

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

---



**BÁO CÁO THỰC HÀNH**

**Bài 6: Cài đặt cầu hình HIDS/NIDS**

**Họ và tên: Vũ Thành Long**

**Mã sinh viên: B21DCAT012**

**Nhóm: 06**

**Môn học: Thực tập cơ sở**

**Giảng viên giảng dạy: Nguyễn Hoa Cường**

**Hà Nội, 2024**

# Mục lục

Bài thực hành số 6: Cài đặt cấu hình HIDS/NIDS .....	2
1. Mục đích .....	2
2. Nội dung thực hành .....	2
I. Cơ sở lý thuyết .....	2
1. Hệ Thống Phát Hiện Tấn Công, Xâm Nhập.....	2
2. Các Kỹ Thuật Phát Hiện Xâm Nhập. ....	3
3. Một số hệ thống phát hiện tấn công, xâm nhập.....	3
II. Thực hành .....	6
1. Cài đặt Snort:.....	6
2. Tiến hành chạy snort: .....	9
III. Tổng kết .....	13
IV. Kết quả đạt được .....	13

# **Bài thực hành số 6: Cài đặt cầu 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**

### **I. Cơ sở lý thuyết**

#### **1. Hệ Thống Phát Hiện Tấn Công, Xâm Nhập**

- Là các công cụ quan trọng trong lĩnh vực bảo mật mạng. Chúng giúp phát hiện, cảnh báo và thậm chí ngăn chặn các hoạt động không mong muốn trên mạng, bao gồm các cuộc tấn công từ bên ngoài và từ bên trong hệ thống. Dưới đây là một cái nhìn tổng quan về các loại hệ thống và kỹ thuật phát hiện xâm nhập.

##### **1.1. Hệ Thống Phát Hiện Xâm Nhập Dựa Trên Chữ Ký (Signature-Based IDS/IPS):**

- Dựa vào việc so sánh các dấu vết của các cuộc tấn công với các chữ ký đã biết trước.
- Hiệu suất cao trong việc phát hiện các cuộc tấn công đã được biết trước, nhưng không hiệu quả đối với các cuộc tấn công mới.

##### **1.2. Hệ Thống Phát Hiện Xâm Nhập Dựa Trên Hành Vi (Behavior-Based IDS/IPS):**

- Theo dõi hành vi của hệ thống và người dùng để phát hiện các hoạt động bất thường.
- Có thể phát hiện các cuộc tấn công mới mà không cần dựa vào các chữ ký đã biết trước.

##### **1.3. Hệ Thống Phát Hiện Xâm Nhập Dựa Trên Học Máy (Machine Learning-based IDS/IPS):**

- Sử dụng các thuật toán học máy để phân loại các hoạt động là bình thường hay độc hại.
- Cần có dữ liệu lớn và phong phú để huấn luyện mô hình.

##### **1.4. Hệ Thống Phát Hiện Xâm Nhập Dựa Trên Luật (Rule-Based IDS/IPS):**

- Sử dụng các quy tắc và luật để phát hiện các mẫu tấn công đã biết trước.
- Linh hoạt trong việc cấu hình và có thể được tinh chỉnh dễ dàng, nhưng không hiệu quả đối với các cuộc tấn công mới.

## **2. Các Kỹ Thuật Phát Hiện Xâm Nhập.**

### **2.1. Phân Tích Dữ Liệu Ghi Log (Log Analysis):**

- Kiểm tra và phân tích các tập tin ghi log từ các thiết bị mạng và hệ thống để phát hiện các hoạt động bất thường.

### **2.2. Phân Tích Dấu Vết (Anomaly Detection):**

- Theo dõi và phát hiện các hành vi không bình thường dựa trên các mô hình hành vi thường gặp.

### **2.3. Kiểm Tra Luồng Giao Tiếp (Traffic Inspection):**

- Kiểm tra lưu lượng mạng để phát hiện các mẫu tấn công, bao gồm cả kiểm tra gói tin và kiểm tra lưu lượng ứng dụng.

### **2.4. Phân Tích Mã Độc (Malware Analysis):**

- Phân tích các tập tin mã độc để phát hiện và hiểu cách thức hoạt động của chúng.

### **2.5. Phân Tích Hành Vi Mạng (Network Behavior Analysis):**

- Theo dõi hành vi của các thiết bị và người dùng trên mạng để phát hiện các hoạt động không bình thường.

### **2.6. Kiểm Tra Chướng Ngại (Honeypots):**

- Triển khai các hệ thống giả mạo để thu thập thông tin về các cuộc tấn công và kẻ tấn công.

