THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

Name: Vruddhi Tolia
Roll No: 115

Date: 25 - 04 - 2021

Lab Assignment No: - 6

<u>Aim</u>: Installation of WireShark

<u>Lab Outcome Attained:</u>

LO 5: -To observe and study the traffic flow and the contents of protocol frames.

<u>Theory: -</u>

Wireshark: -

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. You could think of a network packet analyzer as a measuring device for examining what’s happening inside a network cable, just like an electrician uses a voltmeter for examining what’s happening inside an electric cable (but at a higher level, of course).

Wireshark intercepts traffic and converts that binary traffic into human-readable format. This makes it easy to identify what traffic is crossing your network, how much of it, how frequently, how much latency there is between certain hops, and so forth.

While Wireshark supports more than two thousand network protocols, many of them esoteric, uncommon, or old, the modern security professional will find analyzing IP packets to be of most immediate usefulness. The majority of the packets on your network are likely to be TCP, UDP, and ICMP.

Uses of Wireshark: -

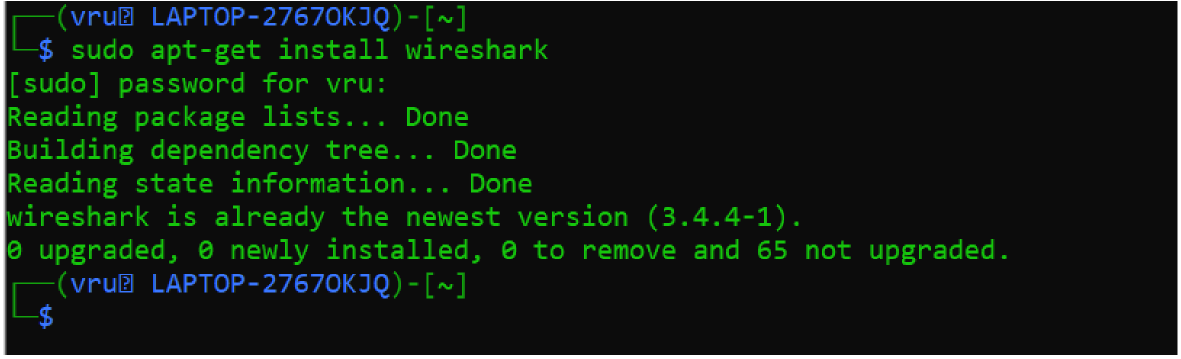
1) It is used by network security engineers to examine security problems.
2) It allows the user to watch all traffic being passed over the network.
3) It is used by network engineers to troubleshoot network issues.

4) It also helps to troubleshoot latency issues and malicious activities on your network.
5) It can help to analyze dropped packets.
6) It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

Screenshots

Installation Process: -

a) Using advanced Package Tool to download and install the wireshark software:
   ➔ Sudo apt-get install wireshark



```
┌──(vru□ LAPTOP-2767OKJQ)-[~]
└─$ sudo apt-get install wireshark
[sudo] password for vru:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wireshark is already the newest version (3.4.4-1).
0 upgraded, 0 newly installed, 0 to remove and 65 not upgraded.
┌──(vru□ LAPTOP-2767OKJQ)-[~]
└─$
```

b) Creating a group called wireshark
   ➔ Sudo groupadd wireshark

c) Modify the user. a: append –G: group (appending user to the group named wireshark)
   ➔ Sudo usermod –a –G wireshark YOUR_USER_NAME

d) Changing group ownership
   ➔ Sudo chgrp wireshark /usr/bin/dumpcap

e) Modifying permissions for the given fie location
   7: Owner can read, write, execute
   5: Group can read, can’t write and execute
   0: others can’t read, can’t write and can’t execute

