

Nội dung và hướng dẫn bài thực hành

Mục đích

Giúp sinh viên hiểu rõ cách phân tích gói tin TCP và nắm vững kỹ năng phân tích lưu lượng mạng.

Yêu cầu đối với sinh viên

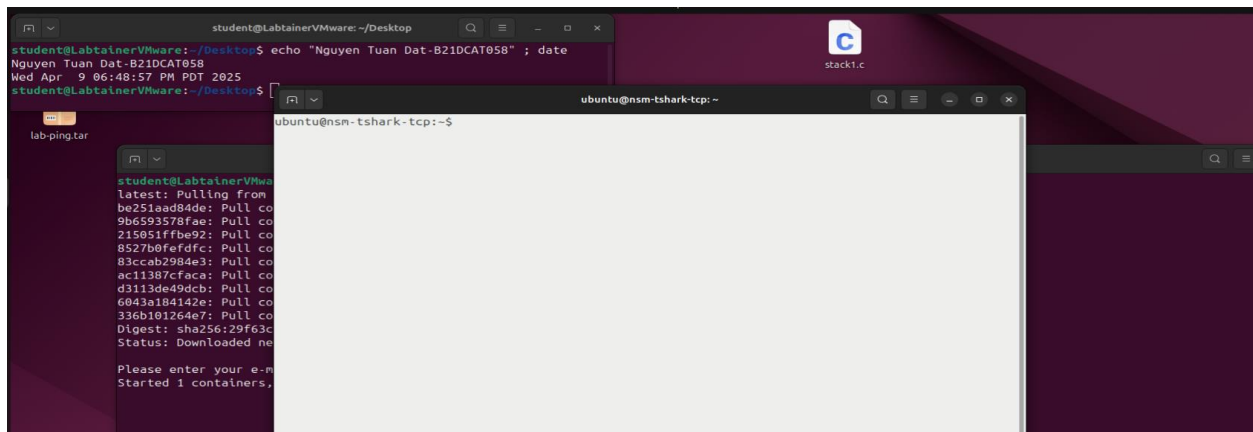
Có kiến thức cơ bản về hệ điều hành Linux, công cụ Tshark.

Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

labtainer -r nsm-tshark-tcp

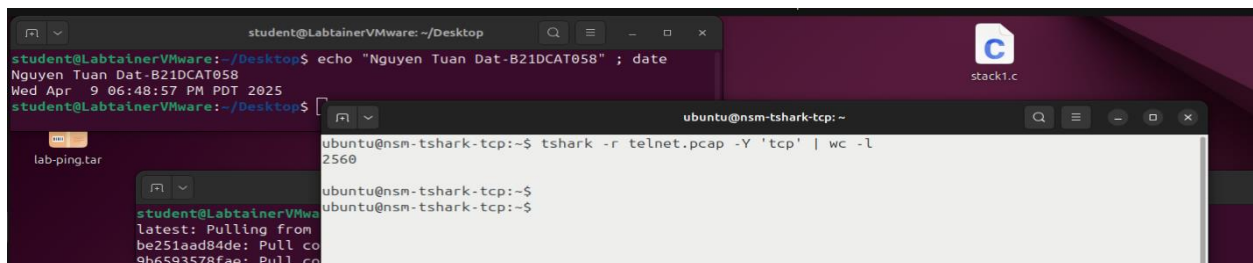


(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Sau khi khởi động xong terminal ảo sẽ xuất hiện.

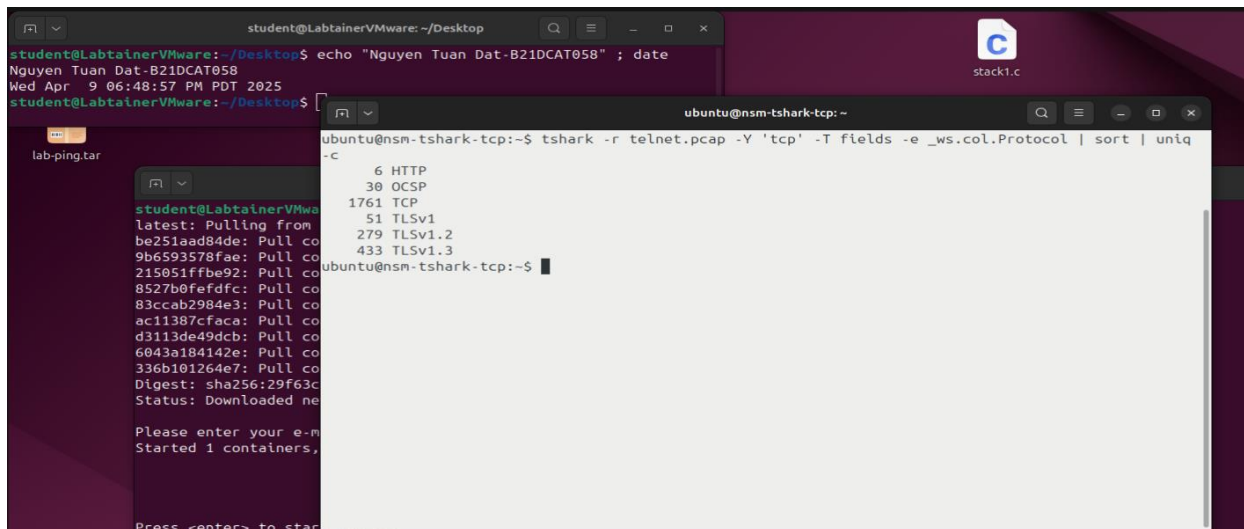
Sinh viên thực hiện đếm xem có bao nhiêu gói tin TCP:

tshark -r telnet.pcap -Y 'tcp' | wc -l



Sinh viên xác định những loại giao thức truyền tải gói tin TCP và số lượng mỗi loại

tshark -r telnet.pcap -Y 'tcp' -T fields -e _ws.col.Protocol | sort | uniq -c

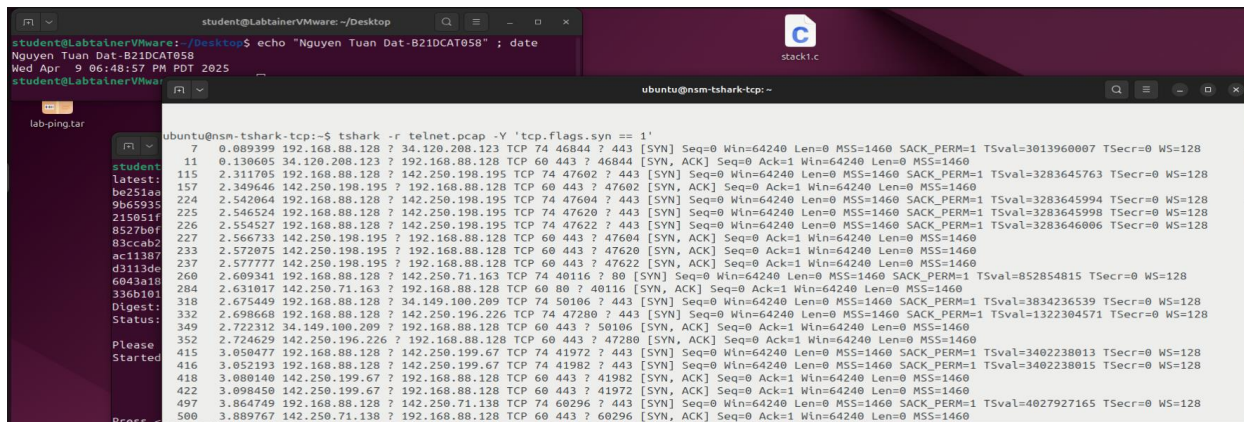


```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr  9 06:48:57 PM PDT 2025
student@LabtainerVMware:~/Desktop$

ubuntu@nsm-tshark-tcp: ~
ubuntu@nsm-tshark-tcp:~$ tshark -r telnet.pcap -Y 'tcp' -T fields -e _ws.col.Protocol | sort | uniq -c
  6 HTTP
 30 OCSP
1761 TCP
  51 TLSv1
 279 TLSv1.2
 433 TLSv1.3
ubuntu@nsm-tshark-tcp:~$
```

Sinh viên thực hiện lọc và hiển thị các gói tin TCP có cờ SYN:

tshark -r telnet.pcap -Y 'tcp.flags.syn == 1'

