NÂNG CAO MỨC ĐỘ BẢO ĐẢM AN NINH HỆ THỐNG MẠNG TẠI VIỆT NAM BẰNG PHƯƠNG PHÁP LÀM NGƯỢC

Lê Hoàng Hiệp[1], Lê Xuân Hiếu[2*], Trần Lâm[3], Đỗ Đình Lực[1]
[1]Trường Đại học Công nghệ thông tin & Truyền thông – ĐH Thái Nguyên,
[2]Đại học Thái Nguyên, [3]VNPT Thái Nguyên

TÓM TẮT

Bài báo này trình bày kết quả đánh giá mức độ an toàn của hệ thống mạng dựa trên kỹ thuật làm ngược lại. Nghiên cứu đã thực hiện triển khai một số cuộc tấn công hệ thống mạng phổ biến, thường gặp như DDoS, SQL Injection, Reverse TCP để định lượng và đánh giá mức độ khả năng phòng thủ an ninh của hệ thống đó dựa trên thực nghiệm mô phỏng. Thông qua việc phân tích các mối đe dọa và các thông số đo lường, nhóm tác giả nhận diện được mức độ an toàn và an ninh của hệ thống mạng. Ba kịch bản tấn công hệ thống mạng sử dụng phương pháp phát hiện xâm nhập kiểu hộp trắng (White Box) bao gồm: (a) tấn công máy chủ web từ bên trong mạng nội bộ, (b) tấn công từ bên ngoài với trường hợp mạng đã tích hợp tường lửa thế hệ cũ và (c) tấn công từ bên ngoài trong trường hợp tích hợp tường lửa thế hệ mới. Kết quả cho thấy với (a) mức độ bị tấn công gây kết quả rất nghiêm trọng (tê liệt máy chủ lên tới 95%); với (b) tỉ lệ này đã giảm còn 63% và với (c) chỉ còn 19%. Kết quả này giúp nhà quản trị xây dựng giải pháp an toàn và an ninh mạng cho hệ thống của mình được tốt hơn để phòng tránh và hạn chế các mối đe dọa tấn công vào hệ thống.

Từ khóa: *Tấn công DDoS; tấn công SQL Injection; tấn công Reverse TCP; tấn công mạng; bảo mật mạng*

Ngày nhận bài: 11/8/2020; Ngày hoàn thiện: 31/8/2020; Ngày đăng: 31/8/2020

IMPROVE NETWORK SECURITY SYSTEM IN VIETNAM USING REVERSE METHOD

Le Hoang Hiep[1], Le Xuan Hieu[2*], Tran Lam[3], Do Dinh Luc[1]
[1]TNU - University of Information and Communication Technology
[2]Thai Nguyen University, [3]VNPT Thai Nguyen

ABSTRACT

This paper presents the results of evaluating the security level of a network based on reverse engineering. A number of common network attacks, such as DDoS, SQL Injection, Reverse TCP were emulatedto quantify and evaluate the level of security defenses of the system based on simulation experiments. Through the threat analysis and security metrics, the level of safety and security of the network were indentified. Three scenarios for a network attack using White Box intrusion detection methods include: (a) attacking a web server from an internal network, (b) attacking from outside in the case of a built-in old firewall and (c) external attacking in the case of a new generation firewall. The results showed that (a) the severity of the attack caused serious results (server paralysis up to 95%); (b) the server paralysis rate was decreased to 63%; and (c) the server paralysis rate was only 19%. The results are promising to help administrators to build better safety and security systems as well as to prevent and limit network connections and threatens attacking their systems.

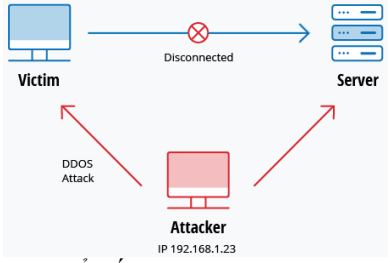
Keywords: *DdoS attack; SQL Injection attack; reverse TCP attack; network attack; network security*

Received: 11/8/2020; Revised: 31/8/2020; Published: 31/8/2020

* Corresponding author. *Email: lxhieucntt@tnu.edu.vn*

1. Giới thiệu

Trong vài năm gần đây, khi nói về vấn đề hệ thống máy tính bị tấn công mạng và an ninh kỹ thuật số, chúng ta thường chỉ thấy những báo cáo về các sự cố bảo mật lớn, với mật độ dày đặc xảy ra tại các cường quốc công nghệ thông tin và một vài quốc gia tâm điểm khác. Tuy nhiên, ngay tại nước ta, tình hình an ninh mạng và an toàn thông tin trong vài năm gần đây cũng đã có những diễn biến cực kỳ nguy hiểm, phức tạp. Song song với mức độ số hoá và việc triển khai số hoá ngày càng gia tăng rất nhanh tại Việt Nam, chúng ta có thể nhận thấy mối quan tâm rõ rệt hơn từ khối doanh nghiệp đối với an ninh mạng và hệ thống. Đây là công việc cực kỳ quan trọng, bởi vì càng ngày sẽ càng có nhiều người dùng và nhiều thiết bị kết nối vào mạng trong các năm tới. Điều này sẽ đem lại nhiều cơ hội lớn cho các doanh nghiệp, nhưng nó cũng đồng nghĩa nguy cơ các mối tấn công tăng theo cấp số nhân, đẩy doanh nghiệp đối mặt với nhiều mối nguy cơ và rủi ro an ninh mạng lớn hơn. An ninh mạng không thể là những xử lý tình huống tức thời, mà cần phải trở thành nền tảng ưu tiên cho bất kỳ nỗ lực chuyển đổi số nào. Việc các cơ quan chức năng/ tổ chức vẫn còn tương đối bị động trước những phương án nâng cao nhận thức của cộng đồng về vấn đề an ninh mạng đã khiến các cá nhân đam mê máy tính cũng như đang hoạt động trong lĩnh vực bảo mật ở nước ta buộc phải chủ động tự tổ chức các sự kiện, cuộc thi lớn nhằm phổ biến thông tin rộng rãi hơn cho cộng đồng cũng như doanh nghiệp. Những sự kiện như vậy sẽ đóng vai trò cực kỳ quan trọng, không chỉ cung cấp những thông tin cụ thể, chính xác nhất về tình hình an ninh mạng ở nước ta, mà còn giới thiệu nhiều dự án bảo mật quy mô lớn với sự góp mặt của các chuyên gia đầu ngành hiện nay.