## **3. Một số hệ thống phát hiện tấn công, xâm nhập.**

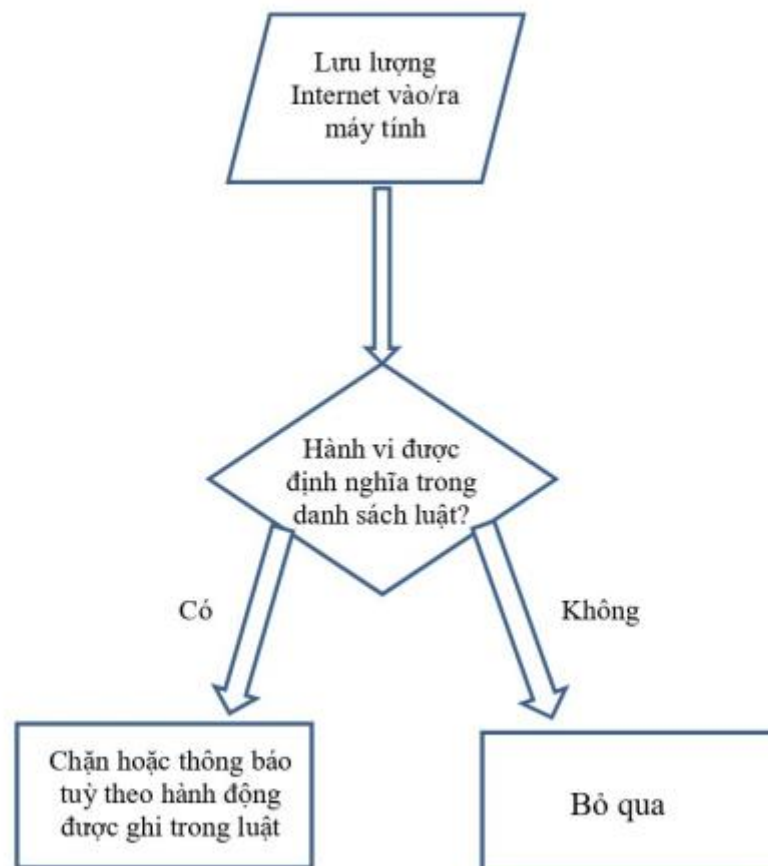
### **3.1. Snort:**

- Định nghĩa: Snort là một hệ thống phát hiện xâm nhập mạng mã nguồn mở (IDS) và hệ thống ngăn chặn xâm nhập (IPS) được phát triển bởi Martin Roesch từ năm 1998. Sau khi Sourcefire - công ty của Roerch được Cisco mua lại vào năm 2013, trách nhiệm phát triển Snort thuộc về Cisco.
- Tính năng: Snort có khả năng thực hiện phân tích lưu lượng thời gian thực và ghi nhật ký gói tin trên mạng Giao thức Internet (IP). Snort thực hiện phân tích

giao thức, tìm kiếm và so sánh nội dung. Snort cũng có thể được sử dụng để phát hiện các cuộc tấn công hoặc thăm dò như tấn công tràn bộ đệm, quét cổng, v.v

- Snort có thể hoạt động theo 1 trong 3 chế độ:

- Sniffer Mode: Snort đọc thông tin các gói tin và hiển thị lên terminal.
- Package Logger Mode: Snort ghi lại lịch sử các gói tin vào tệp tin log lưu trên ổ cứng.
- Network Intrusion Detection System Mode: Snort giám sát lưu lượng internet vào ra máy tính và so sánh với các luật (được đặt bởi quản trị viên). Nếu phát hiện lưu lượng trùng với một luật, Snort sẽ thực hiện một hành động do quản trị viên thiết lập sẵn trong luật đó.



- **Luật Snort:**

- Luật Snort có cấu trúc như sau: **<header>** (**<option>**)
- Header chứa thông tin về kiểu, nguồn, đích của gói tin, cũng như hành động Snort thực hiện nếu phát hiện gói tin thỏa mãn các điều kiện trên.