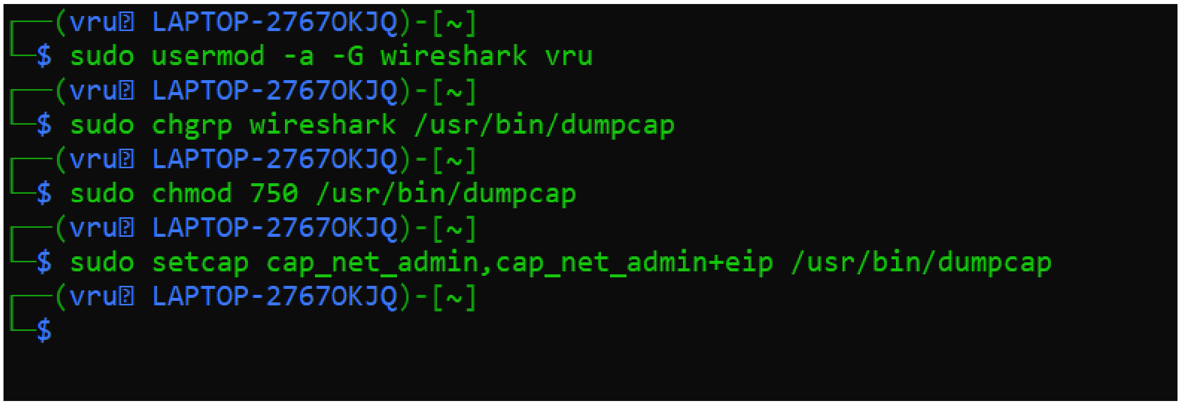
➔ Sudo chmod 750 /usr/bin/dumpcap

f) Capabilities cap_net_raw, cap_net_admin are added to the permitted sets and the effective bit is set.

➔ Sudo setcap cap_net_raw,cap_net_admin=eip /usr/bin/dumpcap

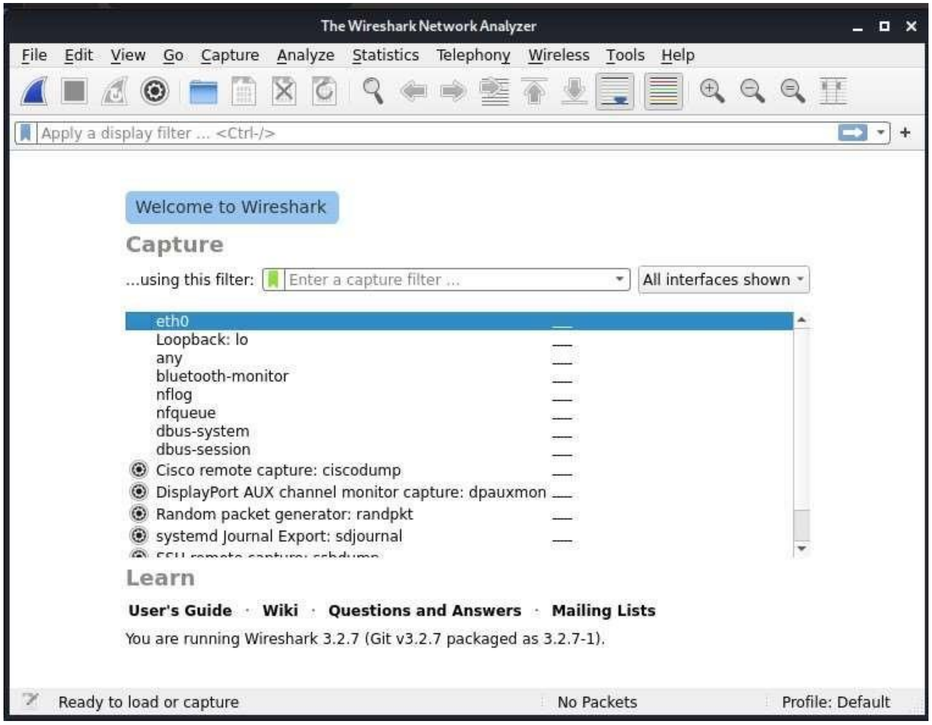
g) Display the name and capabilities

➔ Sudo getcap /usr/bin/dumpcap



```
┌──(vru□ LAPTOP-2767OKJQ)-[~]
└─$ sudo usermod -a -G wireshark vru
┌──(vru□ LAPTOP-2767OKJQ)-[~]
└─$ sudo chgrp wireshark /usr/bin/dumpcap
┌──(vru□ LAPTOP-2767OKJQ)-[~]
└─$ sudo chmod 750 /usr/bin/dumpcap
┌──(vru□ LAPTOP-2767OKJQ)-[~]
└─$ sudo setcap cap_net_admin,cap_net_admin+eip /usr/bin/dumpcap
┌──(vru□ LAPTOP-2767OKJQ)-[~]
└─$
```

