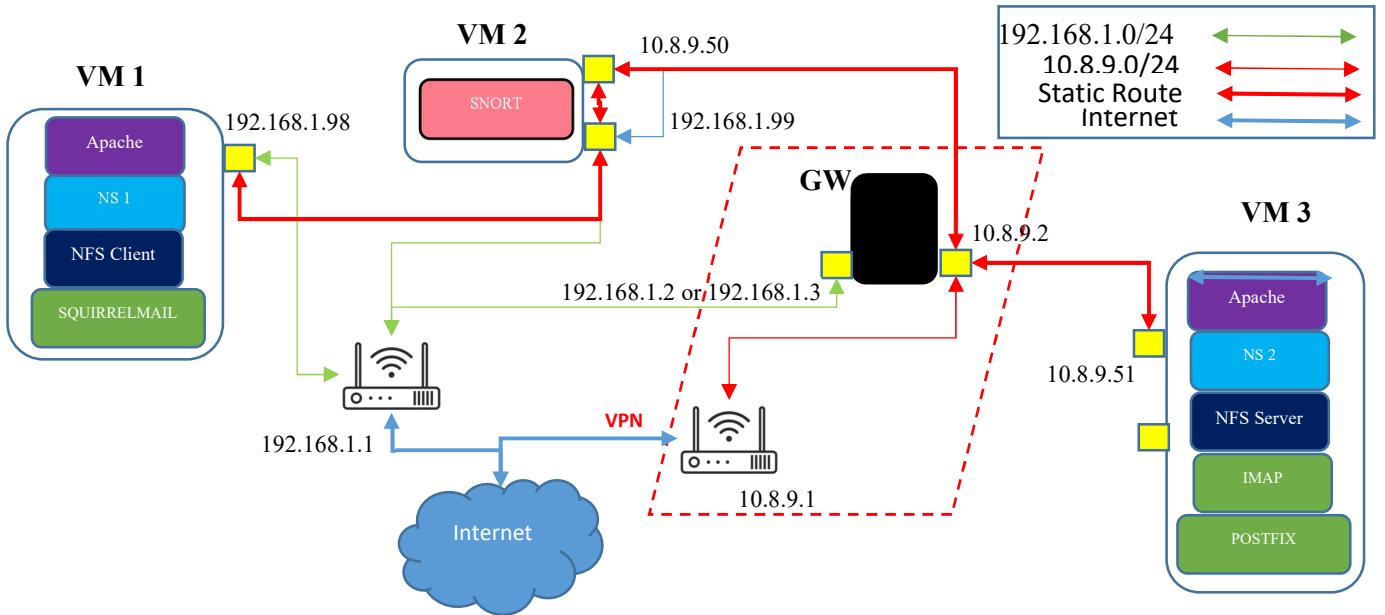


CSIT 432-01
Fall 2023
Final Project
Name: Puja Shah

Table of Contents

| Task no. | Task Name | Page no. |
|-----------------|---|-----------------|
| 1. | Internal Email using Squirrelmail | 3 |
| 2. | Internal Email from VM3 to another VM3 using the mail command | 4 |
| 3. | External Email using Squirrelmail | 6 |
| 4. | Implementing Deep Packet Inspection Using Snort | 9 |
| 5. | Routing | 18 |

Overview of Virtual Computing Infrastructure



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

Squirrelmail sent inbox:

Screenshot of the SquirrelMail 1.4.22 web interface. The current folder is INBOX.Sent. The message details are as follows:

- Subject:** Test for Task 1
- From:** shahp@shahpuja.com
- Date:** Wed, December 13, 2023 11:40 pm
- To:** puja@mail.shahpuja.com
- Priority:** Normal
- Options:** View Full Header | View Printable Version | Download this as a file

The message body contains the text: "Test email for task 1".

Mail received by the other user on VM3:

```

puja@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 user id 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: <bccc97c4c77634066070c77d35722e956.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.

```
ubuntu@mail: ~
GNU nano 4.8
127.0.0.1 localhost
127.0.1.1 t1-ubuntu20-04
10.8.9.51 vm3
10.8.9.155 mail.csit432.com
10.8.9.51 mail.shahpuja.com
192.168.1.98 ns1.shahpuja.com ns1 u3
10.8.9.51 ns2.shahpuja.com ns2 u4

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

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

```
ubuntu@mail: ~
ubuntu@mail:~$ sudo nano /etc/hosts
ubuntu@mail:~$ mail leberkc@mail.csit432.com
Cc:
Subject: Test email from 10.8.9.51 Puja Shah
Test email
```