- Option chứa các tùy chọn cụ thể nhằm hỗ trợ cho việc thực thi hành động trong header ví dụ như: in thông báo ra màn hình nếu phát hiện gói tin, kiểm tra nội dung của gói tin, ghi kết quả ra file log, v.v
- Ví dụ về luật Snort để phát hiện gói tin ping từ máy khác gửi đến:  
**alert icmp any any -> \$HOME\_NET any (msg:"B21DCAT012-Long-Snort phat hien co cac goi tin gui den"; sid:1000001;)**
- Trong đó, "alert" chỉ hành động Snort sẽ thực hiện nếu phát hiện gói tin thỏa mãn yêu cầu. "icmp" chỉ giao thức của gói tin. "any" đầu tiên chỉ địa chỉ IP của nguồn gửi gói tin. "any" thứ hai chỉ cổng của nguồn gửi gói tin. "\$HOME\_NET" chỉ địa chỉ IP đích của gói tin. "any" thứ ba chỉ cổng của đích đến gói tin.
- "msg" sẽ in ra màn hình thông báo ghi trong dấu ngoặc kép. "sid" là mã luật

### 3.2. Suricata:

- **Kiến trúc:** Suricata cũng là một hệ thống phát hiện xâm nhập dựa trên chữ ký nhưng được thiết kế để hỗ trợ phát hiện dựa trên hành vi và sử dụng đa luồng.

- **Tính năng:**

- + Hỗ trợ phát hiện dựa trên chữ ký, hành vi và mô hình.
- + Sử dụng đa luồng để tăng hiệu suất phát hiện và xử lý.
- + Hỗ trợ giao thức nhiều lớp, bao gồm HTTP, SSH, DNS, và nhiều hơn nữa.

### 3.3. Zeek (trước đây là Bro):

- **Kiến trúc:** Zeek là một hệ thống phát hiện xâm nhập dựa trên hành vi. Nó theo dõi và phân tích dữ liệu mạng để phát hiện các hành vi không bình thường.

- **Tính năng:**

- + Tập trung vào việc thu thập và phân tích lưu lượng mạng để phát hiện các mẫu tấn công và hành vi bất thường.
- + Hỗ trợ xử lý các giao thức cụ thể như TCP, UDP, DNS, SSL, và nhiều giao thức khác.
- + Cung cấp một giao diện linh hoạt cho việc phát triển các script và phân tích dữ liệu.

### 3.4. OSSEC:

- **Kiến trúc:** OSSEC là một hệ thống phát hiện xâm nhập dựa trên luật. Nó sử dụng các quy tắc để phát hiện các mẫu tấn công đã biết trước.

- **Tính năng:**

+ Cung cấp phát hiện xâm nhập cho nhiều nền tảng hệ điều hành như Windows, Linux, và MacOS.

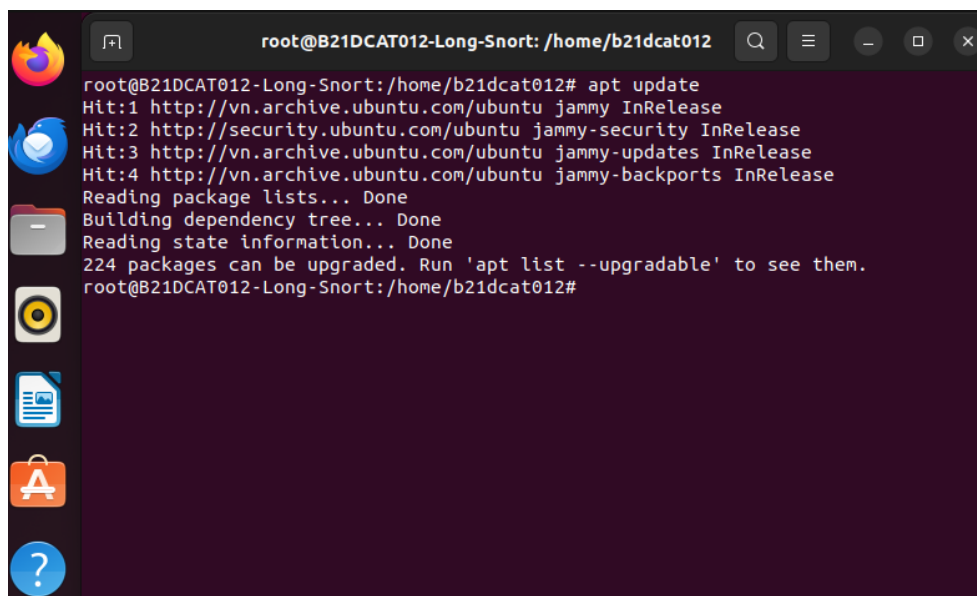
+ Theo dõi các tập tin hệ thống, sự kiện đăng nhập, và các hoạt động hệ thống để phát hiện các mẫu tấn công.

+ Hỗ trợ cảnh báo thời gian thực và tích hợp với các giải pháp bảo mật khác như SIEM (Security Information and Event Management).

