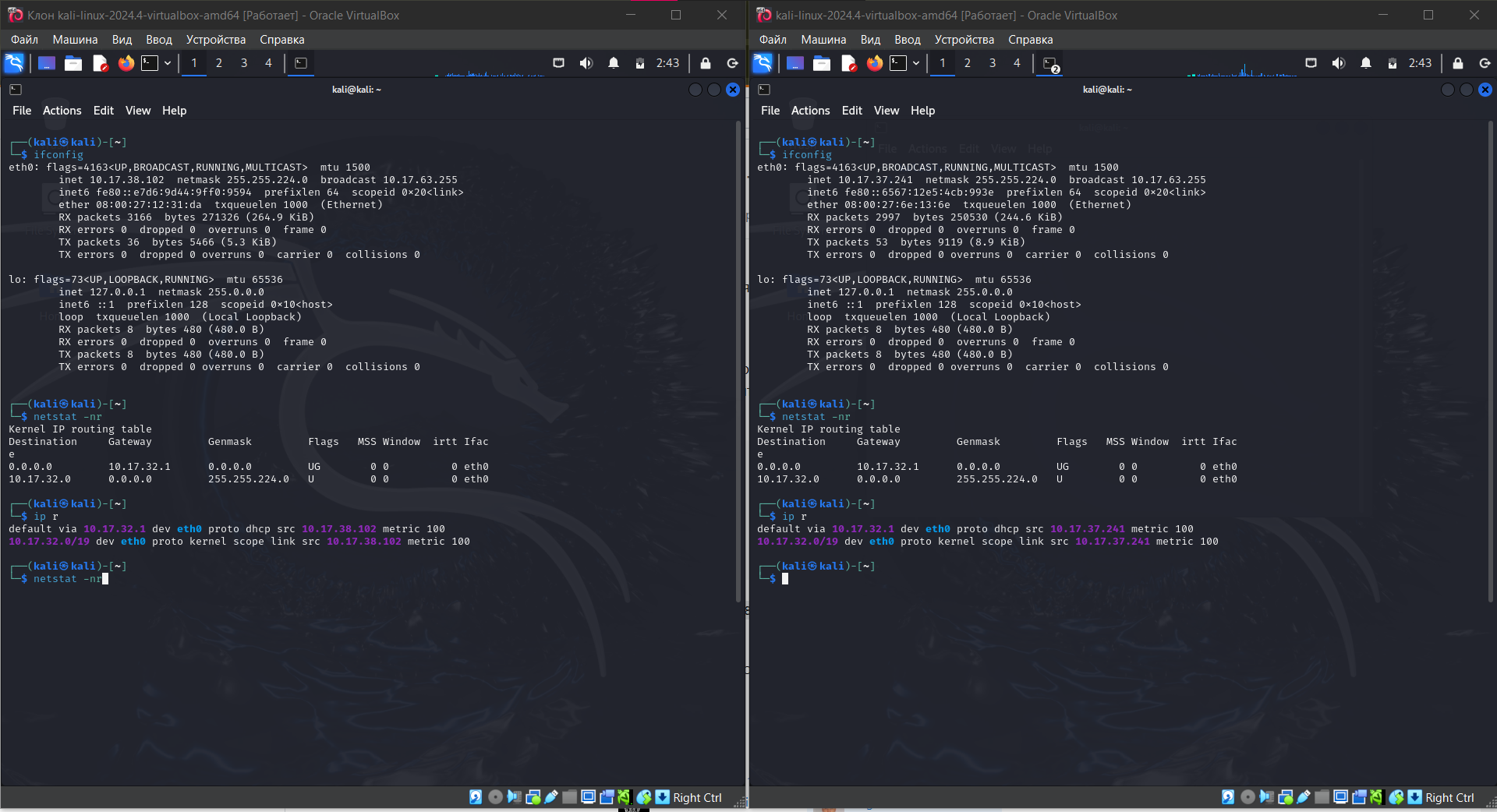
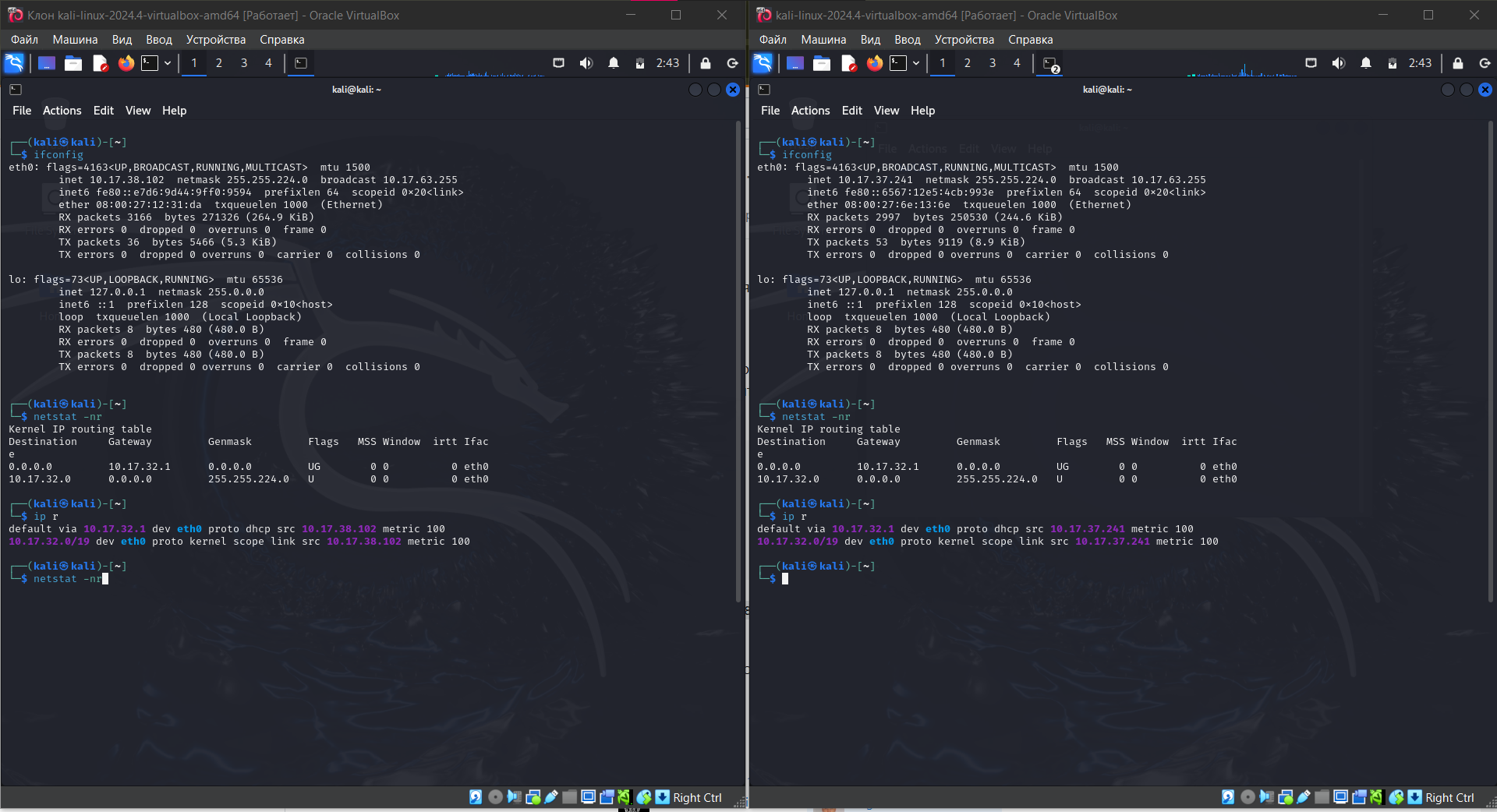
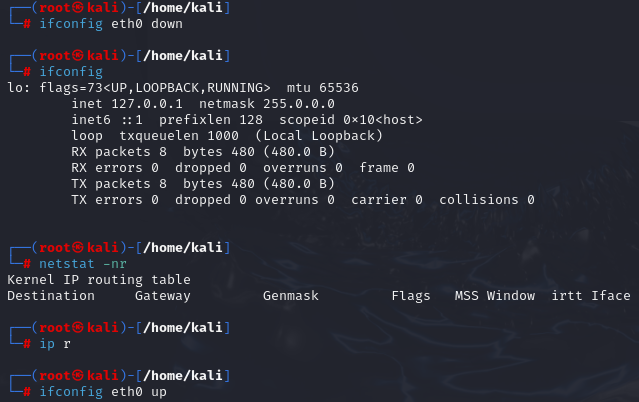
3.

