An Approach to Detect Packets Using Packet Sniffing

Rupam[1], Atul Verma[2], Ankita Singh[3]

Department of Computer Science, Sri Ram Swroop Memorial Group of Professional Colleges Tiwari Gang Faizabad Road, Lucknow, Uttar Pradesh, India.
[1]rupamsrvstv@gmail.com
[2]atulverma16@gmail.com
[3]ankitasingh9126@gmail.com

ABSTRACT

In the past decades computer network have kept up growing in size, complexity and along with it the number of its user is also being increased day by day. Hence the amount of network traffic flowing at each node has increased drastically. So to keep a track on these nodes a packet sniffer is used. 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. Packet sniffers are useful for both wired and wireless networks. The purpose of this paper is to show the basics of packet sniffer, how it works in both switched and non switched environment, its practical approach, its positive vs negative aspects and its safe guards.

KEYWORDS

Network monitor, switched environment, non switched environment, promiscuous mode, spoofing and intrusion.

1. INTRODUCTION

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 or software 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 [2]. For most organizations packet sniffer is largely an internal threat.

Packet sniffers can be operated in both switched and non switched environment. [4] Determination of packet sniffing in a non switched environment is a technology 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 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 sniffing is not possible in switched environment. It is also possible in switched environment.

DOI : 10.5121/ijcses.2013.4302

2. 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 [2].

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.

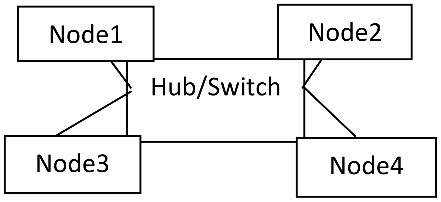


Figure 1: IEEE 802.3 network

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][6]. [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 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:-

2.1. ARP Cache Poisoning

ARP Cache Poisoning can be better explained by an example “man-in-the-middle-attack”.

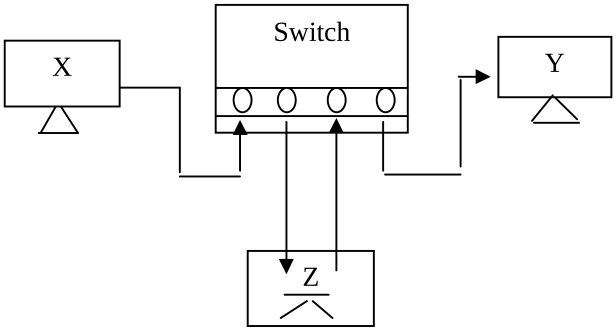


Figure 2: man-in-middle attack

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. This is achieved by ARP Cache Poisoning.

2.2. CAM Table Flooding

[5] 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 atwhere switch starts to broadcast network traffic. [5][7]. Now it becomes easy to sniff the packets.

2.3. Switch Port Stealing

[5]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 [5].

3. SNIFFING METHODS

Three types of sniffing methods are used. These are:

3.1. IP Based Sniffing

[3] 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].

3.2. MAC based Sniffing

[3]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].

3.3. ARP based Sniffing

[3] 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].

4. PRACTICAL APPROACH

A practical approach of this title is developed by us in which we have shown actual packet capturing. This approach is mostly developed for:

1. To make data identity stealing available by tracing the packets from the network.
2. To provide an easy and effective way of sniffing of data packets.
3. To provide a user friendly environment.
4. It is possible only when the server code is running.

4.1. System Analysis

For making a system analysis we should first of all state the requirements of the system. A requirement should be open and it must be defined in detail. There are many types of requirements available: user requirement, system requirement.

When all these requirements are gathered then we make a documentation of these requirements, this is called “system requirement specification”. Now the SRS for our application will be as-

1. Recognize layers and this layer can be Network layer.
2. Recognize layers and this layer can be Transport layer.
3. Recognize layers and this layer can be Application layer.
4. Recognize protocol that is simply UDP protocol.
5. Recognize protocol that is simply TCP protocol.
6. Recognize protocol that is simply HTTP protocol.
7. Analyze free memory size.
8. Find out the packets over a network.

Problem statement should state what we have to achieve and how it can be achieved. For the achievement of desired system we should keep a consideration on our needs, we should have to develop a user manual for the desired system and besides it we have to short list those features which are mandatory and then we have to consider those features which are optional. For better visualization and for providing a user friendly environment we should develop a proper designing. These designs are developed according to our requirements. So if requirements are not specified properly or it includes lack of analysis then designing process suffers from lack of generation of desired system. It should follow some software engineering standards.

