HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

HOÀNG VĂN TÙNG

NGHIÊN CỨU FILE LOG VÀ ỨNG DỤNG TRONG BẢO MẬT SERVER

Chuyên ngành : Hệ thống thông tin

MÃ SỐ : 8.48.01.04

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI – 2020

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: TS. PHAN THỊ HÀ

Phản biện 1: Phùng Văn Ổn

Phản biện 2: Hoàng Xuân Dậu

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: 9..... giờ .35... ngày ...20.. tháng ...06.... .. năm 2020

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

MỞ ĐẦU

Hiện nay, Internet phát triển một cách mạnh mẽ và có nhiều bước chuyển mình vượt bậc đã đóng góp tích cực trong việc phát triển kinh tế, xã hội và đặc biệt là con người. Sự phát triển của internet kéo theo các website trực tuyến được tạo ra ngày càng một nhiều hơn. Và tất nhiên các server lưu trữ web (như hosting, vps) cũng tăng nhanh chóng nhằm đáp ứng nhu cầu tạo website, nhưng cũng đồng thời tạo ra thêm môi trường thu lợi đối với các tin tặc. Với nhiều thủ đoạn lẫn cách thức tinh vi, việc đảm bảo an toàn cho các server lưu trữ web luôn là một bài toán vô cùng nan giải.

Tháng 2/2019, Tập đoàn Bkav đã phát đi cảnh báo về việc đang có một chiến dịch tấn công có chủ đích của các hacker nước ngoài nhằm vào các server public của Việt Nam. Hàng trăm cơ quan, tổ chức tại Việt Nam đã bị hacker tấn công, xâm nhập máy chủ, sau đó thực hiện mã hóa toàn bộ dữ liệu trên server [1]. Hay các cuộc tấn công DDoS vào Wikipedia – website bách khoa hàng đầu thế giới – khiến cho website này bị ngừng hoạt động gần một ngày [2]. Theo Báo cáo an ninh mạng hàng năm của năm 2019 từ Bulletproof, một cuộc tấn công DoS hoặc DDoS có thể gây thiệt hại cho một công ty doanh nghiệp hơn 2 triệu đô la hoặc lên tới 120.000 đô la cho một công ty nhỏ [4].

Khi bị tin tặc tấn công, các server sẽ bị ảnh hưởng rất nhiều có thể dẫn đến việc hoạt động của hệ thống bị ngưng trệ hay mất mát dữ liệu. Điều này không chỉ làm tốn thời gian khắc phục cho người quản trị hệ thống mà kéo theo các hệ lụy về kinh tế hoặc là cả an ninh. Do vậy mà cần sự phát hiện sớm những cuộc tấn công vào server.

Để ngăn chặn nhanh nhất những cuộc tấn công vào server từ tin tặc, người quản trị cần sớm biết những mối nguy hại tiềm ẩn có thể tác động đến hệ thống của mình. Phân tích log của server sẽ giúp người quản trị biết được có những gì đang tác động vào server và đưa ra cách xử lý nhanh chóng [6].

Đề tài này được xây dựng nhằm mục đích nghiên cứu cũng như xây dựng một hệ thống có thể phân tích được các dấu hiệu bất thường trên sever thông qua file log để có thể có những phương án phòng bị cũng như ngăn chặn việc tấn công server.

Việc xây dựng được hệ thống phân tích log cũng giúp cho các quản trị viên có thể nắm bắt được tình hình của server nhanh chóng và chính xác nhất. Điều này không chỉ giúp ngăn chặn hay hiểu rõ cách thức tấn công nhanh hơn bình thường, mà còn giúp giảm chi phí nhân lực để quản trị server.

Xuất phát từ yêu cầu thực tế, học viên đã nghiên cứu áp dụng hệ thống phân tích log vào việc tăng cường bảo mật cho server, luận văn có tựa đề: "Nghiên cứu file log server và ứng dụng trong bảo mật server". Luận văn tập trung vào những vấn đề liên quan đến file log trong server và cách mà file log server có thể giúp người quản trị trong việc bảo mật.

Đề tài nghiên cứu về dữ liệu trong file log của một web server từ đó tìm ra những vấn đề có thể gây ảnh hưởng đến server này. Cụ thể hơn là dựa trên những dữ liệu thu được từ những lưu lượng truy cập, những thay đổi được tạo ra trong server,… để phát hiện ra những bất thường có thể gây tổn hại đến server.

