Лабораторная работа №10

СТУДЕНТ: САХНО

ГРУППА: НФИБД-02-23

Цель

Приобрести практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.

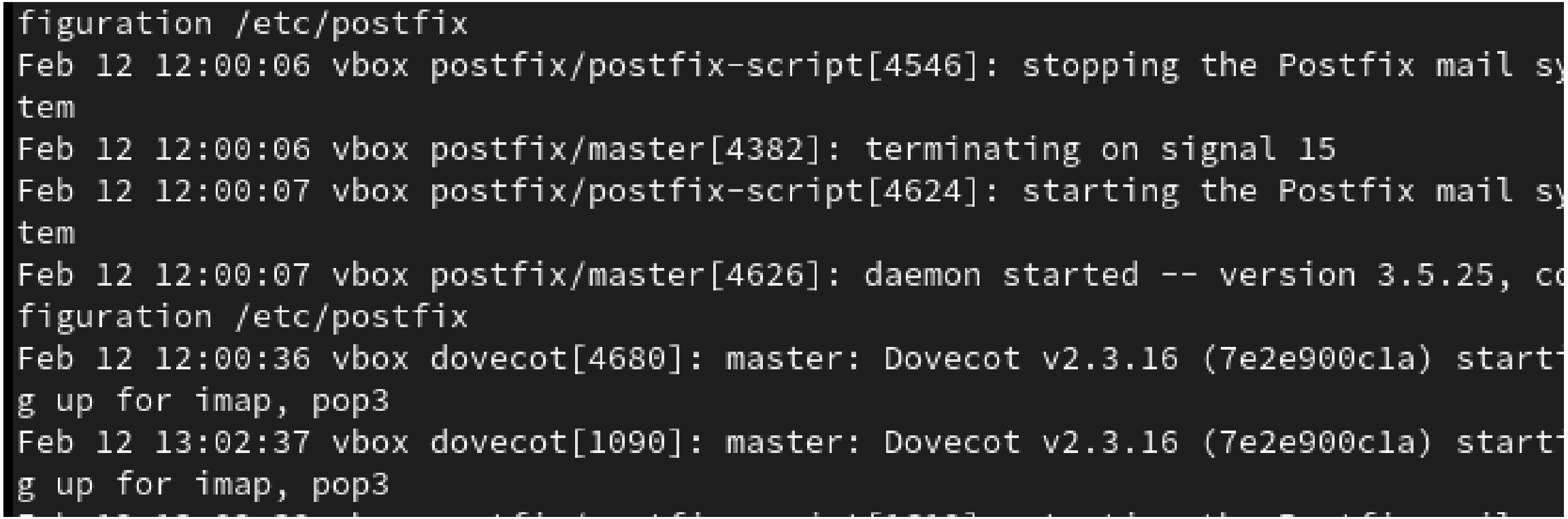
Задания

Настроить Dovecot для работы с LMTP.

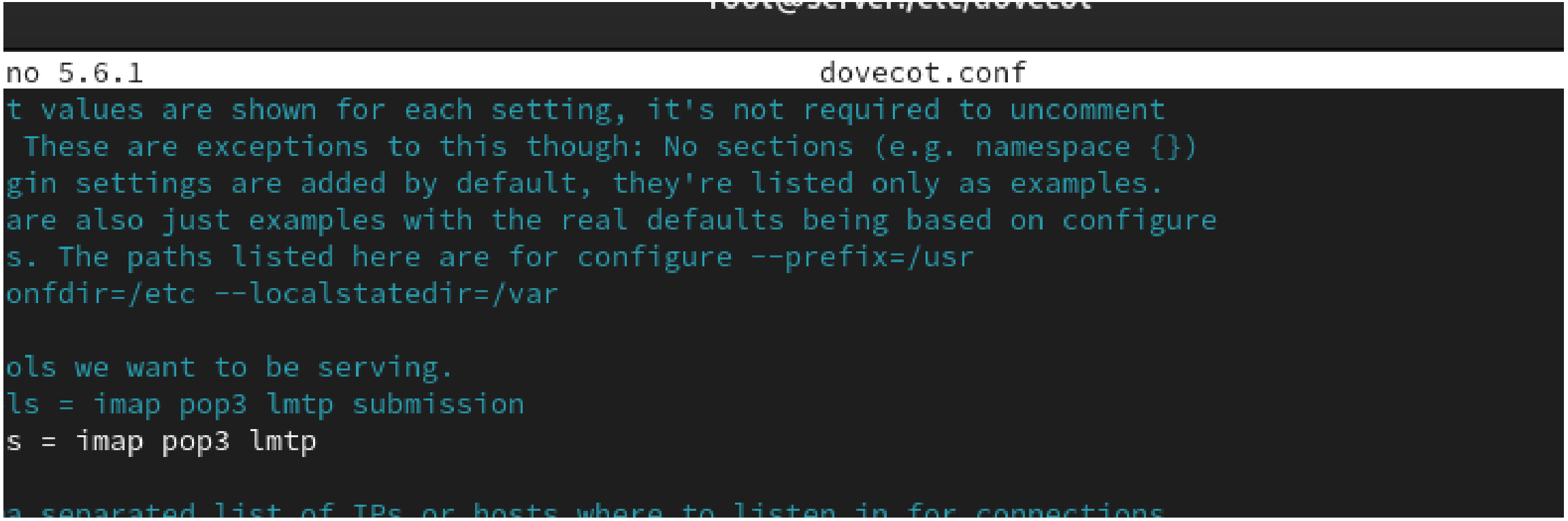
Настроить аутентификацию посредством SASL на SMTP-сервере.