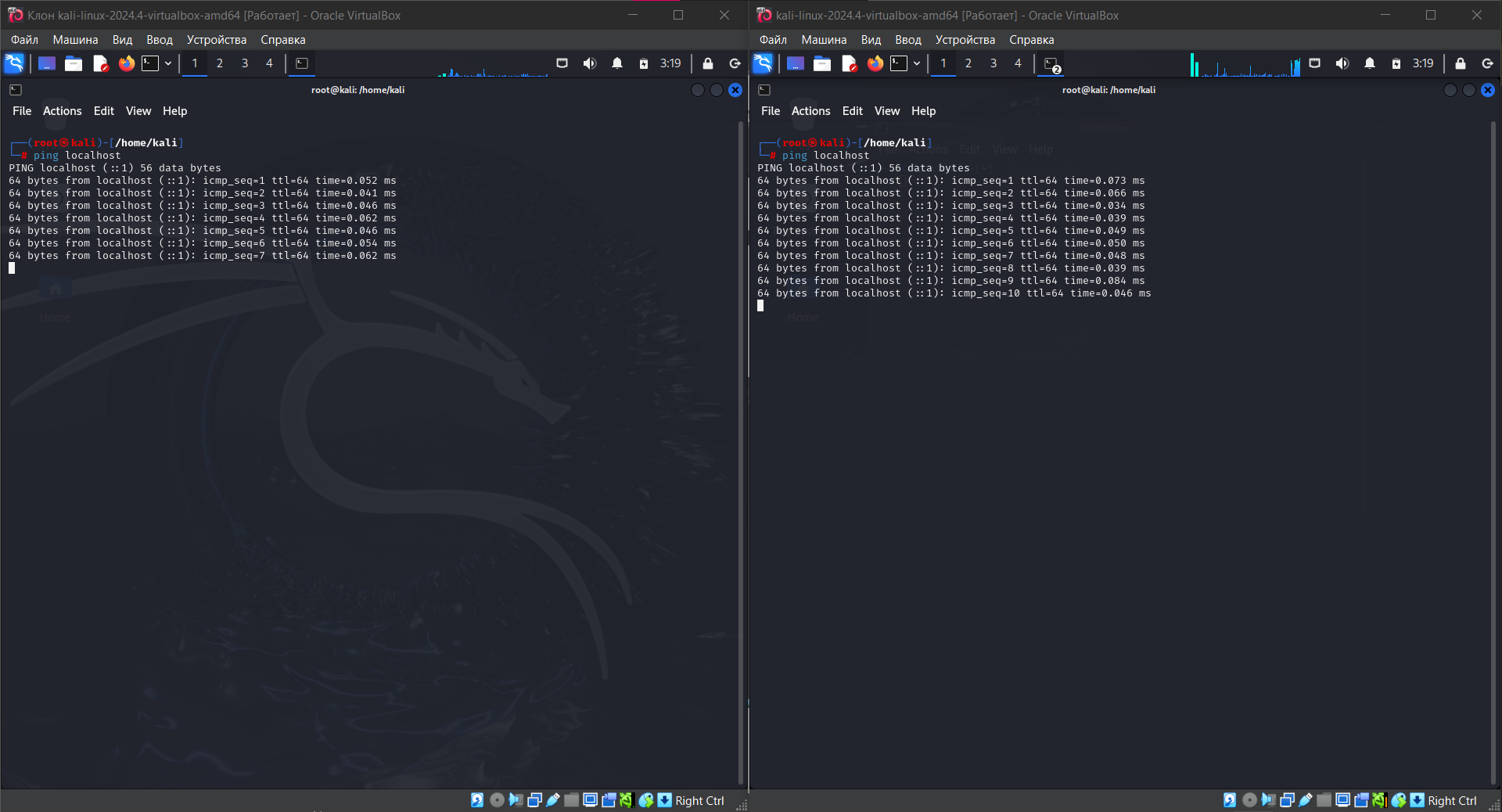
4.



