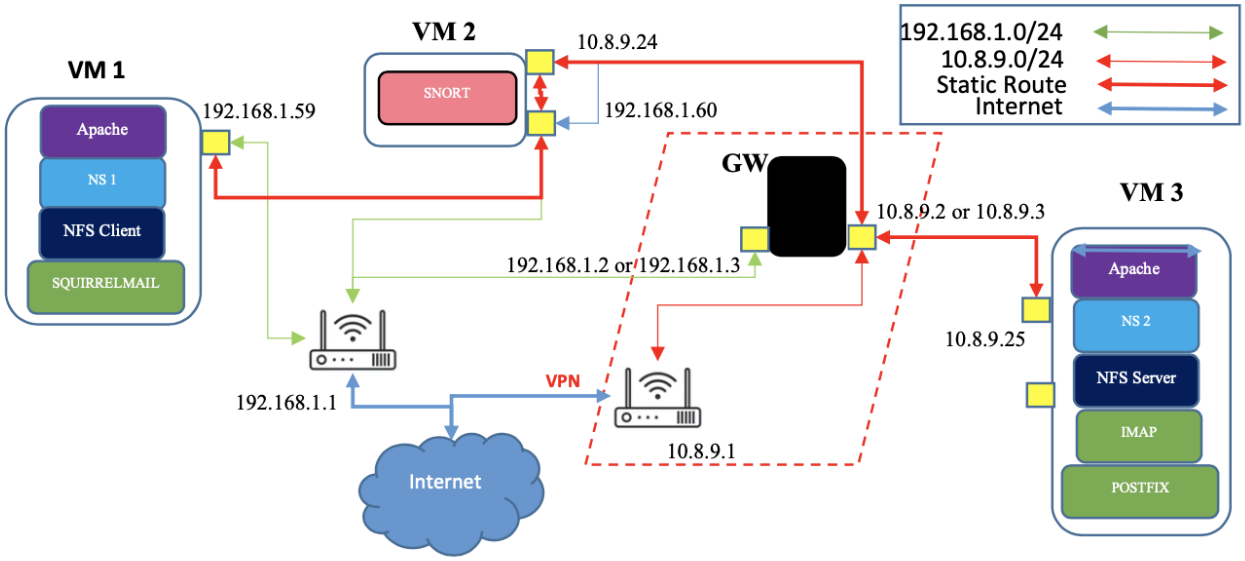
Nafisa Humyra
Dec 2023
Squirrelmail MUA

## Overview of Virtual Computing Infrastructure



There are 5 tasks that I'll be demonstrating in this project, as described below:

| Task | Topic |
|---|---|
| 1 | Internal email using Squirrelmail |
| 2 | Internal email from VM3 to another VM using the mail command |
| 3 | External email using Squirrelmail |
| 4 | Implementing deep packet inspection using Snort IDS |
| 5 | Routing |

# Introduction and Setup

This project demonstrates the setup and configuration of a small-scale email system using virtual machines (VMs), including the implementation of a routing system and a security monitoring solution. The project was executed using three Ubuntu-based VMs, each serving distinct roles in the network infrastructure. Below is a detailed setup and the tasks accomplished during the project.

## Network Configuration

1. **VM Setup:**

- **VM1**: Acts as the client machine with SquirrelMail configured as the Mail User Agent (MUA).
- **VM2**: Configured as a router to route traffic between VM1 and VM3. Snort is installed on VM2 for traffic monitoring.
- **VM3**: Functions as the mail server with SMTP and IMAP services installed and configured.

2. **Routing Configuration**:
VM2 was configured to route all traffic from VM1 to VM3, creating a path:
VM1 -> VM2 -> VM3.

Apache2 was installed on VM3 to serve web content. This setup would be accessed through the routing path. Next, the netplan file on VM2 was updated to define the network interfaces and their configurations. This was necessary to set the correct IP addresses and routing policies.

The routing policies on VM2 were then updated to ensure that it could direct traffic between the VMs. IP forwarding was enabled on VM2 to allow it to forward packets between VM1 and VM3. This step was crucial for VM2 to function as a router.

For the route configuration, traffic from VM1 to VM3 was set to pass through VM2, creating the path VM1 -> VM2 -> VM3. Similarly, the return traffic from VM3 to VM1 was also configured to pass through VM2, ensuring the path VM3 -> VM2 -> VM1.

## Email System Configuration

1. **SquirrelMail on VM1:**
   - SquirrelMail was installed on VM1 to provide a web-based interface for sending and receiving emails.
   - Dependencies such as Apache2, PHP, and other necessary packages were installed and configured.

2. **SMTP Server on VM3**:
   - DNS Configuration - Entries for the SMTP server were created in the DNS forward and reverse zone files to ensure proper mail routing.
   - User Creation - Created users on VM3 for email.
   - Postfix Configuration - Postfix was installed and configured with several important files:
     - transport: Defined routing for specific destination domains, bypassing DNS queries if needed.
     - access: Used for security, including blocking specific senders or recipients.
     - aliases: Set up user aliases to forward emails to multiple recipients.
     - main.cf: The main configuration file for Postfix, containing all essential settings.

3. **IMAP Server on VM3**:

Dovecot Installation - Dovecot was installed to handle IMAP services, allowing email retrieval by clients.

4. **Tunnel Configuration**:

Mozilla Thunderbird - Configured to use a VPN tunnel to securely access the SMTP and IMAP servers, ensuring encrypted communication over the network.

### Security Monitoring with Snort

**Snort Configuration**

- Installed and configured Snort on VM2 to monitor and analyze network traffic passing through the router.

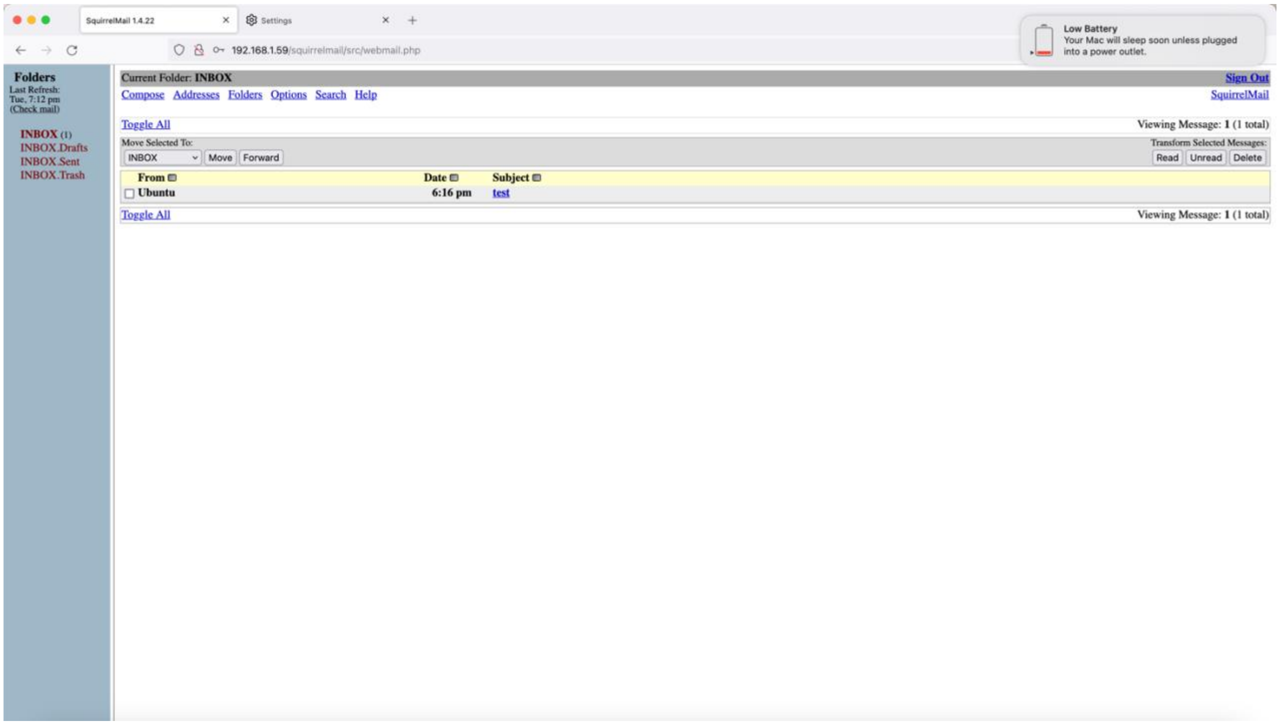
**Traffic Monitoring**

- Specific rules were created in Snort to monitor various types of traffic:
  - HTTP - Monitored web traffic for potential security threats.
  - SMTP - Monitored email traffic for suspicious activity.
  - IMAP - Monitored email retrieval traffic for anomalies.
  - DNS - Monitored DNS queries and responses.
  - NFS - Monitored network file system traffic.

