LAB04-2- tshark sniffing

**Class student ID Name**

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 (9steps) | 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
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. Using the -T we specify we want to extract fields, and with the -e options we identify which fields we want to extract.