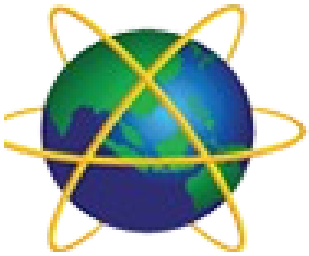


A • P • U

ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

ASSIGNMENT

CT106-3-2-SNA

SYSTEM AND NETWORK ADMINISTRATION

COURSE TITLE:

NETWORK ADMINISTRATION PROJECT

INTAKE CODE:

UC2F1902IT(NC)/UC2F1902IT(CC)

PREPARED BY:

LOKE YE WEI (TP054979)

LOUIS D GARCIA (TP055186)

AK MUHD AMMAR MU'MIN BIN PG MERALI (TP049072)

HAND OUT DATE:

25TH MARCH 2019

HAND IN DATE:

30TH MAY 2019

Contents

Individual Component

1.0 NFS – Loke Yi Wei (TP054979)

a) Put the Dovecot mail directory and the webserver VirtualHost DocumentRoot directories on a new VM NFS mount

b) Set up the VirtualHost users on the NFS server, and allow them ssh access to their staging area.

c) Run the staging area to document root cron jobs on the NFS server

Owner: Loke Yi Wei (TP054979)

Objective – what this does for the system

Network File System (NFS) is a client and server application that lets computer user view, provide the ability to store and update files on a remote computer. Users can access the files and make changes any time using any computer as long as the NFS service is available on all the machines.

List the relevant configuration files, and for each one briefly describe what was done

Locate the required files

/home/vmail/

/var/monkey/htdocs/

1. Find the directory for dovecot mail and VirtualHost DocumentRoot. Location on the files on different machine:
   Dovecot mail: /home/vmail/ (MailHost)
   VirtualHost DocumentRoot: /var/monkey/htdocs/ (WebServer)

Configuring exports file

/etc/exports

1. Go to /etc/exports file to tell the system what files and the path to the files for exporting to another server.
2. In WebServer (VirtualHost DocumentRoot). Edit the file as below:
   /var/monkey/htdocs *(ro,sync,no_root_squash,no_subtree_check)
   The * in the file indicates that all the files in that directory is visible to others and can be mounted to the NFS server. “ro” permission indicates that the file can be read and visible to all other users.
3. In MailHost (Dovecot mail). Edit the file as below:
   /home/vmail *(rw,sync,no_root_squash,no_subtree_check)
   “rw” permission indicates that the file can be read and write.

Configure the NFS service executable

1. After configuring the paths for exporting files, we need to get the NFS service running in our system. Therefore, we need to change the permission of the file to be executable using command for all machines:
   chmod 755 /etc/rc.d/rc.nfsd
   chmod 755 /etc/rc.d/rc.rpc

Checking the available directories for mounting

1. Check the available directories for mounting by executing the code in the gateway machine as follows to show the available directories for mounting in all connected machines:
   showmount -e 192.xx.xx.xx(ip address for WebServer and MailHost)
2. The command below will show the available ports in the NFS services in all the machines:
   rpcinfo -p 192.xx.xx.xx(ip address for WebServer and MailHost)

Mounting the files to NFS server

1. Mount files to the NFS server (gateway), executing the command as follows:
   mount 192.xx.xx.xx: /var/monkey/htdocs /home (example of mounting)

The program will mount the DocumentRoot files, in this case, /var/monkey/htdocs/ and its content to the /home directory on the NFS server (gateway).

Set up staging area and add new user

1. To set up a staging area on the NFS server (gateway). Configure /var/tmp/ for the staging area and created a directory called “raouf” for user account “raouf” and set proper permissions to the staging area.
2. By using “adduser” command, a user called “raouf” with “raouf1” as password added to the system.

Set up new VirtualHost

/usr/monkey/monkey.conf

1. Create a new VirtualHost by editing the /usr/monkey/monkey.conf file and modify it as follows:
   <Virtualhost>
   VirtualServerName **raouf.tinynet.edu**
   VirtualDocumentRoot **/var/monkey/htdocs.raouf**
   VirtualScriptAlias /cgi-bin/ **/var/monkey/htdocs/raouf/scripts/**
   VirtuaForceGetDir off
   </Virtualhost>

Allow user to use SSH service to access the staging area

/etc/ssh/sshd_config

1. We need to allow the user “raouf” to access the staging area /var/tmp/ by using SSH service. Go to /etc/ssh/sshd_config and edit the file as follows:
   # Authentication
   AllowUsers raouf
2. Restart the SSH service to let the changes take place by execute command:
   /etc/rc.d/rc.sshd stop
   /etc/rc.d/rc.sshd start

Set up cron job to run the staging area

/etc/cron.hourly

1. Set up a shell script and name it as “stagearea”. Next, tell the system to execute the staging area by typing the required code in the file.
2. After the shell script has been set up, create a new cron job by executing the code as follows:

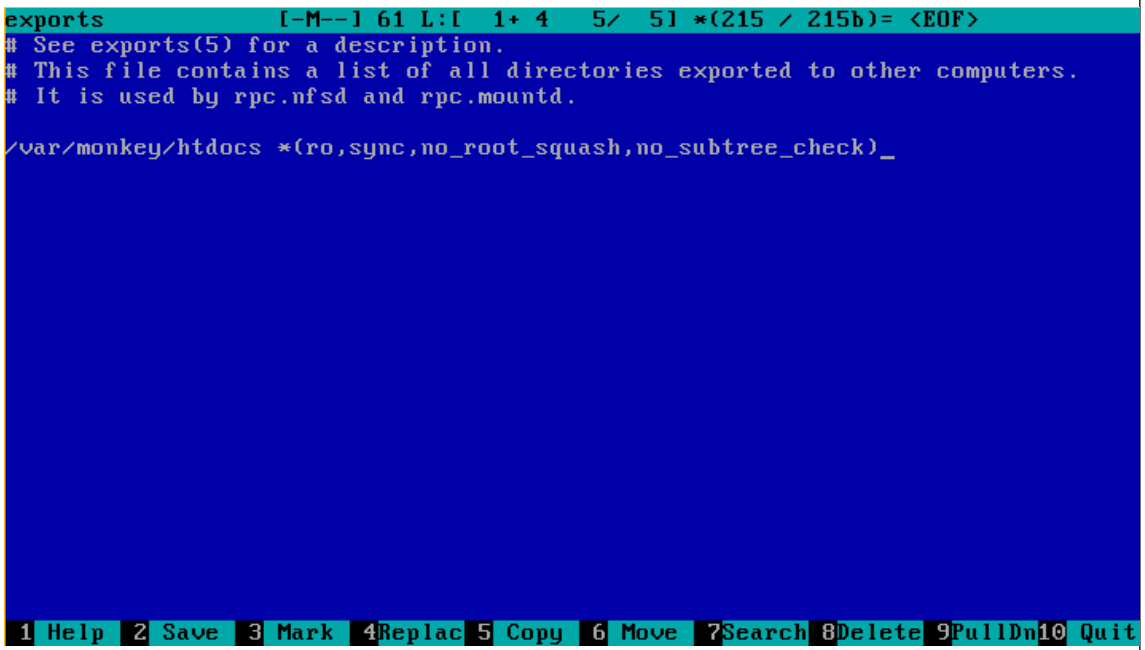
   crontab -e

   47 * * * * var/tmp/ /etc/cron.hourly/stagearea
3. The system will now run the stagearea shell script every 47 minutes.

As all the steps above are done, the system is now able to mount files with NFS server (gateway) from the available directories mentioned. The system will also have a staging area and VirtualHost users can access the staging area with SSH service. The cron job is also running every 47 minutes.

Screenshots of tests, with explanations

/etc/exports file for stating VirtualHost DocumentRoot directory



/etc/exports file for stating dovecot mail directory

```
exports           [----] 54 L:[  1+ 4   5/  5] *(208 / 208b)= <EOF>
# See exports(5) for a description.
# This file contains a list of all directories exported to other computers.
# It is used by rpc.nfsd and rpc.mountd.

/home/vmail *(rw,sync,no_root_squash,no_subtree_check)_

 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

Output when starting /etc/rc.d/rc.nfsd file and /etc/rc.d/rc.rpc services in gateway

```
root@gateway:/etc/rc.d# /etc/rc.d/rc.nfsd start
root@gateway:/etc/rc.d# /etc/rc.d/rc.rpc start
Starting RPC portmapper:  /sbin/rpc.portmap
Starting RPC NSM (Network Status Monitor):  /sbin/rpc.statd
root@gateway:/etc/rc.d#
```

Output when starting /etc/rc.d/rc.nfsd and /etc/rc.d/rc.rpc services in MailHost

```
Starting RPC portmapper:  /sbin/rpc.portmap
Starting RPC NSM (Network Status Monitor):  /sbin/rpc.statd
Starting NFS server daemons:
  /usr/sbin/exportfs -r
exportfs: Warning: /home/vmail does not support NFS export.
  /usr/sbin/rpc.nfsd 8
  /usr/sbin/rpc.mountd
[root@nch1 rc.d]$
```

Showing list of available mount directories in gateway, VirtualHost Document Root for WebServer (var/monkey/htdocs) and dovecot mail directory in MailHost (/home/vmail)

```
root@gateway:/etc/rc.d# showmount -e 192.168.56.145
Export list for 192.168.56.145:
/var/monkey/htdocs *
root@gateway:/etc/rc.d# showmount -e 192.168.76.237
Export list for 192.168.76.237:
/home/vmail *
root@gateway:/etc/rc.d#
```

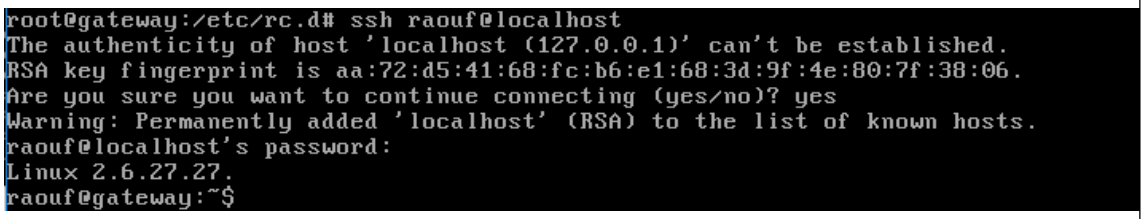
Information for rpc services when executing rpcinfo -p ipaddress

```
root@gateway:/etc/rc.d# rpcinfo -p 192.168.76.237
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  52389  status
    100024    1   tcp  33721  status
    100021    1   udp  46961  nlockmgr
    100021    3   udp  46961  nlockmgr
    100021    4   udp  46961  nlockmgr
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100021    1   tcp  47101  nlockmgr
    100021    3   tcp  47101  nlockmgr
    100021    4   tcp  47101  nlockmgr
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100005    1   udp  36766  mountd
    100005    1   tcp  37801  mountd
    100005    2   udp  36766  mountd
    100005    2   tcp  37801  mountd
    100005    3   udp  36766  mountd
    100005    3   tcp  37801  mountd
root@gateway:/etc/rc.d# _
```

Configuration in /etc/ssh/sshd_config file

```
sshd_config        [----] 16 L:[ 24+15  39/121] *(1124/3326b)=   10 0x00A
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Logging
# obsoletes QuietMode and FascistLogging
SyslogFacility USER
#LogLevel INFO

# Authentication:
AllowUsers raouf_

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

Output of user account “raouf” able to access SSH service.



Obstacles encountered, obstacles overcome

The NFS sever was not able to mount the files from another machine starting. At the end the problem overcome by setting the right permission for the file.

Any Outstanding/Unresolved Issues

N/A

2.0 SUDO - LOUIS D GARCIA (TP055186)

Choose one server and

a) Change the startup display to show a random fortune in color each time a user logs in rather than the command summary and root login

b) Allow no root access: force users to use *sudo*

c) Have different color prompts for normal users and root

Owner: LOUIS D GARCIA (TP055186)

Objective – what this does for the system

Sudo is a standard way to give users some administrative rights without giving out the root password. Changing the startup display to show a random fortune in color and different users color prompts to create a relax and colorful environment system.

