**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG CƠ SỞ TP HCM**

**🕮🕮🕮**

**BÁO CÁO ĐỒ ÁN HỌC PHẦN**

**MÔN HỌC: AN TOÀN MẠNG**

**GIẢNG VIÊN HƯỚNG DẪN: ThS TRẦN THỊ DUNG**

**ĐỀ TÀI: SNORT**

****

**NHÓM 4**

**THÀNH VIÊN MÃ SỐ SINH VIÊN**

**MAI XUÂN Ý N18DCAT105**

**NGUYỄN MẠNH THÌN N18DCAT085**

**TRƯƠNG VĂN NAM N18DCAT051**

**NGUYỄN MINH HẬU N18DCAT019**

**NGUYỄN ĐỨC QUỲNH N18DCAT065**

MỤC LỤC

[**I.** **KIẾN THỨC TỔNG QUAN** 4](#_Toc84280000)

[**1.** **Giới thiệu về IDS/IPS:** 4](#_Toc84280001)

[a) Tổng quan 4](#_Toc84280002)

[b) Phân loại IDS 5](#_Toc84280003)

[2. Giới thiệu về Snort 6](#_Toc84280004)

[**II.** **Cấu hình** 9](#_Toc84280005)

[1. Mô hình Snort cài đặt chung với Web Server(DVWA): 9](#_Toc84280006)

[2. Mô hình Snort cài đặt riêng với Web Server(DVWA): 14](#_Toc84280007)

**BẢNG THUẬT NGỮ**

|  |  |  |
| --- | --- | --- |
| **Thuật Ngữ** | **Tên Chi Tiết** | **Tên Tiếng Việt** |
| **IDS** | Intrusion Detection System | Hệ thống phát hiện xâm nhập |
| **SIEM** | Security information and event management | Hệ thống bảo mật và quản lý sự kiện |
| **IPS** | Intrusion Prevention System | Hệ thống ngăn chặn xâm nhập |
| **HIDS** | Host-based IDS | Hệ thống ngăn chặn xâm nhập trên host |
| **NIDS** | Network-based IDS | Hệ thống ngăn chặn xâm nhập trên toàn mạng |
| **URL** | Uniform Resource Locator | Định vị tài nguyên thống nhất |
| **TCP** | Transmission Control Protocol | Giao thức điều khiển truyền vận |
| **UDP** | User Datagram Protocol | Giao thức dữ liệu người dùng |
| **HTTP** | Hyper Text Transfer Protocol | Giao thức Truyền tải Siêu Văn Bản |
| **FTP** | File Transfer Protocol | Giao thức truyền tải tập tin |
| **PCAP** | Data Files - Packet Capture Data | Thu thập dữ liệu gói |
| **DAQ** | Data Acquisition **And Control** |  |
| **PCRE** |  |  |
| **DMZ** | DMZ zone | Vùng biên giữa mạng nội bộ và vùng Internet. |

