

Computer & Network Lab 3

Professor Dr. Ronny Bull

February 8, 2019

Zuhair Hallak

Abstract

After the set up I configured for my router system of having two network interface which was public interface Ens18 (B class subnet mask) and private interface Ens19 (C class subnet mask). I also, configured Ens18 for my kali virtual machine and gave it IP address. I have been able to ping both this virtual system without any problems. Our next step is being able to access chewy from any place such on our terminal computer. I'm going to forward three ports to desired IP Address. I need to allow ssh port 22 on Kali virtual machine and drop everything else using iptables. We need to make our directory and save the iptables rules as permanent. On my web server virtual system, we need to enable firewalld and set up Ens18 network by giving it IP Address then allow three ports which are 22, 80, 443.

Processes involved in completing the lab:

I have accessed my console for Web virtual system from the VLE web interface and logged into my root user. The first step, is to set up ens18 on the web server and give it IP address. I'm going to open it into vim and config the file calling it ens18. Step two, I went to my router virtual system and used this command below. We forward ssh 22 port to our kali IP address, port 80 http to IP address of web and port 443 to IP address of web virtual system.

Step 1:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth18
:i to insert
:w - saved the config file
:q! and press enter - quits from the editor
systemctl restart network
```

Step 2:

```
firewall-cmd --zone=external --add-forward port=port22:proto=tcp:toport=22:toaddr=192.168.0.2
systemctl restart firewalld
firewall-cmd --zone=external --list-all (list all the ports of external)
```

```
TYPE=Ethernet
BOOTPROTO=static
IPADDR=192.168.0.1
NETMASK=255.255.255.0
GATEWAY=192.168.0.1
DNS=10.42.0.30
ONBOOT=yes
NAME=ens18
DEVICE=ens18
DEFROUTE=yes
PEERDNS=yes
PEERROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_FAILURE_FATAL=no
NAME=ens18
DEVICE=ens18
ZONE=external
```

```
root@schubert:~# firewall-cmd --zone=external --list-all
external (active)
  interfaces: ens18
  sources:
  services: http https ssh
  ports: 443/tcp 80/tcp 22/tcp
  masquerade: yes
  forward-ports:
  icmp-blocks:
  rich rules:
```

Step 3:

The third step, I started enabling firewalld on the web server to protect the local host based system but not entire network.

```
sudo systemctl start firewalld
sudo systemctl enable firewalld
sudo systemctl status firewalld
```

```
root@schubert:~# sudo systemctl start firewalld
root@schubert:~# sudo systemctl enable firewalld
root@schubert:~# systemctl status firewalld
firewalld.service - firewalld - dynamic firewall daemon
Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
Active: active (running) since Wed 2015-01-30 10:19:21 EST; 1min 57s ago
Main PID: 5966 (firewalld)
CGroup: /system.slice/firewalld.service
          └─5966 /usr/sbin/python -Es /usr/sbin/firewalld --no-daemon --pid

* 30 10:19:20 schubert systemd[1]: Starting firewalld - dynamic firewall daemon.
* 30 10:19:21 schubert systemd[1]: Started firewalld - dynamic firewall daemon.
* 30 10:19:21 schubert:
```

Step 4:

The fourth step, is going to allow 3 ports on my web server after seeing up firewalld. We need to make sure that is permanent because if we reboot the web server the ports won't be deleted.

```
firewall-cmd --zone=external --permanent --add-port=433/tcp
firewall-cmd --zone=external --permanent --add-port=80/tcp
firewall-cmd --zone=external --permanent --add-port=22/tcp
sudo systemctl restart firewalld
firewall-cmd --zone=external --list-all
```

```
root@zuhalrWeb ~# firewall-cmd --zone=external --list-all
external (active)
  interfaces: ens18
  sources:
  services: http https ssh
  ports: 443/tcp 80/tcp 22/tcp
  masquerade: yes
  forward-ports:
  icmp-blocks:
  rich rules:

root@zuhalrWeb ~# firewall-cmd --zone=external --permanent --add-port=443/tcp
```

Step 5:

I have tried to ssh into my

kali and it would not let me in by root password. I had to go to the config file edit using vim. I saw title called Log in Authentication. I removed the # number symbol from the root login password.

