WireShark

@June 16, 2022

Documentation of Project:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. In this video, I plan to start with a presentation about what wireshark is, what it is used for, its features and also go over some protocols (includes http, tcp, ip, and udp). I then plan to talk about filters and show various examples by capturing local traffic using the command box. I want to go over is packet sniffing, and if possible username and password sniffing with an example with a login page. Additional content I would want to go over is I/O graphs.

Script:

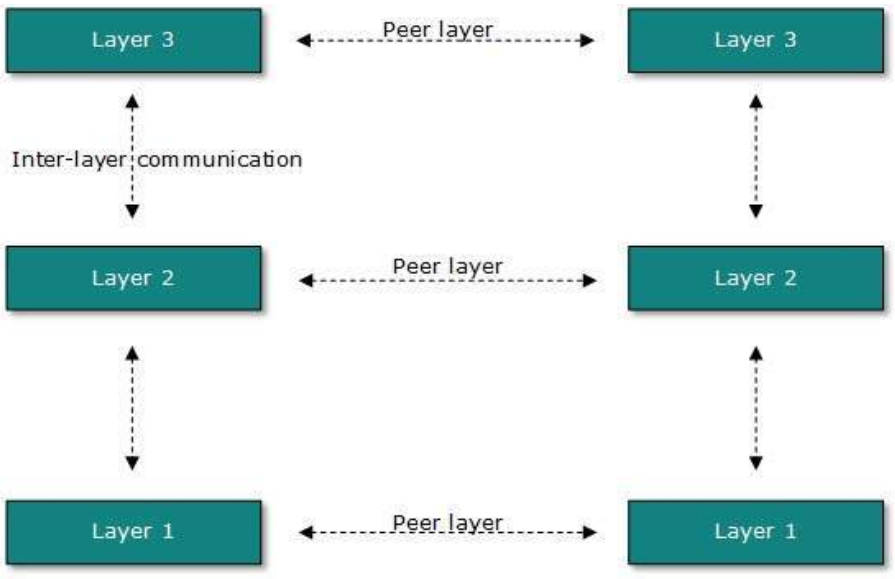
5 minute video

Notes:

Framing some of the concepts:

To ease network engineering, it is divided into multiple layers, that performs a specific task and is independent of one another. They share data by taking input and output from one another.

The task is initialized by either the layer at the lowest level or at the top.



Each layer puts together all procedures, protocols, and methods which it requires to execute its piece of task.

OSI Model

Open System Interconnect, established by International Standard Organization (ISO) in 1984.

(AP Said To Not Dot Product)

Application: providing an interface to application user

Presentation: defines how data in native form of remote host should be presented in the native form of the host

Session: maintains sessions between remote hosts

Transport: end to end delivery between hosts

Network: responsible for address assignment and uniquely addressing hosts in a network

Data Link: reading and writing data from and onto the line

Physical: defines the hardware, cabling wiring, power output, pulse rate

Internet Model:

uses TCP/IP protocol (Transmission Control Protocol/Internet Protocol)

four layered architectures

(Aami Told Inni Laugh)

Application: defines protocol that allows users to interact with the network

Transport: (TCP) defines how network should flow between hosts; ensures data is delivered between hosts (end-to-end delivery)

Internet: (IP) facilitates host addressing and recognition

Link: provides mechanism of sending and receiving actual data

Expanding on the different models: **(compares the different models)**

main aim of layered architecture is to divide the design into small pieces (modularity)

number of layers, functions and contents of each layer will vary from network to network.

Basic elements of layered architecture:

Service: set of actions that a layer provides to the higher layer

Protocol: defines a set of rules that a layer uses to exchange the information with peer entity

Interface: way through which message is transferred from one layer to another layer.

Why do we need Layered Architecture?

