Nghiên cứu giải pháp giám sát an toàn thông tin mã nguồn mở cho cổng thông tin điện tử Trường Đại học Nguyễn Tất Thành

Nguyễn Hoàng Sơn*
Phòng Khoa học Công nghệ, Trường Đại học Nguyễn Tất Thành, Thành phố Hồ Chí Minh
*nguyen.son@ntt.edu.vn

Tóm tắt

Bài báo trình bày nghiên cứu một giải pháp giám sát an toàn thông tin dựa trên các công cụ mã nguồn mở cho cổng thông tin điện tử Trường Đại học Nguyễn Tất Thành. Mục tiêu nhằm giải quyết những hạn chế trong công tác giám sát hiện tại, vốn chỉ dừng ở mức giám sát hoạt động mà thiếu phân tích log và cảnh báo tập trung. Đề tài tập trung vào ba nhiệm vụ chính: (1) khảo sát và đánh giá hiện trạng hệ thống, (2) nghiên cứu, lựa chọn và tích hợp các công cụ mã nguồn mở phù hợp, và (3) triển khai thử nghiệm, xây dựng kịch bản kiểm thử và đánh giá hiệu quả giải pháp. Mô hình thử nghiệm đã tích hợp thành công OSSEC, ELK Stack và Snort, thu thập và phân tích log tập trung, đồng thời thiết lập được cảnh báo cho nhiều tình huống tấn công mạng như DDoS, Brute force, SQL Injection, XSS và CSRF. Kết quả cho thấy giải pháp đề xuất hoàn toàn có khả năng nâng cao năng lực giám sát, phát hiện và cảnh báo sớm các mối đe dọa, góp phần đảm bảo an toàn thông tin cho hệ thống. Tuy nhiên, phạm vi thử nghiệm còn hạn chế, chưa bao quát hết các dạng tấn công phức tạp và đa môi trường. Bài báo cũng đề xuất hướng phát triển mở rộng như kết nối với các API phân tích malware (VirusTotal), bổ sung kênh cảnh báo tự động qua email và đa dạng hóa kịch bản tấn công kiểm thử.

Nhận 22/10/2025
Được duyệt 18/11/2025
Công bố 25/11/2025

Từ khóa
An toàn thông tin; Giám sát hệ thống; SIEM mã nguồn mở; OSSEC; ELK Stack; Snort.

1. Đặt vấn đề

Theo kết quả được báo cáo từ khảo sát của Hiệp hội An ninh mạng quốc gia, 46,15 % cơ quan, doanh nghiệp tại Việt Nam đã từng bị tấn công mạng ít nhất 1 lần trong năm 2024, trong đó 6,77 % thường xuyên bị tấn công. Tổng số vụ tấn công mạng nhắm vào các các đơn vị tại Việt Nam trong năm 2024 ước tính lên tới hơn 659.000 vụ [1]. Đặc biệt, các cổng thông tin điện tử của các cơ sở giáo dục trở thành mục tiêu hấp dẫn do chứa nhiều dữ liệu quan trọng, tuy nhiên nhiều hệ thống vẫn tồn tại lỗ hổng nghiêm trọng, bị tấn công lặp lại nhiều lần để lại nhiều hậu quả mà chưa có giải pháp khắc phục triệt để. Cục An toàn thông tin – Bộ Thông tin và Truyền thông công bố trong Báo cáo tổng hợp tình hình an toàn, an ninh mạng Việt Nam tháng 12/2023 đã có 342 trang thông tin điện tử thuộc lĩnh vực giáo dục sử dụng tên miền .edu.vn và 212 trang của các cơ quan nhà nước mang tên miền .gov.vn bị tin tặc tấn công. Đáng chú ý, một số lượng không nhỏ các website này bị xâm nhập nhiều lần, cho thấy các biện pháp khắc phục hiện tại chưa thực sự triệt để, tiềm ẩn nguy cơ mất an toàn thông tin kéo dài và tái diễn [2].

Các nghiên cứu về hệ thống giám sát an toàn thông tin đều nhấn mạnh vai trò quan trọng của công cụ SIEM trong các Trung tâm Điều hành An ninh (SOC) trong việc thu thập, chuẩn hóa và phân tích các sự kiện bảo mật từ nhiều nguồn khác nhau tuy nhiên SIEM cần phải phát triển để vượt qua các vấn đề về khả năng mở rộng trong tương lai[3]. Mặc dù các giải pháp SIEM thương mại độc quyền đã chiếm ưu thế trên thị trường trong một thời gian dài, nhưng các hệ thống SIEM mã nguồn mở ngày càng được ưa chuộng nhờ khả năng tiếp cận dễ dàng và tính kinh tế, đặc biệt phù hợp với các doanh nghiệp vừa và nhỏ (SME) [4]. Một số công trình đã chỉ ra tích hợp các công cụ mã nguồn mở khác nhau có thể tạo thành môt hệ thống SIEM hoàn chỉnh để tận dụng những ưu điểm của từng công cụ và đáp ứng được các yêu cầu cụ thể của tổ chức và doanh nghiệp. Cụ thể trong nghiên cứu của Manzoor và cộng sự (2025) đã cho thấy khả năng tích hợp của các công cụ Wazuh, ELK, OSSEC và Suricata trong việc hình thành SIEM hoàn chỉnh cho doanh nghiệp vừa và nhỏ.

Nhóm tác giả chỉ ra rằng việc kết hợp các công cụ mã nguồn mở có thể tạo nên "a low-cost yet effective SOC environment"[4]. Nghiên cứu của Kumar và cộng sự (2025), trình bày mô hình tích hợp Zeek + ELK + Wazuh để cải thiện khả năng phát hiện tấn công trong SOC. Nghiên cứu khẳng định rằng sự kết hợp giữa khai thác tối đa ưu điểm của từng thành phần – gồm giám sát gói tin theo thời gian thực, ghi nhật ký tập trung và tương quan cảnh báo – nhằm hình thành một hệ thống SIEM toàn diện [5].

