MỘT SỐ GỢI Ý NHẰM NÂNG CAO VIỆC BẢO VỆ HỆ THỐNG WEBSERVER CỦA HỌC VIỆN CÁN BỘ THÀNH PHỐ HỒ CHÍ MINH

ThS. Phan Trần Điền [(*)]

Sự phát triển vượt bậc của ngành công nghệ thông tin (CNTT) trong những năm trở lại đây, đặc biệt là sự phát triển nhanh chóng của mạng Internet, đã tạo cơ hội cho các cơ quan, doanh nghiệp, cá nhân giới thiệu thông tin của mình trên xa lộ thông tin, cũng như thực hiện các phiên giao dịch trực tuyến trên mạng. Hầu hết các cơ quan, doanh nghiệp hiện nay đều có sử dụng web cho mục đích quảng bá cũng như các mục đích khác. Tuy nhiên, việc bảo vệ an ninh cho hệ thống web lại không được quan tâm một cách đúng đắn. Theo thông tin từ Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (Vncert) thuộc Bộ Thông tin và Truyền thông cho biết, trong tháng 7.2015 vừa qua có 1.007 máy chủ và 2.198 website của Việt Nam bị tấn công mạng. Thực trạng này cho thấy, an ninh mạng vẫn chưa thực sự được quan tâm đúng mức tại các cơ quan, doanh nghiệp, cá nhân có thông tin quảng bá trên mạng.

Từ thực trạng mất an toàn thông tin của một số cơ quan, tổ chức, doanh nghiệp. Người viết xin trình bày về thực trạng an toàn của hệ thống thông tin tại Học viện Cán Bộ Thành Phố:

- Về cơ sở hạ tầng mạng: trong năm 2014, Học viện được trang bị hệ thống các trang thiết bị mới, hiện đại của nhà sản xuất Cisco gồm: Thiết bị chuyển mạch trung tâm, hệ thống tường lửa cứng, thiết bị cân bằng tải… với khoảng 500 máy tính cá nhân trang bị cho khoa, phòng, trung tâm, phòng thực hành. Tuy nhiên, hệ thống tường lửa (firewall) tại Học viện, vẫn chưa thể đáp ứng được nhu cầu ngăn chặn tấn công vào các ứng dụng chạy trên nền tảng công nghệ Web. Bên cạnh đó, thiết bị cân bằng tải vẫn không đáp ứng yêu cầu với số lượng người truy cập vào hệ thống lớn.

- Về hệ thống phần mềm: Hiện tại Học viện đã vận hành hệ thống phần mềm quản lý đào tạo và hệ thống phần mềm thư viện.

- Về quy trình quản lý hệ thống thông tin: Đánh giá mức độ an toàn hệ thống, sao lưu dữ liệu, quy trình quản lý cài đặt trang thiết bị…. chưa được xây dựng tại Học viện.

- Về nhân sự: Chỉ có 3 cử nhân về công nghệ thông tin vận hành hệ thống lớn và hiện đại của Học viện.

(*) Phó Bộ môn Tinh học Ngoại ngữ, Học viện Cán bộ

Từ thực trạng trên, người viết xin gợi ý một số giải pháp để bảo vệ hệ thống Webserver cho Học viện Cán Bộ TPHCM như sau:

1. ***Xây dựng quy trình đánh giá mức độ an toàn của ứng dụng chạy trên nền tảng Web.***

Việc xây dựng quy trình đánh giá này giúp Học viện sớm phát hiện ra được các lỗ hổng trong hệ thống ứng dụng của đơn vị. Việc đánh giá hệ thống sẽ được thực hiện 1 lần/ năm hoặc 2 lần /năm. Hiện nay có một số chuẩn đánh giá mức độ an toàn như: OWASP (Open Web Application Security Project), COBIT(Control objective for Information and Related Techniques, SANS, PCI/DSS (The Payment Card Industry Data Security Standard), (ISO/IEC27001) International Organization for Standardization and International Electrotechnical Commission. Người viết xin trình bày quy trình đánh giá mức độ an toàn theo chuẩn OWASP vì đây là chuẩn mở của cộng đồng thế giới xây dựng, cũng rất dễ sử dụng, tài liệu hướng dẫn rất đầy đủ nhưng không mất phí. Sau đây là các bước để đánh giá mức độ an toàn hệ thống gồm:

•*Bước 1: Thu thập thông tin tổng quát hệ thống*

- Tìm hiểu tất cả các tính năng có nguy cơ xảy ra lỗi: Có thể kiểm tra tính năng của tất cả các ứng dụng web có khả năng phát sinh ra lỗi trong mã nguồn.

