Лабораторная работа № 10. Расширенные настройки SMTP-сервера

10.1. Цель работы

Приобретение практических навыков по конфигурированию SMTP-сервера в части настройки аутентификации.

10.2. Предварительные сведения

10.2.1. Протокол LMTP

Local Mail Transfer Protocol (LMTP) — протокол локальной пересылки почты.

По сути, Dovecot с включённым в него функционалом LMTP выступает в качестве локального агента доставки почты, т.е. является службой приёма почтовых сообщений от SMTP-сервера для последующей их пересылки клиентам локальной сети. Использование Dovecot и протокола LMTP позволяет организовать фильтрацию почты на стороне сервера в момент размещения письма в почтовый ящик, а не на стороне клиента.

10.2.2. Аутентификация посредством SASL

Simple Authentication and Security Layer (SASL) — механизм обеспечения аутентификации и идентификации пользователей, а также защиты данных в протоколах, ориентированных на соединение (например, в IMAP, POP, SMTP, LDAP, telnet, FTP и т.п.).

SASL, по сути, является посредником (промежуточным слоем) между каким-то приложением и взаимодействующим с ним протоколом, добавляя к протоколу команды идентификации и аутентификации пользователя, а также определяя протокол обеспечения безопасности (шифрования). SASL функционирует посредством запросов и ответов, используя определённые в нём механизмы, позволяющие, например, отделить аутентификацию от передачи данных, или задать анонимную аутентификацию, или разрешить передачу пароля пользователя открытым текстом и т.п.

Подробнее о SASL см. в RFC-4422, о связке Postfix и SASL см. в [1].

10.3. Задание

1. Настройте Dovecot для работы с LMTP (см. раздел 10.4.1).
2. Настройте аутентификацию посредством SASL на SMTP-сервере (см. раздел 10.4.2).
3. Настройте работу SMTP-сервера поверх TLS (см. раздел 10.4.3).
4. Скорректируйте скрипт для Vagrant, фиксирующий действия расширенной настройки SMTP-сервера во внутреннем окружении виртуальной машины `server` (см. раздел 10.4.4).

10.4. Последовательность выполнения работы

10.4.1. Настройка LMTP в Dovecote

1. На виртуальной машине `server` войдите под вашим пользователем и откройте терминал. Перейдите в режим суперпользователя:
   ```
   sudo -i
   ```

2. В дополнительном терминале запустите мониторинг работы почтовой службы:
```
sudo -i
tail -f /var/log/maillog
```
3. Добавьте в список протоколов, с которыми может работать Dovecot, протокол LMTP. Для этого в файле `/etc/dovecot/dovecot.conf` укажите
```
protocols = imap pop3 lmtp
```
4. Настройте в Dovecot сервис lmtp для связи с Postfix. Для этого в файле `/etc/dovecot/conf.d/10-master.conf` замените определение сервиса lmtp на следующую запись:
```
service lmtp {
  unix_listener /var/spool/postfix/private/dovecot-lmtp {
    group = postfix
    user = postfix
    mode = 0600
  }
}
```
Эта запись определяет расположение файла с описанием прослушиваемого unix-сокета, а также задаёт права доступа к нему и определяет принадлежность к группе и пользователю `postfix`.
5. Переопределите в Postfix с помощью `postconf` передачу сообщений не на прямую, а через заданный unix-сокет:
```
postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lmtp'
```
6. В файле `/etc/dovecot/conf.d/10-auth.conf` задайте формат имени пользователя для аутентификации в форме логина пользователя без указания домена:
```
auth_username_format = %Ln
```
7. Перезапустите Postfix и Dovecot:
```
systemctl restart postfix
systemctl restart dovecot
```
8. Из-под учётной записи своего пользователя отправьте письмо с клиента (вместо `user` укажите ваш логин):
```
echo .| mail -s "LMTP test" user@user.net
```
В отчёт включите свои пояснения по содержанию логов при мониторинге почтовой службы.
9. На сервере просмотрите почтовый ящик пользователя:
```
MAIL=~/Maildir/ mail
```
Убедитесь, что отправленное вами с клиента письмо доставлено в почтовый ящик на сервере.

10.4.2. Настройка SMTP-аутентификации

1. В файле `/etc/dovecot/conf.d/10-master.conf` определите службу аутентификации пользователей:
```
service auth {
  unix_listener /var/spool/postfix/private/auth {
    group = postfix
    user = postfix
    mode = 0660
  }
  unix_listener auth-userdb {
    mode = 0600
    user = dovecot
```

```
    }
  }
```

В отчёте поясните построчно эту запись.

