```
                                    CIA Lab Assignment:
                                Mail Transfer Agents (2)
```

Team:

Name	MTA	server	IP
Shahrukh (foix)	Exim	foix.prac.os3.nl	145.100.104.110
Adrien (brest)	Sendmail	brest.prac.os3.nl	145.100.104.106
Kotaiba (bristol)	Postfix	bristol.prac.os3.nl	145.100.104.163

Our Team Loop is:

Kotaiba —> Shahrukh —> Adrien —> Kotaiba

Question 1. Now send an email to the loop using your own email address and show what happens on your MTA (logs, error message)

First we need to creat a file /etc/aliases and add the following:

```
loop:           loop@foix.prac.os3.nl
```

Now, restart postfix and load new aliases

```
kotaiba@bristol:~$ sudo postmap /etc/postfix/virtual
kotaiba@bristol:~$ sudo newaliases
kotaiba@bristol:~$ sudo service postfix reload
kotaiba@bristol:~$ sudo postfix reload
```

I sent an email using my os3 mail to loop@bristol.prac.os3.nl and these are the logs:

My os3 mail (SquirrelMail replied)

```
This is the mail system at host bristol.prac.os3.nl.

I'm sorry to have to inform you that your message could not
be delivered to one or more recipients. It's attached below.

For further assistance, please send mail to postmaster.

If you do so, please include this problem report. You can
delete your own text from the attached returned message.

                   The mail system

<loop@bristol.prac.os3.nl>: mail forwarding loop for
loop@bristol.prac.os3.nl
```

Mail.log file

```
Oct 10 13:42:16 bristol postfix/smtpd[24673]: connect from
```

```
mail.serv.os3.nl[145.100.96.25]
Oct 10 13:42:16 bristol postfix/smtpd[24673]: warning: support for
restriction "check_relay_domains" will be removed from Postfix; use
"reject_unauth_destination" instead
Oct 10 13:42:16 bristol postfix/smtpd[24673]: 3FFA0520CC7:
client=mail.serv.os3.nl[145.100.96.25]
Oct 10 13:42:16 bristol postfix/cleanup[24677]: 3FFA0520CC7: message-
id=<61dc8c67cb4a61cff5b926992e7c95ae.squirrel@webmail.os3.nl>
Oct 10 13:42:16 bristol postfix/smtpd[24673]: disconnect from
mail.serv.os3.nl[145.100.96.25] ehlo=1 mail=1 rcpt=1 data=1 quit=1
commands=5
Oct 10 13:42:16 bristol postfix/qmgr[22007]: 3FFA0520CC7:
from=<kalachkar@os3.nl>, size=987, nrcpt=1 (queue active)
Oct 10 13:42:16 bristol postfix/cleanup[24677]: 41DDC520DE7: message-
id=<61dc8c67cb4a61cff5b926992e7c95ae.squirrel@webmail.os3.nl>
Oct 10 13:42:16 bristol postfix/local[24678]: 3FFA0520CC7:
to=<loop@bristol.prac.os3.nl>, relay=local, delay=0.01, delays=0.01/0/0/0,
dsn=2.0.0, status=sent (forwarded as 41DDC520DE7)
Oct 10 13:42:16 bristol postfix/qmgr[22007]: 41DDC520DE7:
from=<kalachkar@os3.nl>, size=1128, nrcpt=1 (queue active)
Oct 10 13:42:16 bristol postfix/qmgr[22007]: 3FFA0520CC7: removed
Oct 10 13:42:17 bristol postfix/smtp[24679]: 41DDC520DE7:
to=<loop@foix.prac.os3.nl>, orig_to=<loop@bristol.prac.os3.nl>,
relay=mail.foix.prac.os3.nl[145.100.104.110]:25, delay=1.5,
delays=0/0/1.4/0.1, dsn=2.0.0, status=sent (250 OK id=1e1svR-0005b1-Nu)
Oct 10 13:42:17 bristol postfix/qmgr[22007]: 41DDC520DE7: removed
Oct 10 13:42:18 bristol postfix/smtpd[24673]: connect from
brest.studlab.os3.nl[145.100.104.106]
Oct 10 13:42:18 bristol postfix/smtpd[24673]: C360E520CC7:
client=brest.studlab.os3.nl[145.100.104.106]
Oct 10 13:42:18 bristol postfix/cleanup[24677]: C360E520CC7: message-
id=<61dc8c67cb4a61cff5b926992e7c95ae.squirrel@webmail.os3.nl>
Oct 10 13:42:18 bristol postfix/qmgr[22007]: C360E520CC7:
from=<kalachkar@os3.nl>, size=1797, nrcpt=1 (queue active)
Oct 10 13:42:18 bristol postfix/local[24678]: C360E520CC7:
to=<loop@bristol.prac.os3.nl>, relay=local, delay=0.01, delays=0/0/0/0.01,
dsn=5.4.6, status=bounced (mail forwarding loop for
loop@bristol.prac.os3.nl)
Oct 10 13:42:18 bristol postfix/cleanup[24677]: C5C52520E29: message-
id=<20171010114218.C5C52520E29@bristol.prac.os3.nl>
Oct 10 13:42:18 bristol postfix/qmgr[22007]: C5C52520E29: from=<>,
size=3766, nrcpt=1 (queue active)
Oct 10 13:42:18 bristol postfix/bounce[24680]: C360E520CC7: sender non-
delivery notification: C5C52520E29
Oct 10 13:42:18 bristol postfix/qmgr[22007]: C360E520CC7: removed
Oct 10 13:42:18 bristol postfix/smtpd[24673]: disconnect from
brest.studlab.os3.nl[145.100.104.106] ehlo=1 mail=1 rcpt=1 data=1 quit=1
commands=5
Oct 10 13:42:18 bristol postfix/smtp[24681]: C5C52520E29:
to=<kalachkar@os3.nl>, relay=smtp.os3.nl[145.100.96.119]:25, delay=0.08,
delays=0/0/0/0.07, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as
```

```
D6DB917AA0E)
Oct 10 13:42:18 bristol postfix/qmgr[22007]: C5C52520E29: removed
```

When Shahrukh tried to send an email to hist loop@foix.prac.os3.nl:

```
---------- Forwarded message ----------
From: Mail Delivery System <MAILER-DAEMON@bristol.prac.os3.nl>
Date: 2017-10-09 15:16 GMT+02:00
Subject: Undelivered Mail Returned to Sender
To: s.zaidi94@gmail.com


This is the mail system at host bristol.prac.os3.nl.

I'm sorry to have to inform you that your message could not
be delivered to one or more recipients. It's attached below.

For further assistance, please send mail to postmaster.

If you do so, please include this problem report. You can
delete your own text from the attached returned message.

                   The mail system

<loop@bristol.prac.os3.nl>: mail forwarding loop for
loop@bristol.prac.os3.nl

Final-Recipient: rfc822; loop@bristol.prac.os3.nl
Original-Recipient: rfc822;loop@bristol.prac.os3.nl
Action: failed
Status: 5.4.6
Diagnostic-Code: X-Postfix; mail forwarding loop for
loop@bristol.prac.os3.nl


---------- Doorgestuurd bericht ----------
From: Shahrukh Zaidi <s.zaidi94@gmail.com>
To: loop@foix.prac.os3.nl
Cc:
Bcc:
Date: Mon, 9 Oct 2017 15:16:43 +0200
Subject: Loop test 3
Loop test 3
```

Question 2. Can you change the behavior of your MTA in response to this loop?

