

Bài thực hành: Phát hiện xâm nhập mạng với Snort

Mục đích:

- Bài thực hành này giới thiệu việc sử dụng hệ thống Snort để cung cấp khả năng phát hiện xâm nhập trong môi trường Linux.

Yêu cầu đối với sinh viên:

- Sinh viên có hiểu biết cơ bản về cấu trúc luật của Snort và cơ chế hoạt động của IDS.
- Sinh viên phải có kiến thức cơ bản về dòng lệnh Linux.
- Sinh viên có khả năng sử dụng và đọc các thông tin thu được từ tcpdump.

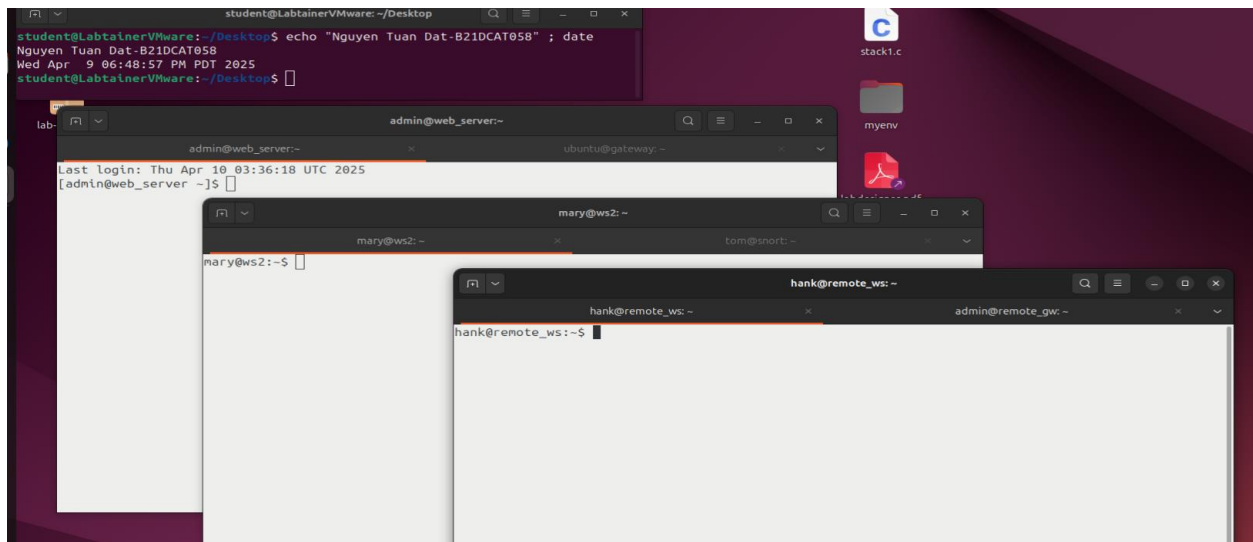
Nội dung thực hành:

- Khởi động bài lab: Trên terminal, gõ lệnh:

labtainer snort

(chú ý: sinh viên sử dụng email *stu.ptit.edu.vn* của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

- Sau khi khởi động, bài lab xuất hiện 6 containers, mỗi container là một máy tính ảo chạy hệ điều hành linux gồm một máy làm máy chủ, một máy làm việc trong mạng nội bộ, một máy làm việc từ xa, hai máy làm gateway, một máy cài Snort để phát cảnh báo.



- Sơ đồ mạng của bài thực hành:

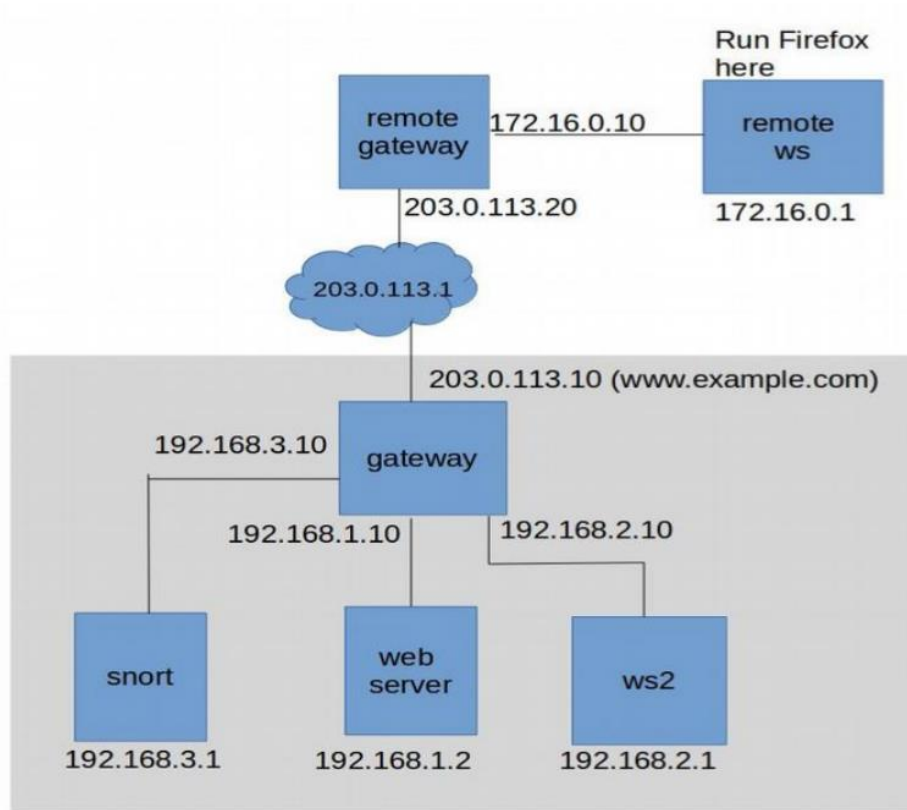
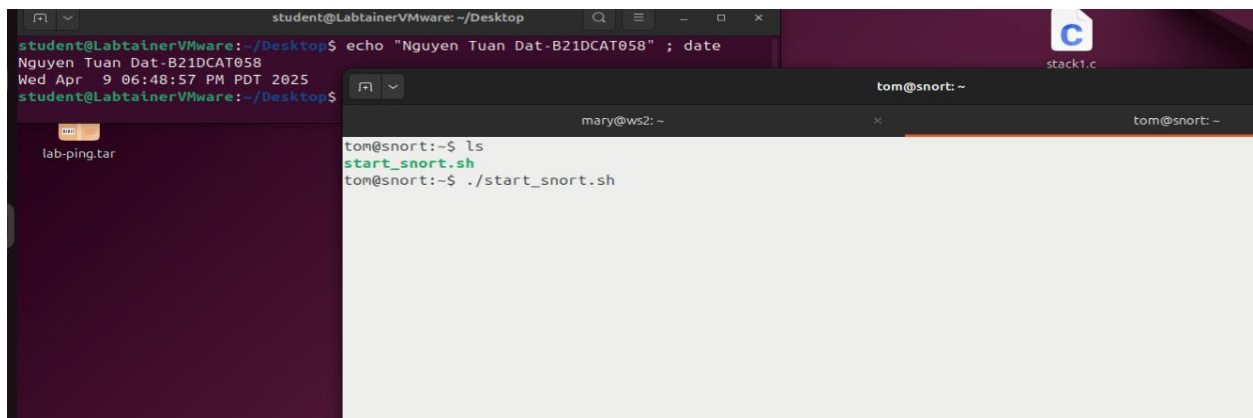


Figure 1: Network topology for the snort lab

- Khởi động snort trên máy “snort” để theo dõi lưu lượng mạng:

`./start_snort.sh`



- Để xem ví dụ về một số quy tắc được cấu hình sẵn, thực hiện quét nmap của `www.example.com` từ máy trạm từ xa:

`sudo nmap www.example.com`

The screenshot shows a multi-terminal environment. The top terminal window displays the output of `start_snort.sh`, showing various ICMP and SNMP traffic. The bottom-right terminal window shows the output of `sudo nmap www.example.com` executed on a remote host, displaying the scan results for `www.example.com` (203.0.113.10), including open ports (22/tcp, 53/tcp, 80/tcp, 443/tcp) and their corresponding services (ssh, domain, http, https).

