SSH over Telnet

Anjali Chava[1],Sravani Alwala[2]
[1]*CSE Dept.,STLW,Hyderabad, Telangana*
[2] *CSE Dept.,STLW,Hyderabad, Telangana*
[1]*anjupvc@gmail.com*
[2] *sravani.alwala15@gmail.com*

Abstract: In recent days most of the computing works rely on remote systems. There are many protocols to communicate with remote systems. But most of these protocols are found to be vulnerable. Telnet is famous protocol to remote communications. One of the biggest disadvantages of this protocol is all information even private information like passwords and usernames is in plain text. SSH overcomes this disadvantage. SSH uses encryption, which means data in secured format that is data is sent unique for sender and receiver.

I.INTRODUCTION

These days internet is very important for all kind of applications. Remote control of applications plays a prominent role. As minute data can be copied, transferred anywhere between remote. The internet as a medium for these works becomes very hazardous. Packet sniffing and session hijacking are the two dangerous attacks that found always vulnerable. Due to the easy availability of complicated tools, it is easy to perform these attacks. The objective of this paper is to show why SSH protocol is preferred to fix above stated dangerous attacks to Telnet protocol.

The paper is divided as follows: In section II, we discuss briefly about the packet sniffing. In section III we will get to know about how telnet protocol is dangerous remote access. In section IV we describe about how SSH differ with Telnet when used over "clear text" protocol and how SSH tunneling allows insecure communications to be used in a secure fashion. Later in section V, we end up with the conclusion, followed by a list of references.

II. PACKET SNIFFING

A sniffer [1] is an application that can capture network packets. Sniffers are called as network protocol analyzers. Packet sniffing is a network attack plan strategy that says about the process of capturing and diverting data when it flows across a network connection. A packet sniffer is a device that is used by network Administrators to analyze when transmitted over a network.

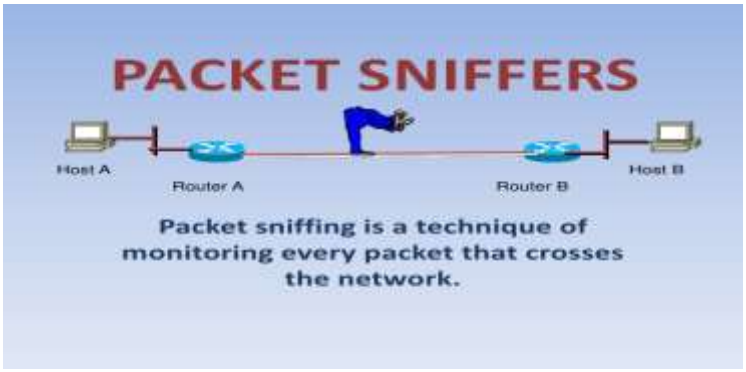

Fig 1: Shows how Packet sniffing is done

III. REASONS FOR NOT USING TELNET

The [3] Telnet protocol lands users in risks. The username, password etc. data are transmitted over the network without encryption. Most of information is sent via physical wire, such as in Ethernet. Most of computers are programmed to respond only to packets that are sent to them. But we can computers to capture all Information that is transmitted over a network irrespective of information that is intended for respective computer

Packet sniffing creates dangerous vulnerability through journey of packets from transmitter to receiver. In recent years, there have been many cases of ISP who have had a single computer on their internal network compromised; Every Telnet connection passing through that ISP had its password captured as a result.

Because of the dangers of password sniffing, and connection hijacking, the Telnet protocol should not be used for remote login for important works like banking works and personal business applications.

IV. SSH PROTOCOL

SSH protocol [2] is very good alternative for traditional protocols like telnet, which is least vulnerable when compared with it.

Advantage of SSH when used over "clear text" protocols: Figure 3 shows how easily a telnet session can be casually viewed by anyone on the network using a network-sniffing application such as Wireshark.

