Для начала на firewall-ах нужно пробросить порт-форвард, а именно с порта 7000 Kali-Wan пробросить порт 3389 на Windows 7. Для начала нужно просканировать firewall, убедиться, что порт 7000 открыт как RDP. После того, как найдем уязвимость, мы ее будем эксплуатировать.

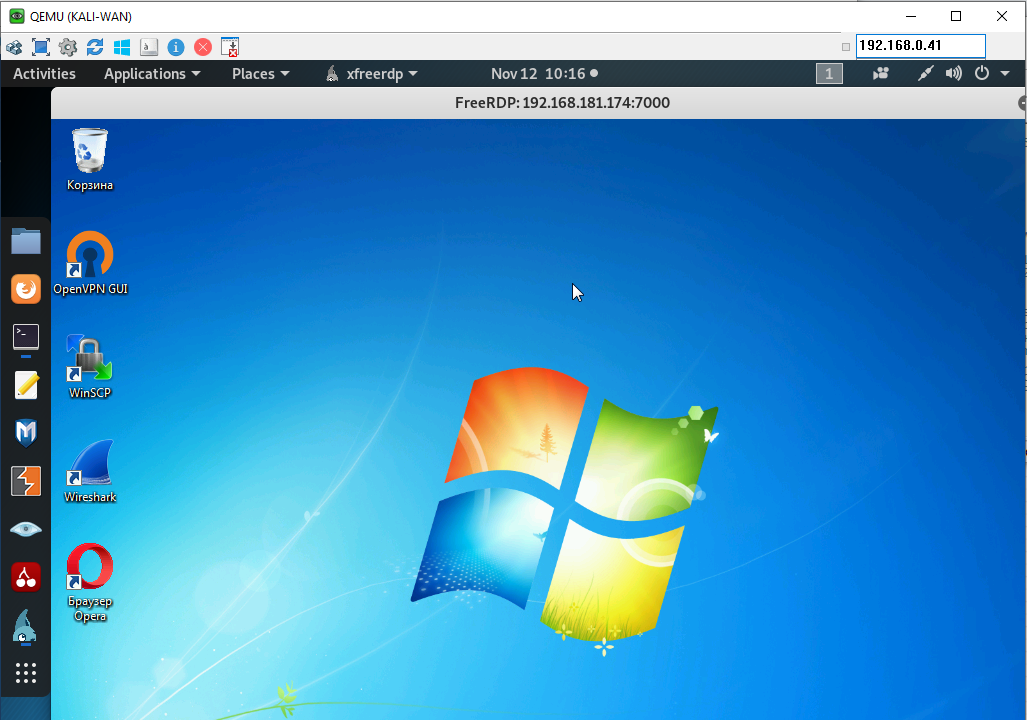


Рис. 1.

Если вдруг не работает, нужно перезапустить Widows7 и перепроверить все адреса. В случае изменения адресов, скорректировать их на файерволах. Теперь сканируем внешний файервол с помощью сетевого сканера nmap.