## II. Thực hành

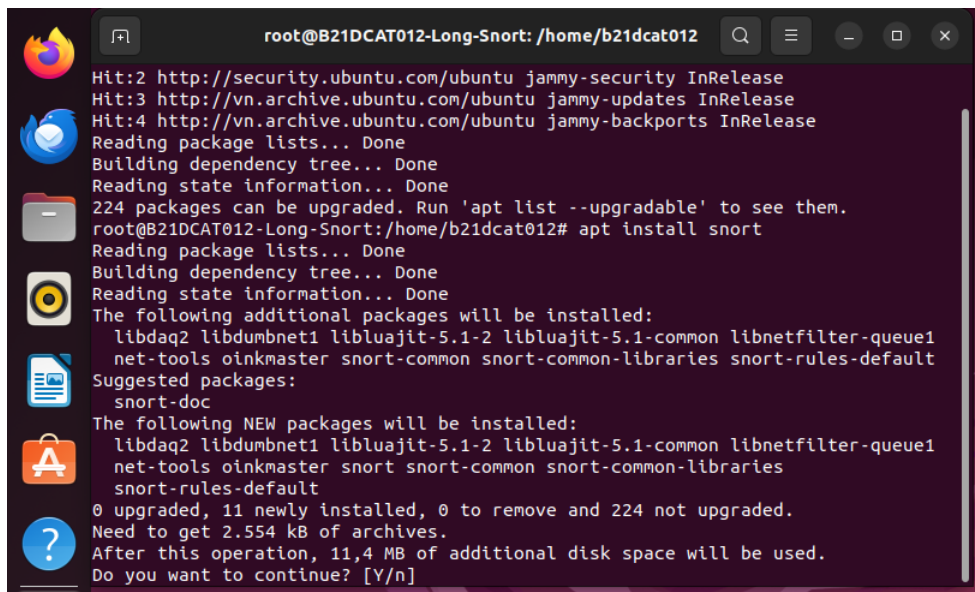
### 1. Cài đặt Snort:

Trước khi cài đặt snort ta cần đảm bảo các dịch vụ của Ubuntu hoạt động ổn định và cập nhật mới. Ta sử dụng lệnh *apt update* để cập nhật dịch vụ.



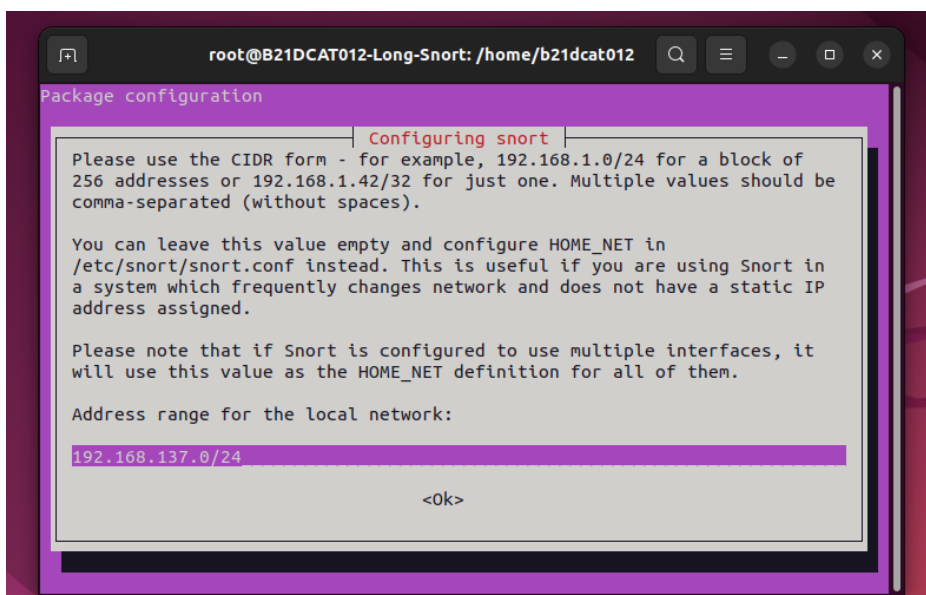
```
root@B21DCAT012-Long-Snort: /home/b21dcat012# apt update
Hit:1 http://vn.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://vn.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://vn.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
224 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@B21DCAT012-Long-Snort: /home/b21dcat012#
```

Sau khi cập nhật, ta tiến hành cài đặt snort. Sử dụng *apt install snort* để cài đặt dịch vụ.



```
root@B21DCAT012-Long-Snort: /home/b21dcat012
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://vn.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://vn.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
224 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@B21DCAT012-Long-Snort:/home/b21dcat012# apt install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1
  net-tools oinkmaster snort snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1
  net-tools oinkmaster snort snort-common snort-common-libraries
  snort-rules-default
0 upgraded, 11 newly installed, 0 to remove and 224 not upgraded.
Need to get 2.554 kB of archives.
After this operation, 11,4 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Sau khi cài đặt xong, dịch vụ snort tự động khởi động. Ta nhập địa chỉ IP máy snort, ở octet cuối ta nhập 0.