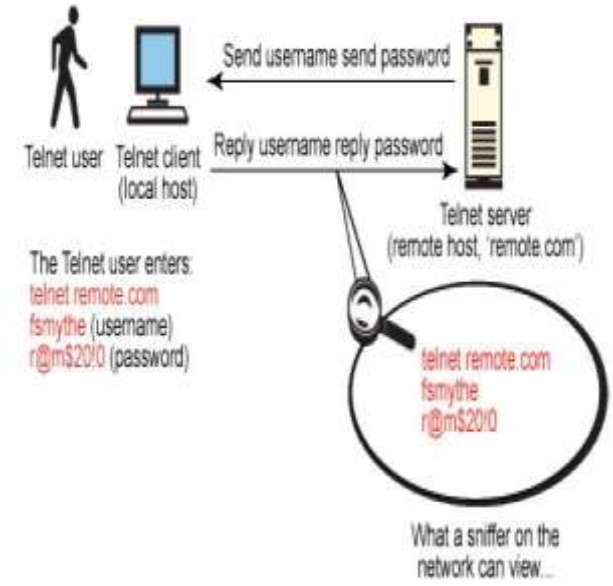

Fig 3: shows Telnet protocol sessions that don't have any kind of encryption

SSH provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server. The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet.

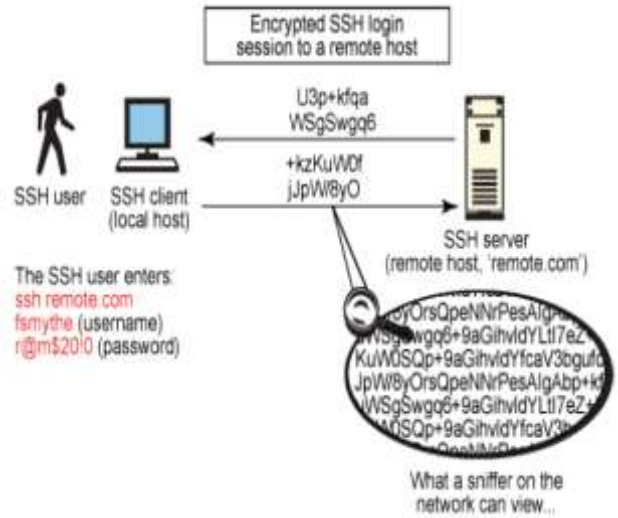

Fig4: SSH protocol sessions are encrypted

Figure 4 provides an overview of a typical SSH session and shows how the encrypted protocol cannot be viewed by any other user on the same network segment.

V.ADVANTAGES

SSH[4] offers encryption for data transfer that restricts hackers and attackers from hacking your server password and user information. Another benefit of using SSH is that it allows you to tunnel other network protocols. As an example, if you wish to transfer any files securely, you can utilize the SSH in order to encrypt the FTP transfers. This can be done with any type of connection, like VNC or Samba both are good for such tasks. With SSH you can manage your dedicated server remotely, monitor logs, install applications, start and stop services, and even manipulate databases. It recognizes normal Unix commands, and you can use it to login as root for full system administration.

VI.CONCLUSION

Effective data transmission with minimal security risks very much important in today's world of communication system. SSH protocol paves a way for this data transmission. In future[5] researches the open architecture of SSH provides considerable flexibility, allowing the use of SSH for a variety of purposes beyond a secure shell.

References

[1] Packet sniffing
https://www.ssh.com/ssh/protocol/
[2] A overview of SSH
https://www.vandyke.com/solutions/ssh_overview/ssh_overview.pdf
[3]An introduction to secure shell
https://www.giac.org/paper/gsec/710/introduction-ssh-secure-shell/101587
[4]Advantages of ssh
http://www.inmotionhosting.com/support/website/linux/ssh-advantages
[5]Authenticated encryption in SSH
https://cseweb.ucsd.edu/~mihir/papers/ssh.pdf

