều. Sau đây là một số lỗi bảo mật thường gặp trên ứng dụng web của các doanh nghiệp [15].

Lỗ hổng 1: Lỗ hổng XSS

Thông qua lỗ hổng XSS, kẻ tấn công có thể chiếm quyền điều khiển phiên người dùng, gỡ bỏ trang web, và có thể đánh cắp thông tin của người dùng dựa trên trình duyệt. Bản chất của dạng tấn công này là dựa vào trình duyệt. Tin tặc có thể chèn mã JavaScript vào các trang web có lỗi XSS, khi người dùng truy cập vào những trang web này, lập tức mã script của tin tặc sẽ hoạt động lưu lại thông tin người dùng.

Lỗ hổng 2: Chèn mã độc hại (Injection flaws)

Hacker có thể sử dụng điểm yếu của các truy vấn đầu vào bên trong ứng dụng để chèn thêm dữ liệu không an toàn, từ đó máy chủ có thể bị tấn công bởi một số dạng như: SQL Injection, Xpath Injection, XML Injection, Buffer overflow, LDAP lookups, Shell command Injection.

Hậu quả là một số hoặc tất cả những dữ liệu quan trọng của doanh nghiệp sẽ bị hacker truy cập trái phép, chúng có thể sửa đổi, xóa bỏ thông tin hoặc thậm chí lợi dụng để tống tiền. Trong các lỗ hổng trên, SQL Injejection là phương thức tấn công thường gặp nhất trong ứng dụng web.

Lỗ hổng 3: Tệp tin chứa mã độc

Nguy cơ bị tấn công tiềm ẩn với việc mã hóa trong tích hợp tệp tin từ xa (RFI) có thể cho phép kẻ tấn công tạo sự thỏa hiệp của máy chủ. Dạng tấn công bằng tệp tin chứa mã độc này có thể ảnh hưởng đến PHP, XML và bất kỳ tập tin nào từ người dùng.

Lỗ hổng 4: CSRF

Một trong những lỗ hổng bảo mật thường gặp trong ứng dụng web là lỗ hổng CSRF. Lợi dụng cơ chế tự động đăng nhập vào một số website, tin tặc có thể điều hướng người dùng thực hiện các đoạn chứa mã độc, nhúng vào các website mà người dùng đang trong phiên làm việc. Từ đó, mã độc sẽ chạy trên trình duyệt của người dùng và hacker sẽ thực hiện các hành vi gian lận. Vì vậy, trong một số diễn đàn hoặc website khi đăng nhập tài khoản, không nên lưu mật khẩu, tên người dùng.

Lỗ hổng 5: Tham chiếu đối tượng trực tiếp không an toàn

Mối đe dọa tiềm ẩn ở đây là những kẻ tấn công có thể lợi dụng những tài liệu tham khảo để truy cập vào quyền của các đối tượng khác mà không cần sự cho phép. Ví dụ: A có thể mạo danh là B để truy cập vào hệ thống.

Việc tham chiếu các đối tượng, tệp tin, file, bản ghi cơ sở dữ liệu cần được thực hiện gián tiếp và những thông tin nhạy cảm nên được che giấu. Bên cạnh đó, việc phân quyền nhà quản trị cũng cần cài đặt bảo mật ở chế độ cao nhất, không cho phép người lạ truy cập trái phép. Một khi hacker có thể xác định được cấu trúc thông tin chuyển tới server, chúng có thể thu thập dữ liệu người dùng, ăn cắp tài khoản thẻ tín dụng...

Lỗ hổng 6: Rò rỉ thông tin và xử lý lỗi không đúng cách

Mối đe dọa tiềm ẩn từ việc rò rỉ thông tin và xử lý lỗi không đúng cách (Broken Authentication and Session Management) có thể giúp tin tặc ăn cắp dữ liệu nhạy cảm, hoặc tiến hành các cuộc tấn công nghiêm trọng hơn. Một ứng dụng web không được bảo mật tốt có thể vô ý rò rỉ thông tin về cấu hình, hoạt động bên trong, hoặc vi phạm sự riêng tư thông qua một loạt các vấn đề ứng dụng.

Lỗ hổng 7: Quản lý xác thực và quản lý phiên yếu

Khâu xác thực (authentication) và trao quyền (authorisation) được sử dụng khá phổ biến trong các ứng dụng web. Nếu một trong 2 khâu này không bảo mật mạnh mẽ thì đây chính là lỗ hổng tiềm ẩn giúp tin tặc xâm nhập vào hệ thống. Mối đe dọa tiềm ẩn ở đây là kẻ tấn công có thể thỏa hiệp mật khẩu, mã khóa hoặc danh tính người dùng. Để hạn chế nguy cơ tấn công, quản trị viên nên thiết lập session thật tốt.

Lỗ hổng 8: Không hạn chế truy nhập vào URL nội bộ

Một trong những giải pháp nhằm hạn chế sự tấn công từ bên trong nội bộ mà nhà quản trị nên làm là hạn chế sự truy cập vào các URL quan trọng. Bạn có thể hạn chế địa chỉ IP, hạn chế sử dụng phân quyền, sự truy cập trực tiếp vào URL.

Lỗ hổng 9: Không kiểm tra sự điều hướng và chuyển tiếp của URL

Lợi dụng sơ hở này, tin tặc có thể điều hướng đường link gốc đến một trang web hoặc 1 ứng dụng lừa đảo hoặc trang web đen. Khi click vào đường dẫn tới

trang web lừa đảo, máy tính của người dùng có thể bị nhiễm mã độc và hacker sau đó có thể ép người dùng tiết lộ thông tin cá nhân.

Lỗ hổng 10: Sử dụng các lỗ hổng có sẵn trong thư viện

Thực tế hiện nay, một số tổ chức và doanh nghiệp Việt Nam chưa cập nhật những bản vá lỗi trong ứng dụng web của mình, và cá nhân cũng vậy. Một số lỗi xuất phát từ thư viện ứng dụng, một số nằm trong plugin cài thêm, số khác ở trong module ứng dụng. Cũng chính vì điều này mà hacker nhanh chóng khai thác các lỗ hổng bảo mật và hàng loạt người dùng, thiết bị bị ảnh hưởng.

1.4. Các phương thức tấn công website phổ biến

1.4.1. Giới thiệu chung

Các lỗ hổng bảo mật web là các điểm yếu cho phép tin tặc tấn công đánh cắp dữ liệu người dùng, dữ liệu hệ thống, kiểm soát ứng dụng web, hoặc thậm chí kiểm soát cả hệ thống máy chủ chạy ứng dụng web.

Hệ thống Website có thể hoạt động và cung cấp dịch vụ cho người dùng thường trải qua các giai đoạn: giai đoạn thiết kế, giai đoạn cài đặt hệ thống và giai đoạn triển khai và vận hành khai thác hệ thống website. Trong cả ba giai đoạn đều có thể phát sinh các lỗ hổng bảo mật.

OWASP là một dự án cộng đồng mở hoạt động với mục đích tăng cường an toàn cho các ứng dụng web. Từ những năm 2010 cho đến nay, OWASP khởi động dự án "OWASP Top 10" nhằm đưa ra danh sách 10 lỗ hổng bảo mật nghiêm trọng nhất trong các ứng dụng web. Kết quả của dự án này đã được công bố vào năm 2017 như sau [19]:

(1) Injection (Chèn mã).

(2) Broken Authentication and Session Management (Xác thực và quản lý phiên yếu).

(3) Cross-Site Scripting (XSS - Thực thi mã script xấu).

(4) Insecure Direct Object References (Tham chiếu các đối tượng trực tiếp không an toàn).

(5) Security Misconfiguration (Lỗi cấu hình an ninh).

(6) Sensitive Data Exposure (Rò rỉ dữ liệu nhạy cảm).

(7) Missing Function Level Access Control (Thiếu kiểm soát truy nhập ở mức tính năng).

(8) Cross-Site Request Forgery (CSRF - Giả mạo yêu cầu).

(9) Using Components with Known Vulnerabilities (Sử dụng các thành phần chứa lỗ hổng đã biết).

(10) Unvalidated Redirects and Forwards (Tái định hướng và chuyển tiếp không được kiểm tra).

Các tấn công ứng dụng web có thể chia thành hai dạng chính: tấn công lỗ hổng bảo mật web và tấn công hạ tầng mạng cung cấp dịch vụ web.

1.4.2. Các phương thức tấn công website [20] [21]

1.4.2.1. Tấn công SQL injection

SQL injection là một kĩ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng trong việc kiểm tra dữ liệu nhập trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu để "tiêm vào" (inject) và thi hành các câu lệnh SQL bất hợp pháp (không được người phát triển ứng dụng lường trước). Hậu quả của nó rất tai hại vì nó cho phép những kẻ tấn công có thể thực hiện các thao tác xóa, hiệu chỉnh… do có toàn quyền trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy. Lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lí bằng các hệ quản trị cơ sở dữ liệu như SQL Server, MySQL, Oracle, DB2, Sysbase. Có 4 dạng tấn công kiểu SQL injection sau:

- Vượt qua kiểm tra lúc đăng nhập
- Sử dụng câu lệnh SELECT
- Sử dụng câu lệnh INSERT
- Sử dụng các Stored-Procedures.

1.4.2.2. Tấn công kiểu Broken Authentication And Session Management

Đây là kiểu tấn công lỗi xác thực và quản lý phiên làm việc (Broken Authentication And Session Management), bao gồm những đoạn chương trình kiểm

tra danh tính và quản lý phiên làm việc của người sử dụng thường hay được làm qua loa không đúng cách. Điều này giúp kẻ thâm nhập có thể ăn cắp mật mã, khóa, mã của các phiên làm việc (session token) hoặc tận dụng những lỗi khác để giả mạo danh tính các người dùng khác.

Quản lý xác thực và phiên bao gồm tất cả các khía cạnh xử lý xác thực và quản lý phiên làm việc. Xác thực là một khía cạnh quan trọng của quá trình này, nhưng ngay cả các cơ chế xác thực vững chắc cũng có thể bị suy yếu do chức năng quản lý có khe hở, bao gồm thay đổi mật khẩu, ghi nhớ mật khẩu, thay đổi tài khoản và nhiều chức năng khác. Vì các cuộc tấn công có thể xảy ra với nhiều ứng dụng web nên chức năng quản lý tài khoản yêu cầu xác thực lại ngay cả khi người sử dụng có phiên làm việc hợp lệ. Một phương pháp xác thực mạnh mẽ hơn là sử dụng phần mềm và phần cứng tuy nhiên phương pháp này rất tốn kém.

Các ứng dụng web thường phải thiết lập phiên để theo dõi các luồng yêu cầu từ người dùng, giao thức HTTP không hỗ trợ khả năng này vì vậy các ứng dụng web phải tự tạo ra nó. Thông thường môi trường ứng dụng web cung cấp khả năng phiên nhưng nhiều nhà phát triển thích tự họ tạo ra một thẻ phiên của riêng họ. Tuy nhiên, chức năng ứng dụng liên quan đến quản lý xác thực và phiên làm việc thường thực hiện một cách chính xác, điều này cho phép kẻ tấn công lấy được mật khẩu, khóa, thẻ phiên hoặc khai thác lỗ hổng để thực hiện các giả mạo danh tính người dùng.

1.4.2.3. Tấn công XSS

Kiểu tấn công thực thi mã script xấu (XSS) là một trong những kĩ thuật tấn công phổ biến nhất hiện nay, đồng thời nó cũng là một trong những vấn đề bảo mật quan trọng đối với các nhà phát triển web và cả những người sử dụng web. Bất kì một website nào cho phép người sử dụng đăng thông tin mà không có sự kiểm tra chặt chẽ các đoạn mã nguy hiểm thì đều có thể tiềm ẩn các lỗi XSS.

Cross-Site Scripting hay còn được gọi tắt là XSS (thay vì gọi tắt là CSS để tránh nhầm lẫn với CSS - Cascading Style Sheet của HTML) là một kĩ thuật tấn công bằng cách chèn vào các website động (ASP, PHP, CGI, JSP ...) những thẻ

HTML hay những đoạn mã script nguy hiểm có thể gây nguy hại cho những người sử dụng khác. Trong đó, những đoạn mã nguy hiểm được chèn vào hầu hết được viết bằng các Client-Site Script như JavaScript, JScript, DHTML và cũng có thể là cả các thẻ HTML. Kĩ thuật tấn công XSS đã nhanh chóng trở thành một trong những lỗi phổ biến nhất của Web Applications và mối đe dọa của chúng đối với người sử dụng ngày càng lớn.

1.4.2.4. Tấn công Insecure Direct Object References

Kiểu tấn công đối tượng tham chiếu trực tiếp không an toàn (Insecure Direct Object References), xảy ra khi người phát triển để lộ một tham chiếu đến những đối tượng trong hệ thống như các tập tin, thư mục hay chìa khóa dữ liệu. Nếu chúng ta không có một hệ thống kiểm tra truy cập, kẻ tấn công có thể lợi dụng những tham chiếu này để truy cập dữ liệu một cách trái phép.

Việc phân quyền yếu cho phép người dùng có thể truy cập dữ liệu của người khác. Hacker có thể xác định được cấu trúc truy vấn gửi đến server và có thể nhanh chóng thu nhập dữ liệu như Credit Card, mã khách hàng, thông tin cá nhân.

1.4.2.5. Tấn công Security Misconfiguration

Kiểu tấn công sai sót trong cấu hình bảo mật (Security Misconfiguration), như là một cơ chế an ninh tốt cần phải định nghĩa những hiệu chỉnh về an ninh và triển khai nó cho các ứng dụng, máy chủ ứng dụng, máy chủ web, máy chủ dữ liệu và các ứng dụng nền tảng.

Tất cả những thiết lập nên được định nghĩa, thực hiện và bảo trì bởi vì rất nhiều hệ thống không được triển khai với thiết lập an toàn mặc định. Các hiệu chỉnh cũng bao gồm cập nhật phần mềm và những thư viện được sử dụng bởi ứng dụng.

1.4.2.6. Tấn công Sensitive Data Exposure

Kiểu tấn công phơi bày các dữ liệu nhạy cảm (Sensitive Data Exposure), bao gồm nhiều ứng dụng web không bảo vệ dữ liệu nhạy cảm như thẻ tín dụng, mã số thuế và những mã xác thực bí mật bằng các phương thức mã hóa hay băm

(hashing). Kẻ tấn công có thể ăn cắp hay thay đổi những dữ liệu nhạy cảm này và tiến hành hành vi trộm cắp, gian lận thẻ tín dụng...

1.4.2.7. Tấn công Missing Function Level Access Control

Kiểu tấn công thiếu chức năng điều khiển truy cập (Missing Function Level Access Control) bao gồm gần như tất cả các ứng dụng web kiểm tra quyền truy cập cấp độ chức năng trước khi thực hiện chức năng mà có thể nhìn thấy trong giao diện người dùng. Tuy nhiên, các ứng dụng cần phải thực hiện kiểm tra kiểm soát truy cập tương tự trên máy chủ khi mỗi chức năng được truy cập. Nếu yêu cầu không được xác nhận, kẻ tấn công sẽ có thể giả mạo yêu cầu để truy cập vào chức năng trái phép.

1.4.2.8. Tấn công CSRF

Kiểu tấn công giả mạo yêu cầu (CSRF) là kiểu tấn công ép buộc trình duyệt web của một người dùng đã đăng nhập gửi những yêu cầu các HTTP giả bao gồm cookie của phiên truy cập và những thông tin tự động khác bao gồm thông tin đăng nhập đến một ứng dụng web. Điều này, cho phép kẻ tấn công buộc trình duyệt web tạo ra những yêu cầu đến ứng dụng web mà ứng dụng không thể biết đây là những yêu cầu giả mạo của kẻ tấn công.

1.4.2.9. Tấn công Using Components with Known Vulnerabilities

Kiểu tấn công sử dụng thành phần đã tồn tại lỗ hổng (Using Components with Known Vulnerabilities) bao gồm các lổ hổng có thể có trong các thành phần (thành phần phát triển ứng dụng) như các thư viện, các framework, và mô-đun phần mềm khác. Các thành phần này gần như luôn luôn chạy với quyền cao nhất trong hệ thống. Vì vậy, nếu bị khai thác, các thành phần này có thể gây mất dữ liệu nghiêm trọng.

Các ứng dụng sử dụng các thành phần tồn tại lổ hổng có thể làm suy yếu phòng thủ của hệ thống, cho phép một loạt các cuộc tấn công và ảnh hưởng đến hệ thống.

1.4.2.10. Tấn công Unvalidated Redirects and Forwards

Kiểu tấn công chuyển hướng và chuyển tiếp thiếu kiểm tra (Unvalidated Redirects and Forwards) là kiểu tấn công ứng dụng web thường chuyển hướng, chuyển tiếp người dùng đến những trang web, website khác và sử dụng những thông tin thiếu tin cậy để xác định trang đích đến. Nếu không được kiểm tra một cách cẩn thận, kẻ tấn công có thể lợi dụng để chuyển hướng nạn nhân đến các trang web lừa đảo hay trang web chứa phần mềm độc hại, hoặc chuyển tiếp để truy cập các trang trái phép.

1.4.2.11. Tấn công DoS, DDoS

Tấn công từ chối dịch vụ (DoS) là kỹ thuật tấn công nhằm không cho phép các truy cập hợp lệ truy cập tới một dịch vụ nào đó, trong đó có dịch vụ web. Đây là hình thức tấn công website khá phổ biến hiện nay. DoS khiến cho hệ thống máy chủ web không thể xử lý kịp các tác vụ và dẫn đến quá tải mạng hoặc tràn bộ đệm (Buffer Overflow). Các cuộc tấn công DOS này thường nhắm vào các Web Server của các doanh nghiệp lớn như ngân hàng, chính phủ hay là các trang thương mại điện tử. Trong tấn công DoS, cuộc tấn công thường xuất phát từ một địa điểm duy nhất, tức là nó sẽ xuất phát tại một điểm và chỉ có một dải IP. Tấn công DoS thường xảy ra tại lớp mạng và lớp ứng dụng.

Tấn công từ chối dịch vụ phân tán (DDoS) là tấn công DoS nhưng tin tặc sử dụng nhiều máy tính khác nhau. Trong dạng tấn công DDoS, tin tặc thường tạo ra các truy cập ảo, kết nối ảo thông qua proxy hay chuyên nghiệp hơn là mạng botnet nhằm đánh sập trang web và phá hỏng cơ sở dữ liệu website.

1.4.2.12. Tấn công APT

Tấn công có chủ đích (APT) được sử dụng để mô tả kiểu tấn công dai dẳng và có chủ đích vào một thực thể được nhắm đến. Thông thường tấn công APT có sự chuẩn bị kỹ càng và được thực hiện, hỗ trợ bởi một tổ chức hoặc cao cấp hơn là chính phủ của một nước nào đó nhằm tìm kiếm thông tin tình báo từ cá nhân, doanh

nghiệp, chính phủ nước khác. Tấn công APT có thể gây tác hại nghiêm trọng hơn tấn công DDoS.

