GIẢI PHÁP KẾT HỢP GIÁM SÁT VÀ ĐÁNH GIÁ AN TOÀN CỔNG THÔNG TIN ĐIỆN TỬ THEO CHUẨN

Hoàng Đăng Hải[1], **Phạm Thiếu Nga**[2]
[1]Học viện Công nghệ Bưu chính Viễn thông
[2]Đại học Xây dựng Hà Nội
Email: haihd@ptit.edu.vn

Tóm tắt: Giám sát và đánh giá an toàn là hai nhiệm vụ tuy có vẻ tách biệt song lại có mối quan hệ mật thiết với nhau. Hầu hết các giải pháp đã biết tới nay thường chỉ tập trung vào một trong hai nhiệm vụ trên. Mặt khác, chưa có giải pháp nào theo một tiêu chuẩn đã công bố. Bài báo này đề xuất một giải pháp kết hợp giám sát tập trung và đánh giá an toàn cho cổng thông tin điện tử theo chuẩn, cụ thể là chuẩn ISO 15408. Ý tưởng của giải pháp là đưa ra một kiến trúc hệ thống xuyên suốt quá trình giám sát, thu thập dữ liệu, đánh giá mức độ an toàn cho mạng giám sát cỡ lớn theo phương thức tập trung. Giải pháp sử dụng dữ liệu thu thập cho cả nhiệm vụ phát hiện nguy cơ tấn công và đánh giá an toàn. Phương pháp thứ bậc phân tích được áp dụng để tính trọng số cho các lớp chức năng an toàn theo ISO 15408 và đưa ra kết quả đánh giá định lượng mức độ an toàn cho cổng thông tin điện tử. Thử nghiệm đã được thực hiện với gần 200 cổng TTĐT.

Từ khóa: Giám sát an toàn, an toàn ứng dụng Web, đánh giá an toàn ứng dụng Web.

I. MỞ ĐẦU

Cổng thông tin điện tử (TTĐT) là một trang Web đặc biệt tập hợp nội dung thông tin và dịch vụ Web vào một bộ khung thống nhất để cung cấp cho người dùng dưới một tên miền chung. Cho tới nay, cổng TTĐT đã trở thành một thành phần không thể thiếu trong hoạt động của mọi cơ quan, tổ chức, doanh nghiệp. Do chứa một lượng thông tin lớn và đa dạng, cổng TTĐT luôn là một mục tiêu tấn công hấp dẫn của tin tặc. Vì vậy, giám sát và đánh giá an toàn cho cổng TTĐT luôn là một chủ đề được quan tâm nhiều và có nhiều thách thức kỹ thuật được đặt ra.

Giám sát và đánh giá an toàn là hai nhiệm vụ tuy có vẻ tách biệt song lại có mối quan hệ mật thiết với nhau. Giám sát an toàn cho cổng TTĐT là một phạm trù của lĩnh vực giám sát an toàn thông tin, là việc theo dõi hoạt động của cổng TTĐT nhằm phát hiện và đưa ra cảnh báo về các nguy cơ tấn công. Giám sát an toàn bao gồm các thành phần tối thiểu là: thu thập dữ liệu, xử lý phân tích, phát hiện và cảnh báo. Đánh giá an toàn cổng TTĐT là xác định mức độ bảo đảm an toàn của cổng, bao gồm việc kiểm tra các lỗ hổng bảo mật tiềm ẩn gây ra nguy cơ tấn công, xác định mức độ phù hợp của các biện pháp bảo vệ. Đánh giá an toàn gồm các thành phần tối thiểu là: thu thập dữ liệu, xử lý phân tích và đánh giá mức độ bảo đảm an toàn. Như vậy, cả hai nhiệm vụ giám sát và đánh giá an toàn đều có chung một số thành phần và đều nhằm theo dõi, kiểm tra, xác định mức độ bảo đảm an toàn cho cổng TTĐT.

Tuy nhiên, hầu hết các giải pháp đã biết tới nay thường chỉ tập trung vào một trong hai nhiệm vụ trên. Các giải pháp giám sát an toàn đã trải qua các giai đoạn phát triển từ các hệ thống giám sát mạng đơn lẻ [1], cho tới các hệ thống giám sát diện rộng [2], các hệ thống giám sát phân tán trên đám mây [3, 4, 5], nhằm giải quyết những vấn đề tồn tại của các hệ thống giám sát truyền thống, ví dụ đối với các tài sản thông tin trên đám mây. Những giải pháp mới, ví dụ [5, 6, 7], chủ yếu đề xuất khắc phục hạn chế về số lượng điểm giám sát (tính mở rộng) [5], không sử dụng agent [6], hay vấn đề xử lý thời gian thực [7]. Một số giải pháp giám sát an toàn đặc thù cho các ứng dụng Web cũng đã được đề xuất, điển hình như [8, 9, 10, 11]. Tuy nhiên có thể thấy, vẫn chưa có giải pháp giám sát an toàn nào tận dụng nguồn dữ liệu thu thập được để kết hợp với nhiệm vụ đánh giá mức độ an toàn cổng TTĐT.

Mặt khác, đã có nhiều giải pháp riêng cho đánh giá mức độ an toàn, cụ thể là cho các ứng dụng Web. Song vẫn chưa có giải pháp đánh giá an toàn nào kết hợp với một hệ thống giám sát an toàn. Điển hình cho các giải pháp đánh giá an toàn ứng dụng Web là phương pháp tính điểm an toàn ứng dụng Web theo tiêu chí chung (CCWAPSS- Common Criteria Web Application Security Scoring) [12], mô hình đánh giá theo chuẩn ISO 15408 [13]. Một số giải pháp đề xuất phương pháp đánh giá cho từng thành phần ứng dụng Web không theo chuẩn như [14, 15, 16, 17, 18].Theo khảo sát của các tác giả, vẫn chưa có mô hình đánh giá định lượng phù hợp chuẩn cho mức độ an toàn cho ứng dụng Web nói chung và cổng TTĐT nói riêng.

Việc kết hợp hai nhiệm vụ giám sát và đánh giá an toàn là cần thiết đối với cổng TTĐT, vì cả hai nhiệm vụ đều có mục tiêu chung là xác định mức độ an toàn, phát hiện các nguy cơ sự cố và mức độ phù hợp của các biện pháp bảo vệ. Sự kết hợp này mang lại hiệu quả và lợi ích do tận dụng được nguồn dữ liệu thu thập được, cho phép

Tác giả liên hệ: Hoàng Đăng Hải
Email: haihd@ptit.edu.vn
Đến tòa soạn: 02/2020, chỉnh sửa: 04/2020, chấp nhận đăng: 04/2020

sử dụng kết quả giám sát và đánh giá để so sánh mức độ an toàn giữa các cổng TTĐT. Ngoài ra, giải pháp đưa ra kết quả đánh giá định lượng theo chuẩn ISO 15408 và kết hợp với phương pháp thứ bậc phân tích để tính trọng số cho các lớp chức năng an toàn theo chuẩn. Đó là những đóng góp chính của bài báo này. Ý tưởng xuyên suốt của giải pháp đề xuất trong bài là một mô hình kết hợp giám sát, thu thập dữ liệu, phân tích, đánh giá an toàn cho một phạm vi cỡ lớn các cổng TTĐT theo phương thức tập trung.

Phần tiếp theo của bài báo như sau:Phần II trình bày các nghiên cứu liên quan giám sát và đánh giá an toàn cổng TTĐT, phần III đề xuất giải pháp kết hợp giám sát tập trung và đánh giá an toàn cổng TTĐT theo chuẩn, phần IV là kết luận của bài.

II. CÁC NGHIÊN CỨU LIÊN QUAN

A. Khái quát các giải pháp giám sát an toàn

Qua khảo sát, có thể khái quát các nhóm giải pháp giám sát an toàn theo các giai đoạn phát triển như sau.

- *Nhóm giải pháp cho các hệ thống đơn lẻ*

Đây là nhóm giải pháp truyền thống phát triển từ các hệ thống quản trị mạng nhằm giám sát truy nhập, theo dõi hoạt động, cảnh báo sự cố [2, 19]. Hệ thống giám sát sử dụng một số công cụ phần mềm đơn lẻ nhằm phát hiện tấn công, nguy cơ sự cố. Điển hình là các công cụ Nmap, Nagios… Nhóm giải pháp này không phục vụ riêng cho cổng TTĐT cũng như các ứng dụng Web, mà chủ yếu giám sát dịch vụ mạng và hệ thống mạng.

- *Nhóm giải pháp tích hợp hệ thống*

Đặc trưng của nhóm giải pháp này là có sự tích hợp các công cụ, hệ thống con vào chung một hệ thống giám sát. Các hệ thống con điển hình được tích hợp như tường lửa, phát hiện xâm nhập (IDS- Intrusion Detection System), ngăn chặn xâm nhập (IPS- Intrusion Prevention System), các bẫy nhử Honeypots, Honeynet [1, 3]. Việc kết hợp nhiều hệ thống con thường gặp nhiều khó khăn do tính phức tạp cao, khả năng tương thích kém, hạn chế về khả năng linh hoạt, mềm dẻo và khả năng mở rộng.

