PSAwise2324Team10Aufgabe09

Mailserver

We created a new VM, VM8, for our mail server.

First, we added an MX record pointing at our mail server to our DNS server. MX stands for mail exchange and is used to decide where mail will be directed. An MX record is structured as follows

```
<name> MX <TTL> <priority> <value>
```

Name is the domain name of the mail server, TTL we left out as it's optional and we don't need it for this course, priority is used to decide which server to send a mail to if there are several matching options. The server with the lowest priority will get the mail unless it is unreachable.

We added the following two records to our DNS server, then restarted bind9 to apply changes:

```
tenmail         IN      A       192.168.10.8      # MX record needs A record
to point at, CNAME is not enough
@               IN      MX 10   tenmail
```

The hostname of our mail server is tenmail.psa-team10.cit.tum.de.

MAT

We used postfix for our MAT, so the first step was `sudo apt install postfix`. During installation, a few prompts need to be answered

- mail configuration type: we picked "Internet", as that is the normal type for a standalone mail server. It both sends and receives mail and doesn't expect a mail relay server.
- system mail name: this will be used to automatically construct a valid email address when only the user part of an address is given; we set it to `tenmail.psa-team10.cit.tum.de`
- recipient for root/postmaster: postmaster@tenmail.psa-team10.cit.tum.de (doesn't exist yet, we will create it later)
- force synchronous updates: no
- local networks: 192.168.0.0/16 127.0.0.0/8
- mailbox size limit: 51200 (default)
- local address extension char: + (default)
- internet protocols to use: ipv4

To set the hostname of this server, we opened /etc/postfix/main.cf and set `"myhostname = tenmail.psa-team10.cit.tum.de"` .
Running `sudo postconf -e 'home_mailbox = Maildir/'` will set the default name of the directory the mails are supposed to be stored in. Now, all mails addressed to user X should be deposited in /home/X/Maildir/.
We also need to reflect this change in the Dovecot config, thus install dovecot-core via apt and open the config file at `/etc/dovecot/conf.d/10-mail.conf` and find the line, where you can set the mailbox location. Make sure this is what it is set to: `mail_location = maildir:~/Maildir`. Restart the dovecot service after saving and closing the file.

SMTP

For SMTP authentication, we used Dovecot SASL.

Run the following commands to adjust some basic settings in /etc/postfix/main.cf:

```
sudo postconf -e 'smtpd_sasl_type = dovecot'
sudo postconf -e 'smtpd_sasl_path = private/auth'
sudo postconf -e 'smtpd_sasl_local_domain ='
sudo postconf -e 'smtpd_sasl_security_options = noanonymous,noplaintext'
sudo postconf -e 'smtpd_sasl_tls_security_options = noanonymous'
sudo postconf -e 'broken_sasl_auth_clients = yes'
sudo postconf -e 'smtpd_sasl_auth_enable = yes'
sudo postconf -e 'smtpd_recipient_restrictions = \
permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination'
```

The security option "noplaintext" makes sure that all the mails are encrypted. "permit_sasl_authenticated", in combination with "reject_unauth_destination" make it so that all mails for authenticated users are accepted and mails with unauthenticated recipients are discarded in the SMTP dialog.

To relay all mails we can't deliver locally, we also need to put the following settings in main.cf:

```
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated
defer_unauth_destination    # accept only authenticated (=> no open relay)
relayhost = 192.168.10.7:587    # this server should relay, port 587 is
standard port for encrypted SMTP
mynetworks = 192.168.0.0/16 127.0.0.0/8
```

We also need to edit the `/etc/dovecot/conf.d/10-master.conf` file so that service auth {...} includes the following:

```
service auth {
  unix_listener /var/spool/postfix/private/auth {
      mode = 0660
      user = postfix
      group = postfix
  }
}
```

After, we need to edit the file `/etc/postfix/master.cf` so that it includes the following text block:

```
smtp      inet  n       -       y       -       -       smtpd
 -o smtpd_client_restrictions=permit_sasl_authenticated,reject
 -o smtpd_sender_restrictions=reject_sender_login_mismatch
 -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
 -o smtpd_sender_login_maps=hash:/etc/postfix/controlled_envelope_senders
 -o authorized_submit_users=root,ida,horva,kastl
```

