

Re: restrict ssh access

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2005-12/msg00169.html>

- *From:* Peter <Retrodog@xxxxxxxxxxxx>
 - *Date:* Tue, 27 Dec 2005 18:07:47 -0000
-

"Xinming He" <xhe@xxxxxxx> wrote in [news:dopr4j\\$9r8\\$1@xxxxxxxxxxxx](mailto:news:dopr4j$9r8$1@xxxxxxxxxxxx):

> We have one ssh server which receives about 6000 failed attempts to
> login using various usernames everyday from malicious hosts (averaging
> about 1000 attempts from each distinct client IP address).
> Does anyone know if there is a way to restrict the number or rate of
> unsuccessful login attempts per client IP address? For example,
> configure ssh server to accept only one ssh connection request per
> minute from the same client IP address. Thanks very much.
>
> Simon(Xinming)
>
>
>

I am having the same problem but not as much quantity as you. I have not fully solved the problem but believe I am on the correct path and just lack a few more settings to stop it completely

are you using the ssh under cygwin by any chance? Im not sure if all of this works for openSSH but it appears as if most of it is a similar program. if so I'll try to relay all of what I have discovered so far.

If you use cygwin go here and look at all the settings of this file

`c:\cygwin\etc\sshd_config`

`# Authentication:`

```
#LoginGraceTime 2m
#PermitRootLogin yes
StrictModes no
#MaxAuthTries 6
```

the following is a portion of my file and the area i believe you want to modify.

I'm guessing you would want to set it like this

Re: restrict ssh access

Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
StrictModes yes
#MaxAuthTries 6

if you want the maximum number of tries to change just take out the # symbol and change the number, same goes for the LoginGraceTime 2m

hope that helps. i have not tried it myself but since I am having the same problem with attackers I think i will try that next to see how and if it works.

=====

you can also try this if you know all the ip address of the computers that are trying to connect to your server

modify the file c:\cygwin\etc\hosts.allow on the server to reflect the specific computers you want to access the service

my particular file says the following (ip's changed to protect the innocent) :)

```
#
# hosts.allow This file describes the names of the hosts which are
# allowed to use the local INET services, as decided
# by the '/usr/sbin/tcpd' server.
#
#
sshd: "some ip address no quotes" <--- put any ip addresses you want here
sshd: 127.0.0.1 <---- this just lets the client computer access only ssh
all: 127.0.0.1 <---- this lets the client computer access all services
sshd: 127.0.0.2 <---- put new address in on the next line
```

you can also do the same thing with hosts.deny to specifically block ip's that you know are attacking you

=====

currently im trying to make it so the client needs a public/private key pair to be able to login. i can get my keys to work properly but i cant eliminate the keyless login feature that asks for a normal password.

Here is some info on how to set up public / private keys the website i got it from is not up at the moment (maybe due to winter break at this guys school) but to give credit here it is

<http://www.mines.edu/~gmurray/HowTo/sshNotes.html>
the following was cut and slightly edited from the above link

For public key private key operation do the following

Re: restrict ssh access

Re: restrict ssh access

Create your keys: You need to create private and public ssh keys and put them in the proper place with the proper permissions. In your home directory create a folder `.ssh` (`$ mkdir .ssh`), if there is none. Create the keys with the command

```
$ ssh-keygen -t dsa
```

The `ssh-keygen` program will ask for a passphrase, just hit the "Enter" key unless for some reason you know you want a passphrase. This creates the keys `id_dsa` and `id_dsa.pub` and puts them in `.ssh/`. The private key `id_dsa` must be readable only by you; change its permissions with

```
$ chmod 600 .ssh/id_dsa
```

Put the public key on the server: In this section we are assuming the remote server is also running OpenSSH. Somehow, you must get the `.ssh/id_dsa.pub` key onto the remote server, whether by email, ftp, carrying it over on a floppy (sneakernet), etc.; the cool way to do it is to use `scp`, which was installed along with `ssh`. Suppose the remote server is named `foobar.edu`, and your account there is "dude". To copy the file to `foobar`, run

```
$ scp .ssh/id_dsa.pub dude@xxxxxxxxxx:
```

Don't forget the trailing colon. You will be asked for dude's password on `foobar` before the copying commences. The file will be copied to dude's home directory on `foobar`.

Install the public key on the remote computer: (We assume the remote computer is running OpenSSH on Linux or UNIX!) Once `id_dsa.pub` is on the remote server, login into the remote server.

>From your home directory (where you should see your newly arrive `id_dsa.pub`) create a `.ssh` folder if none exists. Then append your `id_dsa.pub` to a file in `.ssh` with

```
$ cat id_dsa.pub >> .ssh/authorized_keys
```

This will create the file `authorized_keys` if none exists. The `id_dsa.pub` key may be removed from the remote computer's home directory, if you like. The `.ssh` folder on the remote computer must have the correct permissions, you may set them with

```
$ chmod 4755 .ssh
```

Checking the password-less connection: Now the command

```
$ ssh dude@xxxxxxxxxx
```

Re: restrict ssh access

Re: restrict ssh access

should give you a password-less connection to foobar.edu. Likewise, scp should be password-free.

By the way, all the commands you do by first logging into the remote server can be done remotely using ssh. See the documentation for details.

good luck

.

- **References:**

- ◆ **[restrict ssh access](#)**

- ◇ *From:* Xinming He

- Prev by Date: **[Re: Disable passwords in SSHD Cygwin](#)**
- Next by Date: **[Re: Error when changing expired password during login](#)**
- Previous by thread: **[restrict ssh access](#)**
- Next by thread: **[Re: restrict ssh access](#)**
- Index(es):
 - ◆ **[Date](#)**
 - ◆ **[Thread](#)**