#SNORT FOR LINUX

1. INSTALLING DEPENDENCIES AND INITIAL SETUP.

2. DOWNLOAD SOURCE CODE FOR DAQ AND SNORT (i.e. .tar.gz file).

3. INSTALL SNORT AND DAQ.

4. POST CONFIG.

5. CHANGE FILE AND DIRECTORY OWNERSHIP.

6. EDIT snort.conf & test snort(-T).

7. RUN SNORT IN IDS MODE.

groupadd <groupname(snort)>

useradd <user\_name(snort)> -r -s /usr/sbin/nologin -c SNORT\_IDS -g <group\_name(snort)>

#apt-get update

#apt-get install make tree bison pkg-config checkinstall flex build-essential iptables-dev libnet1 libnet1-dev libc6-dev libc-dev-bin libdnet libdnet-dev libdumbnet1 libdumbnet-dev libghc-zlib-dev libpcre3-dev linux-libc-dev libpcap-dev libnfnetlink-dev libnetfilter-queue1 libnetfilter-queue-dev

repeat the command twice to make sure all dependencies our installed properly

below commands are for installing daq and snort source code setup:

#mkdir /usr/src/snort\_src

#cd /usr/src/snort\_src

#mkdir /dl

#cd /dl

#wget <ip for DAQ source file(.tar.gz)>

#wget <ip for SNORT source file(.tar.gz)>

#tar -zvxf daq(tab)

#cd daq(tab)

#./configure

#make

#make install

#cd ..

#tar -zvxf snort(tab)

#cd snort(tab)

#./configure --enable-sourcefire

#make

#make install

#snort -V

#ldconfig

make these directories for snort:

#mkdir /etc/snort

#mkdir /etc/snort/rules

#mkdir /etc/snort/preproc\_rules

#mkdir /var/log/snort

#mkdir /usr/local/lib/snort\_dynamicrules

copy conf files and map files essential for snort in /etc/snort:

#cp /usr/src/snort\_src/snort(tab)/etc/\*.conf\* /etc/snort

#cp /usr/src/snort\_src/snort(tab)/etc/\*.map /etc/snort

take conf file backup to be safe:

#cp /etc/snort/snort.conf /etc/snort/snort.conf.backup

create these rules for use:

#cd /etc/snort/rules

#touch white\_list.rules black\_list.rules local.rules

edit rules in local.rules for time being.

below commands are for permissions and owner changes:

#chmod -R 5775 /etc/snort

#chmod -R 5775 /var/log/snort/

#chmod -R 5775 /usr/local/lib/snort/

#chmod -R 5775 /usr/local/lib/snort\_dynamicrules/

#chmod -R 5775 /usr/local/lib/snort\_dynamicengine/

#chmod -R 5775 /usr/local/lib/snort\_dynamicpreprocessor/

#chmod -R 5775 /usr/local/lib/pkgconfig/

#chmod -R 5775 /usr/local/bin/daq-modules-config

#chmod -R 5775 /usr/local/bin/u2boat

#chmod -R 5775 /usr/local/bin/u2spewfoo

#chown -R snort:snort /etc/snort

#chown -R snort:snort /var/log/snort/

#chown -R snort:snort /usr/local/lib/snort/

#chown -R snort:snort /usr/local/lib/snort\_dynamicrules/

#chown -R snort:snort /usr/local/lib/snort\_dynamicengine/

#chown -R snort:snort /usr/local/lib/snort\_dynamicpreprocessor/

#chown -R snort:snort /usr/local/lib/pkgconfig/

#chown -R snort:snort /usr/local/bin/daq-modules-config

#chown -R snort:snort /usr/local/bin/u2boat

#chown -R snort:snort /usr/local/bin/u2spewfoo

now we will edit the conf file:

in step 1 last part

change ../ with /etc/snort/

in step 7 delete all include paths

only retain local.rules path and add black and white\_list.rules

#snort -i eth0 -u <snort> -g <snort> -c /etc/snort/snort.conf -T

##snort -i eth0 -u <snort> -g <snort> -c /etc/snort/snort.conf -A console