What is ssh? essay sample

Sociology, Communication

SSH is a Secure Shell that uses a secure encrypted communication protocol designed to replace older insecure protocols like telnet, rsh, and ftp. SSH authentication is done with a username and password combination, which is the default. This is the most simplistic usage we will see. $ ssh

SSH comes with all Linux distributions as well as other Unix variants. SSH is not a complete security solution and it will not protect against trojans, viruses, etc. Why would you want to replace telnet and remote login with SSH? SSH (Secure Shell) is a protocol that can be used to log into a remote machine and provide secure encrypted communications between the Virtual Server and the local computer. The communication is made via encrypted channels. Telnet on the other hand communicates without any encryption, allowing a sniffer to capture information, e. g. user names and passwords. This is why SSH is preferred over Telnet.

SSH uses a public and private key on each system. The private key is the one which you should never give away access to and the public key is the one which you will put on other machines you want to log into. For any given public key, only one possible private key can be its’ other half. The first time a user uses SSH to connect to a remote system, their SSH client program exchanges the public keys, unless keys have been exchanged manually. If keys are exchanged over the network during the first connection, the user essentially trusts the security of the network during the key exchange. On subsequent connections to the same system, the SSH program will check that the keys haven’t changed to ensure that it is still the same system. This is an example of a Telnet unencrypted client-server session:

This is an example of an encrypted SSH client-server session:

How is SSH configured on a Linux computer?

To configure SSH on a Linux computer you need to open ssh server to install it to first work on SSH. Please note that the installation process may be different for different distributions. Open terminal and become root by: su –

For Debian based distributions like Ubuntu/Debian: apt-get install openssh-server For RPM based distributions like openSUSE: zipper install openssh-server Now you need to start the SSH server: /etc/init. d/ssh start

The above command also needs root privileges to run it after installation of the SSH server. Now we need to perform some security measures to avoid security risks. To do those go to sshd-config file and edit these things:
Vim/etc/ssh/sshd-configure

Some things need to be changed for security reasons:
Search for ‘ PermitRootLogin’ without quotes and changes yes to no like this:
From,
PermitRootLogin yes
To,
PermitRootLogin no

This is because we don’t need root user to access the server and most of the attackers use root as userid to hack the server. By adding this to the security measures, you shut down another way for the attackers to get access to your system.

Now you should change the port from the default of 22 to a higher number. This can be anything you have in mind but it should not be easy to guess. Search for the ‘ Port’ keyword and change the number to any number like 5, 000, which is the maximum number. There are a lot of people who will sniff for the default ports in the lower range and then will try different algorithms to log in using lists of different user names.

For port changing you will need to make some changes in the router to allow different ports access from external connections to your server. Sometimes it needs to be changed and sometimes it doesn’t, it just depends on how your router is configured.

For the last and more important one, search for this word at the end of the file ‘ AllowUsers’ without the quotes. If this is not there you can add it to the end of the file. AllowUsers jelly bobwill arif

In the above line, three users will be able to access the machine; you can add more users if you need to by separating each name with a space. This will provide more security to just check for the user names specified here, other user names will be ignored including root.

Although there are more security measures, these will make sure that your server is safe from attackers so they cannot get access to it.
Now it is time to restart the SSH server. To do this enter the following command: /etc/init. d/ssh restart

If you want to stop the server, the command is:
/etc/init. d/ssh stop

The installation and configuration of SSH is now complete. You should now be able to login to your server through SSH from remote machines.

References

Krenz, M. (2006). SSH Tutorial for Linux. Retrieved February 28, 2013 from http://support. suso. com/supki/SSH_Tutorial_for_Linux