

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 10

дисциплина: Администрирование сетевых подсистем

Студент: Бакулин Никита 1032201747

Группа: НПИбд-01-20

МОСКВА

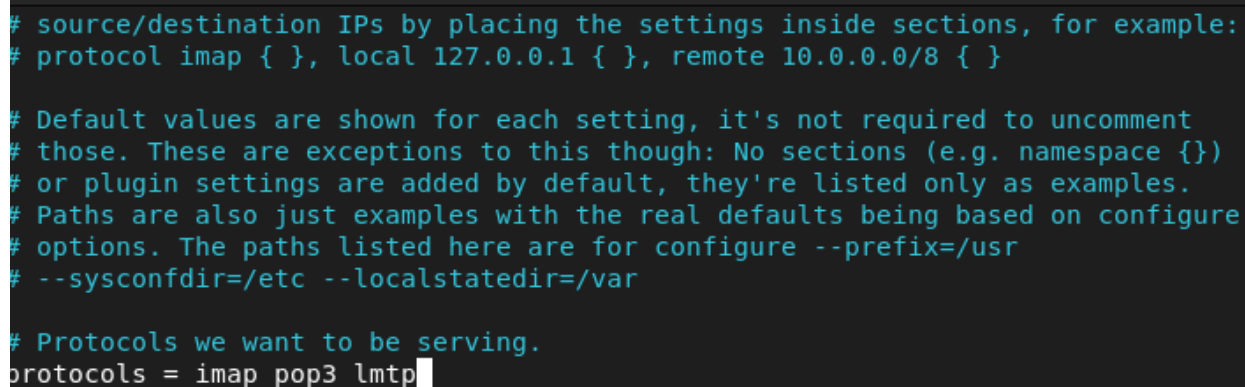
2022 г.

Постановка задачи

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

Выполнение работы

1.
 - 1.1. На виртуальной машине server войдите под вашим пользователем и откройте терминал. Перейдите в режим суперпользователя
 - 1.2. В дополнительном терминале запустите мониторинг работы почтовой службы
 - 1.3. Добавьте в список протоколов, с которыми может работать Dovecot, протокол LMTP. Для этого в файле `/etc/dovecot/dovecot.conf` укажите



```
# source/destination IPs by placing the settings inside sections, for example:
# protocol imap { }, local 127.0.0.1 { }, remote 10.0.0.0/8 { }

# Default values are shown for each setting, it's not required to uncomment
# those. These are exceptions to this though: No sections (e.g. namespace {})
# or plugin settings are added by default, they're listed only as examples.
# Paths are also just examples with the real defaults being based on configure
# options. The paths listed here are for configure --prefix=/usr
# --sysconfdir=/etc --localstatedir=/var

# Protocols we want to be serving.
protocols = imap pop3 lmtp
```

Рисунок 1

- 1.4. 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
    }
    # Create inet listener only if you can't use the above UNIX socket
    #inet_listener lmtp {
        # Avoid making LMTP visible for the entire internet
        #address =
        #port =
    #}
}

```

Рисунок 2

- 1.5. Переопределите в Postfix с помощью postconf передачу сообщений не на прямую, а через заданный unix-сокеты:
- 1.6. В файле /etc/dovecot/conf.d/10-auth.conf задайте формат имени пользователя для аутентификации в форме логина пользователя без указания домена

```

# Username formatting before it's looked up from databases. You can use
# the standard variables here, eg. %Lu would lowercase the username, %n would
# 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

```

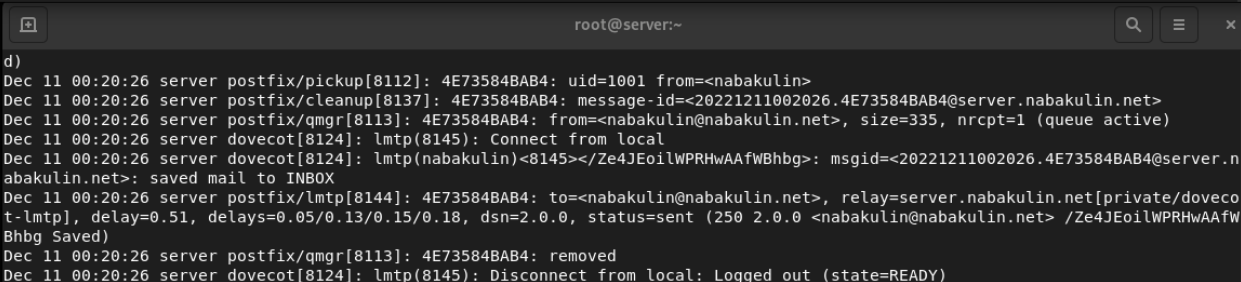
Рисунок 3

- 1.7. Перезапустите Postfix и Dovecot
- 1.8. Из-под учётной записи своего пользователя отправьте письмо с клиента (вместо user укажите ваш логин)
- 1.9. На сервере просмотрите почтовый ящик пользователя