Cổng thông tin điện tử của Trường Đại học Nguyễn Tất Thành (NTTU) là nền tảng trực tuyến quan trọng, vừa cung cấp thông tin – dịch vụ cho cộng đồng trường, vừa hỗ trợ sinh viên, giảng viên và nhân viên trong học tập, nghiên cứu và quản lý. Tuy nhiên, hệ thống hiện mới dừng ở mức giám sát tình trạng hoạt động, chỉ triển khai tường lửa cho một số trang web riêng lẻ và chưa có giải pháp SIEM hoàn chỉnh. Việc thiếu giám sát và phân tích log khiến khả năng phát hiện, cảnh báo và ứng phó với các mối đe dọa an ninh mạng còn hạn chế dẫn đến nguy cơ mất an toàn thông tin và khó khăn trong điều tra, khắc phục sự cố. Đây chính là khoảng trống nghiên cứu mà bài báo này hướng tới nhằm đề xuất và thử nghiệm một giải pháp giám sát tập trung mã nguồn mở, có khả năng phát hiện các mối đe dọa an ninh mạng cho cổng thông tin điện tử của NTTU.

Các đóng góp chính của nghiên cứu như sau:

a. Đề xuất và triển khai mô hình SIEM mã nguồn mở tích hợp OSSEC, Snort và ELK Stack phù hợp với môi trường đại học và nhu cầu giám sát tập trung

b. Xây dựng testbed thử nghiệm và bộ kịch bản tấn công thực tế, đánh giá khả năng thu thập log, phân tích và phát hiện tấn công một cách định lượng.

c. Cung cấp bộ kết quả thực nghiệm chứng minh hiệu quả mô hình, đồng thời đề xuất hướng mở rộng như tích hợp phân tích malware và phát triển cơ chế cảnh báo tự động.

2. Phương pháp nghiên cứu

2.1 Khảo sát hiện trạng hạ tầng công nghệ thông tin và cổng thông tin điện tử.

2.1.1. Đội ngũ quản trị và vận hành hệ thống

NTTU hiện có đội ngũ cán bộ quản trị thông tin với trình độ chuyên môn từ bậc đại học trở lên, đảm nhiệm công tác quản trị, vận hành hệ thống CNTT và ứng dụng trong toàn trường. Bên cạnh đó, nhiều cán bộ đã có thâm niên công tác, tích lũy được kinh nghiệm thực tiễn trong việc xây dựng và quản lý hệ thống thông tin chuyên ngành, hỗ trợ kỹ thuật và đảm bảo an toàn thông tin cho người dùng.

Hiện nay, Phòng Quản trị Thông tin có tổng cộng 15 cán bộ CNTT, trong đó có 5 cán bộ phụ trách quản trị mạng/IT helpdesk và 2 cán bộ chuyên trách về an toàn thông tin. Tuy nhiên, về nhân sự hiện vẫn còn một số hạn chế: (i) phần lớn cán bộ thiếu chuyên môn sâu về an toàn thông tin, chủ yếu được đào tạo ngắn hạn và làm việc dựa vào kinh nghiệm; (ii) lực lượng CNTT có xu hướng giảm do sắp xếp lại tổ chức bộ máy; (iii) việc đầu tư toàn diện cho công tác ATTT của nhà trường chưa được chú trọng đúng mức.

2.1.2. Cổng thông tin điện tử

Cổng thông tin điện tử (ntt.edu.vn) là hạ tầng số trọng yếu của Trường, cung cấp nhiều dịch vụ trực tuyến phục vụ sinh viên, giảng viên và cán bộ. Theo số liệu Google Analytics trong năm 2023, website đã ghi nhận 725.877 lượt truy cập, với trung bình 1.987 người dùng/ngày, cao nhất đạt 5.734 người dùng/ngày, trong đó có 545.379 người dùng mới. Các con số này cho thấy quy mô và tầm quan trọng của hệ thống trong hoạt động đào tạo, nghiên cứu và quản lý của Trường.

Về chức năng, cổng thông tin điện tử tích hợp nhiều hệ thống: (i) quản lý học tập (LMS, thư viện điện tử); (ii) quản lý thông tin sinh viên (SIS, cổng thông tin sinh viên); (iii) quản lý giảng viên và nhân sự; (iv) quản lý hành chính – tài chính; và (v) các dịch vụ tương tác, hỗ trợ như diễn đàn, mạng xã hội nội bộ, hệ thống hỗ trợ trực tuyến.

Về công nghệ, hệ thống được xây dựng trên nền tảng đa dạng: PHP, WordPress, Python, Laravel, ASP.NET, Node.js, Next.js, chạy trên các web server Apache, Nginx và hệ điều hành Ubuntu, Windows, sử dụng cơ sở dữ liệu MySQL. Máy chủ vật lý là Dell PowerEdge R740, với cấu hình mạnh mẽ gồm 2 CPU Intel Xeon Gold 6226R 2.9 GHz, 64GB RAM, 2 ổ SSD 960GB và 2 ổ HDD 2TB, bảo đảm khả năng xử lý và lưu trữ dữ liệu lớn. Về bảo mật, hệ thống hiện áp dụng SSL/TLS và tường lửa ứng dụng web (WAF) nhằm mã hóa dữ liệu và chặn lọc một số tấn công phổ biến.

2.1.3. Đánh giá nguy cơ mất an toàn thông tin

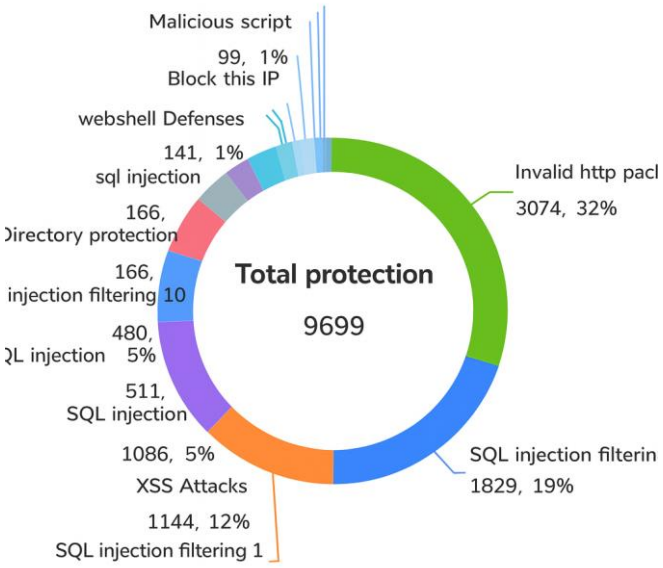
Mặc dù cổng thông tin điện tử đã triển khai nhiều biện pháp bảo mật cơ bản, vẫn tồn tại nhiều nguy cơ tiềm ẩn. Biểu đồ thống kê cho thấy số lượng sự kiện tấn công và cảnh báo ghi nhận lên tới 9.699, trong đó nổi bật là các gói tin HTTP bất hợp lệ (32 %), SQL Injection (19 %), XSS Attacks (5 %), cùng nhiều mối đe dọa khác như webshell, malicious script hay brute force. Điều này cho thấy cổng thông tin điện tử NTTU đang là mục tiêu của nhiều cuộc tấn công mạng, đặc biệt là các cuộc tấn công khai thác lỗ hổng SQL, XSS, DDoS và webshell. WAF đã hoạt động hiệu quả, tuy nhiên cần xem xét bổ sung các

biện pháp bảo vệ, nâng cấp mã hóa và bảo vệ các tệp nhạy cảm như tệp backup, và theo dõi các IP và hành vi tấn công.

Bảng 1 Các nguy cơ, nguyên nhân và hậu quả tiềm ẩn về an toàn thông tin

Nguy cơ	Nguyên nhân	Hậu quả
Cơ sở dữ liệu MySQL	- Kiểm soát đầu vào chưa chặt chẽ - Phân quyền chưa chặt chẽ, mật khẩu yếu, dữ liệu nhạy cảm chưa được mã hóa - Sử dụng phiên bản cũ tiềm ẩn lỗ hổng	- Rò rỉ hoặc thay đổi dữ liệu - Chiếm quyền điều khiển CSDL - Nguy cơ gián đoạn hệ thống
Công nghệ web (PHP, Node.js, Apache)	- PHP: nguy cơ XSS, CSRF - Node.js: rủi ro từ thư viện bên thứ ba - Apache: dễ bị khai thác nếu cấu hình sai (Directory Traversal, SSRF)	- Chèn mã độc, đánh cắp dữ liệu người dùng - Mất quyền kiểm soát máy chủ web - Ảnh hưởng toàn bộ dịch vụ trực tuyến
Quản lý phiên và xác thực	- Cơ chế bảo vệ session ID yếu - Thiếu biện pháp chống chiếm đoạt phiên	- Người tấn công chiếm đoạt tài khoản người dùng - Mất an toàn dữ liệu cá nhân và giao dịch
Thiếu giải pháp SIEM tập trung	- Chỉ dựa vào WAF riêng lẻ - Chưa có cơ chế thu thập log tập trung, phân tích và cảnh báo sớm	- Khó phát hiện tấn công phức tạp - Chậm trễ trong ứng phó sự cố - Giảm hiệu quả giám sát toàn hệ thống

Số liệu thống kê trong tháng 08/2024 được các loại tấn công web đã bị WAF phát hiện và chặn như sau:



Hình 1 Thống kê hoạt động của tưởng lửa Website trong tháng 08/2024 tại trường NTTU

2.2 Nghiên cứu và lựa chọn giải pháp SIEM dựa trên mã nguồn mở.

Căn cứ vào hiện trạng cổng thông tin điện tử NTTU, các điểm yếu, các nguy cơ tiềm ẩn về mất an toàn thông tin có thể xảy ra thì bài toán đặt ra tập trung vào việc giám sát an toàn thông tin nhằm bảo vệ hệ thống khỏi các mối đe dọa và đảm bảo sự an toàn, bảo mật cho dữ liệu và người dùng như sau:

- Giám sát và phát hiện các hành vi bất thường: nhận diện các tương tác bất thường giữa người dùng và ứng dụng web, bao gồm thông tin đăng nhập, giao dịch và dữ liệu nhạy cảm.
- Phát hiện tấn công lỗ hổng bảo mật: nhận diện và ngăn chặn các cuộc tấn công khai thác lỗ hổng bảo mật như SQL Injection, Cross-Site Scripting (XSS), và các lỗ hổng trong mã nguồn ứng dụng.
- Giám sát và phân tích nhật ký truy cập: theo dõi và phân tích nhật ký truy cập để phát hiện sớm các hành vi bất thường hoặc các cuộc tấn công.

