ISSN No:-2456-2165

# Restraining Packet Sniffing & Security: A Brief Overview

Sourabh Saroha
HCL Australia Pty Ltd

**Abstract:- Over the years, with every passing day, the communication systems are increasing in size, complication and laterally the users are also being improved successively. Due to this reason the traffic congestion in the communication network has also raised rapidly. Hence it is necessary to keep an eye on every node in the network, packet sniffer is used. Sometimes a packet sniffer is called a network monitor or network analyser. Many system administrator or network and security administrator use it for monitoring and troubleshooting network traffic. Packet sniffers are convenient for both local area network and radio environment networks. In this paper we have describe the nuts and bolts of packet sniffer, and the workings in both local area network and radio environment networks, outbreak and refuge.**

***Keywords***:- *Protocols, Packet Sniffer, OSI Model,Credencials.*

## I. INTRODUCTION

Packet sniffing is a way of wiretap each packet during its movements across the network; i.e., it's a procedure where the network gets to know that the information is not from the same network, it came from different network. In simple terms Packet sniffing is the repetition of gathering, accumulating, and logging some or all packets that transmitted across computer networks, regardless of how the packet is addressed. Packet sniffers can function as a governmental tool or for malevolent commitments. It depends on the user's intent. Network & Security administrators use them for monitoring and validating network traffic. Packet sniffers are primarily alluring.

The recording of the voice through the phonic conversation can be considered as an attack for this reason it is necessary it is necessary to keep an eye on the network where the information is exchanged. When there is the use of detecting tool, we can protect the important and secret data which also include Email traffic (SMTP, POP, IMAP traffic), Web traffic (HTTP), FTP traffic(Telnet authentication, FTP Passwords, SMB, NFS). The encoded data packets are not changed during the process of sniffing. Packet sniffers be able to watch, demonstrated, and record the congestion. The network layer in the Transmission Control Protocol/Internet Protocol (TCP/IP), the packet sniffer programs are used to declaim packets.

Figure 1 shows a typical packet sniffer package in succession on Ethernet. The packet sniffer listens to the data that arrives at the wire or wireless network of any given environment. These packet sniffers are and can be used in any of the network present, it may local area network, wide area network and many more. If a machine is in the path of two connected machines (X and Y) on a wide area network, the machine can listen to the traffic flowing from X to Y.

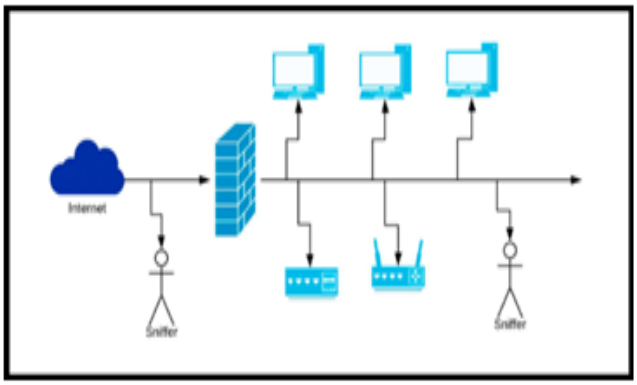


**Fig 1. Packet Sniffer**

The proprietor resolve the problems that are detected by the network and confirm safe link data allocation by resources of the material gathered by packet snipers. Sniffers defense susceptibility exist in the potential to monitor all incoming and outgoing messages, including passwords, usernames or other sensitive material. Network Protocols use network packets transmit information between nodes of the communication channel. Majority of network protocols like HTTP, FTP which transfer information in plain text are exposed to packet sniffing attack. Since, network packet carry secret evidence computer-generated offenders search for secret information in packets and can manipulate packet data. So, use of secure protocols, data encryption technology, network monitoring and Network Scans are used while relocating undisclosed material over the networks. Data confidentiality ensures that no unauthorized entities can decipher the routing information on its way to a destination; reliability talk about to the reliability of records or capitals and it is frequently expressed in rapports of foiling indecorous or unlicensed change. Veracity includes data uprightness (the gratified of the evidence) and source reliability.

ISSN No:-2456-2165

## II. BACKGROUND AND LITERATURE REVIEW

Packet Sniffer is a schmoosed supercomputer solicitation that reflexively accepts edgings of all data-linking layers moving via the system device of a system. This is also known as the Ethernet Sniffer or Network Analyzer. The packet sniffer gathers and stores data for further study that is forwarded to other computers. This can be legally used to track and address network traffic by a network or device administrator. Using the data gathered from the packet sniffer, a director is able to detect incorrect packets and use them to locate bottlenecks and ensure a secure transfer of network traffic. Sniffers protection risks consist of their ability, like passwords and usernames or other confidential material to catch all incoming and outgoing traffic. In principle, since they are inactive in design, it is difficult to detect this sniffing device. (PallaviAsrodia, 2012).

