LAB04-2- tshark sniffing

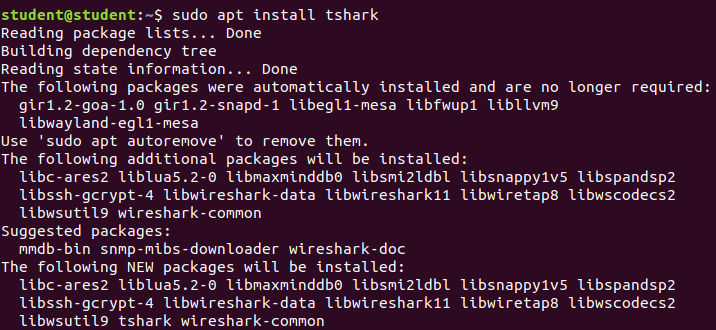
**Class: M03 student ID: B2111933 Name: Truong Dang Truc Lam**

Simulation scenario

|  | Host | Target |
| --- | --- | --- |
| VM type | Virtual box, VMware |  |
| OS | Ubuntu, Centos, kali |  |
| IP | Test-bed IP |  |
| Attacking type | sniffing | |
| Attacking program | tshark | |
| Attacking Process (9 steps) | 1. Install tshark 2. Check the installation 3. List your network devices. 4. Read this file with Wireshark or Tshark later. 5. Use the traditional “pcap” filter to select what to capture from your interface. 6. Display HTTP requests on TCP port 8080 7. Capture Packets with Tshark 8. Read a Pcap with Tshark 9. Extract data from any HTTP requests that are seen. | |

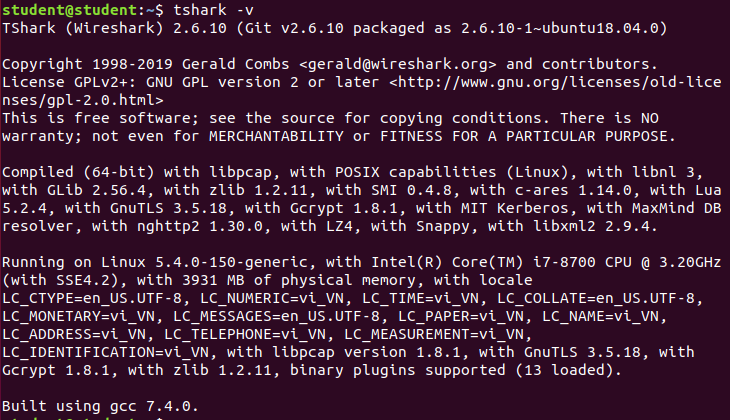
Exercise following commands and explain the each results

1. Install tshark



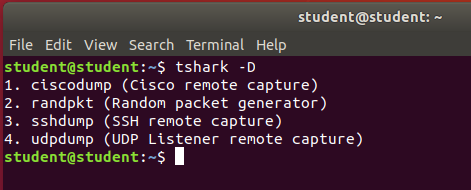
Install tshark

1. Check the installation



Verify the installation

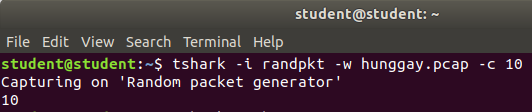
1. List your network devices.



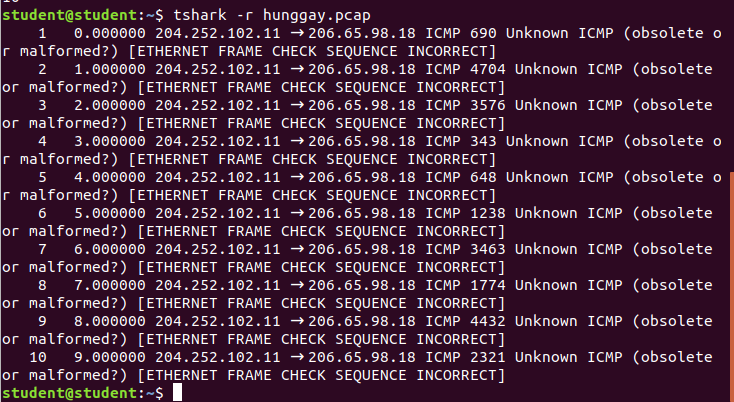
List network devices

.

