Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра интеллектуальных информационных технологий

**Отчет по лабораторной работе №4 по курсу «СиМОИБ»**

**на тему: «Настройка и конфигурирование сервера электронной почты»**

Выполнил студент группы 021702:             Локтев К.А.

Проверил:  Захаров В.В.

**МИНСК 2022**

**Тема:**

Настройка и конфигурирование сервера электронной почты.

**Цель работы:**

Ознакомиться с аспектами настройки и конфигурирования сервера электронной почты.

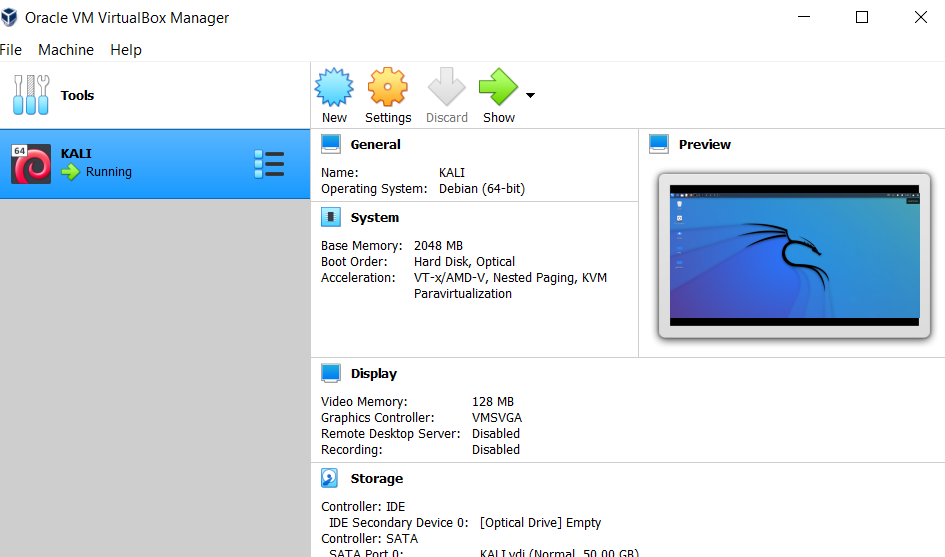
**Задания:**

1. На основном компьютере запустить Виртуальную машину. Измените имя компьютера на уникальное.
2. Установите почтовый сервер. Добавьте пользователей.
3. Сконфигурируйте SMTP сервер без аутентификации отправителя. С помощью клиента Telnet соединитесь с SMTP сервером  (open <адрес>  <port>) , убедитесь, что можно отправить сообщение без авторизации.
4. С помощью клиента Telnet соединитесь с POP3 сервером  (open <адрес>  <port>)  получите сообщения.
5. Сконфигурируйте SMTP сервер с аутентификацией отправителя. Убедитесь, что SMTP сервер требует авторизации (защита от анонимной рассылки).
6. Оформите отчет. В отчет протоколы telnet-сессий.

**Выполнение заданий:**

1) В качестве виртуальной машины была использована kali linux, основанная на debian x64. Всё, что зафиксировано в данном отчёте, дало бы схожие результаты на большинстве unix-систем.

**Виртуальная машина и ее конфигурации:**

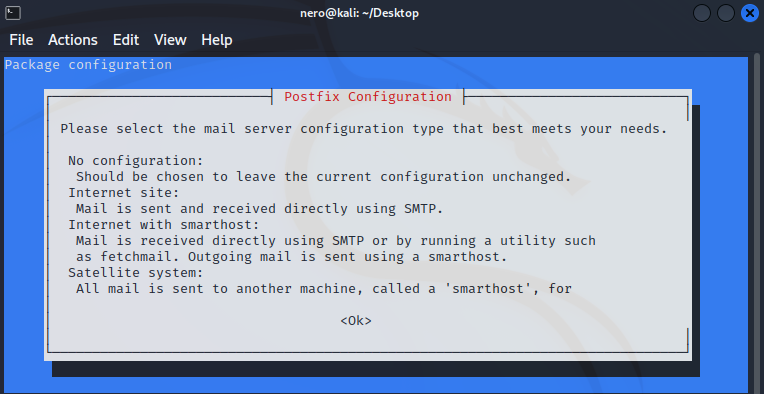


2) Для настройки сервера был выбран пакет Postfix. Postfix – это популярный среди системных администраторов выбор, стандартный почтовый сервер в большинстве современных дистрибутивов Linux.

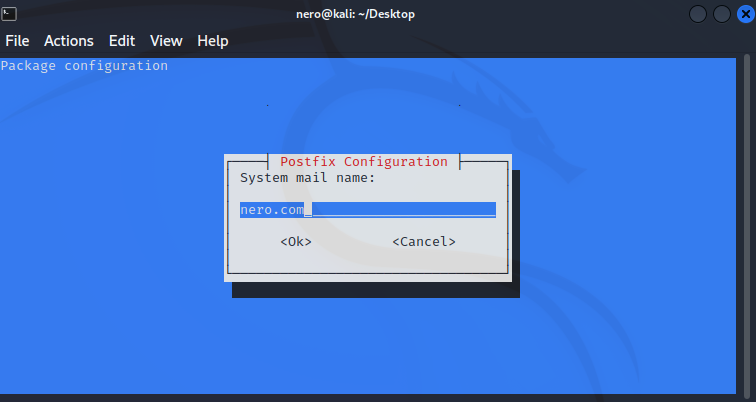
1: **sudo apt-get update**

2: **sudo apt-get -y install postfix**

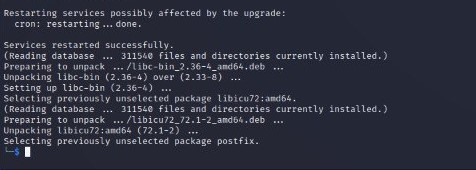
После ввода этих команд в терминал, откроется окно конфигурации postfix. Нас интересует **internet site** конфигурация. Она может отправлять и принимать почтовые отправления.



3: **Присвоение имени системной почте.**

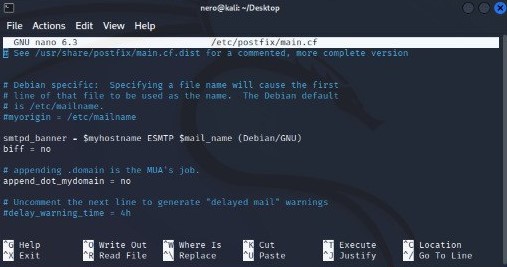


4: **Перезагрузка сервера**



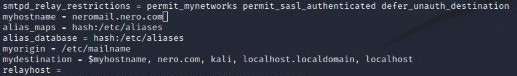
5: **sudo nano /etc/postfix/main.cf**

Далее настраиваем postfix-конфигурацию.



**myhostname:** этот параметр используется для указания имени хоста почтовой системы. Это имя хоста в интернете, для которого Postfix будет получать почту.

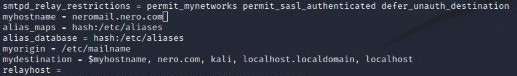
<<**myhostname = neromail.nero.com>>**



**mydomain:** эта настройка позволяет указать почтовый домен, обслуживанием которого занимается сервер, например, example.com:

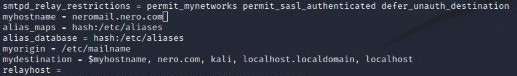
я сразу вписал на вторую позицию в **mydestination**

<<**mydomain=nero.com>>**

****

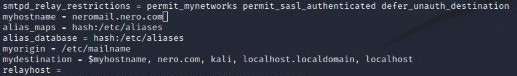
**myorigin:** Этот параметр позволяет указать доменное имя, используемое в почте, отправленной с сервера.

