Laud Mills

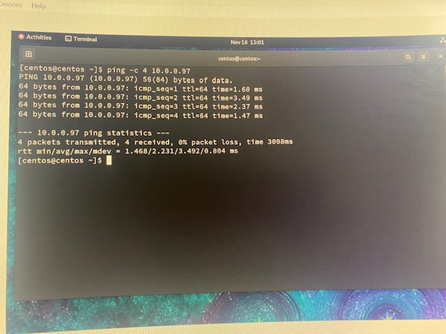
Two CentOS VM’s are needed in this lab. They are referred to as *server* with IP 192.168.100.30/24 and *client* with IP 192.168.100.39/24. Please use the names and IP’s of your VM’s instead.

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

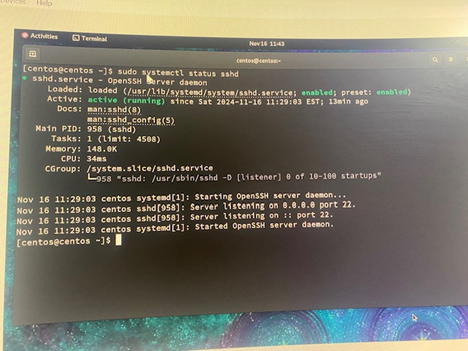
Also make sure to have users peter, wendy and james on server.

1. Verify that the two VM’s can ping each other.

A computer screen shot of a computer

Description automatically generated

1. Verify that ssh is running on server. Capture a screenshot.



1. From client, execute “ssh Peter@10.0.0.110” and, once connected, execute “ifconfig”. The IP of which VM do you see? Capture a screenshot. Finally, quit the session with “exit”.

A computer screen with white text

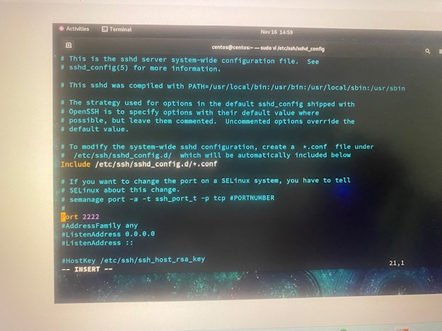
Description automatically generated

I can see the IP of the Server.

1. Why a message regarding the server’s fingerprint is shown only the first time you connect? What local file is the fingerprint stored in?

The message showed up because there is the need for verification of the identity of the server for any SSH connection at the first instance. An initial confirmation will have fingerprints of such connection stored for subsequent connections provided the same trust in place.

1. You will need to modify the file /etc/ssh/sshd\_config on server, so it is recommendable to create a copy as a backup. Then, change the default port to 2222. Capture a screenshot



1. From client, try successfully connecting again as peter. What command did you use?

Command Used: ssh -p 2222 Peter@10.0.0.110

1. We want the SSH server to allow connections from any users except root. If a user mistypes his password, he can try up to 5 times. What options and values should you configure? Indicate whether the options were already this way by default or not.

By editing the /etc/ssh/sshd\_config file particularly the PermitRootLogin line. Once it is uncommented and the value is set to no, the root users cannot access the ssh connection. As a matter of default, the PermitRootLogin is set to allow connection without root password.

Failed login attempts can be limited to five (5) by modifying the sshd\_config file to include the appropriate MaxAuthTries setting. The default is set to 6. Once it is set to 5 and the systemctl for sshd must be restarted.

1. Simulate a brute-force attack by typing a bad password more than 5 times. What message do you get?

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

1. Check that the options ClientAliveInterval and ClientAliveCountMax are commented. Considering the explanations in “man sshd\_config” (or searching online), how much time would a session stay open by default if the client does not interact?

Both ClientAliveInterval and the ClientAliveCountMax are both commented out and set to 0 and 3 respectively by default. By default the session stays open indefinitely if the client does not interact with it. It could however be uncommented and session life customized as needed.

1. Allow only the two users peter and wendy. What option did you set? Try connecting as james and show the output.

Added the line : AllowUsers Peter Wendy to the /etc/ssh/sshd\_config file

For James permission was denied.