Networking using Linux. Lection 2

Networking

- iptables
- DHCP
- DNS
- Q&A.

iptables

All modern operating systems come equipped with a ***firewall*** – a software application that regulates network traffic to a computer. Firewalls create a barrier between a trusted network (like an office network) and an untrusted one (like the internet). Firewalls work by defining rules that govern which traffic is allowed, and which is blocked. The utility firewall developed for Linux systems is ***iptables***.

Prerequisites:

- A user account with sudo privileges
- Access to a terminal window/command line (Ctrl-Alt-T, Ctrl-Alt-F2)

iptables

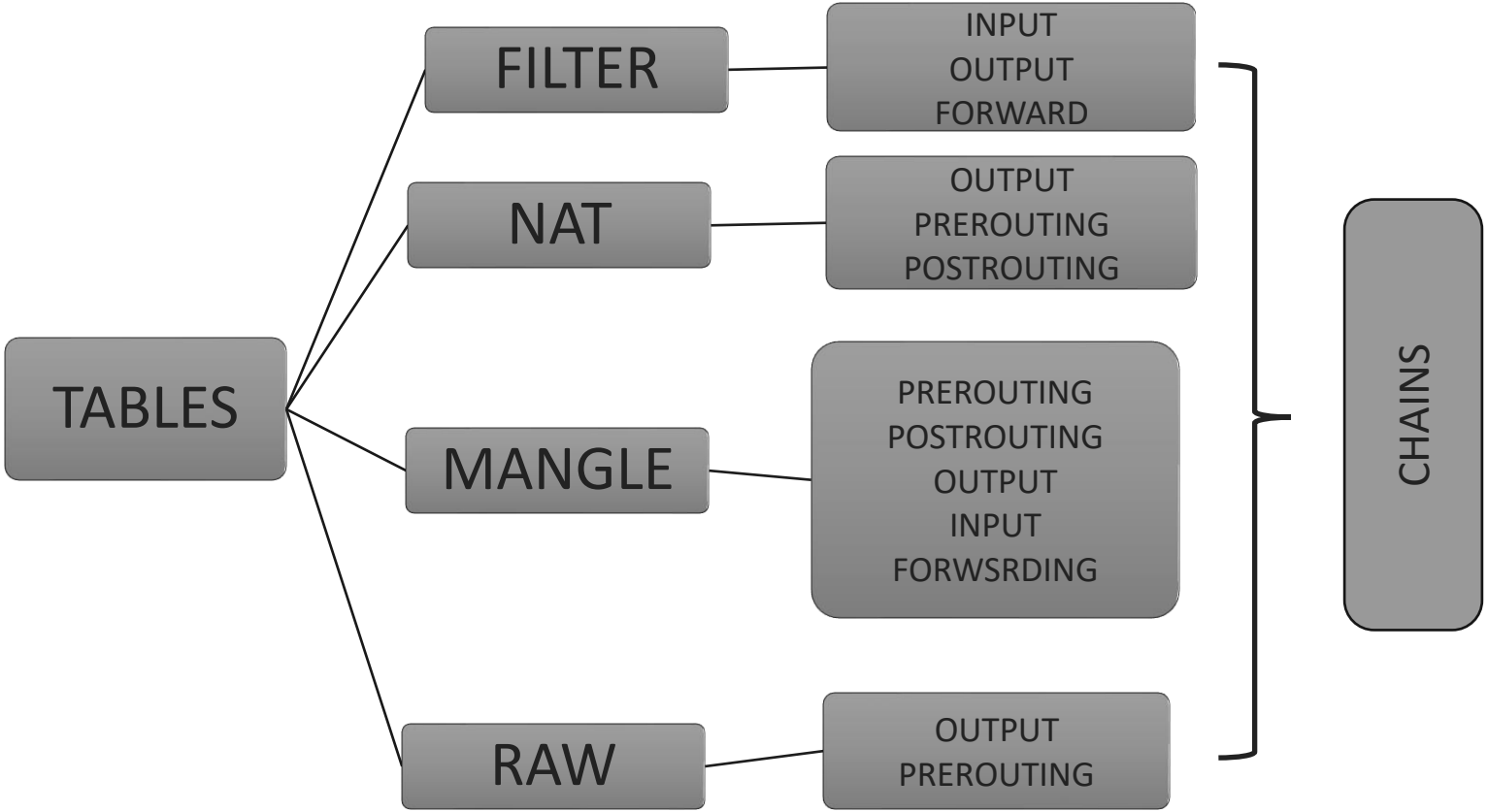
How ***iptables*** work:

Network traffic is made up of packets. Data is broken up into smaller pieces (called packets), sent over a network, then put back together. Iptables identifies the packets received and then uses a set of rules to decide what to do with them.

iptables filters packets based on:

Tables: Tables are files that join similar actions. A table consists of several chains.
Chains: A chain is a string of rules. When a packet is received, ***iptables*** finds the appropriate table, then runs it through the chain of rules until it finds a match.
Rules: A rule is a statement that tells the system what to do with a packet. Rules can block one type of packet, or forward another type of packet. The outcome, where a packet is sent, is called a target.
Targets: A target is a decision of what to do with a packet. Typically, this is to accept it, drop it, or reject it (which sends an error back to the sender).

iptables


TABLES
FILTER
INPUT
OUTPUT
FORWARD
NAT
OUTPUT
PREROUTING
POSTROUTING
MANGLE
PREROUTING
POSTROUTING
OUTPUT
INPUT
FORWSRDING
RAW
OUTPUT
PREROUTING
CHAINS

iptables

Tables and Chains. Linux firewall ***iptables*** has four default tables.

1. ***Filter***

The Filter table is the most frequently used one. It acts as a bouncer, deciding who gets in and out of your network. It has the following default chains:

Input – the rules in this chain control the packets received by the server.

Output – this chain controls the packets for outbound traffic.

Forward – this set of rules controls the packets that are routed through the server.

2. ***Network Address Translation (NAT)***

This table contains NAT (Network Address Translation) rules for routing packets to networks that cannot be accessed directly. When the destination or source of the packet has to be altered, the NAT table is used. It includes the following chains:

Prerouting – this chain assigns packets as soon as the server receives them.

Output – works the same as the output chain we described in the filter table.

Postrouting – the rules in this chain allow making changes to packets after they leave the output chain.

iptables

3. *Mangle*

The Mangle table adjusts the IP header properties of packets. The table has all the following chains we described above:

Prerouting
Postrouting
Output
Input
Forward

4. *Raw*
The Raw table is used to exempt packets from connection tracking. The raw table has two of the chains we previously mentioned:

Prerouting
Output

iptables

Targets

A ***target*** is what happens after a packet matches a rule criteria. The ***targets*** in Linux ***iptables*** are:

Accept – this rule accepts the packets to come through the ***iptables*** firewall.

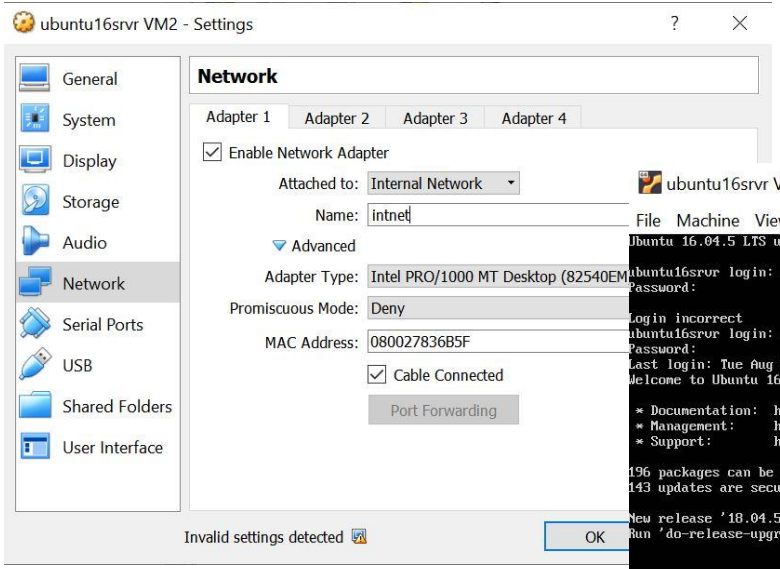
Drop – the dropped package is not matched against any further chain. When Linux ***iptables*** drop an incoming connection to your server, the person trying to connect does not receive an error. It appears as if they are trying to connect to a non-existing machine.

