

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



ĐÀO HƯƠNG GIANG

**PHƯƠNG PHÁP THU THẬP, PHÂN LOẠI VÀ ĐÁNH GIÁ ĐIỂM
YẾU AN TOÀN THÔNG TIN CỦA CÔNG THÔNG TIN ĐIỆN TỬ.**

CHUYÊN NGÀNH : HỆ THỐNG THÔNG TIN

MÃ SỐ: 60.48.01.04

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TSKH HOÀNG ĐĂNG HẢI

HÀ NỘI - 2016

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: PGS.TSKH Hoàng Đăng Hải

Phản biện 1:

Phản biện 2:

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại
Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: ... giờ ngày tháng năm

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

MỞ ĐẦU

Những năm gần đây đã xảy ra hàng loạt các cuộc tấn công Cổng TTĐT trên toàn thế giới, từ việc thay đổi thông tin, hình ảnh đến việc làm sập các trang mạng. Việc tấn công một Cổng TTĐT đã trở nên khá dễ dàng với những kẻ tấn công, trong khi việc phát hiện, phòng ngừa, ngăn chặn từ phía quản trị mạng, quản trị Cổng TTĐT còn lỏng lẻo, nhất là đối với các cơ quan, tổ chức Nhà nước.

Hầu hết các cơ quan, tổ chức Nhà nước đều đã xây dựng Cổng TTĐT. Cổng thông tin này thực chất như một giao diện Web duy nhất của cơ quan, tổ chức phục vụ cho việc tra cứu thông tin, gửi nhận email, điều hành tác nghiệp nội bộ... của tổ chức thông qua mạng máy tính. Nói một cách khác, Cổng TTĐT là một trang web, xuất phát từ đó người sử dụng có thể dễ dàng truy xuất đến các trang web nội bộ và các dịch vụ thông tin khác của cơ quan, tổ chức trên mạng máy tính.

Thực tế cho thấy việc bảo mật Cổng TTĐT ở các cơ quan chính phủ hiện nay đang còn tồn tại những yếu kém, vấn đề an toàn bảo mật chưa được quan tâm đúng mức. Có thể thấy có rất nhiều lý do khiến cho tình trạng bảo mật thông tin còn yếu kém ở Việt Nam nói chung và ở các tổ chức/ cơ quan nhà nước nói riêng. Dưới đây là một số lý 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 Cổng TTĐT, chưa coi trọng đến việc phát hiện và phòng ngừa điểm yếu của cổng

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

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

Việc đánh giá điểm yếu của Cổng TTĐT sẽ giúp các đơn vị có thể hiểu được mức độ an toàn của Cổng TTĐT của mình, nhận thấy tầm quan trọng của việc phải đảm bảo an toàn thông tin cho Cổng TTĐT từ đó các dữ liệu quan trọng mới có thể được an toàn. Qua đó, đơn vị sẽ có ý thức hơn trong việc đảm bảo ATTT cho Cổng, tăng cường các biện pháp an ninh và khả năng của đội ngũ quản trị viên. Hiện nay, các quốc gia phát triển trên thế giới đều đã ý thức được vấn đề này, và ngày càng đầu tư vào việc đánh giá mức độ an toàn của

Cổng TTĐT. Tuy vậy, thì hầu hết các doanh nghiệp, cơ quan, tổ chức tại Việt Nam chưa có các biện pháp đánh giá điểm yếu Cổng TTĐT hoặc có nhưng mà chưa đầy đủ.

Để đánh giá được điểm yếu Cổng TTĐT, việc trước tiên là cần thu thập thông tin. Những khó khăn đặt ra là: thu thập thông tin gì, thu thập bằng cách nào, các bước thu thập như thế nào, sử dụng công cụ nào là tốt nhất... để có thể thu thập được thông tin nhiều nhất.

Sau khi thu thập được thông tin, việc tiếp theo là phân loại thông tin về điểm yếu. Việc phân loại cũng cần phải được thực hiện và xem xét một cách có hệ thống. Đây cũng chính là khó khăn tiếp theo của người thực hiện. Hiện tại, chưa có một bộ tài liệu hay hướng dẫn chuẩn nào về việc phân loại thông tin điểm yếu dành cho Cổng TTĐT. Chính vì vậy, một nhu cầu thực tế đặt ra là cần có phương pháp thu thập và phân loại điểm yếu phù hợp cho Cổng TTĐT

Trên cơ sở thông tin đã thu thập và phân loại thông tin về điểm yếu, việc tiếp theo là đánh giá điểm yếu ATTT cho Cổng TTĐT dựa theo các tiêu chí đánh giá. Các tổ chức tiêu chuẩn thế giới đã đưa ra một số bộ tiêu chí chung cho đánh giá ATTT như: ISO/IEC 15408, bộ tiêu chí OSWAP cho ứng dụng Web, các bộ tiêu chí của một số quốc gia tự xây dựng khác. Tuy nhiên, qua nghiên cứu tìm hiểu, học viện chưa thấy có đề xuất một bộ tiêu chí cụ thể nào cho đánh giá điểm yếu đối với Cổng TTĐT. Chính vì vậy, việc xây dựng một bộ tiêu chí để đánh giá điểm yếu Cổng TTĐT là hết sức cần thiết.

Chính vì những lý do trên, và nhận thấy việc cần thiết phải đảm bảo ATTT cho Cổng TTĐT, học viện chọn đề tài ***“Phương pháp thu thập, phân loại và đánh giá điểm yếu an toàn thông tin của cổng Thông tin điện tử”***

Các trọng tâm nghiên cứu đặt ra đối với luận văn là:

Thứ nhất: Nghiên cứu về cấu trúc Cổng TTĐT, vấn đề bảo mật Cổng TTĐT, các loại điểm yếu phổ biến trên các Cổng TTĐT

Thứ hai: Nghiên cứu, phân tích phương pháp thu thập, phân loại điểm yếu ATTT của Cổng TTĐT. Đưa ra phương pháp phù hợp để thu thập, phân loại điểm yếu ATTT.

Thứ ba: Nghiên cứu, phân tích một số mô hình, phương pháp, công cụ phần mềm cho thu thập thông tin, đánh giá điểm yếu ATTT của Cổng TTĐT. Xây dựng mô hình và các tiêu chí đánh giá điểm yếu phù hợp.

Thứ tư: Xây dựng một tập điểm yếu, tiêu chí đánh giá, các kịch bản thử nghiệm, các bài đo kiểm thử và thực hiện thử nghiệm đánh giá một Cổng TTĐT.

Phạm vi của bài luận văn: Nghiên cứu về các điểm yếu an toàn thông tin của Cổng TTĐT, phương pháp thu thập, phân loại điểm yếu và đánh giá điểm yếu an toàn thông tin của Cổng TTĐT, xây dựng các bài đo, kịch bản thử nghiệm đánh giá điểm yếu ATTT cho một Cổng TTĐT cụ thể.