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

```
ubuntu@mail: ~
ubuntu@mail:~$ sudo nano /etc/hosts
ubuntu@mail:~$ mail leberkc@mail.csit432.com
Cc:
Subject: Test email from 10.8.9.51 Puja Shah
Test email
ubuntu@mail:~$ sudo tail /var/log/mail.log
Dec 14 00:52:04 mail postfix/smtp[151617]: connect to shahpuja.com[198.185.159.1
45]:25: Connection timed out
Dec 14 00:52:34 mail postfix/smtp[151617]: connect to shahpuja.com[198.49.23.144
]:25: Connection timed out
Dec 14 00:53:04 mail postfix/smtp[151617]: connect to shahpuja.com[198.49.23.145
]:25: Connection timed out
Dec 14 00:53:35 mail postfix/smtp[151617]: connect to shahpuja.com[198.185.159.1
44]:25: Connection timed out
Dec 14 00:53:35 mail postfix/smtp[151617]: 6663A43B54: to=<shahp@shahpuja.com>,
relay=none, delay=19600, delays=19479/0.01/120/0, dsn=4.4.1, status=deferred (co
nnect to shahpuja.com[198.185.159.144]:25: Connection timed out)
Dec 14 00:53:40 mail postfix/pickup[151594]: AD18B42BEA: uid=1000 from=<ubuntu@m
ail>
Dec 14 00:53:40 mail postfix/cleanup[151627]: AD18B42BEA: message-id=<2023121405
5340.AD18B42BEA@mail.shahpuja.com>
Dec 14 00:53:40 mail postfix/qmgr[151595]: AD18B42BEA: from=<ubuntu@mail>, size=
375, nrcpt=1 (queue active)
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, ds
n=2.0.0, status=sent (250 2.0.0 Ok: queued as 8B3D0400E2)
Dec 14 00:53:50 mail postfix/qmgr[151595]: AD18B42BEA: removed
ubuntu@mail:~$
```

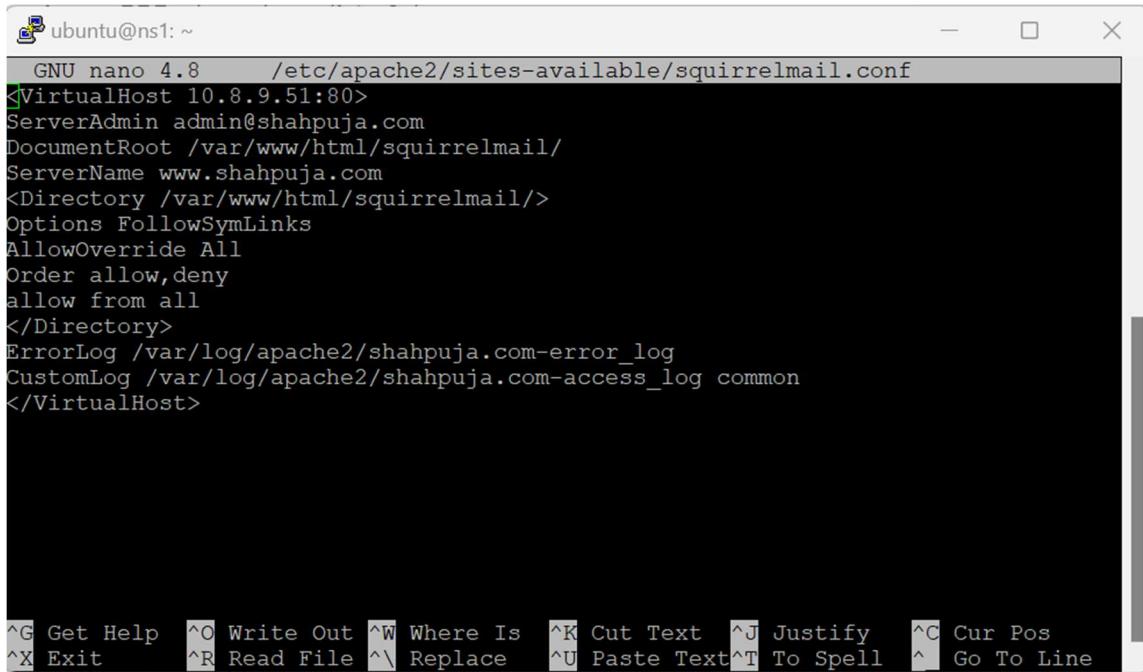
Log entries shows successful email delivery:

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.



```
ubuntu@ns1: ~
GNU nano 4.8      /etc/apache2/sites-available/squirrelmail.conf
<VirtualHost 10.8.9.51:80>
ServerAdmin admin@shahpuja.com
DocumentRoot /var/www/html/squirrelmail/
ServerName www.shahpuja.com
<Directory /var/www/html/squirrelmail/>
Options FollowSymLinks
AllowOverride All
Order allow,deny
allow from all
</Directory>
ErrorLog /var/log/apache2/shahpuja.com-error_log
CustomLog /var/log/apache2/shahpuja.com-access_log common
</VirtualHost>

^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
```

