

Nội dung và hướng dẫn bài thực hành

Mục đích

Giúp sinh viên tìm hiểu khái niệm về giám sát an toàn mạng, sử dụng ELK Stack để thu thập, phân tích log giao thức DNS và phát hiện các hoạt động query domain bất thường trong máy.

Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, công cụ ELK Stack, giao thức DNS và kỹ thuật tấn công DNS Spoofing.

Nội dung thực hành

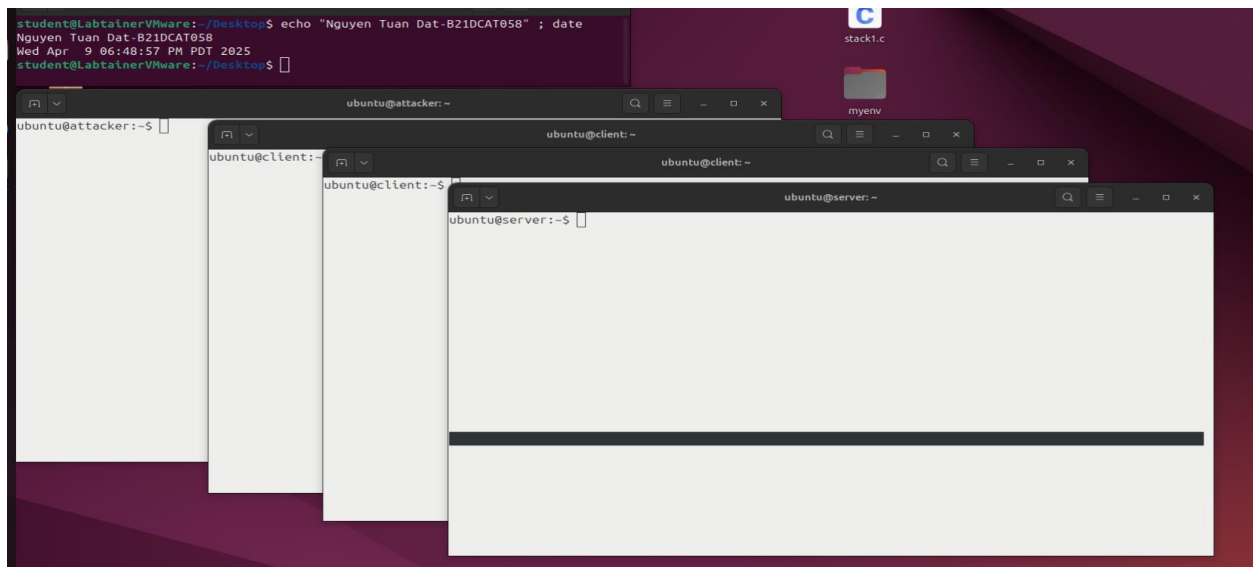
Khởi động bài lab:

Vào terminal, gõ:

```
startlab nsm-elk-dns
```

(chú ý: sinh viên sử dụng mã sinh viên 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 xong bốn terminal ảo sẽ xuất hiện, một cái là đại diện cho máy tấn công: **attacker**, hai cái là đại diện cho máy nạn nhân: **client** (một cái **client1** dùng để cấu hình và chạy tcpdump, tshark, một cái **client2** dùng để truy cập web qua firefox), một cái là đại diện cho máy giám sát: **server**.



Trên terminal **attacker** thực hiện cài đặt ettercap qua một script và chạy dịch vụ Apache

```
sudo su
```

```
sudo echo '
```

```
attempt=1
```

```
max_attempts=3
```

```
while [ $attempt -le $max_attempts ]; do
```

```
  echo "Attempt $attempt: Installing ettercap..."
```

```
  if sudo apt install ettercap-common -y; then
```

```
    echo "Installation successful!"
```

```
    exit 0
```

```
  else
```

```
    echo "Installation failed. Retrying..."
```

```
  fi
```

```
  attempt=$((attempt + 1))
```

```
done
```

```
echo "Installation failed after $max_attempts attempts."
```

```
exit 1' > install_ettercap.sh && sudo chmod +x install_ettercap.sh && sudo
```

```
./install_ettercap.sh && sudo systemctl start apache2
```

```
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-ping.tar

ubuntu@attacker:~$ sudo su
root@attacker:/home/ubuntu# sudo echo '
> attempt=1
> max_attempts=3
> while [ $attempt -le $max_attempts ]; do
>   echo "Attempt $attempt: Installing ettercap..."
>   if sudo apt install ettercap-common -y; then
>     echo "Installation successful!"
>     exit 0
>   else
>     echo "Installation failed. Retrying..."
>   fi
>   attempt=$((attempt + 1))
> done
> echo "Installation failed after $max_attempts attempts."
> exit 1' > install Ettercap.sh && \
> sudo chmod +x install Ettercap.sh && \
> sudo ./install Ettercap.sh && \
> sudo systemctl start apache2
Attempt 1: Installing ettercap...
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ethtool ettercap-graphical geoip-database libgeoip1 liblua5.1-2 liblua5.1-common libnet1
```

