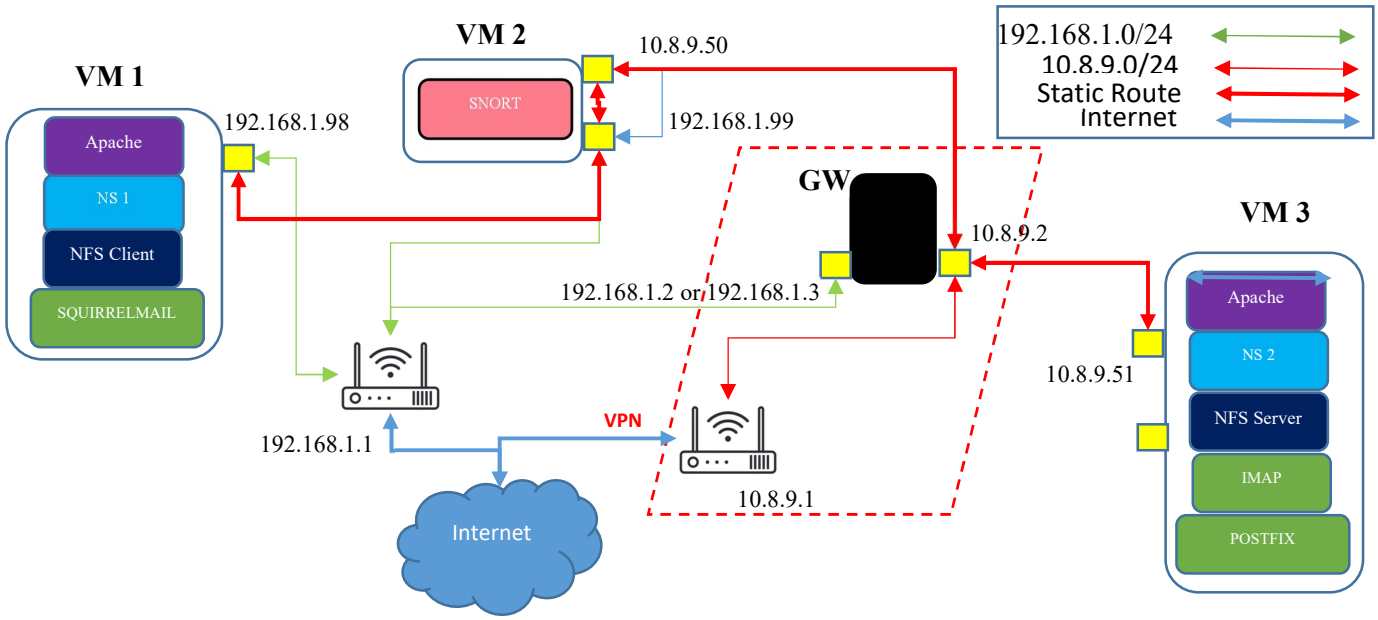
CSIT 432-01
Fall 2023
Final Project
Name: Puja Shah

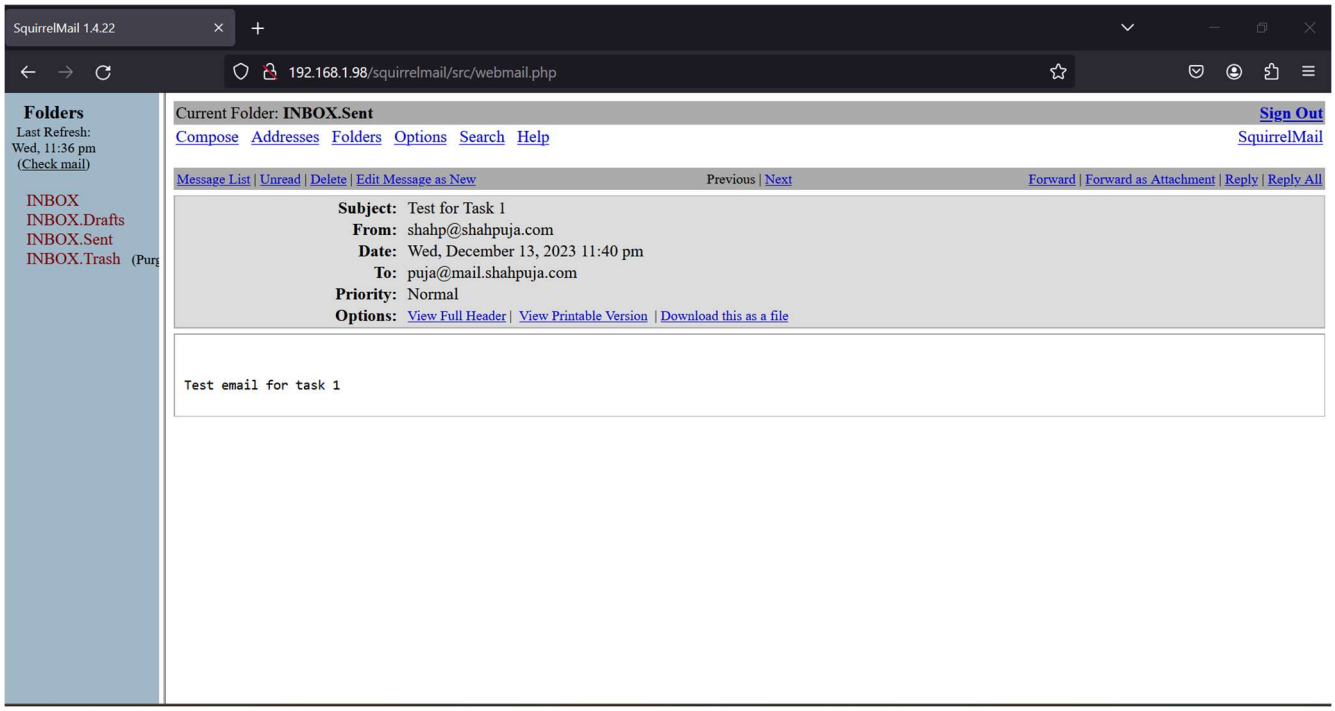
Table of Contents

Overview of Virtual Computing Infrastructure



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

Squirrelmail sent inbox:



Mail received by the other user on VM3:

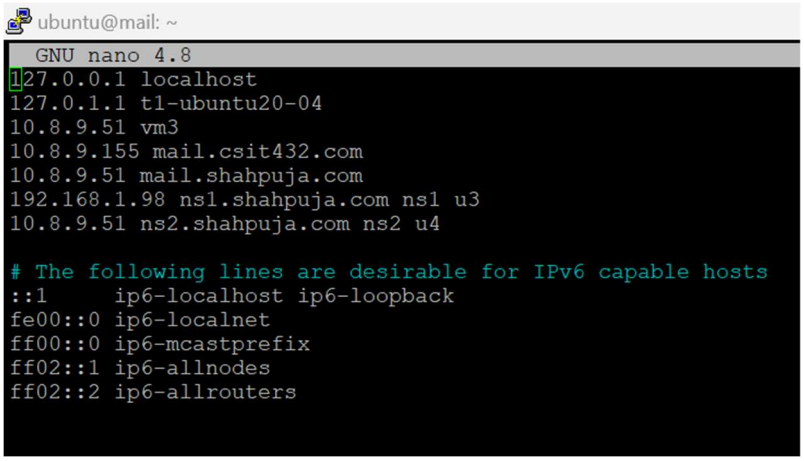
```
puja@mail: /home/ubuntu
ubuntu@mail:~$ su puja
Password:
puja@mail:/home/ubuntu$ mail
"/var/mail/puja": 9 messages 9 new
>N   1 Ubuntu              Sun Nov 19 18:57  14/409   testing SMTP server
 N   2 Ubuntu              Sun Nov 19 19:04  13/403   Testing email
 N   3 Ubuntu              Sun Nov 19 21:27  13/390   Testing
 N   4 Ubuntu              Mon Dec 11 17:55  13/351
 N   5 Mail Delivery Syst Tue Dec 12 12:46  73/2271  Undelivered Mail Returned to Sender
 N   6 Mail Delivery Syst Tue Dec 12 13:42  72/2321  Undelivered Mail Returned to Sender
 N   7 shahp@mail         Wed Dec 13 18:14  13/372   1
 N   8 shahp@shahpuja.com Wed Dec 13 23:37  25/920   Test for Task 1
 N   9 shahp@shahpuja.com Wed Dec 13 23:40  25/937   Test for Task 1
? 9
Return-Path: <shahp@shahpuja.com>
X-Original-To: puja@mail.shahpuja.com
Delivered-To: puja@mail.shahpuja.com
Received: from ns1.shahpuja.com (ns1.shahpuja.com [192.168.1.98])
        by mail.shahpuja.com (Postfix) with ESMTPS id B516243B59
        for <puja@mail.shahpuja.com>; Wed, 13 Dec 2023 23:40:59 -0500 (EST)
Received: by ns1.shahpuja.com (Postfix, from userid 33)
        id A64B4423D8; Wed, 13 Dec 2023 23:40:59 -0500 (EST)
Received: from 192.168.1.2
        (SquirrelMail authenticated user shahp)
        by 192.168.1.98 with HTTP;
        Wed, 13 Dec 2023 23:40:59 -0500
Message-ID: <bcc97c4c77634066070c77d35722e956.squirrel@192.168.1.98>
Date: Wed, 13 Dec 2023 23:40:59 -0500
Subject: Test for Task 1
From: shahp@shahpuja.com
To: puja@mail.shahpuja.com
User-Agent: SquirrelMail/1.4.22
MIME-Version: 1.0
Content-Type: text/plain;charset=iso-8859-1
Content-Transfer-Encoding: 8bit
X-Priority: 3 (Normal)
Importance: Normal

Test email for task 1
?
```