- *Nhóm giải pháp quản lý tập trung diện rộng*

Nhóm giải pháp này có ưu điểm so với các nhóm giải pháp đã nêu trên là có sự tích hợp các công nghệ mới trong giám sát, phát hiện tấn công [1, 20, 21]. Kiến trúc tập trung khắc phục được nhiều hạn chế trong các giải pháp trước đó, cho phép tích hợp nhiều loại công nghệ vào một hệ thống chung, thích ứng với việc mở rộng phạm vi giám sát, cập nhật công nghệ kịp thời. Tuy nhiên, các hệ thống giám sát lớn thường khó kiểm soát, khó tạo được sự liên kết giữa các hệ thống con khi mở rộng, chi phí thường rất cao.

- *Nhóm giải pháp giám sát đặc thù*

Nhóm giải pháp này được phát triển nhằm đáp ứng sự bùng nổ của dữ liệu lớn, điện toán đám mây, tính toán phân tán, sự phát triển của các thiết bị di động và thiết bị thông minh [3, 4, 23, 24]. Một số nghiên cứu mới về các giải pháp giám sát đặc thù điển hình như [8, 11, 5, 6, 7]. Các giải pháp giám sát đặc thù đã trở thành xu hướng khá phổ biến.

Song song với các nghiên cứu đã công bố là các hệ thống giám sát an toàn được phát triển dưới dạng sản phẩm thương mại đóng kín, điển hình như: Complete Website Security (CWS) của Symantec, Web Security Appliance (WSA) của Cisco, QRadar của IBM, PRTG Network Monitor của Paessler, SecureSphere của Impeva. Ngoài ra, còn có các giải pháp phần mềm nguồn mở, điển hình như Observium (*http://www.observium.org*), Nagios (*https://www.nagios.org/*), OpenNMS (*https://www.opennms.org*) và khá nhiều phần mềm giám sát đơn lẻ khác như: N-Stalker Web Application Security Scanner (WASS) của N-Stalker (*https://www.nstalker.com*), Site 24x7 (*https://www.site24x7.com/*), ParosPro (*www.milescan.com*), hay Dynatrace (*https://www.dynatrace.com*).

Mặc dù có nhiều giải pháp và sản phẩm hệ thống giám sát khá đa dạng, vẫn chưa có giải pháp hay hệ thống nào đề cập đến khả năng kết hợp giám sát và đánh giá an toàn cho cổng TTĐT.

B. Khái quát các giải pháp đánh giá an toàn

Đánh giá an toàn được quan tâm từ năm 1993 với việc đề xuất các tiêu chí đánh giá chung (Common Criteria) [12, 25]. Một mô hình đánh giá chung và bộ tiêu chí chung cho đánh giá an toàn đã được đưa ra trong tiêu chuẩn ISO 15408 [13]. Tuy nhiên, mô hình và bộ tiêu chí này không dành riêng cho ứng dụng Web, không có kết quả định lượng trong đánh giá. Biểu diễn kết quả đánh giá chỉ là định tính đạt hoặc không đạt tiêu chuẩn.

Đã có một số công trình nghiên cứu theo hướng định lượng hóa kết quả đánh giá theo tiêu chuẩn, điển hình như [26, 27, 28]. Các giải pháp này sắp xếp các yêu cầu an toàn vào 11 lớp chức năng an toàn theo chuẩn ISO 15408. Mỗi yêu cầu được biểu diễn bằng ba thành phần cơ bản là tính bí mật (C- Confidenciality), tính toàn vẹn (I - Integrity), tính sẵn sàng (A- Availability). Có tổng số 33 phần tử cho 11 lớp được gán giá trị là "0" hoặc "1" thể hiện mức độ an toàn. Tuy nhiên, các tác giả chưa đưa ra cách tính các giá trị "0" và "1" như thế nào. Các mô hình còn có độ phức tạp cao, không khả thi, không áp dụng được cho cổng TTĐT.

Dự án nghiên cứu OWASP [29] đưa ra một mô hình đánh giá các ứng dụng Web sử dụng một bộ tiêu chí chung gọi là CCWAPSS (Common Criteria Web Application Security Scoring) [12]. Mô hình đánh giá đơn giản hóa việc triển khai thông qua việc sắp xếp các yêu cầu an toàn vào các nhóm. Kết quả đánh giá theo hệ thống điểm số từ 1 đến 10 (10 là tốt nhất).Mỗi tiêu chí đánh giá tương ứng với một nhóm lỗ hổng bảo mật ứng dụng Web. Việc đánh giá chủ yếu dựa trên quan sát các điểm yếu điển hình của các ứng dụng Web. Mặc dù mô hình này cho kết quả định lượng tương đối qua điểm số, cách triển khai đơn giản, song kết quả đánh giá vẫn mang tính chủ quan, phụ thuộc vào chuyên gia đánh giá.

Một số công trình nghiên cứu khác không theo hướng áp dụng tiêu chuẩn, đề xuất mô hình đánh giá cho từng thành phần cụ thể của ứng dụng Web, ví dụ trong [14, 16, 17, 30-33] được nêu cụ thể dưới đây.

Các tác giả trong [14] phát triển một công cụ tự động tạo ra các tấn công vào lỗ hổng bảo mật Web và kiểm tra khả năng bảo vệ. Nghiên cứu trong [16] đề xuất một phương pháp sử dụng các tập hồ sơ dựng sẵn tương tự chuẩn ISO 15408 để phân tích mức độ an toàn của máy chủ Web. Các tác giả trong [17] xây dựng một mô hình kiểm thử thụ động cho các dịch vụ Web.Nghiên cứu

trong [30, 31] tập trung vào kiểm tra việc nhập dữ liệu lỗi bằng cách kết hợp phân tích động với kiểm thử truyền thống. Trong [32], một công cụ kiểm thử tấn công mã xuyên trang trực tuyến (online XSS- Cross Site Scripting) được phát triển, thực hiện các bước giả lập một tấn công XSS và kiểm tra khả năng bảo vệ ứng dụng Web. Phương pháp kiểm thử đăng nhập một lần (SSO- Single Sign On) vào ứng dụng Web được nghiên cứu trong [33] với việc sử dụng một công cụ quét SSO để kiểm tra thành phần xác thực.

Một số giải pháp đánh giá an toàn đã được phát triển dưới dạng sản phẩm thương mại đóng kín hoặc sản phẩm nguồn mở. Các sản phẩm thương mại điển hình như: phần mềm Acunetix (*https://www.acunetix.com*), Security AppScan của IBM (*https://www.ibm.com/software/products/en/appscan*), Metasploit của Rapid7 (*https://www.metasploit.com/*), Burp Suite của Portswigger (*https://portswigger.net/ burp*). Một số sản phẩm mã nguồn mở điển hình như: Grabber (*https://github.com/neuroo/grabber*), Wapiti (*http://wapiti.sourceforge.net/*), W3af (*http://w3af.org/*), hay OpenVas (*www.openvas.org*).

Một kết quả khảo sát thực hiện trong [18] cho thấy, chưa có một mô hình phù hợp cho đánh giá an toàn ứng dụng Web khả thi trong thực tiễn. Mặc dù đã có nhiều giải pháp theo hướng chuẩn hoặc không áp dụng tiêu chuẩn, vẫn chưa có giải pháp hay hệ thống nào có sự quan tâm đầy đủ đến khả năng đánh giá định lượng khách quan. Kết quả khảo sát của chúng tôi cũng cho thấy, chưa có giải pháp hay hệ thống nào đề cập đến khả năng kết hợp đánh giá an toàn với giám sát an toàn cho cổng TTĐT. Ngoài ra, xu hướng chuẩn hóa cũng là cần thiết, song chưa được đề cập trong nhiều giải pháp hiện có.

III. GIẢI PHÁP KẾT HỢP GIÁM SÁT VÀ ĐÁNH GIÁ AN TOÀN CỔNG TTĐT THEO CHUẨN

A. *Mô hình kiến trúc hệ thống*

Hình 1 là mô hình kiến trúc hệ thống kết hợp giám sát tập trung và đánh giá an toàn cổng TTĐT.

Bên trái Hình 1 là các cổng TTĐT cần giám sát và đánh giá an toàn. Bên phải là các khối chức năng chính trong hệ thống kết hợp giám sát và đánh giá an toàn, cụ thể gồm:

- Khối thu thập dữ liệu: thực hiện thu thập dữ liệu từ các cổng TTĐT phục vụ cho nhiệm vụ giám sát tập trung và đánh giá an toàn theo chuẩn.
- Khối tổng hợp dữ liệu: làm sạch dữ liệu, chuẩn hóa dữ liệu, gán nhãn và chia tách các tập hợp dữ liệu phục vụ tìm kiếm, truy xuất dữ liệu để xử lý tiếp.
- Khối theo dõi, giám sát: có nhiệm vụ phân tích dữ liệu, so khớp mẫu dấu hiệu theo các tập luật định sẵn để phát hiện nguy cơ tấn công. Kết quả theo dõi, giám sát được hiển thị với các cảnh báo nguy cơ tấn công.
- Khối đánh giá mức độ an toàn: thực hiện phân tích dữ liệu, tính toán định lượng giá trị thể hiện mức độ an toàn theo chuẩn ISO 15408 và hiển thị kết quả đánh giá mức độ an toàn.

Thống kê khảo sát của Splunk (*http://splunk-sizing.appspot.com*) cho thấy, số sự kiện thu thập từmỗi trang thông tin điện tử có thể đạt trung bình từ 3 đến 20 sự kiện/giây (EPS - Events per Second). Nếu số cổng TTĐT cần giám sát là 500, thì tổng số sự kiện *E*cần xử lý tại trung tâm giám sát sẽ có thể lên tới:

$$E = 20\ EPS * 500 = 10.000\ EPS \quad (1)$$

Nếu thiết kế khối thu thập dữ liệu nhận mỗi bản tin sự kiện gồm tối đa 300 Bytes, thì lượng dữ liệu *D*thu thập được từ 500 cổng TTĐT trong 1 giây sẽ là:

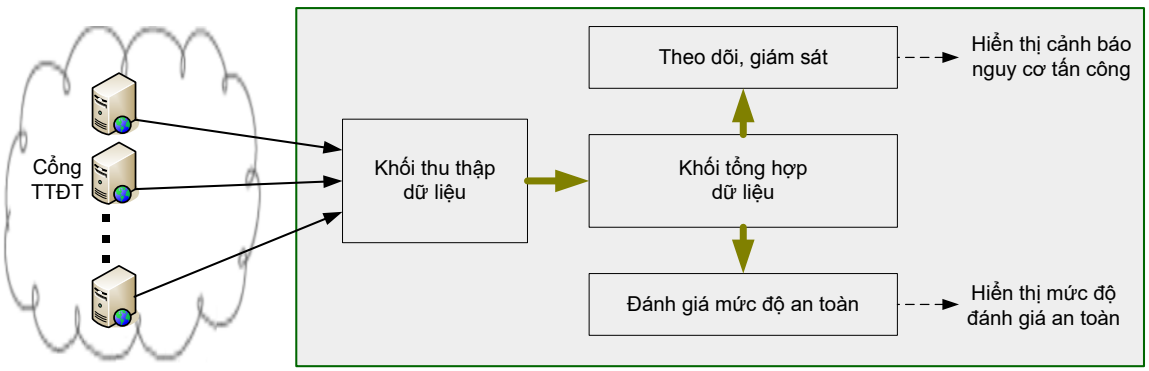
$$D = 300Bytes * 10000 = 3\ Mbytes/s \quad (2)$$

Từ đó, có thể tính được dung lượng đĩa cứng *S*cần dùng để lưu trữ các sự kiện tại trung tâm giám sát trong một ngày (24 giờ * 60 phút * 60 giây) là:

$$S = D * 24 * 60 * 60 = 86.4\ GBytes \quad (3)$$

Nếu dùng Backup dữ liệu, ta sẽ cần dung lượng lưu trữ khoảng 172.8 GBytes. Nếu lưu trữ nhiều ngày, ví dụ theo tháng, ta có thể tính ra tổng dung lượng đĩa cứng cần lưu trữ cho hệ thống.

Những con số nêu trên mới chỉ là tính toán tương đối, song có thể cho ta ước tính sơ bộ năng lực xử lý của hệ thống trung tâm giám sát. Cũng theo Splunk (*http://splunk-sizing.appspot.com*), thiết bị phần cứng phổ biến cho một hệ thống giám sát nêu trên chỉ cần 01 máy chủ Intel Xeon chuẩn, Dual Core, tốc độ CPU từ 2.5 GHz trở lên, RAM tối thiểu 128 GB, ổ đĩa cứng có dung lượng tối thiểu 200 GBytes. Đây cũng là cấu hình máy chủ thông dụng, không yêu cầu quá cao về cấu hình. Nếu số điểm cần giám sát nhiều hơn 500, ta có thể sử dụng máy chủ mạnh hơn, hoặc dùng cấu trúc phân cụm máy chủ. Trong khuôn khổ bài báo, chúng tôi không đi sâu thêm vào nội dung này.



Hình 1. Mô hình kết hợp giám sát tập trung và đánh giá an toàn cổng TTĐT

B. *Nguồn dữ liệu từ cổng TTĐT*

Nguồn dữ liệu thu thập từ các cổng TTĐT có thể rất đa dạng, tùy thuộc vào mục tiêu và phạm vi của mỗi hệ thống giám sát và phương pháp thu thập thông tin. Về nguyên tắc, nguồn dữ liệu chính có thể là: nhật ký hoạt động ghi được tại máy chủ Web cài cổng TTĐT,dữ liệu trạng thái hoạt động của cổng TTĐT và dữ liệu lưu lượng Web.

Theo [34], cổng TTĐT có thể đối mặt với 10 nhóm nguy cơ tấn công chính. Trong phạm vi giải pháp đề xuất của bài báo và theo hướng chuẩn hóa, ta quan tâm đến 10 nhóm dữ liệu về nguy cơ tấn công đối với cổng TTĐT như đã nêu trong [34] như sau:

- *Nguy cơ tấn công chèn mã (Injection):* Nguy cơ khi nhập dữ liệu, ví dụ các tấn công SQL injection, OS injection, LDAP injection... Dữ liệu nhập sai lệch có thể bị kẻ tấn công đưa vào cùng với các biến dữ liệu đầu vào như một phần của lệnh hay câu truy vấn Web. Nguy cơ tấn công kiểu này có thể tạo khả năng truy cập các dữ liệu cổng TTĐT một cách bất hợp pháp.
- *Nguy cơ tấn côngvào phần xác thực (Broken Authentication):* Xác thực hay quản lý phiên bị lỗi. Nguy cơ kẻ tấn công có thể chiếm đoạt mật khẩu, phiên làm việc, định danh người dùng.
- *Nguy cơ tấn công khi lộ dữ liệu nhạy cảm (Sensitive Data Exposure):* Nguy cơ lộ dữ liệu nhạy cảm như thông tin định danh, tài khoản người dùng… do không được bảo vệ, lưu trữ an toàn. Ví dụ, dữ liệu nhạy cảm thiếu mã hóa.
- *Nguy cơ tham chiếu đến đối tượng bên ngoài XML (XML External Entities):* Web có thể chấp nhận một yêu cầu truy vân không an toàn trong XML, tham chiếu không an toàn đến các đối tượng bên trong máy chủ ví dụ như các tệp tin, thư mục, cơ sở dữ liệu. Ví dụ, nguy cơ thực thi mã lệnh từ xa, nguy cơ tạo tấn công từ chối dịch vụ.
- *Nguy cơ thiếu kiểm soát truy nhập (Broken Access Control):* Nguy cơ không có kiểm soát, hạn chế phân quyền truy nhập. Kẻ tấn công có thể chiếm quyền, thay đổi dữ liệu người dùng, thay đổi quyền truy nhập…
- *Nguy cơ cấu hình bảo mật không an toàn (Security Misconfiguration):* Sự cố xảy ra với cấu hình sai, tiêu đề HTTP sai, bộ nhớ vùng làm việc không được bảo vệ…
- *Nguy cơ tấn công xuyên trang (Cross-Site Scripting):* Sự cố do thiếu kiểm soát dữ liệu nhập vào câu truy vấn Web. Dữ liệu bất hợp pháp được gửi đến Web mà không được xác thực. Điều này cho phép kẻ tấn công thực thi các đoạn mã Script làm thay đổi nội dung phản hồi từ máy chủ Web, làm chuyển hướng tới trang khác do tin tặc thiết lập, có thể có chứa mã độc.
- *Nguy cơ giải tuần tự không an toàn (Insecure Desialization):* Nguy cơ này tương tự chuyển hướng, chuyển tiếp không hợp lệ trong phiên bản OWASP Top 10 cũ. Nguy cơ xảy ra khi máy chủ Web cho phép thực thi đoạn mã Script từ xa, cho phép trao đổi các tham số HTML Forms hoặc trao đổi giữa các tiến trình nội bộ không được xác thực.
- *Nguy cơ sử dụng các thành phần có lỗ hổng tiềm ẩn (Using Known Vulnerable Components):* Các thư viện, các tệp tin có chứa lỗ hổng bảo mật tìm thấy trong phản hồi truy vấn Web. Đây là nguy cơ tấn công khai thác lỗ hổng tiềm ẩn.
- *Không ghi được nhật ký và giám sát (Insufficient Logging & Monitoring):* Hệ thống thiếu cơ chế giám sát và ghi lại sự kiện hoạt động khi có lỗi xảy ra, thiếu biện pháp bảo vệ, cảnh báo cần thiết.

C. Khối thu thập dữ liệu

Có hai khả năng thu thập dữ liệu từ các cổng TTĐT là: sử dụng Agent vàkhông dùng Agent.

1) Phương án sử dụng Agent

Agent là một phần mềm cài đặt tại máy chủ chứa cổng TTĐT, làm nhiệm vụ thu thập dữ liệu về hoạt động và nguy cơ sự cố của cổng TTĐT. Agent có thể thu thập nhiều loại dữ liệu khác nhau, bao gồm các tệp nhật ký quan trọng của máy chủ Web như nhật ký truy nhập (Access Logs), nhật ký lỗi (Error Logs), nhật ký hệ thống (System Logs). Agent cũng có thể thu thập dữ liệu lưu lượng Web (request, response), trạng thái hoạt động của cổng TTĐT. Những dữ liệu thu thập sẽ được so khớp với các tập mẫu dấu hiệu để phát hiện các nguy cơ tấn côngvào cổng TTĐT.

