

**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**  
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA AN TOÀN THÔNG TIN**

-----



**MÔN HỌC: THỰC TẬP CƠ SỞ**  
**BÁO CÁO BÀI THỰC HÀNH SỐ 6**

**Giảng viên hướng dẫn : PGS.TS Hoàng Xuân Dậu**  
**Sinh viên thực hiện : Nguyễn Nhật Minh**  
**Mã sinh viên : B21DCAT132**

**Hà Nội, tháng 2 năm 2024**

## **Môn học: INT13147 - Thực tập cơ sở**

### **Bài thực hành số 6 - Cài đặt cấu hình HIDS/NIDS**

#### **1. Mục đích**

- Luyện tập việc cài đặt và vận hành các hệ thống phát hiện xâm nhập cho host (HIDS) và cho mạng (NIDS).
- Luyện tập việc tạo và chỉnh sửa các luật phát hiện tấn công, xâm nhập cho các hệ thống phát hiện xâm nhập thông dụng.

#### **2. Nội dung thực hành**

##### *2.1 Tìm hiểu lý thuyết*

##### **Hệ thống phát hiện xâm nhập là gì?**

Hệ thống phát hiện xâm nhập – IDS (Intrusion Detection Systems) là phần mềm hoặc công cụ bảo mật hệ thống và cảnh báo lỗi khi có các hành vi đáng ngờ xâm nhập vào hệ thống. Mục đích chính của IDS là ngăn ngừa và phát hiện những hành động phá hoại tính bảo mật của hệ thống hoặc những hành vi như dò tìm, quét các cổng

Một hệ thống IDS cần thỏa mãn: tính chính xác, hiệu năng, tính trọn vẹn, chịu lỗi, khả năng mở rộng

Có 2 loại IDS: Network based IDS và Host based IDS

**NIDS:** Hệ thống IDS dựa trên mạng sẽ kiểm tra các giao tiếp trên mạng với thời gian thực (real-time). Nó kiểm tra các giao tiếp, quét header của các gói tin, và có thể kiểm tra nội dung của các gói để phát hiện ra các đoạn mã nguy hiểm hay các dạng tấn công khác nhau. Một Network-Based IDS hoạt động tin cậy trong việc kiểm tra, phát hiện các dạng tấn công trên mạng, ví dụ như dựa vào băng thông (bandwidth-based) của tấn công Denied of Service (DoS).

**HIDS:** Bằng cách cài đặt một phần mềm trên máy chủ, IDS dựa trên máy chủ quan sát tất cả những hoạt động về hệ thống và các file log, lưu lượng mạng thu thập. Hệ thống dựa trên máy chủ cũng theo dõi OS, những cuộc gọi hệ thống, lịch sử và những thông điệp báo lỗi trên hệ thống máy chủ. HIDS thường được cài đặt trên một máy tính nhất định thay vì giám sát hoạt động của một network, HIDS chỉ giám sát các hoạt động trên một máy tính. HIDS thường được đặt trên các host quan trọng và các server trong vùng DMS. Nhiệm vụ của HIDS là theo dõi các thay đổi trên hệ thống

##### **Những loại tấn công thường gặp và IDS tương ứng**

**Tấn công DoS:** NIDS có thể phát hiện được các cuộc tấn công dạng gói tin

**Quét và thăm dò:** NIDS có thể phát hiện các hành động nguy hiểm trước khi chúng xảy ra. HIDS cũng có tác dụng đối với kiểm tấn công này

**Password attack:** một NIDS có thể phát hiện và ngăn chặn cố gắng đoán mật khẩu, nhưng nó không hiệu quả trong việc phát hiện truy cập trái phép file bị mã hóa. Trong khi đó HIDS lại thể hiện hiệu quả trong việc phát hiện đoán mật khẩu cũng như truy cập trái phép

**Privilege-grabbing:** cả NIDS và HIDS đều có thể xác định được việc thay đổi đặc quyền trái phép

**Hostile code insertion:** Không có loại IDS nào chống việc phá hoại từ virus hay trojan. Cách tốt nhất là cài phần mềm diệt virus

Cyber vandalism: sử dụng HIDS trong trường hợp này là hoàn toàn phù hợp. Với NIDS có thể sử dụng dấu hiệu tấn công được định nghĩa trước để phát hiện chính xác việc truy cập trái phép vào hệ điều hành

Security infrastructure attack: HIDS có thể bắt giữ các cuộc đăng nhập mà thực hiện những hành động như trên

### **Về phần mềm snort**

Snort là phần mềm IDS được phát triển bởi Martin Roesch dưới dạng mã nguồn mở. Snort ban đầu được xây dựng trên nền Unix nhưng sau đó phát triển sang các nền tảng khác. Snort được đánh giá rất cao về khả năng phát hiện xâm nhập. Tuy snort miễn phí nhưng nó lại có rất nhiều tính năng tuyệt vời. Với kiến trúc kiểu module, người dùng có thể tự tăng cường tính năng cho hệ thống Snort của mình. Snort có thể chạy trên nhiều hệ thống như Windows, Linux, OpenBSD, FreeBSD, Solaris ...

Bên cạnh việc có thể hoạt động như một ứng dụng bắt gói tin thông thường, Snort còn được cấu hình để chạy như một NIDS.

Snort bao gồm nhiều thành phần, mỗi phần có một chức năng riêng biệt:

Module giải mã gói tin

Module tiền xử lý

Module phát hiện

Module log và cảnh báo

Module kết xuất thông tin

Về bộ luật của snort có cấu trúc luật dạng: rule header | rule option

Phần Header: chứa thông tin về hành động mà luật đó sẽ thực hiện khi phát hiện ra có xâm nhập nằm trong gói tin và nó cũng chứa tiêu chuẩn để áp dụng luật với gói tin đó.

Phần Option: chứa thông điệp cảnh báo và các thông tin về các phần của gói tin dùng để tạo nên cảnh báo. Phần Option chứa các tiêu chuẩn phụ thêm để đối sánh với gói tin.

### *2.2 Chuẩn bị môi trường*

- 01 máy tính (máy thật hoặc máy ảo) chạy Linux với RAM tối thiểu 2GB, 10GB đĩa cứng có kết nối mạng (LAN hoặc Internet).
- 01 máy tính (máy thật hoặc máy ảo) chạy Kali Linux (bản 2021 trở lên)
- Bộ phần mềm Snort tải tại <https://www.snort.org/downloads>

### *2.3 Các bước thực hiện*

- Bước 1: Chuẩn bị các máy tính như mô tả trong mục 2.2. Máy Kali Linux được đổi tên thành <Mã SV-Tên SV>-Kali và máy cài Snort thành <Mã SV-Tên SV>-Snort. Các máy có địa chỉ IP và kết nối mạng LAN.
- Bước 2: Tải, cài đặt Snort và chạy thử Snort. Kiểm tra log của Snort để đảm bảo Snort hoạt động bình thường.
- Bước 3: Tạo các luật Snort để phát hiện 3 dạng rà quét, tấn công hệ thống:
  - + Phát hiện các gói tin ping từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiện thị thông điệp khi phát hiện: “<Mã SV-Tên SV>-Snort phát hiện có các gói Ping gửi đến.”

Phát hiện các gói tin rà quét từ bất kỳ một máy nào gửi đến máy chạy Snort trên cổng

80. Hiện thị thông điệp khi phát hiện: “<Mã SV-Tên SV>-Snort phát hiện có các gói tin rà quét trên cổng 80.”

- + Phát hiện tấn công TCP SYN Flood từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiện thị thông điệp khi phát hiện: “<Mã SV-Tên SV>-Snort phát hiện đang bị tấn công TCP SYN Flood.”
- Bước 4: thực thi tấn công và phát hiện sử dụng Snort
  - + Từ máy Kali, sử dụng lệnh ping để ping máy Snort. Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.

