

sna

by Kapil Pokhrel

Submission date: 04-Aug-2021 09:46AM (UTC+0800)

Submission ID: 1627470918

File name: sna_final_v2docx.docx (1.96M)

Word count: 1370

Character count: 7136

Acknowledgement

We'd want to thank **Infamax College of IT and Management** for everything they've done for us. We're excited to broaden our understanding of Tinynet capabilities.

In compliance with APU(Asia Pacific University) rules and regulations, the project report is developed to meet a portion of the requirement for the degree of BSC.IT (APU). We are grateful to our teacher, **Mr. Santosh Panta**, for his direction and support in completing our work.

Finally, we would like to express our gratitude to Infamax College of IT and Management, as well as our teacher, **Mr. Santosh Pant**, for assisting us in properly planning our assignment.

Kapil Pokhrel(NPI000030)

Shivam Ranabhat(NPI000047)

Bikash Baral(NPI000021)

Contents

1. IP Tables (Shivam Ranabhat: NPI000047).....	3
1.2 Objective	3
1.3 Configurations.....	3
1.4 Screenshots	4
2. SUDO (Kapil Pokhrel : NPI000030)	8
2.1 Objective	8
2.2 Configuration	8
2.3 Screenshots	8
3. STUNNEL (Bikash Baral: NPI000021)	13
3.1 Objectives	13
3.2 Configuration	13
4. Virtual Server.....	23
4.1 Objectives	23
4.2 Configuration	23
5.0 Virtual Server With NFS	28
5.1 Objectives	28
6.0 Compile and Install	33
6.1 Objectives	33
6.2 Configuration	33
References.....	34

1. IP Tables (Shivam Ranabhat: NPI000047)

1.2 Objective

Ip tables is a network administrative tool which is used to filter the IPv4 packet and NAT. The major aim of IP tables is to apply the six available rules of IP tables in order to filter the TCP stack and to prevent the network from processing the TCP stack. And another aim of IP tables is to display all the six rules which is added with hping2 and multi tail.

1.3 Configurations

Now, we should add the available six rules of IP tables in command line which are shown below:

Rule 1: "iptables -A INPUT -p tcp --tcp-flags ALL NONE -j LOG --log-level alert --log-prefix "iptables ALL NONE"

Rule 2: "iptables -A INPUT -p tcp --tcp-flags FIN,SYN FIN,SYN -j LOG --log-level alert --log-prefix "iptables FIN,SYN FIN,SYN"

Rule 3: "iptables -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST -j LOG --log-level alert --log-prefix "iptables SYN,RST SYN,RST"

Rule 4: "iptables -A INPUT -p tcp --tcp-flags FIN,RST FIN,RST -j LOG --log-level alert --log-prefix "iptables FIN,RST FIN,RST "

Rule 5: "iptables -A INPUT -p tcp --tcp-flags FIN,ACK FIN -j LOG --log-level alert --log-prefix "iptables FIN,ACK FIN"

Rule 6: "iptables -A INPUT -p tcp --tcp-flags ACK,URG URG -j LOG --log-level alert --log-prefix "iptables ACK,URG URG"

We use “iptables-L” in order to see all the IP rules.

According to question, we should display the IP tables using hping 2 and multi tail so we should enter the six commands which are shown below:

Rule 1: 'multitail /var/log/syslog -l "hping2 192.168.56.101"

Rule 2: 'multitail /var/log/syslog -l "hping2 -F -S 192.168.56.101"

Rule 3: 'multitail /var/log/syslog -l "hping2 -S -R 192.168.56.101"

Rule 4: 'multitail /var/log/syslog -l "hping2 -F -R 192.168.56.101"

Rule 5: 'multitail /var/log/syslog -l "hping2 -F 192.168.56.101"

Rule 6: 'multitail /var/log/syslog -l "hping2 -U 192.168.56.101"

1.4 Screenshots

```
root@gw-npi000021bikash:~# iptables -A INPUT -p tcp --tcp-flags ALL NONE -j LOG  
--log-level alert --log-prefix "iptables ALL NONE"  
root@gw-npi000021bikash:~# iptables -A INPUT -p tcp --tcp-flags FIN,SYN FIN,SYN  
-j LOG --log-level alert --log-prefix "iptables FIN,SYN FIN,SYN"  
root@gw-npi000021bikash:~# iptables -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST  
-j LOG --log-level alert --log-prefix "iptables SYN,RST SYN,RST"  
root@gw-npi000021bikash:~# iptables -A INPUT -p tcp --tcp-flags FIN,RST FIN,RST  
-j LOG --log-level alert --log-prefix "iptables FIN,RST FIN,RST"  
root@gw-npi000021bikash:~# iptables -A INPUT -p tcp --tcp-flags FIN,ACK FIN -j L  
OG --log-level alert --log-prefix "iptables FIN,ACK FIN"  
root@gw-npi000021bikash:~# iptables -A INPUT -p tcp --tcp-flags ACK,URG URG -j L  
OG --log-level alert --log-prefix "iptables ACK,URG URG"  
root@gw-npi000021bikash:~# _
```

Fig: Six rules of IP Tables

To filter the TCP stack, we have added the six rules of IP tables.

```

root@gw-npi000021bikash:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
LOG        tcp   --  anywhere       anywhere      tcp flags:FIN,SYN,
RST,PSH,ACK,URG/NONE LOG level alert prefix "iptables ALL NONE"
LOG        tcp   --  anywhere       anywhere      tcp flags:FIN,SYN/
FIN,SYN LOG level alert prefix "iptables FIN,SYN FIN,SYN"
LOG        tcp   --  anywhere       anywhere      tcp flags:SYN,RST/
SYN,RST LOG level alert prefix "iptables SYN,RST SYN,RST"
LOG        tcp   --  anywhere       anywhere      tcp flags:FIN,RST/
FIN,RST LOG level alert prefix "iptables FIN,RST FIN,RST"
LOG        tcp   --  anywhere       anywhere      tcp flags:FIN,ACK/
FIN LOG level alert prefix "iptables FIN,ACK FIN"
LOG        tcp   --  anywhere       anywhere      tcp flags:ACK,URG/
URG 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@gw-npi000021bikash:~#

```

Fig: Newly added rules

This shows all the lists of IP tables rules which we have added.