Phân tích các thuật ngữ trong APT (Advanced Persistent Threat)

Advanced: thuật ngữ này trong cụm từ APT chỉ các kiểu tấn công cao cấp hơn các thể loại thông thường. Trong APT, tin tặc sử dụng các malware và các biến thể khác nhau để tiến hành qua mặt và xâm nhập vào hệ thống. Không giống các virus hay chương trình độc hại máy tính khác, các malware này phần lớn có thể qua mặt được các phương pháp bảo vệ truyền thống khác như Firewall, IPS, và phần mềm diệt virus.

Persistent: kiểu tấn công APT thực sự bao giờ cũng có chủ đích nhất định và thuật ngữ Persistent mang ý nghĩa việc tấn công luôn theo sát để đạt được mục đích của nó. Mục tiêu tấn công sẽ không bị tấn công ngay tức thì mà các mã độc sẽ đi theo nhiều đường khác nhau cho đến khi xâm nhập vào hệ thống, sau đó chờ thời cơ. Chúng chỉ thực sự kích hoạt tấn công khi phát hiện đúng mục tiêu.

Threat: chỉ các mối nguy hại liên quan đến an ninh, an toàn thông tin. Theo thống kê của FireEye [22], tấn công APT nằm trong nhóm hiểm họa an toàn thông tin bắt đầu xuất hiện từ giai đoạn 2010-2011. Đây là phương thức tấn công đa dạng, nhanh chóng tạo ra các biến thể để qua mặt các giải pháp an ninh và gây thiệt hại to lớn so với các rủi ro an ninh khác như virus, spyware.

1.5. Kết luận Chương 1

Trong Chương 1, luận văn đã khảo sát, phân loại website dựa trên nhiều tiêu chí, đặc biệt là tiêu chí về mức độ bảo mật. Căn cứ vào thực trạng tấn công website tại Việt Nam và trên thế giới trong những năm gần đây, luận văn đã trình bày các lỗ hổng bảo mật phổ biến của ứng dụng web, các phương thức tấn công website thường gặp và nguy cơ mất an toàn thông tin website của các doanh nghiệp. Từ đó nói lên nhu cầu cấp thiết của việc đảm bảo an toàn thông tin cho website.

Chương tiếp theo, luận văn sẽ nghiên cứu các giải pháp đảm bảo an toàn thông tin cho website.

CHƯƠNG 2. CÁC GIẢI PHÁP ĐẢM BẢO AN TOÀN THÔNG TIN WEBSITE

Trong Chương 2 luận văn sẽ nghiên cứu một số giải pháp đảm bảo an toàn thông tin cho website, cụ thể bao gồm các nội dung sau: triển khai hệ thống phòng thủ, thiết lập và cấu hình hệ thống máy chủ an toàn, vận hành an toàn và phòng chống tấn công từ chối dịch vụ.

2.1. Triển khai hệ thống phòng thủ

Việc triển khai hệ thống phòng thủ hợp lý sẽ giúp phòng, chống và ngăn chặn các cuộc tấn công một cách hiệu quả. Trong phần này, luận văn sẽ nghiên cứu và trình bày một số biện pháp như tổ chức mô hình mạng, thiết lập tường lửa, ứng dụng phòng chống vi-rút, hệ thống phát hiện và ngăn chặn xâm nhập.

2.1.1. Tổ chức mô hình mạng

Việc tổ chức mô hình mạng hợp lý có ảnh hưởng tích cực đến việc đảm bảo an ninh an toàn cho website. Đây là cơ sở đầu tiên cho việc xây dựng các hệ thống phòng thủ và bảo vệ. Ngoài ra, việc tổ chức mô hình mạng hợp lý có thể hạn chế việc tấn công từ bên trong và bên ngoài một cách hiệu quả.

Trong các mô hình mạng hợp lý cần phân biệt rõ ràng giữa các vùng mạng theo chức năng và thiết lập các chính sách an toàn thông tin riêng cho từng vùng mạng theo yêu cầu thực tế

- Vùng mạng ngoài còn gọi là mạng Internet

- Vùng mạng DMZ: Đặt các máy chủ cung cấp dịch vụ trực tiếp ra mạng ngoài như web server, mail server, FTP server, v.v..

- Vùng mạng Server Network: Đặt các máy chủ không trực tiếp cung cấp dịch vụ trực tiếp ra mạng Internet.

- Vùng mạng Private Network: Đặt các thiết bị mạng, máy trạm và máy chủ thuộc mạng nội bộ của đơn vị.

Khi tổ chức mô hình mạng cần lưu ý một số điểm như sau:

- Nên đặt các máy chủ web, máy chủ thư điện tử (mail server), các máy chủ cung cấp dịch vụ ra mạng Internet trong vùng mạng DMZ, nhằm tránh các tấn công mạng nội bộ hoặc gây ảnh hưởng tới an toàn mạng nội bộ nếu các máy chủ này bị cướp quyền điều khiển. Chú ý không đặt các máy chủ chỉ cung cấp dịch vụ cho mạng nội bộ trong vùng mạng này.

- Các máy chủ không trực tiếp cung cấp dịch vụ ra mạng ngoài như máy chủ ứng dụng, máy chủ cơ sở dữ liệu, máy chủ xác thực, v.v.. nên đặt trong môi trường mạng Server Network để tránh tấn công trực tiếp từ Internet và từ mạng nội bộ. Đối với hệ thống thông tin yêu cầu mức bảo mật cao, hoặc có nhiều cụm máy chủ khác nhau có thể chia vùng server network thành các vùng nhỏ hơn độc lập để nâng cao tính bảo mật.

- Cần thiết lập các hệ thống phòng thủ như: tường lửa, thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) để bảo vệ hệ thống, chống tấn công và xâm nhập trái phép. Nên đặt tường lửa và IDS/IPS ở các vị trí sau:

- Đặt tường lửa giữa đường nối mạng Internet với các vùng mạng khác nhằm hạn chế tấn công từ bên ngoài vào.
- Đặt tường lửa giữa các vùng mạng nội bộ và mạng DMZ nhằm hạn chế các tấn công giữa các vùng đó.
- Đặt IDS/IPS tại vùng cần lõi bảo vệ.

Đặt các tường lửa tại những vị trí khác nhau của mạng, mỗi tường lửa lại có những luật riêng để ngăn chặn những tấn công đối với vùng mạng đó. Đảm bảo an ninh an toàn mạng nhưng không ảnh hưởng nhiều đến hiệu năng mạng. Nên đặt một Router ngoài cùng (Router biên) trước khi kết nối đến nhà cung cấp dịch vụ Internet (ISP) để lọc một số lưu lượng không mong muốn và chặn những gói tin đến từ những địa chỉ IP không hợp lệ.

2.1.2. Thiết lập tường lửa

Tường lửa là một thiết bị phần cứng hoặc phần mềm hoạt động trong môi trường máy tính nối mạng nhằm ngăn chặn những lưu lượng bị cấm bởi chính sách an ninh của một cá nhân hoặc tổ chức. Mục đích sử dụng tường lửa là:

- Bảo vệ hệ thống khi bị tấn công.
- Lọc các kết nối, các gói tin dựa trên chính sách truy cập nội dung.
- Áp đặt các chính sách truy cập đối với người dùng hoặc nhóm người dùng.
- Ghi lại nhật ký để hỗ trợ phát hiện xâm nhập và điều tra sự cố.

Cần thiết lập các luật cho tường lửa phù hợp với chính sách an ninh của hệ thống, phù hợp với vị trí và mục đích của tường lửa đó. Tường lửa có thể giúp ngăn chặn các cuộc tấn công, ngăn chặn các kết nối của các mã độc từ trong ra ngoài, v.v.. Ví dụ: thiết lập luật cho tường lửa từ chối tất cả các kết nối từ bên trong máy chủ web ra ngoài Internet ngoại trừ các kết nối đã được thiết lập, tức là chỉ từ chối tất cả các gói tin TCP khi xuất hiện cờ SYN. Điều này sẽ ngăn chặn việc nếu tin tặc có khả năng chạy các kịch bản mã độc trên máy chủ web thì cũng không thể cho các mã độc nối ngược từ máy chủ web về máy tính của tin tặc. Một số vị trí có thể thiết lập tường lửa như [Hình 2.1].

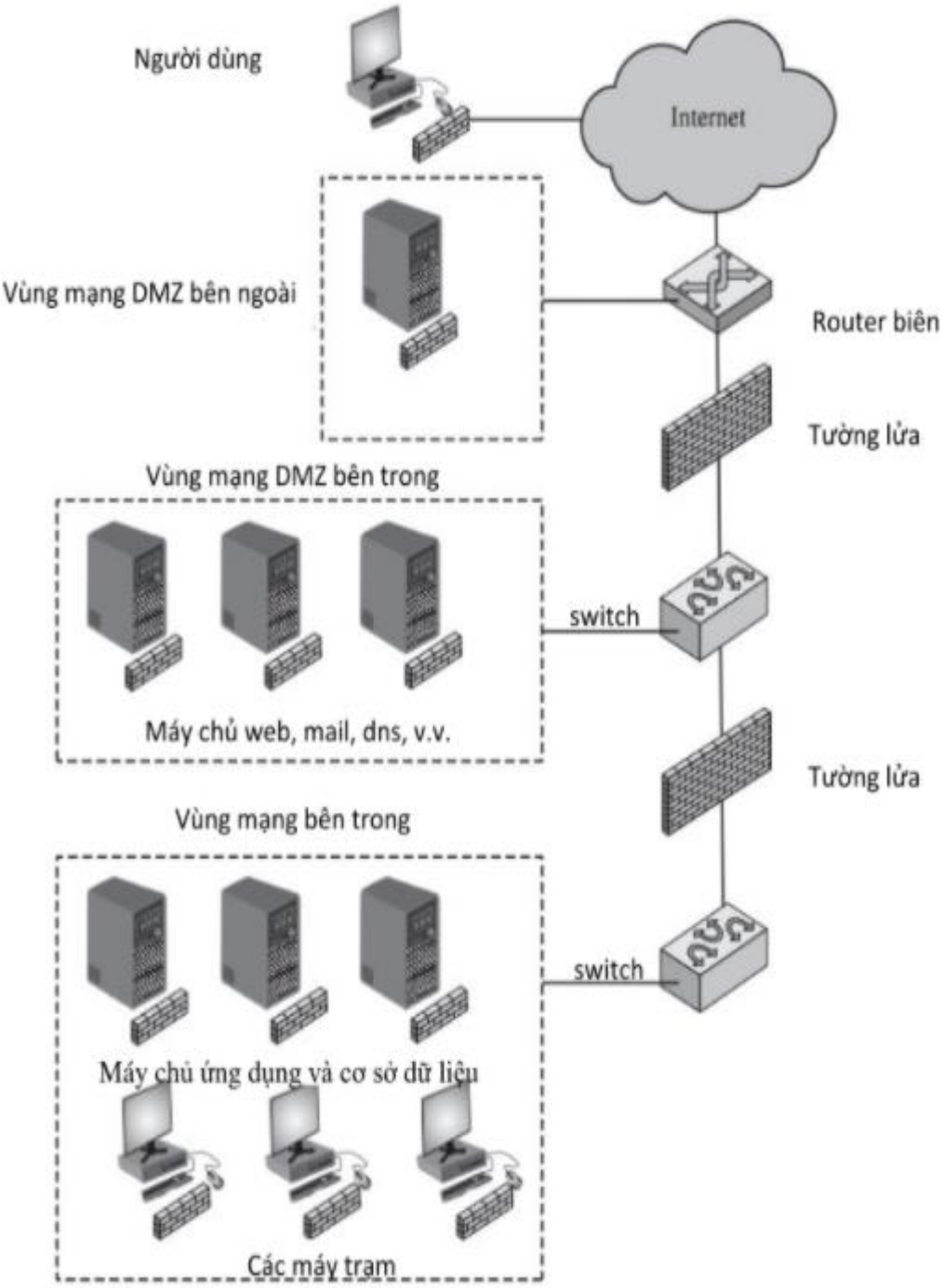
Tuy nhiên, tường lửa cũng có những hạn chế, nó có thể làm chậm quá trình kết nối. Trong một số trường hợp đối với những người có hiểu biết thì có thể vượt qua được tường lửa. Vì vậy, cần chú trọng bảo hệ hệ thống theo chiều sâu.

Tường lửa ứng dụng web (WAF)

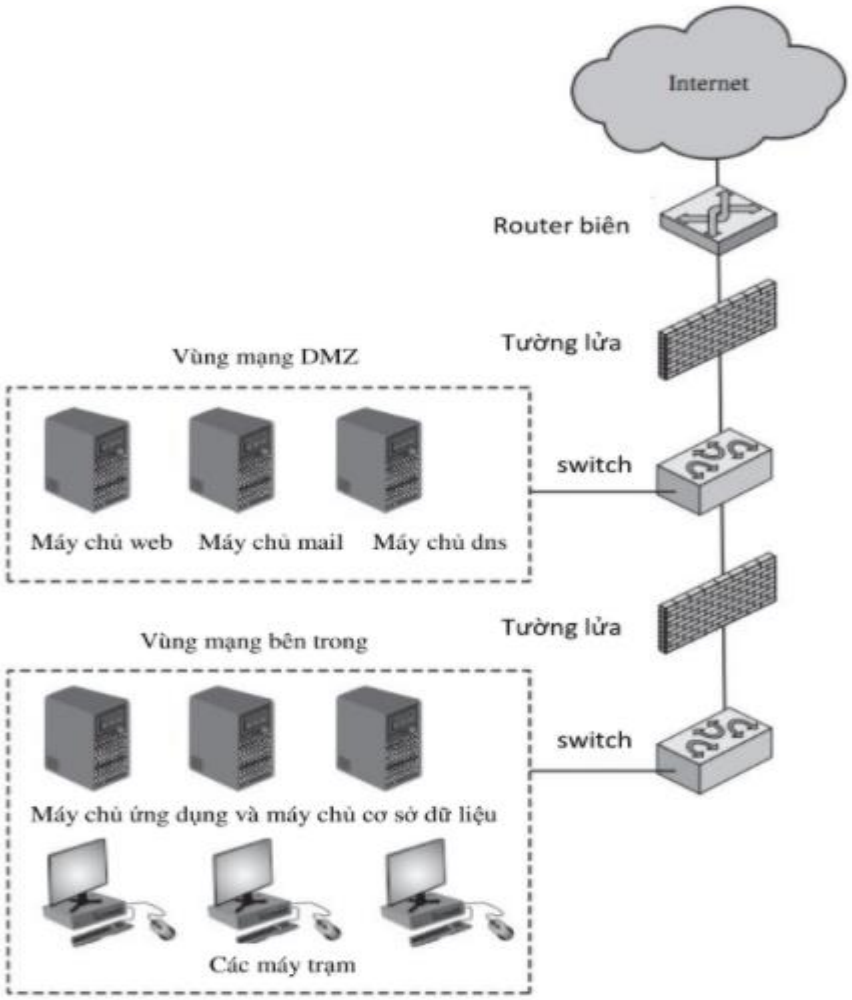
Một tường lửa ứng dụng web thường là một phần mềm, hay một thành phần nhúng được cài đặt ngay trên máy chủ phục vụ web. Đôi khi tường lửa ứng dụng web cũng được cung cấp như một thiết bị phần cứng có cài đặt sẵn phần mềm bên trong. Tường lửa ứng dụng web hoạt động bằng cách sử dụng một bộ lọc với các "luật" được định nghĩa trước hoặc do người dùng thêm vào để giám sát các dữ liệu trao đổi với ứng dụng web thông qua giao thức HTTP. Những quy tắc này giúp phát hiện và chặn các truy vấn nhằm tấn công vào các lỗi phổ biến như XSS, SQL Injection, OS command Injection, Path Traversal, DoS và một số lỗi khác.

Các dữ liệu đi vào hoặc đi ra khỏi ứng dụng web sẽ được tường lưa ứng dụng web kiểm tra so sánh với các dấu hiệu được định nghĩa sẵn và quyết định cho phép dữ liệu đi qua hoặc chặn các dữ liệu đó lại. Đây là một quá trình lọc mà các thiết bị tường lửa lớp dưới không thực chiện được. Việc triển khai tường lửa ứng dụng web

sẽ phần nào hạn chế được các sai sót của người lập trình ứng dụng web. Các tường lửa ứng dụng web nên được cài sẵn giữa mỗi lớp trong kiến trúc web [Hình 2.2]:



Hình 2.1. Một số vị trí có thể đặt tường lửa



Hình 2.2. Ví dụ vị trí đặt tường lửa ứng dụng web

2.1.3. Sử dụng công cụ phát hiện và ngăn chặn xâm nhập (IDS/IPS)

Các công cụ phát hiện xâm nhập (IDS) có tính năng phát hiện dấu hiệu các xâm nhập trái phép, còn các công cụ ngăn chặn xâm nhập (IPS) có tính năng phát hiện và ngăn chặn việc xâm nhập trái phép của tin tặc vào hệ thống. Như các thiết bị mạng, IDS/IPS cũng có thể bị tấn công và chiếm quyền kiểm soát, do đó bị vô hiệu hóa bởi tin tặc. Vì vậy, cần thiết đảm bảo thực hiện một số tiêu chí khi triển khai và vận hành, gồm:

- Xác định công nghệ IDS/IPS đã, đang hoặc dự định triển khai.
- Xác định các thành phần của IDS/IPS.
- Thiết đặt và cấu hình an toàn cho IDS/IPS.

- Xác định vị trí hợp lý để đặt IDS/IPS.

- Có cơ chế xây dựng, tổ chức quản lý hệ thống luật.

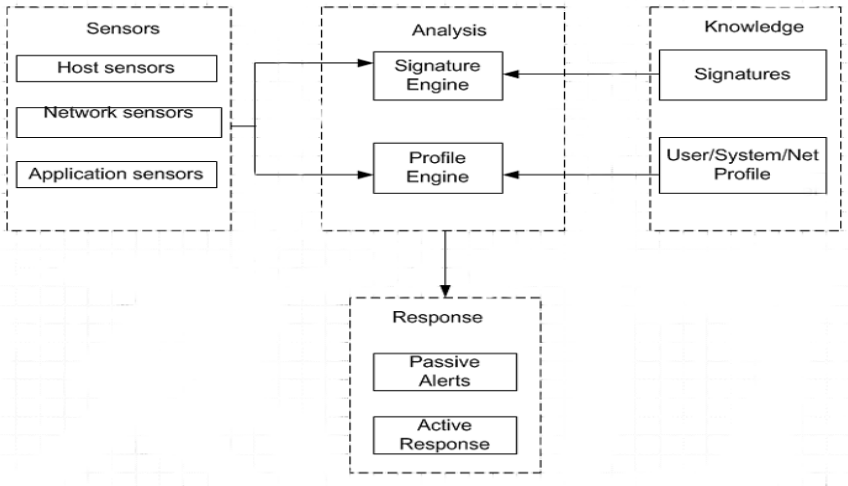
- Hạn chế thấp nhất các tình huống cảnh báo nhầm hoặc không cảnh báo khi có xâm nhập.