Yes, we can. According to the Sources “hopcount_limit (default: 50) The maximal number of Received: message headers that is allowed in the primary message headers. A message that exceeds the limit is bounced, in order to stop a mailer loop.”

And

“prepend_delivered_header (default: command, file, forward) The message delivery contexts where the Postfix local(8) delivery agent prepends a Delivered-To: message header with the address that the mail was delivered to. This information is used for mail delivery loop detection. Specify zero or more of forward, file, or command.”

I add in the main.c file:

```
#loop detection MTA2
prepend_delivered_header = forward
hopcount_limit = 999
```

Now, we check log file again after another try:

```
Oct 10 14:07:54 bristol postfix/smtpd[24932]: connect from
mail.serv.os3.nl[145.100.96.25]
Oct 10 14:07:54 bristol postfix/smtpd[24932]: 12D99520D5B:
client=mail.serv.os3.nl[145.100.96.25]
Oct 10 14:07:54 bristol postfix/cleanup[24936]: 12D99520D5B: message-
id=<be2ff461ba48e560018abf251bdf3d55.squirrel@webmail.os3.nl>
Oct 10 14:07:54 bristol postfix/qmgr[24809]: 12D99520D5B:
from=<kalachkar@os3.nl>, size=981, nrcpt=1 (queue active)
Oct 10 14:07:54 bristol postfix/smtpd[24932]: disconnect from
mail.serv.os3.nl[145.100.96.25] ehlo=1 mail=1 rcpt=1 data=1 quit=1
commands=5
Oct 10 14:07:54 bristol postfix/cleanup[24936]: 14045520DE7: message-
id=<be2ff461ba48e560018abf251bdf3d55.squirrel@webmail.os3.nl>
Oct 10 14:07:54 bristol postfix/local[24937]: 12D99520D5B:
to=<loop@bristol.prac.os3.nl>, relay=local, delay=0.01, delays=0/0/0/0,
dsn=2.0.0, status=sent (forwarded as 14045520DE7)
Oct 10 14:07:54 bristol postfix/qmgr[24809]: 14045520DE7:
from=<kalachkar@os3.nl>, size=1122, nrcpt=1 (queue active)
Oct 10 14:07:54 bristol postfix/qmgr[24809]: 12D99520D5B: removed
Oct 10 14:07:54 bristol postfix/smtp[24938]: 14045520DE7:
to=<loop@foix.prac.os3.nl>, orig_to=<loop@bristol.prac.os3.nl>,
relay=mail.foix.prac.os3.nl[145.100.104.110]:25, delay=0.08,
delays=0/0/0.01/0.07, dsn=2.0.0, status=sent (250 OK id=1e1tKE-0005bS-30)
Oct 10 14:07:54 bristol postfix/qmgr[24809]: 14045520DE7: removed
Oct 10 14:07:54 bristol postfix/smtpd[24932]: connect from
brest.studlab.os3.nl[145.100.104.106]
Oct 10 14:07:54 bristol postfix/smtpd[24932]: 648ED520D5B:
client=brest.studlab.os3.nl[145.100.104.106]
Oct 10 14:07:54 bristol postfix/cleanup[24936]: 648ED520D5B: message-
id=<be2ff461ba48e560018abf251bdf3d55.squirrel@webmail.os3.nl>
Oct 10 14:07:54 bristol postfix/qmgr[24809]: 648ED520D5B:
from=<kalachkar@os3.nl>, size=1791, nrcpt=1 (queue active)
Oct 10 14:07:54 bristol postfix/local[24937]: 648ED520D5B:
to=<loop@bristol.prac.os3.nl>, relay=local, delay=0.01, delays=0.01/0/0/0,
dsn=5.4.6, status=bounced (mail forwarding loop for
loop@bristol.prac.os3.nl)
Oct 10 14:07:54 bristol postfix/cleanup[24936]: 662F8520E29: message-
id=<20171010120754.662F8520E29@bristol.prac.os3.nl>
```

```
Oct 10 14:07:54 bristol postfix/bounce[24939]: 648ED520D5B: sender non-
delivery notification: 662F8520E29
Oct 10 14:07:54 bristol postfix/qmgr[24809]: 662F8520E29: from=<>,
size=3760, nrcpt=1 (queue active)
Oct 10 14:07:54 bristol postfix/qmgr[24809]: 648ED520D5B: removed
Oct 10 14:07:54 bristol postfix/smtp[24940]: 662F8520E29:
to=<kalachkar@os3.nl>, relay=smtp.os3.nl[145.100.96.119]:25, delay=0.01,
delays=0/0/0/0, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 67D9617AA0A)
Oct 10 14:07:54 bristol postfix/qmgr[24809]: 662F8520E29: removed
Oct 10 14:07:54 bristol postfix/smtpd[24932]: disconnect from
brest.studlab.os3.nl[145.100.104.106] ehlo=1 mail=1 rcpt=1 data=1 quit=1
commands=5
```

Source:

1- https://doxfer.webmin.com/Webmin/Postfix_Mail_Server

2- http://www.postfix.org/postconf.5.html#prepend_delivered_header

3- http://www.postfix.org/postconf.5.html#prepend_delivered_header

Question 3.

(a) Create a new subdomain within your domain and add an MX entry to it.

In my bristol.prac.os3.nl file I added:

```
sub     IN      MX      15 mail.bristol.prac.os3.nl.
sub     IN      A       145.100.104.163
```

Proof using dig:

```
kalachkar@desktop-15:~$ dig sub.bristol.prac.os3.nl MX

; <<>> DiG 9.10.3-P4-Ubuntu <<>> sub.bristol.prac.os3.nl MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56342
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sub.bristol.prac.os3.nl.   IN    MX

;; ANSWER SECTION:
sub.bristol.prac.os3.nl. 300    IN    MX    15 mail.bristol.prac.os3.nl.

;; AUTHORITY SECTION:
bristol.prac.os3.nl.    290    IN    NS    ns1.bristol.prac.os3.nl.

;; ADDITIONAL SECTION:
```

```
mail.bristol.prac.os3.nl. 290   IN    A    145.100.104.163
ns1.bristol.prac.os3.nl. 290    IN    A    145.100.104.163
mail.bristol.prac.os3.nl. 290   IN    AAAA
2001:610:158:1046:145:100:104:163
ns1.bristol.prac.os3.nl. 290    IN    AAAA
2001:610:158:1046:145:100:104:163

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Oct 10 15:11:57 CEST 2017
;; MSG SIZE  rcvd: 179
```

(b) Then extend your MTA configuration to handle virtual domains, and have it also handle the email for the newly created domain.

According to the source:

First, we add on in main.cf file:

```
virtual_alias_maps = hash:/etc/postfix/virtual
virtual_alias_domains = sub.bristol.prac.os3.nl
```

Then, in virtual file:

```
kotaiba@sub.bristol.prac.os3.nl kotaiba
```

Finally, We restart postfix server:

```
kotaiba@bristol:/usr/local/etc/nsd$ sudo postmap /etc/postfix/virtual
kotaiba@bristol:/usr/local/etc/nsd$  sudo postfix stop
postfix/postfix-script: stopping the Postfix mail system
kotaiba@bristol:/usr/local/etc/nsd$ sudo postfix start
postfix/postfix-script: starting the Postfix mail system
```

Source:

1- http://www.postfix.org/VIRTUAL_README.html

© Show how you test this.

First, I will send the mail from my os3 mail:

Mail.log file:

```
Oct 10 15:23:12 bristol postfix/smtpd[25585]: connect from
mail.serv.os3.nl[145.100.96.25]
Oct 10 15:23:12 bristol postfix/trivial-rewrite[25588]: warning: do not list
domain sub.bristol.prac.os3.nl in BOTH virtual_alias_domains and
relay_domains
Oct 10 15:23:12 bristol postfix/smtpd[25585]: warning: support for
restriction "check_relay_domains" will be removed from Postfix; use
```

```
"reject_unauth_destination" instead
Oct 10 15:23:12 bristol postfix/smtpd[25585]: 513DA520D5B:
client=mail.serv.os3.nl[145.100.96.25]
Oct 10 15:23:12 bristol postfix/cleanup[25589]: 513DA520D5B: message-
id=<8f1aebd1bfd569af20744e60f5c34824.squirrel@webmail.os3.nl>
Oct 10 15:23:12 bristol postfix/smtpd[25585]: disconnect from
mail.serv.os3.nl[145.100.96.25] ehlo=1 mail=1 rcpt=1 data=1 quit=1
commands=5
Oct 10 15:23:12 bristol postfix/qmgr[25582]: 513DA520D5B:
from=<kalachkar@os3.nl>, size=1019, nrcpt=1 (queue active)
Oct 10 15:23:12 bristol postfix/local[25590]: 513DA520D5B:
to=<kotaiba@bristol.prac.os3.nl>, orig_to=<kotaiba@sub.bristol.prac.os3.nl>,
relay=local, delay=0.01, delays=0.01/0/0/0, dsn=2.0.0, status=sent
(delivered to maildir)
Oct 10 15:23:12 bristol postfix/qmgr[25582]: 513DA520D5B: removed
```

And I received the mail successfully:

```
Return-Path: <kalachkar@os3.nl>
X-Original-To: kotaiba@sub.bristol.prac.os3.nl
Received: from mail.serv.os3.nl (mail.serv.os3.nl [145.100.96.25])
    by bristol.prac.os3.nl (Postfix) with ESMTP id 513DA520D5B
    for <kotaiba@sub.bristol.prac.os3.nl>; Tue, 10 Oct 2017 15:23:12 +0200
(CEST)
Received: from webmail.os3.nl (mail.serv.os3.nl [IPv6:2001:610:158:960::25])
    by mail.serv.os3.nl (Postfix) with ESMTP id 3E24A17AA86
    for <kotaiba@sub.bristol.prac.os3.nl>; Tue, 10 Oct 2017 15:23:12 +0200
(CEST)
Received: from 2001:610:158:1023:f93e:2af9:c9d3:6486
        (SquirrelMail authenticated user kalachkar)
        by webmail.os3.nl with HTTP;
        Tue, 10 Oct 2017 15:23:12 +0200
Message-ID: <8f1aebd1bfd569af20744e60f5c34824.squirrel@webmail.os3.nl>
Date: Tue, 10 Oct 2017 15:23:12 +0200
Subject: Sub tesst
From: kalachkar@os3.nl
To: kotaiba@sub.bristol.prac.os3.nl
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

echo "Sub tesst" mail -s "Sub email"
```

Question 4.

(a) Write a small paragraph that highlights the advantages and disadvantages of SPF and DomainKeys Identified Mail (DKIM).

Sender Policy Framework (SPF): The aim behind it is that senders could specify, via an SPF record published in DNS, what servers were allowed to send email for a particular domain. e.g. only servers foix, brest & ipswitch are allowed to send email for @os3.cnl addresses. However, SPF has many problems. First, it only works on the domain in the SMTP sending protocol, known as the MAIL FROM envelope address.

“Its main use is where to send error/bounce emails if final delivery fails.” So in real life scenario where what the recipient can be anything, there’s no need for the MAIL FROM address to match the From header address in any way. So effectively, the only thing we’re protecting against is the spoofing of an email address no one ever sees.

So In theory, this does help to address one particular type of spam. What you see when messages spammers sent pretending to be you can't be delivered.

In practice, it would only do that if people actually blocked email that failed SPF checks at SMTP time.

The records below are in typical DNS syntax:

```
example.com. IN TXT "v=spf1 ip4:192.0.2.0/24 ip4:198.51.100.123 a -all"
```

“v=” defines the version of SPF used. The following words provide mechanisms to use to determine if a domain is eligible to send mail. The “ip4” and “a” specify the systems permitted to send messages for the given domain. The “-all” at the end specifies that, if the previous mechanisms did not match, the message should be rejected.

DKIM (DomainKeys Identified Mail): is an email authentication method designed to detect email spoofing. It allows the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain. It is intended to prevent forged sender addresses in emails, a technique often used in phishing and email spam.

It allows a particular domain owner (again, via a record published in DNS) to cryptographically sign parts of a message so that a receiver can validate that they haven’t been altered. DKIM is now commonly used. “80% of email delivered to FastMail.com is DKIM signed.”

In practice, DKIM lets a domain associate its name with an email message by affixing a digital signature to it.

Verification is carried out using the signer's public key published in the DNS. A valid signature guarantees that parts of the email have not been modified since the signature was affixed. Usually, DKIM signatures are not visible to end-users, and are affixed or verified by the infrastructure rather than message's authors and recipients. In that respect, DKIM differs from end-to-end digital signatures.

Disadvantages:

Authentication has a few minor drawbacks worth noting. These are relatively minor and only occur in edge cases, but for full disclosure – here are the downsides:

For example, given the signature

```
DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=brisbane;
```

```
    c=relaxed/simple; q=dns/txt; l=1234; t=1117574938; x=1118006938;
    h=from:to:subject:date:keywords:keywords;
    bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
    b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
            VoG4ZHRNiYzR
```

Sources:

1- https://support.google.com/a/answer/33786?hl=en

2- https://blog.fastmail.com/2016/12/24/spf-dkim-dmarc/

3- https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail

4- http://3.bp.blogspot.com/-Sjhz8nkHz-s/U0yIQy08QSI/AAAAAAAAAS0/pwGHrnp99EU/s1600/SPF.png

5- http://2.bp.blogspot.com/-eQ123eQEqB4/U0yIgEIXf_I/AAAAAAAAAS8/Kbwz5xMrP4Q/s1600/DomainKeys_Identified_Mail_(DKIM).png

(b) What would you choose at a first glance and why?

I prefer DKIM since it verify that the messages' content are trustworthy, meaning that they weren't changed from the moment the message left the initial mail server. Which achieved using standard public/private key signing process.

© Configure your system to support one of the two. Your system must support it for both sending and receiving email. You might need additional software packages or patches.

I follow a tutorial to install DKIM.

install:

```
kotaiba@bristol:~$ sudo apt-get install opendkim opendkim-tools
```

Add user postfix to the opendkim group so that Postfix can access OpenDKIM’s socket when it needs to:

```
kotaiba@bristol:~$ sudo adduser postfix opendkim
```

Now, lets start installing and configuring:

Ensure that file permissions are set correctly:

```
kotaiba@bristol:~$ sudo chmod u=rw,go=r /etc/opendkim.conf
```

Create the directories to hold OpenDKIM’s data files, assign ownership to the opendkim user, and restrict the file permissions:

```
root@bristol:~# mkdir /etc/opendkim
```

```
root@bristol:~# mkdir /etc/opendkim/keys
root@bristol:~# chown -R opendkim:opendkim /etc/opendkim
root@bristol:~# chmod go-rw /etc/opendkim/keys
```

Create the signing table /etc/opendkim/signing.table. It needs to have one line per domain that you handle email for. Each line should look like this

```
root@bristol:~# touch /etc/opendkim/signing.table
root@bristol:~# nano /etc/opendkim/signing.table
```

/etc/opendkim/signing

```
*@bristol.prac.os3.nl   bristol
```

Then, Create the key table /etc/opendkim/key.table. It needs to have one line per short domain name in the signing table.

```
root@bristol:~# touch /etc/opendkim/key.table
root@bristol:~# nano /etc/opendkim/key.table
```

/etc/opendkim/key.table:

```
bristol     bristol.prac.os3.nl:201710:/etc/opendkim/keys/bristol.private
```

Then, Create the trusted hosts file /etc/opendkim/trusted.hosts. Its contents need to be:

```
root@bristol:~# touch /etc/opendkim/trusted.hosts
root@bristol:~# nano /etc/opendkim/trusted.host
```

/etc/opendkim/trusted.hosts:

```
127.0.0.1
::1
localhost
bristol
bristol.bristol.prac.os3.nl
bristol.prac.os3.nl
```

Then, Make sure the ownership and permissions on /etc/opendkim and it’s contents are correct

```
root@bristol:~# chown -R opendkim:opendkim /etc/opendkim
root@bristol:~# chmod -R go-rwx /etc/opendkim/keys
```

Generate keys for each domain:

```
root@bristol:~# opendkim-genkey -b 2048 -h rsa-sha256 -r -s 201710 -d
bristol.prac.os3.nl -v

opendkim-genkey: generating private key
opendkim-genkey: private key written to 201710.private
```

```
opendkim-genkey: extracting public key
opendkim-genkey: DNS TXT record written to 201710.txt

root@bristol:~# mv 201710.txt /etc/opendkim/keys/bristol.txt
root@bristol:~# mv 201710.private /etc/opendkim/keys/bristol.private
```

Make sure the ownership, permissions and contents on /etc/opendkim are correct by running the following commands:

```
root@bristol:~# cd /etc
root@bristol:/etc# chown -R opendkim:opendkim /etc/opendkim
root@bristol:/etc# chmod -R go-rw /etc/opendkim/keys
```

Now, Restart:

```
root@bristol:/etc# systemctl restart opendkim
```

and the Configuration file look like this /etc/opendkim.conf:

```
# This is a basic configuration that can easily be adapted to suit a
standard
# installation. For more advanced options, see opendkim.conf(5) and/or
# /usr/share/doc/opendkim/examples/opendkim.conf.sample.

# Log to syslog
Syslog          yes
# Required to use local socket with MTAs that access the socket as a non-
# privileged user (e.g. Postfix)
UMask           002
# OpenDKIM user
# Remember to add user postfix to group opendkim
UserID          opendkim

# Map domains in From addresses to keys used to sign messages
KeyTable        /etc/opendkim/key.table
SigningTable        refile:/etc/opendkim/signing.table

# Hosts to ignore when verifying signatures
ExternalIgnoreList  /etc/opendkim/trusted.hosts
InternalHosts       /etc/opendkim/trusted.hosts

# Commonly-used options; the commented-out versions show the defaults.
Canonicalization    relaxed/simple
Mode            sv
SubDomains      no
#ADSPAction     continue
AutoRestart     yes
AutoRestartRate     10/1M
Background      yes
DNSTimeout      5
SignatureAlgorithm  rsa-sha256
```

```
# Always oversign From (sign using actual From and a null From to prevent
# malicious signatures header fields (From and/or others) between the signer
# and the verifier.  From is oversigned by default in the Debian package
# because it is often the identity key used by reputation systems and thus
# somewhat security sensitive.
OversignHeaders     From
```

Note in this I get Kenneth help

We add now in /etc/postfix/main.cf:

```
# Milter configuration
# OpenDKIM
milter_default_action = accept
# Postfix  ^   2.6 milter_protocol = 6, Postfix  ^   2.5 milter_protocol = 2
milter_protocol = 6
smtpd_milters = inet:localhost:8891
non_smtpd_milters = inet:localhost:8891
#
```

and in bristol.prac.os3.nl zone file we add:

```
;DKIM records
201710._domainkey   IN    TXT    ( "v=DKIM1; k=rsa-sha256; s=email; "
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0ySql41pk2fMBeKC+JVdxMcq80rc8
pn76B/HYi4yMYt6fYIvB5iwpYaiLfCJ6t7hl7aP9zgSNQtPY0zLIRp7+EbjP5qQ07NRvnXNvqVmo
5PX0IwqFlunOJNWqrKImC3K9k9sr2oax1Yc6VCfk1hbZ2YtX/YVC1DH0Bp0A9O3J+2taCmcMe3hR
KsbaR9yqSTUhdKQfgMjBESFV3"
"znqBfgnrQ4V5fywDeOldz/yirj3KktcoDyksdifbndqSmbU/64rcK5xmP60wXj3FnW05B4Bs0H9
LnURngO9py35Z5NQXXEhRAG/KJkMgS3i1Fa9hvWjjew+D2zUq4Vcu5Yj1oHjQIDAQAB" )  ; --
--- DKIM key 201710 for bristol.prac.os3.nl
```

