Configuring SSH Authentication and Secure File Transfer

You'll be setting up SSH on your Kali Linux VM (192.168.64.128) as the server and using your Windows machine (`C:\Users\TD1073>`) as the client.

Step 1: Start and Enable SSH on Kali (Server)

1. Open a terminal in Kali and start the SSH service

```
sudo systemctl start ssh
```

2. Enable SSH to start on boot

```
sudo systemctl enable ssh
```

3. Check if SSH is running:

```
sudo systemctl status ssh
```

Step 2: Configure SSH for Secure Authentication

1. Edit the SSH configuration file

```
sudo nano /etc/ssh/sshd_config
```

Modify the following lines:

- Ensure **password authentication** is enabled (for initial access):

```
PasswordAuthentication yes

PermitRootLogin no

PubkeyAuthentication yes
```

Restart the SSH service to apply changes

```
sudo systemctl restart ssh
```

Step 3: Generate SSH Keys on Windows (Client)

1. Open **PowerShell** on your Windows machine and generate an SSH key:

```
ssh-keygen -t rsa -b 4096
```

Save the key in the default location (C:\Users\TD1073\.ssh\id_rsa).

Copy the public key to Kali

```
type $env:USERPROFILE\.ssh\id_rsa.pub | ssh kali@192.168.64.128
"mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys"
```

Test key-based authentication

```
ssh kali@192.168.64.128
```

If successful, you won't need to enter a password.

Step 4: Generate a Symmetric Key for Secure File Transfer

To use **symmetric encryption** for file transfer:

1. Generate a symmetric key on Kali:

```
openssl rand -base64 32 > my_symmetric_key.key
```

Transfer the key securely (after establishing SSH authentication):

```
scp kali@192.168.64.128:~/my_symmetric_key.key C:\Users\TD1073\
```

Step 5: Encrypt and Transfer Files with Symmetric Key

1. **Encrypt a file** on Kali before transfer:

```
openssl enc -aes-256-cbc -salt -in secret.txt -out secret.enc -pass
file:./my_symmetric_key.key
```

Transfer the encrypted file to Windows

```
scp kali@192.168.64.128:~/secret.enc C:\Users\TD1073\
```

Decrypt on Windows

```
openssl enc -d -aes-256-cbc -in C:\Users\TD1073\secret.enc -out
C:\Users\TD1073\secret.txt -pass
file:C:\Users\TD1073\my_symmetric_key.key
```