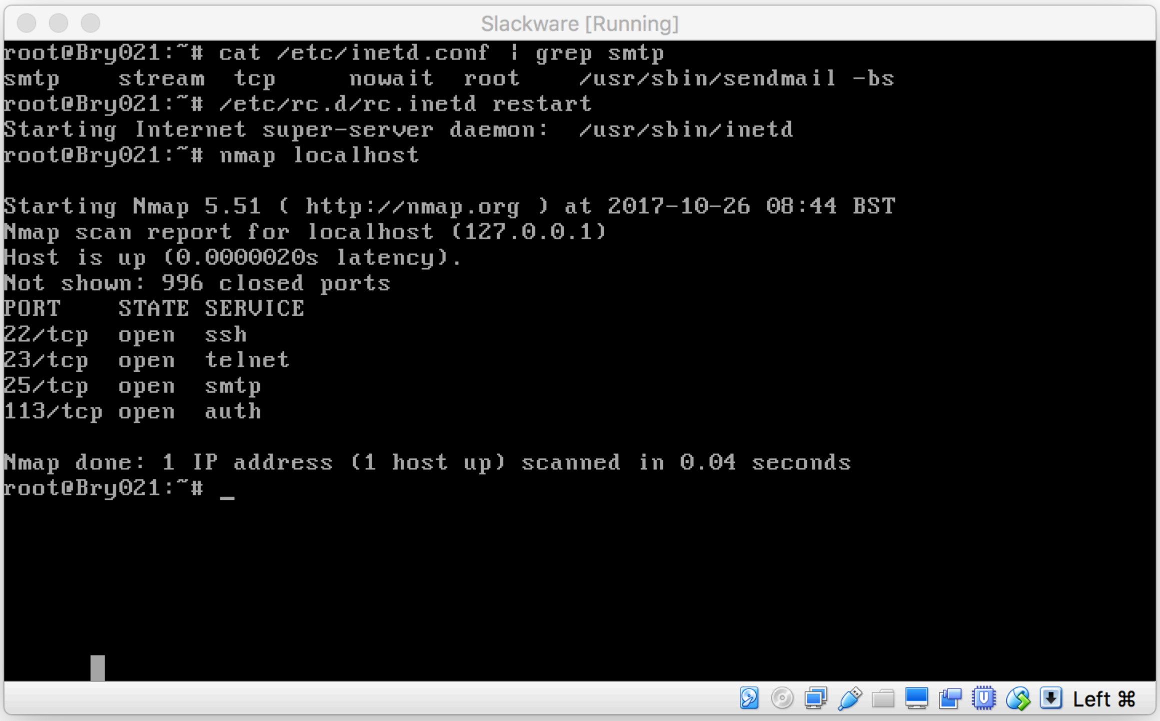
Lab 6 : Email under Linux

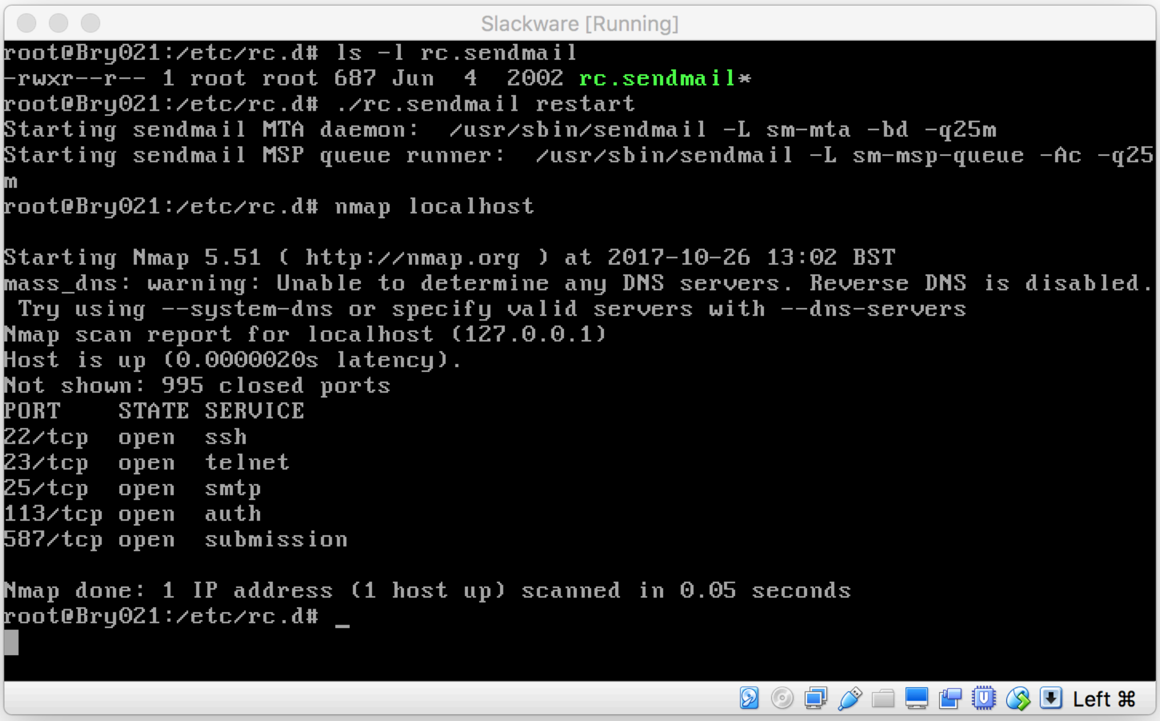
Exercise 0. Enable SMTP service

First let’s try to enable the SMTP service as an internet service, i.e. inetd daemon is going to be reconfigured:



```
root@Bry021:~# cat /etc/inetd.conf | grep smtp
smtp    stream  tcp     nowait  root    /usr/sbin/sendmail -bs
root@Bry021:~# /etc/rc.d/rc.inetd restart
Starting Internet super-server daemon:  /usr/sbin/inetd
root@Bry021:~# nmap localhost

Starting Nmap 5.51 ( http://nmap.org ) at 2017-10-26 08:44 BST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
113/tcp open  auth

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
root@Bry021:~# _
```

However no message is received as the SMTP service is provided by its own daemon (sendmail). Besides the normal procedure would be to uncomment lines in the inetd.conf file instead of inserting them (error prone).



```
root@Bry021:/etc/rc.d# ls -l rc.sendmail
-rwxr--r-- 1 root root 687 Jun  4  2002 rc.sendmail*
root@Bry021:/etc/rc.d# ./rc.sendmail restart
