CONFIGURING AND SECURING SSH

➔**Package - openssh**

➔ **Service - sshd**

➔ **Daemon - sshd**

➔ **Port no - 22**

➔ **Script file - /etc/init.d/sshd**

➔ **Main conf file - /etc/ssh/sshd_config**

The SSH protocol enables systems to communicate in an encrypted and secure fashion over an insecure network.

- ⇨ We can use ssh command to create a secure connection to a remote system , authenticate as a specific user, and we can access interactive shell session as that user
- ⇨ We can run some commands also in remote systems
- ⇨ Syntax of ssh is

#ssh user@host/ip command

#exit or ctrl+d

When a user do ssh to a server it check if it has a copy of that public key in that user in ***~/.ssh/known_hosts***

This is configured in ***/etc/ssh/ssh_known_hosts***

CONFIGURING SSH KEY-BASED AUTHENTICATION

We can configure an SSH server to allow you to authenticate without a password by using key based authentication. This is based on a private-public key scheme.

Here we can have one private key and public key.

Where private key is for private propose and we need to share a public key for authenticate

#ssh-keygen (to create keys)

Default location for keys is ***~/.ssh/***

For sharing a key we use

#ssh-copy-id - i key_path user@remotehost

Using ssh-agent for Non-interactive Authentication

If your SSH private key is protected with a passphrase, you normally have to enter the passphrase to use the private key for authentication.
However, you can use a program called ssh-agent to temporarily cache the passphrase in memory.
If you log in on a text console, log in using ssh, or use sudo or su, you will probably need to start ssh-agent manually for that session. You can do this with the following command:

```
[user@host ~]$ eval $(ssh-agent)
```

Once ssh-agent is running, you need to tell it the passphrase for your private key or keys. You can do this with the ssh-add command.

```
[user@host ~]$ ssh-add Identity added: /home/user/.ssh/id_rsa
(user@host.lab.example.com) [user@host ~]$ ssh-add .ssh/key-with-pass
Enter passphrase for .ssh/key-with-pass: redhatpass
Identity added: .ssh/key-with-pass (user@host.lab.example.com)
```

After successfully adding the private keys to the ssh-agent process, you can invoke an SSH connection using the ssh command. If you are using any private key file other than the default /home/user/.ssh/id_rsa file, then you must use the -i option with the ssh command to specify the path to the private key file.

```
$ssh -i .ssh/pass-ky user@host
```

CONFIGURING THE OPENSSH SERVER

The daemon for ssh is sshd

Conf file for it ***/etc/ssh/sshd_config***

- ⇨ PermitRootLogin yes/no
- ⇨ PasswordAuthentication yes/no