

**ĐẠI HỌC THÁI NGUYÊN  
TRƯỜNG ĐẠI HỌC CNTT VÀ TRUYỀN THÔNG**

---

**LÊ THỊ HẠNH**

**TÌM HIỂU CÔNG CỤ ĐÁNH GIÁ HỆ THỐNG  
ĐẢM BẢO AN TOÀN HỆ THỐNG THÔNG TIN**

**LUẬN VĂN THẠC SĨ: KHOA HỌC MÁY TÍNH**

*Thái Nguyên, tháng 6 năm 2015*

**ĐẠI HỌC THÁI NGUYÊN  
TRƯỜNG ĐẠI HỌC CNTT VÀ TRUYỀN THÔNG**

---

**LÊ THỊ HẠNH**

**TÌM HIỂU CÔNG CỤ ĐÁNH GIÁ HỆ THỐNG  
ĐẢM BẢO AN TOÀN HỆ THỐNG THÔNG TIN**

**Chuyên ngành: Khoa học máy tính  
Mã số: 60 48 01**

**LUẬN VĂN THẠC SĨ: KHOA HỌC MÁY TÍNH**

**NGƯỜI HƯỚNG DẪN KHOA HỌC: TS HỒ VĂN HƯƠNG**

*Thái Nguyên, tháng 6 năm 2015*

## LỜI CAM ĐOAN

Tôi xin cam đoan:

1. Những nội dung trong luận văn này là do tôi thực hiện dưới sự trực tiếp hướng dẫn của thầy giáo TS. Hồ Văn Hương.
2. Mọi tham khảo dùng trong luận văn đều được trích dẫn rõ ràng tên tác giả, tên công trình, thời gian, địa điểm công bố.
3. Mọi sao chép không hợp lệ, vi phạm quy chế đào tạo, hay gian trá, tôi xin chịu hoàn toàn trách nhiệm.

Thái Nguyên, tháng 5 năm 2015

Học viên

Lê Thị Hạnh

## LỜI CẢM ƠN

Tôi xin chân thành cảm ơn trường Đại học Công nghệ thông tin và Truyền thông – Đại học Thái nguyên, cùng tất cả các thầy giáo, cô giáo đã tận tình giảng dạy và giúp đỡ tôi trong suốt quá trình học tập, nghiên cứu.

Tôi xin bày tỏ lòng biết ơn sâu sắc đến thầy giáo TS. Hồ Văn Hương, người đã trực tiếp hướng dẫn và tạo mọi điều kiện thuận lợi giúp đỡ tôi trong quá trình thực hiện đề tài.

Tôi xin trân trọng cảm ơn Ban lãnh đạo, các đồng nghiệp trường Cao đẳng Y tế Thanh Hóa đã ủng hộ và dành thời gian để giúp đỡ tôi hoàn thành luận văn này.

Tuy đã có nhiều cố gắng, nhưng chắc chắn luận văn của tôi còn có rất nhiều thiếu sót. Rất mong nhận được sự góp ý của thầy giáo, cô giáo và các bạn đồng nghiệp.

Xin chân thành cảm ơn!

## MỤC LỤC

LỜI CAM ĐOAN .....	i
LỜI CẢM ƠN.....	iv
DANH SÁCH CÁC HÌNH ẢNH .....	vii
DANH SÁCH CÁC TỪ VIẾT TẮT .....	viii
MỞ ĐẦU .....	1
ĐẶT VẤN ĐỀ.....	1
1.    ĐỐI TƯỢNG VÀ PHẠM VI NGHIÊN CỨU .....	1
2.    PHƯƠNG PHÁP NGHIÊN CỨU.....	2
3.    HƯỚNG NGHIÊN CỨU CỦA ĐỀ TÀI.....	2
4.    BỐ CỤC LUẬN VĂN .....	2
5.    Ý NGHĨA KHOA HỌC CỦA ĐỀ TÀI.....	3
CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN VÀ BẢO MẬT THÔNG TIN.....	4
1.1.    Tổng quan về hệ thống thông Tin.....	4
1.1.1    Khái niệm hệ thống thông tin.....	4
1.1.2    Các thành phần cấu thành nên hệ thống thông tin .....	4
1.1.3    Các nguy cơ mất an toàn thông tin.....	5
1.2.    Hệ thống thông tin an toàn và bảo mật.....	6
1.2.1.    Các đặc trưng của hệ thống thông tin an toàn và bảo mật .....	6
1.2.2.    Các biện pháp đảm bảo an toàn hệ thống thông tin .....	7
1.3.    Một số trang thiết bị đảm bảo an toàn và bảo mật thông tin .....	9
1.3.1.    An toàn và bảo mật thông tin trên các thiết bị mạng .....	9
1.3.2.    An toàn và bảo mật thông tin trong truyền dẫn.....	10
1.4.    Thực trạng an toàn thông tin.....	10
1.4.1.    Thực trạng an toàn thông tin ở Việt Nam và trên Thế giới.....	10
1.4.2.    Nguy cơ mất an ninh thông tin trên công thông tin điện tử .....	12
1.5.    Kết luận chương 1.....	14
CHƯƠNG 2: NGHIÊN CỨU CÁC KỸ THUẬT PHÂN TÍCH, THÂM NHẬP HỆ THỐNG MẠNG .....	15
2.1.    Nghiên cứu một số lỗ hổng trong công thông tin điện tử.....	15
2.1.1.    SQL injection .....	15
2.1.2.    XSS.....	16
2.1.3.    CSRF .....	18
2.1.4.    Tràn bộ đệm.....	20
2.2.    Khai thác các công cụ an ninh mạng .....	21
2.2.1.    Công cụ Sniffer-nghe lén .....	21
2.2.2.    Công cụ hacking.....	23
2.2.3.    Công cụ quét bảo mật website.....	27
2.3.    Tìm hiểu một số công cụ quét bảo mật website .....	30