- Thu thập những nội dung bị lỗi hoặc bị ẩn đi. Có thể sử dụng một số công cụ như Burp Suite. Sử dụng các công cụ phổ biến (các công cụ về tìm kiếm) và kiểm tra các nội dung thường được lưu trong hệ thống: robots.txt, sitemap.xml, .DS_Store, phpinfo.php, info.php, php.php, test.php, test.aspx, phpinfo.php, info.php, php.php, test.php, test.aspx. Với mục tiêu tìm kiếm những đường dẫn, những thông tin về hệ thống dành riêng cho người quản trị.

- Sử dụng kỹ thuật fingerprinting để xâm nhập thử hệ thống và xem hệ thống webserver đang hoạt động trên phiên bản nào.

- Tìm hiểu công nghệ được áp dụng cho các trang Web: Chẳng hạn với ứng dụng web chạy trên nền tảng công nghệ PHP hoặc trên nền tảng Java, ASP.NET thì có hướng kiểm tra và khai thác khác nhau.

- Kiểm tra danh sách người dùng, chức năng của các quyền trong hệ thống với mục tiêu kiểm tra các tính leo thang giữa các người dùng.

•*Bước 2: Tấn công thử bằng các phương thức khác nhau*

- Để phát hiện được các lỗ hổng trong hệ thống, người kiểm định tiến hành tấn công thử hệ thống theo các phương thức khác nhau. Ví dụ như : Các vấn đề về xác thực mật khẩu.

•*Bước 3: Xác định mức độ nghiêm trọng của lỗ hổng*

- Nếu trong quá trình kiểm định hệ thống mà có phát hiện lỗ hổng nghiêm trọng có thể dẫn đến việc phơi bày thông tin quan trọng của doanh nghiệp thì người đánh giá phải tiến hành thông báo ngay cho doanh nghiệp biết để có biện pháp khắc phục. Việc xác định mức độ nghiêm trọng sẽ dựa theo 10 rủi ro ứng dụng web của **OWASP TOP 10.**

•*Bước 4: Báo cho lãnh đạo doanh nghiệp về lỗ hổng và đề xuất một số biện pháp khắc phục*

- Đánh giá và phát hiện lỗ hổng hệ thống chỉ là bước ban đầu của quá trình đánh giá tổng thể, sản phẩm cuối cùng của quá trình này phải là một văn bản có nhiều thông tin dưới dạng báo cáo. Báo cáo sẽ được cung cấp cho lãnh đạo đơn vị.

•*Bước 5: Kết thúc quá trình đánh giá*

- Lập báo cáo tổng kết bao gồm các nội dung sau đây:

o Mô tả sơ bộ về quá trình đánh giá.

o Số lỗ hổng đã phát hiện và khắc phục được.

o Số lỗ hổng đã phát hiện và chưa khắc phục được.

o Một số cảnh báo quan trọng.

o Khuyến cáo và đề xuất khắc phục.

o Tóm lại nội dung trình bày.

o Báo cáo kỹ thuật về biện pháp khắc phục lỗi.

o Báo cáo chi tiết về các lỗ hổng chưa được khắc phục.

2. *Bảo vệ hệ thống Webserver bằng các Rule của phần mềm ModSecurity*

ModSecurity là một chương trình phần mềm mã nguồn mở do Ivan Ristic khởi nguồn. Phiên bản sau cùng của ModSecurity là một tường lửa ứng dụng (WAF) mã nguồn mở sử dụng bộ nguyên tắc để phòng chống lỗi "zero day" và một số lỗ hổng bảo mật được tìm thấy trong ứng dụng Web. ModSecurity còn có thể sử dụng như một bộ lọc bảo mật, xác định các cuộc tấn công, thực hiện xác thực giá trị đầu vào hệ thống web. ModSecurity có khả năng phát hiện những vi phạm về truy cập từ việc phân tích giao thức http, phát hiện các cuộc tấn công vào ứng dụng web khá

phổ biến, phát hiện các chương trình thu thập thông tin, máy quét, các cuộc tấn công bằng mã độc, phát hiện các cuộc truy cập có đính kèm mã độc Trojan. ModSecurity còn có khả năng bảo vệ từ xa mà không cần can thiệp vào mã nguồn hệ thống.

Để bảo vệ hệ thống webserver tại Học viện, có thể sử dụng Rule được triển khai trên phần mềm ModSecurity với cú pháp như sau:

SecRule VARIABLES OPERATOR [TRANSFORMATION_FUNCTIONS, ACTIONS]

Trong cú pháp Rule của ModSecurity có các thành phần: Variables, Operator, Actions. **VARIABLES (Biến)**: Biến được sử dụng cho việc trích xuất các thành phần khác nhau của gói tin http. Hiện nay, ModSecurity đã hỗ trợ 77 loại biến khác nhau để tăng tính linh động trong việc chống lại các kiểu khai thác ở mức cao. **OPERATOR (Toán tử):** Xác định phương pháp và so sánh trùng khớp dữ liệu để kích hoạt hành động. **TRANSFORMATION_FUNCTIONS (Hàm chuyển đổi chức năng):** Chức năng này cho phép chuyển đổi dữ liệu đầu vào trước khi đưa qua cơ chế kiểm tra (chuyển chữ hoa thành chữ thường hoặc decode base64..). **ACTIONS (Hành động):** Chỉ rõ hành động sẽ thực hiện khi toán tử so sánh trùng mẫu.