2) Phương án không dùng Agent

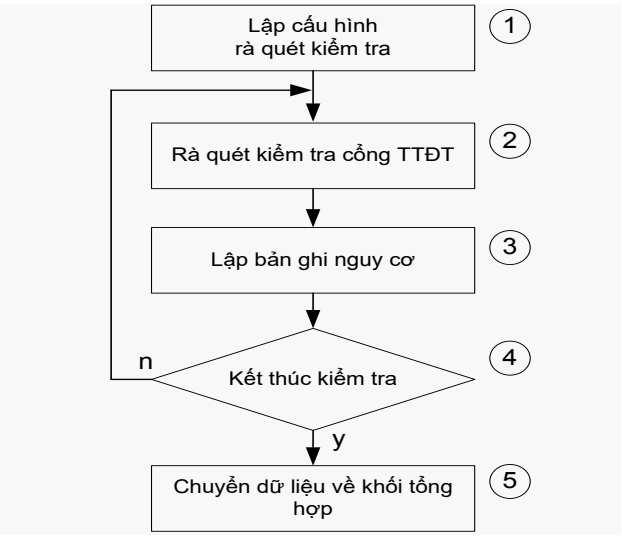
Phương án này có ưu điểm là không cần cài đặt phần mềm tại máy chủ chứa cổng TTĐT để thu thập dữ liệu. Dữ liệu về nguy cơ tấn công cổng TTĐT được thu thập theo hình thức gửi các câu truy vấn từ hệ thống giám sát để rà quét, kiểm tra và nhận phản hồi từ cổng TTĐT về các yêu cầu trên. Các câu truy vấn được thiết kế để thu thập dữ liệu theo 10 nhóm nguy cơ tấn công như đã nêu ở mục B. Lượng dữ liệu thu thập có thể không đầy đủ về hoạt động của máy chủ và cổng TTĐT, song vẫn có thể dùng cho theo dõi hoạt động, phân tích và phát hiện các nguy cơ tấn công điển hình nhất đối với cổng TTĐT theo 10 nhóm nêu trên.

Do ưu điểm trên, phương án không sử dụng Agent được đề xuất trong giải pháp kết hợp giám sát và đánh giá an toàn. Một công cụ phần mềm có tên là EpScan được phát triển nhằm mục đích thu thập dữ liệu theo 10 nhóm nguy cơ, phục vụ giám sát tập trung và đánh giá an toàn cổng TTĐT. Lưu đồ khối của phần mềm EpScan biểu thị trên Hình 2. Phần mềm EpScan gồm các bước chính như sau:

- Bước 1: Lập cấu trúc danh mục cần quét kiểm tra cho cổng TTĐT, lập danh mục nút dữ liệu, đặt thời gian quét.
- Bước 2: Thực hiện các câu truy vấn đọc nội dung phản hồi, trạng thái và các đoạn mã Script có thể bị cài trên cổng TTĐT. Chuẩn hóa định dạng dữ liệu theo các trường tin: Id, địa chỉ URL, nội dung bản tin trả về và mã lỗi xảy ra. Sử dụng các biểu thức chính tắc RegEx (Regular Expression) để kiểm tra phân tách trường tin và phát hiện nguy cơ tấn công.
- Bước 3: Tạo lập bản ghi nguy cơ tấn công theo các trường tin đã chuẩn hóa.
- Bước 4: Kết thúc rà quét kiểm tra khi đã quét hết cấu trúc cổng TTĐT theo danh mục đã lập ở bước 1 hoặc

khi hết thời gian quét đã lập (nhánh y) hoặc lặp lại bước 2 nếu chưa kết thúc (nhánh n).

- Bước 5: Chuyển tiếp dữ liệu về khối tổng hợp dữ liệu cho việc xử lý tiếp theo.



Hình 2. Lưu đồ phần mềm EpScan

D. Khối tổng hợp dữ liệu

Dữ liệu chuyển về khối này được chia tách vào các nút cơ sở dữ liệu tại trung tâm. Mỗi nút cơ sở dữ liệu có thể đặt kích thước là 1 GBytes. Quá trình tổng hợp dữ liệu có thêm bước làm sạch dữ liệu nhằm loại bỏ những dữ liệu có lỗi và dữ liệu không cần thiết cho quá trình phân tích, phát hiện và đánh giá an toàn. Ví dụ, có thể loại bỏ các bản ghi dữ liệu phản hồi từ cổng TTĐT với mã trạng thái là *200 OK* có đồng thời ký hiệu *"-"* trong trường tin *uri-query-node*. Các thử nghiệm cho thấy xác suất có chứa hành vi tấn công trong các bản ghi kiểu này hầu như bằng không, nên có thể loại bỏ bớt các bản ghi này.

Dữ liệu tổng hợp được chuẩn hóavà gán nhãn với tiêu đề định danh để đánh chỉ số và phần thân dữ liệu bao gồm 300 bytes. Một đoạn mã Script được dùng để chuyển các bản tin sự kiện có đánh nhãn vào các nút cơ sở dữ liệu. Giải pháp có thể dùng ở đây là phần mềm nguồn mở Elasticsearch (*https://www.elastic.co/elastic search/*) hoặc Logstash (*https://www.elastic.co/logs-tash*) hoặc đơn thuần là các nút cơ sở dữ liệu tạo lập với MongoDB (*https://www.mongodb.com/*).Đây là các phần mềm nguồn mở cho phép kết hợp và thao tác nhiều kiểu tìm kiếm dữ liệu theo các tiêu chí mong muốn với tốc độ xử lý nhanh theo thời gian thực (xem ví dụ [35]). Elasticsearch là một cỗ máy tìm kiếm phân tán kiểu RESTful, cho phép tìm kiếm phân tán với tốc độ cao qua các giao diện API. Logstash là một phần mềm nguồn mở cho phép xử lý các bản tin sự kiện qua UNIX pipeline, tập hợp dữ liệu đồng thời từ nhiều nguồn, chuyển đổi dữ liệu và cho phép tìm kiếm dữ liệu với tốc độ cao. Lưu trữ với các nút cơ sở dữ liệu MongoDB cũng là một giải pháp đơn giản, khả thi.

E. Khối theo dõi, giám sát

Khối này có nhiệm vụ so khớp các dữ liệu tổng hợp đã thu được với các mẫu dữ liệu dấu hiệu sẵn có để phát hiện nguy cơ tấn công. Các tập mẫu dấu hiệu và cơ chế phát hiện đều sử dụng chuẩn biểu thức chính tắc RegEx (*Regular Expression*). Các tập mẫu dấu hiệu có thể tải về từ các nguồn có sẵn, điển hình như: *https://rules.emergingthreats.net*, hay *https://github.com/emposha/ PHP-Shell-Detector*. Đây là những tập luật nguồn mở, có cập nhật thường xuyên cho các nguy cơ tấn công mới.

Tập mẫu dấu hiệu có sẵn được dùng để so khớp có thể phát hiện các lỗi tương ứng với 10 nhóm nguy cơ tấn công đã nêu ở mục B, cụ thể như các nguy cơ tấn công điển hình sau:

- Injection: SQL Injection, XML Injection, PHP Injection, LDAP Injection,…
- XSS attack.
- Data leakage
- Config file access
- Remote code execution
- Directory traversal
- Web scan
- Web shell
- …

Ví dụ về một cấu trúc RegEx dùng để kiểm tra phát hiện nguy cơ tấn công được biểu thị trên Hình 3.

```
SUSPICIOUS_HTTP_REQUEST_REGEXES = (
    ("potential sql injection",
     r"information_schema|sysdatabases|sysusers|floor\(rand\(|ORD
     \d+|\bUNION\s+(ALL\s+)?SELECT\b|\b(UPDATEXML|EXTRACTVALUE)\(
     ERT\(|VARCHAR\(|\bCOUNT\(\*\)|\b(pg_)?sleep\(|\bSELECT\b.*\F
     \w+|\b(AND|OR|SELECT)\b.*/\*.*\*/|/\*.*\*/.*\b(AND|OR|SELECT
     ]?\d+|ODBC;DRIVER|\bINTO\s+(OUT|DUMP)FILE"),
    ("potential xml injection", r"/text\(\)='"),
    ("potential php injection", r"<\?php"),
    ("potential ldap injection", r"\(\|\(\w+=\*"),
    ("potential xss injection",

     r"<script.*?>|\balert\(|(alert|confirm|prompt)\((\d+|docume
     us)=[^&;\n]+\("),
    ("potential xxe injection", r"\[<!ENTITY"),
    ("potential data leakage",

     r"im[es]i=\d{15}|(mac|sid)=([0-9a-f]{2}:){5}[0-9a-f]{2}|sim
     "),
    ("config file access", r"\.ht(access|passwd)|\bwp-config\.ph
    ("potential remote code execution",
     r"\$_(REQUEST|GET|POST)\[|xp_cmdshell|\bping(\.exe)? -[nc] '
     /tmp/|cmd\.exe|/bin/bash|2>&1|\b(cat|ls) /|chmod [0-7]{3,4}'
     (allow_url_include|safe_mode|auto_prepend_file)"),
    ("potential directory traversal",
     r"(\.{2,}[/\\]+){3,}|/etc/(passwd|shadow|issue|hostname)|[/'
     ),
```

Hình 3. Ví dụ về cấu trúc RegEx trong HTTP request

Ví dụ cho hai bản ghi dữ liệu phản hồi từ cổng TTĐT có nguy cơ tấn công XSS như sau:

203.162.165.173 - - [12/Mar/2019:22:31:12 -0500]"GET /foo.jsp?<SCRIPT>foo</SCRIPT>.jsp HTTP/1.1" 200 578 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

203.162.165.173 - - [12/Mar/2019:23:37:17 -0500] "GET /cgi- bin/cvslog.cgi?file=<SCRIPT>window. alert </SCRIPT > HTTP/1.1" 403 302 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

Hình 4. Ví dụ về hai bản ghi nguy cơ tấn công

Cả hai bản ghi đều có yêu cầu truy nhập chéo sang trang Nessus. Ở bản ghi thứ nhất, mã trạng thái phản hồi của cổng TTĐT là *200 OK*. Điều đó nghĩa là đoạn mã Script *foo.jsp* đã thực hiện. Ở bản ghi thứ 2, ta thấy cổng TTĐT từ chối với phản hồi *403 Forbidden*, nghĩa là cổng

TTĐT đã ngăn chặn được nguy cơ tấn công chuyển sang trang mã độc.

