iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4311

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

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 IV, Apr 2019- Available at www.ijraset.com

Network Packet Sniffer with Proxy Detection Service

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

Abstract: ***In a network communication data is shared between two parties in a packet format via communication link that may be wired or wireless. Data which is shared between parties are important for them. So it is responsibility of every network administrator to provide a secure communication link between the parties for that purpose network administrator can use the network sniffer. Network sniffer is a network monitoring tool. There are so many network sniffing tools available they sniff the entire incoming and outgoing network data packet. All of these tools work in a LAN environment. In a LAN if there are such a system exists which uses the proxies then there may be a chance a user can misuse the services provided by the Ethernet. Suppose you have a wireless open Wi-Fi network, provide access permissions to your client but there is a client who misuse the service and access some malicious sites or having intensity to harm the network services so far that client tries to hide their identity and uses the proxies. Then it becomes important to monitor Ethernet network and find the proxy user. So that if we provide the network sniffer with proxy detection service then it may become a complete sniffing tool.***
Index term: Network packet sniffer, active and passive sniffing, ARP Cache poisoning, CAM Table, MAC address, IP address, Proxy Server and VPN.

I. INTRODUCTION

Network is a combination of two or more computers or electronic devices connected either by using wired or wireless media for sharing data, information or resources.The data which is travelling across a network is not a continuous stream of data in fact it is in a form of packets. In an Ethernet a packet carries maximum of 1500 bytes at the network layer. The packet contains the source address, destination address and information. Whenever a message sends from a source to destination then at first message is breaks into the packets then these packets is transmitted to the network. Packets of a single message travels into the network does not follow the same path, the path chosen by each packets is depend on the link and routing protocol. 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 network 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.

A. Types of Network Sniffing: - There are mainly two type of network sniffing is performed.

1) Passive Sniffing: Passive sniffing is used in shared networks. The problem of using the hub in network is, hub broadcast a data packet to every machine on the network. There is a filter on each machine which chooses whether to receive or reject the packet. If a packet addresses to a machine 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 creates any traffic on network. This sort of sniffing gives the batter result when a network uses the Hub. To avoid passive sniffing most of the networks today are using switches in place of hubs.

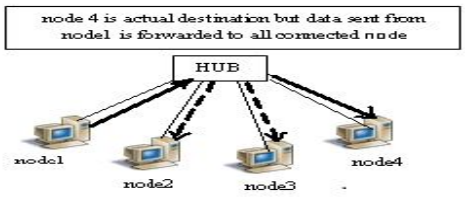


Fig1. Passive Ethernet

©IJRASET: All Rights are Reserved

2) 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.

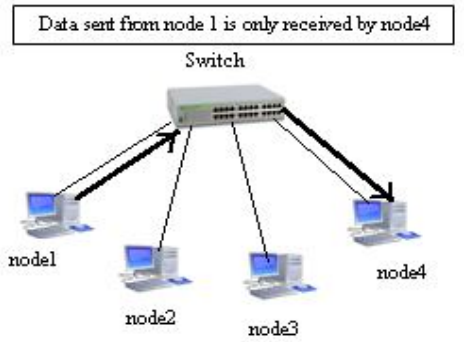


Fig2. Active Sniffing

B. Proxy Server: Proxy server is an intermediary software system or computer device between the host and internet, which separates the end users from the browsing websites. If the host uses the proxy server then the traffic flows through the proxy server and after that it is forwarded to the target website[27*]*.

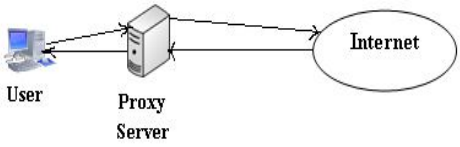


Fig.3 Proxy Server

C. NIC

NIC (Network Interface Card) it is a physical device, which is installed into the devices for connecting them with the network. NIC is also known as network adapter or Ethernet card. A NIC provides the computer with an obsessive full-time association to a network. Physically NIC is a circuit board, has a plug on one side to which it connects with computer's bus and a connector on the opposite side that acknowledges an attachment proper for a given LAN. Legitimately, an Ethernet adopter identifies the address of each incoming and outgoing network packets, calculates the CRC and also acknowledges each frames (i.e. NIC checks the address of each incoming frames from networks and accepts only those frames for which computer is destined and discards all the other frames) and also handles the data communication of a system with the other host in a network.