2. Для Postfix задайте тип аутентификации SASL для `smtpd` и путь к соответствующему unix-сокету:
```
postconf -e 'smtpd_sasl_type = dovecot'
postconf -e 'smtpd_sasl_path = private/auth'
```
3. Настройте Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины (имеется в виду локальных пользователей сервера), обеспечивая тем самым запрет на использование почтового сервера в качестве SMTP relay для спам-рассылок (порядок указания опций имеет значение):
```
postconf -e 'smtpd_recipient_restrictions =
 ↪  reject_unknown_recipient_domain, permit_mynetworks,
 ↪  reject_non_fqdn_recipient, reject_unauth_destination,
 ↪  reject_unverified_recipient, permit'
```
В отчёте прокомментируйте указанные опции.
4. В настройках Postfix ограничьте приём почты только локальным адресом SMTP-сервера сети:
```
postconf -e 'mynetworks = 127.0.0.0/8'
```
5. Для проверки работы аутентификации временно запустим SMTP-сервер (порт 25) с возможностью аутентификации. Для этого необходимо в файле `/etc/postfix/master.cf` заменить строку
```
smtp inet n - n - - smtpd
```
на строку
```
smtp inet n - n - - smtpd
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,rej
 ↪  ect_unknown_recipient_domain,permit_sasl_authenticated,reject
```
6. Перезапустите Postfix и Dovecot:
```
systemctl restart postfix
systemctl restart dovecot
```
7. На клиенте установите telnet:
```
sudo -i
dnf -y install telnet
```
8. На клиенте получите строку для аутентификации, вместо `username` указав логин вашего пользователя, а вместо `password` указав пароль этого пользователя:
```
printf 'username\x00username\x00password' | base64
```
Например, для пользователя `user` с паролем 123456:
```
printf 'user\x00user\x00123456' | base64
```
получим в качестве результата строку для аутентификации в формате base64:
```
dXNlcgB1c2VyADEyMzQ1Ng==
```
9. Подключитесь на клиенте к SMTP-серверу посредством telnet (вместо `user` укажите ваш логин):
```
telnet server.user.net 25
```
Протестируйте соединение, введя
```
EHLO test
```
Проверьте авторизацию, задав:
```
AUTH PLAIN <строка для аутентификации>
```
Например, для пользователя `user`:
```
AUTH PLAIN dXNlcgB1c2VyADEyMzQ1Ng==
```
Завершите сессию telnet на клиенте.

10.4.3. Настройка SMTP over TLS

1. Настройте на сервере TLS, воспользовавшись временным сертификатом Dovecot. Предварительно скопируйте необходимые файлы сертификата и ключа из каталога `/etc/pki/dovecot` в каталог `/etc/pki/tls/` в соответствующие подкаталоги (чтобы не было проблем с SELinux):
   ```
   cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
   cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
   ```
   Сконфигурируйте Postfix, указав пути к сертификату и ключу, а также к каталогу для хранения TLS-сессий и уровень безопасности:
   ```
   postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
   postconf -e
    ↪  'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
   postconf -e 'smtpd_tls_session_cache_database =
    ↪  btree:/var/lib/postfix/smtpd_scache'
   postconf -e 'smtpd_tls_security_level = may'
   postconf -e 'smtp_tls_security_level = may'
   ```
2. Для того чтобы запустить SMTP-сервер на 587-м порту, в файле `/etc/postfix/master.cf` замените строки
   ```
   smtp inet n - n - - smtpd
     -o smtpd_sasl_auth_enable=yes
     -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,rej
    ↪  ect_unknown_recipient_domain,permit_sasl_authenticated,reject
   ```
   на следующую запись:
   ```
   smtp inet n - n - - smtpd
   ```
   и добавьте следующие строки:
   ```
   submission inet n - n - - smtpd
     -o smtpd_tls_security_level=encrypt
     -o smtpd_sasl_auth_enable=yes
     -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,rej
    ↪  ect_unknown_recipient_domain,permit_sasl_authenticated,reject
   ```
3. Настройте межсетевой экран, разрешив работать службе `smtp-submission`:
   ```
   firewall-cmd --get-services
   firewall-cmd --add-service=smtp-submission
   firewall-cmd --add-service=smtp-submission --permanent
   firewall-cmd --reload
   ```
4. Перезапустите Postfix:
   ```
   systemctl restart postfix
   ```
5. На клиенте подключитесь к SMTP-серверу через 587-й порт посредством openssl (вместо `user` используйте свой логин):
   ```
   openssl s_client -starttls smtp -crlf -connect
    ↪  server.user.net:587
   ```
   Протестируйте подключение по telnet:
   ```
   EHLO test
   ```
   Проверьте аутентификацию:
   ```
   AUTH PLAIN <строка для аутентификации>
   ```
6. Проверьте корректность отправки почтовых сообщений с клиента посредством почтового клиента Evolution, предварительно скорректировав настройки учётной записи, а именно для SMTP-сервера укажите порт 587, STARTTLS и обычный пароль.