Tạo một trang web giả mạo với nội dung “HACKED”

```
sudo echo '<html><body><h1>HACKED</h1></body></html>' >
```

```
/var/www/html/index.html
```

```
sudo cat /var/www/html/index.html
```

```
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-ping.tar

root@attacker:/home/ubuntu# sudo echo '<html><body><h1>HACKED</h1></body></html>' > /var/www/html/index.html
root@attacker:/home/ubuntu# sudo cat /var/www/html/index.html
<html><body><h1>HACKED</h1></body></html>
root@attacker:/home/ubuntu#
```

Cấu hình bản ghi DNS trong

```
sudo nano /etc/ettercap/etter.dns
```

```
=====
```

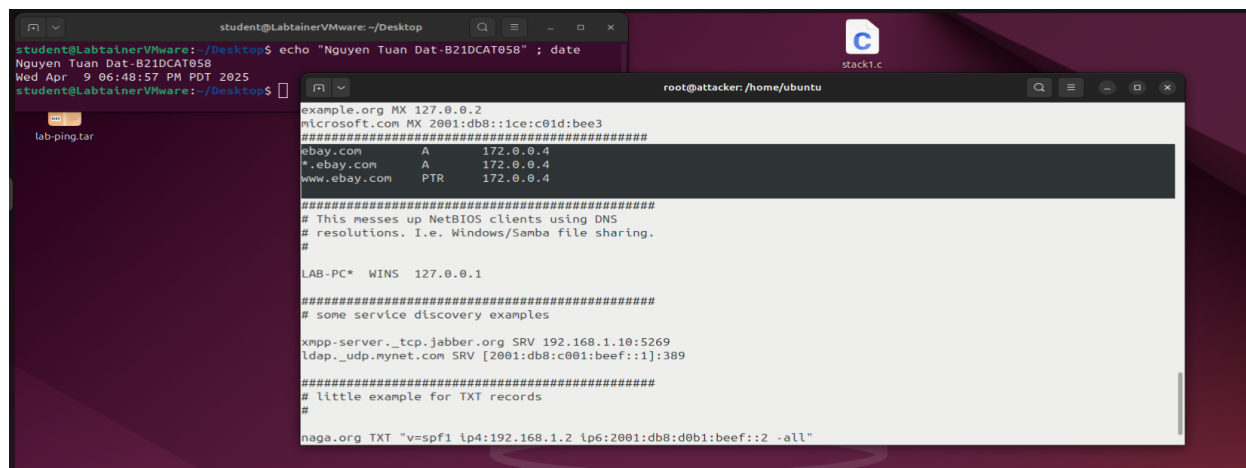
```
ebay.com      A      172.0.0.4
```

```
*.ebay.com    A      172.0.0.4
```

```
www.ebay.com  PTR    172.0.0.4
```

