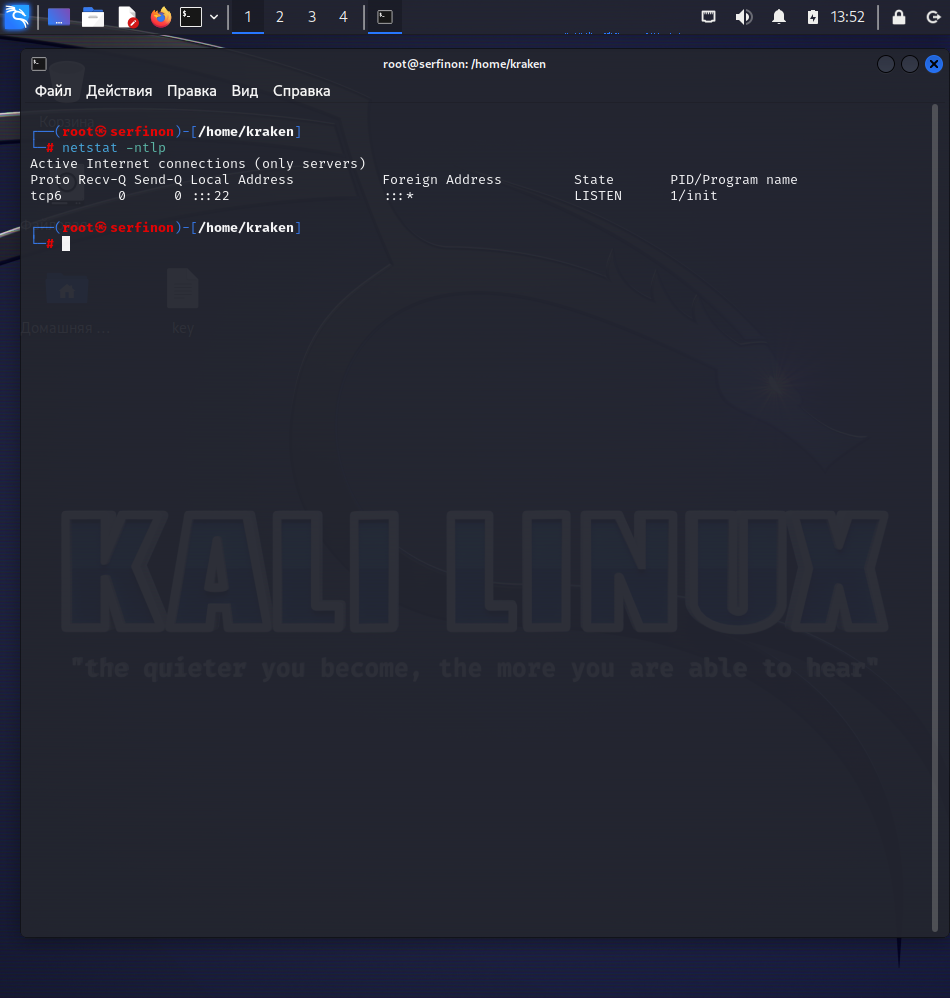
**Цель практической работы**

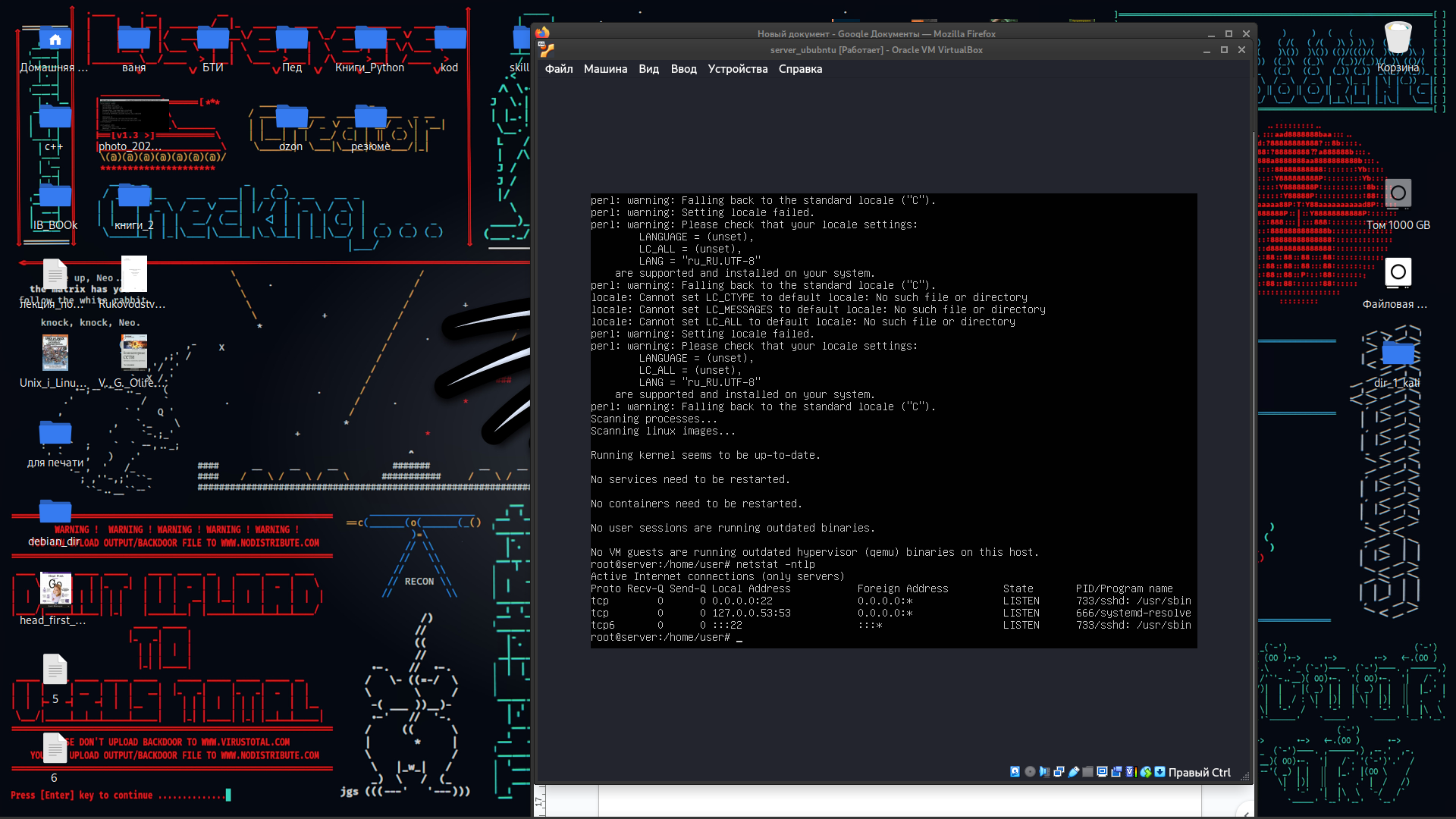
Вы научитесь составлять правила iptables, направленные на блокировку/пропуск трафика по определённым признакам.

**Задание 1. Установка sshd на Ubuntu**

Запустил команду netstat -ntlp, чтобы показать, что демон SSH (sshd) работает на tcp-порту и прослушивает входящие запросы на подключение



На Ubuntu Server ssh поставил при установке.