- Tạm dừng snort. Thêm luật sau vào file `local.rules`, khởi động lại snort và chạy lại bước 2 để theo dõi kết quả trên máy “snort”:

`alert tcp any any -> any any (msg:"TCP detected"; sid:00002;)`

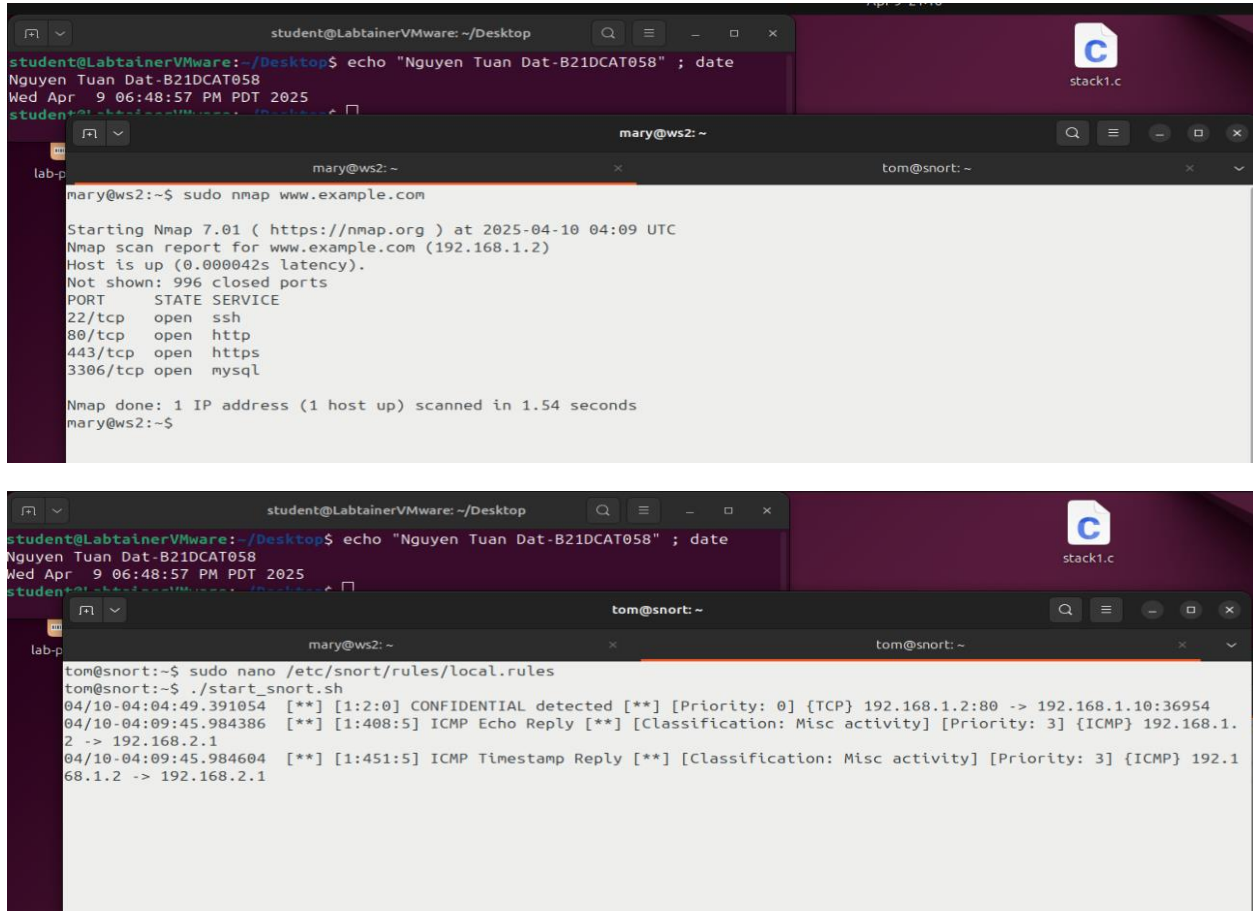
The screenshot shows a terminal window with the `GNU nano 2.5.3` editor open, editing the file `/etc/snort/rules/local.rules`. The rule `alert tcp any any -> any any (msg:"TCP detected"; sid:00002;)` has been added to the `LOCAL RULES` section.

Khởi động lại snort và Truy cập `www.example.com` bằng Firefox (trên remote) để thấy Snort "spam" cảnh báo TCP.

Theo dõi traffic nội bộ (ws2/mary)

Trên ws2:

`sudo nmap www.example.com`



The first screenshot shows a terminal window with the command `sudo nmap www.example.com` being executed. The output displays the Nmap scan results for www.example.com (192.168.1.2), showing that the host is up and listing open ports: 22/tcp (ssh), 80/tcp (http), 443/tcp (https), and 3306/tcp (mysql).