Để giải quyết được bài toán nêu trên, NTTU cần xây dựng một giải pháp giám sát an toàn thông tin toàn diện cho cổng thông tin điện tử: triển khai phần mềm SIEM tích hợp hệ thống phát hiện/xâm nhập có khả năng giám sát, phát hiện hình vi bất thường tương tác giữa người dùng và ứng dụng web (gồm cả thông tin đăng nhập, giao dịch và dữ liệu nhạy cảm) và theo dõi hoạt động của người dùng; giám sát phát hiện tấn công lỗ hổng bảo mật (như SQL injection, XSS), và các lỗ hổng bảo mật trong mã nguồn ứng dụng; giám sát đảm bảo an toàn cho dữ liệu

người dùng, các Database, Giám sát phân tích nhật ký truy cập,…

Như vậy, có thể thấy lựa chọn giải pháp xây dựng một hệ thống giám sát ATTT dựa trên phần mềm mã nguồn mở, triển khai theo mô hình giám sát an toàn thông tin tập trung cho Cổng thông tin của Trường là hợp lý và giải pháp tích hợp OSSEC, ELK Stack là phù hợp để triển khai vì các lý do được mô tả bằng bảng sau đây:

Bảng 2 So sánh, lựa chọn các giải pháp giám sát an toàn thông tin dựa trên các tiêu chí [4,6,7].

Tiêu chí đánh giá	ELK tích hợp OSSEC	ALIEN VAULT OSSIM	Nagios	Icinga	Suricata tích hợp ELK	Zeek tích hợp ELK
Giám sát trên máy chủ	+	+	+	+	-	-
Tính linh hoạt tùy biến cao	+	+	-	+	+	+
Phần mềm miễn phí	+	+	+	+	+	+
Khả năng phân tích log và báo cáo	+	-	-	-	+	+
Khả năng tích hợp các công cụ	+	+	-	+	+	+
Cộng đồng hỗ trợ phát triển	+	+	+	+	+	+

2.3 Triển khai thử nghiệm mô phỏng.

Máy chủ thử nghiệm sử dụng cấu hình 8 vCPU, 16 GB RAM và ổ SSD NVMe (I/O ~ 850 MB/s). Trong 24 giờ thử nghiệm, hệ thống tạo ra khoảng 5,5 GB log từ Apache, Snort và OSSEC.

Trong khuôn khổ của nghiên cứu này, đề xuất mô hình triển khai tập trung, các thành phần cần triển khai bao gồm:

+ Máy chủ OSSEC với các thành phần như sau: Ubuntu 20.04 LTS, OSSEC 3.9.5, Elasticsearch 6.8.0, Filebeat 7.3.0, Kibana 7.3.0.

+ OSSEC agent , Filebeat 7.17.23 và Snort 2.9.20.1 cài tại máy chủ Web.

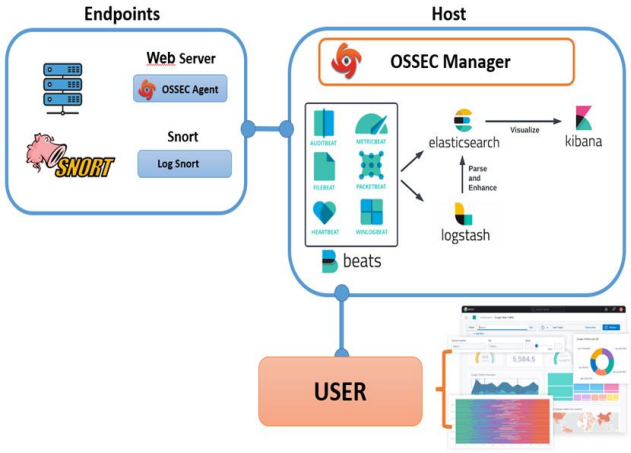
Mô hình giám sát thử nghiệm đối với hệ thống mạng trong hình trên có luồng dữ liệu như sau:

(1)- Các thiết bị mạng, máy chủ, máy trạm, Snort sẽ đẩy nhật ký về máy chủ OSSEC.

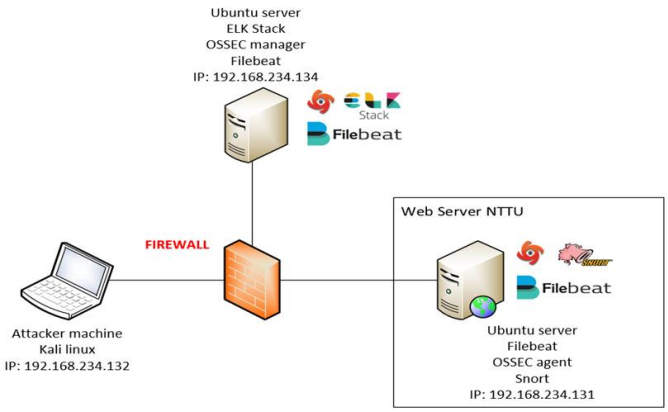
(2)- Tại máy chủ OSSEC manager các sự kiện này được xử lý, các kết quả sau phân tích được so sánh với tập rule đã được thiết lập từ trước đó, nếu khớp với điều kiện của rule nào đó sẽ sinh ra cảnh báo cho hệ thống.

(3)- Tại đây Filebeat được sử dụng để chuyển tiếp các cảnh báo (warning) và các sự kiện tới Elasticsearch. Elasticsearch sẽ lập chỉ mục cho dữ liệu (database index)

(4)- Cuối cùng, Kibana được sử dụng để trực quan hiển thị thông tin qua giao diện WUI và các sự kiện, cảnh báo được hiển thị trực quan hóa bằng biểu đồ, sự kiện dưới dạng đã chuẩn hóa.



Hình 2 Mô hình luồng dữ liệu



Hình 3 Sơ đồ kết nối các thiết bị trong mô hình triển khai thử nghiệm

Mô hình triển khai tất cả trong một: OSSEC, ELK Stack và Snort được cài đặt trên cùng một máy chủ. Mô hình này thích hợp cho các môi trường thử nghiệm và quy mô của tổ chức nhỏ.

