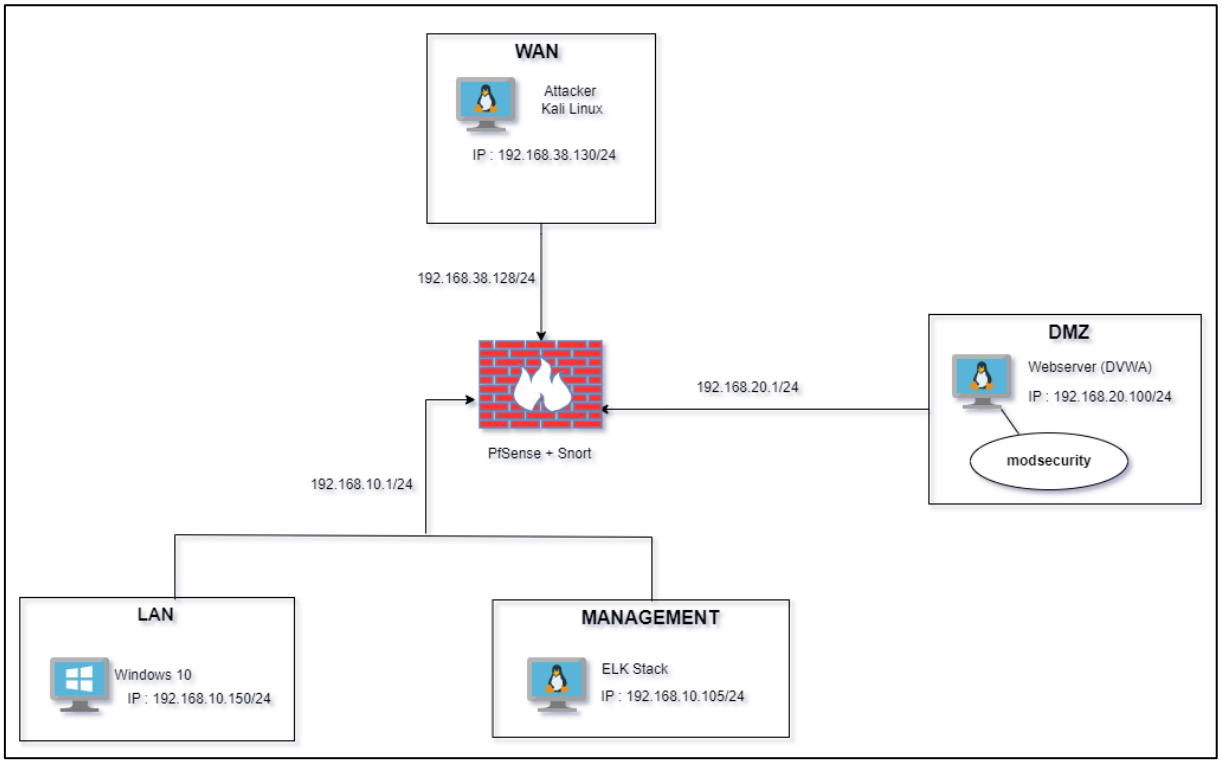
CHƯƠNG 3: TRIỂN KHAI KỊCH BẢN

Kịch bản 1: Phát hiện quét mạng qua theo dõi log Pfsense và Snort

1. Mục tiêu kịch bản.

Phát hiện hành vi quét cổng thông qua việc phân tích log được gửi từ pfSense và Snort đến hệ thống ELK Stack.

2. Các thành phần tham gia



- Pfsense: Ghi log tường lửa.
- Snort: IDS phát hiện hành vi quét mạng.
- ELK Stack: Nhận log, phân tích log và hiển thị kết quả
- Máy ảo Kali: máy tấn công thực hiện **`nmap -sS 192.168.20.100`** (TCP SYN Scan)

3. Luồng xử lý log

- Tấn công được thực hiện

- Attacker dùng lệnh nmap -sS từ máy Kali Linux ở mạng WAN để quét các cổng của máy Webserver trong mạng DMZ.
- Gói tin TCP SYN gửi đến nhiều cổng đích khác nhau, thể hiện hành vi reconnaissance (trinh sát mạng).