This comprehensive setup not only provided a functional email system but also ensured security measures were in place to monitor and protect the network.

## Task 1: Internal email from your Squirrelmail to another user you created

| Task 1 | What's needed? | What to Submit? |
|---|---|---|
| 1. Using Squirrelmail send an email to another user you created on VM3 | **Non ubuntu user account** | 1. Screenshot of Squirrelmail inbox verifying message was received by the other user |


SquirrelMail 1.4.22
Settings
Low Battery
Your Mac will sleep soon unless plugged into a power outlet.
Compose Addresses Folders Options Search Help
Sign Out
SquirrelMail
Toggle All
Move Selected To:
INBOX
Move
Forward
Transform Selected Messages:
Read
Unread
Delete

192.168.1.59/squirrelmail/src/webmail.php

Folders
Last Refresh:
Tue, 7:12 pm
(Check mail)

INBOX (1)
INBOX.Drafts
INBOX.Sent
INBOX.Trash

Current Folder: INBOX

Viewing Message: 1 (1 total)

| From | Date | Subject |
|---|---|---|
| □ Ubuntu | 6:16 pm | test |

Viewing Message: 1 (1 total)

**Table 1:**

| Source IP | Email address of non ubuntu account | Date/Time ping Sent |
|---|---|---|
| 192.168.1.59 (VM1 IP) | doej@mail.nafisahumyra.com | 12/10/23 11:20PM |

## Task 2: Internal email from your VM3 using the mail command to leberkc on 10.8.9.81

| Task 2 | What's needed? | What to Submit? |
|---|---|---|
| Send an email **from your VM3 as the ubuntu user** to the leberkc email account on **10.8.9.81** with | 1. Username for the email address to | 1. Explain what you did to get this to work. Provide **screenshots** for |

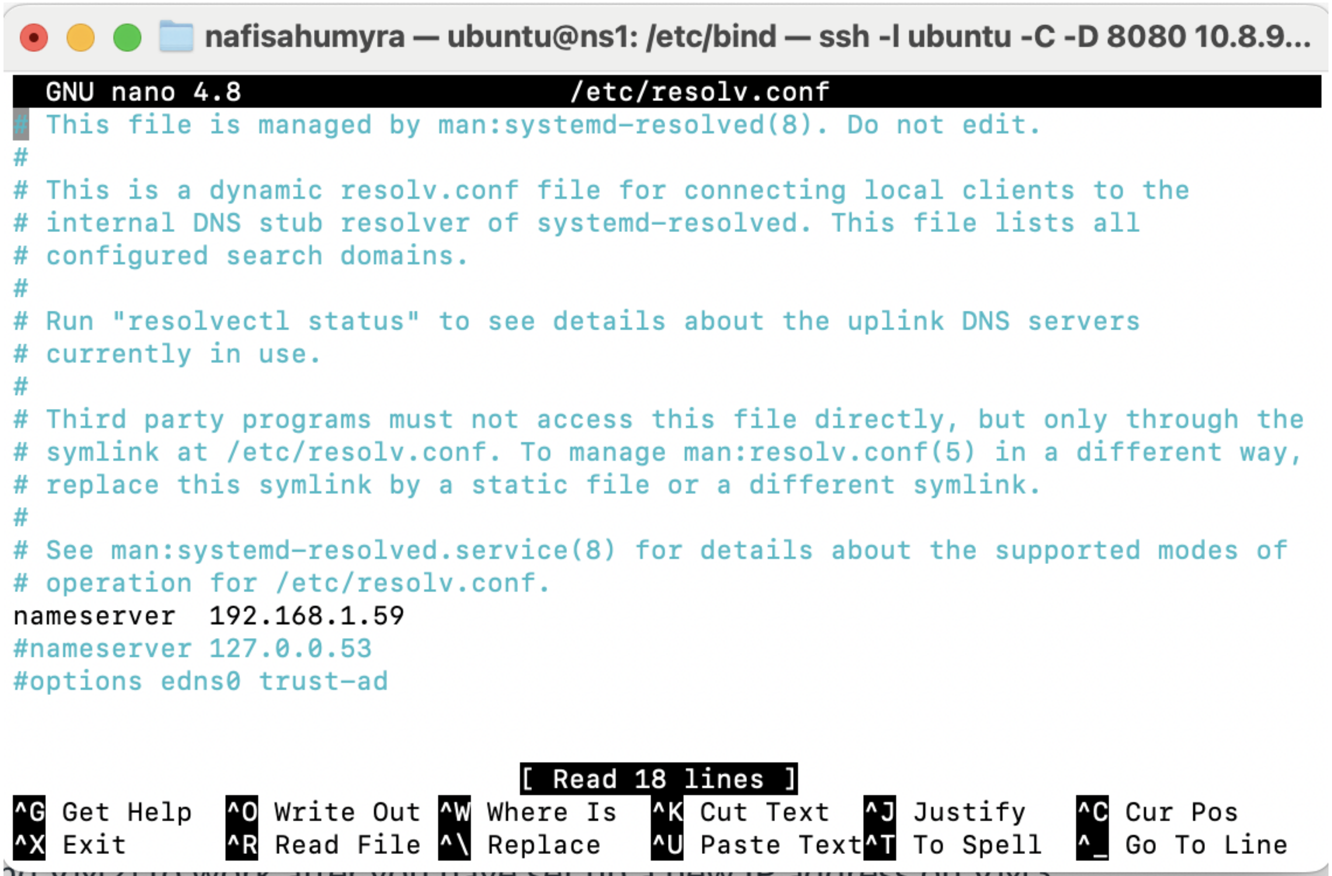
| | | |
|---|---|---|
| domain **leberkc@mail.greenbergthr1.com**. Make sure to state your name and IP address in the message<br>**NOTE**: If you have the 10.8.9.81 IP address, then send your message to leberkc on **10.8.9.93** with domain **leberkc@mail.ranas6.com**<br>Everyone must send the message to the leberkc account on the 10.8.9.81.<br>**DO NOT SEND THE EMAIL TO THE UBUNTU USER** | send the message<br>2. Destination IP address for the email message | any configuration changes required with explanations<br>2. Provide a **table** with the following:<br>a. IP address you sent the message from (source IP)<br>b. IP address where you sent the email message to (destination IP)<br>c. date/time the message was sent |

