Homework Number: hw8

Name: Jiaxing Yang

ECN Login: yang1274

Due Date: 4/02/2020

Firewall

```
#!/bin/sh

#set the macros
block_ip_1="121.121.121.121"
block_ip_2="101.101.101.101"
local_ip=$(hostname -I | sed 's/ //g')


#
# Remove any previous rules or chains, pg
iptables -t filter -F
iptables -t filter -X
iptables -t nat -F
iptables -t nat -X

# For all outgoing packets, change their source IP address to your own machine's IP
address (Hint: Refer to the MASQUERADE target in the nat table). pg  65
iptables -t nat -A POSTROUTING -j MASQUERADE



# Block a list of specific IP addresses (of your choosing) for all incoming
connections.
iptables -A INPUT -s $block_ip_1 -j REJECT
iptables -A INPUT -s $block_ip_2 -j REJECT

echo block the following ip addresses $block_ip_1 $block_ip_2

# Block your computer from being pinged by all other hosts (Hint: ping uses ICMP Echo
requests).
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
echo block from pinged

# pg 54
# Set up port-forwarding from an unused port of your choice to port 22 on your
computer. Test if you can SSH into your machine using both ports (Hint: You need to
enable connections on the unused port as well).
iptables -t nat -A PREROUTING -p tcp -d $local_ip --dport 80 -j DNAT --to-destination
$local_ip:22
echo set port 22

# Allow for SSH access (port 22) to your machine from only the engineering.purdue.edu
domain.
iptables -A INPUT -p tcp -s 128.46.0.0 --dport 22 -j ACCEPT
```

```
iptables -A INPUT -p tcp -s 0.0.0.0/0 --dport 22 -j DROP


# Assuming you are running an HTTPD server on your machine that can make available
your entire home directory to the outside world, write a rule that allows only a
single IP address in the internet to access your machine for the HTTP service.
iptables -A INPUT -p tcp -s 111.111.111.111 --dport 111 -j ACCEPT
iptables -A INPUT -p tcp -s 0.0.0.0/0 --dport 111 -j DROP

# Permit Auth/Ident (port 113) that is used by some services like SMTP and IRC.
iptables -A INPUT -p tcp --dport 113 -j ACCEPT
```

.procmailrc

```
SHELL=/bin/sh
PATH=/usr/local/lib/mh:$PATH
MAILDIR=$HOME/Mail
LOGFILE=$HOME/Mail/logfile
SENDMAIL=/usr/sbin/sendmail
#VERBOSE=1
VERBOSE=0
EOL="
"
LOG="$EOL$EOL$EOL"
LOG="New message log:$EOL"
LOG=`perl GET_MESSAGE_INDEX`
LOG="$EOL"



## Recipe_1:
##
:0 :
* ^From.*purdue\.edu
* ^Subject.*404
my404Folder



## Recipe_2:
##
## This recipe will only be invoked if the subject line
## constains the string 'sports' This email will go into
## your mailbox for the special account.  You need to
## replace the 'your_special_account_name' string with what
## applies to you
##
:0 :
* ^Subject.*sports
/var/mail/ece404t8
```

```
## Recipe_3:
##
## This is an emailing recipe.  It will send to your regular
## Purdue webmail account all messages that originate from
## the purdue.edu domain and that have survived the previous
## recipes.
##
##
## IMPORTANT NOTE: The email address in the last line of the
## recipe is your Purdue webmail address --- the address on
## which you normally receive your email DO NOT put your
## special account name in that line since that would create
## an infinite loop.
##
:0 :
* ^From.*(purdue\.edu[ ]|purdue\.edu>)
!yang1274@purdue.edu



## Recipe_4:
##
## This is one of the recipes in your instructor's spam
## filter. If your drug related spam does not originate from
## Purdue, this recipe will kick in.
##
## IMPORTANT: Since spammers fake their headers, a spam
## message actually coming from outside Purdue may still
## look like it is coming from Purdue.
##
:0 B
* < 10000
* (\<v.codin\>|\<viicodin\>|\<vi.?c0[^a-z]din\>|\<vi.?codin.?\>|v[^a-
z]codin|\<..?a1ium\>|\<val.?iu.?m\>|\<v@[^a-z]ium\>|\<vi0xx\>|va-[^a-
z]ium|\<va1[ ]?[ ]?ium\>|\<valliuum\>|\<pr.ozac\>|\<vall.um\>|\<amb.jen\>|\<ui.tram\>
|\<pro.zac\>|\<val..um\>|\<val...um\>|\<pr...zac\>|>mbie.n|\<v a
l|\<va..um\>|\<v.alium\>|\<va.llum\>|\<va.ll.?um\>|\<va.lium\>|\<vali.um\>|\<przoac|\
<levtira|\<zolotf|lorazpeam|prozaac)
* (\<vi.gra\>|\<v1a[^a-z]gra\>|[^a-z]/iaa?gra\>|\<vii?aa?graa?|\<v[^a-
z]agra\>|\<via[ ][ ]?gra\>|\<vi[ ]+graa?|\<v..agra\>|\<v.agg?ra\>|\<v.agr..a|>i.agra|
g r a|v i
a|\<vi..ra\>|\<v.iagra\>|\<v..agra\>|\<v..agra\>|\<viag.ra\>|\<vaigra|\<vair.a\>|\<va
i..ra\>|\<vai.?gra\>)
* (\<cialli.s\>|\<cia[^a-
z]ii?s\>|\<cia[ ]?[ ]?1is\>|\<cia.?l.?is\>|\<cai[ ]+llis\>|\<xa.?naa?x\>|\<xan[ ]?ax\
>|\<x[^a-z]an@x\>|\<meds\>|\<[0-
9]o-?%|codeinn?e|\<c..alis\>|\<xa.nax\>|\<c.all.s\>|\<xan...ax\>|a.nax\>|i.alis\>|a 1
[it] s|c [it] a 1|c / a|1 /
s|\<ci...lis\>|\<c.ialis\>|\<ci.alls\>|\<c..al.s\>|\<cial.is\>|\<cailis|\<caillis|\<x
naax|\<ca.ilis\>)
* (http://|\<www\>)
{
  LOG="Email Trashed by Recipe_4$EOL"
```

```
  :0 :
  /dev/null
}



## Recipe_5:
##
## This is another recipe from your instructor's spam filter
##
:0 HB
* charset="koi8-r"
{
  LOG="Email trashed because it is in Russian$EOL"

  :0 :
  /dev/null
}



## Recipe_6:
##
## The rest of the email to your special account will be
## deposited in the file spamFolder
##
:0 :
spamFolder
```

Log file