IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 2, February 2022

DOI: 10.17148/IARJSET.2022.9228

PACKET SNIFFER

Parul Manhas[1], Jaismeen[2]

Dept. of CSE, Chandigarh University, Mohali, Punjab, India[1,2]

Abstract: Every network consists of various hosts and other networking devices connected to each other. These devices interact with each other to pass meaningful information. This information is transferred in the form of packets. Packets are basically small units of data sent over the network. When a great amount of data is being shared over the network with no supervision it becomes fairly important to collect, identify, and analyse the different types of packets and details as they cross the network. This is where a packet sniffer comes into existence. Packet sniffer is a program that helps to keep track of the packets sent over the network. This is widely done using protocol analysers like Wireshark, TCPdump, or Windump to collect and evaluate packet details. This paper focuses on making a packet sniffer from scratch using python, socket programming and basic networking knowledge. This paper will also explore the existing softwares for packet analysis in brief.

Keywords: Wireshark, ARP Spoofing, Socket Programming, TCPdump, Wiredump, PCAPInclude at least 4 keywords or phrases.

I.INTRODUCTION

The concept of networking finds its roots even before computers were invented and it has been evolving ever since. Every previous model's drawback becomes an innovation for the next. Likewise is the concept of hubs and switches. Whenever a LAN has to be set up, previously it used to be done using hubs. Hubs, as most of us know it, is not a very intelligent device and works on the fundamentals of broadcasting. Even though communication happened smoothly even then, they were not very efficient and secure. If a packet has to be sent from host A to host B using a hub, then all the devices present on that network receive the packet and ignore it if the packet is not destined to their address. But this can be easily manipulated by setting the NIC to promiscuous mode. This way even the other devices can see the packets that were not supposed to be sent to them.

To solve this major issue, the concept of switches came into existence. Switches are a more intelligent device and only direct the traffic where the source wants to send it. This way other devices will not have access to the packets being sent. But this again was countered by the concept of ARP Spoofing which will be explained in detail in the later parts of this paper. This can be done using packet sniffing. Packet Sniffing is a program that helps to collect, identify and analyse all the outgoing and incoming packets in a network. Packet sniffing is not only used by hackers but can prove to be an efficient tool for network management and detecting malicious activities over the network.

Packet sniffer has many applications. Since anyone can upload anything and everything on the internet without someone to keep a check on it, children get exposed to a lot of noxious stuff online. It therefore, becomes a responsibility to check the kind of data they are consuming and that is where Packet sniffing helps.
Another useful application of packet sniffing can be to manage big networks. If there is any kind of latency or delay in the network, we can sniff the packets and find out where exactly the bottleneck is or where the problems are.
Ethical hacking is yet another field where packet sniffing is most commonly used.

II.RELATED WORKS

Pallavi Asrodia et al [1] in their paper have given more focus on the basics of packet sniffing. They have given the knowledge about the various principles on which the packet sniffer works, what are different approaches and how these approaches work. They have focused on the working principles of the packet sniffer which is used for the analysis of network traffic.

Dr. Dayanand Lal N et al [2] in their paper they have focused on the development of a security tool named as 'Secret Credentials Packet Sniffer. All the secret credentials flowing in the network are sniffed by this security tool. Secret Credentials include mainly username, passwords and cookies etc. They have used various networking protocols where packet sniffers are used.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 2, February 2022

DOI: 10.17148/IARJSET.2022.9228

Ogbu N. Henry et al [3] in their paper they have used a LAN packet sniffer to observe the network traffic for internet security. They have provided internet traffic monitoring using a sniffer at the Local Area Network servers for the protection purposes. They have used static Internet Protocol (IP) for implementation. Ethernet cable of category 6, D-link 16-port switch of windows 8 and some other Local Area Network devices were used to deploy the Local Area Network. For analysing and capturing the IP traffic they have used version 2.0.3 of Wireshark.

Rupam et al [4] in their paper have talked about various approaches to detect the packets using packet sniffer to regulate and stop the network traffic, which causes many problems. Different methods are ARP Cache Poisoning, CAM Table Flooding, Switch Port Stealing etc. Sniffing methods like IP Based Sniffing, MAC based Sniffing, ARP based Sniffing. They had shown that packet sniffers are utilised in intrusion detection.

Tom King [5] in their paper they have used the technique of ARP (Address Resolution Protocol) spoofing. This technique can allow an attacker to eavesdrop on network traffic in a switched environment. They have concluded that the Implementation of a layer three encryption technology such as IPSec solves the sniffing problem completely.

Jhilam Biswas et al [6] in their paper they had shown the focus on to make network administrators and technicians aware about the advantages of monitoring the packets in the network. They had used the Wireshark tool for this. They had given practical examples of most attacks which basically occur on Local Area Network. They captured the data Using a Hub, Port Mirroring or VACL (VLAN-Based ACLS), Bridge Mode, Arp Spoof, Remote Packet Capture.

D. Álvarez et al [7] in their paper they have used an emphasised system which may be brought into action in cooperative environments by giving the main target on link and network layers. They have used two techniques of sniffing - scapy and other one is raw sockets. These techniques are ready to detect the layer 2 and 3 attacks and susceptibilities. By using BSD Packet Filtering they have stepped up these techniques and a multicore architecture in order that it can take the sting of interpretation to classification of service attacks.

İbrahim Ali İbrahim Diyeb et al [8] in their paper they'd differentiate between three non-identical sniffing tools; TCPDump, Wireshark, and Colasoft in step with miscellaneous parameters like their power of detection, filtering, availability, OS that supports the particular Tool, open source, Graphic User Interface, their characteristics and features, qualitative likewise as quantitative parameters. The Wireshark charges no money, is open source code powerful, and promotes an outsized number of network protocols and applications which promotes quite 1000 protocols. Colasoft is closed source by Capsa Co., but it provides more security and filtering characteristics, it has good GUI proficiency with tables, graphs, and matrix maps. TCPDump is an open source, portable and inexpensive tool in terms of memory usage. It is used remotely via Telnet by users and only provides TCP/IP protocol.

Apri Siswanto et al [9] in their paper they had shown that the common bandwidth usage per second is 13 Mbps from a median of 125 users. If the count of users is 500, then the standard user gets 40 kbps with appropriate Internet browsing access. For users to approach information systems or cloud-based systems, the user needs a minimum of 200 Kbps. And in video streaming a user needs 300 kbps. After scrutinising many things they'd shown that it's better to use 100 Mbps internet bandwidth packages.

Muhammad Syaffiq Abdul Malek1 et al [10] in their paper they have used the Wireshark tool packet analyzer. This packet sniffer accommodates many characteristics that are easy to use, user friendly, efficient, and supply accurate data of the packets captured. Wireshark has the flexibility to decrypt HTTP traffic, take off pictures from raw data, observe TLS handshake of HTTPS traffic, and fine-tune websites down.

III.LITERATURE REVIEW:

A.Wireshark: Wireshark is a protocol analyser which helps us supervise our network at a microscopic level. It gives the information of many protocols and the protocols are still being added every day. It helps us to inspect the packet in real time and is also multi-platform, i.e., it can run on Windows, macOs, Linux, Solaris, netBSD and many other Operating Systems. It is user friendly and provides a GUI to look at the captured data. Decryption support is provided for various protocols, like IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
It allows us to apply colouring rules to the packet list for quick, intuitive analysis.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 2, February 2022

DOI: 10.17148/IARJSET.2022.9228

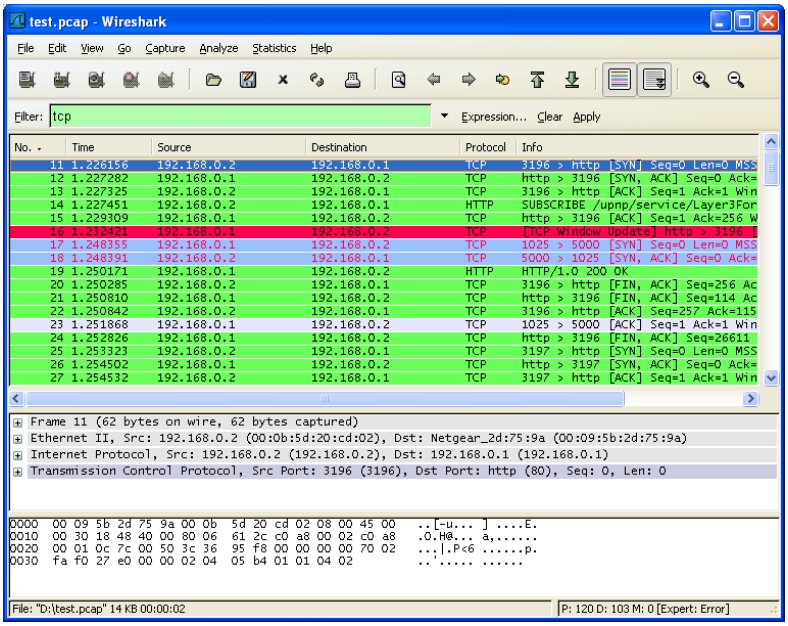

Fig. 1 Wireshark Tool [11]

B. TCPdump: TCPdump is yet another packet analyser which is coded in C/C++. It provides a command line interface. It provides all the information of a packet using various commands. Some of the common tcpdump commands are as follows: tcpdump port 3389 to show traffic related to given port, tcpdump icmp to show traffic of any given protocol, to show only ipv6 traffic, tcpdump ip6 command is used, one can also find traffic using port ranges, command for the same is tcpdump portrange 21-23. Packets can also be searched using packet size. For example, tcpdump less 32, tcpdump greater 64, tcpdump <= 128. Tcpdump also enables us to read/write captures to a file.

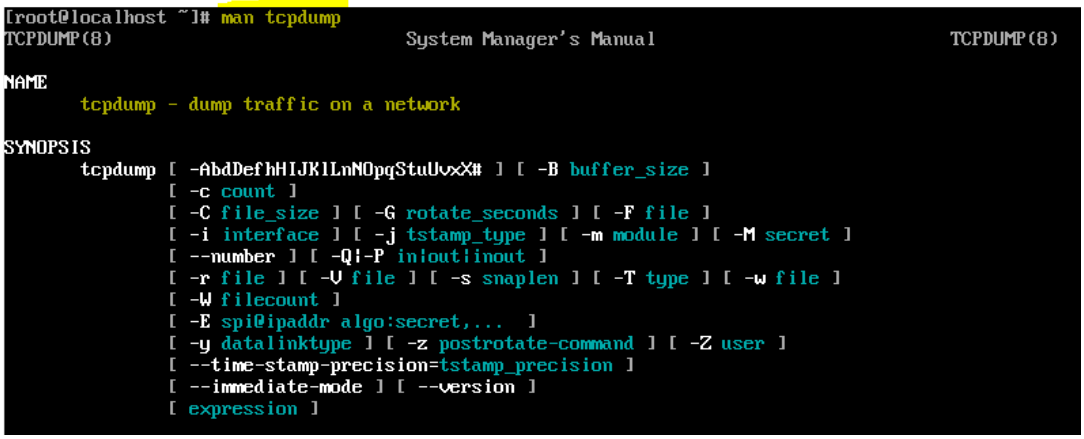

Fig 2. Tcpdump interface [12]

C. PCAP: PCAP stands for Packet Capture and it is an Application Programming Interface which is used for capturing live traffic from a network. It operates on layers 2 to 7 of the OSI model. If we want to Capture any traffic in the form of UDP or TCP then we have to create a file with the .pcap extension. Most Network Analysis tools like Wireshark use pcap for capturing network traffic. To capture pcap files we need two things. First is the interface that we want to sniff on and the second is the type of traffic we are trying to look at or monitor. The type of traffic can either be TCP/IP or UDP. There are different versions of PCAP namely, Libpcap WinPcap, PCAPng and Npcap.

D. ARP spoofing: This is a type of network attack where an attacker tries to scan the packets sent over a network by saying that he is one of the devices participating in the communication. For example if host A wants to send packets to host B. Then the attacker will fake the IP address and MAC address of host A and tell B to respond to the packets received from IP address of host A to the mac address of the attacker's device. This way host B will think that he is communicating with host A but it is actually the attacker who is faking the mac address of host A. The attacker will associate the victim's

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 2, February 2022

DOI: 10.17148/IARJSET.2022.9228

IP address to the attacker's MAC address. The attacker will then get hold of the packet, analyse it and then send it to the original host. Since the source and destination machines are receiving the packets, they would think that a normal communication is going on when in reality, the attacker is keeping a track of the entire communication and analysing all the packets being sent over the network. Firewalls are not able to detect these types of attacks because they are not monitoring all the network devices mostly because they don't know which IP address is mapped with which MAC address. But there is still a solution to this problem. There are ARP spoofing detection tools available with all Operating Systems like XArp for windows and linux.

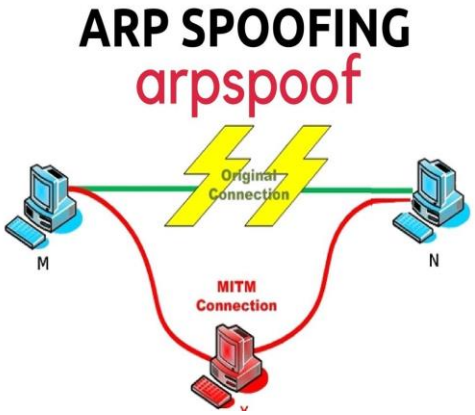

Fig. 2 ARP Spoofing [13]

IV.METHODOLOGY

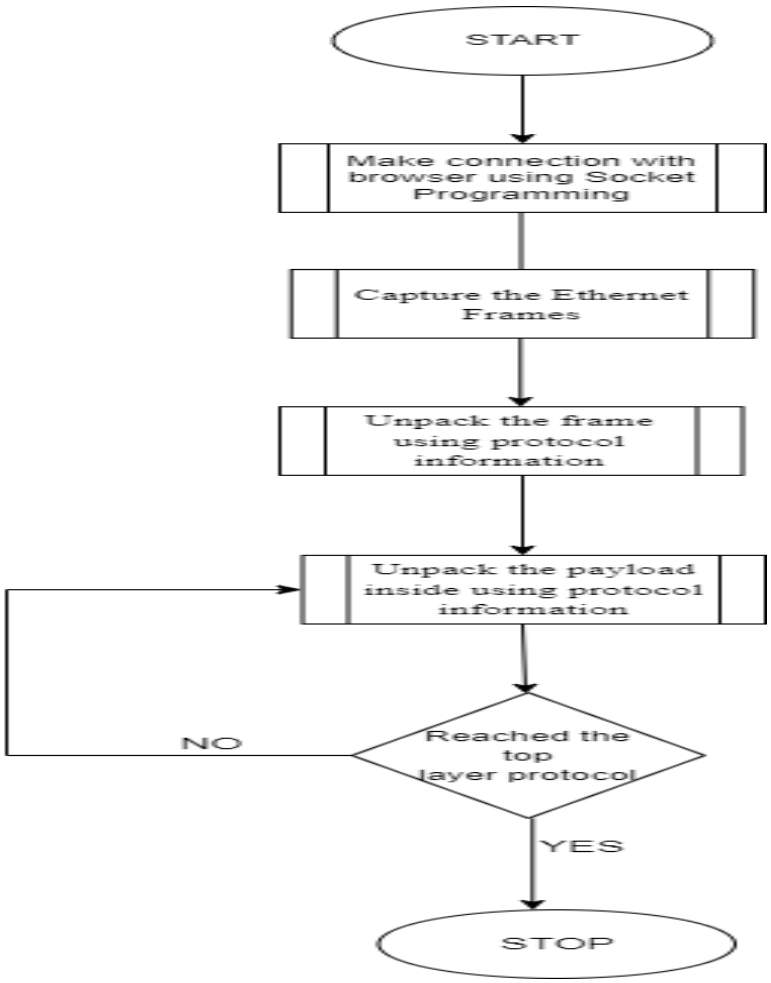

Fig. 3 Flowchart of Packet Sniffer

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 2, February 2022

DOI: 10.17148/IARJSET.2022.9228

1) Capture the Ethernet Frames:

The first and foremost step is to capture the Ethernet frames. Ethernet frames basically contain the information/data to be sent between two communicating nodes along with the necessary set of conditions like source address, destination address, protocol, etc in a specific format standard as defined by IEEE. These frames operate on the data link layer. This is done using socket programming. The two end to end nodes that are connected to exchange information are known as sockets. Inter Process Communication (IPC) takes place between these nodes using named pipes. Once the connection has been established between the sockets. We capture the incoming traffic in the form of ethernet frames.

2) Unpack the frame using the protocol information:

Once we have the frames with us, the next step is to extract meaningful information from with the help of the ethernet frame format provided below:

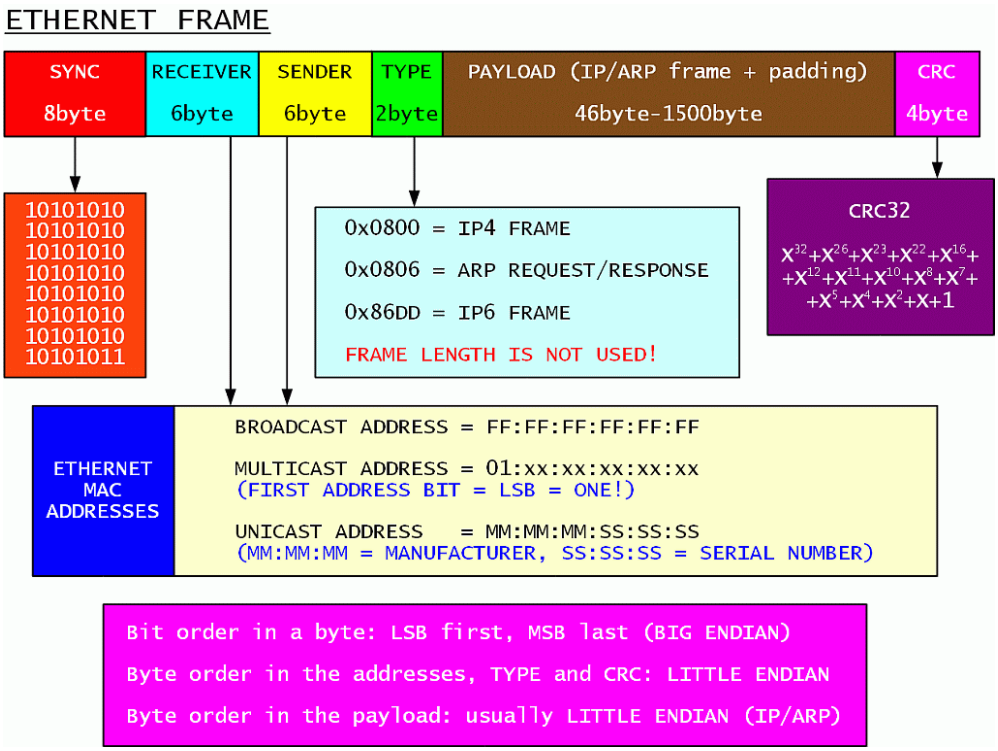

Fig. 4 Ethernet Frame [14]

In the above diagram it is clearly visible that the first 8 bytes are reserved for synchronisation between the two communicating devices. It is further divided into preamble field and SFD field. Preamble field consists of 7 bytes. Preamble bytes are used to inform the receiver when an ethernet frame starts. The SFD field stands for Start Frame Delimiter and it is only one byte long. It is used to stipulate to the receiver that the next byte of the ethernet frame is the MAC address of the destination.

