Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, No. 3, April : 2023

NETWORK MONITORING AND DETECTING PACKETSUSING PACKET SNIFFING METHOD

R.SURYA, MCA. Assistant professor, Department of Information Technology,
Rathinam college of arts and science, Coimbatore-2.

ABSTRACT

In the past five decades computer network have kept up growing in size, complexity, overall in the number of its users as well as being in a permanent evolution. Hence the amount of network traffic flowing at each node has increased drastically. With the development and popularization of network Technology, the management, maintenance and monitoring of network is important to keep the network smooth and improve economic efficiency. So to keep a track on these nodes a packet sniffer is used. Packet sniffers are useful for analyzing network traffic over wired or wireless networks. Sometimes a packet sniffer is called a network monitor or network analyzer. Many system administrator or network administrator use it for monitoring and troubleshooting network traffic. This paper focuses on the basics of packet sniffer; it's working Principle which used for analysis Network traffic, how it works in both switched and non switched environment, its practical approach, its positive vs negative aspects and its safe guards.

KEYWORDS: Packet Filter, Promiscuous mode, Spoofing and Intrusion, Network Monitoring, Network analyzer.

INTRODUCTION

Packet sniffing is the process of capturing the information transmitted across network. In this process NIC capture all traffic that is flow inside or outside with new switches. The replacement of hub with new switches that makes switched environment is widely used because "it increases security". However, the thinking behind is somewhat flawed. It cannot be said that packet network.

Packet Sniffing mainly used in network management, monitoring and ethical hacking. To perform sniffing we use tool named packet sniffer. A packet sniffer, sometimes referred to as a network analyzer, which can be used by a network administrator to monitor and troubleshoot network traffic. Packet sniffing is defined as a technique that is used to monitor every packet that crosses the network. A packet sniffer is a piece of hardware orsoftware that monitors all network traffic [3].Using the information captured by the packet sniffers an administrator can identify erroneous packets and use the data to pinpoint bottlenecks and help to maintain efficient network data transmission. For most organizations packet sniffer is largely an internal threat. Packet sniffers can be operated in both switched and non switched environment.

Determination of packet sniffing in a non switched environment is technologies that can be understand by everyone. In this technology all hosts are connected to a hub. There are a large number of commercial and non commercial tools are available that makes possible eavesdropping of network traffic. Now a problem comes that how this network traffic can be eavesdrop; this problem can be solved by setting network card into a special "promiscuous mode". [4] Now businesses are updating their network infrastructure, replacing aging hubs sniffing is not possible in switched environment. It is also possible in switched environment.

Packet sniffer is a program running in a network attached Device that passively receives all data link layer frames passing through the device's network adapter. It is also known as Network or

Protocol Analyzer or Ethernet Sniffer. The packet sniffer captures the data that is addressed to other machines, saving it for later analysis. It can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic [2]. 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. This is unlike standard network hosts that only receive traffic sent specifically to them. The security threat presented by sniffers is their ability to capture all incoming and outgoing traffic, including clear- text passwords and usernames or other sensitive material. In theory, it's impossible to detect these sniffing tools because they are passive in nature.

PRINCIPLE OF PACKET SNIFFING

When packets transfer from source to destination then it passes through many intermediate devices. A node whose NIC is set in the promiscuous mode receives all information travels in network [5]. Each NIC have physical address which is different from another and network. When packet arrives at NIC then hardware address of frame matched with physical address that NIC have, but if we set it in promiscuous mode then all packets will arrives at that interface. When we use switch which already pass filtered data then we perform some method to capture alldata of network. When NIC accept packets, packets are copied to driver memory then it passes to kernel and kernel passes it to user application.

SNIFFER COMPONENTS

Basic Components of sniffers are:-

A. ***The hardware*****: -**

Most products work from standard network adapters, though some require special hardware. If you use special hardware, you can analyze hardware faults like CRC errors, voltage problems, cable programs, "dribbles", "jitter", negotiation errors, and so forth

*B.****Capture driver:-***This is the most important part. It captures the network traffic from the wire, filters it for the particular traffic you want, and then stores the data in a buffer.

C Buffer:-Once the frames are captured from the network, they are stored in a buffer.

analysis are fully automated. Real-time analysis though, has usually high computational resources requirements.

B. Batched analysis**: -** Batched analysis performs analysis periodically, where the period is enough to accumulate data in so-called data batches. Depending on the batching policies, the response time and associated computational resources requirements may be higher or lower, but in general they offer a higher response time and lower computational resources requirements than real-time analysis (although they require larger storage size)[6].

C. Forensics analysis**:** Forensics analysis are analysis performed when a particular event occurs (triggered analysis). A typical example of forensics analysis is the analysis performed when an intrusion is detected to a particular host. This kind of analysis require that data had been previously stored to be analyzed, and may also require of human intervention. Network data inspection techniques obtain information of network data by inspecting network header fields of each packet, compute them and produce outputs or results. Packet in which packets are decoded and presented in a human readable way. Network analyzers like tcpdump, Wireshark are some

D Decode: - this displays the contents of network traffic with descriptive text so that an analysis can figure out what is going on.

E Packet editing/transmission**:-**Some products contain features that allow you to edit your own

network packets and transmit them onto the network

F. Packet Analysis

Packet analysis can be done on real time or we can analyze packets after storing it. We can analyze both header and actual data, when we store data in memory or we perform real time analysis, decoder is used to decode the data store in packets

NETWORK TRAFFIC ANALYSIS

Network traffic analysis could be defined as: "the inference of information from observation of the network traffic data flow". Analysis in general, and hence network traffic analysis, can be categorized by time (or frequency) criteria and by the purpose of the analysis. Time based analysis categorization regarding time and frequency criteria, any network traffic analysis can be classified in one of the following three categories: real-time analysis, batched analysis and forensics analysis.

A. ***Real-time analysis:*** - It is performed over the data as it is obtained, or using small batches often called buffers to efficiently analyze data. The response time of this kind of analysis, understood as the time elapsed between a certain event occurs and is computed or detected, is low thanks to the low delay obtaining data and the fact that real-time

TOOLS FOR TRAFFIC ANALYSIS

There are various tools for traffic analysis

A .Wire shark: Wire shark 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 Wire shark due to trademark issues. Wire shark is cross-platform using pcap to capture packets; it runs on various Unix-like operating systems and on Microsoft Windows.

B. ***Tcpdump:*** It is a common packet analyzer that runs under the command line. It allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software. Tcpdump works on most Unix-like operating systems: In those systems, tcpdump uses the libpcap library to capture packets. The port of tcpdump for Windows is called Win Dump; it uses WinPcap, the Windows port of libpcap.

C. ***Soft Perfect Network Protocol Analyzer:*** It is an advanced, professional tool for analyzing, debugging, maintaining and monitoring local networks and Internet connections. It captures the data passing through your dial- up connection or network Ethernet card, analyzes this data and then represents it in an easily readable form. Soft Perfect Network Protocol Analyzer is a useful tool for network administrators, security specialists, networkapplication developers and anyone who needs a comprehensive picture of the traffic passing through their network connection or segment of a local area network. SoftPerfect Network Protocol Analyzer presents the results ofits network analysis in a convenient and easily understandable format. It also allows you to defrayments and reassembles network packets into streams[7].

D. ***Capsa:***It is Network Analyzer is a must-have freeware for network administrators to monitor, troubleshoot and diagnose their network. It is designed for personal and small business use. Capsa Network Analyzer Free Edition is an easy-to-use Ethernet packet sniffer (network analyzer or network sniffer) for network monitoring and troubleshooting purposes. It performs real-time packet capturing, 24/7network monitoring, reliable network forensics, advanced protocol analyzing and in-depth packet decoding.

I. HOW PACKET SNIFFER WORKS

Packet sniffer's working can be understood in both switched and non switched environment. For setup of a local network there exist machines. These machines have its own hardware address which differs from the other local area network. Before sending traffic a source host should have its destination host, this destination host is checked in the ARP cache table. If destination host is available in the ARP cache then traffic will be sent to it through a switch, but if it is not available in the ARP cache then source host sends a ARP request and this request is broadcasted to all the hosts. When the host replies the traffic can be send to it. This traffic is sent in two parts to the destination host. First of all it goes from the source host to the switch and then switch transfers it directly on the destination host. So sniffing is not possible. There are several methods through which we can sniff traffic in switched environment.

These methods are:-

ARP Cache Poisoning

ARP Cache Poisoning can be better explained by an example "man-in-the-middle-attack". Suppose we have 3 hosts x, y, z. Host x and y are connected through a switch and they normally Communicate. Assume that z wants to see the communication between x and y. When, x sends traffic which is destined for y it is intercepted by z. z passes this information on to y, pretending that it came from x.

[8].When a non switched environment is considered then all nodes are connected to a hub which broadcast network traffic to everyone. So as soon as a packet comes in the network, it gets transmitted to all the available hosts on that local network. Since all computers on that local network share the same wire, so in normal situation all machines will be able to see the traffic passing through.

