Computer & Network Lab 3

Professor Dr. Ronny Bull

February 8, 2019

Zuhair Hallak

Abstract

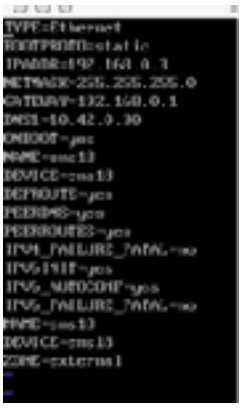
After the set up I configured for my router system of having two network interface which was public interface Ens18 (B class subnet mask) and private interface Ens19 (C class subnet mask). I also, configured Ens18 for my kali virtual machine and gave it IP address. I have been able to ping both this 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.

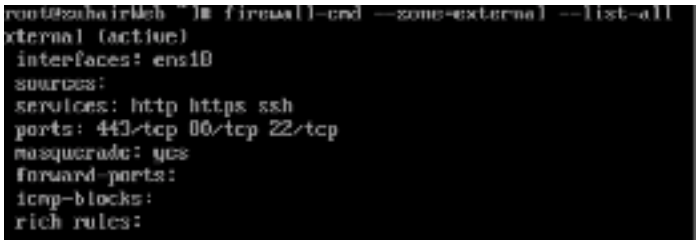
Processes involved in completing the lab:

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.

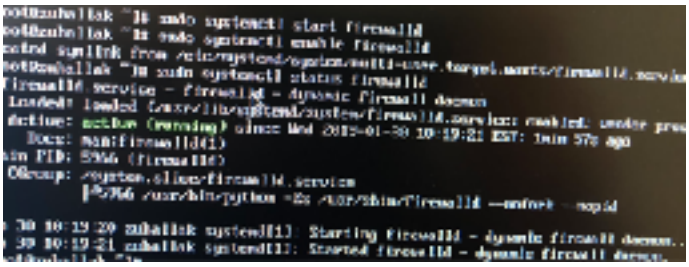
Step 1:
vi /etc/sysconfig/network-scripts/ifcfg-eth18
:i to insert
:w - saved the config file
:q! and press enter - quits from the editor
systemctl restart network

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)





Step 3:
The third step, I started enabling firewalld on the web server to protect the local host based system but not not entire network.
sudo systemctl start firewalld
sudo systemctl enable firewalld
sudo systemctl status firewalld



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

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

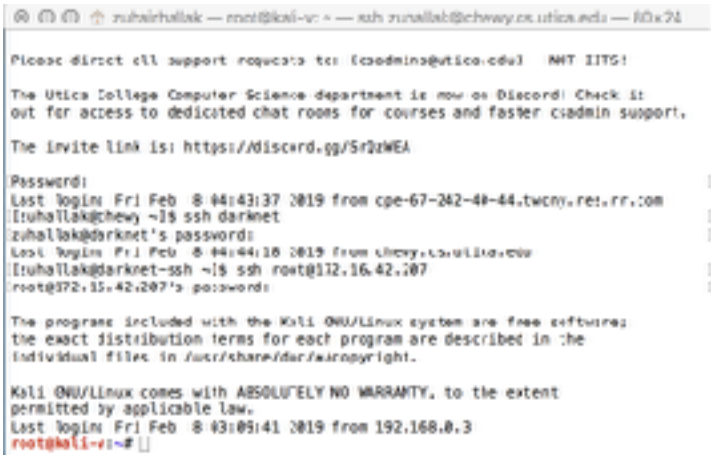
Step 6:

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

Step 7

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



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

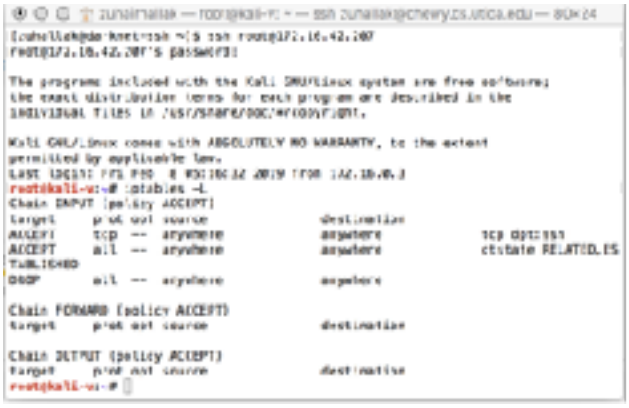
iptables -F

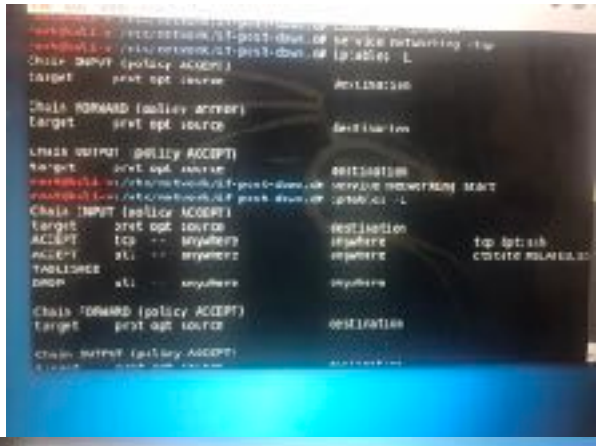
iptables-restore < /etc/iptables/iptables.rules