=====

`sudo cat /etc/ettercap/etter.dns`

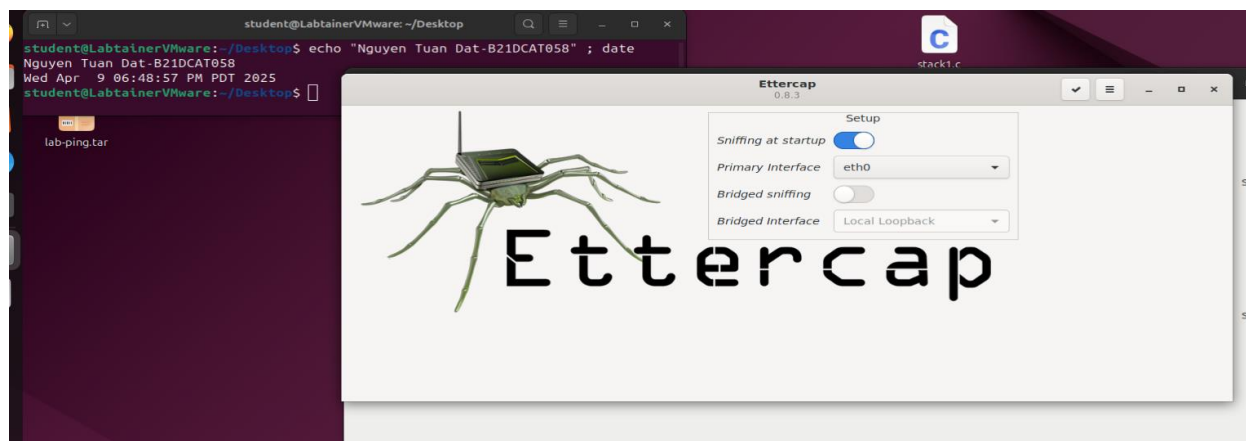


```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr 9 06:48:57 PM PDT 2025
student@LabtainerVMware:~/Desktop$

root@attacker:/home/ubuntu
example.org MX 127.0.0.2
microsoft.com MX 2001:db8::1ce:c01d:bee3
#####
ebay.com A 172.0.0.4
*.ebay.com A 172.0.0.4
www.ebay.com PTR 172.0.0.4
#####
# This messes up NetBIOS clients using DNS
# resolutions. I.e. Windows/Samba file sharing.
#
LAB-PC* WINS 127.0.0.1
#####
# some service discovery examples
xmpp-server._tcp.jabber.org SRV 192.168.1.10:5269
ldap._udp.mynet.com SRV [2001:db8:c001:beef::1]:389
#####
# little example for TXT records
#
naga.org TXT "v=spf1 ip4:192.168.1.2 ip6:2001:db8:d0b1:beef::2 -all"
```

