Literature Review on an Approach to Detect Packets Using Packet Sniffing

Annu Ailawadhi
Student, NCCE, Israna (Panipat),Haryana, India.

Dr.Anju Bhandari
Associate Professor & Head of dept.(CSE),Israna (Panipat),Haryana, India.

Abstract – The Packet Sniffer allows the computer network to observe and analyze all the site visitors passing by means of its community connection. It decodes the network visitors and makes feel of it. When its miles set up on a computer, the network interface of the pc is about to promiscuous mode, being attentive to all the traffic at the network rather than simply the ones packets destined for it. Packet Sniffer is a tool that sniffs without modifying the network's packet. It merely makes a replica of every packet flowing via the network interface and finds the supply and destination Ethernet addresses of the packets. It also decodes the protocols in the packets. Sometimes a packet sniffer is known as a network monitor or network analyzer. Many machine administrator or community administrator use it for tracking and troubleshooting community visitors. Packet sniffers are useful for each wired and Wi-Fi networks. The reason of this paper is to reveal the fundamentals of packet sniffer, how it works in each switched and non-switched environment, its sensible method, its nice vs. poor elements and its safe guards.

Index Terms – Network screen, switched environment, non-switched surroundings, promiscuous mode, spoofing and Intrusion.

1. INTRODUCTION

Packet sniffing is defined as a way this is used to monitor each packet that crosses the community. A packet sniffer is a bit of hardware or software that video display units all community visitors [3]. Using the facts captured by way of the packet sniffers an administrator can pick out erroneous packets and use the records to pinpoint bottlenecks and help to hold efficient community facts transmission [2]. For most organizations packet sniffer is largely an inner danger. Packet sniffers can be operated in each switched and non-switched surroundings. [4] Determination of packet sniffing in a non-switched environment is an era that may be understand with the aid of each person. In this generation all hosts are related to a hub. There are a huge quantity of commercial and non-commercial tools are available that makes possible eavesdropping of community traffic. Now a trouble comes that how this network site visitor can be eavesdrop; this trouble may be solved by means of setting network card right into a special "promiscuous mode". [4] Now corporations are updating their network infrastructure, changing growing older hubs with new switches. The replacement of hub with new switches that makes switched surroundings is broadly used due to the fact "it will increase safety". However, the thinking at the back of is particularly improper. It cannot be said that packet sniffing is not viable in switched surroundings. It is likewise viable in switched environment.

2. EXISTING WORK

Three types of sniffing techniques are used. These are:

2.1. IP Based Sniffing:-

IP based sniffing is the most commonly used method of packet sniffing. In this technique requirement of putting community card into promiscuous mode exist. When community card is ready into promiscuous mode then host may be capable of sniff all packets. A key factor inside the IP based totally sniffing is that it makes use of an IP based clear out, and the packets matching the IP cope with filter is captured most effective. Normally the IP address filter out isn't set so it could seize all of the packets. This approach most effective works in non-switched community [3].

2.2. MAC based totally Sniffing:-

This is the other method of packet sniffing. This is as like IP primarily based sniffing. Same concept of IP based sniffing is likewise used here besides the use of an IP based totally filter. Here also a demand of placing network card into promiscuous mode exists. Here in place of IP cope with clear out a MAC deal with filter out is used and sniffing all packets matching the MAC addresses [3].

2.3. ARP primarily based Sniffing:-

Packet sniffing is a technique of monitoring network traffic. In LANs, packet sniffing and remote network monitoring (RMON) are well-known techniques used by network administrators to monitor LAN behavior and diagnose troubles. It is effective on both switched and non-switched networks. In a non- switched network environment packet sniffing is an easy thing to do. This is because network traffic is sent to a hub which broadcasts it to everyone. Switched networks are completely different in the way they operate. Switches work by sending traffic to the destination host only. This happens because switches have CAM (Content Addressable Memory) tables.

3. RESULTS AND DISCUSSIONS

3.1. HOW PACKET SNIFFER WORKS

Packet sniffer's operating can be understood in each switched and non-switched surroundings. For setup of a local network there exist machines. These machines have its own hardware deal with which differs from the opposite [2]. When a non-switched environment is taken into consideration then all nodes are linked to a hub which broadcast network site visitors to anyone. So as soon as a packet comes within the community, it receives transmitted to all be had hosts on that neighborhood community. Since all computers on that neighborhood community percentage the same twine, so in regular scenario all machines will be able to see the visitors passing thru. When a packet goes to a bunch then firstly community card tests it MAC address, if MAC address suits with the host's MAC deal with then the host will be capable of get hold of the content of that packet otherwise it's going to ahead the packet to other host connected in the community. Now here a want arises to see the content of all packets that passes thru the host. Thus we are able to say that after a host or machine's NIC is setup in promiscuous mode then all the packets this is designed for different machines, is captured without problems by that host or system.

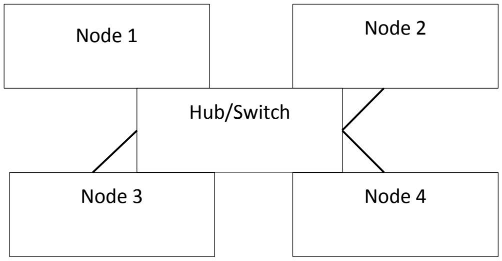

Figure.1. IEEE 802.3 network

When a switched environment is taken into consideration then all hosts are related to a switch as opposed to a hub, its miles known as a switched Ethernet also. Since in switched surroundings packet sniffing is more complicated in comparison to non-switched community, due to the fact a transfer does now not broadcast community site visitors. Switch works on unicast method, it does now not broadcast community traffic, it sends the visitors immediately to the destination host. This takes place because switches have CAM Tables. These tables store information like MAC addresses, transfer port and VLAN information [5][6]. [5] To apprehend working of packet sniffer in switched environment, an ARP cache desk is taken into consideration. This is a table that stores both MAC addresses and IP addresses of the corresponding hosts. This table exists in nearby area community. Before sending traffic supply hosts have to have its destination host, this vacation spot host is checked inside the ARP cache desk. If vacation spot host is available in the ARP cache then visitors may be sent to it thru a switch, but if it isn't to be had within the ARP cache then source host sends a ARP request and this request is broadcasted to all of the hosts. When the host replies the site visitors can be send to it. This traffic is sent in two elements to the vacation spot host. First of all it goes from the source host to the switch and then transfer transfers it at once at the vacation spot host. So sniffing isn't always possible.

3.1.1. ARP Cache Poisoning

ARP Cache Poisoning may be higher explained by way of a suppose we've 3 hosts x, y, z. Host x and y are connected thru a transfer and they commonly talk. Assume that z desires to see the conversation between x and y. When, x sends traffic which is destined for y it's miles intercepted by z. Z passes this records directly to y, pretending that it got here from x. This is finished with the aid of ARP Cache Poisoning.

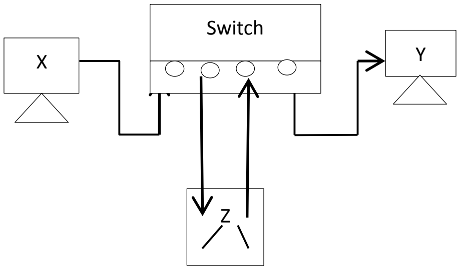

Figure 2: man-in-middle attack

3.1.2. CAM Table Flooding

Content addressable reminiscence desk works with the aid of flooding the CAM tables. CAM desk is a desk that the information like MAC addresses and switch port alongside their Virtual LAN records. A sure wide variety is stored via CAM table due to of being its restore size. As its name implies "CAM desk flooding" right here flooding way floods the transfer with MAC addresses and that is repeated till a factor at where transfer begins to broadcast network site visitors. [5][7]. Now it becomes clean to smell the packets.

3.1.3. Switch Port Stealing

As "transfer port stealing" right here on this approach we should steal the switches port of that host for which site visitors is designed to ship. When this transfer port is stolen through the person then user may be able to sniff the site visitors because a visitor goes through the transfer port first, then to instance "guy-in-the-middle-attack".

3.2. POSITIVE ASPECT

This software continues each tremendous and terrible component. Its effective aspects can be described as:

3.2.1. Network site visitor's evaluation

Traffic analysis is the system of intercepting and inspecting messages on the way to deduce information. It may be completed even on when the messages are encrypted and can't be decrypted. Traffic analysis comes in computer protection. Now a question arises why this visitor's analysis is done. It is accomplished within the context of navy intelligence or counter intelligence. If an attacker desires to advantage information, this records can be important facts. Then to benefit essential records he has to monitor the frequency and timing of community packets. A passive community tracking is being used by network IDS devices to come across feasible threats. This passive monitoring is a good deal extra useful for a security admin. He get the knowledge of community topologies, he get the knowledge approximately to be had offerings, data approximately working structures besides it he may be capable of get statistics about form of vulnerabilities [1].

Network site visitors can be analyzed by way of a community analyzer. A community analyzer is likewise called a protocol analyzer or packet analyzer. Network analyzer is a hardware device that gives safety in opposition to malicious pastime.

Network analyzer can:-

1. Provide element information of activities this is going on the community.

2. Test anti-malware packages and pin-factor capacity vulnerabilities.

3. Detect uncommon packet traits.

4. Identify packet assets or vacation spot.

5. Configure alarm for defined danger.

6. Search of precise statistics string in packets.

7. It captures all the records and shows it.

3.2.2. In Intrusion Detection

Now a day, no person can live without making use of internet due to of its services on hand. Its users are increasing day-to-day. In such increasing atmosphere there are many probabilities of being an intrusion. To control these intrusions an appropriate intrusion detection method is used [10]. In giant corporations existence of intrusion detection is integral. Intrusion Detection is the energetic or steady motion to observe intrusive acts. So a packet sniffer is utilized in intrusion detection by way of which it could reveal network or method pursuits for malicious movements. Intrusion detection is priceless as a result of following purpose:

1. New and new software are developed daily. Regularly they suffer from occurrences of bugs. So intrusion detection is valuable to unravel these bugs.

2. As we all know that internet dimension is increasing day-to-day and number of its customers can also be growing. In an effort to maintain a track on process abuses an intrusion detection procedure is used.

3. In huge organizations to keep a track on incidence of an intrusion, Intrusion Detection method is situated.

3.3. INSTRUMENTS FOR INTRUSION DETECTION

There are various tools for intrusion detection:

3.3.1. Computer Oracle and Password system

This can be a procedure that's used as a device for Intrusion detection. As it's identify implies it is used to check passwords and startup gadgets besides it, it is also used for checking file permissions. These checking are performed through a normal user. Police officers then use comparison to investigate. Many safety instruments which might be clearly designed for UNIX techniques, administrator, programmer, operator or consultant in the uncared for subject of the pc security are combined to make law enforcement officials. [8] There are twelve small protection determine applications that are built-in through police officers.

These packages look for:

1. File directory and gadget permission/modes.

2. Terrible passwords.

3. Protection of passwords.

4. Programs and documents run in /and many others.

5. Existence of SUID records, their writability.

6. A CRC determine towards foremost binaries or key files.

7. Nameless ftp setup.

8. Unrestricted tftp, decode alias in send mail, SUID uudecode problems, hidden shells.

9. Miscellaneous root tests.

10. Checking dates of CERT advisories versus key records.

11. Writability of person's house directories and startup records.

3.3.2. Tripwire

Tripwire is a tool that's truly used for intrusion detection. Each database/system has a couple of documents and every change in these documents is monitored via a protection utility. This utility is called Tripwire. This monitoring is done by means of retaining digital signature of every file. Using these signatures, tripwire checks file integrity. There are numerous digital signature algorithms which might be supplied by using Tripwire. When Tripwire creates digital signature for essential files then this signature is checked in opposition to checksums.

If a change is discovered, it simply approaches there had been some changes within the records by an interloper.

3.3.3. Tiger

It’s just like law enforcement officials. [9]Tiger is a kind of security instrument. It's used no longer best as a security audit but also it's used as an intrusion detection approach. More than one UNIX platforms are supported by using tiger. It's freely available and if we need to take it then we should go by means of the GPL License approach. When it is compared from other instrument then we get that it wants only of POSIX instruments and these tools are written in shell language. Along with various functions it has some fascinating aspects that exhibit its resurrection and this resurrection involves a modular design that's effortless to broaden and it has a double facet where it can be used as an audit tool and as a number intrusion detection instrument. There are many ways wherein free program intrusion detection is presently going. These ways goes from network IDS to the kernel but there's a case that it does not point out file integrity checkers and log checkers. This software is complemented via tiger and presents a framework for collectively working. Tiger may also be freely downloaded from savannah.

3.4. NEGETIVE SIDE

Sniffing applications are determined in two forms: business packet sniffer and Underground packet sniffer. Industrial packet sniffer has constructive aspect seeing that it is utilized in keeping network whereas underground packet sniffer has bad part due to the fact it is commonly utilized by attackers to reap unauthorized entry to far off host [3]. Accordingly we see that this application has some poor points too.

3.4.1. Unauthorized access

Once we perform sniffing then content of packets is seen by using us. For the reason that all the contents are in encrypted type however they can be decrypted through hackers with the aid of imposing a hacking table. If packet involves some personal know-how akin to any one’s consumer name and password then hackers may just use it to obtain authorized entry.

3.4.2. Posting a danger

When community site visitors are analyzed then we are able to submit some malicious pastime. Packet sniffing is a well identified illustration of intrusion ways.

3.4.3. IP Spoofing

To gain unauthorized access to machines, IP spoofing is a strong system. Right here an interloper sends messages to a pc with an IP handle. And this IP tackle indicates that the message is coming from a trusted host. That is used for:

1. Reprogramming routers

2. Denial of provider attack

3.4.4. Man-in-core attack

It is a well-recognized example of ARP Spoofing. That is often referred to as a Bucket bridge assault, or normally Janus assault. Computer safety is a type of active eavesdropping where the attacker makes unbiased connections with the victims and relays messages between them, making them suppose that they are speaking straight to each other over a personal connection, when actually the whole dialog is controlled by the attacker. The attackers have got to be in a position to intercept all messages going between the two victims and inject new ones.

3.5. DEPENDABLE GUARDS

There are lots of ways via which we can protect our packets. One in every of them is with the aid of utilizing encryption. There are three ways to apply encryption on packets.

3.5.1. Link-level encryption

Encryption mechanism is utilized on packets once they get on transmission medium and when they reach on the vacation spot, a decryption mechanism is applied. This mechanism restrict from sniffing. Due to the fact that a packet sniffer gets access to packets at that time when they are transported on the medium. If they are already encrypted, then no knowledge is gained, if they don't seem to be encrypted then packet’s content may also be easily accessed.

3.5.2. Finish-to-end encryption

Packets are transmitted amongst hosts. In finish to end encryption each and every packets are encrypted through the host that transmit the data and they're decrypted via the host when they're acquired on the different finish.

3.5.3. Software level encryption

The application layer makes it possible for the user, whether or not human or software to access the network. It supplies consumer interfaces and help for offerings reminiscent of piece of email, far flung file entry and switch, shared database management and different form of allotted know-how services. So we see that, at this deposit packets include touchy material. So an encryption mechanism will have to be utilized at application degree.

3.5.4. SSL

SSL is nothing, it is at ease socket layer that's used to encrypt packet. In order that we can also be in a position to get comfy channel for database communication or simple mail transfer protocol. We can use whatever call SSL over http in electronic commerce and email that's “HTTPS” [9].

3.5.5. TLS

TLS is nothing, it is transport layer protection. It is centered on SSL. Right here a requirement arises that TLS use the certificates which now a day's known as internet centered certificates [9].

3.5.6. IP security Protocol

It really works in community layer of OSI mannequin. Its work is to encrypt all ship packets [9]. We could also be capable to summarize all these pursuits through showing the following diagram between two strategies:

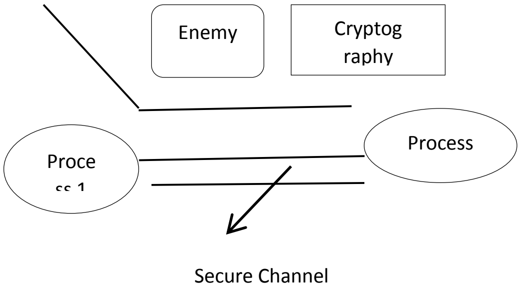

Figure 7: Security process

4. CONCLUSION

This paper proposes a procedure to detect packets by way of packet sniffing. It involves some bad factors but besides these poor elements it's much useful in sniffing of packets. Packet sniffer isn't used for hacking purpose but additionally it is used for network traffic evaluation, packet/site visitors monitoring, troubleshooting and different priceless functions. Packet sniffer is designed for shooting packets and a packet can contain clear text passwords, consumer names or different sensitive material. Sniffing is feasible on each non-switched and switched network. We will use some tools to seize community site visitors that are additional used by researchers. We are able to conclude that packet sniffers can be utilized in intrusion detection. There exist some instruments also that can be utilized for intrusion detection. Accordingly we will say that packet sniffing is a manner through which we can create an intrusion and by way of which we are able to realize an intrusion.

REFERENCES

[1] 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.

[2] Ryan Splanger, "Packet sniffing detection with Anti sniff", University of Wisconsin-Whitewater, May 2003.

[3] Tom King, "Packet sniffing in a switched environment", SANS Institute, GESC practical V1.4, option 1, Aug 4th 2002, updated june/july 2006.

[4] RyanSpangler, "Packetsniffingonlayer2switchedlocalareanetworks", PacketwatchResearch:http://www.packetwatch.net, Dec 2003.

[5] Sconvery, "HackingLayer2: FunwithEthernetSwitches", Blackhat, 2002, Available:http://www.blackhat.com/ presentations/bh-usa-02/bh-us-02-convery-switches.pdf.

[6] http://www.monkey.org/dufsong/dsniff/.

[7] http://www.fish2.com/cops/overview.html.

[8] http://nongnu.org/tiger/.

[9] http://www.securityteam.com/unixfocus/Detecting sniffers on your network .html.

[10] Baykara, Muhammet, and R. Das. "A survey on potential applications of honeypot technology in intrusion detection systems." *International Journal of Computer Networks and Applications* 2.5 (2015): 1-9.