1) How NIC Works: Network Interface Card works as a bridge between the network and computer device that connects a device with other system via internet for data communication. When a host communicates with another host in an Ethernet environment then NIC specifies the logical address and port number of destination host. The IP address or logical address specified by the NIC is converted into MAC (Media Access Control) address, and then packets are inserted into the MAC frames for transmission. Since each IP address is partitioned so that the packets are fitted into the MAC frames. The MAC frame contains the destination address. When a NIC received a network packet then it first check the MAC address of received packet with their own address, if it is matched then accepts the packets otherwise discard it. *An Ethernet card works by taking the information given to it by the system's CPU and sending it to a destination host.* When data is sends from a host then systems NIC makes the data into the transferable form and when the data is received by the host then the system's NIC convert the received data back into the usable form. A single device may have multiple NICs so that there may be a chance to have multiple MAC address of a single system on a network. Network interface cards have a buffer for storing the each incoming and outgoing data so that it becomes possible to solve the latency issues.

©IJRASET: All Rights are Reserved

2) Modes of NIC: Modes of NIC mean the configuration setting of NIC. There are mainly two types of NIC configuration settings in which NIC works that is Promiscuous Mode and Non-Promiscuous Mode

a) Promiscuous Mode: In this configuration setting of NIC, it passes all the received traffic to the central processing unit rather than only those traffic that are destined for it. In this mode all the network traffic which is destined or not destined to a controller device is captured by the NIC. By placing a network sniffer on a network in promiscuous mode, an administrator can analyze the entire network packet.

b) Non Promiscuous Mode: In a non promiscuous mode network card captures only those frames which is directed to it. When a network packet is received by NIC then it compare the MAC address of the packets with their own MAC address, if the address is matched then accepts the packet otherwise filters it. In non-promiscuous mode, only the data destined for a particular controller through MAC addresses is sent to CPU, the rest packets are dropped.

D. Principle used for Packet Sniffing

NIC captures the entire data packets although those packets which are not destined for it when NIC is set to the Promiscuous mode and but when it is sets into the non-promiscuous mode then it accepts only those for which it is destined. In a network communication the when a source nodes sends a data packet to a targeted nodes through a network then these packets reached to the destination host by traversing many intermediate nodes of network. A node whose NIC is set in the promiscuous mode then those node can captures entire data packets although packets are not destined for them. The network packets received by NIC is copied to the device driver memory, which is further passed to the kernel buffer and from the kernel buffer it is used by the user application.

In case of packet sniffer at user level when a live capture session is created then the packets are copied from kernel buffer to a buffer by creating the libPcap. In Linux Kernel, libPcap uses the PF_PACKET socket which bypasses most packet protocol. Each socket has two kernel buffer associated with it one for reading and another for writing. Before copied the next data packet into the buffer, at a time a single packet is handled by the buffer for application processing.

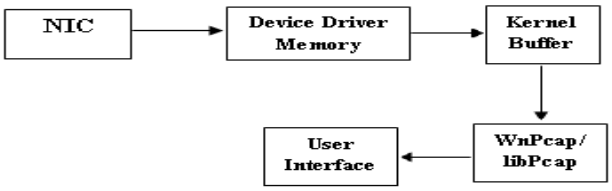


Fig.4 Working Principle of Network Packet Sniffer

E. Technique Used For Network Sniffing

Three types of sniffing techniques are used. These are

1) 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].

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].

3) 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 those hosts for which they are generated, this become possible because of CAM (Content Addressable Memory) tables, which is associated with switch.

©IJRASET: All Rights are Reserved

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

II. EXISTING TOOLS FOR NETWORK SNIFFING

A. SolarWinds Packet Analysis Bundle

It is a deep packet evaluation and analysis tool. It is a bandwidth analyzer. This bandwidth analyzer provides two very useful application to the network administrator i.e. Network Performance Monitor and Netflow Traffic Analyzer.Network Performance Monitor helps to find out the network availability and their response time. It also detects the network performance issue and tries to resolve them. Netflow traffic analyzer detects the users and the applications which consume the most bandwidth.The SolarWinds Packet Analysis Bundle tool inspects the data hold inside the capture packet and check what application causes the most traffic within the network.

