**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC TPHCM**



*Đề tài:*

**Xây dựng hệ thống phát hiện xâm nhập (Snort) cho Linux**

GVHD: **Cao Tiến Thành**

SVTH: Dương Hoàng Khang

MSSV: 19DH110211

**Tháng 10 Năm 2021**

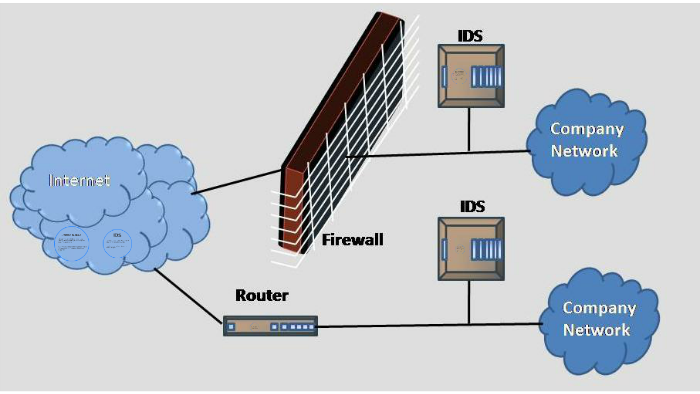
**Mục Lục**

1. **Tổng quan đề tài**
2. **Tóm tắt đề tài**

* Bảo mật và độ tin cậy là mối quan tâm chính của việc sử dụng bất kỳ mạng nào trong cuộc sống hàng ngày của chúng ta. Nhưng với những tiến bộ và phát triển nhanh chóng của công nghệ, các cuộc tấn công ngày càng trở nên tinh vi hơn là phòng thủ. Mặc dù tường lửa và bộ lọc gói (packet filter) có trên Router là những yếu tố cần thiết của cấu trúc liên kết bảo mật mạng tổng thể, nhưng chỉ riêng chúng thì chưa đủ. Vì vậy, để bảo vệ mạng khỏi bị truy cập trái phép ta cần triển khai những phần mềm ISD như Snort. Snort là một trong những ứng dụng IDS và hệ thống phòng chống xâm nhập (IPS) phổ biến nhất và được sự tin dùng của những chuyên viên bảo mật mạng. Việc chọn đề tài này nhầm thực hiện những cuộc xâm nhập mạng giả định và phát ra thông báo cụ thể về các sự xâm nhập mạng trái phép.

1. **Cơ sở lý luận**

* **IDS là gì ?**



( Nguồn: <https://prezi.com/xfnwubog1vvi/what-is-ids/> )

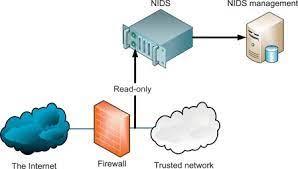
* **IDS** là viết tắt của Intrusion Detection System - Hệ thống Phát hiện Xâm nhập.

Đây là các phần mềm hoặc công cụ giúp bảo mật hệ thống và cảnh báo mỗi khi có xâm nhập. IDS thường là một phần của các hệ thống bảo mật hoặc phần mềm khác, đi kèm với nhiệm vụ bảo vệ hệ thống thông tin.

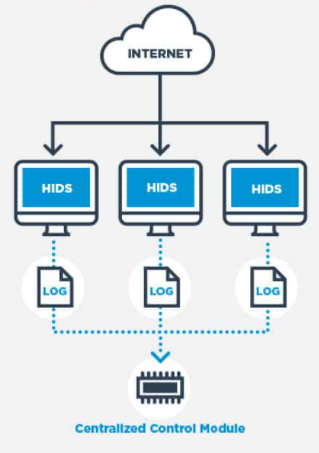
* Các tính năng quan trọng nhất của IDS bao gồm: giám sát traffic mạng và các hoạt động khả nghi; đưa ra các cảnh báo về những điểm bất thường cho hệ thống và đơn vị quản trị mạng; kết hợp với tường lửa, phần mềm diệt virus tạo nên một hệ thống bảo mật hoàn chỉnh.
* IDS cũng có thể phân biệt giữa những tấn công bên trong từ bên trong (từ những người trong công ty) hay tấn công từ bên ngoài (từ các hacker). IDS phát hiện dựa trên các dấu hiệu đặc biệt về các nguy cơ đã biết (giống như cách các phần mềm diệt virus dựa vào các dấu hiệu đặc biệt để phát hiện và diệt virus) hay dựa trên so sánh lưu thông mạng hiện tại với baseline (thông số đo đạc chuẩn của hệ thống) để tìm ra các dấu hiệu khác thường.
* **Phân loại IDS**

IDS được phân thành 5 loại:

* **Hệ thống phát hiện xâm nhập mạng (NIDS)**: Hệ thống phát hiện xâm nhập mạng (NIDS) được thiết lập tại một điểm được quy hoạch trong mạng để kiểm tra lưu lượng từ tất cả các thiết bị trên mạng. Nó thực hiện quan sát lưu lượng truyền trên toàn bộ mạng con và khớp với lưu lượng truyền trên các mạng con với tập hợp các cuộc tấn công đã biết. Khi một cuộc tấn công được xác định hoặc quan sát thấy hành vi bất thường, cảnh báo có thể được gửi đến quản trị viên. Ví dụ về NIDS đang cài đặt nó trên mạng con nơi đặt tường lửa để xem liệu ai đó đang cố gắng bẻ khóa tường lửa. (Snort thuộc loại NIDS).

(Nguồn : <https://www.sciencedirect.com/topics/computer-science/network-based-intrusion-detection-system> )

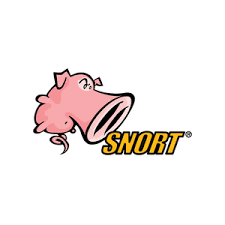
* **Hệ thống phát hiện xâm nhập máy chủ (HIDS)**: Hệ thống phát hiện xâm nhập máy chủ (HIDS) chạy trên các máy chủ hoặc thiết bị độc lập trên mạng. HIDS chỉ giám sát các gói đến và đi từ thiết bị và sẽ cảnh báo cho quản trị viên nếu phát hiện hoạt động đáng ngờ hoặc độc hại. Nó chụp nhanh các tệp hệ thống hiện có và so sánh nó với ảnh chụp nhanh trước đó. Nếu các tệp hệ thống phân tích bị chỉnh sửa hoặc xóa, một cảnh báo sẽ được gửi đến quản trị viên để điều tra. Một ví dụ về việc sử dụng HIDS có thể được nhìn thấy trên các máy quan trọng của nhiệm vụ, những máy này được cho là sẽ không thay đổi cách bố trí của chúng.



( Nguồn : https://hoclamgiau.com.vn/ids-la-he-thong-gi/ )

* **Hệ thống phát hiện xâm nhập dựa trên giao thức (PIDS)**: Hệ thống phát hiện xâm nhập dựa trên giao thức (PIDS) bao gồm một hệ thống hoặc tác nhân luôn thường trú ở đầu phía trước của máy chủ, kiểm soát và diễn giải giao thức giữa người dùng / thiết bị và máy chủ . Nó đang cố gắng bảo mật máy chủ web bằng cách thường xuyên theo dõi luồng giao thức HTTPS và chấp nhận giao thức HTTP liên quan. Vì HTTPS không được mã hóa và trước khi vào ngay lớp trình bày web của nó, hệ thống này sẽ cần phải nằm trong giao diện này, để sử dụng HTTPS.
* **Hệ thống phát hiện xâm nhập dựa trên giao thức ứng dụng (APIDS)**: Hệ thống phát hiện xâm nhập dựa trên giao thức ứng dụng (APIDS) là một hệ thống hoặc tác nhân thường nằm trong một nhóm máy chủ. Nó xác định các xâm nhập bằng cách giám sát và diễn giải thông tin liên lạc trên các giao thức ứng dụng cụ thể. Ví dụ: điều này sẽ giám sát giao thức SQL rõ ràng đối với phần mềm trung gian khi nó giao dịch với cơ sở dữ liệu trong máy chủ web.
* **Hệ thống phát hiện xâm nhập hỗn hợp:** Hệ thống phát hiện xâm nhập hỗn hợp được thực hiện bằng sự kết hợp của hai hoặc nhiều cách tiếp cận của hệ thống phát hiện xâm nhập. Trong hệ thống phát hiện xâm nhập hỗn hợp, tác nhân chủ hoặc dữ liệu hệ thống được kết hợp với thông tin mạng để phát triển một cái nhìn hoàn chỉnh về hệ thống mạng. Hệ thống phát hiện xâm nhập kết hợp hiệu quả hơn so với hệ thống phát hiện xâm nhập khác. Prelude là một ví dụ về Hybrid IDS.