## Task 2

**Sender's Information**

**Configuration Screenshot with Explanation**

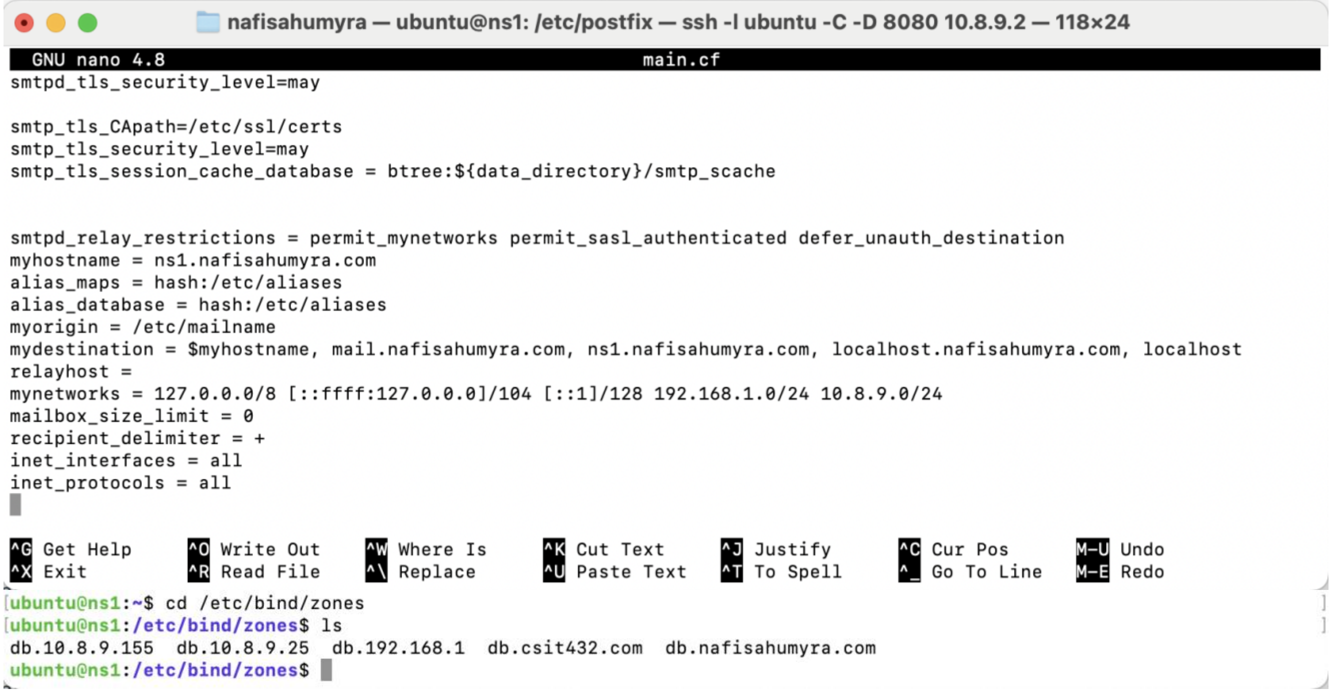
To get the internal email from my VM3 to send to leberkc@mail.csit432.com I had to make changes to configuration files which were main.cf and hosts. Initially when you try to ping the domain mail.csit432.com it will not resolve, as such you must add the IP address of the email account which in this case is 10.8.9.155 followed by the domain mail.csit432.com to the hosts file using the command sudo vi /etc/hosts. Then in the I used the command sudo vi /etc/postfix/main.cf to add the following configuration changes, first I added the domain mail.csit432.com to mydestination and in mynetworks I added the IP address of the account 10.8.9.155 after the loopback. After saving my changes I then restarted postfix using the command sudo service postfix. You would need to edit the named.conf.local to add the zones for csit432.com and 155.9.8.10.in-addr.arpa. In the zones directory, I created db.10.8.9.155 and db.csit432.com. You'd also need to go into /etc/resolv.conf to add the vm ip address on both vm1 and vm3.



nafisahumyra — ubuntu@ns1: /etc/bind — ssh -l ubuntu -C -D 8080 10.8.9...

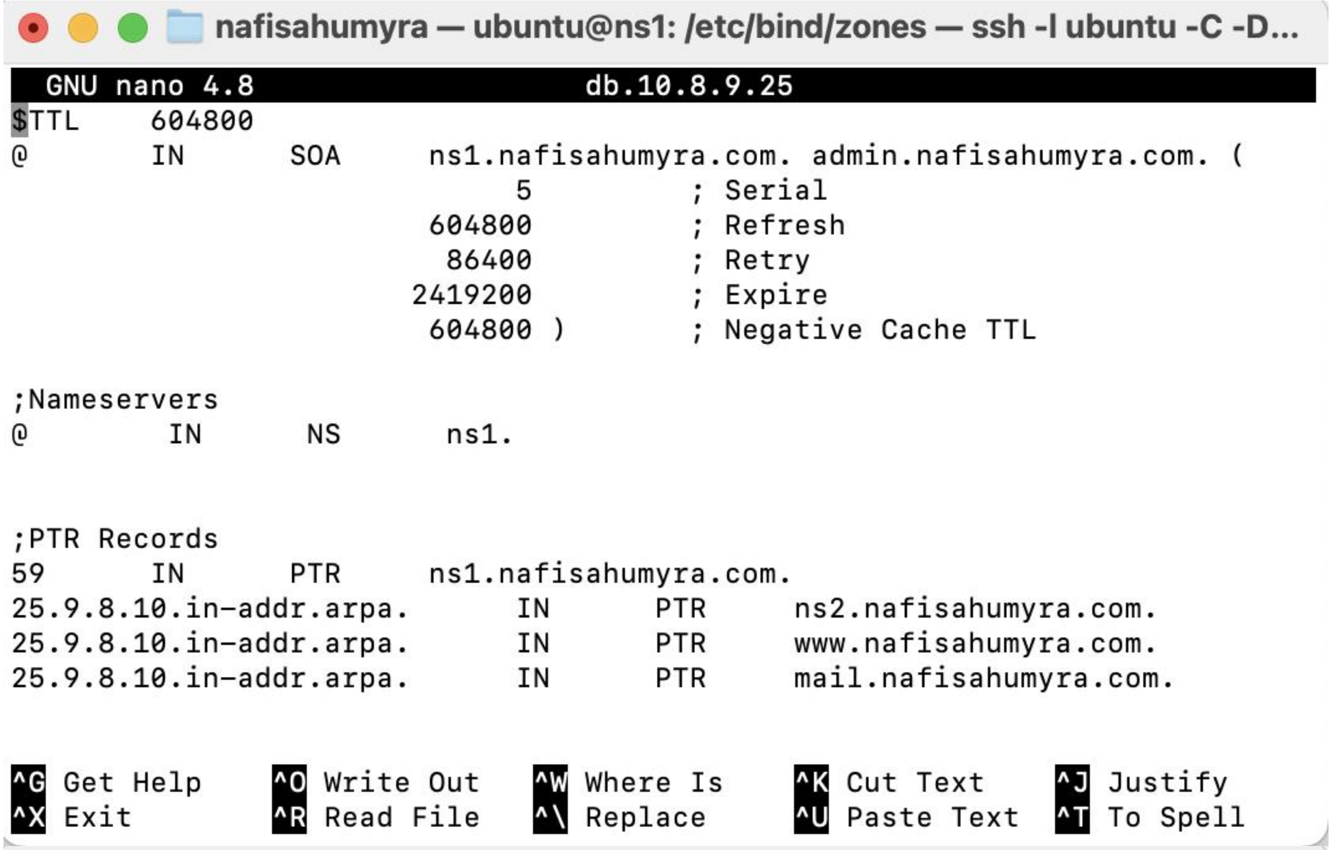
```
 GNU nano 4.8                        /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.
nameserver  192.168.1.59
#nameserver 127.0.0.53
#options edns0 trust-ad


                               [ Read 18 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line
```

nd VM2) to work after you have set up a new IP address on VM3.

