\

Remote Connections

Submitted To:: Prof.Dr.Stefan Traub

Submitted By:: Rahul Tak

Table of Contents

Remote Connection in Linux

In the era of technology where most of servers for big companies are situated not only at one geographical location but they are all over the world. Different companies are operating from different parts of the world and on the basis of the geographical location is pretty difficult to maintain and have access to all the systems and servers available.
For solving this big problem of having remote access to the systems situated all over the world, developers of UNIX, LINUX and Windows developed a service called remote access which lets people connect to any system they want to the connect situated anywhere in the world.

Remote Access or Remote Connection basically means to connect to a server or a system from an remote location for eg. Through an remote access service (RAS) or virtual private network. So this basically very useful for the big company employers to work from home and connect to the system anywhere in the world.

For Eg: An employee of "XYZ" company from Germany wants to handle some situations of the systems in Brazil, from his current location he can access the system and solve the problem easily just by using the services provided such RAS, VPN, SSH, TELNET etc.

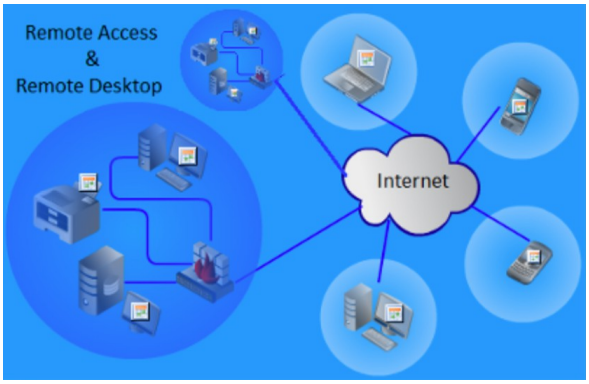

Figure.1

This figure explains the usage of the service that how exactly we can use it for our benefit based on the system in the world on the internet.

A remote access service is based on a client server connection prototype, it connects client to a host system, known as a remote access server. Using the service to use the system as remote control to use it as it was just in front of the person.

These are the steps involved in setting up a successful connection using RAS:

1. Person uses dial up connection at home into the office PC.
2. The responsibility of the office PC is to login into the file server where the required information is stored.
3. The remote PC in home takes the control over the PC in office, allowing the person to have access to all files and information, execute commands and exchange files.

There are many open source, first party, third party applications available in the market for using the above service known as Remote Desktop Services. For eg: TeamViewer, LogMeln etc. These are mainly used by the companies providing desktop troubleshooting services.

As we all know, the more technical we are getting we have pros and cons of every services being developed. If not secured enough these services are exploitable which can be used for ones benefit and could cause a very great loss to the big companies having "as they share confidential information over RAS or some other service".

To contradict this, developers have developed many protocols like VPN, SSH which makes all the data shared through internet or some other connection encrypted which makes it almost impossible for any hacker to decrypt it as it needs to have the correct key and algorithms for decrypting.

SSH → The Secure Shell

If we have many accounts like at home, at office etc and we want to connect everything together so we can have access to all the files and folders altogether, copying files between computers over a network, log into one account remotely from another, or transmit commands to a remote computer for execution. Many programs exist like ftp for file transfers, telnet for remote logins and rsh for remote execution of commands. But the problem with these programs is that they lack security and an intruder can intercept and read all the confidential data passed over these protocols. To overcome we can use encryption to encrypt our data, firewalls etc.

SSH, The Secure Shell, is a popular, powerful, software-based approach to network security. The data is automatically encrypted when sent over a network using SSH and as the data reaches its destination it again automatically be de-crypted. It uses very secure encryption algorithms.

SSH is not similar like UNIX Bourne Shell or C shell nor it is not a command interpreter. Rather, it creates a channel for running a shell on a remote computer, with end-to-end encryption between the two systems. It is a protocol which ensures authentication, encryption and integrity of data transmitted over a network.