1. **So sánh phần mềm với các công nghệ khác**
2. [**Snort**](https://quantrimang.com/url?q=aHR0cHM6Ly9zdXJpY2F0YS1pZHMub3JnL2Rvd25sb2FkLw%3D%3D)



**Snort** là một hệ thống phát hiện xâm nhập mạng, viết tắt là NIDS (Network intrusion detection system). Snort là một mã nguồn mở miễn phí với nhiều tính năng tuyệt vời trong việc bảo vệ hệ thống bên trong, phát hiện và ngăn chặn sự tấn công từ bên ngoài vào hệ thống.

Snort có thể phát hiện tấn công mạng trong thời gian thực, Snort cũng có thể được dùng như một chương trình bắt gói tin (sniffer packet), lưu trữ và kiểm tra logger (packet logger) hoặc xếp chúng, từ đó Snort sẽ tự so sánh mối nguy hiểm của hiểm họa nhằm phát hiện xâm nhập.

1. **Suricata**



Suricata là giải pháp IDS/IPS mã nguồn mở hiệu quả cho các hệ thống mạng chưa được đầu tư các giải pháp IDS/IPS thương mại. Nó được xây dựng từ các thành phần khác nhau và khả năng hoạt động của nó tùy thuộc vào cách thức cấu hình, cài đặt cho hệ thống. Ở chế độ mặc định được xem là cơ chế hoạt động tương đối tối ưu cho việc phát hiện các dạng tấn công mạng.

Suricata có thể được triển khai theo 02 cơ chế: cơ chế phát hiện(IDS) và ngăn chặn(IPS).

1. [**Zeek**](https://quantrimang.com/url?q=aHR0cHM6Ly96ZWVrLm9yZy8%3D) **(có thể bổ trợ thêm cho Snort)**



Trước đây được gọi là Bro, Zeek là một công cụ phân tích mạng mạnh mẽ tập trung vào giám sát an ninh cũng như phân tích lưu lượng mạng nói chung. Ngôn ngữ dành riêng cho domain của Zeek không dựa trên chữ ký truyền thống. Thay vào đó, Zeek ghi lại mọi thứ nó thấy trong kho lưu trữ hoạt động mạng cấp cao

**Bảng so sánh giữa các phần mềm**

| Phần mềm  Tiện ích | Snort | Suricata |
| --- | --- | --- |
| Giải pháp | Phát hiện xâm nhập | Vừa phát hiện xâm nhập, vừa ngăn chặn xâm nhập |
| Loại công cụ | NIDS | NIDS, IPS |
| Dễ cài đặt | Đơn giản, nhanh chóng. Cài đặt có sẵn từ packets. | Tốn thời gian cấu hình hơn Snort. Cài đặt cũng có sẵn từ packets. |
| File cấu hình | snort.conf, threshold.conf | [suricata.yaml](https://www.aldeid.com/wiki/Suricata/Suricata-yaml-configuration-file), classification.config, reference.config, threshold.config |

\*Bảng đánh giá dựa trên sự trải nghiệm và đọc thêm tài liệu hướng dẫn, các demo về các phần mềm trên.

**II.** **Phương pháp đánh giá & hiện thực**

1. **Thiết bị thực hiện**

* Để thực hiện , cần có 2 máy ảo:
* **Máy ảo 1:**

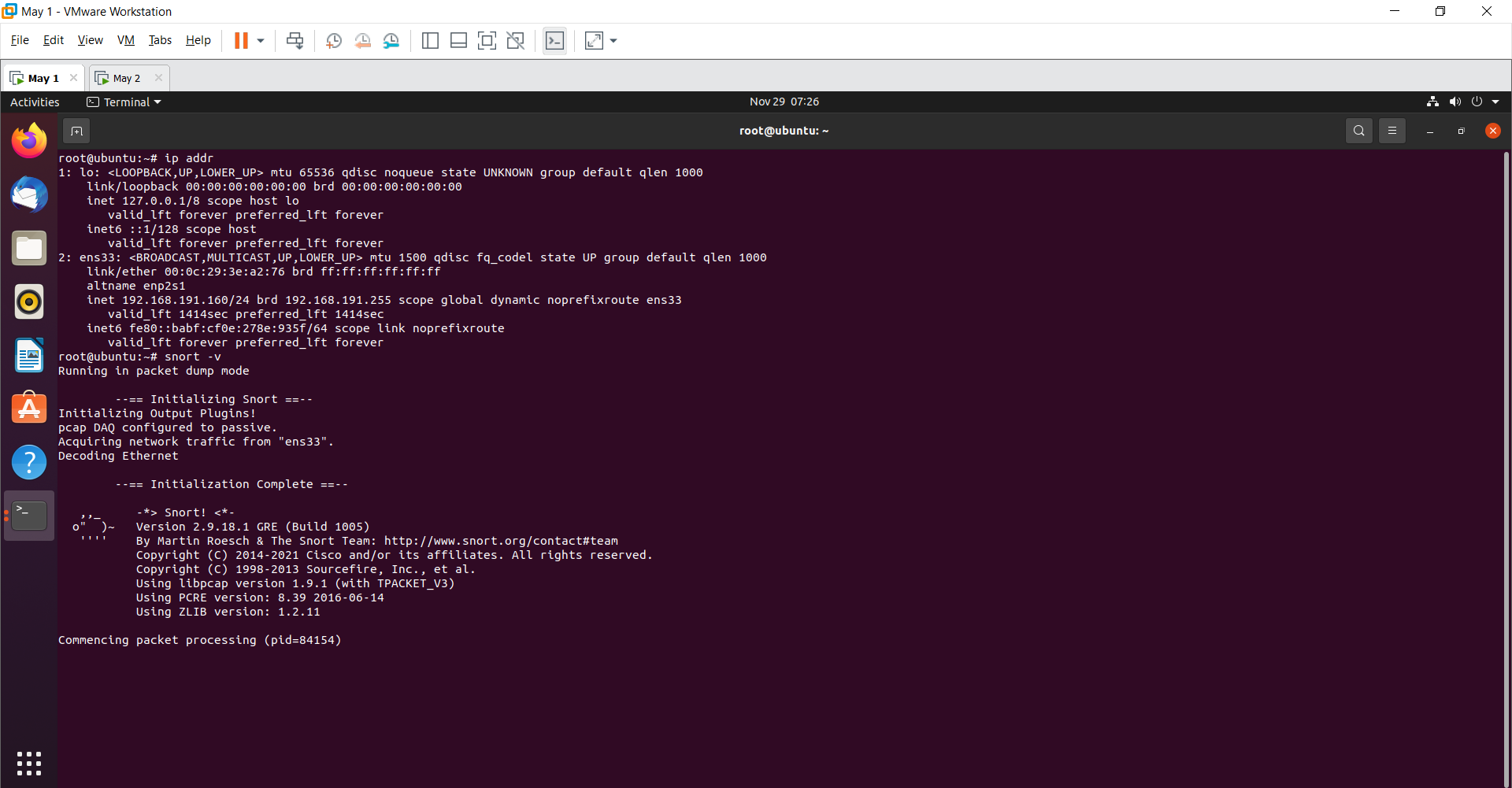
+ Hệ điều hành: Linux(ubuntu)

+ Interface: ens33

+ IP address: 192.168.191.160/24

+ Đã được cài phầm mềm Snort

+ Công việc: Phát hiện xâm nhập mạng, phát ra cảnh báo cho người dùng.



