

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BỘ MÔN THỰC TẬP CƠ SỞ



BÀI 6:
Cài đặt cấu hình
HIDS/NIDS

Giảng viên : Nguyễn Ngọc Diệp
Sinh viên : Nguyễn Đức Anh
Mã sinh viên : B21DCAT031
Hệ : Đại học chính quy

Hà Nội, 3/2024

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

a. Tìm hiểu khái quát về 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.

Các hệ thống phát hiện, ngăn chặn tấn công, xâm nhập (IDS/IPS) là một lớp phòng vệ quan trọng trong các lớp giải pháp đảm bảo an toàn cho hệ thống thông tin và mạng theo mô hình phòng thủ có chiều sâu (defence in depth). IDS (Intrusion Detection System) là hệ thống phát hiện tấn công, xâm nhập và IPS (Intrusion Prevention System) là hệ thống ngăn chặn tấn công, xâm nhập. Các hệ thống IDS/IPS có thể được đặt trước hoặc sau tường lửa trong mô hình mạng, tùy theo mục đích sử dụng. Hình 5.18 cung cấp vị trí các hệ thống IDS và IPS trong sơ đồ mạng, trong đó IDS thường được kết nối vào bộ switch phía sau tường lửa, còn IPS được ghép vào giữa đường truyền từ cổng mạng, phía sau tường lửa.

- Nhiệm vụ chính của các hệ thống IDS/IPS bao gồm:
 - Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập
 - Khi phát hiện các hành vi tấn công, xâm nhập, thì ghi logs các hành vi này cho phân tích bổ sung sau này
 - Ngăn chặn hoặc dừng các hành vi tấn công, xâm nhập
 - Gửi thông báo cho người quản trị về các hành vi tấn công, xâm nhập đã phát hiện được.
- Về cơ bản IPS và IDS giống nhau về chức năng giám sát lưu lượng mạng hoặc các sự kiện trong hệ thống. Tuy nhiên, IPS thường được đặt giữa đường truyền thông và có thể chủ động ngăn chặn các tấn công, xâm nhập bị phát hiện. Trong khi đó, IDS thường được kết nối vào các bộ định tuyến, switch, card mạng và chủ yếu làm nhiệm vụ giám sát và cảnh báo, không có khả năng chủ động ngăn chặn tấn công, xâm nhập.

Có 2 phương pháp phân loại chính các hệ thống IDS và IPS, gồm (1) phân loại theo nguồn dữ liệu và (2) phân loại theo phương pháp phân tích dữ liệu.

❖ Theo nguồn dữ liệu, có 2 loại hệ thống phát hiện xâm nhập:

- Hệ thống phát hiện xâm nhập mạng (NIDS – Network-based IDS): NIDS phân tích lưu lượng mạng để phát hiện tấn công, xâm nhập cho cả mạng hoặc một phần mạng.
- Hệ thống phát hiện xâm nhập cho host (HIDS – Host-based IDS): HIDS phân tích các sự kiện xảy ra trong hệ thống/dịch vụ để phát hiện tấn công, xâm nhập cho hệ thống đó. Hình 5.20 minh họa một sơ đồ mạng, trong đó sử dụng NIDS để giám sát lưu lượng tại cổng mạng và HIDS để giám sát các host thông qua các IDS agent. Một trạm quản lý (Management station) được thiết lập để thu nhập các thông tin từ các

NIDS và HIDS để xử lý và đưa ra quyết định cuối cùng.

❖ Theo phương pháp phân tích dữ liệu, có 2 kỹ thuật phân tích chính:

- Phát hiện xâm nhập dựa trên chữ ký, hoặc phát hiện sự lạm dụng (Signature-based / misuse intrusion detection)
- Phát hiện xâm nhập dựa trên các bất thường (Anomaly intrusion detection).

b. Tìm hiểu về kiến trúc và tính năng của một số hệ thống phát hiện tấn công, xâm nhập, như Snort, Suricata, Zeek, OSSEC, Wazuh...

- **Suricata**

Suricata là một công cụ Giám sát An ninh mạng, IPS và Network IDS hiệu suất cao. Nó là mã nguồn mở và được sở hữu bởi một tổ chức phi lợi nhuận do cộng đồng điều hành, Tổ chức Bảo mật Thông tin Mở (OISF). Suricata được phát triển bởi OISF.

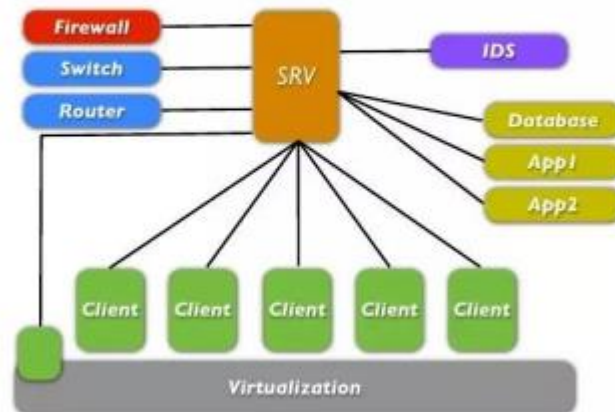
- **Zeek**

Zeek được trình bày như một công cụ để hỗ trợ quản lý ứng phó sự cố an ninh . Nó hoạt động bằng cách bổ sung dựa trên chữ ký các công cụ để tìm và theo dõi các sự kiện mạng phức tạp. Nó được đặc trưng bằng cách cung cấp phản hồi nhanh, ngoài việc sử dụng nhiều luồng và giao thức. Nó không chỉ giúp xác định các sự kiện bảo mật, mà còn nhằm mục đích tạo điều kiện khắc phục sự cố.

- **OSSEC**

OSSEC là hệ thống phát hiện xâm nhập dựa trên host (HIDS) dựa trên log mã nguồn mở, miễn phí, đa nền tảng có thể mở rộng và có nhiều cơ chế bảo mật khác nhau. OSSEC có thể phát hiện xâm nhập bằng cả chữ ký hoặc dấu hiệu bất thường. Các dấu hiệu bình thường và bất thường được mô tả trong bộ luật của OSSEC. OSSEC có một công cụ phân tích và tương quan mạnh mẽ, tích hợp giám sát và phân tích log, kiểm tra tính toàn vẹn của file, kiểm tra registry của Windows, thực thi chính sách tập trung, giám sát chính sách, phát hiện rootkit, cảnh báo thời gian thực và phản ứng một cách chủ động cuộc tấn công đang diễn ra. Các hành động này cũng có thể được định nghĩa trước bằng luật trong OSSEC để OSSEC hoạt động theo ý muốn của người quản trị. Ngoài việc được triển khai như một HIDS, nó thường được sử dụng như một công cụ phân tích log, theo dõi và phân tích các bản ghi lại, IDS, các máy chủ Web và các bản ghi xác thực. OSSEC chạy trên hầu hết các hệ điều hành, bao gồm Linux, OpenBSD, FreeBSD, Mac OS X, Sun Solaris và Microsoft Windows. OSSEC còn có thể được tích hợp trong các hệ thống bảo mật lớn hơn là SIEM (Security information and event management). OSSEC chỉ có thể cài đặt trên Windows với tư cách là một agent.

OSSEC Architecture



• Wazuh

Wazuh là nền tảng mã nguồn mở hợp nhất của XDR và SIEM. Nó miễn phí và có hơn 10 triệu lượt tải xuống hàng năm. Wazuh có các agent được triển khai trên các endpoint cần giám sát. Agent sẽ thu thập dữ liệu sự kiện bảo mật (security event) từ các endpoint được giám sát và chuyển tiếp chúng đến máy chủ Wazuh để phân tích log, phân tích tương quan và đưa ra cảnh báo.

Wazuh có sẵn một số mô-đun giúp nâng cao tình hình bảo mật tổng thể của một tổ chức. Dưới đây là một số mô-đun Wazuh có liên quan.

- Kiểm kê hệ thống (System inventory)
- Phát hiện lỗ hổng bảo mật (Vulnerability detector)
- Đánh giá cấu hình bảo mật (SCA)
- Phát hiện và ứng phó với mối đe dọa

2.2 Tài liệu tham khảo

- Chương 5, Giáo trình Cơ sở an toàn thông tin, Học viện Công nghệ BVCT, 2020.