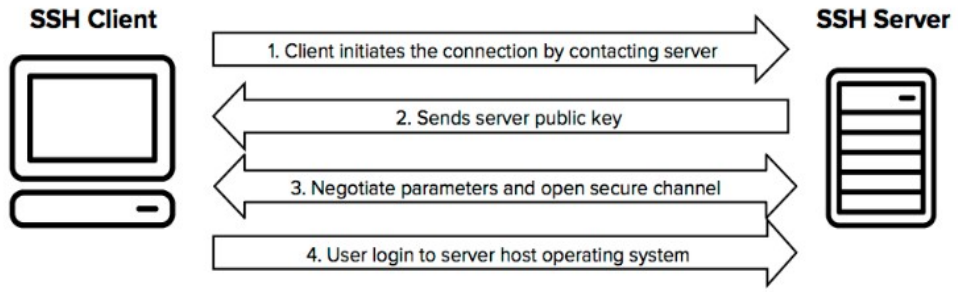

Figure.3

This figure explains the authentication process of SSH between the two host acting one as a client and other as a server.

In the following we are going to connect to a server remotely.

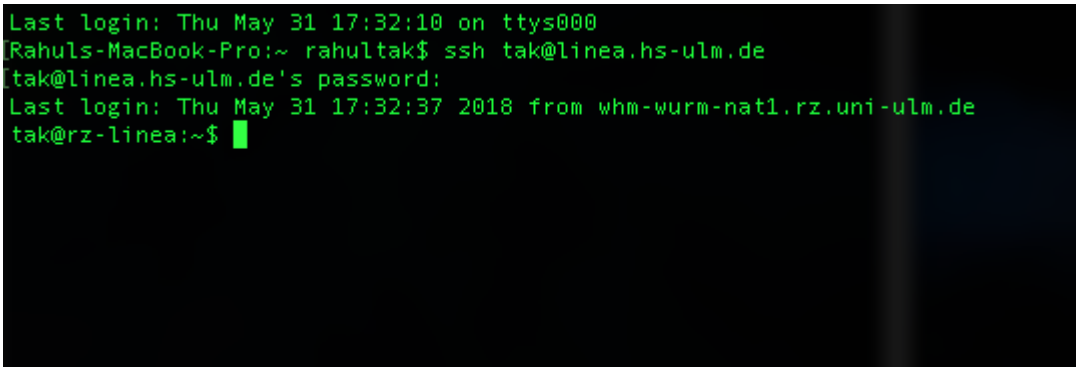

Figure.4

To connect to a server the syntax “ssh username@domain.com/ip” then enter the related password and after the authentication is done we have a remote access to the system.