```
Package configuration
Configuring snort
Please use the CIDR form - for example, 192.168.1.0/24 for a block of
256 addresses or 192.168.1.42/32 for just one. Multiple values should be
comma-separated (without spaces).

You can leave this value empty and configure HOME_NET in
/etc/snort/snort.conf instead. This is useful if you are using Snort in
a system which frequently changes network and does not have a static IP
address assigned.

Please note that if Snort is configured to use multiple interfaces, it
will use this value as the HOME_NET definition for all of them.

Address range for the local network:
192.168.137.0/24
<Ok>
```

Kiểm tra snort đã cài đặt chưa bằng cách kiểm tra version.



```
root@B21DCAT012-Long-Snort: /home/b21dcat012
root@B21DCAT012-Long-Snort:/home/b21dcat012# snort --v

o" )~
' "'

-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.

Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

root@B21DCAT012-Long-Snort:/home/b21dcat012#
```

Hãy sử dụng *systemctl*.

```
root@B21DCAT012-Long-Snort: /home/b21dcat012
root@B21DCAT012-Long-Snort:/home/b21dcat012# systemctl status snort
● snort.service - LSB: Lightweight network intrusion detection system
   Loaded: loaded (/etc/init.d/snort; generated)
   Active: active (running) since Thu 2024-03-14 14:57:43 +07; 43s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 6500 ExecStart=/etc/init.d/snort start (code=exited, status=0/SUCCESS)
    Tasks: 2 (limit: 2217)
   Memory: 78.2M
      CPU: 567ms
    CGroup: /system.slice/snort.service
            └─6521 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g >

Thg 3 14 14:57:43 B21DCAT012-Long-Snort snort[6521]: Preprocessor Ob>
Thg 3 14 14:57:43 B21DCAT012-Long-Snort snort[6521]: Preprocessor Ob>
Thg 3 14 14:57:43 B21DCAT012-Long-Snort snort[6521]: Preprocessor Ob>
Thg 3 14 14:57:43 B21DCAT012-Long-Snort snort[6521]: Preprocessor Ob>
Thg 3 14 14:57:43 B21DCAT012-Long-Snort snort[6521]: Preprocessor Ob>
Thg 3 14 14:57:43 B21DCAT012-Long-Snort snort[6521]: Preprocessor Ob>
Thg 3 14 14:57:43 B21DCAT012-Long-Snort snort[6521]: Preprocessor Ob>
Thg 3 14 14:57:43 B21DCAT012-Long-Snort snort[6521]: Preprocessor Ob>
Thg 3 14 14:57:43 B21DCAT012-Long-Snort snort[6521]: Commencing packet processi>
lines 1-21/21 (END)
```

Hãy thử chạy dịch vụ snort hoặc xem log.

```
root@B21DCAT012-Long-Snort: /home/b21dcat012# snort -q -A console -c /etc/snort/snort.conf -i ens33
03/14-15:02:27.253015  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.137.1:6
3239 -> 239.255.255.250:1900
03/14-15:02:28.253390  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.137.1:6
3239 -> 239.255.255.250:1900
03/14-15:02:29.253304  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.137.1:6
3239 -> 239.255.255.250:1900
03/14-15:02:30.256310  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.137.1:6
3239 -> 239.255.255.250:1900
^C*** Caught Int-Signal
root@B21DCAT012-Long-Snort: /home/b21dcat012#
```

```
root@B21DCAT012-Long-Snort: /var/log/snort#
USER-AGENT: Microsoft Edge/122.0.2365.80 Windows

o|eA|*****Il***A**^**PE#B\<*****IlN*M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Microsoft Edge/122.0.2365.80 Windows

o|eMx|*****Il***mx**^**PE#C\;*****IlN*M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Microsoft Edge/122.0.2365.80 Windows

o|eN|*****Il***n**^**PE#D\;*****IlN*M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Microsoft Edge/122.0.2365.80 Windows

root@B21DCAT012-Long-Snort: /var/log/snort#
```

## 2. Tiến hành chạy snort:

Thiết lập địa chỉ IP dịch vụ snort cần bảo vệ.