Hình 5 là ví dụ về hai bản ghi dữ liệu có nguy cơ tấn công chèn nội dung mã độc. Bản ghi thứ nhất là nhóm nguy cơ thứ 6 (xem mục B) về cấu hình bảo mật không an toàn với mức độ nguy cơ cao (*Severity=3*). Bản ghi thứ 2 là nhóm nguy cơ thứ 4 (xem mục B) về tham chiếu đến đối tượng bên ngoài không an toàn gồm 3 nguy cơ với mức độ cao (*Severity = 3*).

Hình 5. Ví dụ về hai bản ghi dữ liệu nguy cơ tấn công chèn nội dung mã độc

F. Khối đánh giá mức độ an toàn

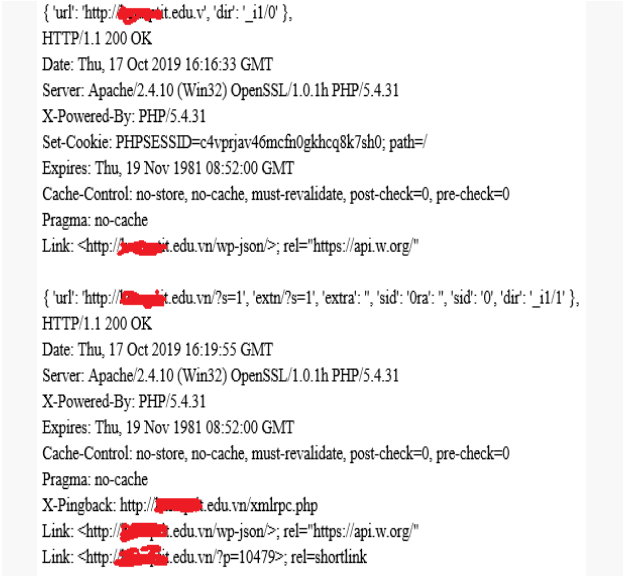
Theo mô hình trong chuẩn ISO 15408 [13],đích đánh giá (TOE - Target Of Evaluation) là cổng TTĐT cần đánh giá. TOE được mô tả bằng các yêu cầu an toàn. Tập các yêu cầu an toàn được xây dựng thành một hồ sơ bảo vệ (PP - Protection Profile) chứa các yêu cầu an toàn cho các loại cổng TTĐT nói chung. Đích an toàn (ST - Security Target) được xây dựng cho một TOE cụ thể dựa theo các yêu cầu an toàn liệt kê trong tập PP và trong môi trường hoạt động cụ thể. Đặc trưng của mô hình là có 11 lớp chứa các yêu cầu chức năng an toàn (SFR- Security Function Requirement). Mỗi lớp đặc trưng cho một nhóm yêu cầu an toàn cho một chức năng cụ thể, điển hình như lớp bảo vệ dữ liệu người dùng, lớp mã hóa dữ liệu, lớp xác thực định danh, v.v. Tập các yêu cầu chức năng an toàn được coi là các tiêu chí chung (Common Criteria).

Để đánh giá mức độ an toàn cho cổng TTĐT, khối đánh giá mức độ an toàn thực hiện truy xuất dữ liệu đã lưu trong khối tổng hợp dữ liệu, ánh xạ vào một tập đích an toàn (Security Target) được tạo theo mẫu của hồ sơ bảo vệ (Protection Profile).Tiếp đó, hệ thống sẽ tính điểm cho từng lớp chức năng an toàn dựa theo tập mẫu của hồ sơ bảo vệ. Mức độ an toàn của cổng TTĐT được tính bằng tổng điểm có trọng số của các lớp chức năng an toàn. Sau đây là mô tả cách tạo hồ sơ bảo vệ theo chuẩn, cách xác định trọng số cho các lớp và cách đánh giáđịnh lượng mức độ an toàn.

1) Tạo hồ sơ bảo vệ theo chuẩn

Cổng TTĐT được đánh giá định lượng mức độ an toàn dựa theo dữ liệu về 10 nhóm nguy cơ đã thu thập được tương ứng với CCWAPSS [12] và bộ tiêu chí chung trong ISO 15408 [13].

Để thực hiện đánh giá theo chuẩn, bước đầu tiên cần tạo một hồ sơ bảo vệ (PP) cho cổng TTĐT. Căn cứ vào 10 nhóm nguy cơ đã mô tả ở mục B và 11 lớp chức năng an toàn của chuẩn, ta lập được hồ sơ bảo vệ là một ma trận gồm 82 hàng và 73 cột. Các hàng tương ứng với 82 tập hợp các nguy cơ có thể kiểm tra được với công cụ phần mềm EpScan đã nêu ở mục C, trong đó, mỗi tập hợp có thể gồm nhiều nguy cơ. Hình 6 là một ví dụ về một tập hợp nguy cơ tấn công XSS thu thập được với 2 nguy cơ.



Hình 6. Ví dụ về một tập hợp nguy cơ tấn công XSS với hai nguy cơ

Các cột của ma trận hồ sơ bảo vệ biểu thị các thành phần của 11 lớp chức năng an toàn theo ISO 15408 [13], cụ thể như sau (con số trong dấu ngoặc là số thành phần của mỗi họ trong một lớp):

- Lớp kiểm toán (FAU- Function Audit) có 6 họ là ARP(1), GEN(2), SAA(2), SAR(3), SEL(1), STG(1).

- Lớp truyền thông (FCO-Function Communi-cation) có 2 họ là NRO(3), NRR(3).

- Lớp hỗ trợ mật mã (FCS-Function Cryptogprahy Support) có 2 họ là CKM(2), COP(1).

- Lớp bảo vệ dữ liệu (FDP-Function Data Protection) có 11 họ là ACC(1), ACF(3), DAU(2), ETC(2), IFC(2), IFF(4), ITC(2), ITT(1), SDI(1), UCT(1), UIT(1).

- Lớp xác thực định danh (FIA-Function Identification Authentication) có 4 họ là AFL(1), ATD(1), UAU(2), UID(1).

- Lớp quản lý an toàn (FMT-Function Security Management) có 6 họ là MOF(1), MSA(2), MTD(1), SAE(1), SMF(1), SMR(1).

- Lớp riêng tư (FPR-Function Privacy) có 3 họ là ANO(1), UNL(1), UNO(1).

- Lớp bảo vệ chức năng an toàn TOE (FPT-Function TSF protection) có 7 họ là FLS(1), ITA(1), ITC(1), ITI(1), ITT(1), PHP(1), RCV(1).

- Lớp sử dụng tài nguyên (FRU- Function Resource Utilisation) có 2 họ là FLT(1), RSA(1).

- Lớp truy nhập TOE (FTA- Function TOE Access) có 4 họ là LSA(1), MCS(1), SSL(1), TSE(1).

- Lớp tuyến tin cậy (FTP- Function Trusted Path) có 2 họ là ITC(3), TRP(3).

Hồ sơ bảo vệ tạo thành một tập mẫu dùng cho đánh giá an toàn, mỗi ô được gán giá trị "0" hoặc "1" tùy theo tác động của nguy cơ tới các thành phần của lớp. Giá trị "0" thể hiện nguy cơ không ảnh hưởng đến thành phần

tương ứng của lớp. Ngược lại, giá trị "1" thể hiện nguy cơ có tác động đến thành phần của lớp tương ứng.

Các tập hợp nguy cơ được sắp xếp vào 5 nhóm: cụ thể là: rất nghiêm trọng (*highcritical*), nghiêm trọng (*critical*), trung bình (*medium*), cảnh báo (*warning*) và cần lưu ý (*alert*). Mỗi nhóm được gán một hệ số khác nhau thể hiện mức độ nghiêm trọng của từng nhóm nguy cơ. Các hệ số cụ thể là h_1, h_2, h_2, h_4, h_5, với $h_1 > h_2 > h_3 > h_4 > h_5$. Trong đó, h_1 ứng với nhóm rất nghiêm trọng, h_5 ứng với nhóm ít nghiêm trọng nhất. Kết quả dữ liệu thu thập từ cổng TTĐT cho mỗi lớp yêu cầu chức năng an toàn có thể bao gồm một vài hoặc cả 5 nhóm nêu trên. Trong hệ thống kết hợp giám sát và đánh giá đã đề xuất, ta đặt các hệ số như sau: $h_1=1.5$, $h_2=1.4$, $h_2=1.3$, $h_4=1.2$, $h_5=1.1$dựa vào kết quả thử nghiệm với gần 200 cổng TTĐT.

2) Xác định trọng số cho các lớp chức năng an toàn

Các lớp chức năng an toàn có thể có mức độ quan trọng khác nhau. Do đó, có thể đặt các trọng số để phản ánh các mức độ đó trong kết quả đánh giá chung cho cổng TTĐT. Ví dụ, đối với cổng TTĐT, lớp FDP được coi quan trọng hơn lớp FCO, lớp FAU quan trọng hơn lớp FTP, v.v. Ta có thể sử dụng các trọng số w_i để gán cho mỗi lớp i của 11 lớp chức năng an toàn.

Các trọng số là cần thiết, song việc xác định trọng số phù hợp có ảnh hưởng đáng kể đến kết quả đánh giá. Vì vậy, ta chọn phương pháp tiến trình thứ bậc phân tích (AHP- Analytic Hierarchy Process) [36] để tính toán các trọng số w_i. Tiến trình AHP bao gồm 4 bước chính như sau:

1- Xây dựng cây phân cấp AHP và ma trận so sánh tiêu chí

2- Tính toán các trọng số

3- Kiểm tra tính nhất quán

4- Tổng hợp kết quả trọng số

Sau đây là chi tiết các bước.

Bước 1. Xây dựng cây phân cấp AHP và ma trận so sánh tiêu chí

Từ kết quả khảo sát với gần 200 cổng TTĐT và để giảm độ phức tạp tính toán, ta chọn ra 6 tiêu chí X_1,X_2, X_3,X_4,X_5,X_6cho phân cấp AHP ứng với các lớp chức năng an toàn đã nêu ở mục F.1) như sau.

Tiêu chí X_1 cho lớp FDP

Tiêu chí X_2 cho các lớp FAU, FMT, FPT

Tiêu chí X_3 cho lớp FTA

Tiêu chí X_4 cho các lớp FCO, FTP, FIA

Tiêu chí X_5 cho các lớp FRU, FPR

Tiêu chí X_6 cho lớp FCS

Hình 7. Lựa chọn 6 tiêu chí cho AHP

Ma trận so sánh cho 6 tiêu chí được xây dựng như sau:

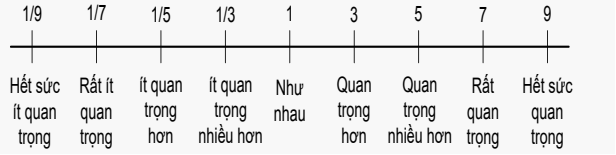
$$A = \left(a_{ij}\right)_{6x6}$$

$$= \begin{Bmatrix} 1 & a_{12} & a_{13}a_{14} & a_{15} & a_{16} \\ a_{21} & 1 & a_{23}a_{24} & a_{25} & a_{26} \\ \vdots & \vdots & \vdots \ \vdots & \vdots & \vdots \\ a_{61} & a_{62} & a_{63}a_{64} & a_{65} & 1 \end{Bmatrix} \quad (4)$$

Mỗi phần tử a_{ij} thể hiện mức độ quan trọng của tiêu chí hàng i so với tiêu chí cột j. Mức độ quan trọng tương đối của tiêu chí i so với j được tính với k (k =*1, 3, 5, 7, 9*), ngược lại của tiêu chí j so với i được tính với *1/k* (nghĩa là *1, 1/3, 1/5, 1/7, 1/9*).

Như vậy, ma trận so sánh gồm các phần tử: $a_{ij} > 0$, $a_{ji} = 1 / a_{ij}$ và $a_{ii} = a_{jj} = 1$.

Thang điểm so sánh mức độ quan trọng của các tiêu chí theo phương pháp AHP như sau.



Hình 8. Thang điểm mức độ quan trọng

Từ thang điểm trên, ta lập được ma trận so sánh AHP theo 6 tiêu chí X_1,X_2, X_3,X_4,X_5,X_6như sau.

Bảng 1. Ma trận so sánh

	X_1	X_2	X_3	X_4	X_5	X_6
X_1	1	3	5	7	7	9
X_2	1/3	1	3	5	5	7
X_3	1/5	1/3	1	3	5	7
X_4	1/7	1/5	1/3	1	3	5
X_5	1/7	1/5	1/5	1/3	1	3
X_6	1/9	1/7	1/7	1/5	1/3	1

Bước 2. Tính toán các trọng số

Thực hiện các bước tính toán theo phương pháp AHP, cụ thể là:

- Tính tổng các cột của ma trận so sánh: Sum_j, với $j$là chỉ số cột, $j = 1 \ldots 6$.
- Chuẩn hóa trọng số theo công thức:

$$c_{ij} = a_{ij} / Sum_j \quad (5)$$

- Tính trọng số trung bình theo công thức:

$$w_i = \frac{\sum_{j=1}^{6} c_{ij}}{6} \quad (6)$$

Thực hiện các bước trên, ta tính được kết quả cho các trọng số như sau:

$w_1 = 0.3984$ $w_2 = 0.2151$ $w_3 = 0.1371$

$w_4 = 0.0762$ $w_5 = 0.0450$ $w_6 = 0.0248$

Bước 3. Kiểm tra tính nhất quán

Theo [36], tính nhất quán của các trọng số được kiểm tra với các giá trị *Lambda max* (λ_{max}), chỉ số nhất quán CI (*Consistency Index*), tỷ số nhất quán CR (*Consistency Ratio*). Giá trị λ_{max} được tính như sau.

$$\lambda_{max} = \frac{\sum_{j=1}^{6} w_j . Sum_j}{6} (7)$$

Từ giá trị Sum_j và w_j, ta tính được: λ_{max} = 6.1574

Theo AHP [36], chỉ số nhất quán CI (*Consistency Index*) được tính theo công thức:

$$CI = \frac{\lambda_{max} - n}{n-1} \quad (8)$$

Trong đó *n* là số tiêu chí.

$$\rightarrow \quad CI = \frac{\lambda_{max} - 6}{6-1} = \frac{6.1574 - 6}{5} = 0.0315 \quad (9)$$

Tỷ số nhất quán CR (*Consistency Ratio*) được tính theo công thức [36]:

$$CR = CI / RI \quad (10)$$

Trong đó RI là chỉ số ngẫu nhiên (*Random Index*).

Với 6 tiêu chí, ta có thể sử dụng bảng tham số trong [36] để chọn RI = 1.24

Tỷ số CR sẽ là:

$$CR = 0.0315 / 1.24 = 0.0254 \quad (11)$$

Kết quả CR = 0.0254 nhỏ hơn 0.1.Do vậy, theo phương pháp AHP [36] ta có thể kết luận là các trọng số đã tính được là phù hợp, chấp nhận được.

Bước 4. Tổng hợp kết quả trọng số

Trọng số cho các lớp chức năng an toàn được tổng hợp trong Bảng 2 như sau.

Bảng 2. Trọng số cho các lớp

Lớp chức năng an toàn	Trọng số
FAU	$w_2 = 0.2151$
FCO	$w_4 = 0.0762$
FCS	$w_6 = 0.0248$
FDP	$w_1 = 0.3984$
FIA	$w_4 = 0.0762$
FMT	$w_2 = 0.2151$
FPR	$w_5 = 0.0450$
FPT	$w_2 = 0.2151$
FRU	$w_5 = 0.0450$
FTA	$w_3 = 0.1371$
FTP	$w_4 = 0.0762$

3) Xác định mức độ an toàn cho cổng TTĐT

Như đã nêu ở phần đầu mục F, các bước tạo hồ sơ bảo vệ theo chuẩn và xác định trọng số cho các lớp chỉ cần thực hiện một lần ban đầu khi thiết lập hệ thống đánh giá.

Quá trình đánh giá mức độ an toàn cho cổng TTĐT bao gồm các bước chính như sau.

- Bước 1: Truy xuất tập dữ liệu đã thu thập lưu trong cơ sở dữ liệu (khối tổng hợp dữ liệu), ánh xạ dữ liệu vào một tập đích an toàn (ST- Security Target) được tạo theo mẫu của hồ sơ bảo vệ (Protection Profile). Mỗi tập dữ liệu tương ứng với một lần quét kiểm tra cổng TTĐT do khối thu thập dữ liệu cung cấp.
- Bước 2: Từ bảng dữ liệu của tập đích an toàn ST, thực hiện tính điểm đánh giá cho từng lớp chức năng an toàn$F_k$theo công thức (12), cụ thể như sau.

$$F_k = h_1 \sum_{n=1}^{N_1} \sum_{i=1}^{M_k} P_{i,k} (12)$$
$$+ h_2 \sum_{n=1}^{N_2} \sum_{i=1}^{M_k} P_{i,k}$$
$$+ h_3 \sum_{n=1}^{N_3} \sum_{i=1}^{M_k} P_{i,k}$$
$$+ h_4 \sum_{n=1}^{N_4} \sum_{i=1}^{M_k} P_{i,k}$$
$$+ h_5 \sum_{n=1}^{N_5} \sum_{i=1}^{M_k} P_{i,k}$$

Trong đó:

F_k là điểm đánh giá cho lớp *k*

$P_{i,k}$ là giá trị điểm của mỗi thành phần *i* thuộc lớp *k* đã gán trong hồ sơ bảo vệ, với *k = 1…11*

M_k là số thành phần có trong mỗi lớp *k*

*n*là từng nguy cơ tấn côngđã kiểm tra được và ghi trong tập đích an toàn ST.

N_k là tổng số nguy cơ tấn côngtrong mỗi tập hợp nhóm nguy cơ.

Các giá trịh_1, h_2, h_2, h_4, h_5, là hệ số của các tập hợp nhóm nguy cơ tương ứng.

- Bước 3: Với các trọng số cho các lớp chức năng an toàn đã thiết lập (xem phần F.2 ở trên), ta tính được tổng điểm đánh giá cho cổng TTĐT như sau.

$$F = \sum_{k=1}^{11} w_k F_k \quad (13)$$

Trong đó,*F* là điểm đánh giá (mức độ an toàn) của cổng TTĐT,w_k là trọng số của lớp F_k với *k = 1…11*.

