

Nội dung và hướng dẫn bài thực hành

Mục đích

Giúp sinh viên làm quen với công cụ Tshark để phân tích và xử lý các gói tin mạng.

Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, công cụ Tshark.

Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

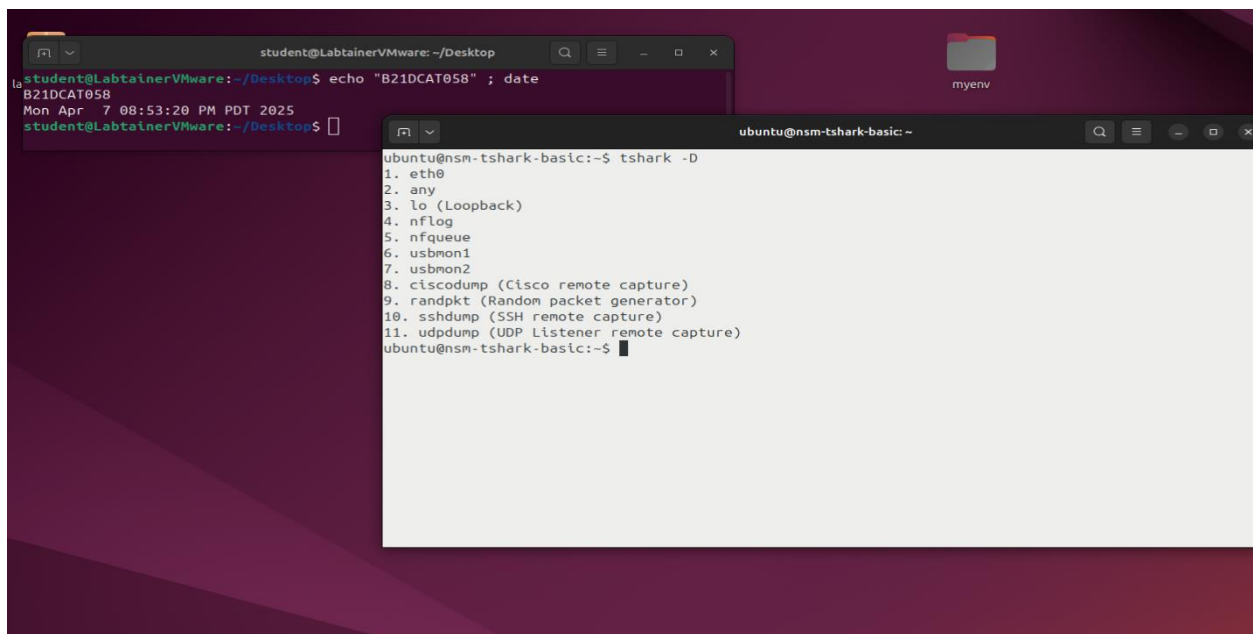
```
labtainer -r nsm-tshark-basic
```

(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 terminal ảo sẽ xuất hiện.

Sinh viên thực hiện liệt kê các giao diện mạng khả dụng:

```
tshark -D
```



Sinh viên đọc các gói tin trong file pcap

```
tshark -r telnet.pcap
```

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware:~/Desktop$

ubuntu@nsm-tshark-basic: ~
3184 42.350145 Vmware_c0:00:08 ? Broadcast ARP 60 Who has 192.168.88.2? Tell 192.168.88.1
3185 42.901796 Vmware_c0:00:08 ? Broadcast ARP 60 Who has 192.168.88.2? Tell 192.168.88.1
ubuntu@nsm-tshark-basic:~$ ^C
ubuntu@nsm-tshark-basic:~$ ^C
ubuntu@nsm-tshark-basic:~$ clear