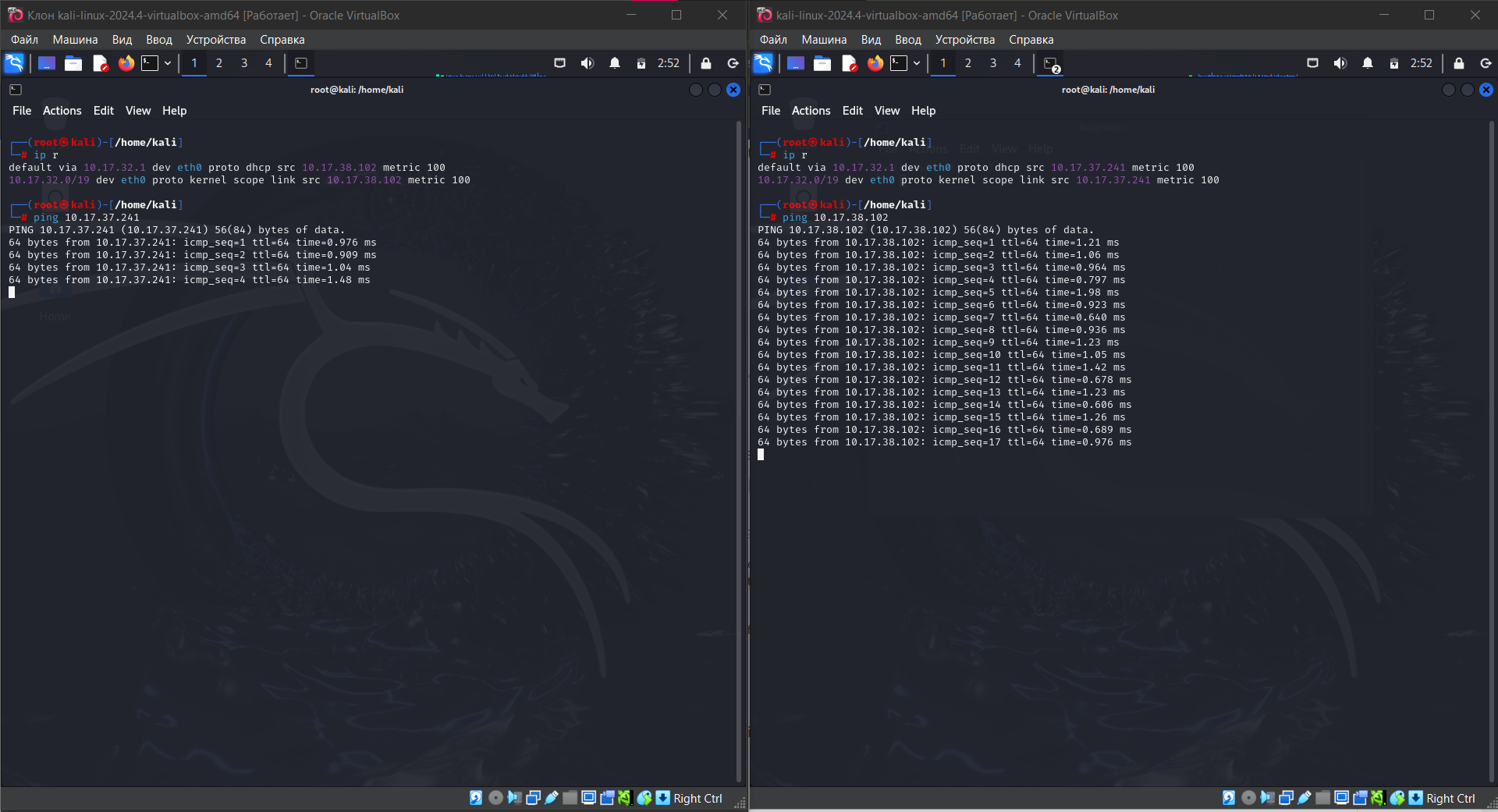
5.



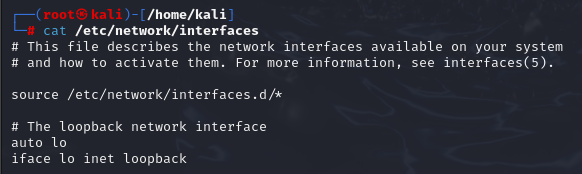
6. 

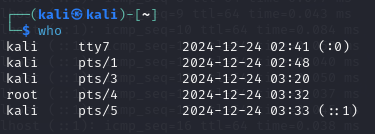
7. 

8.



9.

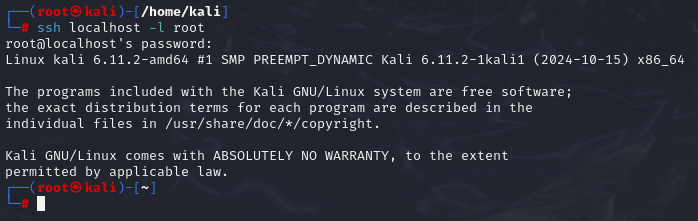


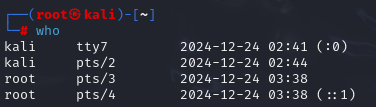
10. 

11.