Source IP	Destination IP	Date/Time Message Sent
192.168.1.98	10.8.9.51	13 Dec 2023 23:40:59

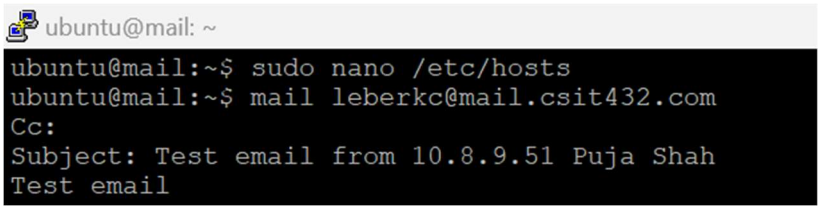
Task 2: Internal email from your VM3 using the mail command to leberkc@csit432.com

csit432.com = 10.8.9.155

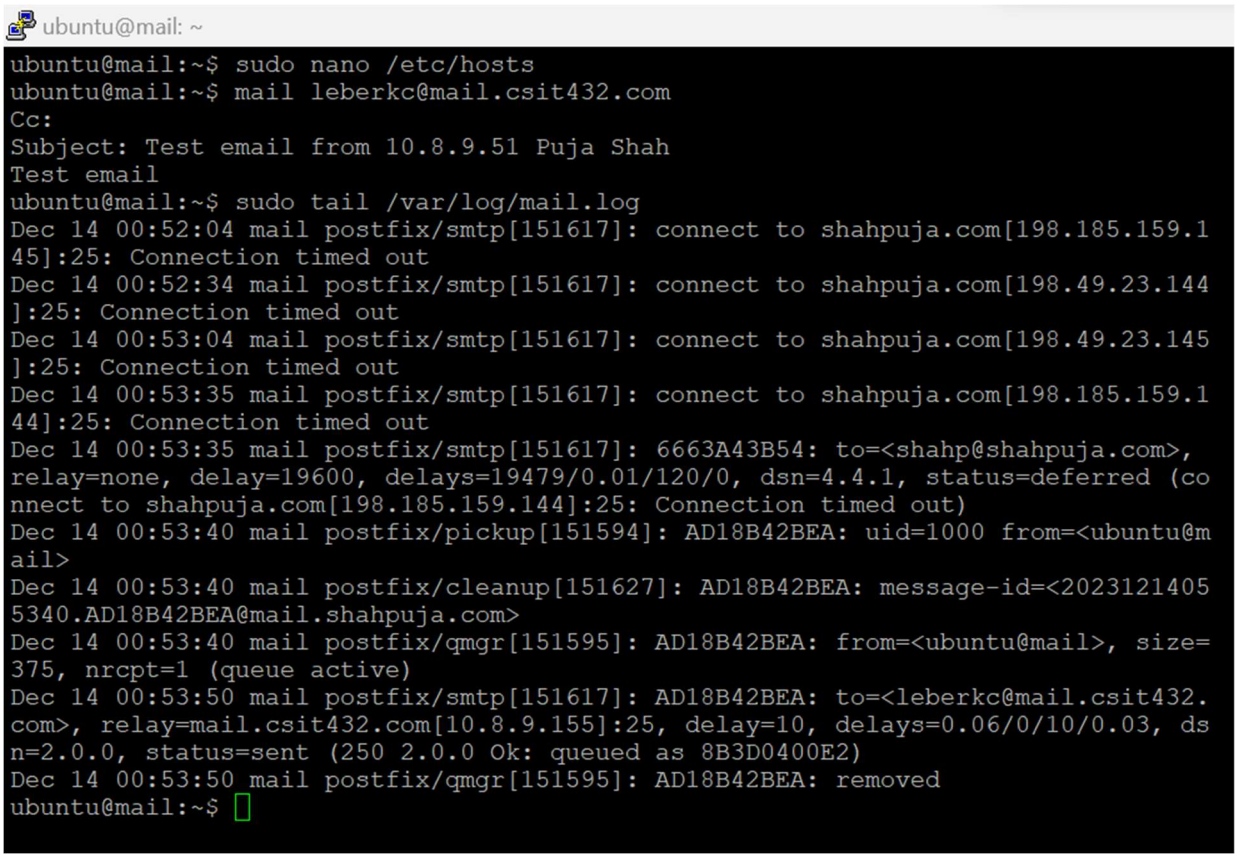
Added 10.8.9.155 mail.csit432.com in sudo nano /etc/hosts file on VM3.



Composed email using 'mail' command as ubuntu user on VM3 and pressed crtl+D to send email on leberkc@mail.csit432.com



Checked log file to see the email status using sudo tail /var/log/mail.log



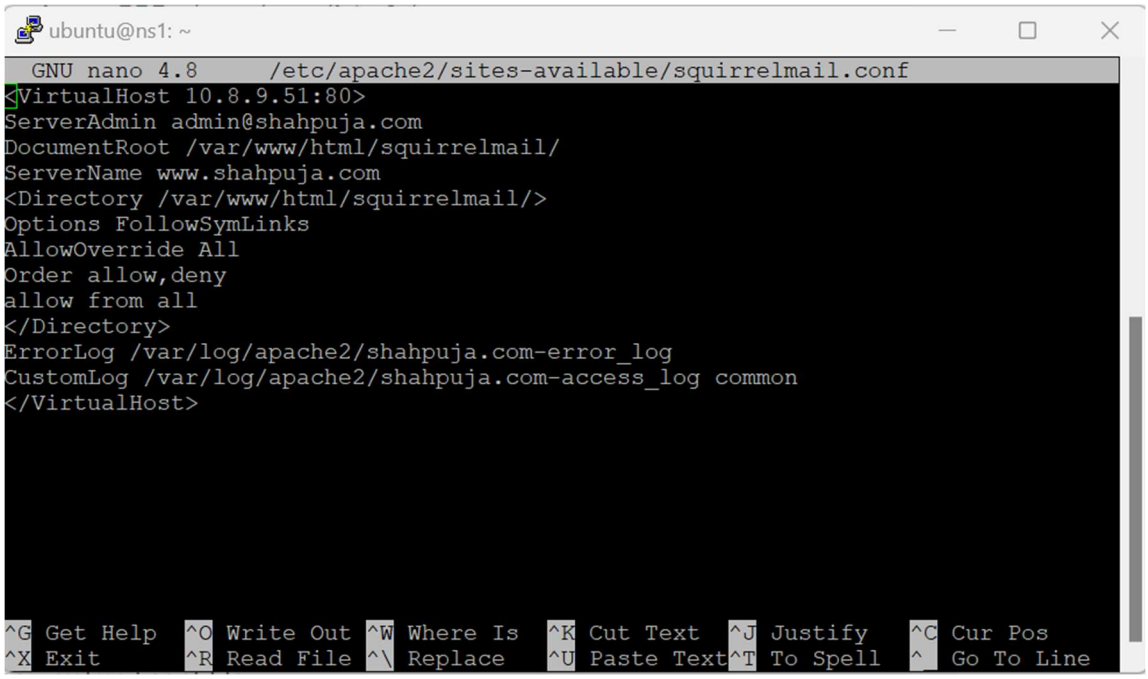
Log entries shows successful email delivery:

Dec 14 00:53:50 mail postfix/smtp[151617]: AD18B42BEA: to=<leberkc@mail.csit432.com>, relay=mail.csit432.com[10.8.9.155]:25, delay=10, delays=0.06/0/10/0.03, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 8B3D0400E2)