Hiện nay có rất nhiều kỹ thuật tấn công vào hệ thống Server có thể kể đến như: DDOS, XSS (Cross Site Scripting), bruteforce, SQL Injection,… Người viết xin trình bày cách bảo vệ hệ thống Website thư viện của Học viên trước tấn công bruteforce. Kỹ thuật tấn bruteforce là kỹ thuật dò tìm tài khoản và mật khẩu một cách bất hợp pháp. Mục đích chính của phương thức này là tấn công vào, những người sử dụng tài khoản và mật khẩu quá đơn giản và phổ biến. Vì vậy, giải pháp sử dụng Rule ModSecurity để theo dõi việc đăng nhập vào hệ thống. Nếu tại cùng một thời điểm mà người dùng thực hiện nhiều kết nối đăng nhập thì ModSecurity sẽ ngăn chặn kết nối và đồng thời ghi cảnh báo vào log quản trị. Mã nguồn của Rule ngăn chặn tấn công bruteforce được viết như sau:

```
# Initialize IP collection
SecAction "initcol:ip=%{REMOTE_ADDR},pass,phase:1,id:'10001'"
# Track accesses to the protected resource
SecRule REQUEST_URI "/ReaderLogin.aspx/Login"
"pass,phase:1,setvar:ip.attempts=+1,expirevar:ip.attempts=60,id:'10002'"
# Was this an authenticated access? (Chained rule)
```

SecRule REQUEST_URI **"/ReaderLogin.aspx/Login"** "chain,pass,phase:3,id:'10003'"

Yes, user is logged in, set counter to 0

SecRule RESPONSE_STATUS "^2..$" "setvar:ip.attempts=0"

Block if more than 3 non-authenticated access attempts

SecRule IP:ATTEMPTS "@gt 3" "phase:1,log,deny,id:'10004'"

Với Rule ModSecurity trên, kẻ tấn công dùng công cụ để dò tìm mật khẩu đăng nhập của độc giả. Nếu sau 3 lần dò tìm thất bại ModSecurity sẽ ngăn cản kẻ tấn công tiếp tục việc dò tìm mật khẩu trong hệ thống.

Tóm lại, vấn đề an toàn thông tin là lĩnh vực khá mới mẻ đối với nước ta. Nó luôn đòi hỏi nhiều kiến thức chuyên sâu trong lĩnh vực công nghệ thông tin và kinh nghiệm thực tiễn. Vì vậy, để nâng cao tính bảo mật cho hệ thống thông tin tại Học viện thì cần xây dựng quy trình đánh giá mức độ an toàn cho hệ thống thông tin. Quy trình này, sẽ giúp cho Học viện sớm tìm ra lỗ hổng từ các ứng dụng trên nền tảng công nghệ Web và cũng từ kết quả tìm được sẽ giúp đội ngũ công nghệ thông tin kết hợp với việc phát triển các Rule trên phần mềm ModSecurity để ngăn chặn một số tấn công như DoS, SQL Injection, XSS, Bruteforce…vào các dữ liệu quan trọng của Học viện về quản lý điểm, hệ thống thông tin thư viện… và đặc biệt hơn là ngăn chặn việc Hacker chiếm quyền điều khiển toàn bộ hệ thống máy chủ thông qua các lỗ hổng trong các ứng dụng web của Học viện.

TÀI LIỆU THAM KHẢO

[1] OWASP, địa chỉ : https://www.owasp.org/index.php/Main_Page

[2] VNCERT, *375 Website bị tấn công chỉ trong 1 tuần* [cập nhật 20/08/2015]

[3] OWASP Foundation(2008), *OWASP testing guide*, United States. Địa chỉ: https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf

[4] The *Open Web Application Security Project (2013), testing checklist*, United States. Địa chỉ: https://www.owasp.org/index.php/Testing_Checklist

[5] The *Open Web Application Security Project (2004), OWASP Web Application Penetration Checklist version 1.1*, OWASP Foundation. Địa chỉ: http://sourceforge.net/projects/owasp/files/

[6] The Open Web Application Security Project (2013), *OWASP Top 10-2013*, OWASP Foundation. Địa chỉ:

http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf