

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



Đề tài:

TÌM HIỂU VÀ TRIỂN KHAI ELK SIEM

Người hướng dẫn:

TS. Huỳnh Thanh Tâm

Sinh viên thực hiện:

Nhóm: 02

TRƯƠNG CHÍ TÀI

(N19DCAT067)

NGUYỄN THÀNH BĂNG

(N19DCAT008)

TẠ ĐỨC TIẾN

(N19DCAT074)

TP.HCM, tháng 04/2023

LỜI CẢM ƠN

Đầu tiên, nhóm chúng em xin gửi lời cảm ơn chân thành đến tất cả thầy cô đã giảng dạy và cho chúng em những kiến thức vô cùng quan trọng và quý báu của mình trong quá trình học tập tại Học viện để chúng em có những kỹ năng và những kiến thức cần thiết để hoàn thành đồ án môn học này.

Đặc biệt, chúng em vô cùng biết ơn thầy TS. Huỳnh Thanh Tâm đã tận tình hướng dẫn, truyền đạt những kiến thức và kinh nghiệm của thầy và dạy bảo em trong quá trình học tập và thực hiện đồ án này. Nhóm em xin chúc gia đình thầy có thật nhiều sức khỏe và thành công trong cuộc sống. Từ đó mang đến cho chúng em cũng như các bạn khác những kiến thức và kinh nghiệm quý báu của thầy.

Cảm ơn tất cả những người bạn đã ít nhiều cho chúng mình những kiến thức và hiểu biết, luôn đồng hành và sát cánh trong quá trình học tập và rèn luyện các kỹ năng. Quan trọng hơn cả là động lực và niềm vui mà chúng mình chắc chỉ có các bạn mới có thể mang lại. Từ đó chúng mình có thể vượt qua những khó khăn và áp lực trong học tập cũng như trong cuộc sống.

Đề tài đã được nhóm hoàn thành đúng tiến độ. Tuy nhiên, nhóm vẫn còn nhiều thiếu sót do chưa có nhiều kinh nghiệm. Mong thầy cô chỉ bảo, đóng góp ý kiến để nhóm em có nhiều hơn những kiến thức và kỹ năng để hoàn thành tốt công tác nghiên cứu, làm việc sau này cũng như trong cuộc sống.

TP. HCM, Ngày ... tháng ... năm

Đại diện nhóm

(Ký và ghi họ tên)

Trương Chí Tài

MỤC LỤC

LỜI MỞ ĐẦU	2
CHƯƠNG 1. CƠ SỞ LÝ THUYẾT	3
<i>1.1 Giới thiệu về SIEM.....</i>	3
1.1.1 Định nghĩa	3
1.1.2 Cách thức hoạt động	3
1.1.3 Các chức năng và trường hợp sử dụng	3
1.1.4 Lợi ích	4
1.1.5 Cách triển khai giải pháp	4
1.1.6 Kiến trúc của SIEM sử dụng ELK Stack	4
<i>1.2 ELK SIEM</i>	5
1.2.1 ELK Stack	5
1.2.2 SIEM sử dụng ELK Stack	6
<i>1.3 Suricata</i>	7
CHƯƠNG 2. THIẾT KẾ VÀ XÂY DỰNG HỆ THỐNG	7
<i>2.1 Mô hình triển khai.....</i>	7
<i>2.2 Cài đặt.....</i>	8
2.2.1 Cài đặt Suricata trên Ubuntu 20.04	8
2.2.2 Cài đặt Elasticsearch and Kibana	13
2.2.3 Cài đặt Filebeat	16
2.2.4 Kết quả:	17
CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM	20
<i>3.1 Kịch bản 1:</i>	20
<i>3.2 Kịch bản 2:</i>	21
TÀI LIỆU THAM KHẢO	22

LỜI MỞ ĐẦU

SIEM là một phần quan trọng trong hệ sinh thái an ninh mạng của tổ chức. SIEM cung cấp cho các nhóm bảo mật một vị trí trung tâm để thu thập, tổng hợp và phân tích khối lượng dữ liệu trong toàn doanh nghiệp, giúp đơn giản hóa quy trình bảo mật một cách hiệu quả.

Đồng thời, SIEM cung cấp các chức năng hoạt động như báo cáo tuân thủ, quản lý sự cố và bảng thông tin ưu tiên hoạt động của mỗi đe dọa. Trong đề tài này, nhóm chúng em sẽ thực hiện triển khai mô hình SIEM sử dụng ELK Stack kết hợp với IDS/IPS Suricata để giám sát phát hiện dấu hiệu của các cuộc tấn công mạng. Nội dung sẽ tập trung vào nghiên cứu ELK Stack và Suricata. Các nội dung liên quan đến các hệ thống SIEM và IDS khác không thuộc phạm vi nội dung nghiên cứu của đề tài này. Nội dung đề tài gồm 3 chương chính. Chương 1 là cơ sở lý thuyết trình bày các khái niệm về SIEM, ELK Stack và Suricata. Chương 2 là thiết kế và xây dựng hệ thống, chương này tập chung vào cài đặt và cấu hình các thành phần của hệ thống SIEM sử dụng ELK Stack và Suricaa. Chương 3 là kết quả thực nghiệm sẽ trình bày 2 kịch bản sau khi hệ thống được hoạt động thành công.

CHƯƠNG 1. CƠ SỞ LÝ THUYẾT

1.1 Giới thiệu về SIEM

1.1.1 Định nghĩa

Quản lý sự kiện và thông tin bảo mật, viết tắt là SIEM, là một giải pháp giúp các tổ chức phát hiện, phân tích và ứng phó với các mối đe dọa bảo mật trước khi chúng ảnh hưởng đến hoạt động kinh doanh.

SIEM, đọc là "sim", kết hợp cả quản lý thông tin bảo mật (SIM) và quản lý sự kiện bảo mật (SEM) vào một hệ thống quản lý bảo mật. Công nghệ SIEM thu thập dữ liệu nhật ký sự kiện từ nhiều nguồn, xác định hoạt động sai lệch so với quy chuẩn bằng việc phân tích theo thời gian thực và thực hiện hành động thích hợp.

Tóm lại, SIEM cung cấp cho các tổ chức khả năng quan sát hoạt động trong mạng của họ để họ có thể ứng phó nhanh chóng với các cuộc tấn công qua mạng tiềm ẩn và đáp ứng các yêu cầu tuân thủ.

Trong thập kỷ qua, công nghệ SIEM đã phát triển để giúp việc phát hiện mối đe dọa và ứng phó với sự cố trở nên thông minh hơn và nhanh chóng hơn nhờ có trí tuệ nhân tạo.

1.1.2 Cách thức hoạt động

Các công cụ SIEM thu thập, tổng hợp và phân tích khối lượng dữ liệu từ các ứng dụng, thiết bị, máy chủ và người dùng của tổ chức theo thời gian thực để các nhóm bảo mật có thể phát hiện và chặn các cuộc tấn công. Các công cụ SIEM sử dụng quy tắc được xác định trước để giúp các nhóm bảo mật xác định mối đe dọa và tạo ra cảnh báo.