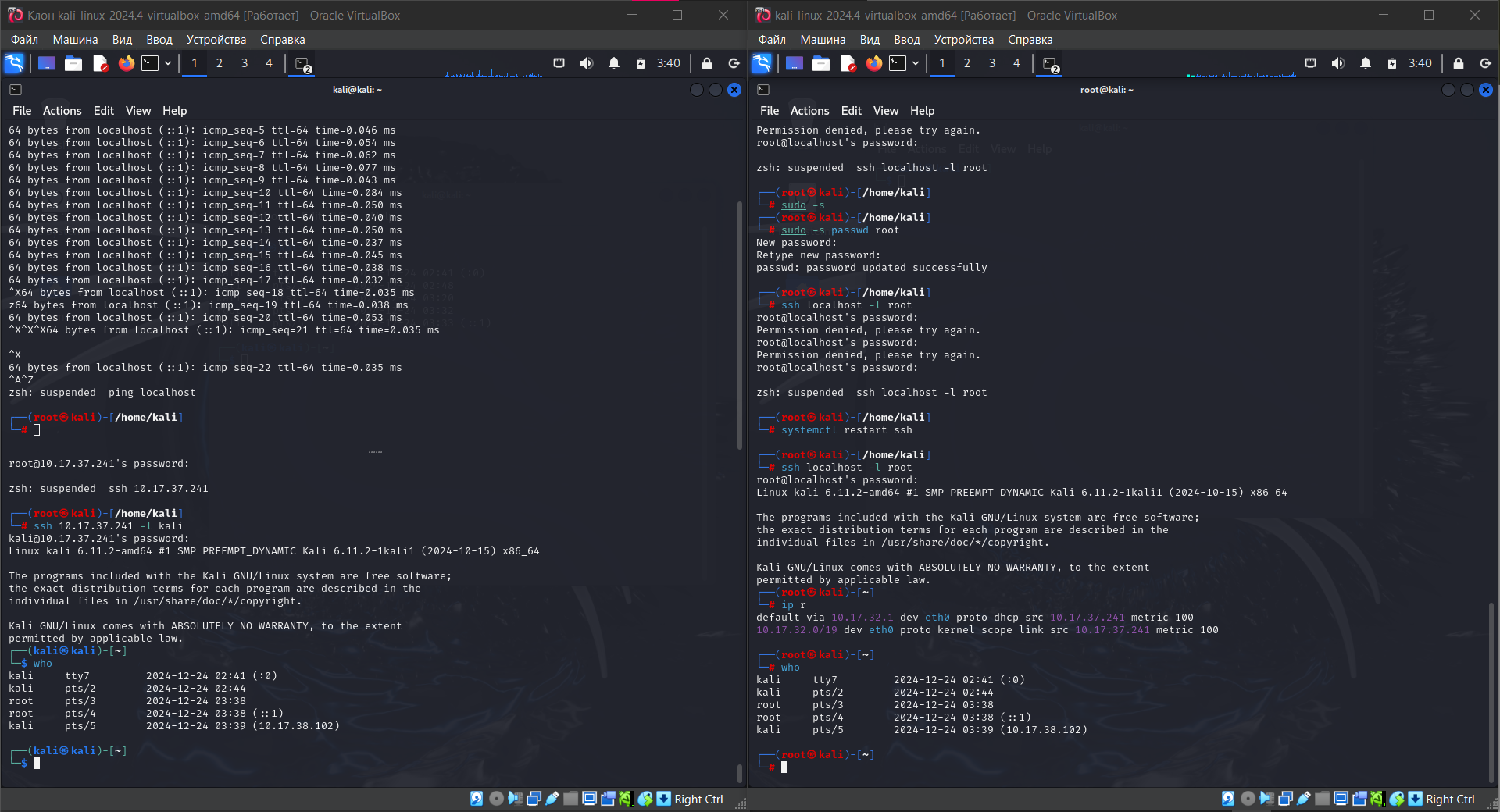


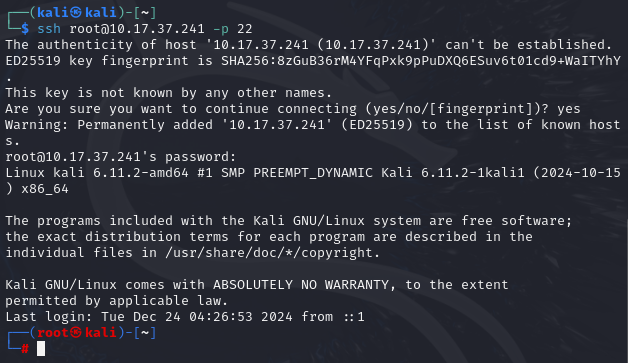
12.



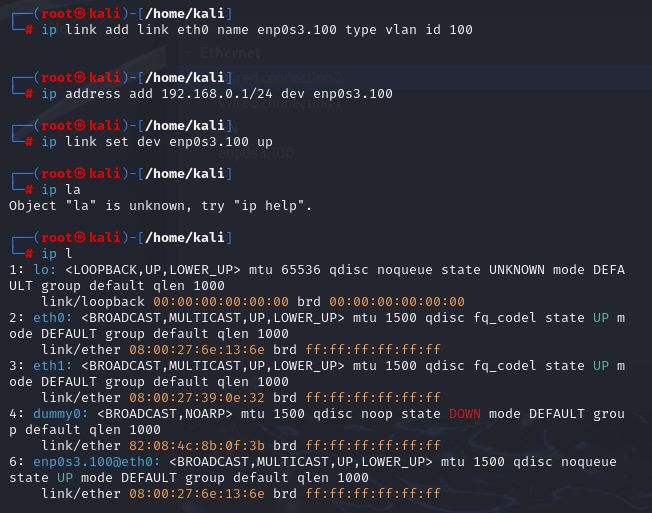


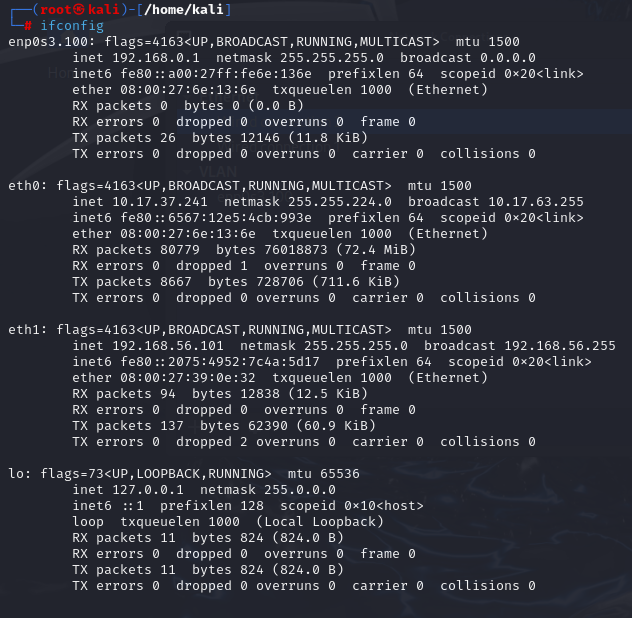
13.