2.3.1.	Acunetix Web Vulnerability Scanner .....	30
2.3.2.	Bkav webscan.....	37
2.3.3.	IBM Rational AppScan .....	40
2.4.	Kết luận chương 2.....	41
<b>CHƯƠNG 3: ĐÁNH GIÁ, LỰA CHỌN CÔNG CỤ VÀ TRIỂN KHAI ÁP DỤNG..</b>		<b>42</b>
3.1.	Đánh giá công cụ dò quét lỗ hổng website.....	42
3.2.	Đề xuất quy trình triển khai, đánh giá công thông tin điện tử.....	45
3.2.1	Mục đích.....	46
3.2.2	Phạm vi áp dụng.....	46
3.2.3	Mô tả quy trình thực hiện.....	46
3.2.4	Đánh giá quy trình.....	48
3.3.	Áp dụng quy trình triển khai đánh giá công thông tin điện tử trường Cao đẳng Y Tế Thanh Hóa sử dụng công cụ Acunetix.....	49
3.3.1.	Xây dựng kịch bản đánh giá công thông tin điện tử. ....	49
3.3.2.	Thực hiện đánh giá.....	50
3.3.3.	Kết quả đánh giá.....	54
3.4.	Áp dụng quy trình triển khai đánh giá công thông tin điện tử tỉnh Thanh Hóa sử dụng công cụ Acunetix.....	60
3.4.1.	Xây dựng kịch bản đánh giá công thông tin điện tử .....	60
3.4.2.	Thực hiện đánh giá.....	60
3.4.3.	Kết quả đánh giá.....	61
3.4.4.	Kết luận chương 3.....	64
<b>KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN .....</b>		<b>65</b>
1.	Kết quả đạt được.....	65
2.	Đánh giá chương trình .....	65
3.	Hướng phát triển trong tương lai .....	66
<b>DANH MỤC TÀI LIỆU THAM KHẢO .....</b>		<b>67</b>

## DANH SÁCH CÁC HÌNH ẢNH

Hình 1.1. Các thành phần của HTTPT .....	5
Hình 1.2. Mô hình CIA .....	7
Hình 2.1: Quá trình thực hiện XSS .....	17
Hình 2.2. Sử dụng đĩa Linux Live CD để truy cập các file .....	24
Hình 2.3. Phá mật khẩu với Ophcrack.....	26
Hình 2.4. Quá trình sinh ra dữ liệu kiểm thử trong CFG .....	29
Hình 2.5. Hệ thống kiểm tra lỗ hổng Bkav WebScan .....	37
Hình 3.1. Màn hình chính khi Crawl .....	51
Hình 3.2. Giao diện chính của Acunetix .....	52
Hình 3.3. Thông tin về server .....	53
Hình 3.4. Giao diện khi đang thực hiện quét.....	54
Hình 3.5. Kết quả đánh giá.....	58
Hình 3.6. Báo cáo tổng hợp.....	58
Hình 3.7. Báo cáo chi tiết .....	59
Hình 3.8. Báo cáo lỗi đường dẫn.....	59
Hình 3.9. Báo cáo kích hoạt mật khẩu.....	59
Hình 3.10. Kết quả đánh giá .....	61
Hình 3.11. báo cáo tổng hợp.....	61
Hình 3.12. Báo cáo chi tiết .....	62
Hình 3.13. Báo cáo về thông tin người dùng.....	62
Hình 3.14. Báo cáo lỗi đường dẫn.....	62

## DANH SÁCH CÁC BẢNG

Bảng 3.1. Nội dung quy trình .....	48
Bảng 3.2. xây dựng kịch bản .....	50
Bảng 3.3. Kết quả theo kịch bản.....	56
Bảng 3.4. xây dựng kịch bản .....	60
Bảng 3.5. Kết quả đánh giá theo kịch bản.....	63

## DANH SÁCH CÁC TỪ VIẾT TẮT

<b>Từ viết tắt</b>	<b>Nội dung</b>
HTTT	Hệ thống thông tin
ATTT	An toàn thông tin
USB	Universal Serial Bus



