NCS 490:
SSH Lab

By: Tony Perez

Novemeber 21, 2014

Abstract

For this lab we sercured our system when using ssh, which we use to connect to our machines remotely. We also setup access so we could access our machine from another without a password.

1 Introduction

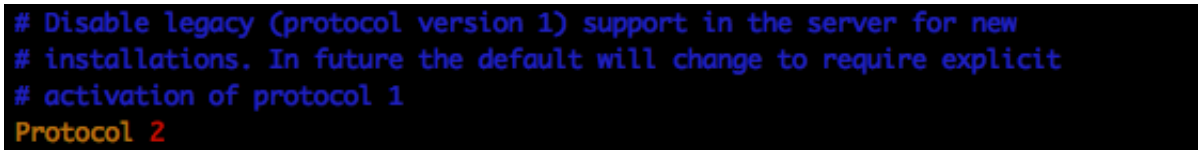
In this lab we will disable root login, limit user logins, disable protocol 1, use a non-standard port, filter SSH at the firewall, and setup private/public keys for authentication.

2 Securing SSH

We will be working in the **sshd_config**. Full path **/etc/ssh/sshd_config**.
Find the line that says **PermitRootLogin no** and make sure it says no.

Next find the **AllowUsers tony** line and put only the users you wish to allow to ssh.

Find **Protocol 2** and make sure it is set to use protocol 2.



Next if you wish you can change the port in which ssh connects to. I will leave mine at 22. To change it find the line **Port 22** which will be commented out and change it to a high port you wish to use.

Now in our iptables ssh should already be allowed. If not then we add it with:

```
# iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
```

And if we want to block someones IP address if they have attempted to connect multiple times, brute force attack.

```
# iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent !  --rcheck --seconds 60 --hitcount
4 --name ssh --rsource -j ACCEPT
```

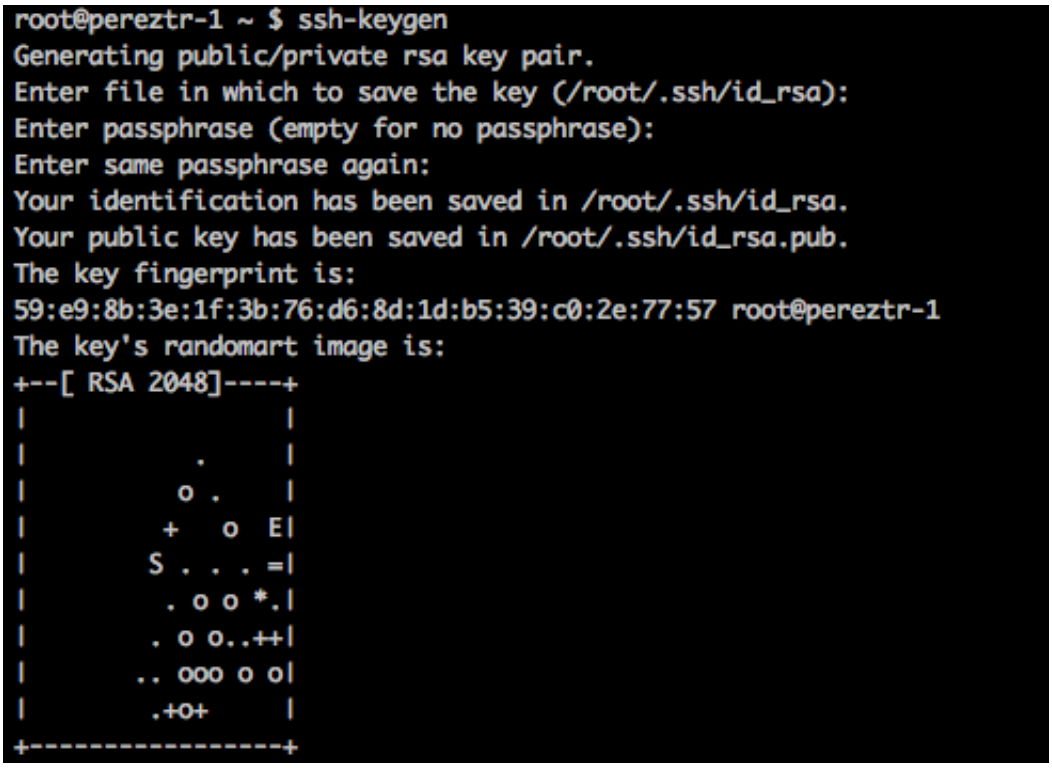
This specific command will block the person's IP address after 4 attempts.

3 Public/Private Key Setup

Now we will generate and copy an authentication key to use to login.
First we must generate a public and private key on the machine we want to give access to (note that you must be logged in as the user you wish to ssh as):

```
# ssh-keygen
```

It will prompt you for the location to be stored and if you want a password. You can leave all of these fields blank if you wish.



Now we must copy our key to the machine we want to connect to. I will copy my key to my second machines, 10.103.67.81 as tony.

```
# scp .ssh/id_rsa.pub tony@10.103.67.81: /.ssh/
```

It will prompt you for your password.
Now you will login in into the machine to copied the public key to.
Next we copy the text in the **id_rsa.pub** to the **authorized_keys** file.

```
# cat id_rsa.pub >>  /.ssh/authorized_keys
```

Now to test we exit from the machine and ssh again and we should not be prompted for a password.

4 Conslusion

SSH is very useful and is well known. This means that it is an open port and so we must secure it because although our data is secured the service could be used against us. We learned to allow only specific users and not root login. We also now use ssh keys to login whih makes it easy for us when logining in from the same machine.