International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Creating an Effective Network Sniffer

Suyash Garg

Jain Deemed to be University, Bangalore, Karnataka, India

ABSTRACT

The sniffer catches these bundles by setting the NIC card in the promiscuous mode and inevitably unravels them. The decoded data can be utilized in any capacity relying on the expectation of the individual concerned who translates the information (for example malevolent or useful reason). Contingent upon the organization structure one can sniff all or just pieces of the traffic from a solitary machine inside the organization. Nonetheless, there are a few techniques to dodge traffic narrowing by changes to access traffic from different frameworks on the organization. This paper centers around the essentials of packet sniffer and its working, creation of packet sniffer on Linux environment and its utilization Intrusion Detection System (IDS).

KEYWORDS: *Intrusion Detection System, NIC, Network sniffer, Ethernet, packets, Tcpdump*

How to cite this paper: Suyash Garg "Creating an Effective Network Sniffer" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.108-112, URL: www.ijtsrd.com/papers/ijtsrd35802.pdf

IJTSRD35802

1. INTRODUCTION

Network sniffer or packet sniffer both are sister term both of have different meaning but on a high level they have same work to sniff network traffic that is going from computer to network (outbound/ Egress) or network traffic that is coming from network to computer (inbound/ ingress) many person think that network sniffer is only use by hacker to launch attack well this statement is not wrong but is also not always true hacker generally try to find low hanging fruit for ex they try to find which software version company/organization uses, open and closed port, bad security practice like employee use same password in multiple account or they try to find pattern of password in leak database etc sniffing a network packet is always last option for any cyber attack but why answer is simple due to large amount of packet that comes every second on a single computer if start network sniffing only in 1 minutes more than thousands of packet was send and comes to my system not only for my system of any system in the world that is connected to internet there are two main reason for this first is reason due network is manage by many protocol work differently but they need one another to complete their work for ex in fig 1 there was screen shot of wire shark that show client communication between NTP(Network Time Protocol) without NTP no one in the world is able communicate NTP sync the clock of every system that connect to internet and there are many protocol that needed to establish a connection between two party

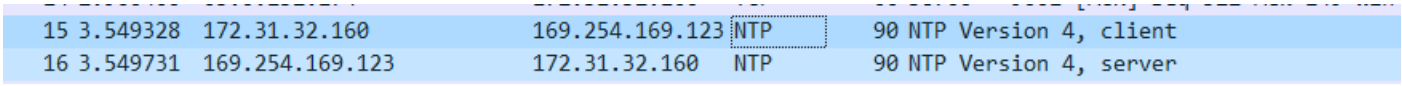

Figure 1

The second reason was this how the internet was made any connection was made is different from another connection and both connection has no relationship to another connection that was made this feature was also known as stateless nature of internet this nature was very important whit out this nature there is no way internet was able to work efficiently there is too much information to store in every network device fig 2 show the packet in hadoop slave sending heartbeat packet to master in every 3 seconds

