# SSH Public Key Authentication Lab

1. Start and login to your Kali Linux virtual machine as user kali with a password of **kali**.

2. Start the SSH daemon by typing **sudo service ssh start**.

3. Open another terminal window and type **ssh localhost -l kali**. When asked to continue connecting, type **yes** and press ENTER. Enter **kali** for the user password. You are now logged in via SSH using a username and password. Type **exit**.

4. You will now configure SSH public key authentication. Enter **ssh-keygen** to generate a unique public and private key pair. Press ENTER to accept the default location and filename for the private key file. Enter **kali** as the passphrase twice to confirm. For production environments always follow organization password policy requirements.

5. Type **cd** and press ENTER to change the current user home directory.

6. Type **cd .ssh** to change to the hidden ssh directory. Type **ls** to list files; notice the private key file (id_rsa) and the public key file (id_rsa.pub).

7. When creating key pairs on other hosts, you must copy the user public key file to the server, specifically, the authorized_keys file in the user .ssh folder. Even though we generated the keys on the SSH server (localhost IP of 127.0.0.1), we will step through how this works. Type **ssh-copy-id -i ~/.ssh/id_rsa.pub kali@127.0.0.1**. When asked to trust the SSH server fingerprint, type **yes** and press ENTER.

8. Enter **ls** and notice the authorized_keys file that the ssh-copy-id command created and copied the public key file to. The ssh-copy-id command also sets the necessary permissions for user access (and nobody else!) to the file.

9. View the copied public key by typing **cat authorized_keys**. The public key must reside on the server and the private key is on the connecting user station (same computer in this example).

10. In another terminal window type **ssh localhost -l kali** once again to login as user **kali**. This time you are asked for the SSH private key passphrase (and not the user password). Enter **kali**. You are now logged in using SSH public key authentication.