Create a new file `/etc/postfix/controlled_envelope_senders` and add the following to it:

```
root@psa-team10.cit.tum.de root
ida@psa-team10.cit.tum.de ida
horva@psa-team10.cit.tum.de horva
kastl@psa-team10.cit.tum.de kastl
```

Compile the new file using the postmap command `postmap controlled_envelope_senders` .
Summarizing all our changes, our Postfix config file now looks like this:

```
smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no
append_dot_mydomain = no
readme_directory = no
default to 3.6 on
compatibility_level = 3.6

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

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


smtpd_relay_restrictions = reject_unknown_recipient_domain permit_mynetworks
permit_sasl_authenticated defer_unauth_destination
myhostname = tenmail.psa-team10.cit.tum.de
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, tenmail.psa-team10.cit.tum.de, localhost,
localhost.psa-team10.cit.tum.de
relayhost =
mynetworks = 192.168.0.0/16 127.0.0.0/8
mailbox_size_limit = 51200
recipient_delimiter =
inet_interfaces = all
```

```
inet_protocols = ipv4
home_mailbox = Maildir/
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
```

After you are done with editing the file, restart the Postfix service using systemctl. In case you need to debug postfix, take a log at the logs at `/var/log/mail.log`.
To test if sending and receiving mails works, we need to install a new tool:

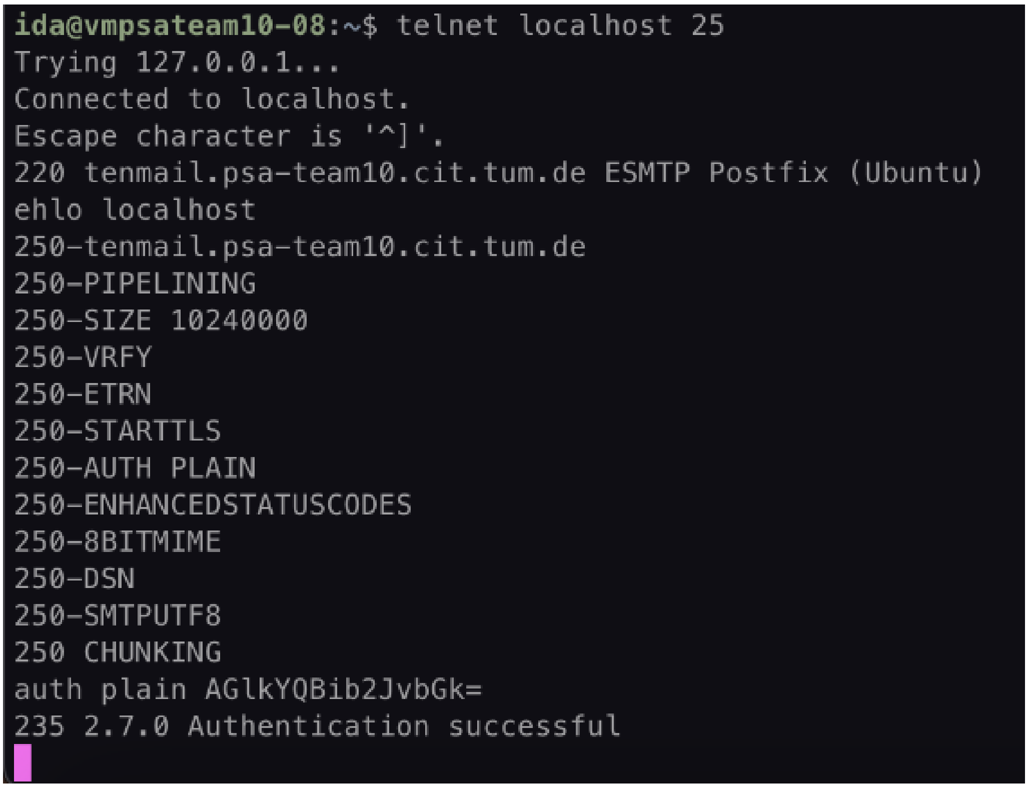
```
sudo apt install mailutils
```

To send a new test mail using this tool, we run this command:

```
echo "This is a test e-mail!" | mail -r [sender address] -s "Test"
[user]@tenmail.psa-team10.cit.tum.de
```

The user who is specified in the command above is the recipient of the email with the content that is given by the echo command.