Hình 1. *Một kiểu tấn công Session Hijacking điển hình*

Những mối de dọa an ninh mạng giờ đây đang diễn biến ở mức độ rất nghiêm trọng. Mọi cơ quan/ tổ chức đều có nguy cơ bị tấn công như nhau. Cơ quan nào có nhiều thông tin nhạy cảm và hệ thống chứa nhiều lỗ hổng bảo mật sẽ dễ bị tin tặc tấn công hơn. Cho nên, tất cả chúng ta cần phải sẵn sàng ứng cứu, khắc phục, xử lý mọi sự cố. Tội phạm mạng/ kẻ tấn công (Hacker/Attacker) luôn không ngừng cải tiến các phương thức triển khai chiến dịch tấn công của mình theo hướng phức tạp và khó lường hơn, nhằm trục lợi trái phép từ người dùng Internet cũng như các tổ chức, doanh nghiệp toàn cầu, ví dụ điển hình như trong Hình 1. Đây là lý do tại sao tất cả các công ty, bất kể quy mô hay lĩnh vực hoạt động, đều buộc phải sở hữu những phương án phòng thủ an ninh mạng đáng tin cậy để tự bảo vệ chính bản thân cũng như khách hàng của mình trước các mối đe dọa tiềm ẩn. Khi chúng ta phát hiện ra một cuộc tấn công mạng đã thực sự xảy ra thì đã/ quá muộn, hậu quả là cơ sở hạ tầng, kinh doanh của một tổ chức bị ảnh hưởng lớn. Trong bối cảnh thế giới số luôn thay đổi, phát triển và ngày càng phức tạp, làm thế nào để bảo vệ chính mình, không chỉ từ những điều đã biết mà còn từ những ẩn số trên mạng, làm thế nào để chuẩn bị và xây dựng khả năng miễn dịch và phòng thủ chống lại mối đe dọa ngày càng phát triển đó. Để giải quyết vấn đề này là cần phải xây dựng khả năng phục hồi không gian mạng hiệu quả. Đây là việc một tổ chức/ doanh nghiệp phải chuẩn bị, tiếp nhận, ứng phó, thích nghi và phục hồi sau một sự cố trong khi vẫn tiếp tục hoạt động và vận hành theo kế hoạch.

Trong nghiên cứu này tập trung nghiên cứu, đánh giá mức độ an toàn hệ thống mạng dựa trên kỹ thuật làm ngược. Thông qua việc phân tích các mối đe dọa và các thông số đo lường sự an toàn của hệ thống, nghiên cứu sẽ thực hiện triển khai một số cuộc tấn công hệ thống mạng phổ biến thường gặp như DDoS, SQL Injection, Reverse TCP để định lượng mức độ khả năng phòng thủ của hệ thống đó dựa trên thực nghiệm mô phỏng. Thông qua đây cũng nhận diện được mức độ an toàn và an ninh hệ thống mạng, từ đó giúp nhà quản trị xây dựng giải pháp an ninh mạng cho hệ thống của mình được tốt hơn.

2. Cơ sở và phương pháp nghiên cứu

2.1. Các kiểu tấn công hệ thống mạng phổ biến

Mục tiêu của các cuộc tấn công mạng là tất cả các hình thức xâm nhập trái phép vào một hệ thống máy tính, website, cơ sở dữ liệu, hạ tầng mạng, thiết bị của một cá nhân hoặc tổ chức thông qua mạng internet với những mục đích gì đi nữa đều là bất hợp pháp. Có nhiều kiểu tấn công mạng trên thực tế hiện nay, tuy nhiên ở đây chỉ tóm tắt các kiểu tấn công được sử dụng trong nghiên cứu này [1]-[3]:

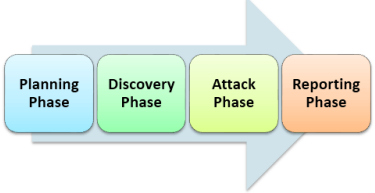
a. Tấn công từ chối dịch vụ (Denial of Service): Các cuộc tấn công từ chối dịch vụ (DoS) được thiết kế để làm cho tài nguyên mạng hoặc máy tính không sẵn sàng để phục vụ cho người dùng như dự định của nó. Kẻ tấn công có thể thực hiện làm từ chối dịch vụ cho từng nạn nhân, chẳng hạn như cố tình nhập sai mật khẩu đủ lần liên tục để khiến tài khoản nạn nhân bị khóa hoặc chúng có thể làm quá tải khả năng của máy tính hoặc băng thông mạng và chặn tất cả người dùng cùng một lúc. Mặc dù một cuộc tấn công mạng từ một địa chỉ IP duy nhất có thể bị chặn bằng cách thêm vào quy tắc tường lửa mới, nhiều hình thức tấn công từ chối dịch vụ phân tán - Distributed Denial-of-Service (DDoS) là có thể, trong đó cuộc tấn công đến từ một số lượng lớn máy tính và việc bảo vệ sẽ trở nên khó khăn hơn nhiều. Các cuộc tấn công như vậy có thể bắt nguồn từ các máy tính zombie của botnet, nhưng một loạt các kỹ thuật khác có thể bao gồm các cuộc tấn công phản xạ và khuếch đại, trong đó các hệ thống vô tội bị lừa gửi dữ liệu đến máy nạn nhân bằng nhiều cách khác nhau.

b. Tấn công cơ sở dữ liệu (SQL Injection Attack): Hacker chèn một đoạn mã code độc hại vào Server sử dụng ngôn ngữ truy vấn có cấu trúc - Structured Query Language (SQL), mục đích là để khiến máy chủ trả về những thông tin quan trọng mà lẽ ra không được tiết lộ. Các cuộc tấn công SQL Injection xuất phát từ các lỗ hổng của website, chẳng hạn hacker có thể tấn công đơn giản bằng cách chèn một đoạn mã độc vào thanh công cụ "Tìm kiếm" là đã có thể dễ dàng tấn công những website với mức bảo mật yếu.