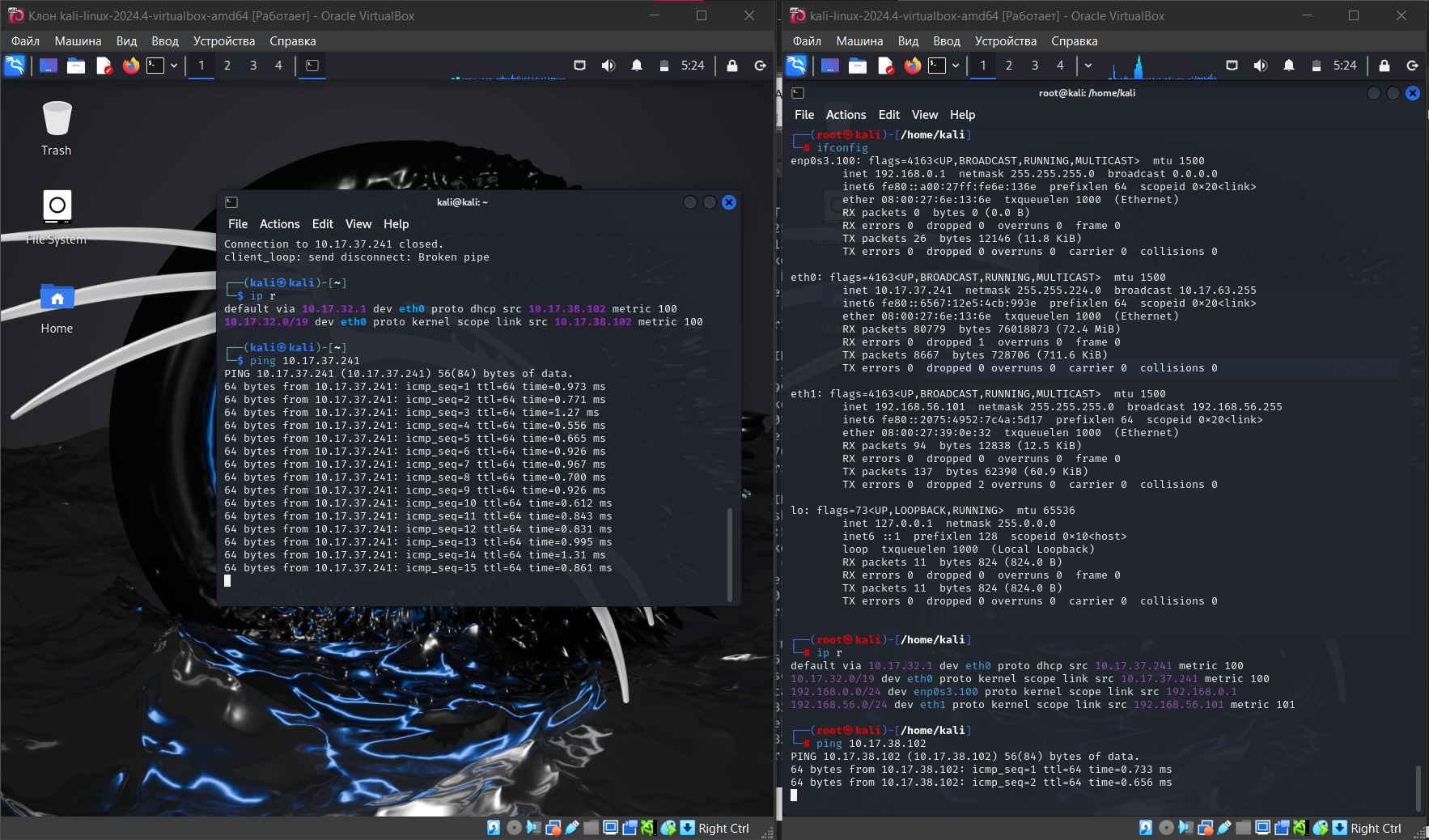
14. 

15-17.





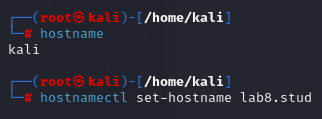
18.

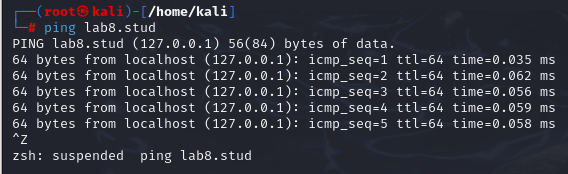


19.

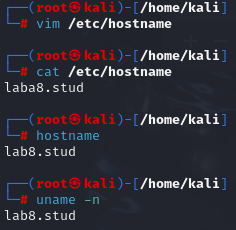


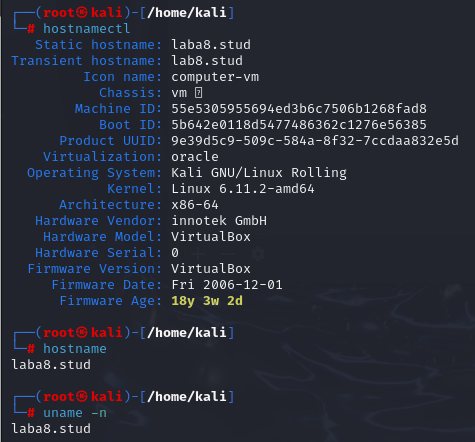
20.

\

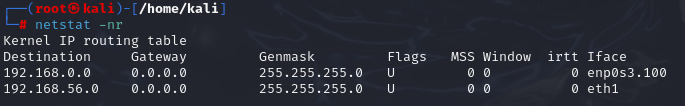


21.