The recipient can find his new email in this directory: `~/Maildir/new` and print it to the console using `cat`.
We can also test if the authentication for our mail server works by using telnet or nc to connect to port 25 on localhost. To log in, we need to encode username and password in this form \000[username]\000[password] in base64 and pass the resulting string in the console as depicted in the picture below.



```
ida@vmpsateam10-08:~$ telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 tenmail.psa-team10.cit.tum.de ESMTP Postfix (Ubuntu)
ehlo localhost
250-tenmail.psa-team10.cit.tum.de
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
auth plain AGlkYQBib2JvbGk=
235 2.7.0 Authentication successful
```

Mail Redirect

We want to redirect emails to mailrelay.cit.tum.de, if emails cannot be transmitted locally within our PSA network.

First, add `relayhost = [mailrelay.cit.tum.de]` to the Postfix config file at `/etc/postfix/main.cf`.
Install the postfix-pcre package via apt as well and add `smtp_generic_maps = pcre:/etc/postfix/generic.pcre` to `/etc/postfix/main.cf`.
Now, create the file `/etc/postfix/generic.pcre` with this regex rule as content: `/([^@]+)@example\.psa-team(\d{1,2})\.cit\.tum\.de/ ${1}@psa-team${2}.cit.tum.de`.
This regex expression matches email addresses belonging to the domain pattern @irgendeinhostname.psa-team##.cit.tum.de and removes "irgendeinhostname" from the domain.

Finally, for double-checking purposes main.cf should look like this:

```
smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no
append_dot_mydomain = no
readme_directory = no
compatibility_level = 3.6

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

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

smtp_generic_maps = pcre:/etc/postfix/generic.pcre
smtpd_relay_restrictions = reject_unknown_recipient_domain permit_mynetworks
permit_sasl_authenticated defer_unauth_destination
myhostname = tenmail.psa-team10.cit.tum.de
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, tenmail.psa-team10.cit.tum.de, localhost,
localhost.psa-team10.cit.tum.de
relayhost = [mailrelay.cit.tum.de]
mynetworks = 192.168.0.0/16 127.0.0.0/8
mailbox_size_limit = 0
recipient_delimiter =
inet_interfaces = all
inet_protocols = ipv4
home_mailbox = Maildir/
smtpd_sasl_type = dovecot
```

```
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
local_recipient_maps = proxy:unix:passwd.byname $alias_maps
```

Do not forget to allow port 25 (SMTP) in your firewall settings.

We can check if a postmaster address exists by sending an email to postmaster@tenmail.psa-team10.cit.tum.de and checking the logs at `/var/log/mail.log` if the email was sent successfully as well as checking Maildir/ of root.
The file /etc/aliases should contain this:

```
# See man 5 aliases for format
postmaster:    root
clamav: root
```

Virus Scanner and Spam Filtering

We choose to install ClamAV for malware and virus detection.

```
sudo apt-get install clamav clamav-daemon
```

Update the ClamAV database via `sudo freshclam`. Then, install the Postfix integration for ClamAV: `sudo apt-get install clamav-daemon clamav-freshclam clamav-milter`.
We also install Amavis to act as a middleware tool between Postfix and Clamav.

```
apt-get install amavisd-new
sudo adduser clamav amavis
```

Clamav uses a lot of memory, so make sure you have about 2GB of free RAM.

Enable and start Amavis via systemctl.

