Protokoll

Openssh-server installieren:

```
apt install openssh-server
```

Netcat installieren:

```
sudo apt install netcat
```

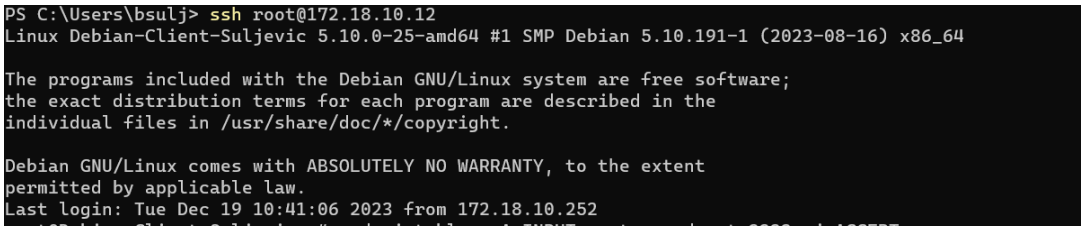
Server mit dem richtigen Port einstellen:

```
nc -l 25565
```

```
root@Debian-Client-Suljevic:~# nc -l 25565
```

Sich mit ssh verbinden

```
ssh root@172.18.10.12
```



Firwall einstellen mittels iptables

Iptables installieren:

```
sudo apt install iptables
```

Die Regeln für die Firewall konfiguriren

```
sudo iptables -A INPUT -p tcp --dport 2222 -j ACCEPT # SSH-Port anpass
```

```
sudo iptables -A INPUT -p tcp --dport 25565 -j ACCEPT # TCP-Server-Por
```

```
root@Debian-Client-Suljevic:~# sudo iptables -A INPUT -p tcp --dport 2222 -j ACCEPT
root@Debian-Client-Suljevic:~# sudo iptables -A INPUT -p tcp --dport 25565 -j ACCEPT
```

Die Regeln speichern

```
sudo apt install iptables-persistent
sudo netfilter-persistent save
sudo netfilter-persistent reload
```

```
root@Debian-Client-Suljevic:~# sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
root@Debian-Client-Suljevic:~# netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
root@Debian-Client-Suljevic:~# netfilter-persistent reload
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables start
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables start
root@Debian-Client-Suljevic:~#
```

Mit Nmap testen:

Nmap installieren:

```
apt install nmap
```

```
nmap localhost
```

```
Host is up (0.0000030s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed ports
PORT     STATE SERVICE
2222/tcp open  EtherNetIP-1
3306/tcp open  mysql
5432/tcp open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
root@Debian-Client-Suljevic:~#
```

Den SSh Zugang dem root entnehmen:

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

Den **PermitRootLogin** auf **no** und **PasswordAuthentication** ebenfalls auf **no** setzen

```
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
PasswordAuthentication no
#PermitEmptyPasswords no
```

Danach den SSH Server neustarten:

```
sudo service ssh restart
```

SSH Port ändern:

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

```
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none
```

Der Port wurde von 22 auf 2222

Benutzer erstellen:

```
sudo adduser mincraft_user

sudo usermod -aG sudo mincraft_user    #Admin Rechte geben
```