2.1.3.1. Hệ thống phát hiện xâm nhập IDS

Hệ thống phát hiện xâm nhập (IDS) là một hệ thống phần cứng hoặc ứng dụng phần mềm theo dõi, giám sát và thu thập thông tin từ các hoạt động ra vào của mạng. Sau đó hệ thống sẽ phân tích để tìm dấu hiệu của sự xâm nhập hoặc tấn công hệ thống trái phép và cảnh báo đến người quản trị hệ thống. Do đó, IDS có khả năng ứng dụng phát hiện tấn công website.

Các thành phần của IDS

Các thành phần của hệ thống IDS được mô tả trong [Hình 2.3].



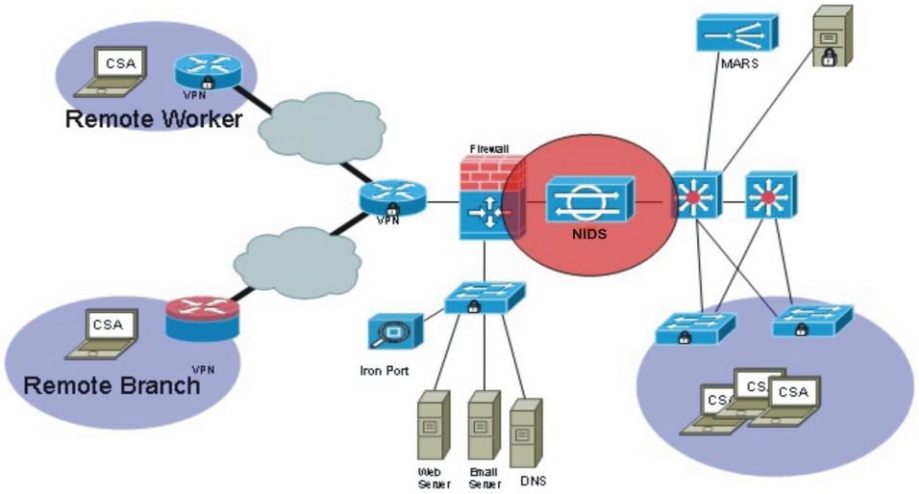
Hình 2.3. Các thành phần của hệ thống IDS

Hệ thống IDS bao gồm các thành phần: Thành phần thu gói tin (Sensors); Thành phần phân tích gói tin (Analysis); Thành phần tri thức (Knowledge) hỗ trợ quá trình phân tích gói tin và Thành phần phản hồi (Respontion) xuất các thông tin cảnh báo.

Phân loại IDS:

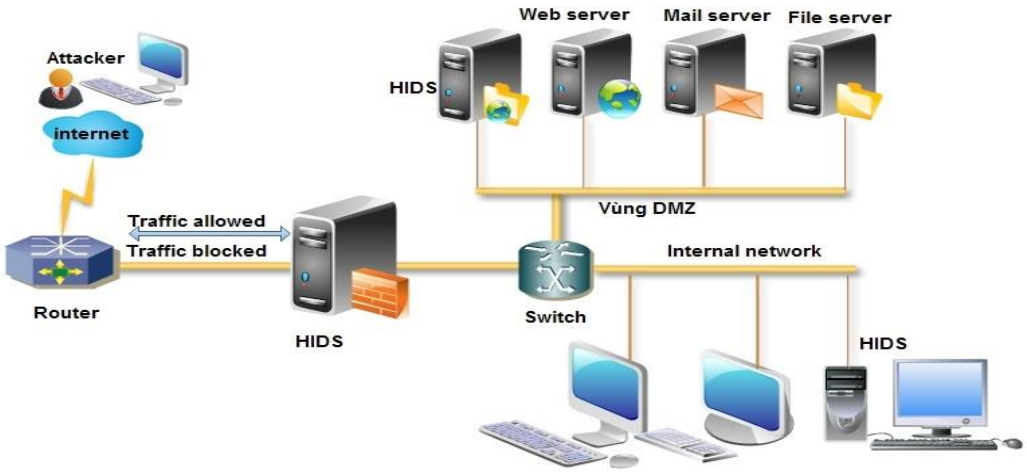
Dựa trên phạm vi giám sát, IDS được chia thành 2 loại:

(1) Network-based IDS (NIDS): Là những IDS giám sát trên toàn bộ mạng. Nguồn thông tin chủ yếu của NIDS là các gói dữ liệu đang lưu thông trên mạng. NIDS thường được lắp đặt tại ngõ vào của mạng, có thể đứng trước hoặc sau tường lửa. [Hình 2.4] mô tả mô hình hệ thống NIDS.



Hình 2.4. Mô hình hệ thống NIDS

(2) Host-based IDS (HIDS): Là những IDS phát hiện xâm nhập máy chủ được cài đặt trên các máy tính (host). [Hình 2.5] mô tả mô hình hệ thống HIDS.



Hình 2.5. Mô hình hệ thống HIDS

HIDS tìm kiếm dấu hiệu xâm nhập vào host cục bộ. Chúng tìm kiếm các hoạt động bất thường, lưu lượng đã gửi đến host được kiểm tra và phân tích trong file log lưu lại rồi chuyển qua host nếu cảm thấy không có dấu hiệu đáng nghi ngờ.

HIDS thường dựa trên các tập luật (rule-based) để phân tích các hoạt động. Nhiệm vụ chính của HIDS là giám sát sự thay đổi trên hệ thống.

Dựa trên kỹ thuật thực hiện, IDS cũng được chia thành 2 loại:

- **Signature-based IDS:** Signature-based IDS phát hiện xâm nhập dựa trên dấu hiệu của hành vi xâm nhập, thông qua phân tích lưu lượng mạng và nhật ký hệ thống. Kỹ thuật này đòi hỏi phải duy trì một cơ sở dữ liệu về các dấu hiệu xâm nhập (signature database), và cơ sở dữ liệu này phải được cập nhật thường xuyên mỗi khi có một hình thức hoặc kỹ thuật xâm nhập mới.

- **Anomaly-based IDS**: phát hiện xâm nhập bằng cách so sánh (mang tính thống kê) các hành vi hiện tại với hoạt động bình thường của hệ thống để phát hiện các bất thường (anomaly) có thể là dấu hiệu của xâm nhập. Ví dụ, trong điều kiện bình thường, lưu lượng trên một giao tiếp mạng của server là vào khoảng 25% băng thông cực đại của giao tiếp. Nếu tại một thời điểm nào đó, lưu lượng này đột ngột tăng lên đến 50% hoặc hơn nữa, thì có thể giả định rằng server đang bị tấn công DoS.

Hệ thống IDS có khả năng ứng dụng phát hiện tấn công website dựa trên các dữ liệu thu thập được kết hợp với các kỹ thuật phát hiện tấn công.

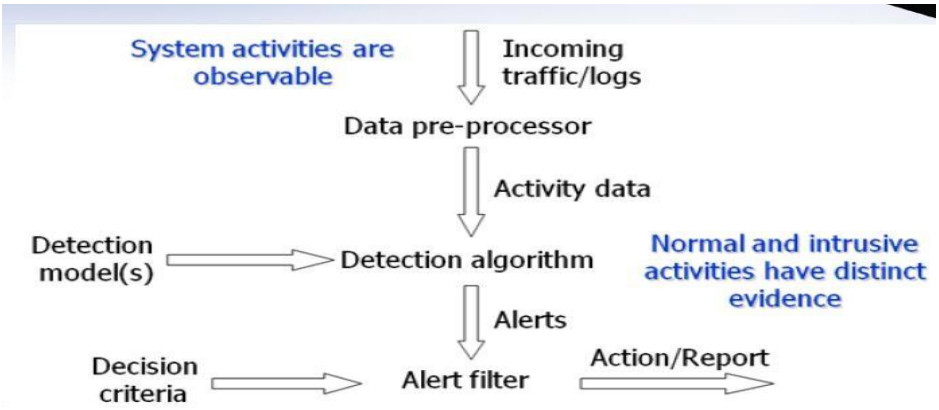
Snort

Một trong những phần mềm IDS phổ biến hiện nay là Snort [23]. Đây là một sản phẩm NIDS mã nguồn mở với hệ thống signature database (gọi là rule database) được cập nhật thường xuyên bởi nhiều thành viên trong cộng đồng Internet.

Snort là một ứng dụng IDS hiện đại với ba chức năng chính: chức năng là một bộ phận lắng nghe gói tin, chức năng lưu lại thông tin gói tin hay chức năng là một hệ thống phát hiện xâm nhập mạng (NIDS). Ngoài ra còn có rất nhiều chương trình add-on cho Snort để có thể quản lý các file log, các tập luật và cảnh báo cho quản trị viên khi phát hiện sự xâm nhập hệ thống. Tuy không phải là phần lõi của Snort, nhưng những thành phần này cung cấp rất nhiều tính năng phong phú để có được một hệ thống phát hiện và phòng chống xâm nhập tốt.

2.1.3.2. Hệ thống ngăn chặn xâm nhập IPS

Hệ thống phòng chống xâm nhập (IPS) là một kỹ thuật, kết hợp các ưu điểm của kỹ thuật tường lửa với hệ thống phát hiện xâm nhập IDS, có khả năng phát hiện các cuộc tấn công và tự động ngăn chặn các cuộc tấn công nhằm vào điểm yếu của hệ thống. Sơ đồ hoạt động của hệ thống IPS mô tả trong [Hình 2.6].



Hình 2.6. Sơ đồ hoạt động của IPS

Ý tưởng của công nghệ IPS là mọi cuộc tấn công chống lại bất cứ thành phần nào của dịch vụ được bảo vệ sẽ bị làm chệch hướng bằng các giải pháp ngăn ngừa xâm nhập. Với "quyền tối thượng", các hệ thống phòng chống xâm nhập có thể "nắm" lấy bất cứ lưu lượng nào của các gói tin mạng và đưa ra quyết định có chủ ý – liệu đây có phải là một cuộc tấn công hay một sự sử dụng hợp pháp – sau đó thực hiện hành động thích hợp để hoàn thành tác vụ một cách trọn vẹn. Kết quả cuối cùng là một nhu cầu có hạn định cho các giải pháp phát hiện hay giám sát xâm nhập một khi tất cả những gì liên quan đến mối đe dọa đều bị ngăn chặn.

Các kiểu triển khai IPS:

Có hai kiểu chính khi triển khai IPS là out-of-band IPS và in-line IPS:

- **Out-of-band IPS (OOB IPS)**: Với hệ thống này luồng dữ liệu vào hệ thống mạng sẽ cùng đi qua đồng thời firewall và IPS. Hệ thống IPS có thể kiểm soát luồng dữ liệu vào, phân tích và phát hiện các dấu hiệu của sự xâm nhập. Với vị trí này, OOB IPS có thể quản lý firewall, chỉ dẫn nó chặn lại các hành động nghi ngờ.

- **In-line IPS**: Vị trí IPS nằm trước firewall, luồng dữ liệu phải đi qua chúng trước khi tới firewall. Điểm khác chính so với OOB IPS là có thêm chức năng traffic-blocking. Điều đó làm cho IPS có thể ngăn chặn lưu lượng nguy hiểm nhanh hơn so với OOB IPS. Tuy nhiên vị trí này sẽ làm cho tốc độ luồng thông tin qua ra vào mạng chậm hơn.

Chức năng chính và các Modul trong IPS

IPS có hai chức năng chính là phát hiện các cuộc tấn công và chống lại các cuộc tấn công đó. Hệ thống IPS gồm 3 modul chính: modul phân tích luồng dữ liệu, modul phát hiện tấn công, modul phản ứng.

- Modul phân tích luồng dữ liệu: Modul này có nhiệm vụ lấy tất các gói tin đi đến mạng để phân tích. Thông thường các gói tin có địa chỉ không phải của một card mạng thì sẽ bị card mạng đó hủy bỏ nhưng card mạng của IPS được đặt ở chế độ thu nhận tất cả. Tất cả các gói tin qua chúng đều được sao chụp, xử lý, phân tích đến từng trường thông tin. Bộ phân tích đọc thông tin từng trường trong gói tin, xác định chúng thuộc kiểu gói tin nào, dịch vụ gì... Các thông tin này được chuyển đến modul phát hiện tấn công.

- Modul phát hiện tấn công: Đây là modul quan trọng nhất trong hệ thống có nhiệm vụ phát hiện các cuộc tấn công. Có hai phương pháp để phát hiện các cuộc tấn công: Misuse Detection (dò sự lạm dụng) và Anomaly Detection (dò sự không bình thường).

- Modul phản ứng: Khi có dấu hiệu của sự tấn công hoặc thâm nhập, modul phát hiện tấn công sẽ gửi tín hiệu báo hiệu có sự tấn công hoặc thâm nhập đến modul phản ứng. Lúc đó modul phản ứng sẽ kích hoạt tường lửa thực hiện chức năng ngăn chặn cuộc tấn công hay cảnh báo tới người quản trị. Tại modul này, nếu chỉ đưa ra các cảnh báo tới các người quản trị và dừng lại ở đó thì hệ thống này được gọi là hệ thống phòng thủ bị động. Modul phản ứng này tùy theo hệ thống mà có các chức năng và phương pháp ngăn chặn khác nhau.

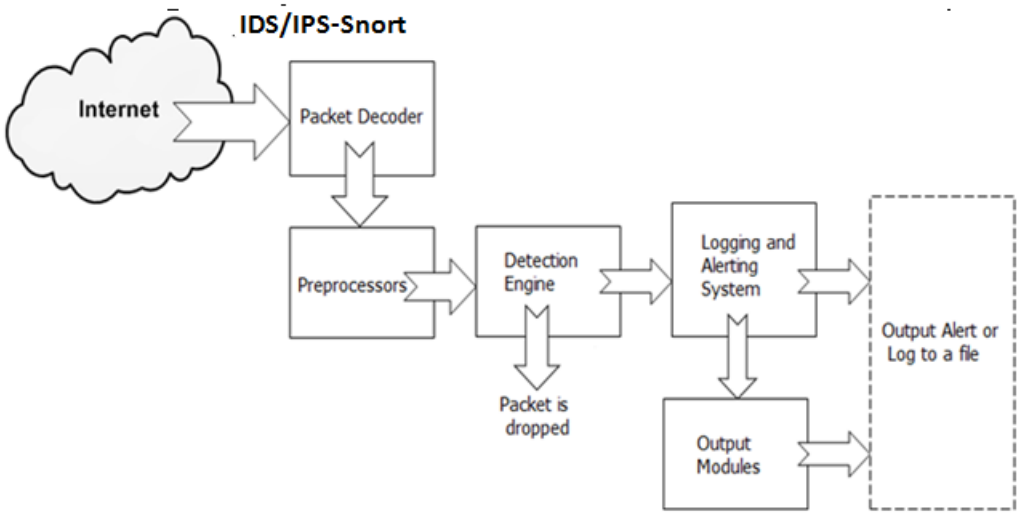
Hai kỹ thuật ngăn chặn thường được áp dụng:

- Kết thúc tiến trình (Terminate session): Cơ chế của kỹ thuật này là hệ thống IPS gửi các gói tin nhằm phá huỷ tiến trình bị nghi ngờ.

- Huỷ bỏ tấn công (Drop attack): Kỹ thuật này dùng tường lửa để hủy bỏ gói tin hoặc chặn đường một gói tin đơn, một phiên làm việc hoặc một luồng thông tin tấn công.

2.1.3.3. Ứng dụng hệ thống IDS/IPS chống tấn công web

Các hệ thống IDS/IPS có khả năng ứng dụng phát hiện và chống tấn công web. Trong [Hình 2.7] dưới đây mô tả mô hình ứng dụng hệ thống IDS/IPS dựa trên Snort chống tấn công website.



Hình 2.7. Mô hình hệ thống IDS/IPS chống tấn công web sử dụng Snort

Nhận xét

Giải pháp sử dụng hệ thống IDS/IPS chống tấn công web là giải pháp khá hữu hiệu nhằm phát hiện và chống tấn công hệ thống website đang hoạt động. Tuy nhiên, việc phân loại cụ thể các tấn công hệ thống website còn bị hạn chế. Khi đó có thể dẫn đến các biện pháp chống tấn công đưa ra của hệ thống không phù hợp. Vì vậy, trong phần tiếp theo, luận văn sẽ nghiên cứu giải pháp ứng dụng các kỹ thuật học máy để khắc phục nhược điểm này.

2.1.4. Ứng dụng phòng chống vi-rút và bảo vệ máy tính cá nhân

Việc cài đặt ứng dụng bảo vệ như phần mềm diệt vi-rút có tác dụng rất lớn trong việc bảo vệ hệ thống. Chúng có thể hạn chế được việc bị cài thêm mã độc trong trường hợp kẻ tấn công đã xâm nhập được vào hệ thống, hoặc hạn chế việc tải lên những mã động khi ứng dụng web bị lỗi. Các chương trình diệt vi-rút phải thỏa mãn các yêu cầu sau:

- Luôn ở trạng thái hoạt động nhằm đảm bảo hệ thống luôn được bảo vệ.
- Đảm bảo tính toàn vẹn của tập tin và tài nguyên.
- Quét các mã độc đính kèm trong thư điện tử.
- Cập nhật dấu hiệu nhận diện vi-rút mới nhất.

Đối với máy tính cá nhân có thể xem xét cài đặt phần mềm bảo vệ an toàn máy tính tích hợp thường bao gồm cả chức năng chống vi-rút, lọc tường lửa cá nhân.

2.2. Thiết lập và cấu hình hệ thống máy chủ an toàn

Đây là phần rất quan trọng trong việc đảm bảo vận hành một website an toàn. Nội dung trong phần này sẽ giúp người quản trị cấu hình hệ thống máy chủ một cách hợp lý, giảm thiểu khả năng bị kẻ xấu tấn công vào máy chủ làm ảnh hưởng đến hoạt động của website. Để vận hành một máy chủ an toàn, việc đầu tiên phải lưu ý là luôn cập nhật phiên bản và bản vá mới nhất cho hệ thống. Ngoài ra, với mỗi loại máy chủ khác nhau sẽ có những biện pháp thiết đặt và cấu hình cụ thể để đảm bảo vận hành an toàn.

2.2.1. Thiết lập và cấu hình hệ điều hành máy chủ

Máy chủ ngày nay thường sử dụng những hệ điều hành khá phổ biến như Linux, Window, v.v.. việc bảo vệ cho máy chủ là thực sự cần thiết. Để đảm bảo cho hệ thống hoạt động an toàn cần thực hiện một số biên pháp sau:

- Khi cài một hệ thống mới thì phải đảm bảo một số yêu cầu sau:

Khả năng hỗ trợ từ các bản phân phối (thông tin vá lỗi, thời gian cập nhật, nâng cấp, kênh thông tin hỗ trợ kỹ thuật).