- pfSense ghi nhận log quét cổng

- pfSense ghi lại log dạng filterlog, chứa các thông tin:
    - giao thức, cổng nguồn, cổng đích, TCP flags (SYN), trạng thái chặn (block)
    - IP nguồn (attacker) và IP đích (nạn nhân)
- Snort trên pfSense cũng phát hiện các mẫu hành vi như "ET SCAN" và sinh cảnh báo với rule ID tương ứng.

- Chuyển log về ELK Stack

- pfSense được cấu hình để đẩy log về SIEM ELK thông qua giao thức syslog
- Cả log filterlog và snort được chuyển tới **Logstash** để xử lý.

- Logstash xử lý và phân tích

- Logstash sử dụng filter (Grok) để phân tích các trường trong log pfSense.
- Dựa vào nội dung và rule ID, Logstash:
    - tách các trường như src_ip, dst_ip, protocol, tcp_flags, msg
- Log sau khi xử lý được gửi vào Elasticsearch.

- Elasticsearch lưu trữ log

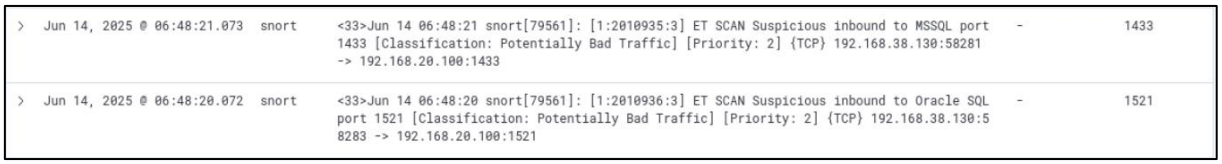
- Log được index theo thời gian, phân loại theo source (prog: filterlog, snort).
- Từ đó có thể truy vấn, tìm kiếm theo các trường đã được phân tích từ trước như src_ip, dst_port

- Kibana hiển thị và cảnh báo

- Dashboard trực quan hiển thị số lượng kết nối bị chặn, IP tấn công phổ biến, rule Snort kích hoạt.
- Alert được kích hoạt khi có log chứa các dấu hiệu port scan từ Snort hoặc quá nhiều gói tin SYN bị block trong thời gian ngắn.

4. Biểu hiện nhận biết tấn công

Dựa trên log Snort

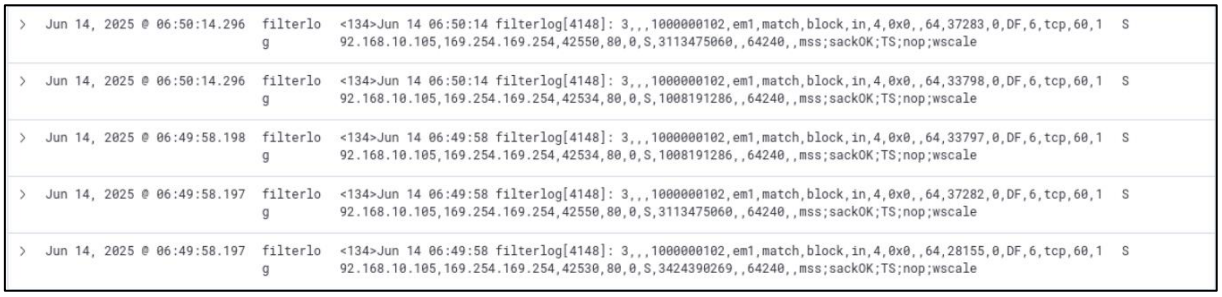


›	Jun 14, 2025 @ 06:48:21.073	snort	<33>Jun 14 06:48:21 snort[79561]: [1:2010935:3] ET SCAN Suspicious inbound to MSSQL port 1433 [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.38.130:58281 -> 192.168.20.100:1433	-	1433
›	Jun 14, 2025 @ 06:48:20.072	snort	<33>Jun 14 06:48:20 snort[79561]: [1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.38.130:58283 -> 192.168.20.100:1521	-	1521

- Snort phát hiện rõ ràng hành vi quét cổng từ attacker bằng các rule của snort

- Cảnh báo ET SCAN là rule signature của Emerging Threats – xác định hành vi quét rất phổ biến của Nmap.