*Applications of packet sniffing program*

- Sorting files during the system. Solving related challenges (in wired and wireless communication network). Connectivity issues.
- Network output review. Therefore, it is possible to locate the bottlenecks in a network or identify the portion of the network through which data was missing.
- Detecting network intruders. (Nimisha P, 2014)

## III. SNIFFING METHODS

Three types of sniffing methods are used. These are:

### *A. IP Based Sniffing*

Theutmost frequently usedtechnique of packet sniffing is Internet Protocol based sniffing. In this process a prerequisite of site system card hooked on licentious manner exist. As soon as system card is fixed into wanton method then swarm resolve be able to snuffle all packets. A significant point in the IP based snuffling is that it uses an IP based filter, and the packets identical the IP address filter is apprehended only. Customarily the IP address sieve is not established so it can seizure all the packets. This technique only the whole kit and caboodle in non-switched network [3].

### *B. MAC based Sniffing*

[3]The second way of sniffing data is packet sniffing. This method is similar to IP based sniffing. The working of MAC based sniffing is analogous to IP based, only the difference is the used of IP filter. Here also a requirement of setting network card into licentious mode survives. A MAC address is used in habitation of IP address filter and sniffing all envelopes corresponding the MAC addresses [3].

### *C. ARP based Sniffing*

[3] The working of ARP based sniffer is different from that of other two.In this method it is not necessary to put the network card in licentious type. The reason is Address Resolution Protocol itself provides the information that the network card does. If there is any change in environment of the network this type gives the better results.

## IV. CASE STUDY

### *A. Troubleshooting Application Data upload with Packet Sniffing*

This case study is related to troubleshooting the application network communications with packet sniffing**.** A business customer from internet network using an Application front end service reported that video data uploading through application would suddenly fail and disconnected several times a day during peak business hours**.**This happened after entering application authentication login credentials. The problem persisted despite replacing the internet connection and gateway**.** Network and Security Professionals checked login authentication and data upload conditions using the data-capture analysis support tool and found that the event would typically occur when user entered credentials and then number of packets had risen dramatically, which occurred just after 10:00 AM. Hence**,** it is considered the possibility that the non-transmission of RTCP packets from the VPN gateway was related in some way to the large number of network data packets upload failure.

### *A. Analysis of Case Study*

The practical implementation of packet sniffing in real time scenario was elaborated above. The problem in the network communication which was solved by trouble shooting the network packets. Packet Sniffers data packet capture were used during the phase of troubleshooting. While troubleshooting, packet sniffer were placed on source machine of business customer and destination server of Application. The TCP and RTCP packets were captured and the issue was identified. The identification of problem and issue present in video based data file upload was facilitated by Packet Sniffing technique. The users was not using the SSH based secured login nor was using a HTTPS or VPN to connect to application server.There are different scenarios and more complex networks are there where Packet Sniffing know how to be cast-off.

### *B. Open Systems Interconnection Model (OSI Model)*

OSI model is hypothetical approach refer to by what method records and evidence drives transversely in the internet. The open system source consist of seven layers that works on various protocols, rules and network policies. The model functions from the topmost as application layer and finishes to physical layer. The number of protocols that works on the OSI model are hypertext transfer protocol, file transfer protocol other protocols that also is address resolution protocol depending upon the application of the user. The OSI Model was initially designed to provide device manufacturers with a collection of design specifications for contact. The OSI model describes an architectural framework which logically partitions the functions needed to facilitate system to system communication.

ISSN No:-2456-2165

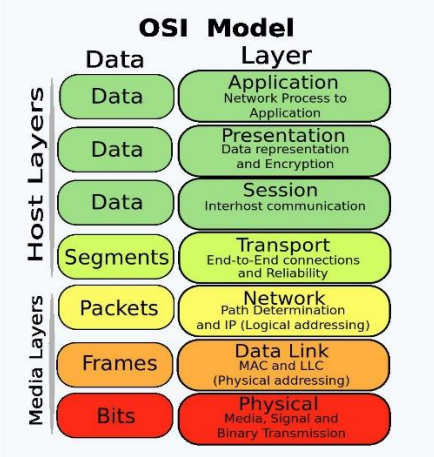

Fig 2: basic model of OSI model

The main function of OSI layers are as follows:
7. Application: It make available diverse amenities to the solicitation and interrelate with the user. Transfer protocols like http, ftp functions in this layer.
6. Presentation: Helps in transfigures the material to various scrambling and encryption methods. This layer is tending with the composition and semantics of the information transmitted.
5. Session: Levers glitches that are not communication concerns to uphold tenacity session.
4. Transport: Agree to take data from session layer and make available end to end communication control.
3. Network: Regulator process of subnet, conveniences course-plotting overcrowding, control and bookkeeping.
2. Data Link: remove the error also controls it. Mostly works on local area network protocols.
1. Physical: it helps in decrypting the data and connects to the data link layer.