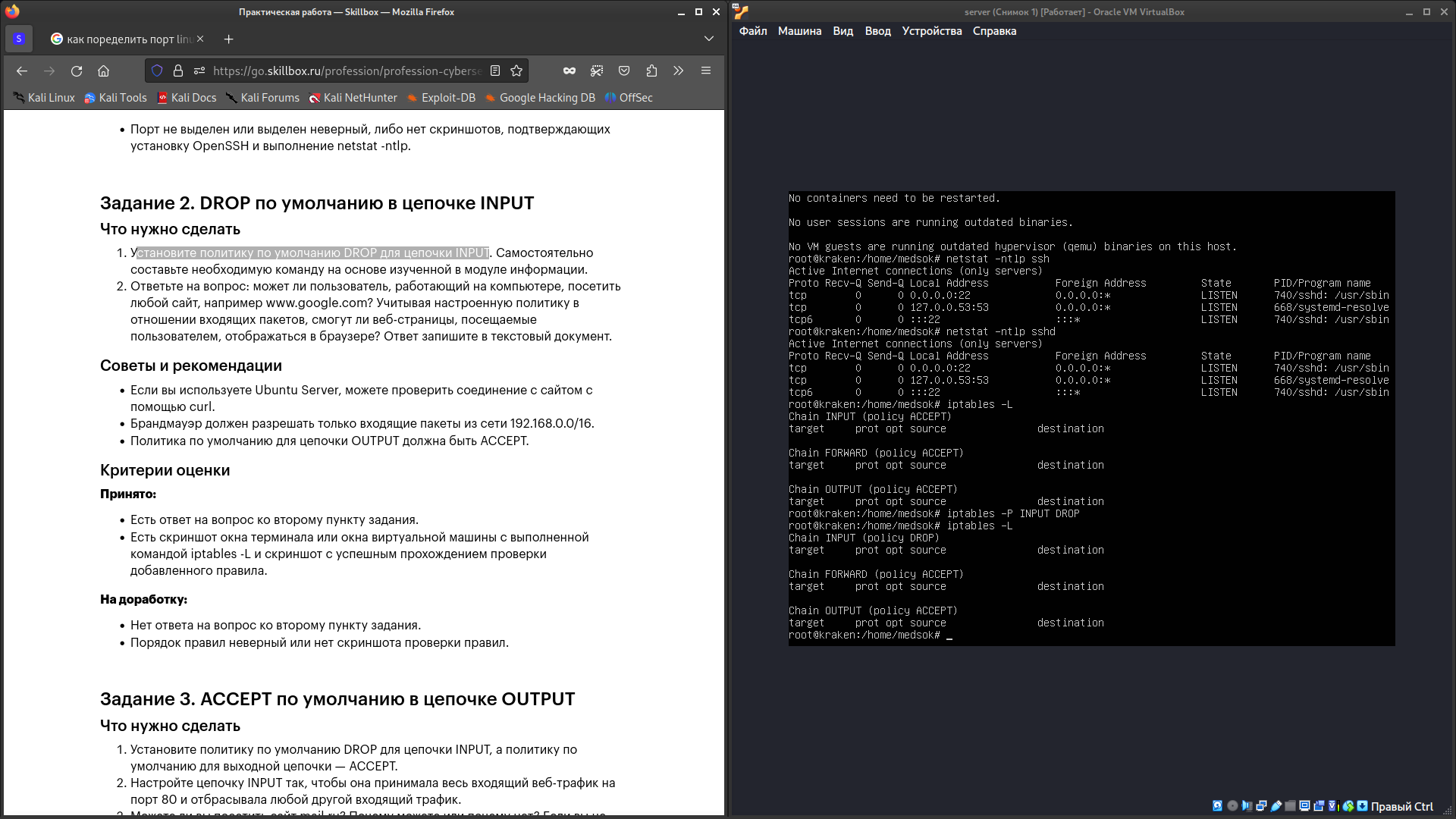


ssh работает на 22 порту по умолчанию, это мы можем наблюдать при выводе команды netstat -ntlp

**Задание 2. DROP по умолчанию в цепочке INPUT**

1.Установил политику по умолчанию DROP для цепочки INPUT.

команда : $ sudo iptables -P INPUT DROP



2.Ответьте на вопрос: может ли пользователь, работающий на компьютере, посетить любой сайт, например www.google.com? Учитывая настроенную политику в отношении входящих пакетов, смогут ли веб-страницы, посещаемые пользователем, отображаться в браузере?

Ответ:

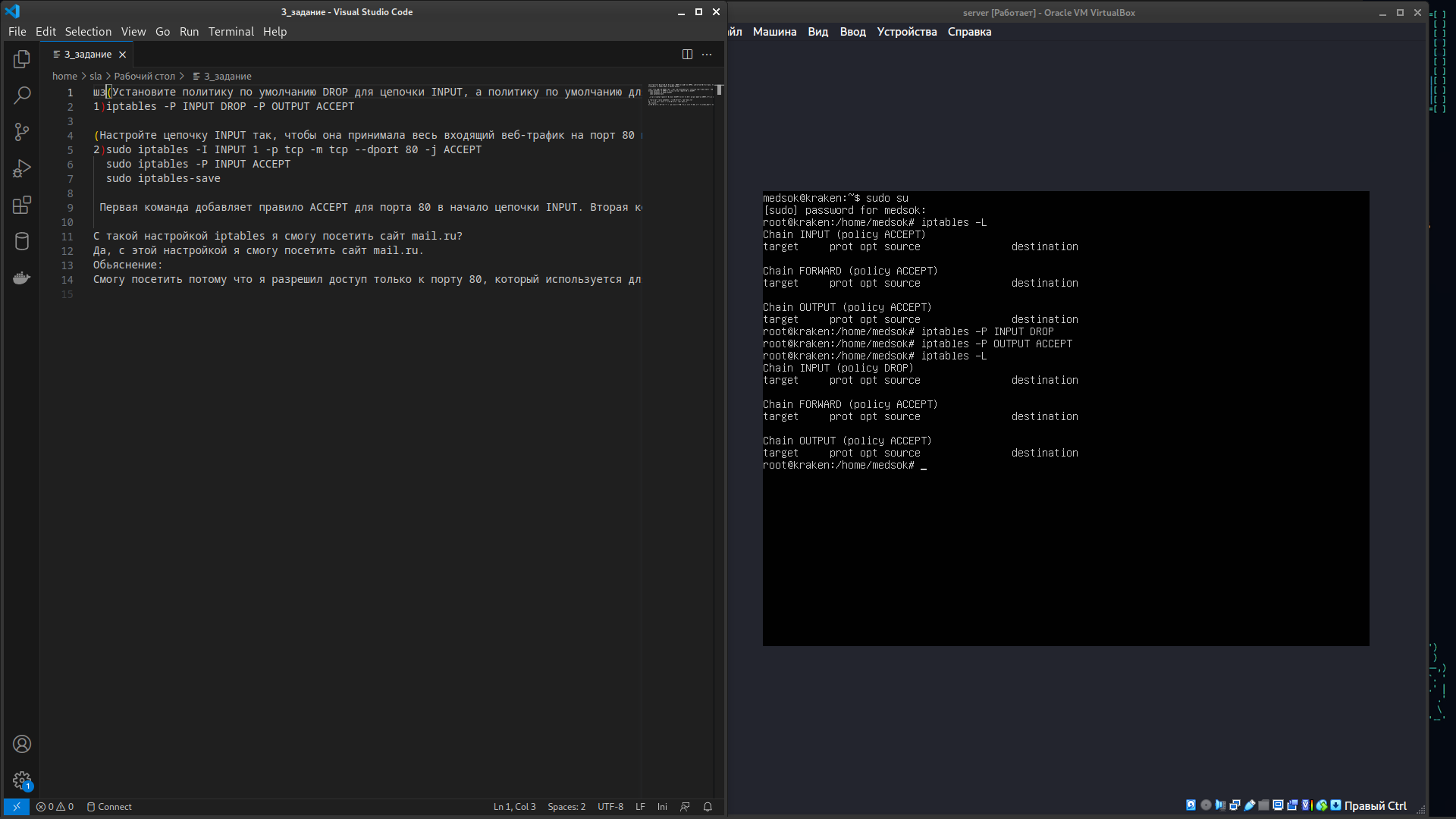
Да, пользователь может посещать любые сайты. Политика INPUT DROP означает блокировку всех входящих пакетов, включая HTTP-запросы, которые используются для загрузки веб-страниц. Однако, это может привести к блокировке доступа к некоторым сайтам, особенно если они используют нестандартные порты или протоколы., пользователь может посещать любые сайты. Политика INPUT DROP означает блоки

ровку всех входящих пакетов, включая HTTP-запросы, которые используются для загрузки веб-страниц. Однако, это может привести к блокировке доступа к некоторым сайтам, особенно если они используют нестандартные порты или протоколы.

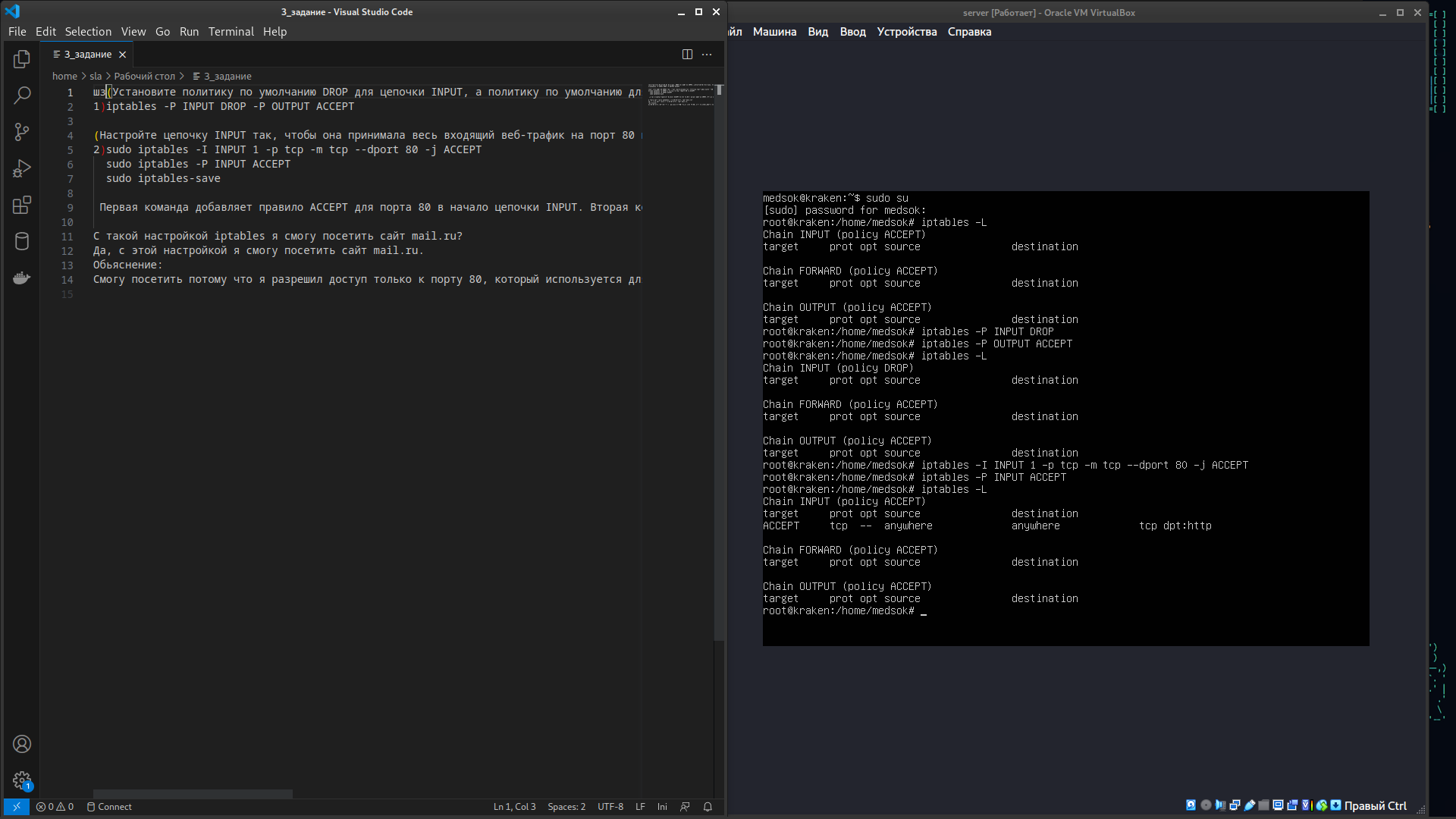
#### **Задание 3. ACCEPT по умолчанию в цепочке OUTPUT**

##### Что нужно сделать

1.Установите политику по умолчанию DROP для цепочки INPUT, а политику по умолчанию для выходной цепочки — ACCEPT.



2.Настройте цепочку INPUT так, чтобы она принимала весь входящий веб-трафик на порт 80 и отбрасывала любой другой входящий трафик.