B. Wireshark

Wireshark is an open sources and freely available network Protocol Analyzer;that monitors the network and data packets flowing through it. It gives the complete details about the network. Wirsshark may run on multiple platforms like Windows, Linux, Mac OS, Solaris, FreeBSD, NetBSD, etc.. It provides the decryption facilities over many protocols like IPsec, ISAKMP, Kerberos, SNMPv3,SSL/TLS,WEP and WPA/WPA2. WireShark has a feature like rich VoIP analysis, standard three packet browser, live capture and offline analysis,read/write many different file formats and capture file compressed with gzip.

C. PRTG Network Monitor

PRTG is a windows compatible packet sniffing software which uses the different technologies like Netflow ,WMI, REST APIs for network traffic sniffing that provides the graphical views of network performance. It filters the data packets according to the IP addresses, protocols, and type of data. One of the main features of this tool is Dashboard, which shows the bandwidth used by the various application and network traffic. The main feature of PRTG is the packet sniffer sensor that tracks the packet, and records the headers of each data packet. PRTG tool monitors the network web traffic, mail traffic, file transfer traffic, infrastructure, traffic, remote control, other UDP and TCP traffic.

D. Steel Central Packet Analyzer

It is a bit level packet sniffing tool which is fully integrated with WireShark. This tool gives the graphical user interface facility that helps to identify the root network problem by using the pre-defined analysis views.

E. TCP Dump

TCP dump is a free software which was initially designed for UNIX system and is often pre-installed on almost all UNIX-like OS.TCP dump is a command line tool which display the TCP/IP and all the packet information which are transmitted and received over a network and also identify the source of network problems.TCP dumps uses the libcap to capture the network packet. In a Windows; port of TCP dump is Win Dump which uses the WinPcap for capturing the network packet.

F. Network Miner

This tool was designed for Windows that can be operated offline which makes the network analysis very simple. This tool has facilities like it can easily detect the host name, OS used by the host and open ports of network hosts.

G. Kismet

This tool was specially developed for wireless network which is compatible with MAC and OSX environment and KisMAC. This tool has facilities like it can detect the hidden network, SSIDs, presence of wireless applications, network hosts and traffic created by them.

H. EtherApe

EtherApe is a open source packet sniffer which has a similar feature as WireShark but the only difference between them is their data representation. This tool has features like it has protocol summary dialog which shows the global traffic statics by protocol,traffic statics by protocol is detected by Node Summary dialog, XML file is exported by Node Static , multiple user chosen nodes are arranged in an inner circle with other nodes where as single node is centered on the display.

©IJRASET: All Rights are Reserved

III. PROPOSED METHODOLGY

Network Sniffer is a very smart tool for capturing the network packet but if we provide the sniffing tool with proxy detection service then there may be more wonder. Since the intensity for developing Network Monitor with Proxy Detection service is to monitor the working of network and securing the network from malicious activity. For the implementation of the Network Monitor Tool with Proxy Detector following two methodologies are proposed:-

1) Network Sniffing Methodology
2) Proxy and VPN detection Methodology

A. Network Sniffing Methodology

1) *Put the NIC into Promiscuous Mode:* In this configuration setting of NIC, it passes all the received traffic to the central processing unit rather than only those traffic that are destined for it. In this mode all the network traffic which is destined or not destined to a controller device is captured by the NIC. By placing a network sniffer on a network in promiscuous mode, an administrator can analyze the entire network packet. So for developing this tool first add the jpcap to the JAVA Library and also download the winpcap for windows or libpcap for Linux operating system.

2) *Check the installation of WinPcap or LibPcap in OS:* LibPcap and WinPcap are liberary for the capturing the packet in Operating System.

a) *WinPcap:* To capture the data from network in windows OS WinPcap is use which is directly interfaced with the network adapter. Therefore the OS must provide a set of primitives to capture the network packets to communicate with the adapter.

WinPcap has the three basic components

i) Packet Capture Driver: It is a part of the Kernel that interacts with NIC to capture the packets.

ii) *Packet.Dll:* It works in a user level which is a dynamic link library used for separates the application from packet capture driver for providing a system independent capture interface and allows the user's application without recompilation of program to be run on different Windows OS.

iii) *WinPcap.Dll:* IT is a static library which uses the service provided by the Packet.dll. It provides a powerful capture interface and manages the interaction with the user display the results of captured packets.

b) *LibPcap:* LibPcap is a widely used open source standard packet capture library for directly capture the packets from NIC which is mainly designed for UNIX OS. It was developed for use with BPF (Berkely Packet Filter) kernel device. BPF can be considered as an OS kernel extension. It is BPF, which enables communication between OS and NIC. LibPcap is a C language library that extends the BPF library constructs. If this library is missing in the OS then we can install it.