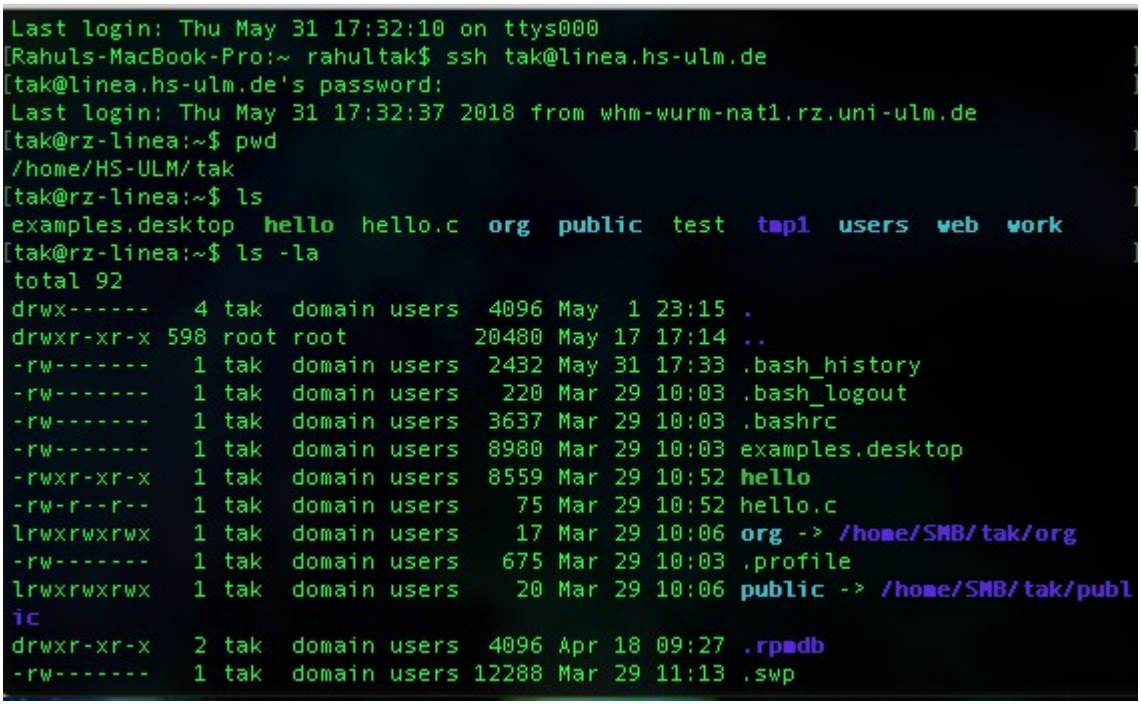

Figure.5

Now, we can execute commands, copy files, remove etc as like the system was in front of us and securely. It replaces securely other protocols like ftp, telnet, rsh which are vulnerable to attacks.

SSH is also not a complete security solution – but then nothing is!. It cannot stop intruders to have active break in attempts or Denial of service attacks and also it wont eliminate other hazards like viruses, backdoors, trojan etc. It does provide robust and user-friendly encryption and authentication.

To have a secure remote access, it is very recommendable to use SSH with an VPN- Virtual Private Network connection, which makes the network connection more secure and hard for intruders to get in.

VPN → Virtual Private Network

VPN which is Virtual Private network is a technology to connect to a private network through a public network from anywhere in the world for eg internet. In simple words, connecting through by using a public wifi network to a system on the office. Sending and receiving data from a public network and using functionality, security and management of the private network.

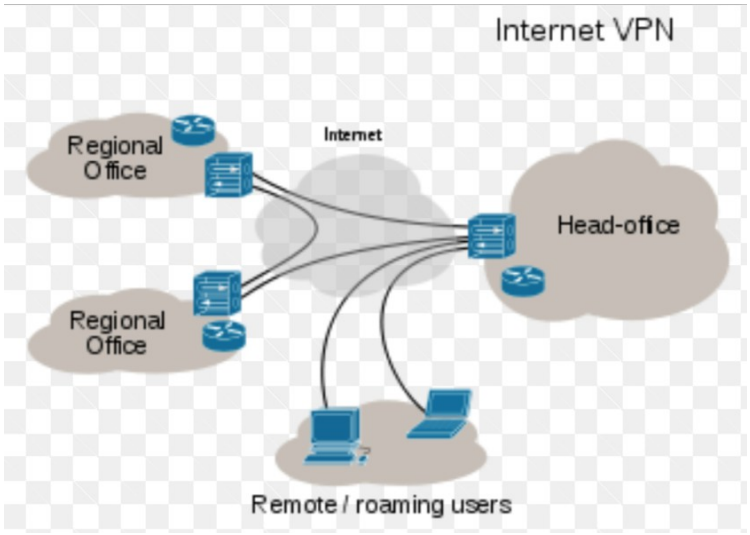

Figure.2

It is a way to simulate a private network over a public network such as internet. The reason of the term "virtual" as because it depends on the use of virtual connections, that means the connections are temporary and they have no physical presence, but it consists of packets routed over various machines on the internet on an ad-hoc basis.

Uses of VPN ::

1. Hiding your browsing activity from your local network and ISP.
2. To access websites which are regionally blocked.
3. Bypassing Internet censorship.
4. Accessing office network while traveling.
5. Accessing home network while traveling.
6. Downloading files from the internet in case your ISP doesn't allow it.

Many VPN products are available on the market like OpenVPN which is free of cost, then they have ExpressVPN, StrongVPN etc for these commercial products you have to pay a subscription fees.