Khởi động Ettercap

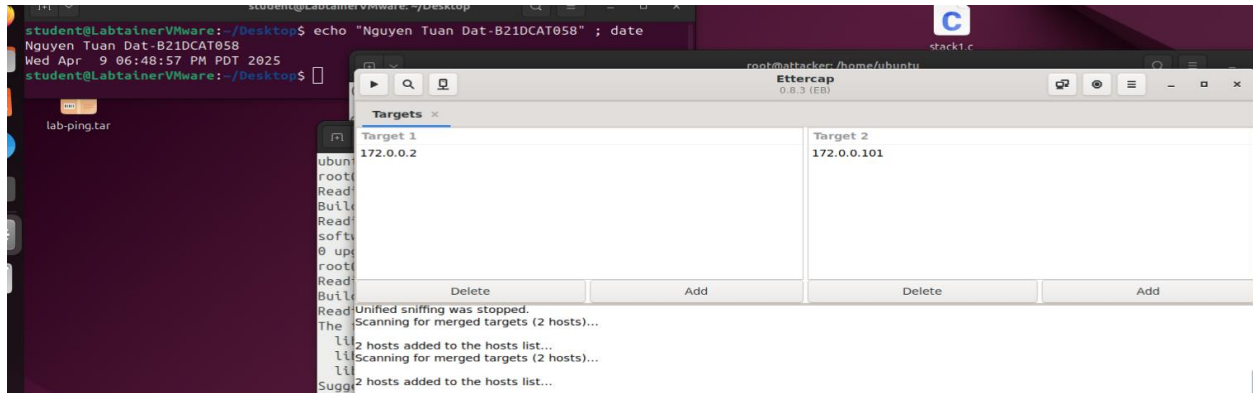
`ettercap -G`



Chọn Host -> Scan for host

ip client (.2) -> target 1

ip gateway (.101) -> target 2

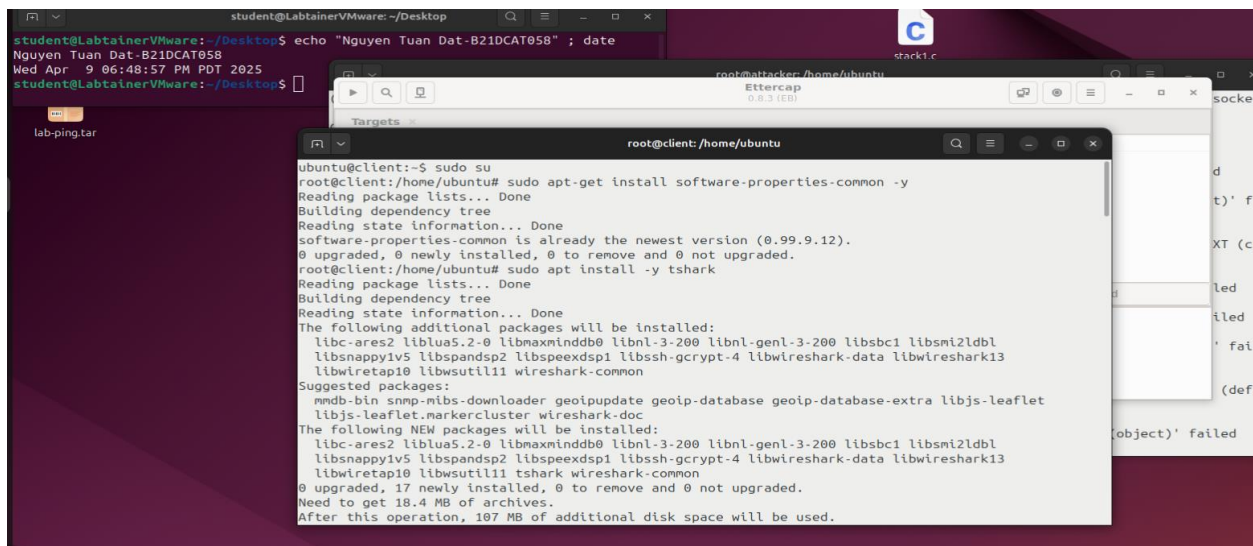


Trên terminal **client1** thực hiện cài đặt tshark.

`sudo su`

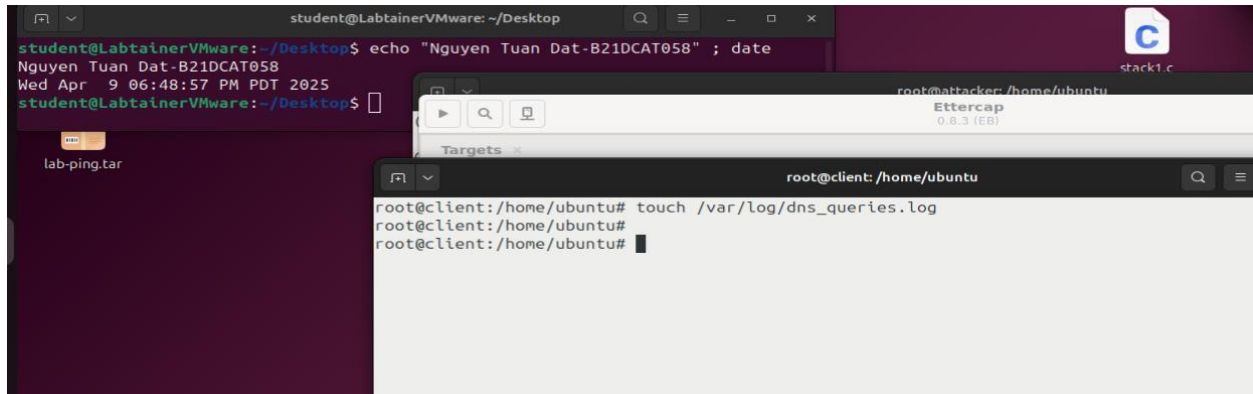
`sudo apt-get install software-properties-common -y`