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr  9 06:48:57 PM PDT 2025
student@LabtainerVMware:~/Desktop$ sudo nmap www.example.com

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-10 04:09 UTC
Nmap scan report for www.example.com (192.168.1.2)
Host is up (0.000042s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp   open  mysql

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
mary@ws2:~$
```

The second screenshot shows the same terminal window with the command `sudo nano /etc/snort/rules/local.rules` being executed. The output displays the Snort logs, showing three detected events: a CONFIDENTIAL detected event, an ICMP Echo Reply event, and an ICMP Timestamp Reply event.

```
student@LabtainerVMware:~/Desktop
student@LabtainerVMware:~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr  9 06:48:57 PM PDT 2025
student@LabtainerVMware:~/Desktop$ sudo nano /etc/snort/rules/local.rules
tom@snort:~$ ./start_snort.sh
04/10-04:04:49.391054  [**] [1:2:0] CONFIDENTIAL detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.168.1.10:36954
04/10-04:09:45.984386  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
04/10-04:09:45.984604  [**] [1:451:5] ICMP Timestamp Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
```

Có thể **không thấy cảnh báo** vì gateway chưa chuyển tiếp traffic từ lan2

Vào container **gateway**, sửa:

`sudo nano /etc/rc.local`

thêm dòng :

`iptables -t mangle -A PREROUTING -i lan2 -j TEE --gateway 192.168.3.1`

và chạy lại : `sudo /etc/rc.local`

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware: ~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr  9 06:48:57 PM PDT 2025
student@LabtainerVMware: ~/Desktop$

lab-p tom@snort:~$ sudo
tom@snort:~$ ./st
04/10-04:04:49.39
04/10-04:09:45.98
2 -> 192.168.2.1
04/10-04:09:45.98
68.1.2 -> 192.168

ubuntu@gateway:~$
admin@web_server:~$
ubuntu@gateway:~$

GNU nano 2.5.3 File: /etc/rc.local Modified
#!/bin/bash
route delete default
route add default gw 203.0.113.1
# get ethernet device names for the two lans and the wan interfaces
lan1=$(ifconfig | grep -B1 "inet addr:192.168.1.10" | awk '$1!="inet" && $1!=="-' {print $1}')
lan2=$(ifconfig | grep -B1 "inet addr:192.168.2.10" | awk '$1!="inet" && $1!=="-' {print $1}')
wan=$(ifconfig | grep -B1 "inet addr:203.0.113.10" | awk '$1!="inet" && $1!=="-' {print $1}')
# flush and delete all chains
#
iptables --flush
iptables -t nat --flush
iptables -t mangle --flush
iptables --delete-chain
iptables -t nat --delete-chain
iptables -t mangle --delete-chain
iptables -t mangle -A PREROUTING -i lan2 -j TEE --gateway 192.168.3.1
# mirror incoming wan traffic to snort
iptables -t mangle -A PREROUTING -i $wan -j TEE --gateway 192.168.3.1
iptables -t mangle -A PREROUTING -i $lan1 -j TEE --gateway 192.168.3.1
# Define NAT for traffic from LANs to the WAN
#
iptables --table nat -I POSTROUTING 1 -o out-interface $wan -j MASQUERADE
^G Get Help ^O Write Out ^K Where Is ^K Cut Text ^J Justify ^C Cur Pos ^V Prev Page
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Linter ^_ Go To Line ^W Next Page
```

Trên ws2, chạy lại nmap để xem Snort đã bắt được chưa:

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware: ~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr  9 06:48:57 PM PDT 2025
student@LabtainerVMware: ~/Desktop$

