# NETW240 Lab : Configure iptables in Linux

Lab Scenario

Assignment

The purpose of this lab is to configure an iptables firewall in Linux. Use the IP addresses that exist when you start Linux.

Virtual Machine Login Information for PLABFED01 and PLABFED02

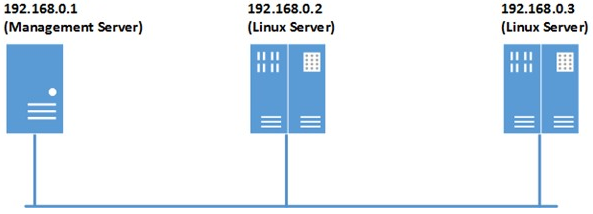
Username: Student   
Password: Password

Username: root   
Password: Password

Lab Diagram

During your session you will have access to the following lab configuration.

WINCONSOLE PLABFED01 PLABFED02



The Linux servers also connect to a private network. The IP address of PLABFED01 is 192.168.240.11 and. The IP address of PLABFED02 is 192.168.240.12.

Connecting to your lab

In this module you will be working on the following equipment to carry out the steps defined in each exercise.

* WINCONSOLE (Management Server)
* PLABFED01 (Linux Server)
* PLABFED02 (Linux Server)

Each exercise will detail which console you are required to work on to carry out the steps.

To start simply click on the named Server from the device list (located on the left hand side of the screen) and click the Power on from the in tools bar. In some cases the devices may power on automatically.

During the boot up process an activity indicator will be displayed in the name tab:

* Black - Powered Off
* Orange - Working on your request
* Green - Ready to access

If the remote console is not displayed automatically in the main window (or popup) click the Connect icon located in the tools bar to start your session.

If the remote console does not appear please try the following option:

* Switch between the HTML 5 and Java client versions in the tools bar.

In the event this does not resolve your connectivity problems please visit our Help / Support pages for additional resolution options.

Iptables Firewall Configuration Step-By-Step

###### General information:

This Linux based firewall is controlled by two programs:

* iptables to handles filtering for IPv4
* ip6tables handles filtering for IPv6

IPTables main files are:

* /etc/sysconfig/iptables – where rule set are saved.
* /sbin/iptables – binary.

At present, there are total four chains:

* INPUT : Default chain originating to system.
* OUTPUT : Default chain generating from system.
* FORWARD : Default chain packets are send through another interface.
* RH-Firewall-1-INPUT : The user-defined custom chain.

Packet Matching Rules

* Each packet starts at the first rule in the chain.
* A packet proceeds until it matches a rule.
* If a match found, then control will jump to the specified target (such as REJECT, ACCEPT, DROP).

Target Meanings

* The target ACCEPT means allow packet.
* The target REJECT means to drop the packet and send an error message to remote host.
* The target DROP means drop the packet and do not send an error message to remote host or sending host.

TASK A: Configure Iptables Firewall

We are going to configure the iptables. Logon to the PLABFED01 as root and type the following commands.

Note: The # symbol before each command is the PROMPT of the root account. Do not type it.

Step 1: To use the iptables service, disable firewalld by typing the following commands:

#systemctl disable firewalld

#systemctl stop firewalld

Step 2: Make sure to install iptables, type the following commands:

#yum -y install iptables-services

#rpm –q iptables

Step 3: To install system-config-firewall tool type the following commands:

#yum -y install system-config-firewall

Step 4: To execute system-config-firewall tool type the following command:

#system-config-firewall

A Firewall Configuration window will pop-up

1. Click on Wizard button on the top left corner.
2. Leave the “Information” page and click on Forward.
3. For Firewall Setting, keep default “system with network access” and click on Forward.
4. For user skill level, keep default “Beginner” and click on forward,
5. For Configuration, select Load “Server” configuration and click on OK, then Click on Apply button on the top left corner and click on YES.
6. Click on X to Close the Firewall Configuration.

To make sure that the rules set were setup, type the following command:

#ls /etc/sysconfig/iptables

If it says “ No such file or directory” you have to execute the system-config-firewall tool in Step 4 again.

The file /etc/sysconfig/iptables is the default rule set.

Step 5: To turn on firewall type the following commands:

#systemctl start iptables

#systemctl enable iptables

Step 6: To check status of the firewall type the following command:

#systemctl status iptables

Note:The below commands are for reference

* To start the firewall type the following command:

#systemctl start iptables

* To restart the firewall type the following command:

#systemctl restart iptables

* To stop the firewall type the following command:

#systemctl stop iptables

* To check status of the firewall type the following command:

#systemctl status iptables

TASK B: Practice manipulating iptables

We are still logged on to the PLABFED01 as root and type along the following commands and observe the outputs.

Step 1: To display default rules with line numbers type the following command:

#iptables --line-numbers -n -L

Note: You can use line numbers to delete or insert new rules into the firewall.

Step 2: To display the status of the firewall type the following command:

#iptables -L -n -v

Where: -L : List rules.

-v : Display detailed information.

-n : Display IP address and port in numeric format.

Step 3: To display INPUT or OUTPUT chain rules, type the following commands:

#iptables -L INPUT -n -v

#iptables -L OUTPUT -n -v --line-numbers

Step 4: You can use the iptables command itself to stop the firewall and delete all rules:

#iptables -F

#iptables –X

Where: -F : Deleting (flushing) all the rules.

-X : Delete chain.