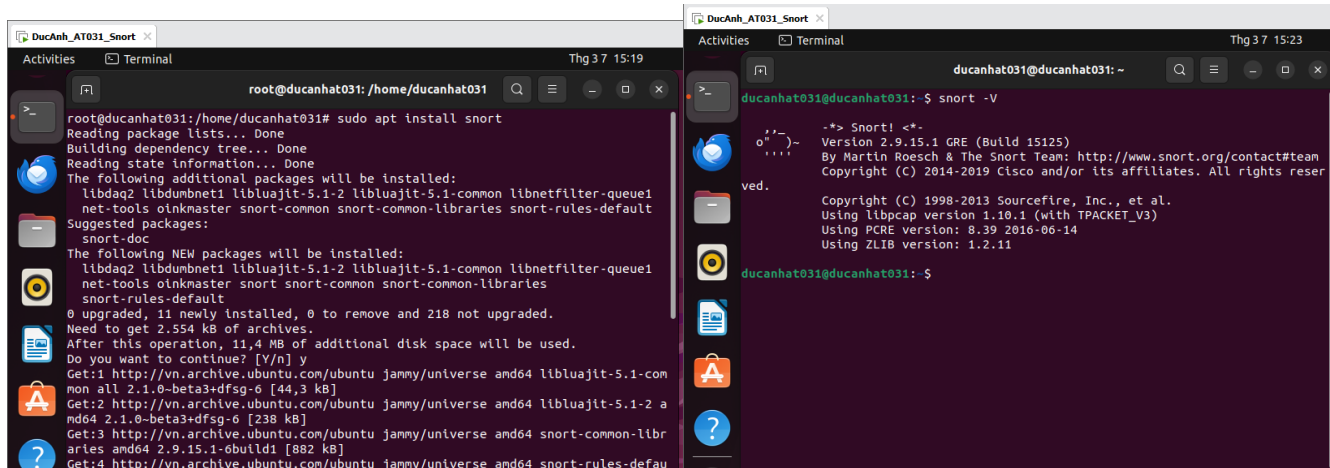
2.3 Chuẩn bị môi trường

- 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>

2.4 Các bước thực hiện

Bước 1: Chuẩn bị các máy ảo

Bước 2: Cài đặt Snort trên Ubuntu. Sau đó kiểm tra phiên bản Snort.

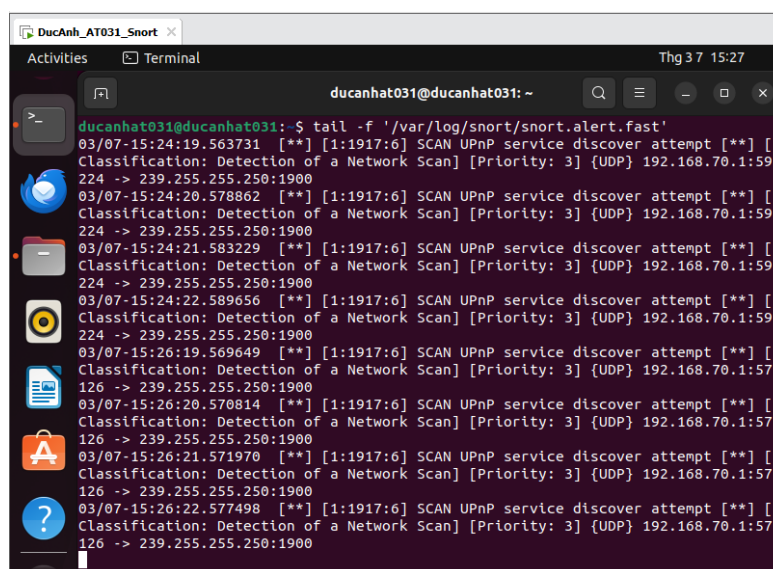


```
root@ducanhat031: /home/ducanhat031# sudo apt install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libdaq2 libdumbnet1 liblua5.1-2 liblua5.1-common libnetfilter-queue1
net-tools oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
snort-doc
The following NEW packages will be installed:
libdaq2 libdumbnet1 liblua5.1-2 liblua5.1-common libnetfilter-queue1
net-tools oinkmaster snort snort-common snort-common-libraries
snort-rules-default
0 upgraded, 11 newly installed, 0 to remove and 218 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] y
Get:1 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 liblua5.1-com
mon all 2.1.0-beta3+dfsg-6 [44,3 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 liblua5.1-2 a
md64 2.1.0-beta3+dfsg-6 [238 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 snort-commo
n-libraries amd64 2.9.15.1-6build1 [882 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 snort-rules-defau
```

```
ducanhat031@ducanhat031: ~$ snort -V
-*> 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
ducanhat031@ducanhat031: ~$
```

