HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI THỰC HÀNH 6

THỰC TẬP CƠ SỞ

Họ và tên: Đinh Quang Hiếu

Mã sinh viên: B19DCAT065

Giảng viên giảng dạy: Hoàng Xuân Dậu

Hà Nội – 2022

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

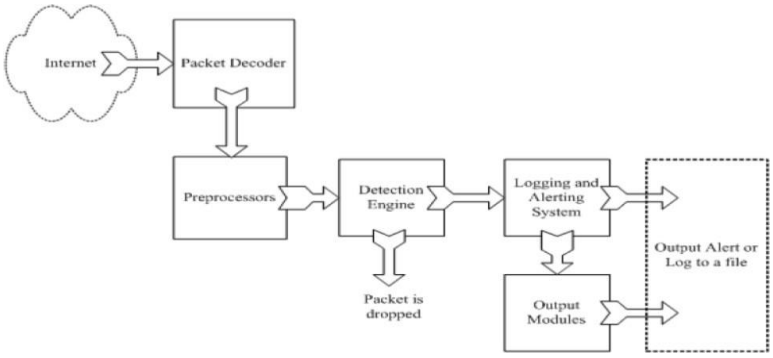
2.1. Tìm hiểu lý thuyết

- Các hệ thống phát hiện tấn công, xâm nhập, phân loại các hệ thống phát hiện xâm nhập, các kỹ thuật phát hiện xâm nhập.

- Hệ thống phát hiện tấn công, xâm nhập IDS là thiết bị phần cứng, phần mềm để thực hiện việc giám sát, theo dõi lưu lượng mạng và thu thập thông tin từ nhiều nguồn khác nhau. Sau đó, sẽ phân tích để tìm ra dấu hiệu của sự bất thường, có nguy cơ bị xâm nhập hay tấn công hệ thống và thông báo đến người quản trị hệ thống để có thể phản hồi lại các cuộc tấn công.
- Phân loại chính: hệ thống phát hiện xâm nhập mạng NIDS và hệ thống phát hiện xâm nhập host HIDS

Kiến trúc và tính năng của hệ thống phát hiện tấn công, xâm nhập Snort

- Kiến trúc : Snort bao gồm nhiều thành phần, mỗi phần có một chức năng riêng biệt
  - ✓ Module giải mã gói tin (packet decoder)
  - ✓ Module tiền xử lý (preprocessors)
  - ✓ Module phát hiện (detection engine)
  - ✓ Module log và cảnh báo(logging and alerting system)
  - ✓ Module kết xuất thông tin (output module)



- Tính năng:
  - ✓ Phát hiện các dấu hiệu xâm nhập
  - ✓ Thực hiện việc lắng nghe và thu bắt gói tin nào di chuyển qua nó
  - ✓ Xuất các thông tin ra các định dang khác nhau tùy theo ta cấu hình