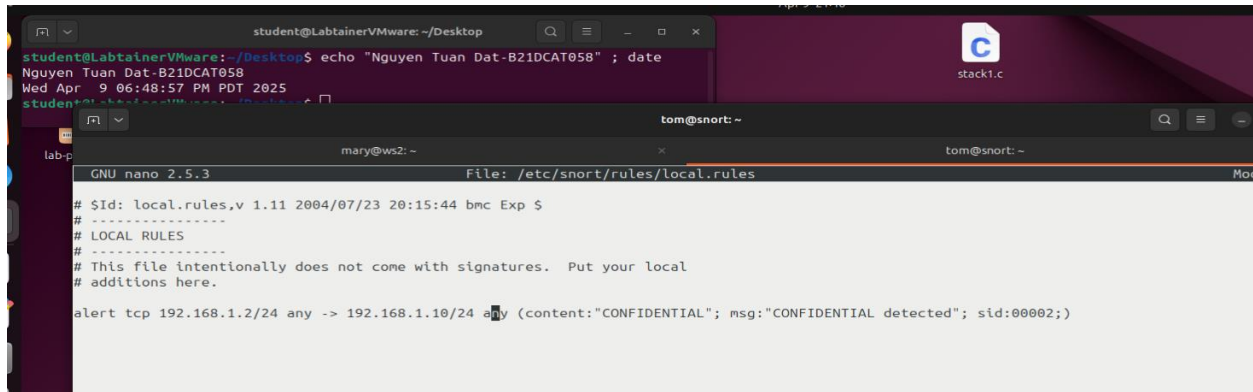
lab-p mary@ws2:~$ sudo nmap www.example.com
mary@ws2:~$
Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-10 04:14 UTC
Nmap scan report for www.example.com (192.168.1.2)
Host is up (0.000046s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp   open  mysql
Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
mary@ws2:~$
```

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware: ~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr  9 06:48:57 PM PDT 2025
student@LabtainerVMware: ~/Desktop$

lab-p tom@snort:~$ ./start_snort.sh
04/10-04:20:22.176214 [**] [1:469:3] ICMP_PING_NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] [ICMP] 192.168.2.1 -> 192.168.1.2
04/10-04:20:22.176214 [**] [1:384:5] ICMP_PING [**] [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.2.1 -> 192.168.2.1
04/10-04:20:22.176243 [**] [1:408:5] ICMP_Echo_Reply [**] [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.2 -> 192.168.2.1
04/10-04:20:22.176442 [**] [1:453:5] ICMP_Timestamp_Request [**] [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.2.1 -> 192.168.1.2
04/10-04:20:22.176459 [**] [1:451:5] ICMP_Timestamp_Reply [**] [Classification: Misc activity] [Priority: 3] [ICMP] 192.168.1.2 -> 192.168.2.1
04/10-04:20:23.552005 [**] [1:1421:11] SNMP_AgentX_tcp_request [**] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.2.1:46714 -> 192.168.1.2:705
04/10-04:20:23.584918 [**] [1:1418:11] SNMP_request_tcp [**] [Classification: Attempted Information Leak] [Priority: 2] [TCP] 192.168.2.1:46714 -> 192.168.1.2:161
```