Feasibility analysis is also an important part of system analysis. We should have to know that our system is feasible in the following environment or not. These environments include Technical feasibility, operational feasibility and economical feasibility. Technical feasibility, that is commonly known to all that the desired system that we are going to develop should be technically feasible. Operational feasibility indicates that system's operation will be properly used or not. So as like technical and operational feasibility economical feasibility indicate that is it possible to develop the system in our desired budget.

4.2. Existing System

Existing system supports only the packet capturing there is no sniffing concept. It can show only the captured packet in the network and it can show only the size of the packet. In this application it cannot show the source machine and destination machine which are involved in the packet transferring.

4.3. Proposed System

In this application it can show the "packet sniffing" concept. In this manner it can show the captured packets and size of the packet and source and destination machine IP addresses which are involved in the packet transferring. It can show this process in graphical manner. It can show the working of different layers in graphical manner. It can give the complete information about the captured packet like which layers are involved and which protocols are involved at that time. And you have a facility to store the information of the packets. It can show the ratio of different layers in graph.

For developing this application we have made five modules they are as:

1. User Interface module
2. Packet sniffing module
3. Analyze layer module
4. Analyze protocol module
5. Free memory module

After summarizing all modules, output comes by using mixed approach of all modules. Now we connect our system into a Local Area Network, after connecting when we run this application then output comes as:

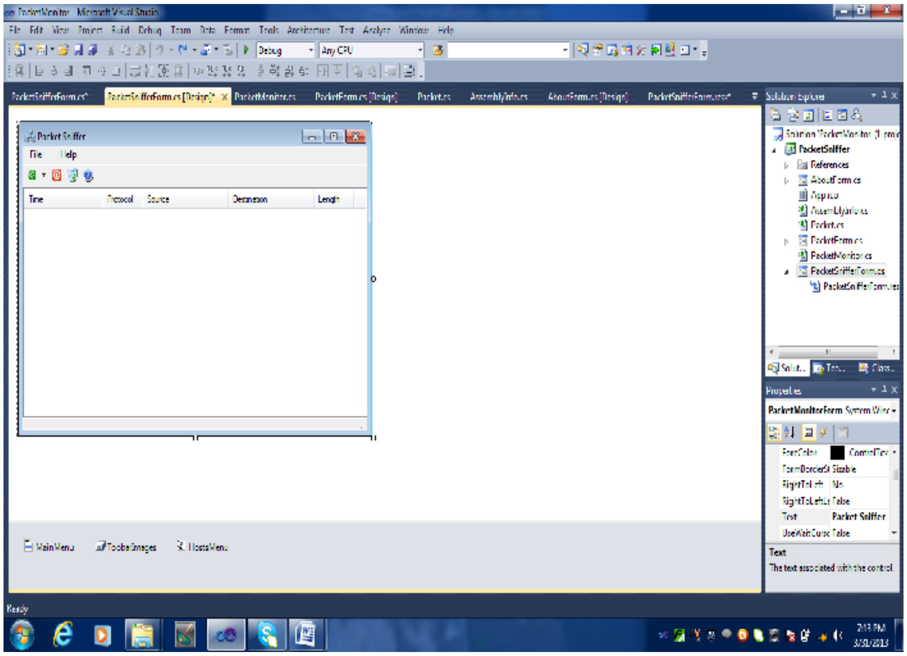
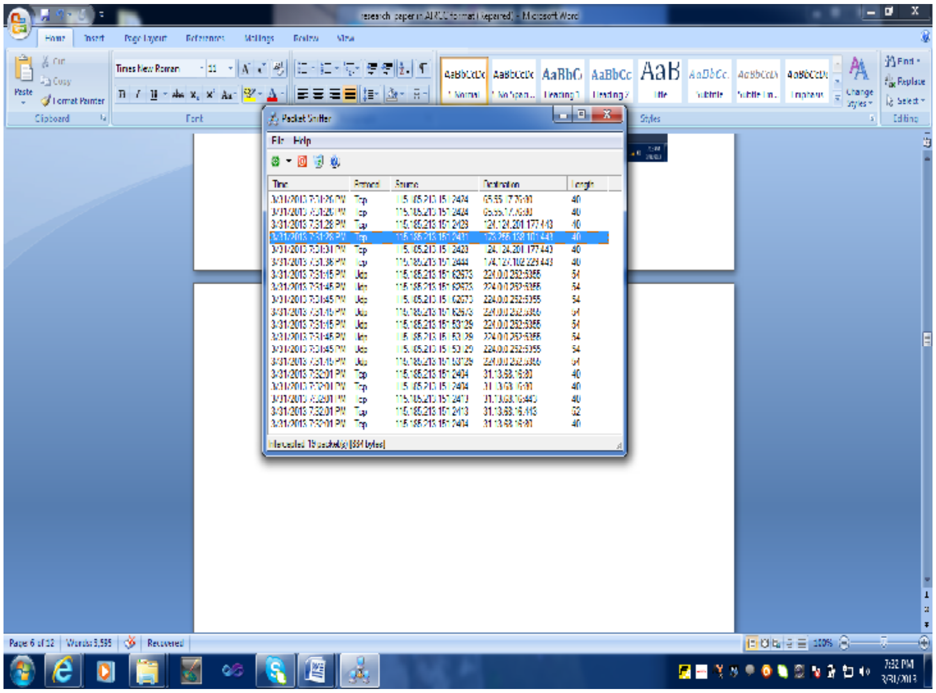


Figure 3: Practical approach 1.

All incoming and outgoing packet's time, its protocol analysis and what it contains source address and what is its destination address and actual size of the packets are shown by this window. Now if we want to know the detailed information of any packet then we choose it, another window opens showing the detailed information of that particular packet.

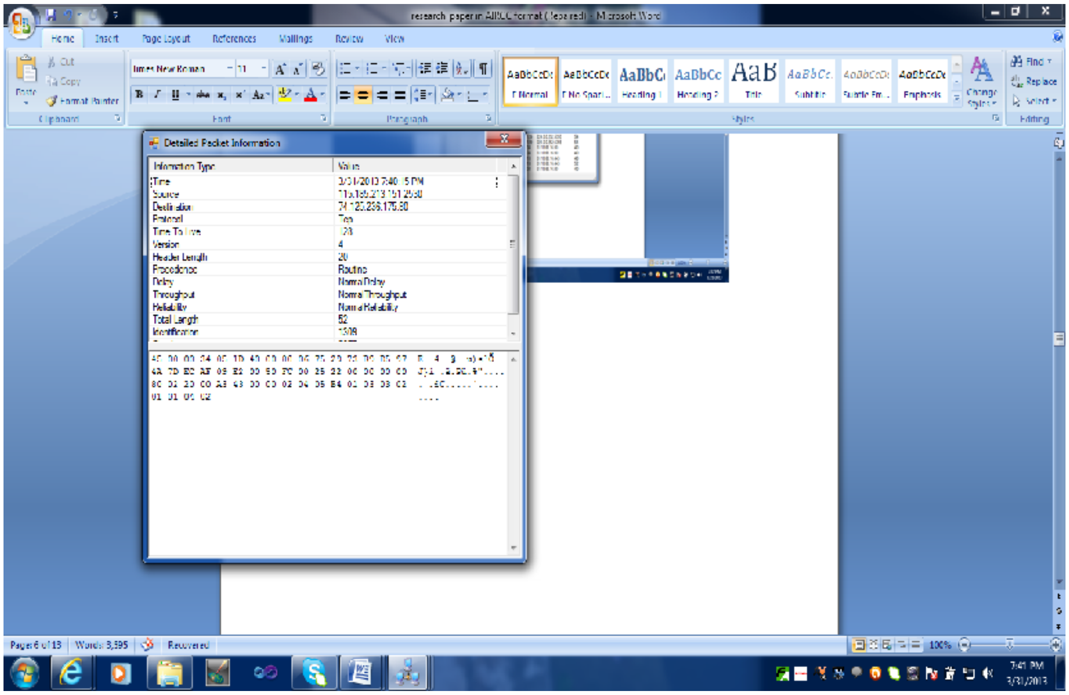


Time	Protocol	Source	Destination	Length
3/31/2013 7:31:26 PM	Tcp	115.185.213.151:2424	65.55.17.76:80	40
3/31/2013 7:31:26 PM	Tcp	115.185.213.151:2424	65.55.17.76:80	40
3/31/2013 7:31:28 PM	Tcp	115.185.213.151:2429	124.124.201.177:443	40
3/31/2013 7:31:28 PM	Tcp	115.185.213.151:2431	173.255.138.101:443	40
3/31/2013 7:31:31 PM	Tcp	115.185.213.151:2429	124.124.201.177:443	40
3/31/2013 7:31:36 PM	Tcp	115.185.213.151:2444	174.127.102.229:443	40
3/31/2013 7:31:45 PM	Udp	115.185.213.151:62673	224.0.0.252:5355	54
3/31/2013 7:31:45 PM	Udp	115.185.213.151:62673	224.0.0.252:5355	54
3/31/2013 7:31:45 PM	Udp	115.185.213.151:62673	224.0.0.252:5355	54
3/31/2013 7:31:45 PM	Udp	115.185.213.151:62673	224.0.0.252:5355	54
3/31/2013 7:31:45 PM	Udp	115.185.213.151:53129	224.0.0.252:5355	54
3/31/2013 7:31:45 PM	Udp	115.185.213.151:53129	224.0.0.252:5355	54
3/31/2013 7:31:45 PM	Udp	115.185.213.151:53129	224.0.0.252:5355	54
3/31/2013 7:31:45 PM	Udp	115.185.213.151:53129	224.0.0.252:5355	54
3/31/2013 7:32:01 PM	Tcp	115.185.213.151:2404	31.13.68.16:80	40
3/31/2013 7:32:01 PM	Tcp	115.185.213.151:2404	31.13.68.16:80	40
3/31/2013 7:32:01 PM	Tcp	115.185.213.151:2413	31.13.68.16:443	40
3/31/2013 7:32:01 PM	Tcp	115.185.213.151:2413	31.13.68.16:443	52
3/31/2013 7:32:01 PM	Tcp	115.185.213.151:2404	31.13.68.16:80	40

Intercepted 19 packet(s) [884 bytes]

Figure 4: Practical approach 2

Detailed information of packet contains information as like timing of coming of packet, source addresses of the packet, destination addresses of the packet, protocol information, time to live of packets, version information, header length, precedence, Delay information, Throughput, Reliability, Total length of packet, Identification and Checksum along with the contents of the packets.