Khả năng tương thích với các sản phẩm của bên thứ 3 (tương thích giữa nhân hệ điều hành với các ứng dụng, cho phép mở rộng mô-đun).

Khả năng vận hành và sử dụng hệ thống của người quản trị (thói quen, kỹ năng sử dụng, tính tiện dụng).

- Cần tối ưu hệ điều hành về những mặt sau:

Đối với chính sách mật khẩu: sử dụng cơ chế mật khẩu mạnh phức tạp (ví dụ: từ 08 ký tự trở lên và bao gồm: ký tự hoa, ký tự thường, ký tự đặc biệt và các chữ số) nhằm chống lại các kiểu tấn công Brute force.

Đối với các dịch vụ không cần thiết: việc gỡ bỏ các gói, dịch vụ không cần thiết sẽ hạn chế khả năng tiếp cận của kẻ tấn công và cải thiện hiệu năng của hệ thống.

Đối với điều khiển truy cập: chỉ định các truy cập được phép đến hệ thống, giới hạn tài khoản được phép sử dụng quyền quản trị cao nhất.

Đối với các kết nối: Sử dụng kết nối an toàn (Ví dụ: SSH) thay cho các kênh kết nối không an toàn như Telnet, FTP, v.v..

Đối với tập tin vật lý: quản lý hệ thống ghi nhật ký (log file) một cách tập trung và nhất quán nhằm phục vụ cho mục đích điều tra khi có sự cố xảy ra.

Đối với tài khoản và nhóm người dùng: Gỡ bỏ các tài khoản chưa sử dụng khỏi máy chủ, vô hiệu hóa tài khoản mặc định không sử dụng, thiết lập một mật khẩu mạnh cho tài khoản quản trị, giới hạn truy cập từ xa.

Đối với tập tin và thư mục: Tập tin và thư mục phải nằm trên phân vùng định dạng an toàn (ví dụ: NTFS), giới hạn quyền truy cập vào thư mục hoặc tập tin của hệ điều hành, giới hạn quyền ghi vào thư mục gốc đối với các tài khoản không thuộc nhóm quản trị, đối với những tài nguyên được chia sẻ: Gỡ bỏ tất cả các chia sẻ không sử dụng (Bao gồm cả chia sẻ mặc định).

Đối với các bản vá lỗi: Cập nhật các phiên bản mới nhất, theo dõi thông tin cập nhật từ nhiều nguồn khác nhau, nên triển khai cập nhật trên hệ thống thử nghiệm trước khi cập nhật vào hệ thống thật.

2.2.2. Thiết lập và cấu hình máy chủ ứng dụng web

Một số máy chủ được sử dụng khá phổ biến trong các ứng dụng web hiện nay là Apache HTTP, Apache Tomcat, IIS,v.v.. Để đảm bảo an toàn cho các máy chủ cần thực hiện một số biện pháp như sau:

- Tối ưu hóa việc sử dụng các mô-đun bằng việc gỡ bỏ những thành phần không cần thiết.

- Giới hạn các quyền truy cập: Tạo các tài khoản, nhóm người dùng riêng (khác tài khoản như Root, Administrator, v.v..) để thực thi. Không cho phép sử dụng các tài khoản mặc định để đăng nhập.

- Điều khiển truy cập: Sử dụng các chỉ mục để điều khiển quá trình truy cập đến các thư mục hệ thống cần hạn chế quyền truy cập, không cho phép duyệt qua thư mục gốc.

- Gỡ bỏ tất cả các tài nguyên không cần thiết như: các trang html mặc định, hướng dẫn sử dụng, thông tin liên quan về máy chủ, điều khiển trạng thái máy chủ, thông tin máy chủ. Trong quá đình cài đặt có thể xuất hiện các ứng dụng mẫu, tài liệu hướng dẫn và một số thư mục không cần thiết khác. Vì vậy cần gỡ bỏ các tập tin, thư mục này nhằm hạn chế thấp nhất nguy cơ bị khai thác thông tin liên quan đến ứng dụng đang sử dụng. Bảo vệ các tập tin cấu hình (ví dụ: .htaccess, context.xml, server.xml, v.v..).

- Tổ chức quá trình ghi nhật ký: Cấu hình ghi nhật ký lỗi, nhật ký truy cập. Đảm bảo toàn bộ thông in của người dùng khi đăng nhập vào hệ thống sẽ đều được ghi lại. Tất cả những dữ liệu khi truy cập đều được ghi lại trong nhật ký.

- Đối với một số trang thông tin cần mã hóa truy cập, nên sử dụng các giao thức mã hóa như SSL hoặc TLS nhằm mã hóa các kết nối an toàn.

- Giới hạn các thông tin về hệ thống như: thông tin về cấu hình máy chủ, thông tin về các phần mềm được cài đặt trên máy chủ.

- Bảo vệ cấu hình máy chủ: Giới hạn truy cập đến thư mục gốc, thư mục chứa tập tin cấu hình của máy chủ web, thư mục chứa các tập tin nhật ký, thư mục chứa các tập tin thực thi, thư mục chứa ứng dụng web.

- Cần thiết lập hạn chế các truy cập từ mạng tới máy chủ, chặn các tài khoản vãng lai, tài khoản khách mặc định nhằm đảm bảo tính bảo mật cao hơn.

- Tắt tất cả các chi tiết thông báo lỗi mà có khả năng đưa ra quá nhiều thông tin. Việc đưa ra quá chi tiết các thông báo lỗi có thể dẫn đến việc các tin tặc có thể lợi dụng để tìm hiểu thông tin về hệ thống.

- Nên cài đặt thư mục gốc của ứng dụng web trên phân vùng đĩa có định dạng bảo mật cao (ví dụ với máy chủ IIS nên lưu trên phân vùng NTFS thay vì FAT hay FAT32, bởi vì khả năng kiểm soát quyền truy cập trên hệ thống tập tin với phân vùng định dạng NTFS mạnh hơn so với các định dạng FAT, FAT32). Khi đã cài đặt thư mục gốc trên phân vùng có định dạng bảo mật cao thì cũng phải thiết lập quyền truy cập thấp nhất cho thư mục gốc này, tránh trường hợp thư mục gốc của ứng dụng web được mặc định quyền đầy đủ cho mọi tài khoản.

- Gỡ bỏ những thành phần không cần thiết được cài đặt ra khỏi máy chủ web, vì những thành phần này khi bị lỗi có thể dẫn đến khả năng máy chủ bị tấn công và chiếm quyền kiểm soát một cách gián tiếp.

- Cần cài đặt bổ sung thêm nhiều tính năng bảo vệ cho máy chủ (như có thể cài đặt ModSecurity cho máy chủ Apache, URL scan cho máy chủ IIS, v.v..).

- Điều chỉnh các thông số tối ưu. Ví dụ thiết lập tham khảo một vài thông số với máy chủ Apache:

Timeout 100

KeepAlive On

MaxKeepAliveRequest 100

KeepAliveTimeout 15

LimitRequestline 512

LimitRequestFields 100

LimitRequestFieldsize 1024

LimitRequestBody 102400

2.2.3. Thiết lập và cấu hình máy chủ cơ sở dữ liệu

Việc thiết lập và cấu hình máy chủ cơ sở dữ liệu an toàn là rất quan trọng và là một quá trình phức tạp, đòi hỏi người quản trị phải hiểu rõ về cơ sở dữ liệu đang sử dụng. Để bảo vệ cho cơ sở dữ liệu an toàn cần thực hiện một số biện pháp sau:

- Luôn cập nhật phiên bản vá lỗi cho cơ sở dữ liệu mới nhất nhằm tránh các lỗi đã được công bố và khai thác.

- Gỡ bỏ các cơ sở dữ liệu không sử dụng đến.

- Gỡ bỏ hoặc vô hiệu hóa những thủ tục lưu trữ hoặc những hàm nhạy cảm có tương tác với hệ thống nhằm tránh việc tương tác đến hệ thống từ cơ sở dữ liệu.

- Tách biệt các cơ sở dữ liệu sử dụng cho các mục đích khác nhau.

- Khóa tất cả các kết nối từ hệ thống hoặc từ ứng dụng khác ngoài ứng dụng web và máy chủ web, không cho phép bất cứ kết nối trực tiếp nào từ Internet đến máy chủ cơ sở dữ liệu.

- Cấu hình ghi nhật ký và theo dõi nhật ký hoạt động của cơ sở dữ liệu một cách hợp lý.

- Giới hạn truy cập đối với các tài khoản sử dụng (Không có quyền xóa hoặc thay đổi cấu trúc cơ sở dữ liệu).

- Phân quyền cho các tài khoản và các tập tin hệ thống.

- Gỡ bỏ hoặc thay đổi các tài khoản mặc định và thiết lập mật khẩu mạnh cho các tài khoản đang sử dụng.

- Có cơ chế sao lưu dữ liệu định kỳ và mã hóa các dữ liệu sao lưu.

- Sử dụng các công cụ để tìm kiếm lỗ hổng trên máy chủ cơ sở dữ liệu (ví dụ MBSA của Microsoft SQL).

2.3. Vận hành an toàn

Khi đã triển khai và thiết lập được một hệ thống an toàn thì việc vận hành hệ thống một cách an toàn là vô cùng quan trọng. Trong phần này luận văn sẽ trình bày các nội dung cơ bản cần thực hiện để vận hành một ứng dụng web an toàn.

2.3.1. Kiểm tra hoạt động ứng dụng web an toàn

Để đảm bảo cho ứng dụng web vận hành an toàn, tránh được các nguy cơ tấn công từ bên ngoài hệ thống có thể tiến hành các bước cơ bản sau:

- Kiểm tra việc lộ thông tin nhạy cảm qua các công cụ tìm kiếm, bước này nhằm đảm bảo ứng dụng web sẽ không hiển thị những thông tin riêng như phiên bản, cấu trúc thư mục, v.v.. lên kết quả của công cụ tìm kiếm.

- Kiểm tra chức năng đăng xuất, đăng nhập có hoàn thành đúng nhiệm vụ hay không.

- Thiết đặt các quyền truy cập thích hợp vào các tập tin và thư mục nhạy cảm. Xóa các tập tin sao lưu dự phòng ra khỏi hệ thống.

- Sử dụng mã xác nhận và chế độ mật khẩu mạnh nhằm tránh trường hợp vượt qua mã xác nhận hoặc đoán mật khẩu ngắn (không cho phép người dùng đặt mật khẩu yếu).

- Kiểm tra quá trình quản lý tài khoản và phiên của ứng dụng, việc gửi những thông tin quan trọng như tên đăng nhập và mật khẩu cần được mã hóa nhằm tránh tình trạng nghe lén dữ liệu trên đường truyền. Bên cạnh đó việc cấp phát và mã hóa phiên đăng nhập cho người dùng cũng cần đảm bảo an toàn nhằm tránh tình trạng tin tặc đoán hay giả mạo phiên.

- Xác định loại mã nguồn hỗ trợ web (PHP, JSP, ASP, v.v..) và nền tảng phát triển web (mã nguồn mở, tự phát triển, v.v..) để có biện pháp bảo vệ hợp lý cũng như cập nhật khắc phục các lỗ hổng được phát hiện.

- Xây dựng hoặc triển khai một hệ thống máy chủ Proxy để chắc rằng các kết nối từ bên ngoài vào và từ bên trong ra sẽ được giám sát để tránh các mối đe dọa cũng như điều tra nguyên nhân khi hệ thống bị tấn công.

- Nếu có nhiều trang web được đặt chung trên máy chủ web, cần có biện pháp cách ly các website này ra, nhằm đảm bảo nếu một trang web bị tấn công và chiếm quyền kiểm soát thì các trang web còn lại sẽ ít bị ảnh hưởng.

- Thiết kế trang báo lỗi chung để trả về cho tất cả các lỗi mà hệ thống có thể gặp phải. Biện pháp này nhằm giảm nguy cơ bị tấn công dựa theo thông báo lỗi của ứng dụng.

2.3.2. Một số biện pháp ứng phó với tấn công

Khi có dấu hiệu của một cuộc tấn công vào website của mình, các đơn vị cần có những biện pháp ứng phó kịp thời làm suy giảm hay ngừng hẳn cuộc tấn công, cũng có thể chuyển hướng cuộc tấn công. Sau đây là một số biện pháp tổng quát:

- Tăng cường khả năng xử lý của hệ thống, thường xuyên gia cố các điểm yếu của ứng dụng. Cập nhật các bản vá lỗi của hệ điều hành và các phần mềm ngay khi được phát hành để tránh việc khai thác tấn công vào các lỗi này. Tối ưu hóa các thuật toán xử lý, mã nguồn hệ thống để nâng cao khả năng xử lý.

- Chú trọng đầu tư hạ tầng mạng, tăng cường số lượng cũng như cấu hình máy chủ và phần mềm an ninh nếu có thể.

- Chú trọng công tác phát hiện sớm các hành vi tấn công. Khi nghi ngờ có tấn công người quản trị cần kiểm tra trên hệ thống nhật ký log của máy chủ, tường lửa, v.v.. nhằm phát hiện các dấu hiệu bất thường, từ đó xác định có hành vi tấn công xảy ra hay không, quy mô, cách thức thế nào.

- Khi tấn công xảy ra cần có biện pháp khẩn cấp nhằm ngăn chặn, đối phó với cuộc tấn công. Thu thập, phân tích tệp tin nhật ký hoạt động nhằm truy tìm nguồn gốc tấn công để có biện pháp ngăn chặn kịp thời. Có thể chặn kết nối, chặn luồng tin từ địa chỉ tấn công. Với tấn công từ chối dịch vụ cần tìm nơi lưu trữ máy chủ điều khiển, xác định ip tấn công để ngăn chặn.

- Khi các cuộc 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.

- Thiết lập lại chính sách an ninh của hệ thống nói chung và chính sách an ninh của tường lửa nói riêng, thay đổi các ngưỡng để thực hiện ngăn chặn tấn công kịp thời.

- Trong nhiều trường hợp có thể thực hiện chuyển hướng cuộc tấn công để giảm bớt thiệt hại, hay có thêm thời gian để ứng phó và ngăn chặn tấn công.

- Thường xuyên cập nhật trao đổi thông tin với các cơ quan có chức năng như Cảnh sát phòng chống tội phạm sử dụng công nghệ cao. Cục An toàn thông tin - Bộ Thông tin và Truyền thông, VNCERT, nhà cung cấp dịch vụ Internet, nhà cung cấp

dịch vụ cho thuê máy chủ, v.v.. để nhận được hỗ trợ cần thiết chống lại các cuộc tấn công, nhất là tấn công từ chối dịch vụ. Khi phát hiện ra dấu hiệu tấn công hay cuộc tấn công xảy ra mà không đủ khả năng phòng chống cần báo ngay cho các cơ quan này để họ giúp đỡ.

2.3.3. Đào tạo đội ngũ nhân lực vận hành hệ thống

Việc đảm bảo an toàn an ninh cho các hệ thống website nói riêng và hệ thống mạng nói chung thì yếu tố con người vẫn là tính chất quyết định. Do đó, vấn đề đặt ra là cần có một đội ngũ nhân lực đủ năng lực chuyên môn và đạo đức để vận hành hệ thống một cách an toàn. Vì vậy, đào tạo nhân lực vận hành hệ thống là một điều không thể thiếu cho bất cứ một hệ thống công nghệ thông tin nào. Để làm được điều này cần thực hiện một số nội dung sau:

- Có chính sách và ngân sách cho việc đào tạo đội ngũ nhân lực an toàn thông tin về cả năng lực chuyên môn lẫn đạo đức nghề nghiệp. Đặc biệt, đội ngũ nhân lực làm công tác này cần hiểu rõ quy định về đạo đức nghề nghiệp đối với cán bộ làm công tác an toàn thông tin mà Hiệp hội an toàn thông tin Việt Nam đã ban hành.

- Yêu cầu đội ngũ nhân lực an toàn thông tin thực hiện đúng nguyên tắc và quyền hạn của mình. Có chính sách đối với những nhân viên đã kết thúc công việc như: xóa bỏ tài khoản, sao chép ổ cứng của người đó khi họ nghỉ việc rồi xóa ổ cứng đó cho người khác dùng để làm bằng chứng nếu vi phạm sau này.

- Tạo điều kiện cho đội ngũ nhân lực an toàn thông tin được tìm hiểu, học hỏi và tập huấn nâng cao năng lực chuyên môn.

- Cần được tập trung và đào tạo nâng cao kinh nghiệm một cách thường xuyên về an toàn thông tin cho đội ngũ nhân lực.

- Thường xuyên phối hợp với các cơ quan nhà nước có chức năng về an toàn thông tin và các đơn vị đào tạo, hỗ trợ về an toàn thông tin để trao đổi kinh nghiệm, tổ chức tham gia tập huấn nâng cao kỹ năng về an toàn thông tin.

2.4. Tấn công từ chối dịch vụ và cách phòng chống

Tấn công từ chối dịch vụ là kiểu tấn công nhằm ngăn cản những người dùng hợp lệ truy cập và sử dụng vào một dịch vụ nào đó. Tấn công từ chối dịch vụ có thể làm ngưng hoạt động của một máy tính, một mạng nội bộ, thậm chí cả một hệ thống mạng rất lớn. Bằng cách chiếm dụng một lượng lớn tài nguyên hệ thống như băng thông, bộ nhớ v.v.. hay làm quá tải tài nguyên hệ thống và làm mất khả năng xử lý các yêu cầu dịch vụ từ những người dùng hợp lệ. Mặc dù tấn công từ chối dịch vụ không có khả năng truy cập vào dữ liệu thực của hệ thống những nó có thể làm gián đoạn các dịch vụ mà hệ thống đó cung cấp. Khi dịch vụ của một hệ thống bị tạm ngưng hoạt động có thể gây ra những thiệt hại vô cùng lớn, chẳng hạn như các hệ thống phục vụ điện, nước, các hệ thống giao dịch điện tử v.v.. Với những hệ thống được bảo mật tốt, khó xâm nhập, việc tấn công từ chối dịch vụ thường được các tin tặc sử dụng để tấn công hệ thống đó.

Tất cả các hệ thống mạng máy tính đều có một giới hạn nhất định như giới hạn về băng thông, giới hạn về bộ nhớ, giới hạn về số lượng yêu cầu của người dùng tại một thời điểm v.v.. Do đó nó chỉ có thể đáp ứng một lượng yêu cầu dịch vụ giới hạn nào đó mà thôi. Như vậy, hầu hết các hệ thống mạng đều có thể trở thành mục tiêu tấn công từ chối dịch vụ. Tùy vào cách thức thực hiện mà tấn công từ chối dịch vụ được biết dưới nhiều tên gọi khác nhau:

- Tấn công từ chối dịch vụ cổ điển (DoS).
- Tấn công từ chối dịch vụ phân tán (DDoS).
- Tấn công từ chối dịch vụ phản xạ nhiều vùng (DRDoS).