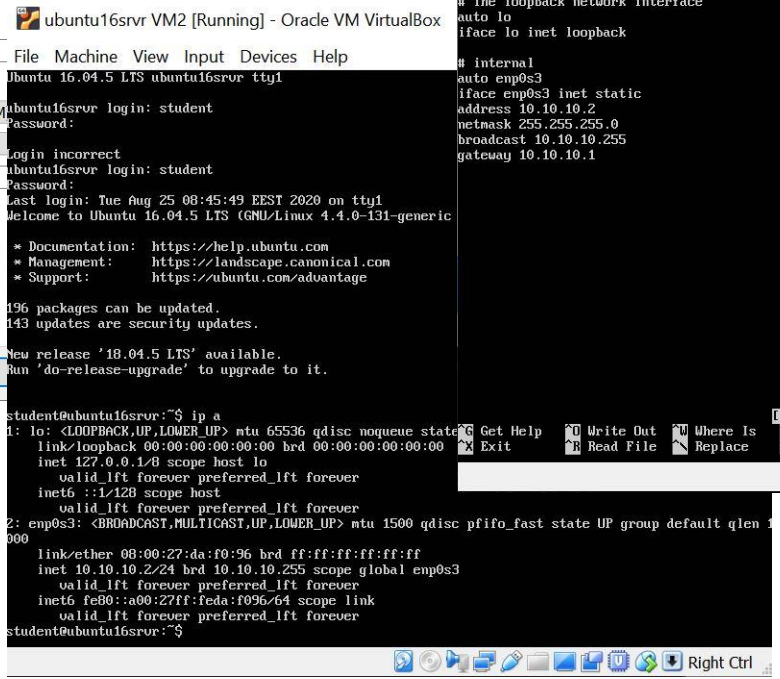
Return – this rule sends the packet back to the originating chain so you can match it against other rules.

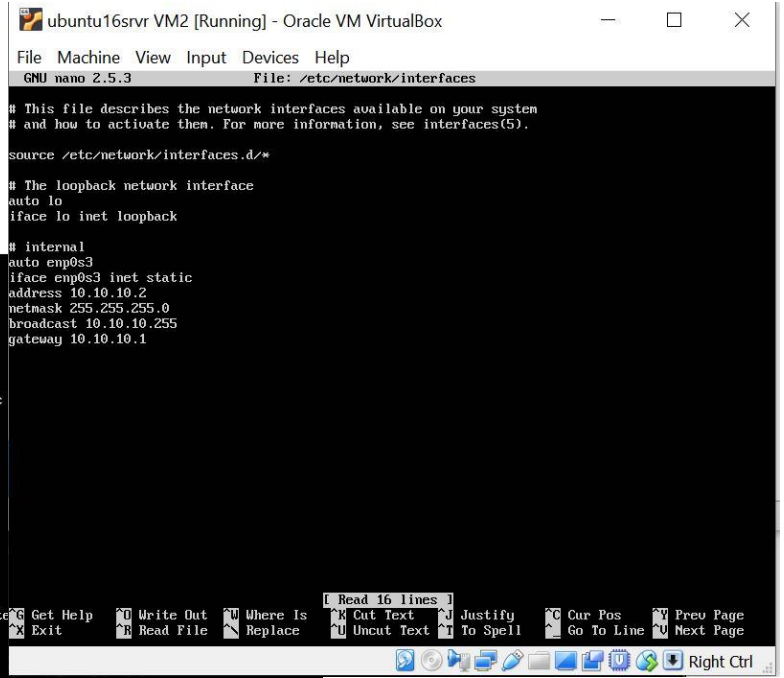
Reject – the ***iptables*** firewall rejects a packet and sends an error to the connecting device.

iptables

Before .....







iptables

Before .....

ubuntu16srvr VM1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
Password:
Last login: Tue Aug 25 07:58:22 EEST 2020 on tty1
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-131-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

196 packages can be updated.
143 updates are security updates.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


