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

Môn: Thực tập cơ sở

BÀI BÁO THỰC TẬP CƠ SỞ

Bài 6: Cài đặt cấu hình HIDS/NIDS

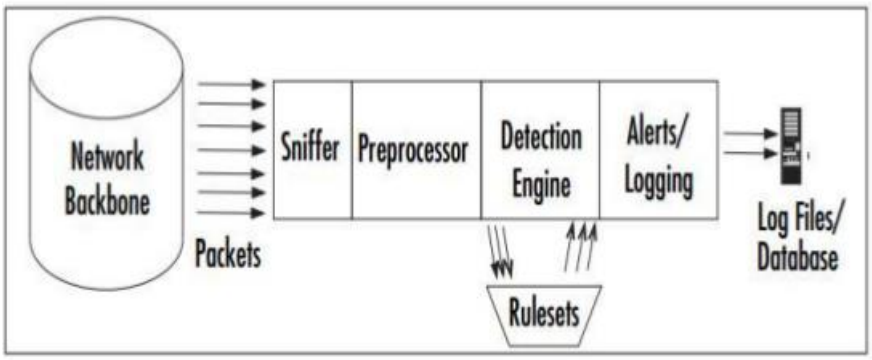
***Họ và tên giảng viên**: PGS.TS.Đỗ Xuân Chợ*
***Họ và tên:** Phạm Thanh Tùng*
***Mã sinh viên:** B20DCAT171*
***Lớp:** D20CQAT03-B*
***Số điện thoại:** 0856915668*

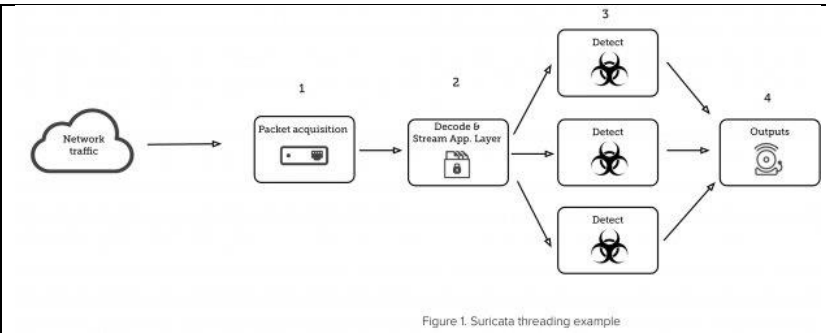
Hà Nội 2023

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(IDS):
  - Một phần mềm ứng dụng hoặc thiết bị được xây dựng để giám sát lưu lượng mạng, đồng thời cảnh báo mỗi khi có các hành vi bất thường xâm nhập vào hệ thống.
  - IDS sẽ thu thập dữ liệu, so sánh với các mẫu có sẵn của các cuộc tấn công và thông qua đó IDS sẽ xác định xem những hoạt động bất thường có phải là dấu hiệu của sự tấn công hay không.
- Phân loại các hệ thống:
  - **NIDS (Network Intrusion Detection System):** Hệ thống phát hiện xâm nhập mạng, hệ thống sẽ tập hợp các gói tin để phân tích sâu bên trong nhằm xác định các mối đe dọa tiềm tàng mà không làm thay đổi cấu trúc của gói tin.
  - **HIDS (Host-based Intrusion Detection System)** : Hệ thống phát hiện xâm nhập dựa trên máy chủ, được cài đặt trực tiếp trên các máy tính cần theo dõi. HIDS giám sát lưu lượng đến và đi từ thiết bị để cảnh báo người dùng về những xâm nhập trái phép.
- Phát hiện xâm nhập, các kỹ thuật phát hiện xâm nhập:
  - **Phát hiện dựa trên chữ ký (Signature-based intrusion detection)**: Đây là phương pháp được thiết kế để tìm ra những nguy hiểm tiềm tàng bằng cách so sánh dung lượng mạng và nhật ký dữ liệu với những mẫu tấn công có sẵn trong hệ thống.
  - **Phát hiện dựa trên sự bất thường (Anomaly-based intrusion detection) :** được thiết kế để xác định các cuộc tấn công không xác định, chẳng hạn như phần mềm độc hại mới và thích ứng với chúng ngay lập tức bằng cách sử dụng máy học.
- Một số hệ thống phát hiện tấn công :