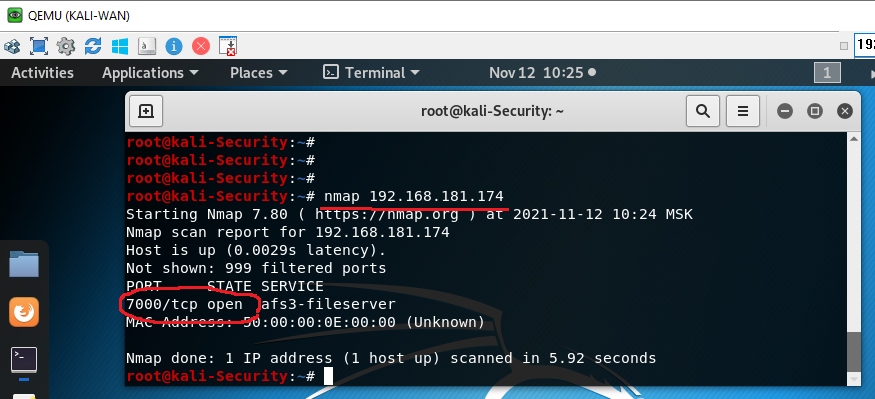
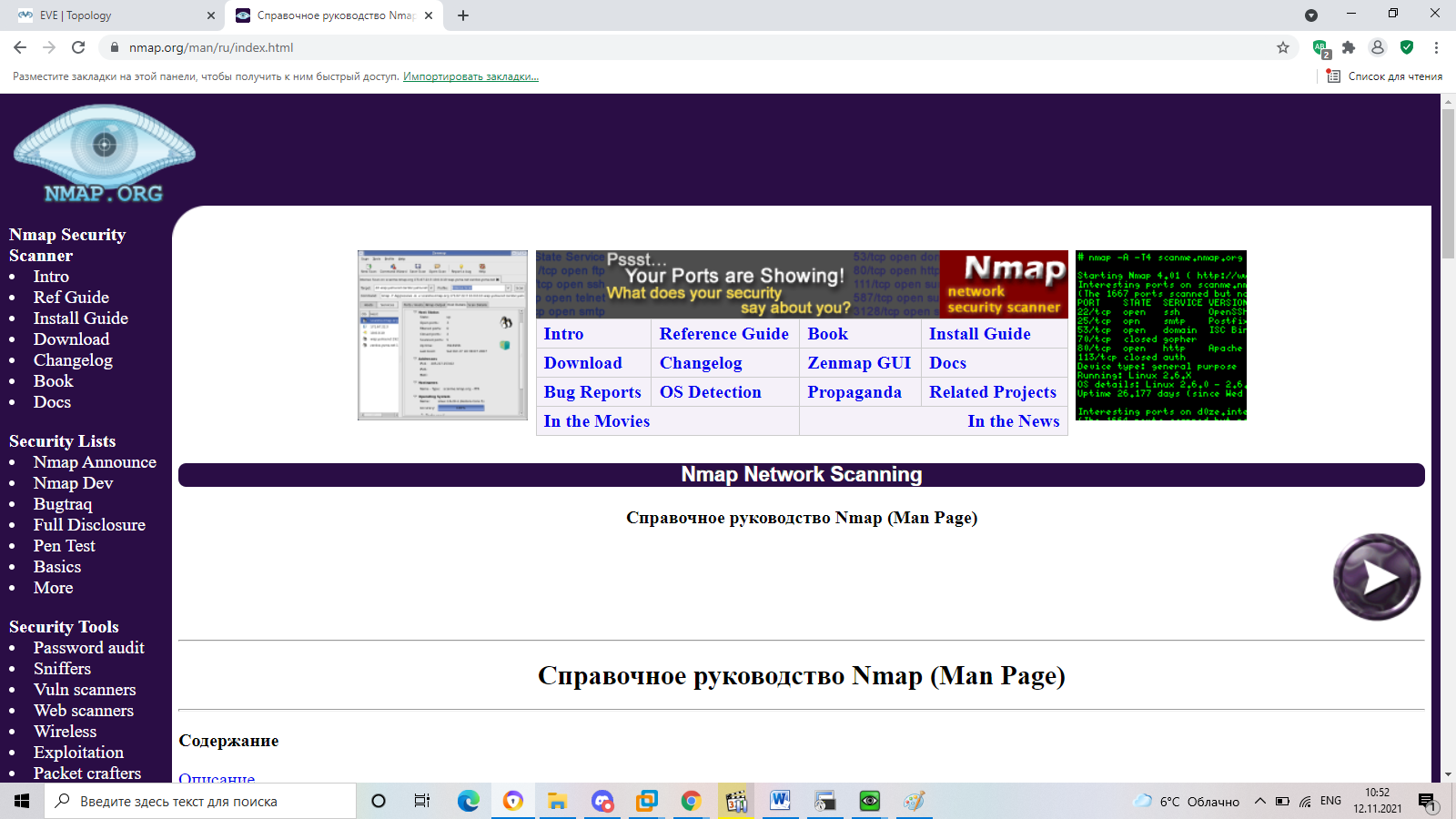


Рис. 2.