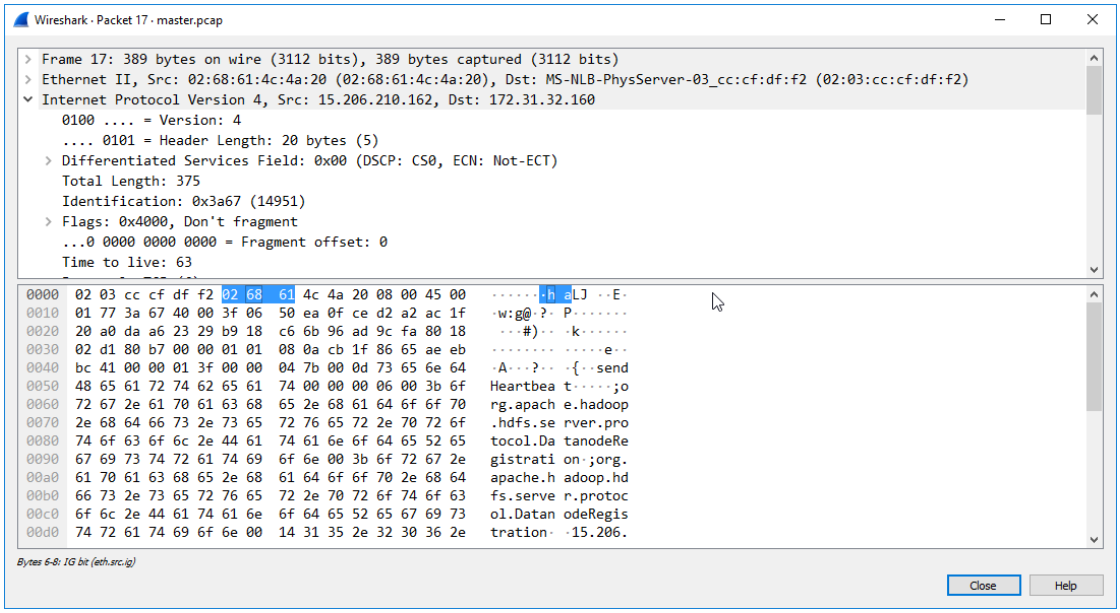

Figure 2

Not just hadoop slave everywhere in the world of networking whenever we follow client server kind of architecture we have to send that small-small packet they are generally known as keep alive packets. This packet sent from client to the server at every fixed amount of time to say that I am client a I am still connected to you this sound very tedious process but believe this method is much faster and reliable then doing TCP three way hand shaking protocol every time whenever client try to connect with server.

Due to the following reason network packet is too big it takes good amount of computing power to find useful information that helps to launch an full-fledge cyber attack.

So packet sniffer is mostly used by research in their research work not generally used by hacker that much like people said and sometimes is not an easy task to launch or start network sniffer in remote system because most network sniffer need admin or very high privilege that generally hacker didn't have

2. Working

Each machine on a local network has its own equipment address which varies from different machines'. At the point when a bundle is sent, it will be communicated to all accessible machines on nearby organization. Inferable from the common guideline of Ethernet, all PCs on a neighborhood network share a similar wire, so in ordinary circumstance, all machines on organization can see the traffic going through yet will be lethargic to those parcels don't have a place with themselves by disregarding. Nonetheless, if the organization interface of a machine is in promiscuous mode, the NIC of this machine can assume control over all bundles and a casing it gets on network, in particular this machine (including its product) is a sniffer. At the point when a bundle is gotten by a NIC, it first looks at the MAC address of the parcel to its own. On the off chance that the MAC address matches, it acknowledges the parcel in any case channels it. This is because of the organization card disposing of the apparent multitude of parcels that don't contain its own MAC address, an activity called promiscuous mode, which fundamentally implies that each organization card is staying out of other people's affairs and perusing just the edges coordinated to it. So as to catch the bundles, NIC must be set in the promiscuous mode. Bundle sniffers which do sniffing by setting the NIC card of its own framework to promiscuous mode, and consequently gets all parcels even they are not expected for it. Thus, bundle sniffer catches the parcels by setting the NIC card into promiscuous mode the bundle showing up at the NIC are duplicated to the gadget driver memory, which is then passed to the part cradle from where it is utilized by the client application fig 3 shows the flow of the packet inside a typical computer/system

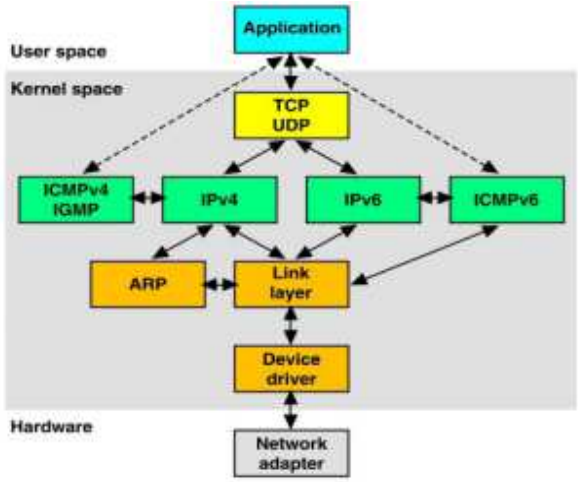

Figure 3

3. SNIFFER COMPONENTS

Basic Components of sniffers are:-

A. The hardware: - Most items work from standard organization connectors, however some require extraordinary equipment. In the event that you utilize uncommon equipment, you can dissect equipment shortcomings like CRC blunders, voltage issues, link programs, "spills", "jitter", arrangement mistakes, etc
B. Capture driver:- This is the most significant part. It catches the organization traffic from the wire, channels it for the specific traffic you need, and afterward stores the information in a cradle.
C. Buffer:-Once the frame are caught from the organization, they are put away in a buffer.
D. Decode: - this shows the substance of organization traffic with illustrative content so an examination can sort out what is happening.
E. Packet editing/transmission:- A few items contain highlights that permit you to alter your own organization bundles and communicate them onto the organization

4. Pcap Library

Pcap comprises of an application programming interface (API) for catching bundles in the organization. UNIX like frameworks actualizes pcap in the libpcap library; Windows utilizes a port of libpcap known as WinPcap. LIBPCAP is a broadly utilized standard parcel catch library that was produced for use with BPF (Berkely Packet Filter). BPF can be considered as an OS portion expansion. It is BPF, which empowers correspondence between working framework and NIC. Libpcap is a C language library that broadens the BPF library develops. Libpcap is utilized to catch the parcels on the organization straightforwardly from the organization connector. This library is an in fabricated element of the working framework. It gives bundle catching and separating capacity. It was initially evolved by the tcpdump designers in the Network Research Group at Lawrence Berkeley Laboratory. In the event that this library is absent in the working framework, we can introduce it sometime in the not too distant future, as it is accessible as an open source.

5. Promiscuous mode

The network interface card works in two modes

1. Non promiscuous mode (normal mode)
2. Promiscuous mode

At the point when a packet is gotten by a NIC, it first analyzes the MAC address of the bundle to its own. In the event that the MAC address matches, it acknowledges the bundle in any case channels it. This is because of the organization card disposing of the apparent multitude of bundles that don't contain its own MAC address, an activity mode called non promiscuous, which essentially implies that each organization card is staying out of other people's affairs and perusing just the edges coordinated to it. So as to catch the bundles, NIC must be set in the promiscuous mode. Bundle sniffers which do sniffing by setting the NIC card of its own framework to promiscuous mode, and thus gets all parcels even they are not proposed for it. In this way, parcel sniffer catches the bundles by setting the NIC card into promiscuous mode. To set an organization card to promiscuous mode, we should simply give a specific ioctl ( ) call to an open attachment on that card and the bundles are passed to the bit. Figure 4 shows how the information sent by gadget A to gadget C is likewise gotten by gadget D which is set in promiscuous mode.