1.1.3 Các chức năng và trường hợp sử dụng

Các hệ thống SIEM có nhiều chức năng khác nhau nhưng thường cung cấp các chức năng cốt lõi sau đây:

- Ghi nhật ký hoạt động quản lý: Hệ thống SIEM tập hợp lượng lớn dữ liệu vào một nơi, sắp xếp dữ liệu đó, rồi xác định xem trong đó có dấu hiệu của mối đe dọa, hoạt động tấn công hoặc vi phạm không.
- Liên hệ tương quan sự kiện: Dữ liệu sau đó được sắp xếp để xác định các mối quan hệ và mẫu, nhằm nhanh chóng phát hiện và ứng phó với các mối đe dọa tiềm ẩn.
- Giám sát và ứng phó với sự cố: Công nghệ SIEM giám sát các sự cố về bảo mật trên mạng của tổ chức và cung cấp các cảnh báo cũng như kiểm tra tất cả hoạt động liên quan đến sự cố.

Hệ thống SIEM có thể giảm thiểu rủi ro trên mạng với một loạt các trường hợp sử dụng như phát hiện hoạt động đáng ngờ của người dùng, giám sát hành vi của người dùng, hạn chế các nỗ lực truy nhập và tạo báo cáo tuân thủ.

1.1.4 Lợi ích

Các công cụ SIEM mang lại nhiều lợi ích có thể giúp củng cố vị thế bảo mật tổng thể của tổ chức, bao gồm:

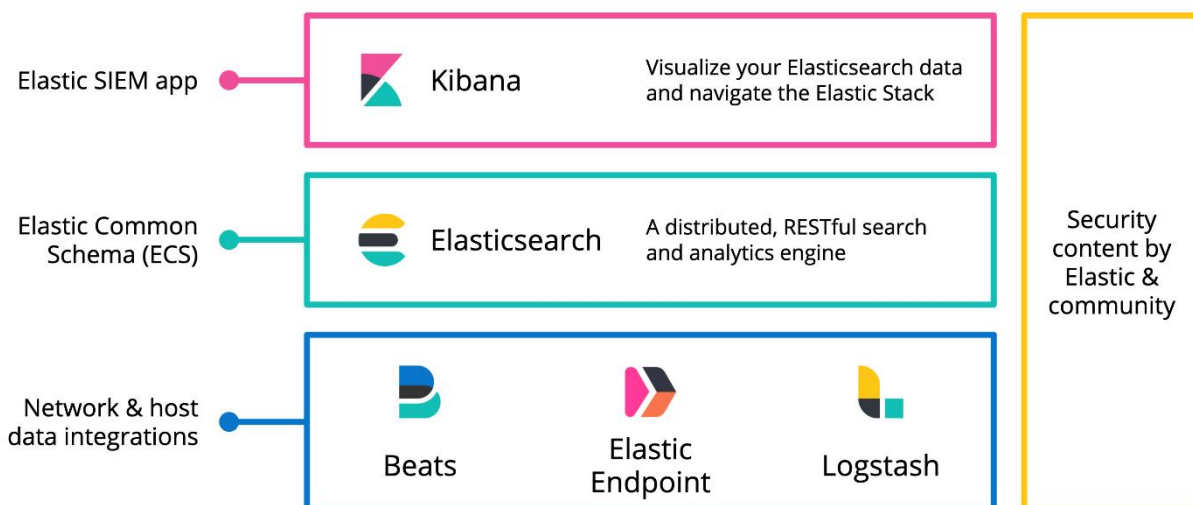
- Dạng xem trung tâm về các mối đe dọa tiềm ẩn
- Nhận dạng và ứng phó với mối đe dọa theo thời gian thực
- Thông tin về mối đe dọa nâng cao
- Kiểm tra và báo cáo về việc tuân thủ theo quy định
- Giám sát người dùng, ứng dụng và thiết bị minh bạch hơn

1.1.5 Cách triển khai giải pháp

Các tổ chức thuộc mọi quy mô sử dụng các giải pháp SIEM để giảm thiểu rủi ro về **an ninh mạng** và đáp ứng các tiêu chuẩn tuân thủ theo quy định. Các biện pháp tốt nhất để triển khai hệ thống SIEM bao gồm:

- Xác định các yêu cầu cho việc triển khai SIEM
- Thực hiện chạy kiểm tra
- Thu thập đủ dữ liệu
- Có kế hoạch ứng phó với sự cố
- Tiếp tục cải thiện SIEM của bạn

1.1.6 Kiến trúc của SIEM sử dụng ELK Stack



1.2 ELK SIEM

1.2.1 ELK Stack

1.2.1.1 Giới thiệu

ELK Stack là tập hợp của 3 sản phẩm mã nguồn mở Elasticsearch, Logstash, và Kibana. Tất cả được phát triển, quản lý và duy trì bởi Elastic.

Elasticsearch là một công cụ phân tích và tìm kiếm toàn văn bản mã nguồn mở, dựa trên công cụ tìm kiếm Apache Lucene.

Logstash là một trình tổng hợp nhật ký thu thập dữ liệu từ nhiều nguồn đầu vào khác nhau, thực hiện các chuyển đổi và cải tiến khác nhau và sau đó gửi dữ liệu đến các điểm cuối được hỗ trợ khác nhau.

Kibana là một lớp trực quan hóa hoạt động trên Elasticsearch, cung cấp cho người dùng khả năng phân tích và trực quan hóa dữ liệu. Và cuối cùng nhưng không kém phần quan trọng.

Beat là thành phần bổ sung và là tác nhân được cài đặt trên các máy chủ để thu thập các loại dữ liệu khác nhau để chuyển tiếp vào ELK Stack.

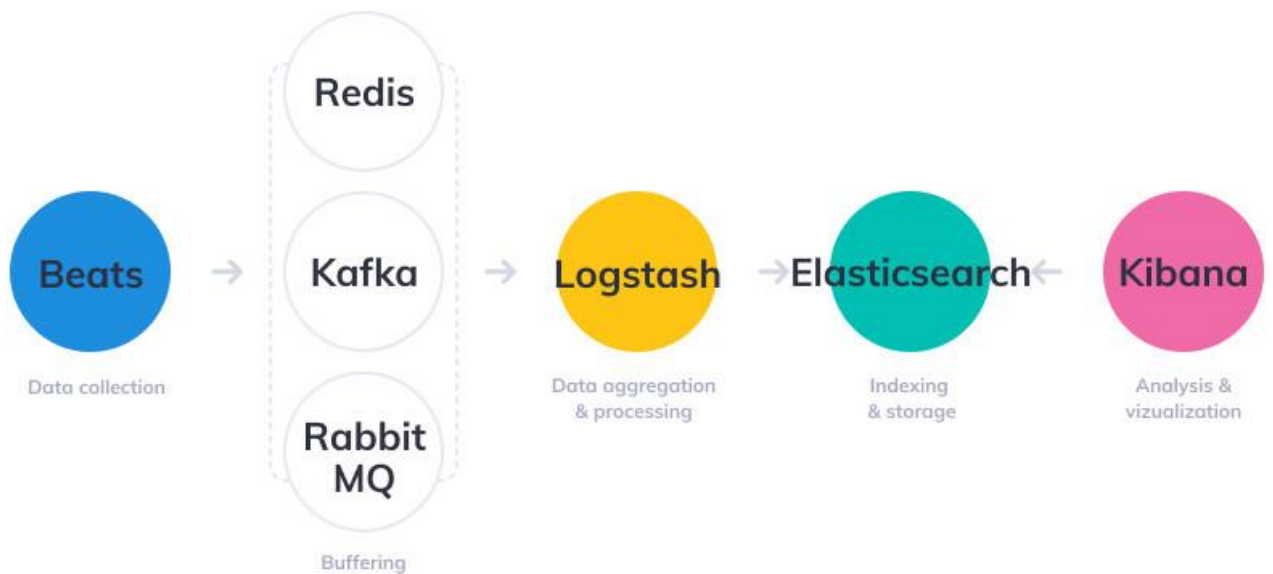
Các thành phần này được sử dụng phổ biến để giám sát, khắc phục sự cố và bảo mật môi trường CNTT (mặc dù có nhiều trường hợp sử dụng ELK Stack cho nghiệp vụ thông minh và phân tích trang web). Beats và Logstash đảm nhận việc thu thập và xử lý dữ liệu, Elasticsearch lập chỉ mục và lưu trữ dữ liệu và Kibana cung cấp giao diện người dùng để truy vấn dữ liệu và trực quan hóa dữ liệu.

