**Exercise: Configure Test Environment for Secure Access**

***NOTE:***These exercises can be run on the Linux Academy Lab Servers using any distribution and version available. Please note however, you will need to start TWO of the Lab Servers to fully complete these exercises, using the default 'user' account on each server.

1. Once you have started your Linux Academy Lab Servers and logged in with the 'user' account and password provided, use the appropriate command to generate a public and private key pair on 'Server1'. Verify the key pair was created by changing to the appropriate directory and listing the files.

2. Exchange the public key with 'Server2' and the 'user' account on that server. Verify that the identity appearing in the appropriate key file matches the user and system name/IP of the originating 'Server1'.

3. Verify that you are able to log into 'Server2' from 'Server1' with the 'user' account without entering a password. Check the hostname file to be sure you are logged into 'Server2'.

4. Repeat Step #1 for 'Server2' (creating and exchanging the 'user' SSH keys with 'Server1'). Create a file on 'Server1' using any method you choose. Use 'secure copy' to copy that file to 'Server2'. Confirm the copy succeeds without password entry.

5. Using 'secure copy', copy the file from Step #4 back to 'Server1' from 'Server2', renaming it to something else during the copy process, verify that no password was required.

1. Once you have started your Linux Academy Lab Servers and logged in with the 'user' account and password provided, use the appropriate command to generate a public and private key pair on 'Server1'. Verify the key pair was created by changing to the appropriate directory and listing the files.

[user@tcox4 ~]$ ssh-keygen

Generating public/private rsa key pair.

Enter file in which to save the key (/home/user/.ssh/id\_rsa):

Created directory '/home/user/.ssh'.

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /home/user/.ssh/id\_rsa.

Your public key has been saved in /home/user/.ssh/id\_rsa.pub.

The key fingerprint is:

b8:49:0a:1f:71:f9:0c:54:c8:8e:30:9b:93:b3:3c:bf user@tcox4.mylabserver.com

The key's randomart image is:

+--[ RSA 2048]----+

|     ..o.        |

|  o  .o.         |

|   \*.o+          |

|  \* .o.=         |

| ..+. o S        |

|  +o + o         |

|   oo o          |

|    .            |

|    E.           |

+-----------------+

[user@tcox4 ~]$ cd .ssh

[user@tcox4 .ssh]$ ll

total 8

-rw-------. 1 user user 1679 Sep 21 14:23 id\_rsa

-rw-r--r--. 1 user user  408 Sep 21 14:23 id\_rsa.pub

2. Exchange the public key with 'Server2' and the 'user' account on that server. Verify that the identity appearing in the appropriate key file matches the user and system name/IP of the originating 'Server1'.

[user@tcox4 .ssh]$ ssh-copy-id 54.86.179.231

The authenticity of host '54.86.179.231 (54.86.179.231)' can't be established.

ECDSA key fingerprint is 0d:0c:b1:1d:e1:cf:6d:9f:51:bf:0f:dc:60:82:a1:73.

Are you sure you want to continue connecting (yes/no)? yes

/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed

/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys

user@54.86.179.231's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh '54.86.179.231'"

and check to make sure that only the key(s) you wanted were added.

[user@tcox4 .ssh]$ ssh 54.86.179.231

Last login: Mon Sep 21 14:22:42 2015 from 216.46.60.98

[user@tcox5 ~]$ cd .ssh

[user@tcox5 .ssh]$ ll

total 4

-rw-------. 1 user user 408 Sep 21 14:24 authorized\_keys

[user@tcox5 .ssh]$ cat authorized\_keys

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDBk5qaPck8F+aHk1BZBNmgqW6TSXctE0N+MddROuqm2TvxMeI4s5bfCpWXSBKqhTo/SFqMjM7nHp4F8stG86VEP5UymiWaeVu6rrzxTrT/9QIlFW+yWv9Mbg/GNN48rqDdZ4931sLsYnKx/dDh1S/iTofQpzgl6LB+bpsgWanaVPIcKJkh0LP9LZXX0+VpPlMrk9Gpn1F0k1EdO5zPYyEI2MkmhJZCMKhz3dOZCIqMuayt1QKSSpyDeVDx3dMMuFddXJOyuWEIYtIJC+u7hIIHV6Bsmzl4PI0dHnvmHk+Sn2DBEIn/K+9aqRQMT9IR2a2TOX1EWBqaNDsxIeLjdhw3 user@tcox4.mylabserver.com

3. Verify that you are able to log into 'Server2' from 'Server1' with the 'user' account without entering a password. Check the hostname file to be sure you are logged into 'Server2'.

[user@tcox4 .ssh]$ ssh 54.86.179.231

Last login: Mon Sep 21 14:22:42 2015 from 216.46.60.98

[user@tcox5 .ssh]$ hostname

tcox5.mylabserver.com

4. Repeat Step #1 for 'Server2' (creating and exchanging the 'user' SSH keys with 'Server1'). Create a file on 'Server1' using any method you choose. Use 'secure copy' to copy that file to 'Server2'. Confirm the copy succeeds without password entry.

[user@tcox4 ~]$ echo "test file" > testfile.txt

[user@tcox4 ~]$ scp testfile.txt 54.86.179.231:/home/user

testfile.txt

5. Using 'secure copy', copy the file from Step #4 back to 'Server1' from 'Server2', renaming it to something else during the copy process, verify that no password was required.

[user@tcox4 ~]$ scp 54.86.179.231:/home/user/testfile.txt copiedfrom.txt

testfile.txt                                                                                                                                                                   100%   10     0.0KB/s   00:00

[user@tcox4 ~]$ ll

total 8

-rw-rw-r--. 1 user user  10 Sep 21 14:31 copiedfrom.txt

drwxr-xr-x. 2 user user   6 Jan  7  2015 Desktop

-rw-rw-r--. 1 user user   0 Sep 21 14:30 testfile.txt