```
root@B21DCAT012-Long-Snort: /home/b21dcat012
GNU nano 6.2 /etc/snort/snort.conf *
# The Debian init.d script is defined in such a way
# that you can run multiple instances.

#####
# 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 192.168.137.130

# 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

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^_ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

Xóa các rules mà dịch snort đã cài đặt sẵn để ta dễ dàng xem được kết quả cần tìm, tránh xung đột giữa các rules.

```
596
597 #include $RULE_PATH/app-detect.rules
598
599
600 #include $RULE_PATH/blacklist.rules
601 #include $RULE_PATH/botnet-cnc.rules
602 #include $RULE_PATH/browser-chrome.rules
603 #include $RULE_PATH/browser-firefox.rules
604 #include $RULE_PATH/browser-ie.rules
605 #include $RULE_PATH/browser-other.rules
606 #include $RULE_PATH/browser-plugins.rules
607 #include $RULE_PATH/browser-webkit.rules
608
609 #include $RULE_PATH/content-replace.rules
610
611 #include $RULE_PATH/exploit-kit.rules
612
613 #include $RULE_PATH/file-executable.rules
614 #include $RULE_PATH/file-flash.rules
615 #include $RULE_PATH/file-identify.rules
616 #include $RULE_PATH/file-image.rules
617 #include $RULE_PATH/file-multimedia.rules
618 #include $RULE_PATH/file-office.rules
619 #include $RULE_PATH/file-other.rules
620 #include $RULE_PATH/file-pdf.rules
621
622 # ICMP standard information queries will trigger these rules, they are very
623 # chatty, only enable if you need them
624 #include $RULE_PATH/icmp-info.rules
625
```

Plain Text Tab Width: 8 Ln 610, Col 1 INS

Thay đổi rules tại local.rules như sau.

```
root@B21DCAT012-Long-Snort: /home/b21dcat012
GNU nano 6.2 /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert icmp any any -> $HOME_NET any (msg: "B21DCAT012-Long-Snort phat hien co c
alert tcp any any -> $HOME_NET 80 (msg: "B21DCAT012-Long-Snort phat hien co cac
alert tcp any any -> $HOME_NET 80 (flags: S; msg: "B21DCAT012-Long-Snort phat h
```

```
*local.rules
/etc/snort/rules
Save

1 # $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
2 # -----
3 # LOCAL RULES
4 # -----
5 # This file intentionally does not come with signatures.  Put your local
6 # additions here.
7 alert icmp any any -> $HOME_NET any (msg: "B21DCAT012-Long-Snort phat hien co cac goi Ping gui
8 den."; sid:1000001;)
9 alert tcp any any -> $HOME_NET 80 (msg: "B21DCAT012-Long-Snort phat hien co cac goi tin ra quet
10 tren cong 80."; sid:1000002;)
11 alert tcp any any -> $HOME_NET 80 (flags: S; msg: "B21DCAT012-Long-Snort phat hien dang bi tan
cong TCP SYN flood"; detection_filter: track by_dst, count 500, seconds 5; sid: 1000003;)
```

Lệnh phát hiện máy tấn công sử dụng dịch vụ ping.

```
alert icmp any any -> $HOME_NET any (msg: "B21DCAT012-Long-Snort phat hien co cac goi Ping gui
den."; sid:1000001;)
```

Lệnh phát hiện máy tấn công sử dụng dịch vụ rà quét trên cổng 80.

```
alert tcp any any -> $HOME_NET 80 (msg: "B21DCAT012-Long-Snort phat hien co cac goi tin ra quet
tren cong 80."; sid:1000002;)
```

Lệnh phát hiện máy tấn công sử dụng TCP SYN Flood.