The next 6 bytes are assigned for Destination address. Since it stores the MAC address of the destination and MAC addresses are 6 bytes long therefore this field has a size of 6 bytes. Destination address in an ethernet frame is useful because a receiver can identify whether the frame was directed towards it or not.

The next 6 bytes is the MAC address of the sender. The receiving device can identify the source using this field.

The next 2 bytes are reserved for the type field. This field tells us about the protocol being used in the communication and this protocol belongs to the upper layer which is the network layer. This is important because on the sender's side, the network layer hands over the message to be sent to the data link layer which in turn packs the data into frames that we are referring to as ethernet frames and sends them to the receiver. The receiving side data link layer receives these frames and unpacks them to send them over to its upper layer (network layer). The type field makes it easier for the data link layer at the receiver's end to identify the protocol to which it should pass the frame to.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 2, February 2022

DOI: 10.17148/IARJSET.2022.9228

The next field is the Payload/Data and Pad Field. It comes with size ranging from 46 bytes(minimum size) to 1500 bytes(maximum size). THis field carries the encapsulated data sent by the upper layer. Due to its fixed range of size, more than 1500 bytes of data and less than 46 bytes of data can not be packed.

The next 4 bytes are reserved for CRC(Cyclic Redundancy Check) or FCS(Frame Check Sequence). This field is used to verify the frame being sent. If the CRC value of sender matches with the CRC value of receiver it means that the frame is good and the receiver accepts it. Otherwise, if they fail to match, it means that the frame is incorrect or corrupted so the entire packet is dropped.

3) Unpack the payload inside the frame using the protocol information :

Now that we have the ethernet frame we need to dig deeper to extract the relevant information which includes the type of protocol being used, the ip address of both the sender as well as receiver, etc. This can be achieved by having a thorough understanding of the ip packet.