Luận văn sử dụng các phương pháp nghiên cứu sau đây:

- Phương pháp nghiên cứu lý thuyết: tổng hợp, thu thập, nghiên cứu tài liệu về an toàn thông tin, các điểm yếu gây mất an toàn thông tin trên Cổng TTĐT hiện nay. Các phương pháp thu thập, phân loại và đánh giá điểm yếu phổ biến hiện nay trên thế giới và tại Việt Nam.
- Phương pháp thực nghiệm: Trên cơ sở lý thuyết đưa ra hệ thống các bài đo để đánh giá điểm yếu của Cổng TTĐT và áp dụng đánh giá cho một Cổng TTĐT thực tế tại Việt Nam hiện nay.

Nội dung của luận văn được trình bày trong các phần chính như sau:

Chương 1 trình bày phương pháp thu thập, phân loại điểm yếu an toàn thông tin của Cổng TTĐT

Chương 2 nghiên cứu, phân tích phương pháp đánh giá điểm yếu an toàn thông tin của Cổng TTĐT, một số công cụ phần mềm cho thu thập thông tin, đánh giá điểm yếu của Cổng TTĐT, xây dựng mô hình đánh giá, các tiêu chí đánh giá.

Chương 3 thực hiện thử nghiệm thu thập, phân loại và đánh giá điểm yếu an toàn thông tin của một Cổng TTĐT cụ thể. Kết quả cụ thể trong chương 3 là xây dựng được các kịch bản thử nghiệm, các bài đo kiểm thử điểm yếu ATTT cho Cổng TTĐT.

CHƯƠNG 1: PHƯƠNG PHÁP THU THẬP, PHÂN LOẠI ĐIỂM YẾU AN TOÀN THÔNG TIN CỦA CÔNG THÔNG TIN ĐIỆN TỬ

1.1 Khái quát về cấu trúc của Cổng TTĐT

1.1.1 Tổng quan về Cổng TTĐT

Cổng Thông tin điện tử (Cổng TTĐT) được hiểu như một trang web mà từ đó người sử dụng có thể dễ dàng truy xuất các trang web và các thông tin dịch vụ khác trên mạng máy tính. Cổng TTĐT khởi đầu thường dùng cho các trang web khổng lồ như Yahoo, Lycos,... Trong phạm vi của luận văn, khái niệm Cổng TTĐT được định nghĩa như sau: *Cổng Thông tin điện tử là điểm truy cập tập trung và duy nhất, tích hợp các kênh thông tin, các dịch vụ và ứng dụng, phân phối tới người sử dụng thông qua một phương thức thống nhất và đơn giản trên nền tảng Web.*

Các loại Cổng TTĐT:

- Cổng thông tin công cộng (public portals)
- Cổng thông tin doanh nghiệp (Enterprise portals)
- Cổng giao dịch điện tử (Marketplace portals)
- Cổng thông tin ứng dụng chuyên biệt (Specialized portals)

Các tính năng cơ bản của Cổng TTĐT: Khả năng cá nhân hóa, tích hợp nhiều loại thông tin, xuất bản thông tin, hỗ trợ nhiều môi trường hiển thị thông tin, khả năng đăng nhập một lần, quản trị Cổng TTĐT, quản trị người dùng

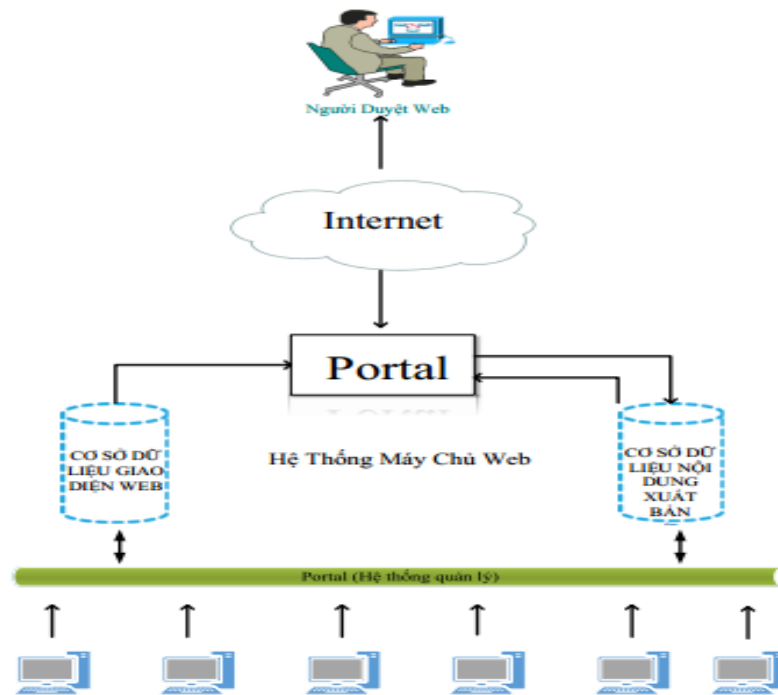


Hình 1- 1: Các tính năng cơ bản của Cổng TTĐT

1.1.2 Cấu trúc Cổng TTĐT

Cổng TTĐT được thiết kế đặc biệt dành cho các cơ quan, tổ chức, doanh nghiệp có nhu cầu phát triển hệ thống thông tin lớn trên môi trường web nhằm thực hiện các giao tiếp

trực tuyến và sử dụng Internet như một công cụ thiết yếu trong các hoạt động cung cấp thông tin, giao tiếp, quản lý và điều hành.



Hình 1- 2: Cấu trúc Cổng TTĐT

1.2 Tổng hợp dữ liệu về bảo mật của Cổng TTĐT, các loại điểm yếu

1.2.1 Tổng hợp dữ liệu về bảo mật của Cổng TTĐT

Thực trạng bảo mật Cổng TTĐT tại các cơ quan nhà nước năm 2015:

Theo báo cáo của VNCERT về thực trạng bảo mật 2015: có tới 90% cơ quan, tổ chức nhà nước phát lời cảnh báo về mức độ mất an toàn thông tin trên hệ thống Cổng TTĐT thuộc cơ quan mình. VNCERT đã gửi rất nhiều cảnh báo đến các cơ quan nhà nước nhưng chỉ một số ít đơn vị có phản hồi.

Chỉ riêng trong quý I/2015: có 365.644 lượt địa chỉ IP Việt Nam tham gia mạng Botnet, tức đã nhiễm mã độc và sẵn sàng tấn công DDOS đến bất kỳ máy tính nào trên thế giới. Trong các địa chỉ IP này, có 896 lượt địa chỉ IP là của các cơ quan nhà nước.