2.2. Chuẩn bị môi trường, công cụ

- 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

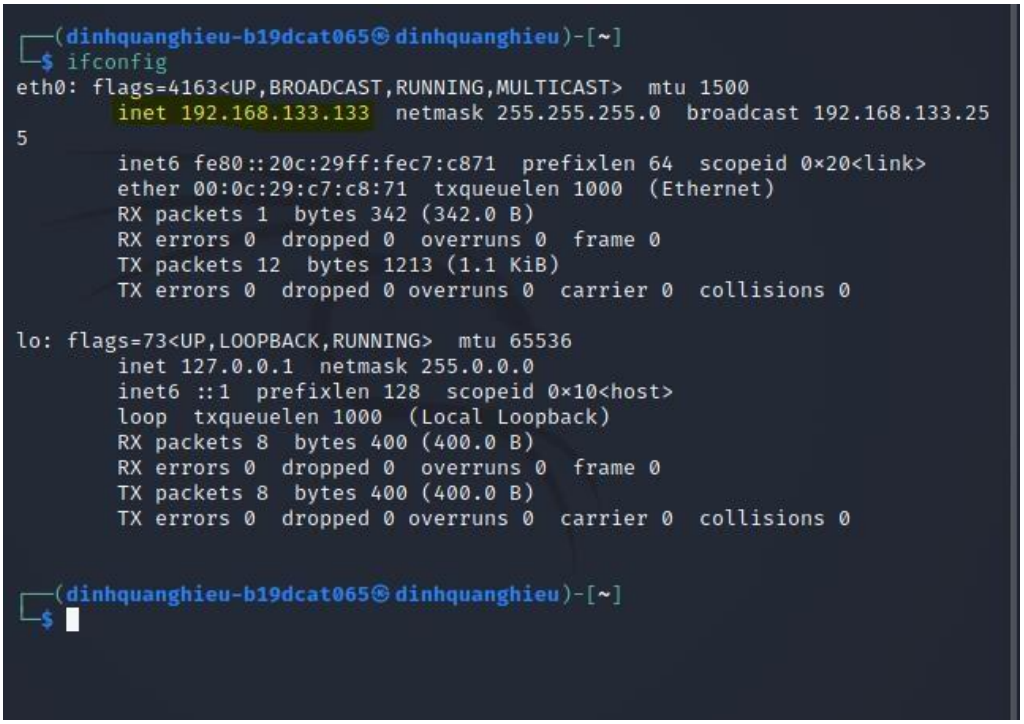
2.3. Các bước thực hiện

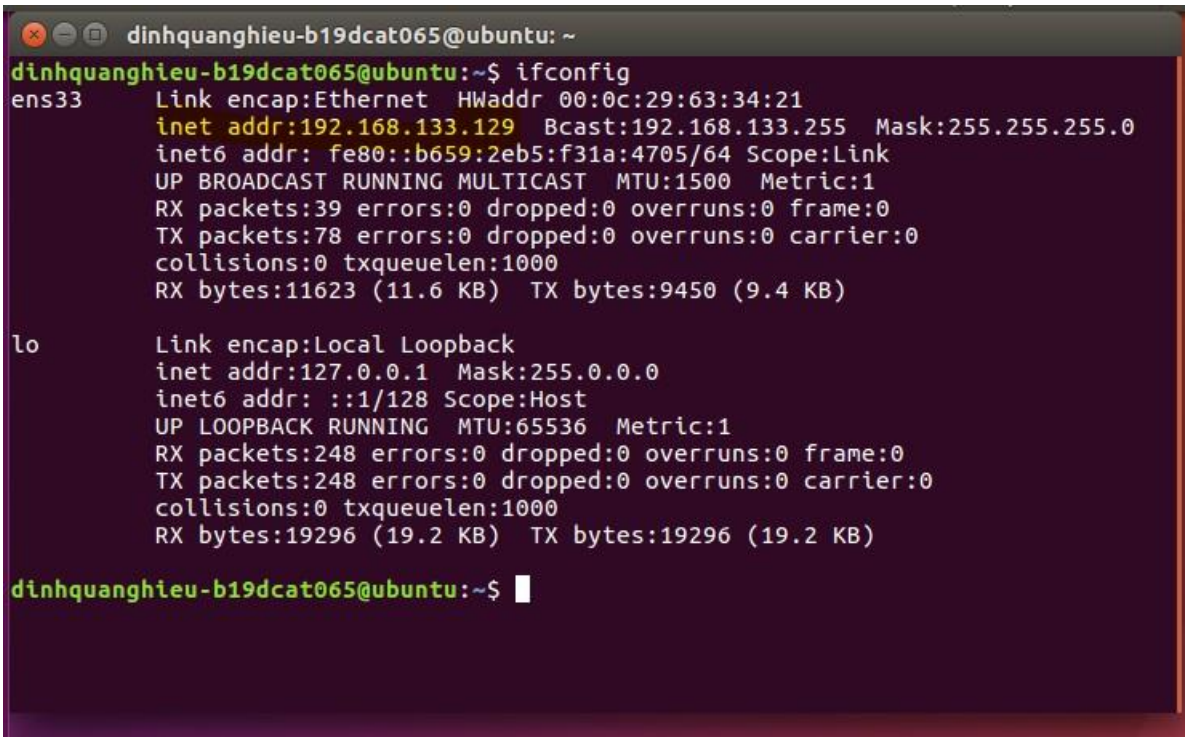
Bước 1:

Chuẩn bị :

