**THE RISK OF SNIFFERS IN COMPUTER NETWORK**

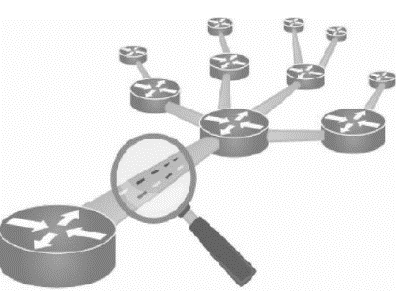
**Abstract :** Computer network continues to grow in size, complexity, and overall number of users

The volume of network traffic flowing through its nodes has increased dramatically with the development and popularization of network technology, network management and maintenance and monitoring it is important to keep the network smooth and improve the economic efficiency for this purpose the packet sniffer is used. Packet sniffing is important in network monitoring to troubleshoot and to log network. Used. Inhaling the packets is important in monitoring the network to discover network errors and record it .The Packet Sniffing Tool is useful in analyzing both wireless and wired network traffic . However, it may be used in illegal acts, such as exploiting network users and interfering with their sensitive information

***Keyword :*** *VPN , Packet, Sniffer, Protocol , Network .*

**1 . Introduction :**

Packet sniffer is a program running in a network attached Device that passively receives all data link layer frames passing through the device’s network adapter. It is also known as Network or Protocol Analyzer or Ethernet Sniffer. The packet sniffer captures the data that is addressed to other machines, saving it for later analysis. It can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic [1]. Network sniffers, aka protocol analyzers, are sold and distributed as tools that can be used to troubleshoot network communications by listening in on the conversations between computers on a network. These conversations consist of a number of packets that contain hardware addresses, IP addresses, application information and, in some cases, data that is being transferred between network computers. If used for troubleshooting, these tools are invaluable to the IT team. If used for less noble purposes, however, they become powerful eavesdropping tools that can, in some cases, cause major disruptions in network operations.



**2. Motives the attackers from sniffing:**

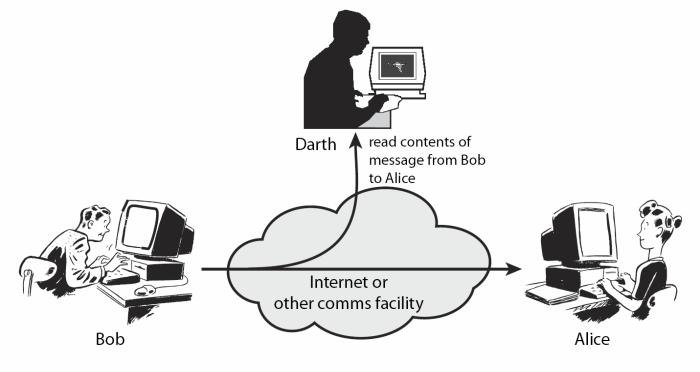
The illegal use of sniffers has its goals :

* Getting username an passwords
* Stealing bank related/transaction related information
* Spying on email and chat messages
* Identity theft

**3.Types of Sniffing**

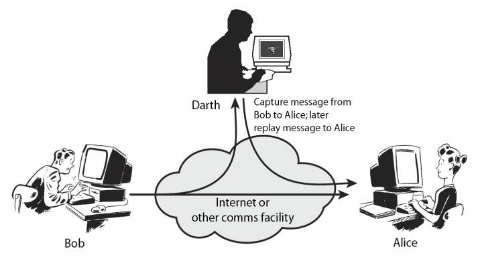
There are two types of sniffing- active and passive. As the name suggests, active involves some activity or interaction by the attacker in order to gain information. In passive the attacker is just hiding dormant and getting the information.

**Passive Sniffing:**

****

This is the process of sniffing through the hub. Any traffic that is passing through the non-switched or unbridged network segment can be seen by all machines on that segment. Sniffers operate at the data link layer of the network. Any data sent across the LAN is actually sent to each and every machine connected to the LAN. This is called passive since sniffers placed by the attackers passively wait for the data to be sent and capture them.

**Active Sniffing:**

****

In this sniffing type, attacker directly interacts with target machine by sending packets and receiving responses.

This sniffing is carried out through Switch. In this type, attacker tries to poison the switch by sending bogus MAC address.

**4. Protocols that are vulnerable to sniffing attacks**

* FTP
* TELNET
* HTTP
* POP
* SNMP

**5 .How a Packet Sniffer Works**

The packet sniffing process can be broken down into three steps: collection, conversion and

analysis [2].

Collection: The Packet sniffer switches the selected network interface into promotion mode. In

this mode, the network card can listen to all network traffics on its particular network segment

to capture the raw binary data from the wire.

Conversion: The captured binary data is converted into a readable form. This is where most of

the advanced command-line-driven packet sniffers stop. At this point, the network data is in a

form that can be interpreted only on a very basic level, leaving the majority of the analysis to

the end user.

Analysis: The packet sniffer takes the captured network data, verifies its protocol based on the

information extracted, and begins its analysis of the protocol’s specific features. Wireshark is

one of the most popular open-source packet analyzer. Originally named Ethereal, in May 2006

the project was named Wireshark due to trademark issue

**6 .Aims and objectives:**

How do you identify a Sniffer?

Identifying the type of sniffer can depend on how sophisticated the attack is. It is possible that the sniffer may go undetected for a large amount of time hiding in the network. There is some anti-sniffer software available in the market to catch the intruders but it may be possible that the sniffers get away with it creating a false sense of security. A sniffer can be software installed onto your system, a hardware device plugged in, sniffer at a DNS level or other network nodes etc. Practical networks are complex and so it becomes difficult to identify sniffers. Since identification is tough, we will be discussing ways to render the sniffed information useless to the attacker.

How does a person secure their data ?

If you are connected to a public network or an insecure network, you may be exposed to these attacks. One of the ways that preserves your privacy within the network is by using VPN ( Virtual Private Network (

**7 . CONCLUSIONS :**

Network security is a sine qua non for any organizational success, considering the value of data

and information transmitted via networks. The Intranet though secured and restricted to

authorized members of an enterprise that owns it is still prone to cyber attacks most times.

It is necessary to watch for new user accounts or high activity on a previously low usage

account, new files with novel or strange file names, accounting discrepancies, changes in file

lengths or dates, attempts to write to system, data modification or deletion, denial of service,

unexplained, poor system performance, anomalies, suspicious probes, suspicious browsing,

inability of a user to log in due to modifications of his/her account, etc.

This necessitates the need for some sniffing software to monitor the packets and activities in an

Intranet.

***REFERENCES :***

[1] Qadeer M.A., Zahid M., Iqbal A., Siddiqui M.R “Network Traffic Analysis and Intrusion Detection Using Packet Sniffer*” ICCSN ‘10 Second International Conference, 2010, Page(s): 313 - 317*

[2] Pallavi A., and Hemlata P. (2012). Network Traffic Analysis using Packet Sniffer. *International*

*Journal of Engineering Research And Applications, 2(3), 854-856*.

[ 3 ] https://www.greycampus.com/blog/information-security/what-is-a-sniffing-attack-and-how-can-you-defend-it