ssh tips and tricks

Created and last modified by Eric Remington on Aug 06, 2014

SSH tips and tricks

How to generate an ssh key pair

ssh-keygen -b 4096 -C "useful comment including who's key it is" -f <filename, dont overwrite your existing id_rsa > -t rsa

Example:

```
vpfjmb:~ edr$ ssh-keygen -b 4096 -C "EDR test key" -f ~/.ssh/id_test -t rsa
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/edr/.ssh/id_test.
Your public key has been saved in /Users/edr/.ssh/id_test.pub.
The key fingerprint is:
6b:ad:96:d8:ae:d2:1e:97:53:5f:ea:a7:a2:af:9d:00 EDR test key
The key's randomart image is:
+--[ RSA 4096]----+
|                 |
|                 |
|                 |
|                 |
|     E S .   .   |
|      . = . o    |
|     ..oB.. o    |
|     . o++=.o  . |
|      oo+=++.oo   |
+-----------------+
vpfjmb:~ edr$ ls -l ~/.ssh/id_t*

-rw-------  1 edr  staff  3243 Jul 24 10:27 /Users/edr/.ssh/id_test

-rw-r--r--  1 edr  staff   738 Jul 24 10:27 /Users/edr/.ssh/id_test.pub

vpfjmb:~ edr$
```

How to set up a remote host so your keypair will work to ssh into it

Note that you should not copy the public key in this example as it will not work for you. It is included to show the output of the cat command

1. Get your public key to the <server>
    a. 2 methods to get your public key onto the server
        i. Via mouse buffer
            1. find your public key. In this example it is named id_test.pub from section "How to generate an ssh key pair"
            2. pfjmb:~ edr$ ls -l ~/.ssh/id_t*

                -rw------- 1 edr staff 3243 Jul 24 10:27 /Users/edr/.ssh/id_test

                -rw------- 1 edr staff   738 Jul 24 10:27 /Users/edr/.ssh/id_test.pub
            3. cat your public key

                cat ~/.ssh/id_test.pub

                ssh-rsa
                AAAAB3NzaC1yc2EAAAADAQABAAACAQDpEbZafAD3FHxwnOS/YvNj7HsfzHW+QtanaHpb5H+r6fdzz/QmrzQggWGhDDQ/q39AuYDYoCpRatrWm3DPoycEbzd/0u62+zvv
                EDR test key
            4. copy the key into your mouse buffer
            5. log into the <server> using your password (since ssh is not set up yet).
            6. execute
                a. cat >> ~/.ssh/authorized_keys
                b. dump/paste your mouse buffer
                c. hit the 'return' key
                d. hit '^D'.
        ii. scp it to the server
            1. scp /.ssh/id_test.pub <server>:~/.ssh
            2. log into the host using your password (since ssh is not set up yet)
            3. cat ~/.ssh/id_test.pub >> ~/.ssh/authorized_keys
2. Use your key to log into the <server>
    a. ssh -i ~/.ssh/id_test <server>

setting up a host in ssh config

You can create a file in the ~/.ssh directory named 'config'. This file is used to set defaults and/or server specific settings. For instance you may not want to always have to type 'ssh someHorriblyLongUserID@someIPaddress'. the config file allows you to define an 'alias' for things like this.

Good ssh resources

- http://linux.about.com/library/cmd/blcmdl5_ssh_config.htm
- http://blogs.atlassian.com/2011/05/advanced_ssh_for_developers/