Log pfSense có nhiều kết nối TCP SYN từ 1 IP



- Nhiều dòng có cùng Source IP → Dest IP, cùng port đích (80), nhưng source port thay đổi.
- Có flag SYN và bị block bởi pfSense.

5. Kết quả hiển thị Dashboard trên Kibana

6. Kết luận

Kịch bản 1 đã mô phỏng hành vi quét mạng sử dụng Nmap. Hệ thống đã ghi nhận các kết nối TCP bất thường trong log của pfSense và các cảnh báo do Snort phát hiện. Log được gửi về SIEM ELK để phân tích, chuẩn hóa, lưu trữ và phục vụ điều tra.

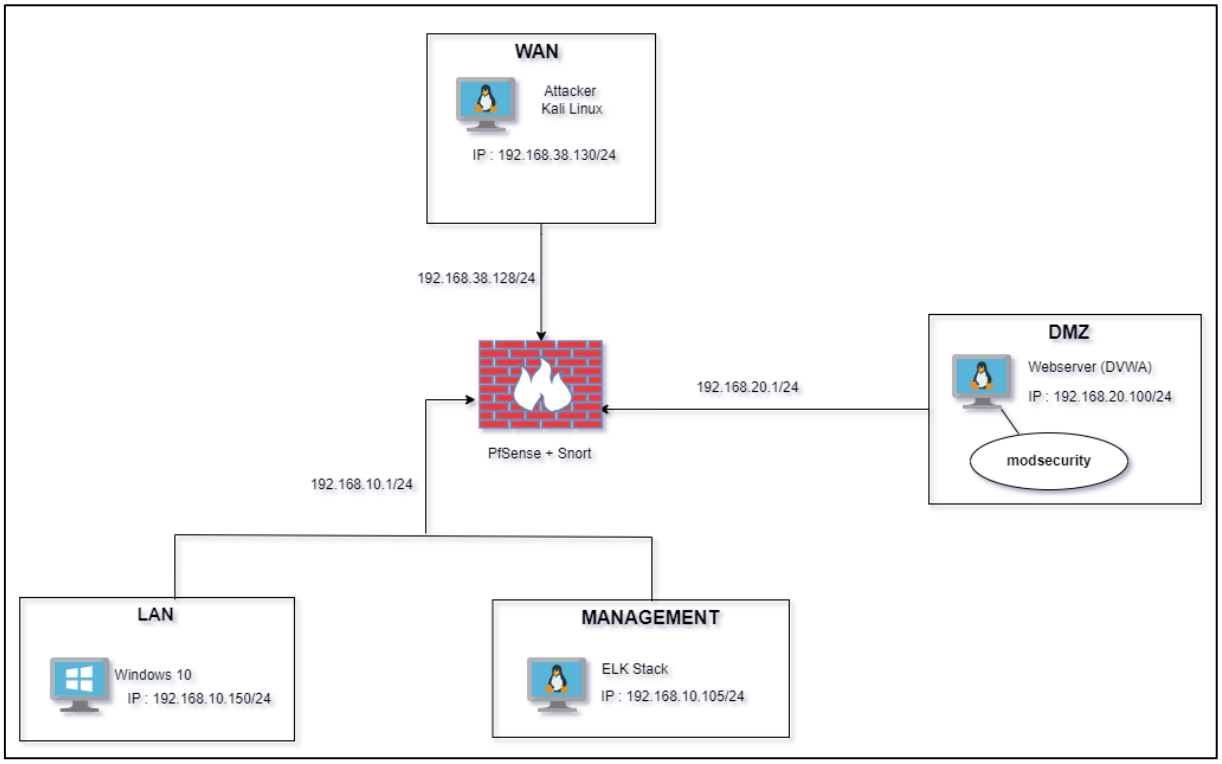
Kết quả cho thấy hệ thống hoạt động hiệu quả trong việc phát hiện hành vi trinh sát mạng (reconnaissance) sớm, góp phần nâng cao khả năng giám sát an ninh mạng.

