ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 1, January 2018

A Framework to Prevent Sniffing Attacks Over Network

Milky Jha, Raghavendra Kumar
M.Tech Scholar, Department of Computer Science and Engineering, Lakshmi Narain College of Technology Jabalpur, (M.P.), India
Asst. Professor, Department of Computer Science and Engineering, Lakshmi Narain College of Technology Jabalpur,(M.P.), India

ABSTRACT: Generally Malicious users make use of different attacks at different levels to steal different level of data. Some of the sniffing attacks that can be used in different levels of networking/transmission are Media Access Control (MAC) Flooding, Dynamic Host Configuration Protocol (DHCP) Attacks, DHCP Starvation Attack, Rogue DHCP Server Attack, Address Resolution Protocol (ARP) Spoofing, MAC spoofing and Domain Name Server (DNS) Poisoning. In this paper, a comparative study has been done with the above mentioned sniffing attacks and the level of recovery that can be done with each sniffing attack.

KEYWORDS: Sniffing, MAC Flooding, DHCP Attacks, ARP Spoofing

I. INTRODUCTION

Packet sniffing is a form of wiretapping applied to the Networks. Through this, attacker can monitor and capture data from networks. Attacker can capture the following information:
1.File Transfer Protocol (FTP) Passwords,
2.Router Configuration,
3.Telnet Passwords
4.DNS traffic
5.Email Traffic
6.Web Traffic
7.Chat Sessions.

Computers can be connected by bus or switch. If the network is connected by bus then it is termed as shared Ethernet. If it is connected by switch then it is termed as switched Ethernet. In Shared Ethernet environment if a packet is send means it will broadcast the packet to all machines. Only destination machine will acknowledge. Other Machines will ignore the packet. This rule is ignored by attacker. In switched Ethernet the switch maintains a table which contains the MAC address of all computers in the Network. So the message is sent to the destination machine only. Though Switch is more secure than Hub, sniffing can be done even in switch.

Sniffing is categorized into various types:
1.MACflooding, 2.DNS poisoning 3.ARP Poisoning 4.Dynamic Host Configuration Protocol (DHCP) Attacks 5.Password sniffing

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 1, January 2018

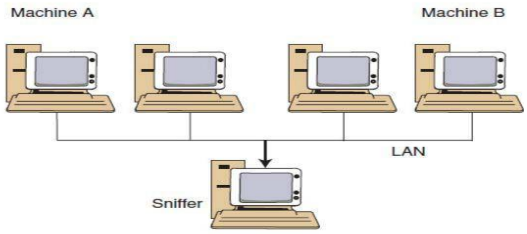

Figure 1: Sniffer in a Local Area Network

The Protocols vulnerable to sniffing are1.Telnet 2.HTTP, 3.POP, 4.IMAP, 5.SMTP, 6.FTP

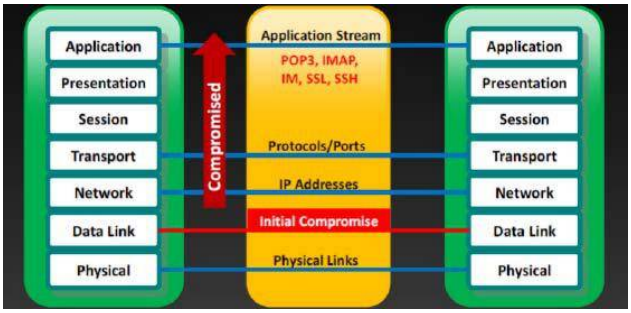

Figure 2: A Sniffer monitors a network and sniffs data

Sniffers operate at the Data link layer. If that layer is sniffer then the upper layers are compromised.