1.2.2 Các loại điểm yếu phổ biến hiện nay trên các Cổng TTĐT

Các loại lỗ hổng được phân làm 3 loại chính như sau:

Loại 1: Những lỗ hổng thuộc loại này cho phép kẻ tấn công thực hiện các hình thức tấn công DoS. Với mức độ nguy hiểm thấp, chỉ ảnh hưởng đến chất lượng dịch vụ, làm

ngưng trệ, gián đoạn hệ thống, không làm phá hỏng dữ liệu hoặc đạt được quyền truy cập bất hợp pháp.

Loại 2: Những lỗ hổng loại này thường cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần kiểm tra tính hợp lệ. Lỗ hổng này thường có trong các ứng dụng, dịch vụ trên hệ thống, có mức độ nguy hiểm trung bình. Thông thường những lỗ hổng này được lợi dụng bởi những người sử dụng trên hệ thống để đạt được quyền root không hợp lệ.

Loại 3: Những lỗ hổng thuộc dạng này cho phép người ngoài hệ thống có thể truy cập bất hợp pháp vào hệ thống, có thể phá hủy toàn bộ hệ thống. Loại lỗ hổng này có mức độ rất nguy hiểm đe dọa đến tính toàn vẹn và bảo mật thông tin của hệ thống. Các lỗ hổng này thường xuất hiện ở những hệ thống quản trị yếu kém hoặc không kiểm soát được cấu hình mạng.

Một số lỗ hổng phổ biến trên Cổng TTĐT:

- Lỗi tràn bộ đệm (B-O)
- Lỗi không kiểm tra đầu vào (U-I)
- Các vấn đề với điều khiển truy cập (A-C)
- Các vấn đề với xác thực, ủy quyền hay mật mã (A-A-C)

1.3 Một số phương pháp thu thập thông tin về điểm yếu

1.3.1 Phương pháp Footprinting

Footprinting là bước đầu tiên trong các bước chuẩn bị cho một cuộc tấn công mạng. Mục tiêu của phần Footprinting là thu thập càng nhiều thông tin về đối tượng thì càng tốt, điều này đồng nghĩa với việc thu thập được càng nhiều thông tin về điểm yếu thì càng tốt.

Mục đích của Footprinting thì cần phải thu thập được các thông tin sau: Domain name, IP Address, Website, Email Address.

1.3.2 Phương pháp Scanning

Scanning là phương pháp rà quét và phát hiện các nguy cơ về điểm yếu, lỗ hổng của đối tượng cần thu thập

Vai trò của scan mạng: Phát hiện Hosts Active trên mạng, Open Port, Application/services, OS, Vulnerability

1.4 Phương pháp phân loại thông tin về điểm yếu

Nhóm điểm yếu về sai sót trong nhập liệu (Injection; SQL injection, OS injection hay LDAP injection...)

Nhóm các điểm yếu về xác thực và quản lý phiên

Nhóm điểm yếu về kiểm duyệt nội dung đầu vào (Cross-Site Scripting (XSS))

Nhóm các điểm yếu phổ biến khác

Nhóm điểm yếu thuộc dạng Malware cổng thông tin

1.5 Kết luận chương 1

Trong chương này, luận văn đã cung cấp các kiến thức về tổng quan Cổng TTĐT (Định nghĩa, cấu trúc, tình hình thực tế hiện nay về Cổng TTĐT). Tổng hợp, thống kê các dữ liệu về công tác bảo mật của Cổng TTĐT. Đưa ra hai phương pháp chính trong việc thu thập thông tin về điểm yếu, dựa vào hai phương pháp đó xây dựng hai mô hình thu thập thông tin về điểm yếu phù hợp và từ đó đưa ra phương pháp phân loại thông tin về điểm yếu. Trong chương tiếp theo, luận văn sẽ đưa ra các phương pháp đánh giá, phân tích điểm yếu phù hợp với Cổng TTĐT hiện nay.

CHƯƠNG 2: PHƯƠNG PHÁP ĐÁNH GIÁ ĐIỂM YẾU AN TOÀN THÔNG TIN CỦA CÔNG THÔNG TIN ĐIỆN TỬ.

2.1. Nghiên cứu, phân tích một số mô hình đánh giá điểm yếu ATTT

2.1.1. Mô hình đánh giá điểm yếu ATTT theo OWASP

OWASP (The Open Web Application Security Project): dự án mở về bảo mật ứng dụng Web. OWASP là một tổ chức quốc tế và là một cộng đồng mở dành riêng cho các tổ chức dùng để tra cứu tài liệu, hiểu biết, phát triển, bổ xung, vận hành và duy trì các ứng dụng cần đến sự tin cậy.

OWASP bao gồm:

- Công cụ và các tiêu chuẩn về an toàn thông tin.
- Kiểm tra bảo mật ứng dụng, lập trình an toàn và các bài viết về kiểm định mã nguồn.
- Thư viện và các tiêu chuẩn điều khiển an ninh.
- Những nghiên cứu mới nhất về an toàn bảo mật.
- Chương trình miễn phí và chương trình mở cho bất cứ ai quan tâm trong việc nâng cao bảo mật ứng dụng.

Việc đánh giá ATTT theo chuẩn OWASP được xây dựng dựa trên OWASP TOP 10. Mục tiêu chính của OWASP Top 10 là để người lập trình, người thiết kế, kỹ sư và quản lý và cả tổ chức biết về hậu quả của những điểm yếu quan trọng nhất trong ứng dụng website. OWASP Top 10 cung cấp những kỹ năng cơ bản để bảo vệ website khỏi những mối nguy hại

2.1.2. Mô hình đánh giá điểm yếu ATTT tại các quốc gia trên thế giới

Mô hình đánh giá an toàn thông tin của Mỹ

Mô hình đánh giá an toàn thông tin của Pháp

Mô hình đánh giá an toàn thông tin của Anh

Mô hình đánh giá an toàn thông tin của Đức

Mô hình đánh giá an toàn thông tin của Hàn Quốc

2.2. Nghiên cứu phân tích một số phương pháp đánh giá điểm yếu ATTT của cổng TTĐT

Bảng 2-1: Bảng các tiêu chí, chỉ tiêu và phương pháp đánh giá mức độ an toàn bảo mật của các cổng TTĐT.