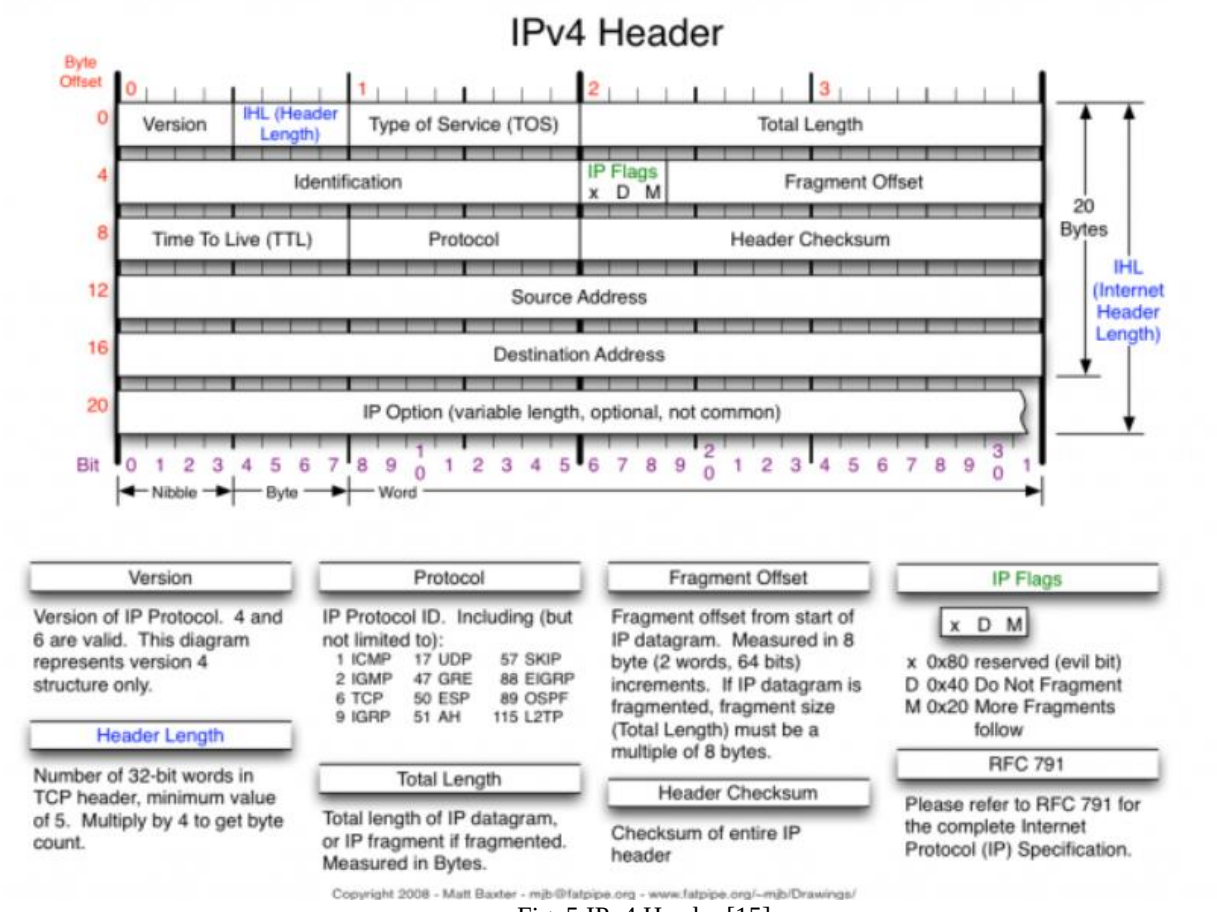

Fig. 5 IPv4 Header [15]

Version – Defines which version of protocol is being used. It can either be IPv4 or IPv6. In case of IPv4 the value of this field is 4 and in case of IPv6 the value of this field is 6.
Header length – The header consists of 32 bit words. The value ranges from 20 bytes to a maximum value of 60 bytes.
Priority and Type of Service – The handling of the datagram is specified here.. The first 3 bits of this field are called the priority bits.
Total length – This field defines the length of the entire packet which is a combination of the header and data. The length ranges from a minimum length of 20 bytes and goes to a maximum of 65,535 bytes.
Identification – fragmented packets are differentiated from different datagrams using this field.
Flags – fragments are identified and controlled using flags.
Fragmented offset – If the packet has a size greater than the normal size required to fit in the datagram ,it undergoes fragmentation and reassembly. That part is handled by this field..
Time to live – Defines the lifetime of a datagram. If the TTL expires before the datagram reaches its destination, the datagram is discarded.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 2, February 2022

DOI: 10.17148/IARJSET.2022.9228

Protocol – Tells about the protocol being used for the communication to take place. For example, TCP has number 6 as its representation and UDP is represented by 17.
Header checksum – Used to verify and validate the header. If the checksum calculated by the router does not match the one specified in the header checksum field, it indicates a discrepancy and hence, the packet is discarded.
Source IP address – the IP address of the sender in the communication.
Destination IP address – the IP address of the receiver in the communication.
Options – This field is rarely filled. Used for testing of the network as well as debugging, security, etc.

4) Keep doing this until we get to the top layer protocol.
This process of unpacking the frames and datagrams is repeated until the program is running and our computer has a stable internet connection and is connected to the network where it can send and receive packets. All the packets are captured and will be analysed thoroughly by unpacking them till we reach the top layer protocol. This way we can have the required packet information and sniff the packets that we want to.