`sudo apt install -y tshark [Chọn YES]`



Tạo file lưu log DNS query

touch /var/log/dns_queries.log



Cấu hình Filebeat để ghi được log DNS query và gửi tới máy giám sát:

sudo nano /etc/filebeat/filebeat.yml

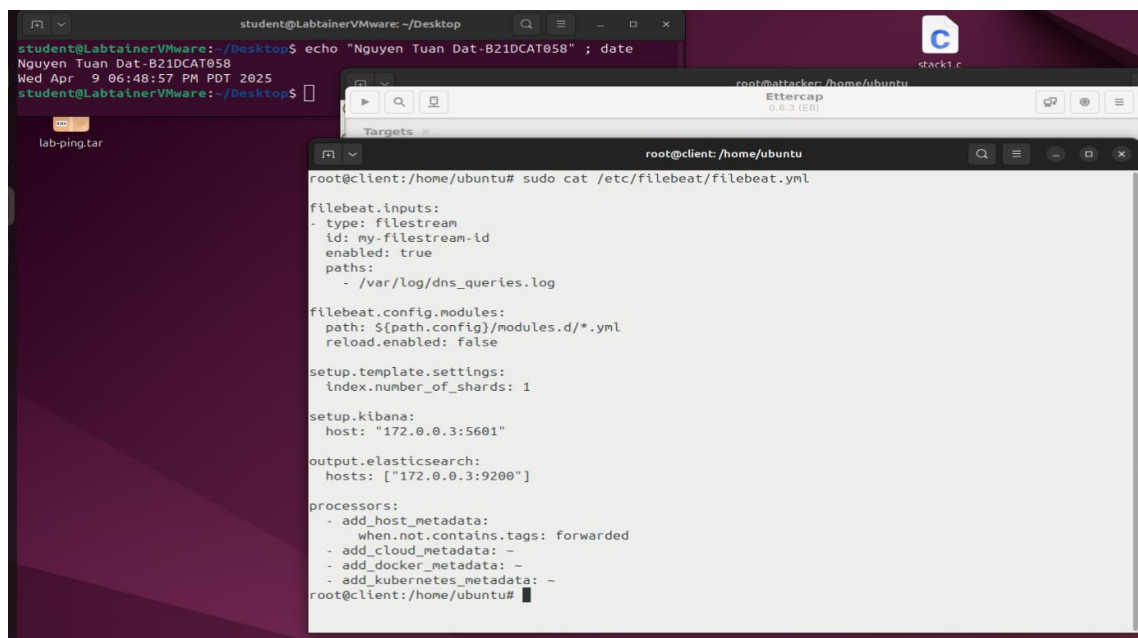
/var/log/dns_queries.log

Elasticsearch: 172.0.0.3:5601

Kibana: 172.0.0.3:9200

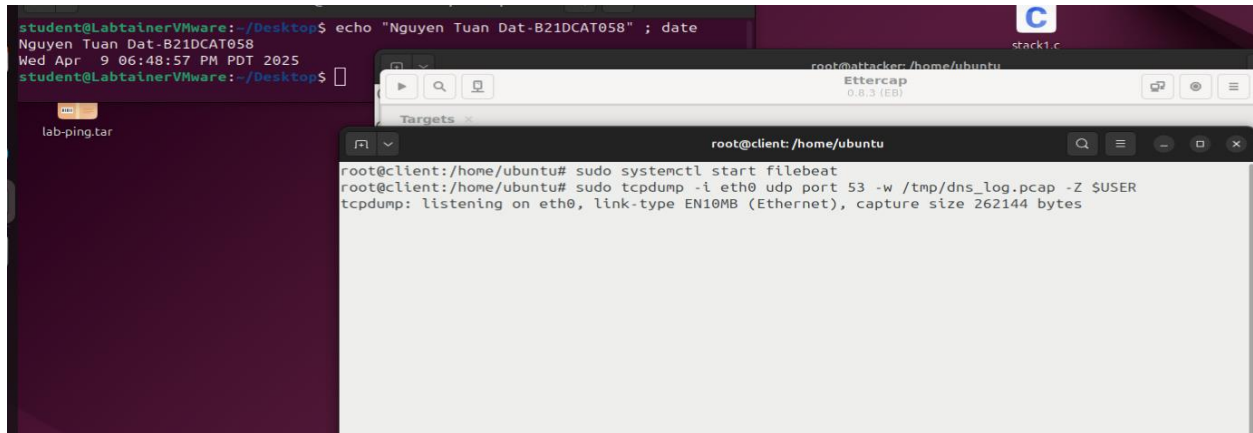
sudo cat /etc/filebeat/filebeat.yml

sudo systemctl start filebeat