c. Tấn công Reverse TCP: Một cuộc tấn công Reverse TCP là một kiểu tấn công khai thác. Mã khai thác là một phần mềm, một đoạn dữ liệu hoặc một chuỗi các câu lệnh nhằm lợi dụng lỗi hoặc lỗ hổng trong ứng dụng hoặc hệ thống để tạo ra hành vi ngoài ý muốn hoặc không lường trước được. Khi thiết bị khởi tạo một kết nối, gọi nó là kết nối thẳng. Nhưng khi chúng ta làm điều ngược lại, server bắt đầu kết nối đến thiết bị, gọi nó là kết nối ngược (rất hiếm). Tường lửa hoạt động theo nguyên tắc cơ bản là chặn tất cả các kết nối đến. Vì vậy, tất cả các kết nối đến (kết nối ngược) sẽ bị chặn bởi tường lửa. Tuy nhiên, nếu máy nạn nhân thiết lập kết nối (kết nối thẳng) thì được phép và kết quả là kẻ tấn công có được kết nối được thiết lập tới máy nạn nhân. Đối với kiểu tấn công Reverse TCP về cơ bản thay vì kẻ tấn công khởi tạo kết nối rõ ràng sẽ bị chặn bởi tường lửa, máy nạn nhân sẽ khởi tạo kết nối tới kẻ tấn công, nhiều khả năng sẽ được tường lửa cho phép và kẻ tấn công sau đó kiểm soát thiết bị và truyền lệnh. Nó là một loại shell tương tác ngược.

2.2. Kiểm tra xâm nhập mạng

a. Pentest, viết tắt của penetration testing (kiểm tra xâm nhập): là hình thức đánh giá mức độ an toàn của một hệ thống mạng bằng các cuộc tấn công mô phỏng thực tế. Hiểu đơn giản, pentest cố gắng xâm nhập vào hệ thống để phát hiện ra những điểm yếu tiềm tàng của hệ thống mà kẻ tấn công/tin tặc có thể khai thác và gây thiệt hại. Mục tiêu của pentest là giúp thực hiện việc phát hiện càng nhiều lỗ hổng càng tốt, từ đó khắc phục chúng để loại trừ khả năng bị tấn công trong tương lai. Người làm công việc kiểm tra xâm nhập được gọi là Pentester. Pentest có thể được thực hiện trên hệ thống mạng máy tính, ứng dụng web, ứng dụng mobile hạ tầng mạng, IoT, ứng dụng và hạ tầng Cloud, phần mềm dịch vụ SaaS, API, source code, hoặc một đối tượng có kết nối với Internet và có khả năng bị tấn công… nhưng phổ biến nhất là pentest web app và mobile app. Những thành phần trên được gọi là đối tượng kiểm thử (pentest target).



Hình 2. *Các pha trong chu trình kiểm tra xâm nhập mạng*

Khi thực hiện xâm nhập hệ thống theo các pha như trong hình 2, Pentester cần có được sự cho phép của chủ (admin) hệ thống hoặc phần mềm đó. Nếu không, hành động xâm nhập sẽ được coi là xâm nhập (hack) trái phép. Thực tế, ranh giới giữa pentest và hack chỉ là sự cho phép của chủ đối tượng. Vì thế, khái niệm pentest có ý nghĩa tương tự như ethical hacking (hack có đạo đức), Pentester còn được gọi là hacker mũ trắng (white hat hacker).

b. Các hình thức pentest:

- *White box Testing:* Trong hình thức pentest White box, các chuyên gia kiểm thử sẽ được cung cấp đầy đủ thông tin về đối tượng mục tiêu trước khi họ tiến hành kiểm thử xâm nhập mạng. Những thông tin này bao gồm: địa chỉ IP, sơ đồ hạ tầng mạng, các giao thức sử dụng, hoặc source code của mục tiêu.

- *Gray box Testing:* Pentest Gray box là hình thức kiểm thử mà Pentester chỉ nhận được một phần thông tin của đối tượng kiểm thử, ví dụ: URL, IP address,… nhưng không có hiểu biết đầy đủ hay quyền truy cập vào đối tượng một cách toàn diện.

- *Black box Testing:* Pentest Black box, hay còn gọi là 'blind testing', là hình thức pentest dưới góc độ của một hacker trong thực tế. Với hình thức này, các chuyên gia kiểm thử không nhận được bất kỳ thông tin nào về đối tượng trước khi thực hiện tấn công. Các Pentester phải tự tìm kiếm và thu thập thông tin về đối tượng để tiến hành kiểm thử xâm nhập mạng. Loại hình pentest này yêu cầu một lượng lớn thời gian tìm hiểu và nỗ lực tấn công, nên chi phí không hề rẻ.

Ngoài ra còn các hình thức pentest khác như: Double - blind testing, External testing, Internal testing, Targeted testing,… tuy nhiên chúng không phổ biến tại Việt Nam và chỉ được sử dụng với nhu cầu đặc thù của một số tổ chức/ doanh nghiệp.

2.3. Mô hình và phương pháp thực hiện

Để thực hiện các hình thức, phương pháp xâm nhập mạng nghiên cứu đã xây dựng mô hình thử nghiệm mô phỏng lại hệ thống mạng nội bộ kết nối ra Internet của một tổ chức/ công ty như trên thực tế. Các thành phần này bao gồm: website được đặt trên máy chủ chạy hệ điều hành Linux, sau đó cài nhiều ứng dụng khác trên máy tính của kẻ tấn công. Máy tính của nạn nhân (Victim) được đặt bên trong mạng nội bộ. Nghiên cứu thực nghiệm sẽ thực hiện kiểm tra xem hệ thống mạng nội bộ có khả năng chống lại các cuộc tấn công như DDoS, SQL Injection, Reverse TCP ở mức độ nào sử dụng phương pháp phát hiện xâm nhập kiểu White Box thông qua ba kịch bản tấn công như sau:

- Kịch bản 1: Thực hiện cuộc tấn công Web server từ bên trong hệ thống mạng nội bộ.