Test:

```
kalachkar@desktop-15:~$ dig TXT 201710._domainkey.bristol.prac.os3.nl
@bristol.prac.os3.nl

; <<>> DiG 9.10.3-P4-Ubuntu <<>> TXT 201710._domainkey.bristol.prac.os3.nl
@bristol.prac.os3.nl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55709
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;201710._domainkey.bristol.prac.os3.nl. IN TXT

;; ANSWER SECTION:
```

```
201710._domainkey.bristol.prac.os3.nl. 300 IN TXT "v=DKIM1; k=rsa-sha256;
s=email; "
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0ySql41pk2fMBeKC+JVdxMcq80rc8
pn76B/HYi4yMYt6fYIvB5iwpYaiLfCJ6t7hl7aP9zgSNQtPY0zLIRp7+EbjP5qQ07NRvnXNvqVmo
5PX0IwqFlunOJNWqrKImC3K9k9sr2oax1Yc6VCfk1hbZ2YtX/YVC1DH0Bp0A9O3J+2taCmcMe3hR
KsbaR9yqSTUhdKQfgMjBESFV3"
"znqBfgnrQ4V5fywDeOldz/yirj3KktcoDyksdifbndqSmbU/64rcK5xmP60wXj3FnW05B4Bs0H9
LnURngO9py35Z5NQXXEhRAG/KJkMgS3i1Fa9hvWjjew+D2zUq4Vcu5Yj1oHjQIDAQAB"

;; AUTHORITY SECTION:
bristol.prac.os3.nl.    300    IN    NS    ns1.bristol.prac.os3.nl.

;; ADDITIONAL SECTION:
ns1.bristol.prac.os3.nl. 300    IN    A    145.100.104.163
ns1.bristol.prac.os3.nl. 300    IN    AAAA
2001:610:158:1046:145:100:104:163

;; Query time: 0 msec
;; SERVER: 145.100.104.163#53(145.100.104.163)
;; WHEN: Fri Oct 13 13:28:10 CEST 2017
;; MSG SIZE  rcvd: 569
```

IT IS WORKING :D NOW, THANK YOU MICK .

.

.

.

FORGET THE SPF STUFF PLZ

I will configure my system to use SPF following a good tutorial:

Now, Let's Try to install SPF :D :

install

```
kotaiba@bristol:~$ sudo apt-get install postfix-policyd-spf-python
```

Then I need to add to my zone file the SPF record:

This means Allow mail from all hosts listed in the MX records for the domain

```
@       IN      TXT     "v=spf1 a mx -all"
```

Edit /etc/postfix/master.cf and add the following to /etc/postfix/master.cf :

```
policyd-spf  unix  -       n       n       -       0       spawn
    user=policyd-spf argv=/usr/bin/policyd-spf
```

Now, add to the /etc/postfix/main.cf file entry to increase the Postfix policy agent timeout, which will

prevent Postfix from aborting the agent if transactions run a bit slowly:

```
policyd-spf_time_limit = 3600
```

Now, in the smtpd_recipient_restrictions entry to add a check_policy_service entry:

in /etc/postfix/main.cf file

```
smtpd_recipient_restrictions = permit_mynetworks
        permit_sasl_authenticated
        check_relay_domains
        reject_unauth_destination
        check_policy_service unix:private/policyd-spf
```

Restart Postfix:

```
kotaiba@bristol:~$ systemctl restart postfix
```

Finally, All the mails that are send from an domain names that not included in my MX records, will be blocked and a bounce-message will be sent.

Source:

1- https://www.linode.com/docs/email/postfix/configure-spf-and-dkim-in-postfix-on-debian-8

(d) Provide full email/MTA headers to prove that SPF/DKIM were implemented correctly on your system (sending and receiving).

DKIM sending check:

I will send email from my kotaiba@bristol.prac.os3.nl to 2qvwmudyvkuuy6@dkimvalidator.com in order to use their online service to check my configuration DKIM validity using this online tool (http://dkimvalidator.com/results).

```
DKIM Information:

DKIM Signature


Message contains this DKIM Signature:
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=bristol.prac.os3.nl;
    s=201710; t=1507897376;
    bh=/TuudOnf4TBMM08eOQp5RBFYL/r3gvrjV3E2zxbTGrE=;
    h=Date:From:To:Subject:From;
    b=Z//6h4A1LaulYufhZodICFfnAWzG8419/TBU33Mo59VHCPgEkqylCu4GLeIvt8AZp
     ujKT4kXWhAiDsr5oth8pguoa96NVBbuda8i0s8cqYql2VFHF5AaQgb0m2n8MB8IgEV
     CwivH+CjNSRY+TGJz3l6Y9HisplNOcS/ZBu1kdOgm/eGeiY98gVZb7YYKl069P4yaC
     MpB4R9vUgO6f76/xI/WVX6XGx2W6PkrtVxXq/i4q30q2QkVKeySLtFU7a1lIBlZeJM
     a84S5KlzK8mPw/2dgF5RS1lbnTIuLR4E6YQRRKRIWwqaJZrtAtmIbW2tSCrXgUZ2KH
     0F9uNmV4RGroQ==
```

```
Signature Information:
v= Version:         1
a= Algorithm:       rsa-sha256
c= Method:          relaxed/simple
d= Domain:          bristol.prac.os3.nl
s= Selector:        201710
q= Protocol:
bh=                 /TuudOnf4TBMM08eOQp5RBFYL/r3gvrjV3E2zxbTGrE=
h= Signed Headers:  Date:From:To:Subject:From
b= Data:
Z//6h4A1LaulYufhZodICFfnAWzG8419/TBU33Mo59VHCPgEkqylCu4GLeIvt8AZp
     ujKT4kXWhAiDsr5oth8pguoa96NVBbuda8i0s8cqYql2VFHF5AaQgb0m2n8MB8IgEV
     CwivH+CjNSRY+TGJz3l6Y9HisplNOcS/ZBu1kdOgm/eGeiY98gVZb7YYKl069P4yaC
     MpB4R9vUgO6f76/xI/WVX6XGx2W6PkrtVxXq/i4q30q2QkVKeySLtFU7a1lIBlZeJM
     a84S5KlzK8mPw/2dgF5RS1lbnTIuLR4E6YQRRKRIWwqaJZrtAtmIbW2tSCrXgUZ2KH
     0F9uNmV4RGroQ==
Public Key DNS Lookup


Building DNS Query for 201710._domainkey.bristol.prac.os3.nl
Retrieved this publickey from DNS: v=DKIM1; k=rsa-sha256; s=email;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0ySql41pk2fMBeKC+JVdxMcq80rc8p
n76B/HYi4yMYt6fYIvB5iwpYaiLfCJ6t7hl7aP9zgSNQtPY0zLIRp7+EbjP5qQ07NRvnXNvqVmo5
PX0IwqFlunOJNWqrKImC3K9k9sr2oax1Yc6VCfk1hbZ2YtX/YVC1DH0Bp0A9O3J+2taCmcMe3hRK
sbaR9yqSTUhdKQfgMjBESFV3znqBfgnrQ4V5fywDeOldz/yirj3KktcoDyksdifbndqSmbU/64rc
K5xmP60wXj3FnW05B4Bs0H9LnURngO9py35Z5NQXXEhRAG/KJkMgS3i1Fa9hvWjjew+D2zUq4Vcu
5Yj1oHjQIDAQAB
Validating Signature


result = invalid
Details: public key: unsupported key type

============================================================
Original Email
============================================================

Received: from bristol.prac.os3.nl (bristol.studlab.os3.nl
[145.100.104.163])
    by relay-4.us-west-2.relay-prod (Postfix) with ESMTP id EC63D160331
    for <2qVwMuDyVkUuY6@dkimvalidator.com>; Fri, 13 Oct 2017 12:22:56 +0000
(UTC)
Received: by bristol.prac.os3.nl (Postfix, from userid 1000)
    id 3B7D8520F1B; Fri, 13 Oct 2017 14:22:56 +0200 (CEST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=bristol.prac.os3.nl;
    s=201710; t=1507897376;
    bh=/TuudOnf4TBMM08eOQp5RBFYL/r3gvrjV3E2zxbTGrE=;
    h=Date:From:To:Subject:From;
    b=Z//6h4A1LaulYufhZodICFfnAWzG8419/TBU33Mo59VHCPgEkqylCu4GLeIvt8AZp
     ujKT4kXWhAiDsr5oth8pguoa96NVBbuda8i0s8cqYql2VFHF5AaQgb0m2n8MB8IgEV
     CwivH+CjNSRY+TGJz3l6Y9HisplNOcS/ZBu1kdOgm/eGeiY98gVZb7YYKl069P4yaC
```

```
     MpB4R9vUgO6f76/xI/WVX6XGx2W6PkrtVxXq/i4q30q2QkVKeySLtFU7a1lIBlZeJM
     a84S5KlzK8mPw/2dgF5RS1lbnTIuLR4E6YQRRKRIWwqaJZrtAtmIbW2tSCrXgUZ2KH
     0F9uNmV4RGroQ==
Date: Fri, 13 Oct 2017 14:22:56 +0200
From: kotaiba <kotaiba@bristol.prac.os3.nl>
To: 2qVwMuDyVkUuY6@dkimvalidator.com
Subject: k
Message-ID: <20171013122256.GA1096@bristol.prac.os3.nl>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Disposition: inline
User-Agent: Mutt/1.5.24 (2015-08-30)

k
```