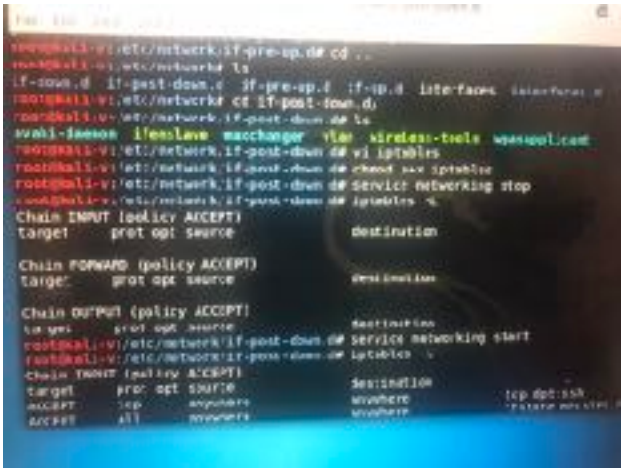
if-post-down.d/iptables (

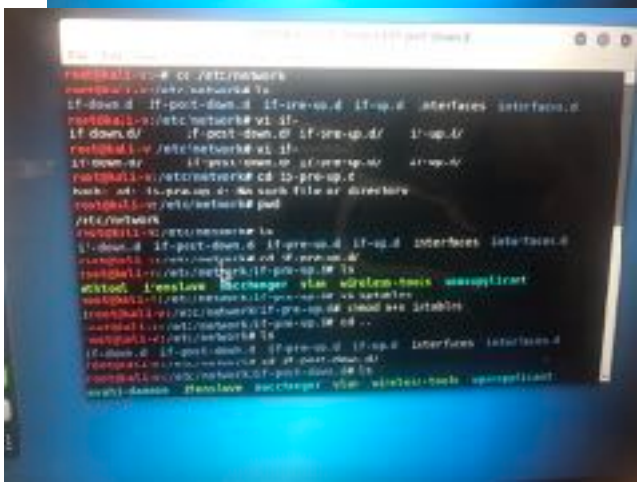
service networking stop

service networking start





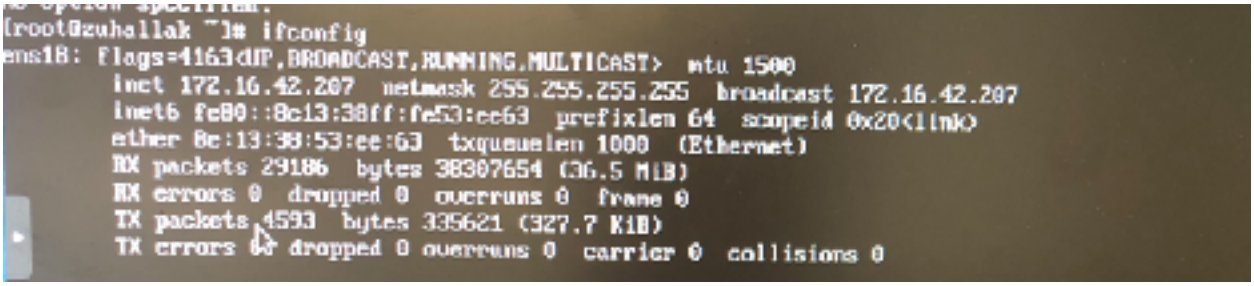




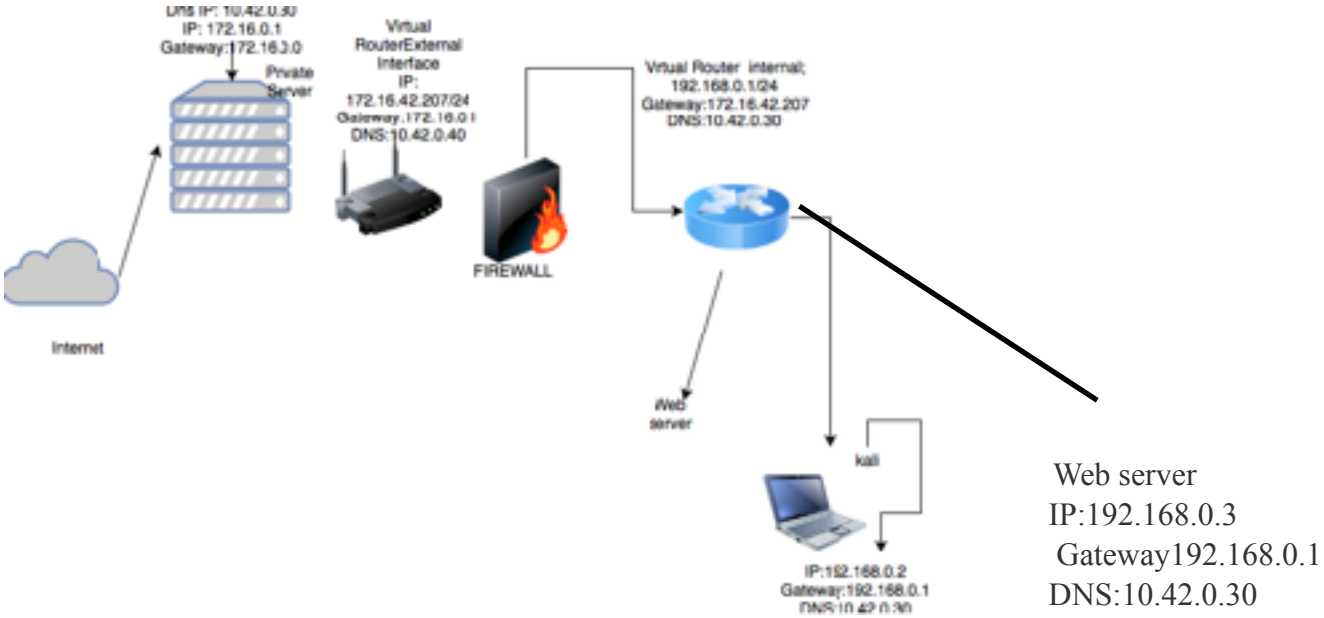
Able to Access Kali from web server

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.



NETWORK DIAGRAM:



Web server
IP:192.168.0.3
Gateway192.168.0.1
DNS:10.42.0.30

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/