- Kịch bản 2: Thực hiện cuộc tấn công Web server từ bên ngoài hệ thống mạng nội bộ (đứng từ Internet để tấn công) trong trường hợp Web server được bảo vệ bởi tường lửa ASA và TMG.

- Kịch bản 3: Thực hiện cuộc tấn công Web server từ bên ngoài hệ thống mạng nội bộ (đứng từ Internet để tấn công) trong trường hợp Web server được bảo vệ bởi tường lửa thế hệ mới Sophos UTM.

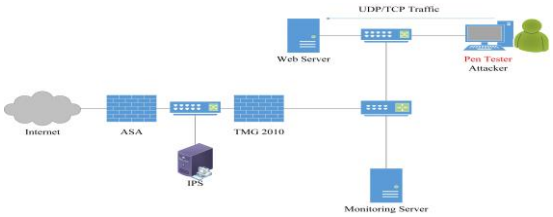
3. Thực nghiệm, đánh giá

3.1. Thực nghiệm tấn công DoS vào hệ thống

Các cuộc tấn công xâm nhập mạng được thực hiện dựa trên việc sử dụng cả hai kỹ thuật TCP và UDP flood. Trong thực nghiệm này sử dụng công cụ đã được cài trên máy kẻ tấn công gửi đến máy chủ một lượng lớn gói tin TCP và UDP đủ nhằm làm tê liệt máy chủ trong ba kịch bản bên dưới đây [4]-[7]:

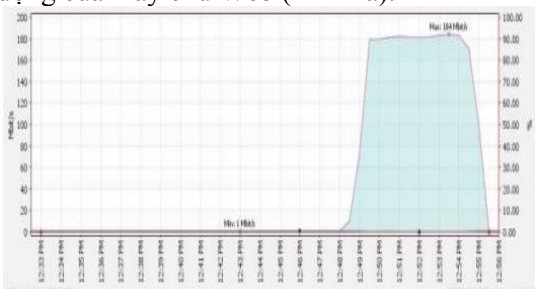
a. Kịch bản 1: Tấn công Web server từ bên trong hệ thống mạng nội bộ:

Sơ đồ mô tả hệ thống mạng và vị trí kẻ tấn công, vị trí nạn nhân như hình. Website của nạn nhân được cài đặt trên hệ điều hành Linux. Kẻ tấn công sử dụng công cụ của mình tấn công DoS máy chủ nạn nhân. Quá trình tấn công này sẽ được theo dõi sử dụng công cụ giám sát mạng PRTG (được cài đặt trên một server khác). Thông qua PRTG ta có thể theo dõi được các thông số đo về tình trạng của hệ thống trước và sau khi bị tấn công như thời gian tải của web, số cổng mà kẻ tấn công sử dụng để xâm nhập mạng,…



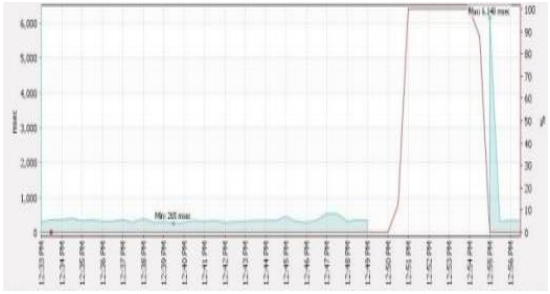
Hình 3. *Kịch bản tấn công DoS từ bên trong mạng nội bộ*

Trong thử nghiệm này, nghiên cứu chỉ sử dụng một máy tính (PC) để thực hiện gửi lượng lớn gói tin TCP và UDP vào cổng số 80 của máy chủ. Qua việc giám sát và đo đạc thông qua công cụ giám sát, kết quả cho biết việc tấn công DoS từ một PC sử dụng TCP flood dường như không ảnh hưởng tới hoạt động của máy chủ Web (hình 4a).



Hình 4a. *Thông số lưu lượng qua Card mạng trên web server*

Tiếp theo đó, nghiên cứu thử nghiệm tấn công UDP flood thông qua cổng 80, kết quả hiển thị trong hình 4a và hình 4b cho thấy kẻ tấn công đã gửi khoảng 185 Mbps và với lưu lượng này đủ để làm dừng hoạt động tải về của Web.

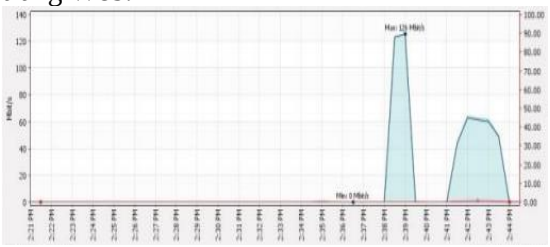


Hình 4b. *Thời gian mở trang web từ bên trong mạng khi bị tấn công UDP flood*

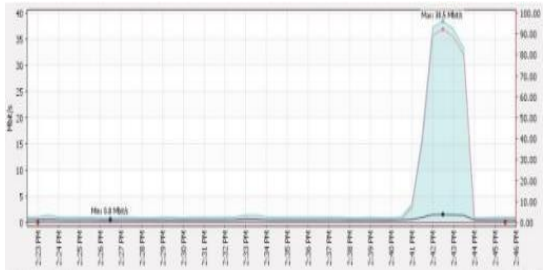
Thông qua thực nghiệm này thấy rằng, bằng cách tấn công UDP flood, kẻ tấn công có thể dễ dàng dừng lại việc tải trang web ngay cả khi kẻ tấn công đó chỉ cần sử dụng một PC duy nhất để thực hiện tấn công.

b. Kịch bản 2: Thực hiện cuộc tấn công Web server từ bên ngoài hệ thống mạng nội bộ (đứng từ Internet để tấn công) trong trường hợp Web server được bảo vệ bởi tường lửa Cisco Adaptive Security Appliance (Cisco ASA) và Forefront Threat Management Gateway (TMG):