Từ máy Kali, sử dụng công cụ nmap để rà quét máy Snort (dùng lệnh: nmap -sV -p80 -A <địa chỉ IP máy Snort>). Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.

- + Từ máy Kali, sử dụng công cụ hping3 để tấn công TCP SYN Flood máy Snort (dùng lệnh: hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source <địa chỉ IP máy Snort>). Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.

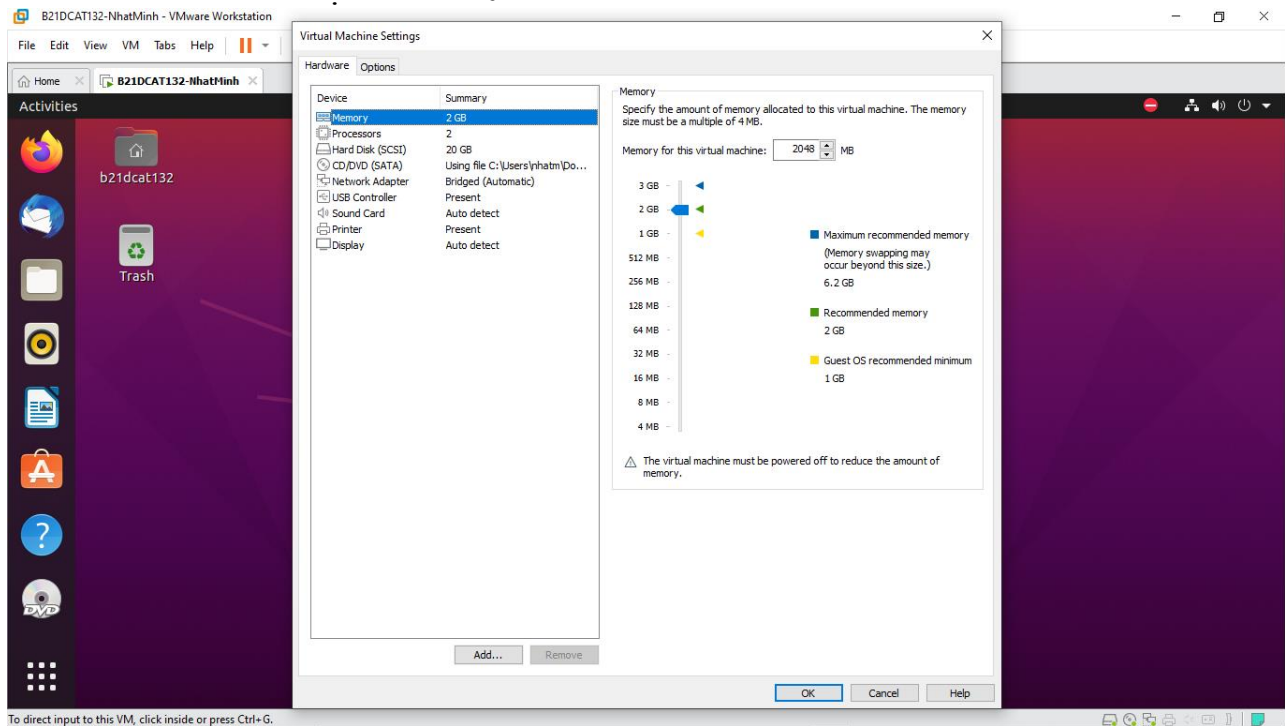
#### 2.4 Kết quả cần đạt

- Hệ thống phát hiện xâm nhập Snort hoạt động ổn định.
- Các luật mới được tạo và lưu vào trong file luật của Snort.
- Snort phát hiện thành công các rà quét tấn công kẻ trên (hiển thị trên giao diện terminal hoặc log của Snort).

