

CS 409

Assignment 2

Done By: January 28

This assignment is going to be postinstall housekeeping.

1. Password your GRUB bootloader and see if it works. You can leave it this way or not, its up to you. Also change some of the other parameters like the timeout so you can see how it works.
2. Boot your system into single user mode to be sure that you know how to do this.
3. Turn off unused services on your system. If you're not sure, don't change it, but you can certainly turn off sendmail, httpd, smb, snmpd, named, ntpd, vncserver, yp*, mysql and postgresql.
4. Insure that telnet and ftp are not running on your system but ssh must be. This means that you need to stop telnetd or ftpd from running via xinetd. Then you need to get sshd running using chkconfig and/or services. When you try to use ssh it will probably fail because you need to open port 22 in your iptables. Don't open it up for everything, just for 153.90.199.0/21 and maybe your home address.
5. Set up logging for your iptables and observe the traffic for a few days. You can turn it off by commenting out the rules and reinstalling your tables, but it is worthwhile to see what shows up in your logs.
6. Make sure that your iptables allow all local traffic to avoid problems with simple local operations.
7. Set up your TCP wrappers by creating a /etc/hosts.deny file that contains only *ALL:ALL*. Then create a hosts.allow that contains only *localhost:ALL*.