Starting sendmail MTA daemon:  /usr/sbin/sendmail -L sm-mta -bd -q25m
Starting sendmail MSP queue runner:  /usr/sbin/sendmail -L sm-msp-queue -Ac -q25
m
root@Bry021:/etc/rc.d# nmap localhost

Starting Nmap 5.51 ( http://nmap.org ) at 2017-10-26 13:02 BST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
113/tcp open  auth
587/tcp open  submission

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
root@Bry021:/etc/rc.d# _
```

Exercise 1. Sending email using mail

1.1. Redirect a file to mail using the syntax below to send it to bob.

mail -s subject **user@domain <** message.txt

1.2. Explain what the following command does:

echo “Welcome to Computer Systems” | **mail -s** “Hello world” bob@anglia.bryant **-c** smith@anglia.bryant **-b** root@anglia.bryant

Answer 1 & 2: This command makes use of pipes to forward the result of the echo command into the message body (Welcome to…)

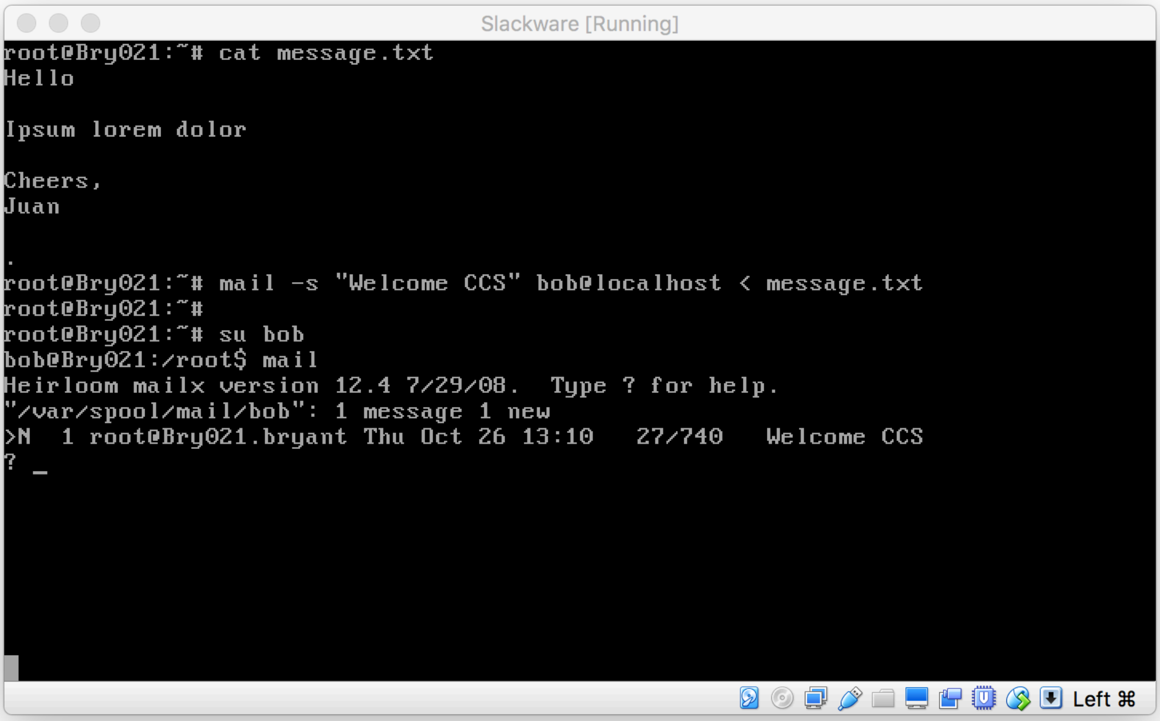
Exercise 2. Checking email

Log in as bob and check that all emails sent to bob are present.