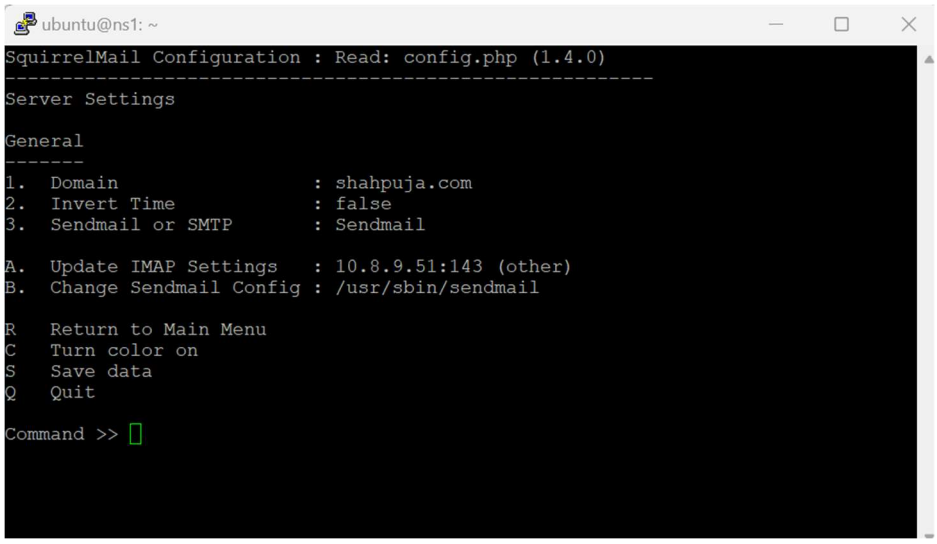
Source IP	Destination IP	Date/Time Message Sent
10.8.9.51	10.8.9.155	14 Dec 2023 00:53:50

Task 3: External email using Squirrelmail

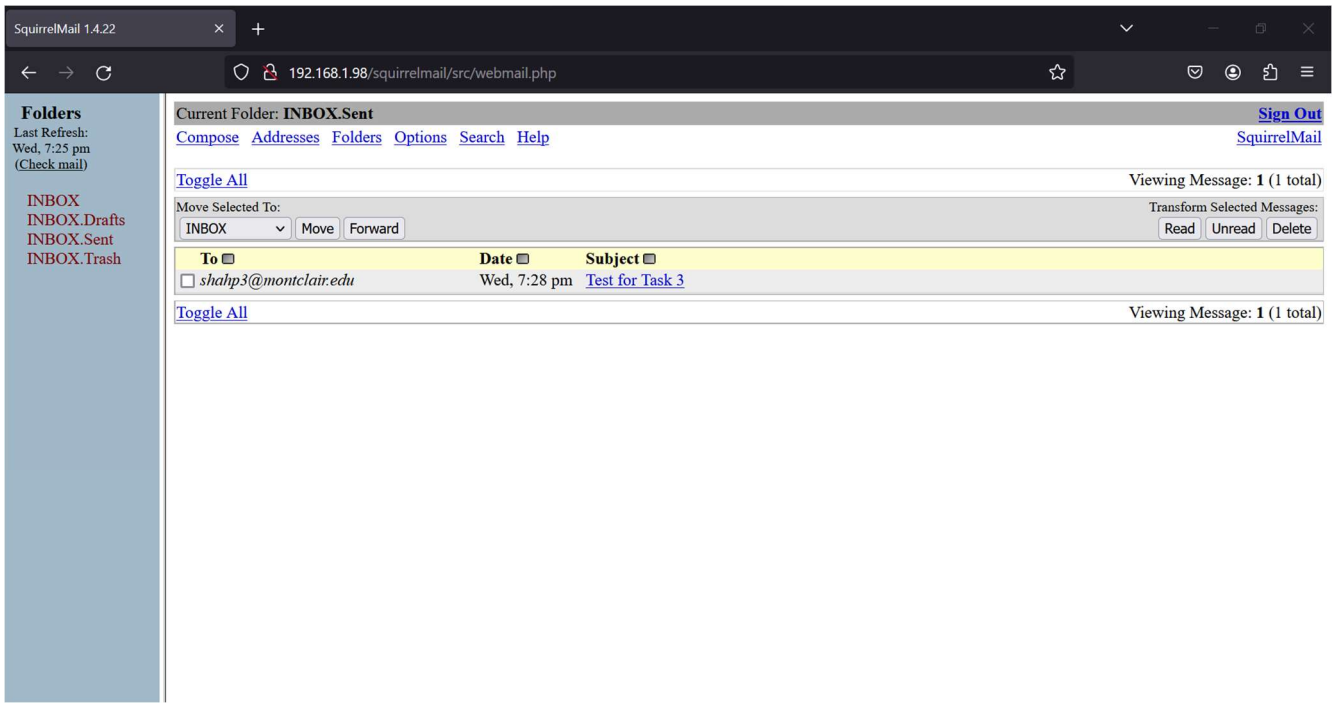
On VM1 sudo nano /etc/apache2/sites-available/squirrelmail.conf file changed virtual host IP to VM3 Secondary IP Address.

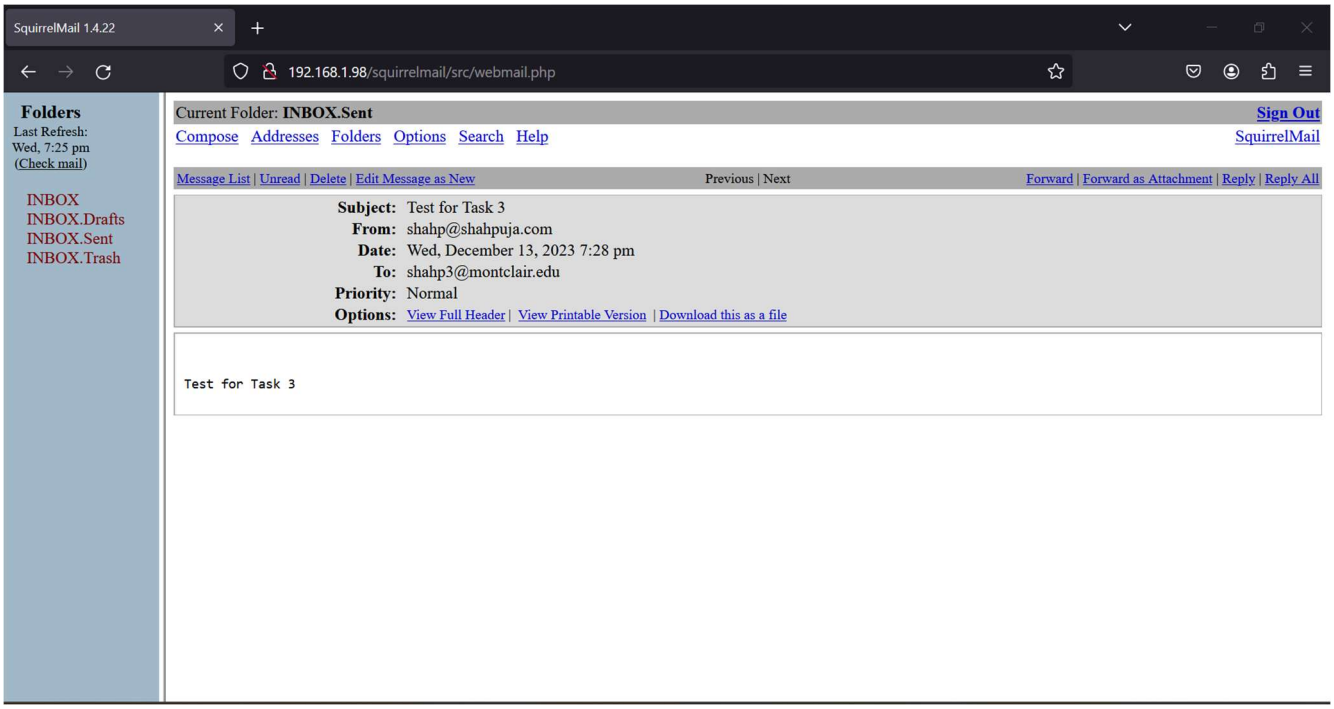


On VM1 sudo perl /var/www/html/squirrelmail/config/conf.pl file, server setting main menu no.2 changed to ‘Sendmail’ from SMTP.