Log là một file ghi lại liên tục các thông báo về hoạt động của hệ thống server hoặc của các dịch vụ được triển khai trên hệ thống hay những file tương ứng. Log file thường là các file văn bản thông thường biểu diễn dưới dạng "clear text" tức là người quản trị có thể dễ dàng đọc được nó, vì vậy mà có thể sử dụng các trình soạn thảo văn bản (vi, vim, nano...) hoặc các trình xem văn bản thông thường (cat, tailf, head...) để kiểm tra những file log server này.

File log server cung cấp cho quản trị viên toàn bộ các thông tin hoạt động của server, hỗ trợ giải quyết các rắc rối mà server gặp phải miễn là họ biết phân tích và ứng dụng các thông tin nhận được vào khắc phục.

Tác dụng của log là vô cùng to lớn, nó có thể giúp quản trị viên theo dõi hệ thống của mình tôt hơn, hoặc giải quyết các vấn đề gặp phải với hệ thống hoặc service. Điều này đặc biệt quan trọng với các hệ thống cần phải online 24/24 để phục vụ nhu cầu của mọi người dùng.

Việc áp dụng phân tích dữ liệu log vào bảo mật của server là một lĩnh vực rất rộng lớn khó để có thể làm chi tiết do vậy trong khuôn khổ của luận đề tài này, học viên sẽ tập trung vào tìm hiểu file log server thông qua đó xây dựng hệ thống phát hiện bất thường và cảnh báo tới người quản trị.

Đề tài sẽ sử dụng ELK Stack làm hệ thống quản lý log bởi rất nhiều điểm mạnh như mã nguồn mở, có thể thu thập được log từ nhiều nguồn khác, có một nền tảng tìm kiếm mạnh mẽ (ElasticSearch), hỗ trợ phân tích số liệu thu thập được (Analytic), quản lý logs tập trung, tìm kiếm và thông báo lỗi một cách tự động.

- **Mục đích, đối tượng, phạm vi và phương pháp nghiên cứu**

  Mục đích nghiên cứu

Mục đích của luận văn đó là tìm hiểu về file log trong server và ứng dụng vào trong việc bảo mật của server.

Đối tượng nghiên cứu

Học viên xác định đối tượng nghiên cứu trong đề tài này là các lý thuyết về file log server cũng như ứng dụng của nó. Bên cạnh đó đề tài còn tập trung vào nghiên cứu **công nghệ mã nguồn mở ELK** (ElasticSearch, LogStash và Kibana) và đưa vào áp dụng trên server dịch vụ lưu trữ công ty iNET.

Phạm vi và phương pháp nghiên cứu

- Phạm vi nghiên cứu
- Nghiên cứu về file log trong server.
- Phân tích file log server trên server lưu trữ web của công ty iNET.
  - Phương pháp nghiên cứu

Tìm hiểu về file log server, các kỹ thuật phân tích file log. Sau đó nghiên cứu công nghệ mã nguồn mở ELK (ElasticSearch, LogStash và Kibana) để đưa vào áp dụng server lưu trữ nhằm cảnh báo sớm tới quản trị viên khi có bất thường xảy ra.

- **Cấu trúc luận văn**

Với mục tiêu đặt ra như vậy, nội dung và kết quả của luận văn sẽ được chia thành 3 chương như sau:

Chương 1: Tổng quan về file log server

Trong chương này, luận văn sẽ đi vào tìm hiểu về file log trong server cũng như bài toán ứng dụng file log này vào việc bảo mật server.

Chương 2: Nghiên cứu và thiết kế hệ thống phân tích log server

Những vấn đề trong việc xử lý file log server thông qua các công cụ và nền tảng sẽ được trình bày trong chương 2 này. Trong chương này, học viên cũng sẽ đề cập đến mô hình cũng như các kỹ thuật phân tích file log server.

Chương 3: Áp dụng thử nghiệm hệ thống phân file log server thực tiễn

Tại chương này học viên sẽ áp dụng triển khai thử nghiệm hệ thống phân tích log trên một server cung cấp dịch vụ lưu trữ nội dung cho website. Từ việc áp dụng triển khai sẽ thu thập các thông tin từ file log server nhận được và đề xuất phương pháp bảo mật cho server.

Chương 1.TỔNG QUAN VỀ FILE LOG SERVER

Chương này trình bày về tổng quan và ý nghĩa của bài toán ứng dụng phân tích file log server trong việc bảo mật server. Đồng thời chương 1 giới thiệu chi tiết về file log trong server, những ứng dụng của file log server đối với quản trị viên trong quá trình hoạt động lẫn bảo mật hệ thống. Những hiểu biết về hệ thống phân tích file log server cũng sẽ được trình bày trong chương này.

