Firewalling

1. Introduction

 A traditional packet filter is one of the basic protection mechanisms for a network. This type of firewall can be installed and configured in several ways, depending upon the level of protection needed. In this assignment, you will explore how to configure a firewall. As usual, you will be using Linux as your base operating system; you'll use *iptables* to make it act as a firewall.

Prerequisites:
Read about *iptables* from the following links:
https://help.ubuntu.com/community/IptablesHowTo

http://www.linuxhomenetworking.com/wiki/index.php/
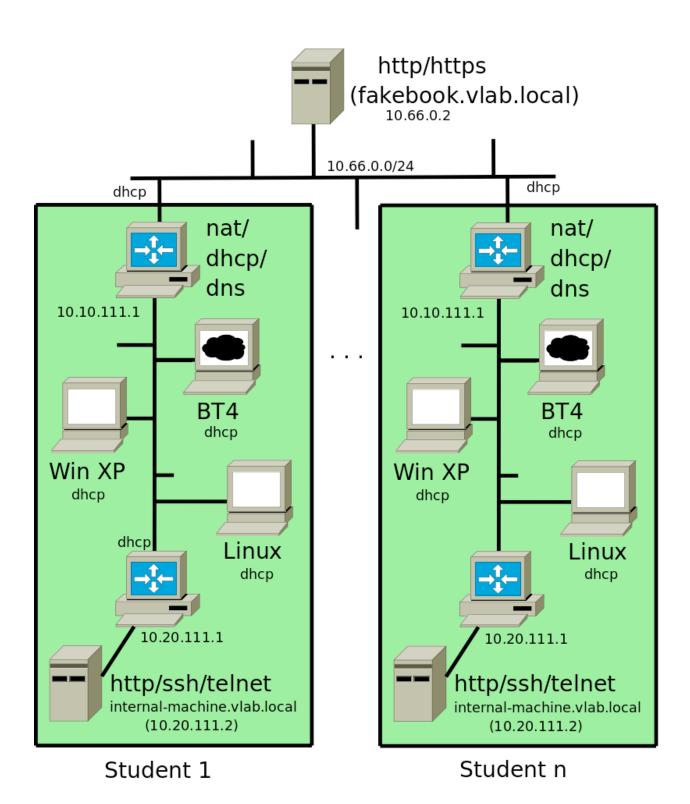Quick_HOWTO_: Ch14_: Linux_Firewalls_Using_iptables

A firewall configuration tool can be found at:
> http://easyfwgen.morizot.net/

Note: ipchains is NOT iptables. Ipchains is an earlier version of a Linux firewall created by the same author. It uses much of the same terminology but processes IP packets differently especially in the processing of forwarded packets.

2. Lab Setup

This lab consists of an internal machine and firewall running iptables along with external machines running WinXP, Linux and Backtrack.   See diagram below.   For the purposes of this lab we won't be using the router at 10.10.111.1 nor the "fakebook" web server. However, you are welcome to use these machines for testing if you wish.   All Firewall and NAT operations must be performed on the 10.20.111.1 firewall.   If you perform the operations on the other firewall you will receive zero points.

http/https
(fakebook.vlab.local)
10.66.0.2

10.66.0.0/24

dhcp

dhcp

nat/
dhcp/
dns

10.10.111.1

BT4
dhcp

Win XP
dhcp

Linux
dhcp

dhcp

10.20.111.1

http/ssh/telnet
internal-machine.vlab.local
(10.20.111.2)

Student 1

nat/
dhcp/
dns

10.10.111.1

BT4
dhcp

Win XP
dhcp

Linux
dhcp

10.20.111.1

http/ssh/telnet
internal-machine.vlab.local
(10.20.111.2)

Student n

. . .

2.1. Part A

Configure the iptables firewall on the network firewall machine to implement the following firewall policy:

For outgoing traffic (from inside to outside) - your internal machine should be able to communicate with the external network and the external machines without restrictions.

For incoming traffic (from the outside to the inside) - all incoming connection requests should be rejected with the following exceptions:

1) The internal machine should respond to a ping from the external machines
2) The internal machine should accept all incoming SSH and http requests from the network 10.10.111.0/24
3) The internal machine should accept any incoming telnet connections from the machine 10.20.111.0/24 only.

Verify that your rules are correct by generating the appropriate traffic. Document your results using screen captures. Be sure to list the ip chains that you are using.

2.2. Part B

Flush all of the firewall rules from the network firewall. Now using the NAT table in iptables performs network address translation so that traffic from the inside machines is translated from a source address of 10.20.111.2 to a source address of 10.10.111.x that is the outside interface of the network firewall. Note that this outside address in which you are translating to is obtained via DHCP. The NAT operations should be performed on the firewall with the ip address of 10.20.111.1. BE SURE NOT TO DO THIS ON THE OTHER FIREWALL. IF YOU DO YOU WILL LOOSE POINTS.

Using wireshark on one of the outside machines verify that the source address is indeed being translated. Also verify that you are able to ping and ssh to one of the external machines.

Document your results using appropriate screen captures.

2.3 Part C

Answer the following questions:

1) In your own words describe how iptables works.

2) What is the difference between input, output and forward chains?

3) What is the difference between deny, reject and accept?

4) Do some research and find some alternative network based firewalls (at least 3). List and describe the pros and cons of each when compared to iptables. The alternative can be commercial, opensource or even a stand along appliance.