Bảng 3 Hạng mục công việc thực hiện:

TT	Hạng mục công việc	Diễn giải	Ghi chú
1.	Thiết lập mô hình mạng như hình vẽ	Kết nối các thiết bị, cấu hình thiết bị	
2.	Chuẩn bị máy chủ OSSEC và ELK Stack	- IP: 192.168.234.134/24	*Ubuntu 20.04 LTS, Apache 2.4.x, OSSEC 3.9.5, Elasticsearch 6.8.0, Filebeat 7.17.23, Kibana 7.3.0, Logstash 7.3.0*
3.	Cài đặt OSSEC server và các thành phần	Kết nối máy chủ OSSEC với hệ điều hành Ubuntu với mạng internet	
4.	Xây dựng website mô phỏng cổng thông tin điện tử trường ĐH Nguyễn Tất Thành	- IP: 192.168.234.131/24	
5.	Cài đặt OSSEC agent trên máy chủ Web	Kết nối các máy chủ và máy trạm vào hệ thống mạng, tiến hành cài đặt OSSEC agent để thu thập log	
6.	Cài đặt Snort và cấu hình Snort để đẩy log Web về máy chủ OSSEC	Thực hiện cài đặt và cấu hình Snort	*Snort 2.9.20.1*

3. Kết quả và thảo luận

3.1. Tích hợp hệ thống:

Trong mô hình thử nghiệm, ba công cụ mã nguồn mở đã được tích hợp nhằm tạo thành một giải pháp giám sát an toàn thông tin tương đối toàn diện:

OSSEC: đóng vai trò hệ thống giám sát xâm nhập dựa trên host (HIDS), thực hiện thu thập log, giám sát tính toàn vẹn tệp tin và cảnh báo các hành vi bất thường [8].

ELK Stack (Elasticsearch – Logstash – Kibana): đảm nhiệm chức năng phân tích log, lưu trữ tập trung và trực quan hóa dữ liệu, giúp quản trị viên theo dõi sự kiện bảo mật một cách trực quan và dễ dàng [9].

Snort: hoạt động như hệ thống phát hiện xâm nhập dựa trên mạng (NIDS), hỗ trợ phát hiện các hành vi tấn công phổ biến dựa trên chữ ký (signature-based detection) [10]. Sự kết hợp này cho phép giám sát cả trên cấp độ máy chủ lẫn cấp độ mạng, đồng thời cung cấp giao diện trực quan để quản lý sự kiện an ninh.

Hình 4 Mô hình tích hợp OSSEC, ELK và Snort

Cấu hình các thành phần thu thập log từ Website Apache như sau:

```
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /var/log/apache2/access.log
    - /var/log/apache2/error.log
```

Hình 5 Cấu hình Filebeat thêm input cho Apache trong tệp cấu hình /etc/filebeat/filebeat.yml

```
filebeat.inputs:
  - type: log
    enabled: true
    paths:
     - /var/log/snort/*.log
  fields:
    log_format: snort-full
    fields_under_root: true
```

Hình 6 Cấu hình Filebeat nhận log nhận log từ Snort trong tệp cấu hình /etc/filebeat/filebeat.yml

```
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/access.log</location>
</localfile>
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/error.log</location>
</localfile>
```

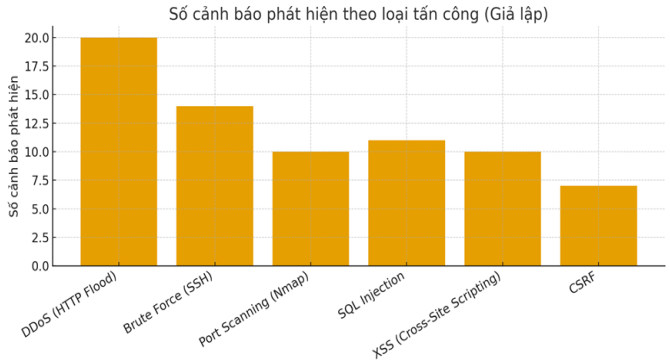
Hình 7 Cấu hình OSSEC để thu thập log từ Apache trong tệp cấu hình /var/ossec/etc/ossec.conf

3.2. Các kịch bản kiểm thử:

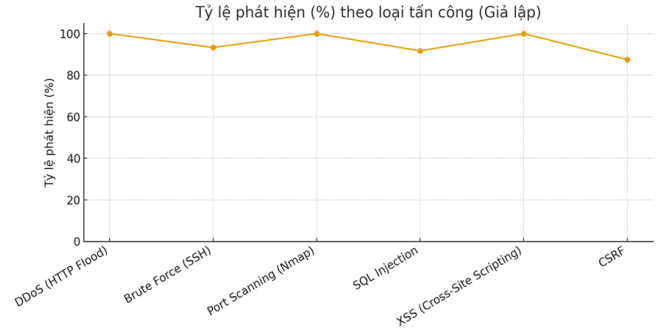
Hệ thống đã được thử nghiệm với các dạng tấn công DDoS, Brute force, Port scanning, SQL Injection, XSS và CSRF. Kết quả cho thấy hệ thống phát hiện thành công các cuộc tấn công, ghi log đầy đủ và đưa ra cảnh báo trực quan trên Kibana như sau:

Bảng 4 Kết quả kiểm thử phát hiện tấn công (mô phỏng).