2.4.1. Tấn công từ chối dịch vụ (DoS)

Tấn công từ chối dịch vụ (DoS) là một hình thức tấn công phổ biến được khá nhiều hacker sử dụng hiện nay. Mục đích của tấn công DoS là cố gắng chiếm băng thông mạng và làm hệ thống mạng bị ngập, khi đó hệ thống mạng sẽ không có khả năng đáp ứng những dịch vụ khác cho người dùng thông thường; Cố gắng làm ngắt kết nối giữa hai máy và ngăn chặn quá trình truy cập vào dịch vụ; Cố gắng chặn

người dùng cụ thể vào một dịch vụ nào đó; Cố gắng ngăn chặn các dịch vụ không cho người khác có khả năng truy cập vào. Khi tấn công DoS xảy ra, người dùng truy cập vào dịch vụ đó sẽ có cảm giác như dịch vụ đó đang bị tắt, không hoạt động hoặc hoạt động chậm. Để tấn công từ chối dịch vụ DoS, hacker sẽ tạo ra một lượng rất lớn các truy cập đến máy tính mục tiêu, khiến nó không kịp xử lý các tác vụ cần thiết, từ đó dẫn đến quá tải và ngừng hoạt động.

Mục tiêu của các cuộc tấn công DoS thường là máy chủ web của các tổ chức như ngân hàng, doanh nghiệp, công ty truyền thông, các trang báo, mạng xã hội, các hệ thống phục vụ điện, nước, các hệ thống giao dịch điện tử v.v.. Tuy nhiên, DoS chỉ xuất phát từ một địa điểm duy nhất và chỉ có 1 dải IP nên có thể bị phát hiện dễ dàng và ngăn chặn được.

2.4.2. Tấn công từ chối dịch vụ phân tán (DDoS)

Tấn công từ chối dịch vụ phân tán (DDoS) là một dạng tấn công từ nhiều máy tính tới một đích, làm cho các yêu cầu hợp lệ của người dùng bình thường bị từ chối. So với DoS cổ điển, sức mạng của DDoS tăng gấp nhiều lần. Hầu hết các cuộc tấn công DDoS nhằm vào việc chiếm dụng băng thông, chiếm dụng tài nguyên hệ thống, gây nghẽn mạng hệ thống, làm cho hệ thống ngưng hoạt động. Để thực hiện DDoS, hacker tìm cách chiếm dụng và điều khiển nhiều máy tính, mạng máy tính trung gian được gọi là botnet (đóng vai trò là zombie) từ nhiều nơi không giới hạn về mặt địa lý để đồng loạt gửi ào ạt các gói tin với số lượng rất lớn tới một mục tiêu đã được xác định nhằm chiếm dụng tài nguyên và làm tràn ngập đường truyền của mục tiêu đó.

Cuộc tấn công DDoS sẽ được thực hiện từ một hệ thống máy tính cực lớn trên mạng toàn cầu và thường dựa vào các dịch vụ có sẵn trên các máy tính trong mạng botnet. Dạng tấn công này rất khó bị phát hiện bởi nó được sinh ra từ nhiều địa chỉ IP trên mạng Internet. Những gói tin đến tường lửa có thể chặn lại, nhưng hầu hết chúng đều đến từ những địa chỉ IP chưa có trong các chính sách luật của tường lửa và là những gói tin hoàn toàn hợp lệ. Nếu có một địa chỉ IP nguồn tấn công thì có thể được chặn bởi tường lửa, bằng cách cấm giao tiếp với địa chỉ nguồn đó. Nhưng

mạng botnet có hàng ngàn tới hàng trăm ngàn địa chỉ IP tấn công thì điều này là vô cùng khó khăn.

2.4.3. Tấn công từ chối dịch vụ phản xạ nhiều vùng (DRDoS)

DRDoS xuất hiện vào đầu năm 2002, được cho là một trong những kiểu tấn công mạnh nhất họ DoS. Nếu được thực hiện bởi kẻ tấn công có tay nghề thì có thể hạ gục bất cứ hệ thống nào trong phút chốc.

Mục tiêu chính của DRDoS 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, v.v.. đều bị vô hiệu hóa.

Về cơ bản, DRDoS là sự phối hợp giữa hai kiểu tấn công 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 giống như DDoS. Kẻ tấn công thực hiện bằng cách giả mạo địa chỉ của máy chủ mục tiêu rồi gửi yêu cầu SYN đến các máy chủ lớn trên mạng, để các máy chủ này gửi các gói tin SYN/ACK đến máy chủ mục tiêu. Các máy chủ lớn, đường truyền mạnh đã vô tình đóng vai trò là các máy tính ma 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 máy chủ lớn tham gia nên máy chủ mục tiêu nhanh chóng bị quá tải, băng thông bị chiếm dụng bởi các máy chủ lớn. Với kiểu tấn công này, tin tặc chỉ cần một máy tính với Modem 56kbps là 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.

2.4.4. Phân loại tấn công DDoS

Tấn công DDoS có thể chia ra thành hai loại chính là tấn công làm cạn kiệt băng thông và tấn công làm cạn kiệt tài nguyên hệ thống.

Tấn công làm cạn kiệt băng thông được thiết kế nhằm làm tràn ngập mạng mục tiêu với những lưu lượng không cần thiết, với mục đích ngăn chặn những lưu lượng hợp lệ đến được với hệ thống cung cấp dịch vụ của mục tiêu. Tấn công làm cạn kiệt băng thông hệ thống có thể chia ra thành hai loại: Tấn công làm lụt hệ thống (Flood Attack) và tấn công khuếch đại (Amplification Attack).

Tấn công làm cạn kiệt tài nguyên là kiểu tấn công trong đó kẻ tấn công gửi những gói tin sử dụng các giao thức sai chức năng thiết kế, hay gửi những gói tin với dụng ý làm tắc nghẽn tài nguyên mạng, làm cho các tài nguyên này không phục vụ được những người dùng thông thường khác. Tấn công làm cạn kiệt tài nguyên có hai dạng: Khai thác lỗ hổng trên các giao thức (Protocol Exploit Attack) và gửi các gói tin không đúng chuẩn (Malformed Packet Attack).

Trong khuôn khổ luận văn, học viên xin liệt kê một số loại tấn công DDoS nổi bật như sau [11][12]:

SYN Flood:

SYN Flood khai thác điểm yếu trong chuỗi kết nối TCP, được gọi là bắt tay ba chiều. Máy chủ sẽ nhận được một thông điệp đồng bộ (SYN) để bắt đầu "bắt tay". Máy chủ nhận tin nhắn bằng cách gửi cờ báo nhận (ACK) tới máy lưu trữ ban đầu, sau đó đóng kết nối. Tuy nhiên, trong một SYN Flood, tin nhắn giả mạo được gửi đi và kết nối không đóng, dẫn đến dịch vụ sập.

UDP Flood:

UDP (User Datagram Protocol) được hiểu là giao thức kết nối không tin cậy. Theo đó, UDP Flood sẽ tấn công gây ngập lụt UDP.

Khi thực hiện phương thức tấn công này, hacker sẽ gửi một lượng lớn các gói tin UDP tới một số cổng ngẫu nhiên trên server. Máy chủ kiểm tra và trả lời với một ICMP Destination Unreachable (gói tin không tìm thấy). Khi số lượng yêu cầu UDP vượt quá ngưỡng cho phép, máy chủ sẽ mất khả năng xử lý request, dẫn đến tình trạng từ chối dịch vụ.

HTTP Flood:

HTTP Flood tấn công, gây quá tải bằng cách gửi hàng loạt yêu cầu GET hoặc POST hợp pháp đến máy chủ. Phương pháp này tuy tiêu tốn ít băng thông hơn các kiểu tấn công từ chối dịch vụ khác nhưng vẫn có thể buộc máy chủ sử dụng nguồn tài nguyên tối đa để xử lý tác vụ.

Ping of Death:

Ping of Death là kỹ thuật tấn công làm quá tải hệ thống máy chủ trực tuyến bằng cách gửi đến các gói tin ICMP có kích thước trên 65.536 byte đến mục tiêu. Bởi kích thước tệp vượt quá mức cho phép của gói tin IP nên chúng sẽ được chia thành từng phần nhỏ và gửi đến hệ thống máy đích. Khi đến nơi, các phần này sẽ được phép lại thành một gói tin hoàn chỉnh vượt quá khả năng xử lý của hệ thống, gây tràn bộ nhớ đệm và khiến máy chủ bị treo. Đây là loại DDoS phổ biến cách đây hai thập kỷ nhưng đã không còn hiệu quả vào thời điểm hiện tại.

Smurf Attack:

Smurf Attack khai thác giao thức Internet (IP) và ICMP (Internet Control Message Protocol) sử dụng một chương trình phần mềm độc hại gọi là smurf. Nó giả mạo một địa chỉ IP và và gửi các gói ICMP đến máy chủ, gây quá tải hệ thống.

Fraggle Attack:

Fraggle Attack sử dụng một lượng lớn lưu lượng UDP đến máy chủ. Nó giống như một cuộc tấn công Smurf nhưng sử dụng UDP nhiều hơn là ICMP.

Slowloris:

Slowloris cho phép kẻ tấn công sử dụng nguồn lực tối thiểu trong một cuộc tấn công và các mục tiêu trên máy chủ web. Khi đã kết nối với mục tiêu mong muốn, Slowloris sẽ cố gắng giữ số liên kết tối đa trong thời gian dài. Khi số lượng kết nối của máy chủ web đạt cực đại (webserver bị đầy kết nối), máy chủ sẽ bắt đầu từ chối những yêu cầu kết nối tiếp theo, bao gồm cả request của người dùng thông thường.

Application Level Attacks:

Application Level Attacks khai thác lỗ hổng trong các ứng dụng. Mục tiêu của loại tấn công này không phải là toàn bộ máy chủ, mà là các ứng dụng với những điểm yếu được biết đến. Đây được xem là loại tấn công tinh vi và gây ra hậu quả lớn nhất.

NTP Amplification:

NTPAmplification khai thác các máy chủ NTP (Network Time Protocol), đây là kiểu tấn công khai thác lỗ hổng tính năng Monlist của máy chủ NTP (Monlist là danh sách các máy tính kết nối với máy chủ NTP). Cụ thể, hacker sẽ gửi request yêu cầu Monlist đến NTP server bằng IP giả. Source IP bị giả mạo chính là địa chỉ IP của máy tính mục tiêu. Vì vậy, các NTP server sẽ liên tục gửi phản hồi Monlist về cho nạn nhân. Điều này khiến hệ thống webserver mục tiêu bị quá tải. Vì sử dụng IP giả mạo và có khả năng khuếch đại và sử dụng băng thông lớn nên NTP Amplification là một kiểu tấn công "ném đá giấu tay" có tính phá hoại rất cao.

Advanced Persistent DoS (APDoS):

Advanced Persistent DoS (APDoS) là một loại tấn công được sử dụng bởi hacker với mong muốn gây ra những thiệt hại nghiêm trọng. APDoS sử dụng nhiều kiểu tấn công đã đề cập như HTTP Flood, SYN Flood, v.v...) và thường tấn công theo kiểu gửi hàng triệu yêu cầu/giây. Các cuộc tấn công của APDoS có thể kéo dài hàng tuần, phụ thuộc vào khả năng của hacker để chuyển đổi chiến thuật bất cứ lúc nào và tạo ra sự đa dạng để tránh các chính sách bảo vệ.

Zero-day DDoS Attacks:

Zero-day DDoS Attacks là tên được đặt cho các phương pháp tấn công DDoS mới, gây quá tải hệ thống bằng cách khai thác các lỗ hổng chưa được vá của máy chủ.

2.4.5. Phòng chống tấn công từ chối dịch vụ

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 các gói tin IP từ các nguồn không tin cậy là hữu hiệu nhất. Không có một cách thức cụ thể nào có thể ngăn chặn hoàn toàn việc bị tấn công DoS/DDoS. Tuy nhiên có vài phương pháp giúp giảm bớt phần nào nguy cơ trở thành nạn nhân của DDoS [14]:

- Mô hình hệ thống cần phải được xây dựng hợp lý, tránh phụ thuộc lẫn nhau quá mức. Bởi khi một bộ phận gặp sự cố sẽ làm ảnh hưởng tới toàn bộ hệ thống

- Thiết lập mật khẩu mạnh (strong password) để bảo vệ các thiết bị mạng và các nguồn tài nguyên quan trọng khác.

- 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 bị tấn công hãy nhanh chóng truy tìm địa chỉ IP đó và chặn 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.

Có rất nhiều giải pháp và ý tưởng được đưa ra nhằm đối phó với các cuộc tấn công kiểu từ chối dịch vụ như trên. Tuy nhiên không có giải pháp và ý tưởng nào là giải quyết triệt để bài toán chống tấn công từ chối dịch vụ. Các hình thái khác nhau của tấn công từ chối dịch vụ liên tục xuất hiện theo thời gian, song song với các giải pháp đối phó. Việc đấu tranh với tấn công từ chối dịch vụ là một thực tế thường xuyên, việc lựa chọn giải pháp nào phụ thuộc vào nhận thức và mức độ đầu tư của mỗi đơn vị.

2.5. Đề xuất ứng dụng các giải pháp đảm bảo an toàn thông tin website đối với các doanh nghiệp vừa và nhỏ

Tùy thuộc vào quy mô, chức năng và yêu cầu tính bảo mật của mỗi website chúng ta có thể triển khai các giải pháp đảm bảo an toàn thông tin khác nhau. Những website yêu cầu tính bảo mật thấp, đôi lúc chỉ cần một máy chủ web với cấu hình cơ bản được đặt trực tiếp trên môi trường mạng Internet. Ngược lại những website yêu cầu tính bảo mật cao thì lại phải kết hợp tổ chức mô hình mạng phức tạp kết hợp quy trình vận hành chặt chẽ.

Trong mục này học viên sẽ tập trung đề xuất các giải pháp đảm bảo an toàn thông tin Website cho các doanh nghiệp vừa và nhỏ bao gồm:

- Tổ chức mô hình mạng cho hệ thống máy chủ web
- Thiết lập tường lửa
- Xây dựng cấu hình hệ thống máy chủ, thiết lập các dịch vụ máy chủ web như hệ điều hành, apache, cơ sở dữ liệu.
- Xây dựng quy trình vận hành website

2.5.1. Phương án tổ chức mô hình mạng cho hệ thống máy chủ web

Xây dựng mô hình mạng bao gồm cụm máy chủ ứng dụng web, máy chủ chứa dữ liệu ảnh CDN và cụm máy chủ chứa cơ sở dữ liệu.

Máy chủ ứng dụng web và máy chủ chứa dữ liệu ảnh cần được đặt trên vùng mạng DMZ. Máy chủ ứng dụng web được cài đặt mã nguồn website PHP và điều hướng cũng như xử lý truy cập bằng dịch vụ Nginx.

Máy chủ ứng dụng web chỉ mở kết nối từ domain và có thể truy cập đến máy chủ CDN ở cùng vùng mạng DMZ để lấy dữ liệu ảnh. Dữ liệu web được lấy từ cơ sở dữ liệu thông qua việc truy cập đến cơ sở dữ liệu tại vùng mạng nội bộ.

Máy chủ chứa cơ sở dữ liệu được đặt ở vùng mạng nội bộ của doanh nghiệp, được cài đặt hệ quản trị cơ sở dữ liệu (MySql). Máy chủ này chỉ mở cổng truy cập trực tiếp từ IP của vùng mạng DMZ - máy chủ ứng dụng web.

Việc tổ chức mô hình mạng máy chủ như vậy giúp cho website của doanh nghiệp có thể tránh được những tấn công trực tiếp đến IP của máy chủ web và máy chủ cơ sở dữ liệu từ môi trường Internet.

2.5.2. Thiết lập tường lửa cho máy chủ web

Máy chủ ứng dụng web nên sử dụng VPS hệ điều hành Centos được cài đặt dịch vụ tường lửa Iptables. Với dịch vụ Iptables ta có thể thiết lập để mở và đóng truy cập từ các IP và cổng khác nhau. Cụ thể ta chỉ cho phép truy cập máy chủ web thông qua truy cập vào website bằng cổng 80 và 443 tương ứng với giao thức http và https.

Sử dụng cấu hình trong Iptables chỉ cho phép truy cập đến máy chủ thông qua 2 cổng trên. Mặc định những truy cập từ cổng khác sẽ bị chặn như SSH, FTP, SMTP…

```
# iptables -I INPUT -p tcp -m tcp --dport 80 -j ACCEPT
# iptables -I INPUT -p tcp -m tcp --dport 443 -j ACCEPT
```

2.5.3. Cấu hình máy chủ web và máy chủ cơ sở dữ liệu

Máy chủ web của doanh nghiệp được đặt ở vùng mạng DMZ với 2 cụm là cụm máy chủ ứng dụng được cài đặt mã nguồn website và máy chủ CDN chứa dữ liệu ảnh của web. Trong đó, máy chủ ứng dụng web sử dụng điều hướng bằng dịch vụ Nginx, để quản lý truy cập đến website cũng như tài nguyên.

Dịch vụ điều hướng Nginx được cấu hình để chỉ mạng nội bộ mới truy cập được mô đun quản trị và duyệt thư mục tài nguyên của website. Còn lại những truy cập của khách vãng lai sẽ chỉ xem được mô đun giao diện người dùng. Như vậy chỉ

những người có quyền quản trị website và sử dụng mạng nội bộ của doanh nghiệp mới được phép truy cập vào mô đun quản trị cũng như duyệt thư mục chứa tài nguyên của website.

Bên cạnh đó máy chủ web cần được cài đặt để lưu thông tin truy cập của tất cả khách thông qua dịch vụ lưu nhật ký của mã nguồn. Điều này cho phép quản trị viên kiểm tra được những truy cập bất thường hoặc những truy cập gặp lỗi trên website.

Máy chủ chứa cơ sở dữ liệu của website được đặt ở môi trường mạng nội bộ, chỉ cho phép truy cập từ IP của máy chủ ứng dụng web với cổng 3306 của hệ điều hành MySql.

2.5.4. Vận hành website

Để vận hành website ổn định và đảm bảo tính bảo mật thông tin, doanh nghiệp cần xây dựng một đội ngũ nhân viên IT và quy trình vận hành chuyên nghiệp.

Đội ngũ IT có nhiệm vụ nâng cấp hệ thống website bao gồm mã nguồn theo yêu cầu tính năng và phần cứng đáp ứng website hoạt động bình thường. Đồng thời vận hành website, thường xuyên kiểm tra những truy cập thông qua hệ thống Logging (nhật ký), tìm ra và giải quyết những vấn đề xảy ra hàng ngày như lỗi web hoặc có tấn công từ tin tặc.

Quyền quản trị trên website phải được phân chia rõ ràng, tài khoản riêng được cấp cho mỗi cá nhân để đảm bảo những hành động trên mô đun quản trị đều được ghi lại và gán trách nhiệm cho từng người.