<<**myorigin =** /etc/mailname>>



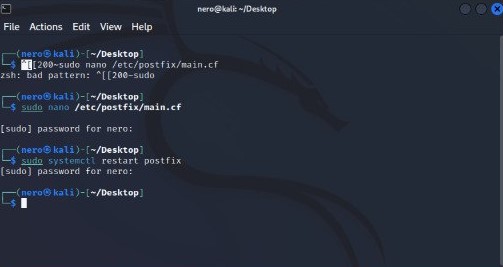
**mydestination:** Этот параметр содержит список доменов, которые сервер Postfix будет считать конечными пунктами назначения для входящей почты.

<<**mydestination = $myhostname, nero.com, kali, localhost.localdo…>>**

****

6: **sudo systemctl restart postfix**

Сохраняем изменения и перезагружаем postfix.

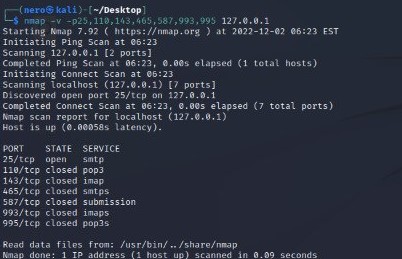


7: echo "This is the body of the email" | mail -s "This is the subject line" neromail.nero.com



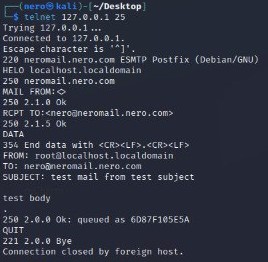
В /var/log/mail.log появилось запись с флагом send. Это значит, что настройка прошла успешно, и всё работает.

3) Соединяемся по telnet c нашим почтовым сервером, перед этим проверив, свободен ли порт.



Порт свободен; подключаемся к серверу.

Сессия telnet



Разбор сессии:

**HELO localhost.localdomain - приветствие**

**MAIL FROM: <> - email от нас**

**RCPT TO: email для**

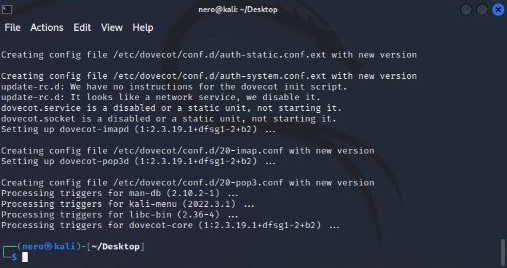
**DATA - составляем письмо**

**QUIT - завершение работы(прощание)**

4) Так как пока что был настроен только протокол SMTP, то следует продолжить настраивать сервер, чтобы получить возможность получать письма с авторизацией и по протоколам POP3 и IMAP.

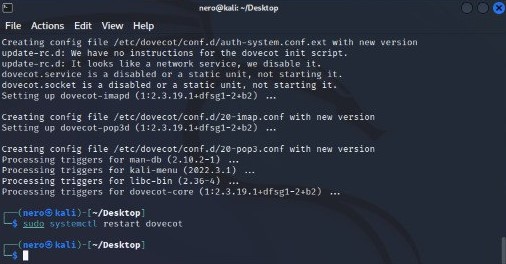
1: sudo apt-get install dovecot-imapd dovecot-pop3d

