

Forum:[Hack Forums](#)

Thread: [SSH Encryption Keys](#)

Consulting Detective - January 2, 2017, 11:36 pm

Hi guys. I just started learning linux command line. I already know how to navigate directories, copy/delete/move files, mysql, drive mounting, sysctl, kernel modules and some other fun stuff.

But for some reason I'm stuck with SSH. I can't get my head around it. I can establish SSH connections between a server and a client. Sad part is when it comes to implementing additional securities like RSA, I'm totally lost. I don't understand the concept of private keys and public keys.

I already looked up youtube, google and other online resources. They say different things, and give out different shell commands.

I was wondering if you guys can help me with this. Or point me to an easy to understand guide. I want to fully grasp this subject before I move on to the next thing I wanna study.

Anyways, thanks in advance. :)

Consulting Detective - January 2, 2017, 11:43 pm

(Jan 3, 2017 12:38 AM)Yani Wrote: [\[CITE\]](#) What part do you not understand?

You can use a key for authentication, to login.

Or you can use a key to encrypt the actual traffic (like HTTPS).

I think it's who has which key, and who generates which. Does the client uploads a key to the server? or does the server uploads a key to the client.

FractumSeraph - January 2, 2017, 11:47 pm

(Jan 3, 2017 12:43 AM)Consulting Detective Wrote: [\[CITE\]](#) I think it's who has which key, and who generates which. Does the client uploads a key to the server? or does the server uploads a key to the client.

You should read my post [here](#) on PGP. It's basically the same.

You have a public key and a private key.

You upload your public key to places like servers, or anything you want to connect to. Once they have the public key, you can use the private key to connect to them.

So instead of asking you for a username and password, they already know the username (public key), so you just have to have the password (private key) on your computer to connect.

Keep your private key safe, it's basically a password.

archangel.dmitry - January 3, 2017, 8:09 am

You should start learning about encryption first instead blindly following guides.

SuckySucky - January 3, 2017, 2:55 pm

https://en.wikipedia.org/wiki/Public-key_cryptography

Guides show you how to set it up, but knowing how it works can save you from all kinds of trouble in

the future.

captainspalding - January 3, 2017, 6:04 pm

You asked about SSH, which can use PGP keys, but what you really want to know about is PGP/GPG specifically.

Using colors is the eli5.

Skip to 02:16 to get past the history.

youtube.com/watch?v=YEBfamv-_do

kawaii - February 11, 2017, 5:03 am

Here, I'll simplify and spoonfeed you this because it's the fastest way.

Run this command:

Code `ssh-keygen -t ed25519`

It'll ask you to set a passphrase, please do so.

Once the generation is complete you'll now have two new files in the directory where you ran that command.

`id_ed25519` is the private key. Keep this secure and don't lose it or forget the passphrase.

`id_ed25519.pub` is the public key. This is the one you upload to your server. Open it in a text editor and paste the contents into the `/.ssh/authorized_keys` file of your user account directory.

ElmagoLoko - February 20, 2017, 5:27 pm

Cybrary have a course about cryptography.

Take a chance and you can learning everything about public key and private key.

It's free