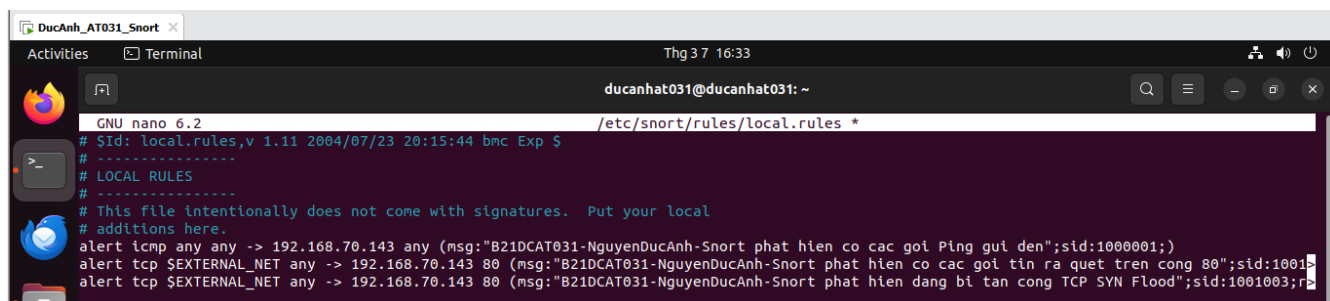
Kiểm tra log của Snort để đảm bảo Snort hoạt động bình thường.



```
ducanhat031@ducanhat031: ~$ tail -f /var/log/snort/snort.alert.fast
03/07-15:24:19.563731  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:59
224 -> 239.255.255.250:1900
03/07-15:24:20.578862  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:59
224 -> 239.255.255.250:1900
03/07-15:24:21.583229  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:59
224 -> 239.255.255.250:1900
03/07-15:24:22.589656  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:59
224 -> 239.255.255.250:1900
03/07-15:26:19.569649  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:57
126 -> 239.255.255.250:1900
03/07-15:26:20.570814  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:57
126 -> 239.255.255.250:1900
03/07-15:26:21.571970  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:57
126 -> 239.255.255.250:1900
03/07-15:26:22.577498  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:57
126 -> 239.255.255.250:1900
```

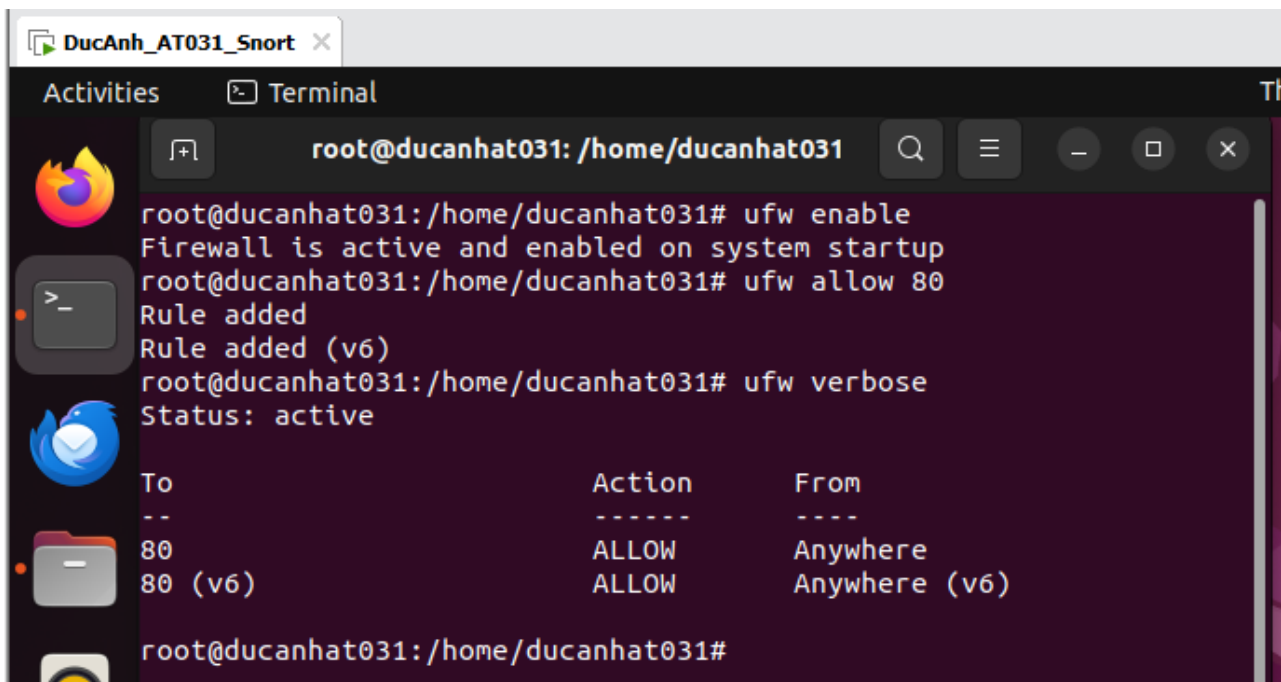
Bước 3: Thêm các luật Snort để phát hiện 3 dạng rà quét, tấn công hệ thống:

- Phát hiện các gói tin ping từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiển thị thông điệp khi phát hiện.
- 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
- 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



```
ducanhat031@ducanhat031: ~$ nano /etc/snort/rules/local.rules
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 -> 192.168.70.143 any (msg:"B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi Ping gui den";sid:1000001;)
alert tcp $EXTERNAL_NET any -> 192.168.70.143 80 (msg:"B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi tin ra quet tren cong 80";sid:1001001;)
alert tcp $EXTERNAL_NET any -> 192.168.70.143 80 (msg:"B21DCAT031-NguyenDucAnh-Snort phat hien dang bi tan cong TCP SYN Flood";sid:1001003;)
```

Để có thể nhận được gói tin, ta tiến hành cho phép gói tin vượt tường lửa



A terminal window titled "DucAnh_AT031_Snort" showing the configuration of the UFW firewall. The user is root at ducanhhat031. The commands and output are as follows:

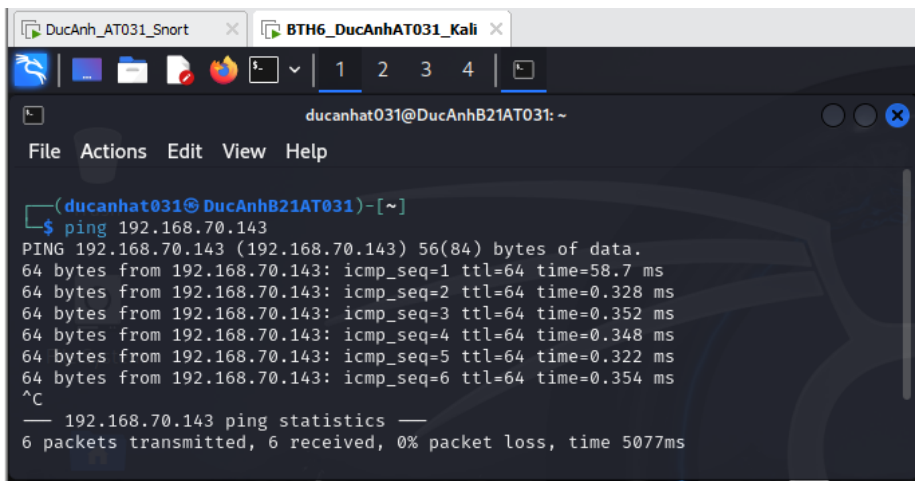
```
root@ducanhhat031:/home/ducanhhat031# ufw enable
Firewall is active and enabled on system startup
root@ducanhhat031:/home/ducanhhat031# ufw allow 80
Rule added
Rule added (v6)
root@ducanhhat031:/home/ducanhhat031# ufw verbose
Status: active
```

To	Action	From
--	-----	----
80	ALLOW	Anywhere
80 (v6)	ALLOW	Anywhere (v6)

```
root@ducanhhat031:/home/ducanhhat031#
```

Bước 4: Thực thi tấn công và phát hiện sử dụng Snort

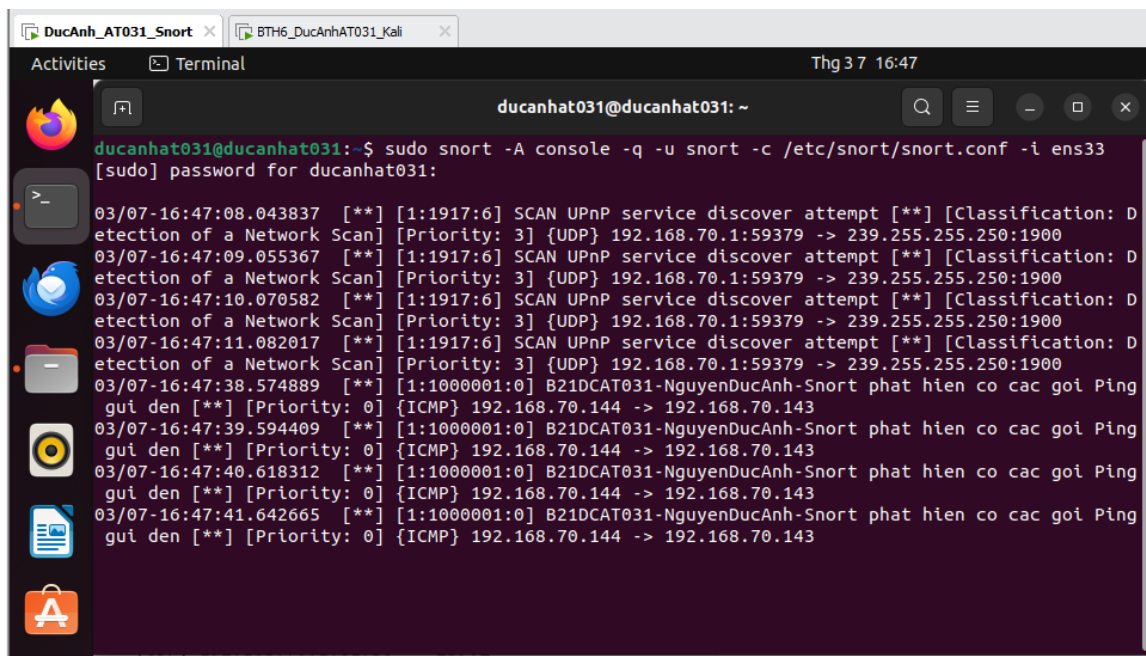
Từ máy Kali tiến hành sử dụng lệnh ping 192.168.70.143 để ping máy Snort



A terminal window titled "BTH6_DucAnhAT031_Kali" showing a ping command being executed from a Kali machine to the Snort machine. The user is ducanhhat031 at DucAnhB21AT031. The output is as follows:

```
(ducanhhat031@DucAnhB21AT031)-[~]
$ ping 192.168.70.143
PING 192.168.70.143 (192.168.70.143) 56(84) bytes of data:
64 bytes from 192.168.70.143: icmp_seq=1 ttl=64 time=58.7 ms
64 bytes from 192.168.70.143: icmp_seq=2 ttl=64 time=0.328 ms
64 bytes from 192.168.70.143: icmp_seq=3 ttl=64 time=0.352 ms
64 bytes from 192.168.70.143: icmp_seq=4 ttl=64 time=0.348 ms
64 bytes from 192.168.70.143: icmp_seq=5 ttl=64 time=0.322 ms
64 bytes from 192.168.70.143: icmp_seq=6 ttl=64 time=0.354 ms
^C
 192.168.70.143 ping statistics —
 6 packets transmitted, 6 received, 0% packet loss, time 5077ms
```

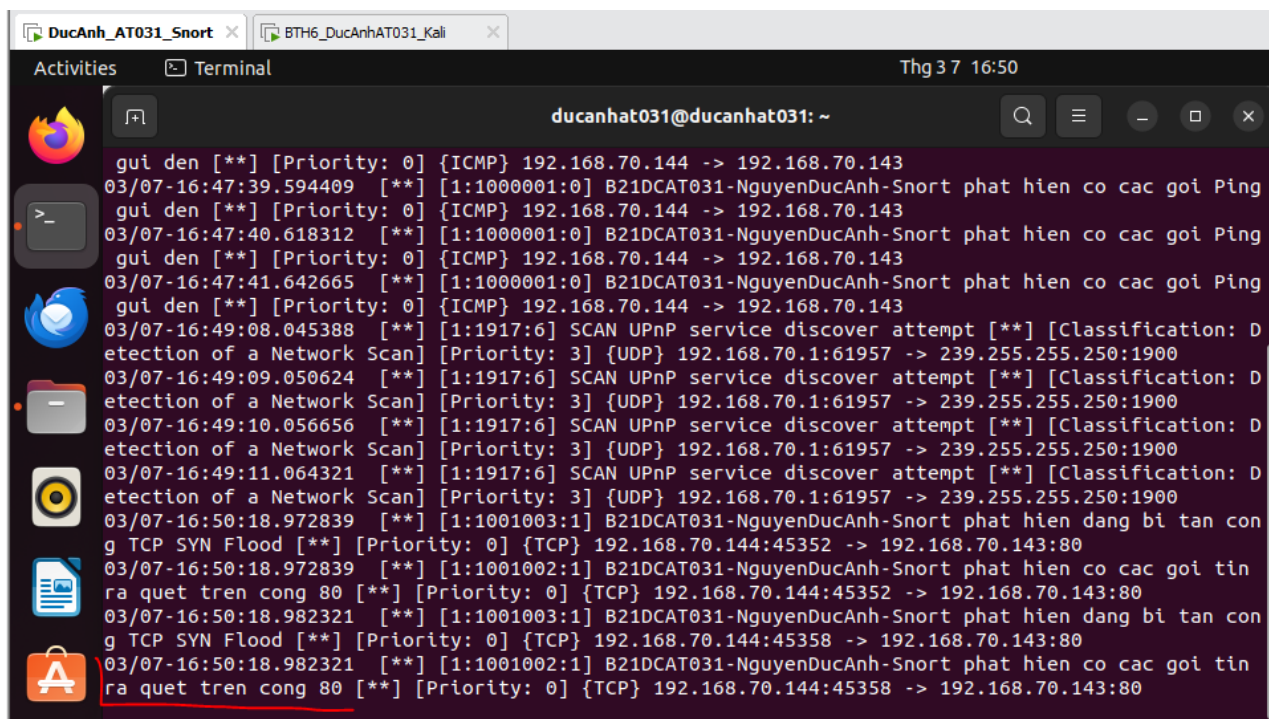
Xem kết quả trên máy Snort. Phát hiện có cảnh báo.



```
ducanhat031@ducanhat031:~$ sudo snort -A console -q -u snort -c /etc/snort/snort.conf -i ens33
[sudo] password for ducanhat031:
03/07-16:47:08.043837 03/07-16:47:09.055367 03/07-16:47:10.070582 03/07-16:47:11.082017 03/07-16:47:38.574889 03/07-16:47:39.594409 03/07-16:47:40.618312 03/07-16:47:41.642665
[**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:59379 -> 239.255.255.250:1900
[**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:59379 -> 239.255.255.250:1900
[**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:59379 -> 239.255.255.250:1900
[**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:59379 -> 239.255.255.250:1900
[**] [1:1000001:0] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi Ping gui den [**] [Priority: 0] {ICMP} 192.168.70.144 -> 192.168.70.143
[**] [1:1000001:0] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi Ping gui den [**] [Priority: 0] {ICMP} 192.168.70.144 -> 192.168.70.143
[**] [1:1000001:0] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi Ping gui den [**] [Priority: 0] {ICMP} 192.168.70.144 -> 192.168.70.143
[**] [1:1000001:0] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi Ping gui den [**] [Priority: 0] {ICMP} 192.168.70.144 -> 192.168.70.143
```