1.1 Giới thiệu bài toán

1.1.1 Tổng quan về bảo mật server

1.1.2 Bài toán ứng dụng phân tích log trong bảo mật server

Bài toán ứng dụng phân tích log trong bảo mật server được hiểu như sau:

- ***Input:*** Dữ liệu log của server công ty iNET.
- ***Outtput:*** Một hệ thống có khả năng thu thập toàn bộ dữ liệu log với khả năng hiển thị trực quan và tự động thông báo khi có lỗi.

Ý nghĩa bài toán

- Bài toán ứng dụng phân tích log server vào bảo mật server đều mang tính ứng dụng rất cao trong thời đại công nghệ số hiện nay.
- Bài toán có ý nghĩa trong nghiên cứu bảo mật hệ thống server giúp cho việc vận hành hệ thống trở nên được thông suốt nhất, giúp cho các doanh nghiệp có thể giảm thiểu được những chi phí không đáng có khi khắc phục các vấn đề do bị tấn công. Không chỉ vậy, nó còn giúp cho quản trị viên có thể nắm rõ hơn được về hệ thống thay vì phân tích thủ công thì có thể dựa vào các số liệu phân tích sẵn để có những thay đổi kịp thời cho server.

1.2 Giới thiệu về file log server

1.2.1 File log server

1.2.2 Ứng dụng của file log server

1.3 Ứng dụng của file log trong bảo mật server

1.3.1 Tổng quan về phân tích log

1.3.2 Một số cuộc tấn công có thể nhận biết được thông qua file log

1.3.3 Hệ thống phân tích log server

1.4 Kết luận

Trong chương này, học viên đã tóm lược ngắn gọn về file log trong server cũng như những ứng dụng của nó. Đồng thời qua đó giới thiệu về bài toán ứng dụng phân tích file log server trong việc bảo mật server. Tiếp theo trong chương 2 học viên sẽ nghiên cứu về công nghệ, kỹ thuật dùng cho việc thiết kế hệ thống phân tích log server.

Chương 2. NGHIÊN CỨU VÀ THIẾT KẾ HỆ THỐNG PHÂN TÍCH LOG SERVER

Chương 2 sẽ giới thiệu về công nghệ được sử dụng để xây dựng hệ thống phân tích log server, các bước và các kỹ thuật phân tích log server đang được áp dụng hiện nay. Cuối chương học viên sẽ phác họa tổng quát một mô hình hệ thống phân tích log server để áp dụng vào thực tiễn.

2.1 Giới thiệu nền tảng và các công cụ phân tích log

Để giải quyết bài toán quản lý dữ liệu log server và tự động cảnh báo khi có bất thường xảy ra, quản trị viên có thể lựa chọn rất nhiều giải pháp công nghệ. Một số giải pháp bao gồm trả phí lẫn mã nguồn mở có thể kể đến như Splunk, Graylog hay ELK stack. Các tính năng nổi trội của các giải pháp giám sát và phân tích dữ liệu log hệ thống ngày nay phải kể đến như khả năng tìm kiếm mạnh mẽ, xây dựng được màn hình giám sát thời gian thực, báo cáo, cảnh bảo ngưỡng, phân tích dữ liệu lịch sử, truy tìm vết, …

Tuy nhiên sau khi cân nhắt học viên quyết định lựa chọn nền tảng công nghệ ELK làm giải pháp công nghệ cho bài toán quản lý và phân tích dữ liệu log do ELK hội tụ một số ưu điểm như:

- Mã nguồn mở, tiết kiệm được chi phí xây dựng hệ thống
- Cộng đồng hỗ trợ phát triển mạnh mẽ
- Hỗ trợ đa nền tảng, đa định dạng log
- ElasticSearch là một công cụ hỗ trợ nhiều tính năng, đáp ứng khối dữ liệu khổng lồ nếu hệ thống server phát triển. ElasticSearch còn có khả năng tương tích với nhiều công cụ, ngôn ngữ phân tích dữ liệu lớn như R, Python, Machine learning.
- Quản trị viên có thể xây dựng các báo cáo, phân tích các dữ liệu thông qua đồ họa trực quan bằng Kibana để đáp ứng những bài toán cần khối lượng dữ liệu lớn, hay phân tích hành vi người dùng, Business Intelligence
- Khả năng tổng hợp và phân loại log tùy biến cao, đáp ứng được những trường hợp dữ liệu log phức tạp.
- Có nhiều phần mềm hỗ trợ tùy biến cao.

