International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

Sniffing Network Data Packet in a LAN Environment by Tampering the CAM Table

Roshani Pandey[1], Anupama Sharma[2]
[1, 2]*Department of Computer Science Engineering, Shri Shankaracharya Institute of Technology and Management, Chhattisgarh Swami Vivekanand Technical University, Bhilai(C.G.),India*

Abstract: ***Now a days Network communication become an important part of every organization as well as part of every human beings. In a computer communication communicated data are in the form of data packets. Network packets in a computer communications can be defined as an amount of data in a limited size. In Internet all traffic travels in the form of packets, the entire file downloads, Web page retrievals, email, all these Internet communications always occur in the form of packets.Packet sniffer is a tool or device that can be used for capturing the packet at data link layer in a Network. Packet sniffer is not only a hackers tool but it can be used both by the hacker for eavesdropping and by the administrators for network monitoring and troubleshooting. 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 in wired as well as Wi-Fi networks for monitoring network. In this paper we studied the various methods for sniffing the data packets traveling across the Network in a LAN.***

Index term*: Network packet sniffer, active and passive sniffing, ARP Cache poisoning, CAM Table, MAC address, IP address.*

I. INTRODUCTION

As the internet introduced as soon as it becomes the part of human beings. In a computer network communicated data is in the form of data packets. Data communication is the process of data sharing from one node to another by using the network entities. Data is important for every organization and human so it is important for every administrator to provide a secure communication over the network. Secure communication means if two entities are communicating sharing a data via internet then third-party do not listen it or we can say data privacy does not compromises. The data which is traveling across a network is not in a continuous stream of data in fact it is in the procedure of packets. As we know that we cannot see the atom through uncovered eye so for that we have needed a device like electronic microscope same is in the case of examining the data packet. Packet sniffer may be utensil or programs that can be used for capturing the packet at data link layer in a network. Packet sniffer is not only a hackers tool but it can be used both by the hacker for eavesdropping and by the administrators for network monitoring and troubleshooting. There are two types of sniffing Passive Sniffing and Active Sniffing.

A. Passive Sniffing

Passive sniffing is used in shared networks where hub is used as a network entity. The problem of using hub in a network is that hub broadcast a data packet to every connected machine. There is a filter on each machine which chooses whether to receive or reject the packet. If a packet address is matched to a machine's address then filter choose to accept it otherwise discard the packet. Sniffer disables this filter so that network traffic can be examined. This stage is called "promiscuous mode". Detection of passive sniffing is difficult because it does not create any traffic on network. This sort of sniffing gives the batter result when a network uses the Hub. Today most of the network uses switch in place of hub to avoid passive sniffing.

B. Active Sniffing

Active sniffing is done on switched network. A switch bounds the sniffer to see the broadcast packets. Switch worked as a central entity than broadcasting, it simply get message from source machine and send it directly to the addressed machine. So for that it doesn't imply sniffing can't be done in a switched network. Media Access Control (MAC) flooding and poisoning of the Address Resolution Protocol table (ARP) are the ways to hack a switched network.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

II. WORKING OF SNIFFERS

Every computer system which is connected in a LAN has a unique identity or unique address, one is MAC(Media Access Control) address and second is IP address which are needed to uniquely identify the each node of the network. MAC address is a physical address which is hard coded into the community card. MAC address uniquely assigned to each NIC by the manufacturer. In a LAN MAC address is used while constructing frame to exchange information to and from a node. Second unique identity that is IP address is employed by application. The second layer of OSI model that is data link layer uses an Ethernet header with the MAC address of the destination node. The network layer of OSI model is accountable for mapping IP address to MAC address, whenever there is a need of MAC address by the data link layer, so for that ARP(Address Resolution Protocol) is used, for which an ARP cache is maintained. It at first check the MAC address of the destination node in a ARP cache. If there are no any entry for IP address are exist then ARP plays an important role for mapping the IP address to the corresponding MAC address. ARP uses the two type of the message for mapping the address one is request ARP and second one is Reply ARP which is exchanged by the nodes for resolving the address problem. The ARP broadcasts a request packet to all the nodes that are connected in LAN the nodes which have that MAC address gives the respond to the source node with its IP address. This IP address is then added to the ARP cache of the source node with their corresponding MAC address. These addresses are then used by the source node for their communication with the corresponding node. There are two basic types of Ethernet environment Shared Ethernet and Switched Ethernet,how sniffers work in both these cases is slightly different.

A. Shared Ethernet

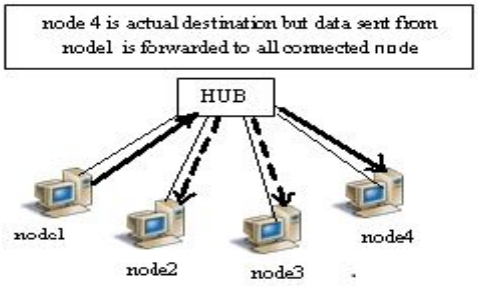

Fig.1 Shared Ethernet

In shared Ethernet environments, all hosts are connected to the identical bus and compete with one another for bandwidth. In such a situation packets meant for one machine are received by all the other machines. Suppose there are few computers connected in a shared LAN and Comp 1 wants to communicate with Comp2 in such a circumstance, it sends a packet into the network with the destination MAC address (that is MAC address of Comp2) along with their own MAC address. All the nodes which are connected in a shared Ethernet like Comp3,Comp4 and so on compare their own MAC address with received frame's MAC address, if it is not matched then discarded the received frames. A system on which sniffer is running. A machine running sniffer breakdowns this law and accepts all frames. Such a computer is said to have been put into promiscuous mode and can effectively listen to all the traffic on the network. The Sniffing in a Shared Ethernet condition is absolutely latent and consequently tough to observe.

B. Switched Ethernet:

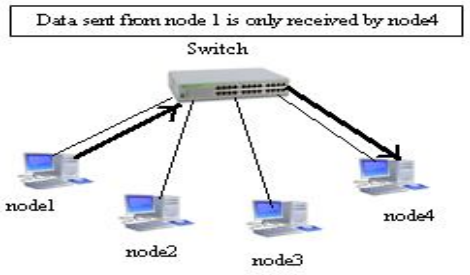

Fig.2 Switched Ethernet

An Ethernet situation in which hosts are connected to a switch instead of a hub is called a Switched Ethernet. In a switch environment a table is keeps up on which MAC address and physical port of connected nodes are maintained that helps in safe communication by sending the packets direct to the destination node. The switch is a wise gadget it does not broadcast the packets to all the LAN's connected nodes. This leads to higher usage of the accessible data transfer capacity and enhanced security. So for sniffing network packets in a switched Ethernet NIC of the system is putted into the promiscuous mode but this become fail for sniff the packets. Accordingly, even many experienced administrator fall into the conviction that exchanged systems are thoroughly secure and invulnerable to sniffing. Anyway a switch is more secure than a Shared Ethernet; the following strategies can at present be used to sniff on a switched Ethernet.

1) ARP Spoofing

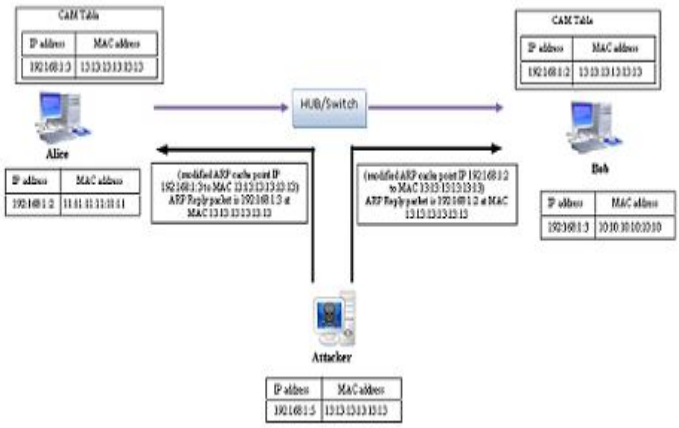

Fig.3 ARP Spoofing

This is an approach where by an attacker sends counterfeit ("spoofed") Address Resolution Protocol (ARP) messages onto LAN. For the most part, the point is to relate the attacker's MAC address with the IP address of another host, (for example, the default passage), resulting any traffic which is implied for that IP address is received by the attacker. ARP spoofing may enables an attacker to catch information frames on a LAN, change the traffic, or stop the traffic out and out. Frequently the assault is utilized as an opening for different assaults, for example, Denial of service attack, man in the middle attack, or Session Hijacking assaults. The assault must be utilized on systems that make utilization of the Address Resolution Protocol (ARP), and are constrained to nearby system portions. By and large, the point of the assault is to relate the attacker's MAC address with the IP address of an objective host, so any traffic bound for the objective host will be sent to the attacker's MAC. The attacker could then decide to:

a) Inspect the packets, and forward the traffic to the genuine default gateway.

b) Modify the information before sending it this is man-in-the-center assault.

c) Launch a Denial of Service assault by delivering a few or the majority of the packets on the system to be dropped

III. EXISTING WORK

Three types of sniffing techniques are used. These are:

A. IP Based Sniffing

IP based sniffing works in a non-switched network or can say works in case of Hub used network. The method which is most widely used for sniffing is IP based sniffing. In this method for sniffing NIC is putted into the promiscuous mode. Whenever NIC of host system is putted into the Promiscuous mode then host may become capable to sniff all the packets that are travels into the network. In the IP based sniffing IP based filter is used for sniffing and only those packets are captured which are matched with the IP address filter. [3].

B. 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].

C. ARP Primarily Based Sniffing

This method may be used in switched as well as non switched environment. IN LANs the administrator of the network most of the time uses the extraordinary methods Packet Sniffer and Remote Network Monitor (RMON) for observing the behaviour of LAN and diagnosing the troubles arising into the network. This technique can be easily performed in case of non-switched environment. Working of switched network is different as compare to working of non-switched network. In case of switch environment traffic are only sends to that host for which they are generated, this become possible because of CAM (Content Addressable Memory) tables, which is associated with switch.

IV. PROPOSED METHODOLGY

A. How Packet Sniffer Works

Packet sniffer's operating can be understood in each switched and non-switched surroundings. For creating a LAN environment some tools or machines are used. 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 neighbourhood community. Since all computers on that neighbourhood 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.

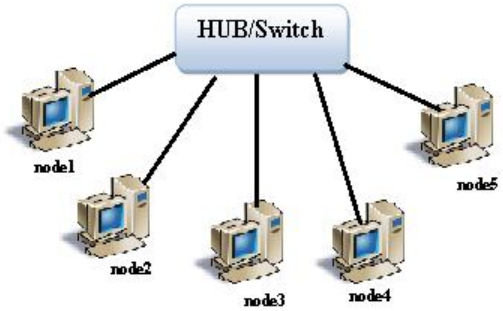

Fig.4 IEEE 802.3 network

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 sniff the network packet into the switch Ethernet, an ARP cache desk is used. In a CAM table the unique identity that is Physical addresses and logical addresses of the hosts are stored, both unique identities are necessary for communication over the network. This table exists in nearby area community. Before sending the traffic to the target host, source host must have IP address and MAC address of the destination host which is most important for performing the secure communication between two node so that source host first checks the address available into the ARP cache, if the address is available into the ARP cache then it sends traffic direct to the destination port with their address. Yet on the off chance that if any of the address is not to be had inside the ARP cache then the source host sends

an ARP request which is broadcasted to the entire switch connected host, then host replies their address by sending an ARP reply to the source host. In a switch environment traffic is first sends from source host to switch and then direct from switch to the destination. So that the communication over switch environment is more secure than the communication over non-switch environment hence sniffing is can't be perform at all the time.

1) ARP Cache Poisoning

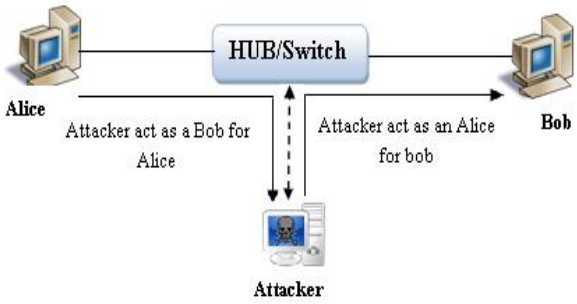

Fig.5 ARP cache Poisoning

ARP cache poisoning is an approach to perform the sniffing in a switched Ethernet. The unauthorized nature of ARP protocol gives a benefit for performing the ARP cache poisoning. In this approach a host can easily sends a fake ARP message to the target host for poison the ARP cache of the target host. This can be understand as suppose there are two host in a switched Ethernet they are generally communicate with each, let there are another host known as eavesdropper wants to sniff the communicated data, so that it sends a fake ARP message by associating the real host IP address and their own MAC address to both the host and pretend as it is those host to which they want to communicate. Results is that whenever a real host sends a data to other real host to which they wants to communicate then it is first received by the eavesdropper then eavesdropper forwarded the data to the target host. So that the eavesdropper has a chance to modify or sniff the data packets by poisoning the ARP cache.

2) CAM Table Flooding: CAM(Content Addressable Memory) table is used in a Switched Ethernet for safe communication to store the Physical address i.e. MAC address of host and corresponding locations of switch port alongside a timestamp for the entry and Virtual LAN records. So for sniff the network data packet CAM table is flooded this is another approach for sniffing a network packet in a switched environment. As the name implies "CAM Table Flooding", CAM table is flooded with so many number of MAC address so that the switch become fail to store or manage the CAM table. The CAM Table Flooding is performed by spoofing the MAC address until the memory become full. Then switch ultimately broadcasted all the packets to the entire switch connected host. [5][7]. Now it becomes clean to smell the packets.

3) Switch Port Stealing: Switch Port Stealing is another Network Sniffing technique in switched Ethernet, this technique worked when ARP poisoning technique become fail to sniff the network packet when the static mapped ARPs are used. In this Switched Ethernet is flooded with ARP packets results that the destination MAC address which is associated with every sending packet is the address of sniffer system means that in this approach sniffer treated as the switch port so that sniffer become capable to see all the network packets.

B. Positive Aspect

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

1) Network Site Visitor's Evaluation: Network packet sniffer captures all the network packets travel into the Ethernet. The information or traffic captured by the sniffer helps the network administrator to identify the malicious or erroneous or vulnerable packets. The main task of every Ethernet administrator is to provide a secured communication in their Ethernet environment. Network packet sniffer sniffs the network packet and helps to detect the malicious packet so that the administrator can control the malicious activity on their Ethernet environment and provides a secure communication. Traffic analysis is a tool for 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. Network sniffer helps an administrator to get all the information related to a network packet like protocol used, source address and destination address. Main reason to introduce a network sniffer is monitor a network and provide a secure communication

in an Ethernet environment. 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, these 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 gets the knowledge of community topologies, he gets the knowledge approximately to be had offerings, data approximately working structure besides it he may be capable of getting statistics about form of vulnerabilities [1].

2) In Intrusion Detection: As a day to day new network technology and applications are developed, chance of attacks into the network is also increased. Network packet sniffer monitors the network and checks for malicious activity into the Ethernet. Network packet sniffer helps the administrator to make the Ethernet free from the intrusions if any occurs into the network by monitoring the network activity. To control the intrusions over a network administrator of the Ethernet uses an appropriate intrusion detection method [10]. In giant corporations existence of intrusion detection is integral. Intrusion Detection is an energetic approached for observing the intrusive acts. So a packet sniffer is utilized in intrusion detection by way of which it could reveal networked or method pursuits for malicious movements. Intrusion detection is priceless as a result of following purpose:

a) As the new software is developed then intrusion detection system helps to solve the bug problems if any occurs in it.
b) As the number of internet users increases then intrusion detection system helps to maintain the working of internet.
c) In huge organization intrusion detection system is used to make the organizational network free from the intrusions.

3) In a Forensic Analysis: Network Packet Sniffer may help police to perform the forensic analysis over a criminal case by monitoring the network and also helps to check that the traffic travels over the network is malicious or not.

4) Speed up the Data Transfer Rate: Network Packet Sniffer monitors the data traveled into the network so that it helps to solve the traffic congestion problem and by solving the network traffic issue data transfer rate is increases.

C. Instruments for Intrusion Detection

There are various tools for intrusion detection:

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:-

a) File directory and gadget permission/modes.
b) Terrible passwords.
c) Protection of passwords.
d) Programs and documents run in /and many others.
e) Existence of SUID records, their writability.
f) A CRC determine towards foremost binaries or key files.
g) Nameless FTP setup.
h) Unlimited File Transfer Protocol, decipher the alias for sending the mail, SUID uudecode issues, concealed shells.
i) Miscellaneous root tests.
j) Checking dates of CERT advisories versus key records.
k) Writability of person's house directories and startup records.

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) 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.

D. 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.

1) Denial of Service Attack: Network Packet Sniffer captures all the network flows data information by using this information an attacker can perform a DoS attack (denial of Service attack). In this attack attacker has intensity to degrade the performance of the target system or interrupted to fully utilize the resources by continue sending too many request at the same time so that the server become fail to responds all the request and causing the crash of server.

2) Hijacking the Network Packet: Once we perform sniffing then content of packets is seen by using network packet sniffer. 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) 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.

4) IP Spoofing: IP spoofing is a type of attack in which the attacker pretend like it is an authentic host to which target communicated. In this attack the attacker masked their own system IP with the real source IP and treated like a trusted host. IP spoofing is a powerful approach for gaining unauthorized access to the target system. This method is mainly used in:

a) Reprogramming routers

b) Denial of provider attack

5) 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.

E. 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. Mainly three approaches are used for Encryption of packets.

1) Link-level Encryption: Network Packet sniffer gets the data packets at time when data packets transmitted in a transport medium. So for preventing the data packet from sniffer encrypt the packets by using some encryption method. For the secure communication over the network source host must encrypt the data packet and transfer to the transport medium which is then decrypted by the destination host when data packet is received. If network packets are already encrypted, then no knowledge is gained by the sniffer, if they don't seem to be encrypted then packet's content may also be easily accessed.

2) Finish-to-end Encryption: In a network, data packets are transferred from one host to another host for the communication purpose. So for the secure communication data packets are encrypted by the source host and decrypted by the destination host. In

finish to end encryption each and every packets are encrypted through the host who transmit the data and they're decrypted by the host who received the transmitted data..

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.

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].

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].

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:

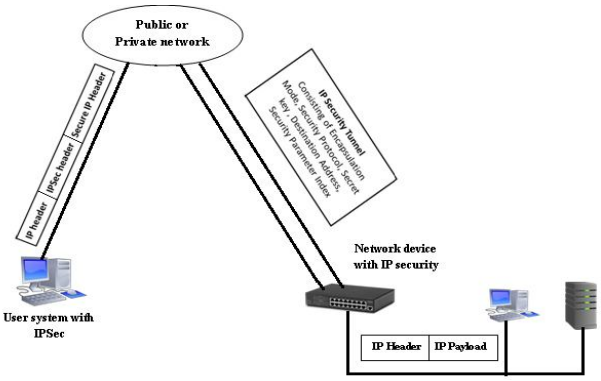

Fig.6 Security process

V. 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] D.Bruschi, A. Ornaghi and E.Rosti, "S-Arp, A secure Address Resolution Protocol," in Computers Society Applications Conference, Proceedings, 19th Annual, IEEE, pp. 66-74, 2003.
[5] W.Lootah, W.Enck and P. Mc Daniel, "Tarp:Ticket based address resolution protocol," Computer networks, Vol.51, no. 15, pp. 4322- 4337,2007.
[6] S. Kumar and S. Tapaswi, "A centralized detection and prevention technique against ARP poisoning," in Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), International Conference in, Kuala Lumpur, Malaysia, pp. 259-264, 2012.
[7] RaviyaRupal.D,DhavalSatasiya,H.Kumar, A.Agrawal, "Detection and Prevention of ARP Poisoning in Dynamic IP configuration," IEEE International Conference on Recent Trends in Electronics Information Communication Technology in, India, May 20-21, 2016.
[8] S.Y. Nam, D.Kim and J.Kim, "Enhanced ARP:Preventing ARP Poisoning based Man-in-the-Middle Attacks," Communications Letters, IEEE, vol.14, no. 2, pp.187-189, 2010.
[9] Zouheir Trabelsi and Hamza Rahmani, "Detection of Sniffers in an Ethernet network," in ISC 2004, pp.170-182,2004.

[10] J.Gao and K.Xia, "ARP Spoofing Detection Algorithm using ICMP protocol," in Computer Communication and Informatics (ICCCI), 2013 International Conference in Coimbatore, India, pp. 1-6, 2013.
[11] F.H.Barbhuiyah, S.Hubballi, S.Biswas and S.Nandi, "A host based DES approach for detecting ARP Spoofing," in Control and Automation (MED), 2010 18th Mediterranean Conference in Marrakech, Morocco, pp.695-700, 2010.
[12] V.Ramachandran and S.Nandi, "Detecting ARP Spoofing: An Active Technique," in Information Systems Security, in Spinger, pp.239-250, 2005.
[13] P.Pandey, "Prevention of ARP Spoofing:A Probe Packet based Technique," in Advance Computing Conference (IACC), 2013 IEEE 3rd international, Ghaziabad, India, pp. 147-153, 2013.
[14] Cisco Systems, "Configuring Dynamic ARP Inspection in Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide, Release 12.2SX", ch. 39, pp. 39:1–39:22, 2006.
[15] C.L.Abad and R.Bonilla, "An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks," in Distributed Computing Systems Workshops, ICDCSW07, 27th International Conference in Toronto, Canada, p.60, 2007.
[16] F.A.Lopes, M.Santos, R.Fidalgo, S.Fernandes, "A Software Engineering Perspective on SDN Programmability", in IEEE communications surveys & tutorials, Vol. 18, No. 2, second quarter 2016.
[17] W. Xia, Y. Wen, C.H. Foh, D. Niyato and H. Xie, "A Survey on Software Defined Networks," IEEE Communications Surveys and Tutorials, Vol.17, issue:1, FirstQuarter,2015.
[18] W.You, K.Qian, Xi He, Y.Qian,"Int. J. Advanced Networking and Applications", in ISSN :0975-0290,Vol. 6 Issue: 3,pp. 2347-2351,2014.
[19] T.Alharbi, D.Durando, F.Pakzad and M.Portmann, "Securing ARP in Software Defined Networks", IEEE 41ST Conference on Local Computer Networks, 2016.
[20] Huan Ma, H.Ding, Y.Yang, Z.Mi, J.Y.Yang, and Z.Xion, "Bayes-Based ARP Attack Detection Algorithm for Cloud Centers", Tsinghua Science and Technology, in ISSNl 1007-0214l l02/10,Vol. 21, No.1, lpp.17-28, in February 2016.
[21] A.M.Abdelsalam, A.el-Sisi, Vamshi reddy, "Mitigating ARP Spoofing Attacks in Software-defined Networks,"in ICCTA ,at Alexandria,Egypt,2015.
[22] M.J. Masoud, Y.Zaradat and I.Jannoud, "On preventing ARP poisoning attack utilizing software defined network paradigm," in Jordan Conference on Applied Electrical Engineering and Computing Technologies(AEECT),IEEE,2015.
[23] J.H.Cox, R.J.Clark and H.L.Owen, "Leveraging SDN for ARP Security," in Southeast Conference, IEEE, 2016.
[24] Rupam,Atul Verma,Ankita Singh,"An Approach to Detect Packet Sniffing,"IJCSE,Vol.4,No3,June 2013, DOI: 10.5121/ijcses.2013.4302