student@ubuntu16srvr:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 08:00:27:ac:1b:56 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feac:1b56/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 08:00:27:4c:53:00 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.1/24 brd 10.10.10.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe4c:5300/64 scope link
       valid_lft forever preferred_lft forever
student@ubuntu16srvr:~$
```

Right Ctrl

ubuntu16srvr VM1 [Running] - Oracle VM VirtualBox

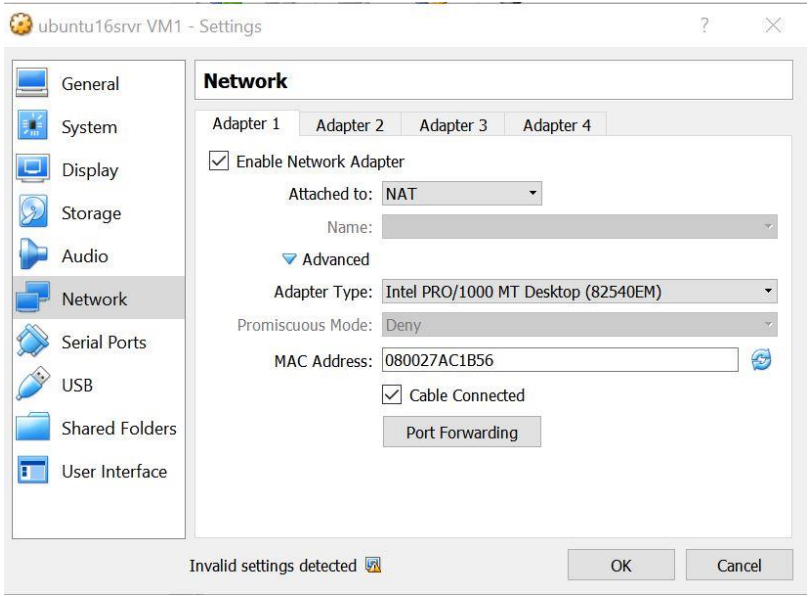
File Machine View Input Devices Help

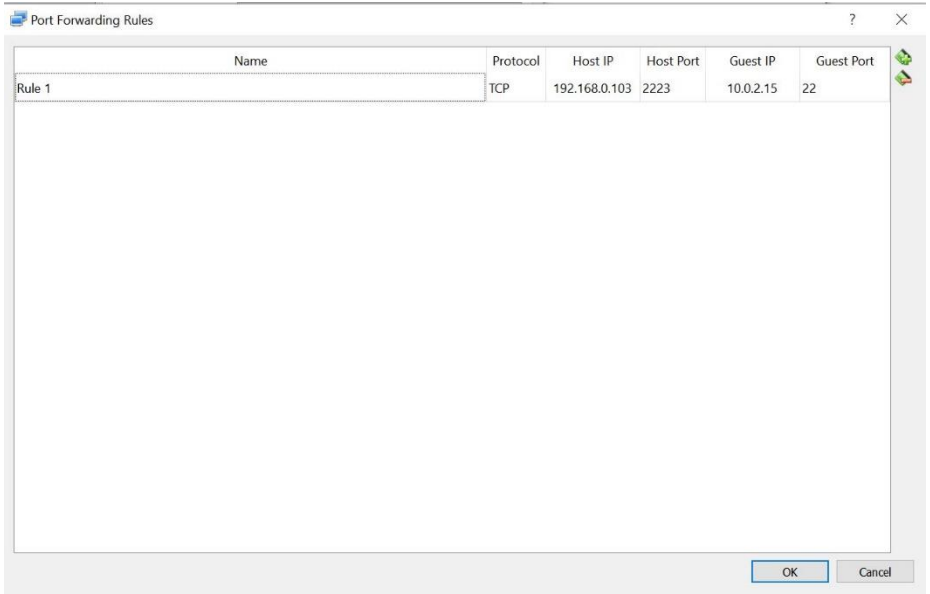
```
  GNU nano 2.5.3                File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# NAT
auto enp0s3
iface enp0s3 inet dhcp

#internal
auto enp0s8
iface enp0s8 inet static
address 10.10.10.1
netmask 255.255.255.0
broadcast 10.10.10.255

                                [ Read 20 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos   ^Y Prev Page
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line ^V Next Page
```

Right Ctrl

iptables

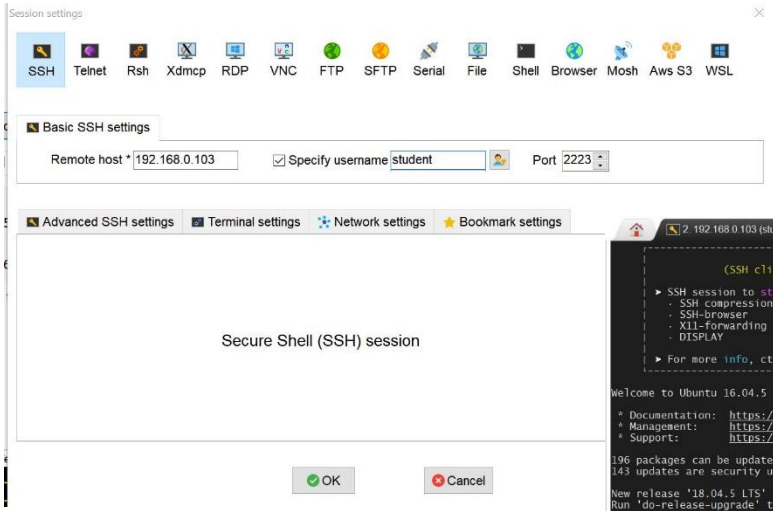
Before .....

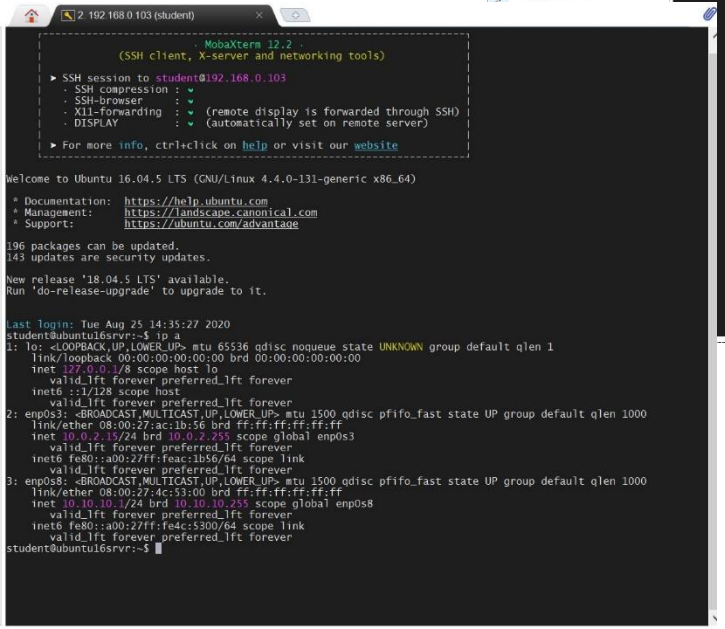


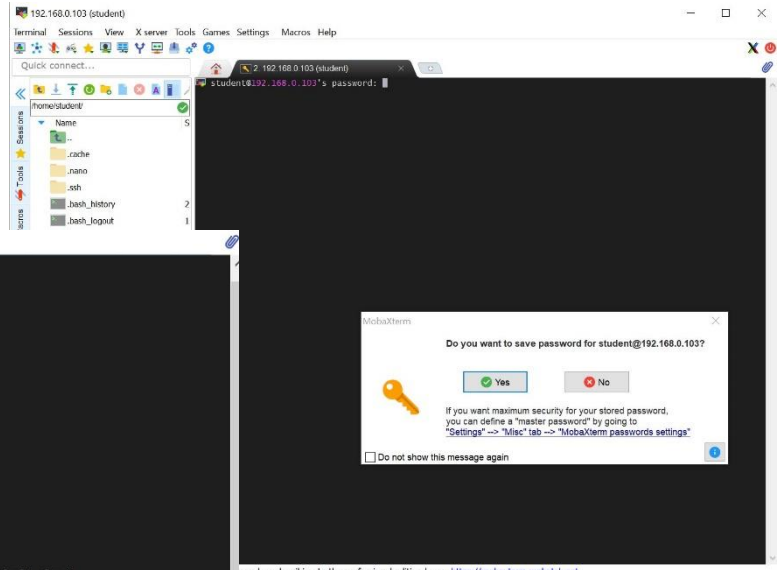


iptables

Before .....







iptables

Now.....

ubuntu16srvr VM1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
student@ubuntu16srvr:~$ iptables
iptables v1.6.0: no command specified
Try `iptables -h' or 'iptables --help' for more information.
student@ubuntu16srvr:~$ sudo apt update
Hit:1 http://ua.archive.ubuntu.com/ubuntu xenial InRelease
Get:2 http://ua.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Get:3 http://ua.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Get:4 http://security.ubuntu.com/ubuntu xenial-security InRelease [109 kB]
Fetched 325 kB in 0s (435 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
190 packages can be upgraded. Run 'apt list --upgradable' to see them.
student@ubuntu16srvr:~$ _
```

Right Ctrl

2. 192.168.0.103 (student) | 3. 192.168.0.103 (student)

```
GNU nano 2.5.3                File: /etc/sysctl.conf                    Modified

#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

###############################################################3
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1


###################################################################
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
#net.ipv4.conf.all.accept_redirects = 0
#net.ipv6.conf.all.accept_redirects = 0
# _or_
# Accept ICMP redirects only for gateways listed in our default
# gateway list (enabled by default)

^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   ^Y Prev Page   M-\ First Line
^X Exit       ^R Read File   ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line ^V Next Page   M-/ Last Line
```

iptables

Now.....