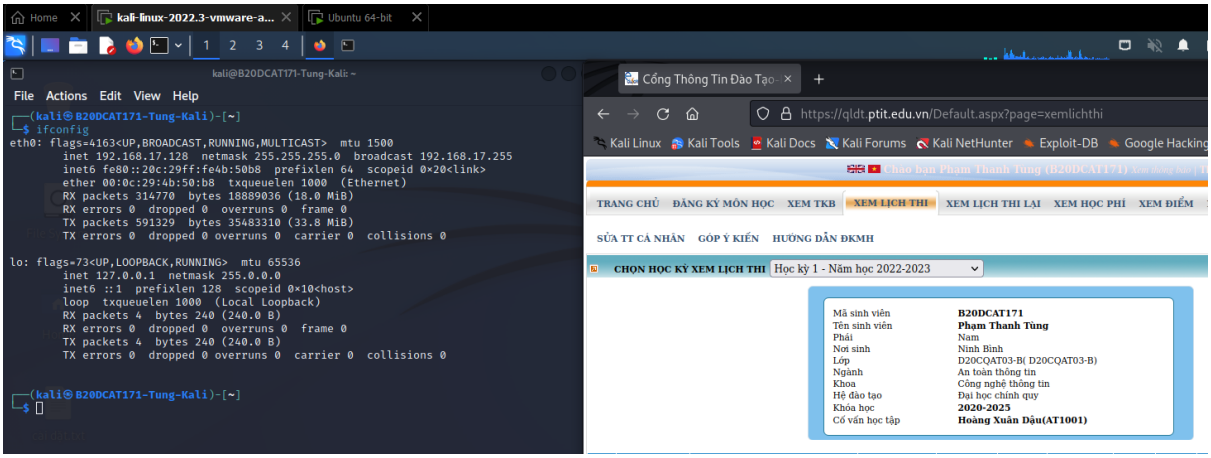
	Kiến trúc
Snort	

Suricata	 Figure 1. Suricata threading example

- Một số tài liệu tham khảo:
  - Chương 5, Giáo trình Cơ sở an toàn thông tin, Học viện Công nghệ BVCT, 2020
  - Snort: https://www.snort.org/#documents
  - Suricata: https://suricata.io/documentation/

2.2. Các bước thực hiện:

- Chuẩn bị các máy tính:
  - Máy Kali Linux:



  - Máy Linux cài đặt Snort

```
root@b20dcat171-Tung-Snort:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:39:ad:34 brd ff:ff:ff:ff:ff:ff
    inet 10.10.19.142/24 brd 10.10.19.255 scope global dynamic ens33
       valid_lft 1753sec preferred_lft 1753sec
    inet6 fe80::b4b:7ce6:31ed:e2e6/64 scope link
       valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:39:ad:3e brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.128/24 brd 192.168.100.255 scope global dynamic ens37
       valid_lft 1675sec preferred_lft 1675sec
    inet6 fe80::4472:450b:fdc0:1460/64 scope link
       valid_lft forever preferred_lft forever
```

- Tải, cài đặt Snort và chạy thử Snort.

```
root@ubuntu: ~
    link/ether 00:0c:29:39:ad:34 brd ff:ff:ff:ff:ff:ff
    inet 10.10.19.142/24 brd 10.10.19.255 scope global dynamic ens33
       valid_lft 1684sec preferred_lft 1684sec
    inet6 fe80::b4b:7ce6:31ed:e2e6/64 scope link
       valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 00:0c:29:39:ad:3e brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.128/24 brd 192.168.100.255 scope global dynamic ens37
       valid_lft 1546sec preferred_lft 1546sec
    inet6 fe80::4472:450b:fdc0:1460/64 scope link
       valid_lft forever preferred_lft forever
root@ubuntu:~# snort -V

   ,,_     -*> 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 1.7.4
           Using PCRE version: 8.38 2015-11-23
           Using ZLIB version: 1.2.8

root@ubuntu:~#
```