Divide and Conquer: reduces the complexity of the design

Modularity: independence of layers

Easy to Modify: implementation in one layer will not affect others

Easy to test: can be analyzed and tested individually

T**he OSI reference model as a reference design of what should happen as each layer of the network stack**

T**he TCP model which is what is generally implemented**

Download and install Wireshark to experiment with it

https://www.wireshark.org/

A pretty comprehensive tutorial on using Wireshark

Outline -

1. What is WireShark?
2. Uses of WireShark
3. What is a packet, TCP/IP/UDP?
4. Features of WireShark
5. Installation of WireShark, start and stop button
6. Filters
   (Whenever we type any commands in the filter command box, it turns **green** if your command is **correct**. It turns **red** if it is **incorrect** or the Wireshark does not recognize your command.)
   ”tcp contains youtube”
   tcp.port == 80 || udp.port == 80 [specific port number]
7. Packet sniffing is defined as the process to capture the packets of data flowing across a computer network. The Packet sniffer is a device or software used for the process of sniffing. (http)
8. I/O graphs

- eventually get too much data here in wireshark as it keep listening to the traffic, so ideally you can stop to inspect the traffic better.
- requests to and from the website
  MAC address and the destination is the mAC address of the webserver
- export data

Script -

WireShark is an open source network scanner monitor that allows you to take a look at traffic and even individual packets that are passing through the particular network interface card you are looking at. It is used for network troubleshooting analysis, software and communications protocol development, and

education. It helps capture network traffic on the local network and stores that data for offline analysis. WireShark also allows you to filter the log either before the capture starts or during analysis to narrow down to what you are looking for in the network trace.

-

Transmission Control Protocol is used on top of Internet Protocol to ensure reliable transmission of packets. It governs how the information is sent and received in the form of packets between source and destination.

Internet Protocol is a unique number assigned to all information technology connected devices such as printers, routers, modems, and so on. Any device that transmits or received internet traffic will be assigned an IP address.

User Datagram Protocol is a communications protocol that is used to establish low latency and loss-tolerating connections between the applications and internet. It speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiving party.

Hypertext Transfer Protocol is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers, but it can also be used for other purposes.

-

“requests to and from the website”

”MAC address and the destination is the MAC address of the webserver”

“eventually get too much data here in wireshark as it keep listening to the traffic, so ideally you can stop to inspect the traffic better.”

-

how to use a filter - “Whenever we type any commands in the filter command box, it turns **green** if your command is **correct**. It turns **red** if it is **incorrect** or the Wireshark does not recognize your command”

-

explain packet sniffing - Packet sniffing is defined as the process to capture the packets of data flowing across a computer network. The Packet sniffer is a device or software used for the process of sniffing.

-

introduce I/O graphs

Presentation

Resources Used -

- https://www.wireshark.org/
- https://www.tutorialspoint.com/data_communication_computer_network/computer_network_models.htm
- https://www.javatpoint.com/wireshark
- https://www.javatpoint.com/osi-model
- https://www.javatpoint.com/computer-network-tcp-ip-model

- https://samsclass.info/106/proj13/p1a_WireShark_HTTP.htm
- https://www.youtube.com/watch?v=TkCSr30UojM

Things to keep in mind:

- eventually get too much data here in wireshark as it keep listening to the traffic, so ideally you can stop to inspect the traffic better.
- requests to and from the website
  MAC address and the destination is the mAC address of the webserver
- export data

Personal Notes -

What is Wireshark?

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.
It captures network traffic on the local network and stores that data for offline analysis. It allows you to filter the log either before the capture starts or during analysis to narrow down to what you are looking for in the network trace.
WireShark is an open source network scanner monitor that allows you to take a look at traffic and even individual packets that are passing through the particular network interface card you are looking at.

What is TCP?

Transmission Control Protocol is used on top of Internet Protocol to ensure reliable transmission of packets. It solves many of the problems that arise from packet-based messaging, such as lost packets, out of order packets, duplicate packets and corrupted packets.
It governs how the information is sent and received in the form of packets between source and destination.

What is IP?

Internet Protocol is a unique number assigned to all information technology connected devices such as printers, routers, modems, and so on. Any device that transmits or received internet traffic will be assigned an IP address.

What is UDP?

User Datagram Protocol is a communications protocol that is used to establish low latency and loss-tolerating connections between the applications and internet. It speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiving party.

What is difference between TCP and UDP?

TCP is connection-oriented protocol, where UDP is connectionless protocol. The speed plays a major difference as TCP is comparatively slower. UDP is much faster, simpler and efficient, however retransmission of lost data packets only occurs with TCP.