3) Add the jpcap package into JAVA library

a) *JPcap- Java Packet Capture:* JPcap is libcap/WinPcap based an open source library file which is implemented by using the programming language C and JAVA for capturing and sending the network packets to the JAVA applications. JPcap is a collection of java classes and interface for capturing Ethernet, IPv4, IPv6, ARP/RARP, TCP, UDP and ICMPv4 packets and by abstracting many network packets type and protocols into java class it can hides the low level details of captured packet. JPcap has the facilities like it can capture the raw packets live from the wire and save it to an offline file and later it is used for analysis. It automatically detect the packet type and generates the java object for corresponding network packet and filters the packets based on the user defined rules. It gives us a facility to develop network application like network analyzer, traffic logger, network intrusion detection system, security tools etc.

4) By using the JPcap package Perform the following Protocol Analysis

a) Analyze network Layer.
b) Analyze Transport Layer.
c) Analyze Application Layer.
d) Analyze UDP Protocol
e) Analyze TCP Protocol
f) Analyze HTTP Protocol
g) Analyze Free Memory Size

©IJRASET: All Rights are Reserved

h) Show Line-graph Representation.
i) Show Pie chart Representation.
j) Find out the Packets over network.
5) After Analyzing the Protocols, Designing the Following Modules
a) User Interface Module.
b) Packet Sniffing Module.
c) Analyze layers Module.
d) Free Memory Module.
e) Protocol Analysis Module.
6) User Interface Module: This module is designed to provide user interaction with the Packet sniffer tool. It gives an easy to use interface to the users. Technically swing is used in Java for preparing this user interface.
7) Packet Sniffing Module: This module is designed to collect the network packets that are transmitted and received by the NIC of that machine on which Packet sniffer is installed. If the NIC is set to the promiscuous mode then it will receives all the packets of connected network.
8) Analyze Layers Module: This module contains the code for analyzing the layers in the system. Mostly in this module we have to discuss about three layers Transport layer, Application Layer, Network Layer. The module shows the graphical representation of the usage of different layers in packet capturing time. It can show the graph in two manners like line graph and pie graph.
9) Free Memory Module: This module represents the memory size in number format as well as in a graphical form. This module also analyzes the utilization of computer memory at the time of network packet capturing.
10) Protocol Analysis Module: To analyze the protocols like Transmission control protocol (TCP), User Datagram Protocol (UDP), Hyper Text Transfer Protocol (HTTP) etc. of the layers this module is designed. This module displays the information of source port, destination port and packet length of the host delivered packet.

B. Proxy and VPN detection Methodology

After capturing the data packets and analyzing the each captured packet we get the IP address of source and destination hosts of each packet, now we will do check the legality of each network connected host by detection of Proxy and VPN user. In order to detect the proxy and VPN uses the following methodology:-

1) Check the Size of Each Captured packet for VPN Detection: The maximum length of the data that can be transmitted by a protocol in one instance is known as the Maximum Transmission unit. By default the MTU size of an Ethernet interface is 1500 bytes, which excludes the header and trailer of Ethernet frame. It means that the Ethernet interface carry the frame larger than 1500 bytes. Every Network Interface, routers which transmit the packets between the host and remote side have its MTU value.When a TCP connection is created by the host web browser or any other software working with the network to the remote side then it adds the maximum segment size (MSS) value into TCP header, it means that the remote side of the maximum TCP data size initiator can receive without packet fragmentation which value is same as the MTU.As hosts open a web page by using the PPTP, L2TP (±IPsec) or IPSec IKE, then data packet is encapsulated into another packet which introduces the overhead. To transmit the large packet which is fragmented to be successfully delivered via network, decreases the data transmission speed and added the some latency. To reduce the excessive fragmentation OS sets the MTU on the VPN interface which is smaller than the real network interface MTU. It means that there is no standard or usual size for PPTP, L2TP or IPSec. The VPN administrator sets the approximately value of MTU for the protocols according to the minimum MTU size among all VPN user. In case of Open VPN within the encapsulated packet decreases but the size is decreases inside the MSS side are set by the MSSfix setting which calculate the Open VPN overhead for the packet encapsulation and encryption. MSS size is sets according to the packets flow without any fragmentation. To work with any link it is configured with MTU 1450 or more by default. Due to this uniqueness of MSS values, we can determine not only if the host is connected via Open VPN but also used connection protocol (IPV4,IPV6), transport protocol (UDP and TCP),cipher, MAC and compression as they affect MSS.
2) Data Gathering Method: In a data gathering method first purchase a proxy service licence through TorGuard. TorGuard provides the service to test the five different proxy connectivity types from hundreds of server across the globe. In this test we also utilize the configurations that are available through free proxy lists and alternative connectivity types such as VPN tunnel and mobile

