Red Hat System Administration I

UNIT 9

Configuring and Securing OpenSSH Service

Objectives

- Log into a remote system using ssh to run commands from a shell prompt.
- Set up ssh to allow secure password-free logins by using a private authentication key file.
- Customize sshd configuration to restrict direct logins as root or to disable password-based authentication.

What is the OpenSSH secure shell (SSH)?

- The term OpenSSH refers to the software implementation of the Secure Shell software used in the system. The OpenSSH Secure Shell, ssh, is used to securely run a shell on a remote system. If you have a user account on a remote Linux system providing SSH services, ssh is the command normally used to remotely log into that system. Thessh command can also be used to run an individual command on a remote system.

Secure Shell examples

- **ssh command**

```
[student@host ~]$ ssh remotehost
student@remotehost's password:
[student@remotehost ~]$ exit
Connection to remotehost closed.
```

```
[student@host ~]$ ssh remoteuser@remotehost
remoteuser@remotehost's password:
```

```
[student@host ~]$ ssh remoteuser@remotehost hostname
remoteuser@remotehost's password:
remotehost.example.com
```

SSH host keys

- ~/.ssh/known_hosts

```
$ cat ~/.ssh/known_hosts
remotehost,192.168.0.101 ssh-rsa AAAAB3Nzac
$ ls /etc/ssh/*key*
ssh_host_dsa_key ssh_host_key ssh_host_rsa_key
ssh_host_dsa_key.pub ssh_host_key.pub ssh_host_rsa_key.pub
```

SSH key-based authentication

- **ssh-keygen**

```
[student@desktopX ~]$ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa): Enter
Created directory '/home/student/.ssh'.
Enter passphrase (empty for no passphrase): redhat
Enter same passphrase again: redhat
Your identification has been saved in /home/student/.ssh/id_rsa.
Your public key has been saved in /home/student/.ssh/id_rsa.pub.
The key fingerprint is:
a4:49:cf:fb:ac:ab:c8:ce:45:33:f2:ad:69:7b:d2:5a
student@desktopX.example.com
The key's randomart image is:
... ...
```

Using SSH Key-based Authentication

- ssh-keygen
- ssh-copy-id serverX
- ssh serverX 'hostname'

Customizing SSH Service Configuration

- /etc/ssh/sshd_config
- PermitRootLogin no|yes|without-password
- PasswordAuthentication yes|no
- systemctl restart sshd.service

Lab

Run lab ssh setup as the student user on both desktopX and serverX. This will create a user account calledvisitor with a password of password.

<lab 1>
Generate SSH keys on desktopX for user visitor and copy the public key to the visitor account on serverX.
<lab 2>
Disable ssh login for the root user and passowrd-based SSH authentication on serverx
<lab 3>
Verify that user root is not allowed to login to serverx by useing ssh, while user visitor user is with the private key.

That's all