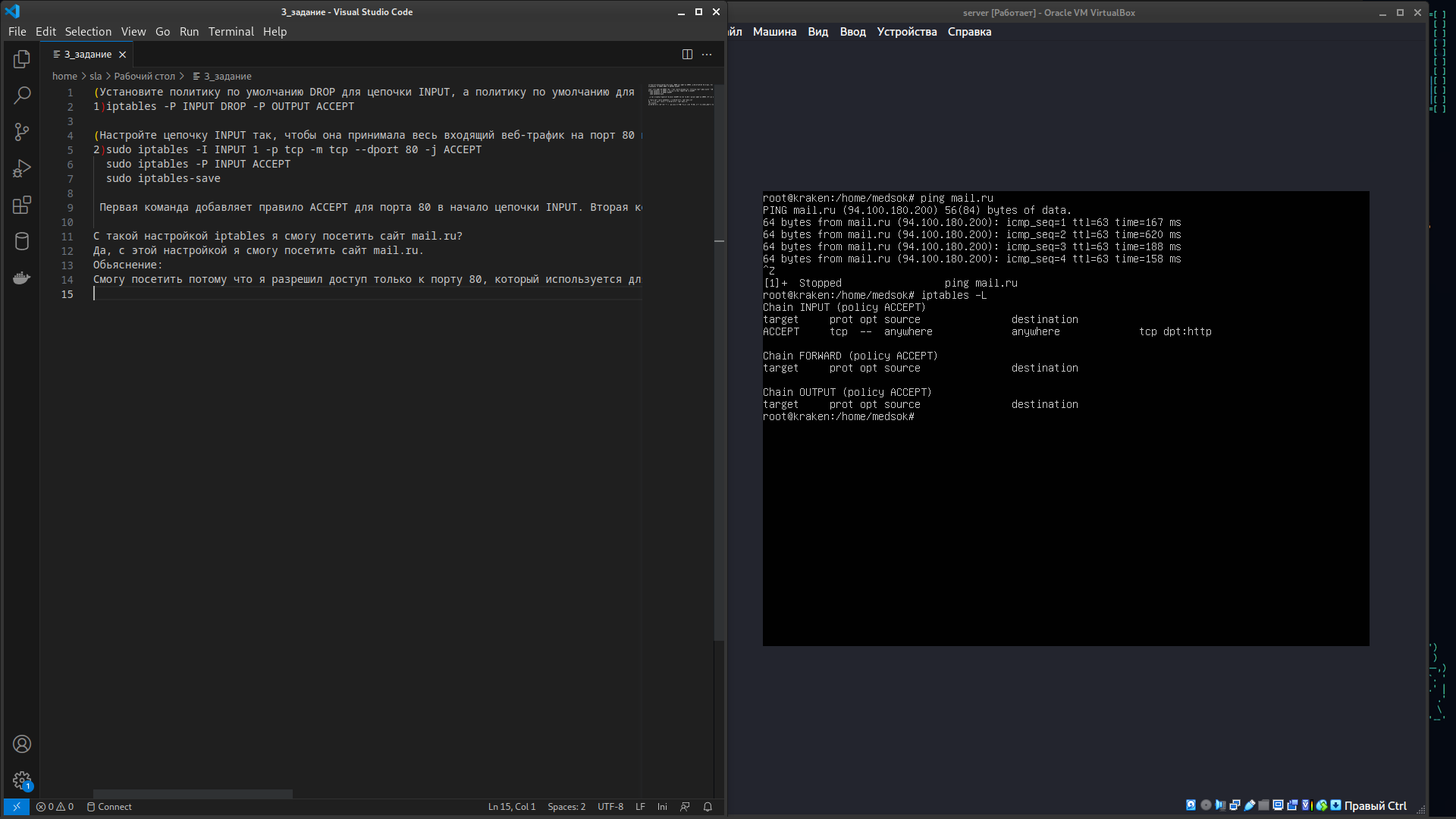


3.Можете ли вы посетить сайт mail.ru? Почему можете или почему нет? Если вы не можете посетить сайт, то какая настройка этого сайта мешает, учитывая, что ваша политика вывода по умолчанию — ACCEPT, а брандмауэр настроен на прием трафика, поступающего на порт 80?

Ответ: Да, с этой настройкой я смогу посетить сайт mail.ru.

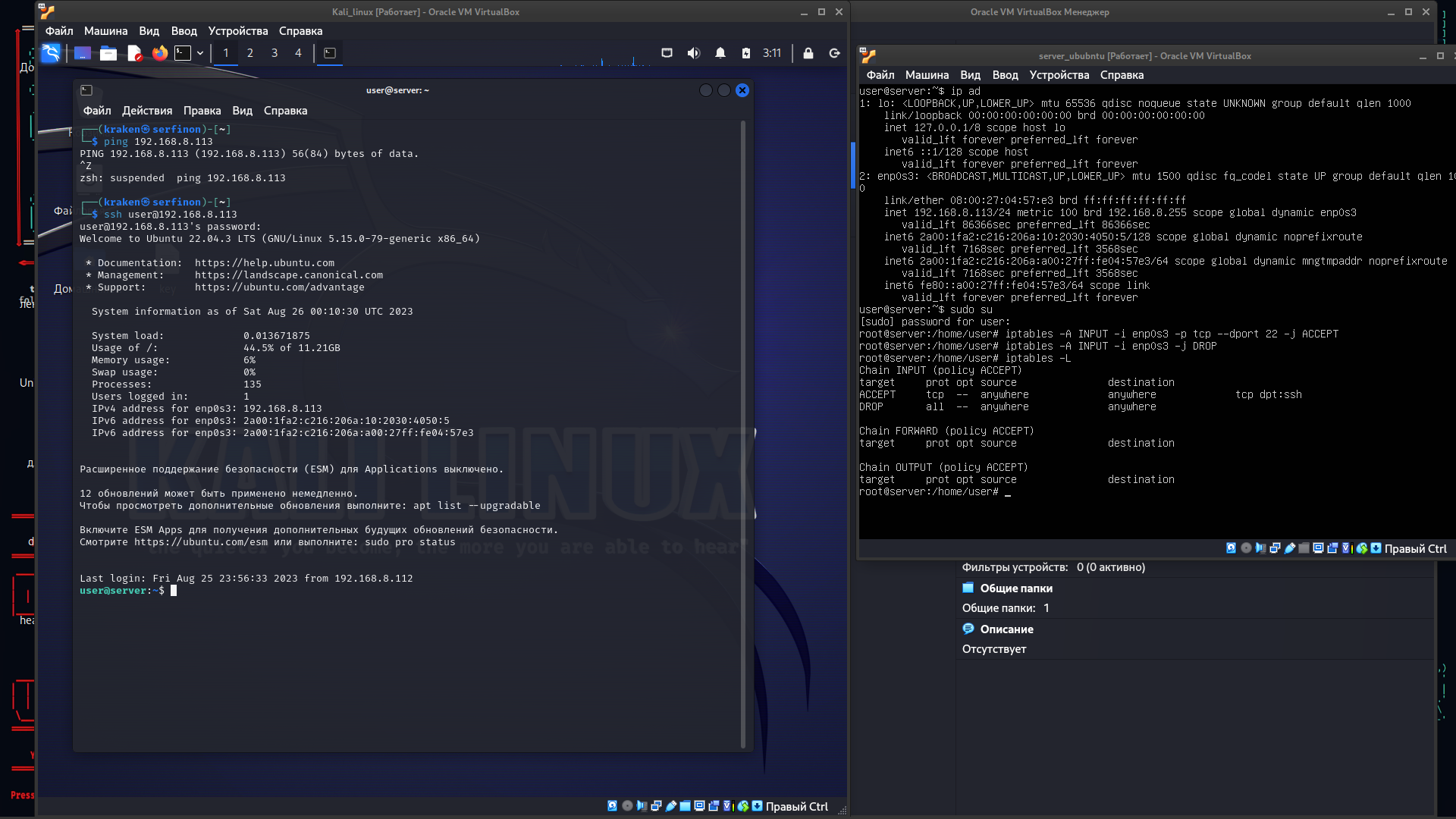
Объяснение:

Смогу посетить потому что я разрешил доступ только к порту 80, который используется для HTTP-трафика. Все остальные порты будут заблокированы.



**Задание 4. ACCEPT для трафика SSH**

1-2.Выполняю вставку в правила в цепочке ввода, чтобы разрешить SSH-трафик.А также на данном скриншоте демонстрирую, что могу подключиться к SSH-серверу, работающему на виртуальной машине Ubuntu, подключившись к ней с другой виртуальной машины (любой) или с физического хоста.