©IJRASET: All Rights are Reserved

connections. When the proxy configuration is completed then establishes the connection with the pre-configured server, which contains a packet logging application and for each connection documents the instance and detect the proxy connection and for the best result gathered test data from different browser.

3) *Reverse DNS Test:* Network interface can easily perform the some usual task like ARP processing, ICMP echo answering or DHCP rebinding. To confirm the IP of target machine an Internet Control Message Protocol request is sends that results the DNS name, that is used to verify the connection path to resolve the same target machine and not to a local IP.
4) *TOR Network Discovery Test:* By parsing the list of publicly available TOR exit nodes identify the majority of TOR (an anonymity network) and then comparing the target machine's public IP against the list.
5) *RBL Database Test:* In this test the IP address which is collected by the packet sniffing module is sends to the third party service in order to use RBL database, where the target Machine's public IP is compared against the RBL database, which can be represent a potential security concern and higher service cost.
6) *HTTP header Testing:* The HTTP header analysis technique is used to detect the HTTP headers and determine the end user's IP address based on their typical proxy header .The transparent proxies does not hides the host's IP address because of it enforces a particular HTTP header in the request, through which the end user's IP address can be identified.

IV. IMPLEMENTATION

For Implementing Network Monitoring Tool with Proxy Detection service in a Java language following steps are used:-

A. The main task performed by network sniffer is monitoring the Ethernet by sniffing entire network packet traveling into the Ethernet, for that purpose putted the NIC into Promiscuous mode
B. Data received by NIC is copied into device driver memory. Then from device driver memory, data is passed to the Kernel Buffer. For implementing the Network Monitor Tool in a java language use the JPcap Package, Download the JPcap Package and added it into the JAVA library
C. By using the JPcap package we can retrieved the data stored in Kernel Buffer and perform the following analysis:
1) Analyze network Layer.
2) Analyze Transport Layer.
3) Analyze Application Layer.
4) Analyze UDP Protocol
5) Analyze TCP Protocol
6) Analyze HTTP Protocol

D. By analyzing the all the required protocol we get the IP addresses of hosts connected in a LAN and Analyzing them for detecting the Proxies if any host uses it . For that purpose taking the following steps:
1) Retrieving the IP Address
2) Retrieving the packet size for VPN detection
3) Sending the ICMP message for Proxy Detection
4) Making the list of publically available Tor exit node
5) RBL dataset Test.

E. For implementing "network monitor tool with proxy detection service" design the following module :
1) User Interface Module
2) Packet Sniffing Module
3) Layers Analyzer Module
4) IP Analyzer Module with Proxy and VPN detection

After summarizing all modules, output comes by using mixed approach of all modules. Now we connect our system into a Local Area Network and capture the source address the proposed tool check the Proxies and will show the result if the proxy is detected.

