

## Activity Network Security

Q1

Nmap found 2 open ports on my notebook which are 6463 and 49510

```
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00077s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65533 closed ports
PORT      STATE SERVICE      VERSION
6463/tcp  open  unknown
| fingerprint-strings:
|_  DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, Kerberos, LDAPBindReq, LDAPSearchReq, LPDString, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:
|_  HTTP/1.1 400 Bad Request
|_  Connection: close
|_  FourOhFourRequest, GetRequest, HTTPOptions:
|_  HTTP/1.1 404 Not Found
|_  Content-Length: 32
|_  Content-Type: application/json
|_  Date: Tue, 22 Sep 2020 04:58:04 GMT
|_  Connection: close
|_  {"code":0,"message":"Not Found"}
49510/tcp  open  bandwidth-test MikroTik bandwidth-test server
```

Nmap scan on the notebook

6463 is opened with unknown reason, but with some research I found that it's being used by Discord

**RPC Server Ports**

The port range for Discord's local RPC server is [6463, 6472]. Since the RPC server runs locally, there's a chance it might not be able to obtain its preferred port when it tries to bind to one. For this reason, the local RPC server will pick one port out of a range of these 10 ports, trying sequentially until it can bind to one. When implementing your client, you should perform the same sequential checking to find the correct port to connect to.

Source: <https://discord.com/developers/docs/topics/rpc>

While 49510 said to be used by Bandwidth test

In the meantime there is no suspicious port opened in the VM. Only the intended ssh (22) and http (80) are open

```
Nmap scan report for 192.168.56.101
Host is up (0.0027s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.41 ((Ubuntu))
|_ http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 11:49
Completed NSE at 11:49, 0.00s elapsed
Initiating NSE at 11:49
Completed NSE at 11:49, 0.00s elapsed
Initiating NSE at 11:49
Completed NSE at 11:49, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 95.40 seconds
```

Nmap scan on the VM

## Q2 OS Scanning

With nmap -O --osscan-guess, it cannot detect my notebook's OS.

While it guessed that my VM is running on Linux, which is correct but it did not specified about the Linux distribution of it. It also list a lot of other possible OS that the VM might use judging from the behavior of it.

```

$ sudo nmap -O --osscan-guess localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-22 11:05 +07
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000083s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.35 seconds

```

### OS check on the notebook

```

$ sudo nmap -O --osscan-guess 192.168.56.101
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-22 11:04 +07
Nmap scan report for 192.168.56.101
Host is up (0.00060s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:E8:37:D3 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.4 - 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Synology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), Linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=9/22%OT=22%CT=1%CU=30874%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=5F6977D2%P=x86_64-apple-darwin19.5.0)SEQ(SP=100%GCD=1%ISR=108%TI=Z%CI=
OS:Z%II=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST1
OS:1NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=F
OS:E88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=
OS:40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%
OS:0=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=0%RD=0%Q=)T6(R=Y%DF=Y%T=4
OS:0%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=0%RD=0%
OS:Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=
OS:Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.28 seconds

```

### OS check on the VM

## Q3

Port scanning from nmap can reveals open ports and its service, it could lead to malicious attack if the attacker tries to get in a sensitive service like ssh login. Even when the ssh isn't set on port 22 nmap can still find the ssh service on other ports.

Source: <https://www.howtogeek.com/369506/htg-explains-what-is-port-scanning/>

IP Address	Description
127.0.0.1	Localhost
10.0.2.15	IP address when network was set to NAT
192.168.56.101	IP address when network is set to host-only adapter
192.168.56.1	My notebook's IP address

```

127.0.0.1 - - [22/Sep/2020:10:30:04 +0700] "GET / HTTP/1.1" 200 3477 "-" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
127.0.0.1 - - [22/Sep/2020:10:30:05 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://localhost/" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
127.0.0.1 - - [22/Sep/2020:10:30:05 +0700] "GET /favicon.ico HTTP/1.1" 404 487 "-" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
10.0.2.15 - - [22/Sep/2020:10:32:12 +0700] "GET / HTTP/1.1" 200 3477 "-" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
10.0.2.15 - - [22/Sep/2020:10:32:13 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://10.0.2.15/" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
10.0.2.15 - - [22/Sep/2020:10:32:13 +0700] "GET /favicon.ico HTTP/1.1" 404 487 "-" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
192.168.56.101 - - [22/Sep/2020:10:39:33 +0700] "GET / HTTP/1.1" 200 3477 "-" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
192.168.56.101 - - [22/Sep/2020:10:39:33 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://192.168.56.101/" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
192.168.56.101 - - [22/Sep/2020:10:39:33 +0700] "GET /favicon.ico HTTP/1.1" 404 492 "-" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
192.168.56.1 - - [22/Sep/2020:10:39:55 +0700] "GET / HTTP/1.1" 200 3477 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15
192.168.56.1 - - [22/Sep/2020:10:39:55 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://192.168.56.101/" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15
192.168.56.1 - - [22/Sep/2020:10:39:55 +0700] "GET /favicon.ico HTTP/1.1" 404 493 "http://192.168.56.101/" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15
192.168.56.1 - - [22/Sep/2020:10:44:14 +0700] "GET / HTTP/1.1" 200 3477 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15

