CS 409
Assignment 11

1. Using nmap do a couple of different scan. For example -sT and -sO. Also, try nmap with the *-O* option, with *-sT -p 1024-60000*.

2. Open port 80 in your iptables and run nmap to see if it finds it. Don't forget to close it when you are all finished..

3. Have someone else scan your system with a simple *-sS* parameter.

4. Install portsentry and tripwire. The rpms are available at the usual sites.

5. Start portsentry if it is not already running (use *service portsentry status* to find out. Then run a portscan against your system from some other host. Check the */var/log/messages* file to make sure that it was detected. Also, look in the /etc/portsentry/portsentry file (probably) to see if that host is now blocked from your system. Try another scan to see what happens.

6. Now look in /var/log/messages again at the point where you made the initial attack. You should see a line like this:

   ```
   Apr 14 07:53:35 malt portsentry[516]: attackalert: Host 153.90.199.78
   has been blocked via dropped route using command:
   "/sbin/iptables -I INPUT -s 153.90.199.78 -j DROP"
   ```

   What is this telling you? Execute *iptables -L* to see if this is true. The new rule will be at the top and will not be identical to the one shown in the messages file. In order to get the host unblocked, execute *service iptables restart* and delete the entries from the blocked file(s). Restart the portsentry service.

7. Now try a more sophisticated scan, such as an -sF, sX or sN and see if that is also detected. You will need to do this from another host or have someone do it for you. Again, when you are done, clean up iptables and your blocked hosts files as needed.

8. Finally, install tripwire and configure it. Make some changes and verify that it works.