10.4.4. Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине `server` перейдите в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`. В соответствующие подкаталоги поместите конфигурационные файлы Dovecot и Postfix:
```
cd /vagrant/provision/server
cp -R /etc/dovecot/dovecot.conf
 ↪  /vagrant/provision/server/mail/etc/dovecot/
cp -R /etc/dovecot/conf.d/10-master.conf
 ↪  /vagrant/provision/server/mail/etc/dovecot/conf.d/
cp -R /etc/dovecot/conf.d/10-auth.conf
 ↪  /vagrant/provision/server/mail/etc/dovecot/conf.d/
cp -R /etc/postfix/master.cf
 ↪  /vagrant/provision/server/mail/etc/postfix/
```
2. Внесите соответствующие изменения по расширенной конфигурации SMTP-сервера в файл `/vagrant/provision/server/mail.sh`:
```
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install postfix
dnf -y install dovecot
dnf -y install telnet

echo "Copy configuration files"
cp -R /vagrant/provision/server/mail/etc/* /etc

chown -R root:root /etc/postfix
restorecon -vR /etc

echo "Configure firewall"
firewall-cmd --add-service smtp --permanent

firewall-cmd --add-service pop3 --permanent
firewall-cmd --add-service pop3s --permanent
firewall-cmd --add-service imap --permanent
firewall-cmd --add-service imaps --permanent

firewall-cmd --add-service smtp-submission --permanent

firewall-cmd --reload

echo "Start postfix service"
systemctl enable postfix
systemctl start postfix

echo "Configure postfix"
postconf -e 'mydomain = user.net'
postconf -e 'myorigin = $mydomain'
postconf -e 'inet_protocols = ipv4'
postconf -e 'inet_interfaces = all'
```

```
postconf -e 'mydestination = $myhostname, localhost.$mydomain,
 ↪  localhost, $mydomain'
#postconf -e 'mynetworks = 127.0.0.0/8, 192.168.0.0/16'

echo "Configure postfix for dovecot"
postconf -e 'home_mailbox = Maildir/'

echo "Configure postfix for auth"
postconf -e 'smtpd_sasl_type = dovecot'
postconf -e 'smtpd_sasl_path = private/auth'

postconf -e 'smtpd_recipient_restrictions =
 ↪  reject_unknown_recipient_domain, permit_mynetworks,
 ↪  reject_non_fqdn_recipient, reject_unauth_destination,
 ↪  reject_unverified_recipient, permit'
postconf -e 'mynetworks = 127.0.0.0/8'


echo "Configure postfix for SMTP over TLS"
cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private

postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
postconf -e 'smtpd_tls_session_cache_database =
 ↪  btree:/var/lib/postfix/smtpd_scache'
postconf -e 'smtpd_tls_security_level = may'
postconf -e 'smtp_tls_security_level = may'

postfix set-permissions

restorecon -vR /etc

systemctl stop postfix
systemctl start postfix
systemctl restart dovecot
```

3. Внесите изменения в файл `/vagrant/provision/client/mail.sh`, добавив установку telnet.

10.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
   - скриншоты (снимки экрана), фиксирующие выполнение работы;
   - подробное описание настроек служб в соответствии с заданием;
   - полные тексты конфигурационных файлов настраиваемых в работе служб;
   - результаты проверки корректности настроек служб в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.

5. Ответы на контрольные вопросы.

10.6. Контрольные вопросы

1. Приведите пример задания формата аутентификации пользователя в Dovecot в форме логина с указанием домена.
2. Какие функции выполняет почтовый Relay-сервер?
3. Какие угрозы безопасности могут возникнуть в случае настройки почтового сервера как Relay-сервера?

Список литературы

1. Postfix SASL Howto. — URL: `http://www.postfix.org/SASL_README.html` (дата обр. 13.09.2021).