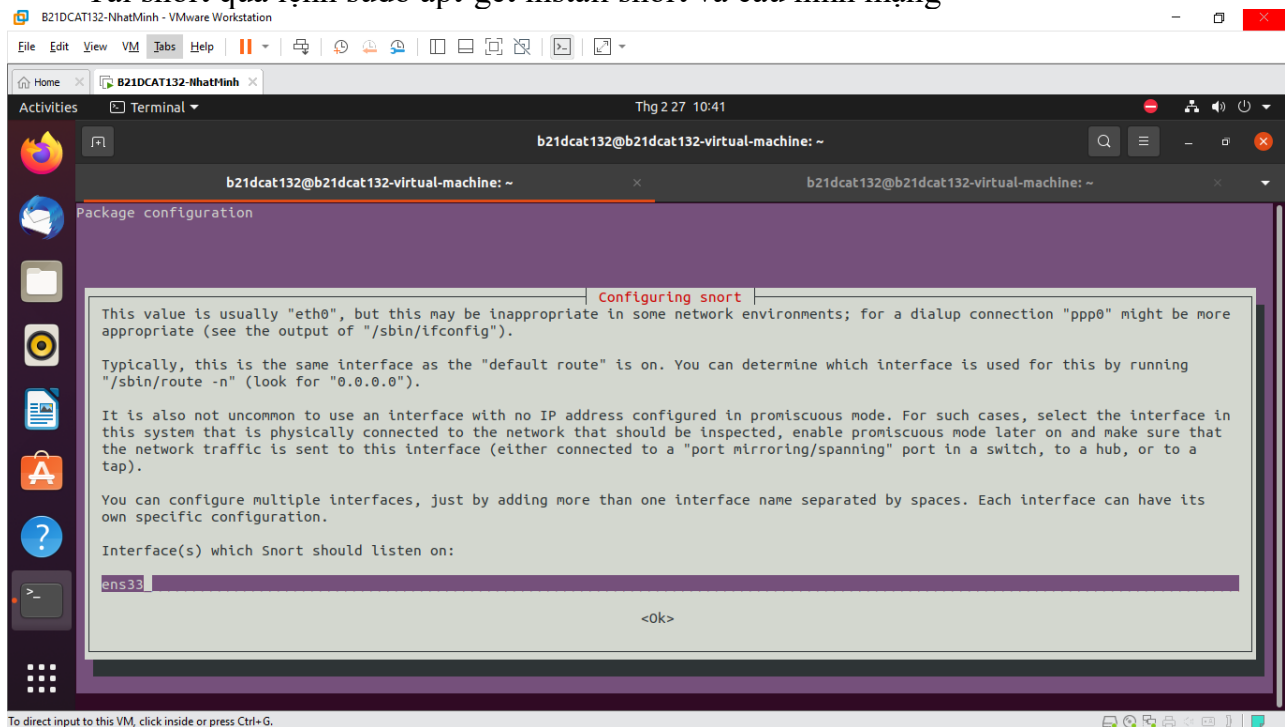
### 3. Thực hành

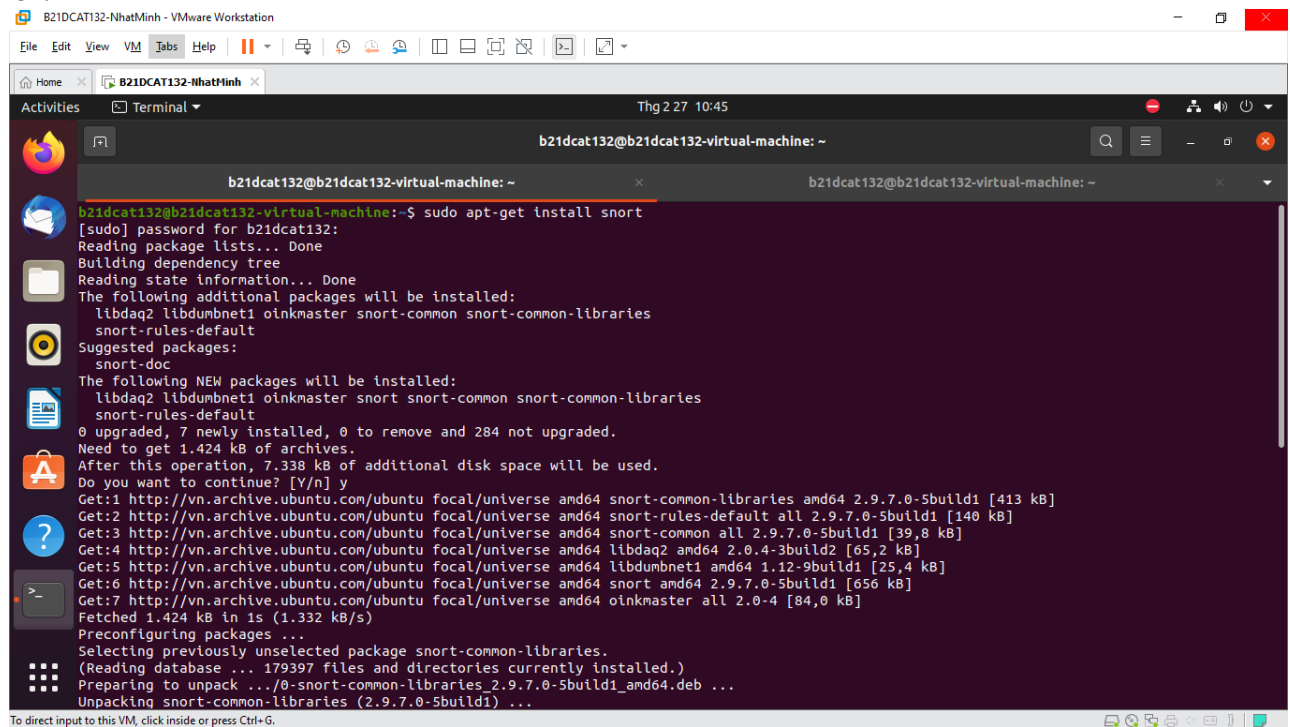
## Nguyễn Nhật Minh – B21DCAT132

### - Cấu hình và cài đặt ubuntu 20



### - Tải snort qua lệnh sudo apt-get install snort và cấu hình mạng

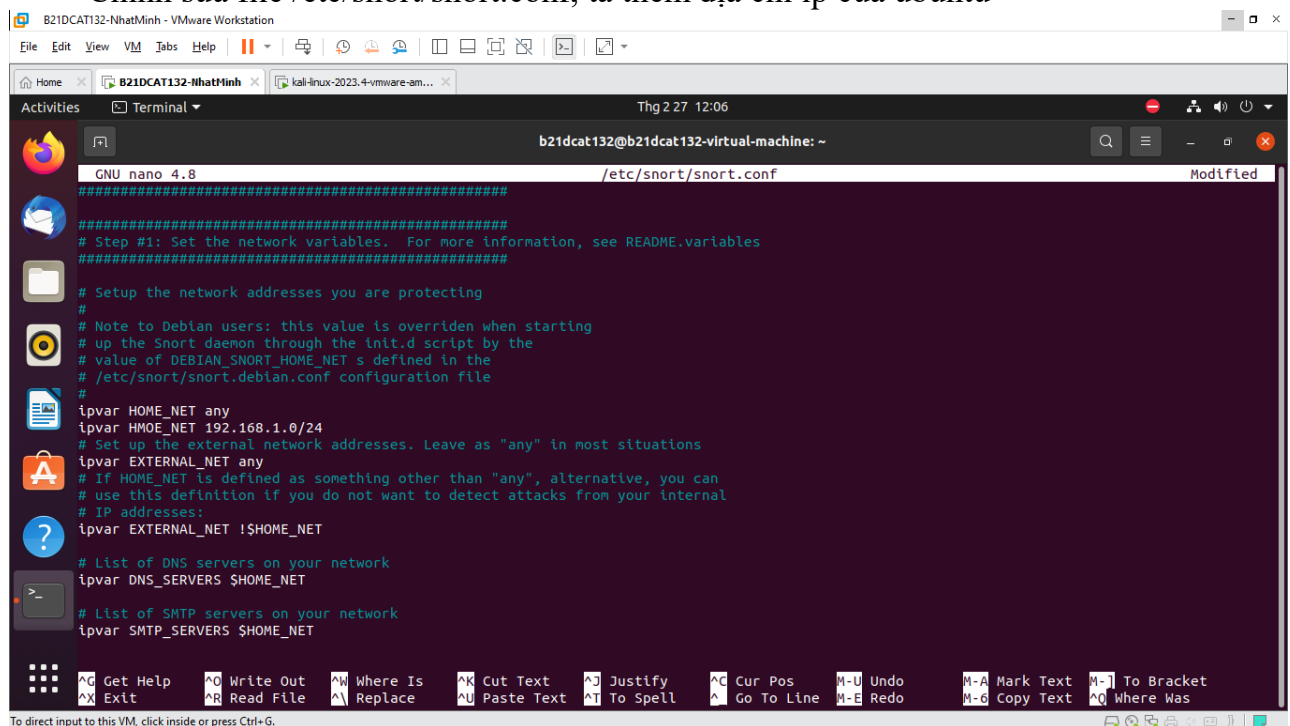




```

b21dcat132@b21dcat132-virtual-machine: ~
b21dcat132@b21dcat132-virtual-machine: ~
b21dcat132@b21dcat132-virtual-machine:~$ sudo apt-get install snort
[sudo] password for b21dcat132:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort-common snort-common-libraries
  snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort snort-common snort-common-libraries
  snort-rules-default
0 upgraded, 7 newly installed, 0 to remove and 284 not upgraded.
Need to get 1.424 kB of archives.
After this operation, 7.338 kB 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 snort-common-libraries amd64 2.9.7.0-5build1 [413 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu focal/universe amd64 snort-rules-default all 2.9.7.0-5build1 [140 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu focal/universe amd64 snort-common all 2.9.7.0-5build1 [39,8 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu focal/universe amd64 libdaq2 amd64 2.0.4-3build2 [65,2 kB]
Get:5 http://vn.archive.ubuntu.com/ubuntu focal/universe amd64 libdumbnet1 amd64 1.12-9build1 [25,4 kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu focal/universe amd64 snort amd64 2.9.7.0-5build1 [656 kB]
Get:7 http://vn.archive.ubuntu.com/ubuntu focal/universe amd64 oinkmaster all 2.0-4 [84,0 kB]
Fetched 1.424 kB in 1s (1.332 kB/s)
Preconfiguring packages ...
Selecting previously unselected package snort-common-libraries.
(Reading database ... 179397 files and directories currently installed.)
Preparing to unpack .../0-snort-common-libraries_2.9.7.0-5build1_amd64.deb ...
Unpacking snort-common-libraries (2.9.7.0-5build1) ...
  