```

Access.log file for apache server

Q5

[illegible]

### Access.log file showing logs with nmap scanning attempts

### After iptables configuring



## Q7

The logs aren't the exact same but are still quite similar to each other, here's the comparing result of access.log before and after iptables rules added.

```

Completed Connect Scan at 15:02, 3747.37% elapsed (65535 total ports)
Initiating Service scan at 15:02
Scanning 2 services on 192.168.56.101
Completed Service scan at 15:02, 6.02s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.56.101.
Initiating NSE at 15:02
Completed NSE at 15:02, 0.11s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Nmap scan report for 192.168.56.101
Host is up (1.0s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Apache httpd 2.4.41 (Ubuntu)
|_ http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
10721/tcp filtered unknown
29485/tcp filtered unknown
30178/tcp filtered unknown
32572/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Read data files from: /usr/local/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 3754.09 seconds
  
```

```

192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "GET /nmaplowercheck160075978 HTTP/1.1" 404 456 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "POST / HTTP/1.1" 200 1192 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "GET /git/HEAD HTTP/1.1" 404 456 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "POST /jdk HTTP/1.1" 404 456 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "GET / HTTP/1.0" 200 1192 "-" "-"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "PROPFIND / HTTP/1.1" 405 524 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "GET /vex/about HTTP/1.1" 404 456 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "VXU / HTTP/1.1" 501 500 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "PROPFIND / HTTP/1.1" 405 524 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "GET /favicon.ico HTTP/1.1" 404 456 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "GET /nmap HTTP/1.1" 404 456 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "GET / HTTP/1.0" 200 1192 "-" "-"
192.168.56.1 - [22/Sep/2020:13:20:18 +0700] "GET / HTTP/1.1" 200 1173 "-" "-"
  
```

Nmap scanning without iptables rules (left) and access.log (right)

```

Initiating Connect Scan at 15:58
Scanning 192.168.56.101 (65535 ports)
Discovered open port 22/tcp on 192.168.56.101
Discovered open port 80/tcp on 192.168.56.101
Connect Scan Timing: About 22.62% done; ETC: 16:00 (0:01:46 remaining)
Connect Scan Timing: About 57.55% done; ETC: 16:00 (0:00:45 remaining)
Completed Connect Scan at 16:00, 98.06s elapsed (65535 total ports)
Initiating Service scan at 16:00
Scanning 2 services on 192.168.56.101
Completed Service scan at 16:00, 6.02s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.56.101.
Initiating NSE at 16:00
Completed NSE at 16:00, 0.17s elapsed
Initiating NSE at 16:00
Completed NSE at 16:00, 0.00s elapsed
Initiating NSE at 16:00
Completed NSE at 16:00, 0.00s elapsed
Nmap scan report for 192.168.56.101
Host is up (0.0019s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Apache httpd 2.4.41 (Ubuntu)
|_ http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 16:00
Completed NSE at 16:00, 0.00s elapsed
Initiating NSE at 16:00
Completed NSE at 16:00, 0.00s elapsed
Initiating NSE at 16:00
Completed NSE at 16:00, 0.00s elapsed
Initiating NSE at 16:00
Completed NSE at 16:00, 0.00s elapsed
Read data files from: /usr/local/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 96.83 seconds
  
```

```

192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "PROPFIND / HTTP/1.1" 405 524 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "POST /jdk HTTP/1.1" 404 456 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "GET /nmaplowercheck1600765208 HTTP/1.1" 404 456 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "GET /git/HEAD HTTP/1.1" 404 456 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "PROPFIND / HTTP/1.1" 405 524 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "POST / HTTP/1.1" 200 1192 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "GET / HTTP/1.0" 200 1192 "-" "-"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "GET /vex/about HTTP/1.1" 404 456 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "VXU / HTTP/1.1" 501 500 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "PROPFIND / HTTP/1.1" 405 524 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "GET /favicon.ico HTTP/1.1" 404 456 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "GET / HTTP/1.0" 200 1192 "-" "-"
192.168.56.1 - [22/Sep/2020:15:50:47 +0700] "GET / HTTP/1.1" 200 1173 "-" "-"
  
```

Nmap scanning with iptables rules configured (left) and access.log after enabling the rules (right)

## Q8

Firewall can be configured to drop any packets that is not related to the service. Use the policy DROP by default and only let the legit packets to the service ports in.

Firewall can also cut off the attack if the system has been scanned too frequently, like 10 times per minute or 100 times.

Source: <https://nmap.org/book/nmap-defenses-firewalls.html>

Q9

```
darkenstardragon@VMUbuntu:/var/log/apache2$ sudo iptables -F INPUT
darkenstardragon@VMUbuntu:/var/log/apache2$ sudo iptables --append INPUT -p tcp -d 192.168.56.101 --dport 80 -j ACCEPT
darkenstardragon@VMUbuntu:/var/log/apache2$ sudo iptables --append INPUT -p tcp -s 192.168.56.1 -d 192.168.56.101 --dport 22 -j ACCEPT
darkenstardragon@VMUbuntu:/var/log/apache2$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination
ACCEPT     tcp  --  anywhere              192.168.56.101      tcp dpt:http
ACCEPT     tcp  --  192.168.56.1          192.168.56.101      tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```