II.MAC FLOODING

Media Access Control (MAC) is a physical address which identifies each node in a computer network. Content Address Memory (CAM) stores the MAC address in switch. The size of CAM is fixed. If the CAM table is flooded with MAC address beyond its capacity, the switch is turned into a hub. Then attackers can easily sniff data

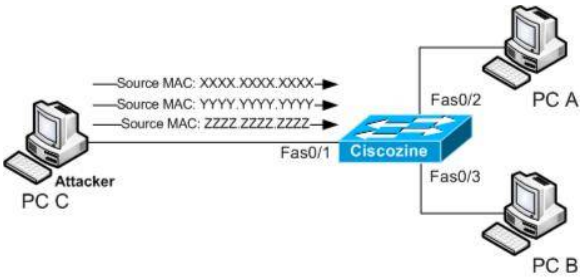

Figure3: MAC Flooding

In figure 3, the attacker uses MAC Flooding concept to turn the switch into hub and thus can easily steal sensitive data. [1]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 1, January 2018

III.DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) ATTACKS

DHCP is a client server protocol which provides IP address to a host. It also provides configuration related information like default gateway, subnet mask. A DHCP relay agent, which passes DHCP requests from one LAN to another so that there need not be a DHCP server on every LAN. It involves the following steps

1. Client broadcast DHCPDISCOVER request asking for DHCP configuration
2. DHCP Relay agent unicast this message to DHCP server

3. DHCP server unicasts DHCPOFFER, which contains client and server's MAC address
4. Relay agent broadcast DHCPOFFER in the client's network
5. Client broadcast DHCPREQUEST asking for DHCP configuration
6. Server unicasts DHCPPACK which contains configuration information.

IV. DHCP STARVATION ATTACK

In this type, the hacker requests large number of DHCPREQUEST and uses all the available IP Address. As a result, the DHCP server cannot issue any more IP Address and in turn leads to Denial of Service (DOS) attack.

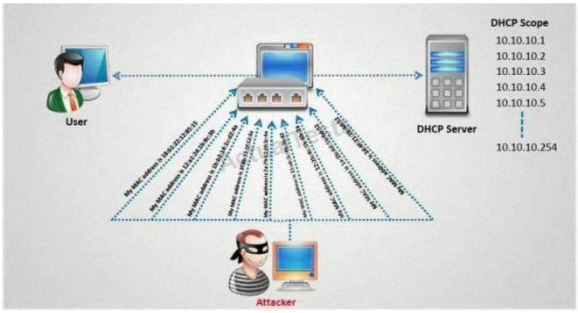

Figure 4: DHCP Starvation Attack

In Figure 4: Attacker Requests a large number of IP addresses to the DHCP server which results in Denial of Service to the other users.

V. ROGUE DHCP SERVER ATTACK

In this attacker will introduce a rogue server. DHCP Server and rogue server both will respond to the DHCP request of the client. The server which responds will be taken by first. The rogue server will respond first. Client will send data to the rogue server which in turn will send to actual server. Thereby attacker monitors and captures all sensitive data. The client will be unaware of all these attacks.

VI. DEFENSE AGAINST DHCP ATTACKS

Port security will limit the maximum number of MAC addresses on the switch port, thereby DHCP attacks can be avoided. DHCP snooping feature is available on switches. In order to defend against rogue DHCP servers, DHCP snooping is configured on the port on which valid DHCP server is connected. Thereby the switch will not allow the other ports to respond to DHCP request. [1]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 1, January 2018

VII. IV.ARP SPOOFING

Address Resolution Protocol (ARP) is a stateless protocol which resolves IP address to MAC Address. If the MAC address is not present in the ARP table, the node will broadcast ARP request. All the nodes will compare their IP address with this. Only one of the node identifies this and respond with this. ARP provides no means of authenticity checking.

The attacker can send any arbitrary IP and Mac address. The victim's computer ARP table store this malicious content.

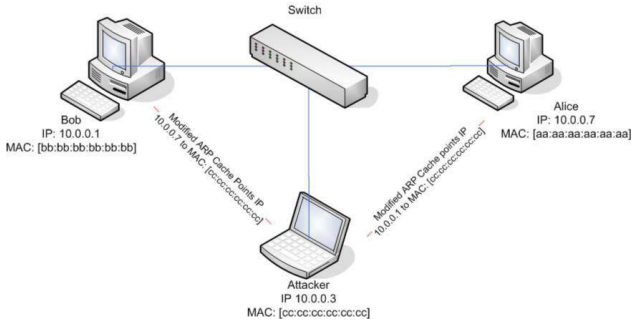

Figure5: ARP Poisoning

Figure 5 explains the concept of ARP Poisoning. The node 10.0.0.7 stores the IP address of 10.0.0.1 and attacker's MAC Address. Similar ARP Poisoning is done for 10.0.0.1 also.