Restore firewall rules from the file /etc/sysconfig/iptables after fluhsing, type:

#systemctl restart iptables

Step 5: To delete a rule on line number 4 and verify it, type the following commands:

#iptables --line-numbers -n -L

#iptables -D INPUT 4

#iptables --line-numbers -n -L

Step 6: To insert rule between 1 and 2, type the following commands:

#iptables -I INPUT 2 -s 202.54.1.2 -j DROP

#iptables --line-numbers -n -L

Step 7:To block an attacker’s ip address called 1.2.3.4, type the following commands:

#iptables -A INPUT -s 1.2.3.4 -j DROP

#iptables --line-numbers -n -L

Step 8: You can use the iptables command itself to stop the firewall and **delete all the rules**:

#iptables -F

Where: -F : Deleting (**flushing**) all the rules.

#iptables --line-numbers -n -L

Step 9: To stop the firewall type the following command:

#systemctl stop iptables

Step 10: To restore firewall rules from the file /etc/sysconfig/iptables, type:

#systemctl restart iptables

Step 11: To save firewall rules in /etc/sysconfig/iptables, type the following command:

#iptables-save

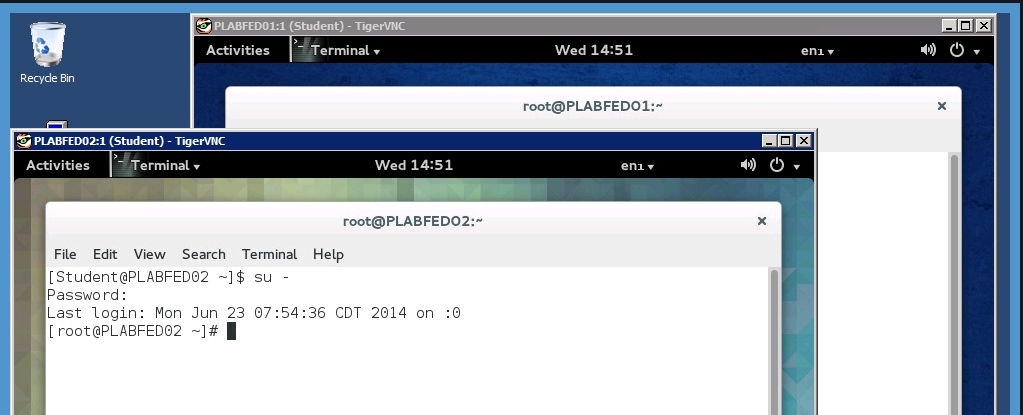
**Note 1):** In this case we did not add more rules since the restart of iptables, the content of the file /etc/sysconfig/iptables does not change.

**Note 2):** If the file /etc/sysconfig/iptables is corrupted, just redo the TASK A Step 4, it will generate a new default rule file.

**Note 3) :** To see more details on iptables’ options type “man iptables”

TASK C: Experiment rules

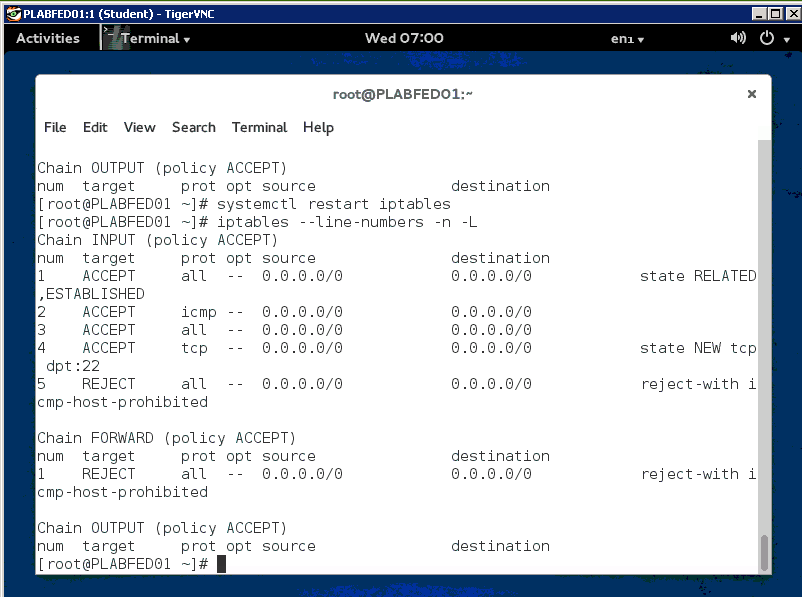
These lab scenarios are focusing on using iptables to improve the security of PLABFED01 Linux server. We use the PLABFED02 Linux server for testing. This part of the lab will require you to switch back and forth between two Linux systems. So logon each system, open a terminal window and switch user to root. From there you can use the mouse to select a system. See example below:



Step 1: On PLABFED01: To restore the default firewall rules (restart) type the following command:

#systemctl restart iptables

The below is the listing of the default iptables rule set



Step 2: On PLABFED01: Look at the INPUT chain, the rule on line number 5 rejects the telnet connections.

* Your task is to delete line number 5 and display the list of iptables with line numbers
* ***Capture the Linux desktop and save this image to your Lab Report document in the space allocated for the modified rule set.***

Step 3: On PLABFED02: Check whether telnet connections to PLABFED01 are possible.

* From PLABFED02 telnet to PLABFED01 and logon as Student with the password Password.
* ***Capture the Linux desktop and save this image to your Lab Report document in the space allocated for the telnet session from PLABFED2.***

Step 4: On PLABFED01: We want to setup the iptables to reject telnet connections.

* Your task is to **Flush (delete)** all the rules and **add** the following rule and display the list of iptables.

#iptables –A INPUT –p tcp –-dport 23 –j DROP

* ***Capture the Linux desktop and save this image to your Lab Report document in the space allocated for the modified rule set.***

Step 5: On PLABFED02: Check whether telnet connections to PLABFED01 are still possible.

* From PLABFED02 telnet to PLABFED01 and logon as Student with the password Password.
* ***Capture the Linux desktop and save this image to your Lab Report document in the space allocated for the telnet session from PLABFED2.***

This concludes lab 7