In the Exercise 1.2 a message was actually sent to bob. If the daemon sendmail is not running, the emails are saved in the filesystem and will be sent once the daemon starts:

# ls -l **/var/spool/mqueue/**

Nevertheless the messages were received correctly (su bob):



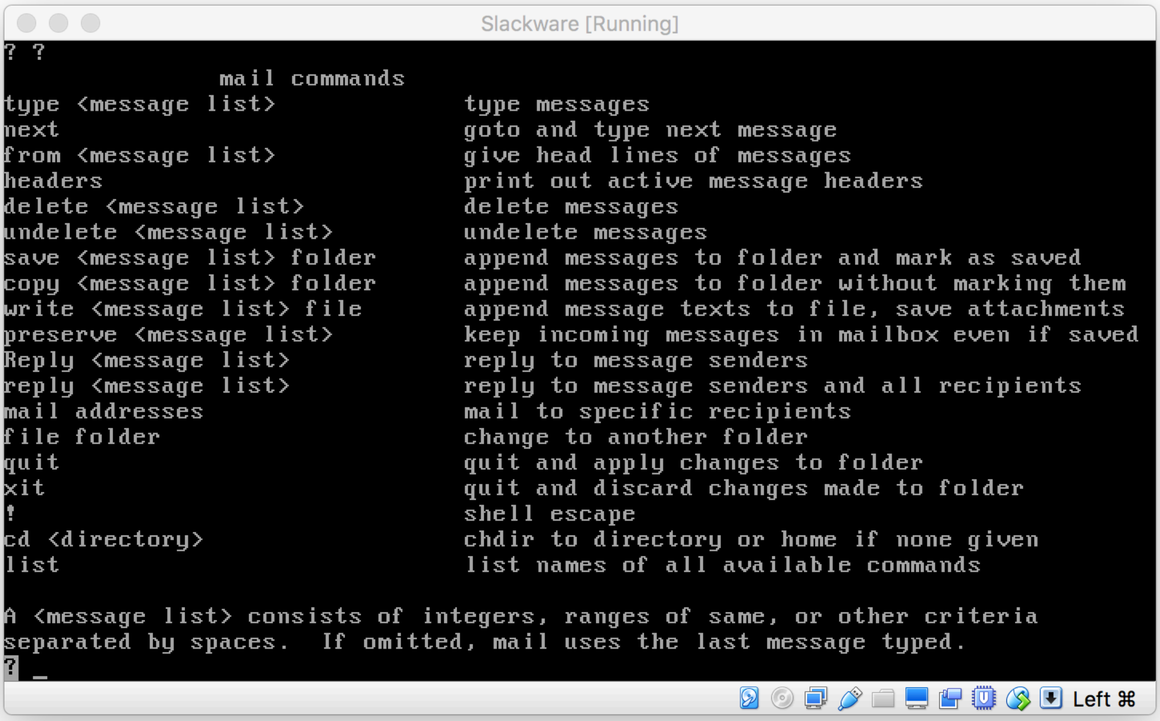
```
root@Bry021:~# cat message.txt
Hello

Ipsum lorem dolor

Cheers,
Juan

.
root@Bry021:~# mail -s "Welcome CCS" bob@localhost < message.txt
root@Bry021:~#
root@Bry021:~# su bob
bob@Bry021:/root$ mail
Heirloom mailx version 12.4 7/29/08.  Type ? for help.
"/var/spool/mail/bob": 1 message 1 new
>N  1 root@Bry021.bryant Thu Oct 26 13:10   27/740   Welcome CCS
? _
```