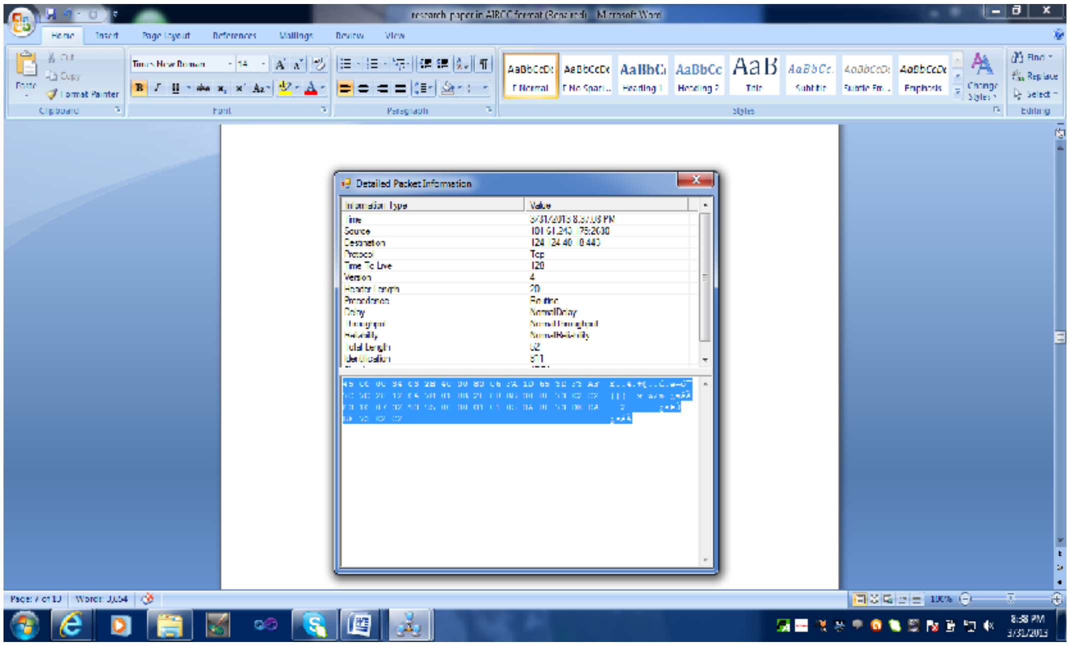
Detailed Packet Information

Information Type	Value
Time	3/31/2013 7:40:15 PM
Source	115.185.213.151:2530
Destination	74.125.236.175:80
Protocol	Tcp
Time To Live	128
Version	4
Header Length	20
Precedence	Routine
Delay	Normal Delay
Throughput	Normal Throughput
Reliability	Normal Reliability
Total Length	52
Identification	1309

```
45 00 00 34 05 1D 40 00 80 06 75 20 73 B9 D5 97   E..4..@...u)s¹Õ
4A 7D EC AF 09 E2 00 50 FC 00 25 22 00 00 00 00   J}ì¯.â.Pü.%"....
80 02 20 00 A3 43 00 00 02 04 05 B4 01 03 03 02   .. .£C.....´....
01 01 04 02                                       ....
```

Figure 5: Practical approach 3

Now we can edit the content of packet and we can transfer again this modified packet in the network. We can store all packets information in the buffer for further analysis.



Detailed Packet Information

Information Type	Value
Time	3/31/2013 8:37:08 PM
Source	101.61.243.175:2000
Destination	124.124.40.10:443
Protocol	Tcp
Time To Live	120
Version	4
Header Length	20
Precedence	Routine
Delay	NormalDelay
Throughput	NormalThroughput
Reliability	NormalReliability
Total Length	52
Identification	811

Figure 6: Practical approach 4

This application may be previously developed but this contains a problem. It is not much feasible for those users who are unknown about the concepts of IP addresses, MAC addresses and promiscuous mode etc. So due to of being unaware they could not understand what is going on exactly. So here we are developing a new concept of providing administrator's name also. As we know that in big organization each system are allotted to a particular user. So to keep a track that which activity is performing by which user is possible to know. When a new user uses this application then he can easily understand that a person sitting at system x what is accessing.

5. POSITIVE ASPECT