2.1.1 Giới thiệu Elasticsearch

2.1.2 Giới thiệu Logstash

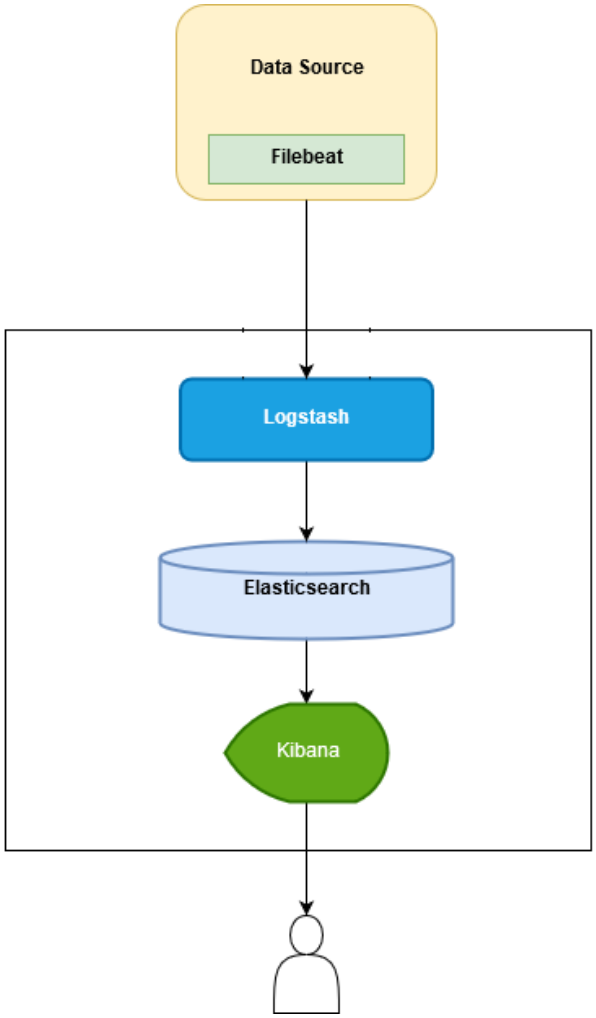
2.1.3 Giới thiệu Kibana

2.2 Các mô hình xử lý file log

2.3 Các kỹ thuật phân tích log server

2.4 Xây dựng hệ thống phân tích log

Trong luận văn này học viên sẽ lựa chọn xây dựng hệ thống phân tích log đơn giản với ELK stack, các bản cài đặt và thư mục file log sẽ nằm chung trên một Server có nhằm áp dụng vào mô hình thử nghiệm trong chương 3..



Hình 2.4: Mô hình phân tích log server

Theo như mô hình trên, luồng dữ liệu sẽ xuất phát từ tệp dữ liệu log và đi theo luồng sau:

- Tệp dữ liệu log sẽ được Filebeat lấy dữ liệu ra và gửi sang Logstash theo tần xuất được cấu hình từ trước. Tại đây Filebeat đóng vai trò là một service lấy log server từ các thư mục được đặt sẵn và đưa sang Logstash xử lý.
- Dữ liệu sau khi được Filebeat chuyển sang Logstash sẽ được chuyển tiếp đến "Filter Plugin". Ở đây dữ liệu sẽ được chuẩn hoá và lọc theo yêu cầu của người quản trị để có thể đưa ra các dữ liệu cần thiết. Đầu ra trong bước Filter này là tài liệu dạng JSON chứa nội dung thông điệp của log.
- Log server sau khi được lọc sẽ được chuyển đến Elasticsearch.
- Dữ liệu JSON khi được đưa tới ElasticSearch sẽ được đánh chỉ mục nhằm phục vụ bài toán tìm kiếm, trực quan hóa dữ liệu, xây dựng báo cáo và phân tích dữ liệu log.
- Dữ liệu sau khi được đánh chỉ mục trong ElasticSearch sẽ được trực quan hóa, xây dựng báo cáo, xây dựng các màn hình giám sát, điều khiển trên Kibana.

2.5 Kết luận

Trong chương này, luận văn đã đề cập đến nền tảng phân tích file log server sẽ được áp dụng, ví dụ cho một mô hình phân tích log server cũng như các kỹ thuật phân tích. Luận văn cũng đã thiết kế một mô hình hệ thống phân tích log server có thể áp dụng được vào thực tiễn nhằm nâng cao khả năng phân tích log. Trong chương sau học viên sẽ tiến hành cài đặt và triển khai trên thực tế mô hình hệ thống phân tích log server và tự động báo lỗi đến quản trị viên.

Chương 3. ÁP DỤNG THỬ NGHIỆM HỆ THỐNG PHÂN TÍCH FILE LOG SERVER VÀO THỰC TIỄN

Trong chương 3 học viên sẽ xây dựng thử nghiệm hệ thống phân tích log ELK trên server chạy dịch vụ lưu trữ của công ty iNET dựa trên mô hình xử lý dữ liệu log trên hệ thống lẫn Logstash tự thiết kế, sau đó sẽ tiến hành phân tích các dữ liệu nhận được để đề xuất bảo mật cho server.

3.1 Cài đặt hệ thống phân tích log server

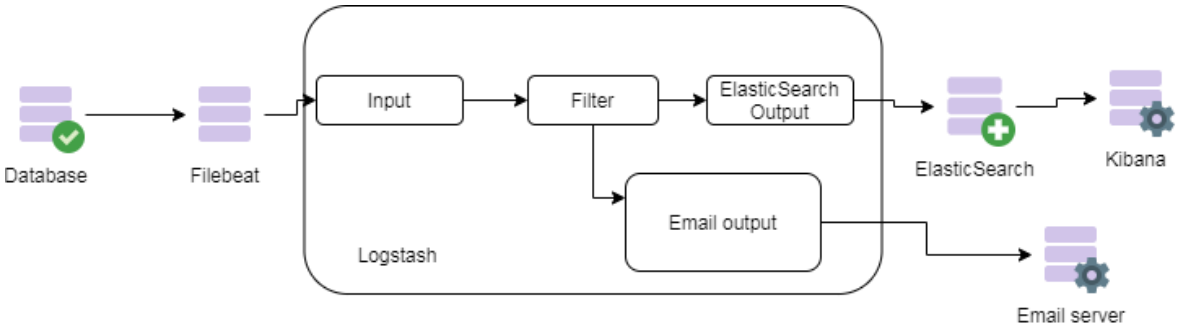
3.1.1 Giới thiệu về hệ thống máy chủ của công ty iNET

Hiện tại iNET không chú trọng quá nhiều vào việc phân tích dữ liệu log server. Dữ liệu log sẽ được người quản trị hệ thống phân tích chỉ khi có lỗi gì xảy ra, nếu không các dữ liệu log sẽ được lưu lại và xóa đi theo định kỳ để giải phóng dung lượng ổ đĩa.

Do vậy học viên sẽ ứng dụng cài đặt hệ thống phân tích log server trên trên server của công ty iNET dựa trên ELK stack nhằm nâng cao khả năng phân tích dữ liệu log, ứng dụng vào bảo mật hệ thống.

3.1.2 Mô hình thử nghiệm

Mô hình cài đặt thử nghiệm hệ thống phân tích log cần được xây dựng theo hướng tối ưu cho việc lấy dữ liệu log lẫn thông báo cho quản trị viên hạn chế tốt nhất việc chồng chéo gây tải nặng lên hệ thống. Dựa theo mục 2.4 thiết kế hệ thống phân tích log, học viên sẽ ứng dụng vào để xây dựng một hệ thống phân tích log thử nghiệm.



Hình 3.2: Mô hình xây dựng hệ thống phân tích log

Dữ liệu log server sẽ được Filebeat trích xuất ra và gửi vào Logstash, sau đó Logstash sẽ lọc nội dung log rồi đưa vào đánh chỉ mục trên ElasticSearch hoặc đưa vào

email server nếu gặp lỗi. Các dữ liệu được đánh chỉ mục trong ElasticSearch sẽ được hiển thị trên Kibana để quản trị viên tiện theo dõi.