Kịch bản 2: Phát hiện và cảnh báo tấn công Web

1. Mục tiêu kịch bản.

Mô phỏng hành vi tấn công SQL Injection (SQLi) và Cross-site Scripting (XSS) nhằm đánh giá khả năng phát hiện, phân tích và cảnh báo tấn công từ hệ thống giám sát log ELK Stack

2. Các thành phần tham gia



- Web Server (DMZ): Chạy ứng dụng DVWA, có ModSecurity.
- ModSecurity: Phát hiện, ghi log và ngăn chặn cuộc tấn công.
- ELK Stack: Nhận log, phân tích log và hiển thị kết quả.
- Pfsense: Định tuyến
- Máy ảo Kali: Thực hiện tấn công SQLi, XSS tới Webserver

3. Luồng xử lý log

- Tấn công được thực hiện từ máy Kali Linux

Attacker sử dụng trình duyệt gửi các payload độc hại đến máy chủ web DVWA. Ví dụ:

- SQL Injection: **`admin' OR 1=1--`**
- Cross-site Scripting (XSS): **`<script>alert(1)</script>`**

- ModSecurity trên Apache ghi nhận và sinh cảnh báo

- Web server được cấu hình sử dụng ModSecurity kết hợp với bộ quy tắc OWASP CRS (Core Rule Set).
- Khi request chứa payload trùng khớp với các rule CRS như:
    - Rule REQUEST-942: SQL Injection
    - Rule REQUEST-941: Cross-site Scripting

- Chuyển log từ web server về máy ELK Stack

- Web server được cấu hình gửi log về ELK qua rsyslog
- Log chuyển về Logstash để xử lý qua port 5140

- Logstash xử lý log ModSecurity

- Dùng bộ lọc Grok để tách các trường: src_ip, rule_id, request_uri, severity, rule_file, msg, v.v.
- Gán nhãn attack_type dựa trên nội dung của trường rule_file, ví dụ

```
if [rule_file] =~ /REQUEST-942/ {
mutate { add_field => { "attack_type" => "SQL Injection"
} }
}
```

- Log sau khi xử lý được gửi đến Elasticsearch với index dạng modsecurity-*.

- Kibana hiển thị dashboard giám sát

- Dashboard trực quan thể hiện:
    - Số lượng tấn công theo thời gian
    - Phân loại theo attack_type
    - Top IP nguồn và URI bị tấn công
    - Bảng log chi tiết từng sự kiện

4. Biểu hiện nhận biết tấn công

Time	src_ip	dst_ip	severity	attack_type	data	rules_file	rule_msg	referrer
Jun 14, 2025 @ 08:08:31.409	192.168.38.130	192.168.20.100	-	Correlation	-	/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf	Inbound Anomaly Score Exceeded (Total Inbound Score: 8 - SQLI=5,XSS=0,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level scores: 8, 0, 0, 0	http://192.168.20.100/dvwa/login.php
Jun 14, 2025 @ 08:08:31.409	192.168.38.130	192.168.20.100	CRITICAL	SQL Injection	Matched Data: s&1c found within ARGS:username: admin' OR 1=1 --	/usr/share/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf	SQL Injection Attack Detected via libinjection	http://192.168.20.100/dvwa/login.php
Jun 14, 2025 @ 08:08:31.409	192.168.38.130	192.168.20.100	WARNING	-	192.168.20.100	/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf	Host header is a numeric IP address	http://192.168.20.100/dvwa/login.php

Hệ thống ghi nhận nhiều cảnh báo (alert) từ ModSecurity cho thấy dấu hiệu tấn công SQL Injection:

- Rule thuộc nhóm REQUEST-942-APPLICATION-ATTACK-SQLI được kích hoạt bởi payload **`admin' OR 1=1`**, chèn vào tham số username.
- Mức độ cảnh báo được gán là CRITICAL.
- RESPONSE-980-CORRELATION xác định điểm bất thường tổng hợp cao, trong đó điểm SQLi đạt 8.
- Đồng thời, xuất hiện cảnh báo về việc sử dụng Host header là địa chỉ IP, cho thấy hành vi gửi request bất thường.