When a packet goes to a host then firstly network card checks it MAC address, if MAC address matches with the host's MAC address then the host will be able to receive the content of that packet otherwise it will forward the packet to other host connected in the network. Now here a need arises to see the content of all packets that passes through the host. Thus we can say that when a host or machine's NIC is setup in promiscuous mode then all the packets that is designed for other machines, is captured easily by that host or machine.

When a switched environment is considered then all hosts are connected to a switch instead of a hub, it is called a switched Ethernet also. Since in switched environment packet sniffing is more complex in comparison to non switched network, because a switch does not broadcast network traffic. Switch works on unicast method, it does not broadcast network traffic, it sends the traffic directly to the destination host. This happens because switches have CAM Tables. These tables store information like MAC addresses, switch port and VLAN information [5]. to understand working of packet sniffer in switched environment, an ARP cache table is considered.

This is a table that stores both MAC addresses and IP addresses of the corresponding hosts. This table exists in This is achieved by ARP Cache Poisoning.

CAM Table Flooding

Content addressable memory table works by flooding the CAM tables. CAM table is a table that stores information like MAC addresses and switch port along with their Virtual LAN information. A certain number of eateries are stored by CAM table due to of being its fix size. As its name implies "CAM table flooding" here flooding means floods the switch with MAC addresses and this is repeated till a point at where switch starts to broadcast network traffic.

[5. Now it becomes easy to sniff the packets[9].

Switch Port Stealing

As its name implies "switch port stealing" here in this method we have to steal the switches port of that host for which traffic is designed to send. When this switch port is stolen by the user then user will be able to sniff the traffic because traffic goes through the switch port first, then to the target host [10].

II. SNIFFING METHODS

Three types of sniffing methods are used. These are:

IP Based Sniffing

IP based sniffing is the most commonly used method of packet sniffing. In this method a requirement of setting network card into promiscuous mode exist. When network card is set into promiscuous mode then host will be able to sniff all packets. A key point in the IP based sniffing is that it uses an IP based filter, and the packets matching the IP address filter is captured only. Normally the IP address filter is not set so it can capture all the packets. This method only works in non switched network [3]

MAC based Sniffing

This is another method of packet sniffing. This is as like IP based sniffing. Same concept of IP based sniffing is also used here besides using an IP based filter. Here also a requirement of setting network card into promiscuous mode exists. Here in place of IP address filter a MAC address filter is used and sniffing all packets matching the MAC addresses [3].

ARP based Sniffing

This method works a little different. It does not put the network card into promiscuous mode. This is not necessary because ARP packets will be sent to us. This is an effective method for sniffing in switched environment. Here sniffing is possible due to of being stateless nature of Address Resolution Protocol [3].

[3]. Daniel Magers "Packet Sniffing: An Integral Part of Network Defense",May 09, 2002 SANS Institute
2000 – 2002.
[4]. All about Tools [Online] Available: http://www.sectools.org/
[5].EtherealPacketSniffing,Available:netsecurity.about.com/od/ readbookreviews/gr/aapro52304.htm.
[6]. Pallavi Asrodia, Hemlata Patel, "Network traffic analysis using packet sniffer",
International Journal of Engineering Research and Application (IJERA), Vol.2, pp. 854-857, Issue 3,May-June 2012.
[7]. Ryan Splanger, "Packet sniffing detection with Antisniff", University of Wisconsin-Whitewater,May 2003.
[8]. Tom King, "Packet sniffing in a switched environment",
SANS Institute, GESC practical
V1.4,option 1, Aug 4th 2002, updated june/july 2006.
[9].RyanSpangler,Packetsniffingonlayer2switchedlocalareanet

III. CONCLUSION

This paper proposes an approach to detect packets through packet sniffing. Packet sniffer is not only used for hacking purpose but also it is used for network traffic analysis, packet/traffic monitoring, troubleshooting and other useful purposes. Packet sniffer is designed for capturing packets and a packet can contain clear text passwords, user names or other sensitive material.

Sniffing is possible on both non switched and switchednetworks.
However, network cards have the ability to enter promiscuous mode, which allows them to listen to all network traffic regardless of if it's directed to them. So we can design a tool that capture network traffic and analyze itand allows user to take only the feature as he need andstore it in file to use it later in his work, then this willreduce the memory that is used to store the data. There are many available tools. Packet sniffer can be enhanced in future by incorporating features like making the packet sniffer program platform independent, and making tool by neural network. 10 GBPS LAN which are used currently, sniffing can do on this rate in future very effectively.

REFERENCES

[1]. 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.
[2]. 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 works", Packet watch Research :http://www.packetwatch.net, Dec 2003.
[10].Sconvery, "HackingLayer2:FunwithEthernetSwitches", Blackhat, 2002,Available: http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf.