Лабораторная работа №10

Администрирование сетевых подсистем

Машков Илья Евгеньевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Задание

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

3 Выполнение лабораторной работы

3.1 Настройка LMTP в Dovecote

На сервере перехожу в режим root, на дополнительном терминале запускаю лог почтового ящика, затем в файле dovecot.conf вношу строку, позволяющую работать с протоколом LMTP (рис. [3.1]).

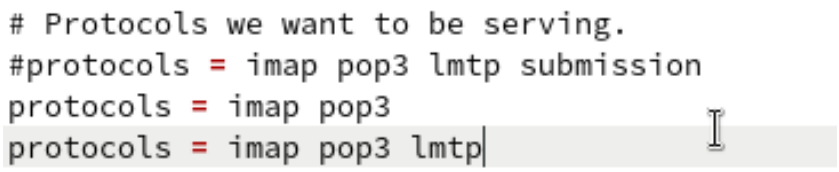

Рис. 3.1: Правка конфига dovecot

Затем в файле 10-master.conf заменяю определение сервиса lmtp (рис. [3.2]).

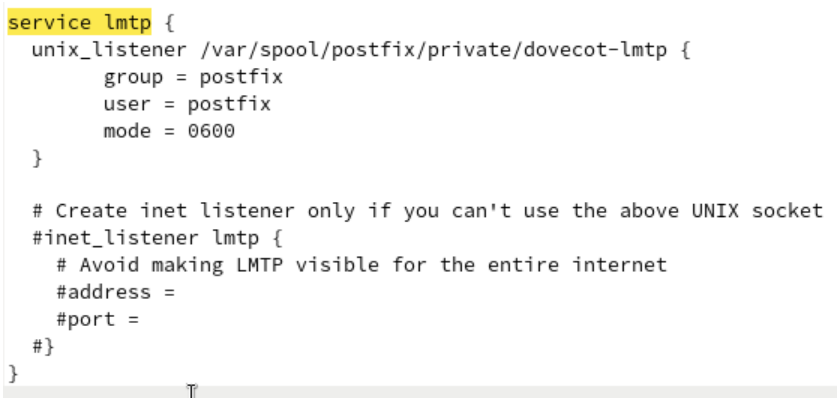

Рис. 3.2: Правка 10-master.conf

Переопределяю postfix так, чтобы он передавал сообщения не на прямую, а через заданный unix-сокет (рис. [3.3]).

```
[root@server ~]# postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lm
tp'
```

Рис. 3.3: Переопределение postfix

В файле 10-auth.conf задаю формат имени пользователя для аунтентификации в форме логина пользователя без указания домена (рис. [3.4]).

```
# drop away the domain if it was given, or "%n-AT-%d" would change the '@'
into
# "-AT-". This translation is done after auth_username_translation changes.
auth_username_format = %Ln
```

Рис. 3.4: Правки в 10-auth.conf

Теперь запускаю клиент и произвожу попытку отправки письма на домен user.net, но, как я уже говорил в прошлых лабораторных такого домена, по некоторым причинам не существует (рис. [3.5]).

```
[user@client ~]$ echo .| mail -s "LMPT test" user@user.net
```

Рис. 3.5: Попытка отправки письма с клиента

В логах вижу, что сообщение, ожидаемо, не ушло и было возвращено на cliet(рис. [3.6]).

Рис. 3.6: Логи почтового ящика

3.2 Настройка SMTP-аутентификации

В файле 10-master.conf определяю службу аунтентификации пользователей (На скрине есть небольшая опечатка: должно быть dovecot, а не doveco) (рис. [3.7]).

```
service auth {
  # auth_socket_path points to this userdb socket by default. It's
typically
  # used by dovecot-lda, doveadm, possibly imap process, etc. Users that
have
  # full permissions to this socket are able to get a list of all
usernames and
  # get the results of everyone's userdb lookups.
  #
  # The default 0666 mode allows anyone to connect to the socket, but the
  # userdb lookups will succeed only if the userdb returns an "uid" field
that
  # matches the caller process's UID. Also if caller's uid or gid matches
the
  # socket's uid or gid the lookup succeeds. Anything else causes a
failure.
  #
  # To give the caller full permissions to lookup all users, set the mode
to
  # something else than 0666 and Dovecot lets the kernel enforce the
  # permissions (e.g. 0777 allows everyone full permissions).
  unix_listener /var/spool/postfix/private/auth {
        group = postfix
        user = postfix
        mode = 0660
  }
  unix_listener auth-userdb {
        mode = 0600
        user = doveco
  }

  # Postfix smtp-auth
  #unix_listener /var/spool/postfix/private/auth {
  #  mode = 0666
  #}
```

Рис. 3.7: Определение службы аунтентификации

Задаю postfix тип аутентификации SASL для smtpd и путь к соответствующему unix-сокету (рис. [3.8]).

```
[root@server ~]# postconf -e 'smtpd_sasl_type = dovecot'
[root@server ~]# postconf -e 'smtpd_sasl_path = private/auth'
```

Рис. 3.8: Здание типа аутентификации postfix

Настраиваю 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 (рис. [3.9]).

Рис. 3.9: Настройка postfix

Затем ограничиваю приём почты только локаьным адресом smtp-сервера сети, а потом вношу изменения в master.cf (рис. [3.10]).

```
smtp       inet n       -       n       -       -       smtpd
   -o smtpd_sasl_auth_enable=yes
   -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknow
n_recipient_domain,permit_sasl_authenticated,reject
```

Рис. 3.10: Правки в master.cf

Перезапускаю postfix и dovecot(рис. [3.11]).

```
[root@server ~]# systemctl restart postfix
[root@server ~]# systemctl restart dovecot
```

Рис. 3.11: Перезапуск postfix и dovecot

На клиенте устанавливаю telnet (рис. [3.12]).

```
[user@client ~]$ sudo -i
[sudo] password for user:
[root@client ~]# dnf -y install telnet
Last metadata expiration check: 3:30:51 ago on Wed 11 Feb 2026 08:02:30 PM MSK.
Dependencies resolved.
================================================================================
 Package        Architecture   Version                 Repository         Size
================================================================================
Installing:
 telnet         x86_64         1:0.17-85.el9           appstream          63 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 63 k
Installed size: 121 k
```

Рис. 3.12: Установка telnet на клиенте

Получаю строку аунтентификации, введя имя пользователя и пароль. Потом совершаю неудачную попытку отправки письма (рис. [3.13]).

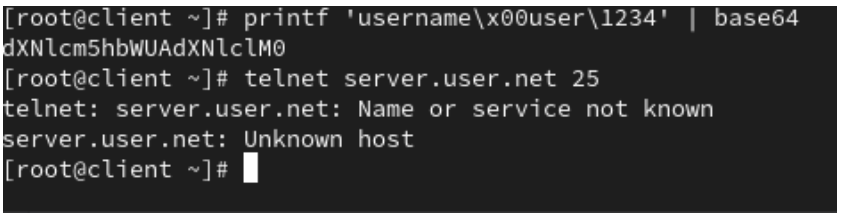

Рис. 3.13: Строка аутентификации и попытка отпраки письма

3.3 Настройка SMTP over TLS

Копирую файлы сертификата в другую директорию, чтобы не иметь проблем с SELinux(рис. [3.14]).

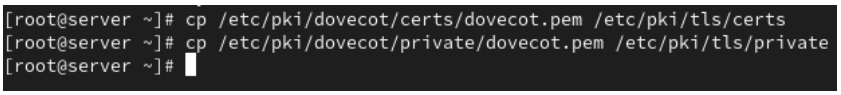

Рис. 3.14: Копирование файлов сертификата

Конфигурирую Postfix, указав пути к сертификату и ключу, а также к каталогу для хранения TLS-сессий и уровень безопасности (рис. [3.15]).

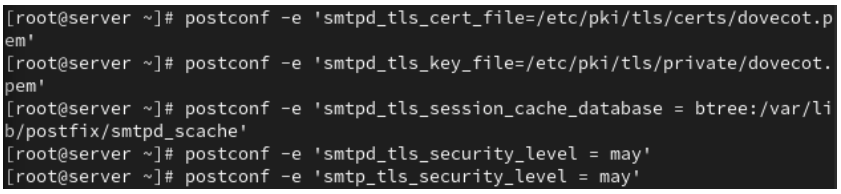

Рис. 3.15: Конфигурирование postfix

Для того чтобы запустить SMTP-сервер на 587-м порту, в файле /etc/postfix/master.cf заменяю строки на следующее (рис. [3.16]).

```
smtp      inet  n       -       n       -       -       smtpd
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,reject_unknow ]
n_recipient_domain,permit_sasl_authenticated,reject
```

Рис. 3.16: Запуск smtp сервера на 587-м порте

Настраиваю межсетевой экран, тем самым разрешив работу службе smpt-submission (рис. [3.17]).

```
[root@server ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp
amqps apcupsd audit ausweisapp2 bacula bacula-client bareos-director bareos-fi
ledaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-tes
tnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent coc
kpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp
 dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dro
pbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-prox
y freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp g
alera ganglia-client ganglia-master git gpsd grafana gre high-availability htt
p http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target
 isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell ku
be-api kube-apiserver kube-control-plane kube-control-plane-secure kube-contro
ller-manager kube-controller-manager-secure kube-nodeport-services kube-schedu
ler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker
ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp
llmnr-udp managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt m
qtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs
nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-v
mconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy pr
ometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio
puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyn
cd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp smtp-su
bmission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sy
nc squid ssdp ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-gui
 syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc to
r-socks transmission-client upnp-client vdsm vnc-server warpinator wbem-http w
bem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-disco
very-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbi
x-agent zabbix-server zerotier
[root@server ~]# firewall-cmd --add-service=smtp-submission
success
[root@server ~]# firewall-cmd --add-service=smtp-submission --permanent
success
[root@server ~]# firewall-cmd --reload
success
[root@server ~]#
```

Рис. 3.17: Настройка межсетевого экрана

Следующие действия я не скринил, т.к. все они потерпели неудачу из-за проблемы, которая тянется за мной со второй лабы.

3.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

Копирую конфиговские файлы dovecot и postfix в настройки внутреннего окружения (рис. [3.18]).

```
[root@server ~]# cd /vagrant/provision/server
[root@server server]# cp -R /etc/dovecot/dovecot.conf
/vagrant/provision/server/mail/etc/dovecot/
cp: missing destination file operand after '/etc/dovecot/dovecot.conf'
Try 'cp --help' for more information.
-bash: /vagrant/provision/server/mail/etc/dovecot/: Is a directory
[root@server server]# cp -R /etc/dovecot/dovecot.conf /vagrant/provision/serve
r/mail/etc/dovecot/
cp: overwrite '/vagrant/provision/server/mail/etc/dovecot/dovecot.conf'? y
[root@server server]# y
bash: y: command not found...
[root@server server]# cp -R /etc/dovecot/conf.d/10-auth.conf /vagrant/provisio
n/server/mail/etc/dovecot/conf.d/
cp: overwrite '/vagrant/provision/server/mail/etc/dovecot/conf.d/10-auth.conf'
? y
[root@server server]# mkdir -p /vagrant/provision/server/mail/etc/postfix/
[root@server server]# cp -R /etc/postfix/master.cf /vagrant/provision/server/m
ail/etc/postfix/
[root@server server]#
```

Рис. 3.18: Настройка параметров внутреннего окружения

Изменяю mail.sh на сервере, добавляя расширенную конфигурацию smpt-сервера (рис. [3.19]).

```
#!/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'
```

Рис. 3.19: mail.sh на сервере

Изменяю mail.sh на клиенте, добавляя установку telnet (рис. [3.20]).

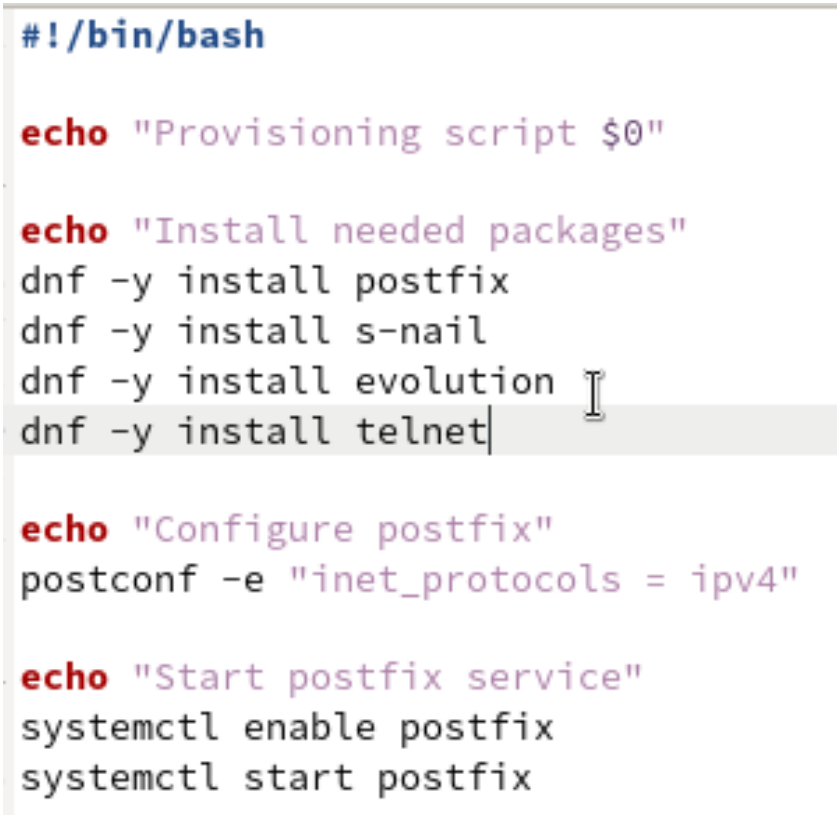

Рис. 3.20: mail.sh на клиенте

4 Выводы

Во время выполнения этой лабораторной работы я приобрёл практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.

Список литературы

Администрирование сетевых подсисем