Exercise 3. Exploring mail

3.1. Describe how to read, reply, send, delete, list and save messages.

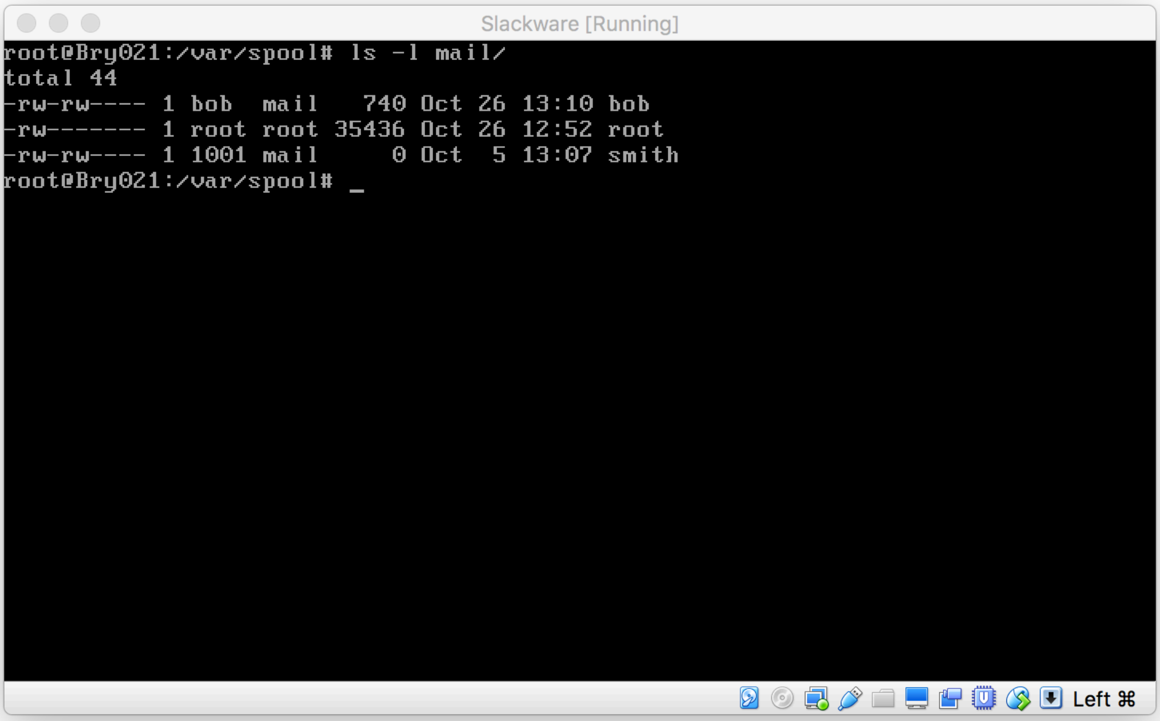
command	argument	description
type	<message list>	next also type to the next message
reply	<message list>	replay to message senders (Replay) and all recipients (replay)
mail	addresses	mail to specific recipients
delete	<message list>	delete messages
headers		list all the active message headers
write <file>	<message list>	append message text to file, save attachments.

To get more info type the command “mail ?”



```
? ?
               mail commands
type <message list>             type messages
next                            goto and type next message
from <message list>             give head lines of messages
headers                         print out active message headers
delete <message list>           delete messages
undelete <message list>         undelete messages
save <message list> folder      append messages to folder and mark as saved
copy <message list> folder      append messages to folder without marking them
write <message list> file       append message texts to file, save attachments
preserve <message list>         keep incoming messages in mailbox even if saved
Reply <message list>            reply to message senders
reply <message list>            reply to message senders and all recipients
mail addresses                  mail to specific recipients
file folder                     change to another folder
quit                            quit and apply changes to folder
xit                             quit and discard changes made to folder
!                               shell escape
cd <directory>                  chdir to directory or home if none given
list                            list names of all available commands

A <message list> consists of integers, ranges of same, or other criteria
separated by spaces.  If omitted, mail uses the last message typed.
? _
```

3.2. What is contained in /var/spool/mail/? What are the security implications?

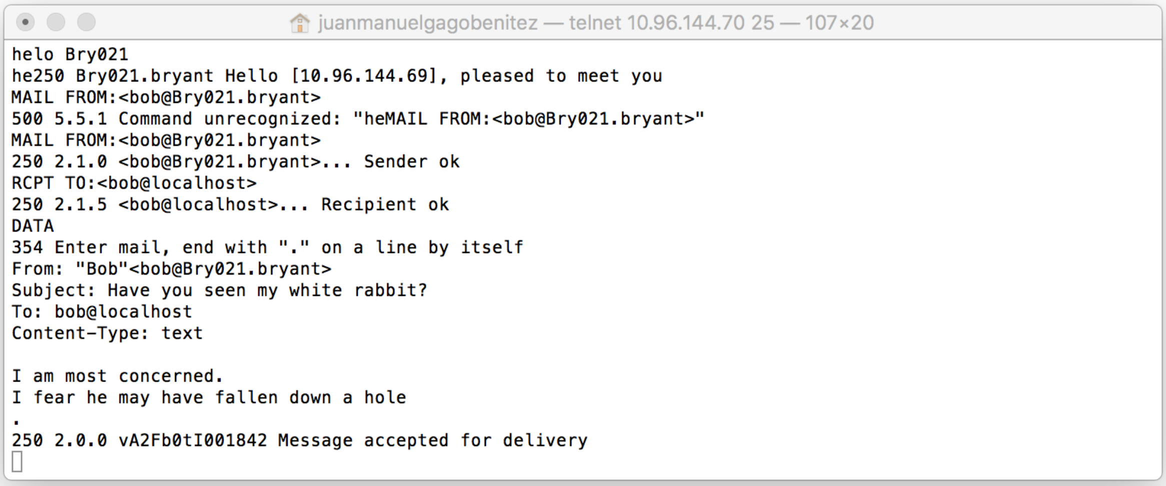


```
root@Bry021:/var/spool# ls -l mail/
total 44
-rw-rw---- 1 bob  mail   740 Oct 26 13:10 bob
-rw------- 1 root root 35436 Oct 26 12:52 root
-rw-rw---- 1 1001 mail     0 Oct  5 13:07 smith
root@Bry021:/var/spool# _
```

