SSH Theory Session

==========

SSH Server and SSH Client

[Secure Shell]

==========

Machine <== Operating System <== User Create <== TASK Perform <== Login <== Local to local <== username + password <== Enter

Types of login method ?

1- Local to local ==> Username + password
2- Remote Login ==> username + Password + IP address of server machine + Client software[Remote session]
1- ssh 2- putty 3- Other tools as well
[xyz.pem OR public key]
==========1- password based [default method] 2- key based
==========
ssh root@192.168.0.100
==========

Package ==> openssh-server ==> server machine ==> sshd [service name]
package ==> openssh-clients ==> ssh ==> command ==> linux based flavor
==> putty OR Other tools as well [Windows machine]

==========
SSH Service ==> Required package ==> mandatory ==> during the OS installation automatically

1- Service ==> running
2- port number ==> open OR on

==========
SSH ===> sshd ==> 110047 ===> 22
FTP ===> vsftpd ==> 23232 ===> 21
Utility ===> Daemon/unit/Service ==> # pidof sshd [Examples of PID this can be anything] ===> Port number

==========

1- using any command ==> command based execution permissions

2- data management ==> file and directory based permissions

==========
==========

1- SSH Services always use for remote login from one machine to another machine.

2- SSH services support on both types of environment LAN and WAN.

3- In client side we can have any operating system to make connection with the server machine.

4- SSH basically is an advance concept of telnet service.

5- SSH is much secure service as compare to telnet because in SSH all information
always transfer in encrypted format but in telnet it was in plain text concept.

==========
==========

SSH
Openssh

IMPORTANT Points About SSH Service

1- SSH stand for Secure Shell.
2- SSH is a network protocol for secure data communication.
3- SSH protocol allows remote command line login.
4- SSH protocol enables remote command execution.
5- To use SSH you need to deploy SSH Server and SSH Client program respectively.
6- Telnet, rlogin, and ftp transmit unencrypted data over internet.
7- OpenSSH encrypt data before sending it over insecure network like internet.
8- OpenSSH effectively eliminate eavesdropping, connection hijacking, and other attacks.
9- OpenSSH provides secure tunneling and several authentication methods.
10- OpenSSH replace Telnet and rlogin with SSH, rcp with scp, ftp with sftp.

==========
==========
Server Side ?

Package ==> openssh-server
Daemon or service or unit ==> sshd
Port Number ==> 22 (by default port number)
Configuration File ==> /etc/ssh/sshd_config
Log File ==> /var/log/secure

==========
Client Side ?

Linux Based ==> openssh-clients [already installed during the OS installation time]
or
ssh username@serverip

Windows based ==> putty.exe OR other tools [need to install manually]

==========

Note:- Both machines must be in network

==========