CENG489 HW3-A: Using the Linux Firewall

1 Overview

The learning objective of this assignment is to gain the insights on how firewalls work by using ufw in Linux. Packet filters act by inspecting the packets; if a packet matches the packet filter's set of rules, the packet filter will either drop the packet or forward it, depending on what the rules say. Packet filters are usually *stateless*; they filter each packet based only on the information contained in that packet, without paying attention to whether a packet is part of an existing stream of traffic. Packet filters often use a combination of the packet's source and destination address, its protocol, and, for TCP and UDP traffic, port numbers.

2 Your Task: Using the UFW Firewall in Linux

Linux has a tool called `iptables`, which is essentially a firewall. It has a nice front end program called `ufw`. In this task, the objective is to use `ufw` to set up some firewall policies, and observe the behaviors of your system after the policies become effective. You need to set up at least two VMs, one called Machine A, and other called Machine B. You run the firewall on your Machine A. Basically, we use `ufw` as a personal firewall. Optionally, if you have more VMs, you can set up the firewall at your router, so it can protect a network, instead of just one single computer. After you set up the two VMs, you should perform the following tasks:

- Prevent A from doing telnet to Machine B.
- Prevent B from doing telnet to Machine A.
- Prevent A from visiting an external web site (e.g. Facebook). You can choose any web site that you like to block, but keep in mind, some web servers have multiple IP addresses.
- Prevent all traffic that has a destination port of 443 and show that you are not able to access a server using HTTPS after implementing this rule.
- Prevent all ICMP traffic and show that you are not able to ping another machine.

You can find the manual of `ufw` by typing `"man ufw"` or search it online. It is pretty straightforward to use. Please remember that the firewall is not enabled by default, so you should run a command to specifically enable it. We also list some commonly used commands in Appendix A.

Before starting the task, go to the default policy file `/etc/default/ufw`. If `DEFAULT_INPUT_POLICY` is `DROP`, please change it to `ACCEPT`. Otherwise, all the incoming traffic will be dropped by default.

A Firewall Lab Cheat Sheet

Using `ufw`. The default firewall configuration tool for Ubuntu is `ufw`, which is developed to ease `iptables` firewall configuration. By default UFW is disabled, so you need to enable it first.

```
[frame=single]
$ sudo ufw enable            // Enable the firewall
$ sudo ufw disable           // Disable the firewall
$ sudo ufw status numbered   // Display the firewall rules
$ sudo ufw delete 2          // Delete the 2nd rule
```