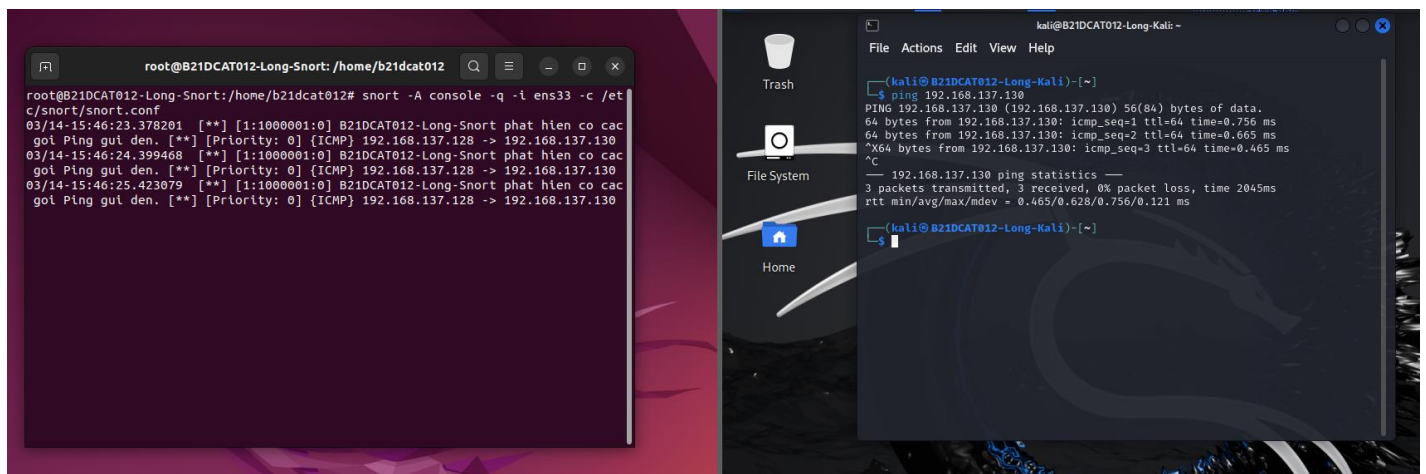
```
alert tcp any any -> $HOME_NET 80 (flags: S; msg: "B21DCAT012-Long-Snort phat hien dang bi tan
cong TCP SYN flood"; detection_filter: track by_dst, count 500, seconds 5; sid: 1000003;)
```

Khởi động lại và chạy lại snort để kiểm tra lệnh có hoạt động.

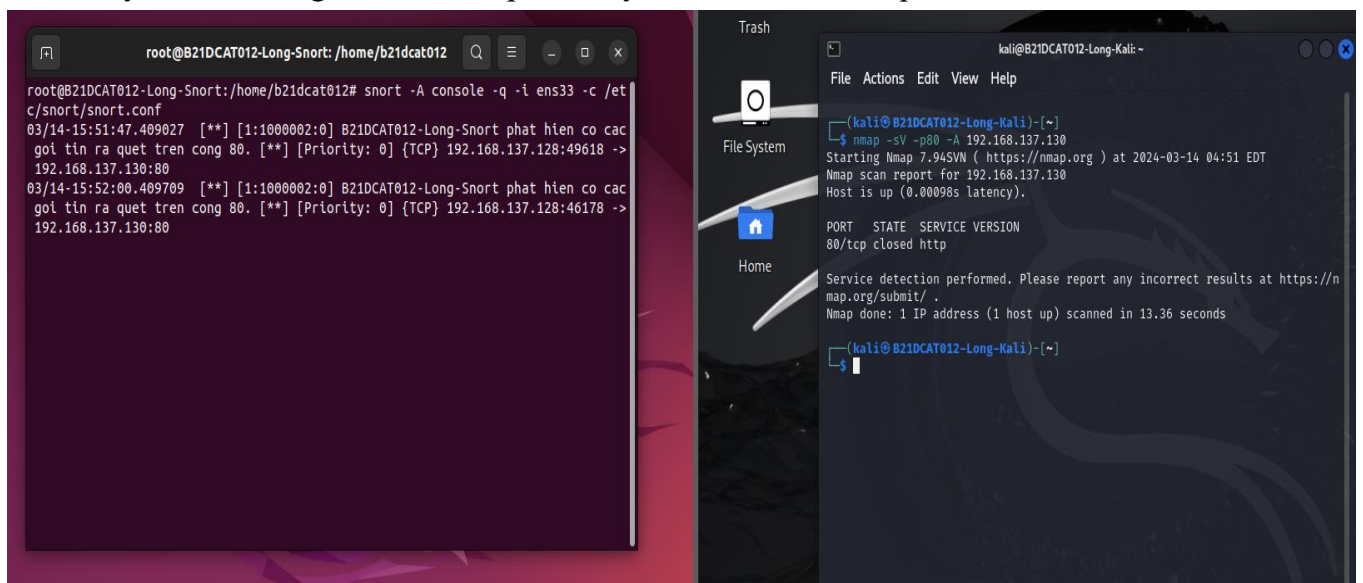
```
root@B21DCAT012-Long-Snort: /home/b21dcat012
root@B21DCAT012-Long-Snort:/home/b21dcat012# systemctl restart snort
root@B21DCAT012-Long-Snort:/home/b21dcat012# systemctl status snort
● snort.service - LSB: Lightweight network intrusion detection system
   Loaded: loaded (/etc/init.d/snort; generated)
   Active: active (running) since Thu 2024-03-14 15:45:41 +07; 8s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 7607 ExecStart=/etc/init.d/snort start (code=exited, status=0/SUCCESS)
    Tasks: 2 (limit: 2217)
   Memory: 40.5M
      CPU: 106ms
   CGroup: /system.slice/snort.service
           └─7629 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g

Thg 3 14 15:45:41 B21DCAT012-Long-Snort snort[7629]: Preprocessor Ob>
Thg 3 14 15:45:41 B21DCAT012-Long-Snort snort[7629]: Preprocessor Ob>
Thg 3 14 15:45:41 B21DCAT012-Long-Snort snort[7629]: Preprocessor Ob>
Thg 3 14 15:45:41 B21DCAT012-Long-Snort snort[7629]: Preprocessor Ob>
Thg 3 14 15:45:41 B21DCAT012-Long-Snort snort[7629]: Preprocessor Ob>
Thg 3 14 15:45:41 B21DCAT012-Long-Snort snort[7629]: Preprocessor Ob>
Thg 3 14 15:45:41 B21DCAT012-Long-Snort snort[7629]: Preprocessor Ob>
Thg 3 14 15:45:41 B21DCAT012-Long-Snort snort[7629]: Preprocessor Ob>
Thg 3 14 15:45:41 B21DCAT012-Long-Snort snort[7629]: Commencing packet processi>
lines 1-21/21 (END)
```

