SSH

Here are some exercises focused on SSH (Secure Shell) and SCP (Secure Copy Protocol), emphasizing key generation and public key authentication, suitable for a network in the 192.168.4.0/24 subnet.

Part 1: SSH Basics

Exercise 1: Installing OpenSSH
Objective: Ensure that OpenSSH server is installed.

1. Check if the OpenSSH server is installed:
```
ssh -V
```

2. If it's not installed (for Rocky Linux):
```
sudo dnf install openssh-server
```

Or for Ubuntu/Debian:
```
sudo apt install openssh-server
```

3. Start the SSH service:
```
sudo systemctl start sshd
```

4. Enable the SSH service to start on boot:
```
sudo systemctl enable sshd
```

Exercise 2: Configuring SSH
Objective: Configure the SSH server (optional).

1. Open the SSH configuration file:
```
sudo nano /etc/ssh/sshd_config
```

2. (Optional) Change the default port or disable root login by modifying the configuration as needed.

3. Restart the SSH service to apply changes:
```
sudo systemctl restart sshd
```

Part 2: Using SSH

Exercise 3: Connecting via SSH
Objective: Connect to a remote machine using SSH.

1. Connect to a remote machine (replace rocky and 192.168.4.X with the actual rockyname and IP address):
```
ssh rocky@192.168.4.X
```
2. Accept the fingerprint when prompted.

Part 3: Generating SSH Keys

Exercise 4: Generating SSH Key Pair
Objective: Generate an SSH key pair for public key authentication.

1. Generate a new SSH key pair:
```
ssh-keygen -t rsa
```

- When prompted, press Enter to accept the default file location (usually ~/.ssh/id_rsa).
- Optionally, set a passphrase for added security.

2. Verify the keys have been created:
```
ls ~/.ssh/
```

Part 4: Setting Up Public Key Authentication

Exercise 5: Copying the Public Key
Objective: Copy the public key to the remote machine for authentication.

1. Use the ssh-copy-id command to copy your public key to the remote server:
```
ssh-copy-id rocky@192.168.4.X
```

2. Enter your password when prompted.

Exercise 6: Testing Public Key Authentication
Objective: Test the SSH connection using public key authentication.

1. Attempt to connect to the remote machine again (this time without a password):
```
ssh rocky@192.168.4.X
```

2. If successful, you should be logged in without being prompted for a password.

Part 5: Using SCP

Exercise 7: Copying Files with SCP
Objective: Use SCP to copy files between local and remote systems.

1. Copy a local file to the remote machine (replace file.txt and 192.168.4.X with the actual file and IP):

```
scp file.txt rocky@192.168.4.X:/path/to/destination/
```

2. Copy a file from the remote machine to your local system:
```
scp rocky@192.168.4.X:/path/to/remote_file.txt ~/
```

Part 6: Managing SSH Keys

Exercise 8: Listing SSH Keys
Objective: List the public keys for SSH authentication.

1. Display the contents of your public key:
```
cat ~/.ssh/id_rsa.pub
```

2. (Optional) You can add additional keys to the ~/.ssh/authorized_keys file on the remote machine if needed.

Exercise 9: Securing SSH
Objective: Enhance SSH security by changing permissions.

1. Ensure the .ssh directory and its contents have the correct permissions:
```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/authorized_keys
```

Part 7: Cleaning Up
Objective: Clean up unused keys (if necessary).

1. If you wish to remove a key from the remote server, edit the ~/.ssh/authorized_keys file on the remote machine and delete the corresponding line.