The threats of ARP Poisoning include:1. Packet Sniffing, 2.SessionHijacking, 3.Manipulating Data, 4.Man in the Middle Attack, 5.Connection Hijacking, 6.Connection Resetting, 7.Stealing Passwords, and 8.Denial of Service (DOS) Attacks. [3]

VIII. DEFENSE AGAINST ARP POISONING DYNAMIC ARP INSPECTION (DAI) VALIDATES THE ARP

Packets in a network. DHCP snooping must be enabled prior to DAI. DAI performs IP to MAC address binding inspection stored in the DHCP snooping database. If any invalid binding is found then discard the ARP Packets. Thus Man in the Middle Attacks is eliminated. [2]

IX. V. SPOOFING ATTACKS

Spoofing allows the hacker to pretend to be authorized user. The types are 1.MAC Spoofing 2.ICMP Router discovery protocol (IRDP)

X. MAC SPOOFING

MAC addresses are used for authorization. These are permanent by design and can be changed by physical hardware.MAC spoofing is nothing but forging MAC address.MAC duplicating or spoofing is sniffing one of the client's MAC address and reusing it. Malicious user can listen and receive all the traffic to the legitimate user.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 1, January 2018

Ways to defend MAC Spoofing:

1. Port security enabling is a way to mitigate MAC spoofing
2. By using DHCP snooping binding table. This table contains the legitimate user's MAC address and IP address. It acts as a firewall between legitimate and malicious users.

3. Dynamic ARP inspection: It verifies MAC address and IP address for all the packets. If any invalid address is found then they are dropped.

XI. IRDP SPOOFING

IRDP is an extension of ICMP protocol. IRDP protocol allows a router to identify the active router's IP address by its advertisements. It allows nodes to listen "Router Advertisement". When the node receives, this may lead to change in the routing table. The node does not check for authenticity of the message. A malicious user can spoof the router itself. A Hacker may change the default route provided by server. Thus the attacker can sniff data

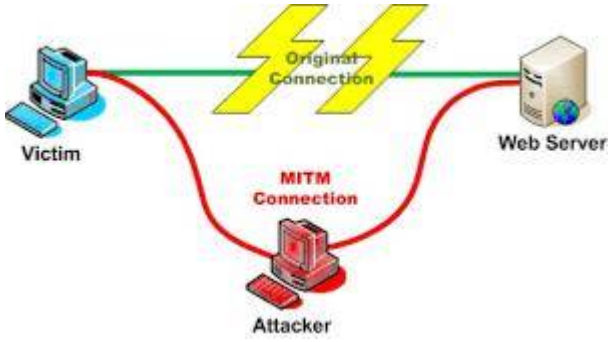

Figure6: IRDP Spoofing

XII. DNS POISONING

Domain Name Server is a Protocol which translates the Domain name to IP address. It maintains a DNS table which contains domain name and its IP address. In DNS Poising/DNS spoofing can be done by manipulating DNS table. So the victim is redirected to malicious server instead of actual server. Once connected it can sniff data. There are 4 ways of DNS Poisoning is there.

1. Intranet DNS spoofing, 2.Internet Spoofing, 3.Proxy server DNS Poisoning, 4.DNS cache poisoning

XIII. INTRANET DNS POISONING

When DNS poisoning is done in Local Area Network then it is known as Intranet DNS Poisoning. The attacker poisons the router in order to get DNS request to his machine. Then DNS response is sent to the legitimate user and thus

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 1, January 2018

legitimate user is redirected to fake website which is created by malicious user instead of actual website. Thus hacker can sniff important data like passwords. So once sniffing is done, the client is again redirected to actual website and client is totally unaware of the scenario.