Видим, что из отсканированных 999 портов открыт порт 7000.

Имеется справочное руководство по nmap на русском языке по адресу: https://nmap.org/man/ru/index.html



Теперь просканируем порт 7000 в агрессивном режиме:

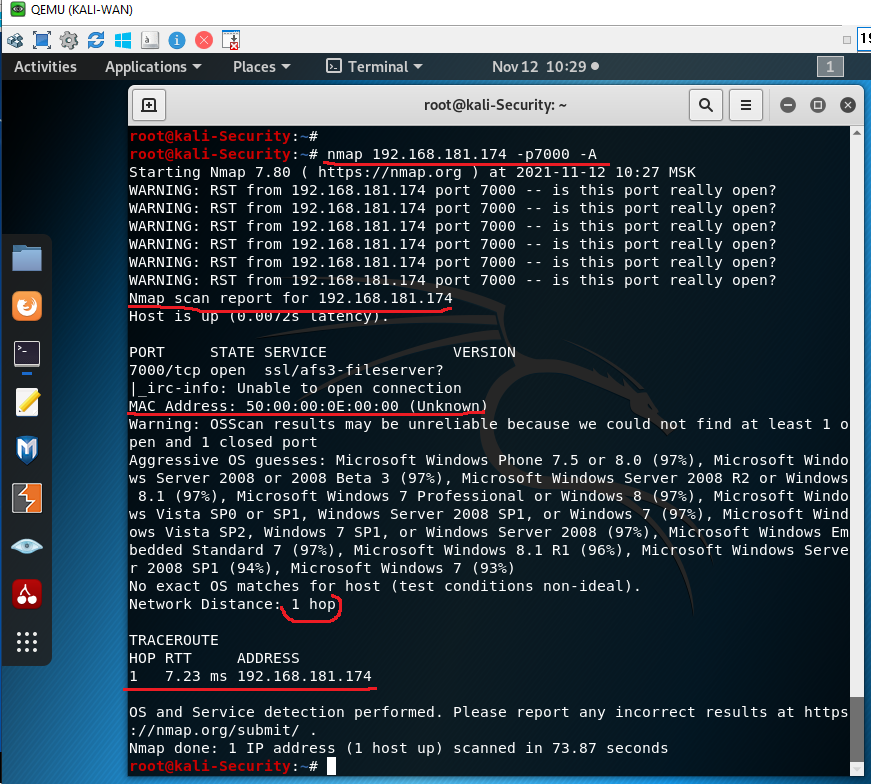


Рис. 3.

Получено очень мало информации: сказано, что там работает какая-то версия Windows, определенная с некоторой степенью вероятности.

Попробуем использовать скрипты для nmap

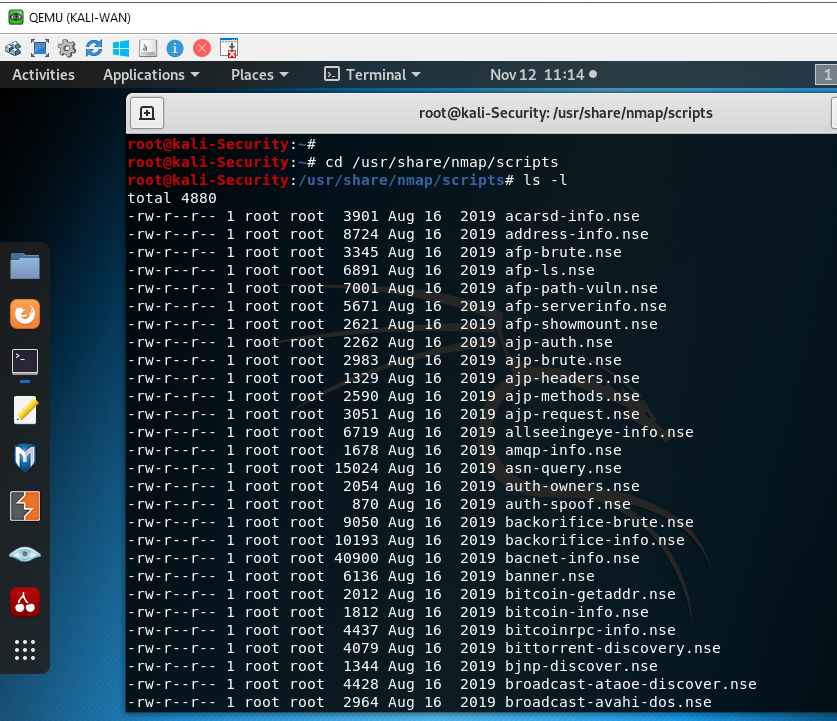


Рис. 4.

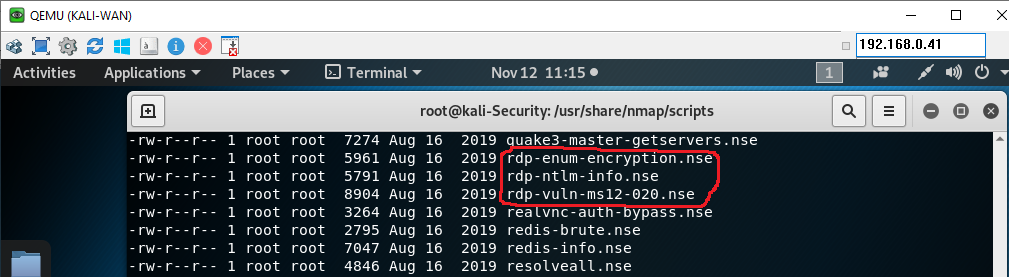


Рис. 5.

Возьмем один из скриптов и посмотрим что за порт 7000

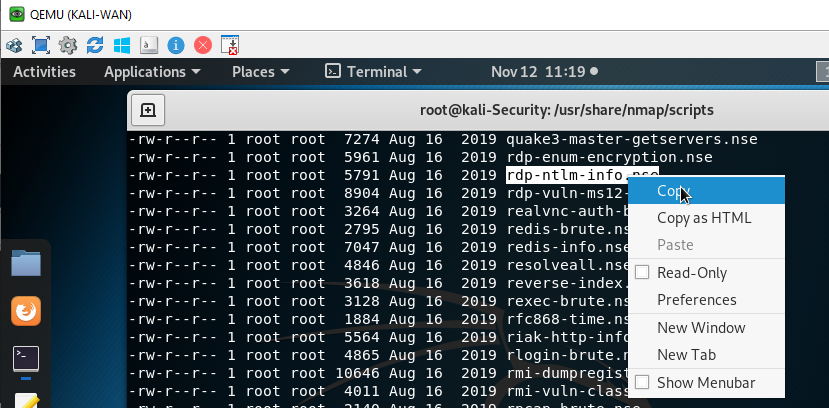


Рис. 6.

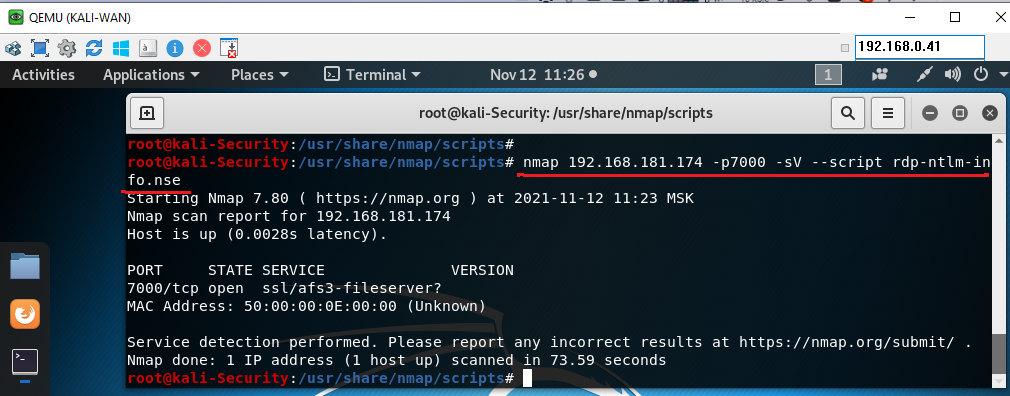


Рис. 7.