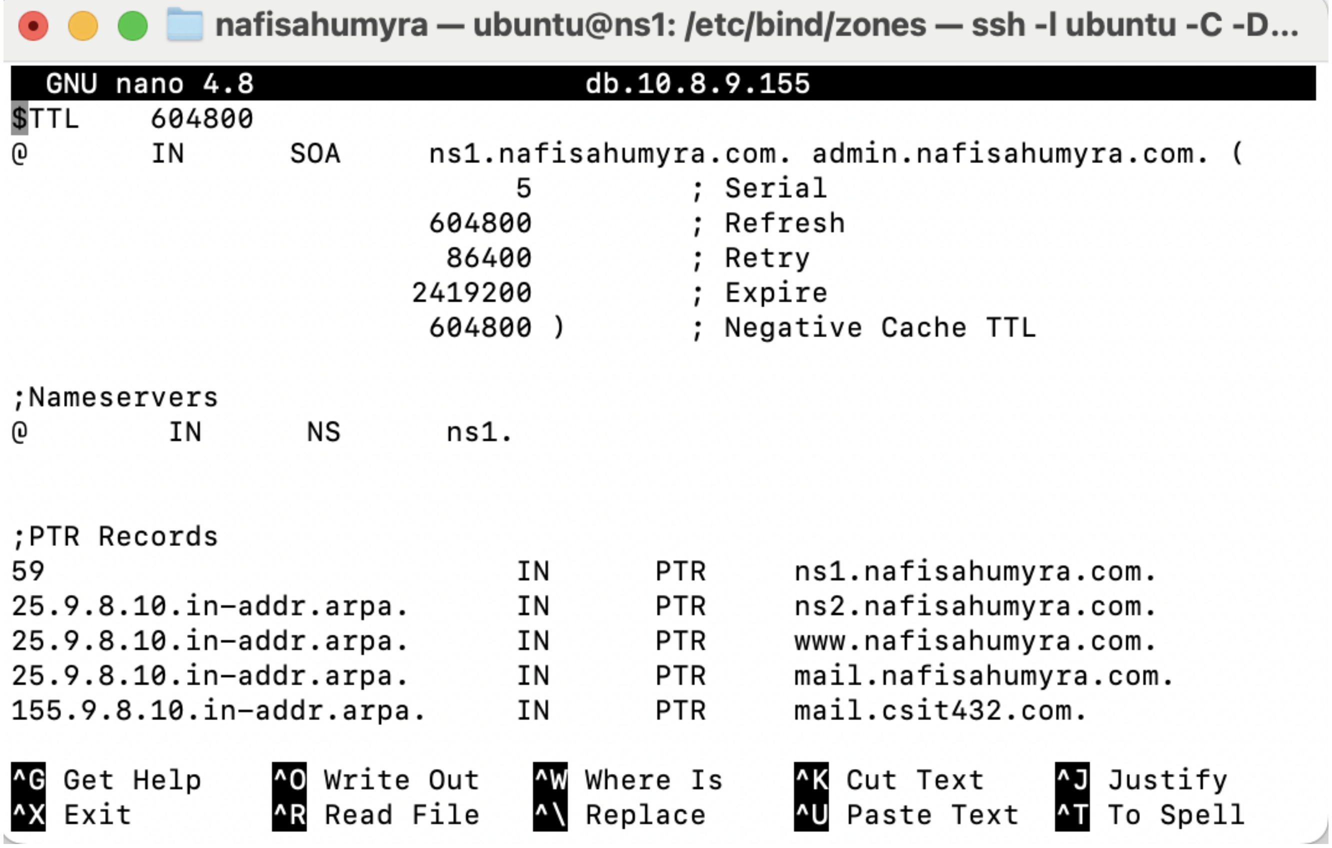


nafisahumyra — ubuntu@ns1: /etc/postfix — ssh -l ubuntu -C -D 8080 10.8.9.2 — 118×24

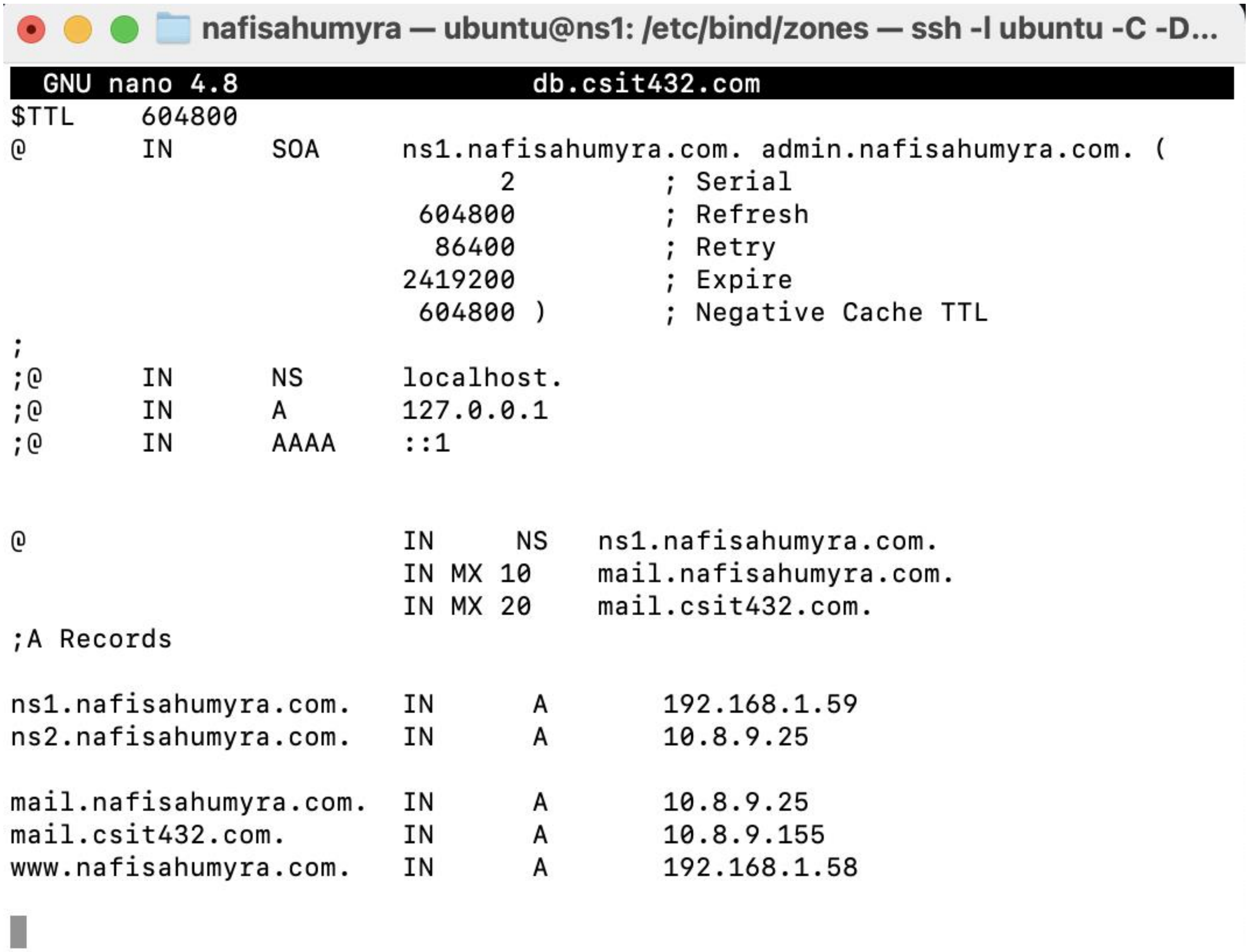
```
  GNU nano 4.8                                   main.cf
smtpd_tls_security_level=may

smtp_tls_CApath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache


smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = ns1.nafisahumyra.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, mail.nafisahumyra.com, ns1.nafisahumyra.com, localhost.nafisahumyra.com, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.1.0/24 10.8.9.0/24
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all


^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      M-U Undo
^X Exit         ^R Read File    ^\ Replace      ^U Paste Text   ^T To Spell     ^_ Go To Line   M-E Redo
ubuntu@ns1:~$ cd /etc/bind/zones
ubuntu@ns1:/etc/bind/zones$ ls
db.10.8.9.155  db.10.8.9.25  db.192.168.1  db.csit432.com  db.nafisahumyra.com
ubuntu@ns1:/etc/bind/zones$
```


nafisahumyra — ubuntu@ns1: /etc/bind/zones — ssh -l ubuntu -C -D...
GNU nano 4.8
db.10.8.9.25

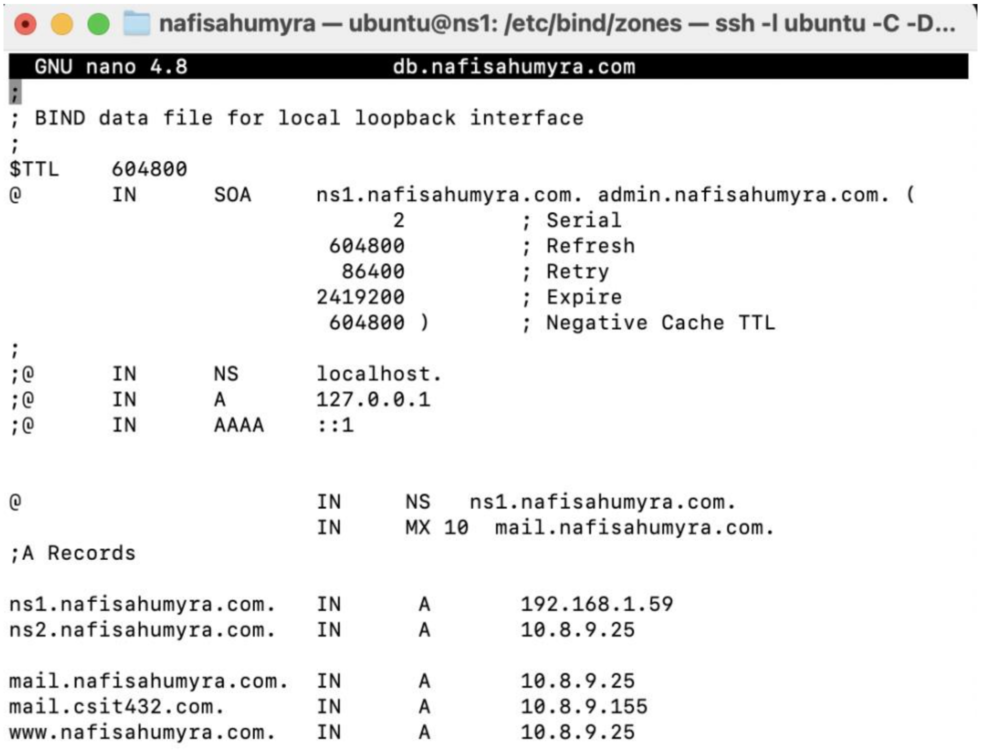
```
$TTL    604800
@       IN      SOA     ns1.nafisahumyra.com. admin.nafisahumyra.com. (
                             5         ; Serial
                        604800         ; Refresh
                         86400         ; Retry
                       2419200         ; Expire
                        604800 )       ; Negative Cache TTL

;Nameservers
@        IN      NS      ns1.


;PTR Records
59      IN      PTR     ns1.nafisahumyra.com.
25.9.8.10.in-addr.arpa.      IN      PTR     ns2.nafisahumyra.com.
25.9.8.10.in-addr.arpa.      IN      PTR     www.nafisahumyra.com.
25.9.8.10.in-addr.arpa.      IN      PTR     mail.nafisahumyra.com.
```


nafisahumyra — ubuntu@ns1: /etc/bind/zones — ssh -l ubuntu -C -D...
GNU nano 4.8
db.10.8.9.155

```
$TTL    604800
@       IN      SOA     ns1.nafisahumyra.com. admin.nafisahumyra.com. (
                             5         ; Serial
                        604800         ; Refresh
                         86400         ; Retry
                       2419200         ; Expire
                        604800 )       ; Negative Cache TTL

;Nameservers
@        IN      NS      ns1.


;PTR Records
59                           IN      PTR     ns1.nafisahumyra.com.
25.9.8.10.in-addr.arpa.      IN      PTR     ns2.nafisahumyra.com.
25.9.8.10.in-addr.arpa.      IN      PTR     www.nafisahumyra.com.
25.9.8.10.in-addr.arpa.      IN      PTR     mail.nafisahumyra.com.
155.9.8.10.in-addr.arpa.     IN      PTR     mail.csit432.com.
```

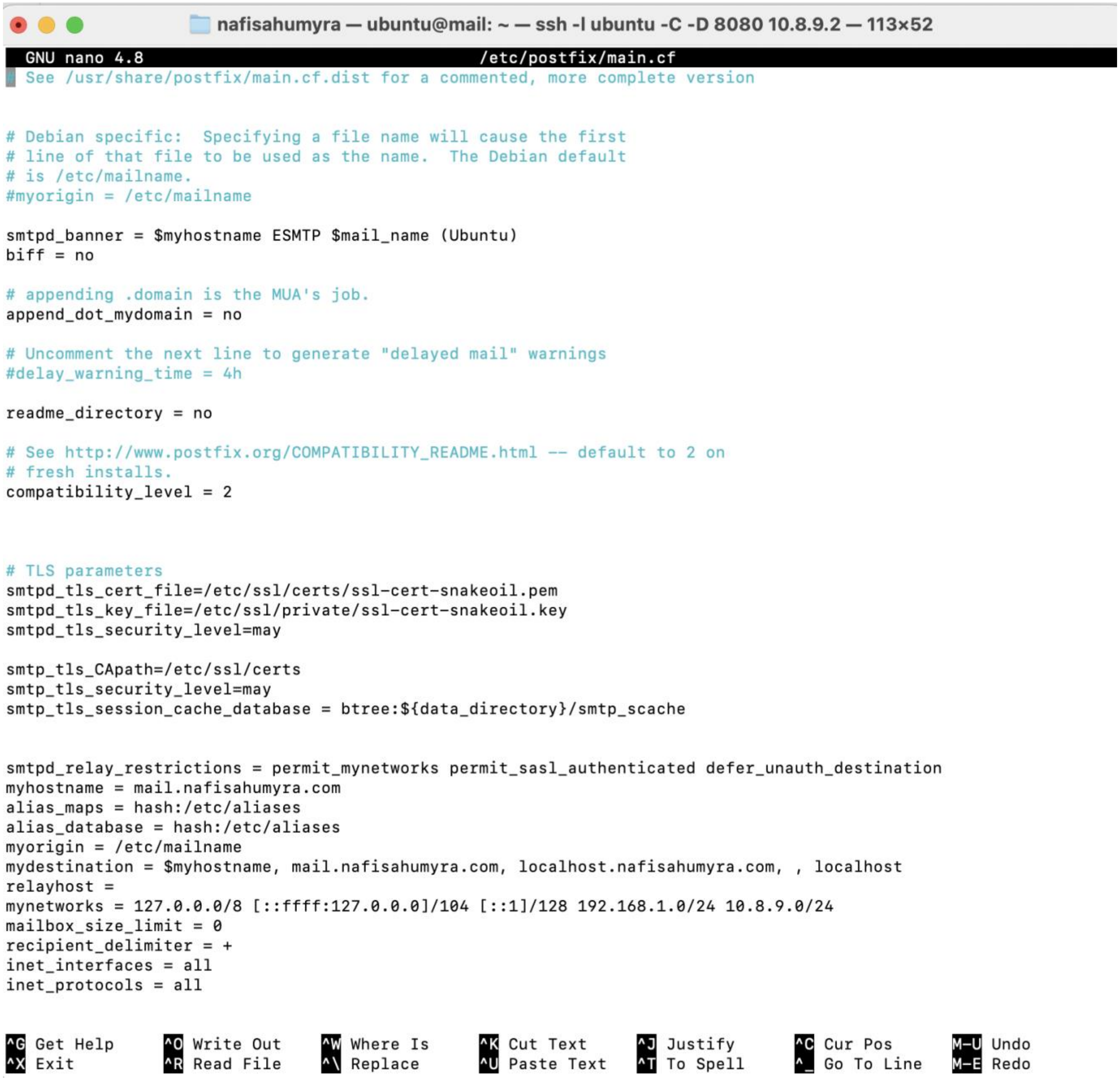

nafisahumyra — ubuntu@ns1: /etc/bind/zones — ssh -l ubuntu -C -D...

```
  GNU nano 4.8                          db.csit432.com
$TTL    604800
@       IN      SOA     ns1.nafisahumyra.com. admin.nafisahumyra.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
;@      IN      NS      localhost.
;@      IN      A       127.0.0.1
;@      IN      AAAA    ::1


@                       IN      NS   ns1.nafisahumyra.com.
                        IN MX 10     mail.nafisahumyra.com.
                        IN MX 20     mail.csit432.com.
;A Records

ns1.nafisahumyra.com.   IN      A       192.168.1.59
ns2.nafisahumyra.com.   IN      A       10.8.9.25

mail.nafisahumyra.com.  IN      A       10.8.9.25
mail.csit432.com.       IN      A       10.8.9.155
www.nafisahumyra.com.   IN      A       192.168.1.58
```