```

- Chỉnh sửa file `/etc/snort/snort.conf`, ta thêm địa chỉ ip của ubuntu



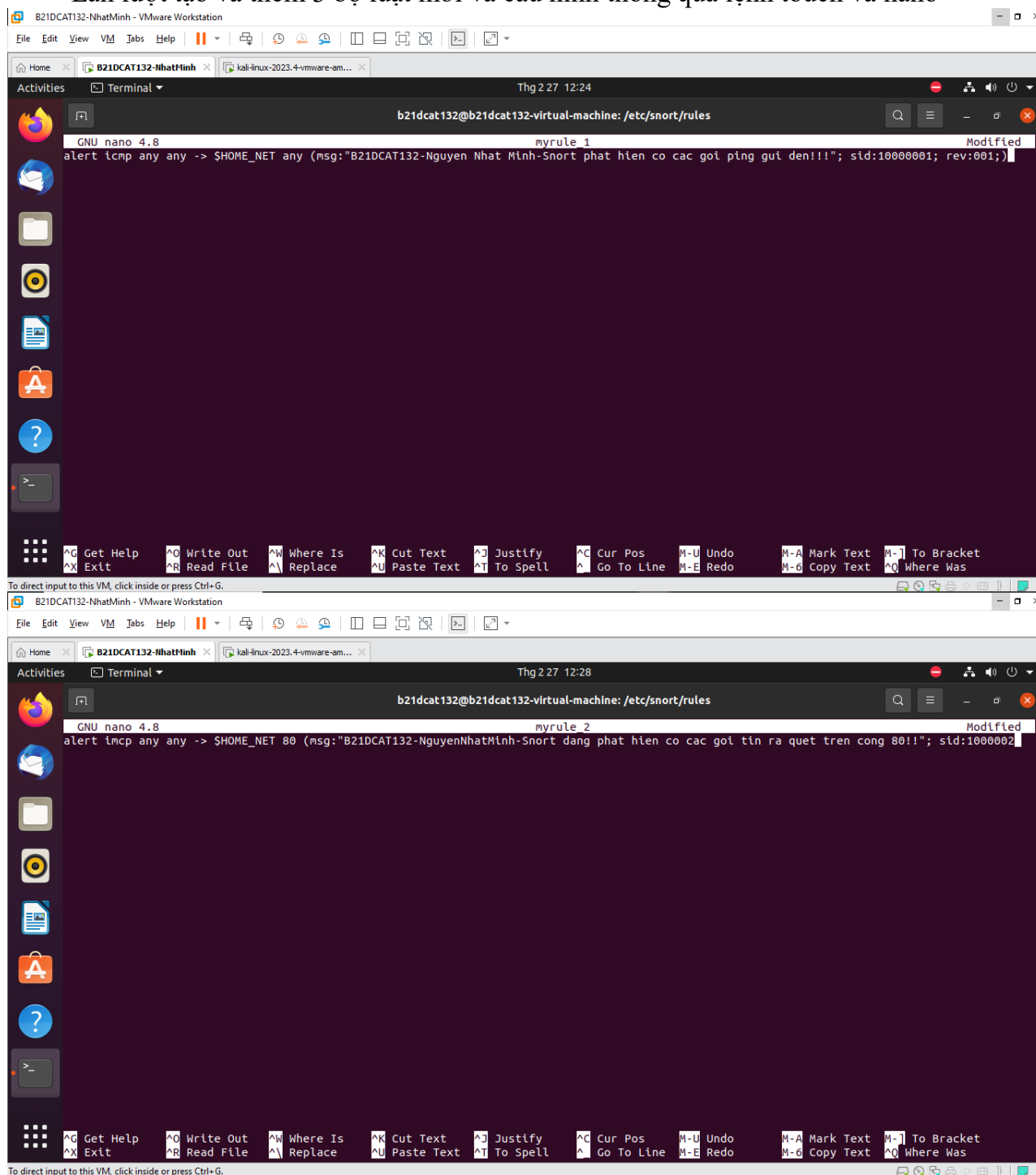
```

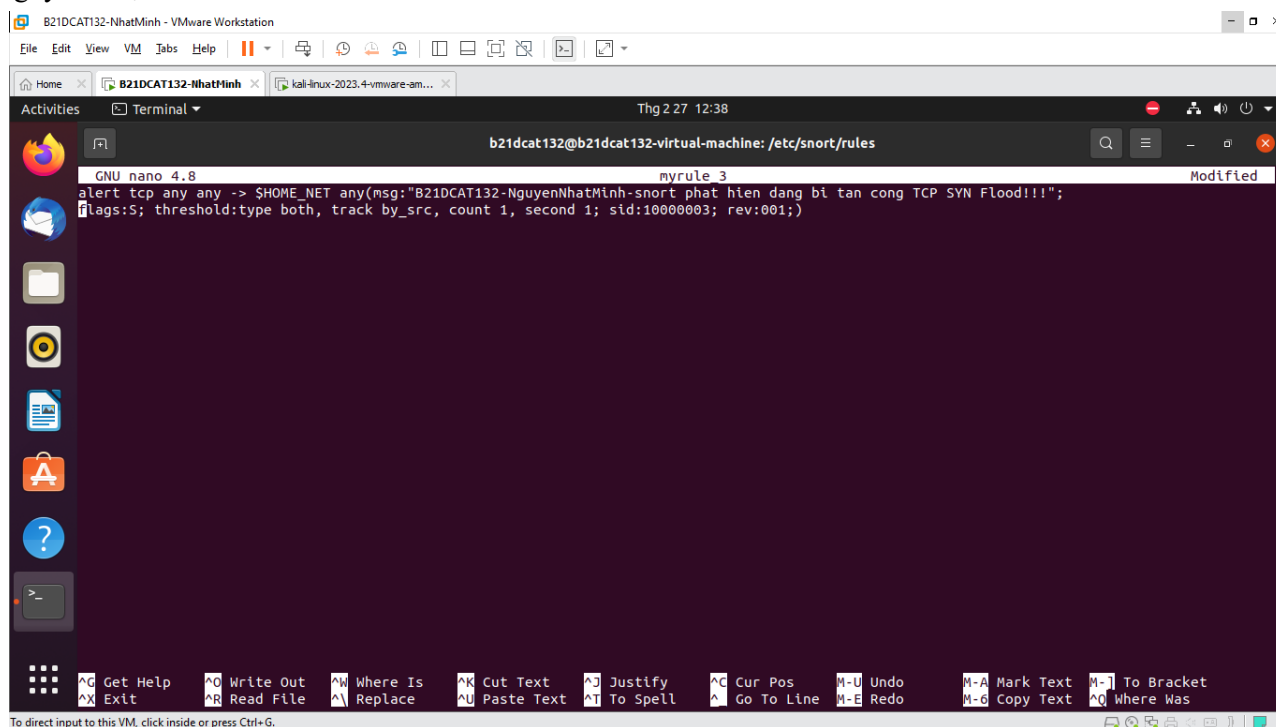
GNU nano 4.8 /etc/snort/snort.conf Modified
#####
#####
##### Step #1: Set the network variables. For more information, see README.variables
#####
#####
# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overridden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET any
ipvar HMOE_NET 192.168.1.0/24
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET
  
