Bu yaziyi yazarken Freebsd 4.6 -4.7 surumlerinden birini kullandiginiz ve unix komutlari hakkinda bilginiz oldugunu varsayiyorum.

Ilk yapmamiz gereken tabiki gerekli portlari yuklemekBunun icin ilk yapmamiz gereken portlarimizin guncel oldugundan emin olmak.Cvsup ile port guncellestirmesi yaptigimda portlarin en guncel surumlerini almasindan dolayi uyumsuzluk problemi yarattigini gordum. Bunun icin sadece snort `u guncellestirmenin daha mantikli olacagini dusundum.Snort.org sayfasina girip snort'un en son surumunu cektikten sonra pkg_add -r /dosya.tar.gz komutuyla bunu port listeme ekliyorum.Simdi normal islemlere donebiliriz.

1. /usr/ports/ftp/wget klasorune girip make && make install && make clean komutunu veriyorum.
2. /usr/ports/graphic/phplot klasorune girip
make WITH_X11 && make install && make clean komutunu veriyorum.Bana yukleme islemine baslarken bir sema cikartiyor ve burda GD2 yi secip Ok diyorum.
3. /usr/ports/databases/adodb klasorune girip make && make install && make clean komutunu veriyorum.
4. /usr/ports/net/libnet klasorune girip make && make install && make clean komutunu veriyorum.
5. /usr/ports/security/snort klasorune girip make -DWITH_MYSQL -DWITH_FLEXRESP && make install komutunu veriyorum.(make clean komutunu vermiyorum cunku work klasoru daha sonra datase'ı yapilandirirken isimize yarayacak.
6. /usr/ports/security/acid klasorune giriyorum ve make && make install komutunu veriyorum.(Burda yine clean yok zira clean kullanirsak snort icindeki work klasorunu de siliyor.)
7. Rehash yazip butun yukledigimiz programlarin shell tarafindan tanindigindan emin oluyoruz.

Simdi sira yukledigimiz programlarin konfigrasyonlarini yapmaya geldi.

Snort icin:
/usr/local/etc klasorune girip chmod 644 snort.conf yapiyoruz.Favori editorunuzle ki benimki pico, snort.conf'u aciyoruz.Burda “var RULE_PATH ./” bolumunu “var RULE_PATH /usr/local/share/snort” olarak degistirip 3. bolumde output datase bolumundeki ilk madddenin onundeki # isaretini kaldiriyoruz.

Apache icin:
/usr/local/etc/apache/httpd.conf dosyasini acip DocumentRoot “/usr/local/www/data” bolumunu DocumentRoot “/usr/local/www/acid” olarak ve <Directory “/usr/local/www/data” bolumunu <Directory “/usr/local/www/acid” olarak degistiriyoruz. Bu arada ben kisisel olarak sadece kendi makinamdan Acid istatistiklerime ulasmak istedigim icin "This controls who gets stuff from this server" kismindaki "all" bolumunu 127.0.0.1 olarak degistirdim.

Acid icin:
Chmod 644 /usr/local/www/acid/acid_conf.php komutunu veriyoruz.Daha sonra

/usr/local/www/acid/acid_conf.php dosyasini acip gerceklerini asagidaki satirlar ile degistiriyoruz:

$alert_dbname = “snort”
$alert_password = “database icin kullanacaginiz sifre”
$ChartLib_path = “/usr/local/lib/php/phplot”
$portscan_file = “/var/log/snort/scan.log”

Mysql icin:
/usr/local/bin/mysql_install_db komutunu veriyorum.
/usr/local/share/mysql klasorune girip burdan az, orta veya cok ram kullanabilcek profillerden birini seciyorum.Bu sizin database'inizi arsivleme vs. icin ne kadar siklikla kullanacaginizla ilgili. Ben kisisel olarak my-larg.cnf yi secip; cp /usr/local/share/mysql/my-large.cnf /etc/my.cnf komutu ile kopyaliyorum.

/usr/local/etc/rc.d/mysql-server.sh start komutunu verip mysql databse'i baslatiyorum.

/usr/local/bin/mysql ile mysql server a baglanip,
SET PASSWORD FOR root@localhost=PASSWORD(‘snort.conf dosyasinda belirttiginiz
sifre”;
FLUSH PRIVILAGES;
Komutlarini veriyoruz.Bunlari yaparken ; isaretinin satir sonlarinda olmasina dikkat edin.
Exit ile mysql den cikiyoruz.
Root komut satirindan echo “CREATE DATABASE snort;” | /usr/local/bin/mysql -u root -p ile database'imizi olusturuyoruz.
Mysql -p komutu ile mysql server'a baglanip INSERT ,SELECT ,DELETE on snort.* to root@localhost; yaziyoruz.Boylece snort database'inin sadece mysql root acoountu ile degistirilebilceginden emin oluyoruz.
/usr/local/bin/mysql-p <
/usr/ports/security/snort/work/snort.1.9.0/contrib./create_mysql snort
mdir /var/log/snort
chown root:operator /var/log/snort/
komutlarindan sonra
mysql -p
mysql> use snort
mysql>show tables:
ile herseyin yolunda gittiginden emin oluyoruz.

Simdi de sira startup scriptimizi hazirlamaya geldi.
/usr/local/etc/rc.d/snort.sh dosyasini pico /usr/local/etc/rc.d/snort.sh ile actiktan sonra :

```
#!/bin/sh

sleep 3
case "$1" in
start)
```

```
if [ -x /usr/local/bin/snort ]; then
/usr/local/bin/snort -c /usr/local/etc/snort.conf i fxp0 -u root -g root -D > /dev/null &
&& echo -n ' snort'
fi
;;
stop)
/usr/bin/killall snort > /dev/null 2>&1 && echo -n ' snort'
;;
*)
echo ""
echo "Usage: basename $0 { start | stop }"
echo ""
exit 64
;;
esac
```

seklinde hazirliyoruz.Bunu kaydettikten sonra ile acilista calismasi icin chmod 755 snort.sh komutunu kullanip executable yapiyoruz.

Update icin ise yine pico /usr/local/etc/snort.rules.update komutuyla dosyayi olusturup;

```
#!/bin/sh

# Update rules

cd /tmp
rm -rf rules
/usr/local/bin/wget http://www.snort.org/downloads/snortrules.tar.gz
tar -xzf snortrules.tar.gz
# rm snortrules.tar*
mv /tmp/rules/*.rules /usr/local/share/snort
```

yazip yine chmod 755 snort.rules.update ile executable yapiyoruz.

Simdi ifconfig yazdigimizda network kartimizin ozelliklerini
"<UP,BROADCAST,RUNNING,**PROMISC**,SIMPLEX,MULTICAST>"
seklinde gormemiz gerekiyor.

Shutdown -r now komutuyla bilgisayarimizi yeniden baslattiktan sonra browser da http://localhost veya http://127.0.0.1/ yazarak Acid konsoluna ulasabiliriz.

Sorulariniz icin bana dionypheles@gmx.net adresinden ulasabilirsiniz.

Ozgur Ozdemircili

www.siberhayat.com
“siber hayatlarimizin bir yansimasi”