

Lab2 - Network Security

1. iptables
 1. Drop all outbound traffic to www.msn.com
 2. Drop all inbound traffic from 192.168.1.X
 3. Install firestarter
 1. rpm -ivh http://www.scs.ryerson.ca/~zereneh/security_seminar/downloads/firestarter-0.9.3-1.i386.rpm
 4. Implement the same rules using firestarter

2. Run snort on interface eth0
 1. Install snort
 1. rpm -ivh http://www.scs.ryerson.ca/~zereneh/security_seminar/downloads/snort-2.1.3-1.i386.rpm
 2. /usr/sbin/snort -A fast -b -d -D -i eth0 -u snort -g snort -c /etc/snort/snort.conf -l /var/log/snort
 3. tail -f /var/log/snort/alerts
 4. nmap host

3. Verify net-tools package using rpm -V
 1. mv /sbin/route /tmp
 2. run rpm -Vv net-tools
 1. check output for “missing” file
 3. mv /tmp/route /sbin/