```

- Lần lượt tạo và thêm 3 bộ luật mới và cấu hình thông qua lệnh touch và nano



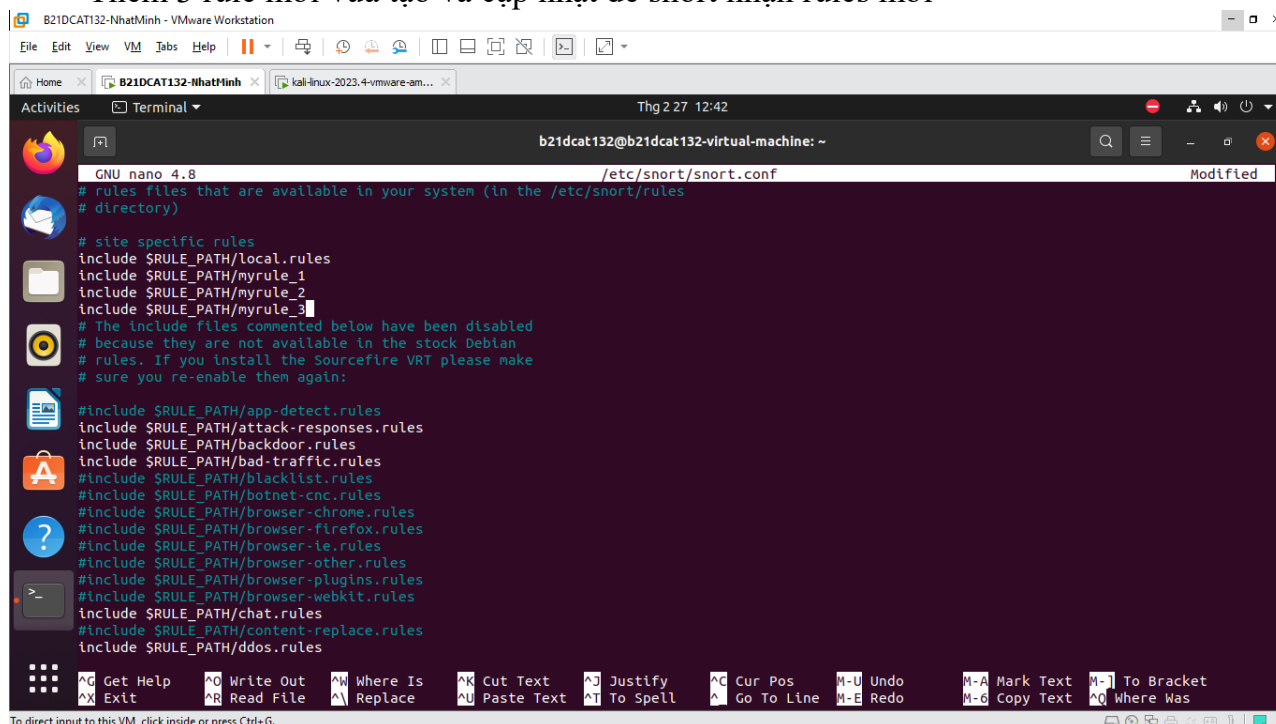


The screenshot shows a VMware Workstation window titled "B21DCAT132-NhatMinh - VMware Workstation". Inside, a terminal window is open with the prompt "b21dcat132@b21dcat132-virtual-machine: /etc/snort/rules". The terminal is running the GNU nano 4.8 editor, editing a file named "myrule\_3". The content of the file is a snort rule: 

```
alert tcp any any -> $HOME_NET any(msg:"B21DCAT132-NguyenNhatMinh-snort phat hien dang bi tan cong TCP SYN Flood!!!"; flags:S; threshold:type both, track by_src, count 1, second 1; sid:10000003; rev:001;)
```

 The terminal window has a status bar at the bottom with various keyboard shortcuts like "Get Help", "Write Out", "Where Is", etc.

## - Thêm 3 rule mới vừa tạo và cập nhật để snort nhận rules mới



The screenshot shows a VMware Workstation window titled "B21DCAT132-NhatMinh - VMware Workstation". Inside, a terminal window is open with the prompt "b21dcat132@b21dcat132-virtual-machine: ~". The terminal is running the GNU nano 4.8 editor, editing a file named "/etc/snort/snort.conf". The content of the file is a configuration for snort, including a list of rules to include: 

```
# rules files that are available in your system (in the /etc/snort/rules directory)

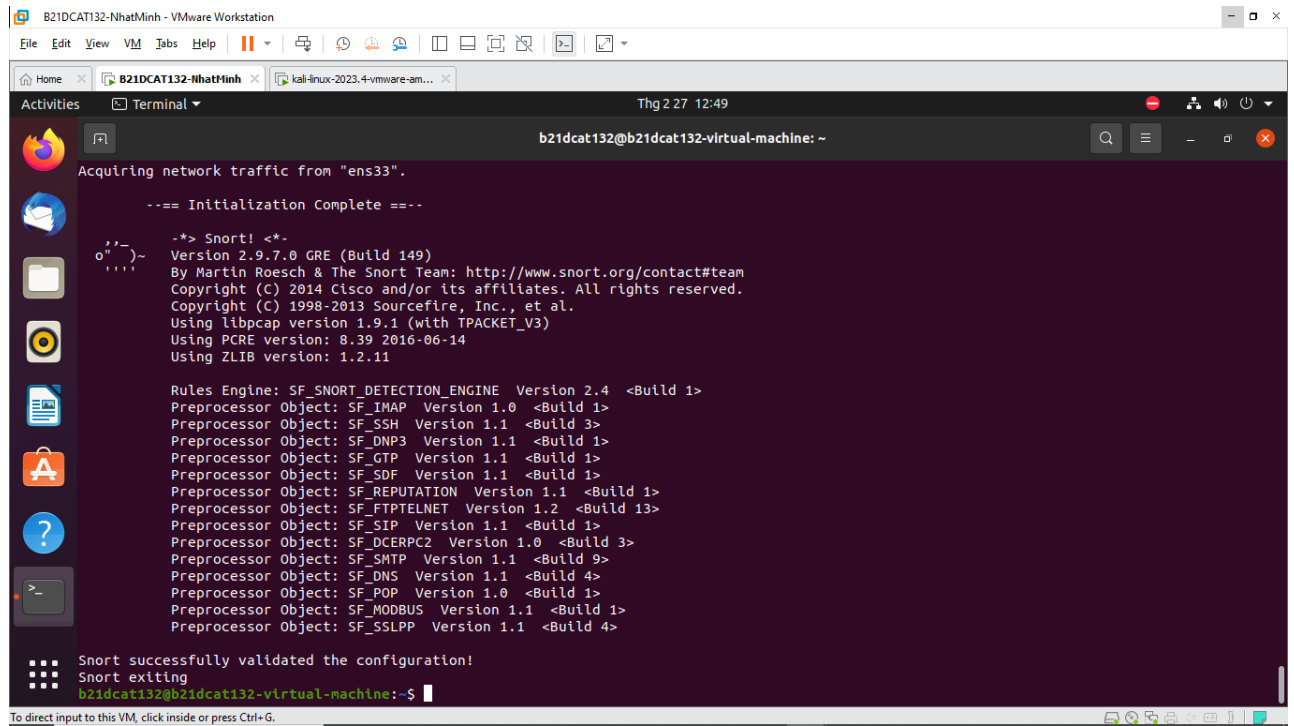
# site specific rules
include $RULE_PATH/local.rules
include $RULE_PATH/myrule_1
include $RULE_PATH/myrule_2
include $RULE_PATH/myrule_3

# The include files commented below have been disabled
# because they are not available in the stock Debian
# rules. If you install the Sourcefire VRT please make
# sure you re-enable them again:

#include $RULE_PATH/app-detect.rules
#include $RULE_PATH/attack-responses.rules
#include $RULE_PATH/backdoor.rules
#include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
include $RULE_PATH/chat.rules
#include $RULE_PATH/content-replace.rules
include $RULE_PATH/ddos.rules
```

 The terminal window has a status bar at the bottom with various keyboard shortcuts like "Get Help", "Write Out", "Where Is", etc.