1.2.1.2 Cách thức hoạt động để phân tích log

Đối với môi trường phát triển quy mô nhỏ thì sử dụng kiến trúc sau:

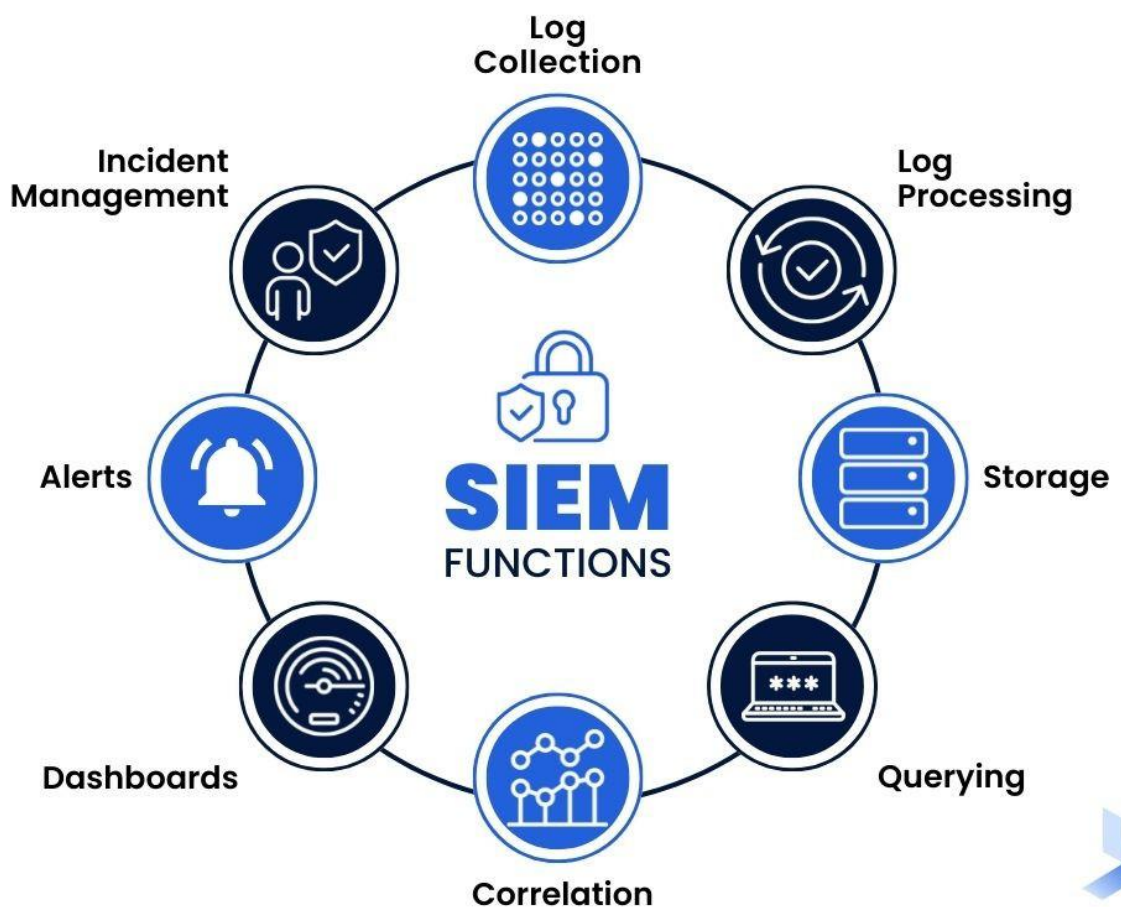


Còn đối với quy mô lớn để xử lý số lượng dữ liệu khổng lồ và phức tạp thì phải bổ sung thành phần giúp tăng khả năng phục hồi (Kafka, RabbitMQ, Redis) và bảo mật (nginx)



1.2.2 SIEM sử dụng ELK Stack

ELK đảm nhận việc thu thập, xử lý và lưu trữ nhật ký. Nhưng không thực hiện các công việc như event correlation, alert và quản lý sự cố như SIEM. Vì vậy có thể sử dụng ELK Stack là một trong những thành phần của SIEM.



1.3 Suricata

Suricata là một công cụ giám sát an ninh mạng (Network Security Monitoring - NSM) sử dụng các tập hợp các chữ ký do cộng đồng tạo và người dùng xác định (còn được gọi là quy tắc - rules) để kiểm tra và xử lý lưu lượng mạng. Suricata có thể tạo ra các sự kiện nhật ký (log), kích hoạt cảnh báo (alert) và giảm (drop) lưu lượng truy cập khi phát hiện các gói hoặc yêu cầu đáng ngờ đến bất kỳ số lượng dịch vụ khác nhau nào đang chạy trên máy chủ.



Source: Stamus Networks

Theo mặc định, Suricata hoạt động như một Hệ thống phát hiện xâm nhập thụ động (Intrusion Detection System - IDS) để quét lưu lượng đáng ngờ trên máy chủ hoặc mạng. Nó sẽ tạo và ghi nhật ký cảnh báo phục vụ cho điều tra sau này. Nó cũng có thể được cấu hình như một Hệ thống ngăn chặn xâm nhập (Intrusion Prevention System - IPS) hoạt động để ghi nhật ký, cảnh báo và chặn hoàn toàn lưu lượng mạng phù hợp với các quy tắc cụ thể.

Có thể triển khai Suricata trên gateway host trong mạng để quét tất cả lưu lượng mạng đến và đi từ các hệ thống khác hoặc bạn có thể chạy cục bộ trên các máy riêng lẻ.

CHƯƠNG 2. THIẾT KẾ VÀ XÂY DỰNG HỆ THỐNG

2.1 Mô hình triển khai

- Hệ thống SIEM triển khai lần này sẽ gồm 4 phần chính:

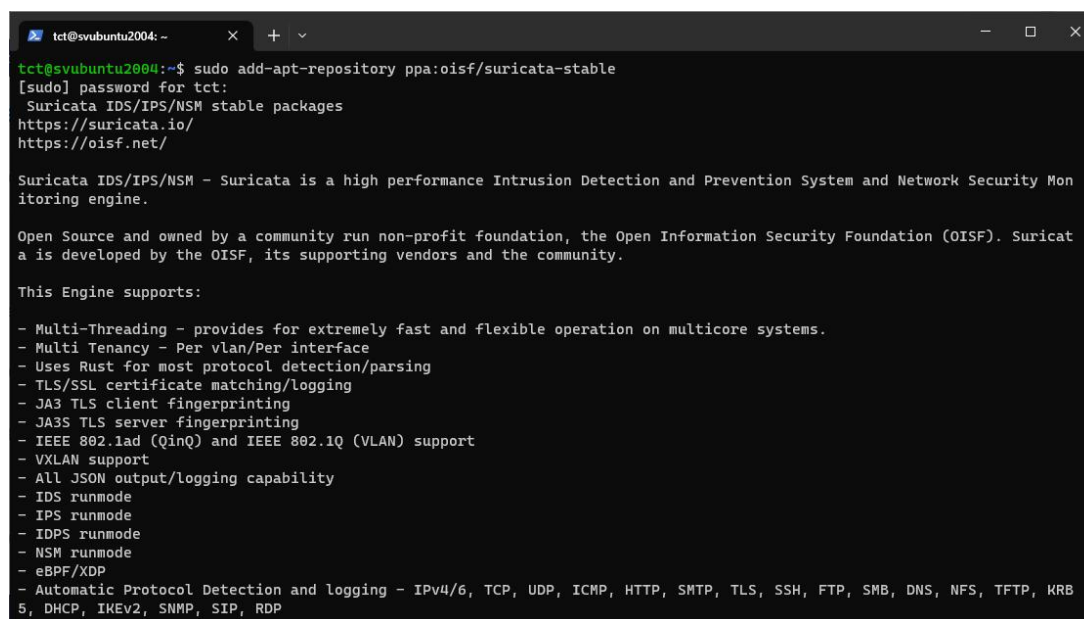
- Elasticsearch để lưu trữ, lập chỉ mục, tương quan và tìm kiếm các sự kiện bảo mật đến từ máy chủ Suricata.
- Kibana để hiển thị và điều hướng xung quanh nhật ký sự kiện bảo mật được lưu trữ trong Elasticsearch.
- Filebeat để parse log của Suricata, và gửi từng sự kiện đến Elasticsearch để xử lý.eve.json
- Suricata để quét lưu lượng mạng cho các sự kiện đáng ngờ và log hoặc drop các gói không hợp lệ.

2.2 Cài đặt

2.2.1 Cài đặt Suricata trên Ubuntu 20.04

- Cài đặt:

`sudo add-apt-repository ppa:oisf/suricata-stable`



```
tct@svubuntu2004: ~$ sudo add-apt-repository ppa:oisf/suricata-stable
[sudo] password for tct:
Suricata IDS/IPS/NSM stable packages
https://suricata.io/
https://oisf.net/

Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and Network Security Monitoring engine.

Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF, its supporting vendors and the community.

This Engine supports:

- Multi-Threading - provides for extremely fast and flexible operation on multicore systems.
- Multi Tenancy - Per vlan/Per interface
- Uses Rust for most protocol detection/parsing
- TLS/SSL certificate matching/logging
- JA3 TLS client fingerprinting
- JA3S TLS server fingerprinting
- IEEE 802.1ad (QinQ) and IEEE 802.1Q (VLAN) support
- VXLAN support
- All JSON output/logging capability
- IDS runmode
- IPS runmode
- IDPS runmode
- NSM runmode
- eBPF/XDP
- Automatic Protocol Detection and logging - IPv4/6, TCP, UDP, ICMP, HTTP, SMTP, TLS, SSH, FTP, SMB, DNS, NFS, TFTP, KRBS, DHCP, IKEv2, SNMP, SIP, RDP
```

`sudo apt install suricata`

```
tct@svubuntu2004:~$ sudo apt install suricata
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhttp2 libhyperscan5 libjansson4 liblua5.1-2
  liblua5.1-common liblzma-dev libnet1 libnetfilter-queue1
Suggested packages:
  liblzma-doc
The following NEW packages will be installed:
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhttp2 libhyperscan5 libjansson4 liblua5.1-2
  liblua5.1-common liblzma-dev libnet1 libnetfilter-queue1 suricata
0 upgraded, 12 newly installed, 0 to remove and 9 not upgraded.
Need to get 5,086 kB of archives.
After this operation, 24.0 MB of additional disk space will be used.
Do you want to continue? [y/n] Y
Get:1 http://vn.archive.ubuntu.com/ubuntu focal/universe amd64 libhyperscan5 amd64 5.2.1-1build1 [2,452 kB]
Get:2 http://ppa.launchpad.net/oisf/suricata-stable/ubuntu focal/main amd64 libhttp2 amd64 1:0.5.42-0ubuntu8 [68.5 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu focal/main amd64 libevent-core-2.1-7 amd64 2.1.11-stable-1 [89.1 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu focal/main amd64 libevent-pthreads-2.1-7 amd64 2.1.11-stable-1 [7,372 B]
Get:5 http://vn.archive.ubuntu.com/ubuntu focal/universe amd64 libhiredis0.14 amd64 0.14.0-6 [30.2 kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu focal/main amd64 libjansson4 amd64 2.12-1build1 [28.9 kB]
Get:7 http://vn.archive.ubuntu.com/ubuntu focal/universe amd64 liblua5.1-common all 2.1.0-beta3+dfsg-5.1build1 [44.3 kB]
Get:8 http://vn.archive.ubuntu.com/ubuntu focal/universe amd64 liblua5.1-2 amd64 2.1.0-beta3+dfsg-5.1build1 [228 kB]
Get:9 http://vn.archive.ubuntu.com/ubuntu focal/main amd64 libnet1 amd64 1.1.6+dfsg-3.1build1 [43.3 kB]
Get:10 http://vn.archive.ubuntu.com/ubuntu focal/universe amd64 libnetfilter-queue1 amd64 1.0.3-1 [12.4 kB]
Get:11 http://vn.archive.ubuntu.com/ubuntu focal-updates/main amd64 liblzma-dev amd64 5.2.4-1ubuntu1.1 [147 kB]
Get:12 http://ppa.launchpad.net/oisf/suricata-stable/ubuntu focal/main amd64 suricata amd64 6.0.10-0ubuntu1 [1,935 kB]
95% [12 suricata 1,708 kB/1,935 kB 88%] 748 kB/s 0s
```

sudo systemctl enable suricata.service

```
tct@svubuntu2004:~$ sudo systemctl enable suricata.service
suricata.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable suricata
```

- Cấu hình lần đầu:

+ **Mở Community Flow ID** giúp cho mình dễ dàng làm việc với các tool khác như Zeek hay Elasticsearch vì Suricata bao gồm ID này trong JSON output nên sẽ giúp cho khớp các từng bản ghi sự kiện trong datasets được tạo bởi các tool khác:

sudo nano /etc/suricata/suricata.yaml: mở file và thay đổi community-id từ false thành true:

```
# enable/disable the community id feature.
community-id: true
# Seed value for the ID output. Valid values are 0-65535.
```

Kết quả sẽ khi kiểm tra sự kiện sẽ như sau:


```
{
  "timestamp": "2023-04-04T16:49:25.028063+0000",
  "flow_id": 1884489195537556,
  "in_iface": "ens33",
  "event_type": "alert",
  "src_ip": "108.157.30.90",
  "src_port": 80,
  "dest_ip": "192.168.180.131",
  "dest_port": 36466,
  "proto": "TCP",
  "community_id": "1:+oZgma/WsgkSCKghMSpPb6+XmXY=",
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2100498,
    "rev": 7,
    "signature": "GPL ATTACK_RESPONSE id check returned root",
    "category": "Potentially Bad Traffic",
    "severity": 2,
    "metadata": {
      "created_at": [
        "2010_09_23"
      ],
      "updated_at": [
        "2010_09_23"
      ]
    }
  }
},
```