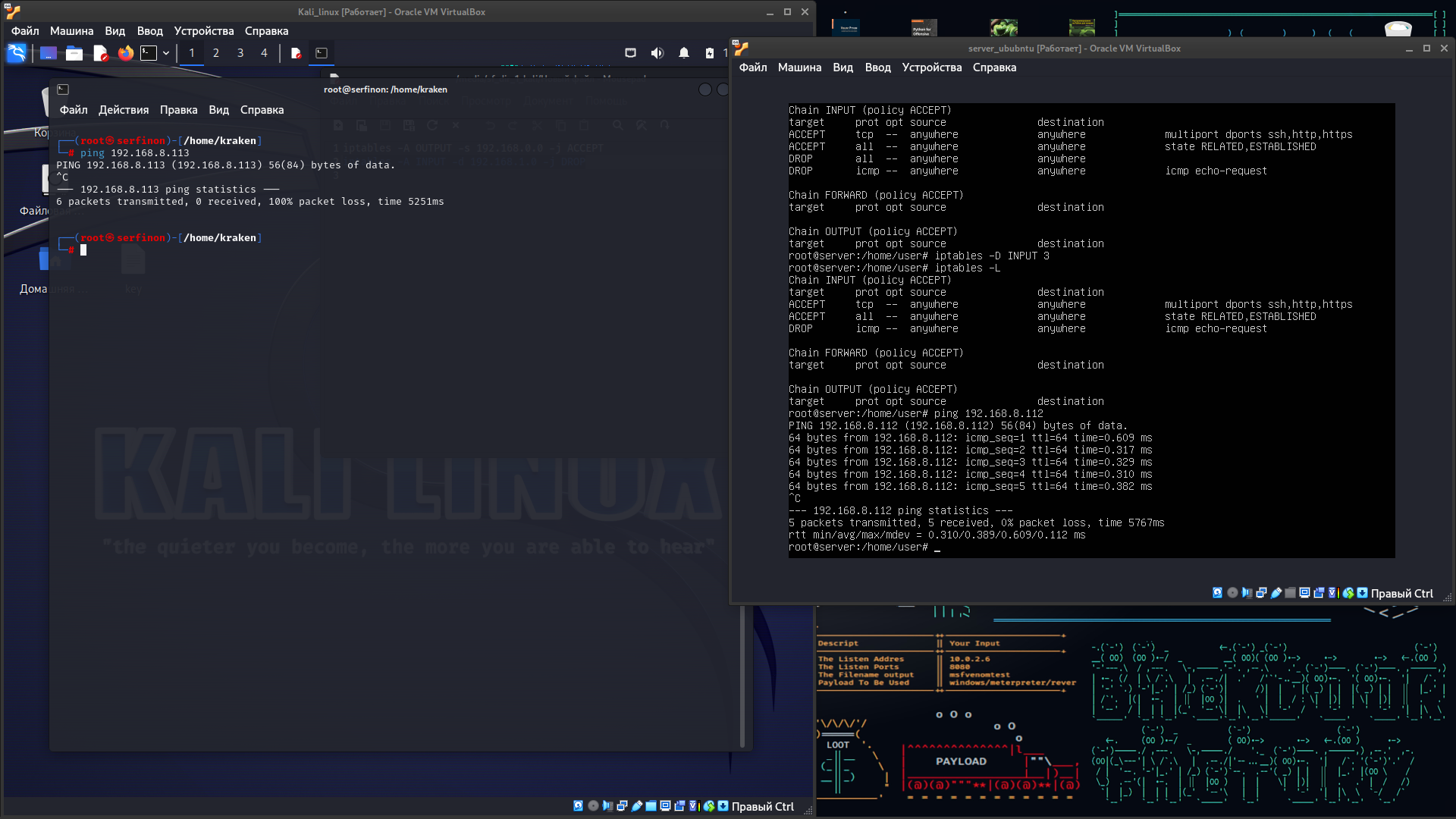


**5.ACCEPT/DROP для цепочек INPUT/OUTPUT**

Что нужно сделать

Настройте таблицу filter iptables так, чтобы сеансы / обмен пакетами, исходящие от виртуальной машины 1 (в качестве источника), были успешными; с другой стороны, сеансы / обмен пакетами, исходящие с удалённого компьютера на виртуальную машину 1 (в качестве получателя), не были успешными.

(Нужно реализовать этот сценарий с минимальным количеством изменений правил и политик, если таковые имеются. Кроме того, объясните, почему ваш набор правил и политик, реализующих указанный сценарий, будет работать. Ответ запишите в текстовый документ.)



Объяснение:

Сокращаем общие кол-во правил:

настроим брандмауэр таким образом чтобы он разрешал трафик ssh,http,https, и блокировал любой другой входящий трафик по протоколу.  
Делаю с помощью опции multiport.Правила выглядят следующим образом:

#iptables -A INPUT -p tcp -m multiport --dports 22,80,443 -j ACCEPT

#iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

#iptables -A INPUT -j DROP

Теперь ssh трафик также доступен при этом мы сократили общие кол-во правил.

Теперь настроим iptables таким образом чтобы можно было блокировать ping извне.Иначе говоря удаленные машины не смогут выполнить ping на нашу машину,но при этом мы сможем сделать ping.

#iptables -A INPUT -p ICMP --icmp-type echo-request -j DROP

#iptables -D INPUT 3

#iptables -L

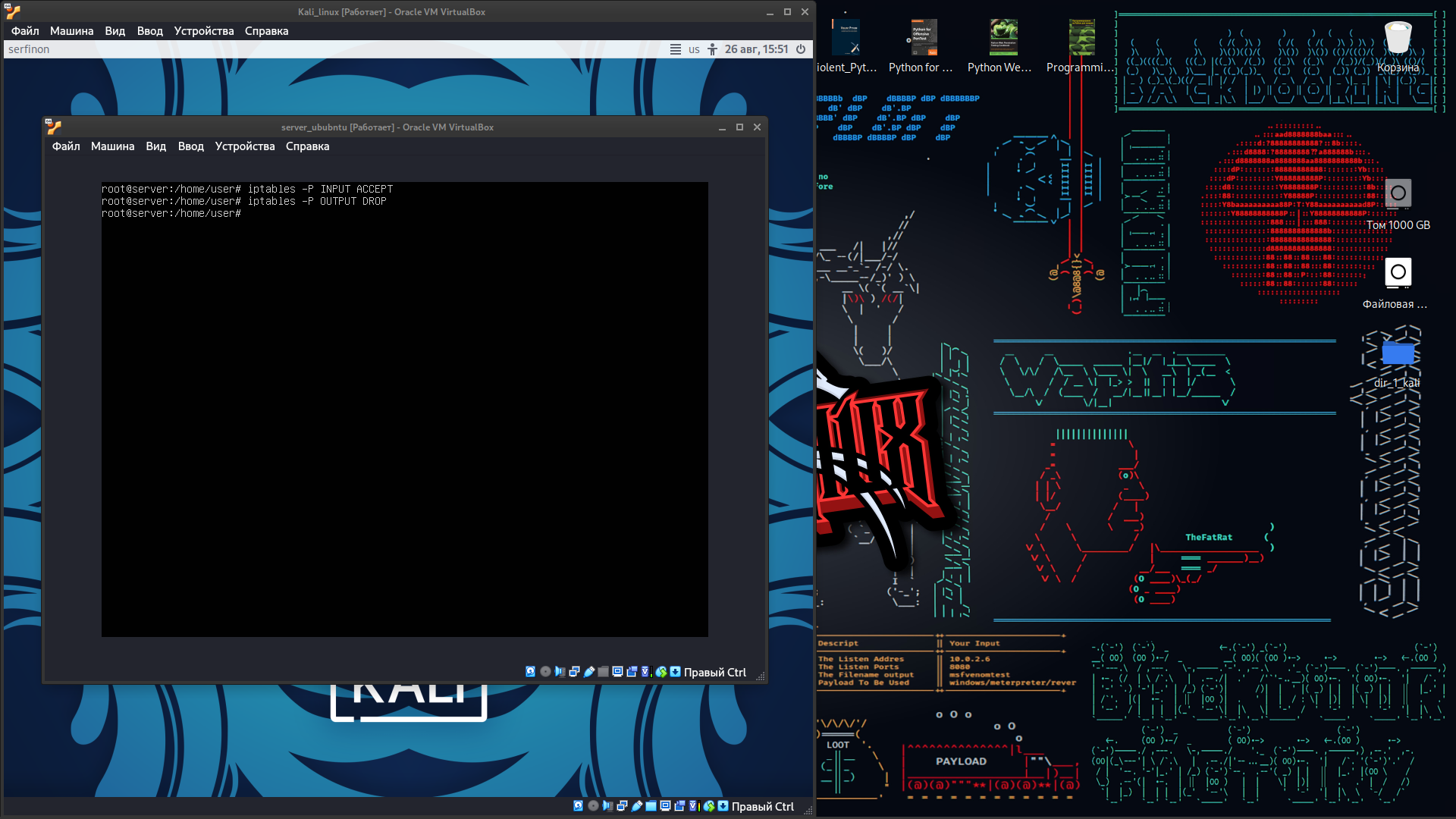
В итоге:

Мы явно указали что сообщение с эхо запросом должно быть удалено.При этом сейчас мы разрешаем сообщения с эхо ответом по умолчанию с условием что цепочка input сейчас настроен на прием сообщений

**Задание 6. DROP INPUT & OUTPUT**

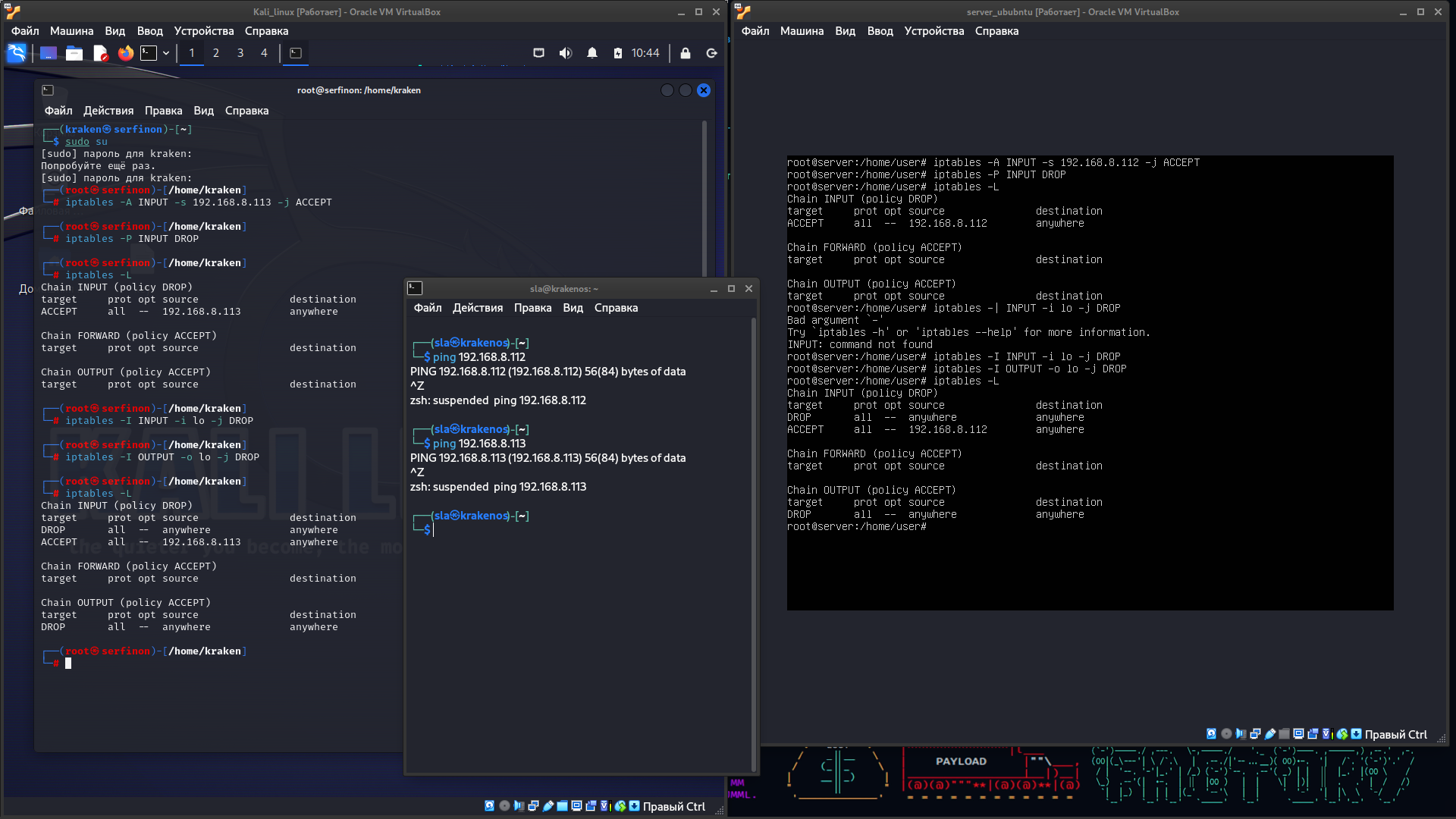
Что нужно сделать

1.Установите политику по умолчанию для цепочек INPUT и OUTPUT вашей таблицы фильтров iptables – DROP с помощью соответствующей команды.