Additionally, install the following packages for Amavis to extract and scan archive files in email messages such as .7z, .cab, .doc, .exe, .iso, .jar, and .rar files.

```
sudo apt install arj bzip2 cabextract cpio rpm2cpio file gzip lhasa nomarch
pax rar unrar p7zip-full unzip zip lrzip lzip liblz4-tool lzop unrar-free
```

Make sure the following lines are uncommented in the Amavis config file:

```
etc/amavis/conf.d/15-content_filter_mode
@bypass_virus_checks_maps = (
   \%bypass_virus_checks, \@bypass_virus_checks_acl,
\$bypass_virus_checks_re);

@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);
```

Set the hostname manually by uncommenting this line and write the correct hostname:

```
/etc/amavis/conf.d/05-node_id
$myhostname = "tenmail.psa-team10.cit.tum.de";
```

After you are done editing the config files, restart the amavis service for the changes to take effect.

We use SpamAssassin for spam detection and filtering.

```
sudo apt-get install spamassassin spamc
sudo apt-get install spamass-milter
```

Make sure the clamav-daemon and spamd services are enabled and active.

We also install the SpamAssassin milter because we want to integrate SpamAssassin via the sendmail milter interface.

This allows us to reject an email when it gets a spam score of more than 15, so it will never be seen by the recipient. You can change this score or add custom rules for spam detection as well, such as rejecting all emails that contain certain words in the subject line.

Add these lines to the Postfix config file main.cf:

```
/etc/postfix/main.cf
milter_default_action = accept
milter_protocol = 6
smtpd_milters = local:spamass/spamass.sock
non_smtpd_milters = $smtpd_milters
```

After saving these changes, edit the milter config file as well such that these lines are uncommented:

```
/etc/default/spamass-milter
OPTIONS="-u spamass-milter -i 127.0.0.1"

# Reject emails with spamassassin scores > 15.
OPTIONS="${OPTIONS} -r 15"
```

After you have finished editing, restart the services:
`sudo systemctl restart postfix spamass-milter`.
To configure Postfix to use our new tools, add the following lines to our configuration files:

```
/etc/postfix/main.cf
content_filter = smtp-amavis:[127.0.0.1]:10024
smtpd_proxy_options = speed_adjust

/etc/postfix/master.cf
scan unix  -       -       n       -       16      smtp
 -o smtp_data_done_timeout=1200
 -o disable_dns_lookups=yes
 -o smtp_send_xforward_command=yes
 -o smtpd_helo_restrictions=
 -o smtpd_client_restrictions=
 -o smtpd_sender_restrictions=
 -o smtpd_relay_restrictions=permit_mynetworks,reject_unauth_destination
 -o smtpd_recipient_restrictions=permit_mynetworks,reject_unauth_destination
 -o mynetworks=127.0.0.0/8
 -o smtpd_error_sleep_time=0
 -o smtpd_soft_error_limit=1001
 -o smtpd_hard_error_limit=1000
 -o receive_override_options=no_header_body_checks
 -o smtpd_milters=inet:127.0.0.1:8891


smtp-amavis   unix   -   -   n   -   2   smtp
 -o syslog_name=postfix/amavis
 -o smtp_data_done_timeout=1200
 -o smtp_send_xforward_command=yes
 -o disable_dns_lookups=yes
 -o max_use=20
 -o smtp_tls_security_level=none

127.0.0.1:10025   inet   n    -     n     -     -    smtpd
 -o syslog_name=postfix/10025
 -o content_filter=
 -o mynetworks_style=host
 -o mynetworks=127.0.0.0/8
 -o local_recipient_maps=
 -o relay_recipient_maps=
 -o strict_rfc821_envelopes=yes
 -o smtp_tls_security_level=none
 -o smtpd_tls_security_level=none
 -o smtpd_restriction_classes=
 -o smtpd_delay_reject=no
 -o smtpd_client_restrictions=permit_mynetworks,reject
 -o smtpd_helo_restrictions=
 -o smtpd_sender_restrictions=
 -o smtpd_recipient_restrictions=permit_mynetworks,reject
 -o smtpd_end_of_data_restrictions=
 -o smtpd_error_sleep_time=0
 -o smtpd_soft_error_limit=1001
 -o smtpd_hard_error_limit=1000
 -o smtpd_client_connection_count_limit=0
 -o smtpd_client_connection_rate_limit=0
 -o
receive_override_options=no_header_body_checks,no_unknown_recipient_checks,no_
address_mappings
```

Also, don't forget to allow traffic to port 10024 (amavis) and 10025 (clamav) in the firewall and make sure to restart all services after saving the new edits.