Now, the screenshots given below shows the rules of IP tables using hping2 and multi tail where each screenshot shows one rule.

```

001 /var/log/syslog F1/<CTRL>+<h>: help          0 - Aug 03 16:50:41 2021
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=20 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=21 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=22 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=23 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=24 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=25 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=26 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=27 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=28 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=29 win=0 rtt=0.1 ms

011 hping2 192.168.56.101      3MB (UMsize) 1274 (PID) - Aug 03 16:51:10 2021

```

Fig: Showing Rule 1

```
001 /var/log/syslog F1/<CTRL>+<h>: help 0 - Aug 03 16:53:58 2021
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=4 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=5 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=6 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=7 win=0 rtt=0.3 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=8 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=9 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=10 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=11 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=12 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=13 win=0 rtt=0.1 ms

011 hping2 -F -S 192.168.56.101 1277 (PID) - Aug 03 16:54:11 20
```

Fig: Showing Rule 2

```
001 /var/log/syslog F1/<CTRL>+<h>: help 0 - Aug 03 16:55:40 2021
HPING 192.168.56.101 (eth1 192.168.56.101): RS set, 40 headers + 0 data bytes

011 hping2 -S -R 192.168.56.101 F1/^h: help 1281 (PID) - Aug 03 16:55:40 20
```

Fig: Showing Rule 3

```
001 /var/log/syslog F1/<CTRL>+<h>: help          0 - Aug 03 16:57:10 2021
HPING 192.168.56.101 (eth1 192.168.56.101): RF set, 40 headers + 0 data bytes

011 hping2 -F -R 192.168.56.101 F1/^h: help      1285 (PID) - Aug 03 16:57:10 20
```

Fig: Showing Rule 4

```
001 /var/log/syslog F1/<CTRL>+<h>: help          0 - Aug 03 16:58:27 2021
HPING 192.168.56.101 (eth1 192.168.56.101): F set, 40 headers + 0 data bytes
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=2 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=3 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=4 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=5 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=6 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=7 win=0 rtt=0.2 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=8 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=9 win=0 rtt=0.1 ms
011 hping2 -F 192.168.56.101      3MB (UMsize) 1289 (PID) - Aug 03 16:58:36 2021
```

Fig: Showing Rule 5

```
001 /var/log/syslog F1/<CTRL>+<h>: help          0 - Aug 03 16:59:47 2021
HPING 192.168.56.101 (eth1 192.168.56.101): U set, 40 headers + 0 data bytes
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=0.7 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=2 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=3 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=4 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=5 win=0 rtt=0.1 ms
len=40 ip=192.168.56.101 ttl=64 DF id=0 sport=0 flags=RA seq=6 win=0 rtt=0.1 ms

011 hping2 -U 192.168.56.101      3MB (UMsize) 1292 (PID) - Aug 03 16:59:53 2021
```

Fig: Showing Rule 6

2. SUDO (Kapil Pokhrel : NPI000030)

2.1 Objective

Depending upon the security policy, sudo allows a permitted user to run a command as superuser or other. The meaning of sudo is task and permission according to the capability of a super user. This feature or software allows normal users to have administrative capabilities in Linux operating systems. SUPERUSER DO (Sudo) is a command that allows a super user to perform tasks and grant permissions.

2.2 Configuration

Using the command “adduser” on mail host we have created two normal users with following details

“Username: kapil; password: kapil

Username: shivam; password: shivam”

2.3 Screenshots

```
root@gw-kapilnpi000030:~# passwd kapil
Changing password for kapil
Enter the new password (minimum of 5 characters)
Please use a combination of upper and lower case letters and numbers.
New password:
Bad password: too simple.
Warning: weak password (enter it again to use it anyway).
New password:
Re-enter new password:
They don't match; try again.
New password:
Re-enter new password:
passwd: password changed.
root@gw-kapilnpi000030:~# useradd shivam
root@gw-kapilnpi000030:~# passwd shivam
Changing password for shivam
Enter the new password (minimum of 5 characters)
Please use a combination of upper and lower case letters and numbers.
New password:
Re-enter new password:
They don't match; try again.
New password:
Re-enter new password:
passwd: password changed.
root@gw-kapilnpi000030:~# _
```

Fig: Adding two normal users

We have edited the file /etc/sudoers to force all users along with two created users to use sudo as follows

```
sudoers      [-M--] 11 L:1 24+11 35/ 48] *(992 /1360b) 0032 0x020  [*][X]
Defaults    editor=/usr/bin/mcedit:/usr/bin/vi

# -----
# Runas alias specification

# -----
# User privilege specification

# Let root run any command on any host as any user.
root      ALL = (ALL) ALL
kapil     ALL = (ALL) ALL
shivam   ALL = (ALL) ALL

# or use this instead for no password
# root      ALL = (ALL) NOPASSWD: ALL

# Uncomment to allow people in group wheel to run all commands
# %wheel    ALL = (ALL) ALL
# or use this instead for no password
# %wheel    ALL = (ALL) NOPASSWD: ALL

# Samples
# %users   ALL=/sbin/mount /mnt/hdc,/sbin/umount /mnt/hdc
1Help  2Save  3Mark  4Replace 5Copy  6Move  7Search 8Delete 9PullDn10Quit
```

Fig: Force to use sudo

The following window shows the color prompt for user kapil:

```
htop      .... to check process and memory use
df -h     .... to check free disk space
links     .... browser (press [esc] for the menu)
mytyip    .... for the name and IP address of this system
poweroff  for system shutdown or reboot for system restart

To open a new login screen, use [Alt] F1 to [Alt] F6
-----
Edit /etc/issue.mytyvm to stop advertising the root password!

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

gw-kapilnpi000030.net-o.tiny.net.edu
192.168.1.18 /24 (eth0)
192.168.56.101 /24 (eth1)
192.168.66.101 /24 (eth2)
192.168.76.101 /24 (eth3)

gw-kapilnpi000030 login: kapil
Password:
No directory, logging in with HOME=/
Linux 4.19.86 [ x86 noPAE gcc 9.2.0 ] 24 Nov 2019 @slackware.com
Last login: Tue Aug  3 18:40:41 +0000 2021 on /dev/tty1.
[kapile@gw-kapilnpi000030:~]$
```

Fig: Color prompt for user kapil

```
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)
mytyip    .... for the name and IP address of this system
poweroff  for system shutdown or reboot for system restart

To open a new login screen, use [Alt] F1 to [Alt] F6
-----
Edit /etc/issue.mytyvm to stop advertising the root password!

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

gw-kapilnpi000030.net-o.tiny.net.edu
192.168.1.18 /24 (eth0)
192.168.56.101 /24 (eth1)
192.168.66.101 /24 (eth2)
192.168.76.101 /24 (eth3)

gw-kapilnpi000030 login: root
Password:
Linux 4.19.86 [ x86 noPAE gcc 9.2.0 ] 24 Nov 2019 @slackware.com
Last login: Tue Aug  3 17:29:30 +0000 2021 on /dev/tty1.
root@gw-kapilnpi000030:~#
```