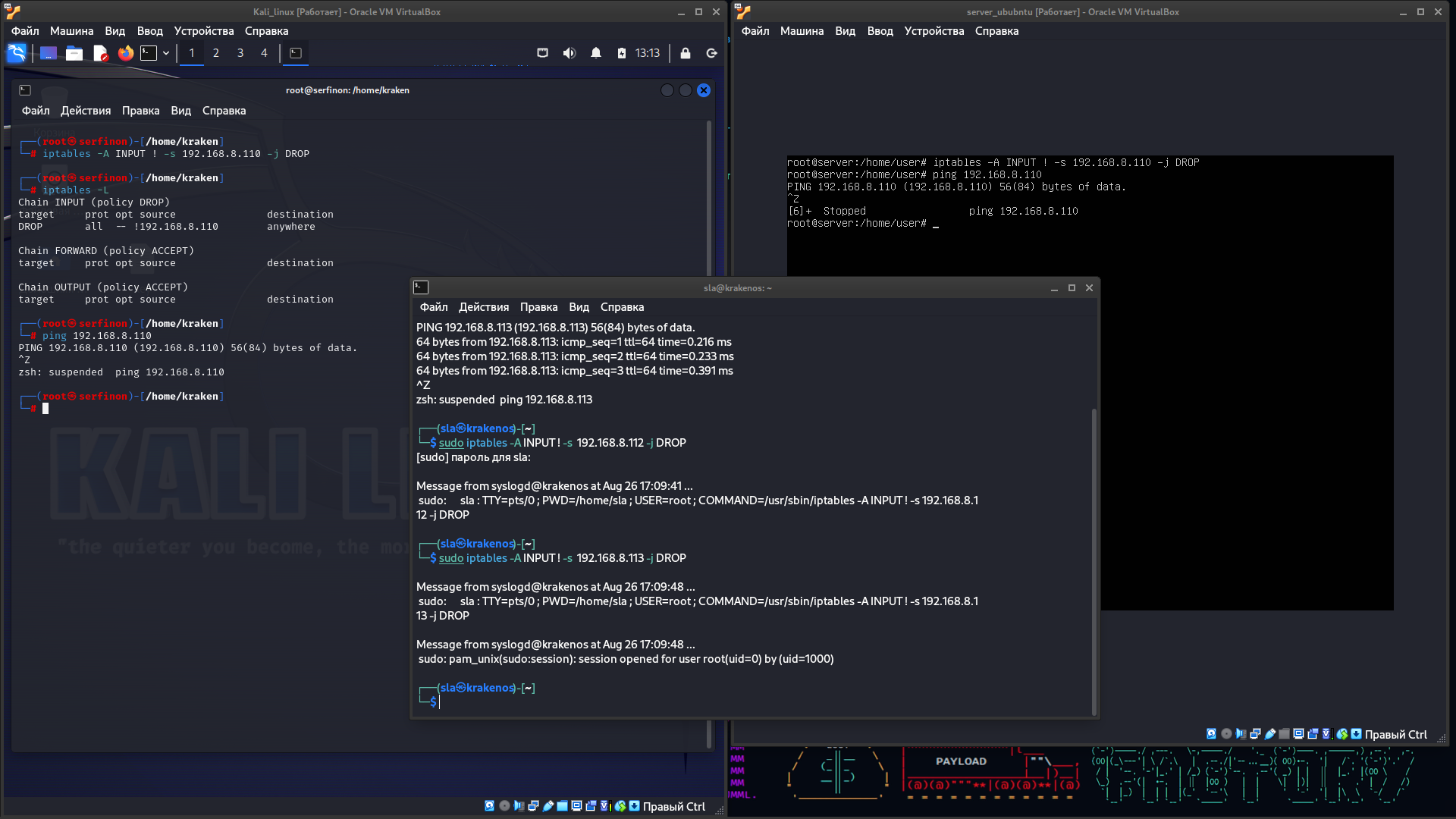


2.Настройте iptables на виртуальной машине следующим образом (выполните части 1 и 2 независимо):

1.разрешите только удалённым машинам пинговать локальную машину и заблокируйте локальной машине возможность пинга других машин;