As we see above “DKIM check: pass”

Since the sending test is worked. Now, lets check for receiving:

I will use an online tool that will help me to do that (https://www.port25.com/authentication-checker/)

Mail.log:

```
Oct 13 14:28:12 bristol postfix/smtpd[1115]: connect from
mail.serv.os3.nl[145.100.96.25]
Oct 13 14:28:12 bristol postfix/smtpd[1115]: warning: support for
restriction "check_relay_domains" will be removed from Postfix; use
"reject_unauth_destination" instead
Oct 13 14:28:12 bristol postfix/smtpd[1115]: warning: restriction
`reject_unauth_destination' after `check_relay_domains' is ignored
Oct 13 14:28:12 bristol postfix/smtpd[1115]: 91B04520C31:
client=mail.serv.os3.nl[145.100.96.25]
Oct 13 14:28:12 bristol postfix/cleanup[1118]: 91B04520C31: message-
id=<5de820cacc6058dd40df35b9bd9b2f82.squirrel@webmail.os3.nl>
Oct 13 14:28:12 bristol postfix/qmgr[25582]: 91B04520C31:
from=<kalachkar@os3.nl>, size=1031, nrcpt=1 (queue active)
Oct 13 14:28:12 bristol postfix/smtpd[1115]: disconnect from
mail.serv.os3.nl[145.100.96.25] ehlo=1 mail=1 rcpt=1 data=1 quit=1
commands=5
Oct 13 14:28:12 bristol postfix/local[1119]: 91B04520C31:
to=<kotaiba@bristol.prac.os3.nl>, relay=local, delay=0.01,
delays=0.01/0/0/0, dsn=2.0.0, status=sent (delivered to maildir)
Oct 13 14:28:12 bristol postfix/qmgr[25582]: 91B04520C31: removed
```

Original mail:

```
Return-Path: <kotaiba@bristol.prac.os3.nl>
Received: from bristol.prac.os3.nl (145.100.104.163) by verifier.port25.com
id hs2p5m2bkd0l for <check-auth@verifier.port25.com>; Fri, 13 Oct
 2017 08:32:27 -0400 (envelope-from <kotaiba@bristol.prac.os3.nl>)
```

```
Authentication-Results: verifier.port25.com; spf=pass
smtp.mailfrom=kotaiba@bristol.prac.os3.nl;
 dkim=pass (matches From: kotaiba@bristol.prac.os3.nl)
header.d=bristol.prac.os3.nl
Received: by bristol.prac.os3.nl (Postfix, from userid 1000)
    id 2E67E520F1B; Fri, 13 Oct 2017 14:32:24 +0200 (CEST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=bristol.prac.os3.nl;
    s=201710; t=1507897944;
    bh=PIvxKsqRIWfk0KxweqtYayNK3Tof/BKNkwSnJe1EvME=;
    h=Date:From:To:Subject:From;
    b=YDRREAdOAZaUN3qOOmn4LdgN/LWw75ubUBV6FB/rQ46uDGDW94239FvUfxU25V1Jq
     kwjB+/FLFMccpRGWB8pUpbymK8pjhJj2VzBwLVPTOorbfnLgtiSwSiAsLOWsBBKMKr
     ilz/aQ5uN6koxALiGdQDpgaOoAQ2xwoD7iV9OA2np112StVlvXKUOvbPwU5nyqZdaq
     gfF7CeCNqEOH064zwdQfD1/+9bNhXWx2V4+ehX7MRuKoZz4dY8PfNyCxmE77elqnOk
     0rlVNIn5LueO5efDOzWgWiQXg4aQQlQrw4D4byd1xip+W9VnoU0lf2o7Dj70fmFKCo
     +scn6I65zmUfw==
Date: Fri, 13 Oct 2017 14:32:24 +0200
From: kotaiba <kotaiba@bristol.prac.os3.nl>
To: check-auth@verifier.port25.com
Subject: DKIM
Message-ID: <20171013123224.GA1131@bristol.prac.os3.nl>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Disposition: inline
User-Agent: Mutt/1.5.24 (2015-08-30)

DKIM
```

and as we see above the signature so it works. :D

Source:

1- http://www.isnotspam.com/

2- https://www.port25.com/authentication-checker/

Question 5. Investigate what generic anti-spam open source software packages are out there, choose one, download it (compile it if necessary) and configure your MTA to use it. Show that it works. Make sure that in your MTA group there are 2 different anti-spam solutions implemented!