nafisahumyra — ubuntu@ns1: /etc/bind/zones — ssh -l ubuntu -C -D...

```
  GNU nano 4.8                  db.nafisahumyra.com
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.nafisahumyra.com. admin.nafisahumyra.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
;@      IN      NS      localhost.
;@      IN      A       127.0.0.1
;@      IN      AAAA    ::1


@                       IN      NS   ns1.nafisahumyra.com.
                        IN      MX 10  mail.nafisahumyra.com.
;A Records

ns1.nafisahumyra.com.   IN       A       192.168.1.59
ns2.nafisahumyra.com.   IN       A       10.8.9.25

mail.nafisahumyra.com.  IN       A       10.8.9.25
mail.csit432.com.       IN       A       10.8.9.155
www.nafisahumyra.com.   IN       A       10.8.9.25
```

Configuration to /etc/postfix/main.cf


nafisahumyra — ubuntu@mail: ~ — ssh -l ubuntu -C -D 8080 10.8.9.2 — 113×52

```
  GNU nano 4.8                                  /etc/postfix/main.cf
# See /usr/share/postfix/main.cf.dist for a commented, more complete version


# Debian specific:  Specifying a file name will cause the first
# line of that file to be used as the name.  The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

readme_directory = no

# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 2 on
# fresh installs.
compatibility_level = 2



# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtp_tls_CApath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache


smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = mail.nafisahumyra.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, mail.nafisahumyra.com, localhost.nafisahumyra.com, , localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.1.0/24 10.8.9.0/24
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all


^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

**Table 2:**

| Source IP | Destination IP | Date/Time Message Sent |
|---|---|---|
| 10.8.9.25 | 10.8.9.155 | 10/15/23 3:43PM |

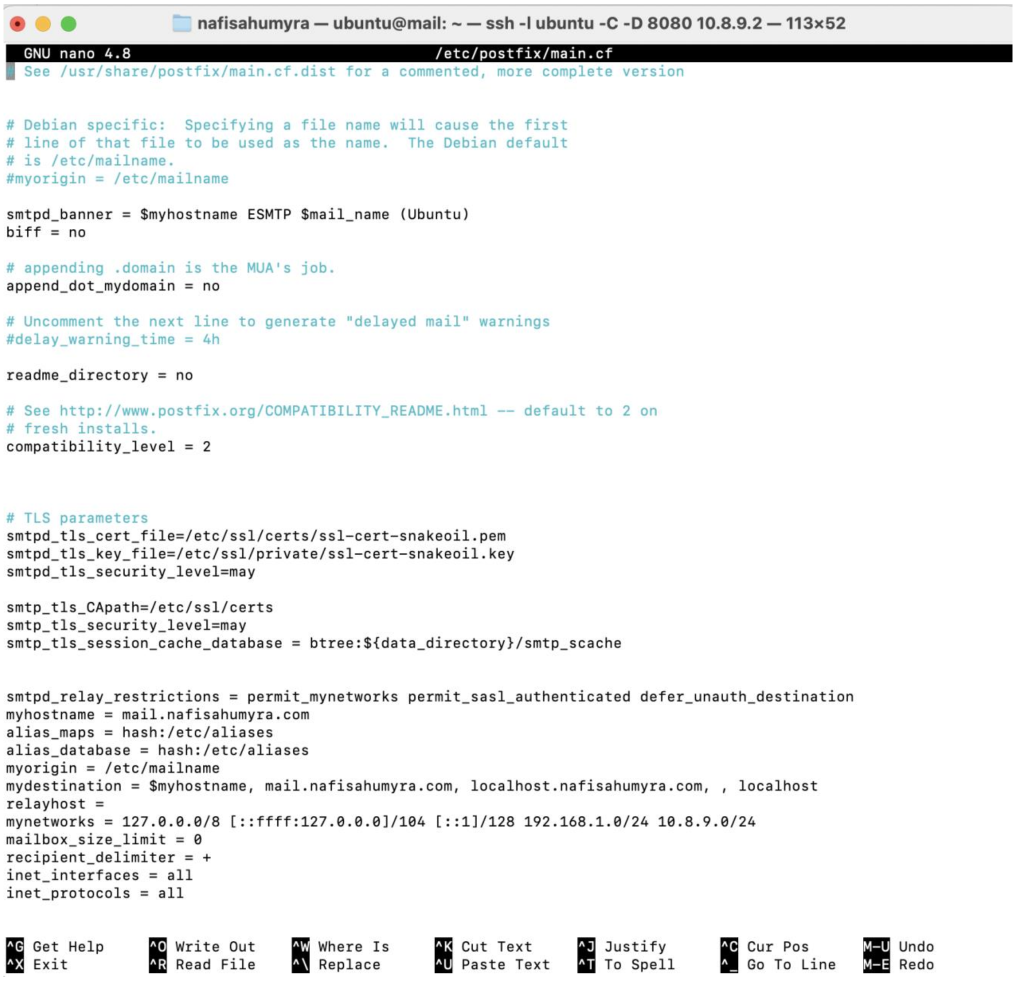
## Task 3: External email using Squirrelmail

| Task 3 | What's needed? | What to Submit? |
|---|---|---|
| Send an email to an external email account using Sqjuirrelmail on your VM1 web browser. | 1. External email address use your netid@montclair.edu | 1. Explain what you did to get this to work. Provide **screenshots** for any configuration changes required with explanations<br>a. Open the email message so the contents are visible. and the IP address of your browser should be visible in the screenshot |

### Configuration Screenshot with Explanation

You'll need to make configuration changes to /etc/postfix/main.cf. Once I saved my configuration changes, I restarted postfix using the command sudo service postfix restart

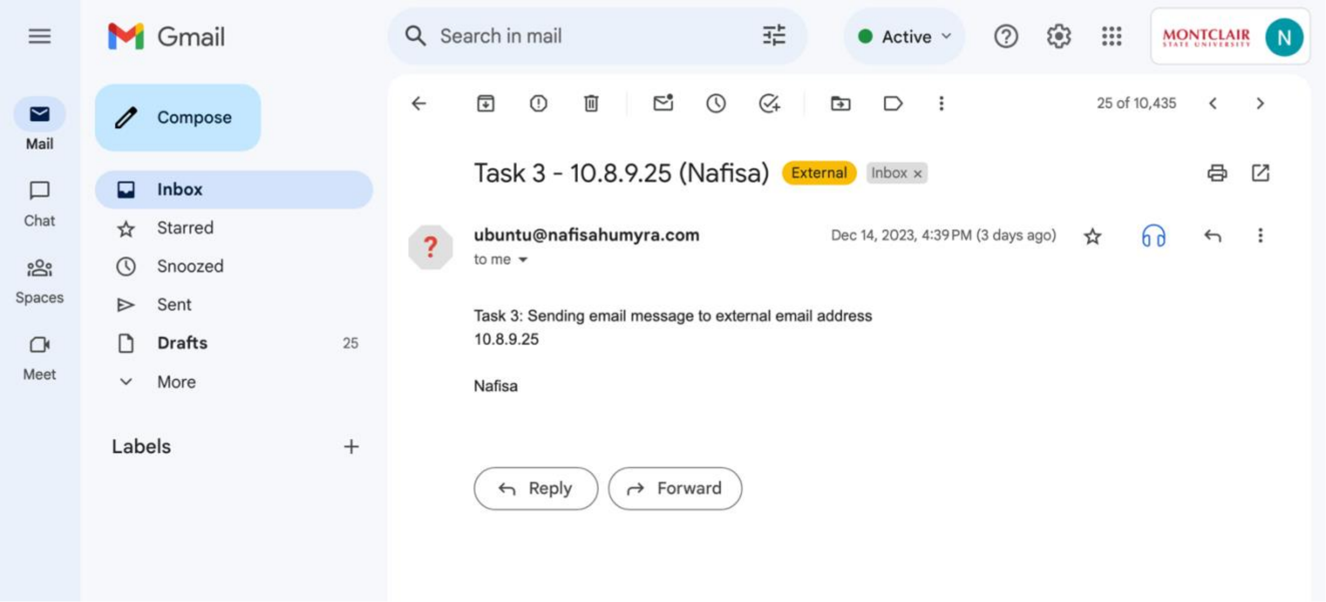
Configuration to /etc/postfix/main.cf



nafisahumyra — ubuntu@mail: ~ — ssh -l ubuntu -C -D 8080 10.8.9.2 — 113×52