+ **Xác định Network Interface để sử dụng:**

`ip -p -j route show default`: chạy lệnh này để kiểm tra tên device default thường là eth hay ens:

```
root@svubuntu2004:/etc/netplan# ip -p -j route show default
[ {
  "dst": "default",
  "gateway": "192.168.180.2",
  "dev": "ens33",
  "protocol": "static",
  "flags": [ ]
} ]
```

`sudo nano /etc/suricata/suricata.yaml`: mở file và thay đổi interface trong af-packet từ thành `ens33`:

```
af-packet:
  - interface: ens33
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
```

+ **Cấu hình Live Rule Reloading**: giúp cho khi mình thêm xóa sửa rule thì không cần phải restart lại Suricata:

`sudo nano /etc/suricata/suricata.yaml`: mở file và thêm rule-reload trong detect-engine là `true` vào cuối file:

```
detect-engine:
  - rule-reload: true
```

- Cập nhật Suricata RuleSets:

Rule sẽ được lưu trong thư mục `/etc/suricata/rules`

+ Sử dụng tool do Suricata cung cấp `suricata-update` để tải các ruleset từ các external provider:

`sudo suricata-update`

```
5/4/2023 -- 06:43:09 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 41878; enabled: 33471;
added: 33; removed 0; modified: 1309
5/4/2023 -- 06:43:10 - <Info> -- Writing /var/lib/suricata/rules/classification.config
5/4/2023 -- 06:43:10 - <Info> -- Testing with suricata -T.
5/4/2023 -- 06:43:41 - <Info> -- Done.
```

+ Liệt kê các default set of rule providers:

`sudo suricata-update list-sources`

```
root@svubuntu2004:/etc/suricata/rules# sudo suricata-update list-sources
5/4/2023 -- 06:48:07 - <Info> -- Using data-directory /var/lib/suricata.
5/4/2023 -- 06:48:07 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
5/4/2023 -- 06:48:07 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
5/4/2023 -- 06:48:07 - <Info> -- Found Suricata version 6.0.10 at /usr/bin/suricata.
Name: et/open
  Vendor: Proofpoint
  Summary: Emerging Threats Open Ruleset
  License: MIT
Name: et/pro
  Vendor: Proofpoint
  Summary: Emerging Threats Pro Ruleset
  License: Commercial
  Replaces: et/open
  Parameters: secret-code
  Subscription: https://www.proofpoint.com/us/threat-insight/et-pro-ruleset
```

+ Có thể thêm external provider bằng lệnh:

`sudo suricata-update enable-source tgreen/hunting`: trong đó `tgreen/hunting` là external provider. Sau đó chạy `suricata-update`:

- Kiểm tra cấu hình:

`sudo suricata -T -c /etc/suricata/suricata.yaml -v`: chạy lệnh này để kiểm tra.

```
root@svubuntu2004:/etc/suricata/rules# sudo suricata -T -c /etc/suricata/suricata.yaml -v
5/4/2023 -- 06:53:41 - <Info> - Running suricata under test mode
5/4/2023 -- 06:53:41 - <Notice> - This is Suricata version 6.0.10 RELEASE running in SYSTEM mode
5/4/2023 -- 06:53:41 - <Info> - CPUs/cores online: 2
5/4/2023 -- 06:53:41 - <Info> - fast output device (regular) initialized: fast.log
5/4/2023 -- 06:53:41 - <Info> - eve-log output device (regular) initialized: eve.json
5/4/2023 -- 06:53:41 - <Info> - stats output device (regular) initialized: stats.log
5/4/2023 -- 06:53:51 - <Info> - 1 rule files processed. 33471 rules successfully loaded, 0 rules fa
5/4/2023 -- 06:53:51 - <Info> - Threshold config parsed: 0 rule(s) found
5/4/2023 -- 06:53:51 - <Info> - 33474 signatures processed. 1234 are IP-only rules, 5313 are inspec
26723 inspect application layer, 108 are decoder event only
5/4/2023 -- 06:54:09 - <Notice> - Configuration provided was successfully loaded. Exiting.
5/4/2023 -- 06:54:10 - <Info> - cleaning up signature grouping structure... complete
```

- Chạy và kiểm tra trạng thái:

```
sudo systemctl start suricata.service
```

```
sudo systemctl status suricata.service
```

```
root@svubuntu2004:/etc/suricata/rules# sudo systemctl status suricata.service
● suricata.service - LSB: Next Generation IDS/IPS
   Loaded: loaded (/etc/init.d/suricata; generated)
   Active: active (running) since Wed 2023-04-05 05:49:44 UTC; 1h 6min ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 8 (limit: 1027)
   Memory: 16.8M
    CGroup: /system.slice/suricata.service
            └─1006 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata
Apr 05 05:49:43 svubuntu2004 systemd[1]: Starting LSB: Next Generation IDS/IPS...
Apr 05 05:49:44 svubuntu2004 suricata[920]: Starting suricata in IDS (af-packet) mode... done.
Apr 05 05:49:44 svubuntu2004 systemd[1]: Started LSB: Next Generation IDS/IPS.
```

`sudo tail -f /var/log/suricata/suricata.log`: chạy lệnh này để kiểm tra test xong chưa nếu rồi thì sẽ có kết quả sau:

- Kiểm tra hoạt động của các rule:

Test thử 1 rule bằng lệnh sau:

```
curl http://testmynids.org/uid/index.html
```

Kết quả:

```
root@svubuntu2004:/etc/suricata/rules# curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
```

Log sẽ được lưu vào 2 file theo cấu hình mặc định của Suricata:

`/var/log/suricata/fast.log`:

```
root@svubuntu2004:/etc/suricata/rules# grep 2100498 /var/log/suricata/fast.log
04/04/2023-16:49:25.028063  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 108.157.30.90:80 -> 192.168.180.131:36466
```

`/var/log/suricata/eve.log`: máy đọc được (cần cài đặt jq trước - `sudo apt install jq`) với định dạng JSON.


```

root@svubuntu2004:/etc/suricata/rules# jq 'select(.alert .signature_id==2100498)' /var/log/suricata/eve.json
{
  "timestamp": "2023-04-04T16:49:25.028063+0000",
  "flow_id": 1884489195537556,
  "in_iface": "ens33",
  "event_type": "alert",
  "src_ip": "108.157.30.90",
  "src_port": 80,
  "dest_ip": "192.168.180.131",
  "dest_port": 36466,
  "proto": "TCP",
  "community_id": "1:+oZgma/WsqkSCKghMSpPb6+XmXY=",
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2100498,
    "rev": 7,
    "signature": "GPL ATTACK_RESPONSE id check returned root",
    "category": "Potentially Bad Traffic",
    "severity": 2,
    "metadata": {
      "created_at": [
        "2010_09_23"
      ],
      "updated_at": [
        "2010_09_23"
      ]
    }
  },
  "http": {
    "hostname": "testmynids.org",
    "url": "/uid/index.html",
    "http_user_agent": "curl/7.68.0",
    "http_content_type": "text/html",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "status": 200,
    "length": 39
  },
}

```

2.2.2 Cài đặt Elasticsearch and Kibana

- Thêm *Elastic GPG key*:

```
curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
```

- Thêm Elastic source list vào `sources.list.d`, nơi apt tìm những nguồn mới:

```
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a
/etc/apt/sources.list.d/elastic-7.x.list
```

- Update server và cài đặt Elasticsearch và Kibana:

```
sudo apt update
```

```
sudo apt install elasticsearch kibana
```

- Kiểm tra `ip private` của server:

```

root@svubuntu2004:/home/tct# ip -brief address show
lo                UNKNOWN        127.0.0.1/8 ::1/128
ens33             UP             192.168.180.131/24 fe80::20c:29ff:fe49:353d/64

```

- Cấu hình Elasticsearch: mặc định thì Elasticsearch cấu hình chỉ chấp nhận kết nối local và không có xác thực nên các tool như Filebeat không thể gửi log tới. Nên cần phải cấu hình mạng và `xpack` module.