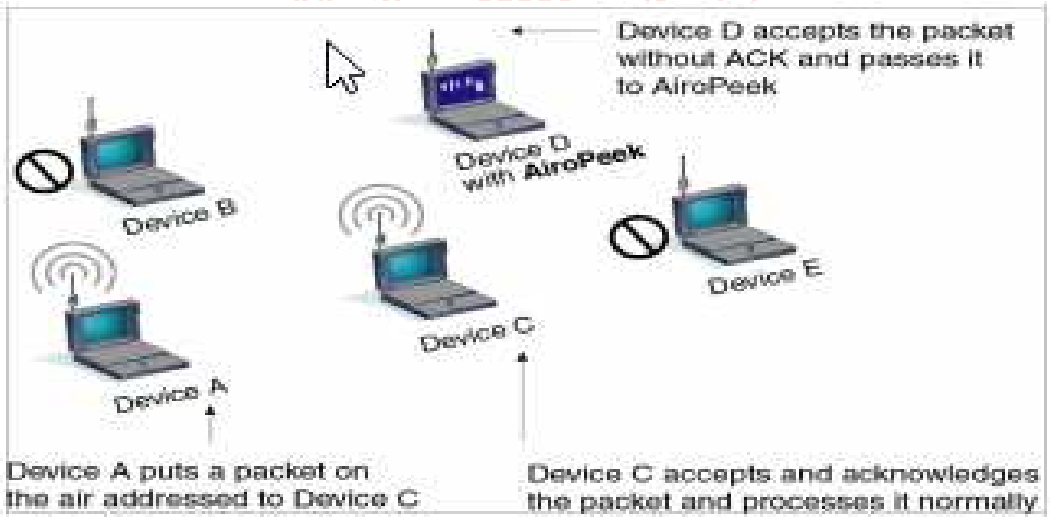

Figure 4

6. BOTTLENECK ANALYSIS

With the expansion of traffic in the organization, the pace of the parcels being gotten by the hub likewise increments. On the appearance of the bundle at NIC, they must be moved to the principle memory for handling. A solitary parcel is moved over the transport. As we realize that the PCI transport has genuine exchange of not more than 40 to 50 Mbps in light of the fact that a gadget can have authority over the transport for certain measure of time or cycles, after that it needs to move the control of the transport. Also, we realize that the slowest part of a PC is circle drive in this way, bottleneck is made recorded as a hard copy the bundles to plate in rush hour gridlock delicate organization. To deal with the jug neck we can put forth an attempt to utilize buffering in the client level application. As indicated by this arrangement, some measure of RAM can be utilized as cradle to defeat bottleneck.

7. The IDS and Packet sniffer

The expression "Intrusion Detection" infers finding assaults and dangers all through an endeavor or association, and reacting to those revelations. A portion of the mechanized reactions normally incorporate informing a security chairman by means of a reassure, email, halting the culpable meeting, closing the framework down, killing down Internet connections, or executing a predefined order technique. In setting to our paper, as we realize that parcel sniffer can be utilized for noxious reason the equivalent can be utilized for intrusion detection moreover. Utilizing this approach, the Intrusion Detection programming is put on the framework, which puts the Ethernet card in "promiscuous mode" with the goal that the product can peruse and investigate all traffic. It does this by looking at both the parcel header fields and bundle substance. The Intrusion Detection programming like parcel sniffers incorporates a motor, which searches for explicit kinds of organization assaults, for example, IP mocking and bundle floods. At the point when the bundle sniffer recognizes a potential issue it reacts quickly by telling to the overseer by different mode, for example, comfort, signaling a pager, sending an email, or in any event, closing down the organization meeting. The outline underneath shows a run of the mill arrangement of sniffers for doing bundle examination. A sniffer is put outside the firewall to identify assault endeavors originating from the Internet. A sniffer is additionally positioned inside the organization to identify Internet assaults, which enter the firewall and to help with distinguishing inner assaults and dangers.

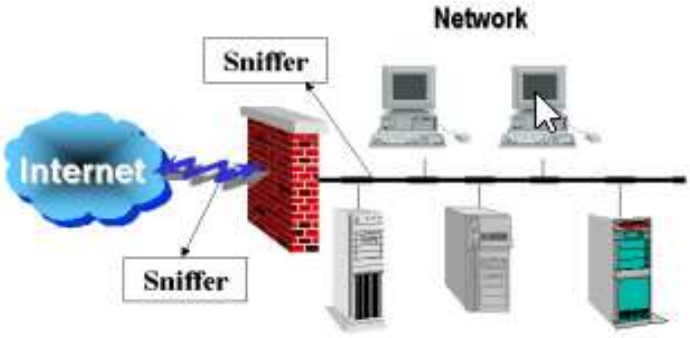

Figure 5

8. Various Network sniffing tool

There are various tools for traffic analysis

A. **Wireshark:** Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, in May 2006 the project was renamed Wireshark due to trademark issues. Wireshark is cross-platform using pcap to capture packets; it runs on various Unix-like operating systems and on Microsoft fig 6 show the typical interface of wireshark in windows OS.

B. **Tcpdump:** It is a typical packet analyzer that provide only CLI interface. It permits the client to capture and show TCP/IP and different parcels being sent or gotten over an organization to which the PC is connected. Dispersed under the BSD permit, tcpdump is free software. Tcpdump chips away at most Unixlike working frameworks: In those frameworks, tcpdump utilizes the libpcap library to catch parcels. The port of tcpdump for Windows is called Win Dump; it utilizes WinPcap, the Windows port of libpcap.