```
  GNU nano 4.8                                        /etc/postfix/main.cf
  See /usr/share/postfix/main.cf.dist for a commented, more complete version


# Debian specific:  Specifying a file name will cause the first
# line of that file to be used as the name.  The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

readme_directory = no

# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 2 on
# fresh installs.
compatibility_level = 2



# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtp_tls_CApath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache


smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = mail.nafisahumyra.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, mail.nafisahumyra.com, localhost.nafisahumyra.com, , localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.1.0/24 10.8.9.0/24
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all


^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

Email message opened in Gmail:



Task 3 - 10.8.9.25 (Nafisa)

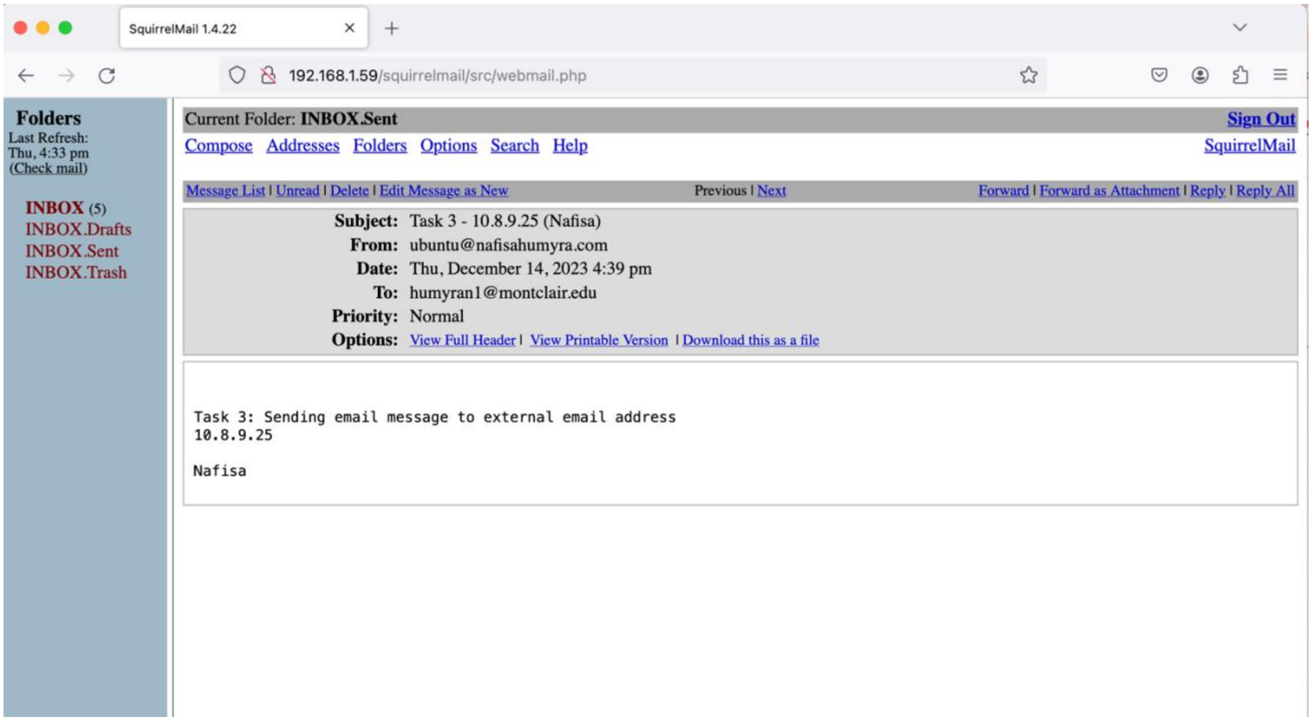
ubuntu@nafisahumyra.com
to me

Dec 14, 2023, 4:39 PM (3 days ago)

Task 3: Sending email message to external email address
10.8.9.25

Nafisa

Email message inside sent inbox folder with IP VM1 address in browser:


SquirrelMail 1.4.22
192.168.1.59/squirrelmail/src/webmail.php
Folders
Last Refresh:
Thu, 4:33 pm
(Check mail)
INBOX (5)
INBOX.Drafts
INBOX.Sent
INBOX.Trash
Sign Out
Compose Addresses Folders Options Search Help
SquirrelMail
Message List | Unread | Delete | Edit Message as New
Previous | Next
Forward | Forward as Attachment | Reply | Reply All

Current Folder: INBOX.Sent

**Subject:** Task 3 - 10.8.9.25 (Nafisa)
**From:** ubuntu@nafisahumyra.com
**Date:** Thu, December 14, 2023 4:39 pm
**To:** humyran1@montclair.edu
**Priority:** Normal
**Options:** View Full Header | View Printable Version | Download this as a file

```
Task 3: Sending email message to external email address
10.8.9.25

Nafisa
```

**Table 3:**

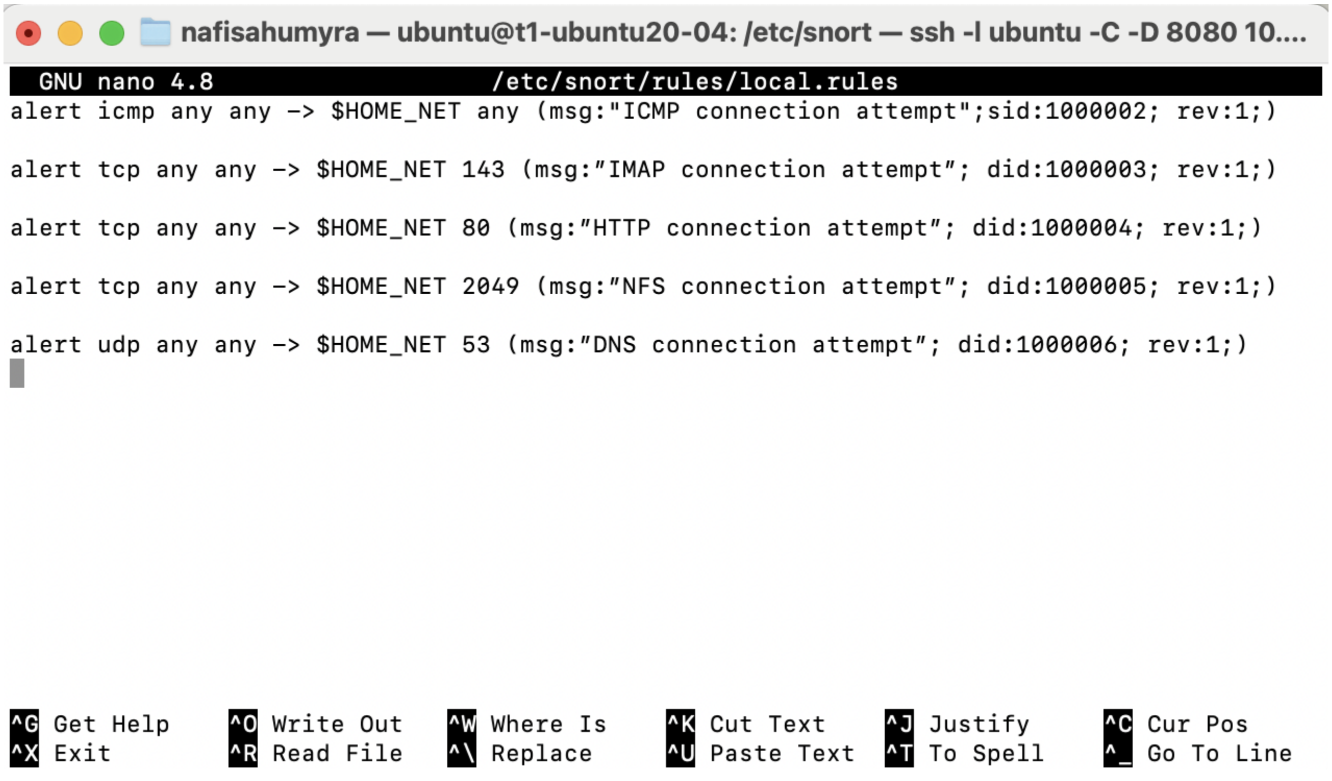
| Source IP | Destination IP | Date/Time Message Sent |
|---|---|---|
| 192.168.1.59 | 192.168.1.1 | 12/14/23 1:22PM |