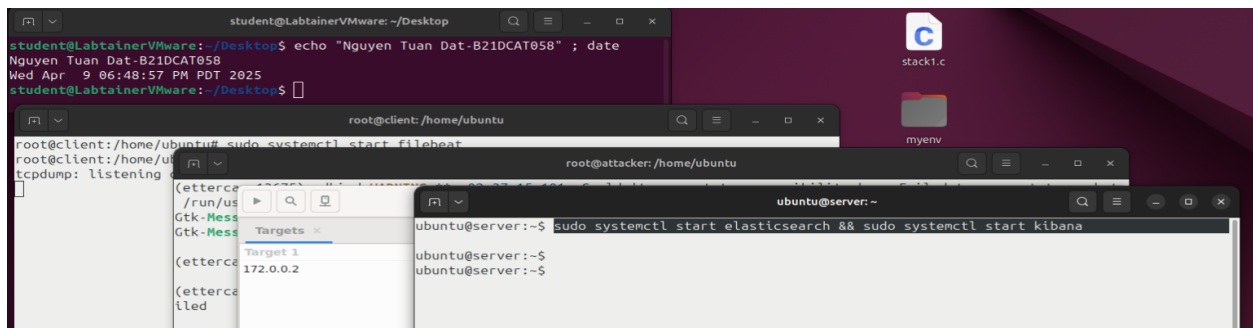
Chạy tcpdump để bắt các gói tin đi qua port 53 (query DNS) và ghi vào một file pcap (sẽ dùng tshark để đọc ra file dns_queries.log)

```
sudo tcpdump -i eth0 udp port 53 -w /tmp/dns_log.pcap -Z $USER
```



Trên máy **server** thực hiện khởi động dịch vụ Elasticsearch và Kibana.

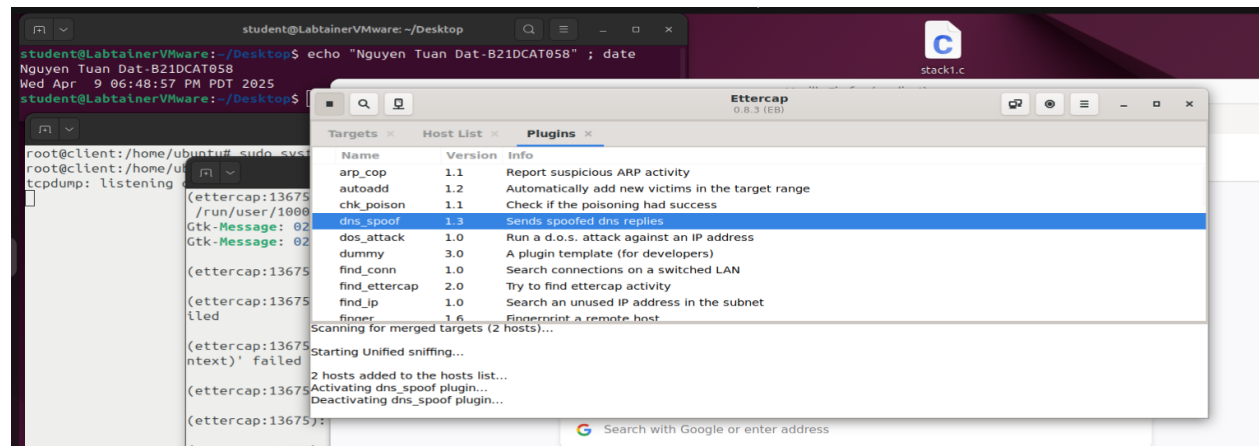
```
sudo systemctl start elasticsearch && sudo systemctl start kibana
```