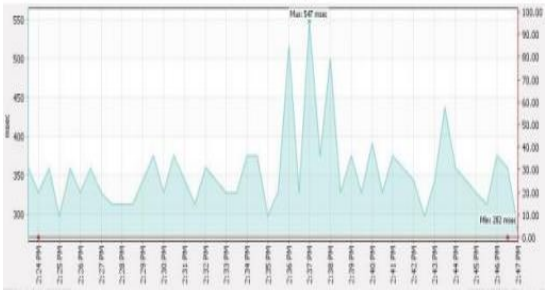
Trong trường hợp này, máy chủ web được đặt bên trong mạng nội bộ, kẻ tấn công đứng từ bên ngoài. Kẻ tấn công sẽ phải vượt qua hai tường lửa đã được cài đặt sẵn trước đó (ASA và TMG) để có thể xâm nhập tới server (như hình 3). Thực nghiệm này vẫn sử dụng tấn công kiểu TCP và UDP flood thông qua cổng 80. Kết quả tấn công TCP flood được hiển thị trong hình 5a, hình 5b và hình 5c. Qua đây cho thấy kẻ tấn công gửi khoảng 60 Mbps lưu lượng vào máy chủ Web, trong khi đó máy chủ Web chỉ nhận thấy có 38,5 Mbps lưu lượng truy cập đến. Điều này có thể giải thích do hệ thống đã được cài đặt tường lửa, chức năng của tường lửa đã được thực thi và ngăn chặn (lọc) các lưu lượng gói tin bất thường (đáng ngờ) vì thế mà chỉ một phần lưu lượng từ kẻ tấn công gửi tới có thể đến được máy chủ Web và dẫn tới cuộc tấn công này không làm ảnh hưởng nhiều tới thời gian tải của trang Web.



Hình 5a. *Lưu lượng từ Card mạng trên PC kẻ tấn công*



Hình 5b. *Lưu lượng từ Card mạng trên máy chủ Web*

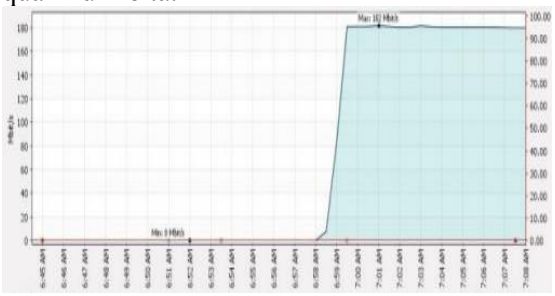


Hình 5c. *Thời gian tải trang Web từ bên ngoài Internet*

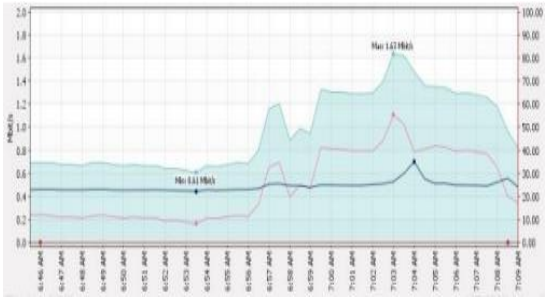
Qua theo dõi kết quả cũng cho thấy, sau khoảng 30 giây, tường lửa ASA đã chặn địa chỉ IP của kẻ tấn công trước mà chưa cần tới tường lửa TMG thực thi.

Tiếp theo, nghiên cứu thực hiện tấn công tương tự bằng việc gửi các gói tin UDP tới máy chủ Web. Trong trường hợp này, kẻ tấn

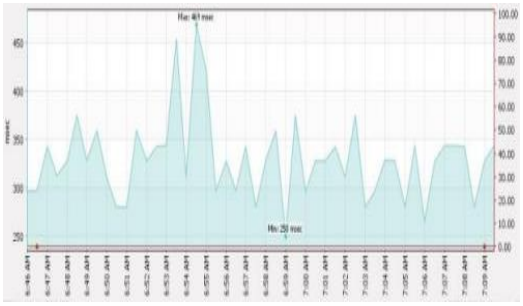
công đã gửi khoảng 180 Mbps. Tường lửa ASA đã tăng mức xử lý đạt hiệu quả tới mức đủ ngăn chặn được hoàn toàn cuộc tấn công này. Hình 6a, hình 6b và hình 6c cho thấy kết quả như mô tả.



Hình 6a. *Lưu lượng từ PC của kẻ tấn công*



Hình 6b. *Lưu lượng từ Card mạng trên máy chủ Web*

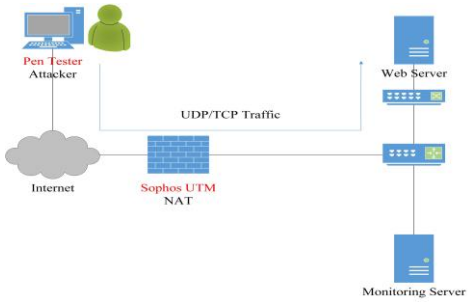


Hình 6c. *Thời gian mở trang web từ bên trong mạng nội bộ khi bị tấn công UDP flood*

Trong cuộc tấn công này, tất cả các dịch vụ có thể truy cập từ Internet đã ngừng hoạt động. Kẻ tấn công đã được kết nối bên ngoài tường lửa và đã sử dụng dung lượng tối đa 1Gbps vì lưu lượng không đi qua thiết bị của nhà cung cấp dịch vụ ISP.

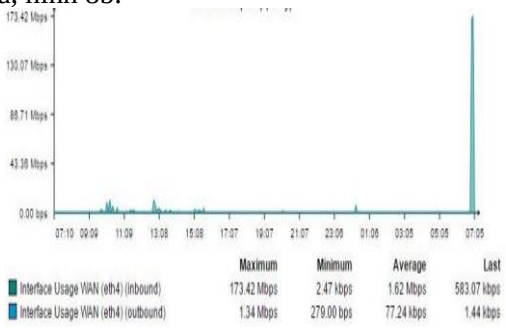
c. Kịch bản 3: Thực hiện cuộc tấn công Web server từ bên ngoài hệ thống mạng nội bộ (đứng từ Internet để tấn công) trong trường hợp Web server được bảo vệ bởi tường lửa thế hệ mới Sophos UTM.

