Secure File Transfer

**3. Secure File transfer:**

Task: Configure SSH for secure remote access to a server. Using SCP, transfer a file from your local machine to the remote server. Document the steps involved, including setting up SSH keys for authentication and using SCP for the transfer.

# Step 1: Generate SSH Key Pair (Local Machine)

* 1. **Open a Terminal on Your Local Machine:**

On Linux or macOS, you can use the built-in terminal.

On Windows, you can use the Windows Subsystem for Linux (WSL), Git Bash, or any terminal emulator of your choice.

# Generate an SSH Key Pair:

Run the following command in the terminal:

ssh-keygen -t rsa -b 4096 -C ["your\_email@example.com"](mailto:your_email@example.com)

Replace ["your\_email@example.com"](mailto:your_email@example.com) with your actual email address.

Press Enter to accept the default file location ( ). Optionally, set a passphrase for added security.

**~/.ssh/id\_rsa**

# Ensure Proper Permissions:

Set proper permissions for the SSH private key:

chmod 600 ~/.ssh/id\_rsa

Set proper permissions for the SSH public key:

chmod 644 ~/.ssh/id\_rsa.pub

# Step 2: Copy Public Key to Remote Server

* 1. **Log in to the Remote Server:**

Connect to the remote server using SSH:

ssh username@remote\_server\_ip

Replace

Replace server.

with your remote server username.

with the actual IP address or domain of your remote

**username**

**remote\_server\_ip**

# Create SSH Directory on the Remote Server:

Create the directory on the remote server if it doesn't exist:

**~/.ssh**

mkdir -p ~/.ssh

# Append Public Key to Authorized Keys:

Run the following command to append the content of your local machine's public key

( ) to the file on the remote server:

**~/.ssh/id\_rsa.pub**

**~/.ssh/authorized\_keys**

cat >> ~/.ssh/authorized\_keys < ~/.ssh/id\_rsa.pub

# Ensure Proper Permissions on the Remote Server:

Ensure proper permissions for the directory:

**~/.ssh**

chmod 700 ~/.ssh

Ensure proper permissions for the file:

**authorized\_keys**

chmod 600 ~/.ssh/authorized\_keys

# Logout from the Remote Server:

Exit the SSH session to the remote server:

exit

By following these steps, you have generated an SSH key pair on your local machine, and the public key has been copied to the authorized keys on the remote server, enabling secure key-based authentication. Ensure that the SSH keys are handled securely and that the private key is not shared or compromised.

# Step 3: Test SSH Connection (Remote Server)

* 1. **Open a New Terminal on Your Local Machine:**

Open a new terminal on your local machine to perform the SSH connection test.

# Test the SSH Connection:

Run the following command to test the SSH connection to the remote server using key-based authentication:

ssh -i ~/.ssh/id\_rsa username@remote\_server\_ip

Replace

Replace server.

with your remote server username.

with the actual IP address or domain of your remote

**username**

**remote\_server\_ip**

# Provide SSH Key Passphrase (if Applicable):

If you set a passphrase for your SSH key during the key generation process, you will be prompted to enter it. Provide the passphrase and press Enter.

# Successful SSH Connection:

A successful connection will show a welcome message or the remote server's command prompt, indicating that you have successfully authenticated using your SSH key.

# Step 4: SCP File Transfer (Local Machine)

* 1. **Open a Terminal on Your Local Machine:**

Open a terminal on your local machine for SCP file transfer.

# Use SCP to Transfer a File:

Run the following command to transfer a file from your local machine to the remote server using SCP:

scp -i ~/.ssh/id\_rsa /path/to/local/file.txt username@remote\_

Replace machine.

**/path/to/local/file.txt**

Replace

**username**

with the actual path to the file on your local

with your remote server username.

Replace server.

Replace

with the actual IP address or domain of your remote

with the desired destination path on the remote server.

**remote\_server\_ip**

**/path/to/remote/**

# Enter SSH Key Passphrase (if Applicable):

If you set a passphrase for your SSH key, you will be prompted to enter it during the SCP file transfer. Provide the passphrase and press Enter.

By following these steps, you can test the SSH connection and transfer a file from your local machine to the remote server using SCP. Ensure that the file transfer is successful and that you can access the remote server securely using key-based authentication.

# Step 5: Verify File Transfer (Remote Server)

* 1. **Log In to the Remote Server:**

Open a terminal on your local machine or use the existing terminal.

# Connect to the Remote Server:

Run the following command to connect to the remote server using SSH:

ssh -i ~/.ssh/id\_rsa username@remote\_server\_ip

Replace

Replace server.

with your remote server username.

with the actual IP address or domain of your remote

**username**

**remote\_server\_ip**

# Verify File Transfer:

Check if the file has been successfully transferred to the specified destination on the remote server. Run the following command:

ls /path/to/remote/

Replace with the actual destination path on the remote server.

**/path/to/remote/**

# Successful File Listing:

If the file transfer was successful, you should see the transferred file listed in the specified destination directory.

file.txt

# Logout from the Remote Server:

Exit the SSH session to the remote server:

exit

# Successful File Transfer Confirmation:

The successful listing of the transferred file confirms that the file has been securely transferred from your local machine to the remote server using SCP and SSH key- based authentication.

# Important Considerations:

Ensure that the file is in the specified destination directory.

Verify the file permissions and ownership on the remote server to ensure that they match the desired configuration.

By completing these steps, you have verified the file transfer to the remote server and confirmed the functionality of the SSH key-based authentication and SCP file transfer process. This ensures a secure and efficient means of transferring files between your local machine and the remote server.