STT	Tiêu chí	Chỉ tiêu	Phương pháp
1	SQL Injection	<ul style="list-style-type: none"> - Chiếm quyền điều khiển Website, cơ sở dữ liệu của hệ thống - Giả mạo danh tính, sửa đổi, xóa trộn dữ liệu, thay đổi & phơi bày dữ liệu, ăn cắp, thêm xóa dữ liệu. - Upshell, Chiếm quyền điều khiển Máy chủ, Local attack 	Black-box
2	Blind SQL Injection	<ul style="list-style-type: none"> - Chiếm quyền điều khiển Website, cơ sở dữ liệu của hệ thống - Giả mạo danh tính, sửa đổi, xóa trộn dữ liệu, thay đổi & phơi bày dữ liệu, ăn cắp, thêm xóa dữ liệu. - Upshell, Chiếm quyền điều khiển Máy chủ, Local attack 	Black-box
3	CRLF	<ul style="list-style-type: none"> - Cross Site ScriPting vulnerabilities - Proxy and web server cache poisoning - Web site defacement - Hijacking the client's session - Client web browser poisoning 	Black-box
4	Htaccess Bypass	<ul style="list-style-type: none"> - Vượt qua việc xác thực người dùng trong cấu hình bảo vệ username và password bảo vệ tập 	Black-box

		tin trong .htaccess.	
5	Remote Commands execution	- Thực thi những câu lệnh có thể gây tổn hại cho hệ thống như xóa CSDL, người dùng xem được nội dung tập tin config, passwd	Black-box
6	XSS	<ul style="list-style-type: none"> - Ăn cắp cookies, mật khẩu, cướp phiên làm việc - Cài các loại virus, trojan, backdoor trên máy tính nạn nhân - Thay đổi giao diện Website. Tuy nhiên nó chỉ chạy trên trình duyệt phía máy khách và chỉ tấn công vào bề mặt Website, không làm thay đổi cấu trúc mã nguồn, cơ sở dữ liệu của Website trên Máy chủ. 	Black-box

Theo tài liệu về kiểm thử thâm nhập (penetration testing) sẽ có 3 phương pháp đánh giá an toàn bảo mật như sau:

Phương pháp Black-box

Phương pháp White-box

Phương pháp Grey-box

2.2.1. Phương pháp Black box

Phương pháp blackbox hay còn gọi là phương pháp kiểm thử hộp đen, phương pháp này người kiểm thử đóng vai trò như là một hacker thực thụ, đi tìm hiểu và tấn công (có giới hạn) vào hệ thống mạng hay Website đã định.

Các bước ở phương pháp này bao gồm:

Thứ nhất: Footprinting: Ở bước này hacker tìm hiểu các thông tin về Website và hệ thống để thu thập được càng nhiều thông tin càng tốt, hacker có thể sử dụng các công cụ sẵn có hoặc open source để thu thập thông tin.

Thứ hai: Scanning: Sau khi đã thu thập đầy đủ các thông tin cần thiết, hacker sẽ bắt đầu rà quét các port giao tiếp của Website và người dùng, nắm biết được các port đang mở, các giao dịch đang được thực hiện, các giao thức đang được sử dụng để duy trì và truyền tải lưu lượng của Website và các lỗi của Website.

Thứ ba Exploit: Là bước quan trọng để chứng minh được rằng lỗ hổng trên Website thu được từ các công cụ rà quét có thực sự gây ra những ảnh hưởng cho hệ thống hay mất mát dữ liệu hay ko.

Thứ tư Update patches: Ở bước này thông thường thì Người quản trị mới có quyền thực hiện, người kiểm thử có thể gửi các văn bản thông báo hướng dẫn hỗ trợ cho Người quản trị thực hiện

Thứ năm Report: Bước này bao gồm các báo cáo phân tích các tình huống, lỗ hổng được đặt ra và đã tìm được nếu được các mối nguy hiểm mà Website đang gặp phải, đưa ra các hình thức, biện pháp khắc phục, chi phí khắc phục cho phía khách hàng được biết.

2.2.2. Phương pháp White box

Là một phương pháp đánh giá được nhận định là đầy đủ và có tính tin cậy cao, ở phương pháp này người kiểm thử được xem như là một nhân viên thực thụ của công ty, nắm rõ một số vấn đề về mặt hệ thống, bố trí các máy chủ, nắm rõ được các port giao tiếp, các dịch vụ đang chạy trên Website.

Phương pháp này bao gồm các giai đoạn sau: Thu thập thông tin, kiểm tra cấu hình Web, kiểm tra bằng việc xác thực, kiểm tra quản lý phiên truy nhập, kiểm tra việc phân quyền, kiểm tra lỗ hổng dữ liệu.

2.3. Nghiên cứu, phân tích một số công cụ phần mềm cho thu thập thông tin, đánh giá điểm yếu/ lỗ hổng bảo mật của Cổng TTĐT

Công cụ Acunetix WVS

Công cụ OWASP WebScarab

Công cụ OWASP ZAP

Công cụ Burp Suite

Công cụ N-Stalker

Công cụ Sandcat

Công cụ Kali Linux

2.4. Xây dựng mô hình đánh giá, các tiêu chí đánh giá, đưa ra phương pháp đánh giá phù hợp với Cổng TTĐT

2.4.1. Mô hình đánh giá

Bị động – Passive mode.

Mục đích của giai đoạn này: Tester hiểu về application, sử dụng các dịch vụ, thành phần ứng dụng. Tools thường được sử dụng để thu thập thông tin. Ví dụ, proxy quan sát tất cả HTTP requests và HTTP response. Kết thúc giai đoạn này, tester cần hiểu được tất cả điểm vào (gates) của ứng dụng. (e.g., HTTP headers, parameters, and cookies). Module Information Gathering sẽ chỉ rõ làm thế nào để tiến hành passive mode test.

Chủ động – Active mode.

Trong giai đoạn này, tester sử dụng các phương pháp khác nhau với mục đích tìm ra những lỗ hổng trên hệ thống website. Có tất cả 9 chủ đề:

Configuration Management Testing – Kiểm tra quản lý, cấu hình hệ thống

Business Logic Testing - Đánh giá Business logic

Authentication Testing - Kiểm tra phần xác thực

Session Management Testing - Kiểm tra quản lý phiên giao dịch

Authorization testing – Kiểm tra quá trình cấp quyền

Data Validation Testing - Đánh giá các kiểm soát thẩm định dữ liệu

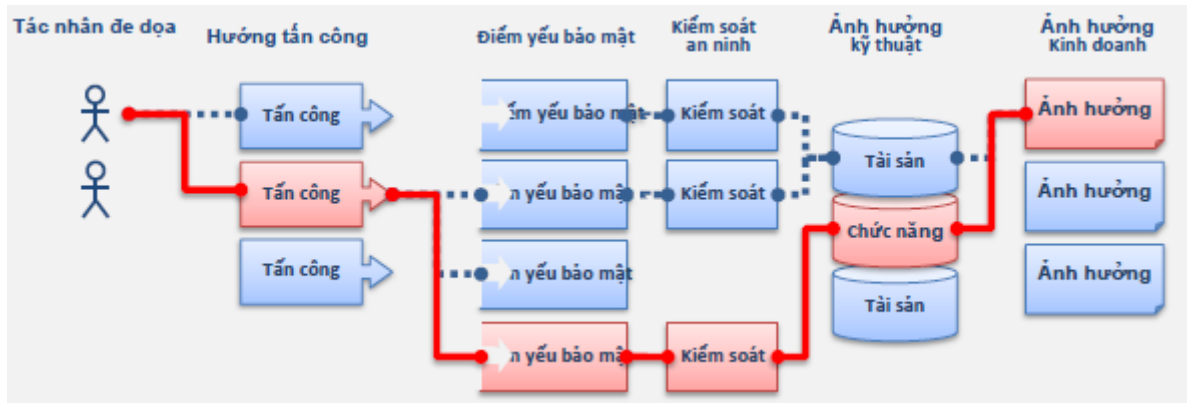
Denial of Service Testing - Tấn công từ chối dịch vụ

Web Services Testing – Đánh giá Webservices

Ajax Testing - Kiểm tra AJAX.