Các log này cho thấy hệ thống đã phát hiện chính xác một cuộc tấn công SQL Injection hướng vào trang đăng nhập ứng dụng web.

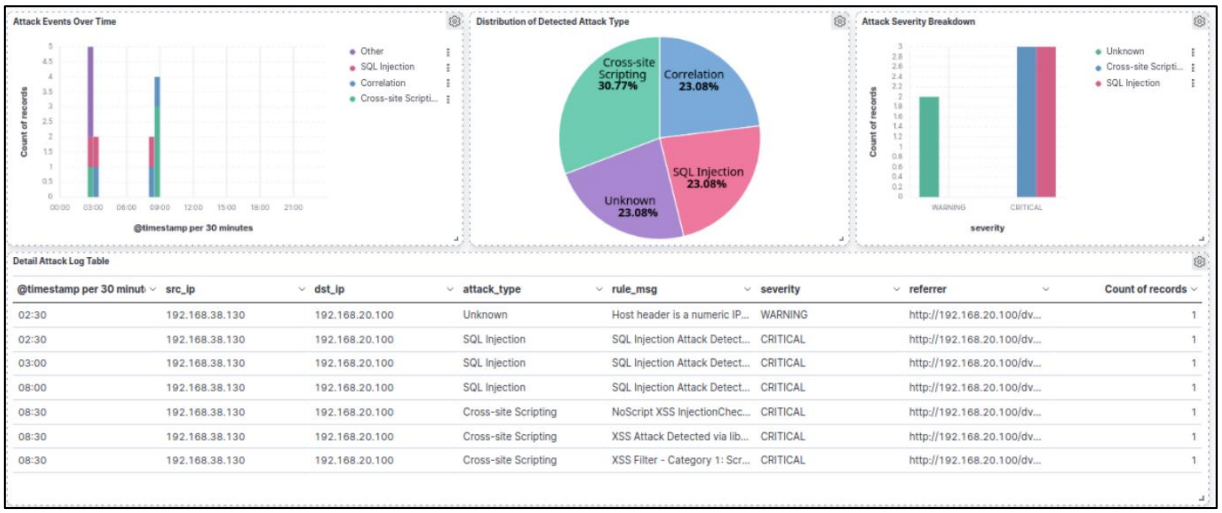
Time	src_ip	dst_ip	severity	attack_type	data	rules_file	rule_msg	referrer
Jun 14, 2025 @ 08:30:02.960	192.168.38.130	192.168.20.100	-	Correlation	-	/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf	Inbound Anomaly Score Exceeded (Total Inbound Score: 18 - SQLI=0,XSS=15,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level scores: 18, 0, 0, 0	http://192.168.20.100/dvwa/vulnerabilities/xss_r/
Jun 14, 2025 @ 08:30:02.959	192.168.38.130	192.168.20.100	CRITICAL	Cross-site Scripting	Matched Data: XSS data found within ARGS:name: <script>alert(1)</script>	/usr/share/modsecurity-crs/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf	XSS Attack Detected via libinjection	http://192.168.20.100/dvwa/vulnerabilities/xss_r/
Jun 14, 2025 @ 08:30:02.959	192.168.38.130	192.168.20.100	WARNING	-	192.168.20.100	/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf	Host header is a numeric IP address	http://192.168.20.100/dvwa/index.php

Hệ thống ghi nhận cảnh báo từ ModSecurity thể hiện dấu hiệu rõ ràng của một cuộc tấn công XSS:

- Rule thuộc nhóm REQUEST-941-APPLICATION-ATTACK-XSS phát hiện payload <script>alert(1)</script> được chèn vào tham số name, mức độ cảnh báo là CRITICAL.
- RESPONSE-980-CORRELATION được kích hoạt với tổng điểm anomaly là 18, trong đó điểm XSS đạt 15.
- Ngoài ra, xuất hiện thêm cảnh báo từ rule 920 về việc sử dụng Host header là địa chỉ IP – hành vi thường gặp khi attacker sử dụng công cụ tự động gửi request.