3.1.3 Cài đặt hệ thống phân tích log bằng ELK stack

- Cấu hình file beat

Filebeat sẽ có nhiệm vụ truyền dữ liệu log từ thư mục chứa sang Logstash.

```
#Cấu hình đầu vào filebeat

- type: log

  paths:

    - \filebeat\logaccess\*.log

  fields:

    type: apache

    fields: access

  fields_under_root: true

  encoding: utf-8

- type: log

  paths:

    - \filebeat\logerror\*

  fields:

    type: error log

    fields: error

  fields_under_root: true
```

encoding: utf-8#

Cấu hình đầu ra filebeat

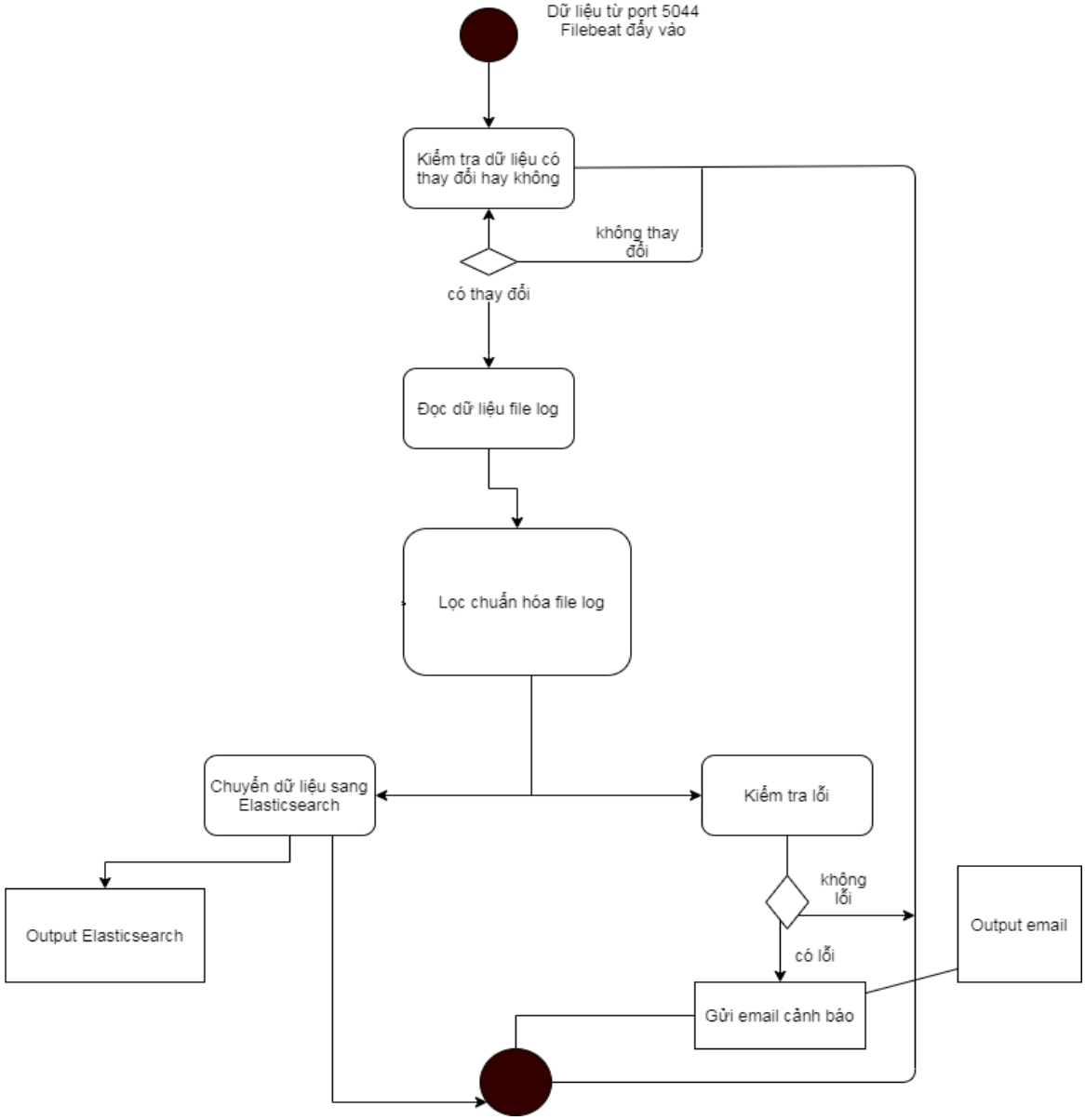
output.logstash:

hosts: ["localhost:5044"]

#đầu ra tại đây để cổng mặc định của Logstash, dữ liệu sau khi lấy sẽ được chuyển đến port 5044

- **Cấu hình Logstash**

Mô hình xử lý dữ liệu của Logstash sẽ được sử dụng để cấu hình file config.