The folder is quite different from the output queue (Exercise 2). In fact, this folder contains the inboxes of the different users in the system (remember that smith were deleted in a previous Lab).

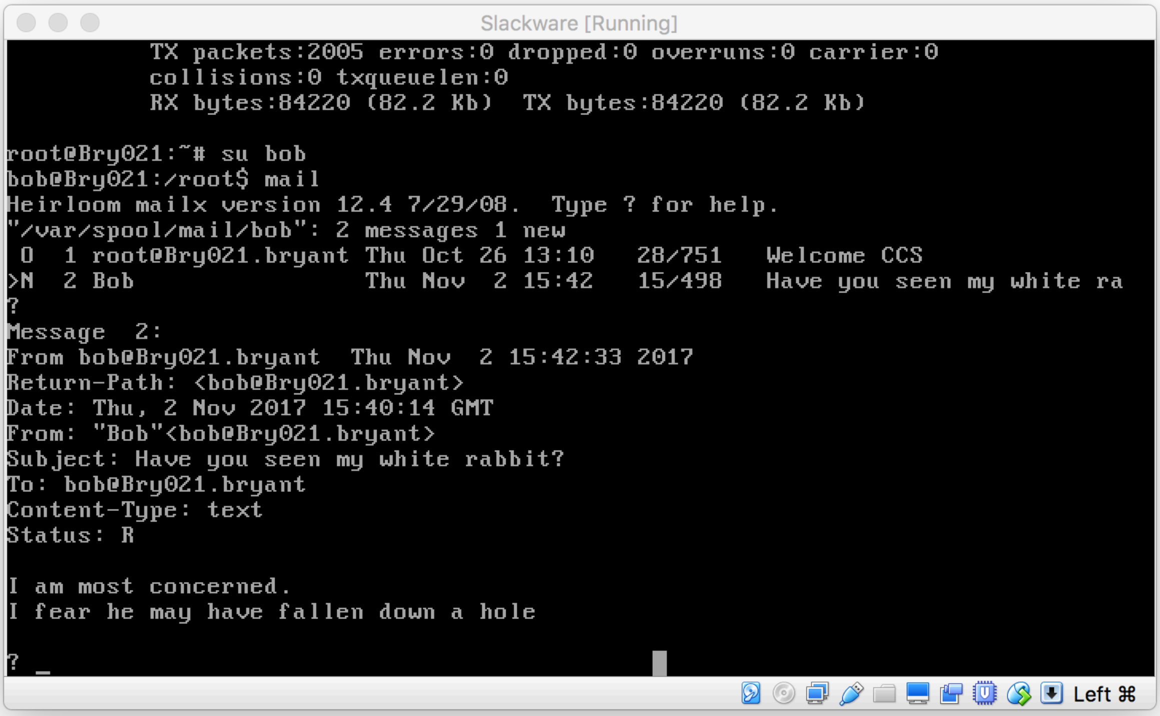
Conceptually, you can think of /var/spool/mail/ as a file in your home directory. It pretty much belongs to you. It's in a different location because that file needs to be available during email delivery.

3.3. From your host machine, telnet to your VM on port 25 and send a message to bob@localhost from root@localhost by talking to the server (see example of SMTP session)



```
helo Bry021
he250 Bry021.bryant Hello [10.96.144.69], pleased to meet you
MAIL FROM:<bob@Bry021.bryant>
500 5.5.1 Command unrecognized: "heMAIL FROM:<bob@Bry021.bryant>"
MAIL FROM:<bob@Bry021.bryant>
250 2.1.0 <bob@Bry021.bryant>... Sender ok
RCPT TO:<bob@localhost>
250 2.1.5 <bob@localhost>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
From: "Bob"<bob@Bry021.bryant>
Subject: Have you seen my white rabbit?
To: bob@localhost
Content-Type: text

I am most concerned.
I fear he may have fallen down a hole
.
250 2.0.0 vA2Fb0tI001842 Message accepted for delivery
```

