ANTI-SPAM - TARPITS

I do not like spam - at all. I have already gone through a couple of articles on how to use *postfix* and other software to help combat this scourge of the internet. Well here is something else you can do to make spammers lives a bit more difficult, a *smtp* tarpit. You see a spammer lives on speed, it is the speed at which they can send emails which makes their job worthwhile, by implementing a *tarpit* you slow down any spam attempts, thus starving any potential spammers of their most precious resource.

What do you need?
Well, you need a linux box with *perl*, *xinetd*, *iptables* and your email server. Now I am also using a *postfix/amavisd/spamassassin* combination, so my script for getting my blacklisted IP addresses centres around that and may need to be adapted. You also need to download a very nifty *perl* script called *smtarpit* (from here). Once you have the *smtarpit* file, do the following;

- *cp smtarpit /usr/local/bin*
- *cp smtpcli /usr/local/bin*
- *mkdir /usr/local/etc/log*

Ok, now you need to set it up to listen. I used the *xinetd telnet* configuration file as I sure as heck am never actually going to use *telnet*. So put this in */etc/xinetd.d/telnet* ..

```
service telnet
{
       socket_type     = stream
       protocol        = tcp
       wait            = no
       user            = root
       server          = /usr/local/bin/smtarpit
       log_on_success  = PID HOST
       log_on_failure  = HOST USERID
       instances       = 10
}
```

Now when you start *xinetd*, you should have a listening process on port 23. Once thats done, we are all set to divert all the nasties there.

Making life difficult
I use the following script to *grep* through my mail log and filter out any bad people, I then add them to master blacklist which I then use to setup diverts into my smtp tarpit. I am assuming that your email server has no firewall rules setup, if it has the script will need modification (put it into a separate chain or something). Also, I make no claim that my script is a work of art, you are free to use it and change it, it works for me and thats it. I have it in my */admin/bin* folder called *spam-ip*..

```
#SETUP VARIABLES
MASTER=/admin/conf/mast.ip
LOG=/var/log/maillog
TMP=/tmp/tmp.ip.bl
ADD=/admin/conf/other.ip
EXCEPT="<exception ip addresses>"
FLAG=0

#GETTING IP'S - USED FOR POSTFIX/AMAVISD/SPAMASSASSIN
echo "Getting IP's.."
cat $LOG | grep -e "Blocked SPAM" | gawk '{ print $9 }' | cut -f 2 -d "[" | cut -f 1 -d
"]" | sort | uniq >> $TMP
cat $LOG | grep -e "blocked using" | gawk '{ print $10 }' | cut -f 2 -d "[" | cut -f 1
-d "]" | sort | uniq > $ADD

#CREATING THE MASTER LIST
cat $ADD >> $TMP
cat $MASTER >> $TMP
cat $TMP | sort | uniq > $MASTER
cat $MASTER > $TMP
```

```
rm -rf $MASTER
touch $MASTER

#REMOVE YOUR EXCEPTIONS
for t in `cat $TMP`
 do
  FLAG=0
  for k in $EXCEPT
   do
    if [ "$t" == "$k" ]
     then
      echo match
      FLAG=1
     fi
   done
  if [ $FLAG == 1 ]
   then
    echo match2
   else
    echo $t >> $MASTER
  fi
 done

#CREATE A SYSLOG MESSAGE OF THE NUMBER OF BLOCKED IP'S
CNT=`cat $MASTER | wc -l`
echo "Got $CNT unique IP's.."
logger "==smtarpit== $CNT unique IP's.."

#CLEAR THE FIREWALL
iptables -t nat -F

#BLACKLISTING THE IP'S
echo "Blacklisting IP's.."
for x in `cat $MASTER`
 do
  iptables -t nat -A PREROUTING -s $x -d <mail_server> -m tcp -p tcp --dport 25 -j DNAT
--to-dest <mail_server>:23
 done

rm -rf $TMP
```

I then schedule it hourly through *crontab*..

```
50 * * * * /admin/bin/spam-ip
```

So once thats done, a spammer can send me one mail or he needs to end up on a RHBL server and I will then divert him to the tarpit, where he can sit for as long as he likes while I laugh. The cronjob also ensures that it will keep updating itself. To check the logs you can check the files in */usr/local/etc/log* or if you want to see the current status, use the *smtpcli* utility.

Final Words

A tarpit is a way of making the spammers life a bit more difficult, it also has the knock-on effect of dropping the load on your email server system as your server no no longer has to process all that junk. We can also live in the hope that if a spammer gets stuck for long enough that they will remove you from the list altogether. As always, have fun and learn.