# **KIẾN THỨC TỔNG QUAN**

1. **Giới thiệu về IDS/IPS:**

### Tổng quan

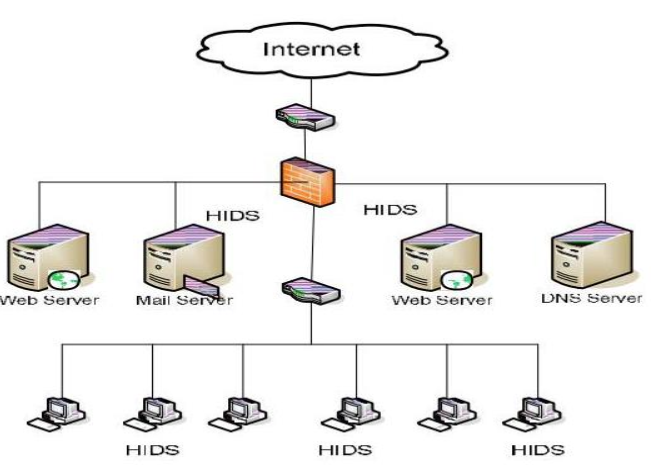
* IDS là một thiết bị hoặc ứng dụng phần mềm giám sát mạng, hệ thống máy tính có nhiệm vụ theo dõi, phát hiện và ***có thể*** ngăn cản sự xâm nhập, cũng như các hành vi khai thác trái phéptài nguyên của hệ thống được bảo vệ mà có thể dẫn đến việc làm tổn hại đến tính bảo mật, tính toàn vẹn và tính sẵn sàng của hệ thống. Bất kỳ hoạt động hoặc vi phạm nào được phát hiện thường báo cáo cho quản trị viên hoặc thu thập tập trung bằng hệ thống SIEM. Một hệ thống SIEM kết hợp các kết quả đầu ra từ nhiều nguồn và sử dụng các kỹ thuật lọc báo động để phân biệt hoạt động ác ý từ các báo động sai lầm.
* IPS có các chức năng của một IDS, ngoài ra bổ sung thêm khả năng ngăn ngừa các hoạt động xâm nhập không mong muốn.Khi một hệ thống IDS có khả năng ngăn chặn các nguy cơ xâm nhập mà nó phát hiện được thì nó được gọi là một IPS.
* Tùy thuộc vào quy mô, tính chất của từng mạng máy tính cụ thể cũng như chính sách an ninh của người quản trị mạng.
  + Trong trường hợp các mạng có quy mô nhỏ, với một máy chủ an ninh, thì giải pháp IPS thường được cân nhắc nhiều hơn do tính chất kết hợp giữa phát hiện, cảnh báo và ngăn chặn của nó.
  + Tuy nhiên với các mạng lớn hơn thì chức năng ngăn chặn thường được giao phó cho một sản phẩm chuyên dụng. Khi đó, hệ thống cảnh báo sẽ chỉ cần theo dõi, phát hiện và gửi các cảnh báo đến một hệ thống ngăn chặn khác. Sự phân chia trách nhiệm này sẽ làm cho việc đảm bảo an ninh cho mạng trở nên linh động và hiệu quả hơn.



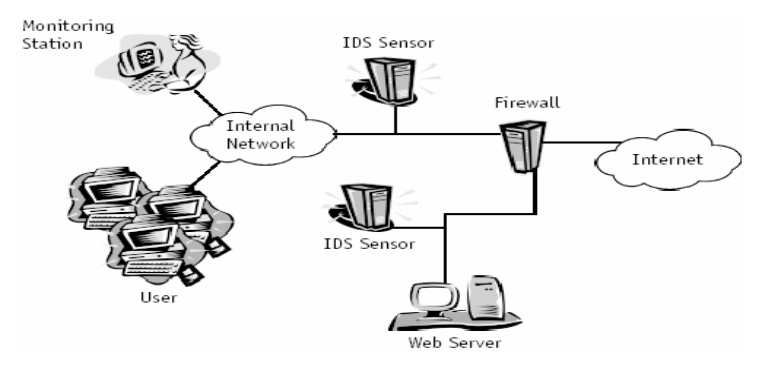
1. Mô tả chức năng của IDS và IPS trong hệ thống.

### Phân loại IDS

* Thông thường phân loại các hệ thống IDS dựa vào đặc điểm của nguồn dữ liệu thu thập được. Trong trường hợp này, các hệ thống IDS được chia thành các loại sau:
  + **Host-based IDS (HIDS)**:
    - Giám sát hoạt động của từng máy tính riêng biệt được cài đặt trên các máy tính(host) HIDS cài đặt trên nhiều kiểu máy chủ khác nhau, trên máy trạm làm việc hoặc máy notebook HIDS cho phép thực hiện một cách linh hoạt trên các đoạn mạng mà NIDS không thực hiện được. Nguồn thông tin chủ yếu của HIDS ngoài lưu lượng đến và đi trên máy chủ còn có hệ thống dữ liệu system log và system audit.
    - Lưu lượng đã gửi đến host được phân tích và chuyển qua host nếu chúng không tiềm ẩn các mã nguy hiểm HIDS cụ thể hơn với các nền ứng dụng và phục vụ mạnh mẽ cho hệ điều hành.
    - Nhiệm vụ chính của HIDS là giám sát sự thay đổi trên hệ thống:
      * Các tiến trình – process.
      * Các entry của registry.
      * Mức độ sử dụng của CPU.
      * Các thông số vượt ngưỡng cho phép trên hệ thông file.
    - Host-based IDS tìm kiếm dấu hiệu của xâm nhập vào một host cục bộ, thường sử dụng các cơ chế kiểm tra và phân tích các thông tin đến và đi , các thông tin được logging, lịch sử audit log. Tìm kiếm các hoạt động bất thường như login, truy nhập file không thích hợp, bước leo thang các đặc quyền không được chấp nhận.
    - HIDS thường được cài đặt trên một máy tính nhất định. Thay vì giám sát hoạt động của một Network segment, HIDS chỉ giám sát các hoạt động trên một máy tính. Nó thường được đặt trên các Host xung yếu của tổ chứcvà các server trong vùng DMZ.