Установка пакета dovecot

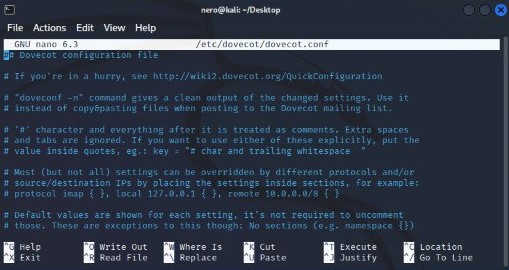


2: sudo systemctl restart dovecot

Перезапуск сервиса для корректной работы

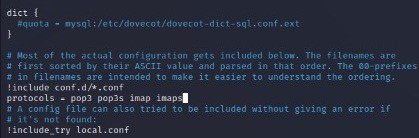


3: sudo nano /etc/dovecot/dovecot.conf



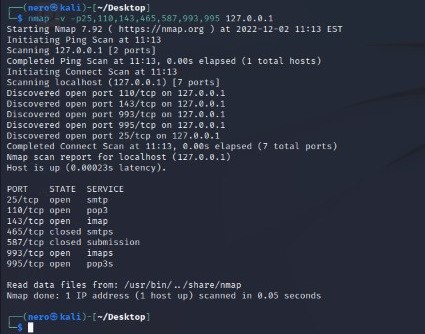
Настройка конфигурации

<<**protocols = pop3 pop3s imap imaps**>>

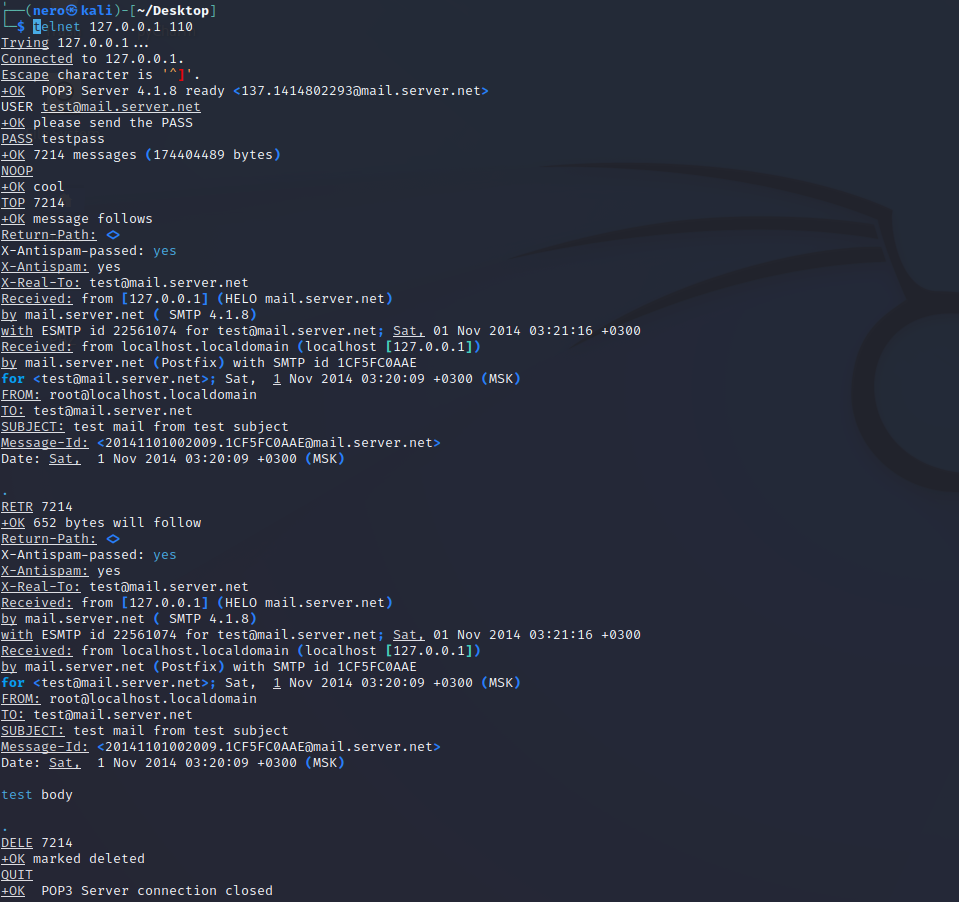


4: Проверяем что нужные порты открыты

**nmap -v -p25,110,143,465,587,993,995 127.0.0.1**

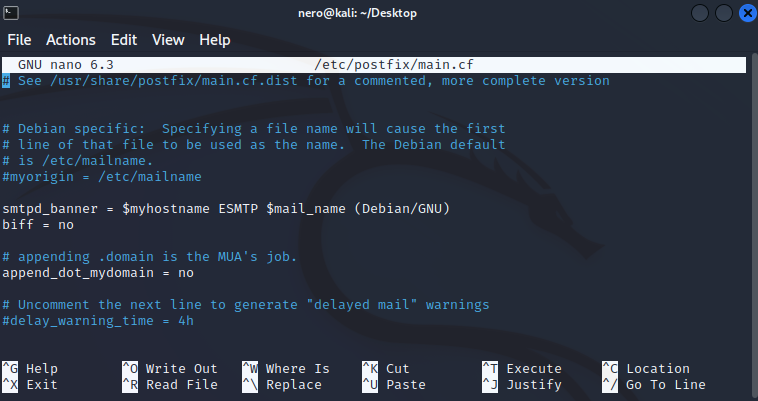
