Netzwerktools

Netzwerkkonfig Debian

https://wiki.debian.org/NetworkConfiguration

https://www.digitalocean.com/community/tutorials/how-to-list-and-delete-iptables-firewall-rules-de

NMAP

udp Scan für openvpn

```
nmap -Pn -sU -p 1194 dvsdnet2.devoteam.de
```

Netcat

tcp

```
netcat [options] host port
```

udp

```
netcat -u host port
```

Port Scanning (statt nmap)

```
netcat -z -v domain.com1-1000
```

Netcat listening

```
create an UDP server using nc on port 11090
nc -ul 11090

check whether an UDP server is listening on 11190
nc -vz -u <hostname> 11090

send a packet to the UDP server
echo -n "hello" | nc -4u -w1  <hostname> 1118
```

SS - another utility to investigate sockets

https://phoenixnap.com/kb/ss-command

ss = alle offenen nicht horchenden sockets mit aktiven verbindungen

horchende und nicht horchende

```
ss -a
```

nur horchende

```
ss -l nur horchende
```

nur tcp

```
ss -t nur tcp
```

alle tcp

```
ss -at  alle tcp
```

alle udp

```
ss -u  udp

ss -au alle udp

ss  -lu  alle horchenden udp
```

alle sockets

```
ss -f unix   alle unix sockets

ss -w alle raw sockets
```

spezielle zieladresse

```
ss dst 104.21.3.132
```

spezielle quelladresse

```
ss src 192.168.100.2
```

spezielle prozess-id

```
ss -p  process IDs
```

NETSTAT

Ports checken

Alle TCP ports auflisten, auf denen jemand horcht, inklusive PID und name des daemons.

```
sudo netstat -plnt
```

Beispiel

```
$ sudo netstat -plnt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address   Foreign Address             State
PID/Program name
tcp        0      0 0.0.0.0:3306                0.0.0.0:*
LISTEN      3686/mysqld
tcp        0      0 :::443                      :::*
LISTEN      2218/httpd
tcp        0      0 :::80                       :::*
LISTEN      2218/httpd
tcp        0      0 :::22                       :::*
LISTEN      1051/sshd
```

Liste filtern

If the list of listening daemons is long, you can use `grep` to filter it. For example, to filter out everything except the default web server port `80`, run the following command:

```
$ sudo netstat -plnt | grep ':80'
tcp   0      0 :::80                       :::*
LISTEN      8448/httpd
```

Analyze the results

Common outcomes include the following results:

- Nothing is listening on the port. Check the service configuration files, and then restart the service.
- The correct service is listening on the correct port. In this case you need to test the service more thoroughly. Skip to the article on testing the listening service for response using netcat.
- Something other than the expected service appears to be listening on the port.

Note: A super-server, such as xinetd, might be listening on the port. Check your xinetd configuration to ensure that this behavior is acceptable.

If something else is listening on the port, you can disable the program by running `sudo service httpd stop`, or change its configuration so that it no longer listens on the port. When `netstat` shows the port is free, enable the correct service (for example `sudo service vsftpd start`).

If you make any changes because the incorrect service is listening, run the `netstat` command again. If `netstat` doesn't show the program listening on the correct port, you need to address its configuration before you go any further.

If you make changes at this point, be sure to test your setup to verify that you have resolved your issue.

If using the `netstat` did not resolve your port issues, continue to test connections to the service by using the netcat command.

IPTABLES

iptables -nvL

iptables -nvL -t nat

TCPDUMP

tcpdump -i vmbr0 -nn port 1194

tcpdump -i vmbr1 -nn port 1194