Loại tấn công	Số lần thử nghiệm	Số cảnh báo phát hiện	Tỷ lệ phát hiện (%)
DDoS (HTTP Flood)	20	20	100.0
Brute Force (SSH)	15	14	93.3
Port Scanning (Nmap)	10	10	100.0
SQL Injection	12	11	91.7
XSS (Cross-Site Scripting)	10	10	100.0
CSRF	8	7	87.5

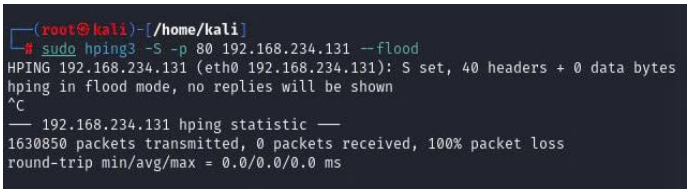


Hình 8 Số cảnh báo phát hiện theo loại tấn công (giả lập)

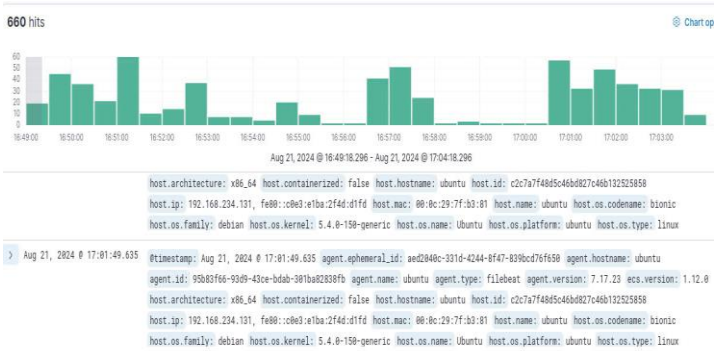


Hình 9 Tỷ lệ phát hiện (%) theo loại tấn công (giả lập)

3.2.1 Tấn công từ chối dịch vụ phân tán (DDoS):



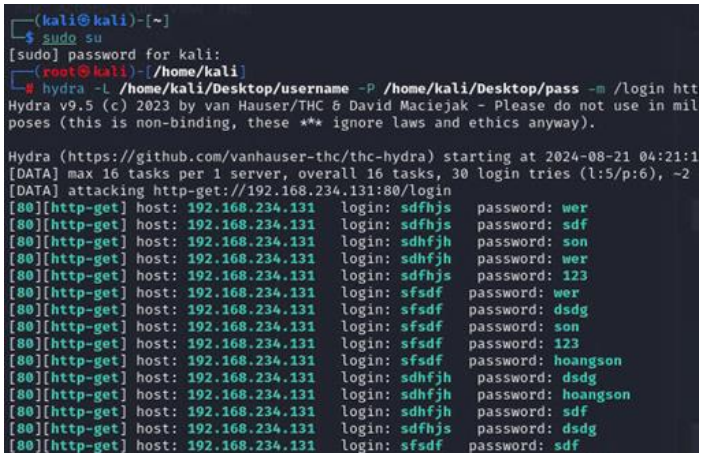
Hình 10 Tại máy Kali, thực hiện tấn công DOS với dạng SYN Flood bằng lệnh Hping3



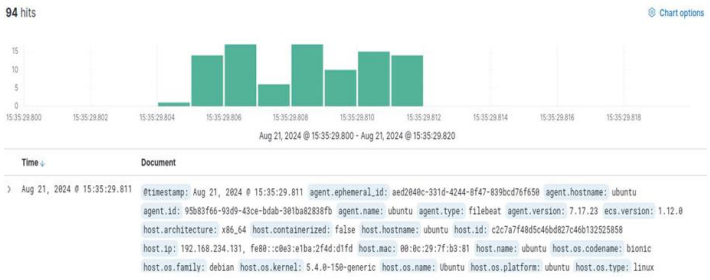
Hình 11 Trên Kibana hiển thị cảnh báo sự kiện bất thường

Hình 12 Hiển thị cảnh báo trên WUI – tấn công DOS

3.2.2 Tấn công Brute Force vào dịch vụ xác thực.



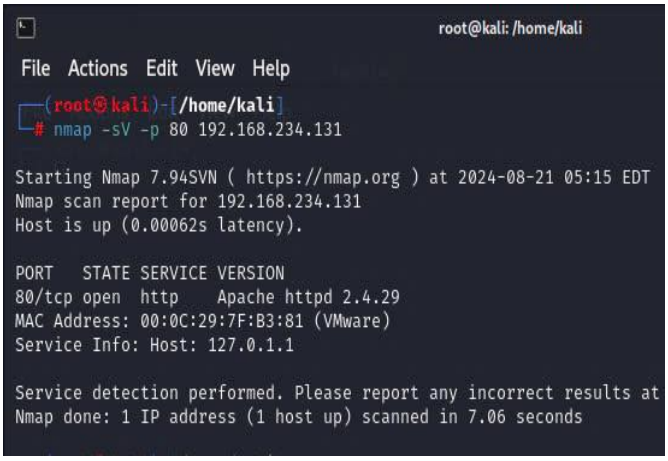
Hình 13 Tại máy Kali, thực hiện tấn công Brute Force bằng lệnh Hydra



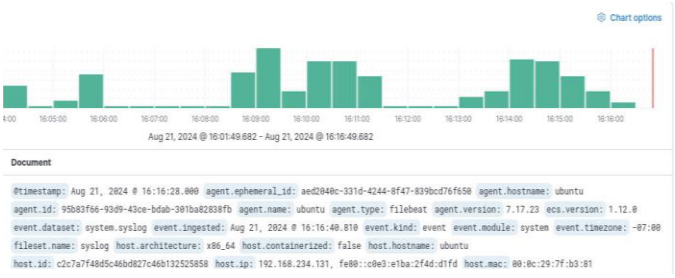
Hình 14 Trên Kibana hiển thị cảnh báo sự kiện tăng cao bất thường