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```

/etc/elasticsearch/elasticsearch.yml

```
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
#network.host: 192.168.0.1
network.bind_host: ["127.0.0.1", "your_private_ip"]
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
```

+ Thêm vào cuối file:

```
discovery.type: single-node
```

```
xpack.security.enabled: true
```

discovery.type: single-node: cho phép Elasticsearch chạy ở chế độ single-node.

xpack.security.enabled: true: bật các tính năng bảo mật trong Elasticsearch.

/etc/elasticsearch/elasticsearch.yml

```
...
discovery.type: single-node
xpack.security.enabled: true
```

+ Thêm các firewall rule để cho phép các client khác có thể truy cập:

```
sudo ufw allow in on ens33
```

```
sudo ufw allow out on ens33
```

+ Bật Elasticsearch:

```
sudo systemctl start elasticsearch.service
```

+ Cấu hình Elasticsearch Password:

```
cd /usr/share/elasticsearch/bin
```

```
sudo ./elasticsearch-setup-passwords auto
```

```
Initiating the setup of passwords for reserved users elastic,apm_system,kibana,kibana_system,logstash_system
The passwords will be randomly generated and printed to the console.
Please confirm that you would like to continue [y/N]y
```

```
Changed password for user apm_system
PASSWORD apm_system = eWqzd0asAmxZ0gcJpOvn
```

```
Changed password for user kibana_system
PASSWORD kibana_system = 1HLVxfqZMd7aFQ56Uab1
```

```
Changed password for user kibana
PASSWORD kibana = 1HLVxfqZMd7aFQ56Uab1
```

```
Changed password for user logstash_system
PASSWORD logstash_system = wUjY59H91WGvGaN8uFLc
```

```
Changed password for user beats_system
PASSWORD beats_system = 2p81hIdAzWKknhzA992m
```

```
Changed password for user remote_monitoring_user
PASSWORD remote_monitoring_user = 85HF85F16cPslJlA8wPG
```

```
Changed password for user elastic
PASSWORD elastic = 6kNbsxQGYZ2EQJiqJpgl
```

- Cấu hình Kibana:

+ Bật xpack.security trong Kibana và tạo key:

```
cd /usr/share/kibana/bin/
```

```
sudo ./kibana-encryption-keys generate -q
```

Output

```
xpack.encryptedSavedObjects.encryptionKey: 66fbd85ceb3cba51c0e939fb2526f585
xpack.reporting.encryptionKey: 9358f4bc7189ae0ade1b8deec7f38ef
xpack.security.encryptionKey: 8f847a594e4a813c4187fa93c884e92b
```

+ Mở file và thêm các dòng và cuối file:

```
sudo nano /etc/kibana/kibana.yml
```

```
xpack.encryptedSavedObjects.encryptionKey: 66fbd85ceb3cba51c0e939fb2526f585
```

```
xpack.reporting.encryptionKey: 9358f4bc7189ae0ade1b8deec7f38ef
```

```
xpack.security.encryptionKey: 8f847a594e4a813c4187fa93c884e92b
```

+ Cấu hình kết nối mạng Kibana:

```
nano /etc/kibana/kibana.yml
```

/etc/kibana/kibana.yml

```
# Kibana is served by a back end server. This setting specifies the port to use.
#server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are
# The default is 'localhost', which usually means remote machines will not be able to connect
# To allow connections from remote users, set this parameter to a non-loopback address.
#server.host: "localhost"
server.host: "your_private_ip"
```

+ Cấu hình Kibana credential:

```
sudo ./kibana-keystore add elasticsearch.username
```

Nhập "kibana_system".

```
sudo ./kibana-keystore add elasticsearch.password
```

Nhập kibana_system password ở phần trên vào.

+ Mở Kibana:

```
sudo systemctl start kibana.service
```

2.2.3 Cài đặt Filebeat

- Sau khi đã cài đặt Elasticsearch và Kibana thành công thì cài đặt Filebeat trên Suircata server để gửi log tới Elasticsearch:

```
curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
```

```
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a
/etc/apt/sources.list.d/elastic-7.x.list
```

```
sudo apt update
```

```
sudo apt install filebeat
```

```
sudo nano /etc/filebeat/filebeat.yml
```

/etc/filebeat/filebeat.yml

```
. . .
# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify an additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  #host: "localhost:5601"
  host: "your_private_ip:5601"

. . .

output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["your_private_ip:9200"]

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  username: "elastic"
  password: "6kNbsxQGYZ2EQJiqJpg1"
```

