Few sshd server Security Tips that will improve your server security

Author : admin

On each and every newly installed Linux or FreeBSD server. I'm always very cautious about three configuration directives for the ssh server.
This are **X11Forwarding , Protocol and PermitRootLogin**

One needs to be very watchful about this three ones, as tuning the right values surely prevents the server from many of the security issues that might rise up with the SSH server.

Many Linuxes like Debian and Ubuntu comes with **X11Forwarding yes** e.g. (X11Forwarding) enabled by default, this is an useless option in most of the cases as the servers I do administrate does not run a X environment.

Some older Linux distributions I have dealt with has the ssh **Protocol 1** enabled by default and therefore, whether I do inherit an old server I have to start administrating the first thing I do is to check if the **/etc/ssh/sshd_config**'s **Protocol 1** option is enabled and if it is enabled I disable it.

PermitRootLogin is also an option which I often turn off as logging in via remote ssh is potentially dangerous as root password might get sniffed.

In overall the 3 sshd option's I do check out in **/etc/sshd/sshd_config** on each newly installed Linux server are:

X11Forwarding yes
PermitRootLogin yes
Protocol 1

I always change this three options in my **/etc/sshd/sshd_config**
to:

X11Forwarding no
PermitRootLogin no
Protocol 2

One other options sshd server options which is good to be tuned is:

LoginGraceTime 120

Decreasing it to:

LoginGraceTime 60

is generally a good idea.

Of course after the changes I do restart the ssh daemon in order for the new configuration to take place:

linux:~# /etc/init.d/sshd restart
...