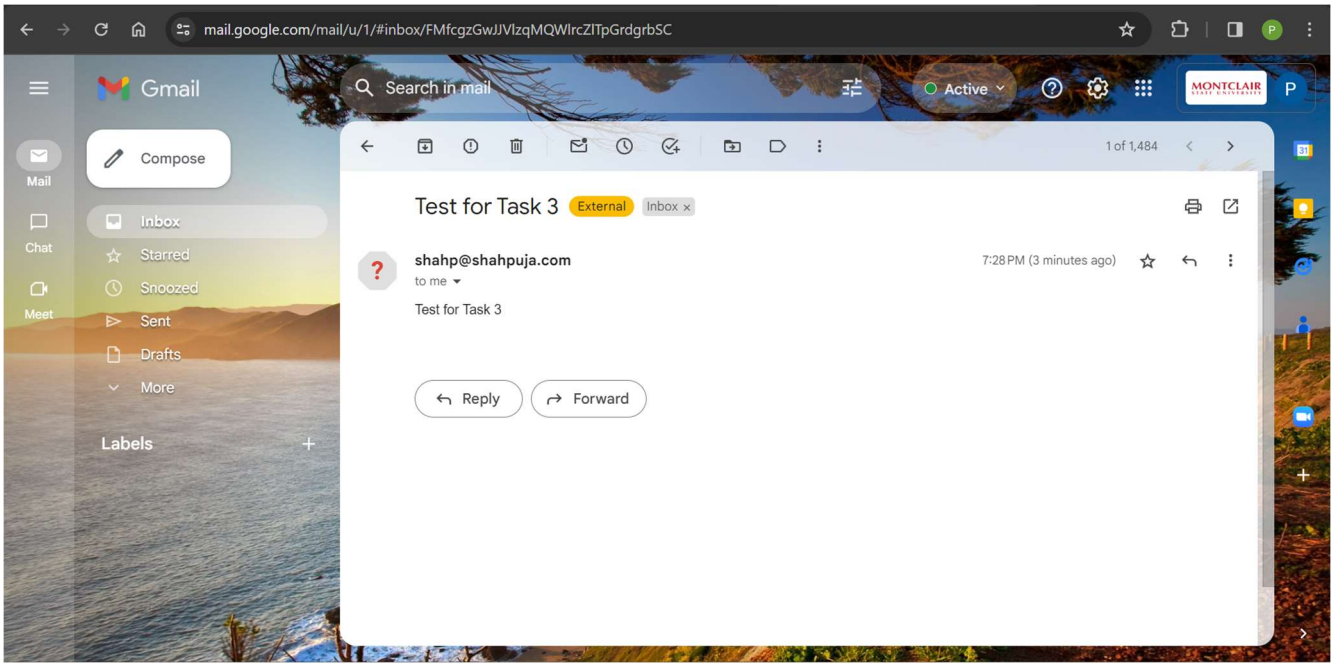


Squirrelmail sent inbox:





Email received to Montclair inbox:

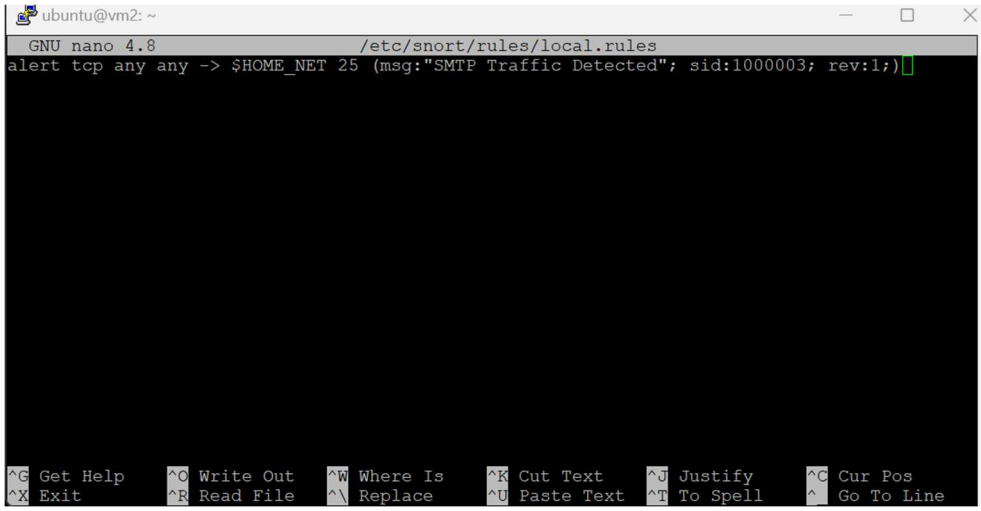


Source IP	Destination IP	Date/Time Message Sent
192.168.1.98	130.68.124.243	13 Dec 2023 19:28:00

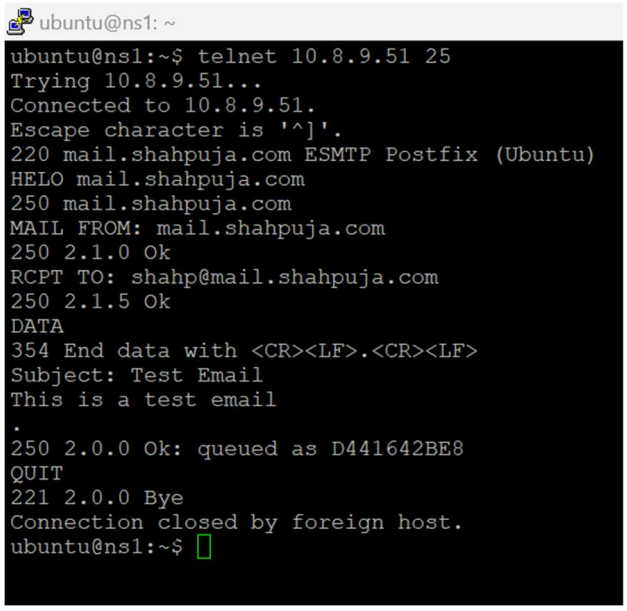
Task 4: Snort

SMTP:

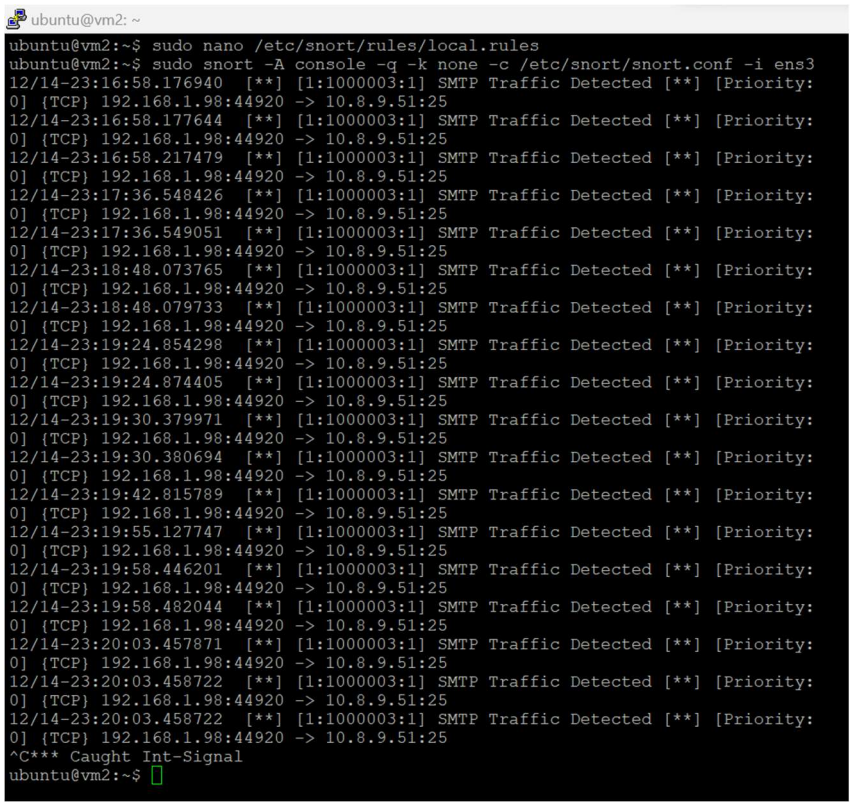
Added SMTP detection rule in sudo nano /etc/snort/rules/local.rules. This rule alerts on any TCP traffic going from any source to port 25 (SMTP).



Used ‘telnet’ to simulate an SMTP connection to VM3.