**Task 4: Snort**

| Task 4 | What's needed? | What to Submit? |
|---|---|---|
| Configure rules in Snort to:<br>2. Detect SMTP, IMAP, HTTP, NFS, and DNS traffic and save the output to a file | Snort installed and configured on VM2. Routes configured from VM1→VM2→VM3 | 2. Screenshot of your snort rules<br>3. File that contains captured data<br>4. Table that identifies:<br>a. IP address that used SMTP, IMAP, HTTP, NFS, and DNS along with the date and time |

## Task 4

**Screenshot of Snort Rules**


nafisahumyra — ubuntu@t1-ubuntu20-04: /etc/snort — ssh -l ubuntu -C -D 8080 10....

```
  GNU nano 4.8                     /etc/snort/rules/local.rules
alert icmp any any -> $HOME_NET any (msg:"ICMP connection attempt";sid:1000002; rev:1;)

alert tcp any any -> $HOME_NET 143 (msg:”IMAP connection attempt”; did:1000003; rev:1;)

alert tcp any any -> $HOME_NET 80 (msg:”HTTP connection attempt”; did:1000004; rev:1;)

alert tcp any any -> $HOME_NET 2049 (msg:”NFS connection attempt”; did:1000005; rev:1;)

alert udp any any -> $HOME_NET 53 (msg:”DNS connection attempt”; did:1000006; rev:1;)
```

**Table 4**

| VM1 IP Address | Protocol | Date and Time Protocol was used? |
|---|---|---|
| **192.168.1.59** | **SMTP** | **12/16/23 5:32 PM** |

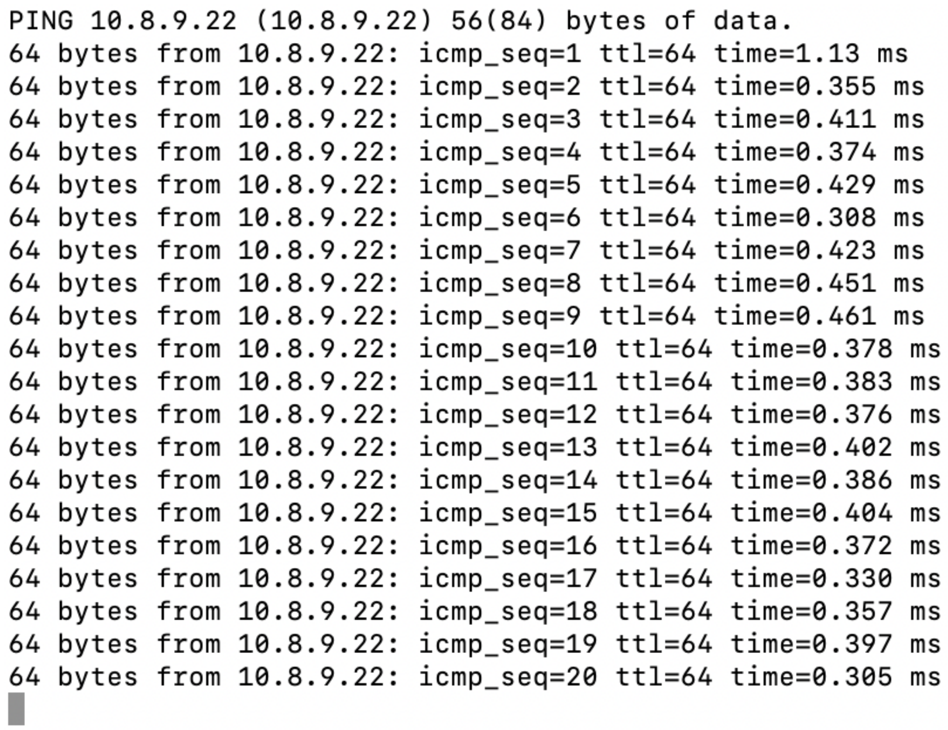
| | | |
|---|---|---|
| **192.168.1.59** | **IMAP** | **12/16/23 5:32 PM** |
| **192.168.1.59** | **HTTP** | **12/16/23 5:33 PM** |
| **192.168.1.59** | **NFS** | **12/16/23 5:34 PM** |
| **192.168.1.59** | **DNS** | **12/16/23 5:34 PM** |

## Task 5: Routing

| Task 5 | What's needed? | What to Submit? |
|---|---|---|
| 1. Ping any VM3 IP address 10.8.9.xx from your VM1<br>2. Completing this task may complicate collecting snort data for Task 4. Complete task 4 before completing Task 5 | **Routes configured from VM1→VM2→VM3**<br>You will need to partner with other students for this task | 5. Screenshot of ping output on VM1 showing ping reply from any VM3 10.8.9.xxx IP address |

### Task 5

**Configuration Screenshot with Explanation**



```
PING 10.8.9.22 (10.8.9.22) 56(84) bytes of data.
64 bytes from 10.8.9.22: icmp_seq=1 ttl=64 time=1.13 ms
64 bytes from 10.8.9.22: icmp_seq=2 ttl=64 time=0.355 ms
64 bytes from 10.8.9.22: icmp_seq=3 ttl=64 time=0.411 ms
64 bytes from 10.8.9.22: icmp_seq=4 ttl=64 time=0.374 ms
64 bytes from 10.8.9.22: icmp_seq=5 ttl=64 time=0.429 ms
64 bytes from 10.8.9.22: icmp_seq=6 ttl=64 time=0.308 ms
64 bytes from 10.8.9.22: icmp_seq=7 ttl=64 time=0.423 ms
64 bytes from 10.8.9.22: icmp_seq=8 ttl=64 time=0.451 ms
64 bytes from 10.8.9.22: icmp_seq=9 ttl=64 time=0.461 ms
64 bytes from 10.8.9.22: icmp_seq=10 ttl=64 time=0.378 ms
64 bytes from 10.8.9.22: icmp_seq=11 ttl=64 time=0.383 ms
64 bytes from 10.8.9.22: icmp_seq=12 ttl=64 time=0.376 ms
64 bytes from 10.8.9.22: icmp_seq=13 ttl=64 time=0.402 ms
64 bytes from 10.8.9.22: icmp_seq=14 ttl=64 time=0.386 ms
64 bytes from 10.8.9.22: icmp_seq=15 ttl=64 time=0.404 ms
64 bytes from 10.8.9.22: icmp_seq=16 ttl=64 time=0.372 ms
64 bytes from 10.8.9.22: icmp_seq=17 ttl=64 time=0.330 ms
64 bytes from 10.8.9.22: icmp_seq=18 ttl=64 time=0.357 ms
64 bytes from 10.8.9.22: icmp_seq=19 ttl=64 time=0.397 ms
64 bytes from 10.8.9.22: icmp_seq=20 ttl=64 time=0.305 ms
```