h) Running wireshark

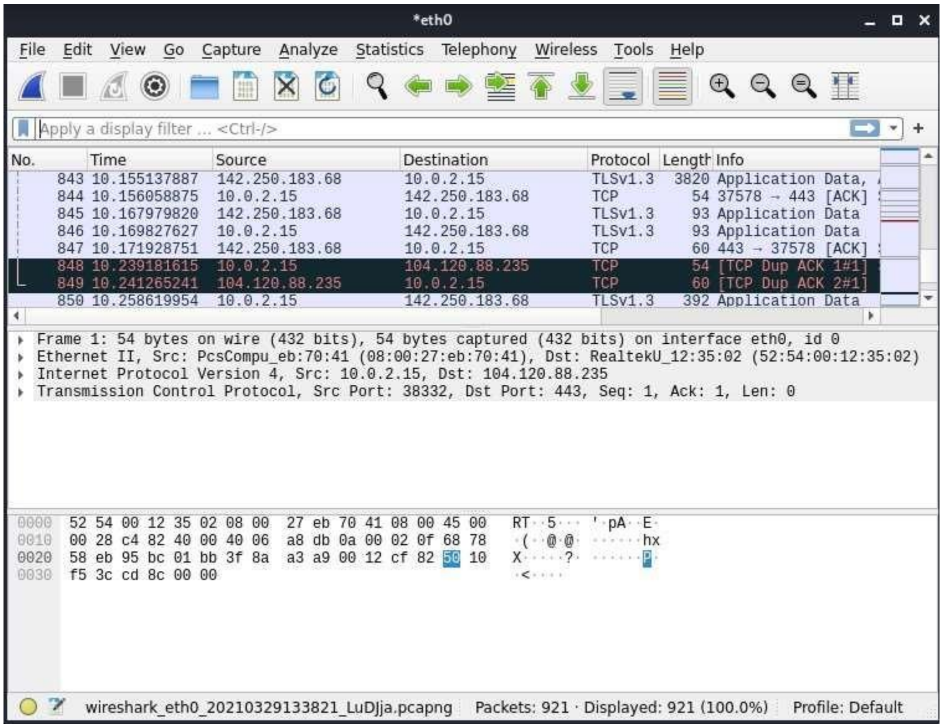

The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

```
eth0
Loopback: lo
any
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
```

You are running Wireshark 3.2.7 (Git v3.2.7 packaged as 3.2.7-1).

Ready to load or capture | No Packets | Profile: Default

i) Example of wireshark capturing packets transmitting


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.     Time          Source           Destination      Protocol Length Info
    843 10.155137887  142.250.183.68   10.0.2.15        TLSv1.3   3820 Application Data,
    844 10.156058875  10.0.2.15        142.250.183.68   TCP         54 37578 → 443 [ACK]
    845 10.167979820  142.250.183.68   10.0.2.15        TLSv1.3     93 Application Data
    846 10.169827627  10.0.2.15        142.250.183.68   TLSv1.3     93 Application Data
    847 10.171928751  142.250.183.68   10.0.2.15        TCP         60 443 → 37578 [ACK]
    848 10.239181615  10.0.2.15        104.120.88.235   TCP         54 [TCP Dup ACK 1#1]
    849 10.241265241  104.120.88.235   10.0.2.15        TCP         60 [TCP Dup ACK 2#1]
    850 10.258619954  10.0.2.15        142.250.183.68   TLSv1.3    392 Application Data
```

```
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_eb:70:41 (08:00:27:eb:70:41), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 104.120.88.235
Transmission Control Protocol, Src Port: 38332, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
```

```
0000  52 54 00 12 35 02 08 00  27 eb 70 41 08 00 45 00   RT··5···  '·pA··E·
0010  00 28 c4 82 40 00 40 06  a8 db 0a 00 02 0f 68 78   ·(··@·@·  ······hx
0020  58 eb 95 bc 01 bb 3f 8a  a3 a9 00 12 cf 82 50 10   X·····?·  ······P·
0030  f5 3c cd 8c 00 00                                  ·<····
```

wireshark_eth0_20210329133821_LuDJja.pcapng   Packets: 921 · Displayed: 921 (100.0%)   Profile: Default

<u>Conclusion:</u> Therefore, wireshark was successfully installed and captured its packets.