1. Read this file with Wireshark or Tshark later.

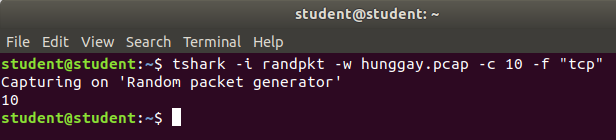


Capture packets with output

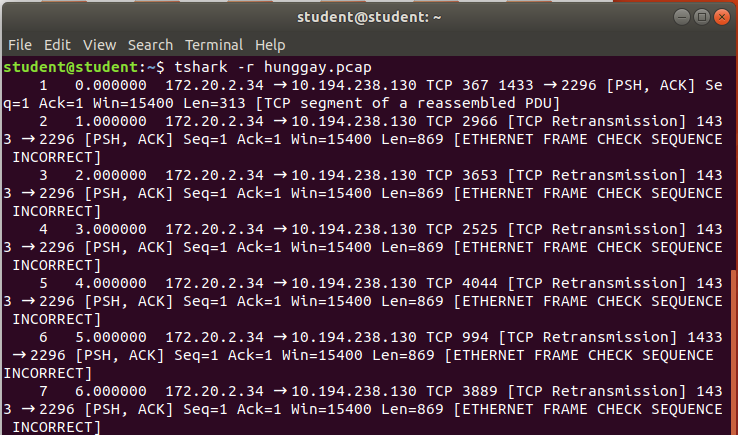


Read the saved file

1. Use the traditional “pcap” filter to select what to capture from your interface.

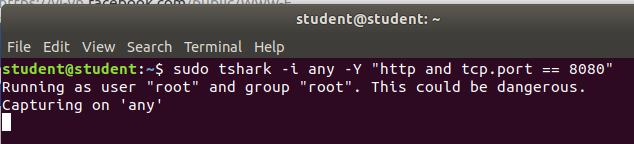


Traditional “pcap” filter



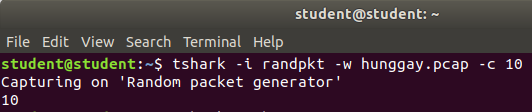
Result with filter

1. Display HTTP requests on TCP port 8080



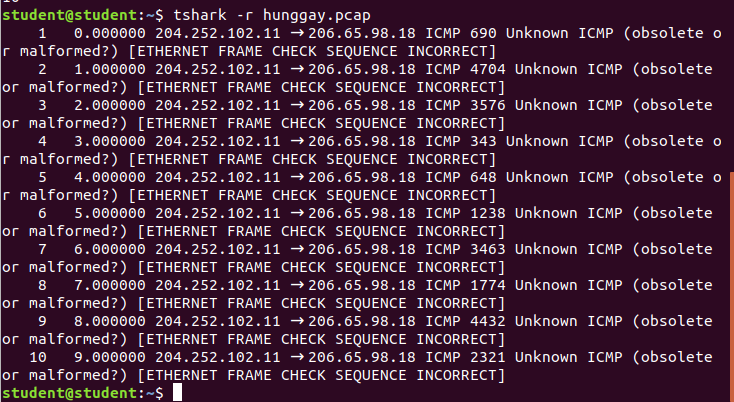
Port 8080 not open

1. Capture Packets with Tshark



Capture packets with output

1. Read a Pcap with Tshark



Read the saved file

1. Extract data from any HTTP requests that are seen. Using the -T we specify we want to extract fields, and with the -e options we identify which fields we want to extract.



Extract data from any HTTP requests