V.CONCLUSION

Network Packet Sniffers are a very important part of the layered defence model. Packet sniffers are handy tools that can be used for genuine as well as malicious purposes. The consequences depend on which purpose they are used in. Packet sniffer gives us the advantages of doing traffic analysis, troubleshooting, Data Processing, some instructional purposes and network traffic monitoring. Packet sniffer is very user friendly and it is very easy to use. It can easily adopt the new changes. It takes less memory storage because we can easily export the captured data to a database. When computers communicate with each other they only listen to the traffic which are just meant for them but network cards have the ability to enter the promiscuous mode which in turn makes them able to listen to all the traffic regardless of if it is for them or not. Packet sniffers can capture things like username, clear text, passwords or other sensitive material. It may also be used by attackers to capture plain text data or research user behaviour. That is why some measures can be taken during the implementation of the protocols so that we can ensure that there is no use for an intended purpose. Sniffing is possible on switched and non-switched networks. There are various tools available for network traffic analysers but each of them have some limitations. Some tools required large memory, some tools only captured network traffic without analysis. By this research we can conclude that the packet sniffer is very good to be used in intrusion detection.

REFERENCES:

[1] Asrodia, Pallavi, and Hemlata Patel. "Network traffic analysis using packet sniffer." International journal of engineering research and applications 2.3 (2012): 854-856.
[2] Nayak, Mr Parikshith, S. H. Brahmananda, and Mrs Sahana DS. "An Approach to Sniff Sensitive Information by Packet Sniffing."
[3] Ogbu, Henry N., and Moses Adah Agana. "Intranet Security using a LAN Packet Sniffer to Monitor Traffic." arXiv preprint arXiv:1910.10827 (2019).
[4] Verma, Atul, and Ankita Singh. "An approach to detect packets using packet sniffing." International Journal of Computer Science and Engineering Survey 4.3 (2013): 21.
[5] King, Tom. "Packet sniffing in a switched environment." SANS Institute, GESC practical 1 (2002).
[6] Biswas, Jhilam. "An insight into network traffic analysis using packet sniffer." International Journal of Computer Applications 94.11 (2014).
[7] Robles, David Álvarez, et al. "Performance Analysis of Packet Sniffing Techniques Applied to Network Monitoring." IEEE Latin America Transactions 19.3 (2021): 490-499.
[8] Diyeb, Ibrahim Ali Ibrahim, Anwar Saif, and Nagi Ali Al-Shaibany. "Ethical network surveillance using packet sniffing tools: A comparative study." International Journal of Computer Network and Information Security 10.7 (2018): 12.
[9] Siswanto, Apri, Abdul Syukur, and Evizal Abdul Kadir. "Network traffic monitoring and analysis using packet sniffer." 2019 International Conference on Advanced Communication Technologies and Networking (CommNet). IEEE, 2019.
[10] Malek, Muhammad Syaffiq Abdul, and Ahmad Roshidi Amran. "A Study of Packet Sniffing as an Imperative Security Solution in Cybersecurity." Journal of Engineering Technology 9.1 (2021): 96-101.
[11] https://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayFilterSection.html
[12] https://www.techplayon.com/tcpdump-for-linux-system-a-tool-for-ip-packet-analysis/
[13] https://www.pcnerds.co.za/using-ssltrip-and-arpspoof-to-get-user-passwords/
[14]https://guidedhacking.com/threads/python-win32-sockets-packet-sniffer-network-to-host-endianess.15013/
[15] https://countuponsecurity.com/2013/04/01/the-evil-bit/

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 2, February 2022

DOI: 10.17148/IARJSET.2022.9228

BIOGRAPHY

Parul Manhas is a third year student at Chandigarh University, currently pursuing Bachelors of Technology in Computer Science and Engineering. Her field of interest is networking, cloud computing and image processing.

Jaismeen is a third year student at Chandigarh University, currently pursuing Bachelors of Technology in Computer Science and Engineering. Her field of interest is networking, programming and front end development.