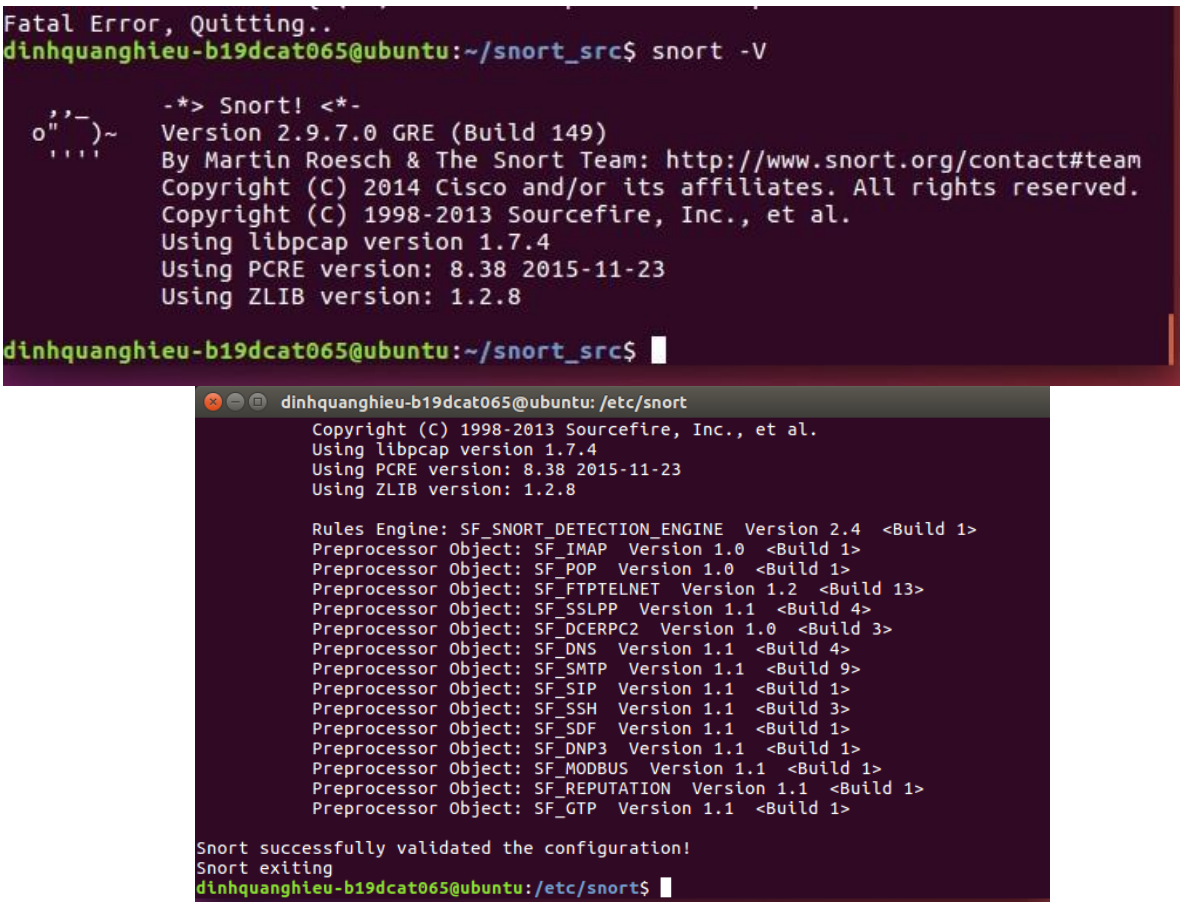
- Máy Kali Linux được đổi tên thành < Mã SV-Tên SV>-Kali
- Máy cài Snort thành <Mã SV-Tên SV>-Snort.

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:

- Tạo tệp luật mới local.rules

```
Snort exiting
dinhquanghieu-b19dcat065@ubuntu:/etc/snort$ sudo nano /etc/snort/rules/local.rules
```

- Phát hiện các gói tin ping từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiển thị thông điệp khi phát hiện: "-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. Hiển thị thông điệp khi phát hiện: "-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. Hiển thị thông điệp khi phát hiện: "-Snort phát hiện đang bị tấn công TCP SYN Flood."

```
dinhquanghieu-b19dcat065@ubuntu: ~
 GNU nano 2.5.3                File: /etc/snort/rules/local.rules                Modified

# $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:"b19dcat065-Hieu_snort phat hien cac goi ping gui den"; sid:1000002; rev:1;)
alert tcp any any -> $HOME_NET 80 (msg:" b19dcat065-Hieu_snort phat hien cac goi tin quet ten cong 80"; sid:1000003; rev:1;)
alert tcp any any -> $HOME_NET any (msg:"b19dcat065-Hieu_snort phat hien bi tan cong TCP SNY Flood"; flags:S;  sid:1000004;$
```