This application keeps both positive and negative aspects. Its positive aspects can be defined as:

5.1. Network traffic analysis

Traffic analysis is the process of intercepting and examining messages in order to deduce information. It can be performed even on when the messages are encrypted and cannot be decrypted. Traffic analysis comes in computer security. Now a question arises why this traffic analysis is performed. It is performed in the context of military intelligence or counter intelligence. If an attacker wants to gain information, this information may be important information. Then to gain important information he has to monitor the frequency and timing of network packets. A passive network monitoring is being used by network IDS devices to detect possible threats. This passive monitoring is much more beneficial for a security admin. He get the knowledge of network topologies, he get the knowledge about available services, information about operating systems besides it he will be able to get information about type of vulnerabilities [1].

Network traffic can be analyzed by a network analyzer. A network analyzer is also called a protocol analyzer or packet analyzer. Network analyzer is a hardware device that provides security against malicious activity.

Network analyzer can:-
1. Provide detail information of activities that is going on the network.
2. Test anti-malware programs and pin-point potential vulnerabilities.
3. Detect unusual packet characteristics.
4. Identify packet sources or destination.
5. Configure alarm for defined threat.
6. Search of specific data string in packets.
7. It captures all the information and displays it

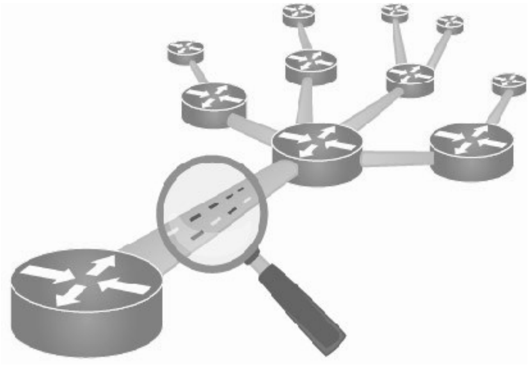


Figure 7: Network traffic analysis

Network analyzer is mostly used in comparison to other techniques because it gives assurance to minimize the probability of an attack.