Từ máy Kali, sử dụng công cụ nmap để rà quét máy Snort (dùng lệnh: `nmap -sV -p80 -A 192.168.70.143`)

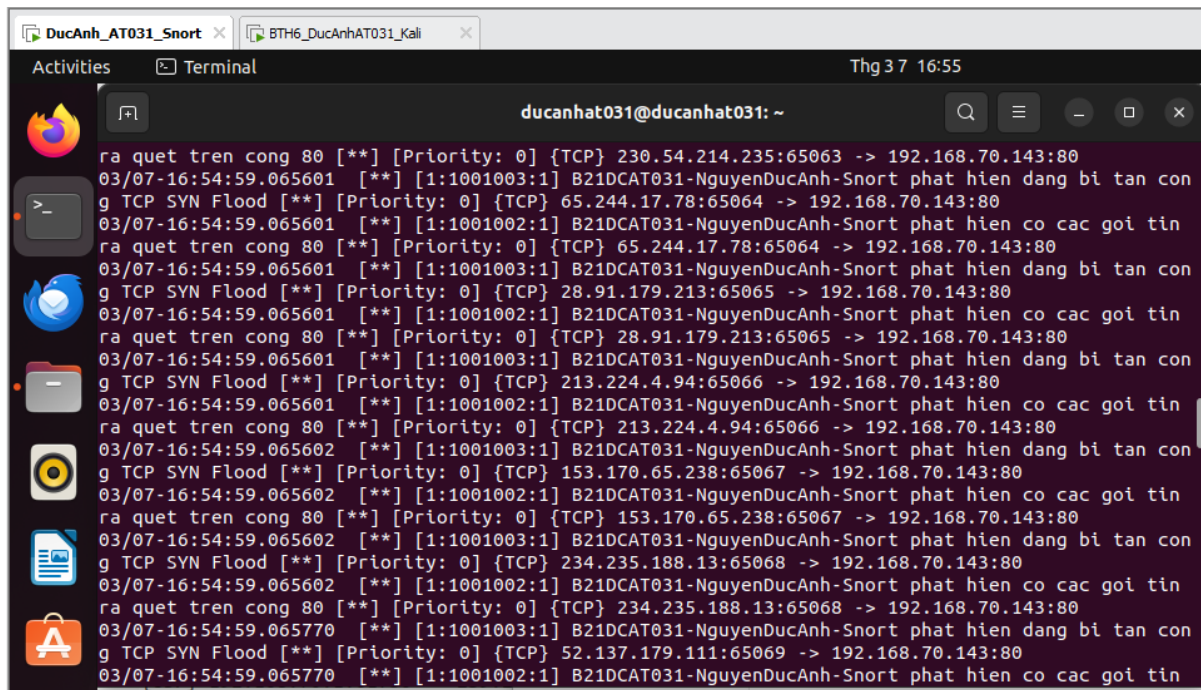
Trên máy Snort kiểm tra kết quả phát hiện có cảnh báo.



```
gui den [**] [Priority: 0] {ICMP} 192.168.70.144 -> 192.168.70.143
03/07-16:47:39.594409 03/07-16:47:40.618312 03/07-16:47:41.642665 03/07-16:49:08.045388 03/07-16:49:09.050624 03/07-16:49:10.056656 03/07-16:49:11.064321 03/07-16:50:18.972839 03/07-16:50:18.972839 03/07-16:50:18.982321 03/07-16:50:18.982321 03/07-16:50:18.982321
[**] [1:1000001:0] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi Ping gui den [**] [Priority: 0] {ICMP} 192.168.70.144 -> 192.168.70.143
[**] [1:1000001:0] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi Ping gui den [**] [Priority: 0] {ICMP} 192.168.70.144 -> 192.168.70.143
[**] [1:1000001:0] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi Ping gui den [**] [Priority: 0] {ICMP} 192.168.70.144 -> 192.168.70.143
[**] [1:1000001:0] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi Ping gui den [**] [Priority: 0] {ICMP} 192.168.70.144 -> 192.168.70.143
[**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:61957 -> 239.255.255.250:1900
[**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:61957 -> 239.255.255.250:1900
[**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:61957 -> 239.255.255.250:1900
[**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.70.1:61957 -> 239.255.255.250:1900
[**] [1:1001003:1] B21DCAT031-NguyenDucAnh-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 192.168.70.144:45352 -> 192.168.70.143:80
[**] [1:1001002:1] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi tin ra quet tren cong 80 [**] [Priority: 0] {TCP} 192.168.70.144:45352 -> 192.168.70.143:80
[**] [1:1001003:1] B21DCAT031-NguyenDucAnh-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 192.168.70.144:45358 -> 192.168.70.143:80
[**] [1:1001002:1] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi tin ra quet tren cong 80 [**] [Priority: 0] {TCP} 192.168.70.144:45358 -> 192.168.70.143:80
```