Các log này xác nhận hệ thống đã phát hiện chính xác một cuộc tấn công Cross-site Scripting với mức độ nghiêm trọng cao.

5. Kết quả hiển thị trên Kibana

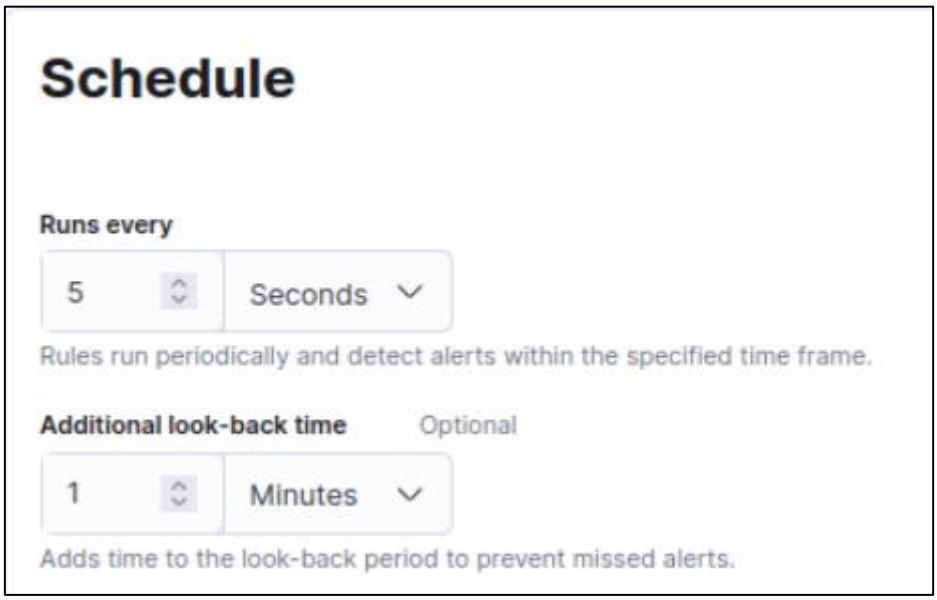


6. Rule & Alert

Tạo rule cảnh báo với custom query sử dụng KQL (Kibana Query Language):

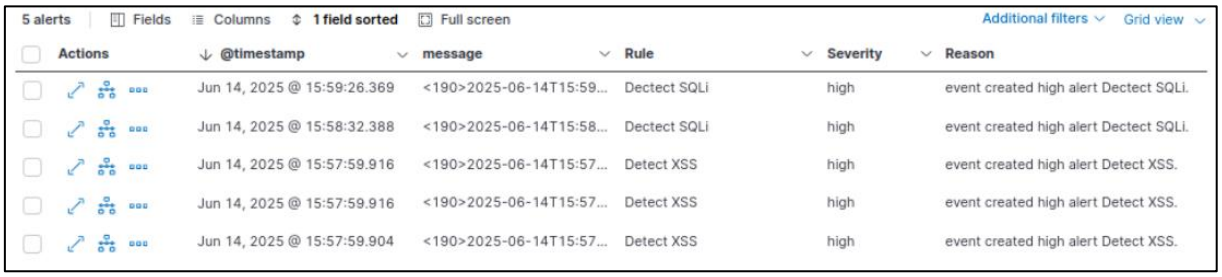
`attack_type : "SQL Injection"` (rule Detect SQLi)

`attack_type : "Cross-site Scripting"` (rule Detect XSS)



- Tần suất kiểm tra 5 giây/lần
- Rule sẽ quay lại xem dữ liệu của 1 phút trước mỗi lần chạy

Hệ thống sinh cảnh báo khi phát hiện tấn công



7. Tổng kết

Kịch bản 2 đã mô phỏng thành công các tấn công SQL Injection và Cross-site Scripting. Hệ thống ELK Stack đã thu thập log từ ModSecurity, phân tích chính xác các payload tấn công, phân loại theo attack_type và sinh cảnh báo tự động.

Dashboard và rule cảnh báo cho thấy khả năng phát hiện sớm và giám sát hiệu quả các hành vi tấn công web phổ biến.