2.4.2. Các tiêu chí đánh giá

Việc xây dựng các tiêu chí đánh giá mức độ bảo mật cổng thông tin của các cơ quan nhà nước đồng nghĩa với việc đánh giá các mức độ rủi ro khi cổng thông tin bị các Hacker tấn công. Kẻ tấn công có thể lợi dụng nhiều con đường khác nhau thông qua ứng dụng công nghệ thông tin của tổ chức/ doanh nghiệp để làm tổn hại doanh nghiệp hay tổ chức đó. Mỗi con đường thể hiện một rủi ro khác nhau mà có thể có hoặc không gây ra sự chú ý. Thường thì những con đường này khá dễ để tìm ra và vận dụng để phá hoại, tuy nhiên cũng có những trường hợp rất phức tạp. Vì vậy, để có thể xác định những rủi ro cho tổ chức/ doanh nghiệp cần tính toán khả năng hiện hữu của mỗi nguy hiểm, những yếu tố tấn công và những điểm yếu bảo mật.



Hình 2- 1: Sơ đồ hướng tấn công và mức độ ảnh hưởng của các tác nhân

Theo OWASP Top 10, các mức độ rủi ro (hay tiêu chí) đánh giá mức độ bảo mật Cổng TTĐT được chia theo các mức sau:

Lỗi nhúng mã – Injection.

Phá hỏng cơ chế chứng thực và quản lý phiên làm việc – Broken Authentication and Session Management.

Thực thi mã Script xấu (XSS) – Cross-Site Scripting (XSS).

Đối tượng tham chiếu thiếu an toàn – Insecure Direct Object References

Sai sót trong cấu hình an ninh – Security Misconfiguration

Đề lộ những dữ liệu nhạy cảm – Sensitive Data Exposure

Thiếu chức năng cho điều khiển truy cập – Missing Function Level Access Control

Sai sót hạn chế truy cập – Cross – Site Request Forgery

Lợi dụng lỗ hổng biết trước – Using Components with Known Vulnerabilities

Chuyển hướng và chuyển tiếp thiếu thẩm tra – Unvalidated Redirects and Forwards

2.5. Kết luận chương 2

Trong chương này, luận văn đã đưa ra các mô hình đánh giá điểm yếu của các tổ chức, các quốc gia phát triển trên thế giới. Tập trung đi sâu vào nghiên cứu, phân tích hai phương pháp đánh giá điểm yếu phổ biến nhất hiện nay là Black box và White Box. Phân tích một số công cụ phần mềm cho thu thập thông tin điểm yếu. Từ đó, xây dựng mô hình đánh giá và đưa ra các tiêu chí đánh giá điểm yếu an toàn thông tin cho Cổng TTĐT. Tiếp theo chương 3, luận văn sẽ tiến hành thử nghiệm trên một Cổng TTĐT thực tế

CHƯƠNG 3: THỬ NGHIỆM THU THẬP, PHÂN LOẠI VÀ ĐÁNH GIÁ ĐIỂM YẾU AN TOÀN THÔNG TIN CỦA MỘT CỔNG TTĐT

3.1. Khái quát về các đặc trưng kỹ thuật của cổng TTĐT đánh giá

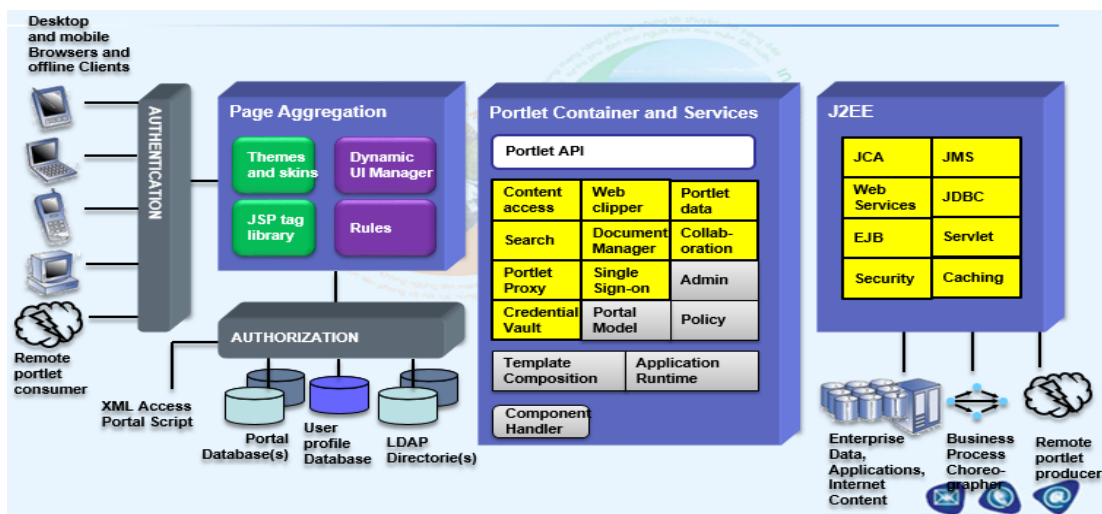
3.1.1. Giới thiệu về Cổng TTĐT

Cổng thông tin điện tử của Học viện Công nghệ Bưu chính Viễn thông, được truy cập từ địa chỉ <http://portal.ptit.edu.vn>. Cổng TTĐT được xây dựng với mục đích giúp Lãnh đạo Học viện có một công cụ để quản lý điều hành các hoạt động của Học viện trên môi trường hiện đại, linh hoạt.

Vì vậy, Cổng TTĐT của Học viện đã trở thành một điểm truy cập duy nhất của người dùng cuối (lãnh đạo Học viện, giảng viên, sinh viên, gia đình, các phòng ban, các khoa, khách,.....) mà tại đó, tất cả các yêu cầu của người dùng đều được đáp ứng về các khía cạnh: thông tin, con người, quy trình và ứng dụng.

Với tầm quan trọng của Cổng TTĐT đối với các hoạt động trong Học viện, vì vậy việc đảm bảo an toàn cho Cổng chính là nhiệm vụ chính của các cán bộ quản trị viên, vì lý do đó mà đề tài lựa chọn Cổng TTĐT làm đối tượng để tiến hành thu thập, phân loại và đánh giá điểm yếu ATTT.