PLEASE ALSO FORGET ABOUT MAIL SCANNER I WILL USE Spamassassin BECAUSE AFTER WORKING ON MAILSCANNER FOR 2 HOURS IT IS NOT WORKING

I will choose MailScanner:

Install:

```
kotaiba@bristol:~$ sudo wget
https://s3.amazonaws.com/msv5/release/MailScanner-5.0.6-5.deb.tar.gz
kotaiba@bristol:~$ tar -zxf MailScanner-5.0.6-5.deb.tar.gz
kotaiba@bristol:~/MailScanner-5.0.6-5$ sudo dpkg -i MailScanner-5.0.6-5-
noarch.deb
```

Then edit the /etc/Mailscanner/Mailscanner.conf:

```
Run As User = postfix
Run As Group = postfix
Incoming Queue Dir = /var/spool/postfix/hold
Outgoing Queue Dir = /var/spool/postfix/incoming
MTA = postfix
```

Then in main.cf

```
header_checks = regexp:/etc/postfix/header_checks
```

file /etc/postfix/header_checks add:

```
 /^Received:/ HOLD
```

Edit the script in /usr/sbin/MailScanner and change

Old

```
#!/usr/bin/perl -U -I /usr/local/lib/MailScanner
```

New

```
#!/usr/local/bin/perl5.26.1 -U -I /usr/local/lib/MailScanner
```

Starting MailScanner:

```
NOT WORKING :D FIX HERE
```

Now, I Will choose Spamassassin:

Install, Adding Spamassassin User , and Setting Up Spamassassin:

```
kotaiba@bristol:~$ sudo apt-get install spamassassin spamc
root@bristol:~# groupadd spamd
root@bristol:~# useradd -g spamd -s /bin/false -d /var/log/spamassassin
spamd
root@bristol:~# mkdir /var/log/spamassassin
root@bristol:~# chown spamd:spamd /var/log/spamassassin
```

Setting Up Spamassassin:

IN /etc/default/spamassassin file:

```
To enable Spamassassin we change  ENABLED=0 to ENABLED=1

To enable automatic rule updates in order to get the latest spam filtering
rules we change CRON=0 to CRON=1
```

```
we Create Variable : SAHOME="/var/log/spamassassin/"

Change option to OPTIONS="--create-prefs --max-children 2 --username spamd \
-H ${SAHOME} -s ${SAHOME}spamd.log" which will specifies the username
Spamassassin will run under as spamd, as well as add the home directory,
create the log file, and limit the child processes that Spamassassin can
run.
```

Now, Start the Spamassassin daemon by using the following code:

```
root@bristol:~# service spamassassin start
```

Now, we need to configure postfix:

in /etc/postfix/master.cf:

```
Find the the line

smtp      inet  n       -       -       -       -       smtpd

and add the following

-o content_filter=spamassassin
```

Now, Postfix will pipe the mail through Spamassassin.

To setup after-queue content filter add the following line to the end of the file

```
spamassassin unix -     n       n       -       -       pipe
        user=spamd argv=/usr/bin/spamc -f -e
        /usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

Restart postfix:

```
service postfix restart
```

Configuring Spamassassin on your VPS:

in /etc/spamassassin/local.cf file (uncomment it):

```
rewrite_header Subject [***** SPAM _SCORE_ *****]

required_score           3.0

use_bayes               1

bayes_auto_learn        1
```

restart spam assassin.

```
service spamassassin restart
```

```
</code

Test the Spammer:
<code>
Return-Path: <kalachkar@os3.nl>
X-Original-To: kotaiba@bristol.prac.os3.nl
Received: by bristol.prac.os3.nl (Postfix, from userid 1004)
    id 4F1C8521159; Fri, 13 Oct 2017 15:53:26 +0200 (CEST)
X-Spam-Checker-Version: SpamAssassin 3.4.1 (2015-04-28) on
bristol.prac.os3.nl
X-Spam-Level:
X-Spam-Status: No, score=0.0 required=3.0 tests=TVD_SPACE_RATIO
autolearn=ham
    autolearn_force=no version=3.4.1
Received: from mail.serv.os3.nl (mail.serv.os3.nl [145.100.96.25])
    by bristol.prac.os3.nl (Postfix) with ESMTP id 03847520F92
    for <kotaiba@bristol.prac.os3.nl>; Fri, 13 Oct 2017 15:53:25 +0200
(CEST)
Received: from webmail.os3.nl (mail.serv.os3.nl [IPv6:2001:610:158:960::25])
    by mail.serv.os3.nl (Postfix) with ESMTP id 27EED17A9CA
    for <kotaiba@bristol.prac.os3.nl>; Fri, 13 Oct 2017 15:53:22 +0200
(CEST)
Received: from 2001:610:158:1023:b0d2:a617:9ddc:456b
        (SquirrelMail authenticated user kalachkar)
        by webmail.os3.nl with HTTP;
        Fri, 13 Oct 2017 15:53:23 +0200
Message-ID: <62ea03b0e8703e565cf8585610748fe5.squirrel@webmail.os3.nl>
Date: Fri, 13 Oct 2017 15:53:23 +0200
Subject: gfgfgfd
From: kalachkar@os3.nl
To: kotaiba@bristol.prac.os3.nl
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

gfdgfdgf

FIX HERE
```

Again, It WORKS :D

Source:

1- https://www.mailscanner.info/postfix/

2- https://www.digitalocean.com/community/tutorials/how-to-install-and-setup-spamassassin-on-ubuntu-12-04

Question 6. Investigate these methods and add authentication to your MTA. Show that it works.

“SMTP Authentication, often abbreviated SMTP AUTH, is an extension of the Simple Mail Transfer Protocol whereby an SMTP client may log in using an authentication mechanism chosen among those supported by the SMTP server. The authentication extension is mandatory for submission servers.”

“STARTTLS is a way to take an existing insecure connection and upgrade it to a secure connection using SSL/TLS. Note that despite having TLS in the name, STARTTLS doesn't mean you have to use TLS, you can use SSL.”

Now, to add authentication to my Postfix I will use Cyrus SASL which is a “Simple Authentication and Security Layer (SASL) is a specification that describes how authentication mechanisms can be plugged into an application protocol on the wire. Cyrus SASL is an implementation of SASL that makes it easy for application developers to integrate authentication mechanisms into their application in a generic way.”

I will follow a good and easy tutorial to install and configure it:

Install SASL administration tools

```
kotaiba@bristol:~$ sudo apt-get install sasl2-bin
```

Then, Enable SASL daemon at startup we need to edit /etc/default/saslauthd