1. Mô hình hệ thống HIDS trong mạng
   * **Network-based IDS (NIDS)**:
     + Giám sát trên toàn bộ mạng. Nguồn thông tin chủ yếu của NIDS là các gói dữ liệu đang lưu thông trên mạng như (cables, wireless) bằng cách sử dụng các card giao tiếp.
     + NIDS xác định các truy cập trái phép bằng việc giám sát các hoạt động mạng được tiến hành trên toàn bộ các phân mạng của hệ thống, NIDS sử dụng bộ dò và bộ cảm biến cài đặt trên toàn mạng. Những bộ dò này theo dõi trên mạng nhằm tìm kiếm những lưu lượng trùng với những mô tả sơ lược được định nghĩa hay là những dấu hiệu.
     + Khi một gói dữ liệu phù hợp với qui tắc phát hiện xâm nhập của hệ thống. Bộ cảm biến gửi tín hiệu cảnh báo đến trung tâm điều khiển và có thể được cấu hình nhằm tìm ra biện pháp ngăn chặn những xâm nhập xa hơn hay đơn giản là phát đi một cảnh báo được tạo ra để thông báo đến nhà quản trị và các file log được lưu vào cơ sở dữ liệu.
     + NIDS thường được lắp đặt tại ngõ vào của mạng (Inline), có thể đứng trước hoặc sau firewall.

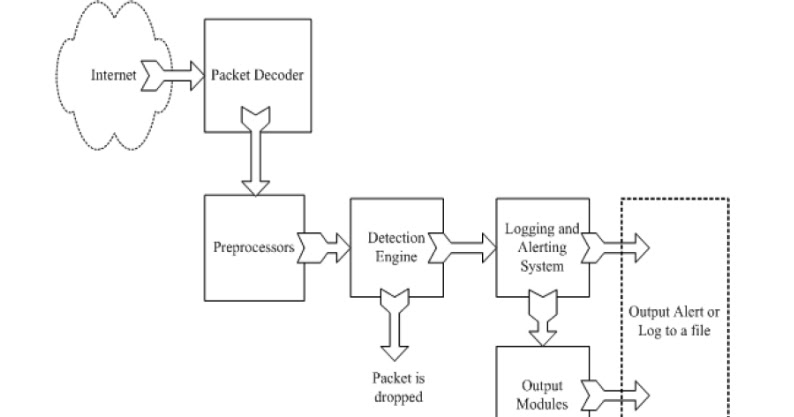


1. Mô hình NIDS trong mạng

## Giới thiệu về Snort

1. **Giới thiệu chung**

* Được viết bởi Martin Roesch vào năm 1998. Hiện tại, Snort được phát triển bởi Sourcefire, nơi mà Roesch đang là người sáng lập và CTO,được sở hữu bởi Cisco từ năm 2013.
* Snort là một kiểu NIDS, thực hiện giám sát các gói tin ra vào hệ thống.
* Là một mã nguồn mở miễn phí với nhiều tính năng trong việc bảo vệ hệ thống bên trong, phát hiện sự tấn công từ bên ngoài vào hệ thống.



1. Mô hình kiến trúc của Snort

* Theo mô hình kiến trúc trên, Snort được chia làm các phần:
  + Module Decoder: Xử lý giải mã các gói tin
  + Module Preprocessors: Tiền xử lý
  + Module Detection Engine: Phát hiện xâm nhập
  + Module Logging and Alerting System: Lưu log và cảnh báo
  + Output Module: Kết xuất thông tin.