* **Máy ảo 2:**

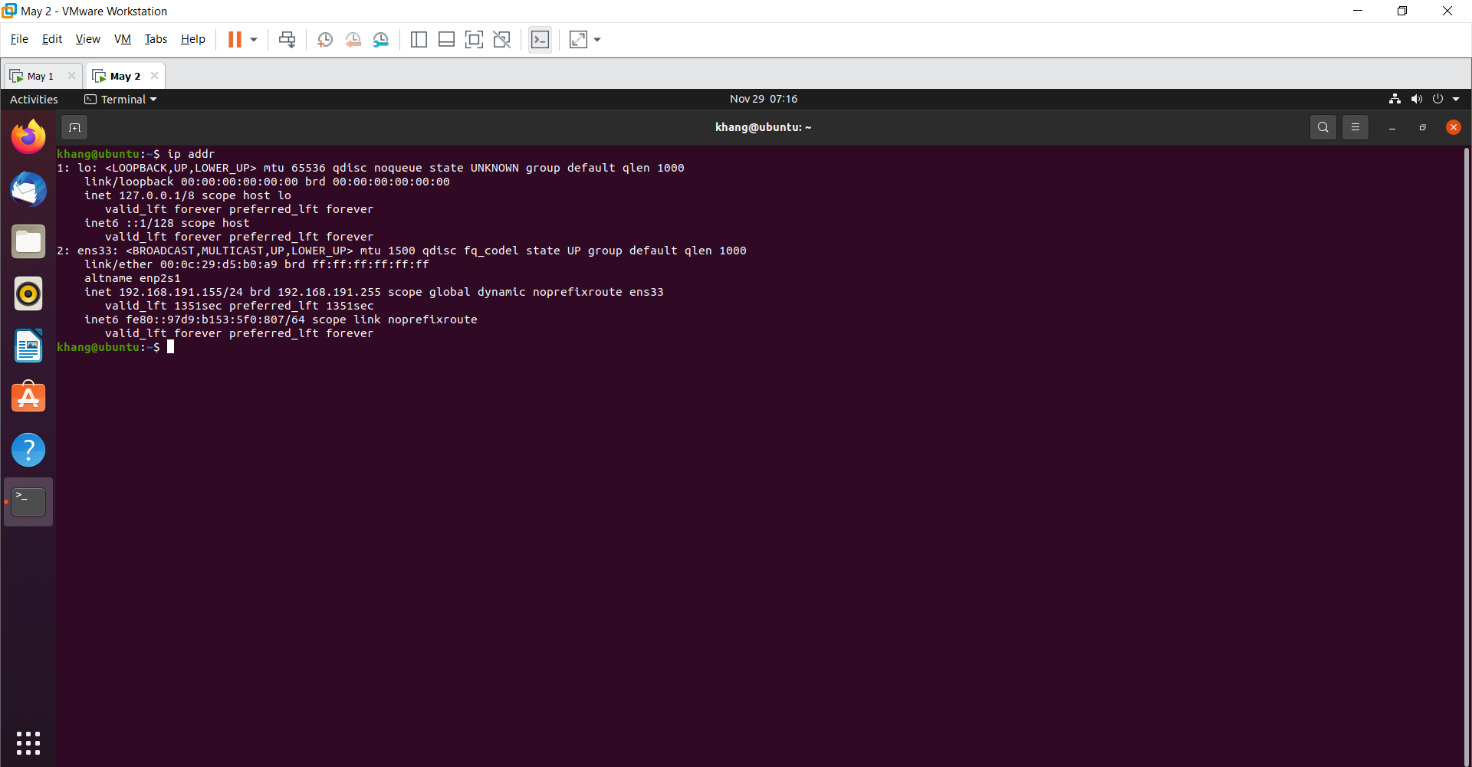
+ Hệ điều hành: Linux(ubuntu)

+ Interface: ens33

+ IP address: 192.168.191.155/24

+ Máy bình thường

+ Công việc: Thực hiện những cuộc xâm nhập mạng, tương tác với Máy ảo 1.



1. **Tiến hành cấu hình Snort và cài rules**

**\*Rules là gì?**

- Rules những quy tắc được quản trị viên hay người dùng Snort viết ra theo cấu trúc rules của Snort đặt ra. Các quy tắc cụ thể như cảnh báo, log, ngắt kết nối, v.v.. Rules chứa hành động, giao thức của quy tắc, địa chỉ IP nguồn và đích và netmark, và thông tin về cổng nguồn và cổng đích.

- Cấu trúc của Rules:

**[action][protocol][sourceIP][sourceport] -> [destIP][destport] ( [Rule options]** )

**+ action: Đ**ứng đầu tiên trong cấu trúc của rules, nó được gọi là hành động của quy tắc, hành động này cho Snort biết phải làm gì khi nó tìm thấy một packet phù hợp với tiêu chí quy tắc(thường là alert). Ngoài ra còn những hành động khác ngoài alert như: log, pass, activate,…

**+ protocol:** Loại lưu lượng (giao thức) Trường tiếp theo trong quy tắc đặt rules. Có bốn giao thức mà Snort hiện đang phân tích là:TCP, UDP, ICMP và IP.

+ **source IP**: IP nguồn xâm nhập đến máy có cấu hình Snort.(điền biến hoặc chữ)

+ **source port**: Port nguồn. (điền biến hoặc chữ)

+ **->** : cho biết hướng của lưu lượng truy cập mà rules áp dụng.

+ **dest IP**: IP của máy bị xâm nhập. (điền biến hoặc chữ)

+ **desport**: cổng của máy bị xâm nhập. (điền biến hoặc chữ)

+ **Rule option**: Các tùy chọn quy tắc tạo thành trung tâm của công cụ phát hiện xâm nhập của Snort, kết hợp tính dễ sử dụng với sức mạnh và tính linh hoạt. Tất cả các tùy chọn quy tắc Snort được tách biệt với nhau sử dụng dấu chấm phẩy (;). Các từ khóa tùy chọn quy tắc được phân tách khỏi các đối số của chúng bằng dấu hai chấm (:).

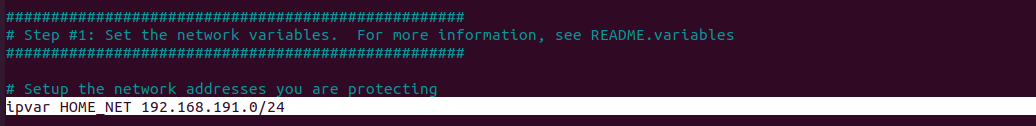
Ví dụ:

**alert icmp any any -> $HOME\_NET any (msg:"Phat hien Ping!!!"; sid:1000002; rev:1;)**

* Rule này sẽ phát ra cảnh báo nếu ai đó ping vào máy của mình(không có ip cụ thể), thông qua giao thức icmp từ bất kỳ port nào và địa chỉ IP nguồn.
* Rule này được cấu hình trong file snort.conf.
* **Tiến hành cấu hình Snort**
* **Thao tác trên máy 1( máy cài Snort):**
* Đầu tiên, gõ lệnh **nano /etc/snort/snort.conf** để tiến hành chỉnh sửa file cấu hình cho Snort.