```
switch START to yes.
```

Start it manually for the first time :

```
kotaiba@bristol:~$ sudo service saslauthd start
```

Now,Enable PAM authentication for SASL which is “A pluggable authentication module (PAM) is a mechanism to integrate multiple low-level authentication schemes into a high-level application programming interface (API). ”

Check that PAM is part of the MECHANISMS variable in /etc/default/saslauthd :

```
MECHANISMS="pam"
```

Then, create /etc/pam.d/smtp :

```
#
# /etc/pam.d/smtp - specify PAM SMTP behavior
#

@include common-auth
@include common-account
@include common-password
@include common-session
```

Now, we need to Enable SASL for Postfix

Add to /etc/postfix/main.cf :

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_local_domain =
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
```

Create /etc/postfix/sasl/smtpd.conf :

```
pwcheck_method: saslauthd
mech_list: PLAIN LOGIN
```

Adjust OPTIONS in /etc/default/saslauthd :

```
OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd"
```

Add postfix user to sasl group :

```
kotaiba@bristol:~$ adduser postfix sasl
```

Now, we install dovecot:

```
kotaiba@bristol:~$ sudo apt install dovecot-common
kotaiba@bristol:~$ sudo apt-get install libsasl2-dev
```

Now, we add to /etc/dovecot/conf.d/10-master.conf :

```
  unix_listener auth-userdb {
    #mode = 0666
    #user =
    #group =
  }

  # Postfix smtp-auth
  unix_listener /var/spool/postfix/private/auth {
    mode = 0660
    user = postfix
    group = postfix
  }
```

Now, we need to restart restart all services (postfix, salsauthd):

```
kotaiba@bristol:~$ sudo service postfix restart
kotaiba@bristol:~$ sudo service saslauthd restart
```

Test our configuration:

To find out what SASL implementations are compiled into Postfix:

```
kotaiba@bristol:~$ postconf -a
cyrus
dovecot
```

After working on dovecot configuration and debugg it, and restart everything.

Let's try it:

```
kotaiba@kotaiba:~$ telnet 145.100.104.163 25
Trying 145.100.104.163...
Connected to 145.100.104.163.
Escape character is '^]'.
220 bristol.prac.os3.nl ESMTP Postfix
EHLO bristol
250-bristol.prac.os3.nl
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH DIGEST-MD5 NTLM CRAM-MD5 PLAIN LOGIN
250-AUTH=DIGEST-MD5 NTLM CRAM-MD5 PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
```

AFTER I RECEIVED YOUR FEEDBACK “Please show clearly that you authenticate with a password/credentials.”, I got Kenneth help to do it.

First, we create a user:

```
kotaiba@bristol:/etc/postfix$ sudo saslpasswd2 kotaiba
Password:
Again (for verification):
kotaiba@bristol:~$:/etc/postfix$ sudo chown :postfix /etc/sasldb2
```

Now, lets test:

```
kotaiba@kotaiba:/etc/postfix$ telnet 145.100.104.163 25
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 bristol.prac.os3.nl ESMTP Postfix
EHLO kotaiba
250-bristol.prac.os3.nl
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5 NTLM LOGIN PLAIN
250-AUTH=DIGEST-MD5 CRAM-MD5 NTLM LOGIN PLAIN
```

```
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 SMTPUTF8
AUTH CRAM-MD5
334 PDYyODUxODA4My4xNTM3MzUzMEBjb3BlbmhhZ2VuLnByYWMub3MzLm5sPg==
a2VubmV0aCBlMTEyNDM5NTZl
235 2.7.0 Authentication successful
MAIL FROM: kotaiba@bristol.prac.os3.nl
250 2.1.0 Ok
RCPT TO: kotaiba.alachkar@os3.nl
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Hello Pederborne
.
250 2.0.0 Ok: queued as B46A8E800DC
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

SMTP will give a challenge:

```
334 PDYyODUxODA4My4xNTM3MzUzMEBjb3BlbmhhZ2VuLnByYWMub3MzLm5sPg==
```

Using gen-auth we can create a response to the server:

```
kotaiba@bristol:~$ sudo gen-auth
encryption type: CRAM-MD5
username: kotaiba
password:
challenge: PDYyODUxODA4My4xNTM3MzUzMEBjb3BlbmhhZ2VuLnByYWMub3MzLm5sPg==
a2VubmV0aCBlMTEyNDM5NTZlM2E
```

Log:

```
Oct 26 02:29:22 bristol postfix/smtpd[12588]: B46A8E800DC:
client=localhost[127.0.0.1], sasl_method=CRAM-MD5,
sasl_username=kotaiba@bristol.prac.os3.nl
Oct 26 02:29:47 bristol postfix/cleanup[12624]: B46A8E800DC: hold: header
Received: from bristol (localhost [127.0.0.1])??by bristol.prac.os3.nl
(Postfix) with ESMTPA id B46A8E800DC??for <krijsbergen@os3.nl>; Sat, 26 Oct
2017 02:29:10 +0200 (CEST) from localhost[127.0.0.1];
from=<kotaiba@bristol.prac.os3.nl> to=<kotaiba.alachkar@os3.nl@os3.nl>
proto=ESMTP helo=<bristol>
Oct 26 02:29:47 bristol postfix/cleanup[12624]: B46A8E800DC: message-
id=<20171026002922.B46A8E800DC@bristol.prac.os3.nl>
Oct 26 02:29:47 bristol MailScanner[12582]: New Batch: Scanning 1 messages,
1622 bytes
Oct 26 02:29:47 bristol MailScanner[12582]: Virus and Content Scanning:
Starting
```

```
Oct 26 02:29:52 bristol postfix/smtpd[12588]: disconnect from
localhost[127.0.0.1] ehlo=1 auth=1 mail=1 rcpt=1 data=1 quit=1 commands=6
Oct 26 02:30:05 bristol MailScanner[12582]: Requeue: B46A8E800DC.A6940 to
C199CE8027B
Oct 26 02:30:05 bristol MailScanner[12582]: Uninfected: Delivered 1 messages
Oct 26 02:30:05 bristol postfix/qmgr[12546]: C199CE8027B:
from=<kotaiba@bristol.prac.os3.nl>, size=394, nrcpt=1 (queue active)
```

as we see in the log (it works)

Source:

1- https://en.wikipedia.org/wiki/SMTP_Authentication

2- https://www.fastmail.com/help/technical/ssltlsstarttls.html

3- https://help.ubuntu.com/community/Postfix

4- https://uname.pingveno.net/blog/index.php/post/2014/02/01/Configure-Postfix-as-STMP-standalone-single-domain-server-using-Unix-users-and-PAM-on-Debian

5- https://en.wikipedia.org/wiki/Pluggable_authentication_module

6- http://www.postfix.org/SASL_README.html#server_sasl

7- https://linuxconfig.org/how-to-perform-auth-digest-md5-cram-md5-command-line-smtp-authentication