NWTK

SSH

Gabriel Martin
3BHIT
October 4th 2023

Contents

1 Introduction to SSH

SSH (Secure Shell) is a cryptographic network protocol that allows secure communication and remote access to systems over an unsecured network. It encrypts the data transmitted between the client and server, providing confidentiality and integrity. SSH can be used to issue terminal commands on the host remotely as well as transfer files and stream a graphical UI.

2 SSH Server vs. Client

We differentiate between an SSH server that listens to the default SSH port 22 and allows connections depending on the configuration (f.e. OpenSSH Server) and the SSH client that connects to a server. These clients are typically preinstalled on all common operation systems as command line tools but there are also standalone applications like PuttY that aim to make the usage of SSH easier.

3 Installing OpenSSH Server on Debian Linux

To install SSH on Debian Linux, you can use your package manager (typically apt or aptitude). First, we update our package repositories and call install for

the package we want, in our case the openssh-server.

```
sudo apt update
sudo apt install openssh-server
```

4 Configuring Access for Root via Password

By default, SSH does not allow the root user to login via password for security reasons. To enable root login via password, you have to change the configuration accordingly:

1. Open the SSH server configuration file in a text editor:

   ```
   sudo vim /etc/ssh/sshd_config
   ```

2. Locate the line that says `PermitRootLogin` and change it to:

   ```
   PermitRootLogin yes
   ```

3. Save the file and exit the text editor.

4. Restart the SSH service to apply the changes:

   ```
   sudo systemctl restart ssh
   ```

5 Connecting with SSH Clients

You can connect to your SSH server using SSH clients like a terminal client or PuTTY.

5.1 Terminal Client

To connect using a terminal client, you can use the ssh command followed by username@hostname. This might look something like this:

```
ssh root@my-server.local
```

You will be prompted for your SSH key passphrase or password (if you didn't disable password authentication).

5.2 PuTTY (Windows)

To connect using PuTTY, download and install PuTTY from the official website (`https://www.putty.org/`) or using winget. Open PuTTY, enter the server IP, choose the SSH protocol, and click "Open." You will be prompted for your username and password or SSH key passphrase.

```
winget install PuttY.PuttY
```

6 Setting Up Key Authentication

While password authentication provides an easy way to connect to our servers it is not recommended for securing access to important servers. Another downside is that we have to enter our password every time we want to connect. This is especially bad when we want to run automated scripts over ssh. That's where public and private key authentication comes in.

1. Generate an SSH key pair on your local machine if you don't already have one:

   ```
   ssh-keygen -t rsa -b 2048
   ```

2. Copy your public key to the server:

   ```
   ssh-copy-id username@your_server_ip
   ```

3. Disable password authentication (optional but recommended for security):

   ```
   PasswordAuthentication no
   ```

7 Conclusion

SSH provides a secure way to access and manage your Debian Linux server remotely. By following this guide, you can install SSH, configure access, and set up key authentication for enhanced security.