ubuntu@nsm-tshark-basic:~$ tshark -r telnet.pcap
1 0.000000 192.168.88.128 ? 192.168.88.2 DNS 101 Standard query 0x762e A incoming.telemetry.mozilla.org OPT
2 0.001238 192.168.88.128 ? 192.168.88.2 DNS 101 Standard query 0xe6a1 AAAA incoming.telemetry.mozilla.org OPT
3 0.003380 192.168.88.128 ? 192.168.88.2 DNS 101 Standard query 0xfb70 Unknown (65) incoming.telemetry.mozilla.org OPT
4 0.081805 192.168.88.2 ? 192.168.88.128 DNS 176 Standard query response 0x762e A incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.services.mozilla.com A 34.120.208.123 OPT
5 0.081805 192.168.88.2 ? 192.168.88.128 DNS 239 Standard query response 0xe6a1 AAAA incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.services.mozilla.com SOA ns-1507.awsdns-60.org OPT
6 0.083956 192.168.88.128 ? 192.168.88.2 DNS 116 Standard query 0xccbb AAAA telemetry-incoming.r53-2.services.mozilla.com OPT
7 0.089399 192.168.88.128 ? 34.120.208.123 TCP 74 46844 ? 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3013960007 TSecr=0 WS=128
8 0.090758 192.168.88.2 ? 192.168.88.128 DNS 116 Standard query response 0xccbb AAAA telemetry-incoming.r53-2.services.mozilla.com OPT
9 0.107550 192.168.88.2 ? 192.168.88.128 DNS 239 Standard query response 0xfb70 Unknown (65) incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.services.mozilla.com SOA ns-1507.awsdns-60.org OPT
10 0.108237 192.168.88.128 ? 192.168.88.2 DNS 116 Standard query 0xbafa Unknown (65) telemetry-incoming.r53-2.servi
```

Sinh viên thống kê các giao thức trong file pcap:

tshark -r telnet.pcap -q -z io,phs

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware:~/Desktop$

ubuntu@nsm-tshark-basic: ~
3183 41.886262 192.168.88.128 ? 34.120.208.123 TCP 54 60542 ? 443 [ACK] Seq=14499 Ack=4674 Wln=62780 Len=0
3184 42.350145 Vmware_c0:00:08 ? Broadcast ARP 60 Who has 192.168.88.2? Tell 192.168.88.1
3185 42.901796 Vmware_c0:00:08 ? Broadcast ARP 60 Who has 192.168.88.2? Tell 192.168.88.1
ubuntu@nsm-tshark-basic:~$ ^C
ubuntu@nsm-tshark-basic:~$ clear

ubuntu@nsm-tshark-basic:~$ tshark -r telnet.pcap -q -z io,phs

=====
Protocol Hierarchy Statistics
Filter:

eth
  ip
    udp
      dns
        data
          ntp
            mdns
              tcp
                ssl
                  tcp.segments
                    ssl
                      http
                        ocsf
                          data-text-lines
ip6
  udp
    mdns
  arp
=====
eth          frames:3185 bytes:2145122
ip           frames:3181 bytes:2144835
udp          frames:621 bytes:263591
dns          frames:278 bytes:35484
data         frames:337 bytes:227653
ntp          frames:4 bytes:360
mdns         frames:2 bytes:174
tcp          frames:2560 bytes:1881244
ssl          frames:772 bytes:825254
tcp.segments frames:105 bytes:306105
ssl          frames:91 bytes:267088
http         frames:36 bytes:22434
ocsf         frames:30 bytes:20443
data-text-lines frames:3 bytes:892
ip6          frames:1 bytes:107
udp          frames:1 bytes:107
mdns         frames:1 bytes:107
arp          frames:3 bytes:180
=====
ubuntu@nsm-tshark-basic:~$
```

Sinh viên thống kê các địa chỉ IP trong file pcap dưới dạng cây:

tshark -r telnet.pcap -q -z ip_hosts,tree

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware:~/Desktop$

ubuntu@nsm-tshark-basic: -
mdns frames:1 bytes:107
arp frames:3 bytes:180
ubuntu@nsm-tshark-basic:~$ clear
ubuntu@nsm-tshark-basic:~$ tshark -r telnet.pcap -q -z ip_hosts,tree
=====
IPv4 Statistics/All Addresses:
Topic / Item Count Average Min val Max val Rate (ms) Percent Burst r
-----
All Addresses 3181
79 192.168.88.128 3180 0.0759 99.97% 1.8200
79 151.101.228.159 1037 0.0248 32.60% 2.4400
91 34.120.208.123 395 0.0094 12.42% 0.4500
94 192.168.88.2 278 0.0066 8.74% 0.1800
88 142.250.198.36 233 0.0056 7.32% 0.9500
5 34.149.100.209 125 0.0030 3.93% 0.3000
02 142.250.198.195 123 0.0029 3.87% 0.6400
7 104.244.42.1 115 0.0027 3.62% 0.1800
29
```

Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

```
stoplab nsm-tshark-basic
```

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Khởi động lại bài lab:

Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

```
labtainer -r nsm-tshark-basic
```

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 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/nsm-tshark-basic
Successfully copied 236kB to nsm-tshark-basic-igrader:/home/instructor/b21dcat058.nsm-tshark-basic.lab
Successfully copied 2.56kB to /home/student/labtainer_xfer/nsm-tshark-basic
Labname nsm-tshark-basic

Student | statistic_proto | ip_tree | network_interfa | view_packet |
=====|=====|=====|=====|=====|
b21dcat058 | Y | Y | Y | Y |

What is automatically assessed for this lab:
network_interface: list the available network interfaces.
view_packet: displays packets in a pcap file.
statistic_protocol: statistic about the protocol in the file pcap
ip_tree: statistic on detected IP addresses in the form of a tree
student@LabtainerVMware:~/labtainer/labtainer-student$ stoplab
Results stored in directory: /home/student/labtainer_xfer/nsm-tshark-basic
student@LabtainerVMware:~/labtainer/labtainer-student$
```