As we already know, Amavis listens on port 10024 for incoming and outgoing emails. We want to add port 10026 (unassigned) because it is a good practice to use a different port for email submissions from authenticated users.

To do this, we need to define the new port in the configuration of Amavis and also create a new policy for outgoing emails that originates from authenticated users. Make sure any new line is added between the "use strict;" and "1;" lines and restart the Amavis service.

```
/etc/amavis/conf.d/50-user
use strict;

#
# Place your configuration directives here.  They will override those in
# earlier files.
#
# See /usr/share/doc/amavisd-new/ for documentation and examples of
# the directives you can use in this file
#
$inet_socket_port = [10024,10026];
$interface_policy{'10026'} = 'ORIGINATING';

$policy_bank{'ORIGINATING'} = {  # mail supposedly originating from our users
  originating => 1,  # declare that mail was submitted by our smtp client
  allow_disclaimers => 1,  # enables disclaimer insertion if available

  # notify administrator of locally originating malware
  virus_admin_maps => ["virusalert\@psa-team10.cit.tum.de"],
  spam_admin_maps  => ["virusalert\@psa-team10.cit.tum.de"],
  warnbadhsender   => 1,

  # force MTA conversion to 7-bit (e.g. before DKIM signing)
  smtpd_discard_ehlo_keywords => ['8BITMIME'],
  bypass_banned_checks_maps => [1],  # allow sending any file names and types
  terminate_dsn_on_notify_success => 0,  # don't remove NOTIFY=SUCCESS option
  $undecipherable_subject_tag = '***Encrypted Message***',
};

#------------ Do not modify anything below this line -------------
1;  # ensure a defined return
```

We also need to reflect this change in Postfix, so add this to the master.cf file as well:

```
/etc/postfix/master.cf
submission      inet    n       -       y       -       -       smtpd
 -o syslog_name=postfix/submission
 -o smtpd_tls_security_level=encrypt
 -o smtpd_tls_wrappermode=no
 -o smtpd_sasl_auth_enable=yes
 -o
smtpd_relay_restrictions=permit_mynetworks,permit_sasl_authenticated,reject
 -o smtpd_sasl_type=dovecot
 -o smtpd_sasl_path=private/auth
 -o content_filter=smtp-amavis:[127.0.0.1]:10026
```

Don't forget to reload the postfix service again.

Testing

The test script is located on VM9.

```
#!/bin/bash

echo "EHLO example.com" | nc -w 3 tenmail.psa-team10.cit.tum.de 25 | grep -q
"250-STARTTLS" && echo "Open relay test: PASS" || echo "Open relay test: FAIL"


echo "Sending a new email ..."
echo "First check it with an unknown recipient"
echo "This is a test email to check if unknown recipients are rejected!" |
mail -s "Test" testtestest@ptesttesttest.de
grep "to=<.*@.*>" /var/log/mail.log | grep "status=deferred" | tail -n 1
echo "===================================================================="

echo "Sending a new email to postmaster ..."
echo "This is a test email to postmaster!" | mail -s "Test"
postmaster@tenmail.psa-team10.cit.tum.de
newest_mail_root=$(ls -t /root/Maildir/new | head -n 1)
cat "/root/Maildir/new/$newest_mail_root"
echo "===================================================================="

echo "Sending a new email to user ida"
echo "This is a test email!" | mail -s "Test" ida@tenmail.psa-
team10.cit.tum.de
echo "Check if user ida has a new email ..."
newest_mail=$(ls -t /home/ida/Maildir/new | head -n 1)
cat "/home/ida/Maildir/new/$newest_mail"
```