

Make Basic Steps in Securing your Server

Sheetal Joseph

June 21, 2005

Having complete control over SSH access is the first step we could take to secure our box from intruders! There are many steps we could take to secure SSH access. To list a few:

1. Modify `sshd` so as to
 - (a) Restrict SSH access by binding `sshd` to a single IP that is different than the main IP of the server
 - (b) Change the SSH port to a different port than port 22.
 - (c) Disable direct Root Login
2. Disable telnet
3. Set up the server to e-mail you everytime someone logs in as root.
4. Set an SSH Legal Message

1 Modifying `sshd`

To do the above all you need to do is modify the `/etc/ssh/sshd_config` to suit your needs. Here is how you can do it:

1. SSH into server and login as root.
2. At the command prompt type : `vi /etc/ssh/sshd_config`
3. Go to the section of the file that looks like : Code:

```
#Port 22
#Protocol 2, 1
#ListenAddress 0.0.0.0
#ListenAddress ::
```

- (a) Uncomment and change

```
#Port 22
```

to the port number of your choice. Remember 49151 is the highest port number

- (b) Uncomment and change

```
#Protocol 2, 1
```

to look like

```
Protocol 2
```

- (c) Uncomment and change

```
#ListenAddress 0.0.0.0
```

to look like

```
ListenAddress 123.123.123.15 (use one of your own IP Addresses that has been assigned to your s
```

4. To disable direct Root Login, scroll down until you find

```
#PermitRootLogin yes
```

and uncomment it and make it look like

```
PermitRootLogin no
```

5. Save and exit.

6. Restart SSH

```
/etc/rc.d/init.d/sshd restart
```

7. Login to SSH in a new terminal with the new IP, port, user etc. If you face any issues, you can always go back to your open terminal and fix it.

2 Disabling Telnet

You should also disable Telnet access as it is very insecure. To disable telnet,

1. SSH into server and login as root.
2. At command prompt type: `vi /etc/xinetd.d/telnet`
3. Change `disable = no` to `disable = yes`
4. Save and Exit
5. At command prompt type: `/etc/init.d/xinetd restart`

3 Root login Alert

You could also set up the server to e-mail you everytime someone logs in as root. To have the server e-mail you everytime someone logs in as root:

1. SSH into server and login as root.

2. At command prompt type: `vi .bash_profile`
3. Scroll down to the end of the file and add the following line:

```
echo 'ALERT - Root Shell Access on:' `date` `who` | mail -s "Alert: Root Access from  
`who` | awk '{print $6}'" you@email.com
```

4. Save and exit.

4 Setting up an SSH Legal Message

You can also set an SSH Legal Message To set up an SSH legal message:

1. SSH into server and login as root.
2. At command prompt type: `vi /etc/motd`
3. Enter your message, save and exit. Note: I use the following message...

```
This computer system is for authorized users only. All activity is logged and regularly  
checked by systems personnel. Individuals using this system without authority or in  
excess of their authority are subject to having all their services revoked.
```

```
Any illegal services run by user or attempts to take down this server or its services  
will be reported to local law enforcement, and said user will be punished to the full  
extent of the law.
```

```
Additionally, IRC (or Related Software), bnc, ptlink, PsyBNC, eggdrop, BitchX, or any  
related application may NOT be used or stored (Compressed or Otherwise) on this  
Server. Failure to comply will result in immediate account termination.
```

```
SPAMMING OR MASS-MAILING OF ANY KIND WILL BE GROUNDS FOR IMMEDIATE ACCOUNT TERMINATION  
WITHOUT THE POSSIBILITY OF REACTIVATION OR REFUNDS OF SERVICES PAID.
```

```
Anyone using this system consents to these terms.
```