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

```

ubuntu@ns1: ~
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Server Settings

General
-----
1. Domain           : shahpuja.com
2. Invert Time     : false
3. Sendmail or SMTP : Sendmail

A. Update IMAP Settings : 10.8.9.51:143 (other)
B. Change Sendmail Config : /usr/sbin/sendmail

R  Return to Main Menu
C  Turn color on
S  Save data
Q  Quit

Command >> 

```

Squirrelmail sent inbox:

SquirrelMail 1.4.22

Current Folder: INBOX.Sent

[Compose](#) [Addresses](#) [Folders](#) [Options](#) [Search](#) [Help](#)

[Sign Out](#) [SquirrelMail](#)

Viewing Message: 1 (1 total)

Move Selected To: [INBOX](#) [Move](#) [Forward](#)

| To | Date | Subject |
|--------------------------------------|--------------|---------------------------------|
| shahp3@montclair.edu | Wed, 7:28 pm | Test for Task 3 |

[Toggle All](#)

Transform Selected Messages: [Read](#) [Unread](#) [Delete](#)

Viewing Message: 1 (1 total)

SquirrelMail 1.4.22

192.168.1.98/squirrelmail/src/webmail.php

Folders
Last Refresh: Wed, 7:25 pm
(Check mail)

INBOX
INBOX.Drafts
INBOX.Sent
INBOX.Trash

Current Folder: INBOX.Sent

[Compose](#) [Addresses](#) [Folders](#) [Options](#) [Search](#) [Help](#)

[Sign Out](#) [SquirrelMail](#)

[Message List](#) | [Unread](#) | [Delete](#) | [Edit Message as New](#)

Previous | Next [Forward](#) | [Forward as Attachment](#) | [Reply](#) | [Reply All](#)

Subject: Test for Task 3
From: shahp@shahpuja.com
Date: Wed, December 13, 2023 7:28 pm
To: shahp3@montclair.edu
Priority: Normal
Options: [View Full Header](#) | [View Printable Version](#) | [Download this as a file](#)

Test for Task 3

Email received to Montclair inbox:

mail.google.com/mail/u/1/#inbox/

Gmail

Compose

Inbox

Starred

Snoozed

Sent

Drafts

More

Labels

Search in mail

Active

Montclair State University

Test for Task 3 External Inbox

shahp@shahpuja.com to me

7:28PM (3 minutes ago)

Test for Task 3

Reply Forward

| 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).

```
ubuntu@vm2: ~
GNU nano 4.8          /etc/snort/rules/local.rules
alert tcp any any -> $HOME_NET 25 (msg:"SMTP Traffic Detected"; sid:1000003; rev:1;)[]

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

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

```
ubuntu@ns1: ~$ telnet 10.8.9.51 25
Trying 10.8.9.51...
Connected to 10.8.9.51.
Escape character is '^].
220 mail.shahpuja.com ESMTP Postfix (Ubuntu)
HELO mail.shahpuja.com
250 mail.shahpuja.com
MAIL FROM: mail.shahpuja.com
250 2.1.0 Ok
RCPT TO: shahp@mail.shahpuja.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Test Email
This is a test email
.
250 2.0.0 Ok: queued as D441642BE8
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
ubuntu@ns1:~$
```

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

```
ubuntu@vm2:~$ sudo nano /etc/snort/rules/local.rules
ubuntu@vm2:~$ sudo snort -A console -q -k none -c /etc/snort/snort.conf -i ens3
12/14-23:16:58.176940  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:16:58.177644  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:16:58.217479  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:17:36.548426  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:17:36.549051  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:18:48.073765  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:18:48.079733  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:19:24.854298  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:19:24.874405  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:19:30.379971  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:19:30.380694  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:19:42.815789  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:19:55.127747  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:19:58.446201  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:19:58.482044  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:20:03.457871  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:20:03.458722  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
12/14-23:20:03.458722  [**] [1:1000003:1] SMTP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:44920 -> 10.8.9.51:25
^C*** Caught Int-Signal
ubuntu@vm2:~$
```

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).

```
ubuntu@vm2:~$ GNU nano 4.8          /etc/snort/rules/local.rules      Modified
#alert tcp any any -> $HOME_NET 25 (msg:"SMTP Traffic Detected"; sid:1000003; rev:1;)
alert tcp any any -> $HOME_NET 143 (msg:"IMAP Traffic Detected"; sid:1000004; rev:1;)

^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
```

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