```

[root@server.nabakulin.net ~]# postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lmtp'
[root@server.nabakulin.net ~]# systemctl restart postfix
[root@server.nabakulin.net ~]# systemctl restart dovecot
[root@server.nabakulin.net ~]# exit
logout
[nabakulin@server.nabakulin.net ~]$ echo .| mail -s "LMTP test" nabakulin@nabakulin.net
[nabakulin@server.nabakulin.net ~]$ MAIL=~/.Maildir/ mail
s-nail version v14.9.22. Type '?' for help
/home/nabakulin/Maildir: 5 messages 1 new 3 deleted
 4 nabakulin          2022-12-10 19:48  18/645  "test
>N 5 nabakulin@nabakulin. 2022-12-11 00:20  18/608  "LMTP test
& exit
[nabakulin@server.nabakulin.net ~]$

```



```

d)
Dec 11 00:20:26 server postfix/pickup[8112]: 4E73584BAB4: uid=1001 from=<nabakulin>
Dec 11 00:20:26 server postfix/cleanup[8137]: 4E73584BAB4: message-id=<20221211002026.4E73584BAB4@server.nabakulin.net>
Dec 11 00:20:26 server postfix/qmgr[8113]: 4E73584BAB4: from=<nabakulin@nabakulin.net>, size=335, nrcpt=1 (queue active)
Dec 11 00:20:26 server dovecot[8124]: lmtp(8145): Connect from local
Dec 11 00:20:26 server dovecot[8124]: lmtp(nabakulin)<8145></Ze4JEoilWPRHwAAfWBhbg>: msgid=<20221211002026.4E73584BAB4@server.nabakulin.net>; saved mail to INBOX
Dec 11 00:20:26 server postfix/lmtp[8144]: 4E73584BAB4: to=<nabakulin@nabakulin.net>, relay=server.nabakulin.net[private/dovecot-lmtp], delay=0.51, delays=0.05/0.13/0.15/0.18, dsn=2.0.0, status=sent (250 2.0.0 <nabakulin@nabakulin.net> /Ze4JEoilWPRHwAAfWBhbg Saved)
Dec 11 00:20:26 server postfix/qmgr[8113]: 4E73584BAB4: removed
Dec 11 00:20:26 server dovecot[8124]: lmtp(8145): Disconnect from local: Logged out (state=READY)

```

Рисунок 4

2.

2.1. В файле /etc/dovecot/conf.d/10-master.conf определите службу аутентификации пользователей

```

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 auth-userdb {
        mode = 0600
        user = dovecot
        #group =
    }

    # Postfix smtp-auth
    unix_listener /var/spool/postfix/private/auth {
        group = postfix
        user = postfix
        mode = 0600
    }

    # Auth process is run as this user.
    #user = $default_internal_user
}

```

Рисунок 5

2.2. Для Postfix задайте тип аутентификации SASL для smtpd и путь к соответствующему unix-сокету

2.3. 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)

2.4. В настройках Postfix ограничьте приём почты только локальным адресом SMTP сервера сети

2.5. Для проверки работы аутентификации временно запустим SMTP-сервер (порт 25) с возможностью аутентификации. Для этого необходимо в файле `/etc/postfix/master.cf` заменить строку

```
# =====  
# service type private unpriv chroot wakeup maxproc command + args  
#          (yes)   (yes)   (no)   (never) (100)  
# =====  
smtp      inet  n       -       n       -       -       smtpd -o smtpd_sasl_auth_enable=yes -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated,reject
```

Рисунок 6

2.6. Перезапустите Postfix и Dovecot