3.1.2. Mô hình tổng quan



Hình 3- 1: Mô hình tổng quan xây dựng Cổng TTĐT

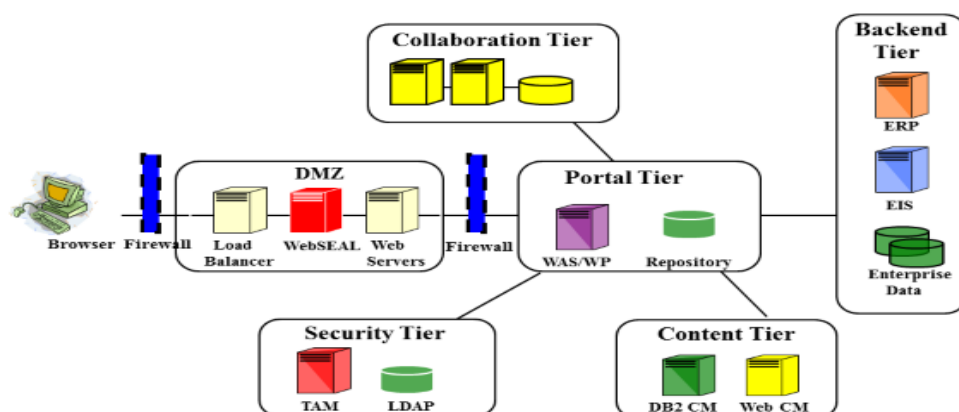
3.1.3. Kiến trúc hệ thống

Cổng TTĐT được xây dựng trên nền tảng của IBM WebSphere Portal sử dụng công nghệ J2EE phát triển cho Doanh nghiệp. Được hỗ trợ trên nền tảng công vụ mạnh, hệ thống Cổng thông tin được thiết kế và triển khai dựa trên mô hình đa tầng, phân lớp.

Cổng TTĐT Học viện tổng hợp một số tính năng cơ bản sau:

- Sử dụng cơ chế cập nhật một lần
- Hệ thống hỗ trợ chuẩn truyền thông bảo mật SSL
- Có các giải pháp chống tấn công DOS, DDOS khả dụng
- Có cơ chế phân tải và chịu lỗi
- Có nhật ký hệ thống

Mô hình kiến trúc:



Hình 3- 2: Mô hình kiến trúc xây dựng Cổng TTĐT

3.2. Xây dựng kịch bản thử nghiệm các bài kiểm thử

3.2.1. Kịch bản thử nghiệm:

Việc thử nghiệm được tiến hành theo các bước sau:

Bước 1: Sử dụng phương pháp rà quét: Black-box

Bước 2: Người dùng sử dụng công cụ rà quét từ một máy tính bất kỳ trên mạng Internet

Bước 3: Nhập vào URL của Cổng TTĐT Học viện CNBCVT hoặc Cổng TTĐT Bộ TTTT

Bước 4: Chọn module quét: Tất cả (quét tất cả các module mà công cụ cung cấp)

Bước 5: Đợi kết quả trả về

3.2.2. Các bài đo kiểm

Bài đo SQL Injection

Bài đo Blind SQL Injection

Bài đo CRLF

Bài đo Htaccess Bypass

Bài đo Remote Commands execution

Bài đo XSS

3.3. Các bước thử nghiệm

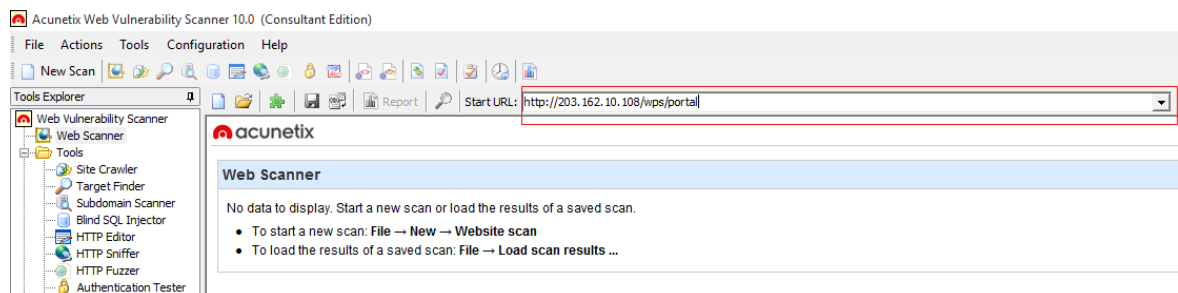
Để tiến hành thử nghiệm, luận văn lựa chọn công cụ rà quét từ xa, và đóng vai trò như một hacker, tiến hành rà quét theo mô hình black-box. Cổng TTĐT thử nghiệm:

<http://ptit.edu.vn> và công cụ sử dụng: Acunetix WVS.

Quy trình thực hiện thử nghiệm được tiến hành qua các bước sau:

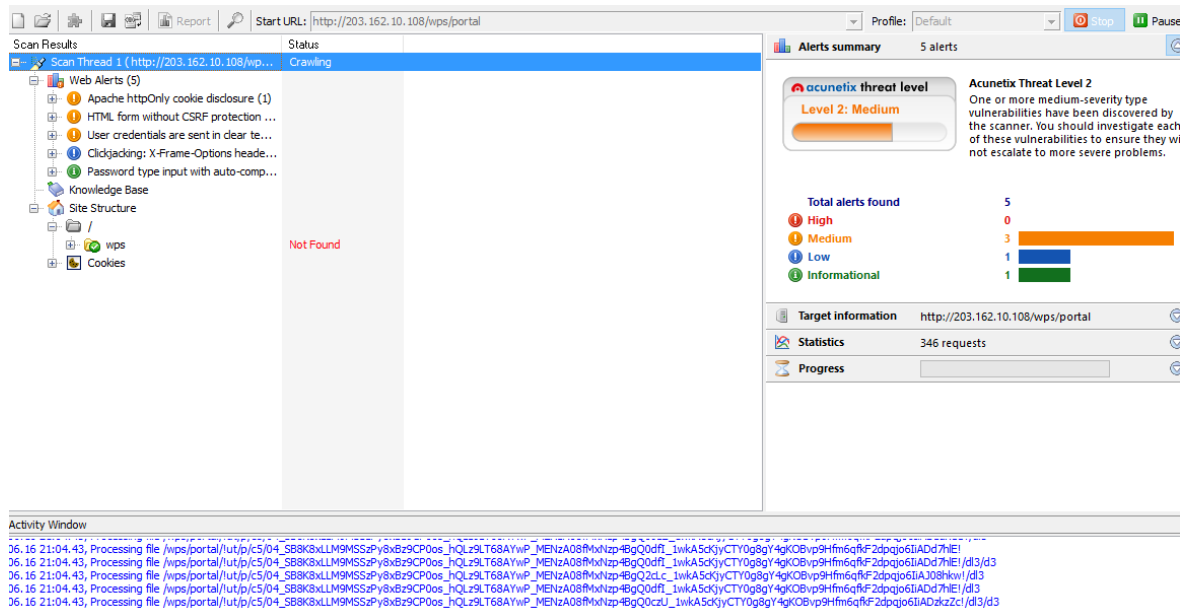
Bước 1: Cài đặt công cụ rà quét Acunetix WVS