Dữ liệu của website bao gồm dữ liệu ảnh, văn bản và dữ liệu trong cơ sở dữ liệu cần được quản trị viên thường xuyên backup để đảm bảo khi có sự cố xảy ra, có thể khôi phục lại bình thường một cách nhanh chóng, tránh mất dữ liệu quan trọng của hệ thống.

2.6. Kết luận Chương 2

Trong Chương 2, luận văn đã khảo sát 04 nhóm giải pháp đảm bảo thông tin cho website, bao gồm: triển khai hệ thống phòng thủ, thiết lập và cấu hình hệ thống

máy chủ an toàn, vận hành an toàn và phòng chống tấn công từ chối dịch vụ. Trong đó, tập trung vào các giải pháp phòng chống tấn công từ chối dịch vụ. Từ đó phân tích ứng dụng thực tế các giải pháp cho việc đảm bảo an toàn Website của doanh nghiệp vừa và nhỏ, đảm bảo chi phí hợp lý và mức độ an toàn cần thiết.

Trên cơ sở đó, trong chương tiếp theo, luận văn sẽ tiến hành đánh giá mức độ bảo mật website của Sở Thông tin và Truyền thông Hà Nội và đưa ra các giải pháp nâng cao mức độ bảo mật.

CHƯƠNG 3. ĐÁNH GIÁ MỨC ĐỘ BẢO MẬT WEBSITE CỦA SỞ THÔNG TIN VÀ TRUYỀN THÔNG HÀ NỘI

Trong Chương 3 luận văn tiến hành đánh giá mức độ bảo mật website Sở Thông tin và Truyền thông Hà Nội và đưa ra các giải pháp nâng cao bảo mật.

3.1. Đặc điểm website của doanh nghiệp vừa và nhỏ

*** Về chức năng**

- Cung cấp thông tin doanh nghiệp, dịch vụ và sản phẩm cho khách hàng tiếp cận thông qua Internet.

- Tăng khả năng tương tác giữa doanh nghiệp và khách hàng như tư vấn khách hàng, lấy ý kiến đánh giá, phản hồi về dịch vụ sản phẩm.

- Tăng độ uy tín cho doanh nghiệp, thu hút thêm lượng khách hàng tiềm năng.

*** Về mức độ bảo mật**

Website của các doanh nghiệp vừa và nhỏ (các website thương mại điện tử, các diễn đàn, mạng xã hội nhỏ…) thường lưu trữ, hiển thị những thông tin của khách hàng như thông tin cá nhân, thông tin thanh toán, hình ảnh cá nhân. Những thông tin này đều mang tích chất nhạy cảm, do đó cần mức độ bảo mật cao.

*** Về hệ thống**

- Sử dụng phần cứng server web yếu, không thiết kế hệ thống phòng thủ, dễ dàng bị tấn công DDoS.

- Không có đội quản trị viên cho website, thường thì chỉ một hay vài người đảm nhận nhiệm vụ làm nội dung dùng chung tài khoản.

- Không sử dụng chứng chỉ SSL, HTTPS.

- Không bảo vệ giao diện quản trị viên.

- Sử dụng những plugin cũ, có nhiều lỗ hổng trong bảo mật.

- Tài khoản và mật khẩu truy cập quyền quản trị viên dễ đoán.

- Không sao lưu dữ liệu website thường xuyên.

3.2. Tiêu chí đánh giá độ bảo mật website của doanh nghiệp vừa và nhỏ

Có rất nhiều cách để hacker có thể tấn công một website, cũng chính vì vậy chúng ta có nhiều tiêu chí để đánh giá xem website đó có thật sự an toàn hay không.

Để thuận tiện cho việc đánh giá mức độ bảo mật website và đảm bảo tính hiệu quả, chính xác, học viên đã tổng hợp và lựa chọn một số tiêu chí phổ biến thường được sử dụng để đánh giá độ bảo mật của website, những tiêu chí này có thể dễ dàng đánh giá trực quan mức độ bảo mật của một website mà không cần phải xâm nhập quá sâu vào hệ thống. Cụ thể như sau:

*** Khả năng ngăn chặn spam**

Trong khi nội dung của một bài viết trên website rất tốt nhưng lại bị những kẻ xấu tấn công bằng cách gửi nhiều bình luận rác với nội dung không liên quan hoặc các đường link sang trang web khác. Không chỉ ở mục bình luận, nhiều website cho phép khách hàng gửi nội dung câu hỏi hoặc thắc mắc lên hệ thống, đây cũng là một nơi có thể gặp nguy cơ spam nội dung xấu.

Điều này vừa làm mất tính uy tín của website không chỉ đối với người dùng mà còn đối với trình đọc của google robots. Nguy hiểm hơn, các đường dẫn trong bình luận có thể dẫn đến những website độc hại mà bạn không thể kiểm soát.

Do vậy một website cần có cơ chế kiểm soát bình luận, đánh giá, gửi câu hỏi của người dùng, tránh tình trạng spam nội dung rác.

*** Khả năng chống tấn công DDoS**

Các cuộc tấn công DDoS hoạt động bằng cách tạo ra hàng loạt các truy vấn giả mạo tới trang web mục tiêu. Máy chủ nơi đặt website không đủ khả năng chịu tải sẽ ngừng hoạt động và đưa trang web về trạng thái ngoại tuyến. Nguy hiểm hơn có thể tạo ra các lỗ hổng bảo mật để hacker thực hiện những tấn công xâm nhập hoặc nhúng mã độc.

*** Khả năng chống tấn công Brute Force**

Brute Force là kiểu tấn công tương tự như DDoS nhưng mang tính tập trung hơn, đều cố gắng lặp đi lặp lại những truy vấn giả mạo lên máy chủ, nhưng kiểu

Brute Force mang mục đích bẻ khóa thông tin đăng nhập hoặc những dữ liệu nhạy cảm được mã hóa của website.

Có một số cách để giảm thiểu hoặc ngăn chặn những mối đe dọa như :

Thực hiện theo dõi User Agent trên các lần truy vấn gửi biểu mẫu và giám sát chúng để biết các lần thử lặp lại. Từ đó loại bỏ những truy cập vượt quá giới hạn cho phép.

Tăng độ phức tạp cho mật khẩu như sử dụng ký tự đặc biệt, không cho phép thay đổi mật khẩu đã trùng lặp, quản lý thông báo lỗi tốt hơn.

Sử dụng cơ chế chứng thực Basic Authentication hoặc Digest Authentication

*** Khả năng chống tấn công XSS**

Một trong những chiến thuật tấn công hay được tin tặc sử dụng đó là XSS, mục đích của tấn công này là làm hỏng giao diện trang web, lấy cắp thông tin từ cookie.

Bất kỳ biểu mẫu nhập thông tin nào trên trang web cũng không được phép chấp nhận thực thi mã nhúng như JavaScript. Nếu không thì ứng dụng web đó có thể dễ bị tấn công bởi XSS.

*** Khả năng chống tấn công SQL injection**

Đây là kiểu tấn công vô cùng phổ biến và ưa thích khác mà hacker thích sử dụng để truy cập vào cơ sở dữ liệu của trang web. Hầu hết các cơ sở dữ liệu máy chủ web được quản lý bởi SQL (Mysql, Oracle, MysqlServer, PostgreSql…). Tấn công này được thực hiện bằng cách nhúng các đoạn mã SQL vào biểu mẫu nhập thông tin, các thanh công cụ tìm kiếm trên trang web. Những đoạn mã độc này nếu không được tiền xử lý trước khi thực thi trên cơ sở dữ liệu sẽ mang đến rủi ro lớn như lộ thông tin nhạy cảm, thậm chí bị xóa dữ liệu.

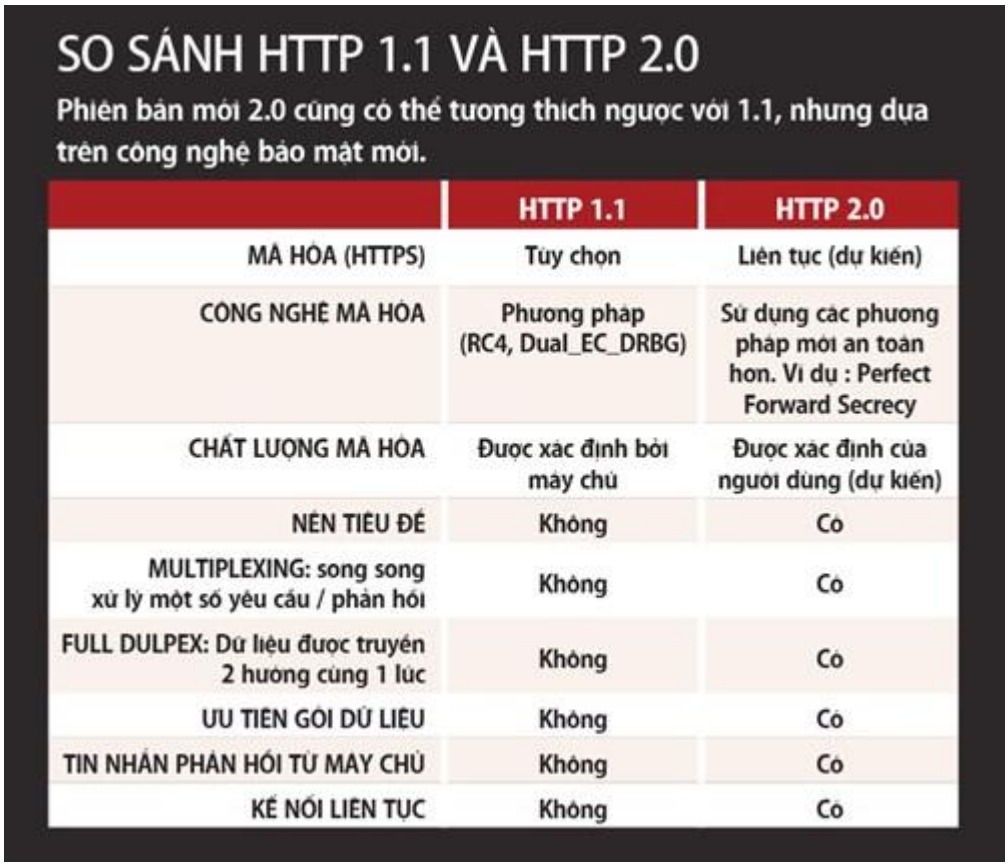
Để tránh tấn công SQL Injection, trang web phải ngăn chặn được việc nhúng mã SQL vào những biểu mẫu nhập thông tin hay thanh tìm kiếm trên toàn bộ website.

*** Trang web có chứng chỉ SSL hay không?**

Chứng chỉ SSL hay giao thức https cung cấp cho website một lớp bảo mật cực kỳ tốt. Nó ngăn chặn để lộ thông tin nhạy cảm của khách hàng như thông tin đăng nhập, thẻ tín dụng hoặc những thông tin khách hàng đã nhập vào biểu mẫu trên website.

*** Trang web có sử dụng HTTP/2 hay không?**

Khác với http/1.1 dùng dữ liệu dạng text với hiệu năng và tính bảo mật thấp, http/2 truyền dữ liệu dạng nhị phân kết hợp các phương thức mã hóa mới giúp tác vụ được thực hiện hiệu quả và tốn kém ít thời gian hơn [Hình 3.1].



Hình 3.1. So sánh HTTP 1.1 và HTTP 2.0

*** Khả năng chống tấn công lỗi chứng thực yếu (Insufficient Authentication)**

Một số trang web cho phép người dùng truy cập vào tài nguyên nhạy cảm mà không có đủ quyền. Cụ thể, một user không phải quyền quản trị nhưng vẫn truy cập được vào các thư mục lưu trữ dữ liệu quan trọng như hình ảnh khách hàng, thông tin thanh toán, tài liệu dự án...

Để đối phó, cần thực hiện thiết lập cơ chế điều khiển truy cập thông qua các bộ lọc như .htaccess, nginx.conf (Nginx) hay httpd.conf (Apache)

*** Khả năng chống tấn công liệt kê thư mục (Directory Indexing)**

Đây là chức năng của máy chủ cho phép liệt kê tất cả nội dung bên trong một thư mục mà không có tập tin cơ sở (index.html/ home.html/ default.html). Trong các thư mục đó có thể chứa nội dung quan trọng: tập tin cơ sở dữ liệu dự phòng, tập tin cấu hình, tập tin lưu trữ tạm thời, các kịch bản…

Biện pháp đối phó với dạng tấn công này tương tự với tấn công lỗi chứng thực yếu, cần phải thiết lập quyền truy cập vào các thư mục trên máy chủ. Hoặc chặn trực tiếp tính năng liệt kê thư mục trên máy chủ web.

*** Khả năng chống tấn công lỗ hổng tải lên tệp tin thực thi.**

Hacker có thể khai thác lỗ hổng trong tính năng tải tập tin lên trên website để đẩy các tập tin chứa mã độc, tập tin thực thi lên máy chủ. Sau đó khống chế máy chủ bằng cách thực thi các tập tin vừa được tải lên. Những tập tin mã độc này được gọi là WebShell, thường được viết bằng ngôn ngữ lập trình chung với trang web đó. Chỉ cần tin tặc có thể tải được các tệp tin WebShell này lên hệ thống của trang web mục tiêu thì xem như tin tặc đã có toàn quyền kiểm soát website đó, cho dù không biết tài khoản và mật khẩu của máy chủ này là gì.

*** Khả năng sao lưu dữ liệu**

Không một trang web nào đảm bảo 100% an toàn trước những tấn công của tin tặc. Cũng chính vì lý do đó, dữ liệu của một website hay ứng dụng web cần được sao lưu thường xuyên trong suốt quá trình hoạt động.

Những dữ liệu cần backup bao gồm: cơ sở dữ liệu, dữ liệu ảnh, tập tin dữ liệu văn bản, mã nguồn. Quan trọng hơn nữa là nên tạo một cơ chế tự động sao lưu, cơ chế này cho phép hệ thống tự động sao lưu dữ liệu theo lịch và lưu trữ ở một nơi an toàn.

3.3. Đánh giá mức độ bảo mật website của Sở Thông tin và Truyền thông Hà Nội

3.3.1. Sở Thông tin và Truyền thông Hà Nội và hệ thống website

Sở Thông tin và Truyền thông thành phố Hà Nội (sau đây gọi tắt là Sở) là cơ quan chuyên môn thuộc Ủy ban nhân dân Thành phố có chức năng tham mưu, giúp

Ủy ban nhân dân Thành phố quản lý nhà nước về: báo chí; xuất bản; bưu chính; viễn thông; tần số vô tuyến điện; công nghệ thông tin; điện tử; phát thanh và truyền hình; thông tin đối ngoại; bản tin thông tấn; thông tin cơ sở; hạ tầng thông tin truyền thông; quảng cáo trên báo chí, trên môi trường mạng, trên xuất bản phẩm và quảng cáo tích hợp trên các sản phẩm, dịch vụ bưu chính, viên thông, công nghệ thông tin.

Sở chịu sự chỉ đạo, quản lý về tổ chức, biên chế và công tác của Ủy ban nhân dân Thành phố, đồng thời chịu sự chỉ đạo, kiểm tra, hướng dẫn về chuyên môn, nghiệp vụ của Bộ Thông tin và Truyền thông.

Cơ cấu tổ chức của Sở bao gồm Lãnh đạo Sở (Giám đốc và 03 Phó Giám đốc); 07 phòng, ban chuyên môn (Văn phòng Sở, Thanh tra Sở, Phòng Kế hoạch - Tài chính, Phòng Công nghệ thông tin, Phòng Báo chí - Xuất bản - Truyền thông, Phòng Bưu chính - Viễn thông và Phòng Thông tin điện tử); 03 đơn vị sự nghiệp trực thuộc Sở (Trung tâm dữ liệu nhà nước, Cổng Giao tiếp điện tử Hà Nội và Trung tâm Giao dịch công nghệ thông tin và truyền thông).

Là Sở ngành dẫn đầu toàn thành phố về mức độ ứng dụng công nghệ thông tin trong hoạt động quản lý nhà nước, Sở đang cung cấp 28 dịch vụ công trực tuyến mức độ 3 trên website của Sở tại địa chỉ https://sotttt.hanoi.gov.vn/, và tích hợp trên cổng dịch vụ công quốc gia. Ngoài ra, website của Sở có đặt đường dẫn trực tiếp đến cổng dịch vụ công của thành phố Hà Nội với tổng số 1828 thủ tục hành chính.

Với những đặc điểm website của doanh nghiệp vừa và nhỏ đã nêu ở mục 3.1, có thể nhận thấy một số điểm tương đồng với website của Sở Thông tin và Truyền thông Hà Nội. Cụ thể:

- Về chức năng: website của Sở cung cấp, cập nhật những thông tin về hoạt động của sở, những văn bản chỉ đạo liên quan của Thành phố, những thông tin này đều là thông tin nhạy cảm, nếu bị tin tặc tấn công làm sai lệch sẽ gây ra hậu quả vô cùng nghiêm trọng, đặc biệt trong tình hình diễn biến dịch bệnh Covid-19 phức tạp như hiện nay.

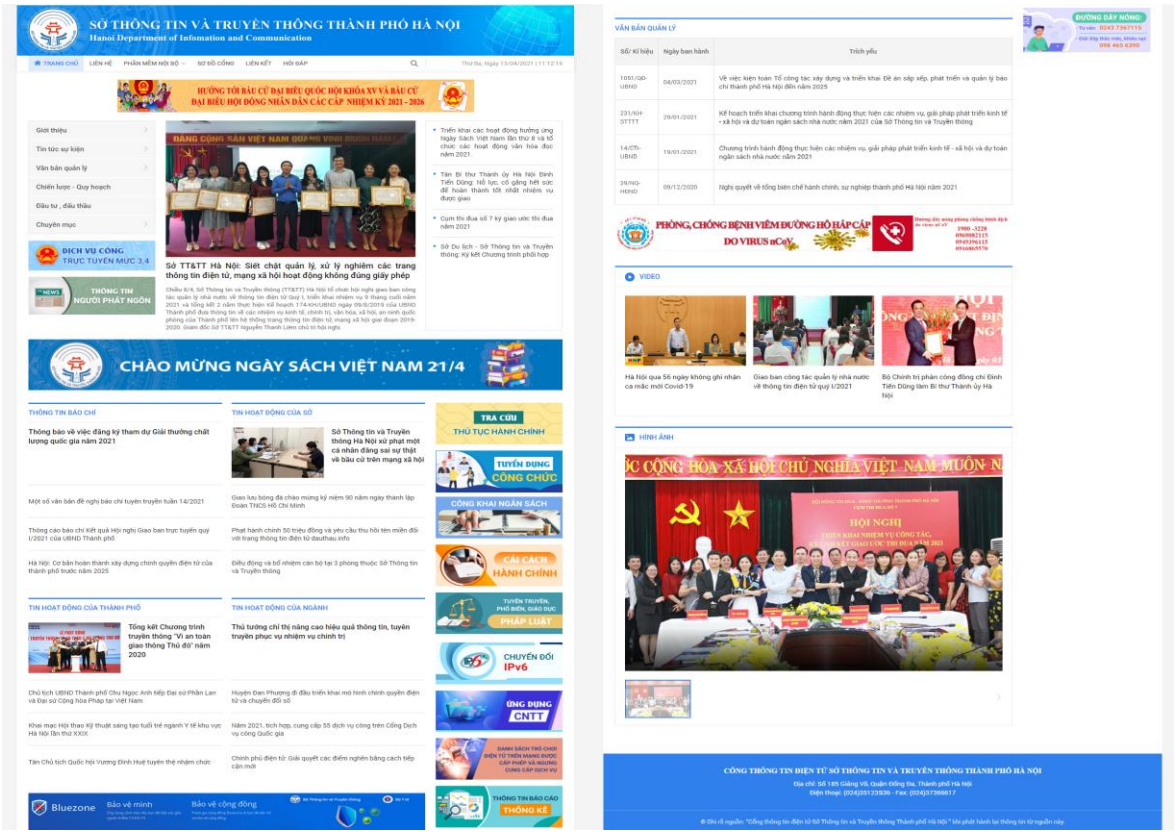
- Về mức độ bảo mật: website của doanh nghiệp vừa và nhỏ và website của Sở đều yêu cầu độ bảo mật cao do chứa đựng những thông tin nhạy cảm, quan trọng.