```
[root@server.nabakulin.net ~]# postconf -e 'smtpd_sasl_type = dovecot'  
[root@server.nabakulin.net ~]# postconf -e 'smtpd_sasl_path = private/auth'  
[root@server.nabakulin.net ~]# postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, permit_mynetworks, reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, permit'  
[root@server.nabakulin.net ~]# postconf -e 'mynetworks = 127.0.0.0/8'  
[root@server.nabakulin.net ~]# vi /etc/postfix/master.cf  
[root@server.nabakulin.net ~]# systemctl restart postfix  
[root@server.nabakulin.net ~]# systemctl restart dovecot  
Job for dovecot.service failed because the control process exited with error code.  
See "systemctl status dovecot.service" and "journalctl -xeu dovecot.service" for details.  
[root@server.nabakulin.net ~]# systemctl restart dovecot
```

Рисунок 7

2.7. На клиенте установите telnet

2.8. На клиенте получите строку для аутентификации, вместо username указав логин вашего пользователя, а вместо password указав пароль этого пользователя

2.9. Подключитесь на клиенте к SMTP-серверу посредством telnet (вместо user укажите ваш логин)

```
[root@client.nabakulin.net ~]# printf 'nabakulin\x00nabakulin\x00password' | base64
bmFiYWt1bGluAG5hYmFrdWxpbGwYXNzd29yZA==
[root@client.nabakulin.net ~]# telnet server.nabakulin.net 25
Trying 192.168.1.1...
Connected to server.nabakulin.net.
Escape character is '^]'.
220 server.nabakulin.net ESMTP Postfix
EHLO test
250-server.nabakulin.net
250-PIPELINING
250-SIZE 10240000
250-VRIFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN bmFiYWt1bGluAG5hYmFrdWxpbGwYXNzd29yZA==
235 2.7.0 Authentication successful
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Рисунок 8

3.

- 3.1. 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)
- 3.2. Для того чтобы запустить SMTP-сервер на 587-м порту, в файле /etc/postfix/master.cf замените строки

```
# =====
# service type private unpriv chroot wakeup maxproc command + args
# (yes) (yes) (no) (never) (100)
# =====
smtp inet n - n - - smtpd
#smtp inet n - n - 1 postscreen
#smtpd pass - - n - - smtpd
#dnsblog unix - - n - 0 dnsblog
#tlsproxy unix - - n - 0 tlsproxy
submission inet n - n - - smtpd -o smtpd_sasl_auth_enable=yes -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated,reject
```

Рисунок 9

- 3.3. Настройте межсетевой экран, разрешив работать службе smtp-submission
- 3.4. Перезапустите Postfix

```
[root@server.nabakulin.net ~]# cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
[root@server.nabakulin.net ~]# cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
[root@server.nabakulin.net ~]# postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
[root@server.nabakulin.net ~]# postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
[root@server.nabakulin.net ~]# postconf -e 'smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_scache'
[root@server.nabakulin.net ~]# postconf -e 'smtpd_tls_security_level = may'
[root@server.nabakulin.net ~]# postconf -e 'smtp_tls_security_level = may'
[root@server.nabakulin.net ~]# vi /etc/postfix/master.cf
[root@server.nabakulin.net ~]# vi /etc/postfix/master.cf
[root@server.nabakulin.net ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps apcupsd audit bacula bacula-client bb bgp bitco
in bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine cockpit collectd condor-collector ctdb
dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-
server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-c
lient ganglia-master git grafana gre high-availability http https imap imaps ipp ipp-client ipsec irc ircs iscsi-target isns je
nkins kadmin kdeconnect kerberos kibana klogon kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-controller-
manager kube-scheduler kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr managesieve matrix mdns memcache m
inidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovir
t-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmpoxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus pr
oxy-dhcp ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba
samba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroak-lansync spotify-sync squid ssdp ssh
ssh-custom steam-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-so
cks transmission-client upnp-client vdsms vnc-server wbem-http wbem-https wireguard wsman wsmans xdmcp xmpp-bosh xmpp-client xmp
p-local xmpp-server zabbix-agent zabbix-server
[root@server.nabakulin.net ~]# firewall-cmd --add-service=smtp-submission
success
[root@server.nabakulin.net ~]# firewall-cmd --add-service=smtp-submission --permanent
success
[root@server.nabakulin.net ~]# firewall-cmd --reload
success
[root@server.nabakulin.net ~]# systemctl restart postfix
```