Phân biệt nội bộ và bên ngoài truy cập **plan.html**

Sửa local.rules

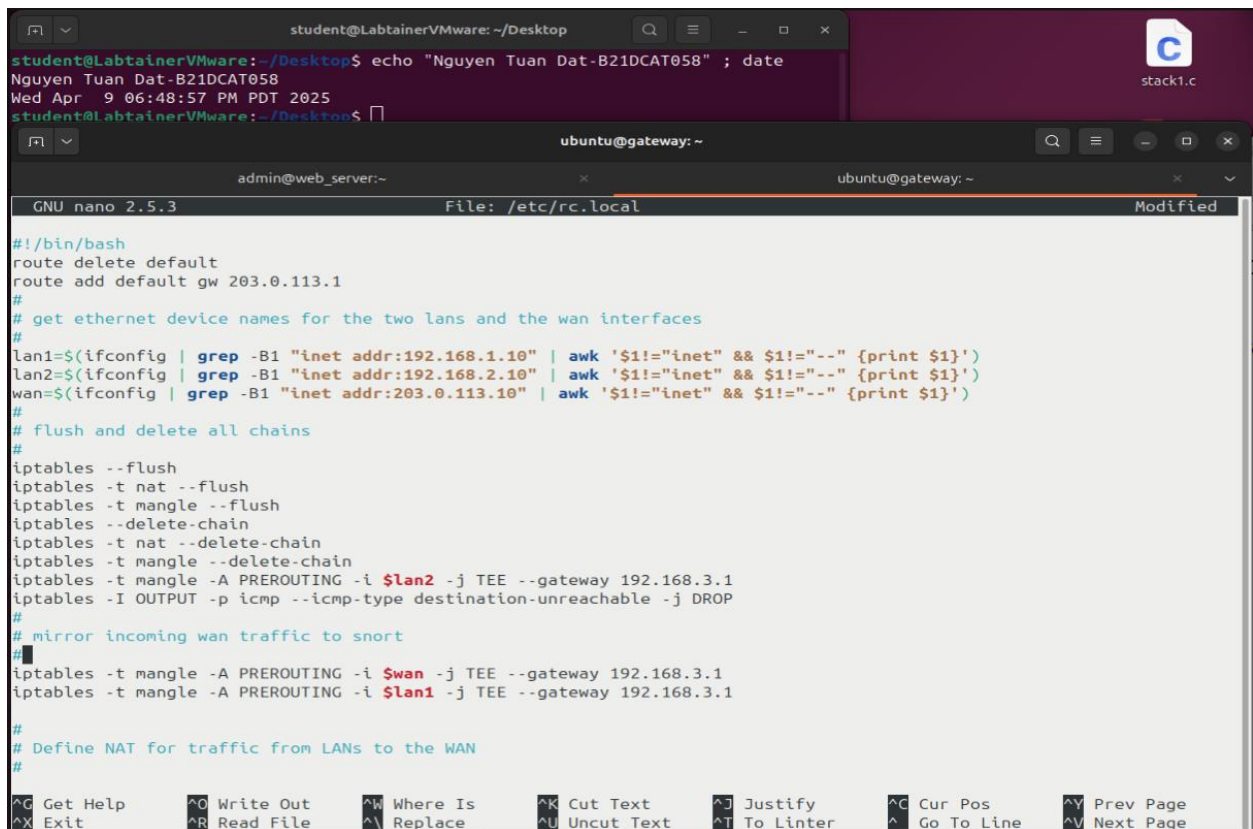


```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr  9 06:48:57 PM PDT 2025
student@LabtainerVMware:~/Desktop$

tom@snort: ~
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 tcp 192.168.1.2/24 any -> 192.168.1.10/24 any (content:"CONFIDENTIAL"; msg:"CONFIDENTIAL detected"; sid:00002;)
```

