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#.VTFeMZOgapo

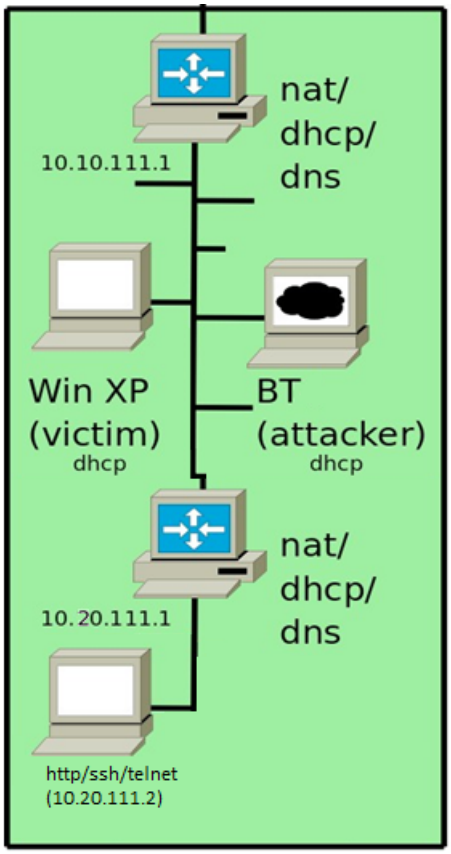
A firewall configuration tool can be found at: http://easyfwgen.morizot.net/

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 Kali. 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 for this lab must be performed on 10.20.111.1 (internal router/firewall). If you perform the operations on the other firewall you will receive zero points.



2.1. Part A

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

For outgoing traffic (from 10.20.111.0/24 to 10.10.111.0/24) - your internal machine should be able to communicate with the external network and the external machines without restrictions.

For incoming traffic (from the 10.10.111.0/24 to the 10.20.111.0/24) - all incoming connection requests should be rejected with the following exceptions:

1) [15 pts] The internal machine should respond to a ping from 10.10.111.0/24
2) [15 pts] The internal machine (10.20.111.2) should accept all incoming SSH and http requests from 10.10.111.0/24
3) [20 pts] The internal machine should accept telnet connections from the Kali Machine only. You may need to note the address received via DHCP on the Kali machine in order to build this rule.

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.

All firewall rules must be stateful.

2.2. Part B

Flush all of the firewall rules from the internal 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.

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.

[30 pts] Part B is worth 30 points

2.3. Part C

Answer the following questions:

1) [5 pts] In your own words describe how iptables works.

2) [5 pts] What is the difference between input, output and forward chains?

3) [5 pts] What is the difference between deny, reject and accept?

4) [5 pts] Do some research and find some three alternative network based firewalls. List and describe the pros and cons of each when compared to iptables. The alternative can be commercial, opensource or even a stand-alone appliance.

3. What to Submit

For Part A and B, provide documentation showing the iptables rules for items along with a screenshot of the iptables –L output, and document that you verified that the rules are working properly. For Part C, answer the questions in sufficient detail.