- Tạo các luật Snort để phát hiện 3 dạng rà quét, tấn công hệ thống:

```
 GNU nano 2.5.3                File: /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 -> any any (msg: "B20DCAT171-Tung-Snort phat hien co cac goi tin ping gui den";sid:10000001;rev:1;)
alert TCP any any -> any any (msg: "B20DCAT171-Tung-Snort phat hien dang bi tan cong SYN Flood";threshold: type both, $
alert TCP any any -> any 80 (msg: "B20DCAT171-Tung-Snort phat hien cac goi tin ra quet cong 80";sid:10000003;rev:3;)
```

- Từ máy Kali, sử dụng lệnh ping để ping máy Snort.

```
┌──(kali㉿B20DCAT171-Tung-Kali)-[~/Desktop]
└─$ ping 10.10.19.142
PING 10.10.19.142 (10.10.19.142) 56(84) bytes of data.
64 bytes from 10.10.19.142: icmp_seq=1 ttl=64 time=0.459 ms
64 bytes from 10.10.19.142: icmp_seq=2 ttl=64 time=0.547 ms
64 bytes from 10.10.19.142: icmp_seq=3 ttl=64 time=0.218 ms
64 bytes from 10.10.19.142: icmp_seq=4 ttl=64 time=0.785 ms
64 bytes from 10.10.19.142: icmp_seq=5 ttl=64 time=0.525 ms
64 bytes from 10.10.19.142: icmp_seq=6 ttl=64 time=0.693 ms
64 bytes from 10.10.19.142: icmp_seq=7 ttl=64 time=0.446 ms
^C
── 10.10.19.142 ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6087ms
rtt min/avg/max/mdev = 0.218/0.524/0.785/0.169 ms
```

```
root@b20dcat171-Tung-Snort:~# snort -A console -q -u snort -c /etc/snort/snort.c
onf -i ens33
05/18-19:27:36.153652  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 10.10.19.129 -> 10.10.19.142
05/18-19:27:36.153652  [**] [1:10000001:1] B20DCAT171-Tung-Snort phat hien co ca
c goi tin ping gui den [**] [Priority: 0] {ICMP} 10.10.19.129 -> 10.10.19.142
05/18-19:27:36.153652  [**] [1:384:5] ICMP PING [**] [Classification: Misc activ
ity] [Priority: 3] {ICMP} 10.10.19.129 -> 10.10.19.142
05/18-19:27:36.153688  [**] [1:10000001:1] B20DCAT171-Tung-Snort phat hien co ca
c goi tin ping gui den [**] [Priority: 0] {ICMP} 10.10.19.142 -> 10.10.19.129
05/18-19:27:37.175218  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 10.10.19.129 -> 10.10.19.142
05/18-19:27:37.175218  [**] [1:10000001:1] B20DCAT171-Tung-Snort phat hien co ca
c goi tin ping gui den [**] [Priority: 0] {ICMP} 10.10.19.129 -> 10.10.19.142
05/18-19:27:37.175218  [**] [1:384:5] ICMP PING [**] [Classification: Misc activ
ity] [Priority: 3] {ICMP} 10.10.19.129 -> 10.10.19.142
05/18-19:27:37.175247  [**] [1:10000001:1] B20DCAT171-Tung-Snort phat hien co ca
c goi tin ping gui den [**] [Priority: 0] {ICMP} 10.10.19.142 -> 10.10.19.129
05/18-19:27:38.199044  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 10.10.19.129 -> 10.10.19.142
```