Bước 2: Nhập địa chỉ IP/ đường link của cổng TTĐT



Hình 3- 3: Nhập địa chỉ IP của Cổng TTĐT Học viện để rà quét

Bước 3: Tiến hành rà quét và nhận kết quả

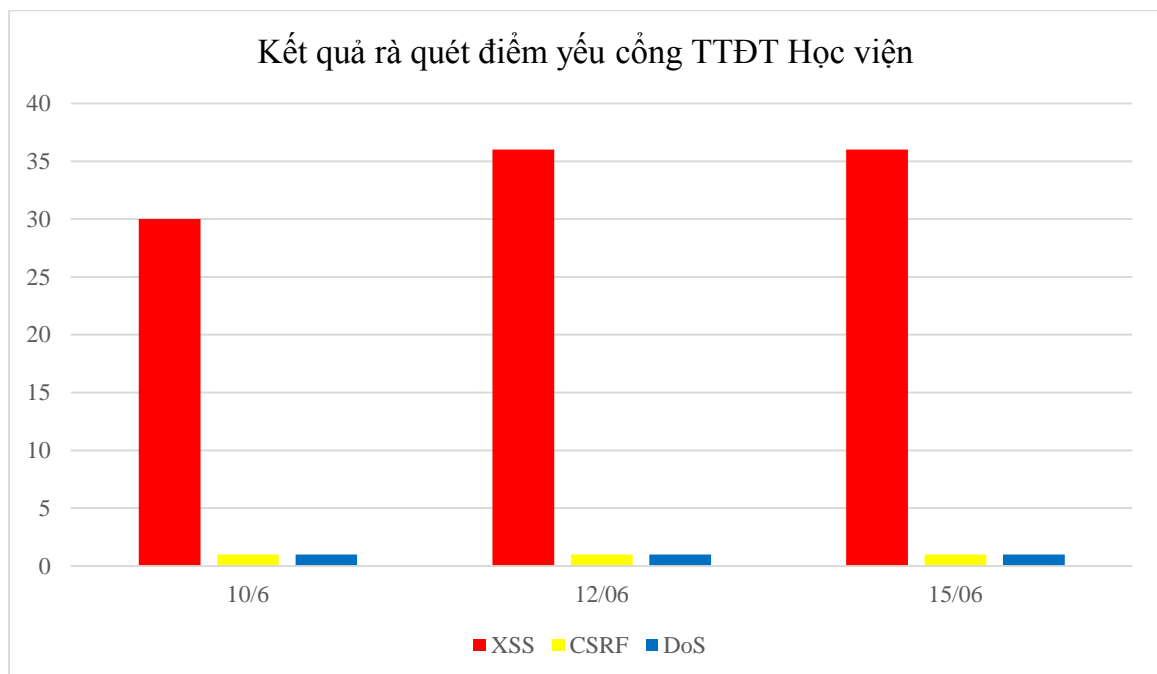


Hình 3- 4: Quá trình rà quét Cổng TTĐT

3.4. Đánh giá thử nghiệm:

3.4.1. Kết quả thử nghiệm

Sau khi tiến hành rà quét bằng công cụ Acunetix WVS tại các thời điểm khác nhau, kết quả thu được như sau:

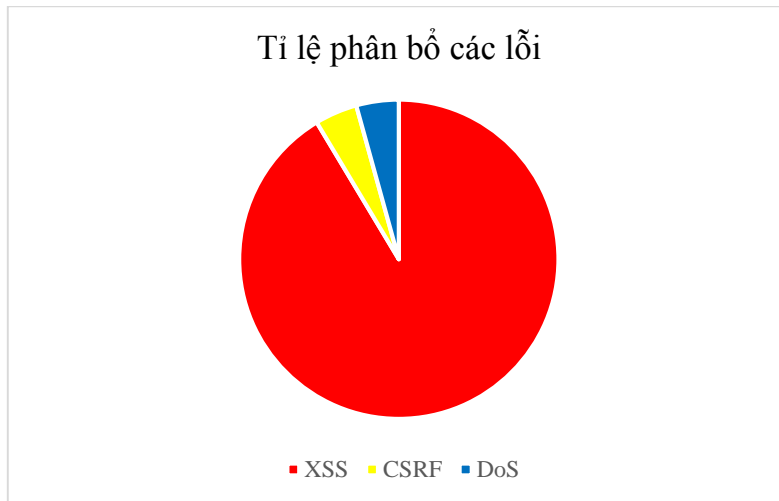


Hình 3- 5: Kết quả rà quét cổng TTĐT Học viện qua 3 lần quét

Kết quả qua 3 lần rà quét, tại các thời điểm khác nhau chúng ta có thể thấy điểm yếu thu được chủ yếu là thuộc nhóm điểm yếu về kiểm duyệt nội dung đầu vào, ngoài ra là các điểm yếu thuộc dạng CSRF và DoS.

3.4.2. Phân tích, đánh giá kết quả

Từ kết quả thu được, có thể thấy mức độ phân bố số lượng lỗi qua các lần rà quét là tương đương với nhau. Lỗi ở mức cao tập trung chủ yếu vào loại Cross site scripting (XSS)



Hình 3- 6: Tỉ lệ phân bố các lỗi rà quét

Có thể thấy, lỗi XSS chiếm đến hơn 90% tổng số lỗi quét được và đều thuộc dạng lỗi cao. Như đã trình bày ở những chương trước, XSS là nhóm lỗi thuộc dạng điểm yếu về kiểm duyệt nội dung đầu vào, là nhóm lỗi rất dễ bị tấn công và vô cùng nguy hiểm. Cách đơn giản nhất để khai thác lỗi này là chèn thêm ký tự vào chính đường link dẫn đến website. Vì vậy, cần phải có các biện pháp khắc phục và sửa lỗi này.

Một số cách cơ bản nhất để khắc phục và vá lỗi là:

- Không cho phép bất kỳ HTML tag nào nhập vào từ người dùng.
- Lọc tất cả các Active Script từ HTML code.