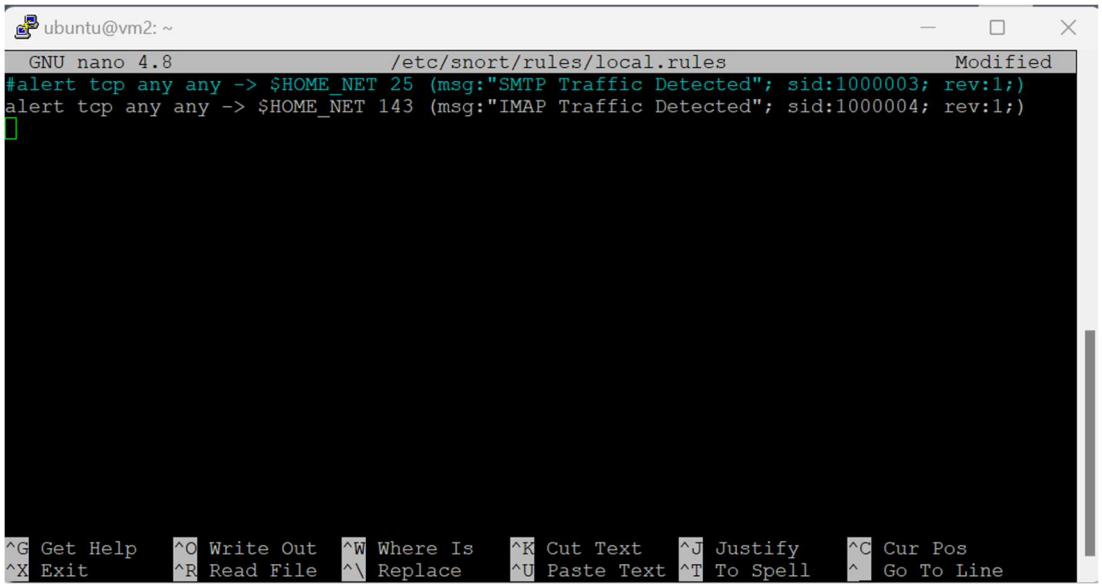


Demonstrates that snort on VM2 is capturing SMTP traffic generated by the simulated SMTP session from VM1 to VM3.

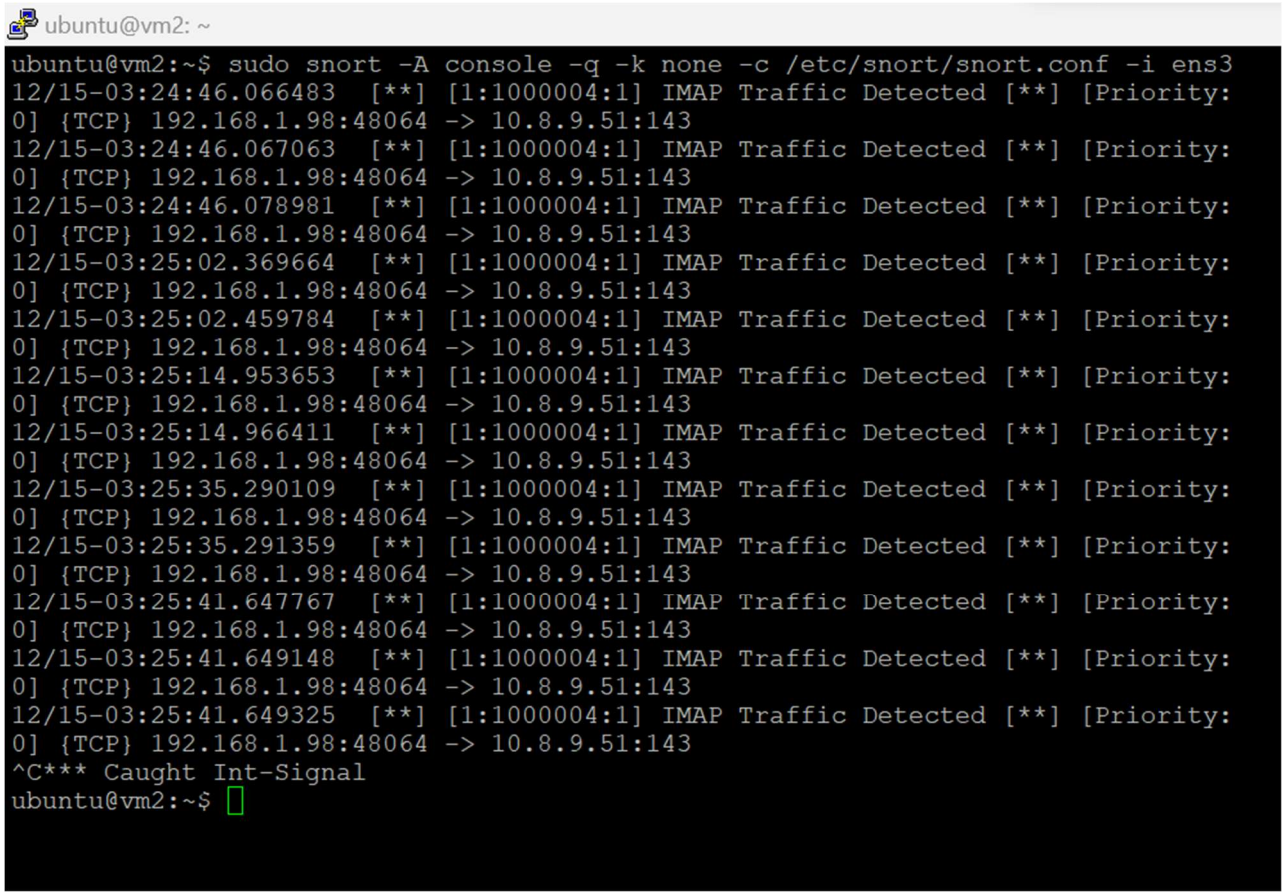


IMAP:

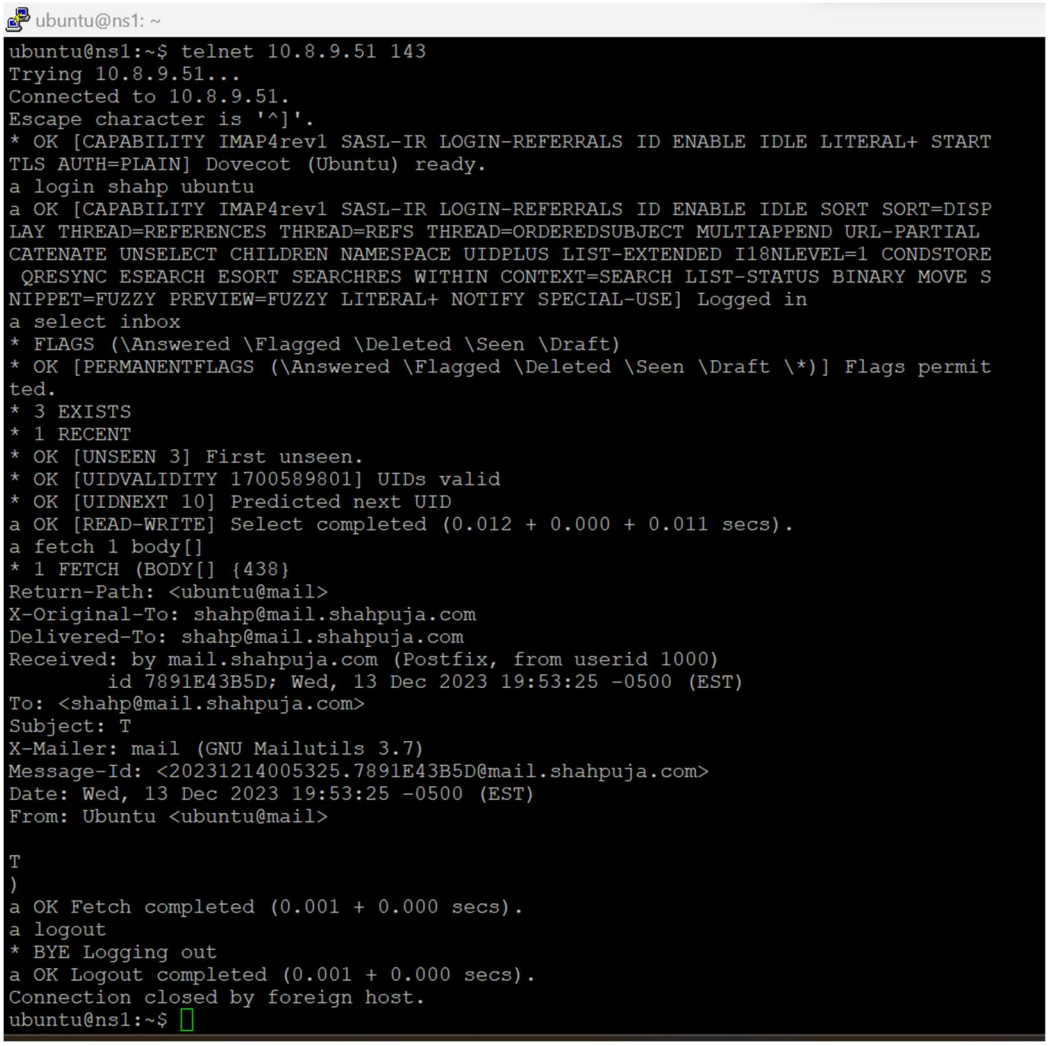
Added IMAP detection rule in /etc/snort/rules/local.rules. This rule alerts on TCP traffic going from any source to port 143 (IMAP).



Demonstrates that snort on VM2 is capturing IMAP traffic generated by the simulated IMAP session from VM1 to VM3.

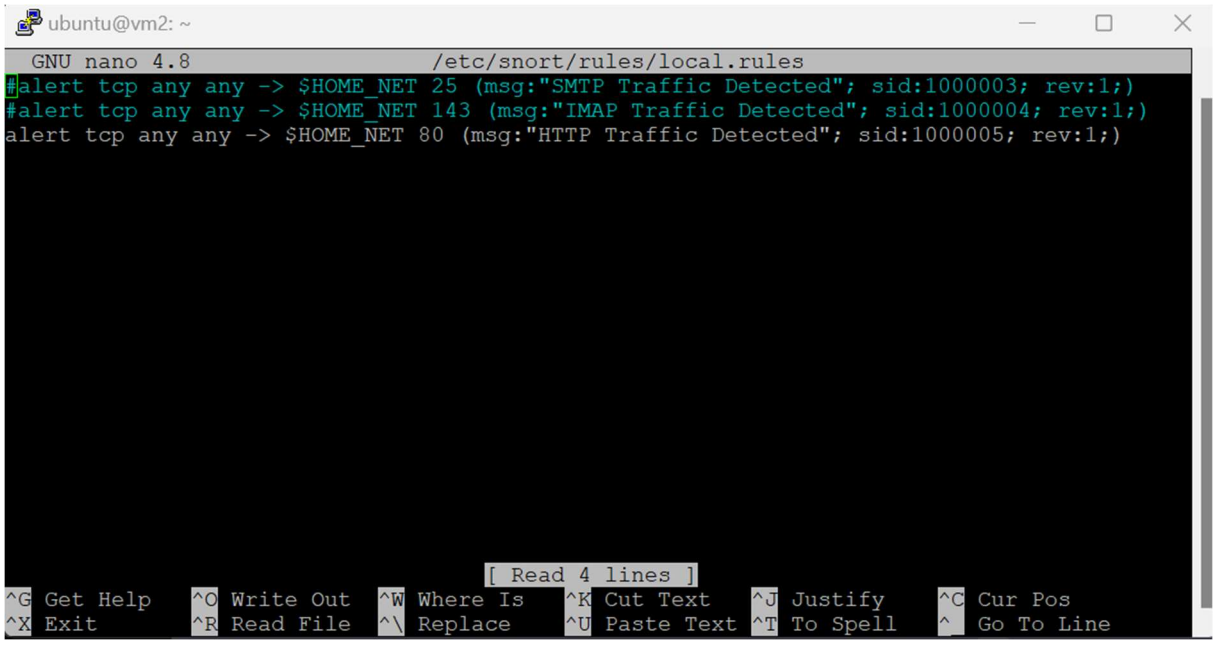


Used ‘telnet’ (VM1) to simulate an IMAP connection to VM3.

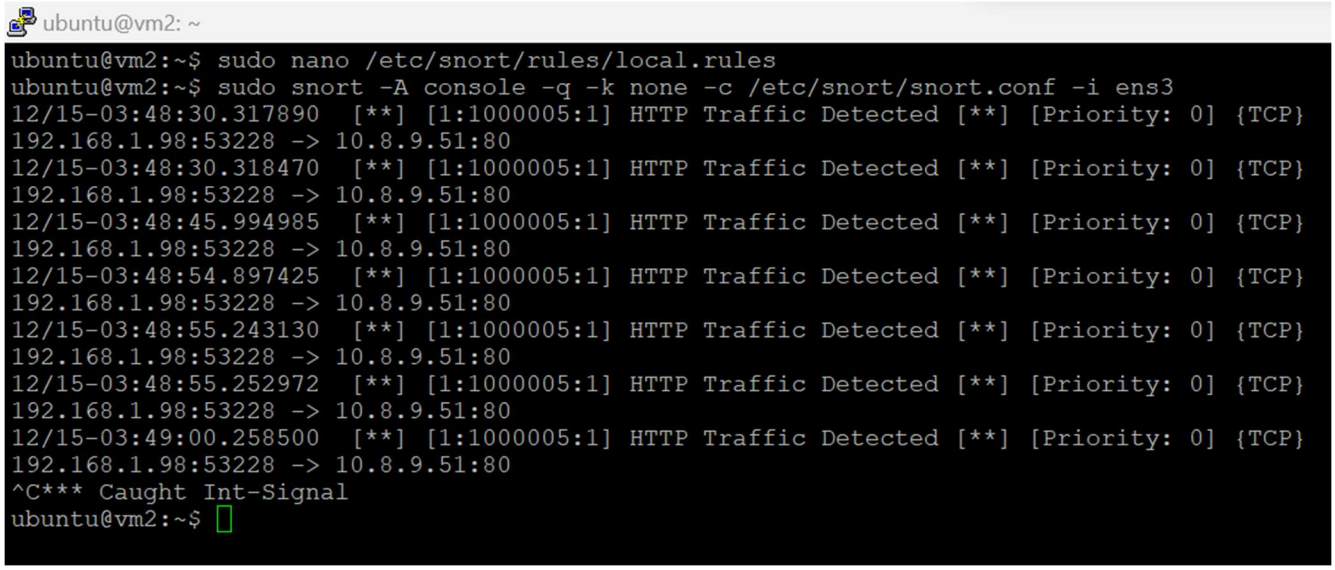


HTTP:

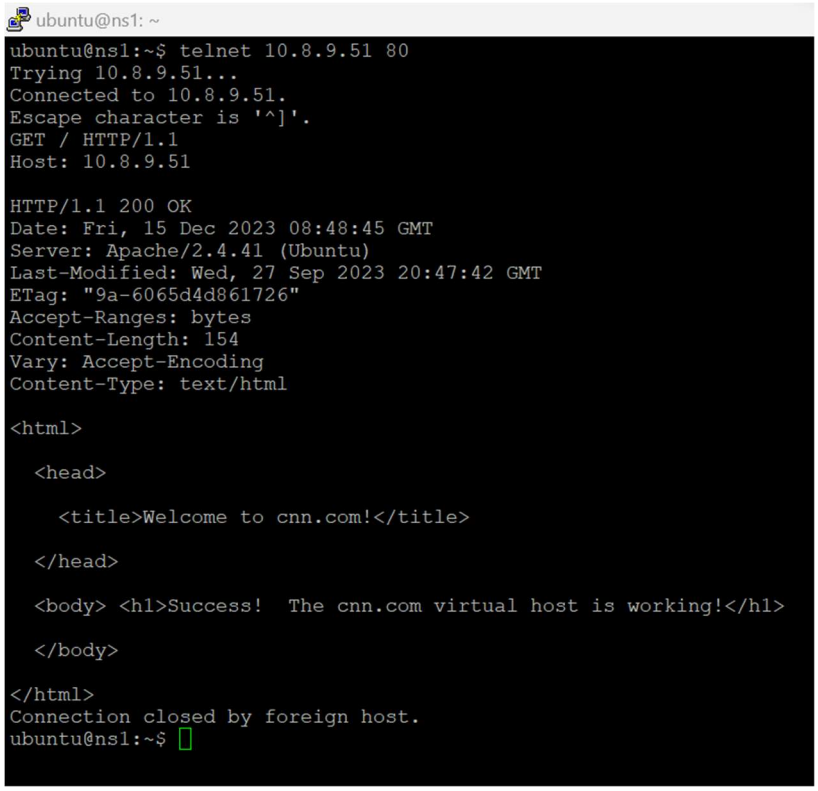
Added HTTP detection rule to /etc/snort/rules/local.rules. This rule alerts on any TCP traffic going from any source to port 80 (HTTP).



Demonstrate that snort on VM2 is capturing HTTP traffic generated by the simulated HTTP session from VM1 to VM3.

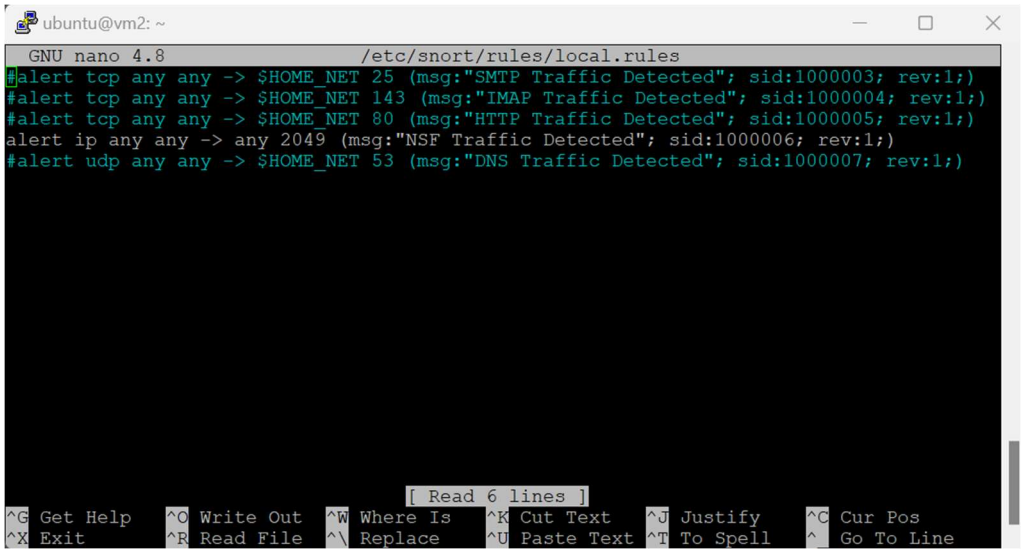


VM1:

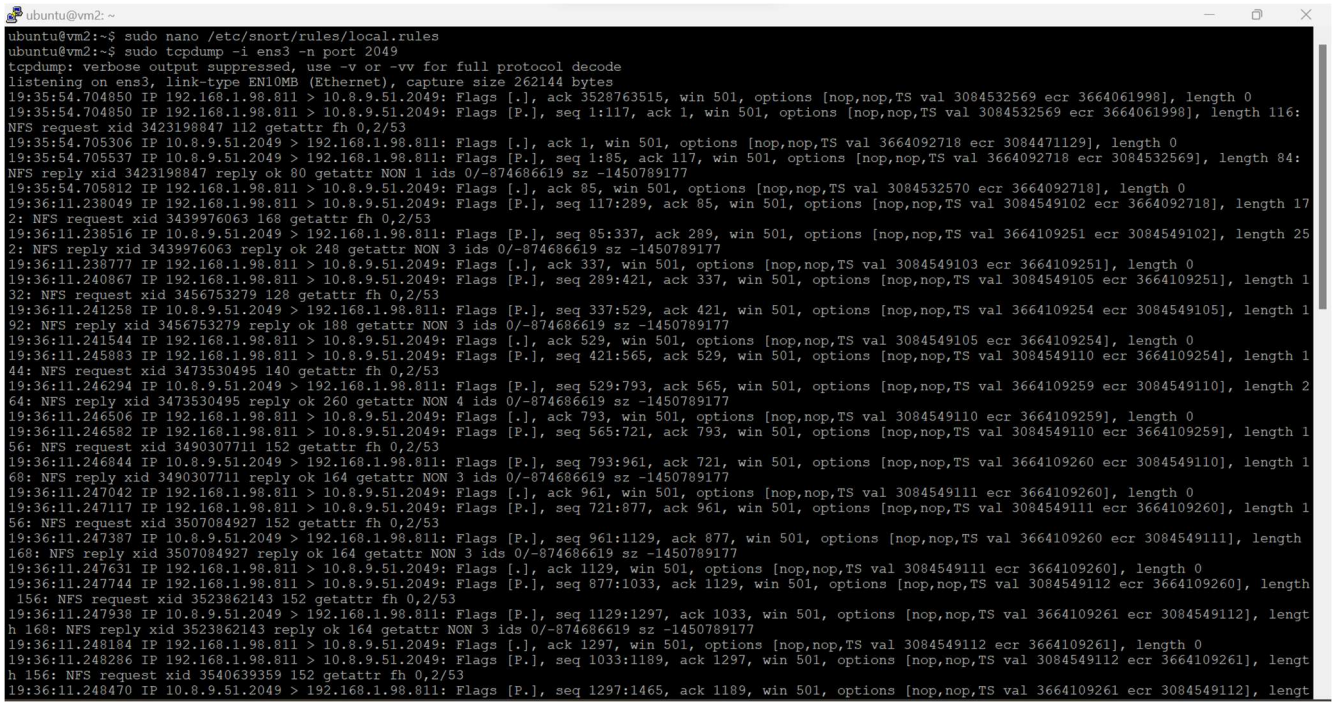


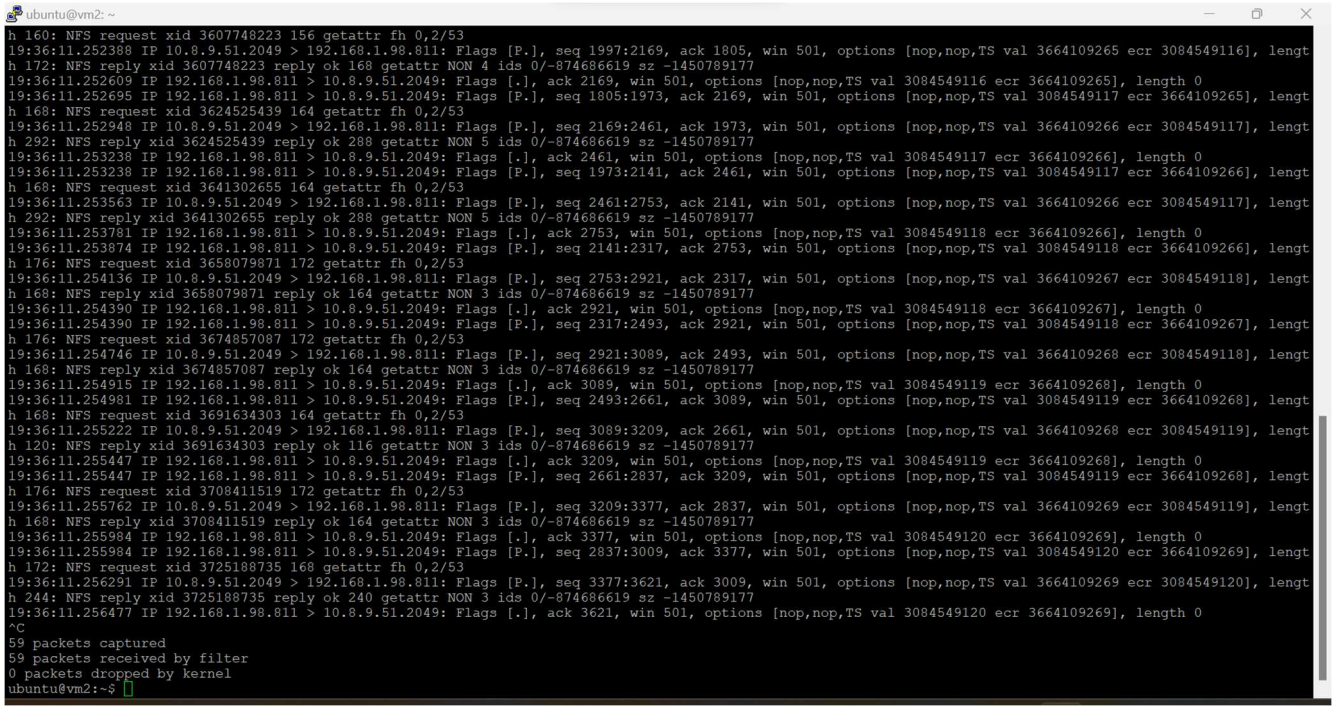
NFS:

Added NFS detection rule to /etc/snort/rules/local.rules. This rule will generate an alert message whenever it detects any IP traffic going to port 2049 (NFS).

