# Homework Number: 09

# Name: Yuan Liu

# ECN login: liu1827

# Due Date: 04/02/2020

**Firewall404.sh:**

#! /bin/sh

# Homework Number: 09

# Name: Yuan Liu

# ECN Login: liu1827

# Due Date: 04/02/2020

# 1: Remove any previous rules or chains

sudo iptables -t filter -F

sudo iptables -t filter -X

sudo iptables -t mangle -F

sudo iptables -t mangle -X

sudo iptables -t nat    -F

sudo iptables -t nat    -X

sudo iptables -t raw    -F

sudo iptables -t raw    -X

# 2: Change source IP to my own IP

sudo iptables -t nat -A POSTROUTING -j MASQUERADE

# 3: Block a list of IP address

sudo iptables -A INPUT -s 123.123.123.123 -j REJECT

sudo iptables -A INPUT -s 125.125.125.125 -j REJECT

sudo iptables -A INPUT -s 222.222.222.222 -j REJECT

# 4: Block from being pinged

sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

# 5: Set up port-forwarding from an unused port to port 22

sudo iptables -t nat -A PREROUTING -p tcp -d 10.0.2.15 --dport 80 -j DNAT --to-destination 10.0.2.15:22

# 6: Allow for SSH access only from engineering.purdue.edu

sudo iptables -A INPUT -s 128.46.0.0 -p tcp --dport 22 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 22 -j REJECT

# 7: Allow only a single IP address

sudo iptables -A INPUT -s 124.124.124.124 -p tcp --dport 80 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 80 -j REJECT

# 8: Permit Auth/Ident

sudo iptables -A INPUT -p tcp --dport 133 -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/ece404k3

## 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>)

!liu1827@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 liu1827@purdue.edu Thu Apr 2 13:56:25 2020

Subject: sports

Folder: /var/mail/ece404k3 5537

New message log:

2

procmail: Couldn't determine implicit lockfile from "/usr/sbin/sendmail"

From liu1827@purdue.edu Thu Apr 2 13:59:46 2020

Subject: 123

Folder: /usr/sbin/sendmail -oi liu1827@purdue.edu 5482

New message log:

3

From ThisWeekonOWN-xtdlua1yuidurjkid1i@cmail19.com Thu Apr 2 14:03:04 2020

Subject: The Wait Is Over! Watch the Season 5 Premiere of 'If Loving You Is Wr

Folder: spamFolder 157308

New message log:

4

procmail: Couldn't determine implicit lockfile from "/usr/sbin/sendmail"

From liu1827@purdue.edu Thu Apr 2 14:09:24 2020

Subject: 123

Folder: /usr/sbin/sendmail -oi liu1827@purdue.edu 5488

New message log:

5

From lawrencelew1225@gmail.com Thu Apr 2 14:10:36 2020

Subject: 123

Folder: spamFolder 4549