RedHat Certified System Administrator (RHEL 9)

SUMMARY

SSH (Secure SHell)

- SSH is a service, check it "`systemctl status sshd.service`".
- If not installed you can install it using "`yum install openssh-server`"
- SSH supports two types of authentication:
  - Password-based authentication
  - Public key-based authentication

PS: Root login may be disabled by default (check the option PermitRootLogin in /etc/ssh/sshd_config, more options in "man sshd_config").

Password-Based Authentication

- Password-based authentication is the default authentication method for SSH.
- Password-based authentication is not recommended because it is vulnerable to brute-force/dictionary attacks.
- Password-based authentication can be disabled by setting the PasswordAuthentication option to no in the /etc/ssh/sshd_config file.
  - "PasswordAuthentication no", Don't forget to restart the sshd service after changing the configuration file.

Public Key Based Authentication

- Public key-based authentication is more secure than password-based authentication.
- Public key-based authentication uses a pair of keys
- The public key is used to verify the signature of the client on the server machine.
- The public key is stored in the ~/.ssh/authorized_keys file on the server.

Steps to Configure Key Based Authentication

1. Generate a key pair on the client machine

```
ssh-keygen
```

   - Follow the instructions, you can enter a passphrase or leave it empty.
2. Copy the public key to the server machine

```
ssh-copy-id user@server
```

   - user: Username on the server machine
   - server: IP address or hostname of the server machine
3. Login to the server machine using the private key

```
ssh user@server
```

   _PS:_ Only your current user on the client machine can login to the server machine using the private key. In fact, its public key (stored in ~/.ssh/id_rsa.pub) is the one that has been sent to the authorized_keys file on the server machine. If you want to login (passwordless) to the server machine using another user, you have to redo the same steps while you are logged in as that other user.