Настроить работу SMTP-сервера поверх TLS.

Скорректировать скрипт для Vagrant, фиксирующий действия расширенной настройки SMTP-сервера во внутреннем окружении виртуальной машины server.


figuration /etc/postfix
Feb 12 12:00:06 vbox postfix/postfix-script[4546]: stopping the Postfix mail sy
tem
Feb 12 12:00:06 vbox postfix/master[4382]: terminating on signal 15
Feb 12 12:00:07 vbox postfix/postfix-script[4624]: starting the Postfix mail sy
tem
Feb 12 12:00:07 vbox postfix/master[4626]: daemon started -- version 3.5.25, co
figuration /etc/postfix
Feb 12 12:00:36 vbox dovecot[4680]: master: Dovecot v2.3.16 (7e2e900c1a) start
g up for imap, pop3
Feb 12 13:02:37 vbox dovecot[1090]: master: Dovecot v2.3.16 (7e2e900c1a) start
g up for imap, pop3

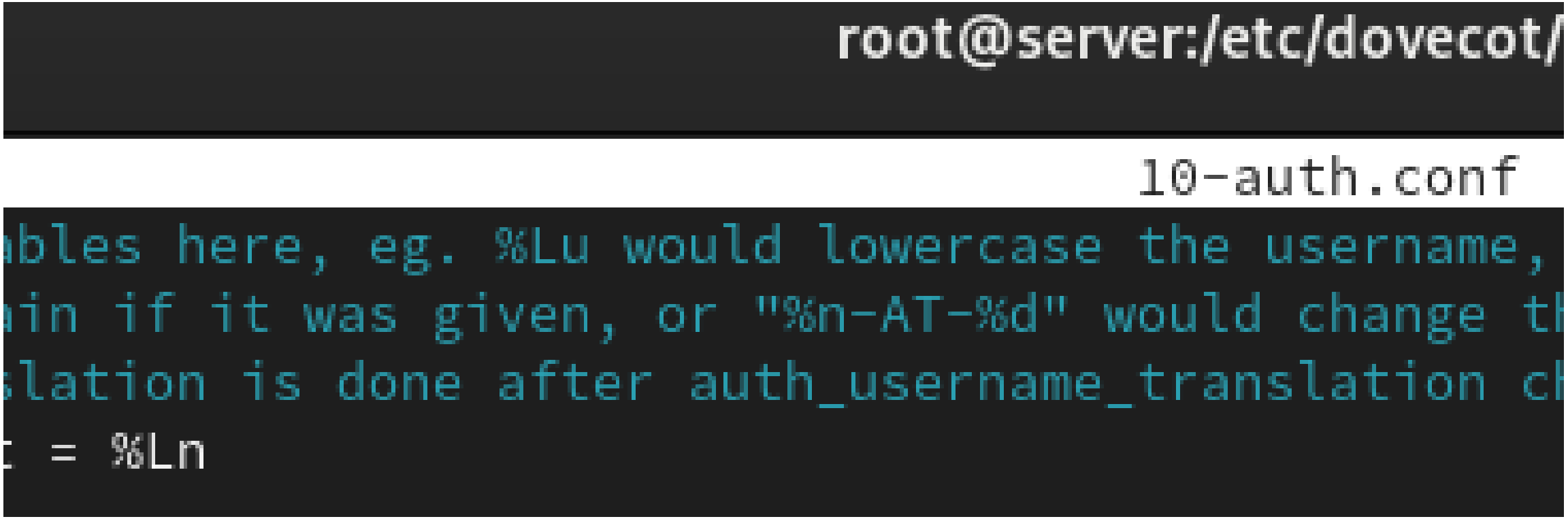
Задание №1


no 5.6.1
dovecot.conf
t values are shown for each setting, it's not required to uncomment
These are exceptions to this though: No sections (e.g. namespace {})
gin settings are added by default, they're listed only as examples.
are also just examples with the real defaults being based on configure
s. The paths listed here are for configure --prefix=/usr
onfdir=/etc --localstatedir=/var
ols we want to be serving.
ls = imap pop3 lmtp submission
s = imap pop3 lmtp

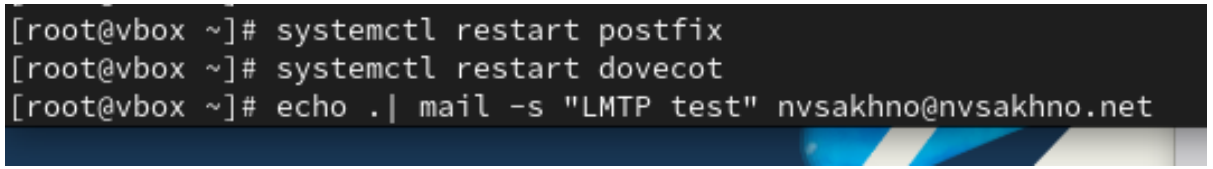
Задание №1

```
  GNU nano 5.6.1                                    10-master.conf
  }
}

service submission-login {
  inet_listener submission {
    #port = 587
  }
}

service lmtp {
  unix_listener /var/spool/postfix/private/dovecot-lmtp {
        group = postfix
        user = postfix
        mode = 0600
        }
```

Задание №1


root@server:/etc/dovecot/
10-auth.conf
ables here, eg. %Lu would lowercase the username,
ain if it was given, or "%n-AT-%d" would change th
slation is done after auth_username_translation ch
= %Ln

Задание №1


[root@vbox ~]# systemctl restart postfix
[root@vbox ~]# systemctl restart dovecot
[root@vbox ~]# echo .| mail -s "LMTP test" nvsakhno@nvsakhno.net

Задание №1

```
  GNU nano 5.6.1                                  10-master.conf
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).
```

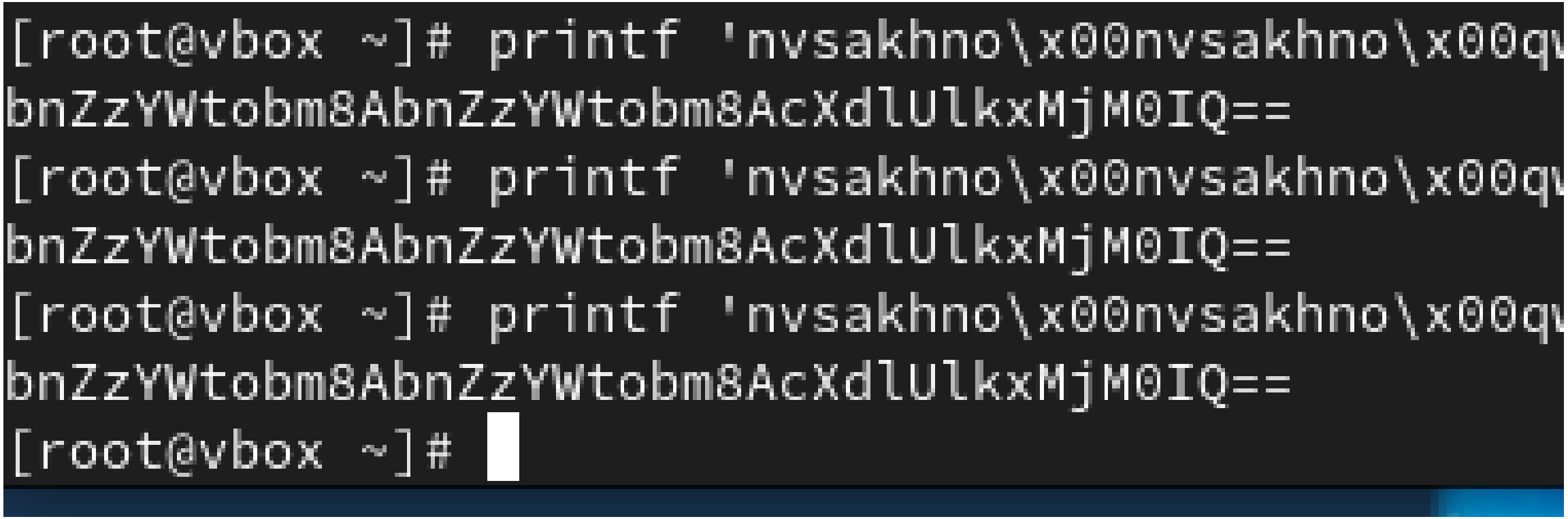
Задание №2

```
ot@vbox ~]# postconf -e 'smtpd_recipient_rest
eject_unknown_recipient_domain, permit_mynetw
eject_non_fqdn_recipient, reject_unauth_dest
eject_unverified_recipient, permit'
tconf: fatal: -e, -X, or -# accepts no multi-
ot@vbox ~]# postconf -e 'mynetworks = 127.0.0
ot@vbox ~]#
```