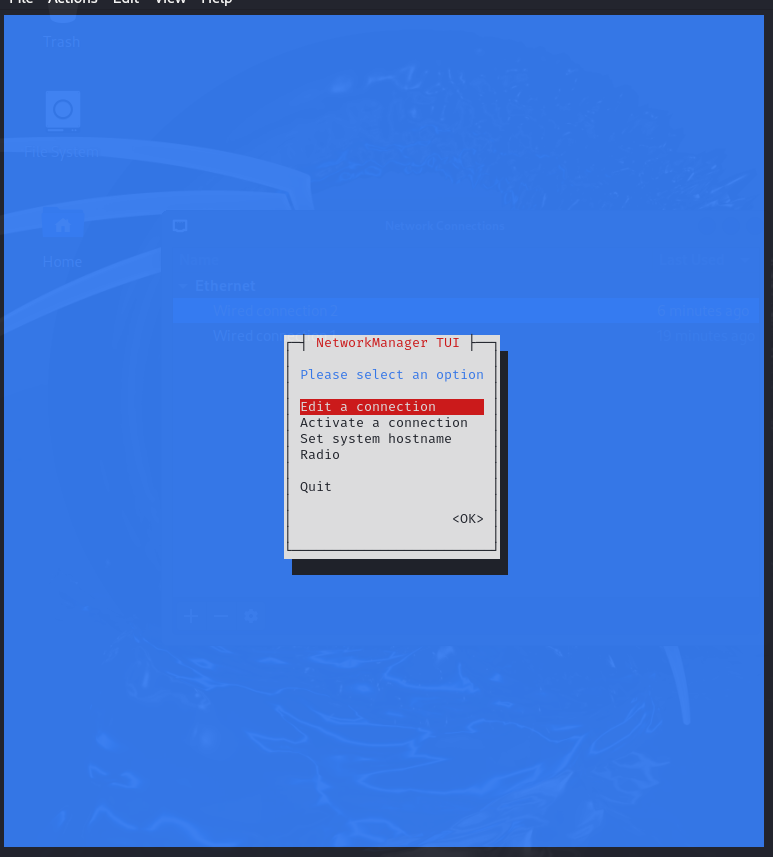




22.

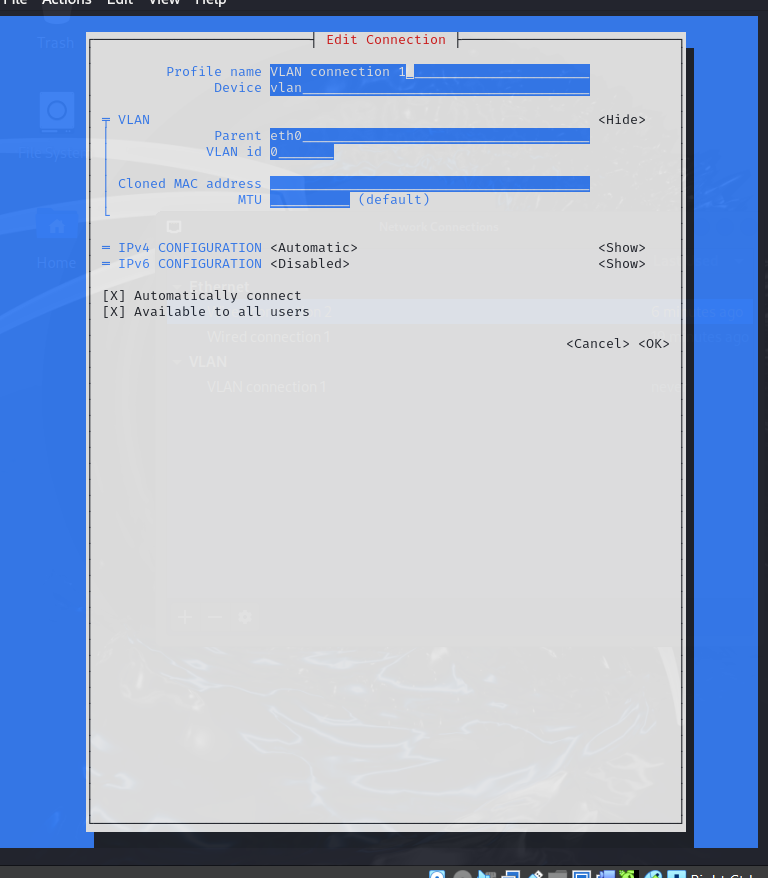


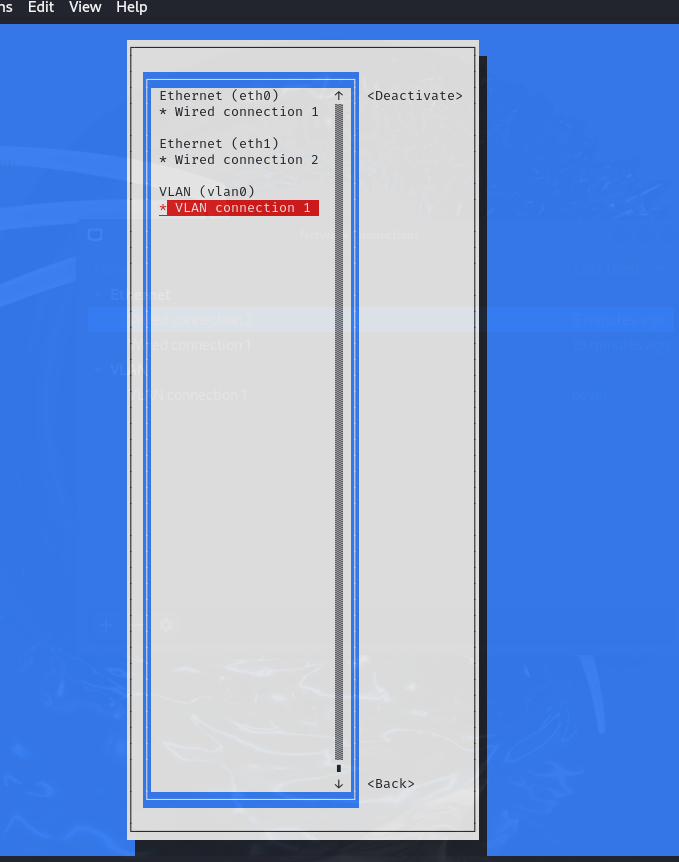
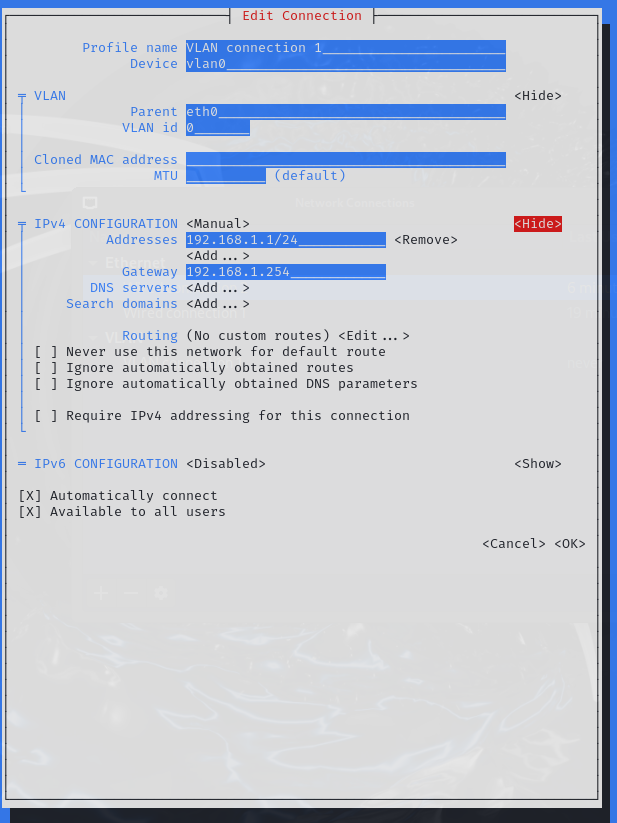
23.