```
ubuntu@vm2:~$ sudo snort -A console -q -k none -c /etc/snort/snort.conf -i ens3
12/15-03:24:46.066483  [**] [1:1000004:1] IMAP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:48064 -> 10.8.9.51:143
12/15-03:24:46.067063  [**] [1:1000004:1] IMAP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:48064 -> 10.8.9.51:143
12/15-03:24:46.078981  [**] [1:1000004:1] IMAP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:48064 -> 10.8.9.51:143
12/15-03:25:02.369664  [**] [1:1000004:1] IMAP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:48064 -> 10.8.9.51:143
12/15-03:25:02.459784  [**] [1:1000004:1] IMAP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:48064 -> 10.8.9.51:143
12/15-03:25:14.953653  [**] [1:1000004:1] IMAP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:48064 -> 10.8.9.51:143
12/15-03:25:14.966411  [**] [1:1000004:1] IMAP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:48064 -> 10.8.9.51:143
12/15-03:25:35.290109  [**] [1:1000004:1] IMAP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:48064 -> 10.8.9.51:143
12/15-03:25:35.291359  [**] [1:1000004:1] IMAP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:48064 -> 10.8.9.51:143
12/15-03:25:41.647767  [**] [1:1000004:1] IMAP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:48064 -> 10.8.9.51:143
12/15-03:25:41.649148  [**] [1:1000004:1] IMAP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:48064 -> 10.8.9.51:143
12/15-03:25:41.649325  [**] [1:1000004:1] IMAP Traffic Detected [**] [Priority: 0] {TCP} 192.168.1.98:48064 -> 10.8.9.51:143
^C*** Caught Int-Signal
ubuntu@vm2:~$ 
```

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

```

 ubuntu@ns1: ~
ubuntu@ns1:~$ telnet 10.8.9.51 143
Trying 10.8.9.51...
Connected to 10.8.9.51.
Escape character is ']'.
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ START
TLS AUTH=PLAIN] Dovecot (Ubuntu) ready.
a login shahp ubuntu
a OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISP
LAY THREAD=REFRENCES THREAD=REFS THREAD=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL
CATENATE UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 CONDSTORE
QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE S
NIPPET=FUZZY PREVIEW=FUZZY LITERAL+ NOTIFY SPECIAL-USE] Logged in
a select inbox
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags permit
ted.
* 3 EXISTS
* 1 RECENT
* OK [UNSEEN 3] First unseen.
* OK [UIDVALIDITY 1700589801] UIDs valid
* OK [UIDNEXT 10] Predicted next UID
a OK [READ-WRITE] Select completed (0.012 + 0.000 + 0.011 secs).
a fetch 1 body[]
* 1 FETCH (BODY[] {438}
Return-Path: <ubuntu@mail>
X-Original-To: shahp@mail.shahpuja.com
Delivered-To: shahp@mail.shahpuja.com
Received: by mail.shahpuja.com (Postfix, from userid 1000)
           id 7891E43B5D; Wed, 13 Dec 2023 19:53:25 -0500 (EST)
To: <shahp@mail.shahpuja.com>
Subject: T
X-Mailer: mail (GNU Mailutils 3.7)
Message-Id: <20231214005325.7891E43B5D@mail.shahpuja.com>
Date: Wed, 13 Dec 2023 19:53:25 -0500 (EST)
From: Ubuntu <ubuntu@mail>

T
)
a OK Fetch completed (0.001 + 0.000 secs).
a logout
* BYE Logging out
a OK Logout completed (0.001 + 0.000 secs).
Connection closed by foreign host.
ubuntu@ns1:~$ 
```

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).

```
ubuntu@vm2: ~
GNU nano 4.8          /etc/snort/rules/local.rules
#alert tcp any any -> $HOME_NET 25 (msg:"SMTP Traffic Detected"; sid:1000003; rev:1;)
#alert tcp any any -> $HOME_NET 143 (msg:"IMAP Traffic Detected"; sid:1000004; rev:1;)
alert tcp any any -> $HOME_NET 80 (msg:"HTTP Traffic Detected"; sid:1000005; rev:1;)

[ Read 4 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
```

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

```
ubuntu@vm2:~$ sudo nano /etc/snort/rules/local.rules
ubuntu@vm2:~$ sudo snort -A console -q -k none -c /etc/snort/snort.conf -i ens3
12/15-03:48:30.317890  [**] [1:1000005:1] HTTP Traffic Detected [**] [Priority: 0] {TCP}
192.168.1.98:53228 -> 10.8.9.51:80
12/15-03:48:30.318470  [**] [1:1000005:1] HTTP Traffic Detected [**] [Priority: 0] {TCP}
192.168.1.98:53228 -> 10.8.9.51:80
12/15-03:48:45.994985  [**] [1:1000005:1] HTTP Traffic Detected [**] [Priority: 0] {TCP}
192.168.1.98:53228 -> 10.8.9.51:80
12/15-03:48:54.897425  [**] [1:1000005:1] HTTP Traffic Detected [**] [Priority: 0] {TCP}
192.168.1.98:53228 -> 10.8.9.51:80
12/15-03:48:55.243130  [**] [1:1000005:1] HTTP Traffic Detected [**] [Priority: 0] {TCP}
192.168.1.98:53228 -> 10.8.9.51:80
12/15-03:48:55.252972  [**] [1:1000005:1] HTTP Traffic Detected [**] [Priority: 0] {TCP}
192.168.1.98:53228 -> 10.8.9.51:80
12/15-03:49:00.258500  [**] [1:1000005:1] HTTP Traffic Detected [**] [Priority: 0] {TCP}
192.168.1.98:53228 -> 10.8.9.51:80
^C*** Caught Int-Signal
ubuntu@vm2:~$
```

VM1:

```
ubuntu@ns1: ~
ubuntu@ns1:~$ telnet 10.8.9.51 80
Trying 10.8.9.51...
Connected to 10.8.9.51.
Escape character is '^]'.
GET / HTTP/1.1
Host: 10.8.9.51

HTTP/1.1 200 OK
Date: Fri, 15 Dec 2023 08:48:45 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Wed, 27 Sep 2023 20:47:42 GMT
ETag: "9a-6065d4d861726"
Accept-Ranges: bytes
Content-Length: 154
Vary: Accept-Encoding
Content-Type: text/html

<html>
  <head>
    <title>Welcome to cnn.com!</title>
  </head>
  <body> <h1>Success! The cnn.com virtual host is working!</h1>
  </body>
</html>
Connection closed by foreign host.
ubuntu@ns1:~$
```

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).

```
ubuntu@vm2: ~
GNU nano 4.8          /etc/snort/rules/local.rules
#alert tcp any any -> $HOME_NET 25 (msg:"SMTP Traffic Detected"; sid:1000003; rev:1;)
#alert tcp any any -> $HOME_NET 143 (msg:"IMAP Traffic Detected"; sid:1000004; rev:1;)
#alert tcp any any -> $HOME_NET 80 (msg:"HTTP Traffic Detected"; sid:1000005; rev:1;)
alert ip any any -> any 2049 (msg:"NSF Traffic Detected"; sid:1000006; rev:1;)
#alert udp any any -> $HOME_NET 53 (msg:"DNS Traffic Detected"; sid:1000007; rev:1;)

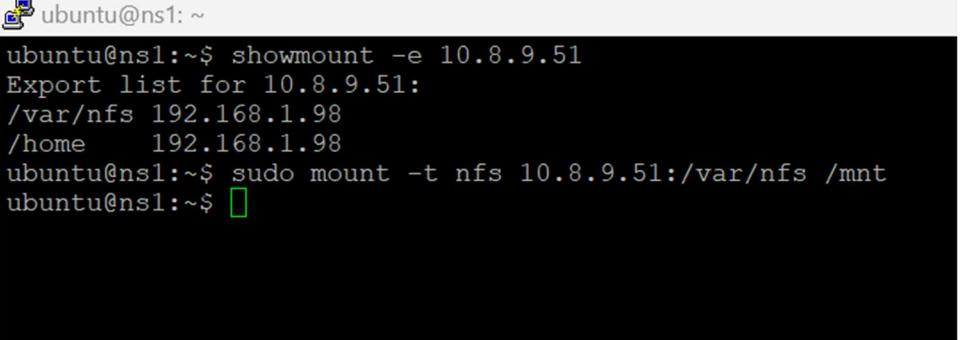
[ Read 6 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit     ^R Read File  ^\ Replace   ^U Paste Text ^T To Spell  ^  Go To Line
```

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