Với kiến trúc thiết kế theo kiểu module, người dùng có thể tự tăng cường tính năng cho hệ thống Snort của mình bằng việc cài đặt hay viết thêm mới các module. Cơ sở dữ liệu luật của Snort đã lên tới 2930 luật và được cập nhật thường xuyên bởi một cộng đồng người sử dụng. Snort có thể chạy trên nhiều hệ thống nền như Windows, Linux, OpenBSD, FreeBSD, NetBSD, Solaris, HP-UX, AIX, IRIX, MacOS.

1. **Chi tiết kiến trúc của Snort**

* Module Decoder – Giải mã:

Snort sử dụng thư viện pcap để bắt mọi gói tin trên mạng lưu thông qua hệ thống. Gói tin sau khi được giải mã sẽ đưa vào Module tiền xử lý.

* Module Preprocessors – Tiền xử lý:

Module này rất quan trọng đối với bất kỳ hệ thống nào để có thể chuẩn bị gói dữ liệu đưa vào cho Module phát hiện phân tích.Tiền xử lý có 03 nhiệm vụ chính:

* Kết hợp lại các gói tin: Khi một dữ liệu lớn được gửi đi, thông tin sẽ không đóng gói toàn bộ vào một gói tin mà thực hiện phân mảnh, chia thành nhiều gói tin rồi mới gửi đi. Khi Snort nhận được các gói tin này, nó phải thực hiện kết nối lại để có gói tin ban đầu. Module tiền xử lý giúp Snort có thể hiểu được các phiên làm việc khác nhau.
* Giải mã và chuẩn hóa giao thức (decode/normalize): cCông việc phát hiện xâm nhập dựa trên dấu hiệu nhận dạng nhiều khi thất bại khi kiểm tra các giao thức có dữ liệu có thể được biểu diễn dưới nhiều dạng khác nhau. Ví dụ: một Web server có thể nhận nhiều dạng URL: URL viết dưới dạng hexa/unicode hay URL chấp nhận dấu / hay . Nếu Snort chỉ thực hiện đơn thuần việc so sánh dữ liệu với dấu hiệu nhận dạng sẽ xảy ra tình trạng bỏ sót hành vi xâm nhập. Do vậy, 1 số Module tiền xử lý của Snort phải có nhiệm vụ giải mã và chỉnh sửa, sắp xếp lại các thông tin đầu vào.
* Phát hiện các xâm nhập bất thường (nonrule/anormal):các plugin dạng này thường để xử lý với các xâm nhập không thể hoặc rất khó phát hiện bằng các luật thông thường. Phiển bản hiện tại của Snort có đi kèm 2 plugin giúp phát hiện xâm nhập bất thường đó là portscan và bo (backoffice). Portscan dùng để đưa ra cảnh báo khi kẻ tấn công thực hiện quét cổng để tìm lỗ hổng. Bo dùng để đưa ra cảnh báo khi hệ thống nhiễm trojan backoffice.
* Module Detection Engine – Phát hiện xâm nhập
* Đây là module quan trọng nhất của Snort. Nó chịu trách nhiệm phát hiện các dấu hiệu xâm nhập. Module sử dụng các luật (rule) được định nghĩa từ trước để so sánh với dữ liệu thu thập được, từ đó xác định xem có xâm nhập xảy ra hay không.
* Một vấn đề quan trọng đối với module detection engine là thời gian xử lý gói tin: một IDS thường nhận rất nhiều gói tin và bản thân nó cũng có rất nhiều luật xử lý. Khi lưu lượng mạng quá lớn thì có thể xảy ra việc bỏ sót hoặc không phản hồi đúng lúc. Khả năng xử lý của module phát hiện phụ thuộc vào nhiều yếu tố: số lượng các luật, tốc độ hệ thống, băng thông mạng

* Module detection engine có khả năng tách các phần của gói tin ra và áp dụng luật lên tưng phần của gói tin:
* IP HEADER.
* Header ở tầng transport: TCP, UDP
* Header ở tầng application: DNS, HTTP, FTP,...
* Phần tải (payload) của gói tin.
* Do các luật trong Snort được đánh số thứ tự ưu tiên nên một gói tin khi bị phát hiện bởi nhiều luật khác nhau, cảnh báo được đưa ra theo luật có mức ưu tiên cao nhất.
* Module Logging and Alerting System – Ghi lại log và cảnh báo:

- Tùy thuộc vào module phát hiện (detection engine) có nhận dạng được xâm nhập hay không mà gói tin có thể bị ghi log hay đưa ra cảnh báo. Các file log là các file dữ liệu có thể ghi dưới nhiều định dạng khác nhau như tcpdump, xml, syslog, log file.