## MỞ ĐẦU

### ĐẶT VẤN ĐỀ

Vấn đề bảo đảm an toàn cho các hệ thống thông tin (HTTT) là một trong những vấn đề quan trọng cần cân nhắc trong suốt quá trình thiết kế, thi công, vận hành và bảo dưỡng HTTT. Cũng như tất cả các hoạt động khác trong đời sống xã hội, từ khi con người có nhu cầu lưu trữ và xử lý thông tin, đặc biệt là từ khi thông tin được xem như một bộ phận của tư liệu sản xuất, thì nhu cầu bảo vệ thông tin càng trở nên bức thiết. Bảo vệ thông tin là bảo vệ *tính bí mật* của thông tin và *tính toàn vẹn* của thông tin. Một số loại thông tin chỉ còn ý nghĩa khi chúng được giữ kín hoặc giới hạn trong một số các đối tượng nào đó, ví dụ như thông tin về chiến lược quân sự chẳng hạn. Đây là tính bí mật của thông tin. Hơn nữa, thông tin không phải luôn được con người ghi nhớ do sự hữu hạn của bộ óc, nên cần phải có thiết bị để lưu trữ thông tin. Nếu thiết bị lưu trữ hoạt động không an toàn, thông tin lưu trữ trên đó bị mất đi hoặc sai lệch toàn bộ hay một phần, khi đó tính toàn vẹn của thông tin không còn được bảo đảm.

Khi máy tính được sử dụng để xử lý thông tin, hiệu quả xử lý thông tin được nâng cao lên, khối lượng thông tin được xử lý càng ngày càng lớn lên, và kéo theo nó, tầm quan trọng của thông tin trong đời sống xã hội cũng tăng lên. Nếu như trước đây, việc bảo vệ thông tin chỉ chú trọng vào vấn đề dùng các cơ chế và phương tiện vật lý để bảo vệ thông tin theo đúng nghĩa đen của từ này, thì càng về sau, vấn đề bảo vệ thông tin đã trở nên đa dạng hơn và phức tạp hơn.

Vì vậy, an toàn bảo mật thông tin sẽ là vấn đề rất nóng bỏng. Đây là cuộc đấu tranh không có hồi kết vì kẻ xấu luôn lợi dụng không gian mạng để rửa tiền, ăn cắp tài khoản hay thực hiện những mục đích cạnh tranh không lành mạnh. CNTT còn phát triển thì cuộc đấu tranh bảo đảm an ninh, ATTT sẽ còn tiếp tục và quyết liệt hơn. Vấn đề là ý thức trách nhiệm của những người thiết kế hệ thống cũng như người sử dụng. Xuất phát từ thực tế đó luận văn đi sâu vào “*Tìm hiểu công cụ đánh giá hệ thống đảm bảo an toàn hệ thống thông tin*”.

### 1. ĐỐI TƯỢNG VÀ PHẠM VI NGHIÊN CỨU

- Lý thuyết về an toàn và bảo mật hệ thống thông tin

- Thực trạng an toàn thông tin ở Việt Nam và Thế giới
- Các kỹ thuật phân tích, thâm nhập hệ thống mạng
- Một số công cụ quét bảo mật website.

## 2. PHƯƠNG PHÁP NGHIÊN CỨU

Sử dụng các phương pháp nghiên cứu chính sau:

- Phương pháp nghiên cứu lý thuyết: Tìm hiểu lý thuyết về an toàn và bảo mật hệ thống thông tin, các nguy cơ gây mất an toàn thông tin, các biện pháp đảm bảo an toàn hệ thống thông tin. Nghiên cứu các kỹ thuật phân tích, thâm nhập hệ thống mạng.
- Phương pháp thực nghiệm: Lựa chọn, cài đặt công cụ và thực thi kiểm thử bảo mật.
- Phương pháp trao đổi khoa học, lấy ý kiến chuyên gia.

## 3. HƯỚNG NGHIÊN CỨU CỦA ĐỀ TÀI

- Nghiên cứu, tìm hiểu các vấn đề về an toàn hệ thống thông tin.
- Nghiên cứu các kỹ thuật phân tích, thâm nhập hệ thống mạng.
- Đánh giá hệ thống an toàn, bảo mật thông tin từ đó xây dựng và phát triển công cụ kiểm tra, đánh giá an toàn thông tin.

## 4. BỐ CỤC LUẬN VĂN

Luận văn được chia làm 3 chương:

Chương 1: Tổng quan về an toàn và bảo mật thông tin. Chương này chủ yếu trình bày về các vấn đề chung như: vai trò nhiệm vụ của HTTT, các yêu cầu của một hệ truyền thông an toàn và bảo mật, trình bày các nguy cơ mất ATTT và giới thiệu một số trang thiết bị đảm bảo an toàn và bảo mật thông tin.

Chương 2: Nghiên cứu các kỹ thuật phân tích, thâm nhập hệ thống mạng. Nội dung chương này chủ yếu tìm hiểu các công cụ an ninh mạng như đi sâu vào nghiên cứu, đánh giá ưu nhược điểm một số công cụ quét bảo mật website.