Рисунок 10

3.5. На клиенте подключитесь к SMTP-серверу через 587-й порт посредством openssl (вместо user используйте свой логин)

```
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 7200 (seconds)
TLS session ticket:
0000 - ff f1 eb 58 3c 69 74 b2-de 62 43 4d b2 0b 73 32    ...X<it..bCM..s2
0010 - 24 ee 80 f9 69 49 0a 78-12 8a 51 da c6 10 17 eb    $....iI.x...Q....
0020 - 66 16 24 e1 eb c1 e2 93-26 7e 46 85 67 ec bf 0b    f.$.....&-F.g...
0030 - 1a 7e 7a 81 30 fc cc f6-89 c7 e7 d5 90 f3 e4 83    .~z.0.....
0040 - 8e 69 1a d1 14 07 6b e9-28 ef 75 49 e0 20 c0 4c    .i....k.(.uI. .L
0050 - 74 dd 73 a5 12 ac a9 7c-dd 5d c9 b5 11 76 df 02    t.s....|.].v..
0060 - a3 01 d2 4d 94 f8 62 7f-53 20 18 e2 17 7f 28 99    ...M..b.S ....(
0070 - 19 a6 61 82 c4 c7 de ab-15 24 e7 53 3f 65 58 4d    ..a.....$.S?eXM
0080 - d8 a7 84 77 0d e6 28 bd-9a 88 36 61 27 32 dd a1    ...w..(...6a'2..
0090 - ac 37 eb 72 c6 a8 9d 2a-59 15 07 fc 9b 6a 13 4d    .7.r...*Y....j.M
00a0 - 7b 1c 31 60 01 16 32 88-98 cd 9e 84 a7 1e c3 ed    {.l'..2.....
00b0 - 22 db 67 19 c4 82 db 9f-35 3e f9 4c a4 32 c0 70    ".g.....5>.L.2.p
00c0 - 64 36 7f d9 aa 4c 21 ee-45 4d 58 88 c8 cb 93 2f    d6...L!.EMX..../

Start Time: 1670719002
Timeout : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0
---
read R BLOCK
EHLO test
250-server.nabakulin.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250-CHUNKING
AUTH PLAIN bmFiYWtlbGluAG5hYmFrdWxpbGwYXNzd29yZA==
235 2.7.0 Authentication successful
```

Рисунок 11

3.6. 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

The screenshot shows the 'Server Type: SMTP' configuration window in the Evolution mail client. The 'Description' field states: 'For delivering mail by connecting to a remote mailhub using SMTP.' Under the 'Configuration' section, the 'Server' field is set to 'mail.nabakulin.net' and the 'Port' is set to '587'. The checkbox 'Server requires authentication' is checked. Under the 'Security' section, the 'Encryption method' is set to 'STARTTLS after connecting'. Under the 'Authentication' section, the 'Type' is set to 'Check for Supported Types' and 'PLAIN'. The 'Username' field is set to 'nabakulin'.

Рисунок 12

	nabakulin <nabakulin@...>	test	Yesterday 19:48
	nabakulin@nabakulin....	LMTP test	Today 00:20
	nabakulin <nabakulin...>	test tls	Today 00:39

Рисунок 13

4. 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

```
[root@server.nabakulin.net ~]# cd /vagrant/provision/server
[root@server.nabakulin.net server]# cp -R /etc/dovecot/dovecot.conf /vagrant/provision/server/mail/etc/dovecot/
cp: overwrite '/vagrant/provision/server/mail/etc/dovecot/dovecot.conf'? y
[root@server.nabakulin.net server]# cp -R /etc/dovecot/conf.d/10-master.conf /vagrant/provision/server/mail/etc/dovecot/conf.d/
[root@server.nabakulin.net server]# cp -R /etc/dovecot/conf.d/10-auth.conf /vagrant/provision/server/mail/etc/dovecot/conf.d/
cp: overwrite '/vagrant/provision/server/mail/etc/dovecot/conf.d/10-auth.conf'? y
[root@server.nabakulin.net server]# cp -R /etc/postfix/master.cf /vagrant/provision/server/mail/etc/postfix/
```

Рисунок 14

4.1. 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 s-nail
dnf -y install dovecot 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 = nabakulin.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

```

Рисунок 15

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

```
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install postfix
dnf -y install s-nail
dnf -y install evolution
dnf -y install telnet

echo "Configure postfix"
postconf -e 'inet_protocols = ipv4'

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

Рисунок 16

Контрольные вопросы

1. Какие функции выполняет почтовый Relay-сервер?
Пересылает почту
2. Какие угрозы безопасности могут возникнуть в случае настройки почтового сервера как Relay-сервера?
Спам и вредоносные рассылки