# **Cấu hình**

## Mô hình Snort cài đặt chung với Web Server DVWA.

1. Mô hình mạng:

- Máy chủ Ubuntu version 18.04.5 LTX x86\_64

- Snort version 2.9.18.1

- Web server(DVWA) apache2 version 2.4.29

- Máy attacker: máy chính có ip là:

- Phần mềm attack:

1. Các bước cấu hình

* Cài đặt Snort :

1. Thực hiện update và cài đặt các gói hỗ trợ:Pcap,PCRE, libdnet, DAQ,lib:

apt install -y build-essential

apt install -y libpcap-dev libpcre3-dev libdumbnet-dev

apt install -y bison flex

apt install -y zlib1g-dev liblzma-dev openssl libssl-dev libnghttp2-dev

1. Tạo thư mục chứa sources code cài đặt và cài đặt:

mkdir -p ~/snort\_src

cd ~/snort\_src

**Tải, giải nén, cài đặt gói DAQ:**

wget <https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz>

tar -xzvf daq-2.0.7.tar.gz

cd daq-2.0.7

./configure

make

make install

**Tải gói Snort:**

wget <https://www.snort.org/downloads/snort/snort-2.9.18.1.tar.gz>

tar -xzvf snort-2.9.18.1.tar.gz

cd snort-2.9.18.1

./configure --enable-sourcefire

make

make install

Cập nhật thư viện:

ldconfig

**Cấu hình snort NIDS mode :**

# Tạo các thư mục Snort

mkdir /etc/snort

mkdir /etc/snort/rules

mkdir /etc/snort/rules/iplists

mkdir /etc/snort/preproc\_rules

mkdir /usr/local/lib/snort\_dynamicrules

mkdir /etc/snort/so\_rules

# tạo file để lưu trữ rule và danh sách IP

touch /etc/snort/rules/iplists/black\_list.rules

touch /etc/snort/rules/iplists/white\_list.rules

touch /etc/snort/rules/local.rules

touch /etc/snort/sid-msg.map

# Tạo thư mục lưu trữ log

mkdir /var/log/snort

mkdir /var/log/snort/archived\_logs

# Phân quyền

chmod -R 5775 /etc/snort

chmod -R 5775 /var/log/snort

chmod -R 5775 /var/log/snort/archived\_logs

chmod -R 5775 /etc/snort/so\_rules

chmod -R 5775 /usr/local/lib/snort\_dynamicrules

# Chuyển quyền

chown -R snort:snort /etc/snort

chown -R snort:snort /var/log/snort

chown -R snort:snort /usr/local/lib/snort\_dynamicrules

**Sử dụng cấu hình có sẵn coppy vào thư mục /etc/snort**

cd ~/snort\_src/snort-2.9.18.1/etc/

cp \*.conf\* /etc/snort

cp \*.map /etc/snort

cp \*.dtd /etc/snort

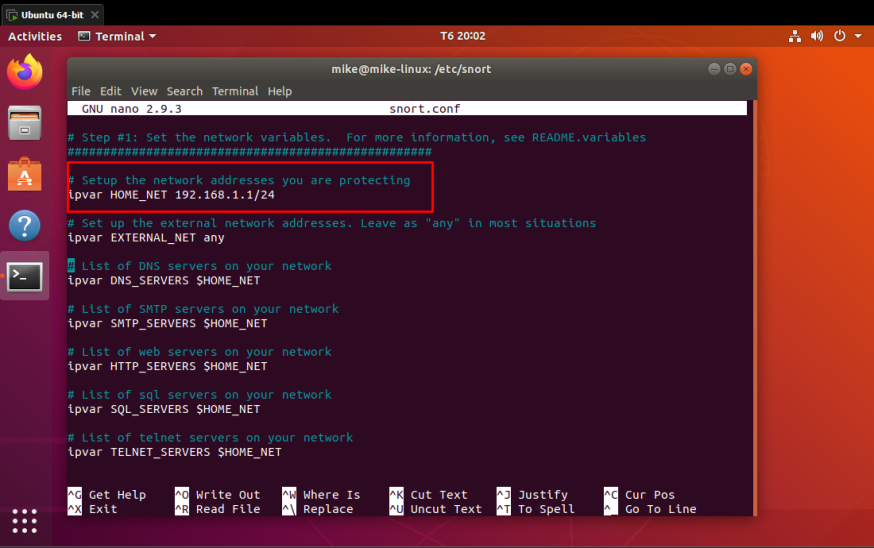
cd ~/snort\_src/snort-2.9.18.1/src/dynamic-preprocessors/build/usr/local/lib/snort\_dynamicpreprocessor/

cp \* /usr/local/lib/snort\_dynamicpreprocessor

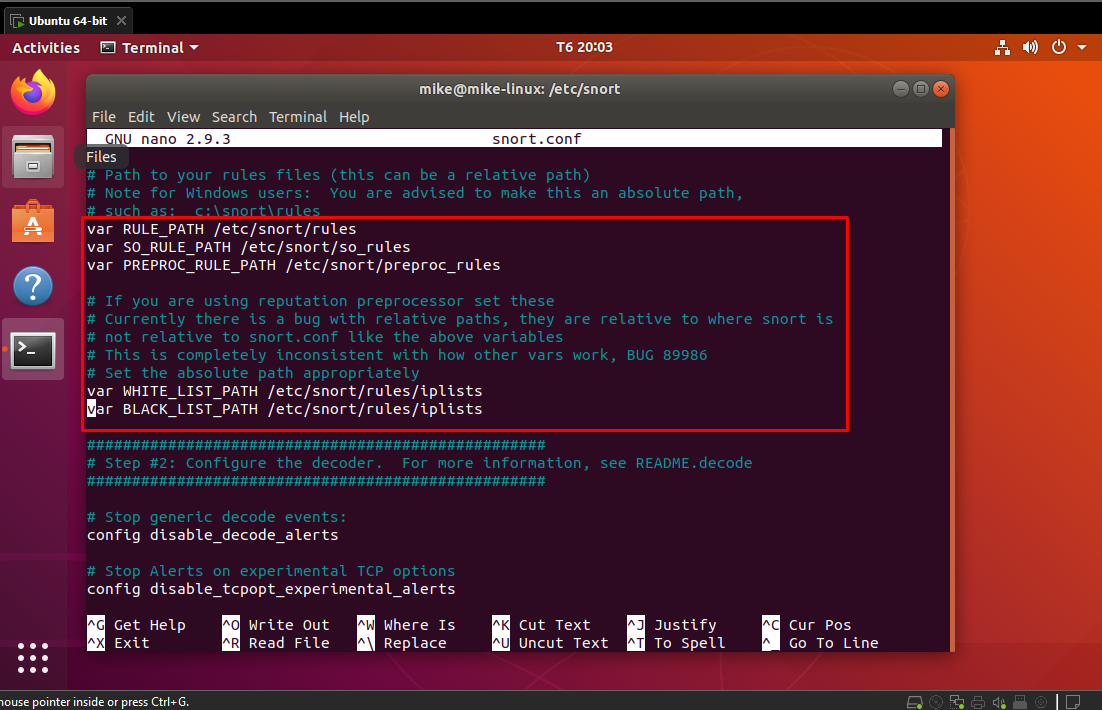
**Chỉnh sửa các cấu hình cơ bản trong snort.conf**

sudo nano /etc/snort/snort.conf

Chỉnh sửa home\_net:

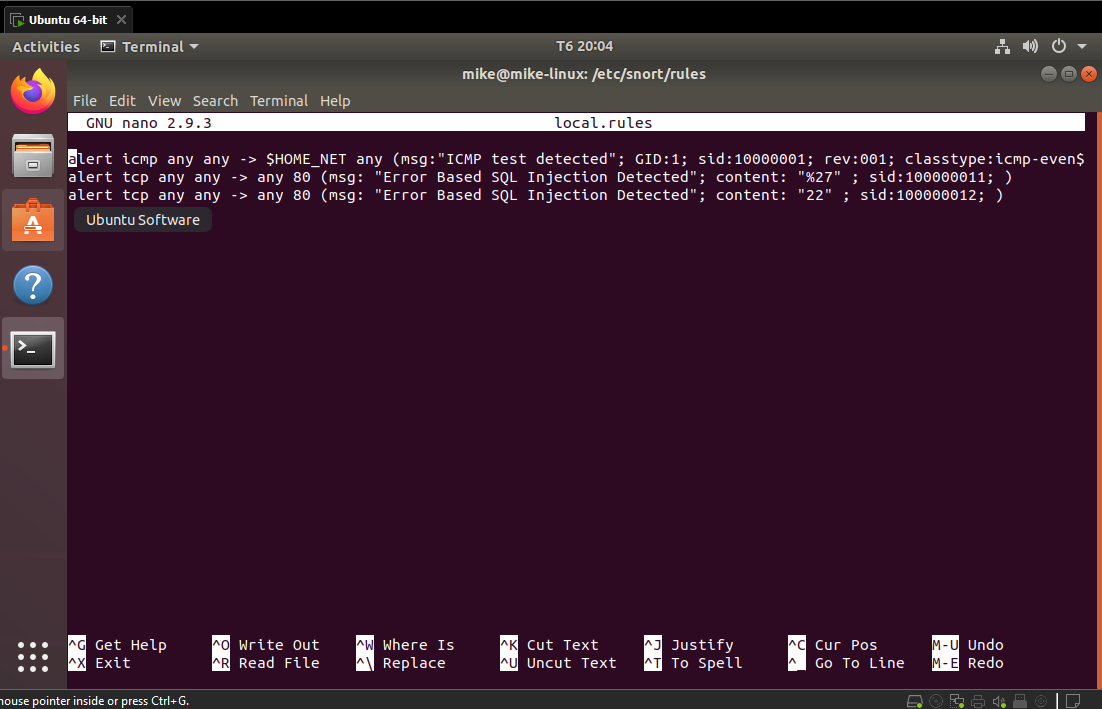


Chỉnh sửa đường dẫn các rule:

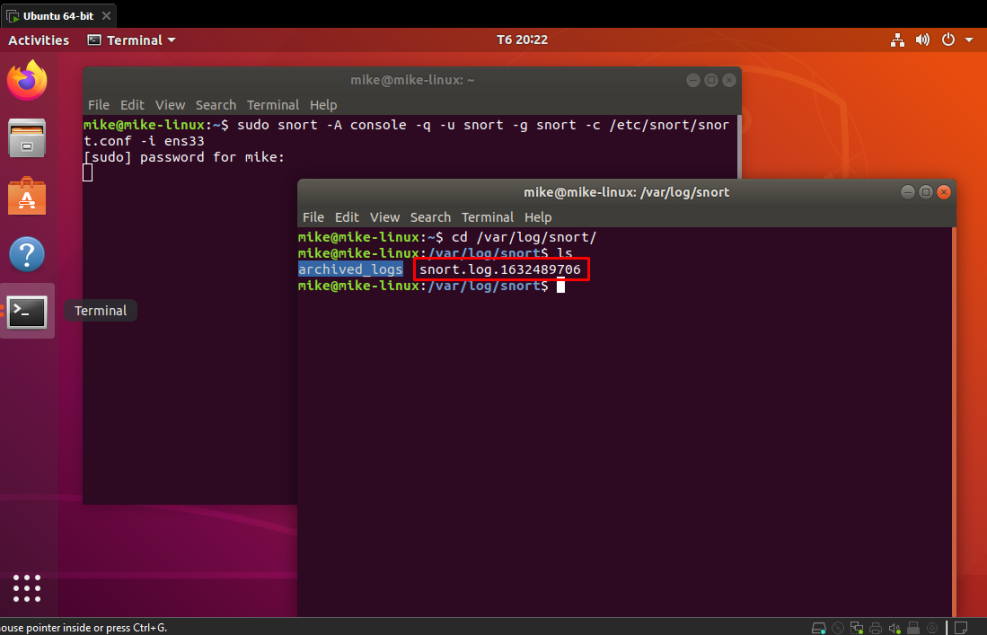


Thêm đường dẫn chứa các rules mới.