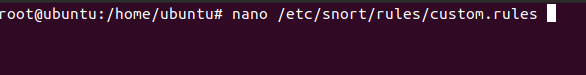
* Đi đến phần “ #setup the network addresses you are protecting “ set địa chỉ mạng mà cần bảo vệ. Máy 1 với IP là 192.168.191.160/24 cho nên set 192.168.191.0/24 .



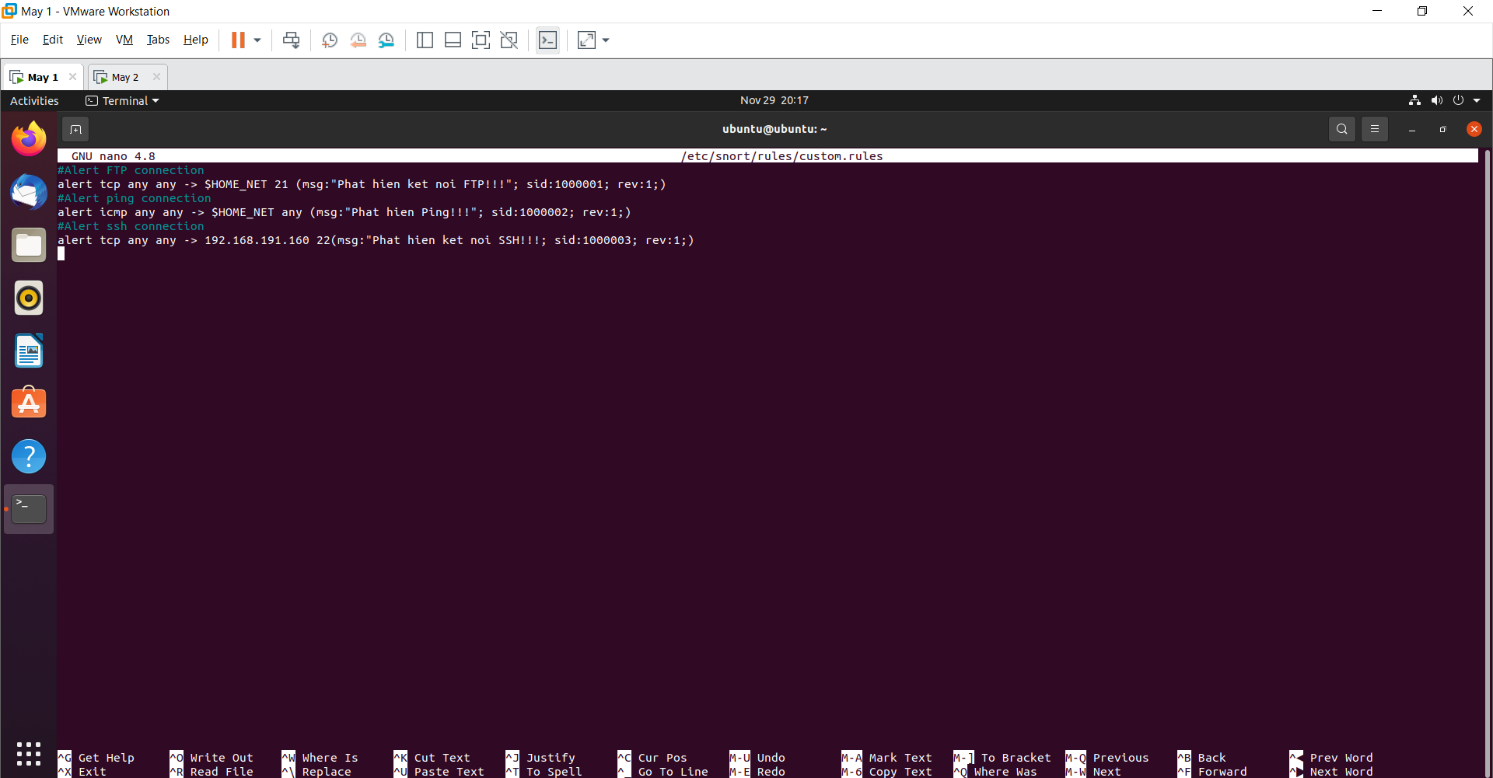
* Tạo file custom.rules để chứa rules



* Gõ lệnh nano /etc/snort/rules/custom.rules để thêm rules



* Trường hợp này, em thêm vào rules: phát hiện ping, kết nối ssh, ftp.