- Về hệ thống: Mặc dù website của Sở yêu cầu độ bảo mật cao nhưng hiện tại vẫn chưa được quan tâm đúng mực, chưa có đội ngũ quản trị riêng mà chỉ có một số ít nhân sự đảm nhận nhiệm vụ làm nội dung, thực hiện đăng tải những thông tin, văn bản đã được lãnh đạo phê duyệt.

Nhận thấy những điểm tương đồng nêu trên, học viên đã lựa chọn đánh giá mức độ bảo mật website của Sở để phù hợp với yêu cầu của đề tài nhưng vẫn có ý nghĩa thực tiễn, phục vụ cho công việc quản lý nhà nước của học viên tại Sở Thông tin và Truyền thông Hà Nội. [Hình 3.2] mô tả giao diện trang chủ của website của Sở Thông tin và Truyền thông Hà Nội.

3.3.2. Đánh giá mức độ bảo mật website của Sở Thông tin và Truyền thông Hà Nội

Về mặt giải pháp đảm bảo an toàn thông tin website, thì website của Sở Thông tin và Truyền thông Hà Nội cơ bản đã tuân theo các đề xuất như trong mục 2.5 (Trình bày ở Chương 2).



Hình 3.2. Giao diện trang chủ website Sở Thông tin và Truyền thông Hà Nội

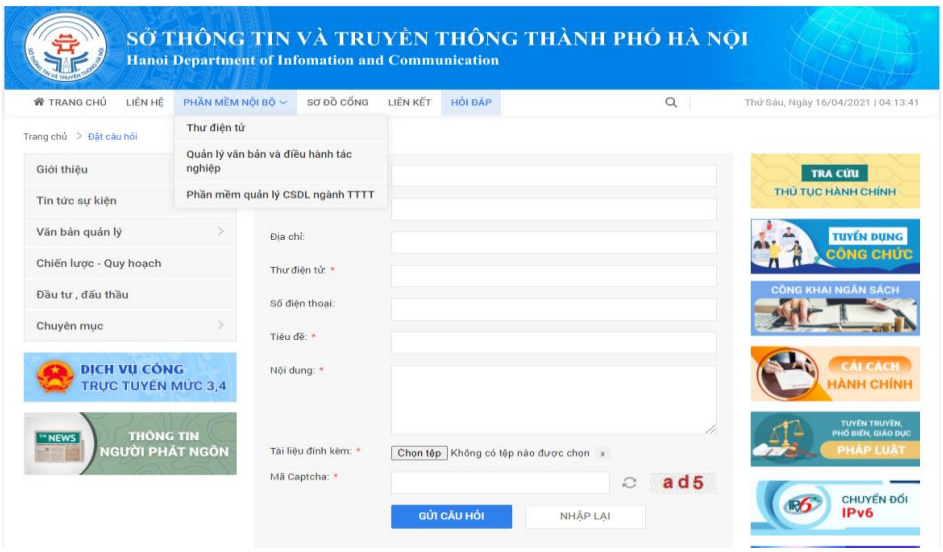
Cùng với những tiêu chí đã nêu ở mục 3.2, học viên tiến hành đánh giá mức độ bảo mật website của Sở Thông tin và Truyền thông Hà Nội. Cụ thể như sau:

*** Khả năng ngăn chặn spam**

Website của Sở hiện chỉ cung cấp một form cho phép người dùng nhập câu hỏi, góp ý ở địa chỉ : https://sotttt.hanoi.gov.vn/dat-cau-hoi.htm

Nội dung biểu mẫu nhập được kiểm tra các kiểu dữ liệu tương ứng, đồng thời khi gửi biểu mẫu cần phải điền mã captcha tự động sinh sau mỗi truy cập, nếu captcha không khớp sẽ không thể gửi biểu mẫu thông tin. Nội dung gửi lên hệ thống đều phải qua kiểm duyệt chứ không hiển thị lên danh sách câu hỏi trên giao diện trang web.

Đánh giá: Website đã có cơ chế chặn spam nội dung rác trong các biểu mẫu nhập thông tin người dùng.



*** Khả năng chống tấn công DDoS**

Máy chủ của website hiện đang dùng Nginx để phân tải cũng như điều hướng truy cập. Với Nginx có thể thực hiện được một số tác vụ nhằm hạn chế tấn công DDoS như:

Giới hạn tần suất gửi các truy cập từ một địa chỉ IP

Giới hạn số lượng truy cập từ 1 IP đến một địa chỉ bất kỳ trên website

Chặn một số IP nghi ngờ

Giới hạn số lượng kết nối đến máy chủ, nếu vượt quá số lượng truy cập sẽ từ chối yêu cầu.

Đánh giá: Website đã triển khai phân tải bằng Nginx, tránh được một phần rủi ro bị tấn công DDoS.

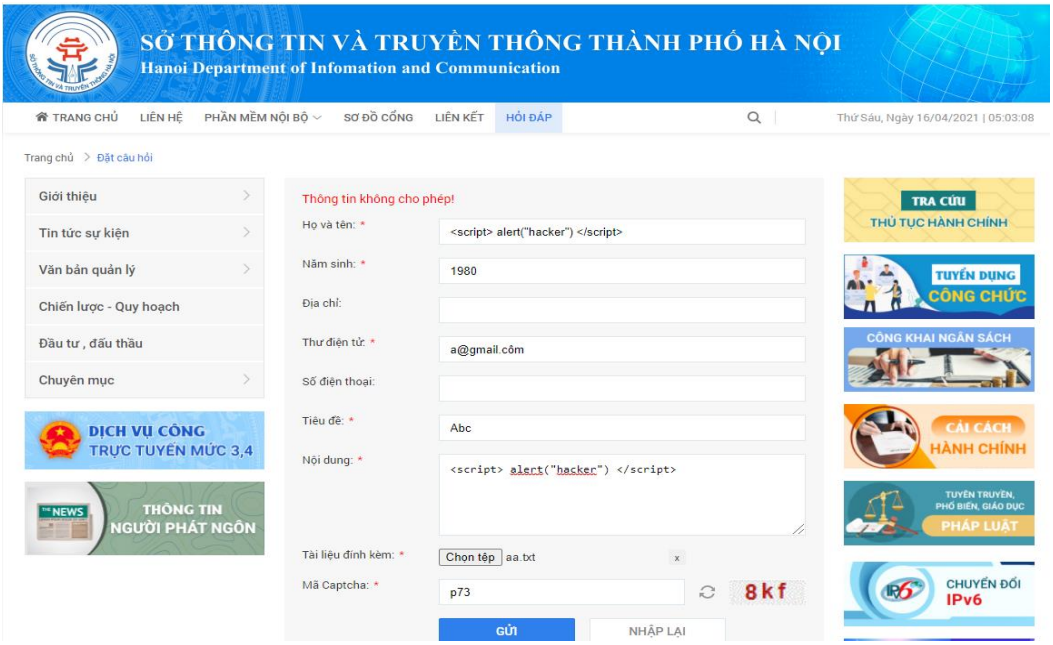
*** Khả năng chống tấn công Brute Force**

Website của Sở không cho phép khách vãng lai đăng ký hay đăng nhập trên hệ thống. Đồng thời trang quản trị CMS cũng không công khai trên mạng internet, chỉ có thể truy vấn bằng mạng nội bộ.

Đánh giá: Website không có rủi ro bị tấn công BruteForce.

*** Khả năng chống tấn công XSS**

Tiến hành thử nhúng mã script vào biểu mẫu nhập thông tin của website là phần đặt câu hỏi. Hệ thống đã chặn không cho phép gửi các thông tin chứa đoạn mã thực thi.



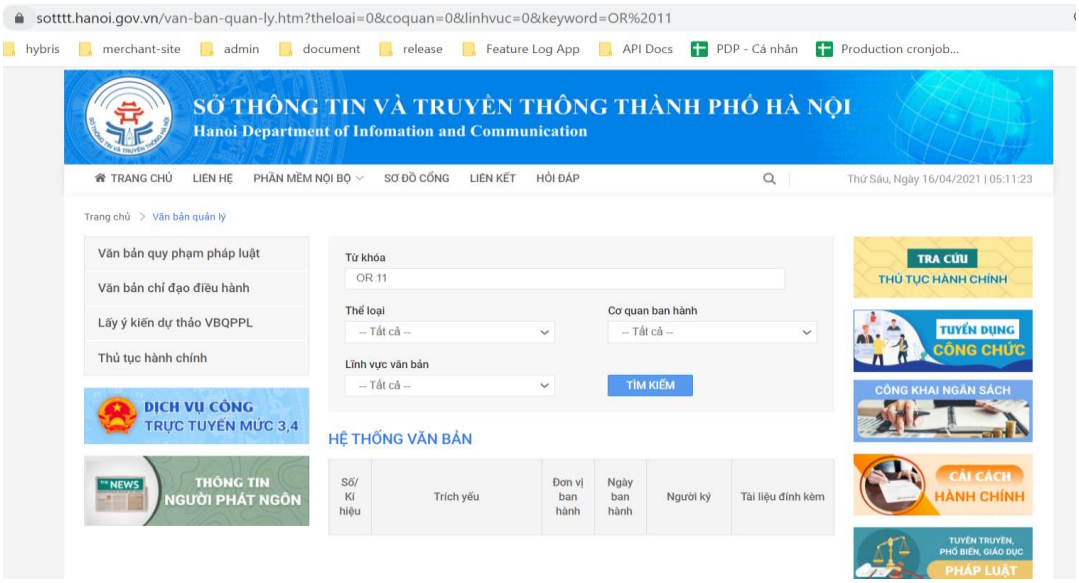
Đánh giá: Website có khả năng chống tấn công XSS

*** Khả năng chống tấn công SQL Injection**

Tại trang tìm kiếm văn bản trên website: https://sotttt.hanoi.gov.vn/van-ban-quan-ly.htm

Thực hiện nhập thông tin tìm kiếm vào trường Từ Khóa với nội dung nhằm tấn công SQL Injection : ‘OR 1=1’

Hệ thống tự động xóa những ký tự đặc biệt = và ‘’



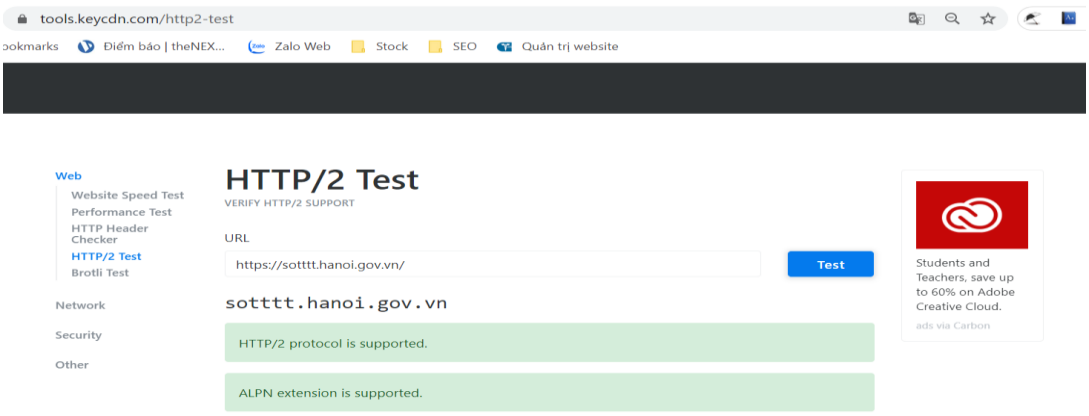
Đánh giá : Website đã có cơ chế ngăn chặn tấn công SQL Injection.

*** Chứng chỉ SSL**

Hiện tại website https://sotttt.hanoi.gov.vn/ đã có chứng chỉ SSL, nếu truy cập bằng giao thức http, hệ thống tự động chuyển hướng sang giao thức https thông qua Nginx.

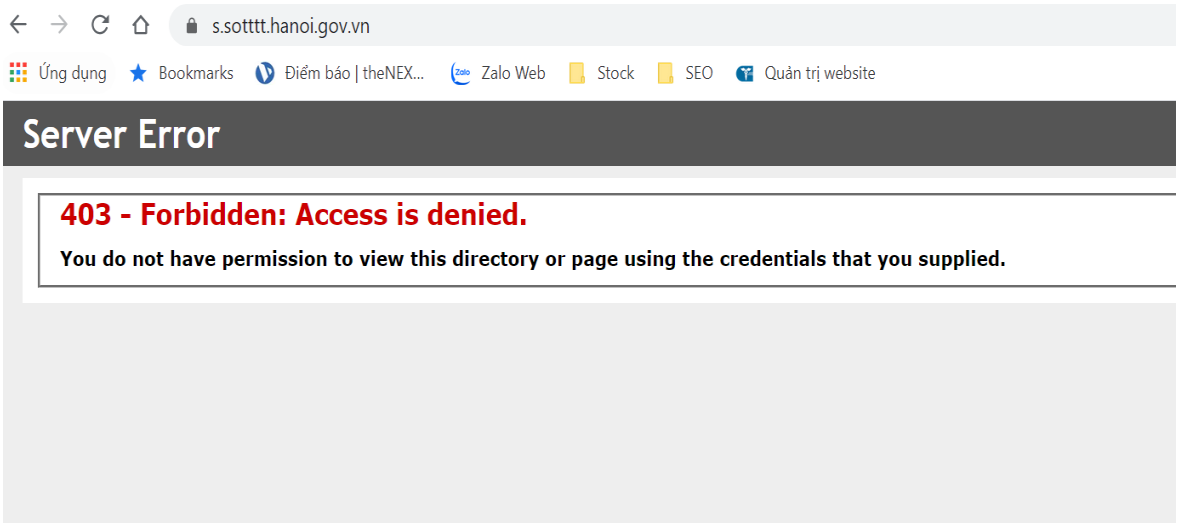
*** Giao thức Http/2.0**

Dùng công cụ kiểm tra trang web có hỗ trợ http/2.0 cho trang web, kết quả hiện tại website đã hỗ trợ giao thức http/2.0



*** Khả năng chống tấn công dựa vào lỗi chứng thực yếu**

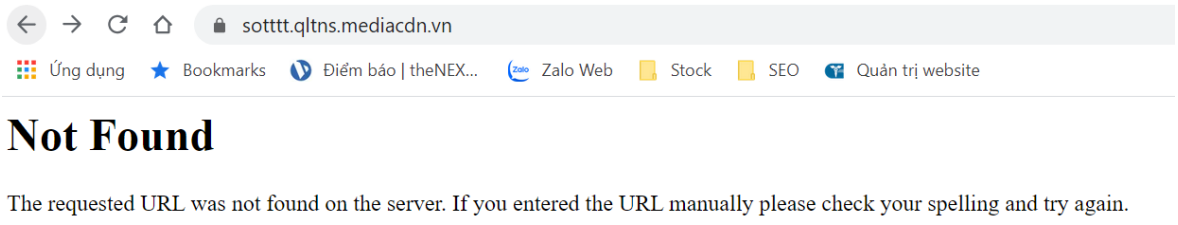
Thực hiện truy vấn vào địa chỉ bảo mật bằng quyền quản trị mà không có quyền này. Hệ thống báo lỗi 403 - Forbidden, như vậy website đã tránh được nguy cơ tấn công lỗi chứng thực yếu.



*** Khả năng chống tấn công liệt kê thư mục**

Thực hiện cố tình truy vấn vào tên miền chứa dữ liệu ảnh của website: https://sotttt.qltns.mediacdn.vn/

Hệ thống báo URL không tồn tại, như vậy không thể truy cập các thư mục chứa dữ liệu của website thông qua tấn công liệt kê thư mục.

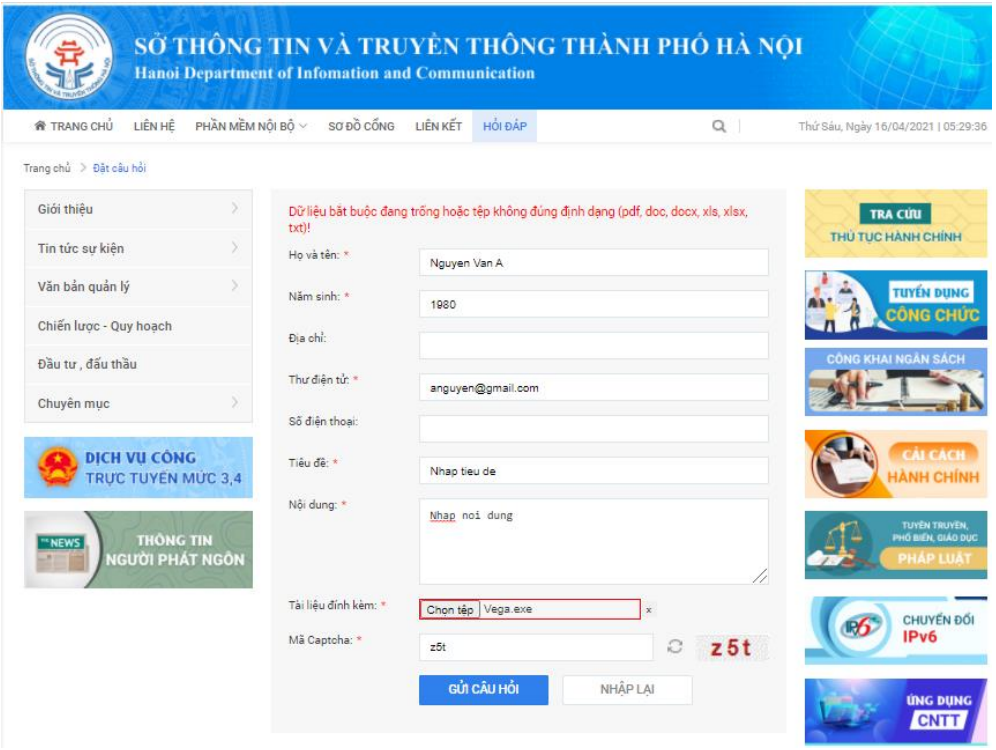


*** Khả năng chống tấn công tải lên tập tin thực thi**

Hiện website có duy nhất một form cho phép tải tập tin lên hệ thống là mục đặt câu hỏi tại địa chỉ : https://sotttt.hanoi.gov.vn/dat-cau-hoi.htm

Tại đây, hệ thống chỉ cho phép tải lên những tập tin dữ liệu định dạng văn bản bao gồm : pdf, doc, docx, xls, xlsx, txt

Thực hiện tải tập tin với định dạng thực thi là .exe, hệ thống báo lỗi không được phép tải lên.