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.

```
┌──(dinhquanghieu-b19dcat065㉿dinhquanghieu)-[~]
└─$ ping 192.168.133.129                                                    148 ×
PING 192.168.133.129 (192.168.133.129) 56(84) bytes of data.
64 bytes from 192.168.133.129: icmp_seq=1 ttl=64 time=0.751 ms
64 bytes from 192.168.133.129: icmp_seq=2 ttl=64 time=0.503 ms
64 bytes from 192.168.133.129: icmp_seq=3 ttl=64 time=0.520 ms
64 bytes from 192.168.133.129: icmp_seq=4 ttl=64 time=0.572 ms
64 bytes from 192.168.133.129: icmp_seq=5 ttl=64 time=0.495 ms
64 bytes from 192.168.133.129: icmp_seq=6 ttl=64 time=0.538 ms
64 bytes from 192.168.133.129: icmp_seq=7 ttl=64 time=0.523 ms
^C
--- 192.168.133.129 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6148ms
rtt min/avg/max/mdev = 0.495/0.557/0.751/0.082 ms

┌──(dinhquanghieu-b19dcat065㉿dinhquanghieu)-[~]
└─$
```

```
dinhquanghieu-b19dcat065@ubuntu: ~
dinhquanghieu-b19dcat065@ubuntu:~$ sudo nano /etc/snort/rules/local.rules
[sudo] password for dinhquanghieu-b19dcat065:
dinhquanghieu-b19dcat065@ubuntu:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i ens33
03/24-03:16:39.258518  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority:
3] {ICMP} 192.168.133.133 -> 192.168.133.129
03/24-03:16:39.258518  [**] [1:1000002:1] b19dcat065-Hieu_snort phat hien cac goi ping gui den [**] [
Priority: 0] {ICMP} 192.168.133.133 -> 192.168.133.129
03/24-03:16:39.258518  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {I
CMP} 192.168.133.133 -> 192.168.133.129
03/24-03:16:39.258616  [**] [1:1000002:1] b19dcat065-Hieu_snort phat hien cac goi ping gui den [**] [
Priority: 0] {ICMP} 192.168.133.129 -> 192.168.133.133
03/24-03:16:39.258616  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority:
 3] {ICMP} 192.168.133.129 -> 192.168.133.133
03/24-03:16:40.285866  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority:
3] {ICMP} 192.168.133.133 -> 192.168.133.129
03/24-03:16:40.285866  [**] [1:1000002:1] b19dcat065-Hieu_snort phat hien cac goi ping gui den [**] [
Priority: 0] {ICMP} 192.168.133.133 -> 192.168.133.129
03/24-03:16:40.285866  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {I
CMP} 192.168.133.133 -> 192.168.133.129
03/24-03:16:40.285898  [**] [1:1000002:1] b19dcat065-Hieu_snort phat hien cac goi ping gui den [**] [
Priority: 0] {ICMP} 192.168.133.129 -> 192.168.133.133
03/24-03:16:40.285898  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority:
 3] {ICMP} 192.168.133.129 -> 192.168.133.133
03/24-03:16:41.309853  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority:
```

- 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

```
└─$ sudo nmap -sV -p80 -A 192.168.133.129
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-24 06:23 EDT
Nmap scan report for 192.168.133.129
Host is up (0.00064s latency).

PORT   STATE  SERVICE VERSION
80/tcp closed http
MAC Address: 00:0C:29:63:34:21 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.64 ms 192.168.133.129

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.42 seconds

┌──(dinhquanghieu-b19dcat065㉿dinhquanghieu)-[~]
└─$
```

```
dinhquanghieu-b19dcat065@ubuntu:~$ sudo snort -A console -q -c /etc/snort/snort.conf -i ens
33
03/24-06:40:58.319303  [**] [1:1000003:1]  b19dcat065-Hieu_snort phat hien cac goi tin quet
 ten cong 80 [**] [Priority: 0] {TCP} 192.168.133.133:42120 -> 192.168.133.129:80
03/24-06:40:58.538895  [**] [1:365:8] ICMP PING undefined code [**] [Classification: Misc a
ctivity] [Priority: 3] {ICMP} 192.168.133.133 -> 192.168.133.129
03/24-06:40:58.538925  [**] [1:409:7] ICMP Echo Reply undefined code [**] [Classification:
Misc activity] [Priority: 3] {ICMP} 192.168.133.129 -> 192.168.133.133
03/24-06:40:58.564402  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Prior
ity: 3] {ICMP} 192.168.133.133 -> 192.168.133.129
03/24-06:40:58.564430  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity]
[Priority: 3] {ICMP} 192.168.133.129 -> 192.168.133.133
03/24-06:40:58.589714  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [C
lassification: Misc activity] [Priority: 3] {ICMP} 192.168.133.129 -> 192.168.133.133
03/24-06:40:58.614809  [**] [1:1000003:1]  b19dcat065-Hieu_snort phat hien cac goi tin quet
 ten cong 80 [**] [Priority: 0] {TCP} 192.168.133.133:44514 -> 192.168.133.129:80
03/24-06:40:58.640368  [**] [1:1000003:1]  b19dcat065-Hieu_snort phat hien cac goi tin quet
 ten cong 80 [**] [Priority: 0] {TCP} 192.168.133.133:44515 -> 192.168.133.129:80
```