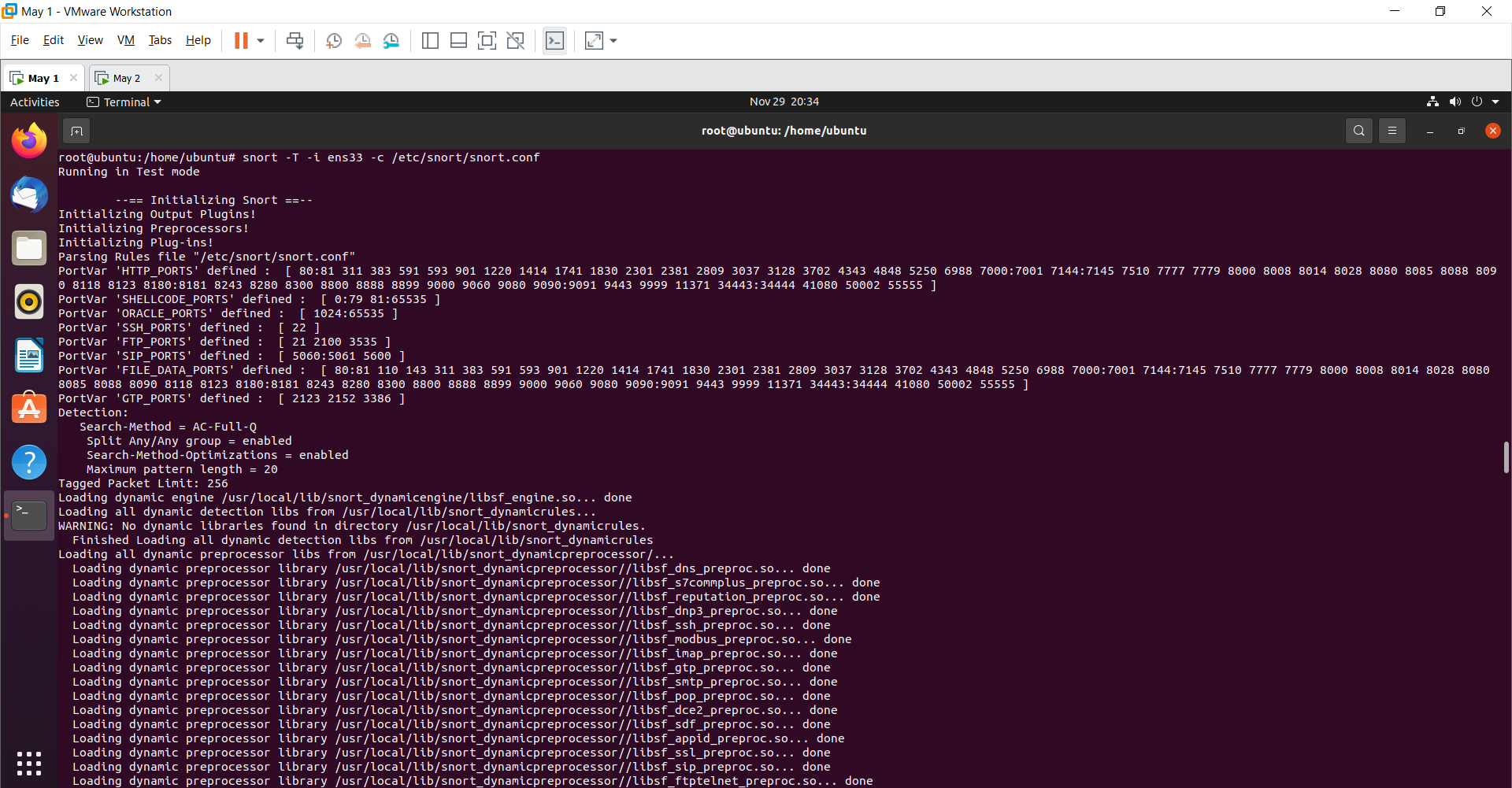


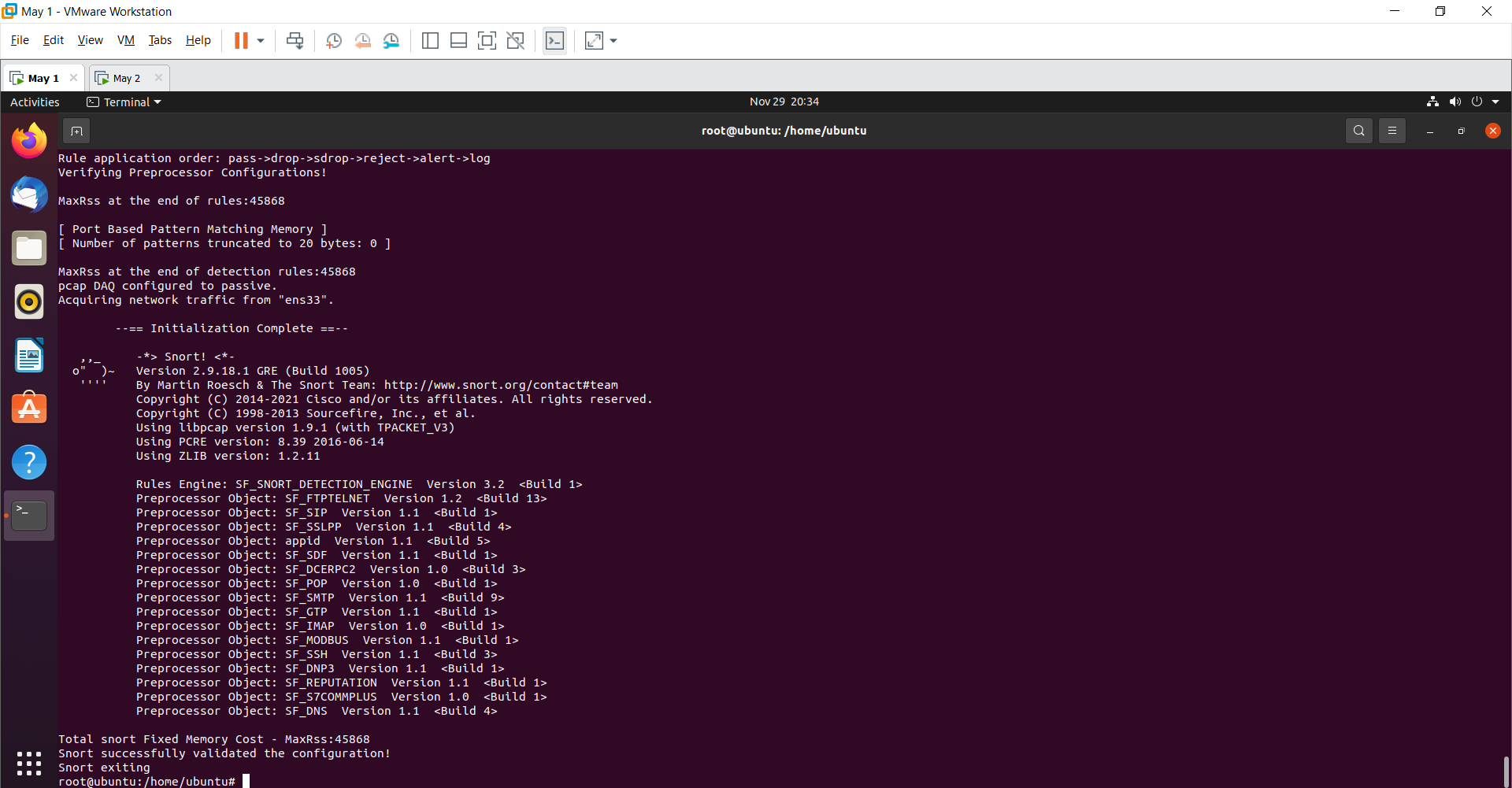
* Sau khi thoát ra và lưu lại file custom.rules. Ta phải kiểm tra rằng những rules vừa set ở trên đã load hay chưa, ta gõ dòng lệnh:

**snort -T -i ens33 -c /etc/snort/snort.conf**

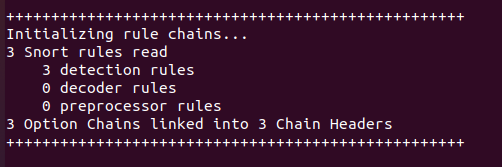
****

* Sau đó hiện lên những dòng thông tin sau:



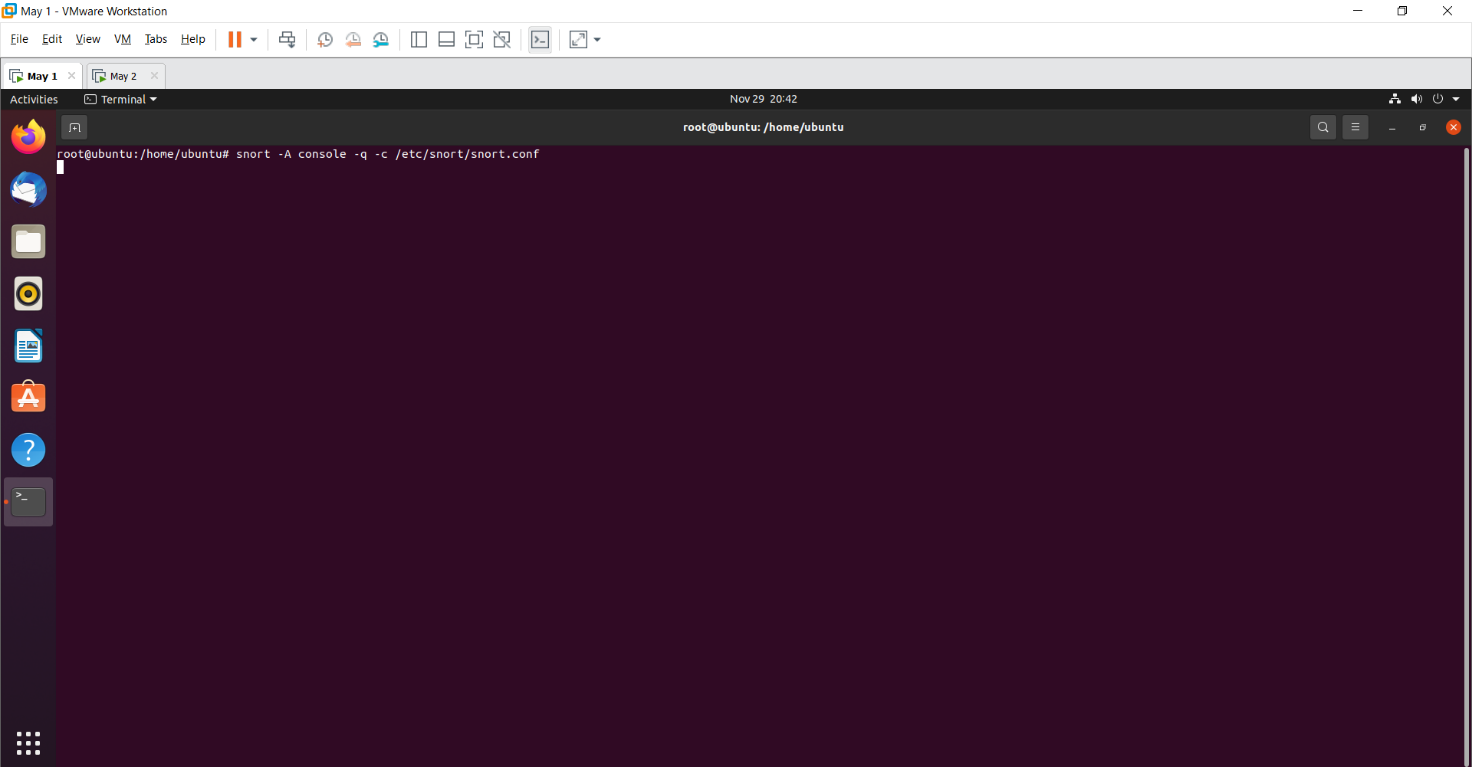


* Kéo lên kiểm tra dòng này, nếu hiện lên số rules đã đọc bằng với rules đã set trong custom.rules thì chứng tỏ đã được load.

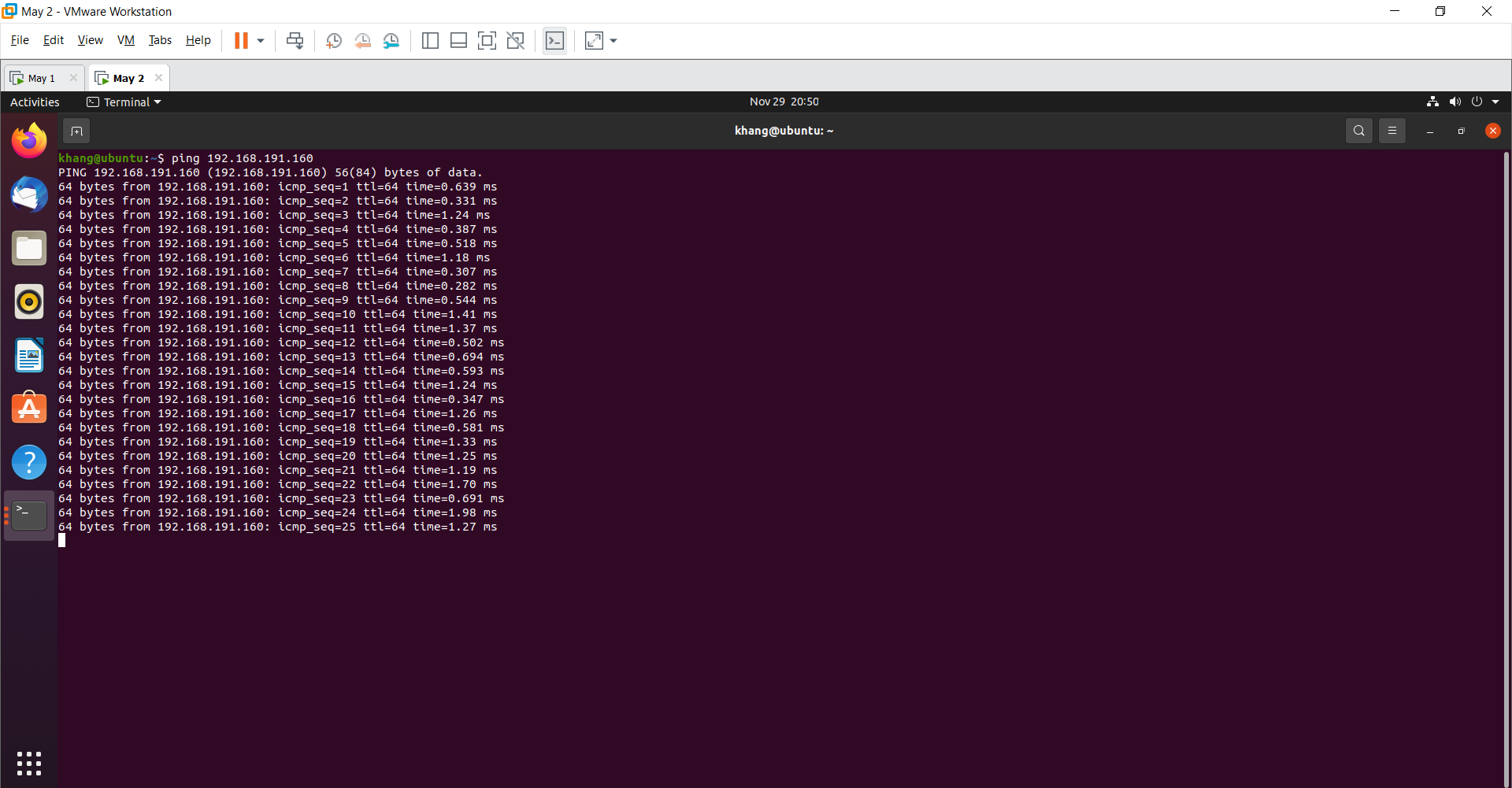


* Tiến hành chạy dòng lệnh dưới đây để khởi động Snort:

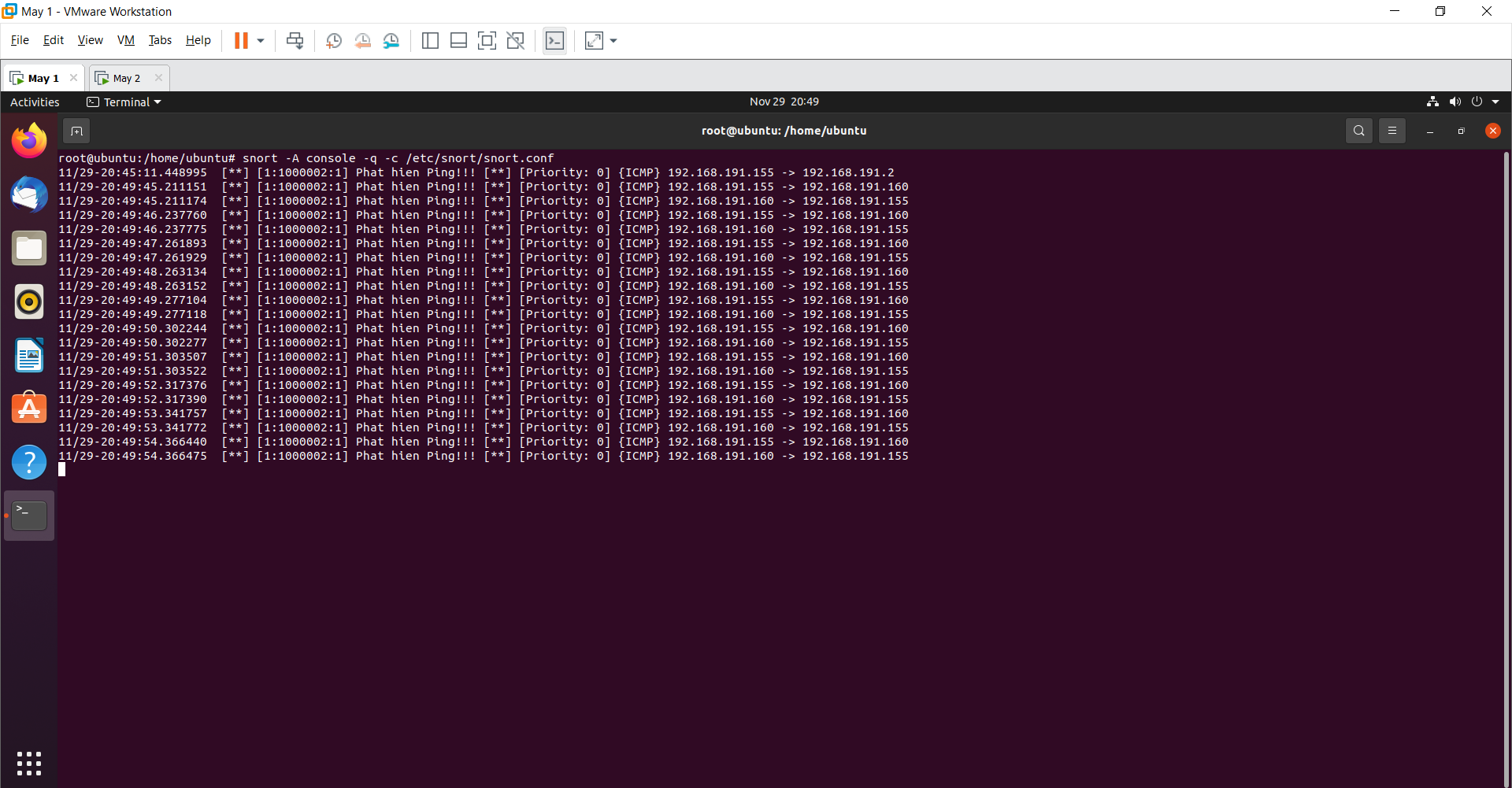
**sudo snort -A console -q -c /etc/snort/snort.conf**