## V. PACKET SNIFFING WITH RESPECT TO NETWORKING PROTOCOLS

Network Protocols function in countless layers of OSI Model. Networking protocols are hand-me-down for communication and relocating data into a number of nodes of the network**.** Network Protocols depend on network packets for transmitting information and identifications. Henceforth, arrangement Packets are noteworthy inscriptions of packet sniffing programs. Several conversation cards procedures have diverse device for transporting information. Some of the application layer protocols like HTTP, FTP, and telnet transfer the information and credentials in ordinary manuscript. This makes these protocol liable to packet sniffing attack**.**An assailant can unveiling innumerable bouts like ARP satirizing to apprehension credentials that are reassigned in plain text. By the side of discretion and veracity of evidence is wholly concerned as the user can deploy and bring alteration in the information. Presentation layer protocols Secure Socket Layer, Transport Layer Security, alters information into many encoded text. The amalgamation of protocols from application layer and presentation layer like HTPPS, SSH transfer credentials in encrypted information which varieties them impervious to packet sniffing attack. These exchange cards protocols contrivance cryptographic algorithm to renovate data into encrypted cryptograph which checks sniffing attack. Some of the protocols are secure version over their unsecure protocol. Example, https over HTPPS, SSH over telnet etc. Finally, to maintain confidentiality, integrity and availability of information, encrypted and secure protocols should be always be used that transfer information in encrypted text.

## VI. WORKING OF HTTP PROTOCOL IN APPLICATION LAYER

The packet sniffer program is perform in the application layer for the practical application we have used the local host. Some of the programs are performed in this section.

### *1) Step 1:*

In this part the a secret message is send to the destination in the form of plain text message, the work of the packet sniffer is to have a look on all the transmitted data and received data through the network. The user or the sender can send the data in the form of first name, password, any ID's, token etc.

Fig 3: Packet sniffer running in the background

### *2) Step 2:*

Each packets that are from the transmitter to the receiver, being monitored by the sniffer that is running in the background.

Fig 4: local host with the identifications

### *3) Step 3:*

The packet sniffer program keep a watch on the encoded data that are present in the wired or wireless network. When the program find the useful data i.e. the e-mail id, username in the simple sentence, it immediately apprehensions the information. The program apprehensions other identifications alike cookie, session id.

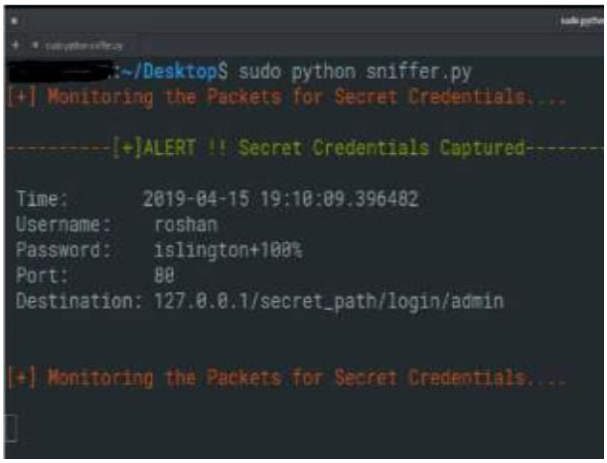

Figure 5: Capture of secret identifications by python script

***Deterrence in contrast to Packet Sniffing***

There are various issues related to Packet Sniffing which are to be prevented so as to protect any loss of the data. Ways to avoid the problems:

1) Only the primary channels should be used to transfer any type of confidential type of data or information. We can also use the encrypted standard which will helps not to corrupt the data in the domain of the user.
2) Also by using the virtual private network the transmitted data can be secure between the source and the destination.

