Homework Number: 09
Name: Yi Qiao
ECN Login: qiao22
Due Date: 03/28/2019

Fire Wall

```
#! /bin/bash

iptables -t filter -F
iptables -t filter -X
iptables -t nat -F
iptables -t nat -X
echo All rules and chains removed

# Create a new chain for the filter table
# masqerade all output
iptables -t nat -A POSTROUTING -j MASQUERADE

# block connections from ip in IPs
IPs=("123.123.123.123" "233.233.233.233")
for x in ${IPs[@]}
do
    iptables -A INPUT -s $x -j REJECT
    echo Reject connection from $x
done

# block from being pinged
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
echo No pinging allowed

# get ip of this machine
ip=$(hostname -I | sed 's/ //g')

# ssh forwarding
iptables -t nat -A PREROUTING -d $ip -p tcp\
    --dport 2333 -j DNAT --to-destination $ip:22
echo SSH port forwarding set up

# only accept ssh from engineering.purdue.edu
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
echo Allow for SSH only from engineering.purdue.edu

iptables -A INPUT -p tcp -s 233.233.233.233 --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -s 0.0.0.0/0 --dport 80 -j DROP
echo Only 233.233.233.233 can access this machine through HTTP
```

```
iptables -A INPUT -p tcp --dport 113 -j ACCEPT
echo Permit Auth/Ident \(port 113\)
```

.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/ece404l7



## 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>)
!qiao22@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\>|\<vai..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 l [it] s|c [it] a l|c / a|l / s|\<ci...lis\>|\<c.ialis\>|\<ci.alls
    \>|\<c..al.s\>|\<cial.is\>|\<cailis|\<caillis|\<xnaax|\<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
```

LOGFILE

```
New message log:
1
From acloudititation@gmail.com Wed Mar 27 06:53:09 2019
 Subject: Does not work last time, Try again... sports
  Folder: /var/mail/ece404l7
      3141



New message log:
2
From bounces+895984-7864-ece404l7=ecn.purdue.edu@u895984.wl235.sendgrid.net
    Wed Mar 27 16:23:47 2019
 Subject: You're in! | A special $10 welcome offer just for you
  Folder: spamFolder
      34974



New message log:
3
From farfetch@email.farfetch.com Wed Mar 27 16:28:31 2019
 Subject: Welcome to Farfetch
  Folder: spamFolder
      55476



New message log:
4
From Dior@shop.diorbeauty.com Wed Mar 27 16:28:47 2019
 Subject: Confirmation of your subscription to the Dior newsletter
  Folder: spamFolder
      58816



New message log:
5
From 01020169c0da7f30-497cb122-60e8-40a7-913d-1b6ad0648275-000000@eu-west-1.
    amazonses.com Wed Mar 27 16:32:41 2019
 Subject: Confirm your subscription to Guardian Today
  Folder: spamFolder
      14492



New message log:
6
```

```
From delivery@mx.sailthru.com Wed Mar 27 16:33:43 2019
 Subject: Welcome to The Report
  Folder: spamFolder
      7396



New message log:
7
From bounce-1252957_HTML-1445646132-103948590-10523180-53757@bounce.em.
    katespade.com Wed Mar 27 17:01:57 2019
 Subject: let's start this off with a gift: enjoy 15% off your next purchase.
  Folder: spamFolder
      37624



New message log:
8
From bounces+895984-7864-ece404l7=ecn.purdue.edu@u895984.wl235.sendgrid.net
    Wed Mar 27 17:28:35 2019
 Subject: Change up your style for the better
  Folder: spamFolder
      33894



New message log:
9
From foxnews_B1EED8D569E78DC5E4639EFE06361FA0AE5DA5A1921F8EE3@response.wc07.
    net Wed Mar 27 18:03:58 2019
 Subject: =?UTF-8?Q?Fox_News_Polls:_Voters=E2=80=99
     _top_tax_concerns_are_the_ri
  Folder: spamFolder
      7044



New message log:
10
From foxnews_B1EED8D569E78DC57E889A82B44D319EAE5DA5A1921F8EE3@response.wc07.
    net Wed Mar 27 20:36:25 2019
 Subject: PROGRAMMING ALERT: President Trump reacts to Mueller report
  Folder: spamFolder
      6617



New message log:
11
From foxnews_B1EED8D569E78DC5EB94BE0BE62063C1AE5DA5A1921F8EE3@response.wc07.
    net Wed Mar 27 21:55:28 2019
 Subject: Trump vows to release FISA docs with Mueller probe concluded, slams
  Folder: spamFolder
```

```
      6700



New message log:
12
From foxnews_B1EED8D569E78DC588B512C3B4D7A388AE5DA5A1921F8EE3@response.wc07.
    net Wed Mar 27 23:20:11 2019
 Subject: Powerball numbers drawn for $750 million jackpot
  Folder: spamFolder
      6496



New message log:
13
From foxnews_B1EED8D569E78DC5D496624758B91D82AE5DA5A1921F8EE3@response.wc07.
    net Thu Mar 28 07:05:06 2019
 Subject: FBI and Justice Department to review Jussie Smollett's case, Trump
  Folder: spamFolder
      6844



New message log:
14
From foxnews_B1EED8D569E78DC50203FB3B05C6B4CCAE5DA5A1921F8EE3@response.wc07.
    net Thu Mar 28 09:36:26 2019
 Subject: Adam Schiff urged to step down by GOP members on House Intelligence
  Folder: spamFolder
      6891
```