Hình 3.3 Mô hình xử lý dữ liệu trong logstash

Cấu hình chi tiết cho file config của Logstash

```
#Cấu hình đầu vào Logstash

#Lấy dữ liệu từ filebeat được chuyển qua port 5044

input {

   beats {

      port => "5044"

   }

}

#Cấu hình file filter

filter {

# cấu hình theo dạng mặc định của file apache

filter {

  if [fields] =="access" {

grok {

          match => { "message" => "%{COMBINEDAPACHELOG}" }

          overwrite => "message"

       }          overwrite => "message"

       }

  }

if [fields] =="error"  {
```

```
   grok {
          match => { "message" => "%{APACHE_ERROR_LOG}" }
       }
}
 mutate {
    remove_field => "host"
}
     date {
   match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]
     }
  geoip {
     source => "clientip"
   }
}
output {
#đầu ra cho elasticsearch
  elasticsearch {
   hosts => ["localhost:9200"]
         index => "%{[@metadata][filebeat]}-%{+YYYY.MM.dd}"
```

```
  }

   stdout { codec => rubydebug }

#đầu ra cho email báo lỗi

   if "access denied" in [message] {

email {

port => 587

address => "smtp.gmail.com"

username => "sin****gum16@gmail.com"

password => "Tung*****"

authentication => "plain"

use_tls => true

from => " sin****gum16@gmail.com "

subject => " Cảnh Báo: Phát hiện có truy cập bị chặn"

to => "htv.sky.1994@gmail.com"

via => "smtp"

body => "%{message}"

}
```

- **Cấu hình Elasticsearch và Kibana**

Để có thể hiển thị các dữ liệu được lập chỉ mục trong ElasticSearch, học viên sẽ cấu hình port chạy Kibana lẫn port của ElasticSearch:

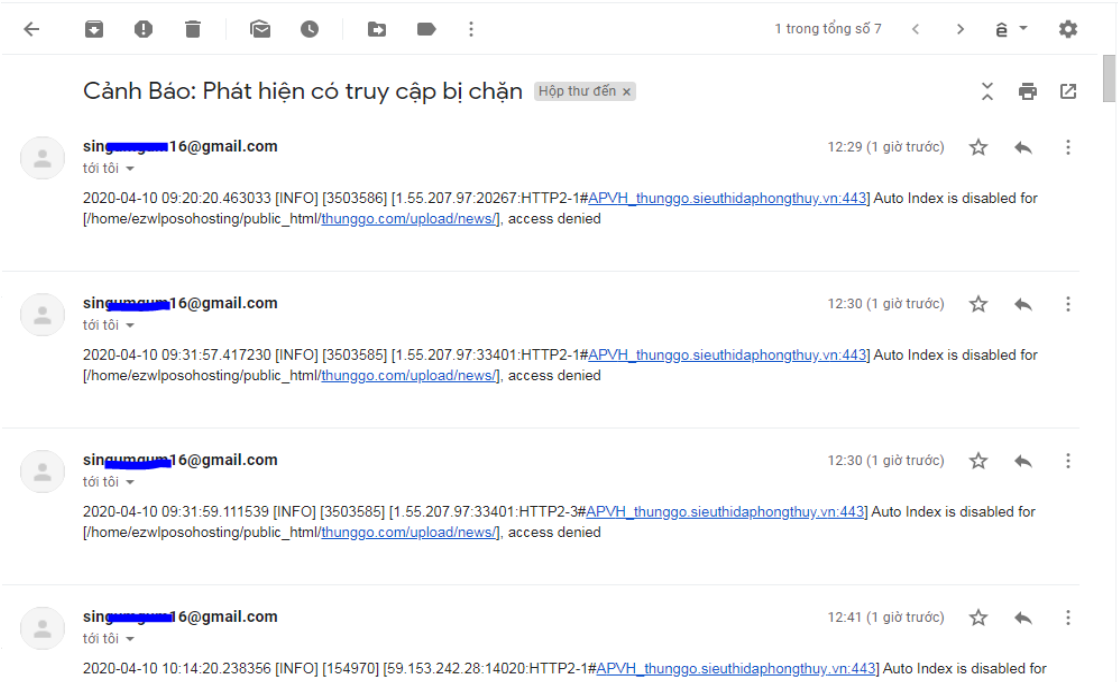
```
# Kibana is served by a back end server. This setting specifies the port to use.

server.port: 5601

# The URLs of the Elasticsearch instances to use for all your queries.

elasticsearch.hosts: ["http://localhost:9200"]
```

3.2 Vận hành và thử nghiệm

Dữ liệu log sẽ được chia ra các trường như hình ảnh dưới kèm theo một filter ở bên trái cho phép lựa chọn các trường dữ liệu nào cần thiết cho việc phân tích.