4. 192.168.0.103 (student)

```
· MobaXterm 12.2 ·
(SSH client, X-server and networking tools)

➤ SSH session to student@192.168.0.103
  · SSH compression : ✓
  · SSH-browser     : ✓
  · X11-forwarding  : ✓  (remote display is forwarded through SSH)
  · DISPLAY         : ✓  (automatically set on remote server)

➤ For more info, ctrl+click on help or visit our website

Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-131-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

196 packages can be updated.
143 updates are security updates.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Tue Aug 25 15:18:12 2020
student@ubuntu16srvr:~$ sudo iptables -S
[sudo] password for student:
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
student@ubuntu16srvr:~$ sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
student@ubuntu16srvr:~$ sudo iptables -A FORWARD -i enp0s8 -o enp0s3 -m state --state RELATED,ESTABLISHED -j ACCEPT
student@ubuntu16srvr:~$ sudo iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT
student@ubuntu16srvr:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A FORWARD -i enp0s8 -o enp0s3 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT
student@ubuntu16srvr:~$
```

iptables

Now.....

ubuntu16srvr VM1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
Ubuntu 16.04.5 LTS ubuntu16srvr tty1

ubuntu16srvr login: student
Password:
Last login: Tue Aug 25 15:14:43 EEST 2020 from 10.0.2.2 on pts/0
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-131-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

196 packages can be updated.
143 updates are security updates.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


student@ubuntu16srvr:~$ sudo iptables -S
[sudo] password for student:
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
student@ubuntu16srvr:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A FORWARD -i enp0s8 -o enp0s3 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT
student@ubuntu16srvr:~$ _
```

Right Ctrl

ubuntu16srvr VM2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
student@ubuntu16srvr:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.10.10.1      0.0.0.0         UG    0      0        0 enp0s3
10.10.10.0      *               255.255.255.0   U     0      0        0 enp0s3
student@ubuntu16srvr:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=21.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=21.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=22.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=23.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=116 time=22.8 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=116 time=24.6 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 21.741/22.921/24.667/1.022 ms
student@ubuntu16srvr:~$
```

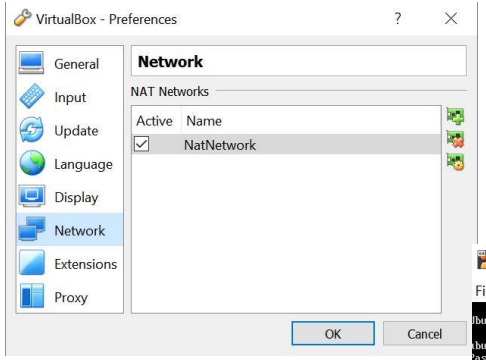
To make changes persistent some action should be done…