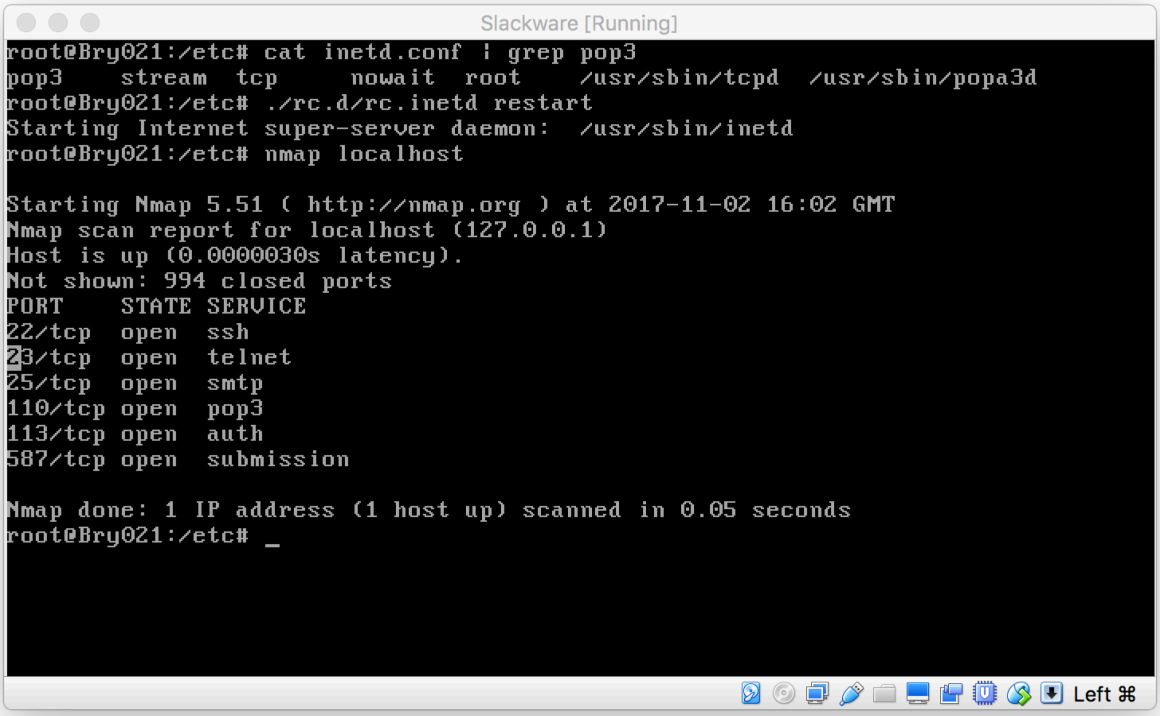
Notice how easy is to “impersonate” an SMTP server. You can have a “conversation” with a server and even manually perform a mail transaction. This is useful for debugging, but also makes abuse.



```
          TX packets:2005 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:84220 (82.2 Kb)  TX bytes:84220 (82.2 Kb)

root@Bry021:~# su bob
bob@Bry021:/root$ mail
Heirloom mailx version 12.4 7/29/08.  Type ? for help.
"/var/spool/mail/bob": 2 messages 1 new
 O  1 root@Bry021.bryant Thu Oct 26 13:10   28/751    Welcome CCS
>N  2 Bob                Thu Nov  2 15:42   15/498    Have you seen my white ra
?
Message  2:
From bob@Bry021.bryant  Thu Nov  2 15:42:33 2017
Return-Path: <bob@Bry021.bryant>
Date: Thu, 2 Nov 2017 15:40:14 GMT
From: "Bob"<bob@Bry021.bryant>
Subject: Have you seen my white rabbit?
To: bob@Bry021.bryant
Content-Type: text
Status: R

I am most concerned.
I fear he may have fallen down a hole

? _
```

3.4. Enable POP3 via /etc/inetd.conf and restarting the daemon

The daemon is now running on port 110 (nmap localhot).



```
root@Bry021:/etc# cat inetd.conf | grep pop3
pop3    stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/popa3d
root@Bry021:/etc# ./rc.d/rc.inetd restart
Starting Internet super-server daemon:  /usr/sbin/inetd
root@Bry021:/etc# nmap localhost

Starting Nmap 5.51 ( http://nmap.org ) at 2017-11-02 16:02 GMT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
110/tcp open  pop3
113/tcp open  auth
587/tcp open  submission

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
root@Bry021:/etc# _
```

3.5. POP3 session from the Virtual Machine.

See next page. Notice how to use the commands USER, PASS, LIST, RETR, DELE.