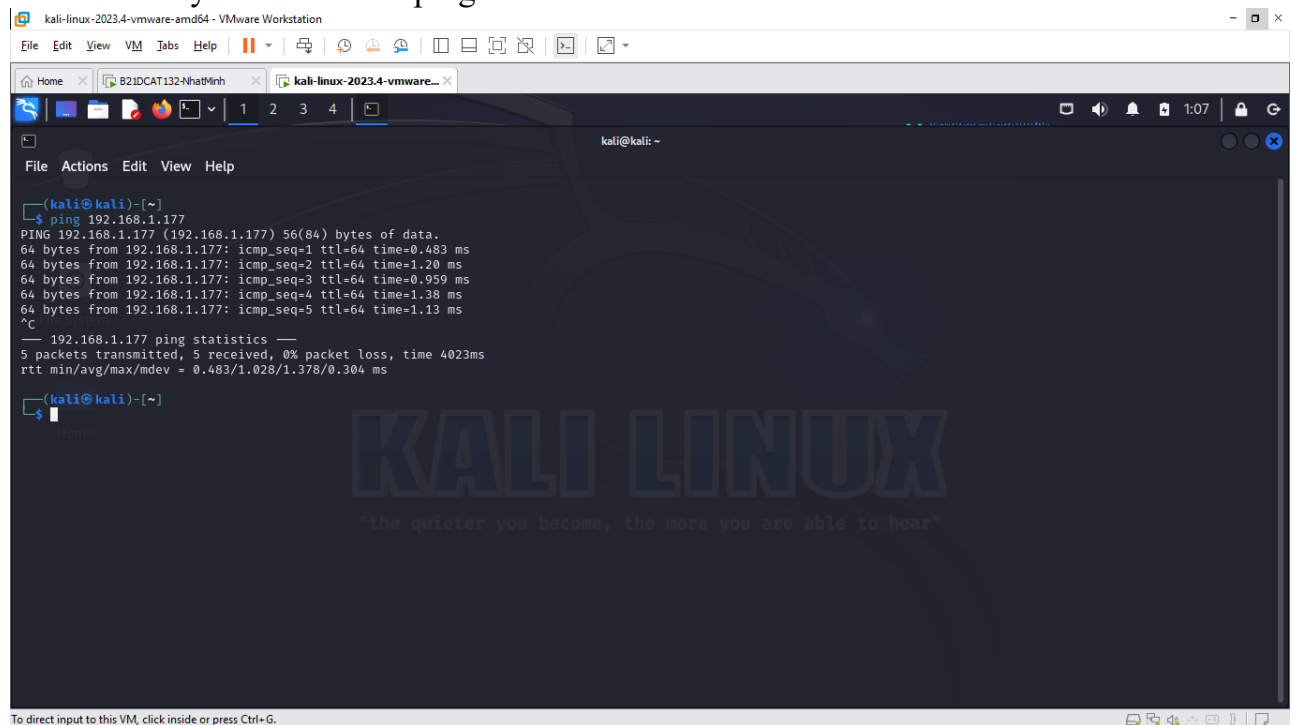




The screenshot shows a terminal window titled "B21DCAT132-NhatMinh - VMware Workstation". The terminal output displays the Snort initialization process. It starts with "Acquiring network traffic from 'ens33'." followed by "--== Initialization Complete ==--". Then, it shows the Snort version (2.9.7.0 GRE (Build 149)) and copyright information. A list of preprocessors and their versions is shown, including SF\_IMAP, SF\_SSH, SF\_DNP3, SF\_GTP, SF\_SDF, SF\_REPUTATION, SF\_FTPTELNET, SF\_SIP, SF\_DCERPC2, SF\_SMTP, SF\_DNS, SF\_POP, SF\_MODBUS, and SF\_SSLPP. The output concludes with "Snort successfully validated the configuration!" and "Snort exiting".

```
b21dcat132@b21dcat132-virtual-machine: ~  
Acquiring network traffic from "ens33".  
  
--== Initialization Complete ==--  
  
--*-- Snort! <*-  
o''-- Version 2.9.7.0 GRE (Build 149)  
.... By Martin Roesch & The Snort Team: http://www.snort.org/contact#team  
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.  
Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
Using libpcap version 1.9.1 (with TPACKET_V3)  
Using PCRE version: 8.39 2016-06-14  
Using ZLIB version: 1.2.11  
  
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>  
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>  
Preprocessor Object: SF_SSH Version 1.1 <Build 3>  
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>  
Preprocessor Object: SF_GTP Version 1.1 <Build 1>  
Preprocessor Object: SF_SDF Version 1.1 <Build 1>  
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>  
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>  
Preprocessor Object: SF_SIP Version 1.1 <Build 1>  
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>  
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>  
Preprocessor Object: SF_DNS Version 1.1 <Build 4>  
Preprocessor Object: SF_POP Version 1.0 <Build 1>  
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>  
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>  
  
Snort successfully validated the configuration!  
Snort exiting  
b21dcat132@b21dcat132-virtual-machine:~$
```

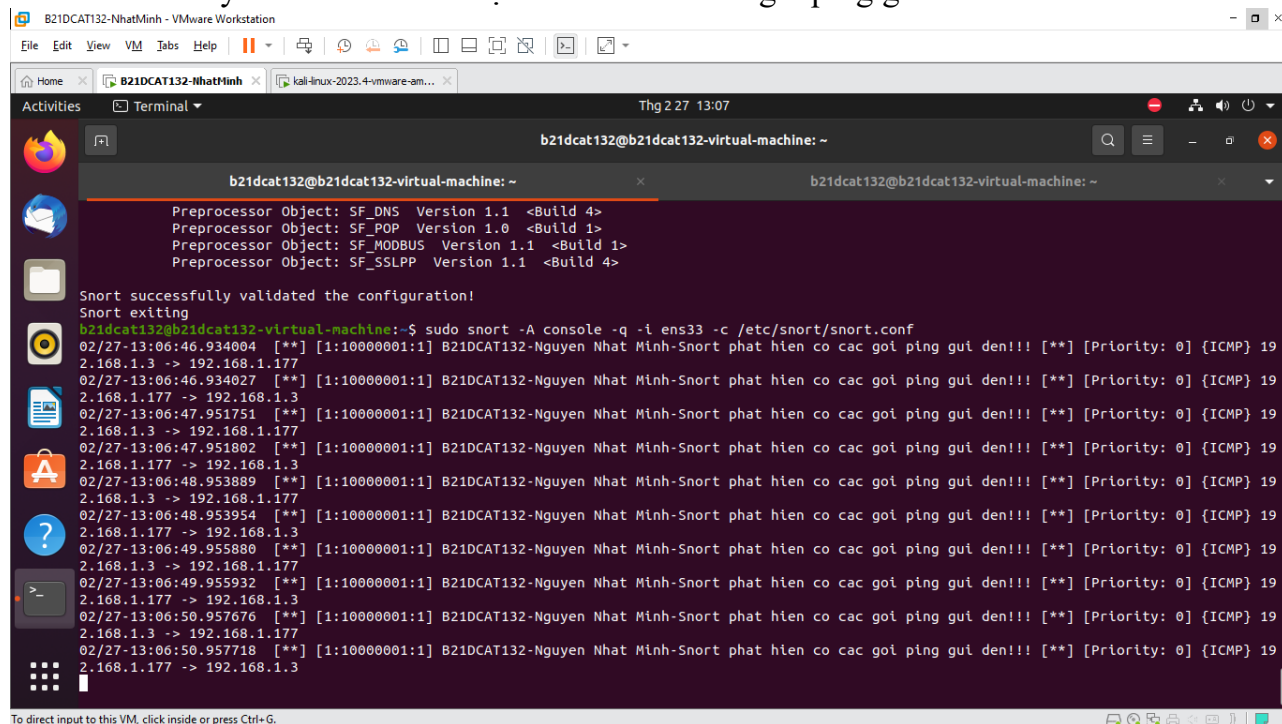
## Trên máy kali tiến hành ping tới ubuntu



