openssh-server
SYT 3

htl
Hollabrunn

Installation

OpenSSH-Server ermöglicht den Remote-Login via SSH.

```
apt install openssh-server
```

htl Hollabrunn

Temporären root-Login mit Passwort erlauben

- Konfigurationsfile vom openssh-server editieren

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

- Suche den Eintrag **PermitRootLogin**
  - Cursor in Zeile platzieren und mit Strg+K ausschneiden und anschließen mit 2x Strg+U einfügen damit die ursprüngliche Einstellung als Kommentar verfügbar bleibt
  - Value im duplizierten Eintrag von **prohibit-password** auf **yes** ändern
  - # an Zeilenanfang kennzeichnet ein Kommentar, daher die # entfernen

Start-Ende-Neustart openssh-server

- Nach der Installation läuft der Dienst standardmäßig
- Beenden:

```
systemctl stop ssh.service
```

- Starten:

```
systemctl start ssh.service
```

- Neustarten (Beenden+Starten, z.B. um Änderungen in der Konfiguration anzuwenden):

```
systemctl restart ssh.service
```

- Status einsehen:

```
systemctl status ssh.service
```

IP Adresse ermitteln

- bevor eine ssh-Verbindung aufgebaut werden kann muss die IP-Adresse ermittelt werden

```
ip address
```

oder

```
hostname -I
```

- VM Netzwerkmodus: Netzwerkbrücke bzw. Bridged Network

htl Hollabrunn

Verbindung via ssh vom Hostbetriebssystem

- HostOS (verlangt root-Passwort):

```
ssh root@172.18.8.123
```

ECDSA key fingerprint is SHA256:QsWRQFncwgaFWx8w4DNRInA7QO0rjRoUbz/gR3zAS1k.

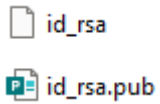
- wird beim ersten Verbindungsaufbau angezeigt
- Überprüfung durch Vergleich am openssh-server (VM):

```
ssh-keygen -l -f /etc/ssh/ssh_host_ecdsa_key.pub
```

Private/Public-Key Pair

→ Generierung Private/Public Key-File (C:\Users\<Username>\.ssh)

```
ssh-keygen -b 4096
```



→ Public Key-File am openssh-server ablegen (scp – secure copy)

```
scp id_rsa.pub root@172.18.8.123:
```

Die Kopie liegt am Linux-Client unter: `/root/.ssh/id_rsa.pub`

Authorized Keys am openssh-server

- Die Datei “authorized_keys” beinhaltet die SSH-Keys die zum Login konfiguriert wurden.

→ Inhalt des Public-Key-File in authorized_keys einfügen

```
cat /root/id_rsa.pub > /root/.ssh/authorized_keys
```

Redirect:

> überschreibt ein File falls vorhanden

>> fügt Daten am Ende eines Files hinzu

htl Hollabrunn

Verbindung via ssh mit Public/Private-Key

- HostOS:

```
ssh root@172.18.8.123
```

- Diesmal sollte keine Passworteingabe notwendig sein.

- TODO: Cleanup!

Cleanup

- Änderungen im openssh-server Konfigurationsfile zurücksetzen:

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

- Kopie des Public-Key-Files vom openssh-server löschen:

```
rm /root/id_rsa.pub
```