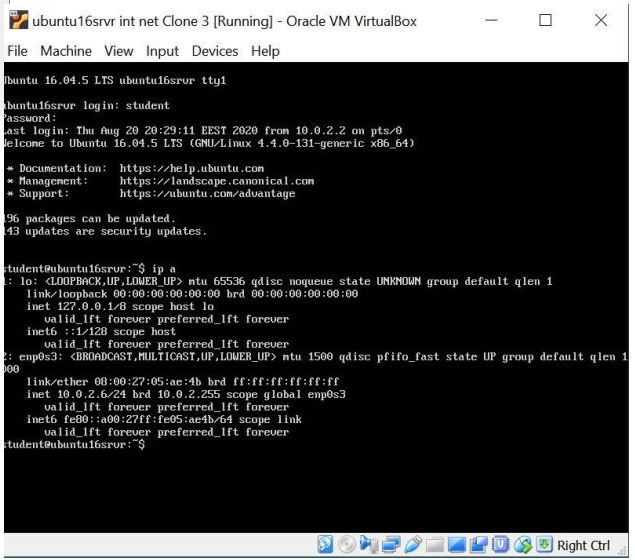
DHCP

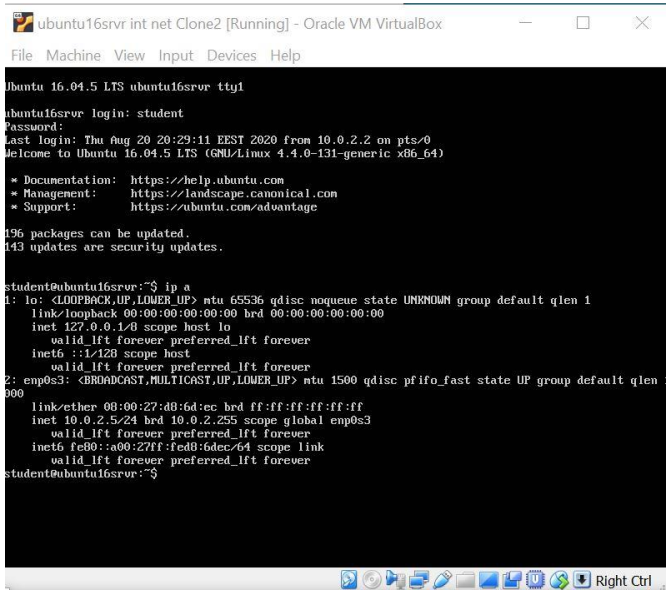
In computer science, the Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks, whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on the network, so they can communicate with other IP networks. A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider (ISP), reducing the need for a network administrator or a user to manually assign IP addresses to all network devices.

DHCP

VB DHCP on NAT Networks







DHCP

DHCP installation and configuring

1. The Internet Systems Consortium (ISC) Dynamic Host Configuration Protocol (DHCP) server is free, open-source, and easy to install. Both enterprises and small networks have used ISC DHCP in production for many years.

2. Dnsmasq is a lightweight, easy to configure, DNS forwarder and DHCP server. It is designed to provide DNS and optionally, DHCP, to a small network. It can serve the names of local machines which are not in the global DNS. The DHCP server integrates with the DNS server and allows machines with DHCP-allocated addresses to appear in the DNS with names configured either in each host or in a central configuration file. Dnsmasq supports static and dynamic DHCP leases and BOOTP/TFTP for network booting of diskless machines

DHCP

Dnsmasq installation and configuring:

> apt-get update
> apt-get install dnsmasq

ubuntu16srvr internal network Clone1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
GNU nano 2.5.3                    File: /etc/dnsmasq.conf

# and this sets the source (ie local) address used to talk to
# 10.1.2.3 to 192.168.1.1 port 55 (there must be a interface with that
# IP on the machine, obviously).
# server=10.1.2.3@192.168.1.1#55

# If you want dnsmasq to change uid and gid to something other
# than the default, edit the following lines.
#user=
#group=

# If you want dnsmasq to listen for DHCP and DNS requests only on
# specified interfaces (and the loopback) give the name of the
# interface (eg eth0) here.
# Repeat the line for more than one interface.
interface=enp0s3
```

ubuntu16srvr internal network Clone1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
GNU nano 2.5.3                    File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
address 10.10.10.1
netmask 255.255.255.0
```

ubuntu16srvr internal network Clone1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
GNU nano 2.5.3                    File: /etc/dnsmasq.conf

# Uncomment this to enable the integrated DHCP server, you need
# to supply the range of addresses available for lease and optionally
# a lease time. If you have more than one network, you will need to
# repeat this for each network on which you want to supply DHCP
# service.
dhcp-range=10.10.10.10,10.10.10.20,12h
```

DHCP

Dnsmasq installation and configuring:

ubuntu16srvr int net Clone 3 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
GNU nano 2.5.3                File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet dhcp
```

ubuntu16srvr int net Clone 3 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
student@ubuntu16srvr:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 08:00:27:05:ae:4b brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.10/24 brd 10.10.10.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe05:ae4b/64 scope link
       valid_lft forever preferred_lft forever
student@ubuntu16srvr:~$ _
```

ubuntu16srvr int net Clone2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
GNU nano 2.5.3                File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet dhcp
```

ubuntu16srvr int net Clone2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
student@ubuntu16srvr:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
    link/ether 08:00:27:d8:6d:ec brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.15/24 brd 10.10.10.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed8:6dec/64 scope link
       valid_lft forever preferred_lft forever
student@ubuntu16srvr:~$
```