Hình 15 Hiển thị cảnh báo trên WUI – tấn công Brute Force

3.2.3 Quét cổng (Port Scanning) để dò tìm dịch vụ mở.



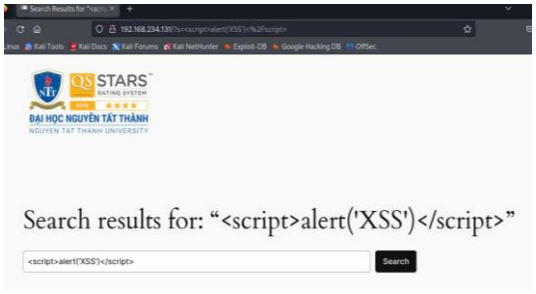
Hình 16 Tại máy Kali, thực hiện tấn công hình thức Scan port bằng lệnh Nmap



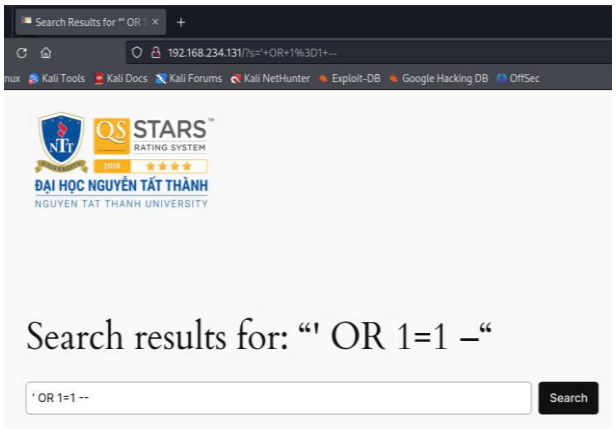
Hình 17 Trên Kibana hiển thị cảnh báo sự kiện tăng cao bất thường

Hình 18 Hiển thị cảnh báo trên WUI – tấn công Scan port bằng Nmap

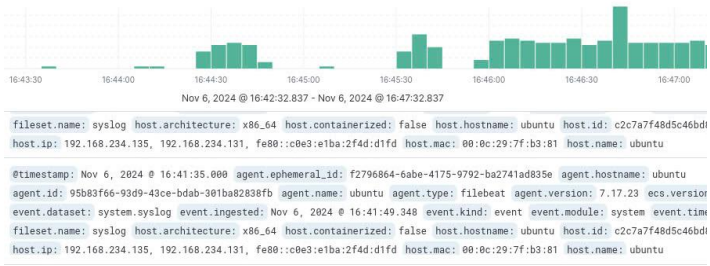
3.2.4 Cross-Site Scripting (XSS), SQL Injection:



Hình 19 Nhập nhiều lần payload XSS <script>alert('XSS')</script> vào trường tìm kiếm từ máy Kali vào Website



Hình 20 Nhập nhiều lần chuỗi sau vào trường tìm kiếm từ máy Kali máy Kali vào Website NTTU:' OR 1=1 –



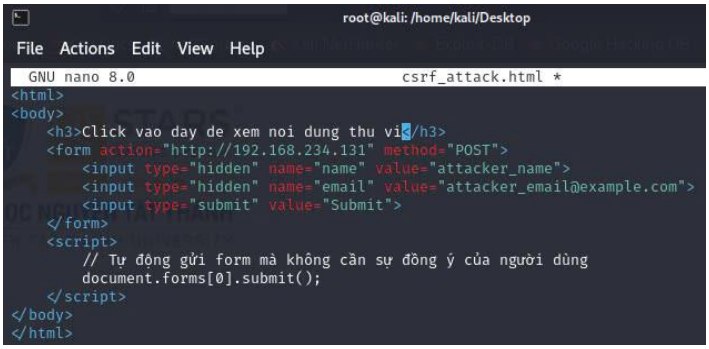
Hình 21 Trên Kibana hiển thị cảnh báo sự kiện tăng cao bất thường

Hình 22 Hiển thị cảnh báo trên WUI – tấn công XSS

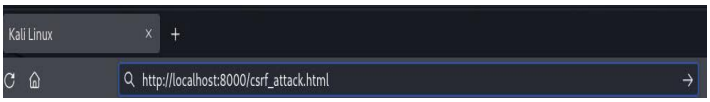
Hình 23 Hiển thị cảnh báo trên WUI – tấn công SQL Injection

3.2.5 Cross-Site Request Forgery (CSRF):

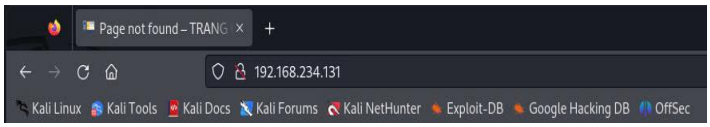
Kết quả kiểm thử cho thấy, hệ thống đã phát hiện thành công các cuộc tấn công trên, ghi nhận log đầy đủ, đồng thời hiển thị cảnh báo trực quan trên giao diện Kibana. Điều này chứng minh tính hiệu quả của mô hình tích hợp trong việc nhận diện các mối đe dọa an ninh mạng phổ biến.



Hình 24 Tạo file HTML giả mạo csrf_attack.html từ máy Kali linux



Hình 25 Truy cập trang HTML từ trình duyệt http://localhost:8000/csrf_attack.html



Hình 26 Khi truy cập trang này, JavaScript trong file HTML sẽ tự động gửi yêu cầu POST đến địa chỉ mục tiêu http://192.168.234.131

Hình 27 Hiển thị cảnh báo trên WUI Kibana – tấn công CSRF

3.3. Đánh giá:

Giải pháp tích hợp mang lại hiệu quả trong môi trường thử nghiệm, tuy nhiên hạn chế về phạm vi kịch bản tấn công và chưa triển khai trên diện rộng. Kết quả thử nghiệm cho thấy giải pháp tích hợp OSSEC – ELK Stack

– Snort mang lại hiệu quả rõ rệt trong môi trường thử nghiệm:

+ Khả năng thu thập log đa nguồn và phân tích tập trung được đảm bảo.