****

* **Tiến hành demo**
* **Demo đầu tiên bằng cách ping**
* Ở Máy 2, tiến hành ping qua Máy 1.

****

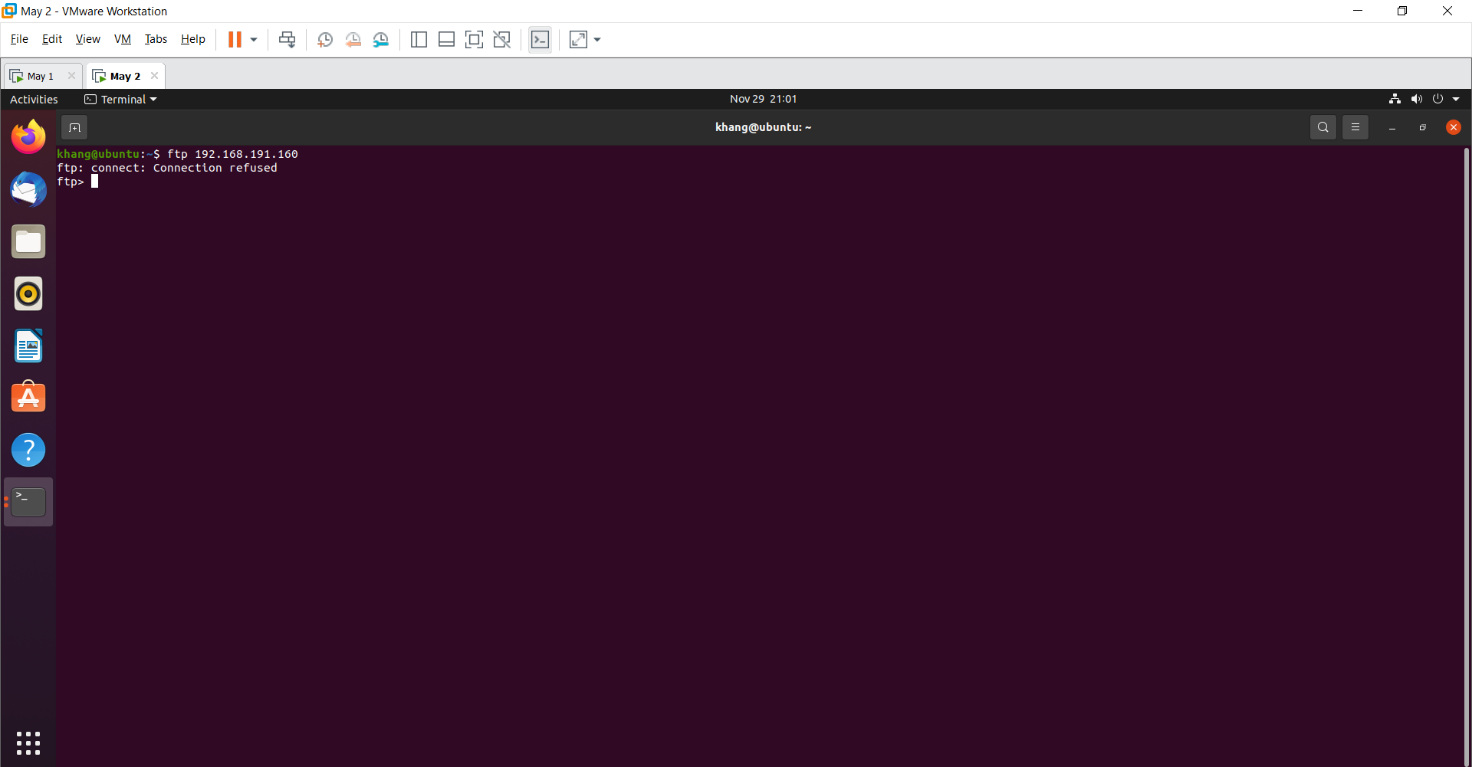
* Ở máy 1, snort phát lên alert thông báo ping cho người dùng từ địa chỉ ip của máy 2.



**Mô tả: Sau khi Máy 2 ping tới Máy 1 thì Snort phát hiện và gửi message”Phat hien ping!!!” tới người dùng, giao thức ICMP và hiện địa chỉ IP của máy đã ping tới Máy 1 là 192.168.191.155.**

* **Demo thứ 2 bằng lệnh ftp :**

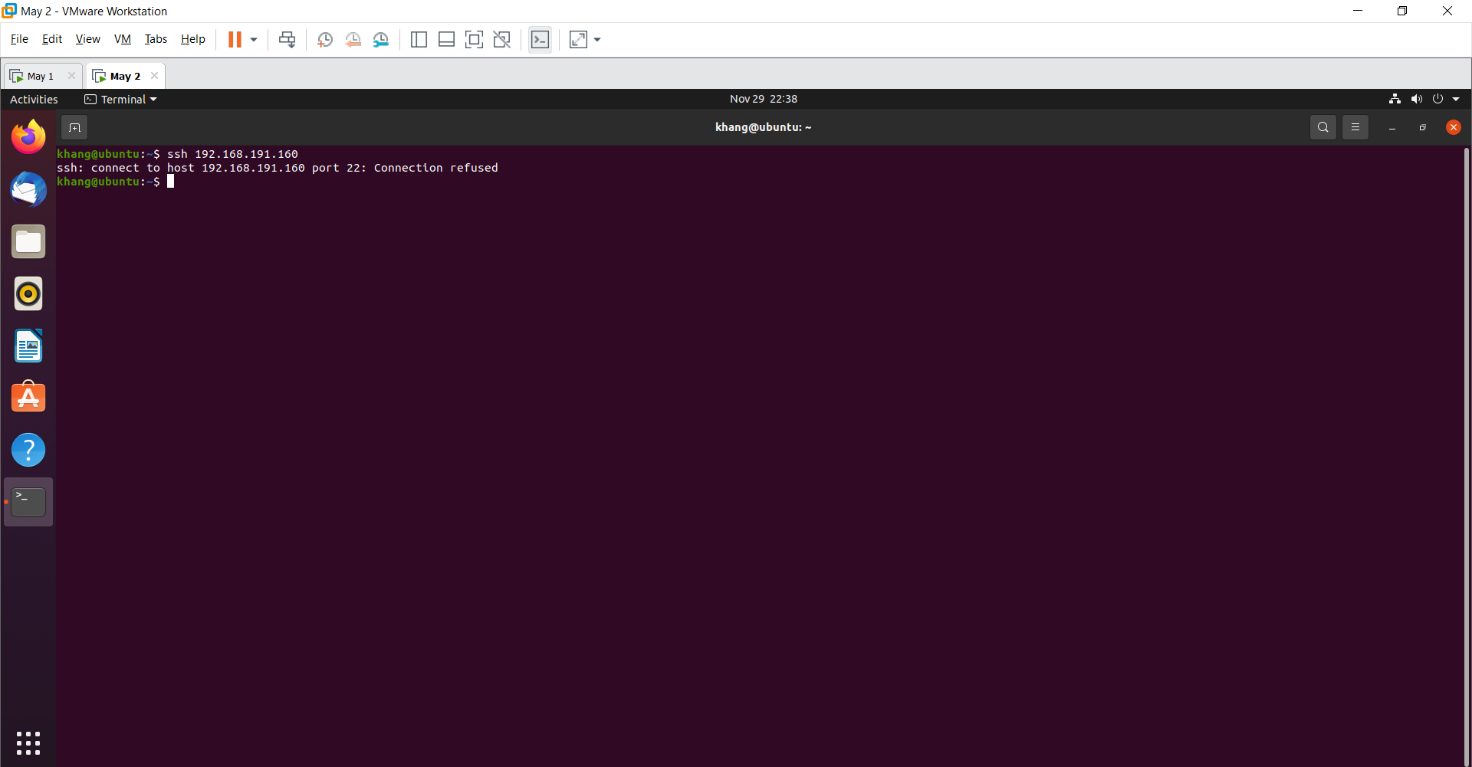
**Ở máy 2, gõ lệnh ftp 192.168.191.160**