Các phiên bản tường lửa thế hệ cũ trước đây đã lỗi thời vì chức năng của chúng không đủ khả năng ngăn chặn các cuộc tấn công mạng ngày càng tinh vi và mạnh mẽ hơn trước rất nhiều. Việc ra đời tường lửa thế hệ mới, là phiên bản nâng cao của tường lửa truyền thống với nhiều chức năng tích hợp sẵn, có sức mạnh và hiệu năng cao hơn nhiều lần như chức năng bảo vệ máy chủ Web, email, lọc gói tin, phát hiện xâm nhập,… Trong nghiên cứu này tiếp tục thực nghiệm bằng cách lựa chọn tường lửa Sophos UTM thay thế các tường lửa truyền thống, cũ như ASA, TMG. Sơ đồ mô hình thực nghiệm được thể hiện trong hình 7:

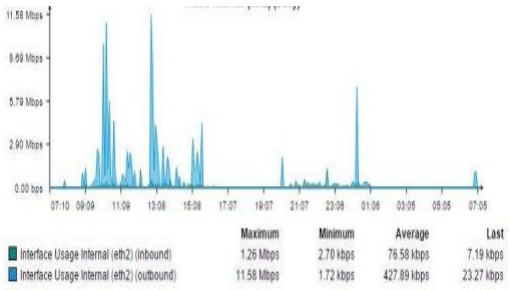


Hình 7. *Mô hình thực nghiệm tấn công mạng với tường lửa Sophos UTM*

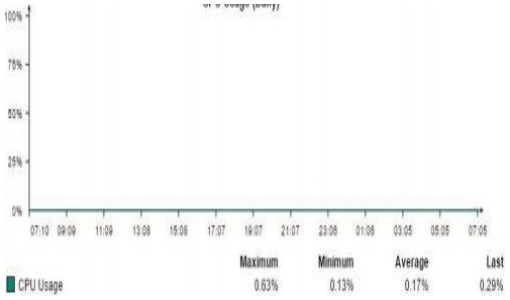
Cách thực nghiệm tương tự như khi hệ thống tích hợp tường lửa truyền thống ASA và TMG bằng việc gửi lưu lượng TCP và UDP flood. Tuy nhiên, qua kết quả cho thấy đã có sự khác biệt rõ rệt đó là hiệu năng của tường lửa thế hệ mới Sophos UTM đã được thực thi tốt hơn nhiều so với ASA, TMG. Sophos UTM có thể xử lý lưu lượng bình thường trong khi vẫn giữ được hoạt động của trang Web trong quá trình bị tấn công. Kết quả như hình 8c cho thấy hiệu suất của CPU trước và sau cuộc tấn công dường như không đổi (mức thay đổi rất thấp ở mức trung bình là 0,19%). Lưu lượng truy cập chỉ đi/ nằm trong khu vực đoạn mạng từ kẻ tấn công tới Card mạng WAN của tường lửa Sophos UTM khi cuộc tấn công UDP flood diễn ra như trong hình 8a, hình 8b:



Hình 8a. *Lưu lượng trên Card mạng WAN của tường lửa Sophos UTM*



Hình 8b. *Lưu lượng trên Card mạng LAN của tường lửa Sophos UTM*



Hình 8c. *Mức sử dụng hiệu suất CPU của tường lửa Sophos UTM*

d. Nhận xét chung về kết quả tấn công mạng sử dụng kiểu DoS:

Thông qua nghiên cứu thực nghiệm trên cho thấy, nguy cơ tiềm ẩn cao nhất từ các cuộc tấn công vào hệ thống mạng của doanh nghiệp/ tổ chức là khi các cuộc tấn công sử dụng kiểu UDP flood. Bảng 1 là kết quả tóm tắt so sánh các kịch bản tấn công đã thực nghiệm bên trên:

Bảng 1. *Kết quả thực nghiệm so sánh*

Tấn công DoS	Mức độ làm dừng tải nội dung trang Web	Chặn các dịch vụ khác	Tải lưu lượng bên trong mạng
Tấn công TCP bên trong mạng	Không	Không	Có
Tấn công UDP bên trong mạng	Có	Không	Có
Tấn công TCP tới hệ thống có tích hợp ASA/TMG	Không	Không	Có
Tấn công UDP tới hệ thống có tích hợp ASA/TMG	Có	Có	Có
Tấn công TCP tới hệ thống có tích hợp Sophos UTM	Không	Không	Có
Tấn công UDP tới hệ thống có tích hợp Sophos UTM	Không	Không	Có

Qua bảng so sánh (Bảng 1) ta thấy, để giảm thiểu nguy cơ tấn công từ kẻ tấn công ngày càng tinh vi, các hệ thống mạng hiện nay cần nâng cấp/ cập nhật các hệ thống tường lửa mới, hiện đại hơn.

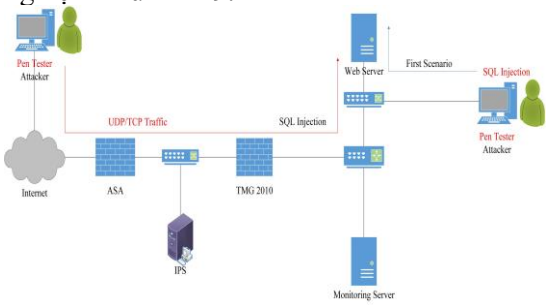
3.2. Thực nghiệm tấn công SQL Injection vào hệ thống

Trong thực nghiệm này sử dụng một số công cụ sau để thực hiện tấn công xâm nhập mạng giả định:

- Acunetix Web Vulnerability Scanner: công cụ này cho phép quét ứng dụng web để nhận dạng các lỗ hổng tiềm ẩn.
- Burp Suite: công cụ này cho phép bắt các gói tin từ máy client đến ứng dụng web và trích xuất thu thập dữ liệu quét được.
- SQLMAP: cho phép thâm nhập vào bên trong cơ sở dữ liệu sau khi xác định các lỗ hổng của hệ thống.