24.

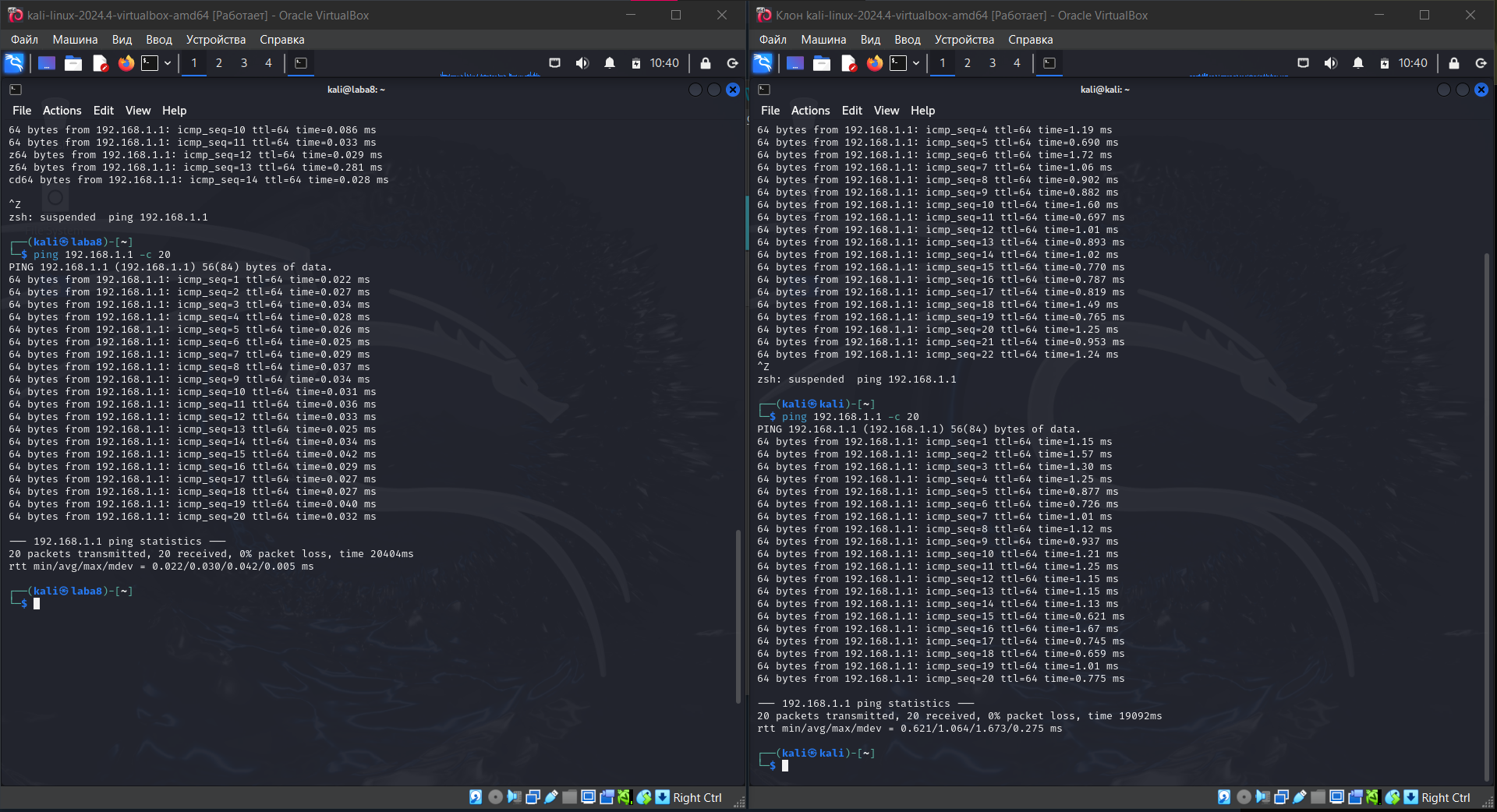




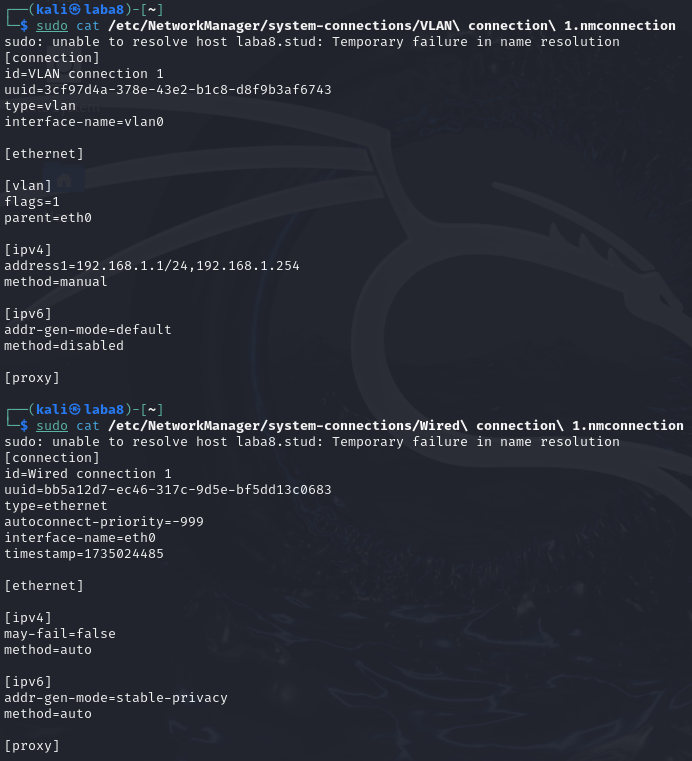




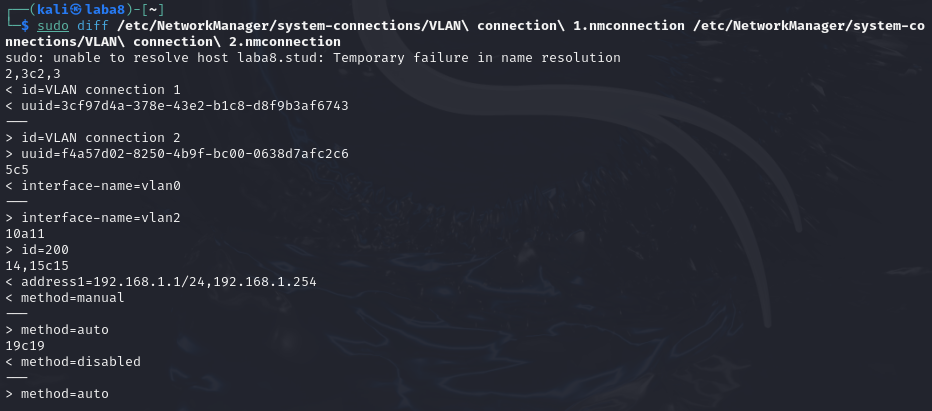
25.



26.

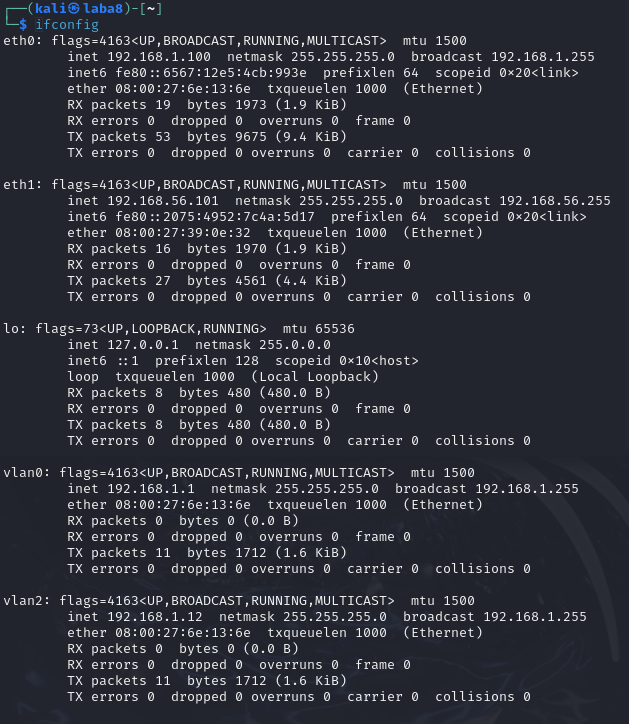


27.





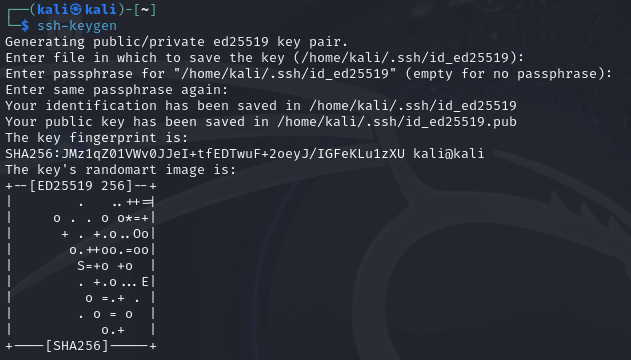
28.

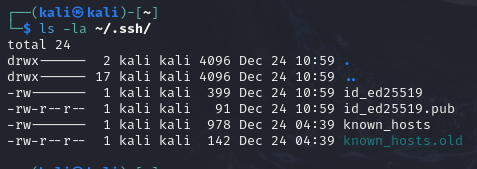


Устройства, созданные через ip: Они не сохраняются после перезагрузки, так как команда ip вносит изменения только в оперативную конфигурацию сети.

Устройства, созданные через nmtui/nmcli: Эти устройства сохраняются, так как их конфигурация записана в файлы /etc/sysconfig/network-scripts/.