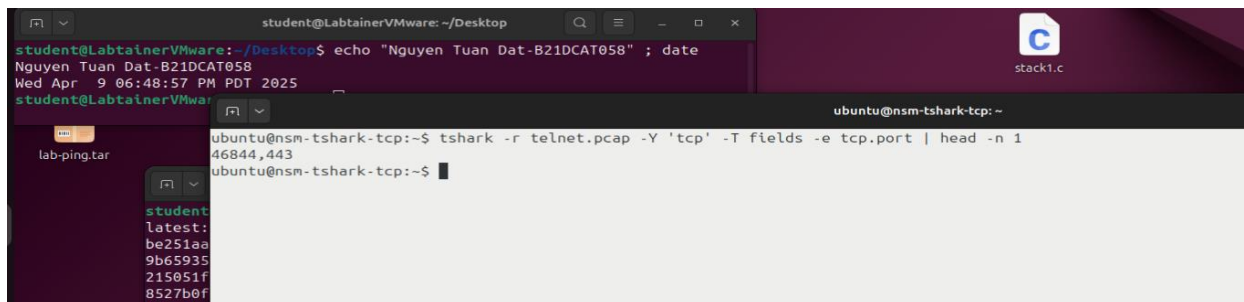


```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr  9 06:48:57 PM PDT 2025
student@LabtainerVMware:~/Desktop$

ubuntu@nsm-tshark-tcp: ~
ubuntu@nsm-tshark-tcp:~$ tshark -r telnet.pcap -Y 'tcp.flags.syn == 1'
  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
 11  0.130605 34.120.208.123 ? 192.168.88.128 TCP 60 443 ? 46844 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 TSval=3283645763 TSecr=0 WS=128
 115 2.311785 192.168.88.128 ? 142.250.198.195 TCP 74 47602 ? 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3283645994 TSecr=0 WS=128
 157 2.349646 142.250.198.195 ? 192.168.88.128 TCP 60 443 ? 47602 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 TSval=3283645994 TSecr=0 WS=128
 224 2.542064 192.168.88.128 ? 142.250.198.195 TCP 74 47604 ? 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3283645994 TSecr=0 WS=128
 225 2.546524 192.168.88.128 ? 142.250.198.195 TCP 74 47620 ? 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3283645994 TSecr=0 WS=128
 226 2.554527 192.168.88.128 ? 142.250.198.195 TCP 74 47622 ? 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3283646006 TSecr=0 WS=128
 227 2.566733 142.250.198.195 ? 192.168.88.128 TCP 60 443 ? 47604 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 TSval=3283646006 TSecr=0 WS=128
 233 2.572075 142.250.198.195 ? 192.168.88.128 TCP 60 443 ? 47620 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 TSval=3283646006 TSecr=0 WS=128
 237 2.577777 142.250.198.195 ? 192.168.88.128 TCP 60 443 ? 47622 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 TSval=3283646006 TSecr=0 WS=128
 260 2.609341 192.168.88.128 ? 142.250.71.163 TCP 74 48116 ? 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=852854815 TSecr=0 WS=128
 284 2.631017 142.250.71.163 ? 192.168.88.128 TCP 60 80 ? 48116 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 TSval=3834236539 TSecr=0 WS=128
 318 2.675449 192.168.88.128 ? 34.149.100.209 TCP 74 50106 ? 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1322304571 TSecr=0 WS=128
 332 2.698686 192.168.88.128 ? 142.250.196.226 TCP 74 47280 ? 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1322304571 TSecr=0 WS=128
 349 2.722312 34.149.100.209 ? 192.168.88.128 TCP 60 443 ? 50106 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 TSval=3402238013 TSecr=0 WS=128
 352 2.724629 142.250.196.226 ? 192.168.88.128 TCP 60 443 ? 47280 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 TSval=3402238013 TSecr=0 WS=128
 415 3.059477 192.168.88.128 ? 142.250.199.67 TCP 74 41972 ? 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3402238013 TSecr=0 WS=128
 416 3.052193 192.168.88.128 ? 142.250.199.67 TCP 74 41982 ? 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3402238013 TSecr=0 WS=128
 418 3.080140 142.250.199.67 ? 192.168.88.128 TCP 60 443 ? 41982 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 TSval=3402238013 TSecr=0 WS=128
 422 3.098450 142.250.199.67 ? 192.168.88.128 TCP 60 443 ? 41972 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 TSval=3402238013 TSecr=0 WS=128
 427 3.064749 192.168.88.128 ? 142.250.71.138 TCP 74 60296 ? 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4027927165 TSecr=0 WS=128
 497 3.089767 142.250.71.138 ? 192.168.88.128 TCP 60 443 ? 60296 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 TSval=4027927165 TSecr=0 WS=128
 500 3.089767 142.250.71.138 ? 192.168.88.128 TCP 60 443 ? 60296 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 TSval=4027927165 TSecr=0 WS=128
ubuntu@nsm-tshark-tcp:~$
```

Tìm cổng nguồn và cổng đích của gói tin TCP:

tshark -r telnet.pcap -Y 'tcp' -T fields -e tcp.port | head -n 1



```
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@nsm-tshark-tcp: ~
ubuntu@nsm-tshark-tcp:~$ tshark -r telnet.pcap -Y 'tcp' -T fields -e tcp.port | head -n 1
46844,443
ubuntu@nsm-tshark-tcp:~$
```

Kết thúc bài lab:

Checkwork

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "Nguyen Tuan Dat-B21DCA7058" ; date
Nguyen Tuan Dat-B21DCA7058
Wed Apr  9 06:48:57 PM PDT 2025
student@LabtainerVMware:~/Desktop$

lab-ping
student@LabtainerVMware:~/Labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/nsn-tshark-tcp
Successfully copied 125kB to nsn-tshark-tcp-lgrader:/home/instructor/b21dcat058.nsn-tshark-tcp.lab
Successfully copied 2.56kB to /home/student/labtainer_xfer/nsn-tshark-tcp
Labname nsn-tshark-tcp

Student          | first_port | tcp_packet_coun | protocol_packet | SYN_packet_filt |
=====|=====|=====|=====|=====|
b21dcat058       | Y          | Y              | Y              | Y              |
What is automatically assessed for this lab:
tcp_packet_count: count the number of TCP packets in a pcap file.
protocol_packet_count: show the count of each unique protocol present in the TCP packets of the pcap file.
SYN_packet_filter: Filter packets with the SYN flags
first_port: shows out the source and destination ports of the first TCP packet in the pcap file.
student@LabtainerVMware:~/labtainer/labtainer-student$
```