Computer Science 530 - Lab Assignment #6 -- Fall 2021

Due: Friday November 12, 2021, 4:30 p.m.

Overview

Infrastructure for Lab

You will use two virtual machines, CLIENT and SERVER, in this lab. Both virtual machines are instances of fedora30-fall20.ova, which you have downloaded and installed in virtualbox in previous labs. I have included the .ova file again the google drive directory for this lab in case you need it, but you may use the version already downloaded if you need to construct a new base virtual machine, or you can use the virtual machine already installed to make clones using the populate scripts.

In previous labs, some students had problems setting up their virtual machines because of several issues, including sometimes not running the appropriate scripts to clone machines to configure networks or to establish internal settings for the machines. In other cases, the scripts did not run because vboxmanage was not in the search path for the shell (or command prompt) where the scripts were run. Please review last year's general lab instructions for virtualbox **here,** for guidance on setting up these virtual machines correctly (paying particular attention to the discussion of search path for vboxmanage, as well as the need to create a "base" snapshot for the fedora30-fall20 virtal machine, before it can be cloned by the populate script. Please be aware that the download instructions for scripts and ova files are different than what is in last years instructions, but the new locations are described in each lab.

Location of files

The ova file for the one based appliances is available in the CSci530 google drive in the folder for Lab 6 here.

Please note that you may need to login to google drive with your USC account in order to access these files.

(you can use the version previously downloaded if you like, or clone from the pevious installation). The files in the google drive for lab 4 are:

My Drive > 2021 Lab 6 ▾					
Name	Owner	Last modified	↑	File size	
📁 lab6scripts.windows	me	6:55 PM me		—	
📁 lab6scripts.linapp	me	6:56 PM me		—	
📄 fedora30-fall20.ova	me	7:01 PM me		4.37 GB	

You will note that there is a directoy with scripts (or BATCH files) for this lab. There is a directory for windows machines, and another for Linux and apple systems. Download the scripts from the directory that is relevant to your machine. The scripts in these directories are used to clone the virtual machines (populate), start them (poweron), configure the network between them (construct network, set internal settings for the guest machine (guestOS-internal-setting), power them off, and get rid of them when you are done with the lab (destroy).

You will run these scripts at the appropriate time for the experment nftables below.

Some notes on this instance of fedora Linux

We have already loaded most of the programs you will need for this lab into the virtual appliance. When you start the virtual machine you will be asked to login. The password for both the root and students accounts is "c$l@bLinuX". The third character is the letter "l" as in lab.

Some useful resources for this lab

The following materials may be of use to you in learning about firewalls and the tools you will use in this lab.

- Slides from last years (2020) lab instruction for the firewall lab.
- Netfilter documentation
- nftables quick reference guide
- nftables how to guude
- General instructions for setting up virtualbox and installing virtual machines from 2020 Semester(some locations are different this year, but this document is still a useful reference)

Firewalls Lab

[In fall 2021 - for this lab you are only expected to perform the lab exercises for the nftables command in linux, linked from bullet 1 of the outline below.]

There are additional links in bullet 1, and also 2 and 3 which are for more advanced elements on the topic of firewalls. These cannot be accomplished using your current virtual machine setup. For these advanced sections of the lab you should review the material to understand how it fits into the context of that part of the lab which you are performing. You do not need to execute and perform these other parts of the lab, bt you may be asked questions regarding the description that you will review.

The material covered in this lab falls into three components:

1. Firewalls for *self*-protection (co-location of the protective firewall and protected service on same machine) using the nftables commands in linux. <-- this is the part you will complete.
   - It is possible to obtain a similar capability using the built-in Windows' XP firewall. [You will not actually execute this part of the lab. Just review the information provided.]

2. Firewalls for *net*-protection (location of the protective firewall on the path to a protected service that's on another machine) another example: contrasting self-vs net-protection of a Windows service (Windows' vs router's firewall) [You will not actually execute this part of the lab. Just review the information provided.]

3. Creating firewalls in a small commercial router [You will not actually execute this part of the lab. Just review the information provided.]

After you have performed the above lab components, answer the following questions.

1. Windows XP's firewall by default lets nothing in and everything out. Comment on whether we should consider this an "optimistic" or "pessimistic" stance?

2. Here is a script that sets up a firewall.

```
1 # flush existing rules and tables
2 nft flush ruleset
3
4 nft add table ip mytable
5 nft 'add chain ip mytable myinputchain { type filter hook input priority 1; policy drop; }'
6 nft 'add chain ip mytable myoutputchain { type filter hook output priority 1; policy drop; }'
7 nft 'add chain ip mytable myforwardchain { type filter hook forward priority 1; policy drop; }'
8
9 ########## first service ##########
10 nft add rule mytable myoutputchain udp dport 53 ip daddr 0.0.0.0/0 accept
11 nft add rule mytable myinputchain udp sport 53 ip saddr 0.0.0.0/0 accept
12
13
14 ########## second service ##########
15 nft add rule mytable myoutputchain tcp dport 80 ip daddr 0.0.0.0/0 accept
16 nft add rule mytable myinputchain tcp sport 80 ip saddr 0.0.0.0/0 accept
```

a. briefly state in declarative English what the script above expresses in nftables syntax. Include mention of the effects of each of its four main sections, in terms of resulting behavior. For example, the first main section discards existing tables/chains/rules. (Look up the port numbers found in the script if you don't recognize them.)

b. for different reasons, removal of either lines 10 and 11, or else lines 15 and 16, will obstruct the primary behavior otherwise possible under this firewall. What's the reason when lines 10 and 11 are removed?

c. what's the reason when lines 15 and 16 are removed?

3. You have a home LAN containing 2 computers. The first computer is a general purpose PC running Windows XP. The second computer is a typical commercial router, perhaps a Netgear WGR614. The router, in addition to being on the LAN, is on the internet (it has 2 NICs).

a. You want to run a web server on your XP box. To enable, do you need to make the firewall adjustment on the router, XP, or both?

b. You want to prevent the XP box from conversing with the internet using certain protocols. To do it, do you need to make the corresponding firewall adjustment on the router, XP, or both?

4. The Netgear WGR614 which you can learn about through the link, is a smart device, not a dumb one. Because it's actually a computer. Though humble in appearance, it contains a CPU, memory, operating system-- the defining essentials. In addition, it has 2 network interfaces. To use this computer as a router for PCs, you need to connect them to it. You could do that just as you connect PCs to each other, by plugging them into a common switch. For marketability the small commercial router makers build a switch into their boxes. You got to have one; they're cheap to build in; the competitors do it. So you can hardly find a router that is not a router-with-switch.

Consider the switch built in to the WGR614. Physically, the number of computer connections it provides in the form of RJ-45 connection sockets is 4. Visibly. Electronically, by contrast, how many computer connections does this built-in switch have altogether? That is, if it is an n-port switch (electronically), what is n?