Fig: Color prompt for root

We have edited **/etc/profile** in order to start up a display that show different colors each time a user logs in.

```
profile           [ -M- ] 47 L:[ 44+12 56/ 71] *(1623/1877b) 0010 0x00A [*][X]
elif [ "$SHELL" = "/bin/zsh" ]; then
    PS1='z@%m:%~%# '
elif [ "$SHELL" = "/bin/bash" ]; then
    PS1='$ '
else
    if [ $(id -u) -ne 0 ]; then
        # non-root user
        # PS1='u@%h:%w$ '
        PS1='[\u033[01;32m]\u033[00m]\u033[01;31m]\u033[00m%\u033[01;31m]\u033[00m$ '
    else
        # root user
        # PS1='u@\u033[01;31m%\u033[01;31m\u033[01;31m$ '
        PS1='[\u033[01;31m%\u033[01;31m]\u033[01;31m$\u033[01;31m'_
    fi
fi

PS2='> '
export PATH DISPLAY LESS TERM PS1 PS2

# Append any additional sh scripts found in /etc/profile.d/
for profile_script in /etc/profile.d/*.*sh ; do
    if [ -x $profile_script ]; then
        1Help 2Save 3Mark 4Replace 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

Fig: Editing the profile to display different colors

At the end, we have edit `/etc/issue.mytym` in order to stop the advertising root password as below:

```
Issue.mytinyvm [-M--] 16 L:[ 1+13 14/ 18] *(840 /1096b) 0069 0x045 [*][X]
6m   Welcome to TinyNet          www.my-tiny.net      mytinyVM (ovl)^[[0m
6m -----
7m   Some useful commands:^[[0m
3m     mc^[[0m      .... to view - edit - copy - move - delete files
3m     htop^[[0m      .... to check process and memory use
3m     df -h^[[0m      .... to check free disk space
3m     links^[[0m      .... browser (press Esc for the menu)
3m     mytip^[[0m      .... for the name and IP address of this system
3m     poweroff^[[0m  for system shutdown or ^[[1;33mreboot^[[0m for system
                  To open a new login screen, use ^[[1;32m[Alt] F1^[[0m to ^[[1;32m[Alt] F6^[[0m
6m -----
7m     # Edit ^[[1;35m/etc/issue.mytinyvm^[[1;37m to stop advertising the root pa
                  get started, login as ^[[1;36mroot^[[0m with password ^[[1;36mtoor^[[0m, both l
6m -----^[[0m
1Help 2Save 3Mark 4Replace 5Copy 6Move 7Search 8Delete 9PullDown 10Quit
```

Fig: Stop advertising the root password

3. STUNNEL (Bikash Baral: NPI000021)

3.1 Objectives

Stunnel is a multi-platform and open-source application which provides a global tunneling service for TLS/SSL. It may be used to protect the encrypted connections for both client and server. Similarly, it uses X public key encryption. Stunnel operates by listening to another port and redirecting traffic to unsecured port. Stunnel ensures for error messages and also allows users to connect their domain to send a mail.

3.2 Configuration

For establishing the communication between all the tiny net servers gateway, mail host, LDAP host and web server should be configured with Linux 2.6(32 bit) with the installation of base system into partitions.

Open **/etc/rc.d.d/xinetd** and follow the steps listed below:

1. Rename **/etc/rc.d.d/xinetd/telnet** to **/etc/rc.d.d/inetd** and set execute bits.

2. 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

3. 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

4. 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: bikashbarall000@gmail.com

RCPT To: bikashnpi000021@mailhost.tinynet.edu

DATA

Subject: individual sna

my name is kapil.

. (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 “bikashnpi000021@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

bikashnpi000021@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=tinytnet',  
    'base' => 'o=tinytnet.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”.

For configuring stunnel following process are followed:

1. At first run gateway then mail host and webserver.
2. To set executable bits go to **/etc/rc.d/stunnel** then modify the file as given 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. Then to modify the file “rc.yp” to “rc.stunnel” go to **/etc/rc.d/rc.inetd2** two times under Start NIS.

Similarly, for configuring host system following process are followed:

1. At first open the page using the URL 192.168.56.252/ in order to download TinyNetCA certificate from Squirrel mail page.
2. Then install the certificate as trusted root certificate to host system and web browser.
3. At last, clear the caches to access the Squirrel mail login page with URL 192.168.56.252/

Test with Screenshots

192.168.56.252/squirrelmail/src/login.php



SquirrelMail
webmail
for
nuts

SquirrelMail version 1.4.22
By the SquirrelMail Project Team

SquirrelMail Login

Name:

Password:

Fig: Squirrel Mail login page

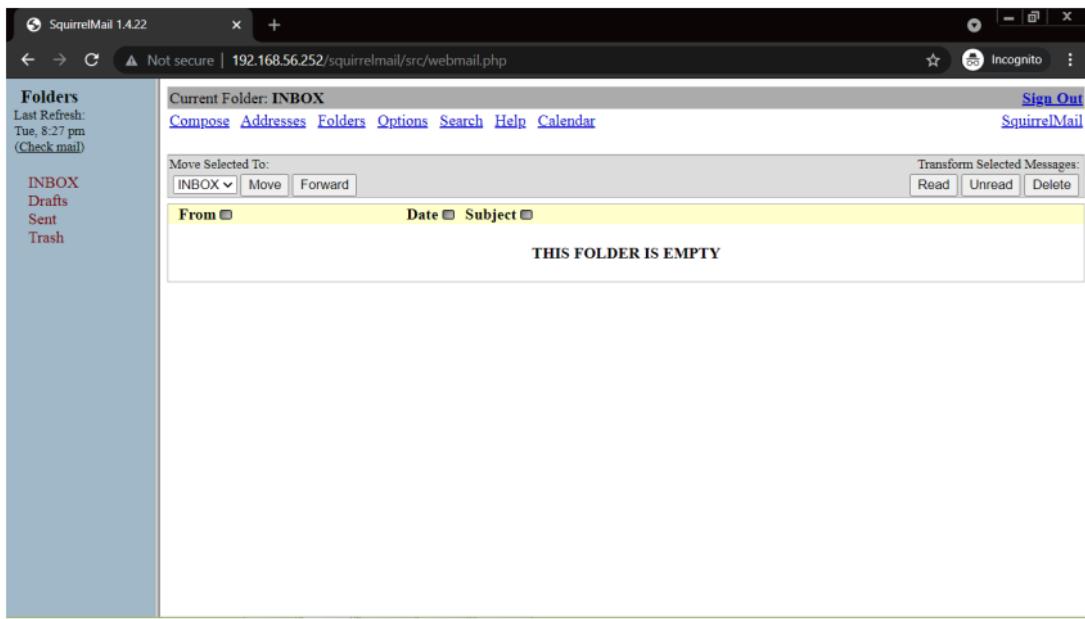


Fig: Empty Inbox

```
/home/vmail/bikashnpi000021/inbox          678/678          100%
From bikashbarali1000@gmail.com Tue Aug 03 15:27:59 2021
Return-Path: <bikashbarali1000@gmail.com>
Delivered-To: bikashnpi000021@mailhost.tinynet.edu
Received: from sending.host.name (localhost [127.0.0.1])
          by mailhost.tinynet.edu (Postfix) with SMTP id 903AEF4
          for <bikashnpi000021@mailhost.tinynet.edu>; Tue, 3 Aug 2021 15:24:17 +0
000 (UTC)
Subject: individual sna
Message-Id: <20210803152717.903AEF4@mailhost.tinynet.edu>
Date: Tue, 3 Aug 2021 15:24:17 +0000 (UTC)
From: bikashbarali1000@gmail.com
X-IMAPbase: 1628004479 0000000000
X-UID: 1
Status: R0
X-Keywords:

Content-Length: 18

my name is kapeel

1 Help 2 Unwrap 3 Quit 4 Hex 5 Goto 6 7 Search 8 Raw 9 Format 10 Quit
```

Fig: Sending mail

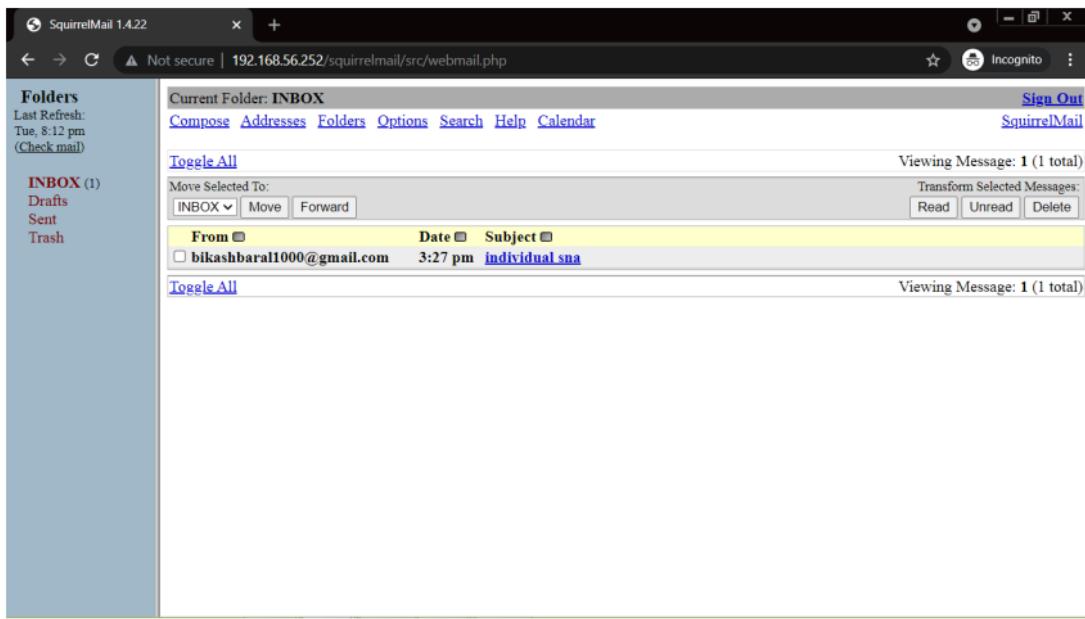


Fig: Mail received

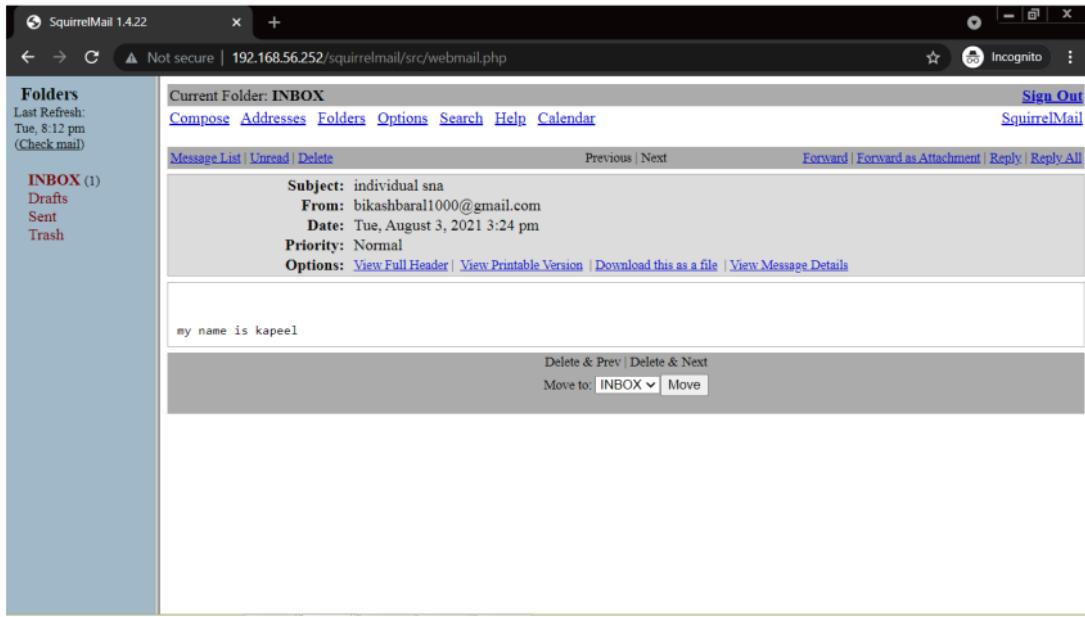


Fig: Details of received mail

```

tcp      0      0 0.0.0.0:http          0.0.0.0:*      LISTEN
1158/monkey
tcp      0      0 0.0.0.0:domain       0.0.0.0:*      LISTEN
1044/dnsmasq
tcp      0      0 0.0.0.0:ssh           0.0.0.0:*      LISTEN
1058/sshd
tcp      0      0 0.0.0.0:telnet        0.0.0.0:*      LISTEN
1053/xinetd
tcp      0      0 0.0.0.0:smtp          0.0.0.0:*      LISTEN
1149/postfix
tcp      0      0 0.0.0.0:submission    0.0.0.0:*      LISTEN
1149/postfix
tcp6     0      0 ::1:domain           ::1:*          LISTEN
1044/dnsmasq
udp      0      0 0.0.0.0:domain        0.0.0.0:*      LISTEN
1044/dnsmasq
udp      0      0 0.0.0.0:bootps        0.0.0.0:*      LISTEN
1044/dnsmasq
udp      0      0 0.0.0.0:bootpc        0.0.0.0:*      LISTEN
1011/dhcpacd
udp      0      0 0.0.0.0:33886         0.0.0.0:*      LISTEN
1044/dnsmasq
udp6     0      0 ::1:domain           ::1:*          LISTEN
1044/dnsmasq
root@gw-npi000021bikash:~# 

```

Fig: Gateway listening port

```

root@mail-nc:~# mc
root@mail-nc:~# mc
root@mail-nc:~# mc

root@mail-nc:~# netstat -tulp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address      State
PID/Program name
tcp      0      0 0.0.0.0:submission      0.0.0.0:*      LISTEN
1085/postfix
tcp      0      0 0.0.0.0:imap           0.0.0.0:*      LISTEN
1095/dovecot
tcp      0      0 0.0.0.0:http          0.0.0.0:*      LISTEN
1102/monkey
tcp      0      0 0.0.0.0:ssh           0.0.0.0:*      LISTEN
994/sshd
tcp      0      0 0.0.0.0:telnet        0.0.0.0:*      LISTEN
989/xinetd
tcp      0      0 0.0.0.0:smtp          0.0.0.0:*      LISTEN
1085/postfix
udp      0      0 0.0.0.0:bootpc        0.0.0.0:*      LISTEN
980/dhcpacd
root@mail-nc:~# 

```

Fig: Mailhost listening port

```
To get started, login as root with password toor, both lowercase
-----
web-na.net-a.tiny.net.edu
 192.168.56.224 /24 (eth0)
 192.168.56.252 /24 (eth0:0)

web-na login: root
Password:
Linux 4.19.86 [ x86 noPAE gcc 9.2.0 ] 24 Nov 2019 @slackware.com
Last login: Tue Aug  3 18:44:53 +0000 2021 on /dev/tty1.
root@web-na:~# netstat -tulp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
PID/Program name
tcp      0      0 0.0.0.0:httpp            0.0.0.0:*
1022/monkey
tcp      0      0 0.0.0.0:ssh             0.0.0.0:*
998/sshd
tcp      0      0 0.0.0.0:telnet          0.0.0.0:*
993/xinetd
udp      0      0 0.0.0.0:bootpc          0.0.0.0:*
983/dhcpcd
root@web-na:~#
```

Fig: Webserver Listening Port

4. Virtual Server

4.1 Objectives

With the proper configuration, virtual servers allow a webserver to access and manage multiples websites. For security measures we have configured permissions, owners and cron. Similarly, two new users are also created with their own virtual host.

4.2 Configuration

Two users

“Username: kapil; password: kapil

Username: sivam; password: sivam” were created in monkey.conf using command **adduser** which is shown below:

```
monkey.conf      [-M--I 73 L:I 57+11  68/142] *(1908/3674b) 0010 0x00A  [*][X]

# <Virtualhost>
#   VirtualServerName www.example.org
#   VirtualDocumentRoot /var/www/example/htdocs
#   VirtualScriptAlias /cgi-bin/ /var/www/example/scripts/
#   VirtualForceGetDir off
# </Virtualhost>

<Virtualhost>
  VirtualServerName kapil.tinyt.net.edu
  VirtualDocumentRoot /var/monkey/htdocs/kapil
  VirtualScriptAlias /cgi-bin/ /var/monkey/htdocs/kapil/cgi-scripts/
  VirtualForceGetDir off
</Virtualhost>

<Virtualhost>
  VirtualServerName sivam.tinyt.net.edu
  VirtualDocumentRoot /var/monkey/htdocs/sivam
  VirtualScriptAlias /cgi-bin/ /var/monkey/htdocs/sivam/cgi-scripts/
  VirtualForceGetDir off
</Virtualhost>

# -----
# 1Help  2Save  3Mark  4Replace 5Copy  6Move  7Search 8Delete 9PullDown 10Quit
```

Fig: creating users in monkey.conf

Now, we have created the default home directories for two users using the following commands

useradd -m kapil

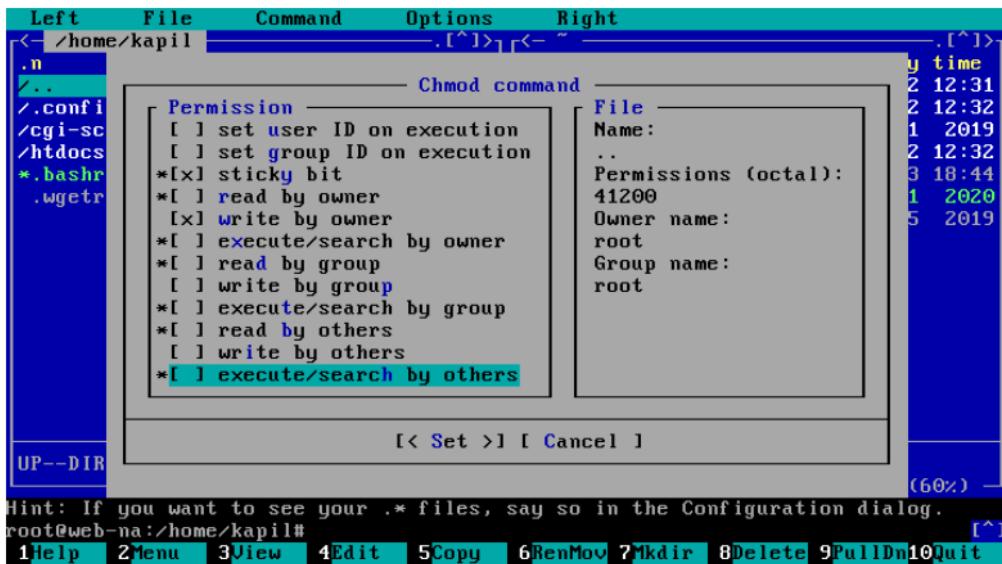
useradd -m sivam

```
192.168.56.224 /24 (eth0)
192.168.56.252 /24 (eth0:0)

web-na login: root
Password:
Linux 4.19.86 [ x86 noPAE gcc 9.2.0 ] 24 Nov 2019 @slackware.com
Last login: Tue Aug  3 18:37:41 +0000 2021 on /dev/tty1.
root@web-na:~# cd /home
root@web-na:/home# useradd -m kapil
root@web-na:/home# passwd kapil
Changing password for kapil
Enter the new password (minimum of 5 characters)
Please use a combination of upper and lower case letters and numbers.
New password:
Re-enter new password:
passwd: password changed.
root@web-na:/home# useradd -m sivam
root@web-na:/home# passwd sivam
Changing password for sivam
Enter the new password (minimum of 5 characters)
Please use a combination of upper and lower case letters and numbers.
New password:
Re-enter new password:
passwd: password changed.
root@web-na:/home#
```

Fig: creating default home directories

We have changed the permission so that two users “kapil” and “sivam” cannot access them



Now, we changed the permission successfully and set to owner only who can read, write and execute the files and others users are set to nobody.

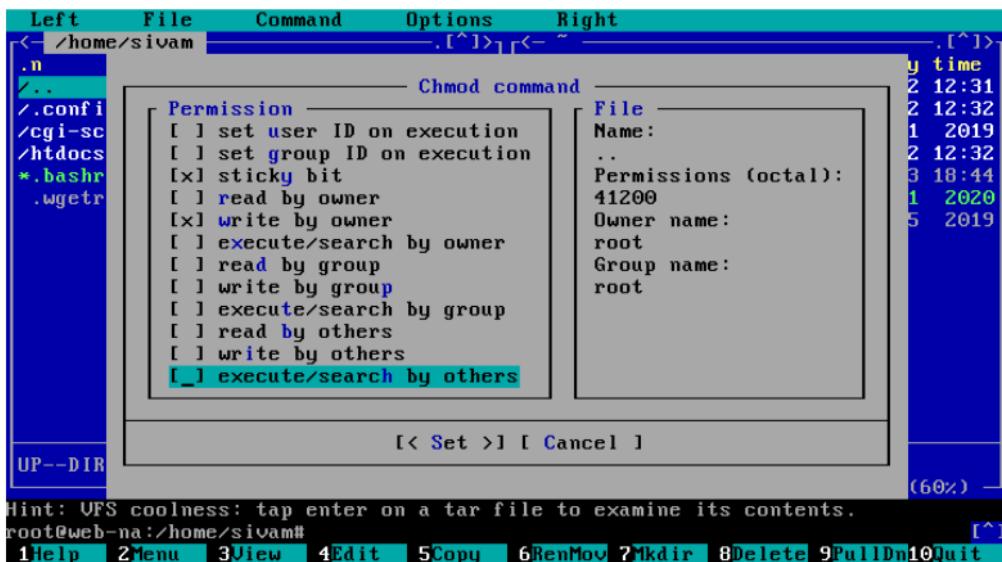


Fig: Changing permission

Adding appropriate cnames in /etc/dnsMasq.d/cnames to dnsMasq on the Gateway server which is shown below:

```
cnames      [-M--]  0 L:[ 8+22  30/ 31] *(1254/1255b) 0010 0x00A  [*][X]
# Here is where you give civilised names (cname) that real people.
# can remember by providing an alias. The cname must be unique, .
# but there can be more than one cname pointing to the same target..
# Additional directives (dhcp-fqdn, expand-hosts) require..
# these to be Fully Qualified Domain Names.

# Format is nicename [COMMA SPACE] uglyname from /etc/HOSTNAME

cname = npi000047-ws.tiny.net.edu, npi000047-ws.net-a.tiny.net.edu
cname = npi000047-ld.tiny.net.edu, npi000047-ld.net-b.tiny.net.edu
cname = npi000047-mh.tiny.net.edu, npi000047-mh.net-c.tiny.net.edu

cname = www.tiny.net.edu, neta-ws.net-a.tiny.net.edu
cname = webmail.tiny.net.edu, npi000047-ws.net-a.tiny.net.edu
cname = bananas.tiny.net.edu, nah1.net-a.tiny.net.edu

cname = ldap.tiny.net.edu, npi000047-ld.net-b.tiny.net.edu
cname = mailhost.tiny.net.edu, npi000047-mh.net-c.tiny.net.edu
cname = mail.tiny.net.edu, npi000047-mh.net-c.tiny.net.edu

1Help  2Save  3Mark  4Replace  5Copy  6Move  7Search  8Delete  9PullDn 10Quit
```

Fig: Changing cnames

Similarly, to move files automatically from the home directories to virtual document root we have set up a cron job in /var/spool/cron/crontabs/root as shown below:

```
root      [-M--] 0 L:I 7+22 29/ 36] *(1337/1344b) 0010 0x00A [*][X]
# Jobs that need different timing may be entered into the crontab as before,
# but most really don't need greater granularity than this. If the exact
# times of the hourly, daily, weekly, and monthly cron jobs do not suit your
# needs, feel free to adjust them.
#
# Run hourly cron jobs at 47 minutes after the hour:
47 * * * * /usr/bin/run-parts /etc/cron.hourly 1> /dev/null
#
# Run daily cron jobs at 4:40 every day:
40 4 * * * /usr/bin/run-parts /etc/cron.daily 1> /dev/null
#
# Run weekly cron jobs at 4:30 on the first day of the week:
30 4 * * 0 /usr/bin/run-parts /etc/cron.weekly 1> /dev/null
#
# Run monthly cron jobs at 4:20 on the first day of the month:
20 4 1 * * /usr/bin/run-parts /etc/cron.monthly 1> /dev/null

*/10 * * * * mv -f /home/kapil/htdocs/* /var/monkey/htdocs/kapil/
*/10 * * * * mv -f /home/kapil/cgi-scripts/* /var/monkey/htdocs/kapil/cgi-script

*/10 * * * * mv -f /home/sivam/htdocs/* /var/monkey/htdocs/sivam/
*/10 * * * * mv -f /home/sivam/cgi-scripts/* /var/monkey/htdocs/sivam/cgi-script
```

1Help 2Save 3Mark 4Replace 5Copy 6Move 7Search 8Delete 9PullDn10Quit

Fig: Adding lines for cron job

5.0 Virtual Server With NFS

5.1 Objectives

The main objectives of NFS are listed below:

- a. NFS which behaves as a server put the webserver directories over a new virtual machine.
- b. NFS creates directories under home directories and NFS server and also use the ssh files which allows them to run cron jobs.

Configuration

1. /etc/monkey/monkey.conf

Given screen was already setup in virtual server and configured in NFS.

