

Forum:[Hack Forums](#)

Thread: [How to Secure a Server / VPS | Beginner Friendly](#)

Cryptic™ - March 1, 2016, 3:43 pm

Most people that buy VPSs here have little to no knowledge of basic server security.

Here are some good things you should do to your server as soon as you get it.

This guide will give tell you about the things I do when I get my first get my servers.

Note: This thread is based on the Centos 6 operating system, if you use Centos 7 or another variant of Linux like Ubuntu / Debian some commands may be slightly different.

Like in centos we use yum whereas in Debian/Ubuntu you would use apt-get I will try my best to include commands for both.

Change the root password

Code passwd

I always use a 20-25 character long password, which consists of Uppercase and Lowercase Letters
Numbers
Symbols

A good site to use is <https://strongpasswordgenerator.com/>

It'll spit out passwords like "t~4=&':71\$_}@8(ZQ)@Q" which is exactly what you want.

Update your system

You should always update your system to have the latest versions of everything installed to ensure any vulnerabilities found in the OS have been patched.

Centos:

Code yum update -y

Debian/Ubuntu:

Code apt-get update -y

and apt-get upgrade -y

Install Fail2Ban

Fail2Ban is a nifty tool to have installed, which blocks malicious users/bots from bruteforcing your VPS.

Centos

Code yum install fail2ban -y

If you get an error saying it's not found or something, click [here](#)

Debian/Ubuntu

Code apt-get install fail2ban -y

The default config works fine but you can tweak it, just google it.

Important Links:

<https://www.digitalocean.com/community/tutorials/how-to-protect-ssh-with-fail2ban-on-centos-6>

<https://www.digitalocean.com/community/tutorials/how-to-protect-ssh-with-fail2ban-on-ubuntu-14-04>

Add a non-root user

Having root be able to login remotely is a huge security risk. It's the most targetted account. If you get root of a server, your like the god of the server. You have FULL ACCESS to EVERYTHING.

Code `useradd usernamehere`
`passwd usernamehere`

For the password, use a secure password just like you did for root at the beginning of this guide.

Next we have to give this non-root user permissions.

Run the command `Code visudo`

It will open up a file, scroll down till you see

Quote: `root ALL=(ALL:ALL) ALL`

Right below it add

Code `TheUsernameYouCreatedHere ALL=(ALL:ALL) ALL`

Save the file.

Setup SSH Keys!

I cringe every-time I see an HF user hosting something on a VPS that allows remote root logins and do not use SSH Keys and thinking their secure password 'imAl33tHax4or' is going to protect them.

I'm a Mac/Linux user so I simply go to terminal on MY machine and run the command.

Code `ssh-keygen -t rsa`

If you use Windows, Putty or any other SSH client has an option to generate SSH keys.

This generates an SSH Key which looks similar to this

Quote: The key fingerprint is:

`4a:dd:0a:c6:35:4e:3f:ed:27:38:8c:74:44:4d:93:67 demo@a`

The key's randomart image is:

`+-[ RSA 2048]-----+`

```
|      .oo.  |
|      . o.E |
|      + . o  |
|      . = .  |
|      = S = . |
|      o + = + |
|      . o + o . |
|      . o    |
|              |
```

`+-----+`

I then copy the Public SSH key onto the server by running the command

Code `ssh-copy-id user@123.45.56.78`

Note: user is the new user account we created a few steps ago. DO NOT USE ROOT

If you use Windows you can use an FTP client to place the public key you generated on your machine into the /user/home/.ssh folder on your server.

Important Link(s): <https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys--2>

Disable Root Login and Password Based Authentication

SSH server settings are stored in the /etc/ssh/sshd_config file. To disable root logins open up the file by running

Code nano etc/ssh/sshd_config

If you do not have nano installed you can use vi or just install it by running Code yum install nano -y
Set PermitRootLogin to no.

Also, disable password based authentication completely. To do so
Set PasswordAuthentication to no.

Save the file and then run the following command

Code service sshd restart

That is pretty much it. There are steps you can take to further secure your box, such as locking the root account (command passwd -l root)

I may post a more in-depth/advanced tutorial in the future, but I feel that this guide should put you in a good place.

If you have any questions, just post below.

BooGod - March 1, 2016, 3:54 pm

Nice guide, I knew you would do something good from it.

Cryptic™ - March 1, 2016, 3:57 pm

(Mar 1, 2016 04:54 PM)BooGod Wrote: [\[CITE\]](#) Nice guide, I knew you would do something good from it.

After I saw how insecure [Elfonzo](#)'s server's were. I searched if there were any decent server security guides on HF, and there weren't any.