C. **Soft Perfect Network Protocol Analyzer:** It is a advanced, proficient instrument for examining, troubleshooting, keeping up and observing nearby networks and Internet associations. It catches the information leaving through your dial-behind association or network Ethernet card, examines this information and afterward speaks to it in an effectively comprehensible structure. Soft Perfect Network Protocol Analyzer is a valuable apparatus for network executives, security pros, network application engineers and any individual who needs an exhaustive image of the traffic going through their network association or portion of a neighborhood. Soft Perfect Network Protocol Analyzer presents the consequences of its network investigation in a helpful and effectively reasonable configuration. It likewise permits you to defrayments and reassembles network parcels into streams.

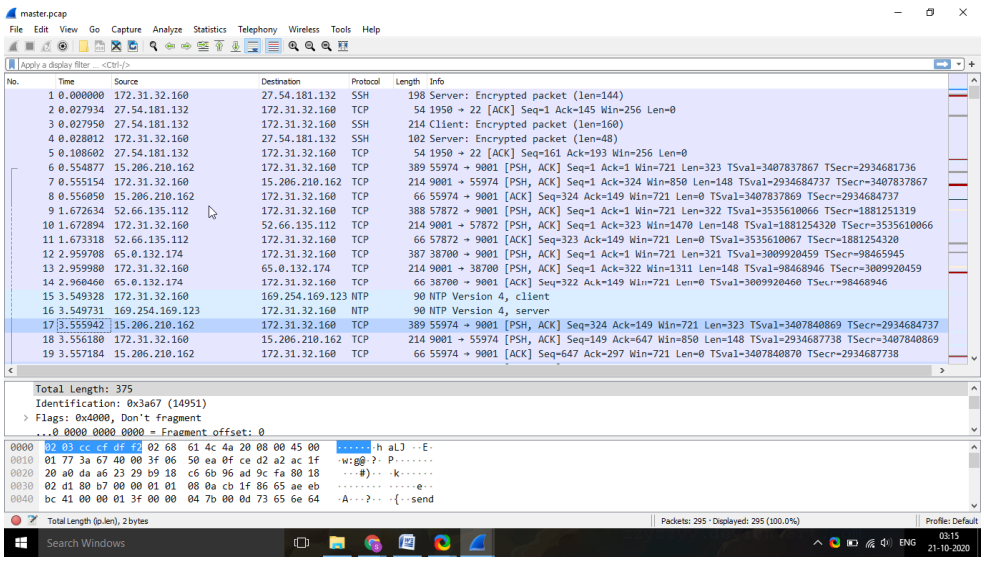

Figure 6

9. Conclusion

In conclusion I have something to network sniffer is not a tool made for the hacker by the hacker network sniffing tool can be used by system administration, network administration, researcher, can be used increases the performance of the system by directly looking in side wire or can be used as a sub feature in more complex tool like IDS(Intrusion Detection System), IPS(Intrusion Prevention System) and Firewall are some of the example where we can use Packet sniffer tool.

10. Reference

[1] G. Varghese, "Network Algorithmic: An Interdisciplinary Approach to Designing Fast Networked Devices", San Francisco, CA: Morgan Kaufmann, 2005.

[2] A. Dabir, A. Matrawy, "Bottleneck Analysis of Traffic Monitoring Using Wireshark", 4th International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov. 2007, Page(s):158 - 162

[3] S. Ansari, Rajeev S.G. and Chandrasekhar H.S, "Packet Sniffing: A brief Introduction", IEEE Potentials, Dec 2002- Jan 2003, Volume:21, Issue:5, pp:17 – 19

[4] Hornig, C., "A Standard for the Transmission of IP Data grams over Ethernet Networks", RFC-894, Symbolic Cambridge Research Center, April 1984.

[5] S. Ansari, Rajeev S.G. and Chandrasekhar H.S, "Packet Sniffing: Brief Introduction", IEEE Potentials, Dec 2002- Jan 2003, Volume: 21 Issue: 5, pp: 17 –19

[6] Qadeer M.A., Zahid M., Iqbal A., Siddiqui M.R "Network Traffic Analysis and Intrusion Detection Using Packet Sniffer" ICCSN '10 Second International Conference, 2010, Page(s): 313 – 317

[7] Bo Yu"Based on the network sniffer implement network monitoring Computer Application and System Modeling (ICCASM), 2010 International Conference on Volume: 7, 2010, Page(s): V7-1 - V7-3