```
monkey.conf      [-M--] 73 L:1 57+11 68/1421 *(1908/3674b) 0010 0x000  [♦] TEXT
#   <Virtualhost>
#     VirtualServerName www.example.org
#     VirtualDocumentRoot /var/www/example/htdocs
#     VirtualScriptAlias /cgi-bin/ /var/www/example/scripts/
#     VirtualForceGetDir off
#   </Virtualhost>

<Virtualhost>
  VirtualServerName kapil.tinytng.net.edu
  VirtualDocumentRoot /var/monkey/htdocs/kapil
  VirtualScriptAlias /cgi-bin/ /var/monkey/htdocs/kapil/cgi-scripts/
  VirtualForceGetDir off
</Virtualhost>

<Virtualhost>
  VirtualServerName sivam.tinytng.net.edu
  VirtualDocumentRoot /var/monkey/htdocs/sivam
  VirtualScriptAlias /cgi-bin/ /var/monkey/htdocs/sivam/cgi-scripts/
  VirtualForceGetDir off
</Virtualhost>

# -----
1Help  2Save  3Mark  4Replace 5Copy  6Move  7Search 8Delete 9PullDown 10Quit
```

Figure: Virtual hosts for user Kapil and Shivam

2. /etc/exports

Given screen shows the files added to NFS server using the following command:

file/var/monkey/htdocs*.tinynet.edu(ro,sync,no_subtree_check,no_root_squash)

```
exports      [-M--] 61 L:1  1+ 4   5/  51 *(215 x 215b)= <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.

/var/monkey/htdocs *(ro,sync,no_subtree_check,no_root_squash)

1 Help 2 Save 3 Mark 4 Select 5 GoBack 6 Back 7 Forward 8 Previous 9 Next 10 Exit 11 Done 12 Quit
```

Following are the steps using which we created NFS

1. A disk file “TinyNetConfig.iso” was used to mount on the newly created base system and was configured using no role.



Figure: C0nfigure NFS using no role

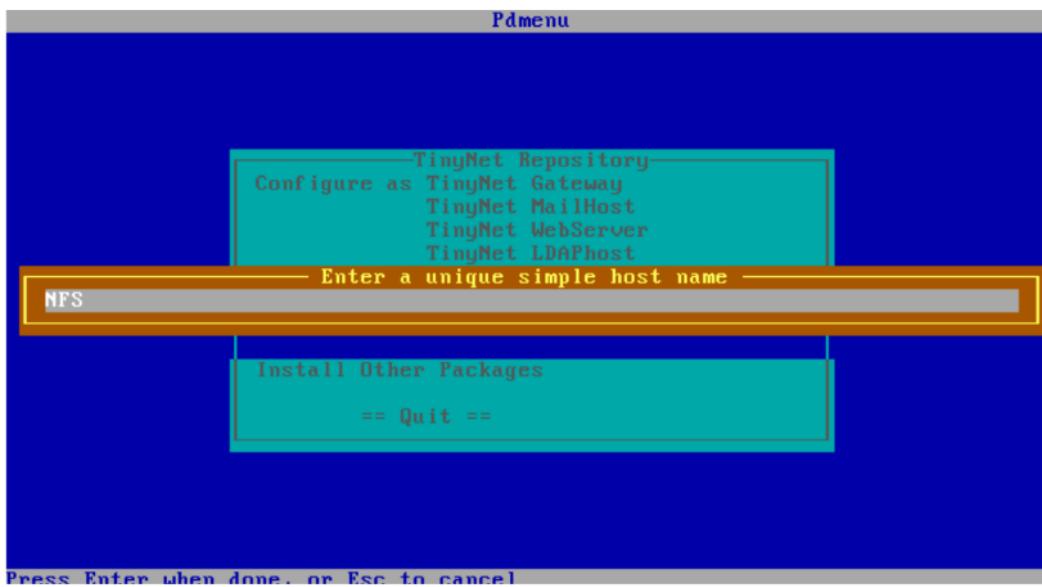


Figure: Entering the unique simple hostname

2. The execute permission was set to owner, group and other on two files `/etc/rc.d/rc.rpc` and `/etc/rc.d/rc.nfsd`

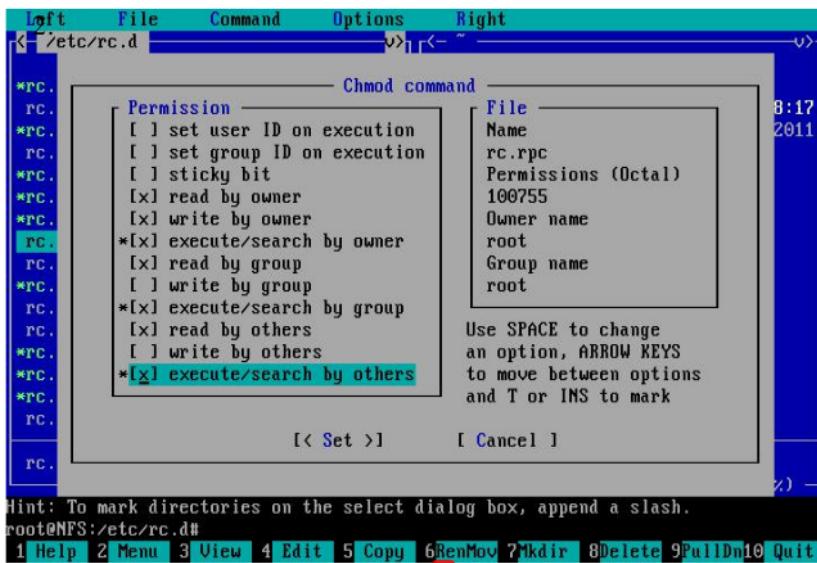


Figure: Executing the permission for rc.rpc in NFS

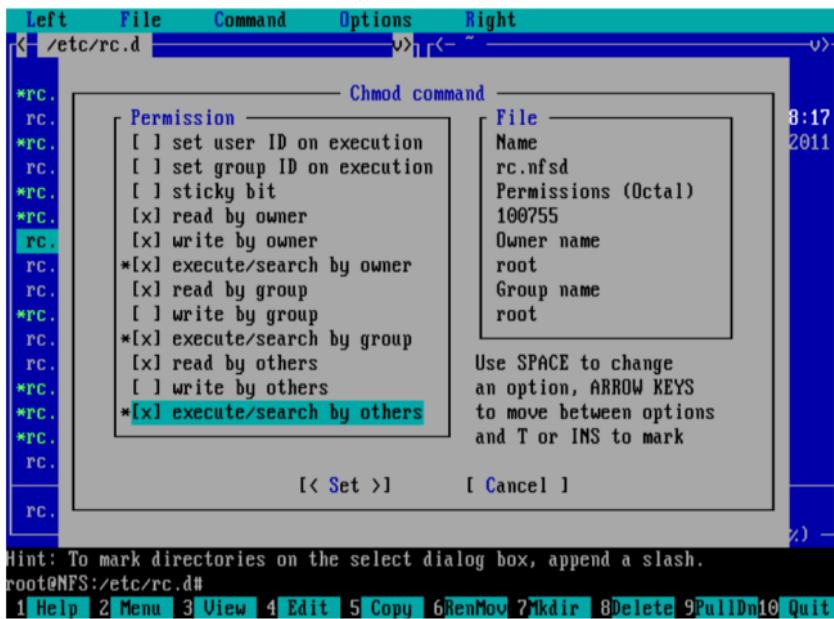


Figure: Executing the permissions for rc.nfsd in NFS

Above permissions were set on webserver.

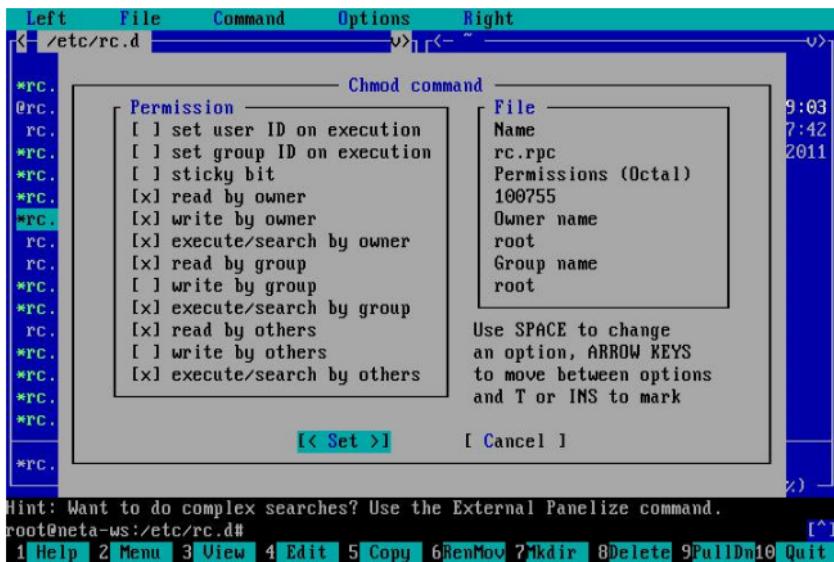


Figure: Executing the permission for rc.rpc in webserver

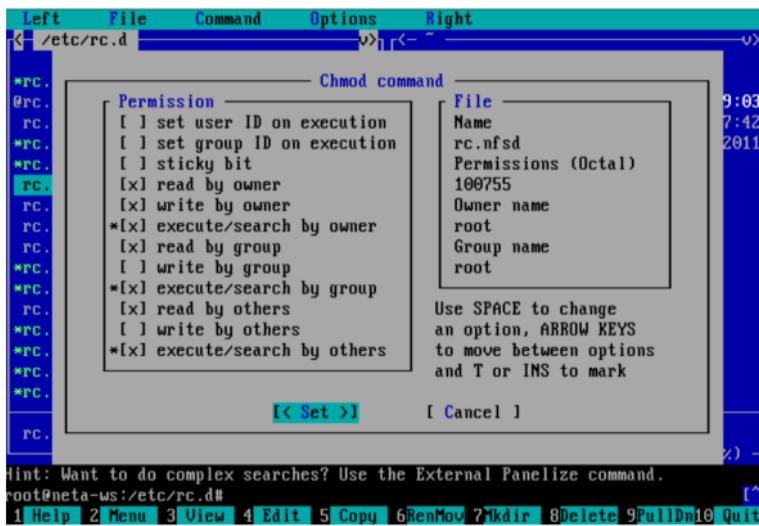


Figure: Executing the Permission for rc.nfsd in webserver

Now the following process is used to restart the service

1

- a. rc.rpc and rc.nfsd both were well run on NFS and webserver.

/etc/rc.d/rc.rpc start

/etc/rc.c/rc.nfsd start