****

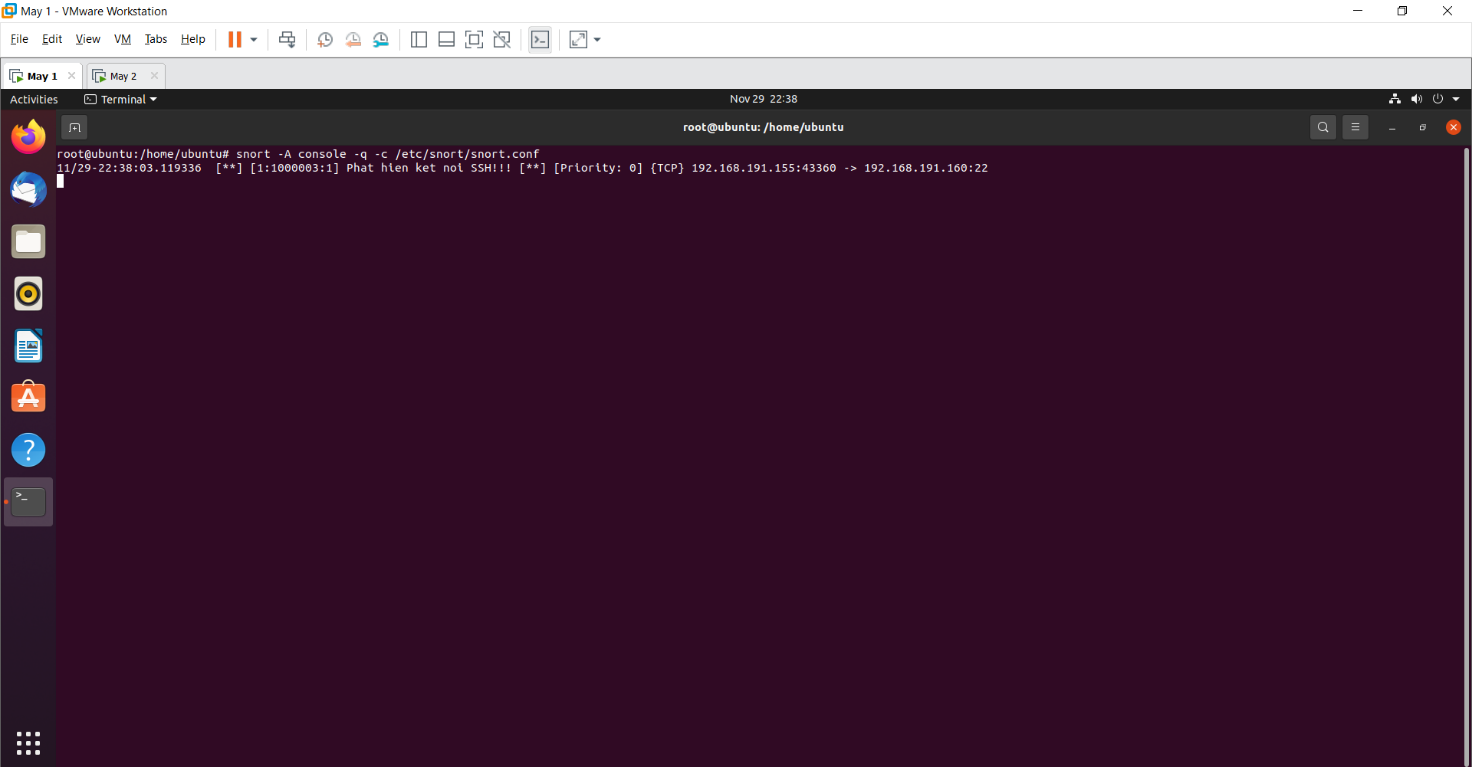
**Ngay máy 1 xuất hiện alert với message “phat hien ket noi ftp” với địa chỉ của Máy 2 đang kết nối tới máy 1. **

* **Demo thứ 3 bằng lệnh ssh**

**Ở máy 2, gõ lệnh ssh 192.168.191.160**

****

**Tại máy 1, hiện dòng cảnh báo với message là” Phat hien ket noi SSH!!!”, giao thức tcp, IP nguồn là 192.168.191.155(Máy 1)**

****

1. **Kết luận**

* **Snort cấu hình khá dễ dàng, nhanh, miễn phí, tài liệu hướng dẫn cài và sử dụng trên website www.snort.org khá tường minh và dễ hiểu cho những người mới sử dụng.**
* **Kết quả thực hiện demo cho thấy, Snort làm rất tốt công việc của mình. Sau khi nhập lệnh từ máy 2 thì máy 1 lập tức cảnh báo trên terminal, thể hiện sự nhanh chóng, hiệu quả trong việc phát hiện xâm nhập mạng. Có thể thấy sự nhanh chóng ấy giúp đưa ra những cảnh báo sớm nhất đến quản trị viên cũng như người sử dụng các sự xâm nhập và sau đó đưa ra biện pháp ngăn chặn nhanh nhất để có thể bảo vệ dữ liệu, những thứ quan trọng nhất khỏi những tay hacker.**

**Tài liệu tham khảo**

* **https://www.snort.org/**
* [**https://www.unixmen.com/install-snort-nids-ubuntu-15-04/**](https://www.unixmen.com/install-snort-nids-ubuntu-15-04/)
* [**https://upcloud.com/community/tutorials/install-snort-ubuntu/**](https://upcloud.com/community/tutorials/install-snort-ubuntu/)
* [**https://resources.infosecinstitute.com/topic/snort-rules-workshop-part-one/**](https://resources.infosecinstitute.com/topic/snort-rules-workshop-part-one/)
* **https://www.digitalocean.com/community/tutorials/how-to-install-suricata-on-ubuntu-20-04**
* [**https://www.aldeid.com/wiki/Suricata-vs-snort**](https://www.aldeid.com/wiki/Suricata-vs-snort)
* [**https://www.geeksforgeeks.org/intrusion-detection-system-ids/**](https://www.geeksforgeeks.org/intrusion-detection-system-ids/)