****

Telnet сессия по получения письма по POP3



5) Добавляем авторизацию в POSTFIX и DOVECOT

1: sudo nano etc/postfix/main.cf



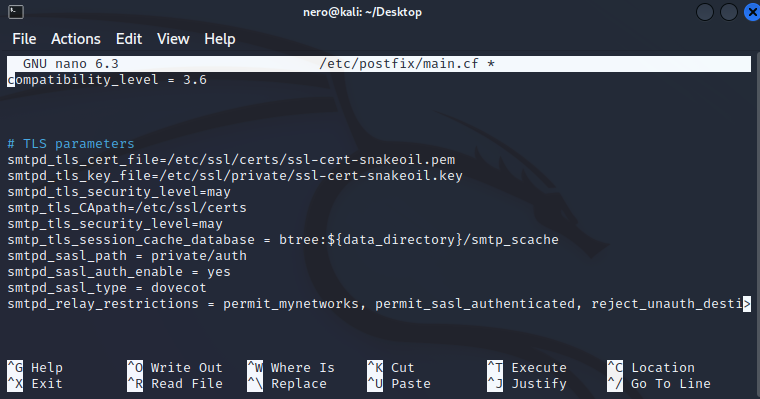
Открываем файл конфигурации postfix и добавляем следующее:

smtpd\_sasl\_path = private/auth

smtpd\_sasl\_auth\_enable = yes

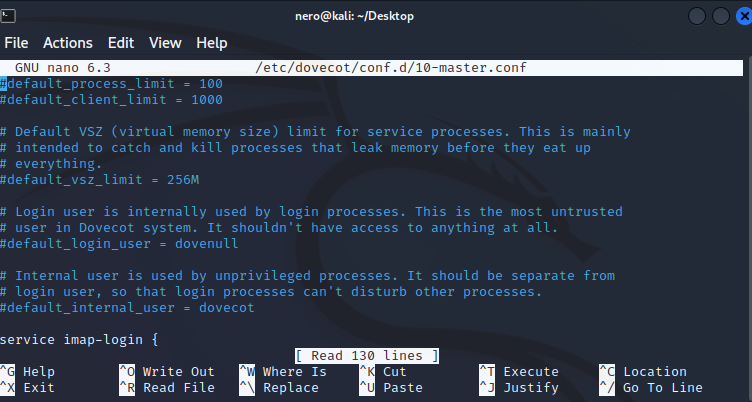
smtpd\_sasl\_type = dovecot

smtpd\_relay\_restrictions = permit\_mynetworks, permit\_sasl\_authenticated, reject\_unauth\_destination