Cấu hình rule thông báo message khi máy khác ping tới:

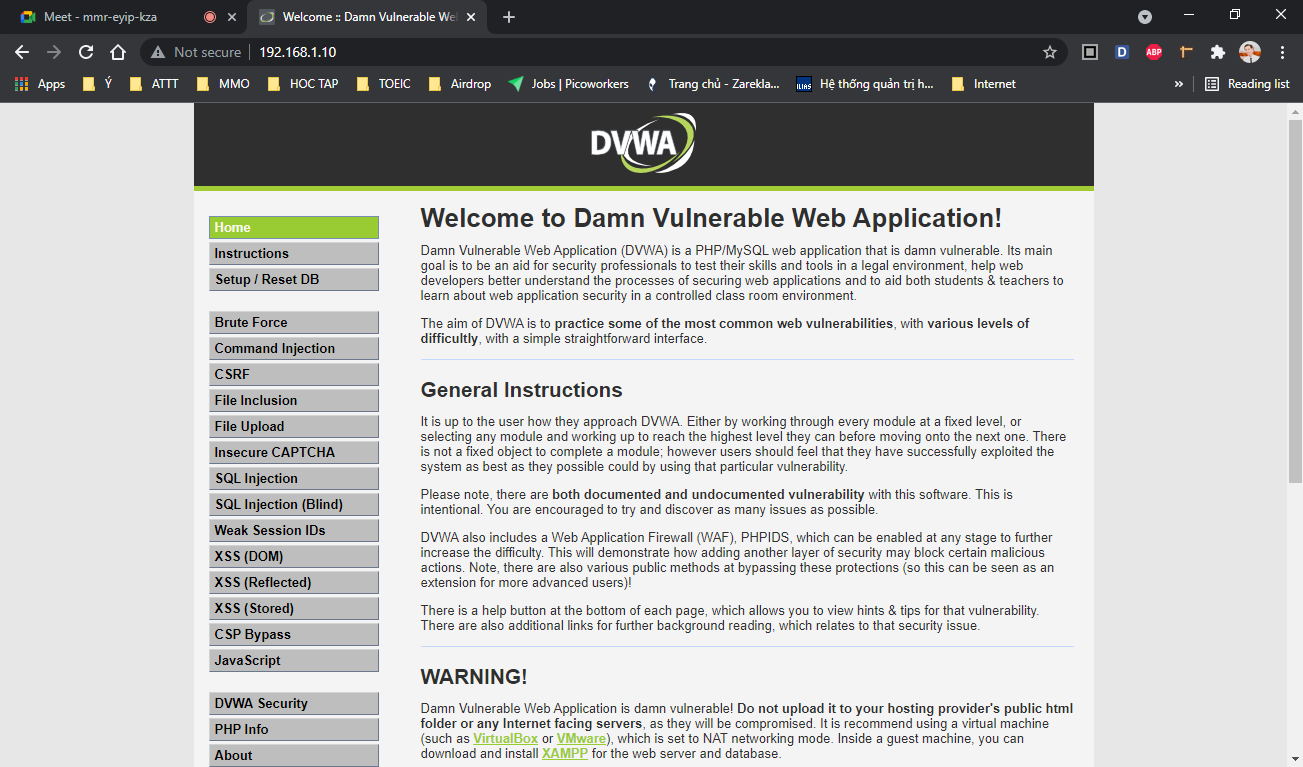


Thực hiện ping từ một máy bất kỳ trong mạng tới máy snort:



* Cài đặt webserver: Apache2

Sử dụng template của DVWA tại https://dvwa.co.uk/



* Cài đặt mysql, php hỗ trợ cho DVWA.

1. Demo
2. Nhận xét

## Mô hình Snort cài đặt riêng với Web Server DVWA.

1. Mô hình mạng:
2. Các bước cấu hình
3. Demo
4. Nhận xét