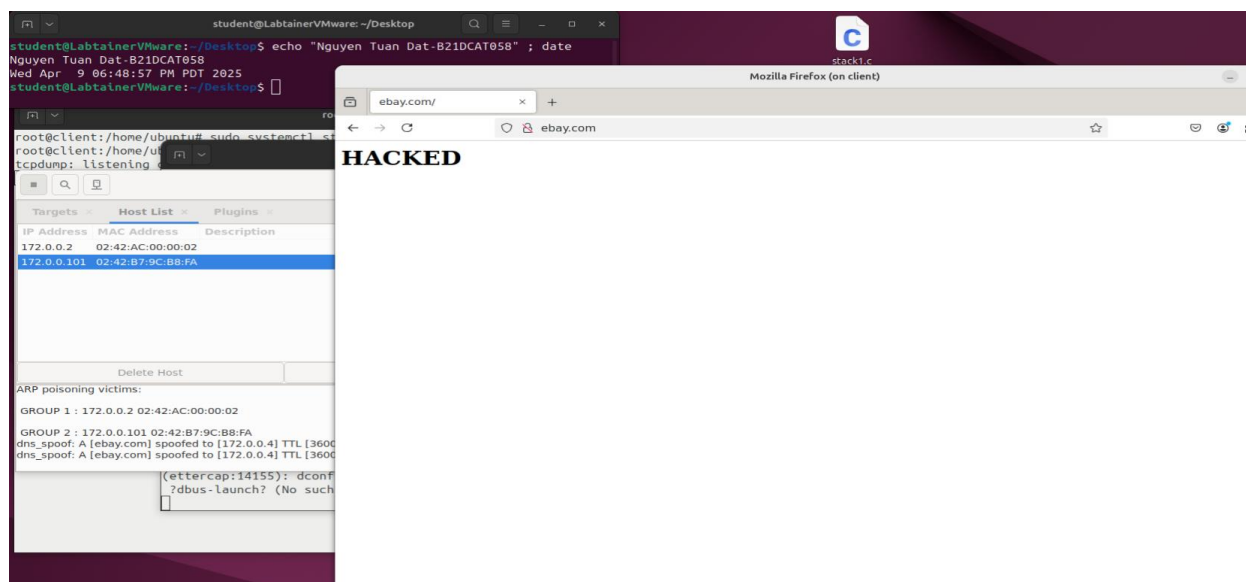
The image shows a Kali Linux desktop environment. On the left, a terminal window is open, displaying a login session for 'student@Laba1nerVMWare'. The user has run the command 'echo "Nguyen Tuan Dat-B21DCA7058" ; date', which outputs the name and the current date and time. On the right, a web browser window is open to the eBay homepage. The browser's address bar shows 'https://www.ebay.com'. The page features a search bar, navigation links like 'Sign in' and 'Register', and a large banner for 'Returns made simple'. Below the banner, there are links to various product categories such as 'Luxury', 'Sneakers', 'PBA', 'Refurbished', 'Trading cards', 'Pre-loved Luxury', and 'Toys'.

Trên máy **attacker** dùng công cụ Ettercap để thực hiện tấn công DNS spoofing đến máy **client**.

Manage plugins -> DNS Spoof



Sau khi dùng máy **client2** truy cập lại trang web ebay.com và thấy trang web đã bị chuyển sang “HACKED”.