Khởi động máy tấn công Kali. Sử dụng dịch vụ ping tới máy snort. Ghi lại kết qu

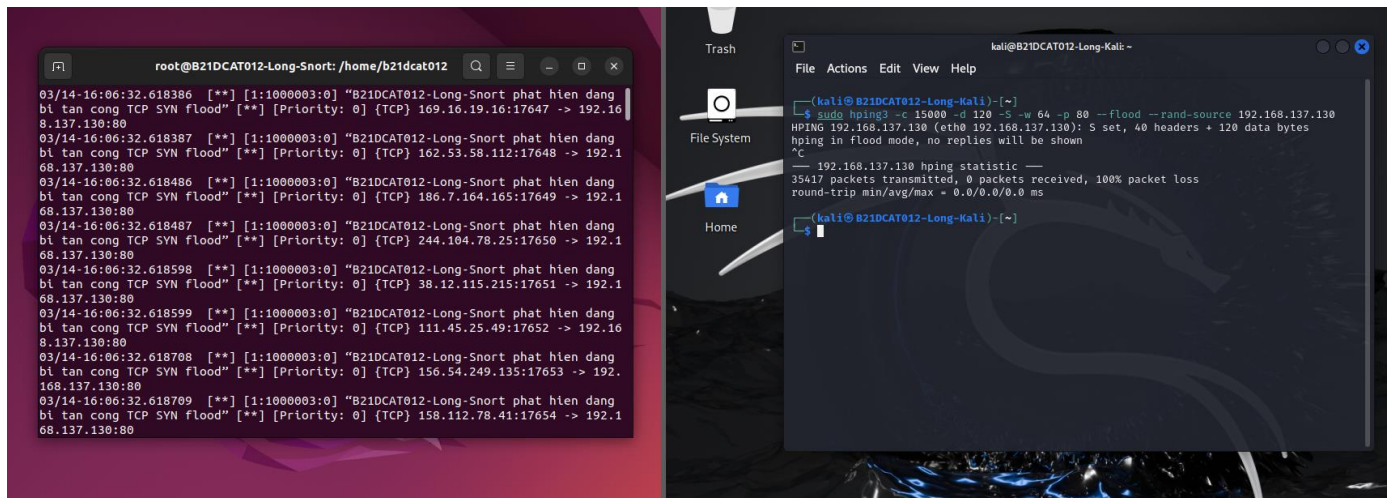


Máy Kali sử dụng dịch vụ nmap tới máy snort. Ghi lại kết quả.





Máy Kali sử dụng dịch vụ hping3 để tấn công TCP SYN Flood tới máy snort. Ghi lại kết quả.



### III. Tổng kết

- 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.
- Dùng các dịch vụ để tấn công.

### IV. Kết quả đạt được

- 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).