So I figured I'd write one up.

Cryptic™ - March 1, 2016, 5:01 pm

Updated the guide with a tip on locking the root account.

Only run passwd -l root if you added your other account to the sudoers file by running visudo as shown in Step 4.

Or else you'll be permanently locked out of your server and will need a reinstall.

AdderallXR - March 1, 2016, 6:41 pm

thanks for this going try it out now <3

?Citizen Z / Napalm - March 1, 2016, 11:59 pm

(Mar 1, 2016 04:57 PM)Cryptic™ Wrote: [\[CITE\]](#) After I saw how insecure [Elfonzo](#)'s server's were. I searched if there were any decent server security guides on HF, and there weren't any.

So I figured I'd write one up.

Whats really funny is that i linked it to Elfonzo because i was helping him with something.

BooGod - March 2, 2016, 3:47 am

(Mar 1, 2016 04:57 PM)Cryptic™ Wrote: [\[CITE\]](#) After I saw how insecure [Elfonzo](#)'s server's were. I searched if there were any decent server security guides on HF, and there weren't any.

So I figured I'd write one up.

I know, that's what I am talking about his ProtonPay.com site.

Raaz - March 2, 2016, 3:58 am

Nice guide mate, waiting for the more advance version.

Freebooter - March 2, 2016, 5:29 pm

Nice one Cryptic™ very nice tutorial if i can i will give you +3 rep hold on i can do this i'm on it!

Emoticon - March 2, 2016, 8:26 pm

And if you want to be even more of a perfectionist, have openssh listen on 127.0.0.1 only and connect through a tor hidden service exclusively

That's what I do with things I give a shit about. Other than that I just set user:pass to root:fuck

Doctor Blue - March 3, 2016, 7:23 am

I have my servers configured to require double authentication if I'm not at home. If I'm at home, I just need my SSH key, otherwise I also have to plug in my Yubikey.

Some other good points to include is drop-by-default firewall rules, making sure services like MySQL only listen on loopback, only allowing SFTP or FTPS and maybe in the long run, how to use SELinux.

I have most of this configuration in a bash script, so when I get a new server I just run it and it will save my public keys, fix up the firewall rules and add a cron to update software automatically.

I don't personally use fail2ban because good luck bruteforcing a combination of 4096 bit keys along with a one time password. I do use it on my mail server, though.

"If you get root of a server, your like the god of the server."

You're*

EDIT: Yes I'm a bit paranoid.

blusmurf - March 3, 2016, 7:43 am

1.Disable any unused service. Especially old service like xinetd.

2.Use iptables or ufw to restrict listening port. Only open necessary ports and know your running services.

3. Do not use FTP. Use SFTP instead.

4. This may be obscurity over security = Change SSH listening port from 22 to another port (example: 2222) - But it won't survive portscan/nmap though, it's just you can defeat first wave of attack from script kiddies.

5. Install Intrusion Detecting System like Tripwire may help.

ra1d - March 3, 2016, 1:36 pm

Awesome guide, I personally use almost all of those security measures.
Only recently started messing around with linux servers.

wander is a multi dwc - March 3, 2016, 10:51 pm

I'd say that changing the SSH port is a fundamental step in securing a server.

Along with that, it would be helpful to some users if you could explain a bit more about how sudo works.

Also, found an error. In the last part, it's /etc/ssh/sshd_config, not etc/ssh/sshd_config

Cryptic™ - March 4, 2016, 8:27 am

(Mar 3, 2016 11:51 PM)Queenie Wrote: [\[CITE\]](#) I'd say that changing the SSH port is a fundamental step in securing a server.

Along with that, it would be helpful to some users if you could explain a bit more about how sudo works.

Also, found an error. In the last part, it's /etc/ssh/sshd_config, not etc/ssh/sshd_config
You can change the lock on the door, but the door can still be broken into if your lock lacks reinforcement.

Changing SSH port will mitigate some attacks, meaning most bots that will try to get into your box will give up, but if someone was serious about it they could always run a port scan and then find your SSH port.

SirNoobHack - March 4, 2016, 11:41 am

This guy helped to stop a bruteforce attack on my server. Very HQ tutorial. Thanks.

wander is a multi dwc - March 4, 2016, 5:57 pm

(Mar 4, 2016 09:27 AM)Cryptic™ Wrote: [\[CITE\]](#) You can change the lock on the door, but the door can still be broken into if your lock lacks reinforcement.

Changing SSH port will mitigate some attacks, meaning most bots that will try to get into your box will give up, but if someone was serious about it they could always run a port scan and then find your SSH port.

It's always a start to something..