```
vim /etc/ssh/sshd_config
systemctl restart sshd
systemctl status ssh
```

```
root@kali:~# vim /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.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#KexAlgo /etc/ssh/ssh_host_rsa_key
#KexAlgo /etc/ssh/ssh_host_ecdsa_key
#KexAlgo /etc/ssh/ssh_host_ed25519_key

#Ciphers and keying
#RekeyLimit default none

#Logging
#SyslogFacility AUTH
#LogLevel INFO

#Authentication:
#LoginGraceTime 3m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 4

#etc/ssh/sshd_config" 1224, 3244C
```

```
root@kali:~# systemctl restart sshd
root@kali:~# systemctl status sshd
sshd.service: sshd is running
root@kali:~#
```

Step 6:

We are going to edit bash script by using this commands. We are going to use this phrase *ssh web* to connect automatically to our web server using its IP Address

```
ls -a
vim .bashrc
Restart the terminal
```

```
root@kali:~# vim .bashrc
root@kali:~#
```

```
root@kali:~# ssh web
root@192.168.0.3's password:
root@kali:~#
```

Step 7

I was able to ssh into my chewy using my computer terminal to my kali system using its IP address.

```

root@kali:~# ssh zuhair@chewy.cs.utica.edu
Please direct all support requests to: csadmin@utica.edu NHT IITS!

The Utica College Computer Science department is now on Discord! Check it
out for access to dedicated chat rooms for courses and faster csadmin support.

The invite link is: https://discord.gg/5r2zWEA

Password:
Last login: Fri Feb  8 04:43:37 2019 from cpe-67-242-48-44.twcnv.net.rr.com
[zuhair@chewy ~]$ ssh darknet
zuhair@darknet's password:
Last login: Fri Feb  8 04:44:18 2019 from chewy.cs.utica.edu
[zuhair@darknet-ssh ~]$ ssh root@172.16.42.107
root@172.16.42.107's password:

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Feb  8 03:05:41 2019 from 192.168.0.3
root@kali-vi-#

```

Step 8:

We need to add three port to the iptables

iptables -L

iptables -A INPUT -p tcp --dport ssh -j ACCEPT

iptables -A INPUT -m conntrack --ctstate ESTABLISHED, RELATED -j ACCEPT

iptables -P INPUT DROP

Step 9:

cd /etc/network/if-post-down.d/iptables (flushing iptables-save)

chmod a+x iptables

cd /etc/network/if-pre-up.d/iptables (bring up iptables save)

chmod a+x iptables

iptables-save > /etc/iptables/iptables.rules

iptables -F

iptables-restore < /etc/iptables/iptables.rules

if-post-down.d/iptables (

service networking stop

service networking start

```

root@kali-vi-# iptables -F
root@kali-vi-# iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source                destination

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
root@kali-vi-#

```

```

root@kali-vi-# ssh zuhair@chewy.cs.utica.edu
[zuhair@darknet-ssh ~]$ ssh root@172.16.42.107
root@172.16.42.107's password:

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Feb  8 03:06:32 2019 from 172.16.42.1
root@kali-vi-# iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
ACCEPT    tcp  --  anywhere              anywhere           tcp options
ESTABLISHED all  --  anywhere              anywhere
DROP      all  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
root@kali-vi-#

```

```

root@kali:~# cat /etc/network/interfaces
auto lo
iface lo inet loopback

root@kali:~# cat /etc/network/if-post-down.d/service_networking_stop
root@kali:~# cat /etc/network/if-post-down.d/iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

root@kali:~# cat /etc/network/if-post-down.d/service_networking_start
root@kali:~# cat /etc/network/if-post-down.d/iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

```

```

root@kali:~# cat /etc/network/if-pre-up.d/service_networking_start
root@kali:~# cat /etc/network/if-pre-up.d/iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

```

```

root@kali:~# cat /etc/network/if-pre-up.d/service_networking_start
root@kali:~# cat /etc/network/if-pre-up.d/iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

```

