CPTR 427 Lab #12 Name

Linux & Windows Firewall

# Lab Ops

## Windows:

1. Your windows server is already installed.
   1. Windows has pretty good default rules.
   2. Make sure you review the rules and are able to understand and explain any rule in effect.

## Linux

1. Make sure the following are installed:
   1. iptables
   2. open ssh client and server
2. Create the following rule sets for your firewall:
   1. passicmp – rules to allow deny ICMP packets
   2. TCP-STF – rules to allow deny different TCP states
   3. CON-TRK – setup connection tracking so we don’t have to traverse all the other rules for established connections.
   4. SRC-CHK – Check to disallow sources you don’t want (maybe other malicious users on this network)
   5. FWL-IN – Make sure to allow SSH in and any other services you have running.
   6. FWL-OUT – What will you allow out? At least you should allow unprivileged ports.
3. Make sure the firewall rules you create are run at boot. Where in the sequence should you put it?
4. Setup your servers to receive automatic security updates once a day between 1 and 4 in the morning.

# How to Install?

There is good documentation online. Part of being a good sysadmin is finding answers to problems. I’ve given you a task list and the order to do it in. Find the information necessary. If you get lost, ASK, I’ve probably done this X too many times.

# Demos/Questions

1. List the services currently running on both servers.
2. Show that your linux firewall will start at startup
3. List the Linux firewall rules from the command prompt
4. When should you run the firewall script during the boot sequence? (e.g. before or after some specific service)
5. What iptables command would you add to prohibit access to a web server on your system? and where would you add it?
6. Show the list of rules in your windows server (I’ll ask you about some of them).