- 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.

```
  --apd-send       Send the packet described with APD (see docs/APD.txt)
┌──(dinhquanghieu-b19dcat065㉿dinhquanghieu)-[~]
└─$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.
133.129
HPING 192.168.133.129 (eth0 192.168.133.129): S set, 40 headers + 120 data by
tes
hping in flood mode, no replies will be shown
^C
--- 192.168.133.129 hping statistic ---
8645326 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(dinhquanghieu-b19dcat065㉿dinhquanghieu)-[~]
└─$                                                                    1 ✘
```

```
dinhquanghieu-b19dcat065@ubuntu: ~
[Priority: 0] {TCP} 102.68.103.142:35657 -> 192.168.133.129:80
03/24-03:29:28.833904  [**] [1:1000004:1] b19dcat065-Hieu_snort phat hien bi tan cong TCP SNY Flood [**]
[Priority: 0] {TCP} 161.199.50.138:35658 -> 192.168.133.129:80
03/24-03:29:28.833941  [**] [1:1000004:1] b19dcat065-Hieu_snort phat hien bi tan cong TCP SNY Flood [**]
[Priority: 0] {TCP} 200.3.28.85:35659 -> 192.168.133.129:80
03/24-03:29:28.833949  [**] [1:1000004:1] b19dcat065-Hieu_snort phat hien bi tan cong TCP SNY Flood [**]
[Priority: 0] {TCP} 7.147.149.198:35660 -> 192.168.133.129:80
03/24-03:29:28.834000  [**] [1:1000004:1] b19dcat065-Hieu_snort phat hien bi tan cong TCP SNY Flood [**]
[Priority: 0] {TCP} 98.103.7.214:35661 -> 192.168.133.129:80
03/24-03:29:28.834014  [**] [1:1000004:1] b19dcat065-Hieu_snort phat hien bi tan cong TCP SNY Flood [**]
[Priority: 0] {TCP} 213.111.95.220:35662 -> 192.168.133.129:80
03/24-03:29:28.834132  [**] [1:1000004:1] b19dcat065-Hieu_snort phat hien bi tan cong TCP SNY Flood [**]
[Priority: 0] {TCP} 145.95.255.76:35665 -> 192.168.133.129:80
03/24-03:29:28.834152  [**] [1:1000004:1] b19dcat065-Hieu_snort phat hien bi tan cong TCP SNY Flood [**]
[Priority: 0] {TCP} 186.200.110.145:35666 -> 192.168.133.129:80
03/24-03:29:28.834333  [**] [1:1000004:1] b19dcat065-Hieu_snort phat hien bi tan cong TCP SNY Flood [**]
[Priority: 0] {TCP} 164.40.120.115:35667 -> 192.168.133.129:80
03/24-03:29:28.834353  [**] [1:1000004:1] b19dcat065-Hieu_snort phat hien bi tan cong TCP SNY Flood [**]
[Priority: 0] {TCP} 40.41.145.96:35668 -> 192.168.133.129:80
03/24-03:29:28.834395  [**] [1:1000004:1] b19dcat065-Hieu_snort phat hien bi tan cong TCP SNY Flood [**]
[Priority: 0] {TCP} 213.103.79.97:35669 -> 192.168.133.129:80
03/24-03:29:28.834406  [**] [1:1000004:1] b19dcat065-Hieu_snort phat hien bi tan cong TCP SNY Flood [**]
[Priority: 0] {TCP} 195.164.155.74:35670 -> 192.168.133.129:80
03/24-03:29:28.834461  [**] [1:1000004:1] b19dcat065-Hieu_snort phat hien bi tan cong TCP SNY Flood [**]
```

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 (hiển thị trên giao diện