Laud Mills

Two CentOS VM’s are needed in this lab. They are referred to as *server* with IP 192.168.100.30/24 and *client* with IP 192.168.100.39/24. Please use the names and IP’s of your VM’s instead.

Make sure to execute iptables -F on both VM’s to flush any active firewall rules.

Also make sure to have user peter on server, and user barbara on client.

Passwordless connection

Tutorial: <https://yourtoolbox.blogspot.com/2012/08/ssh-connection-with-no-password.html>

1. Disable password authentication and allow only public key authentication on the SSH server. What options did you modify and how?

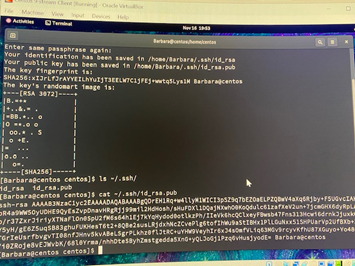
This can be done by editing the /etc/ssh/sshd\_config file as follows: uncommenting the PasswordAuthentication and setting it to no and then uncomment the PubkeyAuthentication and set it to yes. You then restart the sshd and can verify status by using systemctl status sshd.

1. Try connecting as peter and explain what happens.

Permission denied (publickey,gssapi-keyex,gssapi-with-mic)

1. To allow this user to connect to another user in the server, you must establish an exchange of the public key. This must be set up for every pair of users, that is, it only allows a user in the client to connect to a user in the server. Create a public and private key as the user barbara on client. Leave the passphrase empty and the default files for the keys. What algorithm was used to create the keys? Capture a screenshot.

The algorithm used is the RSA algorithm.



1. On server, login as peter, then create a directory .ssh under your home directory.

Used this process to do this task: su Peter then mkdir ~/.ssh verify the directory: ls -ld ~/.ssh

1. Now we need to place barbara’s key in a special file in peter’s home on server. The key can be copied manually, for instance sending it by email if it was different people and not a lab you control yourself. However, there is a straightforward method using the command ssh-copy-id. Show how you did it.

NOTE: As you disabled the access with password and it is needed in this step, undo the changes in step #1 (two options changed). Then redo the changes afterwards.

After disabling PasswordAuthentication and PublickeyAuthentication in /etc/ssh/sshd  
\_config I restart sshd on the server then logged in as Barbara on the client machine the used the command ssh-copy-id -p 2222 [Peter@10.0.0.110](mailto:Peter@10.0.0.110) to check that the key was successfully copied to Peter’s directory I logged in as Peter then used the command:

cat ~/.ssh/authorized\_keys

1. What key belonging to barbara has been stored in the directory .ssh in peter’s home? In which file? Is it barbara’s public or private key?

It is Barbara’s Publickey that has been stored in Peter’s home in the ~/.ssh/authorized\_keys file.