sudo filebeat modules enable suricata

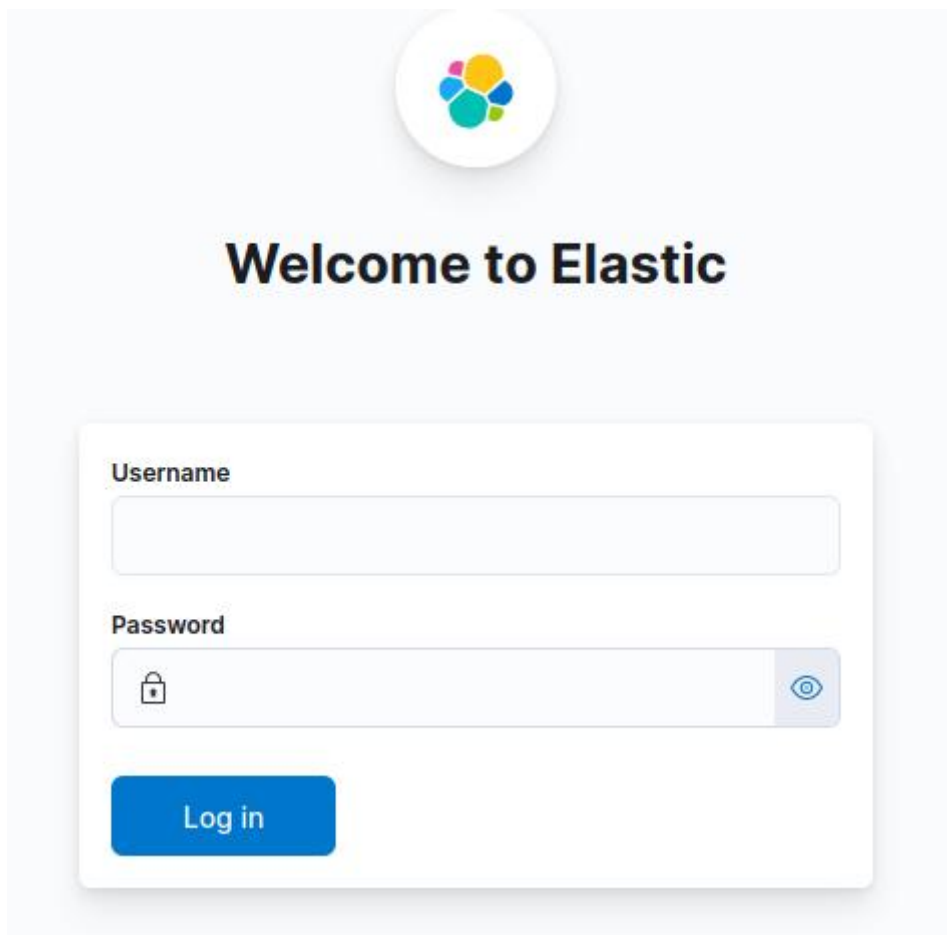
sudo filebeat setup

sudo systemctl start filebeat.service

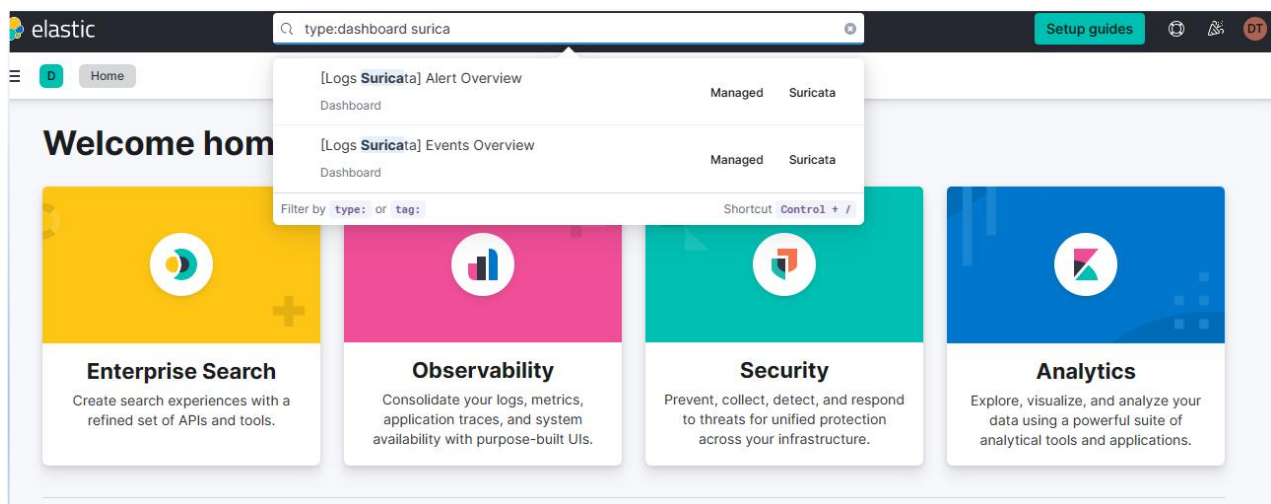
2.2.4 Kết quả:

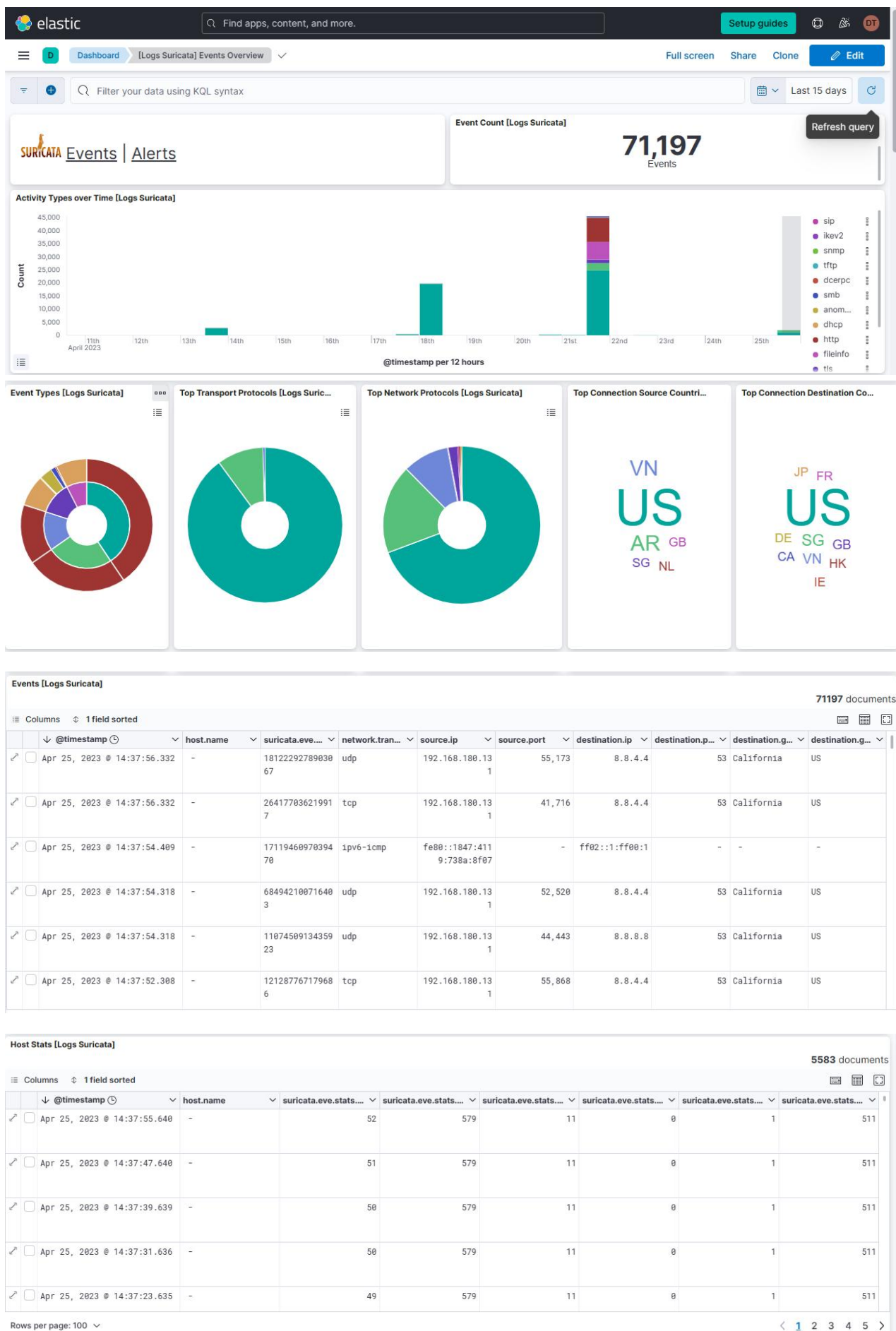
ssh -L 5601:your_private_ip:5601 your_ssh_username@your_public_ip -N