```

root@kali:~# cat /etc/network/if-pre-up.d/service_networking_start
root@kali:~# cat /etc/network/if-pre-up.d/iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

```

Able to Access Kali from web server

Identification of any issues or delays as well as resolutions:

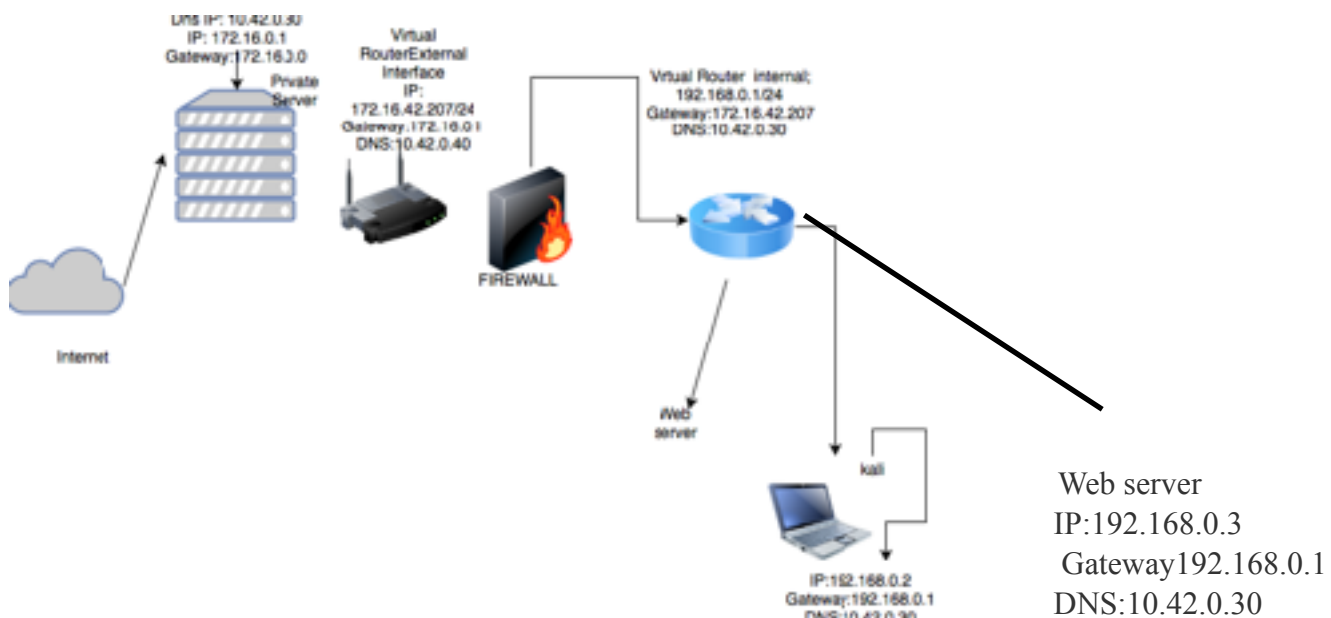
I had b class section subnet in my ens18 which made me not being able to ssh into my kali. I went to my ens18 file and I edit it using vim. I changed my subnet to 255.255.0.0. I was able to ssh with no problem. I had difficult of being able to solve this lab. I did not know where to start such as it had forward port command that you are suppose to use in your router and never said about you need to do it three times. Also, the web server ens18 network should be set up first before going to the router and forwarding the ports. That was little bit confusing of what I should get things done.

```

root@zuhallak ~# ifconfig
ens18: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.42.207 netmask 255.255.255.255 broadcast 172.16.42.207
    inet6 fe80::8c13:38ff:fe53:ee63 prefixlen 64 scopeid 0x20<link>
    ether 8c:13:38:53:ee:63 txqueuelen 1000 (Ethernet)
    RX packets 29186 bytes 38307654 (36.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4593 bytes 335621 (327.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

NETWORK DIAGRAM:



Conclusion:

The Lab 3 was completed successful after that delay that occurred by not being able to set up iptables, ssh into my kali, configuring end 18 into web server, and in which system do I forward the ports to.

Reference:

<https://wreckedsecurity.com/secure-communication/how-to-make-kali-linux-iptables-firewall-persistent/>

https://docs.fedoraproject.org/en-US/Fedora/19/html/Security_Guide/sec-Configure_Port_Forwarding-CLI.html

<https://www.cyberciti.biz/faq/howto-start-stop-ssh-server/>

<https://superuser.com/questions/808496/difference-between-iptables-default-policy-to-drop-and-inserting-a-seperate-po>

<https://www.thegeekstuff.com/2011/02/iptables-add-rule/>

<https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-firewalld-on-centos-7>

<https://support.rackspace.com/how-to/connecting-to-a-server-using-ssh-on-linux-or-mac-os/>