OPS535 Lab 1

Purpose

Libvirtd provides firewall rules to allow access to virtual machines, but assumes all connections will originate from them. It does not have a good setup to allow clients from outside your network to connect to servers you might be hosting on VMs. In this lab you will gain experience managing the firewall rules that allow greater control over traffic, along with routing information to control where outgoing traffic is sent.

Pre-Requisites

The pre-lab must be complete so that your virtual machines share access to a private network.
Shut down your VMs and delete the default virtual network from your host.

Investigation 1: Virtual Networks

Perform the following steps on your host

1. Use the skills you learned in previous courses to create a new virtual network called default (we are only keeping the same network name as the old one so we don't have to change it in every VM).
    - The address range to provide is determined based on your Network Number (obtained through blackboard): 192.168.X.0/24.
    - Do not provide DHCP.
    - Allow it to forward to any physical device, but set the mode to 'Open'. In virt-manager, the major difference between the three modes is the firewall rules that it will set up for you.
2. Boot each virtual machine and provide it a static address according to the following table. Do not alter the address it already has for your internal network.

Hostname	Address for external network
vm1.<yourdomain>.ops	192.168.X.53/24
vm2.<yourdomain>.ops	192.168.X.2/24
vm3.<yourdomain>.ops	192.168.X.3/24

Investigation 2: Advanced uses of FirewallD

Having removed the default network, you have also removed the firewall settings it was providing for you that allowed your machines to communicate with the outside world. Perform the following steps on your host.

1. Set the virtual interface that is assigned to your new virtual network to be part of the ‘external’ zone. Make sure the change will be permanent.
    - Due to a known issue, you will have to restart the NetworkManager service before this change becomes apparent.
2. Ensure Masquerading is set to off for this zone.
    - While masquerading would allow our machines to reach the network outside by hiding their internal addresses behind the host machine’s address, it would not help us allow new connections to be made to the servers inside our network. We will have to set that up ourselves.
3. Remove all services from this zone except for ssh and dns (which you may need to add yourself).
4. Now that you have removed the excess clutter from the zone, examine it using firewall-cmd --zone=external --list-all (assuming you have not already done so).
    - You may also wish to use the old iptables commands to list individual chains. Pay particular attention to FORWARD and POSTROUTING.
5. Using the --direct option, add a rule to the FORWARD chain that will allow traffic addressed to machines in your 192.168.X.0/24 network.
    - While this (and the next step) should also work with the incoming/outgoing interface options, it does not seem to. Use the destination address only.
6. Using the --direct option, add a rule to the FORWARD chain that will allow traffic from machines in your 192.168.X.0/24 network addressed to anywhere else.
7. The previous two steps will allow traffic between your virtual machines and the outside world, however most machines will not currently respond to them, as they are using addresses in one of the private address ranges. This is not an issue for the other machines in the lab, as they will be expecting these addresses but anyone outside (e.g. when you try to get updates) will not respond.
8. Using the --direct option, add a rule to the POSTROUTING chain of the nat table to masquerade all traffic coming from your virtual network. Use a priority value of 3 (we will need to add a few rules before this one shortly).
    - This will cause traffic coming from your network to use your host’s external facing address. Unfortunately, this puts us right back where we started; any traffic your virtual machines send out will have the actual address hidden. We will need to add some rules before this to allow us to communicate with the other machines in the lab without being masqueraded.

9. Using the --direct option, add a rule to the POSTROUTING chain of the nat table to ACCEPT all traffic coming from your virtual network that has a destination in 172.16.0.0/16. Use a priority value of 2 so that this rule will happen before the one you just added.
10. Using the --direct option, add a rule to the POSTROUTING chain of the nat table to ACCEPT all traffic coming from your virtual network that has a destination in 192.168.0.0/16. Use a priority value of 2 so that this rule will happen before the masquerading one.
    - This rule will allow you to communicate with machines in other students' own networks. We have lumped all of them into one /16 rule instead of having to add a separate rule for each student you wish to communicate with.
11. Use firewall-cmd and iptables -L to examine your firewall again. You should see the rules you added in the FORWARD chain of the filter table, and in the POSTROUTING_direct chain of the nat table.
    - Make sure the two rules you added to POSTROUTING that ACCEPT traffic addressed to 172.16.0.0/16 and 192.168.0.0/16 appear before the masquerade rule you added.
    - Once you are satisfied with your firewall, use firewall-cmd –runtime-to-permanent to save it.
12. Now that your VMs can be reached by the outside world, it is important to differentiate the traffic that is on their internal network from traffic with the outside world. Boot each of your VMs and set the interface that is connected to your internal network to be in the zone called internal, while the interface connected to the open network you just created should be set in the zone called external.
    - Make the same changes to the external zone you did on the host (i.e. no masquerading, and delete the unneeded services).
    - Make sure these changes persist past rebooting.

Investigation 3: Routing

In the previous investigation you configured the firewall on the host to allow your virtual machines to communicate with other students' networks as well as the outside world, but they can not actually reach the other networks yet, as they do not know where to send the traffic. By virtue of having an address in the 172.16.0.0/16 network, your host should already have a routing table entry for that network, but your virtual machines will not. In addition, none of your machines know how to reach other students' virtual machines. The use of routing files will fix that.

1. You could use scripts to constantly re-add routing information using the ip route command (there is a link in the weekly readings with examples of this), but it is better to configure the files that NetworkManager will use to determine routes on a permanent basis.

- In the same directory as your ifcfg files, you can create files using the name route-<interface> (where <interface> is the name of the interface you wish to create routing rules for, e.g. route-eth0 would hold routing rules for eth0).

2. On your host machine create a file for your actual network interface (the one that has the 172.16.X.1 address).
   - Add an entry for each 192.168.Y.0/24 network, accessible via 172.16.Y.1. Check for an announcement on blackboard regarding what Y value to go up to.
   - **Note: Do not include your own network in this list.**
3. On each virtual machine create a file for the interface that has access to the outside world.
   - Add an entry for the 172.16.0.0/16 network, accessible via 192.168.X.1 (your own host's address in this network).
     - This will cause your virtual machines to direct traffic addressed to anything in that address range to your host (which knows whose host to pass the traffic on to).
   - Add an entry for each 192.168.Y.0/24 network, accessible via your host's address in this network. Check for an announcement on blackboard regarding what Y value to go up to. **Note: Do not include your own network in this list.**
     - This will direct all traffic your VMs send to another student's VMs to pass through your host, which already knows whose host to pass the traffic on to.
4. From your host and all VMs, ping another student's host and VMs. You should get responses back. If not, go back and trouble shoot your routing rules.

Completing the Lab

You should now have a better network configuration for your VMs. Each machine has access to the internal-only network it already had, but now has the second network interface configured to allow access to other nearby networks (e.g. other networks in the same organization) without undergoing Network Address Translation.

Follow the instructions on blackboard to submit the lab.

Exploration Questions

1. What does the priority number in a direct rule for firewalld affect?
2. How are direct rules different from rich-rules?