3.6. What ports are used by SMTP and POP3?

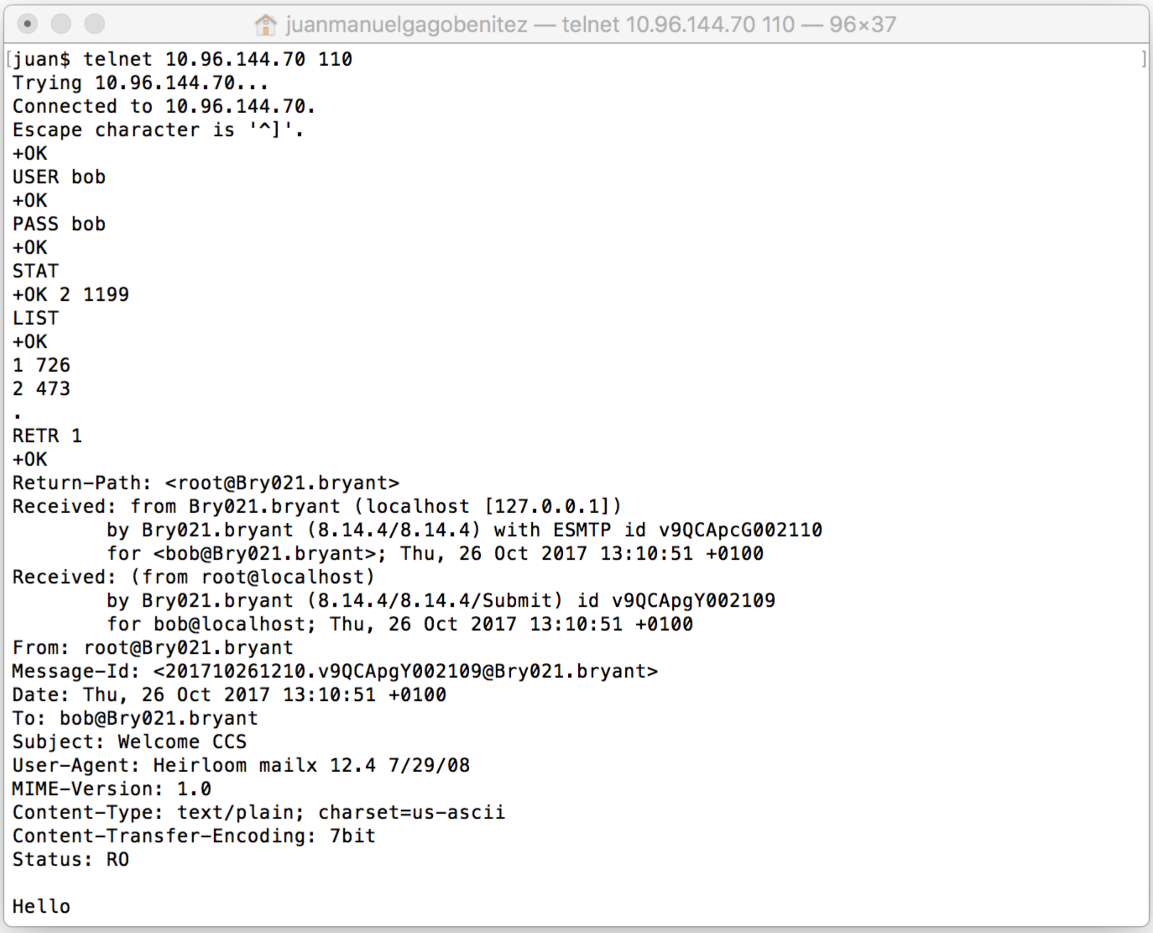
SMTP (25) and POP3 (110)

* SMTP is used when email is delivered from an email client to an email server or when email is delivered from one email server to another.