©IJRASET: All Rights are Reserved

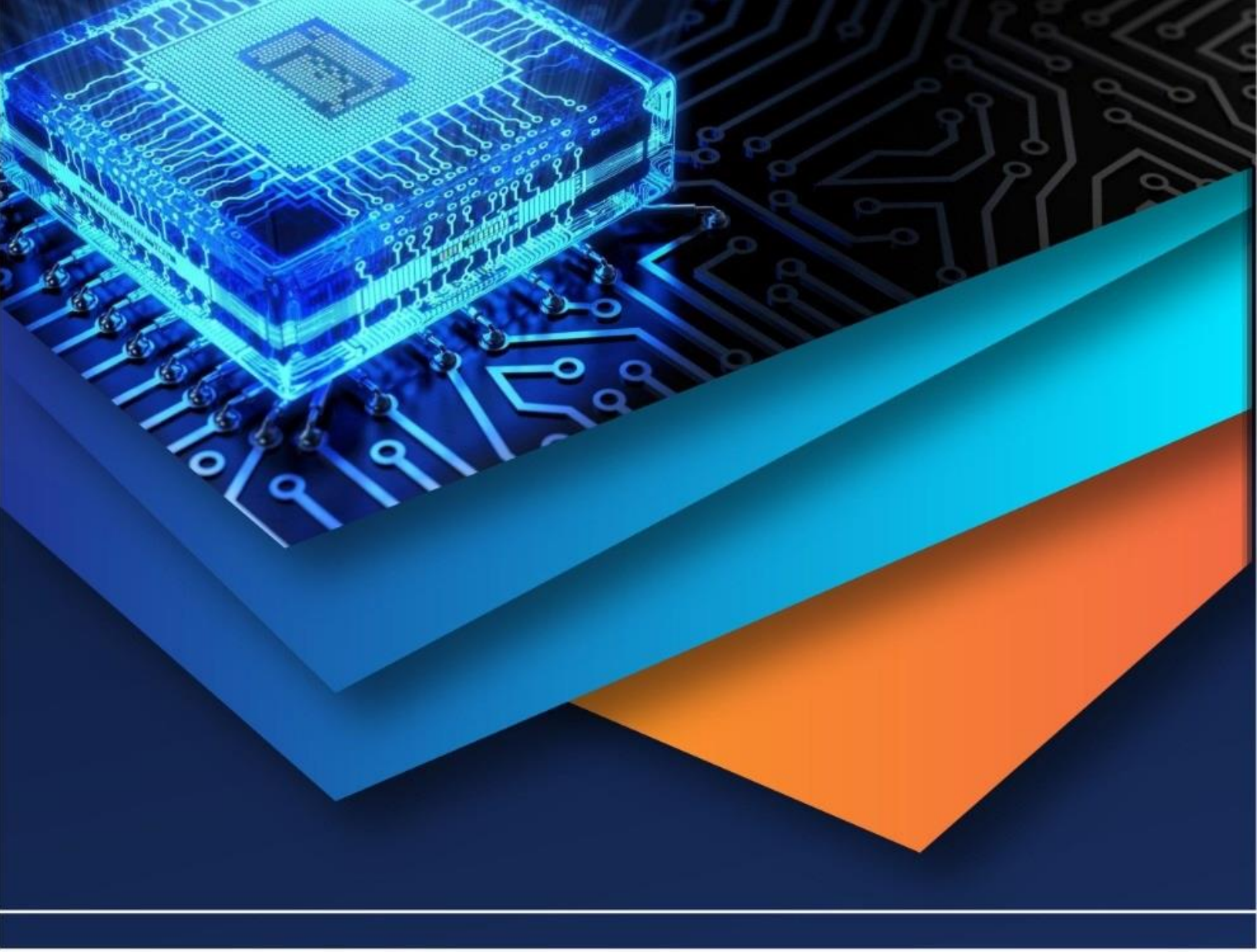
V. CONCLUSION

This paper proposes a procedure to detect packets by way of packet sniffing. This project monitor the network packet and get the source address of each network traveling packets and after capturing the IP of each network packet analyze it for the proxy detection. This project 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 capturing and analyzing 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
[25] Mandeep Pannu, Bob Gill, Robert Bird, Kai Yang, Ben Farrel,"Exploring Proxy Detection Methodology,"Confrence,IEEE,2016
[26] Zhipeng Chen, Peng Zhang, Qingyun Liu," ProxyDetector: A Guided Approach to Finding Web Proxies, 2017 IEEE 42nd Conference on Local Computer Networks.
[27] Surbhi Gupta, Puneet Bhalla, " Securing Wi-Fi Network Via Proxy Servers," Research Inventy: International Journal Of Engineering And Science Vol.3, Issue 7 (August 2013), PP 01-05
[28] Oluwabukola,Awodele Oludele,A.C Ogbonna, Ajeagbu Chigozirim, and Anyeahie Amarachi," A Packet Sniffer (PSniffer) Application for Network Security in Java," in Informing Science and Information Technology Volume 10, 2013

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)