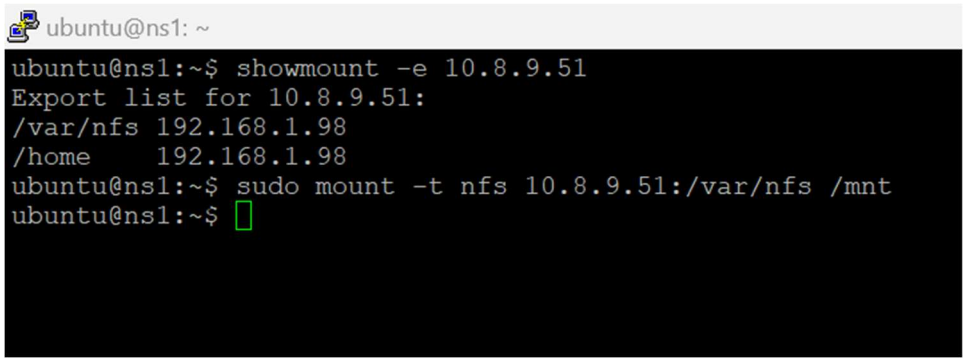


Displays NFS traffic in real-time using ‘tcpdump’:



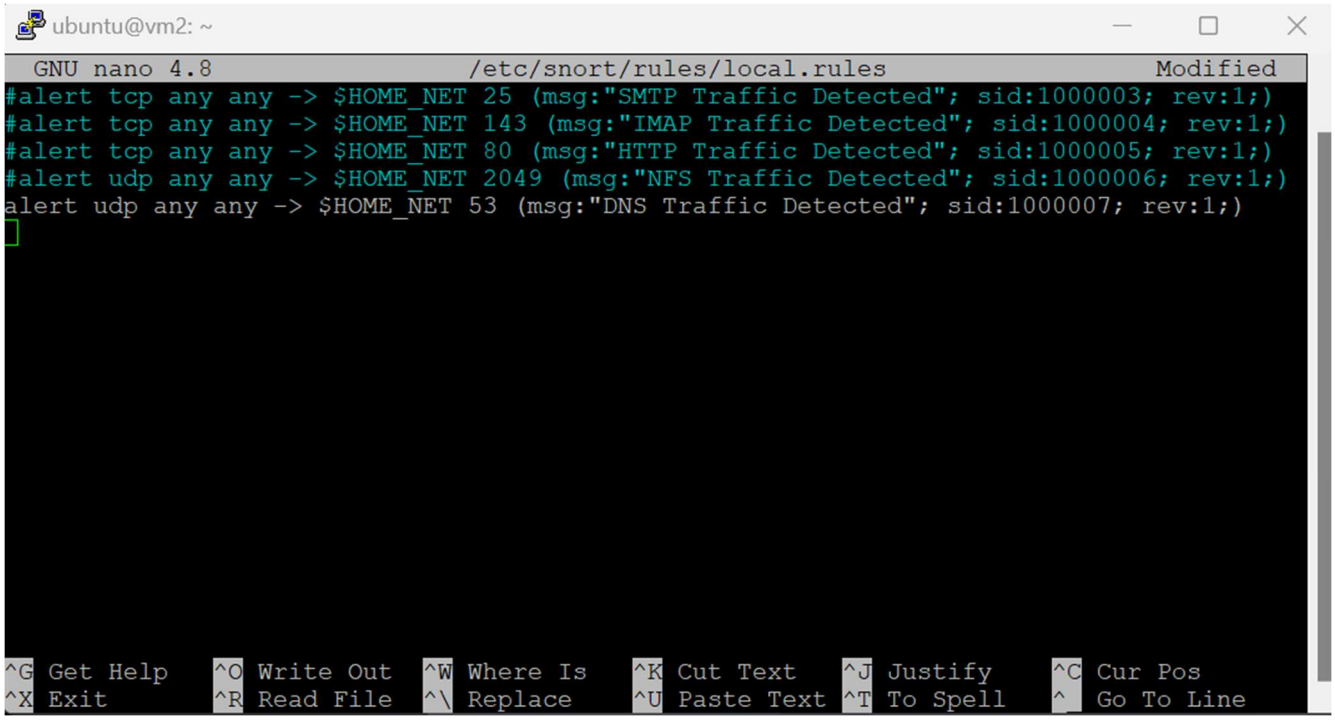


VM1:



DNS:

Added DNS detection rule to /etc/snort/rules/local.rules. This rule alerts on any UPD traffic going from any source to port 53 (DNS).



Demonstrates that snort on VM2 is capturing DNS traffic generated by the simulated DNS query from VM1 to VM3.

```
ubuntu@vm2: ~
ubuntu@vm2:~$ sudo nano /etc/snort/rules/local.rules
[sudo] password for ubuntu:
ubuntu@vm2:~$ sudo snort -A console -q -k none -c /etc/snort/snort.conf -i ens3
12/15-17:09:45.150213  [**] [1:1000007:1] DNS Traffic Detected [**] [Priority: 0] {UDP}
 192.168.1.98:38911 -> 10.8.9.51:53
^C*** Caught Int-Signal
ubuntu@vm2:~$
```

VM1:

```
ubuntu@ns1: ~
ubuntu@ns1:~$ dig shahpuja.com @10.8.9.51

; <<>> DiG 9.16.1-Ubuntu <<>> shahpuja.com @10.8.9.51
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43050
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 05b5df9936066cb001000000657ccea95d009be9b3641bc2 (good)
;; QUESTION SECTION:
;shahpuja.com.                  IN      A

;; AUTHORITY SECTION:
shahpuja.com.           604800  IN      SOA     ns1.shahpuja.com. admin.shahpuja
.com. 32 604800 86400 2419200 604800

;; Query time: 36 msec
;; SERVER: 10.8.9.51#53(10.8.9.51)
;; WHEN: Fri Dec 15 17:09:45 EST 2023
;; MSG SIZE  rcvd: 115

ubuntu@ns1:~$
```

VM1 IP Address	Protocol	Date and Time Protocol was used?
192.168.1.98	SMTP	14 Dec 2023 23:16:58
192.168.1.98	IMAP	15 Dec 2023 03:24:46
192.168.1.98	HTTP	15 Dec 2023 03:48:30
192.168.1.98	NFS	15 Dec 2023 19:35:54
192.168.1.98	DNS	15 Dec 2023 17:09:45

Task 5:

Configure routes from VM1 --> VM2 --> VM3

On VM1:

sudo ip route add 10.8.9.155/32 via 192.168.1.99

10.8.9.155 is the Secondary IP address on your VM3

192.168.1.99 is the Primary address on your VM2

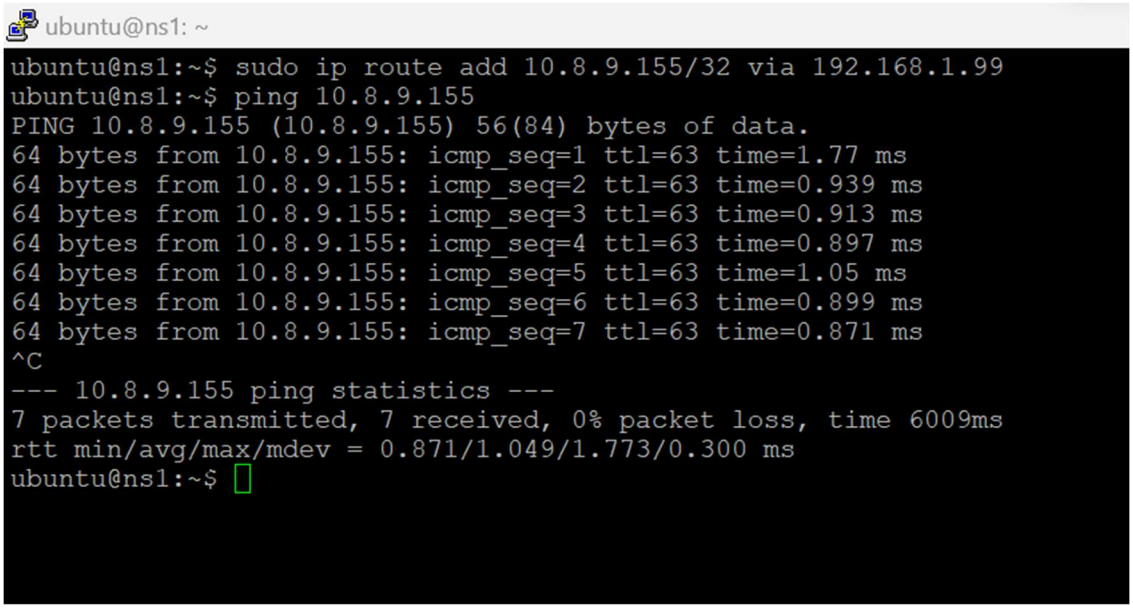
Configure routes from VM3 -->VM2 -->VM3

On VM3:

sudo ip route add 192.168.1.98/32 via 10.8.9.50

192.168.1.98 is the Primary IP address on your VM1

10.8.9.50 is the Secondary IP address on your VM2



Source IP	Destination IP	Date/Time Ping Sent
192.168.1.98	10.8.9.155	15 Dec 2023 18:30:09