5.2 In Intrusion Detection

Now a day, no one can live without using internet due to of its services available. Its users are increasing day by day. In such increasing environment there are many chances of being an intrusion. To handle these intrusions an appropriate intrusion detection system is used. In big organizations existence of intrusion detection is necessary. Intrusion Detection is the active or continuous action to detect intrusive acts. So a packet sniffer is used in intrusion detection through which it can monitor network or system activities for malicious activities. Intrusion detection is useful due to of following reason:

1. New and new softwares are developed every day. Sometimes they suffer from occurrences of bugs. So intrusion detection is useful to resolve these bugs.
2. As we know that internet size is increasing day by day and number of its users is also increasing. So to keep a track on system abuses an intrusion detection system is used.
3. In big organizations to keep a track on occurrence of an intrusion, Intrusion Detection system is established.

6. TOOLS FOR INTRUSION DETECTION

There are various tools for intrusion detection:

6.1. Computer Oracle and Password System

This is a technique that is used as a tool for Intrusion detection. As its name implies it is used to check passwords and startup devices besides it, it is also used for checking file permissions.

These checkings are performed by a normal user. COPS then use comparison to determine if any anomalies have occurred.

Many security tools that are basically designed for UNIX systems, administrator, programmer, operator or consultant in the neglected area of the computer security are combined to make COPS. [8] There are twelve small security check programs which are integrated by COPS. These programs look for:

1. File directory and device permission/modes.
2. Poor passwords.
3. Security of passwords.
4. Programs and files run in /etc/rc*.
5. Existence of SUID files, their writability.
6. A CRC check against important binaries or key files.
7. Anonymous ftp setup.
8. Unrestricted tftp, decode alias in send mail, SUID uudecode problems, hidden shells.
9. Miscellaneous root checks.
10. Checking dates of CERT advisories versus key files.
11. Writability of user's home directories and startup files.
12. The kuang expert system.

6.2. Tripwire

Tripwire is a tool that is basically used for intrusion detection. Each database/system has several files and every modification in these files is monitored by a security utility. This utility is called Tripwire. This monitoring is done by maintaining digital signature of each file. Using these signatures, tripwire checks file integrity. There are many digital signature algorithms that are offered by Tripwire. When Tripwire creates digital signature for important files then this signature is checked against checksums. If a difference is found, it simply means there have been some changes in the files by an intruder.

6.3. Tiger

It is similar to COPS. [9]Tiger is a type of security tool. It is used not only as a security audit but also it is used as an intrusion detection system. Multiple UNIX platforms are supported by tiger. It is freely available and if we want to take it then we should go through the GPL License process. When it is compared from other tool then we get that it needs only of POSIX tools and these tools are written in shell language. Along with various applications it has some interesting features that show its resurrection and this resurrection includes a modular design that is easy to expand and it has a double edge where it can be used as an audit tool and as a host intrusion detection tool. There are many ways in which free software intrusion detection is currently going. These ways goes from network IDS to the kernel but there is a case, that it does not mention file integrity checkers and log checkers. This tool is complemented by tiger and provides a framework for together working. Tiger can be freely downloaded from savannah.

7. NEGETIVE ASPECT

Sniffing programs are found in two forms: Commercial packet sniffer and Underground packet sniffer. Commercial packet sniffer has positive aspect because it is used in maintaining network whereas underground packet sniffer has negative aspect because it is mostly used by attackers to gain unauthorized access to remote host [3]. Thus we see that this application has some negative aspects too.

7.1. Unauthorized access

When we perform sniffing then content of packets is viewed by us. Since all the contents are in encrypted form but they can be decrypted by hackers by implementing a hacking table. If packet contains some private information such as anyone’s user name and password then hackers may use it to gain authorized access.

7.2. Posting a threat

When network traffic is analyzed then we can post some malicious activity. Packet sniffing is a well known example of intrusion methods.

7.3. IP Spoofing

To gain unauthorized access to machines, IP spoofing is a powerful technique. Here an intruder sends messages to a computer with an IP address. And this IP address indicates that the message is coming from a trusted host. This is used for:

1. Reprogramming routers
2. Denial of service attack

7.4. Man-in-middle attack

This is a well known example of ARP Spoofing. This is also known as a Bucket bridge attack, or sometimes Janus attack. Computer security is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones.

8. SAFE GUARDS

There are many ways through which we can protect our packets. One of them is by using encryption. There are three ways to apply encryption on packets.