List the relevant configuration files, and for each one briefly describes what was done

Create normal users in the system (WebServer)

1. In this task, multiple user accounts are required to set up in the system to carry out the functions.
2. We created three normal user accounts in the system. We created the user accounts by execute “adduser” command and enter the user details as follows:
   #user account 1: apu; password: apu1
   #user account 2: loke; password: loke1
   #user account 3: raouf; password: raouf1
3. After the “adduser” command and all the required information has been entered,
   the system will now have three user accounts set up and ready to use.

Make changes to sudoers

/etc/sudoers

1. We need to force the users to use sudo. By configure the /etc/sudoers file, the system will force the users to use sudo.
2. Therefore, we need to go to /etc/sudoers file and edit the file as follows:

   # User privilege specification

   root ALL=(ALL) ALL

   apu ALL=(ALL) ALL

   loke ALL=(ALL) ALL

   raouf ALL=(ALL) /usr/sbin/monkey -D
3. User “raouf” is configured to have access to /usr/sbin/monkey -D only to make the output to have significant difference with the other users.

Different color prompts for normal users and root

/etc/profile

1. Different color prompts are needed to differentiate the user type that logged in into the system.
2. Go to /etc/profile file and edit the file as below:

   # Set a default shell prompt

   …

   else

   # PS1='\u@\h:\w\$ ' # commented this line

   if ["`id -u`" = "0"]; then

   PS1='[\[\033[01;31m\]\u@\h \[\033[01;34m\]\W\[\033[00m\]]#
   '

   else

   PS1='[\[\033[01;32m\]\u@\h \[\033[01;34m\]\W\[\033[00m\]]$
   '

   fi

   fi

With the configuration above, the command is to tell the system to verify the type of the user logged in. If the user ID is = 0 (root), the system will use red color (01;31m). However, if the user ID is not = 0 (not root), which is another user. Then the system will use green color (01;32m) as color prompts.

After configured, the system (WebServer) won't allow any root access and force users to use sudo. The system will also show red color prompts to user logged in as root account and normal user account will be show in green color prompt.

Screenshots of tests, with explanations

Creating normal user

```
Press ENTER to continue without adding any additional groups
Or press the UP arrow to add/select/edit additional groups
:

Home directory [ /home/apu ]

Shell [ /bin/bash ]

Expiry date (YYYY-MM-DD) []:

New account will be created as follows:

---------------------------------------
Login name.......:  apu
UID..............:  001
Initial group....:  users
Additional groups:  [ None ]
Home directory...:  /home/apu
Shell............:  /bin/bash
Expiry date......:  [ Never ]

This is it... if you want to bail out, hit Control-C.  Otherwise, press
ENTER to go ahead and make the account.
```

```
Creating new account...


Changing the user information for apu
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Changing password for apu
Enter the new password (minimum of 5, maximum of 127 characters)
Please use a combination of upper and lower case letters and numbers.
New password: ****
Bad password: too short.
Warning: weak password (enter it again to use it anyway).
New password: ****
Re-enter new password: ****
Password changed.


Account setup complete.
root@nah1:~# _
```

Output of sudo

```
root@nah1:~# /etc/rc.d/rc.sshd
usage /etc/rc.d/rc.sshd start|stop|restart
root@nah1:~# /etc/rc.d/rc.sshd start
root@nah1:~# /etc/rc.d/rc.sshd stop
root@nah1:~# ls -1 /usr/bin/sudo
/usr/bin/sudo*
root@nah1:~#
```

Configuration in /etc/sudoers file

```
sudoers            [----]  0 L:[ 11+22  33/ 33] *(681 / 681b)= <EOF>

# Cmnd alias specification

# Defaults specification

# Runas alias specification

# User privilege specification
root<-->ALL=(ALL) ALL
apu<--->ALL=(ALL) ALL
loke<-->ALL=(ALL) ALL
raouf<->ALL=(ALL) /usr/sbin/monkey -D

# Uncomment to allow people in group wheel to run all commands
# %wheel<------>ALL=(ALL)<----->ALL

# Same thing without a password
# %wheel<------>ALL=(ALL)<----->NOPASSWD: ALL

# Samples
# %users  ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
# %users  localhost=/sbin/shutdown -h now
_
 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

Output of “raouf” acessing to midnight commander as root

```
nah1 login: raouf
Password: ******

raouf@nah1:~$ sudo mc

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:
Sorry, user raouf is not allowed to execute '/usr/bin/mc' as root on nah1.
raouf@nah1:~$ _
```

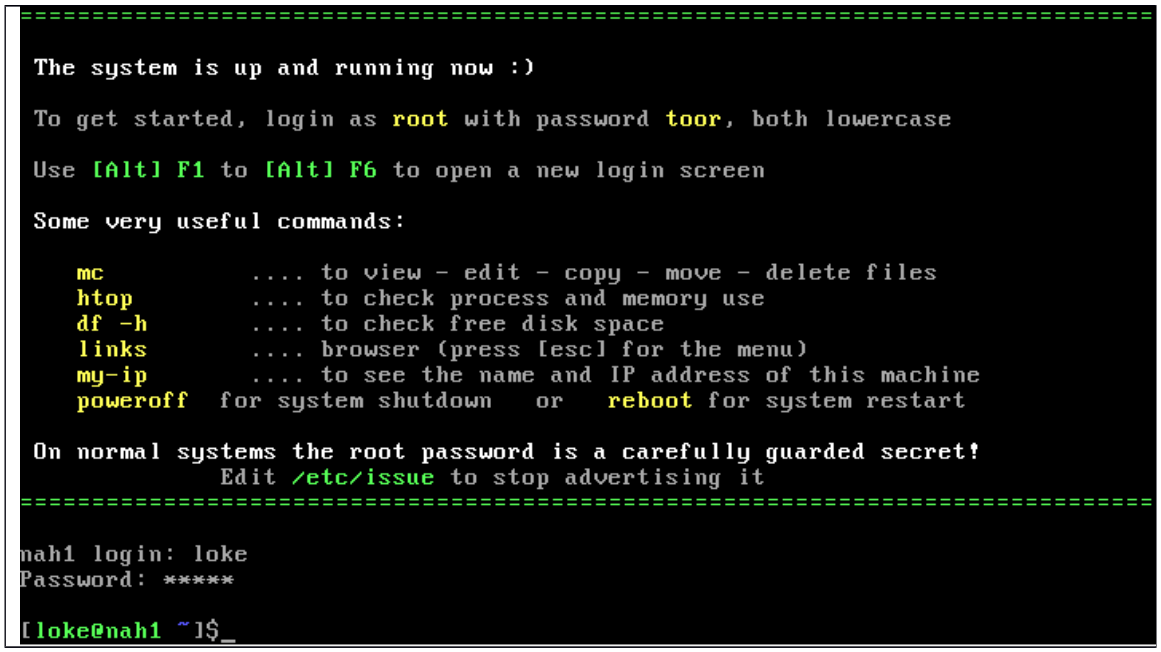
Output of “raouf” accessing to monkey script

```
raouf@nah1:~$ sudo /usr/sbin/monkey -D
Monkey HTTP Daemon 0.9.2
Built : Jan  6 2009 00:26:48
Home  : http://monkeyd.sourceforge.net
Error: Port busy.
raouf@nah1:~$
```

The colour prompt for “root” is red

```
 The system is up and running now :)

 To get started, login as root with password toor, both lowercase

 Use [Alt] F1 to [Alt] F6 to open a new login screen

 Some very useful commands:

    mc           .... to view - edit - copy - move - delete files
    htop         .... to check process and memory use
    df -h        .... to check free disk space
    links        .... browser (press [esc] for the menu)
    my-ip        .... to see the name and IP address of this machine
    poweroff  for system shutdown   or   reboot for system restart

 On normal systems the root password is a carefully guarded secret!
              Edit /etc/issue to stop advertising it
================================================================================

nah1 login: root
Password: ****

Last login: Sun May 26 09:09:59 +0000 2019 on tty1.
[root@nah1 ~]#
```

The color prompt for normal users is green



Obstacles encountered, obstacles overcome

During the modify on color prompts in /etc/profile, minor typing mistakes causing the users color prompts unable to show up. At the end of it, successfully overcome it by scroll down and copy the similar symbol and replace at necessary part.

Any Outstanding/Unresolved Issues

N/A

3.0 Basic VPN - AK MUHD AMMAR MU'MIN BIN PG MERALI (TP049072)

a) Setup *openvpn* using static keys

b) Have two sets of config files, one for tun and one for tap

Owner: AK MUHD AMMAR MU'MIN BIN PG MERALI (TP049072)

Objective – what this does for the system

Using the static key to encrypt the connection between server and client. It implements virtual private network techniques for creating secure point to point connection in bridged configurations.

List the relevant configuration files, and for each one briefly describes what was done

General configuration

1. Switch the current working directory to the TinyNetConfig.iso cd located and run the SetupMenu file.
2. In the SetupMenu file, choose "Install Other Packages" and install "OpenVPN" in order to set up using static keys later.

Key and certificate generation

/usr/doc/openvpn-2.0.9/easy-ra

1. Swap the working directory to /usr/doc/openvpn-2.0.9/easy-ra/vars file and clean all the existing files before building a new certificate and static key for openvpn service. Using command below:
   Cd /usr/doc/openvpn-2.0.9/easy-ra
   . ./vars
2. Clean all of the existing configuration files there before building a new certificate and a static key for openvpn service. Using command below:
   ./clean-all

3. Build a new certificate and static key by command:
   ./build-ca
4. Information are needed to fill up that will be incorporated into the certificate request. Server and client have to configure as the same, therefore using command ./build-key-server for server and client. Once everything is done, the certificate and key will be generated. Server and client run the same certificate and key for authentication to communicate.
5. In the same working directory, use the command ./build-dh to generate a Diffie-Hellman encryption key which will encrypts the communication between server and client.

Sever configuration

server.conf

1. Defines the port the openvpn listens on which is port 1194.
2. Proto tcp defines which server use and tcp is used because it will create a routed IP tunnel for tun service.
3. Server configures server mode and supplies a VPN subnet and the server will take 10.8.0.1 for itself as default.
4. Use “keepalive 10 120”, causes ping-like message to be sent back and forth over the link so that each side knows when the other side has gone down. 10 20 defines that pinging every 10 seconds, assuming that remote peer is down if no ping is received during a 120 seconds time period.
5. User “comp-lzo” enables compression on the VPN link. And enable “persist-key” and “persist-tun” options will intend to avoid accessing certain resources on restart.
6. “status openvpn-status.log” outputs a short status file including current connections and rewrite the file openvpn-status.log every minute.

Client configuration

client.conf

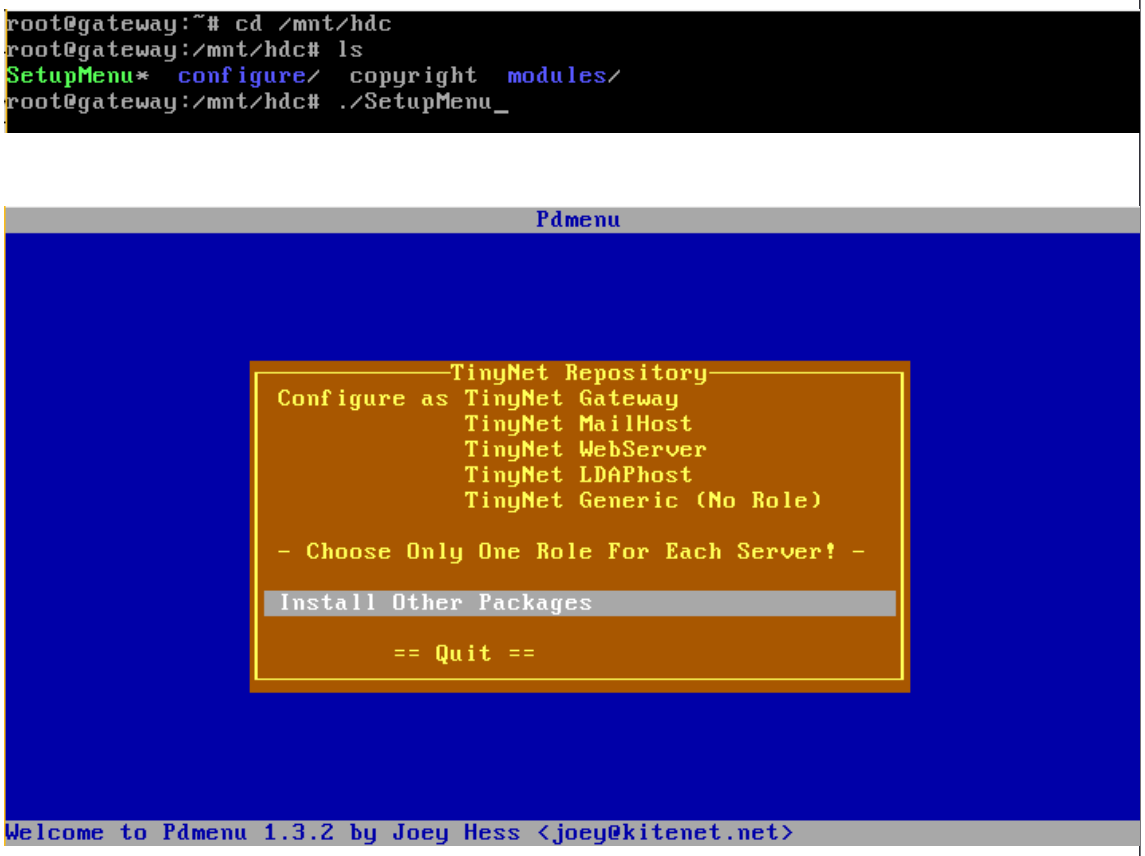
1. Almost same configure as server.conf but modify some, specifies “client” for

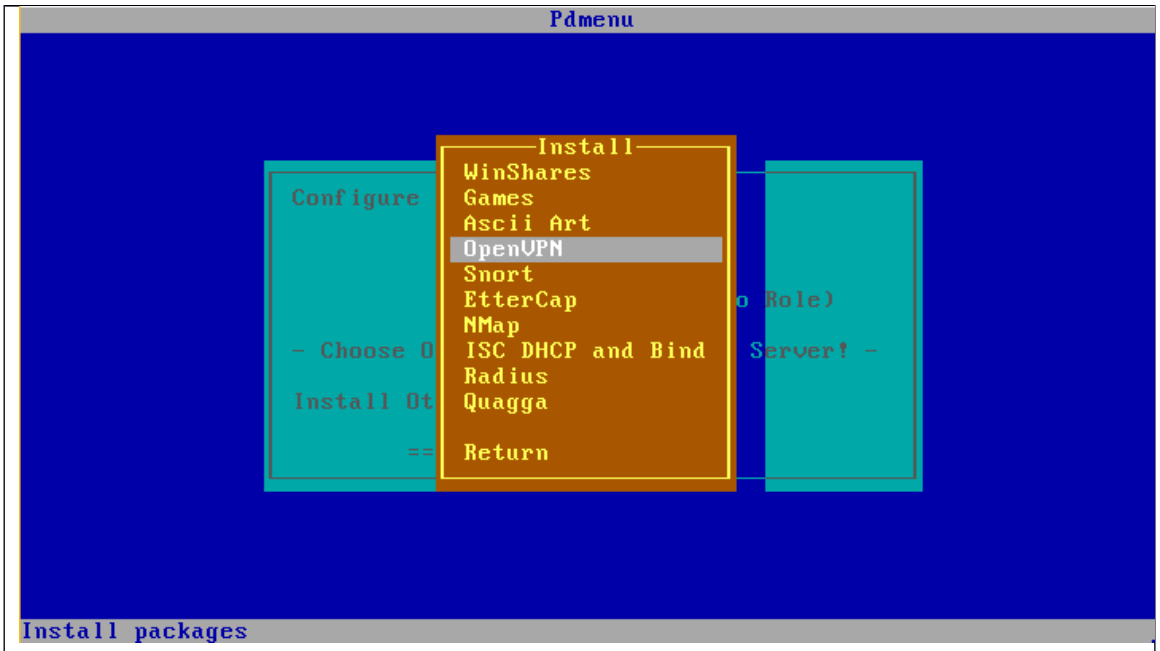
the role in that particular machine.

2. “remote 192.168.76.101 1194” defines the internet protocol and port of the server.
3. “nobind” to tell the client do not be binded to a specific local port.

Screenshots of tests, with explanations

Run SetupMenu file to install OpenVPN






```
Installing iproute2-2.6.26-1.lzm ...done.
Installing openvpn-2.0.9-1.lzm ...done.

Press Enter to return to Pdmenu._
```

Building new certificate and static key

```
root@gateway:~# cd /usr/doc/openvpn-2.0.9/easy-rsa
root@gateway:/usr/doc/openvpn-2.0.9/easy-rsa# . ./vars
NOTE: when you run ./clean-all, I will be doing a rm -rf on /usr/doc/openvpn-2.
.9/easy-rsa/keys
root@gateway:/usr/doc/openvpn-2.0.9/easy-rsa# ./clean-all
root@gateway:/usr/doc/openvpn-2.0.9/easy-rsa# ./build-ca
Generating a 1024 bit RSA private key
................++++++
.....++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [KG]:
```

Filling up the instruction to generate the certificate and key

```
root@gateway:/usr/doc/openvpn-2.0.9/easy-rsa# . ./vars
NOTE: when you run ./clean-all, I will be doing a rm -rf on /usr/doc/openvpn-2.
.9/easy-rsa/keys
root@gateway:/usr/doc/openvpn-2.0.9/easy-rsa# ./clean-all
root@gateway:/usr/doc/openvpn-2.0.9/easy-rsa# ./build-ca
Generating a 1024 bit RSA private key
................++++++
.....++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [KG]:MY
State or Province Name (full name) [NA]:KL
Locality Name (eg, city) [BISHKEK]:KP
Organization Name (eg, company) [OpenVPN-TEST]:APU
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:YIWEI
Email Address [me@myhost.mydomain]:MAX@LOKE.YIWEI
root@gateway:/usr/doc/openvpn-2.0.9/easy-rsa#
```

Building key for server to generate a set of server keys and certificates

```
writing new private key to 'YIWEI.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [KG]:MY
State or Province Name (full name) [NA]:KL
Locality Name (eg, city) [BISHKEK]:KP
Organization Name (eg, company) [OpenVPN-TEST]:APU
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:YIWEI
Email Address [me@myhost.mydomain]:MAX@LOKE.YIWEI
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:admin
An optional company name []:MAX
Using configuration from /usr/doc/openvpn-2.0.9/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'MY'
stateOrProvinceName   :PRINTABLE:'KL'
localityName          :PRINTABLE:'KP'
organizationName      :PRINTABLE:'APU'
organizationalUnitName:PRINTABLE:'IT'
commonName            :PRINTABLE:'YIWEI'
emailAddress          :IA5STRING:'MAX@LOKE.YIWEI'
Certificate is to be certified until May 22 17:38:00 2029 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
root@gateway:/usr/doc/openvpn-2.0.9/easy-rsa#
```

Generate encrytion key using ./build-dh command

```
root@gateway:/usr/doc/openvpn-2.0.9/easy-rsa# ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.............................+.....................................................
.....................................................................................
.........................+.........................+.............+.................
.....................................................................................
.....+.....................................+.....................................
.............+.....................................................................
.....................+.....................................+.....................+..
.....................................................................................
.....................................+.....................+.........+.......
.............+.....................................................................
.....................................................................+.....................+..
.....................................................................................
.....................+.............+.....................................................
.....................................+.....................................+.........
.....................................................................................
+........+.....................................+.....................+.........
.....................................................................................
...................++*++++++*
root@gateway:/usr/doc/openvpn-2.0.9/easy-rsa#
```

Configuration for server.conf

```
server.conf        [----] 25 L:[  1+11  12/305] *(173 /10145b)=   10 0x00A
port 1194
proto tcp
dev tun
ca ca.crt
cert server.crt
dh dh1024.pem
server 10.8.0.0 255.255.255.0
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log_

#############################################################
# Sample OpenVPN 2.0 config file for                        #
# multi-client server.                                      #
#                                                           #
# This file is for the server side                          #
# of a many-clients <-> one-server                          #
# OpenVPN configuration.                                    #
#                                                           #
# OpenVPN also supports                                     #
# single-machine <-> single-machine                         #
 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

Configuration for client.conf

```
client.conf        [----]  8 L:[  1+11  12/137] *(154 /3583b)=   10 0x00A
cleint
dev tun
proto udp
remote 192.168.76.101 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
comp-lzo

################################################
# Sample client-side OpenVPN 2.0 config file   #
# for connecting to multi-client server.       #
#                                              #
# This configuration can be used by multiple   #
# clients, however each client should have     #
# its own cert and key files.                  #
#                                              #
# On Windows, you might want to rename this    #
# file so it has a .ovpn extension             #
 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

Obstacles encountered, obstacles overcome

Server.conf and client.conf missing, no overcome solution.

Any Outstanding/Unresolved Issues

Yes, server.conf and client.conf are missing and can’t be found.

Group Component

4.0 Base System

a) using stunnel for communication between servers and

b) using the mail submission port.

Owner: Loke Yi Wei (TP04979)

Objective – what this does for the system

The configuration of stunnel is to create a secure connection between client and server. The mail submission port is a computer program to receive electronic mail and mail user agent. It ensures there is no error message send to the recipient and there is a dedicated port number, which is port number 587 that allow user to connect with their domain to send a mail.

List the relevant configuration files, and for each one briefly describe what was done

The following steps is configuration of each virtual machines (Gateway, Mailhost, LDAPHost, Webserver) for create an environment to send mail to the Mailhost.

Create all four virtual machines

1. OS type linux 2.6 (32bit), RAM 96MB, virtual storage with vdi and 200MB size and set fixed size in order to execute file faster.
2. Install the base system into partition.

After all the four virtual machines are set up

/etc/rc.d/rc.xinetd

1. User have to configure the network services such as telnet, IMAP and etc. in

Gateway and Mailhost.

2. Rename the /etc/rc.d/rc.xinetd file to /etc/rc.d/inetd file and set the execute bits.
3. Go the /etc/xinetd.d/telnet file, uncomment the “only_from” line and enable only from the localhost address as below code:

   only_from = 127.0.0.1

   disable = no
4. Use “htop” to check either the /etc/rc.d/rc.inetd is running, restart it to let the changes take place.

   /etc/rc.d/rc.inetd stop

   /etc/rc.d/rc.inetd start
5. Ensure the SMTP and IMAP can communicate by using following command in Mailhost:

   imap can communicate well. In mail host:

   telnet localhost 25

   HELO mailhost.tinynet.edu

   MAIL From: TheBoss@example.com

   RCPT To: mailadmin@mailhost.tinynet.edu

   DATA

   Subject: System Upgrade

   We are upgrading the system. Please send me your password.

   . (Yes, it just a dot)

   QUIT

To make sure the mail can be retrieved by speaking IMAP.

1. use telnet on the MailHost to act like a mail client. “telnet localhost 143” is the dovecot imap service is listening on port 143. Command as following:

   telnet localhost 143

   11 login “mailadmin@mailhost.tinynet.edu” “admin” 21

   23 select “INBOX”

   32 FETCH 1 BODY[]

   34 LOGOUT

2. Check the mailbox of Mailhost whether did the it receive mail from Gateway.

Configure to let the mail send from Webserver to Gateway can be forward to Mailhost

1. Start Gateway and Mailhost. In Mailhost, configure user permission /var/log/dovecot.IMAP file and /var/log/dovecot.LDA file to vmail, so the users is able to communicate to the Mailhost and save the information into "postfix.log". Use command to configure:
   chown vmail:vmail /var/log/dovecot.IMAP
   chown vmail:vmail /var/log/dovecot.LDA
2. Change the email that would like to address for by edit /home/vmail/mail-pwd to have mailhost not mail.tinynet.edu:
   # here is the important one – all the system mail arrives here
   mailadmin@mailhost.tinynet.edu:{PLAIN}admin::::::

Configuration for Webserver

1. Change the default location for serving webpages Server_root in /etc/monkey/monkey.conf file
   /var/monkey/htdocs to **/var/www**
2. In the same file as previous, modify the Indexfile directive by swapping the comment with below one line to add index.php to the list of pages Monkey so that it only will serve if only a directory and no page is specified in the URL. Changes as below:
   #Indexfile index.html index.htm
   Indexfile index.html index.htm index.php
3. Change the Server_ScriptAlias in /etc/monkey/monkey.conf file from /var/monkey/ to /var/www/ as following:
   Server_ScriptAlias /cgi-bin/ /var/www
4. Uncomment the AddScript line to let Monkey pass the content of file that ends with .php to the PHP interpreter.
5. Go to /var/www/squirrelmail/config/config_svr_ldap.php file and edit the file pointer towards the local host as following code:
   $ldap_server[0] = Array(

'host' => 'localhost',

'name' => 'ldap o=tinynet',

'base' => 'o=tinynet.edu'

);

6. Check process running the background using command “htop” and kill monkey process with “SIGNTERM”, then restart the monkey process by command “usr/sbin/monkey -D”.

Configuration for stunnel

1. Startup Gateway, Mailhost and Webserver.
2. Go to /etc/rc.d/rc.stunnel file to set the executable bits and modify the file as below:

   ls -1 /etc/stunnel/*.server.conf 2>/dev/null | while read LINE; do

   echo "Starting stunnel with $LINE"

   /usr/sbin/stunnel $LINE

   done
3. Go to /etc/rc.d/rc.inetd2 file and modify the file by change the “rc.yp” to “rc.stunnel” twice under Start NIS.

On the host system

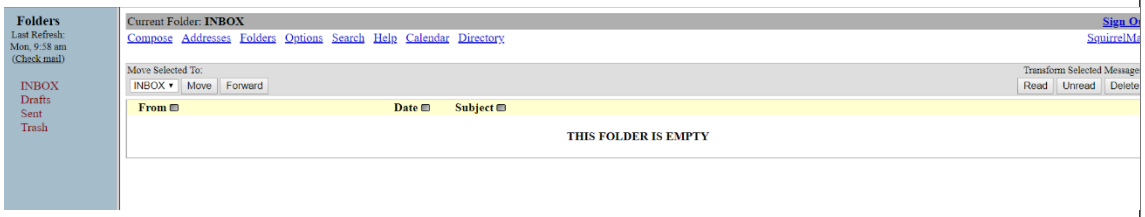
1. Open the page url 192.168.56.252/ to tinynet Squirrelmail page to download the TinyNetCA certificate.
2. Install the certificate to the host system store and web browser as a Trusted Root Certificates.
3. Clear the caches at the host system web browser and access to the Squirrelmail login page with url https://192.168.56.252/

After all the steps above, the base system is now able to send mail and check with Squirrelmail.

Screenshots of tests, with explanations

Login to Squirrelmail using my student number (tp054979) as configured in /home/vmail/mail-pwd

After logged in page

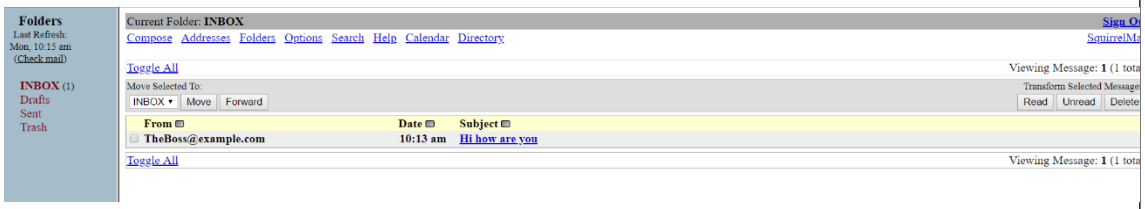


The inbox is empty now, therefore next screenshot will be showing send mail

Sending mail

```
root@nch1:~# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mailhost.tinynet.edu ESMTP Postfix
HELO mailhost.tinynet.edu
250 mailhost.tinynet.edu
MAIL From: TheBoss@example.com
250 2.1.0 Ok
RCPT To: tp054979@mailhost.tinynet.edu
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Hi how are you
Today is 28 May and my student ID is TP054979
.
250 2.0.0 Ok: queued as 876FBCB8
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
root@nch1:~#
```

Mail received by previous mail send



Mail content

Gateway listening port

```
root@gateway:~# netstat -tulp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 *:submission            *:*                     LISTEN
4436/master
tcp        0      0 *:http                  *:*                     LISTEN
4447/monkey
tcp        0      0 *:smtps                 *:*                     LISTEN
4368/stunnel
tcp        0      0 *:domain                *:*                     LISTEN
4339/dnsmasq
tcp        0      0 *:ssh                   *:*                     LISTEN
4362/sshd
tcp        0      0 *:telnet                *:*                     LISTEN
4357/xinetd
tcp        0      0 *:smtp                  *:*                     LISTEN
4436/master
udp        0      0 *:domain                *:*
4339/dnsmasq
udp        0      0 *:bootps                *:*
4339/dnsmasq
root@gateway:~# _
```

Mailhost listening port

```
root@nch1:~# netstat -tulp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 *:imaps                 *:*                     LISTEN
4370/stunnel
tcp        0      0 *:nfsd                  *:*                     LISTEN
_
tcp        0      0 *:ldap                  *:*                     LISTEN
4374/stunnel
tcp        0      0 *:submission            *:*                     LISTEN
4363/master
tcp        0      0 *:imap                  *:*                     LISTEN
4400/dovecot
tcp        0      0 *:sunrpc                *:*                     LISTEN
4231/rpc.portmap
tcp        0      0 *:http                  *:*                     LISTEN
4377/monkey
tcp        0      0 *:34192                 *:*                     LISTEN
4297/rpc.mountd
tcp        0      0 *:47989                 *:*                     LISTEN
```

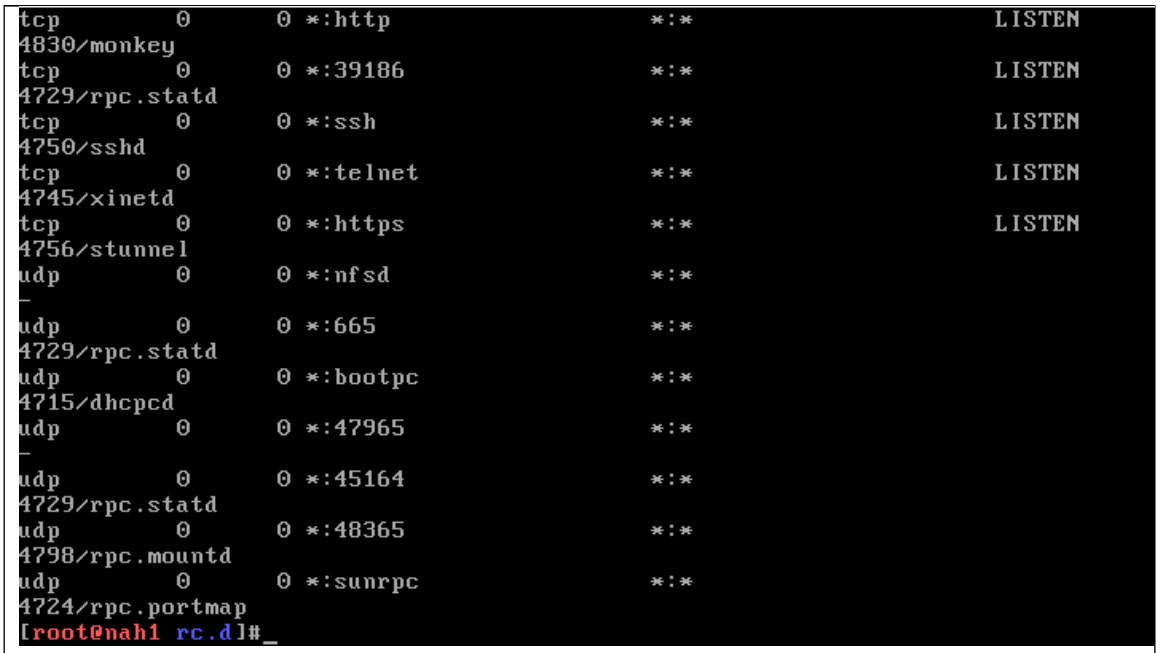
(continue previous page screenshot)

```
tcp        0      0 *:47989                 *:*                     LISTEN
4236/rpc.statd
tcp        0      0 *:ssh                   *:*                     LISTEN
4257/sshd
tcp        0      0 *:telnet                *:*                     LISTEN
4252/xinetd
tcp        0      0 *:59352                 *:*                     LISTEN
-
tcp        0      0 *:smtp                  *:*                     LISTEN
4363/master
udp        0      0 *:nfsd                  *:*
-
udp        0      0 *:58662                 *:*
-
udp        0      0 *:bootpc                *:*
4222/dhcpcd
udp        0      0 *:45010                 *:*
4236/rpc.statd
udp        0      0 *:sunrpc                *:*
4231/rpc.portmap
udp        0      0 *:1020                  *:*
4236/rpc.statd
udp        0      0 *:49534                 *:*
4297/rpc.mountd
root@nch1:~#
```

Webserver listening port

```
[root@nah1 rc.d]#netstat -tulp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 *:34592                 *:*                     LISTEN
-
tcp        0      0 *:nfsd                  *:*                     LISTEN
-
tcp        0      0 *:52357                 *:*                     LISTEN
4798/rpc.mountd
tcp        0      0 *:ldap                  *:*                     LISTEN
4760/stunnel
tcp        0      0 *:submission            *:*                     LISTEN
4760/stunnel
tcp        0      0 *:imap                  *:*                     LISTEN
4760/stunnel
tcp        0      0 *:sunrpc                *:*                     LISTEN
4724/rpc.portmap
tcp        0      0 *:http                  *:*                     LISTEN
```

(continue preiosu page screenshot)



Obstacles encountered, obstacles overcome

N/A

Any Outstanding/Unresolved Issues

N/A

5.0 LDAP

a) Setup the LDAP sever with two domains (o= and dc=)

b) Configure dovecot and squirrelmail to use LDAP

c) Get LDAP using stunnel (with screenshot of listening ports)

Owner: Loke Yi Wei (TP054979)

Objective – what this does for the system

Setting up the LDAP with multiple domains create a hierarchical structure for storing information. The system creates organizational units, individuals and resources in the network. By configuring dovecot, users can use LDAP to access squirrelmail with secure connection of stunnel encryption.

List the relevant configuration files, and for each one briefly describe what was done

Making LDAP file executable and restart the LDAP service

/etc/rc.d/rc.ldap

1. Make the LDAP service available to executable by changing the proper permission using chmod. Command used:
   Chmod 755 /etc/rc.d/rc.ldap
2. Apply the changes by restarting rc.ldap service Command used:
   /etc/rc.d/rc.ldap stop
   /etc/rc.d/rc.ldap start

Configure LDAP domain file

/etc/openldap.slapd.conf

1. Configure the LDAP file to let the LDAP service know how to manage information. Therefore, changes are made in /etc/openldap/slapd.conf file:
   access to *

by dn=”cn=LDAPAdmin,o=tinynet.edu” write

by self write

by * read

2. in the same file, under the line of rootdn "cn=LDAPAdmin,dc=tinynet,dc=edu", make the same change as above.

Create the first DIT (o=tinynet.edu), “o=” is the first domain.

/etc/openldap/topclass.ldif

1. Make the first DIT of the LDAP service with “o=” form by modify changes to the /etc/openldap/topclass.ldif file:

   dn: cn=LDAPAdmin,o=tinynet.edu

   objectClass: organizationalRole

   objectClass: simpleSecurityObject

   cn: LDAPAdmin

   description: LDAP Administrator

   userPassword: {PLAIN}slapmesilly

2. Add the first DIT or domain that configured previously by execute the codes:

   ldapadd -x -D "cn=LDAPAdmin,o=tinynet.edu" -w slapmesilly -f /etc/openldap/topclass.ldif

3. Adding user data with codes below:

   ldapadd -x -D "cn=LDAPAdmin,o=tinynet.edu" -w slapmesilly -f /etc/openldap/userdata.ldif

Create the second DIT (dc=tinynet,dc=edu), “dc=” is the second domain.

/etc/open/topclass.ldif

1. After the first DIT domain has been used, the second domain will be use as “dc=” form.
2. Making changes to the /etc/openldap/topclass.ldif file for LDAP Root, LDAP Admin and 3 users.

   LDAP Root:

   dn: **dc=tinynet,dc=edu**

objectClass: top

objectClass: dcObject

objectClass: organization

o: **MyTinyNet**

dc: tinynet

description: LDAP Root

LDAP Admin:

dn: cn=LDAPAdmin,**dc=tinynet,dc=edu**

objectClass: organizationalRole

objectClass: simpleSecurityObject

cn: LDAPAdmin

userPassword: {PLAIN}slapmesilly

description: LDAP Administrator

3 users:

dn: ou=UserNetA,**dc=tinynet,dc=edu**

ou: UserNetA

objectClass: top

objectClass: organizationalUnit

description: User on Net-A

UserNetB and UserNetC is configured same as UserNetA.

Edit the user account information.

/etc/openldap/userdata.ldif

1. Modify the user account information to use the “dc=” form:

   dn: cn=Barbara Jensen,ou=UserNetA,**dc=tinynet,dc=edu**

   dc: tinynet

   ou: UserNetA

   cn: Barbara Jensen
2. Notify the system to create second DIT domain that configured in the LDAP

file earlier. Command used:

%ldapadd -x -D "cn=LDAPAdmin,dc=tinynet,dc=edu" -w slapmesilly -f /etc/openldap/topclass.ldif

Configure dovecot in Mailhost

/etc/dovecot/dovecot.conf

1. Configure Dovecot service to use LDAP service by modify the /etc/dovecot/dovecot.conf file to uncomment the passdb ldap and userdb ldap section as below code:

```
passdb ldap {
        # Path for LDAP configuration file
        args = /etc/dovecot/dovecot-ldap.conf
}
userdb ldap {
        # Path for LDAP configuration file
        args = /etc/dovecot/dovecot-ldap.conf
}
```

Change the dovecot default address to LDAP server address

/etc/dovecot/dovecot-ldap.conf

1. Tell the system to access LDAP address so the dovecot service can use LDAP service. Modify the code as below in /etc/dovecot-ldap.conf file by changing from the localhost address to the LDAP address:

   Hosts = ldap.tinynet.edu

Create a configuration file for second DIT domain

/etc/dovecot/dovecot-ldap-dc.conf

1. After LDAP address had been configured, the second DIT have to configure too to use LDAP Service.
2. Make a copy of /etc/dovecot/dovecot-ldap.conf and rename it to /etc/dovecot/dovecot-ldap-dc.conf.

3. Edit the /etc/dovecot/dovecot-ldap.conf file by changing the domain to “dc=” form as the code below:

   dn = dn=LDAPAdmin,**dc=tinynet,dc=edu**

   dnpass = slapmesilly

   base = **dc=tinynet,dc=edu**

   scope = subtree

Configure squirrelmail in WebServer

var/www/squirrelmail/config/config_svr_ldap.php

1. Squirrelmail is require to use LDAP service.
2. Therefore, changes is needed to done in /var/www/squirrelmail/config.svr.ldap.php file. Code is added in the file where out of comment section:

   $**ldap_server[0] = Array(**

   ‘host’ => ‘ldap.tinynet.edu’,

   ‘name’ => ‘ldap dc=tinynet,dc=edu’

   ‘base’ => ‘dc=tinynet,dc=edu’

   );

/config_plugins.php

1. Tell the squirrelmail to use the LDAP plugin by uncomment code in the var/www/squirrelmail/config/config_plugins.php file to become below code:

   $plugins[8] =’ldapquery’;

Get LDAP using stunnel

/etc/rc.d/rc.stunnel

1. With stunnel, LDAP service can run more secure.
2. Make /etc/rc.d/rc.stunnel executable. Command used:

   chmod 755 /etc/rc.d/rc.stunnel
3. Edit /etc/rc.d/rc.stunnel file to get stunnel working:

From:

/usr/sbin/stunnel $LINE

To:

/etc/stunnel $LINE

After all the changes above, LDAP is now set up with domains, which are (o=) and (dc=). Dovecot service and squirrelmail are able to use LDAP service. Stunnel is open for LDAP to be use.

Screenshots of tests, with explanations

Creating the first DIT in /etc/openldap/topclass.ldif file

```
topclass.ldif      [----]  0 L:[  1+ 0   1/ 33] *(0   / 638b)=  100 0x064
dn: o=tinynet.edu
objectClass: top
objectClass: organization
o: tinynet.edu
description: LDAP Root

dn: cn=LDAPAdmin,o=tinynet.edu
objectClass: organizationalRole
objectClass: simpleSecurityObject
cn: LDAPAdmin
description: LDAP Administrator
userPassword: {PLAIN}slapmesilly

dn: ou=UserNetA,o=tinynet.edu
ou: UserNetA
objectClass: top
objectClass: organizationalUnit
description: User on Net-A

dn: ou=UserNetB,o=tinynet.edu
ou: UserNetB
objectClass: top
objectClass: organizationalUnit
 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

Using command to add the top level of first DIT

```
root@nbh1:/etc/openldap# ldapadd -x -D "cn=LDAPAdmin, o=tinynet.edu" -w slapmes
lly -f /etc/openldap/topclass.ldif
adding new entry "o=tinynet.edu"
ldapadd: Already exists (68)

root@nbh1:/etc/openldap#
```

Adding use data into the first DIT

```
root@nbh1:/etc/openldap# ldapadd -x -D "cn=LDAPAdmin,o=tinynet.edu" -w slapmesi
lly -f /etc/openldap/userdata.ldif
adding new entry "cn=Barbara Jensen,ou=UserNetA,o=tinynet.edu"
ldapadd: Already exists (68)

root@nbh1:/etc/openldap# _
```

Creating the second DIT in /etc/openldap/topclass.ldif file

```
topclass.ldif      [-M--] 34 L:[  1+ 6   7/ 33] *(134 / 648b)=   10 0x00A
dn: o=tinynet.edu
objectClass: top
objectClass: organization
o: tinynet.edu
description: LDAP Root

dn: cn=LDAPAdmin,dc=tinynet,dc=edu
objectClass: organizationalRole
objectClass: simpleSecurityObject
cn: LDAPAdmin
description: LDAP Administrator
userPassword: {PLAIN}slapmesilly

dn: ou=UserNet,dc=tinynet,dc=edu
ou: UserNetA
objectClass: top
objectClass: organizationalUnit
description: User on Net-A

dn: ou=UserNet,dc=tinynet,dc=edu
ou: UserNetB
objectClass: top
objectClass: organizationalUnit
 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

Editing the user data in /etc/openldap/userdata.ldif file

```
userdata.ldif      [----]  0 L:[  1+ 0   1/ 88] *(0   /1839b)=  100 0x064
dn: cn=Barbara Jensen,ou=UserNetA,dc=tinynet,dc=edu
dc: tinynet
ou: UserNetA
cn: Barbara Jensen
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
mail: bjensen@net-a.tinynet.edu
givenname: Barbara
sn: Jensen
uid: bjensen
title: Account Executive
userPassword: {PLAIN}LetMeIn

dn: cn=Jared Padalecki,ou=UserNetA,dc=tinynet,dc=edu
dc=tinynet
ou: UserNetA
cn: Jared Padalecki
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

Adding use data into the second DIT

```
root@nbh1:/etc/openldap# ldapadd -x -D "cn=LDAPAdmin,dc=tinynet,dc=edu" -w slap
esilly -f /etc/openldap/topclass.ldif
adding new entry "o=tinynet.edu"
ldapadd: Already exists (68)

root@nbh1:/etc/openldap# _
```

Configuring the /etc/dovecot/dovecot.conf file making it to use LDAP

```
dovecot.conf       [----]  0 L:[ 39+22  61/119] *(1493/3122b)=  125 0x07D

  passdb ldap {
    # Path for LDAP configuration file
    args = /etc/dovecot/dovecot-ldap.conf
  }

  userdb ldap {
    # Path for LDAP configuration file
    args = /etc/dovecot/dovecot-ldap.conf
  }

  passdb passwd-file {
    args = /home/vmail/mail-pwd
  }

  userdb static {
    args = uid=vmail gid=vmail.
  }

  mechanisms = plain.
  ssl_require_client_cert = no
  ssl_username_from_cert = no
}
 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

Change localhost address to LDAP address in /etc/dovecot/dovecot-ldap.conf

```
dovecot-ldap.conf   [----]  0 L:[  1+ 0   1/ 56] *(0   /1851b)=   35 0x023
# Address or name of the LDAP server that will be used..
# If the server is in the same machine, "localhost" will suffice.
hosts = ldap.tinynet.edu

# Make dovecot use TLS (no point if the server is 'localhost')
tls = no

# Encoding used by the LDAP server when it returns the password
default_pass_scheme = PLAIN

# Bind to the LDAP directory using version 2 is depecated but supported
ldap_version = 3

# Tell Dovecot to bind to the LDAP directory using the mail client.
# user's credentials - see the documentation for costs and benefits
auth_bind = no

# Tell Dovecot to bind to the LDAP directory using these credentials
# Make sure this matches something in the directory or slapd.conf
dn = cn=LDAPAdmin,o=tinynet.edu
dnpass = slapmesilly

# LDAP search base: where to start searching through the directory
 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

Configuring /etc/dovecot/dovecot-ldap-dc.conf file for second DIT domain

```
dovecot-l~p-dc.conf    [----]  0 L:[ 13+ 1  14/ 56] *(405 /1859b)=   35 0x023

# Tell Dovecot to bind to the LDAP directory using the mail client.
# user's credentials - see the documentation for costs and benefits
auth_bind = no

# Tell Dovecot to bind to the LDAP directory using these credentials
# Make sure this matches something in the directory or slapd.conf
dn = dn=LDAPAdmin,dc=tinynet,dc=edu
dnpass = slapmesilly

# LDAP search base: where to start searching through the directory
base = dc=tinynet,dc=edu
scope = subtree

# passdb lookup: tell dovecot
# which LDAP attributes are associated with the user's password
# and the search filter, e.g., (&(objectClass=posixAccount) (uid=%u))
pass_attrs = userPassword=password
pass_filter = (mail=%n@%d)

# userdb lookup: tell dovecot
# which LDAP attributes map to uid, gid, home and mail.
#   (note the use of static text for mail - see the documentation)
 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

Configure var/www/squirrelmail/config/config_svr_ldap.php file in WebServer to make squirrelmail use LDAP

```
config_svr_ldap.php    [----] 35 L:[  3+20  23/ 25] *(639 / 646b)=   39 0x027
/**
 * LDAP server(s)
 *   Array of arrays with LDAP server parameters. See
 *   functions/abook_ldap_server.php for a list of possible
 *   parameters
 *
 * EXAMPLE:
 *   $ldap_server[0] = Array(
 *       'host' => 'memberdir.netscape.com',
 *       'name' => 'Netcenter Member Directory',
 *       'base' => 'ou=member_directory,o=netcenter.com'
 *   );.
 *
 *   NOTE: please see security note at the top of this file when
 *   entering a password.
 */
// Add your ldap server options here
$ldap_server[0] = Array(
      'host' => 'ldap.tinynet.edu',
      'name' => 'ldap dc=tinynet,dc=edu',
      'base' => 'dc=tinynet,dc=edu'
);.
 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

Configuring var/www/squirrelmail/config/config_plugins.php file to enable LDAP

plugin

```
config_plugins.php   [-M--]  0 L:[ 26+22  48/ 50] *(1239/1241b)=   10 0x00A

# 3rd party -
# allows users to search the Directory Servers by name and
# lookup phone numbers, addresses, and other data.
$plugins[8] = 'ldapquery';

# standard with 1.4.22
# fix bug_report.php for postfix.conf alias.
# generates lots of good system info
#
#$plugins[8] = 'bug_report';

# IMAP command workshop where you can select pre-made commands,
# send them to the IMAP server and see the response.
#$plugins[10] = 'info';

# - worth trying?
#$plugins[11] = 'administrator';

# 3rd party -
# shows php call stack
#$plugins[12] = 'debugger';

 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

Configuring rc.stunnel file to make stunnel use LDAP

```
rc.stunnel          [----]  0 L:[  1+ 1   2/ 22] *(10   / 527b)=   35 0x023
#!/bin/sh
#
# Stunnel naming convention: /etc/stunnel/host.<client|server>.conf

if [ "$1" = "start" -o "$1" = "" ]; then

      ls -1 /etc/stunnel/*.server.conf 2>/dev/null | while read LINE; do
         echo "Starting stunnel with $LINE"
         /usr/sbin/stunnel /etc/stunnel $LINE
      done

      ls -1 /etc/stunnel/*.client.conf 2>/dev/null | while read LINE; do
         echo "Starting stunnel with $LINE"
         /usr/sbin/stunnel /etc/stunnel $LINE
      done
fi

if [ "$1" = "stop" ]; then
   killall stunnel
fi


 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

Obstacles encountered, obstacles overcome

N/A

Any Outstanding/Unresolved Issues

N/A

6.0 Cross-System Multitail

a) Use one easy method to setup *Multitail* to show the postfix logfiles on the Gateway and the Mailserver in separate windows, and demonstrate using email via telnet

b) Use a different easy method to setup *Multitail* to show the postfix logfiles on the Gateway and the Mailserver in a single window with different colors, and demonstrate using email via telnet

Owner: Loke Yi Wei (TP054979)

Objective – what this does for the system

In Linux administration, the key to troubleshoot problems is to watch the log files. Some troubleshooting required to follow up more than one log file. Therefore, using Multitail can show up multiple terminal windows and display in one console screen.

List the relevant configuration files, and for each one briefly describe what was done

Setting up SSH Multiplexing

1. In Gateway and Mailhost, edit the /etc/ssh/ssh_config file by adding as below:
   host *
   ControlPath /tmp/ssh-%r@%h:%p
   ControlMaster auto
   # ControlPersist 10m
2. Using “netstat -tulp” command to ensure rc.sshd is running in both Gateway and Mailhost.
3. In Gateway, enter the following into console to log in ssh:
   ssh root@mailhost.tinynet.edu
   yes
   password: toor

4. Press “alt+F2” to open a new terminal. In the new terminal enter as below, it will shows the initial status of postfix.log in both Gateway and Mailhost. When send email through squirrelmail, it able to see the status of postfix.log in Gateway and Mailway:
   multitail /var/log/postfix.log -1 “ssh root@mailhost.tinynet.edu tail -f /var/log/postfix.log”

Gateway and the Mailserver in a single window with different colors

1. In Mailhost, command as below:
   Mkfifo /tmp/foo
   Ln -s /bin/bash /bin/rbash
   Cat /tmp/foo |basdnc -lkv 23432 |/bin/rbash 1>/tmp/foo &
2. In Gateway, command the following to change the colour to differentiate the postfix.log:
   Multitail -ci yellow /var/log/postfix.log -ci red -L “echo ‘tail /var/log/postfix.log’ |nc (ip address of Mailhost) 23432”

Screenshots of tests, with explanations

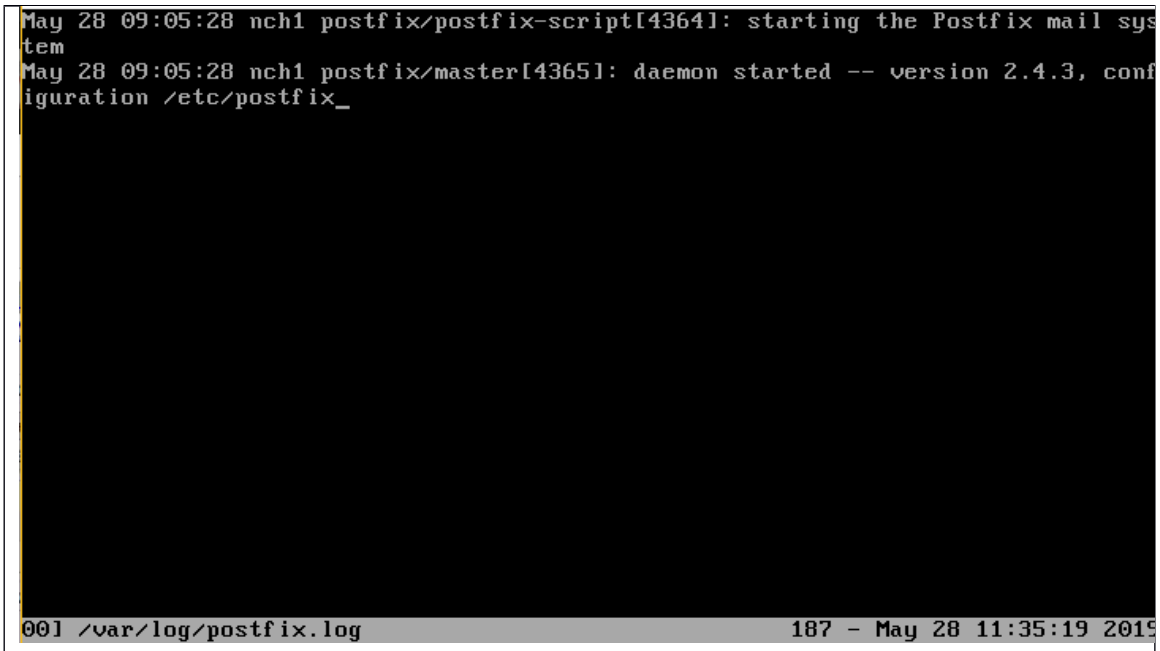
Configuration in /etc/ssh/ssh_config file

```
ssh_config          [----] 23 L:[ 28+22  50/ 50] *(1570/1570b)= <EOF>
#   GSSAPIDelegateCredentials no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/identity
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   Port 22
#   Protocol 2,1
#   Cipher 3des
#   Ciphers aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no

host *
    ControlPath /ump/ssh-%r@%h:%p
    ControlMaster auto
    #ControlPersist 10m_
 1 Help  2 Save  3 Mark  4Replac 5 Copy  6 Move  7Search 8Delete 9PullDn10 Quit
```

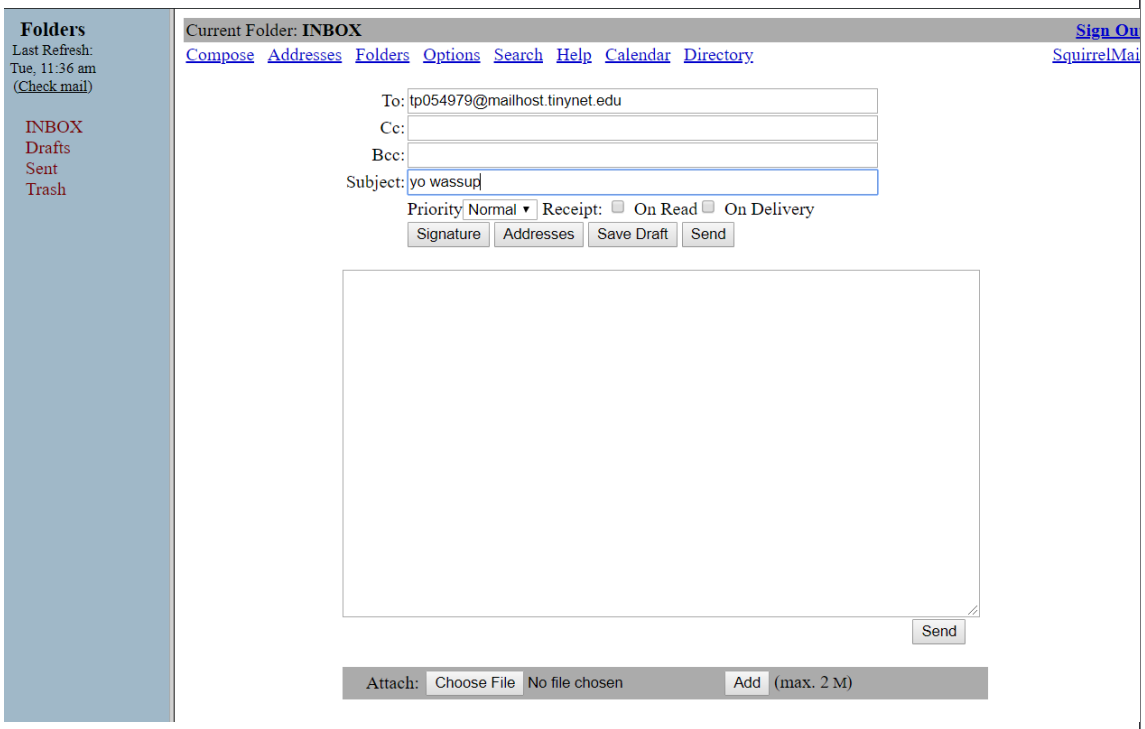
Log in to ssh

```
root@tp054979:/etc/ssh# ssh root@mailhost.tinynet.edu
The authenticity of host 'mailhost.tinynet.edu (192.168.76.229)' can't be estab
ished.
RSA key fingerprint is 81:74:76:65:51:af:13:65:02:03:c1:c5:33:b5:32:bc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mailhost.tinynet.edu,192.168.76.229' (RSA) to the l
st of known hosts.
root@mailhost.tinynet.edu's password:
Last login: Tue May 28 09:06:20 2019
Linux 2.6.27.27.
root@nch1:~#
```

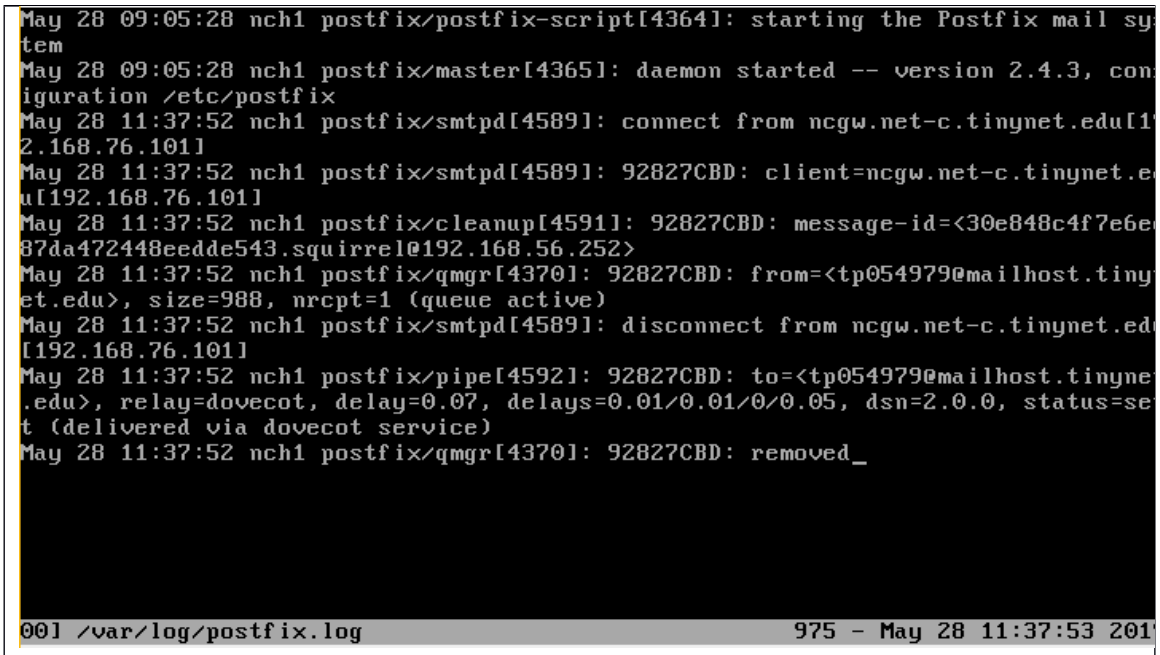
Start to see the status of postfix.log in Gateway and Mailhost before test to send mail



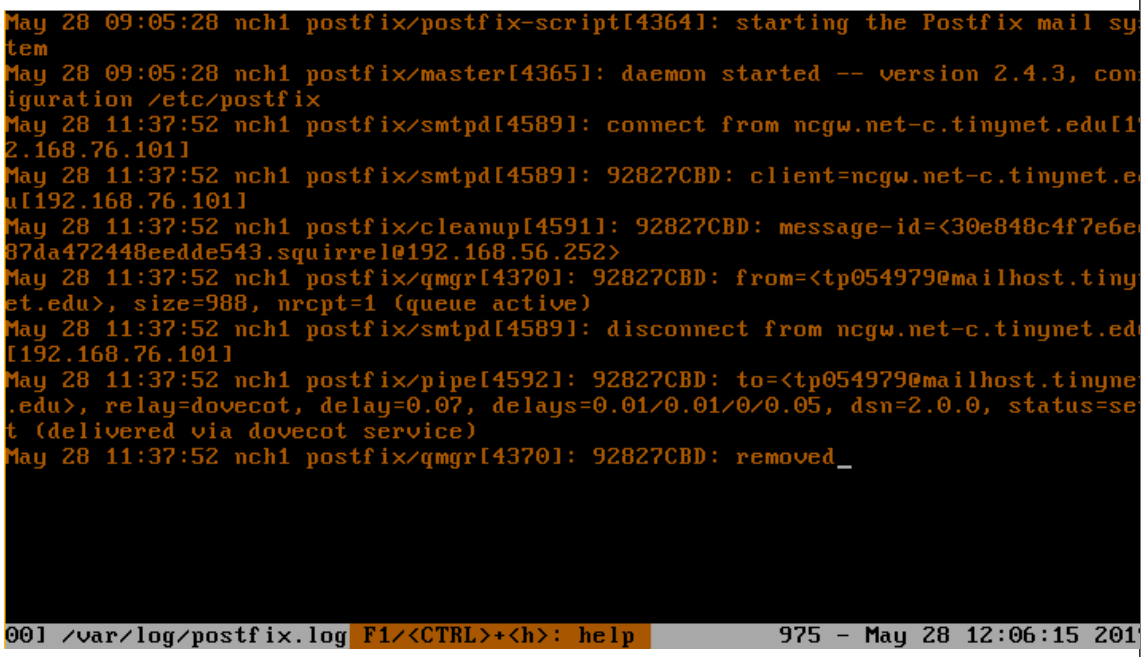
Send mail via Squirrelmail



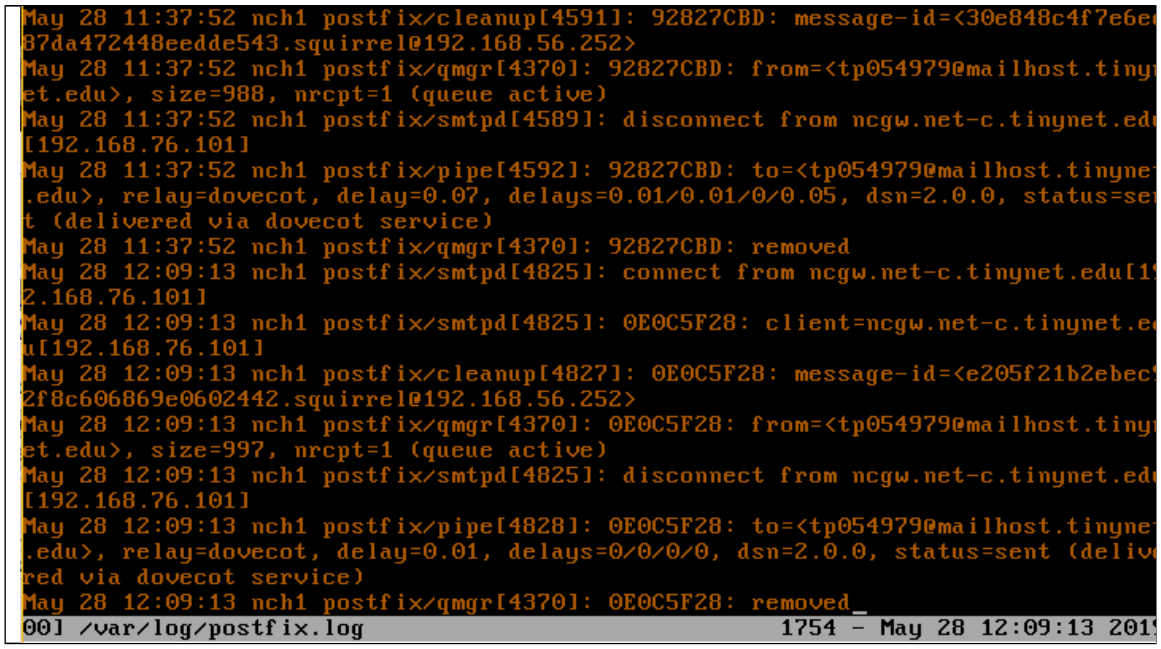
Mail sent, and the output of postfix.log



Output of postfix.log in color before sending mail



Output of postfix.log in color after mail sent



Obstacles encountered, obstacles overcome

N/A

Any Outstanding/Unresolved Issues

N/A

7.0 Iptables

a) Add the six “Rules for things that no proper TCP stack should be processing” from the IPTables Quick Reference section -p --protocol tcp but use a LOG target

b) Use hping2 and Multitail to show the rules are working

Owner: Loke Yi Wei (TP054979)

Objective – what this does for the system

Iptables is a command line firewall that allow or block traffic by policy chains. When a connection tries to establish itself to the system, iptables will looks for a rule in the list to match the connection. If iptables doesn’t find one then it will resorts to the default action. Iptables have 3 chains, which are “INPUT, FORWARD AND OUTPUT” and packet will only hit one of it.

List the relevant configuration files, and for each one briefly describe what was done

Add rules

1. Rule 1: iptables -A INPUT -p tcp –tcp-flags ALL NONE -j LOG –log-level alert –log-prefix “iptables ALL NONE”
2. Rule 1: iptables -A INPUT -p tcp –tcp-flags FIN,SYN FIN,SYN -j LOG –log-level alert –log-prefix “iptables FIN SYN FIN SYN”
3. Rule 1: iptables -A INPUT -p tcp –tcp-flags SYN,RST SYN,RST -j LOG –log-level alert –log-prefix “iptables SYN,RST SYN,RST”
4. Rule 1: iptables -A INPUT -p tcp –tcp-flags FIN,RST FIN,RST -j LOG –log-level alert –log-prefix “iptables FIN,RST FIN,RST”
5. Rule 1: iptables -A INPUT -p tcp –tcp-flags FIN,ACK FIN -j LOG –log-level alert –log-prefix “iptables FIN,ACK FIN”
6. Rule 1: iptables -A INPUT -p tcp –tcp-flags ACK, URG URG -j LOG –log-level alert –log-prefix “iptables ACK, URG URG”

Test each of the rules

1. Rule 1: multitail /var/log/syslog -l “hping2 192.168.56.101”
2. Rule 2: multitail /var/log/syslog -l “hping2 -F -S 192.168.56.101”
3. Rule 3: multitail /var/log/syslog -l “hping2 -S -R 192.168.56.101”
4. Rule 4: multitail /var/log/syslog -l “hping2 -F -R 192.168.56.101”
5. Rule 5: multitail /var/log/syslog -l “hping2 -F 192.168.56.101”
6. Rule 6: multitail /var/log/syslog -l “hping2 -U 192.168.56.101”

Screenshots of tests, with explanations

Adding rules

```
root@tp054979:~# iptables -A INPUT -p tcp --tcp-flags ALL NONE -j LOG --log-lev
l alert --log-prefix "iptables ALL NONE"
root@tp054979:~# iptables -A INPUT -p tcp --tcp-flags FIN,SYN FIN,SYN -j LOG --
og-level alert --log-prefix "iptables FIN, SYN FIN,SYN"
root@tp054979:~# iptables -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST -j LOG --
og-level alert --log-prefix "iptables SYN,RST SYN,RST"
root@tp054979:~# iptables -A INPUT -p tcp --tcp-flags FIN,RST FIN,RST -j LOG --
og-level alert --log-prefix "iptables FIN,RST FIN,RST"
root@tp054979:~# iptables -A INPUT -p tcp --tcp-flags FIN,ACK FIN -j LOG --log-
evel alert --log-prefix "iptables FIN,ACK FIN"
root@tp054979:~# iptables -A INPUT -p tcp --tcp-flags ACK,URG URG -j LOG --log-
evel alert --log-prefix "iptables ACK,URG URG"
root@tp054979:~#
```

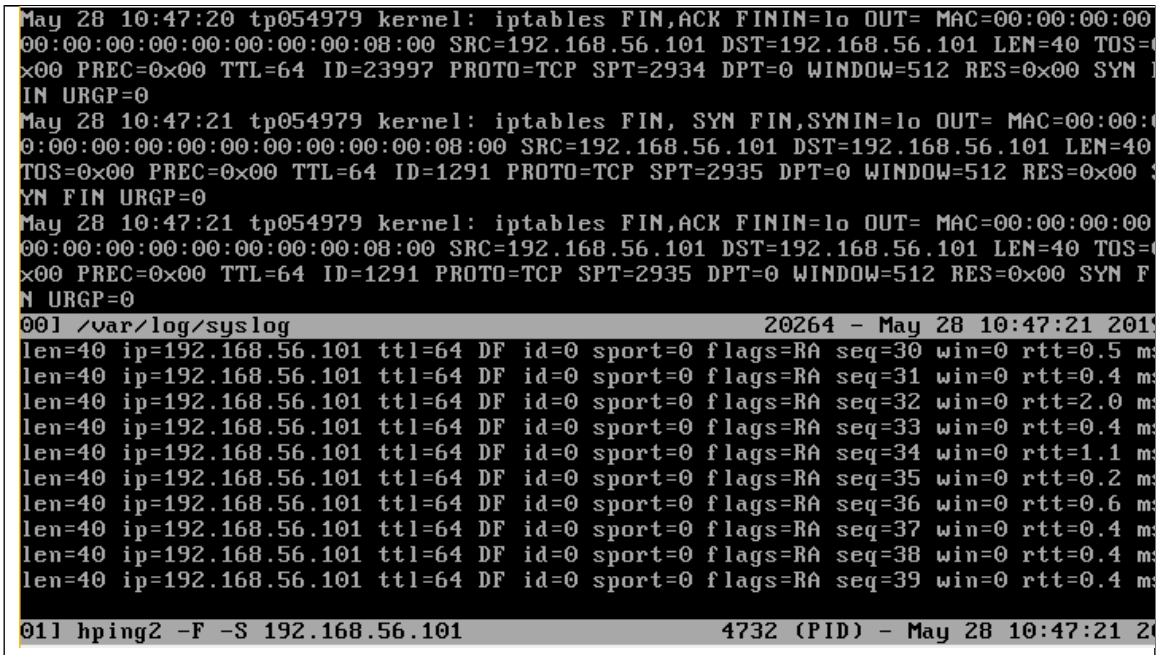
Using “iptables -l” to list out the fiter rules

```
DROP       tcp  --  anywhere             anywhere            tcp flags:FIN,SYN,
ST,PSH,ACK,URG/NONE
LOG        tcp  --  anywhere             anywhere            tcp flags:FIN,SYN,
ST,PSH,ACK,URG/NONE LOG level alert prefix `iptables ALL NONE'
LOG        tcp  --  anywhere             anywhere            tcp flags:FIN,SYN,
ST,PSH,ACK,URG/NONE LOG level alert prefix `iptables ALL NONE'
LOG        tcp  --  anywhere             anywhere            tcp flags:FIN,SYN,
ST,PSH,ACK,URG/NONE LOG level alert prefix `iptables ALL NONE'
LOG        tcp  --  anywhere             anywhere            tcp flags:FIN,SYN/
IN,SYN LOG level alert prefix `iptables FIN, SYN FIN,SYN'
LOG        tcp  --  anywhere             anywhere            tcp flags:SYN,RST/
YN,RST LOG level alert prefix `iptables SYN,RST SYN,RST'
LOG        tcp  --  anywhere             anywhere            tcp flags:FIN,RST/
IN,RST LOG level alert prefix `iptables FIN,RST FIN,RST'
LOG        tcp  --  anywhere             anywhere            tcp flags:FIN,ACK/
IN LOG level alert prefix `iptables FIN,ACK FIN'
LOG        tcp  --  anywhere             anywhere            tcp flags:ACK,URG/
RG LOG level alert prefix `iptables ACK,URG URG'

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@tp054979:~# _
```

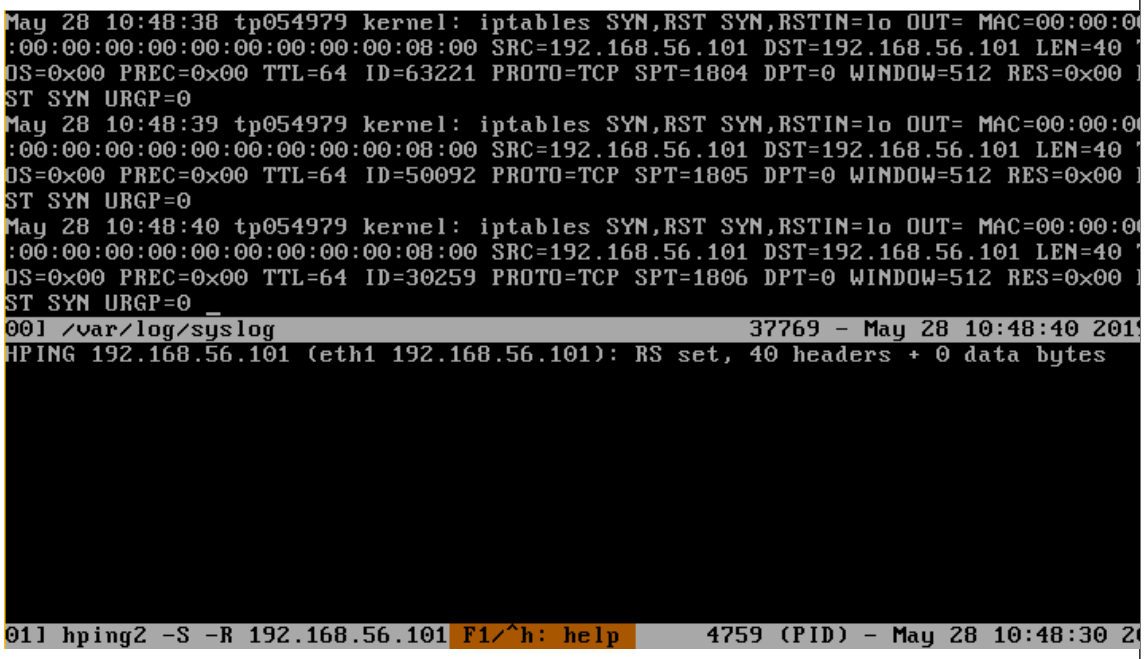
Output of rule 1

```
May 28 10:54:10 tp054979 kernel: iptables ACK,URG URGIN=lo OUT= MAC=00:00:00:00
00:00:00:00:00:00:00:00:08:00 SRC=192.168.56.101 DST=192.168.56.101 LEN=40 TOS=
x00 PREC=0x00 TTL=64 ID=48410 PROTO=TCP SPT=1841 DPT=0 WINDOW=512 RES=0x00 URG
RGP=0
May 28 10:54:11 tp054979 kernel: iptables ACK,URG URGIN=lo OUT= MAC=00:00:00:00
00:00:00:00:00:00:00:00:08:00 SRC=192.168.56.101 DST=192.168.56.101 LEN=40 TOS=
x00 PREC=0x00 TTL=64 ID=221 PROTO=TCP SPT=1842 DPT=0 WINDOW=512 RES=0x00 URG UR
P=0
May 28 10:54:12 tp054979 kernel: iptables ACK,URG URGIN=lo OUT= MAC=00:00:00:00
00:00:00:00:00:00:00:00:08:00 SRC=192.168.56.101 DST=192.168.56.101 LEN=40 TOS=
x00 PREC=0x00 TTL=64 ID=49411 PROTO=TCP SPT=1843 DPT=0 WINDOW=512 RES=0x00 URG
RGP=0 _
00] /var/log/syslog F1/<CTRL>+<h>: help          114958 - May 28 10:54:42 201
HPING 192.168.56.101 (eth1 192.168.56.101): NO FLAGS are set, 40 headers + 0 da
a bytes
01] hping2 192.168.56.101       2MB (VMsize)  4778 (PID) - May 28 10:54:42 201
```

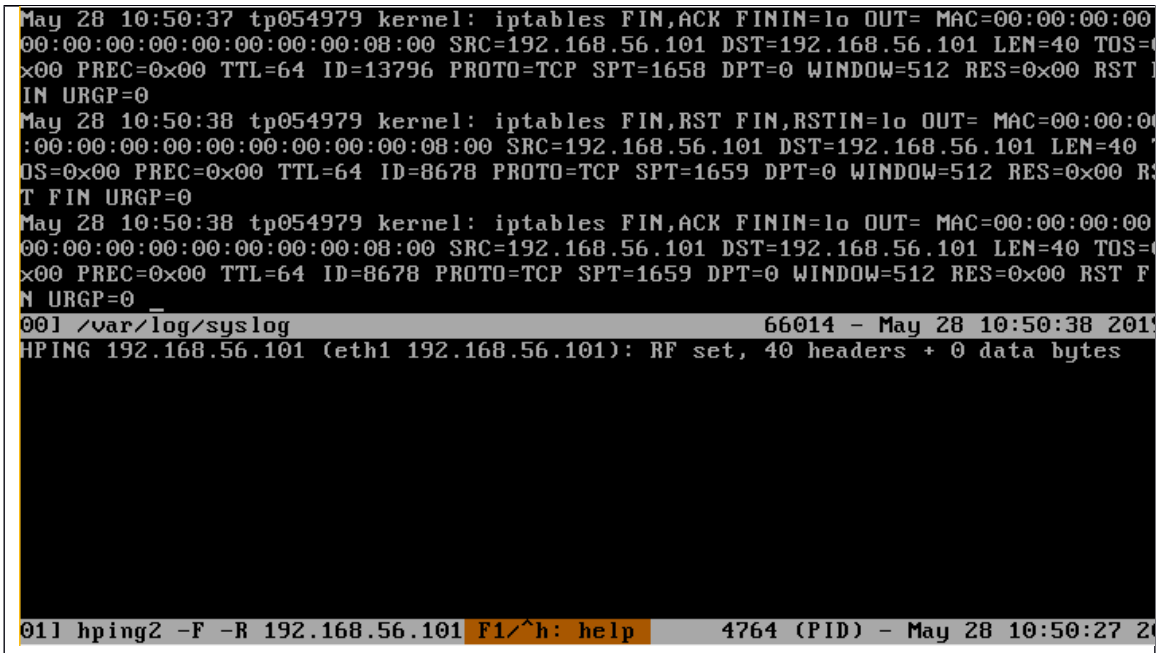
Output of rule 2



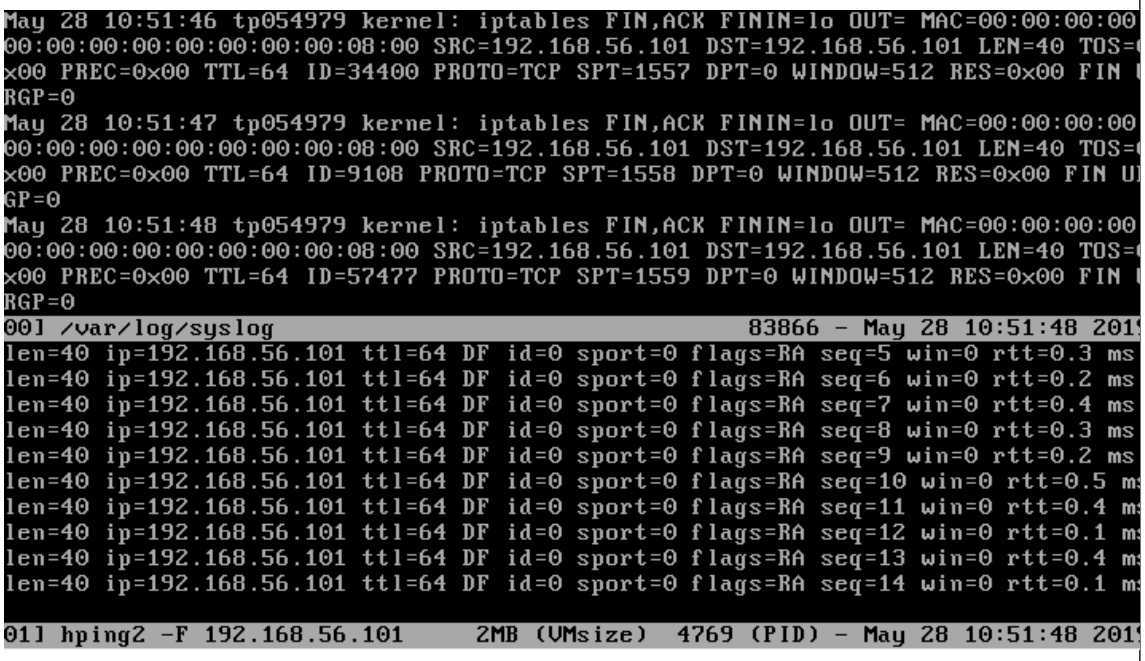
Output of rule 3



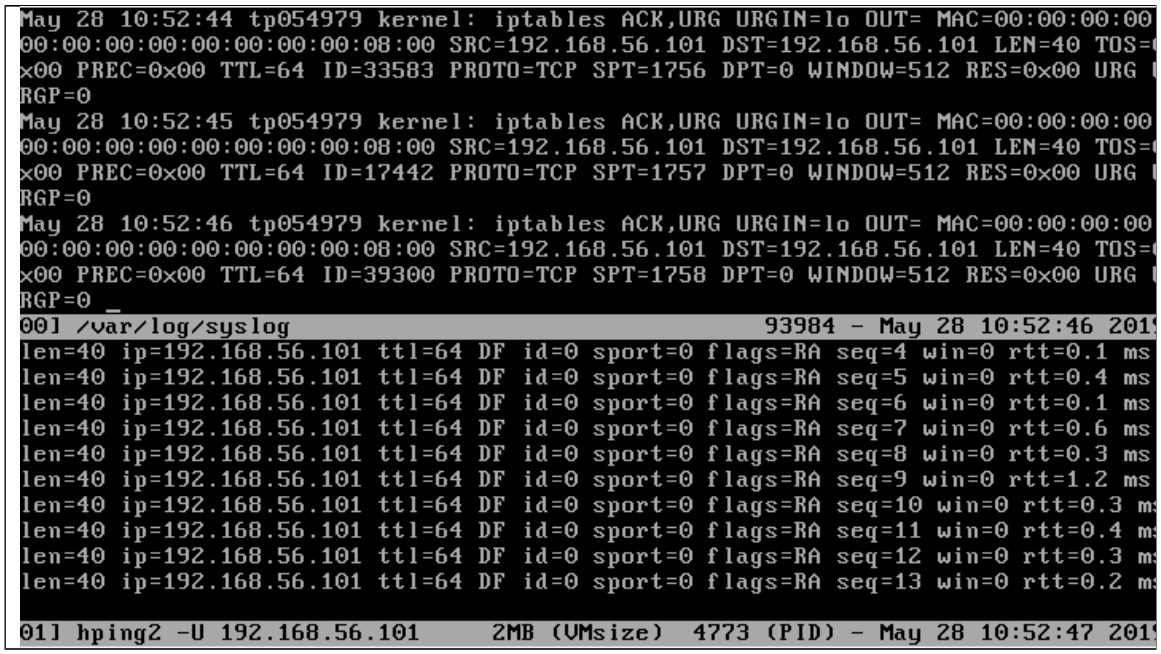
Output of rule 4



Output of rule 5



Output of rule 6



Obstacles encountered, obstacles overcome

N/A

Any Outstanding/Unresolved Issues

N/A