## VII. CONCLUSION AND FUTURE WORK

For any layered model it is very necessary to protect the information that is transmitted inn the network between the source and the destination. It is very easy to use the network sniffer for the actual communication or it can be also used malevolent purposes**.** This might furthermore exist for network traffic flow, data handling, troubleshooting and instructional tenacities, and determinations of bout. Prevention should be taken so that there should not be any misuse of any protocols during the implementations. Effective use of data encryption techniques, Secured SSH login, HTTPS protocol use and network tunnel connectivity using virtual private network (VPN) can be some of way of preventions from Security point of view. In the same way, instance working on the study proved that many envelop and encrypt of data. In this paper we have given the practical implementation of the packet sniffer being used in the network and also the protective measures. There are many ongoing projects are present that are all working on this topic. As many are working on it there are some areas where we can focus on is to decrypt the encrypted data in the environment in which it is present, also in ipv6 network.

## REFERENCES

[1]. EtherealPacketSniffing,Available:netsecurity.about.com/od/readbookreviews/gr/aapro52304.htm.
[2]. Miller, R. (2019). The OSI Model: An Overview. SANS Institute. Page(s):5-12
[3]. PallaviAsrodia, H. (2012). Network Traffic Analysis Using Packet Sniffer. International Journal of Engineering Research and Applications.
[4]. Tom King, “Packet sniffing in a switched environment”, SANS Institute, GESC practical V1.4, option 1, Aug 4th 2002, updated June/July 2006.
[5]. Ryan Spangler, “Packetsniffingonlayer2switchedlocalareanetworks”,
[6]. Sconvery, “HackingLayer2:FunwithEthernetSwitches”, Blackhat, 2002, Available:http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf.
[7]. Rupam, AtulVerma, Dr, and Ankita Singh. "An Approach to Detect Packets Using Packet Sniffing." International Journal of Computer Science & Engineering Survey (2013): n. page. Web.
[8]. Nucci A &Papagianaaki, K (2009). Design , Measurement and Management of Large-Scale IP Networks
[9]. Sanders, C., & Smith, J. (2014). Applied Network Security Monitoring
[10]. Protocol Layers and the OSI Model [2018] , Online Available at https://docs.oracle.com/cd/E19455-01/806-0916/ipov-7/index.htmlAccessed on [2019.04.28 ].
[11]. Credentials packet sniffing: https://iotsecuritynews.com/packet-sniffer-to-sniff-sensitive-credentials-only/
[12]. PacketwatchResearch:http://www.packetwatch.net, Dec 2003.
[13]. Cristina L. Abad, Rafael I. Bonilla, “An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks”, 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07), IEEE,June 2007.
[14]. H. AbdelallahElhadj, H. M. Khelalfa, H. M. Kortebi, “An Experimental Sniffer Detector: Sniffer Wall”, S´Ecurit´e des Communications sur Internet (SECI02), September 2002.
[15]. Daniel Susid, “An evaluation of network based sniffer detection; Sentinel”, School of Economics and Commercial Law, GÖTEBORG UNIVERSITY Department of Informatics, 2004.
[16]. Jorge Belenguer, Carlos T. Calafate, “A low-cost embeddedIDS to monitor and prevent Man-in-the-Middle attacks onwired LAN environments”, International Conference onEmerging Security Information, Systems and Technologies, IEEE, pp. 122-127, October 2007.
[17]. Ryan Spangler, “Packet Sniffer Detection with AntiSniff”. University of Wisconsin, Department of Computer and Network Administration, May 2003.
[18]. RaedAlomoudi, Long Trinh, Darleen Spivey, “Protecting Vulnerabilities or Online Intrusion: The Efficacy of Packet Sniffing in the Workplace”, Florida Atlantic University ISM 4320, 2004.
[19]. Dick Hazeleger, “Packet Sniffing: A Crash Course”, Netherlands, 2001.
[20]. Chris Senders, Practical Packet Analysis, using Wireshark to solve real-world network problems, No Starch Press Inc, San Francisco, 2007.

[21]. Sabeel Ansari, Rajeev S.G., Chandrashekar H.S, "Packet Sniffing: A Brief Introduction", VOL. 21, pp. 17-19, IEEE, December 2002.
[22]. A. Meehan, G. Manes, L. Davis, J. Hale, S. Shenoi, "Packet Sniffing for Automated Chat Room Monitoring and Evidence Preservation", Proceedings of the Second annual IEEE Systems, Man and Cybernetics Information Assurance Workshop, New York, pp. 285-288, June 2001.
[23]. Greg Barnett, Daniel Lopez, Shana Sult, Michael Vanderford, "Packet Sniffing: Network Wiretapping", Group project, INFO 3229-001, 2002.
[24]. Ryan Spangler, "Packet Sniffing on Layer 2 Switched Local Area Networks", Packetwatch Research, December 2003.
[25]. Thomas M. Chen, Lucia Hu, "Internet Performance Monitoring", Proceedings of the IEEE, pp. 1592-1603, VOL. 90, NO. 9, September 2002.