a. Kịch bản 1: Tấn công xâm nhập hệ thống mạng từ bên trong mạng nội bộ:

Trong thực nghiệm này, nghiên cứu sử dụng một số ứng dụng Web có các lỗ hổng bảo mật để tấn công. Máy tính của kẻ tấn công đã được cài đặt các công cụ cần thiết cho một cuộc tấn công SLQ Injection. Sơ đồ thực nghiệm như hình 9:



Hình 9. *Sơ đồ mạng mô phỏng cho cuộc tấn công SQL Injection từ mạng LAN và Internet*

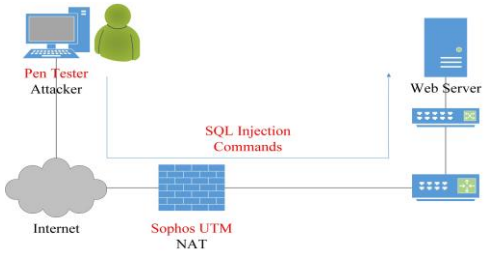
Với mô hình mạng như hình 9, các ứng dụng Web được quét và tìm các lỗ hổng bảo mật sử dụng công cụ Acunetix. Qua dữ liệu thu thập được cho thấy hệ thống xuất hiện nhiều điểm yếu/ lỗ hổng bảo mật trong hệ điều hành, loại máy chủ Web, công nghệ đã cài đặt,… để từ đó kẻ xấu có thể tấn công thông qua kỹ thuật SQL Injection.

b. Kịch bản 2: Tấn công xâm nhập hệ thống mạng SQL Injection từ bên ngoài mạng Internet đối với hệ thống đã tích hợp tường lửa truyền thống

Với thực nghiệm này, kẻ tấn công đứng từ bên ngoài mạng nội bộ. Trong tình huống này

kẻ tấn công cần phải vượt qua nhiều tường lửa khác nhau (ASA, TMG) để có quyền truy cập vào các ứng dụng Web. Các tấn công SQL Injection được thực hiện tại lớp ứng dụng trong khi tường lửa ASA chỉ cho phép lọc lưu lượng truy cập tại lớp vận chuyển (Transoport layer) của mô hình TCP/IP. Qua thực nghiệm cho thấy, tường lửa ASA không thể ngăn chặn các cuộc tấn công SQL Injection. Tuy nhiên, với trường hợp hệ thống có tích hợp tường lửa thế hệ mới, kết quả cho thấy có sự khác biệt rõ rệt hơn so với sử dụng tường lửa truyền thống.

c. Kịch bản 3: Tấn công xâm nhập hệ thống mạng SQL Injection từ bên ngoài mạng Internet đối với hệ thống đã tích hợp tường lửa thế hệ mới Sophos UTM



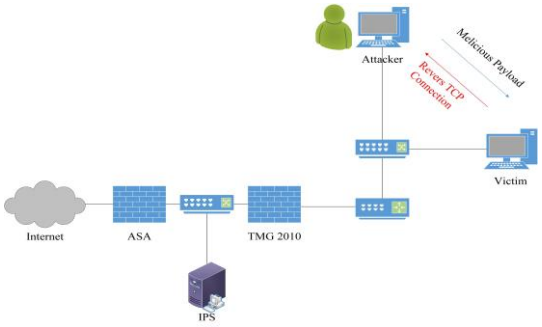
Hình 10. *Sơ đồ mạng với kiểu tấn công SQL Injection tích hợp tường lửa Sophos UTM*

Sơ đồ kịch bản trường hợp này được mô tả như trong hình 10. Qua kết quả xác minh độ mạnh của tường lửa Sophos UTM cho thấy có sự khác biệt rõ ràng so với sử dụng tường lửa truyền thống bảo vệ hệ thống. Với các tấn công kiểu SQL Injection đối với hệ thống có sử dụng tường lửa Sophos UTM đều không có nhiều tác dụng bởi chức năng của tường lửa có thể ngăn cản các cuộc tấn công này một cách hiệu quả.

3.3. Thực nghiệm tấn công Reverse TCP vào hệ thống

a. Kịch bản 1: Tấn công Reverse TCP xâm nhập hệ thống từ bên trong mạng cục bộ

Để thực hiện cuộc tấn công này, nghiên cứu sử dụng máy tính PC của nạn nhân đã được cài đặt hệ điều hành Window 10 với đầy đủ tính năng và chương trình diệt virus. Trên máy tính của nạn nhân đã được cài đặt Metasploit Framework (là một gói tiêu chuẩn của hệ điều hành Linux). Cả hai máy tính của kẻ tấn công và nạn nhân đều nằm bên trong mạng nội bộ như hình 11:



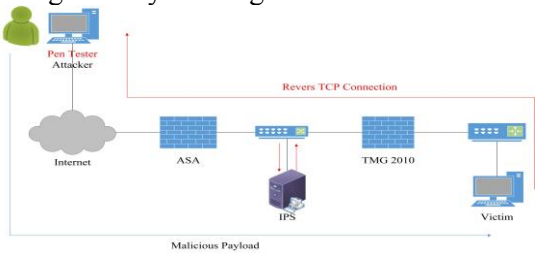
Hình 11. *Sơ đồ mạng mô phỏng cuộc tấn công Reverse TCP từ bên trong mạng nội bộ*

Trong thực nghiệm này, nghiên cứu đã đưa mã độc vào một phần mềm để khi nạn nhân cài đặt nó, phần mềm sẽ tạo ra một liên kết và gửi ngược lại cho kẻ tấn công. Thông qua kiểm tra chương trình diệt virus cho thấy chương trình diệt virus không thể phát hiện được mã độc này. Tiếp theo, nghiên cứu đã cấu hình máy tính của kẻ tấn công để nhận kết nối từ máy tính nạn nhân. Kẻ tấn công gửi email cho nạn nhân với những nội dung hấp dẫn khiến nạn nhân tin tưởng và truy cập các nội dung và bị lừa cài đặt các ứng dụng chứa mã độc mà kẻ tấn công cố tình mong muốn.