- Từ máy Kali, sử dụng công cụ hping3 để tấn công TCP SYN Flood máy Snort

```
┌──(root㉿B20DCAT171-Tung-Kali)-[/home/kali/Desktop]
└─# hping3 -S --flood -a 10.10.19.129 10.10.19.142
HPING 10.10.19.142 (eth0 10.10.19.142): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.19.142 hping statistic ---
1570779 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
root@b20dcat171-Tung-Snort:~# snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33
05/18-19:37:46.961798  [**] [1:10000002:2] B20DCAT171-Tung-Snort phat hien dang bi tan cong SYN Flood [**]
[Priority: 0] {TCP} 10.10.19.129:2988 -> 10.10.19.142:0
05/18-19:38:06.000837  [**] [1:10000002:2] B20DCAT171-Tung-Snort phat hien dang bi tan cong SYN Flood [**]
[Priority: 0] {TCP} 10.10.19.129:65521 -> 10.10.19.142:0
05/18-19:38:26.000829  [**] [1:10000002:2] B20DCAT171-Tung-Snort phat hien dang bi tan cong SYN Flood [**]
[Priority: 0] {TCP} 10.10.19.129:42965 -> 10.10.19.142:0
05/18-19:38:46.000865  [**] [1:10000002:2] B20DCAT171-Tung-Snort phat hien dang bi tan cong SYN Flood [**]
[Priority: 0] {TCP} 10.10.19.129:27636 -> 10.10.19.142:0
05/18-19:39:06.000874  [**] [1:10000002:2] B20DCAT171-Tung-Snort phat hien dang bi tan cong SYN Flood [**]
[Priority: 0] {TCP} 10.10.19.129:2288 -> 10.10.19.142:0
05/18-19:39:26.000847  [**] [1:10000002:2] B20DCAT171-Tung-Snort phat hien dang bi tan cong SYN Flood [**]
[Priority: 0] {TCP} 10.10.19.129:32730 -> 10.10.19.142:0
05/18-19:39:46.000839  [**] [1:10000002:2] B20DCAT171-Tung-Snort phat hien dang bi tan cong SYN Flood [**]
[Priority: 0] {TCP} 10.10.19.129:30264 -> 10.10.19.142:0
05/18-19:40:06.001024  [**] [1:10000002:2] B20DCAT171-Tung-Snort phat hien dang bi tan cong SYN Flood [**]
[Priority: 0] {TCP} 10.10.19.129:4626 -> 10.10.19.142:0
^C*** Caught Int-Signal
```

Máy Kali gửi gói tin rà quét cho máy Snort

```
┌──(root㉿B20DCAT171-Tung-Kali)-[/home/kali/Desktop]
└─# nmap -sV -p80 10.10.19.142
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-18 22:42 EDT
Nmap scan report for 10.10.19.142
Host is up (0.00047s latency).

PORT   STATE  SERVICE VERSION
80/tcp closed http
MAC Address: 00:0C:29:39:AD:34 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

```
root@b20dcat171-Tung-Snort:~# snort -A console -q -i ens33 -c /etc/snort/snort.conf
05/18-19:43:07.888515  [**] [1:10000003:3] B20DCAT171-Tung-Snort phat hien cac goi tin ra quet cong 80 [**]
 [Priority: 0] {TCP} 10.10.19.129:33004 -> 10.10.19.142:80
05/18-19:43:18.928936  [**] [1:10000003:3] B20DCAT171-Tung-Snort phat hien cac goi tin ra quet cong 80 [**]
 [Priority: 0] {TCP} 10.10.19.129:43596 -> 10.10.19.142:80
05/18-19:43:20.897076  [**] [1:10000003:3] B20DCAT171-Tung-Snort phat hien cac goi tin ra quet cong 80 [**]
 [Priority: 0] {TCP} 10.10.19.129:59133 -> 10.10.19.142:80
05/18-19:43:25.480978  [**] [1:10000003:3] B20DCAT171-Tung-Snort phat hien cac goi tin ra quet cong 80 [**]
 [Priority: 0] {TCP} 10.10.19.129:46588 -> 10.10.19.142:80
05/18-19:43:26.949211  [**] [1:10000003:3] B20DCAT171-Tung-Snort phat hien cac goi tin ra quet cong 80 [**]
 [Priority: 0] {TCP} 10.10.19.129:55500 -> 10.10.19.142:80
05/18-19:43:35.281125  [**] [1:10000003:3] B20DCAT171-Tung-Snort phat hien cac goi tin ra quet cong 80 [**]
 [Priority: 0] {TCP} 10.10.19.129:45320 -> 10.10.19.142:80
05/18-19:43:36.709103  [**] [1:10000003:3] B20DCAT171-Tung-Snort phat hien cac goi tin ra quet cong 80 [**]
 [Priority: 0] {TCP} 10.10.19.129:44418 -> 10.10.19.142:80
05/18-19:43:40.505003  [**] [1:10000003:3] B20DCAT171-Tung-Snort phat hien cac goi tin ra quet cong 80 [**]
 [Priority: 0] {TCP} 10.10.19.129:48209 -> 10.10.19.142:80
05/18-19:43:43.885197  [**] [1:10000003:3] B20DCAT171-Tung-Snort phat hien cac goi tin ra quet cong 80 [**]
 [Priority: 0] {TCP} 10.10.19.129:61628 -> 10.10.19.142:80
```