```
root@NFS:/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@NFS:/etc/rc.d# /etc/rc.d/rc.nfsd start
root@NFS:/etc/rc.d# _
```

Figure: Restarting the service on NF

6.0 Compile and Install

6.1 Objectives

Setting up GCC Virtual Machine

A TinyNet-gcc..iso file is used to create a virtual machine, with 320 MB of RAM and 550 MB of hard drive memory. You can access the basic operating system by downloading lilionst.sh.

6.2 Configuration

Required packages are installed.

It is installed from TinyNetConfig.iso and customized on the optical drive using the Asciiart software.

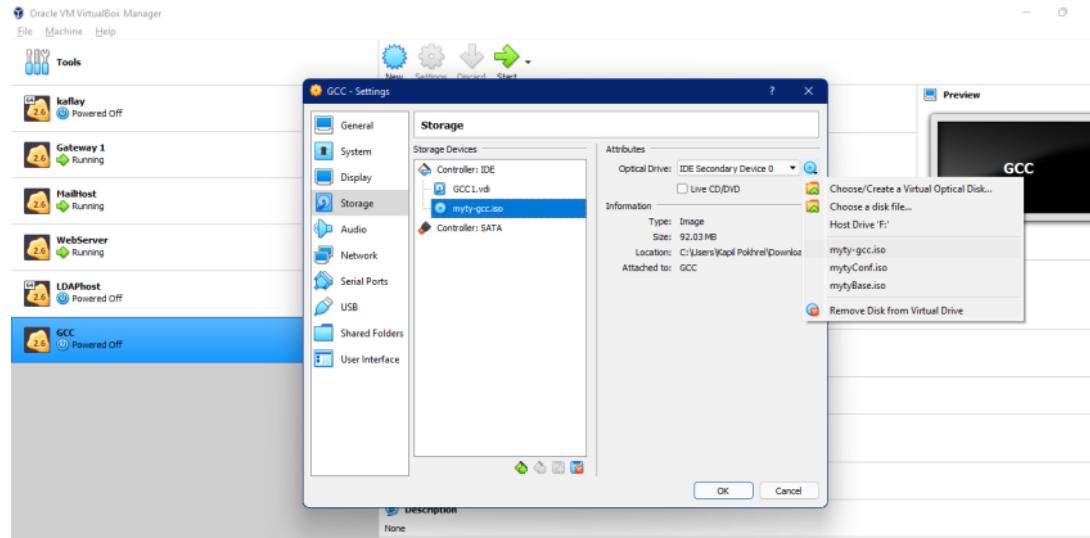


Figure: mytyconfig.iso file configuration

References

8%
SIMILARITY INDEX

0%
INTERNET SOURCES

0%
PUBLICATIONS

8%
STUDENT PAPERS

PRIMARY SOURCES

1 Submitted to Asia Pacific University College of
Technology and Innovation (UCTI)
Student Paper 8%

Exclude quotes Off

Exclude bibliography On

Exclude matches Off