15.4. Configure the `/etc/ssh/sshd_config` file

The `/etc/ssh/sshd_config` file is the system-wide configuration file for OpenSSH which allows you to set options that modify the operation of the daemon. This file contains keyword-value pairs, one per line, with keywords being case insensitive. Here are the most important keywords to configure your sshd for top security; a complete listing and/or special requirements are available in the man page for sshd(8).

Edit the `sshd_config` file, vi `/etc/ssh/sshd_config` and add/or change, if necessary, the following parameters:

```
# This is ssh server systemwide configuration file.

Port 22
ListenAddress 192.168.1.1
HostKey /etc/ssh/ssh_host_key
ServerKeyBits 1024
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin no
IgnoreRhosts yes
IgnoreUserKnownHosts yes
StrictModes yes
X11Forwarding no
PrintMotd yes
SyslogFacility AUTH
LogLevel INFO
RhostsAuthentication no
RhostsRSAAuthentication no
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords no
AllowUsers admin
```

This tells sshd_config file to set itself up for this particular configuration setup with:

`Port 22`

> The option `Port` specifies on which port number ssh daemon listens for incoming connections. The default port is 22.

`ListenAddress 192.168.1.1`

> The option `ListenAddress` specifies the IP address of the interface network on which the ssh daemon server socket is bind. The default is `0.0.0.0`; to improve security you may specify only the required ones to limit possible addresses.

`HostKey /etc/ssh/ssh_host_key`

The option `HostKey` specifies the location containing the private host key.

`ServerKeyBits 1024`

The option `ServerKeyBits` specifies how many bits to use in the server key. These bits are used when the daemon starts to generate its RSA key.

`LoginGraceTime 600`

The option `LoginGraceTime` specifies how long in seconds after a connection request the server will wait before disconnecting if the user has not successfully logged in.

`KeyRegenerationInterval 3600`

The option `KeyRegenerationInterval` specifies how long in seconds the server should wait before automatically regenerated its key. This is a security feature to prevent decrypting captured sessions.

`PermitRootLogin no`

The option `PermitRootLogin` specifies whether root can log in using ssh. Never say `yes` to this option.

`IgnoreRhosts yes`

The option `IgnoreRhosts` specifies whether rhosts or shosts files should not be used in authentication. For security reasons it is *recommended to no use rhosts or shosts files for authentication*.

`IgnoreUserKnownHosts yes`

The option `IgnoreUserKnownHosts` specifies whether the ssh daemon should ignore the user's `$HOME/.ssh/known_hosts` during RhostsRSAAuthentication.

`StrictModes yes`

The option `StrictModes` specifies whether ssh should check user's permissions in their home directory and rhosts files before accepting login. This option must always be set to **`yes`** because sometimes users may accidentally leave their directory or files world-writable.

`X11Forwarding no`

The option `X11Forwarding` specifies whether `X11` forwarding should be enabled or not on this server. Since we setup a server without GUI installed on it, we can safely turn this option off.

`PrintMotd yes`

The option `PrintMotd` specifies whether the ssh daemon should print the contents of the `/etc/motd` file when a user logs in interactively. The `/etc/motd` file is also known as the *message of the day*.

`SyslogFacility AUTH`

The option `SyslogFacility` specifies the facility code used when logging messages from sshd. The facility specifies the subsystem that produced the message--in our case, AUTH.

`LogLevel INFO`

The option `LogLevel` specifies the level that is used when logging messages from sshd. INFO is a good choice. See the man page for sshd for more information on other possibilities.

`RhostsAuthentication no`

The option `RhostsAuthentication` specifies whether sshd can try to use rhosts based authentication. Because rhosts authentication is insecure you shouldn't use this option.

`RhostsRSAAuthentication no`

The option `RhostsRSAAuthentication` specifies whether to try rhosts authentication in concert with RSA host authentication.

`RSAAuthentication yes`

The option `RSAAuthentication` specifies whether to try RSA authentication. This option must be set to **`yes`** for better security in your sessions. RSA use public and private key pairs created with the ssh-keygen1utility for authentication purposes.

`PasswordAuthentication yes`

The option `PasswordAuthentication` specifies whether we should use password-based authentication. For strong security, this option must always be set to **`yes`**.

`PermitEmptyPasswords no`

The option `PermitEmptyPasswords` specifies whether the server allows logging in to accounts with a null password. If you intend to use the scp utility to make automatic backups over the network, you must set this option to **`yes`**.

`AllowUsers admin`

The option `AllowUsers` specifies and controls which users can access ssh services. Multiple users can be specified, separated by spaces.

Prev Home Next
Configure the `/etc/ssh/ssh_config file` Up Configure OpenSSH to use TCP-Wrappers/inetd super server