LAB Manual

PART A

(PART A : TO BE REFFERED BY STUDENTS)

**Experiment No.4**

**A.1 Aim:**

To install network sniffer (Wireshark) and analyze the working of packet sniffing

**A.2 Prerequisite:**

Role of packet sniffers in network security

**A.3 Outcome:**

**After successful completion of this experiment students will be able to** 1. Appreciate wireshark as a tool to analyze the packets travelling in a network.

2. Know how this tool can be used by malicious intruders to capture and analyze

network traffic.

**A.4 Theory:**

A packet sniffer, sometimes referred to as a network monitor or network analyzer, can be used by a network or system administrator to monitor and troubleshoot network traffic. Using the information captured by the packet sniffer an administrator can identify erroneous packets and use the data to pinpoint bottlenecks and help maintain efficient network data transmission. In its simple form a packet sniffer simply captures all of the packets of data that pass through a given network interface. By placing a packet sniffer on a network in promiscuous mode, a malicious intruder can capture and analyze all of the network traffic.

Wireshark is a network packet analyzer. A network packet analyzer will try to capture

network packets and tries to display that packet data as detailed as possible.

Wireshark is a free application that allows you to capture and view the data travelling back and forth on your network, providing the ability to drill down and read the contents of each packet — filtered to meet your specific needs. It is commonly utilized to troubleshoot network problems as well as to develop and test software. This open source protocol analyzer is widely accepted as the industry standard, winning its fair share of awards over the years.

**Downloading**

Wireshark can be downloaded at no cost from the wireshark foundation website for both macOS and Windows operating systems. Unless you are an advanced user, it is recommended that you only download the latest stable release. During the setup process (Windows only) you should choose to also install WinPcap if prompted, as it includes a library required for live data capture. The application is also available for Linux and most other UNIX-like platforms including  redhat, Solaris, and FreeBSD. The binaries required for these operating systems can be found towards the bottom of the download page in the third party packages section.

**Step 1: Start Wireshark!**  
To open wireshark in Linux (after you have downloaded it) open it in a terminal with: “gksudo wireshark” – this will open the wireshark GUI.

**Step 2: Wireshark GUI**  
Once the wireshark GUI has opened, you’ll see that the dashboard has a left column box called ‘Interface List’. This list lets you know which devices and capture cards you can use. At the top of the application there is an option called ‘Capture Options’ which is exactly that, it allows you to modify and tweak how you would like to capture the packets of data that are being transmitted over your network.

**Step 3. Wireshark Interface**  
If you have a look at your interface list  you’ll see that one of your devices is actually sending and receiving packets. Options include *promiscuous mode* and *capture mode* etc. Have a play around with these and understand what each of these functions does – and you will rapidly learn how to effectively use wireshark.

**Step 4. Capture Interface Options**  
This screen shot shows the wireshark capture interfaces, in other words, it shows what processes and platforms are receiving and sending data on your machine. If you have a wireless card, then it will show it, etc.

**Step 5. The Main Packets Panel**  
Once you are happy with the interface you’d like to use, go ahead and click ‘start’ and wireshark will show all the packets that are being transmitted over your network. If you open a web browser or for exampl,e watch a video on YouTube, you’ll notice a sudden surge of packet data. The whole point here is to find patterns or anything that looks suspicious. Taking the columns at the top of the wireshark interface from left to right, the first number is the ‘packet number’. The second column shows how many seconds it has been since the start of the capture. The third column is the source IP Address and the fourth column shows the destination IP Address. The fifth column is the protocol that sent the packet, i.e. it could be DNS, TCP (Transmission Control Protocol) or even HTTP.

Filtering the packets is key when using wireshark – done by using the search bar within the interface (top left). If you right click on a packet of interest you can ‘follow TCP stream’ and you get a ton of raw information.

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the portal or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)***

|  |  |
| --- | --- |
| Roll. No.: N049 | Name: Tarun Tanmay |
| Class: MBATech CE, 3 Year | Batch: B3 |
| Date of Experiment: 22/7/2020 | Date of Submission: 22/7/2020 |
| Grade: | |

**B.1**

**Input and Output:**

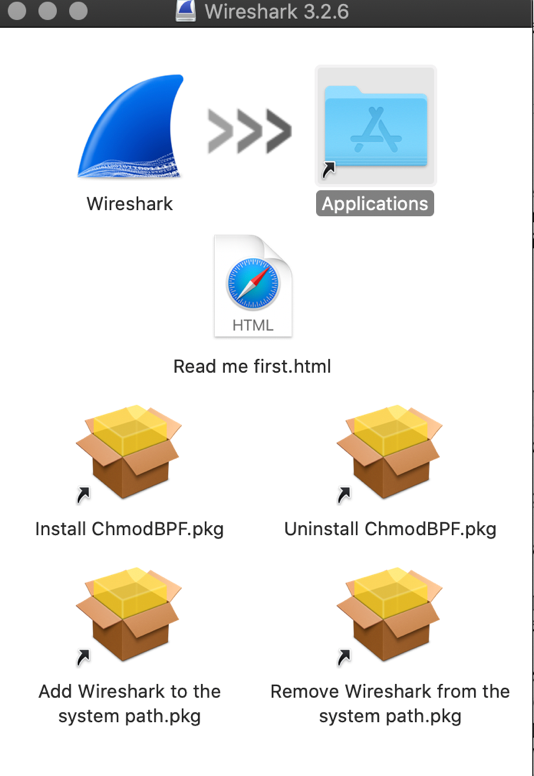
***(Paste your program input and output in following format, If there is error then paste the specific error in the output part. In case of error with due permission of the faculty extension can be given to submit the error free code with output in due course of time. Students will be graded accordingly.)***

**Input:**

Download and install wireshark network analyzer.

**Output:**

**Installation:**

****

**This is the installation wizard that will assist in installing the required files to run the software**

**License agreements that are needed to run the required software. This allows clear understanding of the legal matters surrounding the use of the software.**

**A picture containing game, drawing

Description automatically generated**

**These are the files being extracted and saved on the computer. Now these will be stored and installed in the selected folder to run WireShark.**

**Wireshark:**

**A screenshot of a cell phone

Description automatically generated**

**Interface upon opening the application.**

**A screen shot of a computer

Description automatically generated**

**Packet trace actively running on Wifi. This captures all types of packets currently running through the Wifi.**

**A screenshot of a computer

Description automatically generated**

**Packet trace with “dns” filter applied. This now displays only the DNS packets. The other packets are still being traced but they are no longer being displayed.**

**B.2 Observations and learning:**

The wireshark interface is easy to use but requires practice. There are many available functons, that provide an excess of data to the user. Using wireshark appropriately will learnt only via practice.

The GUI is effective, and the application doesn’t need extra hardware. This software can be used to trace all the data passing through a network.

**B.3 Conclusion:**

A powerful packet tracer that will help use analyze the security of a network.

**B.5 Questions of Curiosity**

***(To be answered by student based on the practical performed and learning/observations)***

Q1: Give the uses of wireshark tool

Wireshark provides us with:

* Live capture and offline analysis.
* VoIP analysis.
* Decryption support for many protocols, including IPsec, ISAKMP, Kerberos.
* Deep inspection of multiple protocols like TCP, STUN.

Q2: List some other packet sniffing tools.

* Burp Suite
* DNSChef
* rtpbreak
* SniffJoke
* VoIPHopper