3.5. Kết luận chương 3

Ở chương 3, luận văn đã trình bày phương pháp thu thập các điểm yếu của cổng TTĐT dựa vào phương pháp Scanning, phân tích các điểm yếu theo phương pháp Black box và đánh giá điểm yếu dựa vào các tiêu chí đã trình bày ở những chương trước đó. Ngoài ra, chương 3 còn đưa ra được các bài đo kiểm thử điểm yếu ATTT. Và áp dụng thành công trong việc thu thập, phân loại và đánh giá các điểm yếu ATTT tại một cổng TTĐT trong thực tế.

KẾT LUẬN

Có thể thấy, việc đảm bảo ATTT cho Cổng TTĐT là rất quan trọng và nên được các cơ quan nhà nước chú trọng. Thực tế cho thấy rằng, nếu như các tổ chức, cơ quan nhà nước không thật sự quan tâm đến vấn đề ATTT của Cổng TTĐT thì hậu quả rất nghiêm trọng. Kẻ tấn công có thể lợi dụng các lỗ hổng, điểm yếu an ninh của Cổng TTĐT để tấn công vào các hệ thống bên trong, đánh sập hệ thống, lấy cắp hoặc phá hoại những dữ liệu quan trọng.

Những năm gần đây, việc thu thập, phân loại và đánh giá các điểm yếu an toàn thông tin đã bắt đầu được áp dụng tại các website của các cơ quan, các doanh nghiệp nhưng chưa thực sự được áp dụng đối với Cổng TTĐT. Ngoài ra, việc thu thập, phân loại và đánh giá điểm yếu chưa được hệ thống hóa và chưa được áp dụng vào thực tế một cách hiệu quả mà hầu hết là thực hiện tùy theo trình độ của đội ngũ cán bộ quản trị. Việc thu thập, phân loại và đánh giá điểm yếu ATTT ngày nay đã được hỗ trợ bởi rất nhiều công cụ mã nguồn mở hoặc công cụ có bản quyền nhưng quá trình rà quét chưa theo bất kỳ quy trình hay chuẩn nào, vì vậy sẽ dẫn đến tình trạng rà quét thiếu thông tin cần thiết.

Kết quả đạt được

Trong phạm vi giới hạn của luận văn, học viên đã hệ thống hóa được những kiến thức về các điểm yếu ATTT hiện nay nói chung và các điểm yếu của hệ thống Cổng TTĐT nói riêng, từ đó giúp người đọc có cái nhìn trực quan nhất về tình hình thực tế trong việc đảm bảo ATTT của Cổng TTĐT hiện nay.

Luận văn đã nghiên cứu được cấu trúc của cổng TTĐT, đưa ra những vấn đề cần quan tâm để có thể đảm bảo được ATTT cho cổng TTĐT. Luận văn đã đưa ra được phương pháp thu thập thông tin về điểm yếu ATTT một cách khoa học nhất, giúp người thực hiện có thể thu thập được các thông tin với số lượng nhiều nhất có thể. Từ việc thu thập thông tin điểm yếu đó luận văn cũng đã xây dựng được mô hình đánh giá, bộ tiêu chí đánh giá điểm yếu ATTT, các bài đo thử nghiệm, kịch bản thử nghiệm để phân tích, đánh giá điểm yếu ATTT cho Cổng TTĐT theo chuẩn OWASP. Phần thực nghiệm của luận văn, học viên đã tiến hành thu thập thông tin, phân loại và đánh giá điểm yếu của cổng thông tin điện tử Học viện Công nghệ Bưu chính Viễn thông. Từ kết quả thu được, học viên đã trao đổi, phối hợp với quản trị viên để có những phương án và biện pháp khắc phục đảm bảo ATTT cho Cổng TTĐT của học viện cũng như các hệ thống liên quan.

Hạn chế

Do hạn chế về mặt thời gian và kinh nghiệm bản thân, vì vậy luận văn vẫn chưa thể thống kê được hết các điểm yếu hiện nay mà chỉ đưa ra được những tập điểm yếu chính, vì vậy chưa thể khai thác hết được những điểm yếu ATTT của Công TTĐT.

Hướng phát triển tiếp theo

Dựa vào những nội dung đã xây dựng được trong luận văn và thực tế hiện nay chưa có bất kỳ đề tài nào nói về việc đảm bảo ATTT cho Công TTĐT. Vì vậy, học viên sẽ tiếp tục phát triển và hoàn thiện hơn về các phương pháp thu thập, phân loại và đánh giá điểm yếu ATTT. Từ đó có thể xây dựng được một hệ thống giám sát, phát hiện và đánh điểm yếu tại các tổ chức/ cơ quan nhà nước và sau đó có thể mở rộng ra các doanh nghiệp, tổ chức trong và ngoài nước.

TÀI LIỆU THAM KHẢO

Tài liệu Tiếng Việt

- [1] Hoàng Đăng Hải (2014), Tài liệu môn An ninh mạng, *Học viện Công nghệ Bưu chính Viễn thông, Hà Nội.*
- [2] Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (2011), *Hướng dẫn một số biện pháp kỹ thuật cơ bản đảm bảo cho công/trang thông tin điện tử, Bộ Thông tin và Truyền thông, Hà Nội.*
- [3] Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (2009), *TCVN ISO/IEC 27001:2009, Bộ Thông tin và Truyền thông, Hà Nội.*
- [4] Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (2009), *TCVN ISO/IEC 27001:2011, Bộ Thông tin và Truyền thông, Hà Nội.*
- [5] Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (2011), *TCVN ISO/IEC 8709:2011, Bộ Thông tin và Truyền thông, Hà Nội.*
- [6] Viện khoa học kỹ thuật Bưu điện (2011), *TCVN ISO/IEC 27002:2011, Bộ Thông tin và Truyền thông, Hà Nội.*

Tài liệu Tiếng Anh

- [7] Rafay Baloch (2015), *Ethical hacking and penetration testing guide, Taylor and Francis Group, LLC*
- [8] Ron Ben-Natan, Richard Gornitsky, Tim Hanis (2004), *Mastering IBM WebSphere Portal, Wiley Publishing, Inc*
- [9] Jeremial Grossman (2007), *XSS Attacks, Syngress*
- [10] HyunChul Joh1, and Yashwant K. Malaiya - Defining and Assessing (2011), *Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics.*
- [11] Georgia Weidman (2014), *Penetration testing*
- [12] OWASP testing guide 2015, *OWASP*

Link website tham khảo

- [13] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology ngày 20/03/2016
- [14] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project. Ngày 13/04/2016
- [15] <https://www.owasp.org/index.php/Category:Vulnerability> ngày 20/04/2016

- [16] <http://antoanthongtin.vn> ngày 10/03/2016
- [17] <https://voer.edu.vn/m/mo-hinh-kien-truc-he-thong-cong-thong-tin-dien-tu/3d7d1ef2>
ngày 20/03/2016
- [18] http://www.ibm.com/developerworks/websphere/techjournal/0604_collet/0604_collet.html ngày 30/03/2016