Từ các trọng số trong Bảng 2, ta có:

$$F = w_1 F_{FDP} + w_2 (F_{FAU} + F_{FMT} + F_{FMT})$$
$$+ w_3 F_{FTA}$$
$$+ w_4 (F_{FCO} + F_{FTP} + F_{FIA})$$
$$+ w_5 (F_{FRU} + F_{FPR})$$
$$+ w_6 F_{FCS}$$

Trong đó, các giá trị F_{FDP}, F_{FAU}, F_{FMT}, F_{FPT}, F_{FTA}, F_{FCO}, F_{FTP}, F_{FIA}, F_{FRU}, F_{FPR}, F_{FCS} là điểm đánh giá của từng lớpnhư liệt kê trong Bảng 2.

Các tác giả bài báo đã thực hiện thử nghiệm giải pháp cho gần 200 cổng TTĐT. Kết quả thử nghiệm cho thấy giải pháp kết hợp giám sát và đánh giá là khả thi, cho phép xác định mức độ an toàn cho từng cổng TTĐT, đặc biệt là cho phép so sánh mức độ an toàn giữa các cổng TTĐT.

Để minh họa kết quả đánh giá, chúng tôi chọn ra hai cổng TTĐT (ký hiệu là cổng TTĐT A và cổng TTĐT B). Từ tập dữ liệu thu thập được từ các cổng TTĐT đã lưu trong khối tổng hợp dữ liệu cho lần quét kiểm tra, hệ thống tính được các điểm đánh giá cho các lớp chức năng an toàn của hai cổng TTĐT A và cổng TTĐT B như biểu thị trọng Bảng 3.Với các trọng số cho các lớp đã xác định ở phần trên, ta tính được điểm đánh giá cho các cổng TTĐT A và cổng TTĐT B là:

$F_A = 69.84, F_B = 62.36$

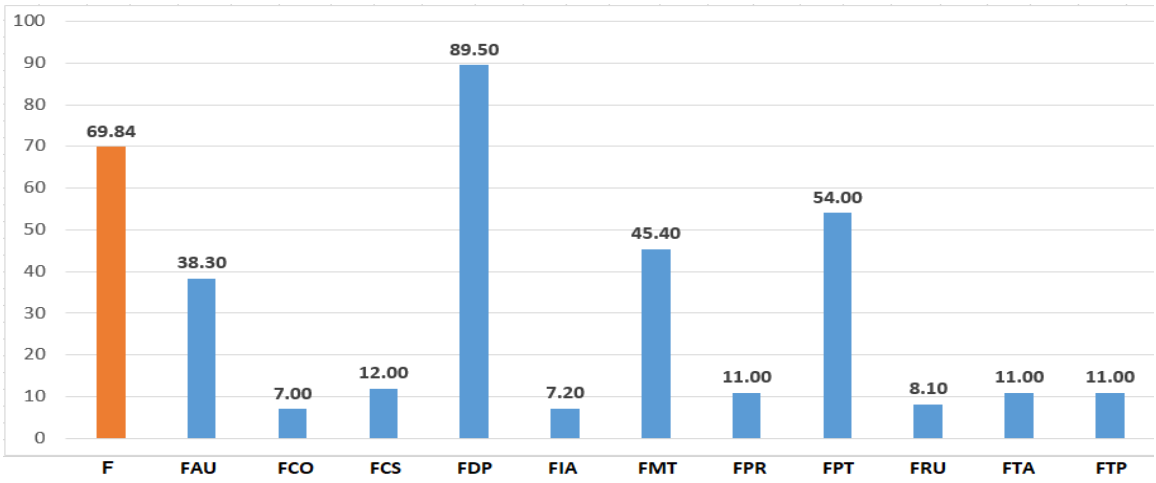
Hình 9 và Hình 10 là kết quả thử nghiệm đánh giá mức độ an toàn cho hai cổng TTĐT đã chọn. Giá trị F_A và F_B được biểu thị bằng cột màu đậm ngoài cùng bên trái các hình (biểu thị bằng ***F***). Các cột còn lại là điểm đánh giá cho từng lớp của mỗicổng TTĐT.

Đồ thị được biểu diễn trên thang điểm 100. Giá trị 100% là tốt nhất. Với cổng TTĐT A, giá trị FDP là an toàn nhất (89.50%), giá trị FCO là kém an toàn nhất (7.00%). Đối với cổng TTĐT B, giá trị FDP là an toàn nhất (72.30%), giá trị FPR là kém an toàn nhất (14.30%).

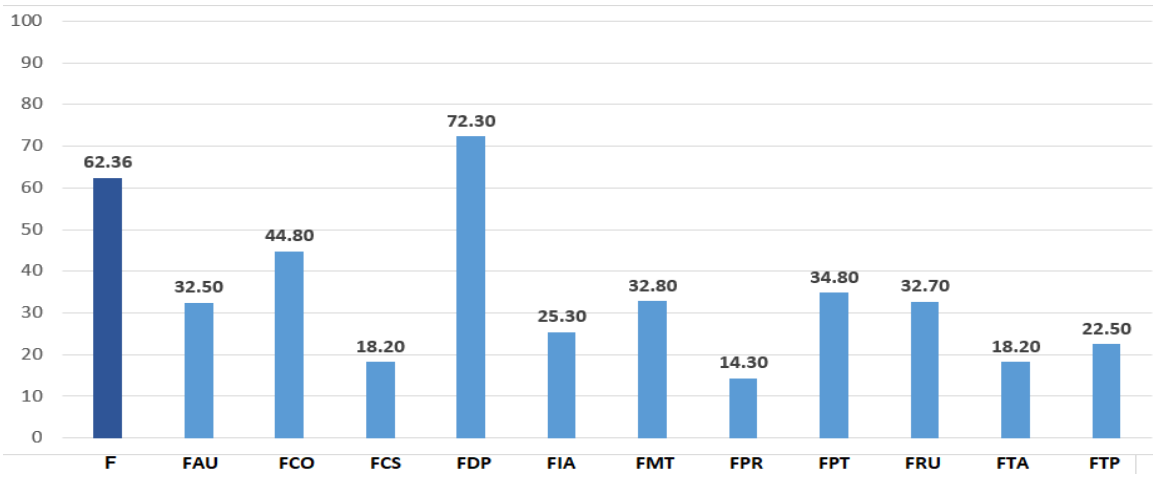
Như đã nêu, bên cạnh khả năng đánh giá mức độ an toàn cho từng lớp chức năng và cho toàn bộ cổng TTĐT, ta còn có thể so sánh mức độ an toàn giữa các cổng TTĐT. Như trong ví dụ đã nêu, cổng TTĐT A được đánh giá là an toàn hơn cổng TTĐT B, do $F_A = 69.84 > F_B = 62.36$.

Bảng 3. Kết quả điểm đánh giá cho hai cổng TTĐT A và cổng TTĐT B

Lớp chức năng an toàn	Điểm cho cổng TTĐT A	Điểm cho cổng TTĐT B
FDP	*38.30*	*32.50*
FCO	*7.00*	*44.80*
FCS	*12.00*	*18.20*
FDP	*89.50*	*72.30*
FIA	*7.20*	*25.30*
FMT	*45.40*	*32.80*
FPR	*11.00*	*14.30*
FPT	*54.00*	*34.80*
FRU	*8.10*	*32.70*
FTA	*11.00*	*18.20*
FTP	*11.00*	*22.50*



Hình 9. Điểm đánh giá các lớp chức năng an toàn của cổng TTĐT A



Hình 10. Điểm đánh giá các lớp chức năng an toàn của cổng TTĐT B

IV. KẾT LUẬN

Giám sát và đánh giá an toàn cho cổng TTĐT là hai nhiệm vụ thường không tách rời khi xem xét mức độ an toàn của cổng TTĐT, song tới nay vẫn chưa có giải pháp nào quan tâm đồng thời đến điều này. Bài báo đề xuất một giải pháp kết hợp giám sát tập trung và đánh giá an toàn cho cổng TTĐT. Nguồn dữ liệu thu thập cho giám sát và đánh giá được thiết kế phù hợp với 10 nhóm nguy cơ đã được công bố trong chuẩn OWASP Top 10, đồng thời tương thích với 11 lớp chức năng an toàn của chuẩn ISO 15408. Việc kết hợp này mang lại hiệu quả và lợi ích vì tận dụng được nguồn dữ liệu giám sát thu thập được, cho phép sử dụng dữ liệu thu thập được để đánh giá mức độ an toàn và so sánh mức độ an toàn giữa các cổng TTĐT.

Mặt khác, hầu hết các giải pháp đánh giá hiện có vẫn chủ yếu là định tính, chưa theo tiêu chuẩn, còn phụ thuộc vào chủ quan của chuyên gia đánh giá. Do đó, bài báo đã đề xuất giải pháp đánh giá định lượng theo chuẩn ISO 15408. Phương thức AHP đã được áp dụng để xác định các trọng số phù hợp cho các lớp chức năng an toàn theo chuẩn. Sử dụng nguồn dữ liệu thu thập được từ cổng TTĐT, hệ thống thực hiện ánh xạ vào tệp đích an toàn theo chuẩn dựa theo một tập mẫu hồ sơ bảo vệ thiết lập ban đầu. Trên cơ sở đó, hệ thống tính điểm đánh giá cho từng lớp, tính điểm tổng các lớp theo trọng số đã xác định để đưa ra mức đánh giá an toàn cho cổng TTĐT. Kết quả đánh giá cho thấy tính khả thi của giải pháp, đưa ra mức độ an toàn định lượng, khách quan và đáp ứng nhu cầu so sánh mức độ bảo đảm an toàn giữa các cổng TTĐT.