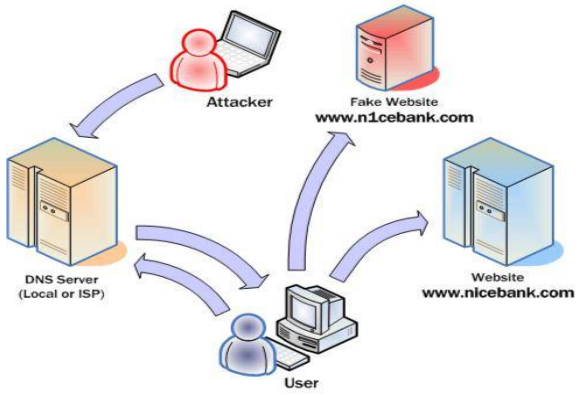

Figure7: DNS Poisoning

XIV. INTERNET DNS SPOOFING

It is otherwise known as remote DNS Poisoning. Attacker sends a Trojan to legitimate user which changes the DNS IP address to attacker's IP address. Thus sniffing confidential data is done.

XV. PROXY SERVER DNS POISONING Attacker sends a Trojan to change Proxy settings of

the user to malicious user's fake website. Thus data can be sniffed.

XVI. DNS CACHE POISONING

The DNS system contains cache which contains domain names and respective IP addressed. When a request comes it first checks DNS cache. If the entries are found then it is redirected accordingly. This DNS resolver cache is modified by attacker. If the DNS resolver cannot validate the DNS responses then it is redirected to malicious server. [4]

XVII. SNIFFING TOOLS

The various sniffing tools used by hackers are as follows:

- Wireshark allows us to capture live network data. This network data can be filtered by IP address, Protocols and Ports.
- Capsa Network Analyzer captures all data transmitted over the network. It captures IP address and MAC address of each host in the network.
- MSN Sniffer 2 captures MSN chats across all computers in the same LAN.
- Colasoft Packet is a packet generator or Packet Editor Tool. Attacker can use this tool to create malicious network packets to carry out the attack on the network.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 1, January 2018

XVIII. STEPS USED BY SNIFFERS

Step 1: Hacker finds out the switch of the network and connects to one of its ports.

Step 2: Once connected, discovers network topology using network discovery hacking tools like wireshark

Step 3: By analyzing the network, sniffer gets the IP of victim's machine using tool like Capsa Network Analyzer

Step 4: Once he knows IP of the victim, he sends fake messages using the tool like Colasoft Packet

Step 5: The Previous step results in the Man in the Middle Attack (MITM)

Step 6: Now the attacker succeeds in sniffing the packets.

XIX. DEFENSE AGAINST SNIFFING The countermeasures are as follows:

- Use Encryption to protect confidential information.
- Use static IP addresses and static ARP tables to prevent attackers from adding the spoofed ARP entries.
- Restrict the network to authorized users only
- Use IPV6 instead of IPV4
- Use encrypted session such as SSH instead of telnet.
- Use HTTPS instead of HTTP to protect usernames and passwords.
- Use of switches is better than Hubs as switches deliver data only to the recipient.
- Password authenticate the shared folders and services
- Encrypt the communication between PC and access point to prevent MAC address spoofing

XX. SNIFFER DETECTION TECHNIQUE

The sniffer leaves no trace, since it does not transmit data. Systems should be checked for promiscuous mode. Promiscuous mode is a mode of the Network Interface Card (NIC) that allows all the packets without validating its destination address. Stand alone sniffers are difficult to detect as they do not send packets. The reverse DNS Lookup can be used to detect non stand-alone sniffers. An Intrusion Detection System is a security mechanism that helps us to detect sniffing activities.

Ping Method: A Ping request has to be sent to the suspect machine with incorrect MAC address. Only the sniffer will respond to this.

ARP Method: ARP should be added to all the nodes. The node which runs in promiscuous mode will cache the MAC address. The Ping message should be sent with different MAC. Only the sniffer node will be able to respond.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 1, January 2018

Promiscuous Detection Tool: Promqryui tool will helps us to detect the node which is in promiscuous mode.

XXI. PROPOSED SOLUTION

To detect Sniffing is to do sniffing pen testing

1. Using the tool macof, the switch should be checked for failopen mode where it broadcasts the data and this may lead to sniffing. If so the system is prone to MAC flooding.
2. Using the tool Gobbler, DHCP starvation attack can be checked.
3. WinArpattacker tool is used to find ARP poisoning. It changes the ARP table by manipulating MAC address
4. SMAC is a tool used for MAC spoofing and it changes the MAC address in the network card

Once all the tests are performed, it is analyzed and has to take countermeasures to fill the gap in security

XXII. RESULT AND ANALYSIS

Packet sniffing and network capture is done with wireshark. In figure 8, wireshark displays the TCP conversations and thus sniffers can identify port number, sequence number and IP address of a legitimate user.

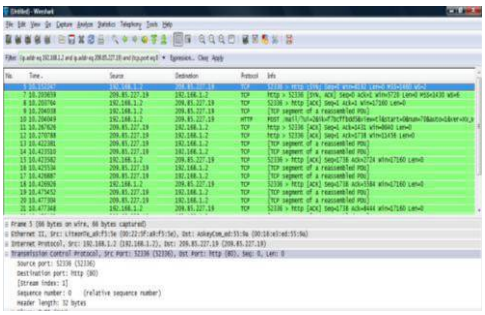

Figure8: Sniffing Network

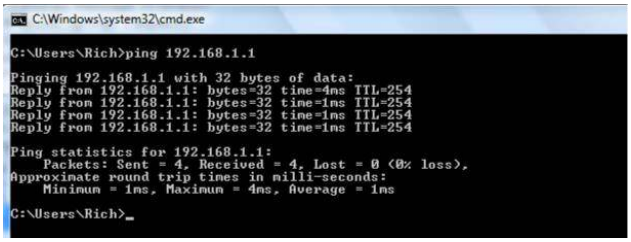

Figure9: Ping Method

In the above figure ICMP traffic is done using Ping command

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 1, January 2018

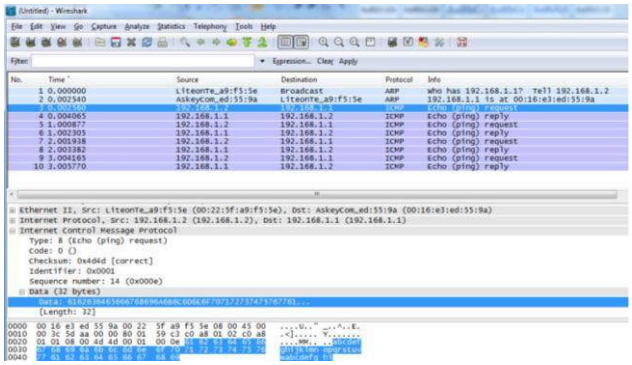

Figure10: ARP Poisoning

Figure 10 explains ARP Poisoning, ICMP traffic is monitored

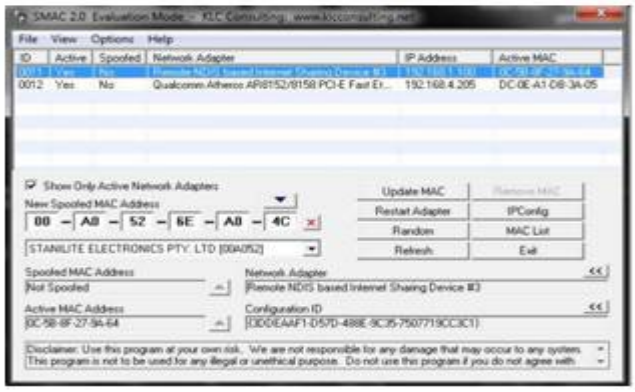

Figure 11: Spoofing a MAC using SMAC

Figure 11 explains spoofing a Mac using smac tool.

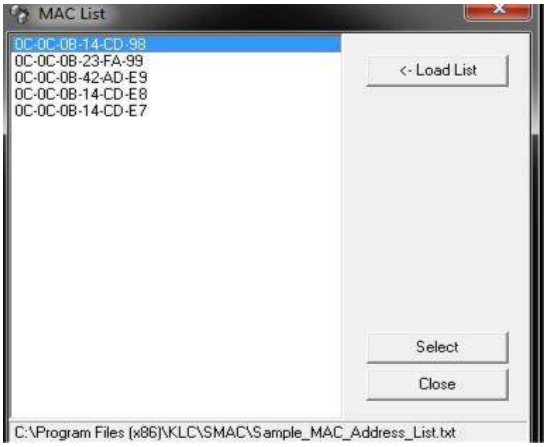

Figure 12:Mac list

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 1, January 2018

Figure 12 in the network which can be spoofed using smac.