Ничего определенного nmap нам не дает, попробуем другим сканером. Это сканнер уязвимостей Nessus

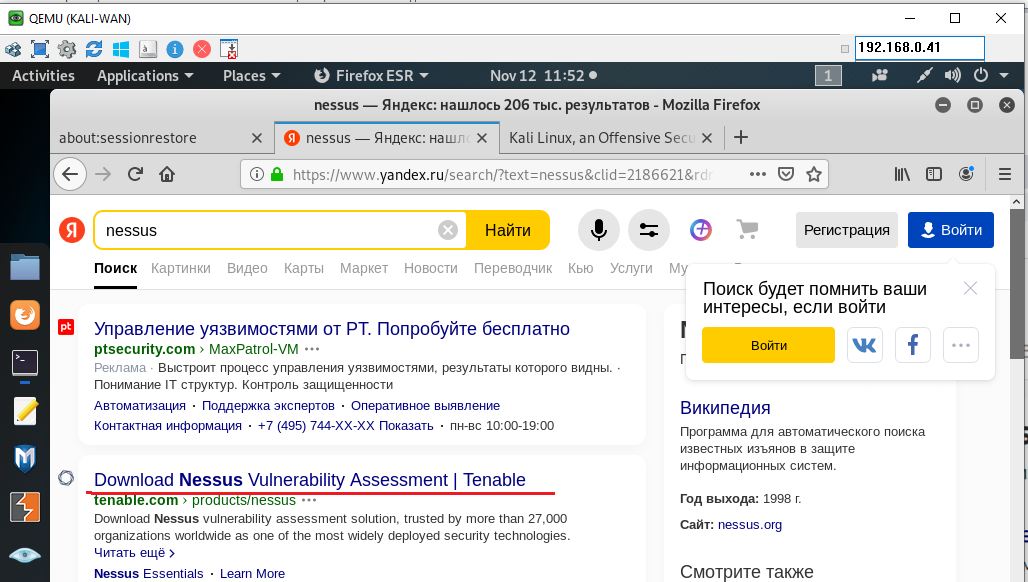


Рис. 8.