LỜI CẢM ƠN

Bài báo được thực hiện trong khuôn khổ đề tài cấp Nhà nước mã số KC.01.08/16-20 của Bộ Khoa học và Công nghệ. Một phần tài trợ từ đề tài ASEAN IVO "A Hybrid Security Framework for IoT Networks" của Viện NICT (Nhật Bản).Các tác giả xin trân trọng cảm ơn các nguồn tài trợ cho nhóm thực hiện nghiên cứu.

TÀI LIỆU THAM KHẢO

[1] R. Bejtlich, The Tao of Network Security Monitoring Beyond Intrusion Detection, Addison Wesley, 2004.

[2] L. Heberlein, G. Dias, K. Levitt, B. Mukherjee, J. Wood, and D. Wolber, "A Network Security Monitor," Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, pp. 296–304 (May 1990).

[3] K.Alhamazani, et.al., An Overview of the Commercial Cloud Monitoring Tools: Research Dimensions, Design Issues and State-Of-The-Art. Journal Computing, Vol 97, Issue 4, Apr.2015, pp.357-377.

[4] M. Kolomeec, A. Chechulin, A. Pronoza, I. Kotenkom.Technique of Data Visualization: Example of Network Topology Display for Security Monitoring. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 7:1 (Mar. 2016), pp. 58-78.

[5] A. Ghaleb, I. Tracre, K. Ganame. A Framework Architecture for Agentless Cloud Endpoint Security Monitoring. Proc. of IEEE Conference on Communications and Network Security (CNS) 2019, 10-12 June 2019.

[6] I. Sharafa, A.H. Lashkari, A.A. Ghorbani. An Evaluation Framework for Network Security Visualizations. Computers & Security, Vol. 84, July 2019, pp. 70-92.

[7] Y. Suna, H. Wang. Intelligent Computer Security Monitoring Information Network Analysis. Proc. of IEEE Conference on Communications and Network Security (CNS) 2019, 10-12 June 2019.

[8] H. Haywood. Web portal for managing premise security. US Patent No. 14,154,096 A1. US Patents May. 2014.

[9] M.J. Ranum, R.Gula. System and Method for Strategic Anti-malware Monitoring. US Patent No. 9,088,606 B2. US Patents Jul. 2015.

[10] N.M.Daswani, A.Ranadive, S.Rizvi. Monitoring forProblems and Detecting Malware. US Patent No. 9,154,364 B2. US Patents Apr. 2015.

[11] J.Ngoc Ki Pang, N.Yadav, et.al. Application Monitoring Prioritization. US Patent No. 15,173,477 A1. US Patents Dec. 2016.

[12] F. Charpentier. Common Criteria Web Application Security Scoring(CCWAPSS).Technical Report. November 2007, http://www.xmco.fr/whitepapers/ccwapss_1.1.pdf

[13] ISO/IEC 15408. Information technology - Security Techniques-Evaluation criteria for IT security; Part 1: Introduction and General Model; Part 2:Security Functional Components; Part 3: Security Assurance Components.https://www.iso.org/standard/, 2010.

[14] J. Fonseca, M.Vieira, H.Madeira. Evaluation of Web Security Mechanisms Using Vulnerability & Attack Injection. IEEE Transactions on Dependable and Secure Computing, Vol 11, Issue 5, Sept.-Oct. 2014, pp.440-453.

[15] Y. Zhou, D. Evans. Understanding and Monitoring Embedded Web Scripts. IEEE Symposium on Security and Privacy, 2015, pp. 850-865.

[16] J.Pandey, M.Jain. An Analytical study and synthesis on Web server security. COMPUSOFFT, Intl. Jourrnal of advanced computer technology 4(4), April 2015, pp.1690-1694.

[17] A.R. Cavalli, A.Benameur, W.Mallouli, K. Li. A Passive Testing Approach for Security Checking and its Practical Usage for Web Services Monitoring.Proc. of Conférence Internationale sur Les NOuvelles TEchnologies de la REpartition, June 2016.

[18] Y.L. Ruan , X.Q. Yan. Research on Key Technology of Web Application Security Test Platform. Proc. of Intl. Conference onEducation, Management and Social Science (EMSS) 2018, pp.218–223.

[19] L. Heberlein, K. Levitt, B. Mukherjee. Internetwork Security Monitor: An Intrusion-Detection System for Large-Scale Networks. Proc. of the 15th National Information Systems Security Conference, Oct. 1992, pp. 262–271.

[20] M. Trecka, et.al. Network Security and Surveillance system. US Patent No. 6,453,345. US Patents 2002.

[21] T.Drees, L.Rachitsky, D.Taylor. Systems and Methods for Isolating Local Performance Variation in Website Monitoring. US Patent No. 7,546,368 B2. US Patents Jun. 2009

[22] R. Simon, L. Ahuja. Website monitoring: Contemporary Way to Test and Verify. Global Journal of Enterprise Information System, January-June 2012, Volume-4 Issue-I.

[23] U.Erlingsson, Y.Xie, B.Livshits, C.Fournet. Enhanced Security and Performance of Web Applications, US Patent No. 8,677,141 B2. US Patents Mar. 2014.

[24] L.V.Goldspink, M.Ducket. Website Monitoring and Cookie Setting. US Patent No. 8,880,710 B2. US Patents Nov. 2014.

[25] D.H. Hoang, T.N. Pham. Evaluating the Security Levels of the Web-Portals Based on the Standard ISO/ IEC 15408. Proc. of Intl. Symposium on Information and Communication Technology (SoICT) 2018, Dec. 2018, pp. 463-469.

[26] A. Richard. Evaluation of the Security of Components in Distributed Information Systems. TR. LITH-ISY-EX-3430-2003, LinköpingUniversity, Sweden (2003).

[27] M. Peterson. CAESAR- A Proposed Method for Evaluating Security inComponent-based Distributed Information Systems.TR. LITH-ISYEX-3581-2004, Linköping University, Sweden. 2004.

[28] J. Hallberg, A. Hunstad, M. Peterson. A Framework for System Security Assessment. Proc. of the Sixth Annual IEEE Information Assurance Workshop (IAW'05), 2005, pp.224–231.

[29] J. Williams. OWASP Testing Guide 3.0, OWASP Foundation.http://www.owasp.org/index.php/OWASP_Testing_Guide. 2008.

[30] A. Petukhov, D. Kozlov. Detecting Security Vulnerabilities in Web Applications Using Dynamic Analysis with Penetration Testing. Proc. of OWASPApplication Security, Europe 2008 Conference, June 2008, pp.1–16.

[31] M. Pistoia, O. Segal, O. Tripp. Detecting Security Vulnerabilitiesin Web Applications. US Patent US13174628. US Patents 2011.

[32] W.Pei, N. Chen, D.Litong. Online XSS Testing Tool Based onPHP. Journal of Modern Electronics Techniques 20 (2015), pp.41–43.

[33] Y. Zhou, D.Evans. SSOScan: Automated Testing of Web Applications for Single Sign-On Vulnerabilities. IEEE Proceedings of the 23rdUSENIX Security Symposium, San Diego, CA, 2014, pp.495–510.

[34] OWASP Projects. https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/

[35] C. Vega, P. Roquero, et.al. Loginson: A Transform and Load System for Very Large Scale Log Analysis in Large IT Infrastructures. Journal of Supercomputing. Springer.No.7, Mar. 2017.

[36] L.T. Saaty. The Analytic Hierarchy Process, McGraw-Hill International, New York, 1980.

COMBINED SOLUTION FOR SECURITY MONITORING AND EVALUATION OF WEB-PORTALS USING STANDARDIZATION

Abstract: Security monitoring and security evaluation are two tasks that seam to be separate, but have a close relationship with each other. Most of the known solutions often focus on either one of these two tasks. On the other hand, there is still no solution to this problem using a published standard. This paper proposes a combined solution for security monitoring and security evaluation of Web-Portals using starndardization, namely the standard ISO 15408. The idea of this solution is to provide a seamless system architecture across various processes such as monitoring, collecting data, security evaluating in a centralized large scale monitoring network. Our system uses collected data for both attack threats detection and security evaluation. The Analytic Hierarchy Process (AHP) is applied to calculate the weights for security function classes according to the standard ISO 15408 and to provide a quantitative evaluation of the security level for Web-Portals. Tests were conducted with nearly 200 Web-Portals to show the feasibility of our solution.

Keywords: Security Monitoring, Web application security, Web application security evaluation.

Hoàng Đăng Hải, TS (1999), TSKH (2002) tại CHLB Đức, PGS (2009). Hiện đang đang công tác tại Học viện Công nghệ Bưu chính Viễn thông. Lĩnh vực nghiên cứu: Mạng và hệ thống thông tin, các giao thức truyền thông, chất lượng dịch vụ, mạng IoT, an toàn thông tin, an toàn mạng.

Phạm Thiếu Nga. TS. (2000) tại CHLB Đức.

Hiện đang là giảng viên chính tại Khoa Công nghệ thông tin, Đại học Xây dựng, Hà Nội. Lĩnh vực nghiên cứu: logic mờ, điều khiển mờ, mạng và hệ thống thông tin, mạng WSN, mạng IoT, hệ trợ giúp quyết định, hệ chuyên gia, đánh giá an toàn thông tin.