+ Các cuộc tấn công phổ biến được phát hiện và cảnh báo chính xác, giúp giảm thiểu nguy cơ bỏ sót sự kiện quan trọng.

+ Giao diện trực quan trên Kibana hỗ trợ quản trị viên dễ dàng theo dõi và xử lý sự cố.

Tuy nhiên, hệ thống vẫn tồn tại một số hạn chế:

+ Phạm vi kịch bản tấn công kiểm thử còn giới hạn, chưa bao phủ các dạng tấn công nâng cao (APT, ransomware, shellshock,…).

+ Mô hình mới chỉ triển khai trên quy mô thử nghiệm, chưa áp dụng trong môi trường thực tế với nhiều máy chủ và thiết bị mạng khác nhau.

+ Chưa tích hợp các chức năng phản ứng tự động hoặc kết nối với các nguồn dữ liệu tình báo mối đe dọa (Threat Intelligence).

+ Nhìn chung, kết quả nghiên cứu bước đầu khẳng định tiềm năng ứng dụng của giải pháp SIEM mã nguồn mở trong việc giám sát và bảo vệ hệ thống cổng thông tin điện tử tại NTTU, đồng thời đặt nền móng cho việc mở rộng và hoàn thiện trong giai đoạn tiếp theo.

4. Kết luận và đề xuất

Nghiên cứu đã chỉ ra rằng cổng thông tin điện tử của NTTU, với vai trò là hạ tầng trọng yếu trong quản lý và cung cấp dịch vụ số, đang đối diện với nhiều nguy cơ mất an toàn thông tin do hạn chế trong công tác giám sát và cảnh báo. Qua khảo sát hiện trạng, phân tích các nguy cơ tiềm ẩn và thử nghiệm mô hình tích hợp OSSEC – ELK Stack – Snort**,** nghiên cứu đã chứng minh tính khả thi của việc áp dụng các giải pháp SIEM mã nguồn mở nhằm tăng cường khả năng giám sát, phát hiện và cảnh báo bất thường trong hệ thống.

Bài báo đã nghiên cứu, lựa chọn và triển khai giải pháp giám sát an toàn thông tin dựa trên các công cụ mã nguồn mở tích hợp OSSEC, ELK Stack và Snort cho cổng thông tin điện tử NTTU. Kết quả thử nghiệm cho thấy hệ thống có khả năng giám sát, phát hiện và cảnh báo sớm các mối đe dọa an ninh mạng. Tuy nhiên, để áp dụng vào thực tế, cần mở rộng triển khai trên môi trường thật, bổ sung thêm các kịch bản tấn công phức tạp, tích hợp thêm các dịch vụ như VirusTotal API để phân tích malware, và phát triển kênh cảnh báo tự động qua email hoặc ứng dụng di động.

Lời cảm ơn

Tôi xin cảm ơn Trường Đại học Nguyễn Tất Thành, Thành phố Hồ Chí Minh đã hỗ trợ cho nghiên cứu này

Tài liệu tham khảo

1. Hiệp hội An ninh mạng Quốc gia. (2024). *Báo cáo khảo sát an ninh mạng Việt Nam năm 2024.*

2. Cục An toàn thông tin – Bộ Thông tin và Truyền thông. (2023). *Báo cáo tổng hợp tình hình an toàn, an ninh mạng Việt Nam năm 2023*.

3. International Journal of Research Publication and Reviews. (2025). *Security Information and Event Management (SIEM)*. *IJRPR*, 6(4).

4. Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). *Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs*. PLOS ONE, 19(3).

5. Kumar, R., Singh, M., & Kaur, J. (2025). Integration of open-source intrusion detection and log analytics tools for enhanced SIEM functionality. *International Journal of Information Security and Privacy*, *19*(2), 55–70.

6. M Sheeraz et al. (2024). *Revolutionizing SIEM Security: An Innovative Correlation … Sensors*, *24*(15):4901

7. Likitha, R., Tarun, N., Pallavi, P., & Gaonkar, V. V. (2024, December). *Enhancing threat detection: Integrating ELK stack with Suricata for SIEM. International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE).*

8. Cid, D., Hay, A., & Bray, R. (2008). *OSSEC host-based intrusion detection guide*. *Elsevier*.

9. Soma, V. (2024). *Monitoring and Observability with ELK (Elasticsearch, Logstash, Kibana)*. Journal of Engineering and Applied Sciences Technology.

10. Asad, M., Adhikari, M., & Gashi, I. (2024). *A perspective–retrospective analysis of diversity in signature-based open-source network intrusion detection systems*. *International Journal of Information Security*, 23(4), 791-808.

Open-source information security monitoring for the electronic portal of Nguyen Tat Thanh University

Nguyen Hoang Son*
Department of Science and Technology, Nguyen Tat Thanh University, Ho Chi Minh City
*nguyen.son@ntt.edu.vn

Abstact
This paper presents an open-source information security monitoring solution for the electronic portal of Nguyen Tat Thanh University. The study addresses limitations of the current monitoring approach, which lacks centralized log analysis and real-time alerting. The work focuses on three main tasks: (1) assessing the existing system, (2) selecting and integrating appropriate open-source security tools, and (3) implementing a testbed with attack scenarios to evaluate system performance. The proposed model integrates OSSEC, the ELK Stack, and Snort to provide centralized log collection, correlation, and alerting. The system successfully detects multiple attack types, including DDoS, brute-force, SQL injection, XSS, and CSRF. Experimental results indicate that the solution enhances monitoring capability, threat detection, and early warning for the university portal. However, the test scope remains limited and does not fully cover advanced or multi-layer attack vectors. Future work includes integration with malware analysis APIs (e.g., VirusTotal), automated alert channels such as email notifications, and broader penetration-testing scenarios.

Keywords Information security; System monitoring; Open-source SIEM; OSSEC; ELK Stack; Snort.