29.



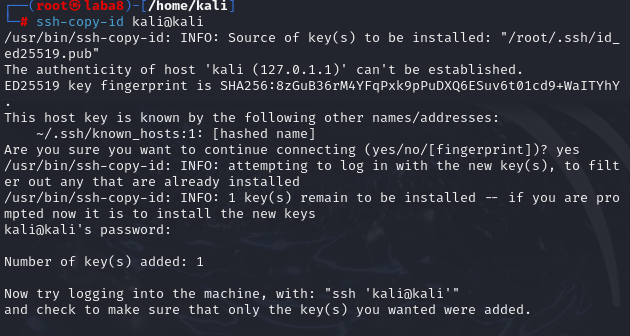


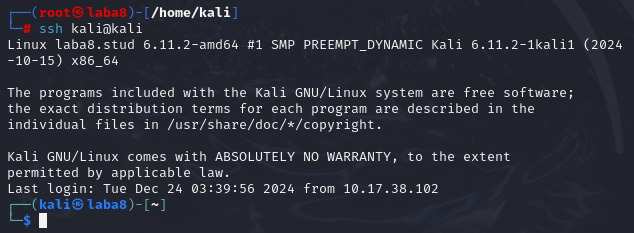
Ключи сохраняются в директории ~/.ssh/:

id\_rsa — приватный ключ.

id\_rsa.pub — публичный ключ.

30.





Использование SSH-ключей с защитой паролем надежно, так как:

Публичный ключ безопасно передается и не может быть использован без приватного ключа.

Приватный ключ защищен паролем (если задан).

Это исключает необходимость передачи пароля по сети, минимизируя риск перехвата.