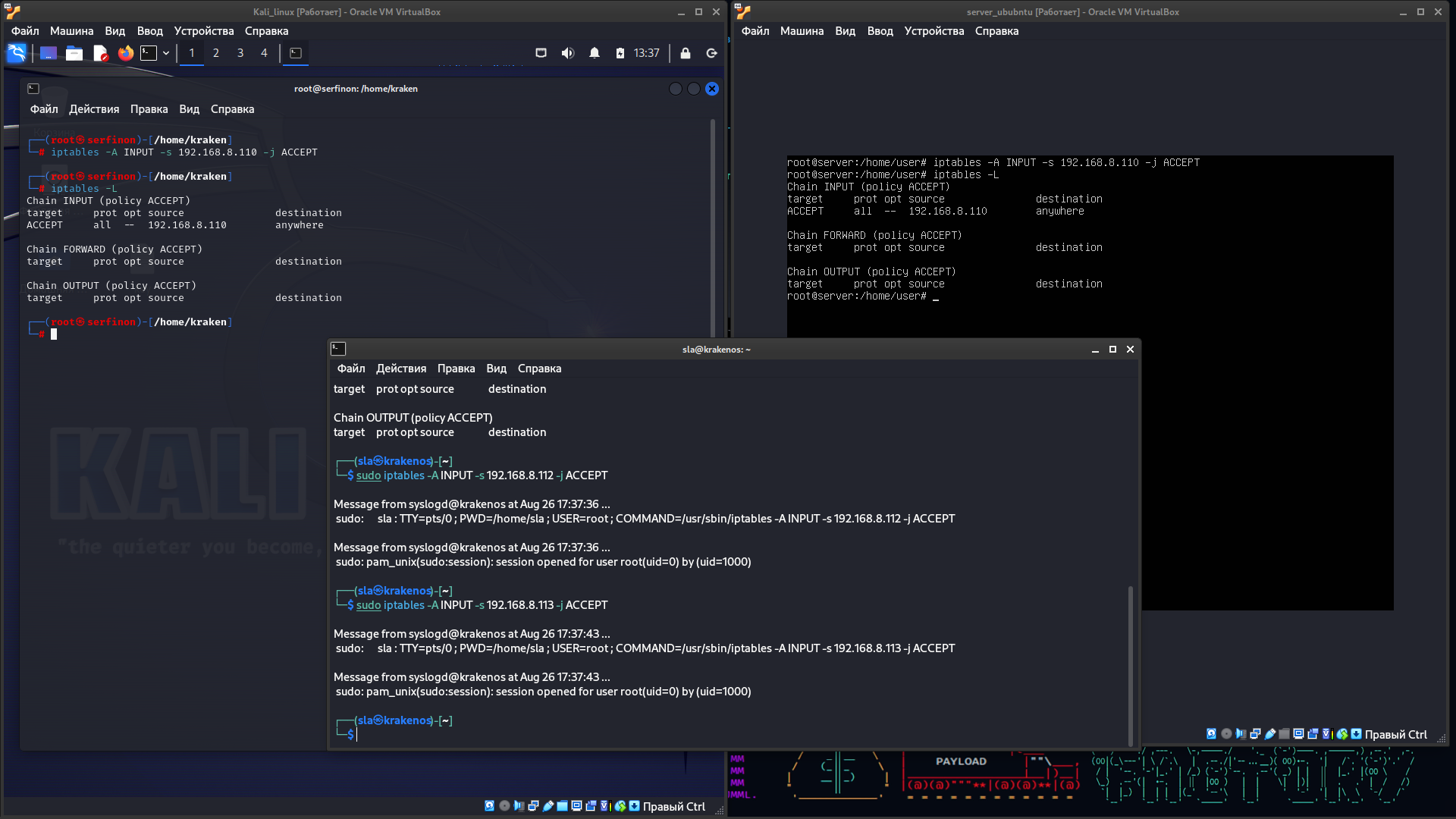


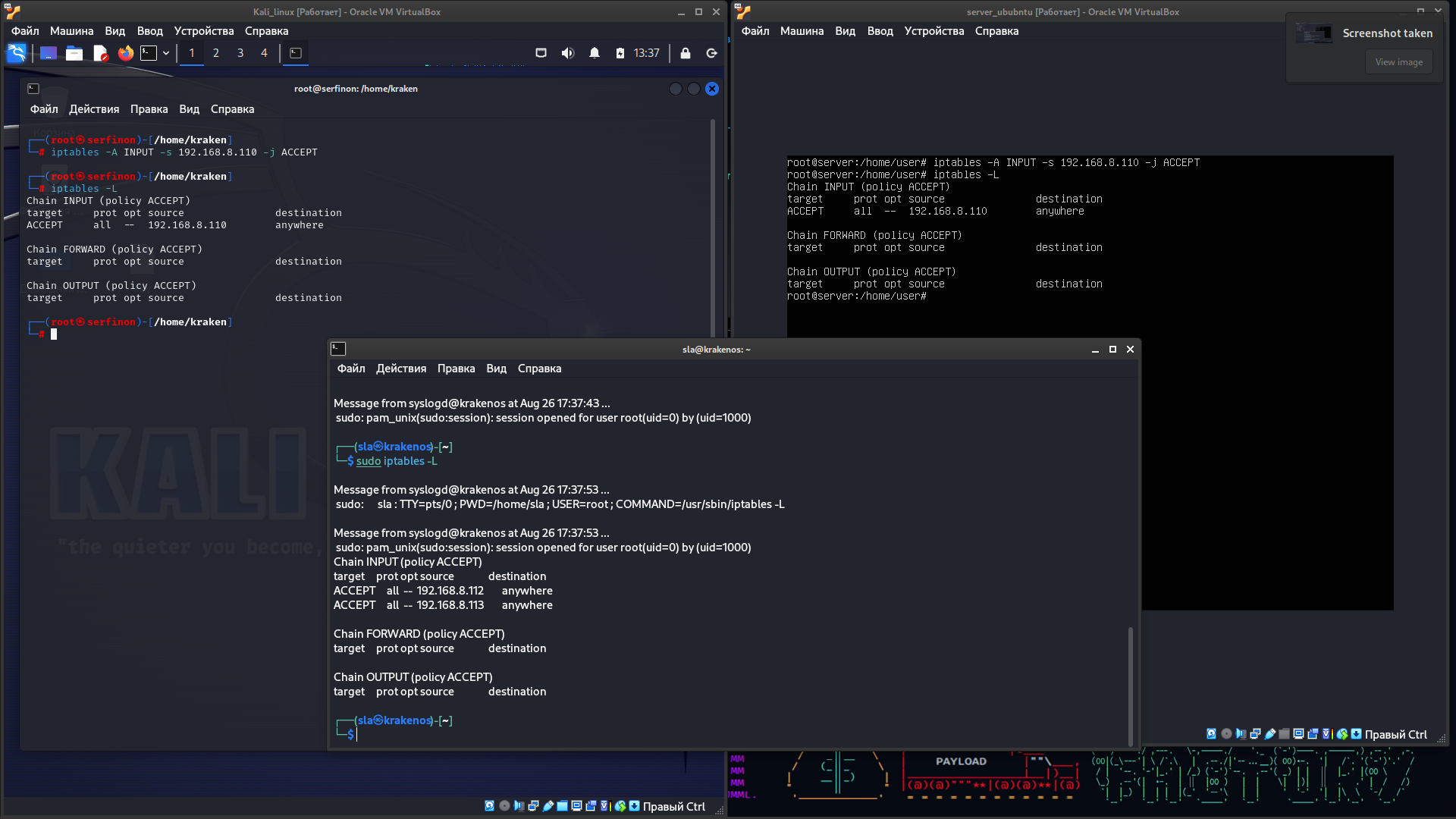
2.разрешите пинговать удалённые компьютеры только локальному компьютеру и заблокируйте пинг от удалённых компьютеров на локальном компьютере;



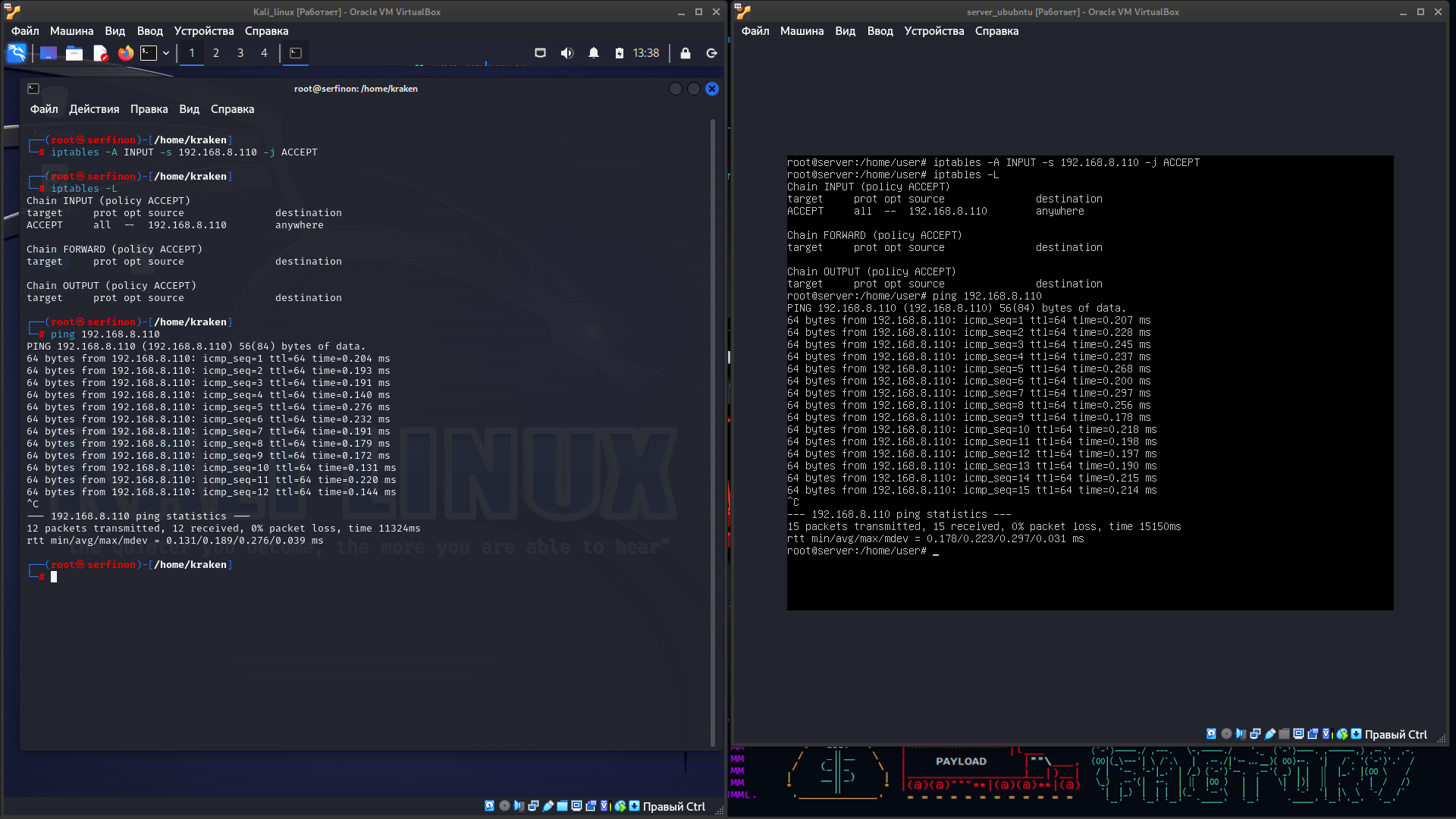
3.разрешите ping в обоих направлениях: от локальной машины к удаленной машине и наоборот.

Добавляю правила на локальную машину и удаленные машины



Правила на локальной машине  


Пингую локальную машину



пингую удаленные машины

