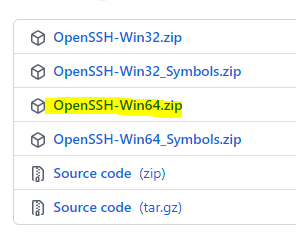
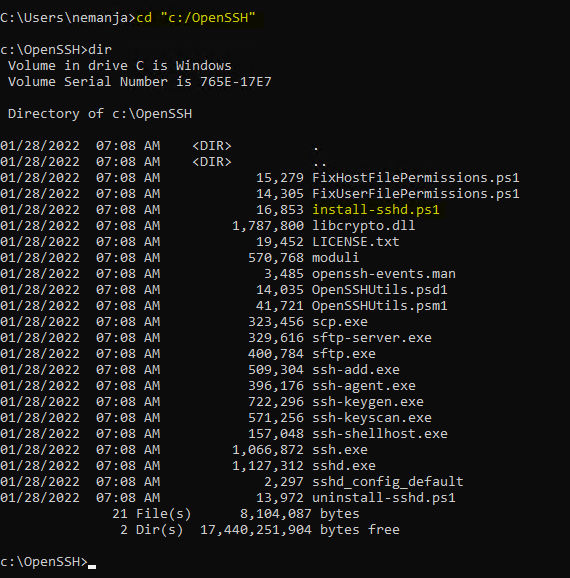
Download OpenSSH from github and extract it:

<https://github.com/PowerShell/Win32-OpenSSH/releases/tag/V8.6.0.0p1-Beta>

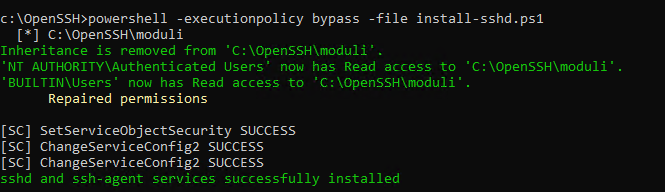


Navigate to the extracted folder and find install-sshd.ps1 file:

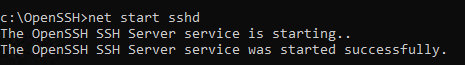


Run the installer:

**powershell -executionpolicy bypass -file install-sshd.ps1**



To start SSH server, run **net start sshd**:



Open port 22 in Windows firewall:

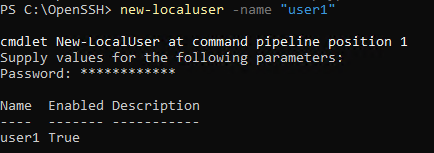
Run **new-netfirewallrule -name sshd -displayname 'OpenSSH Server (sshd)' -enable true -direction Inbound -protocol TCP -action Allow -localport 22** from PowerShell:



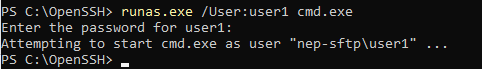
Run **set-service sshd –startuptype Automatic** (PowerShell again) to set start type to automatic:



Still in PowerShell, create a new local user - **new-localuser -name "user1"**:



Run cmd prompt as the new user - **runas.exe /User:user1 cmd.exe**:



Navigate to the user folder, create .ssh folder and from the folder run key generator file – ssh-keygen.exe in the ssh folder downloaded from the github:

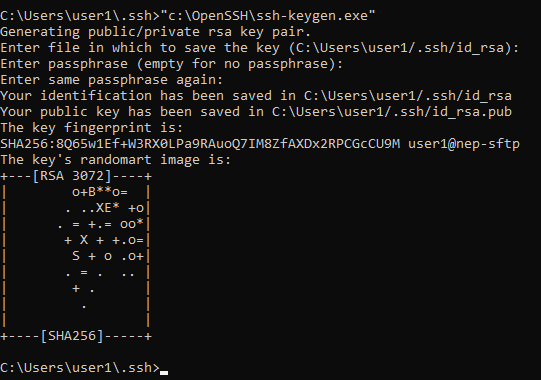
**cd %userprofile%**

**mkdir .ssh**

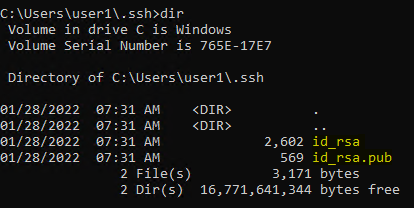
**cd .ssh**

**"c:\OpenSSH\ssh-keygen.exe"**





Dir:



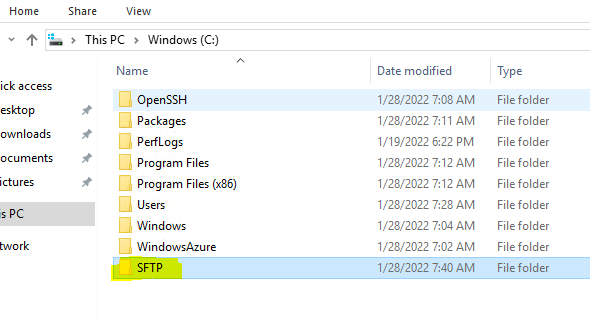
id\_rsa is private key while idrsa.pub is public key.

We need to add the public key to authorized keys:

**.ssh>copy id\_rsa.pub authorized\_keys**:



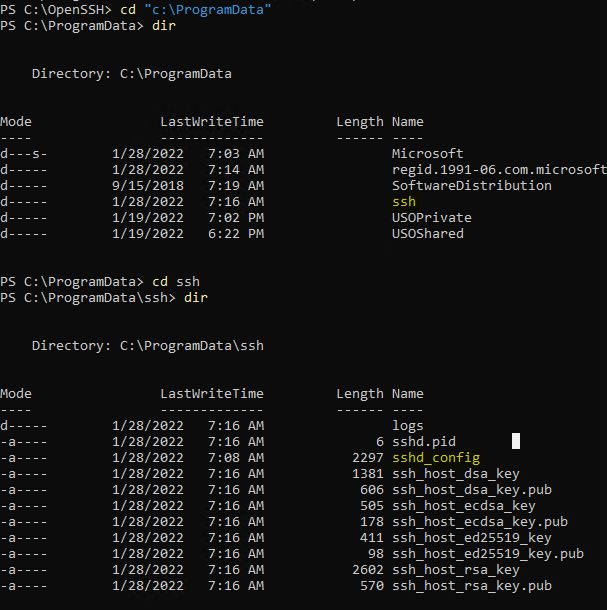
Now create a folder we will use to store incoming files:

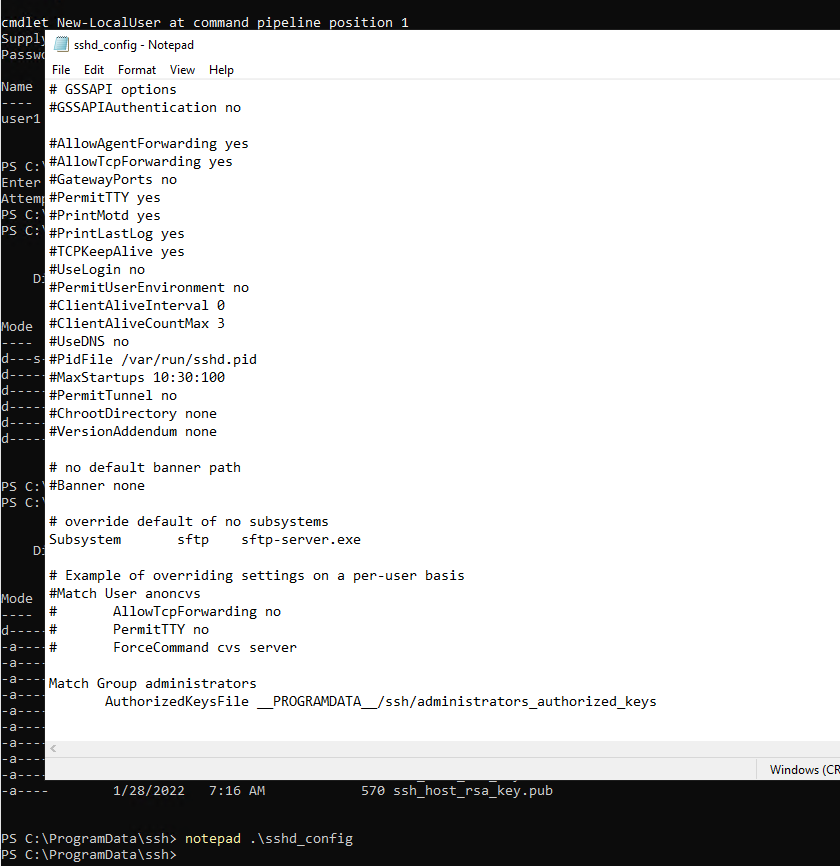


For configuration, navigate to admin cmd and run:

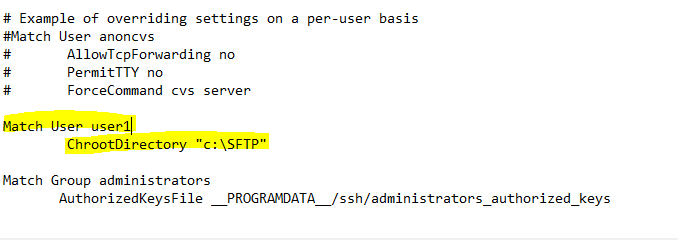
**cd "c:\ProgramData\ssh"**

**notepad .\sshd\_config**





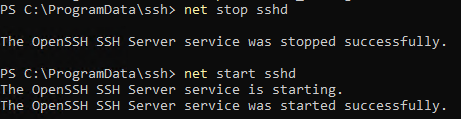
To match the user with the folder we have created, which will also set the folder to be root for the user, add the following line to the location:



Save the changes and stop and start the SFTP:

**net stop sshd**

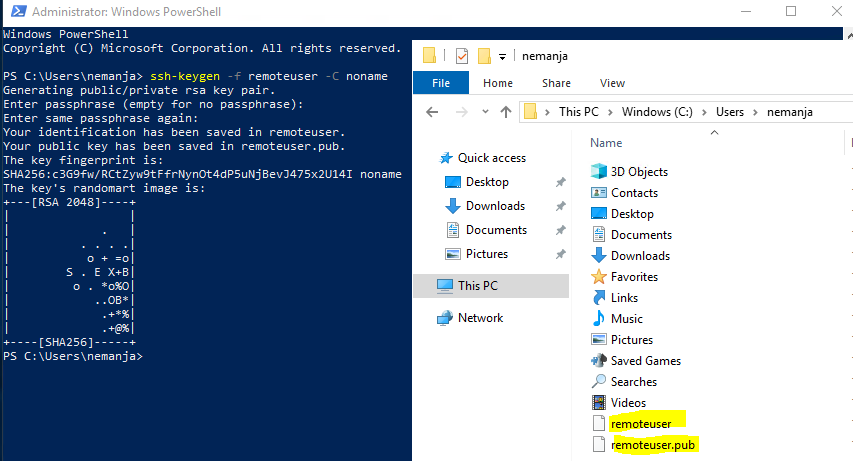
**net start sshd**



As the server is ready, we can set the client. Open the client machine. I’m using a VM in the same Vnet and will be using private IP address. From the client, run PowerShell and generate ssh key pair:

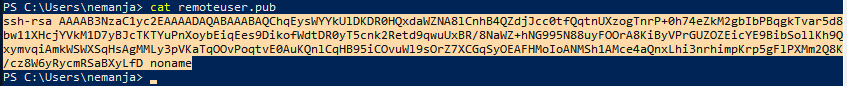
**ssh-keygen -f remoteuser -C noname**

The pair will appear in the user folder:



For the next step, we will copy the public key to sftp server. Open the key and copy it:

cat remoteuser.pub



Navigate to server again, start the cmd as local user and navigate to .ssh folder:

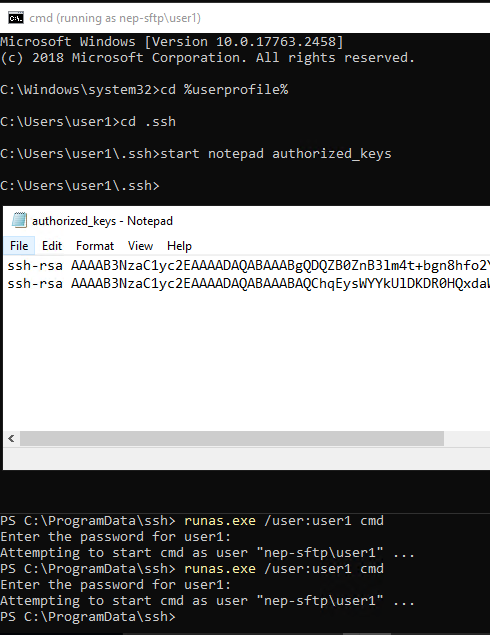
**runas.exe /user:user1 cmd**

**cd %userprofile%**

**cd .ssh**

**start notepad authorized\_keys**

Paste the public key and save the changes:



SFTP from the client using the following line:

**sftp -i remoteuser** [**user1@10.32.0.4**](mailto:user1@10.32.0.4):