Задание №2

```
# ==========================================================================
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 syslog_name=postfix/submission
#  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_tls_auth_only=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
  -o smtpd_recipient_restrictions==reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated,rejec
#  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
#smtps     inet  n       -       n       -       -       smtpd
```

Задание №2


[root@vbox ~]# printf 'nvsakhno\x00nvsakhno\x00qv
bnZzYWtobm8AbnZzYWtobm8AcXdlUlkxMjM0IQ==
[root@vbox ~]# printf 'nvsakhno\x00nvsakhno\x00qv
bnZzYWtobm8AbnZzYWtobm8AcXdlUlkxMjM0IQ==
[root@vbox ~]# printf 'nvsakhno\x00nvsakhno\x00qv
bnZzYWtobm8AbnZzYWtobm8AcXdlUlkxMjM0IQ==
[root@vbox ~]#

Задание №2

```
t/certs/dovecot.pem /etc/pki/tls/certs
t/private/dovecot.pem /etc/pki/tls/private
tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
tls_key_file=/etc/pki/tls/private/dovecot.pem'
tls_session_cache_database = btree:/var/lib/postfix/sm

tls_security_level = may'
tls_security_level = may'
```

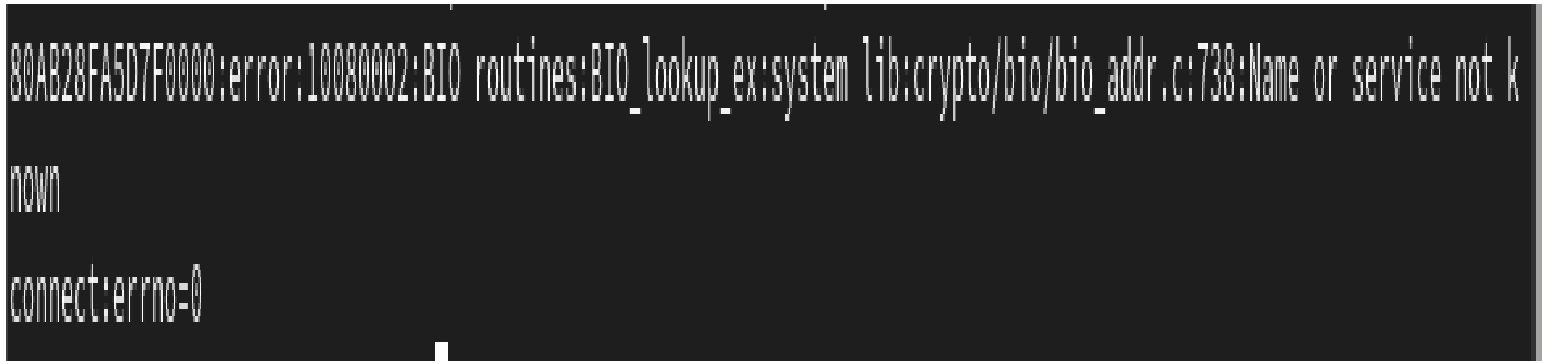
Задание №2

```
#               (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 syslog_name=postfix/submission
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_tls_auth_only=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
  -o smtpd_recipient_restrictions==reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated,r>
#  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
```