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 192.168.70.143`)

Trên máy Snort phát hiện có cảnh báo.



```
ducanh031@ducanh031: ~
ra quet tren cong 80 [**] [Priority: 0] {TCP} 230.54.214.235:65063 -> 192.168.70.143:80
03/07-16:54:59.065601 [**] [1:1001003:1] B21DCAT031-NguyenDucAnh-Snort phat hien dang bi tan con
g TCP SYN Flood [**] [Priority: 0] {TCP} 65.244.17.78:65064 -> 192.168.70.143:80
03/07-16:54:59.065601 [**] [1:1001002:1] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi tin
ra quet tren cong 80 [**] [Priority: 0] {TCP} 65.244.17.78:65064 -> 192.168.70.143:80
03/07-16:54:59.065601 [**] [1:1001003:1] B21DCAT031-NguyenDucAnh-Snort phat hien dang bi tan con
g TCP SYN Flood [**] [Priority: 0] {TCP} 28.91.179.213:65065 -> 192.168.70.143:80
03/07-16:54:59.065601 [**] [1:1001002:1] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi tin
ra quet tren cong 80 [**] [Priority: 0] {TCP} 28.91.179.213:65065 -> 192.168.70.143:80
03/07-16:54:59.065601 [**] [1:1001003:1] B21DCAT031-NguyenDucAnh-Snort phat hien dang bi tan con
g TCP SYN Flood [**] [Priority: 0] {TCP} 213.224.4.94:65066 -> 192.168.70.143:80
03/07-16:54:59.065601 [**] [1:1001002:1] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi tin
ra quet tren cong 80 [**] [Priority: 0] {TCP} 213.224.4.94:65066 -> 192.168.70.143:80
03/07-16:54:59.065602 [**] [1:1001003:1] B21DCAT031-NguyenDucAnh-Snort phat hien dang bi tan con
g TCP SYN Flood [**] [Priority: 0] {TCP} 153.170.65.238:65067 -> 192.168.70.143:80
03/07-16:54:59.065602 [**] [1:1001002:1] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi tin
ra quet tren cong 80 [**] [Priority: 0] {TCP} 153.170.65.238:65067 -> 192.168.70.143:80
03/07-16:54:59.065602 [**] [1:1001003:1] B21DCAT031-NguyenDucAnh-Snort phat hien dang bi tan con
g TCP SYN Flood [**] [Priority: 0] {TCP} 234.235.188.13:65068 -> 192.168.70.143:80
03/07-16:54:59.065602 [**] [1:1001002:1] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi tin
ra quet tren cong 80 [**] [Priority: 0] {TCP} 234.235.188.13:65068 -> 192.168.70.143:80
03/07-16:54:59.065770 [**] [1:1001003:1] B21DCAT031-NguyenDucAnh-Snort phat hien dang bi tan con
g TCP SYN Flood [**] [Priority: 0] {TCP} 52.137.179.111:65069 -> 192.168.70.143:80
03/07-16:54:59.065770 [**] [1:1001002:1] B21DCAT031-NguyenDucAnh-Snort phat hien co cac goi tin
```

3. 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)