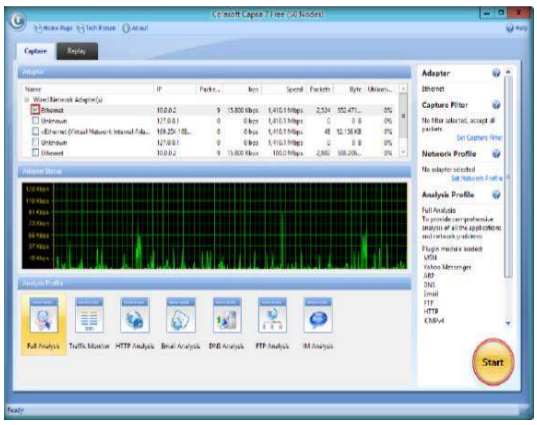

Figure 13:Colasoft capsa Network Analyzer

Figure 13 explains the network traffic which can be spoofed using colasoft

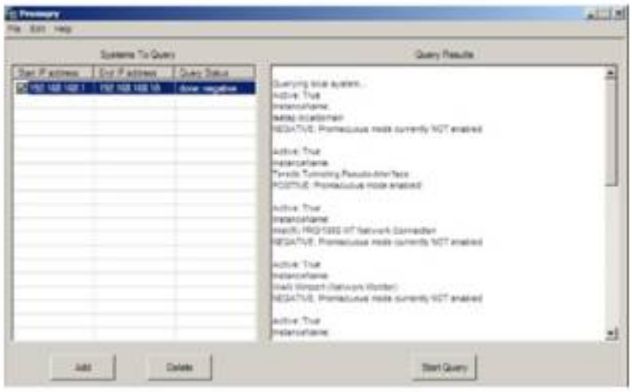

Figure 14:Promiscuous mode detection

Figure 14 explains promiscuous mode detection using promqry tool

XXIII. CONCLUSION

This paper proposes an approach to detect packets through packet sniffing. Sniffer is not only used for hacking purpose but also it is used for network traffic analysis, packet/traffic monitoring, troubleshooting and other useful purposes. Packet sniffers can be used in intrusion detection. There exist some tools also that can be used for intrusion detection. Packet sniffing is a technique through which an intrusion can be created and through which an intrusion can be detected.

REFERENCES

[1]A Novel Web Content Spoofing Technique on WLAN and Its Countermeasures, 2014 International Symposium on Communications and Information Technologies (ISCIT), Sumedt Jitpukdebodin ,and Roongroj Chokngamwong, Supakorn Kungpisdan
[2] Sniflyzer: A Network Sniffer, OPEN JOURNAL OF INFORMATION SECURITY AND APPLICATIONS, Volume 1, Number 2, September 2014,Varsha Khokhar, Shehnaz Khan, Priyanka Muppuri, Prachi Ahlawat

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 1, January 2018

[3] An Approach to Detect Packets Using Packet Sniffing, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.3, June 2013, Rupam , Atul Verma , Ankita Singh
[4] V. Mishra and N. Verma, "Security againstPassword Sniffing using Database Triggers",International General of Research in AdventTechnologies, Vol. 2, March 2014.
[5] B. Singh Thakur and S. Chaudhary, "ContentSniffing Attack Detection in Client and Server Side:A Survey", International Journal of AdvancedComputer Research, Vol. 3, Issue 10, June 2013.
[6] S. I. A. Qadri and K. Pandey, "Tag Based ClientSide Detection of Content Sniffing Attack withFile", International Journal of Advanced ComputerResearch, Vol. 2, Issue 5, September 2012.
[7] S. Pandey and A. S. Chauhan, "Secure ContentSniffing for Web Browser: A Survey", InternationalJournal of Advanced Research in Computer andCommunication Engineering, Vol. 2, Issue 9,September 2013.
[8] A Literature Reviewon Sniffing Attacks in ComputerNetwork, International Journal of Advanced Engineering Research and Science (IJAERS) [Vol-1, Issue-2, July 2014], Anubhi Kulshrestha, Sanjay Kumar Dubey
[9]