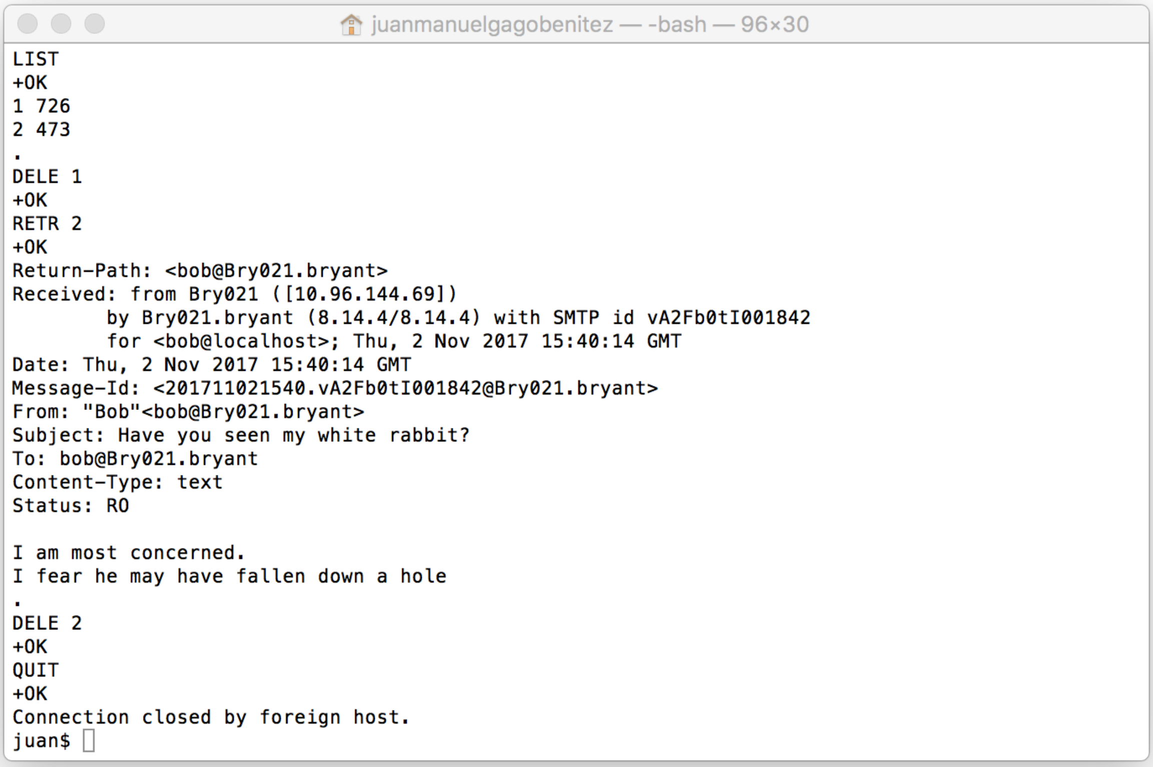
* POP3 allows an email client to download an email from an email server. The POP3 protocol is simple and does not offer many features except for download. Its design assumes that the email client downloads all available email from the server, deletes them from the server and then disconnects.

More info at https://www.hmailserver.com/documentation/latest/?page=whatis_pop3imapsmtp

3.5. From your host machine, telnet to your VM on port 110. Explore talking to the server (see example of POP3 session).



```
juan$ telnet 10.96.144.70 110
Trying 10.96.144.70...
Connected to 10.96.144.70.
Escape character is '^]'.
+OK
USER bob
+OK
PASS bob
+OK
STAT
+OK 2 1199
LIST
+OK
1 726
2 473
.
RETR 1
+OK
Return-Path: <root@Bry021.bryant>
Received: from Bry021.bryant (localhost [127.0.0.1])
        by Bry021.bryant (8.14.4/8.14.4) with ESMTP id v9QCApcG002110
        for <bob@Bry021.bryant>; Thu, 26 Oct 2017 13:10:51 +0100
Received: (from root@localhost)
        by Bry021.bryant (8.14.4/8.14.4/Submit) id v9QCApgY002109
        for bob@localhost; Thu, 26 Oct 2017 13:10:51 +0100
From: root@Bry021.bryant
Message-Id: <201710261210.v9QCApgY002109@Bry021.bryant>
Date: Thu, 26 Oct 2017 13:10:51 +0100
To: bob@Bry021.bryant
Subject: Welcome CCS
User-Agent: Heirloom mailx 12.4 7/29/08
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Status: RO

Hello
```



```
LIST
+OK
1 726
2 473
.
DELE 1
+OK
RETR 2
+OK
Return-Path: <bob@Bry021.bryant>
Received: from Bry021 ([10.96.144.69])
        by Bry021.bryant (8.14.4/8.14.4) with SMTP id vA2Fb0tI001842
        for <bob@localhost>; Thu, 2 Nov 2017 15:40:14 GMT
Date: Thu, 2 Nov 2017 15:40:14 GMT
Message-Id: <201711021540.vA2Fb0tI001842@Bry021.bryant>
From: "Bob"<bob@Bry021.bryant>
Subject: Have you seen my white rabbit?
To: bob@Bry021.bryant
Content-Type: text
Status: RO

I am most concerned.
I fear he may have fallen down a hole
.
DELE 2
+OK
QUIT
+OK
Connection closed by foreign host.
juan$
```

Exercise 4. Optional

4.1. What is IMAP? List the difference between POP3 and IMAP.

* IMAP allows users to store their email on remote servers. This two-way protocol also allows the user to synchronise their email among multiple devices, which is extremely important today, when most people have at least two devices - their laptop and smartphone.

* Conversely POP is a much simpler protocol that only allows downloading messages from your Inbox to your local computer. Generally, once transferred, the email is on your local computer and removed from FastMail.

4.2. What is PGP encryption? How does it work?

In addition to encrypting and decrypting email, PGP is used to sign messages so that the receiver can verify both the identity of the sender and the integrity of the content. PGP uses a private key that must be kept secret and a public key that sender and receiver must share. The technology is also known as GnuPG (Privacy Guard), which is a fully compatible GPL-licensed alternative.

https://support.kraken.com/hc/en-us/articles/201648223-What-is-PGP-encryption-