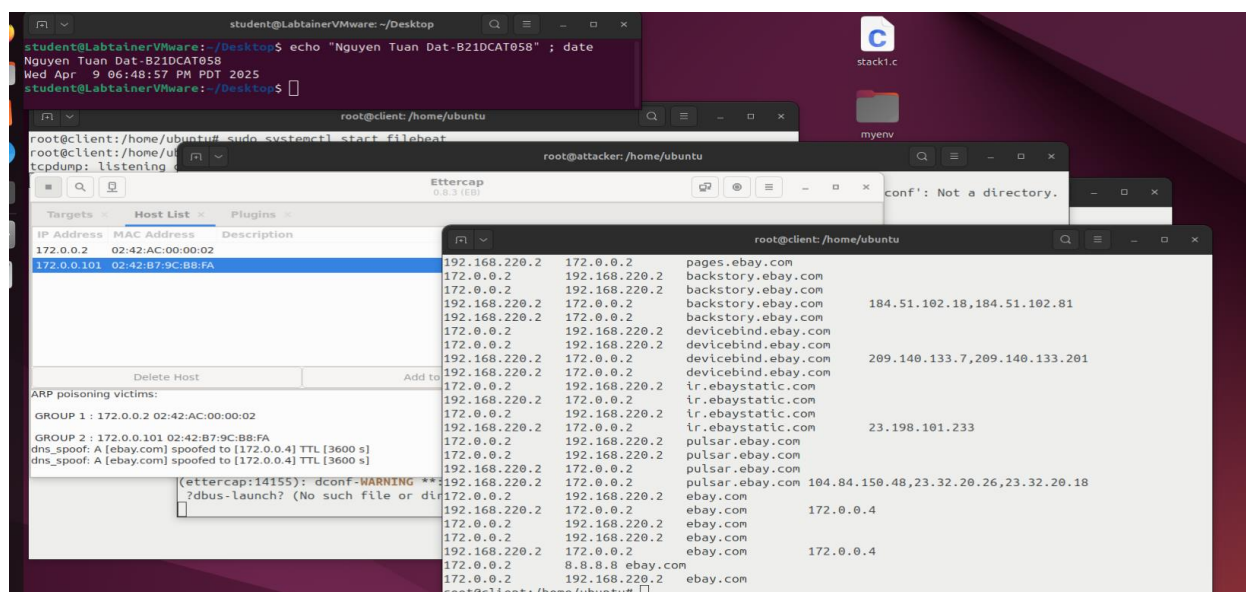


Thực hiện đọc gói tin pcap ra thành file log và xem file đó có query ebay.com không

`sudo su`

`sudo tshark -r /tmp/dns_log.pcap -T fields -e ip.src -e ip.dst -e dns.qry.name -e dns.a > /var/log/dns_queries.log`

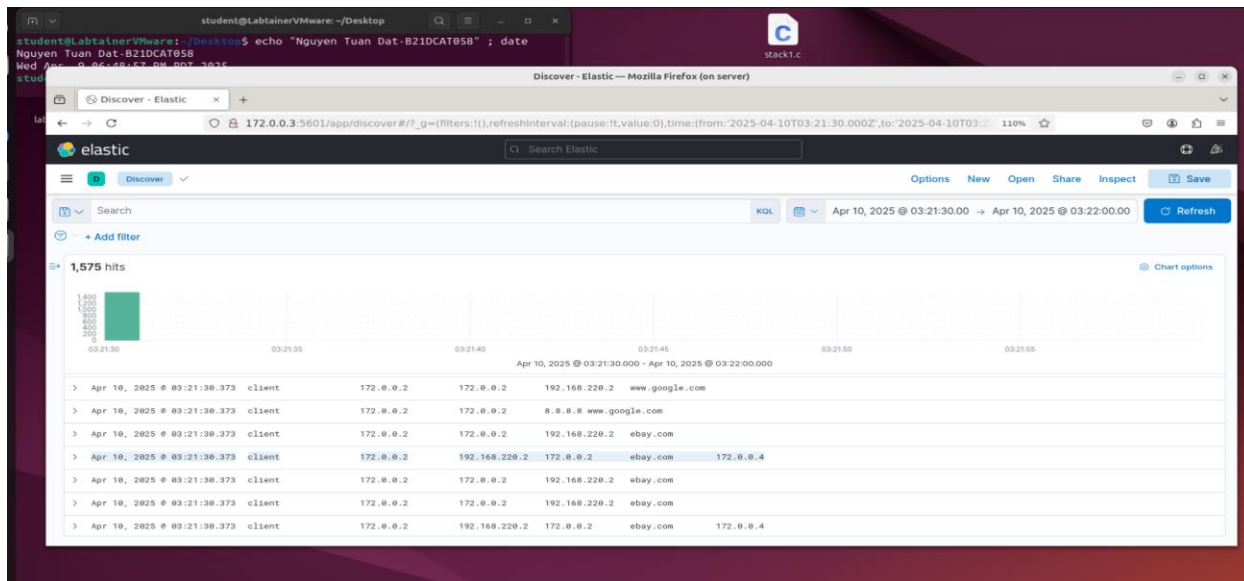
`cat /var/log/dns_queries.log | grep ebay`



Sinh viên xem được nội dung log giao thức DNS từ máy **server** coi như đã hoàn thành bài.

firefox

Truy cập: 172.0.0.3:5601 xem log query DNS (cần cấu hình 1 bước để nhận agent)



Kết thúc bài lab:

Checkwork