Sửa file rc.local

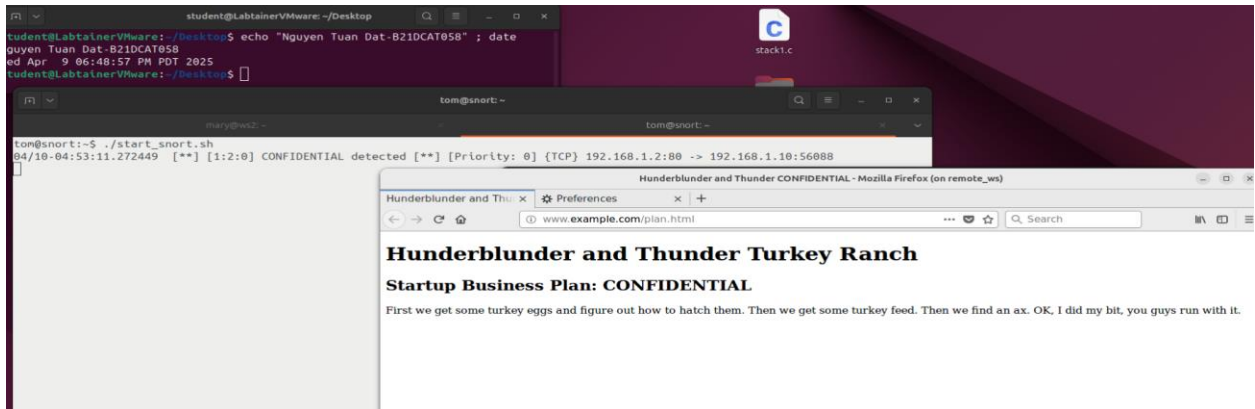


```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr  9 06:48:57 PM PDT 2025
student@LabtainerVMware:~/Desktop$

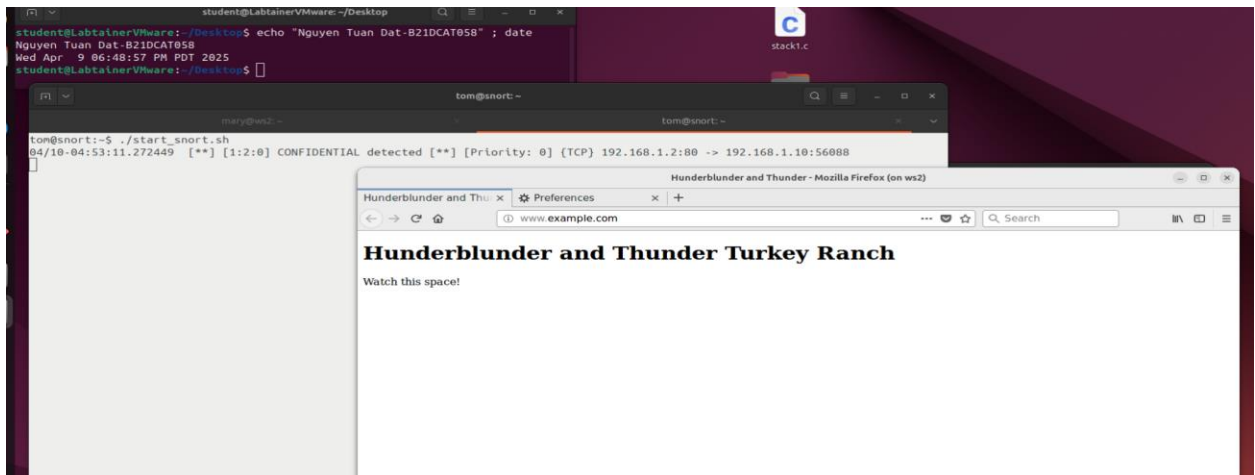
ubuntu@gateway: ~
admin@web_server:~
ubuntu@gateway: ~
GNU nano 2.5.3 File: /etc/rc.local Modified
#!/bin/bash
route delete default
route add default gw 203.0.113.1
#
# get ethernet device names for the two lans and the wan interfaces
#
lan1=$(ifconfig | grep -B1 "inet addr:192.168.1.10" | awk '{ $1!="inet" && $1!="--" {print $1}}')
lan2=$(ifconfig | grep -B1 "inet addr:192.168.2.10" | awk '{ $1!="inet" && $1!="--" {print $1}}')
wan=$(ifconfig | grep -B1 "inet addr:203.0.113.10" | awk '{ $1!="inet" && $1!="--" {print $1}}')
#
# flush and delete all chains
#
iptables --flush
iptables -t nat --flush
iptables -t mangle --flush
iptables --delete-chain
iptables -t nat --delete-chain
iptables -t mangle --delete-chain
iptables -t mangle -A PREROUTING -i $lan2 -j TEE --gateway 192.168.3.1
iptables -I OUTPUT -p icmp --icmp-type destination-unreachable -j DROP
#
# mirror incoming wan traffic to snort
#
iptables -t mangle -A PREROUTING -i $wan -j TEE --gateway 192.168.3.1
iptables -t mangle -A PREROUTING -i $lan1 -j TEE --gateway 192.168.3.1
#
# Define NAT for traffic from LANs to the WAN
#
^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      ^Y Prev Page
^X Exit          ^R Read File    ^_ Replace      ^U Uncut Text   ^T To Linter    ^_ Go To Line    ^V Next Page
```

Kỳ vọng:

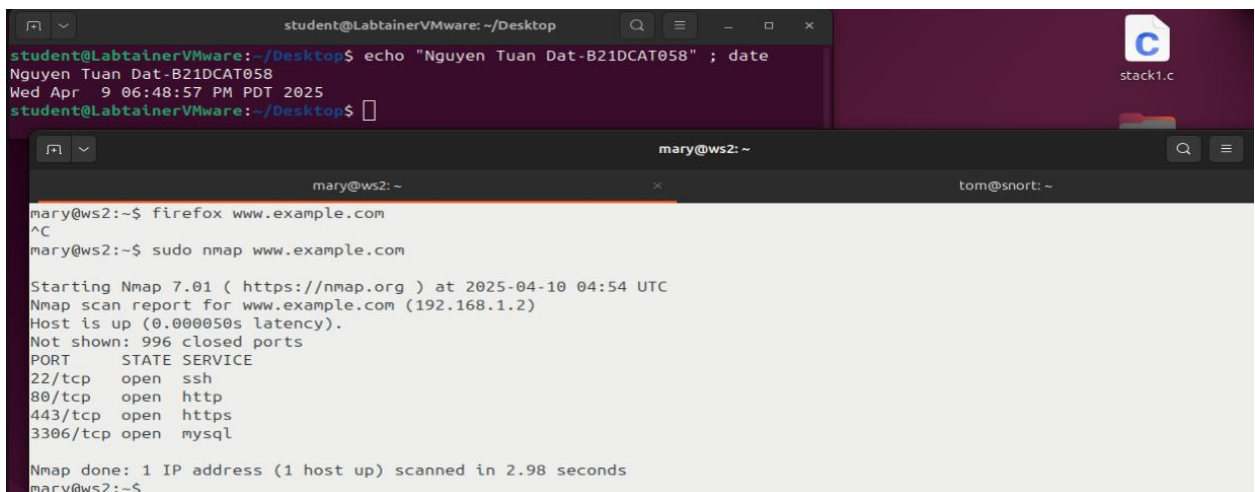
- remote truy cập: Snort báo CONFIDENTIAL