8.1. Link-level encryption

Encryption mechanism is applied on packets when they get on transmission medium and when they reach on the destination, a decryption mechanism is applied. This mechanism prevent from sniffing. Since a packet sniffer gets access to packets at that time when they are transported on the medium. If they are already encrypted, then no information is gained, if they are not encrypted then packet’s content can be easily accessed.

8.2. End-to-end encryption

Packets are transmitted among hosts. In end to end encryption each packets are encrypted by the host that transmit the data and they are decrypted by the host when they are received at the other end.

8.3. Application level encryption

The application layer enables the user, whether human or software to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management and other type of distributed information services. So we see that, at this layer packets contain sensitive material. So an encryption mechanism should be applied at application level.

Besides it we can protect ourselves/our packets through:

8.4. SSL

SSL is nothing, it is secure socket layer that is used to encrypt packet. So that we can be able to get secure channel for database communication or simple mail transfer protocol. We can use something call SSL over http in electronic commerce and E-mail that is “HTTPS” [10].

8.5. TLS

TLS is nothing, it is transport layer security. It is based on SSL. Here a requirement arises that TLS use the certificates which now a day’s called web based certificates [10].

8.6. IP Security Protocol

It works in network layer of OSI model. Its work is to encrypt all send packets [10]. We may be able to summarize all these activities by showing the following diagram between two processes:

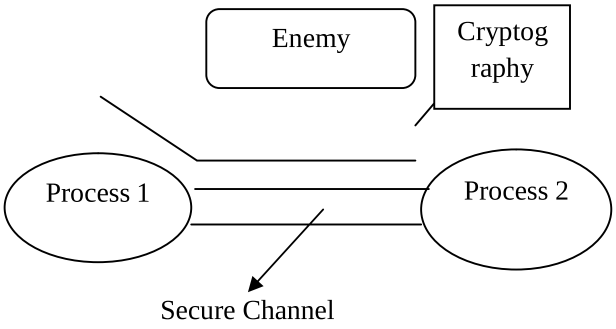


Figure 8: Security process

9. CONCLUSION

This paper proposes an approach to detect packets through packet sniffing. It includes some negative aspects but besides these negative aspects it is much useful in sniffing of packets. 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 switched networks. We can use some tools to capture network traffic that are further used by researchers.

We can conclude that packet sniffers can be used in intrusion detection. There exist some tools also that can be used for intrusion detection. Thus we can say that packet sniffing is a technique through which we can create an intrusion and through which we can detect an intrusion.

ACKNOWLEDGEMENT

The special thanks goes to our helpful guide **Dr. Atul Verma.** The guidance and support that he provided us, helps really in completion of paper. The co-operation is much indeed appreciated. However, it would have not been possible without the kind support and help of our college. We would like to extend our sincere thanks to all of them.

We are highly indebted to **SRMCEM** for their guidance and constant supervision. We would like to express our gratitude towards our friends for their co-operation and encouragements.

REFERENCES

[1] EtherealPacketSniffing,Available:netsecurity.about.com/od/readbookreviews/gr/aapro52304.htm.
[2] 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.
[3] Ryan Splanger, "Packet sniffing detection with Anti sniff", University of Wisconsin-Whitewater, May 2003.
[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] RyanSpangler, "Packetsniffingonlayer2switchedlocalareanetworks", PacketwatchResearch:http://www.packetwatch.net, Dec 2003.
[6] Sconvery, "HackingLayer2:FunwithEthernetSwitches", Blackhat, 2002, Available:http://www.blackhat.com/ presentations/bh-usa-02/bh-us-02-convery-switches.pdf.
[7] http://www.monkey.org/dufsong/dsniff/.
[8] http://www.fish2.com/cops/overview.html.
[9] http://nongnu.org/tiger/.
[10] http://www.securityteam.com/unixfocus/Detecting sniffers on your network .html.

Authors

Rupam is a B.tech Final year student of Computer Science department, Sri Ram Swroop Memorial Group of Professional Colleges, affiliated to Uttar Pradesh Technical University.

Dr. Atul Verma is working as an Assistant Professor in the Dept. of Computer in SRMGPC. He has completed his graduation from Integral University. He obtained his Ph.D degree in computer science. He has 6 years of teaching experience.

Ankita Singh is a B.tech Final year student of Computer Science department, Sri Ram Swroop Memorial Group of Professional Colleges, affiliated to Uttar Pradesh Technical University.