```
ubuntu@vm2:~$ sudo nano /etc/snort/rules/local.rules
ubuntu@vm2:~$ sudo tcpdump -i ens3 -n port 2049
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
19:35:54.704850 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [.], ack 3528763515, win 501, options [nop,nop,TS val 3084532569 ecr 3664061998], length 0
19:35:54.704850 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P..], seq 1:117, ack 1, win 501, options [nop,nop,TS val 3084532569 ecr 3664061998], length 116: NFS request xid 3423198847 112 getattrib fh 0/2/53
19:35:54.705306 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [.], ack 1, win 501, options [nop,nop,TS val 3664092718 ecr 3084471129], length 0
19:35:54.705357 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P..], seq 1:85, ack 117, win 501, options [nop,nop,TS val 3664092718 ecr 3084532569], length 84: NFS reply xid 3423198847 reply on 80 getattrib NON 1 1ids 0-874686619 sz -1450789177
19:35:54.705812 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [.], ack 85, win 501, options [nop,nop,TS val 3084532570 ecr 3664092718], length 0
19:36:11.238049 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P..], seq 117:289, ack 85, win 501, options [nop,nop,TS val 3084549102 ecr 3664092718], length 172: NFS request xid 3439976063 168 getattrib fh 0/2/53
19:36:11.238516 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P..], seq 85:337, ack 289, win 501, options [nop,nop,TS val 3664109251 ecr 3084549102], length 25
2: NFS reply xid 3439976063 reply on 248 getattrib NON 3 3ids 0-874686619 sz -1450789177
19:36:11.238777 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [.], ack 337, win 501, options [nop,nop,TS val 3084549103 ecr 3664109251], length 0
19:36:11.240867 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P..], seq 289:421, ack 337, win 501, options [nop,nop,TS val 3084549105 ecr 3664109251], length 132: NFS request xid 3456753279 128 getattrib fh 0/2/53
19:36:11.241258 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P..], seq 337:529, ack 421, win 501, options [nop,nop,TS val 3664109254 ecr 3084549105], length 192: NFS reply xid 3456753279 reply on 188 getattrib NON 3 3ids 0-874686619 sz -1450789177
19:36:11.241544 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [.], ack 529, win 501, options [nop,nop,TS val 3084549105 ecr 3664109254], length 0
19:36:11.245883 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P..], seq 421:565, ack 529, win 501, options [nop,nop,TS val 3084549110 ecr 3664109254], length 144: NFS request xid 3473530495 140 getattrib fh 0/2/53
19:36:11.246294 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P..], seq 529:793, ack 565, win 501, options [nop,nop,TS val 3664109259 ecr 3084549110], length 264: NFS reply xid 3473530495 reply on 260 getattrib NON 4 4ids 0-874686619 sz -1450789177
19:36:11.246506 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [.], ack 793, win 501, options [nop,nop,TS val 3084549110 ecr 3664109259], length 0
19:36:11.246582 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P..], seq 565:721, ack 793, win 501, options [nop,nop,TS val 3084549110 ecr 3664109259], length 156: NFS request xid 3490307711 152 getattrib fh 0/2/53
19:36:11.246844 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P..], seq 793:961, ack 721, win 501, options [nop,nop,TS val 3664109260 ecr 3084549110], length 168: NFS reply xid 3490307711 reply on 164 getattrib NON 3 3ids 0-874686619 sz -1450789177
19:36:11.247042 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [.], ack 961, win 501, options [nop,nop,TS val 3084549111 ecr 3664109260], length 0
19:36:11.247117 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P..], seq 721:877, ack 961, win 501, options [nop,nop,TS val 3084549111 ecr 3664109260], length 156: NFS request xid 3507084927 152 getattrib fh 0/2/53
19:36:11.247387 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P..], seq 961:1129, ack 877, win 501, options [nop,nop,TS val 3664109260 ecr 3084549111], length 168: NFS reply xid 3507084927 reply on 164 getattrib NON 3 3ids 0-874686619 sz -1450789177
19:36:11.247631 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [.], ack 1129, win 501, options [nop,nop,TS val 3084549111 ecr 3664109260], length 0
19:36:11.247744 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P..], seq 877:1033, ack 1129, win 501, options [nop,nop,TS val 3084549112 ecr 3664109260], length 156: NFS request xid 3523862143 152 getattrib fh 0/2/53
19:36:11.247938 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P..], seq 1129:1297, ack 1033, win 501, options [nop,nop,TS val 3664109261 ecr 3084549112], length 168: NFS reply xid 3523862143 reply on 164 getattrib NON 3 3ids 0-874686619 sz -1450789177
19:36:11.248184 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [.], ack 1297, win 501, options [nop,nop,TS val 3084549112 ecr 3664109261], length 0
19:36:11.248286 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P..], seq 1033:1189, ack 1297, win 501, options [nop,nop,TS val 3084549112 ecr 3664109261], length 156: NFS request xid 3540639355 152 getattrib fh 0/2/53
19:36:11.248470 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P..], seq 1297:1465, ack 1189, win 501, options [nop,nop,TS val 3664109261 ecr 3084549112], length
```