- ws2 truy cập: KHÔNG báo



- ws2 nmap: Có cảnh báo ICMP NMAP




```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr 9 06:48:57 PM PDT 2025
student@LabtainerVMware:~/Desktop$

tom@snort: ~
tom@snort:~$ ./start_snort.sh
04/10-04:53:11.272449 1:2:0 CONFIDENTIAL detected [**] [Priority: 0] {TCP} 192.168.1.2:80 -> 192.168.1.10:56088
04/10-04:54:47.735376 1:469:3 ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.2.1 -> 192.168.1.2
04/10-04:54:47.735376 1:384:5 ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.2.1 -> 192.168.1.2
04/10-04:54:47.735406 1:408:5 ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
04/10-04:54:47.735568 1:453:5 ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.2.1 -> 192.168.1.2
04/10-04:54:47.735585 1:451:5 ICMP Timestamp Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
04/10-04:54:49.075977 1:1418:11 SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.2.1:60042 -> 192.168.1.2:161
04/10-04:54:49.100478 1:1421:11 SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.2.1:60042 -> 192.168.1.2:705
```

- remote nmap: Có cảnh báo ICMP NMAP

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr 9 06:48:57 PM PDT 2025
student@LabtainerVMware:~/Desktop$

tom@snort: ~
tom@snort:~$ ./start_snort.sh
14/10-04:54:47.735585 1:451:5 ICMP Timestamp Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.1.2 -> 192.168.2.1
14/10-04:54:49.075977 1:1418:11 SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.2.1:60042 -> 192.168.1.2:161
14/10-04:54:49.100478 1:1421:11 SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.2.1:60042 -> 192.168.1.2:705
14/10-04:55:34.107809 1:469:3 ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 203.0.113.20 -> 203.0.113.10
14/10-04:55:34.107809 1:384:5 ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 203.0.113.20 -> 203.0.113.10
14/10-04:55:34.108239 1:453:5 ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP} 203.0.113.20 -> 203.0.113.10
14/10-04:55:35.478345 1:1421:11 SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 203.0.113.20:38665 -> 203.0.113.10:705
14/10-04:55:35.526166 1:1418:11 SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 203.0.113.20:38665 -> 203.0.113.10:161

hank@remote_ws: ~
hank@remote_ws:~$ sudo nmap www.example.com
Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-10 04:55 UTC
Nmap scan report for www.example.com (203.0.113.10)
Host is up (0.000035s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 1.55 seconds
hank@remote_ws:~$
```

Kết thúc bài lab:

Checkwork

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr 9 06:48:57 PM PDT 2025
student@LabtainerVMware:~/Desktop$

student@LabtainerVMware: ~/labtainer/labtainer-student
student@LabtainerVMware:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/snort
Successfully copied 25.2MB to snort-igrader:/home/instructor/b21dcat058.snort.lab
Successfully copied 2.56kB to /home/student/labtainer_xfer/snort
Labname snort

=====
Student | snort_local_conf | snort_remote_conf | snort_remote_flr | snort_local_flr | proper_config | snort_local_nmap |
=====
b21dcat058 | y | y | y | y | y | y |
=====
What is automatically assessed for this lab:

snort_local_conf: Snort alerts for CONFIDENTIAL access from local
snort_remote_conf: Snort alerts for CONFIDENTIAL access from remote
snort_remote_flr, snort_local_flr: the httpd log entries that occurred during specific snort sessions
proper_config: Was there a snort session with remote alarm, no local alarm, and a local nmap alarm
during which the plan was accessed locally & remotely?
```