Nhưng khi thực hiện đổi định dạng của tập tin thực thi từ .exe sang .txt (bản chất vẫn là tập tin thực thi của hệ điều hành window). Lúc này thực hiện tải lên, hệ thống vẫn cho tải lên thành công.

Đánh giá: Đây là lỗi khá nghiêm trọng, khi hệ thống chưa phát hiện được nội dung file có đúng theo yêu cầu hay không.

*** Sao lưu dữ liệu website**

Hiện nay website của Sở đang có các CronJob tự động sao lưu dữ liệu website theo lịch cố định.

3.4. Đề xuất một số giải pháp nâng cao bảo mật

Với những kết quả đánh giá theo các tiêu chí đã đưa ra, có thể thấy website https://sotttt.hanoi.gov.vn/ của Sở có độ bảo mật khá cao, có thể tránh được những rủi ro tấn công cơ bản nhất từ tin tặc. Bên cạnh đó vẫn có những vấn đề cần khắc phục hoặc tăng cường như khả năng chống tấn công DDoS hay khả năng ngăn chặn việc tải lên tập tin thực thi. Vì vậy, phần tiếp theo của luận văn

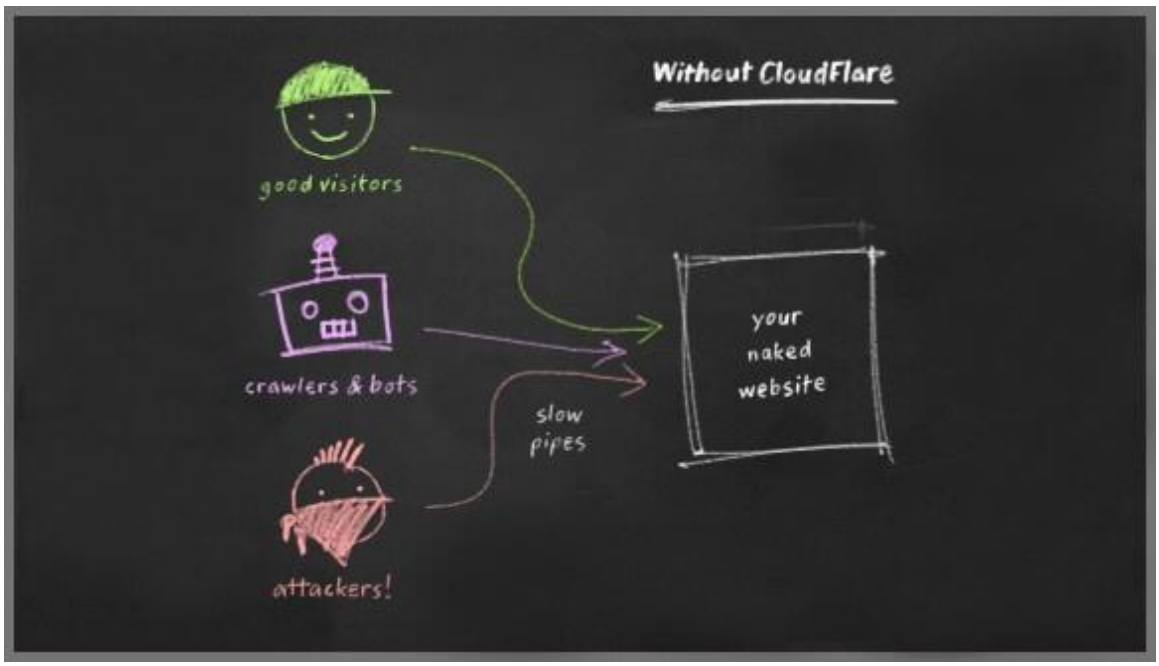
sẽ đề xuất một số giải pháp để nâng cao tính bảo mật và độ an toàn đối với website của Sở.

3.4.1. Sử dụng CloudFlare chống DDoS cho website

Hiện tại website của Sở chưa có cơ chế mạnh mẽ chống tấn công DDoS. Do đó có thể bổ sung một phương pháp hiệu quả hơn thay vì chỉ sử dụng phân tải bằng Nginx.

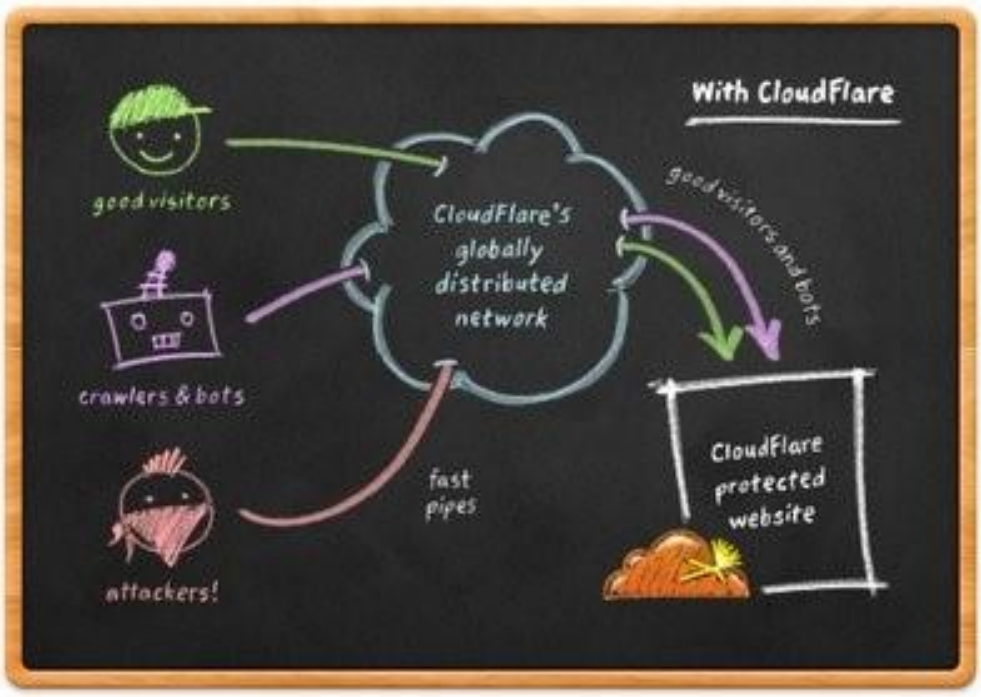
Một trong những cơ chế hiệu quả và đang được sử dụng thịnh hành đó là CloudFlare. Trước tiên CloudFlare là một dịch vụ CDN & DDNS kết hợp để gia tăng tốc độ & tính bảo mật cho website. Khi website sử dụng CloudFlare, mọi truy xuất đến website đó sẽ được định tuyến qua hệ thống thông minh của CloudFlare.

[Hình 3.3] và [Hình 3.4] dưới đây sẽ giúp hiểu hơn về cơ chế hoạt động của CloudFlare.



Hình 3.3 Hệ thống website không sử dụng CloudFlare

Website không sử dụng CloudFlare, mọi truy cập vào website đều là trực tiếp, bao gồm truy cập của khách, của các máy và cả những mối nguy cơ tấn công vào website.



Hình 3.4. Hệ thống website sử dụng CloudFlare

Trường hợp sử dụng CloudFlare thì mọi truy vấn đến website sẽ không còn là truy vấn trực tiếp nữa mà phải đi qua CloudFlare. Và chỉ những truy cập tin cậy mới có thể thông qua CloudFlare để đi đến website. Các truy vấn bị nghi ngờ như tấn công hệ thống của các tin tặc, spam bot, tấn công DDoS… sẽ bị ngăn chặn và loại bỏ.

Đồng thời website cũng được CloudFlare che dấu địa chỉ IP máy chủ web, cũng tránh được rủi ro tấn công DDoS.

Để sử dụng CloudFlare cho website, cần phải đăng ký tài khoản CloudFlare tại địa chỉ : https://dash.cloudflare.com/sign-up

Sau đó tiến hành thay đổi DNS hiện tại thành DNS của Cloudflare. Tất cả cấu hình chỉ cần thực hiện trên hệ thống CloudFlare, đều có hướng dẫn chi tiết đến từ nhà cung cấp.

3.4.2. Chống tấn công tải lên tập tin thực thi

Như tiêu chí đánh giá bảo mật - tấn công tải lên tập tin thực thi, website của Sở Thông tin và Truyền thông Hà Nội vẫn gặp lỗi có thể tải lên hệ thống tập tin có

định dạng văn bản nhưng thực chất là tập tin thực thi (chỉ cần đổi tên mở rộng của của tập tin).

Để ngăn chặn tải lên tập tin không đúng định dạng trong ngông ngữ lập trình PHP, ta cần thêm hàm kiểm tra dựa theo MimeType của tập tin. Cụ thể ta cần kiểm tra xem tập tin lên có đúng định dạng txt, doc, docs, pdf, xls, xlsx:

Tương ứng các MimeType sau :

text/plain
application/msword
application/vnd.openxmlformats officedocument.wordprocessingml.document
application/pdf
application/vnd.ms-excel
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet

Function kiểm tra MimeType của tập tin :

```
<?php
$mimetype = mime_content_type($_FILES['file']['tmp_name']);
if(in_array($mimetype, array(application/msword ', ' application/vnd.openxmlformats officedocument.wordprocessingml.document', ' application/pdf',' text/plain',' application/vnd.ms-excel',' application/vnd.openxmlformats-officedocument.spreadsheetml.sheet'))) {
  uploadFile();
  echo 'OK';
} else {
   echo 'Không đúng định dạng file!';
}
```

Như vậy với hàm kiểm tra này ta đã chặn được việc tải lên các tập tin dữ liệu với tên mở rộng là tập tin văn bản nhưng bản chất là các tập tin thực thi.

3.5. Kết luận Chương 3

Trong Chương 3, luận văn đã giới thiệu sơ lược về Sở Thông tin và Truyền thông Hà Nội và hệ thống website; khảo sát và đưa ra bộ tiêu chí đánh giá mức độ bảo mật website nói chung, thực hiện đánh giá thực tế mức độ bảo mật website của Sở. Từ đó đề xuất một số giải pháp để nâng cao tính bảo mật và độ an toàn đối với website của Sở.

KẾT LUẬN

Trước tình hình an ninh mạng ngày càng trở nên nóng bỏng với hàng loạt vụ tấn công nhắm vào website của các cơ quan nhà nước và doanh nghiệp, đặc biệt là các doanh nghiệp vừa và nhỏ với số lượng tăng lên theo từng năm và mức độ ngày càng tinh vi, phức tạp. Nhận ra tính cấp thiết, ý nghĩa khoa học và thực tiễn của vấn đề nghiên cứu các giải pháp bảo mật cho website, học viên đã chọn đề tài **"Nghiên cứu giải pháp bảo mật website cho các doanh nghiệp vừa và nhỏ"** cho luận văn tốt nghiệp trình độ đào tạo thạc sĩ, phù hợp với đặc thù công việc quản lý nhà nước tại Sở Thông tin và Truyền thông Hà Nội, nơi học viên đang công tác.

Học viên đã tìm tòi, nghiên cứu, tổng hợp thông tin từ nhiều nguồn tài liệu trong và ngoài nước, các diễn đàn về bảo mật thông tin, cũng như kinh nghiệm quản lý về an ninh thông tin của học viên để thực hiện các nội dung của luận văn. Mặc dù những nội dung về lý thuyết mà học viên tổng hợp được không phải là mới, nhưng nó rất có ý nghĩa đối với học viên, qua đó học viên đã được học hỏi, trau dồi kiến thức cho bản thân, tạo tiền đề giúp cho học viên thực hiện những mục tiêu cao hơn trong tương lai. Cùng với sự hướng dẫn tận tình của thầy giáo hướng dẫn, luận văn đã đạt được một số kết quả sau đây:

- Khảo sát thực trạng bảo mật website tại Việt Nam và trên thế giới, nghiên cứu tổng quan về bảo mật website, các tiêu chí phân loại website. Từ những kiến thức tổng hợp được, đưa ra tiêu chí mới để phân loại website, đó là ***phân loại website dựa trên mức độ bảo mật***.

- Nghiên cứu 04 nhóm giải pháp đảm bảo an toàn thông tin cho website, bao gồm: triển khai hệ thống phòng thủ, thiết lập và cấu hình hệ thống máy chủ an toàn, vận hành an toàn và phòng chống tấn công từ chối dịch vụ. Trong đó, tập trung đi sâu vào các giải pháp phòng chống tấn công từ chối dịch vụ. Đề xuất ứng dụng các giải pháp để đảm bảo anh toàn thông tin website cho các doanh nghiệp vừa và nhỏ phù hợp với thực tế, đảm bảo an toàn và tiết kiệm kinh phí.

- Giới thiệu sơ lược về Sở Thông tin và Truyền thông Hà Nội và hệ thống website, khảo sát và tổng hợp ra bộ tiêu chí đánh giá mức độ bảo mật website nói chung, thực hiện đánh giá thực tế mức độ bảo mật website của Sở Thông tin và Truyền thông Hà Nội. Từ đó đề xuất một số giải pháp để nâng cao tính bảo mật và độ an toàn đối với website của Sở.

Qua các kết quả đánh giá ban đầu cho thấy, website Sở Thông tin và Truyền thông Hà Nội có độ bảo mật khá cao, có thể tránh được những rủi ro tấn công cơ bản nhất từ tin tặc như: có khả năng chặn spam, chống tấn công Brute Force, XSS, SQL Injection, chống tấn công liệt kê thư mục, lỗi chứng thực yếu... Bên cạnh đó vẫn còn tồn tại những hạn chế như khả năng chống tấn công DDoS và chống tấn công tải lên tập tin thực thi chưa cao.

Để nâng cao tính bảo mật và độ an toàn website của Sở Thông tin và Truyền thông Hà Nội, khắc phục những tồn tại nêu trên, học viên đã đề xuất thực hiện 02 giải pháp. Trong đó, giải pháp sử dụng CloudFlare để chống tấn công DDoS cho website và giải pháp bổ sung thêm hàm kiểm tra trong ngôn ngữ lập trình PHP dựa theo MimeType của tập tin để kiểm tra chính xác định dạng của tệp tin, ngăn chặn việc tải lên tệp tin thực thi.

Trong thời gian tới, học viên sẽ làm việc với đội ngũ quản trị website của Sở Thông tin và Truyền thông Hà Nội để đề xuất thực hiện các giải pháp nâng cao tính bảo mật nêu trên. Đồng thời, bản thân học viên sẽ tiếp tục nghiên cứu sâu hơn lĩnh vực an toàn thông tin nói chung và bảo mật website nói riêng, nhằm phục vụ cho những nhiệm vụ khác của Sở Thông tin và Truyền thông Hà Nội và cho công việc kiểm tra, rà soát, xử lý vi phạm trên môi trường mạng mà học viên đang phụ trách.

DANH MỤC TÀI LIỆU THAM KHẢO

Tiếng Việt

[1] TS. Hoàng Xuân Dậu (2017) - "Bài giảng an toàn ứng dụng web và cơ sở dữ liệu", Học viện Công nghệ Bưu chính Viễn thông.

[2] ThS. Lê Phúc (2010) - "Bài giảng an toàn và bảo mật hệ thống thông tin", Học viện Công nghệ Bưu chính Viễn thông.

Tiếng Anh

[3] JEONG, G. et al, "Generic unpacking using entropy analysis", Malicious and Unwanted Software (MALWARE), 2010 5th International Conference on.

[4] I. Ahrmad, A.B. Abdullah, A.S. Alghamdi (2009) - "Application of Artificial Neural Netword in Detection ò Probing Attacks", IEEE, ISEA 2009.

Trang Web

[5] https://phuongnamvina.com/

[6] https://thietkewebso.com/

[7] http://bkav.com.vn/

[8] http://vncert.gov.vn

[9] http://antoanthongtin.vn/

[10] https://vi.wikipedia.org/

[11] https://quantrimang.com/

[12] https://wiki.matbao.net/

[13] https://resources.cystack.net/

[14] https://vncloud.vn/

[15] https://bizflycloud.vn/

[16] https://www.vietnamplus.vn/

[17] https://vietnamnet.vn/

[18] https://sotttt.hanoi.gov.vn/

[19] https://owasp.org/

[20] https://securitybox.vn/

[21] https://securitydaily.net/

[22] https://www.pfsense.org/

[23] https://www.snort.org/

[24] https://www.noron.vn/

BẢN CAM ĐOAN

Tôi cam đoan đã thực hiện việc kiểm tra mức độ tương đồng nội dung luận văn qua phần mềm DoIT một cách trung thực và đạt kết quả mức độ tương đồng 18% toàn bộ nội dung luận văn. Bản luận văn kiểm tra qua phần mềm là bản cứng luận văn đã nộp để bảo vệ trước hội đồng. Nếu sai tôi xin chịu các hình thức kỷ luật theo quy định hiện hành của Học viện.

Hà Nội, ngày ..... tháng ..... năm 2021

HỌC VIÊN CAO HỌC

Nguyễn Xuân Giang

Hệ thống hỗ trợ nâng cao chất lượng tài liệu

KẾT QUẢ KIỂM TRA TRÙNG LẶP TÀI LIỆU

THÔNG TIN TÀI LIỆU

Tác giả	Nguyễn Xuân Giang
Tên tài liệu	NGHIÊN CỨU GIẢI PHÁP BẢO MẬT WEBSITE CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ
Thời gian kiểm tra	18-05-2021, 00:45:02
Thời gian tạo báo cáo	18-05-2021, 01:10:19

KẾT QUẢ KIỂM TRA TRÙNG LẶP

Điểm	18
Nguồn trùng lặp tiêu biểu	[text.123doc.org, thuvienphapluat.vn, 123doc.org]

HỌC VIÊN **NGƯỜI HƯỚNG DẪN KHOA HỌC**

NGUYỄN XUÂN GIANG **PGS. TS. LÊ HỮU LẬP**