Thông qua thực nghiệm này (và liên hệ trên thực tế) cho thấy, kẻ tấn công có thể giành quyền truy cập/ kiểm soát máy tính của người dùng/ nạn nhân trong trường hợp nạn nhân có ít kinh nghiệm, kiến thức và dễ bị lừa bởi các nội dung ảo; sau đó click và cài đặt các ứng dụng chứa mã độc do kẻ tấn công gửi tới, từ đó bị chiếm quyền kiểm soát.

b. Kịch bản 2: Tấn công Reverse TCP xâm nhập hệ thống từ bên ngoài, với trường hợp hệ thống tích hợp tường lửa ASA, TMG hoặc IPS

Với thực nghiệm trên cho thấy, kẻ tấn công có thể truy cập vào bên trong máy nạn nhân ngay cả khi máy nạn nhân đã cài chương trình diệt Virus. Trong thực nghiệm này sẽ kiểm tra mức độ tấn công khi hệ thống đã tích hợp tường lửa truyền thống.



Hình 12. *Sơ đồ mạng mô phỏng cuộc tấn công Reverse TCP từ bên ngoài mạng Internet*

Trong thực nghiệm này, nạn nhân được đặt sau tường lửa ASA, TMG và hệ thống phát hiện xâm nhập IPS. Kẻ tấn công thực hiện từ bên ngoài mạng Internet và cần phải có địa chỉ IP công cộng nếu muốn tấn công vào nạn nhân. Trong thực nghiệm này cho thấy, tường lửa truyền thống và hệ phát hiện xâm nhập IPS đã không thể ngăn chặn được các truy cập trái phép.

c. Kịch bản 3: Tấn công Reverse TCP xâm nhập hệ thống từ bên ngoài, với trường hợp hệ thống tích hợp tường lửa Sophos UTM

Thực nghiệm này sử dụng tường lửa thế hệ mới với cùng mô hình sơ đồ mạng như trong hình 12 (chỉ thay thế ASA bởi Sophos UTM, và không cần dùng TMG). Kết quả cho thấy, mọi cố gắng của kẻ tấn công đều bị ngăn chặn bởi tường lửa này. Điều này cho thấy, với các tường lửa có các tính năng cập nhật hiện đại sẽ đóng vai trò rất quan trọng trong việc ngăn chặn các cuộc tấn công kiểu Reverse TCP.

d. Nhận xét chung về kết quả tấn công mạng sử dụng kiểu Reverse TCP:

Từ thực nghiệm đã trình bày cho thấy, kẻ tấn công có thể truy cập vào hệ thống trong trường hợp là gián điệp (đứng bên trong mạng nội bộ) hoặc khi đứng bên ngoài mạng Internet. Tuy nhiên, nếu hệ thống có tích hợp các loại tường lửa mới, hiện đại thì sẽ cản trở việc tấn công ở mức tối đa. Kết quả so sánh được thể hiện như trong bảng 2:

Bảng 2. *Kết quả so sánh các kiểu tấn công Reverse TCP qua 3 kịch bản*

Kiểu tấn công	Mức độ xâm nhập máy tính của nạn nhân	Phát hiện tấn công	Mức độ tải của mạng
Reverse TCP bên trong mạng nội bộ	Có	Không	Không
Reverse TCP với hệ thống tích hợp ASA, TMG, IPS	Có	Không	Không
Reverse TCP với hệ thống tích hợp Sophos UTM	Không	Không	Không

4. Kết luận

Thông qua việc nghiên cứu, đánh giá thực nghiệm một số kiểu tấn công phổ biến trên các hệ thống mạng mô phỏng lại các sơ đồ mạng thực tế của các tổ chức/ công ty tại Việt Nam cho thấy các hệ thống này luôn có thể bị tấn công bởi các kiểu tấn công điển hình như DoS, SQL Injection hoặc Reserve TCP bất kỳ lúc nào, đặc biệt là khi kẻ tấn công dùng hình thức tấn công kiểu UDP flood thông qua tấn công DoS, SQL Injection. Những vấn đề về điểm yếu hệ thống này có thể được hạn chế, tránh được khi hệ thống được tích hợp các giải pháp phòng thủ như sử dụng các loại tường lửa mới (tường lửa cứng hoặc mềm), hiện đại được cập nhật các tính năng mạnh mẽ như có khả năng phát hiện các dấu hiệu bất thường, lọc gói tin cấp độ cao, cảnh báo cho người quản trị các mối nguy hiểm,…

Bên cạnh vấn đề kỹ thuật, nghiên cứu cũng cho thấy rằng, sự cảnh giác cao độ cũng như sự chuẩn bị kiến thức về an ninh, an toàn mạng cho nhà quản trị luôn luôn rất quan trọng, với phương châm phòng hơn tránh để từ đó nhà quản trị có các giải pháp phù hợp, linh động, cập nhật với các cuộc tấn công mới, ngày càng tinh vi và khó lường được hiệu quả hơn.

TÀI LIỆU THAM KHẢO/REFERENCES

[1]. R. Baloch, *Ethical Hacking and Penetration Testing Guide*, CRC Press, 2015.

[2]. L. H. Hiep et al., "Study to applying Blockchain technology for preventing of spam email," *TNU Journal of Science and Technology*, vol. 208, no. 15, pp. 161-167, 2019.

[3]. A. Maraj et al., "Testing of network security systems through DoS attacks," *Embedded Computing (MECO), 6th Mediterranean Conference on. IEEE*, 2017.

[4]. A. Maraj et al., "Testing techniques and analysis of SQL injection attacks," *Knowledge Engineering and Applications (ICKEA), 2017 2nd International Conference on. IEEE*, 2017.

[5]. T. Hayajneh et al., "Performance and Information Security Evaluation with Firewalls," *International Journal of Security and Its Applications, SERSC*, vol. 7, no. 6, pp. 355-372, 2013.

[6]. D. Loganathan, and K. Ramesh, "Prevention Mechanism for Denial of Service in Web Applications Services," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 4, pp. 480-484, 2015.

[7]. G. Weidman, *Penetration Testing: A Hands-on Introduction to Hacking*, No Starch Press, 2014.