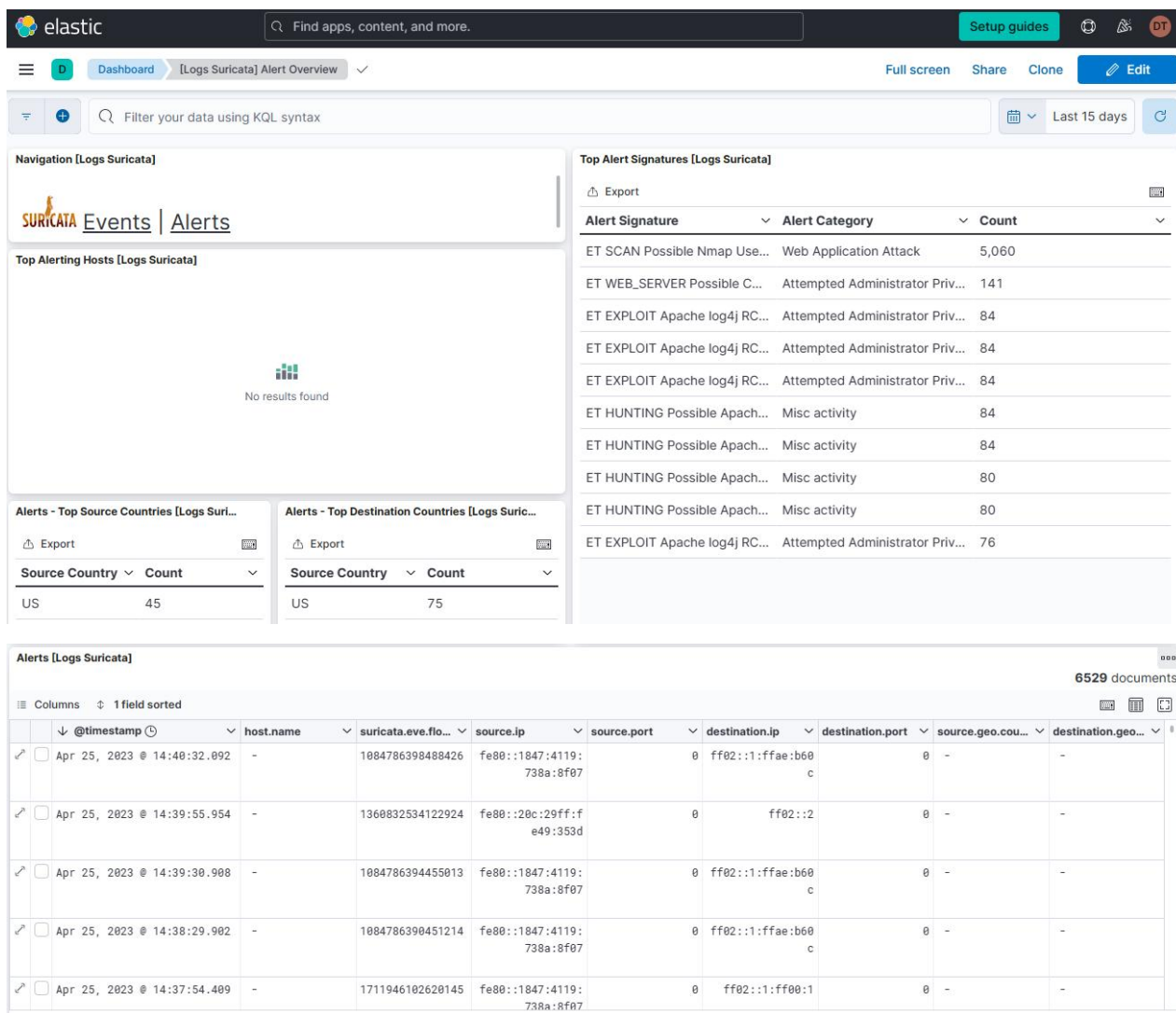
Truy cập 127.0.0.1:5601:



- Sử dụng username=elastic và password=copy ở hình trên.







CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM

3.1 Kịch bản 1:

- Phát hiện các dấu hiệu tấn công: khi sử dụng Nessus để quét lỗ hổng.

Alert Signature	Alert Ca...	Count
ET EXPLOIT Cisco RV320/RV325 Config Disclosure Attempt Inbound (...)	Attempted ...	1
ET EXPLOIT Possible CVE-2014-3704 Drupal SQLi attempt URLENCO...	Web Applic...	1
ET POLICY HTTP POST contains pass= in cleartext	Potential C...	1
ET POLICY Possible Kali Linux hostname in DHCP Request Packet	Potential C...	1
ET SCAN Possible Nmap User-Agent Observed	Web Applic...	2,606
ET WEB_SERVER ColdFusion adminapi access	Web Applic...	1
ET WEB_SERVER ColdFusion administrator access	Web Applic...	4
ET WEB_SERVER Possible IIS Integer Overflow DoS (CVE-2015-1635)	Web Applic...	1
SURICATA Applayer Detect protocol only one direction	Generic Pr...	1
SURICATA Applayer Mismatch protocol both directions	Generic Pr...	1

Alerts [Logs Suricata] 2634 documents

	@timestamp	host.name	suricata eve.flow...	source.ip	source.port	destination.ip	destination.port	source.geo.cou...	destination.geo...
<input type="checkbox"/>	Apr 21, 2023 @ 14:23:16.577	-	892673416547346	192.168.180.129	59,974	192.168.180.134	80	-	-
<input type="checkbox"/>	Apr 21, 2023 @ 14:23:16.576	-	672899948009356	192.168.180.129	59,958	192.168.180.134	80	-	-
<input type="checkbox"/>	Apr 21, 2023 @ 14:23:16.574	-	1350716646276257	192.168.180.129	59,956	192.168.180.134	80	-	-
<input type="checkbox"/>	Apr 21, 2023 @ 14:23:16.572	-	1260543807894372	192.168.180.129	59,944	192.168.180.134	80	-	-
<input type="checkbox"/>	Apr 21, 2023 @ 14:23:16.570	-	1523891875130987	192.168.180.129	59,930	192.168.180.134	80	-	-

Rows per page: 100

3.2 Kịch bản 2:

Tấn công CVE-2017-7269 nhưng Suricata không bắt được và cần phải chỉnh lại rule, cập nhật rule đỏ thành xanh trong đó bỏ đi option pcre (perl regex) để có thể phát hiện dấu hiệu tấn công:

```

alert http $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"ET WEB_SERVER
Microsoft IIS Remote Code Execution (CVE-2017-7269)"; flow:to_server,established;
http.header; content:"If[3a 20 3c]"; pcre:"/If[x3a\x20\x3c[^\r\n>]+?(?:[\x7f-\xff])/mi";
reference:url,github.com/edwardz246003/IIS_exploit/blob/master/exploit.py;
classtype:attempted-user; sid:2024107; rev:3; metadata:affected_product Microsoft_IIS,
attack target Web_Server, created at 2017 03 28, cve cve 2017 7269, deployment

```

```
Datacenter, former_category WEB_SERVER, performance_impact Low,  
signature_severity Major, updated_at 2020_08_04;)
```

```
alert http any any -> any any (msg:"ET WEB_SERVER Microsoft IIS Remote Code  
Execution (CVE-2017-7269)"; flow:to_server,established; http.header; content:"If3a 20  
3c|"; reference:url,github.com/edwardz246003/IIS_exploit/blob/master/exploit.py;  
classtype:attempted-user; sid:2024107; rev:3; metadata:affected_product Microsoft_IIS,  
attack_target Web_Server, created_at 2017_03_28, cve cve_2017_7269, deployment  
Datacenter, former_category WEB_SERVER, performance_impact Low,  
signature_severity Major, updated_at 2020_08_04;)
```

- Sau khi cập nhật rule thì cần restart lại server suricata để nhận rule:

```
sudo systemctl restart suricata.service
```

- Kết quả phát hiện thành công:

Top Alert Signatures [Logs Suricata]		
 Export 		
Alert Signature	Alert Ca...	Count
ET WEB_SERVER Microsoft IIS Remote Code Execution (CVE-2017-7269)	Attempted ...	16

TÀI LIỆU THAM KHẢO

- [1] [Suricata User Guide — Suricata 6.0.11 documentation](#)
- [2] [Welcome to Elastic Docs | Elastic](#)

TP. HCM, ngày tháng năm 2023
XÁC NHẬN CỦA GIẢNG VIÊN HƯỚNG DẪN

TS. Huỳnh Thanh Tâm