The screenshot shows a terminal window titled "kali-linux-2023.4-vmware-amd64 - VMware Workstation". The terminal output shows the execution of the "ping" command to the IP address 192.168.1.177. The output displays the results of five ping requests, including the number of bytes received, the sequence number, the TTL, and the time taken for each request. The ping statistics at the bottom show 5 packets transmitted, 5 received, 0% packet loss, and a time of 4023ms. The round trip time (rtt) is also displayed.

```
kali@kali: ~  
File Actions Edit View Help  
  
--(kali@kali)-[~]  
$ ping 192.168.1.177  
PING 192.168.1.177 (192.168.1.177) 56(84) bytes of data:  
64 bytes from 192.168.1.177: icmp_seq=1 ttl=64 time=0.483 ms  
64 bytes from 192.168.1.177: icmp_seq=2 ttl=64 time=1.20 ms  
64 bytes from 192.168.1.177: icmp_seq=3 ttl=64 time=0.959 ms  
64 bytes from 192.168.1.177: icmp_seq=4 ttl=64 time=1.38 ms  
64 bytes from 192.168.1.177: icmp_seq=5 ttl=64 time=1.13 ms  
^C  
--- 192.168.1.177 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4023ms  
rtt min/avg/max/mdev = 0.483/1.028/1.378/0.304 ms  
  
--(kali@kali)-[~]  
$
```

## - Trên máy ubuntu đã xuất hiện cảnh báo có các gói ping gửi tới



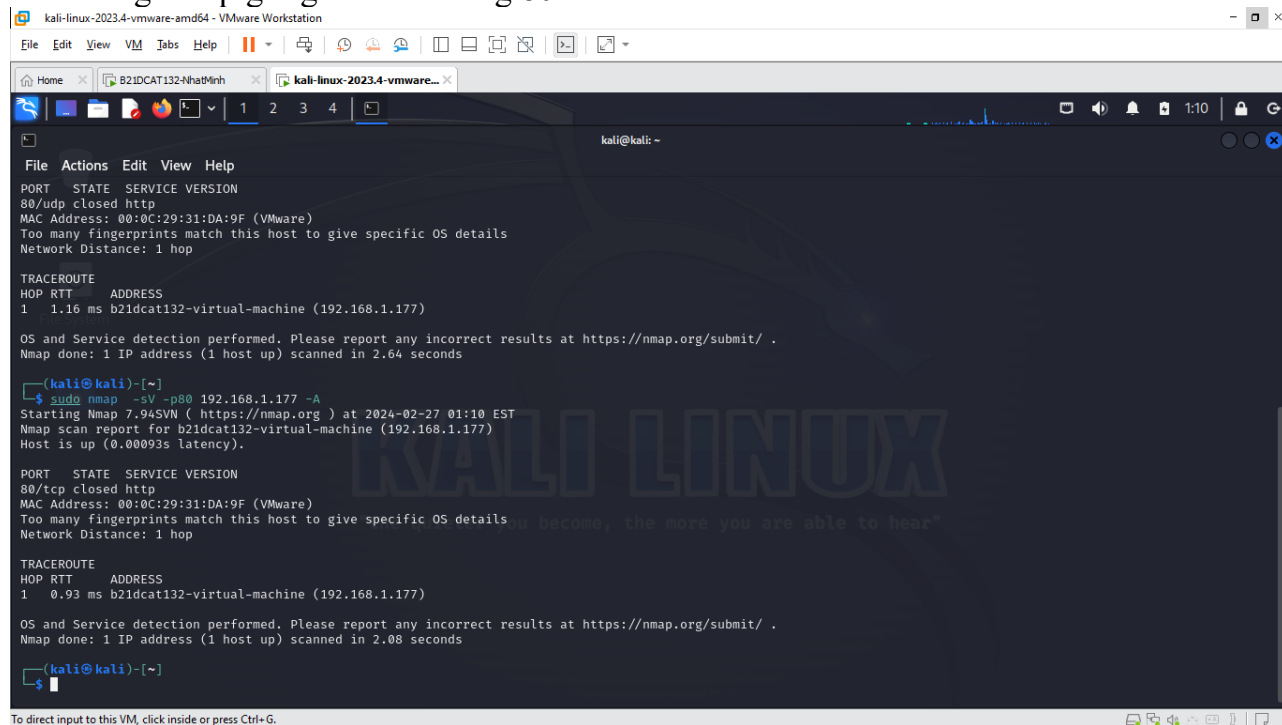
The screenshot shows a terminal window titled "b21dcat132@b21dcat132-virtual-machine: ~". The terminal displays the output of the command `sudo snort -A console -q -i ens33 -c /etc/snort/snort.conf`. The output shows the Snort configuration being validated successfully and then exiting. Below this, a series of log entries are displayed, each showing a timestamp, IP addresses, and a message indicating that Snort has detected ping packets from 192.168.1.3 to 192.168.1.177. The log entries are as follows:

```

02/27-13:06:46.934004  [**] [1:10000001:1] B21DCAT132- Nguyen Nhat Minh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.3 -> 192.168.1.177
02/27-13:06:46.934027  [**] [1:10000001:1] B21DCAT132- Nguyen Nhat Minh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.177 -> 192.168.1.177
02/27-13:06:47.951751  [**] [1:10000001:1] B21DCAT132- Nguyen Nhat Minh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.3 -> 192.168.1.177
02/27-13:06:47.951802  [**] [1:10000001:1] B21DCAT132- Nguyen Nhat Minh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.177 -> 192.168.1.177
02/27-13:06:48.953889  [**] [1:10000001:1] B21DCAT132- Nguyen Nhat Minh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.3 -> 192.168.1.177
02/27-13:06:48.953954  [**] [1:10000001:1] B21DCAT132- Nguyen Nhat Minh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.177 -> 192.168.1.177
02/27-13:06:49.955880  [**] [1:10000001:1] B21DCAT132- Nguyen Nhat Minh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.3 -> 192.168.1.177
02/27-13:06:49.955932  [**] [1:10000001:1] B21DCAT132- Nguyen Nhat Minh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.177 -> 192.168.1.177
02/27-13:06:50.957676  [**] [1:10000001:1] B21DCAT132- Nguyen Nhat Minh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.3 -> 192.168.1.177
02/27-13:06:50.957718  [**] [1:10000001:1] B21DCAT132- Nguyen Nhat Minh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.177 -> 192.168.1.177

```

## Dùng nmap gửi gói tin tới cổng 80



The screenshot shows a terminal window titled "kali@kali: ~". The terminal displays the output of the command `sudo nmap -sV -p80 192.168.1.177 -A`. The output shows the Nmap scan results for the target IP address 192.168.1.177. The scan is performed on port 80/tcp, which is closed. The output also shows the MAC address and network distance. The scan results are as follows:

```

PORT      STATE SERVICE VERSION
80/tcp    closed http
MAC Address: 00:0C:29:31:DA:9F (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.93 ms b21dcat132-virtual-machine (192.168.1.177)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds

```

## - Trên ubuntu đã xuất hiện cảnh báo có gói tin rà quét tới cổng 80

```

b21dcat132@b21dcat132-virtual-machine: ~
02/27-13:10:05.707620 [**] [1:10000001:1] B21DCAT132- NguyenNhatMinh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.177 -> 192.168.1.3
02/27-13:10:05.732419 [**] [1:10000001:1] B21DCAT132- NguyenNhatMinh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.177 -> 192.168.1.3
02/27-13:10:05.757736 [**] [1:10000002:1] B21DCAT132- NguyenNhatMinh-Snort dang phat hien co cac goi tin ra quet tren cong 80!! [**] [Priority:
0] {TCP} 192.168.1.3:37667 -> 192.168.1.177:80
02/27-13:10:05.783522 [**] [1:10000002:1] B21DCAT132- NguyenNhatMinh-Snort dang phat hien co cac goi tin ra quet tren cong 80!! [**] [Priority:
0] {TCP} 192.168.1.3:37668 -> 192.168.1.177:80
02/27-13:10:05.809047 [**] [1:10000002:1] B21DCAT132- NguyenNhatMinh-Snort dang phat hien co cac goi tin ra quet tren cong 80!! [**] [Priority:
0] {TCP} 192.168.1.3:37669 -> 192.168.1.177:80
02/27-13:10:06.818803 [**] [1:10000001:1] B21DCAT132- NguyenNhatMinh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.3 -> 192.168.1.177
02/27-13:10:06.818853 [**] [1:10000001:1] B21DCAT132- NguyenNhatMinh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.177 -> 192.168.1.3
02/27-13:10:06.844028 [**] [1:10000001:1] B21DCAT132- NguyenNhatMinh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.3 -> 192.168.1.177
02/27-13:10:06.844243 [**] [1:10000001:1] B21DCAT132- NguyenNhatMinh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.177 -> 192.168.1.3
02/27-13:10:06.868834 [**] [1:10000001:1] B21DCAT132- NguyenNhatMinh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.177 -> 192.168.1.3
02/27-13:10:06.894657 [**] [1:10000002:1] B21DCAT132- NguyenNhatMinh-Snort dang phat hien co cac goi tin ra quet tren cong 80!! [**] [Priority:
0] {TCP} 192.168.1.3:37667 -> 192.168.1.177:80
02/27-13:10:06.919976 [**] [1:10000002:1] B21DCAT132- NguyenNhatMinh-Snort dang phat hien co cac goi tin ra quet tren cong 80!! [**] [Priority:
0] {TCP} 192.168.1.3:37668 -> 192.168.1.177:80
02/27-13:10:06.944996 [**] [1:10000002:1] B21DCAT132- NguyenNhatMinh-Snort dang phat hien co cac goi tin ra quet tren cong 80!! [**] [Priority:
0] {TCP} 192.168.1.3:37669 -> 192.168.1.177:80
02/27-13:10:06.978862 [**] [1:10000001:1] B21DCAT132- NguyenNhatMinh-Snort phat hien co cac goi ping gui den!!! [**] [Priority: 0] {ICMP} 19
2.168.1.177 -> 192.168.1.3

```

## Trên kali tiến hành tấn công TCP SYN Flood

```

kali@kali: ~
File Actions Edit View Help
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 01:10 EST
Nmap scan report for b21dcat132-virtual-machine (192.168.1.177)
Host is up (0.00093s latency).

PORT      STATE SERVICE VERSION
80/tcp    closed http
MAC Address: 00:0C:29:31:DA:9F (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1 0.93 ms b21dcat132-virtual-machine (192.168.1.177)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds

(kali@kali)~$ hping3 -C 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.177
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket

(kali@kali)~$ sudo hping3 -C 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.177
7
HPING 192.168.1.177 (eth0 192.168.1.177): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
-- 192.168.1.177 hping statistic --
2965139 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(kali@kali)~$

```

## - Trên ubuntu xuất hiện cảnh báo bị tấn công đồng thời có gói tin tới cổng 80

```

b21dcat132@b21dcat132-virtual-machine: ~
02/27-13:14:36.623910 00000002:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện có các gói tin ra quet trên cổng 80!! [Priority: 0] [TCP] 76.148.79.238:18076 -> 192.168.1.177:80
02/27-13:14:36.624005 00000003:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện đang bị tấn công TCP SYN Flood!!! [Priority: 0] [TCP] 220.177.145.196:18077 -> 192.168.1.177:80
02/27-13:14:36.624005 00000002:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện có các gói tin ra quet trên cổng 80!! [Priority: 0] [TCP] 220.177.145.196:18077 -> 192.168.1.177:80
02/27-13:14:36.624241 00000003:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện đang bị tấn công TCP SYN Flood!!! [Priority: 0] [TCP] 208.244.202.73:18078 -> 192.168.1.177:80
02/27-13:14:36.624241 00000002:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện có các gói tin ra quet trên cổng 80!! [Priority: 0] [TCP] 208.244.202.73:18078 -> 192.168.1.177:80
02/27-13:14:36.624379 00000003:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện đang bị tấn công TCP SYN Flood!!! [Priority: 0] [TCP] 253.138.187.165:18079 -> 192.168.1.177:80
02/27-13:14:36.624379 00000002:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện có các gói tin ra quet trên cổng 80!! [Priority: 0] [TCP] 253.138.187.165:18079 -> 192.168.1.177:80
02/27-13:14:36.624615 00000003:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện đang bị tấn công TCP SYN Flood!!! [Priority: 0] [TCP] 14.180.54.173:18080 -> 192.168.1.177:80
02/27-13:14:36.624615 00000002:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện có các gói tin ra quet trên cổng 80!! [Priority: 0] [TCP] 14.180.54.173:18080 -> 192.168.1.177:80
02/27-13:14:36.624711 00000003:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện đang bị tấn công TCP SYN Flood!!! [Priority: 0] [TCP] 86.176.161.18:18081 -> 192.168.1.177:80
02/27-13:14:36.624711 00000002:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện có các gói tin ra quet trên cổng 80!! [Priority: 0] [TCP] 86.176.161.18:18081 -> 192.168.1.177:80
02/27-13:14:36.624911 00000003:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện đang bị tấn công TCP SYN Flood!!! [Priority: 0] [TCP] 210.167.119.245:18082 -> 192.168.1.177:80
02/27-13:14:36.624911 00000002:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện có các gói tin ra quet trên cổng 80!! [Priority: 0] [TCP] 210.167.119.245:18082 -> 192.168.1.177:80
02/27-13:14:36.624951 00000003:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện đang bị tấn công TCP SYN Flood!!! [Priority: 0] [TCP] 133.165.14.248:18083 -> 192.168.1.177:80
02/27-13:14:36.624951 00000002:1 B21DCAT132-PhanNhatMinh-Snort đang phát hiện có các gói tin ra quet trên cổng 80!! [Priority: 0] [TCP] 133.165.14.248:18083 -> 192.168.1.177:80

```

## 4. Kết luận

Bài thực hành hoàn thành vào thứ 3 ngày 27 tháng 2

```

user 0m0,000s
sys 0m0,000s
b21dcat132@b21dcat132-virtual-machine:~$ date
Thứ ba, 27 Tháng 2 năm 2024 14:04:30 +07
b21dcat132@b21dcat132-virtual-machine:~$ echo > B21DCAT132-PhanNhatMinh
b21dcat132@b21dcat132-virtual-machine:~$

```