Project 2: Firewall and iptables

CSE 468 Computer Network Security

Due Date: Feb 23, 2014 11:59PM

1 Overview

The learning objective of this project for students is to gain hands-on experiences with the usage and functionality of iptables. Iptables can be used as single commands under root privilege. You can also write the commands in a script file and execute the file instead. In this project, you are required to use a script (rc.firewall) as illustrated by the instructor in class. An example of the script file can be found on Blackboard. You will learn iptables configuration for packet filtering and NAT from this project.

2 Project Description and Tasks

2.1 Environment Setup

The network consists of three VMs: Gateway, Client, and Server. They simulate a typical network application scenario: the Server resides in a private network; the Client resides in a public network; the Gateway protects the Server from public access by using iptables. The network topology is illustrated as in Fig. 1.

2.1.1 Wireshark Tool

Wireshark is a useful sniffer tool for analyzing network performance and problems. You should at least install Wireshark on your Gateway VM to capture snapshots for your report (see Section 3 for detailed requirements). You can find useful links on using Wireshark in Section 4. Do remember that you need to run Wireshark under root privilege. Otherwise, you will see a warning telling you no interface is found.

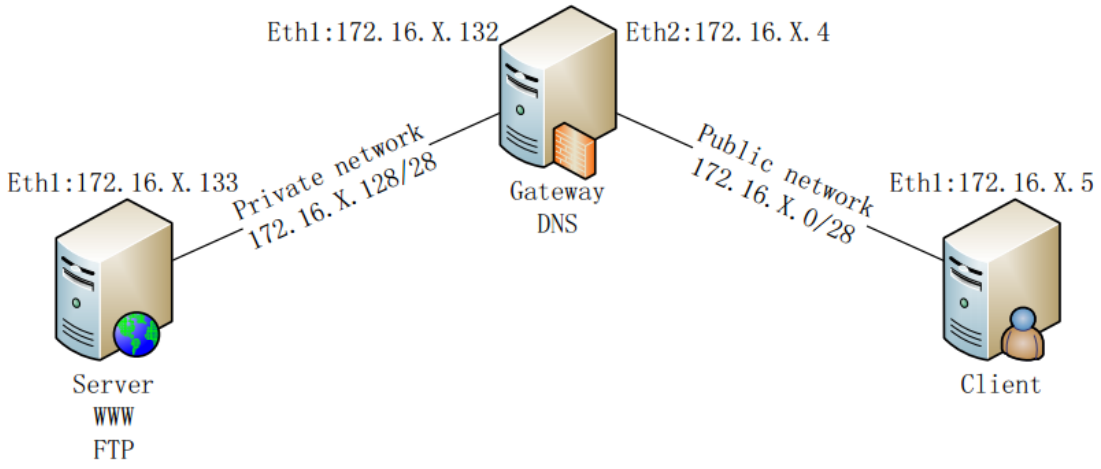

Figure 1: Network Topology

(X represents your project number in vLab. Your current IP address should be 172.24.x.x/28)

2.1.2 FTP Server vsftpd

To test the effects of iptables, you will need to use FTP service in this project. You can install vsftpd on your Server VM and provide FTP service from this VM. The way how to install vsftpd is similar to installing apache2 in Project 1. You can find useful links in Section 4.

2.2 Project Tasks

Students need to setup iptables on the Gateway VM to satisfy the following requirements:

1 Use iptables NAT to make the Client VM and Server VM access to the Internet.

2 Install a FTP server on Server VM and configure FTP server as a passive mode.

3 Use NAT to hide Server VM from Client VM (i.e., without proper iptables NAT setup, Client cannot talk with Server);

4 Client can Ping Gateway, but cannot Ping Server.

5 Gateway can Ping Server. Server can Ping Gateway.

6 Server can initiate an SSH connection to Gateway.

7 Client can initiate an SSH connection to Server, using Gateway as NAT.

8 Client can access Website hosted on Server, using Gateway as NAT. (i.e., Client cannot directly visit the website on the Server, if Client need to visit the Webserver, it needs go through the Gateway).

9 Allow Client to access Server's FTP service and download a test file from Server to Client.

10 Allow Client and Server issue DNS query requests to your local DNS server.

11 All other traffic should be dropped.

2.3 Tips

- In Section 1.3 of the example rc.firewall file, the location of iptables may be different depending on where you put your rc.firewall file. You should put correct route to find iptables from the folder where your own rc.firewall file locates.
- Once you finish editing your rc.firewall file, you may need to change the file mode so that the file can be executable. You can find useful information on changing file mode in Section 4.
- To enable downloading file from FTP server, you may need to change the configuration of the FTP server. You can refer to Section 4 for detailed information. The "anon_root" value may not be set by default. You need to add this value in the configuration file.
- When testing your script file, it is better to test the tasks one by one. You can use "#" to comment out irrelevant commands.

3 Project Report

You should submit a report to record detailed project process as required on Blackboard. In addition to the general requirements, you need to fulfill the following points:

- You need to use Wireshark to capture both the incoming and outgoing packets on both interfaces (as depicted in Fig. 1) of Gateway VM. You need to show the snapshots of key packets captured for each task (if applicable).
- You need to show the step-by-step process of configuring iptables for each requirement in your report. Explanations and illustrations on how your firewall works are also required;
- You need to include your script file (rc.firewall) as appendix in your report.

4 Helpful Documents

4.1 Wireshark

- How to Use Wireshark to Capture, Filter and Inspect Packets: http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-andinspect-packets/

4.2 Iptables

- A short iptables turtorial (on Blackboard);
- iptables configuration example (on Blackboard).

4.3 vsftpd FTP Server Installation and Configuration

- FTP Server: https://help.ubuntu.com/lts/serverguide/ftp-server.html
- Howto: Easy FTP with vsftpd: http://ubuntuforums.org/showthread.php?t=518293
- Set up an anonymous FTP server: http://www.g-loaded.eu/2008/12/02/set-up-an-anonymous-ftp-server-with-vsftpdin-less-than-a-minute/

4.4 Change File Mode

- Chmod: http://en.wikipedia.org/wiki/Chmod