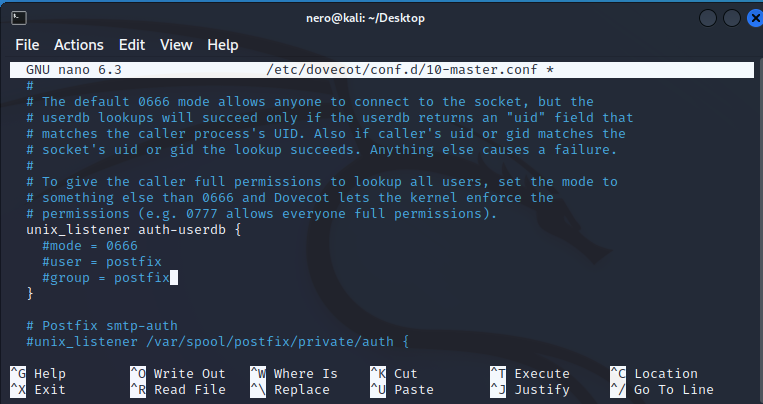


(где **smtpd\_sasl\_path** — путь до плагина аутентификации по механизму SASL; **smtpd\_sasl\_auth\_enable** — разрешает или запрещает аутентификацию по механизму SASL; smtpd\_sasl\_type — тип плагина, который используется для SASL-аутентификации; **smtpd\_relay\_restrictions** — правила разрешения и запрета использования MTA при пересылке.)

2: sudo nano /etc/dovecot/conf.d/10-master.conf

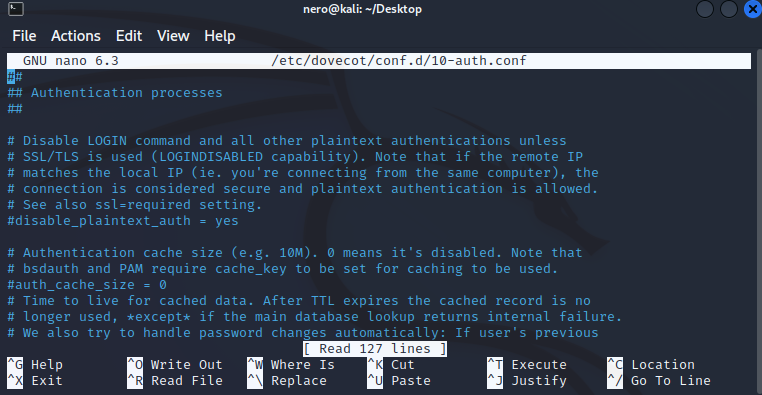


Открываем настройки аутентификации в dovecot, и приводим опцию **service auth** к следующему виду:

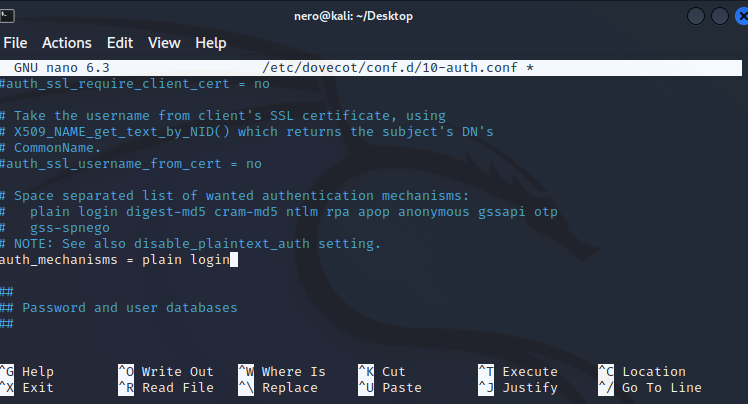


3: Настройки аутентификации приводим к следующему виду:

sudo nano /etc/dovecot/conf.d/10-auth.conf



auth\_mechanisms = plain login



В этом же файле проверяем, что снят комментарий со следующей строки:

!include auth-system.conf.ext

4: перезапускаем dovecot и postfix

Проверяем авторизацию:

**Вывод:**

В ходе выполнения лабораторной работы были изучены основы построения безопасных приложений и способыобеспечения безопасного соединения с сервером.

Как было выяснено ещё в третьей лабораторной работе, в современном мире при использовании сети интернет необходимо использовать протокол HTTPS, а не устаревший HTTP, в интересах собственной же безопасности. “Общение” через протокол HTTPS происходит в два этапа: handshake (ассиметричное шифрование) и обмен данными (симметричное шифрование).

Протокол HTTPS является, по сути, тем же HTTP с шифрующей “прослойкой” в виде TLS или SSL (TSL является более современной и безопасной).