Hình 3.4: Giao diện quản lý dữ liệu log tổng quan trên Kibana

Hệ thống sẽ tự động báo lỗi cho quản trị viên thông qua mail được cài đặt sẵn.



Hình 3.5 Hệ thống gửi mail báo lỗi cho quản trị viên

3.3 Phân tích các dữ liệu thu được từ log Server

3.4. Đánh giá, đề xuất bảo mật cho server

3.5 Kết luận

Chương 3 luận văn đã trình bày chi tiết về việc triển khai hệ thống phân tích log trên server của công ty iNET dựa trên công nghệ ELK stack cho phép quản trị viên có thể quản lý log tập trung, nhận thông báo lỗi từ sớm giúp sớm khắc phục các lỗi hệ thống. Bên cạnh đó mô hình vận hành hệ thống phân tích và luồng lấy dữ liệu log được học viên thiết kế cũng hoạt động theo ý muốn giúp dữ liệu log được tập trung toàn bộ trên hệ thống phục vụ cho việc phân tích dễ dàng hơn.

Việc cài đặt thành công hệ thống phân tích log trên server của công ty iNET sẽ tạo tiền đề cho việc triển khai cho những server khác nâng cao khả năng phòng ngự bảo mật. Một số thử nghiệm đánh giá về dữ liệu log thu được trên server công ty iNET cũng đã được học viên thực hiện. Với việc chọn các yếu tố quan trọng, loại bỏ các yếu tố dư thừa khi phân tích dữ liệu log; học viên đã có thể xác định được nguy cơ xảy ra của các cuộc tấn công nhằm vào server. Bên cạnh đó chương 3 tổng hợp một số đề xuất cho server nhằm nâng cao khả năng chống tấn công cho sever, hạn chế mức thấp nhất những tác động gây hại giảm tải việc phải giám sát hệ thống quá nhiều.

KẾT LUẬN

1. Những đóng góp của luận văn:

Với mục tiêu nghiên cứu bài toán tìm hiểu file log và ứng dụng file log vào bảo mật server. Luận văn đã đi sâu vào nghiên cứu về các vấn đề xung quanh file log, và những ứng dụng của file log đối với server.

Những kết quả đã đạt được trong luận văn:

- Tìm hiểu tổng quan về file log server, những ứng dụng của file log server trong việc vận hành lẫn bảo mật hệ thống, những cách thức phân tích và cách nhận biết tấn công thông qua file log.
- Tìm hiểu về công nghệ ELK stack và dựa vào công nghệ học viên đã xây dựng được một mô hình tổng quát hệ thống phân tích log server.
- Tìm hiểu về hệ thống máy chủ công ty iNET, sau đó tiến hành xây dựng mô hình hệ thống phân tích log cho những máy chủ trên. Thông qua mô hình hệ thống phân tích log, học viên đã cấu hình chạy thử nghiệm thành công hệ thống phân tích dữ liệu log và cảnh báo lỗi đến quản trị viên.

2. Hướng phát triển luận văn

Tuy đạt được một số kết quả đã nêu ở trên, nhưng luận văn còn có những hạn chế do điều kiện về mặt thời gian lẫn trình độ của học viên. Vì vậy, hướng nghiên cứu tiếp theo của học viên đó là:

- Áp dụng thêm các công cụ khác vào hệ thống phân tích file log nhằm nâng cấp tính năng, nâng cao khả năng quản trị server lẫn dữ liệu log.
- Những hình thức tấn công vào hệ thống server đang phát triển không ngừng theo thời gian. Tin tặc hiện đang áp dụng những hình thức tấn công đa dạng hơn, khó để phát hiện và ngăn chặn hơn đang là bài toán khó trong bảo mật server đối với các quản trị viên. Luận văn sẽ phát triển theo hướng tìm hiểu về các hình thức tấn công mới nhất, thông qua tìm hiểu cách thức để áp dụng vào việc phân tích log.
- Không chỉ dùng dữ liệ trong phân tích log vào bảo mật server, luận văn có thể phát triển theo hướng ứng dụng vào những vấn đề liên quan đến người dùng nhằm cải thiện chất lượng của hệ thống.

- Ứng dụng của file log server vào bảo mật server là vô cùng lớn. Quản trị viên hoàn toàn có thể phát triển hệ thống SIEM (hệ thống giám sát an ninh mạng) bằng những dữ liệu log trên server để quản lý server một cách toàn diện nhất.