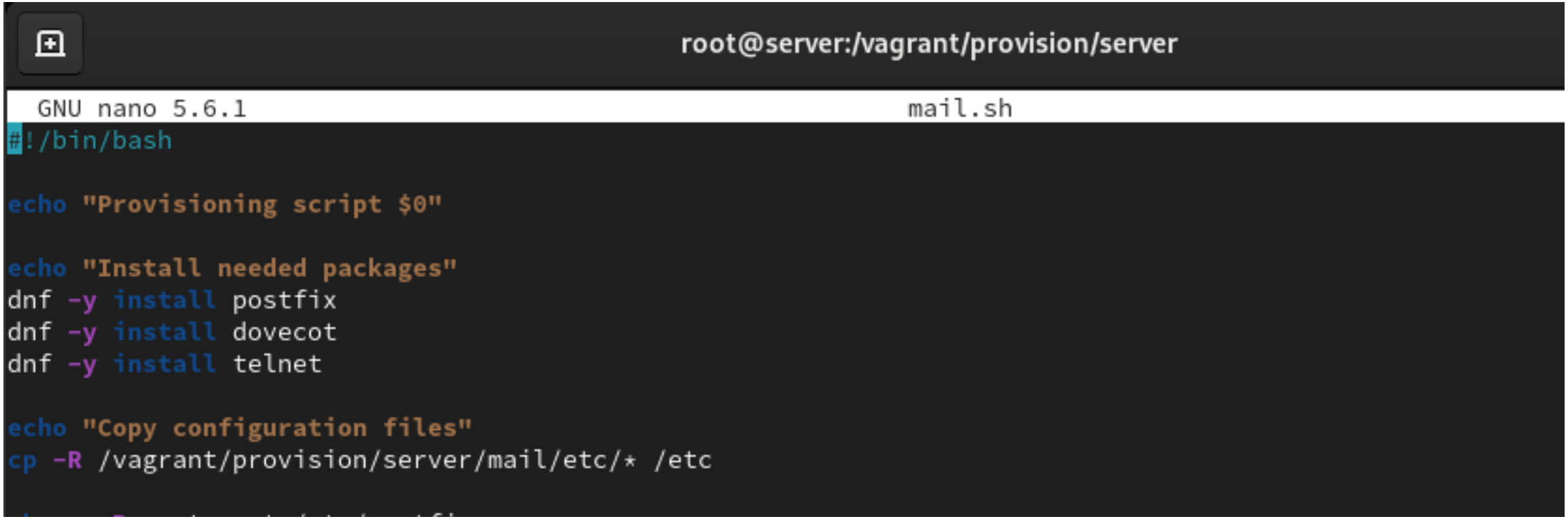
Задание №2

```
[root@server.dmbelicheva.net postfix]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacu
la-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine checkmk-ag
ent cockpit collectd condor-collector cratedb ctdb dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry dock
er-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeip
a-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability
 http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jellyfin jenkins kadmin kdeconnec
t kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-c
ontroller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker
kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-tcp llmnr-udp manage
sieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd netbios-ns netdata-da
shboard nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwe
bapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps3netsrv ptp pulseaudio pupp
etmaster 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 snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssd
p ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tile38
tinc tor-socks transmission-client upnp-client vdsm vnc-server wbem-http wbem-https wireguard ws-discovery ws-discovery-c
lient ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabb
ix-server zerotier
```

Задание №2


80AB28FA5D7F0000:error:10080002:BIO routines:BIO_lookup_ex:system lib:crypto/bio/bio_addr.c:738:Name or service not k
nown
connect:errno=0

Задание №2


root@server:/vagrant/provision/server
GNU nano 5.6.1
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

Задание №2

Контрольные вопросы

Приведите пример задания формата аутентификации пользователя в Dovecot в форме логина с указанием домена.

auth_username_format = %Lu%d

Какие функции выполняет почтовый Relay-сервер?

обеспечивает приём сообщения, временное хранение (часто не больше нескольких минут в случае мгновенных сообщений, до недели в случае электронной почты), пересылку сообщения узлу-получателю (или следующему релею)

Какие угрозы безопасности могут возникнуть в случае настройки почтового сервера как Relay-сервера?

спам, перехват и изменение электронных сообщений.

Вывод:

В процессе выполнения данной лабораторной работы я приобрел практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.