```
ubuntu@vm2:~ h 160: NFS request xid 3607748223 156 getattr fh 0,2/53  
19:36:11.1252388 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P.], seq 1997:2169, ack 1805, win 501, options [nop,nop,TS val 3664109265 ecr 3084549116], length 0  
h 172: NFS reply xid 3607748223 reply ok 168 getattr NON 4 ids 0/-874686619 sz -1450789177  
19:36:11.252609 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [!..], ack 2169, win 501, options [nop,nop,TS val 3084549116 ecr 3664109265], length 0  
19:36:11.252695 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P.], seq 1805:1973, ack 2169, win 501, options [nop,nop,TS val 3084549117 ecr 3664109265], length 0  
h 168: NFS request xid 3624525439 164 getattr fh 0,2/53  
19:36:11.252948 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P.], seq 2169:2461, ack 1973, win 501, options [nop,nop,TS val 3664109266 ecr 3084549117], length 0  
h 292: NFS reply xid 3624525439 reply ok 288 getattr NON 5 ids 0/-874686619 sz -1450789177  
19:36:11.253238 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [!..], ack 2461, win 501, options [nop,nop,TS val 3084549117 ecr 3664109266], length 0  
19:36:11.253238 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P.], seq 1973:2141, ack 2461, win 501, options [nop,nop,TS val 3084549117 ecr 3664109266], length 0  
h 168: NFS request xid 3641302655 164 getattr fh 0,2/53  
19:36:11.253563 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P.], seq 2461:2753, ack 2141, win 501, options [nop,nop,TS val 3664109266 ecr 3084549117], length 0  
h 292: NFS reply xid 3641302655 reply ok 288 getattr NON 5 ids 0/-874686619 sz -1450789177  
19:36:11.253781 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [!..], ack 2753, win 501, options [nop,nop,TS val 3084549118 ecr 3664109266], length 0  
19:36:11.253874 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P.], seq 2141:2317, ack 2753, win 501, options [nop,nop,TS val 3084549118 ecr 3664109266], length 0  
h 176: NFS request xid 3658079871 172 getattr fh 0,2/53  
19:36:11.254136 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P.], seq 2753:2921, ack 2317, win 501, options [nop,nop,TS val 3664109267 ecr 3084549118], length 0  
h 168: NFS reply xid 3658079871 reply ok 164 getattr NON 3 ids 0/-874686619 sz -1450789177  
19:36:11.254390 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [!..], ack 2921, win 501, options [nop,nop,TS val 3084549118 ecr 3664109267], length 0  
19:36:11.254390 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P.], seq 2317:2493, ack 2921, win 501, options [nop,nop,TS val 3084549118 ecr 3664109267], length 0  
h 176: NFS request xid 3674857087 172 getattr fh 0,2/53  
19:36:11.257446 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P.], seq 2921:3089, ack 2493, win 501, options [nop,nop,TS val 3664109268 ecr 3084549118], length 0  
h 168: NFS reply xid 3674857087 reply ok 164 getattr NON 3 ids 0/-874686619 sz -1450789177  
19:36:11.259415 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [!..], ack 3089, win 501, options [nop,nop,TS val 3084549119 ecr 3664109268], length 0  
19:36:11.259481 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P.], seq 2493:2661, ack 3089, win 501, options [nop,nop,TS val 3084549119 ecr 3664109268], length 0  
h 168: NFS request xid 3691634303 164 getattr fh 0,2/53  
19:36:11.255222 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P.], seq 3089:3209, ack 2661, win 501, options [nop,nop,TS val 3664109268 ecr 3084549119], length 0  
h 120: NFS reply xid 3691634303 reply ok 166 getattr NON 3 ids 0/-874686619 sz -1450789177  
19:36:11.255447 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [!..], ack 3209, win 501, options [nop,nop,TS val 3084549119 ecr 3664109268], length 0  
19:36:11.255447 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P.], seq 2661:2837, ack 3209, win 501, options [nop,nop,TS val 3084549119 ecr 3664109268], length 0  
h 176: NFS request xid 3708411519 172 getattr fh 0,2/53  
19:36:11.255762 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P.], seq 3209:3377, ack 2837, win 501, options [nop,nop,TS val 3664109269 ecr 3084549119], length 0  
h 168: NFS reply xid 3708411519 reply ok 164 getattr NON 3 ids 0/-874686619 sz -1450789177  
19:36:11.255984 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [!..], ack 3377, win 501, options [nop,nop,TS val 3084549120 ecr 3664109269], length 0  
19:36:11.255984 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [P.], seq 2837:3009, ack 3377, win 501, options [nop,nop,TS val 3084549120 ecr 3664109269], length 0  
h 172: NFS request xid 3725188735 176 getattr fh 0,2/53  
19:36:11.256291 IP 10.8.9.51.2049 > 192.168.1.98.811: Flags [P.], seq 3377:3621, ack 3009, win 501, options [nop,nop,TS val 3664109269 ecr 3084549120], length 0  
h 244: NFS reply xid 3725188735 reply ok 240 getattr NON 3 ids 0/-874686619 sz -1450789177  
19:36:11.256477 IP 192.168.1.98.811 > 10.8.9.51.2049: Flags [!..], ack 3621, win 501, options [nop,nop,TS val 3084549120 ecr 3664109269], length 0  
c  
59 packets captured  
59 packets received by filter  
0 packets dropped by kernel  
ubuntu@vm2:~
```

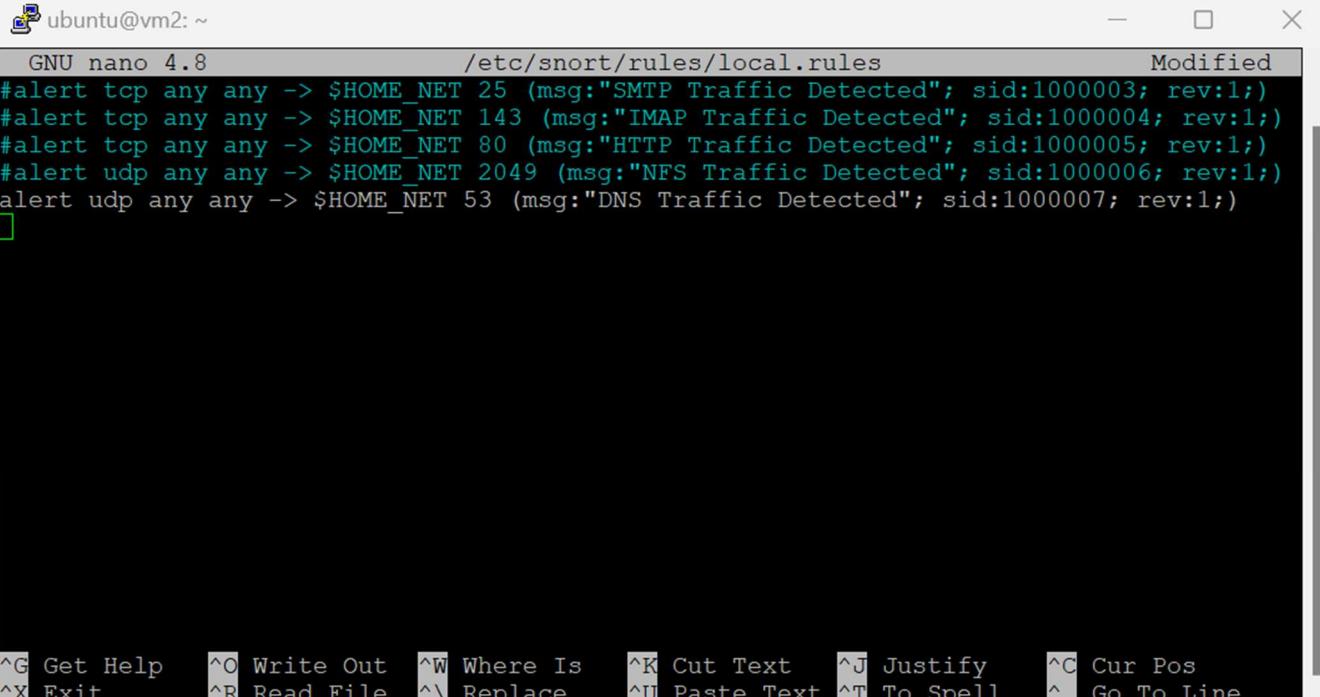
VM1:



```
ubuntu@ns1:~$ showmount -e 10.8.9.51
Export list for 10.8.9.51:
/var/nfs 192.168.1.98
/home   192.168.1.98
ubuntu@ns1:~$ sudo mount -t nfs 10.8.9.51:/var/nfs /mnt
ubuntu@ns1:~$
```

DNS:

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



```
ubuntu@vm2:~$ nano /etc/snort/rules/local.rules
GNU nano 4.8                               /etc/snort/rules/local.rules                         Modified
#alert tcp any any -> $HOME_NET 25 (msg:"SMTP Traffic Detected"; sid:1000003; rev:1;)
#alert tcp any any -> $HOME_NET 143 (msg:"IMAP Traffic Detected"; sid:1000004; rev:1;)
#alert tcp any any -> $HOME_NET 80 (msg:"HTTP Traffic Detected"; sid:1000005; rev:1;)
#alert udp any any -> $HOME_NET 2049 (msg:"NFS Traffic Detected"; sid:1000006; rev:1;)
alert udp any any -> $HOME_NET 53 (msg:"DNS Traffic Detected"; sid:1000007; rev:1;)
```

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

```
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:~$ 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: 05b5df9936066cb001000000657cce95d009be9b3641bc2 (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

```
ubuntu@ns1:~$ sudo ip route add 10.8.9.155/32 via 192.168.1.99
ubuntu@ns1:~$ ping 10.8.9.155
PING 10.8.9.155 (10.8.9.155) 56(84) bytes of data.
64 bytes from 10.8.9.155: icmp_seq=1 ttl=63 time=1.77 ms
64 bytes from 10.8.9.155: icmp_seq=2 ttl=63 time=0.939 ms
64 bytes from 10.8.9.155: icmp_seq=3 ttl=63 time=0.913 ms
64 bytes from 10.8.9.155: icmp_seq=4 ttl=63 time=0.897 ms
64 bytes from 10.8.9.155: icmp_seq=5 ttl=63 time=1.05 ms
64 bytes from 10.8.9.155: icmp_seq=6 ttl=63 time=0.899 ms
64 bytes from 10.8.9.155: icmp_seq=7 ttl=63 time=0.871 ms
^C
--- 10.8.9.155 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 0.871/1.049/1.773/0.300 ms
ubuntu@ns1:~$ 
```

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