Exercises: SSH (Secure SHell): ccTLD Workshop: Amman, Jordan

November 29, 2007

Exercises

Using SSH to Admin your Box

1. Copy Your admin Account Public Key to the root Account
2. Update /etc/ssh/sshd_config

Notes (CRITICAL)

1. The "#" and "$" characters before commands represents your system prompt and is not part of the command itself. "#" indicates a command issued as root while "$" indicates a command issued as a normal user.
2. ***italics***: Items that are in *italics* are to be replaced with something of your choice. For instance, *username* means choose your own username, don't literally choose the word "username".

1.) Copy Your admin Account Public Key to the root Account [Top]

For this exercise we want you to copy /home/admin/.ssh/id_rsa.pub over to your neighbor's machine and place the file in /root/.ssh/authorized_keys.

Note, you cannot log in directly to your neighbor's machine as root, so you must take advantage of the fact that you can get in as the userid *admin* and then you can become root once you are logged in.

So, here are the steps to do this:

```
$ cd /home/admin/.ssh
$ scp id_rsa.pub admin@pcN:/tmp/.
$ ssh admin@pcN
[admin@pc1 ~]$ su - [enter root password when requested]
# cd /root/.ssh [if ".ssh" is not there do mkdir .ssh]
# cat /tmp/id_rsa.pub >> authorized_keys
# rm /tmp/id_rsa.pub
# exit
```

Now your public key is in the /root/.ssh/authorized_keys file on your neighbor's machine. You cannot log in yet to your neighbor's machine as root since the file /etc/ssh/sshd_config is configured to block all root access. Our next exercise will change this.

2.) Update /etc/ssh/sshd_config [Top]

We have placed an sshd_config file on the noc server that you can copy to your machine to accomplish what we want to do. This configuration file only allows access to your machine via ssh if someone has their public key in the account they are trying to connect with. In addition, this file allows you to connect directly as root. This can actually be very useful, especially if you need to copy over a large number of files with root privileges.

For this exercise you must be root. Do the following:

```
# cd /etc/ssh
# cp sshd_config sshd_config.bak
# ftp noc
username: anonymous
password: your_email
ftp> cd pub/FreeBSD/configs
ftp> lcd /etc/ssh
ftp> get sshd_config
ftp> exit
```

Now you can restart your ssh server and the new configuration will take affect, *but* you must coordinate this with your neighbors first. If they are still accessing your box to copy over keys, then wait to to do this until they are done. If you don't, then they won't be able to log in and finish these exercises.

If your neighbor or neighbors are not ready, just go on to the final exercise and come back to this last step later.

To restart your ssh server (as root) do:

```
# /etc/rc.d/sshd restart
```

Once your neighbor has done this as well try loggin in on their machine as root from your local account. For instance, if you are in a terminal window as root you could do:

```
# su - admin
[admin@pc2 ~]$ ssh root@pcN
```

You should be prompted for your passphrase, and you should be able to log in directly to your neighbor's machine as root! This is a very useful tool.

Be sure to exit your session on their machine:

```
# exit
```

And, have a look at the file /etc/ssh/sshd_config. Maybe compare it to /etc/ssh/sshd_config.bak to see some of the differences.

Note that this file will work for Linux as well.

Be sure everyone on your machine completes this exercise.

[Return to Top]

Hervey Allen

Last modified: Thu Nov 29 01:32:34 EET 2007