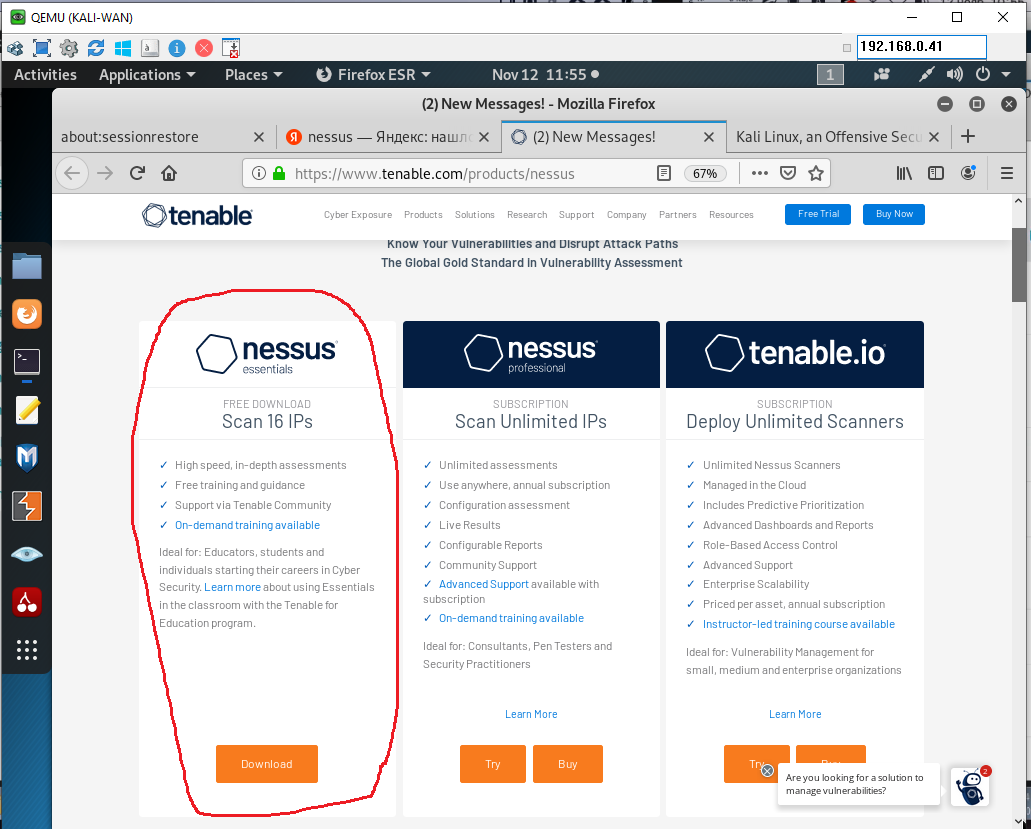


Рис. 9.

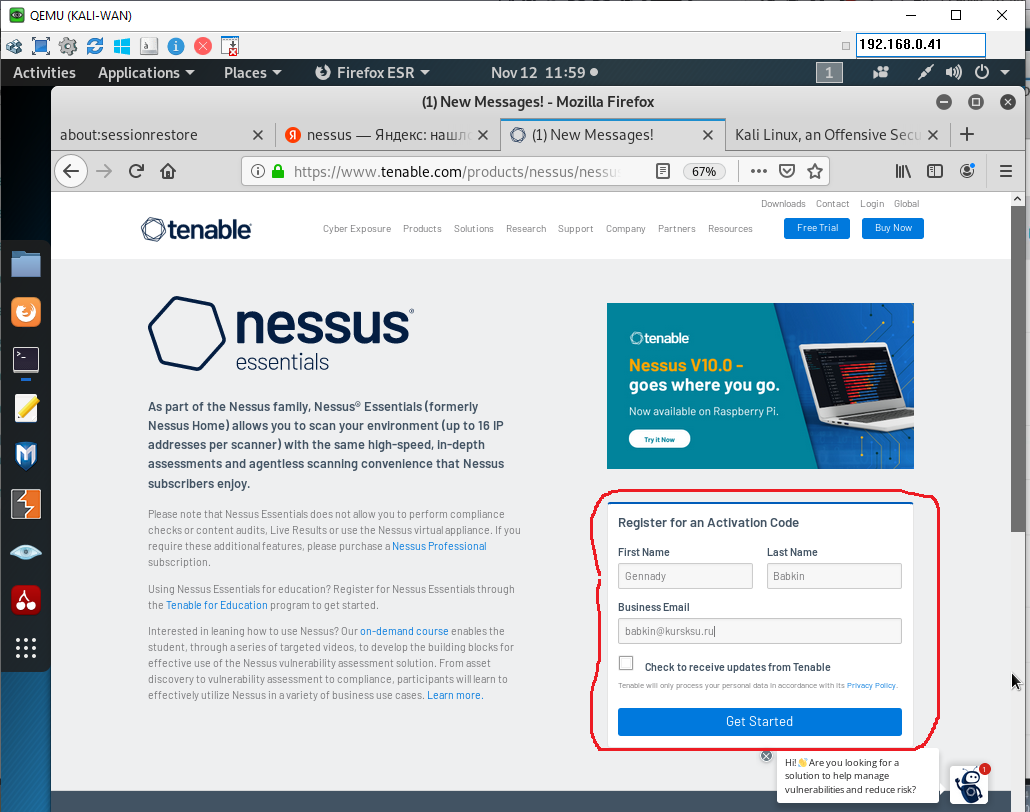


Рис. 10.

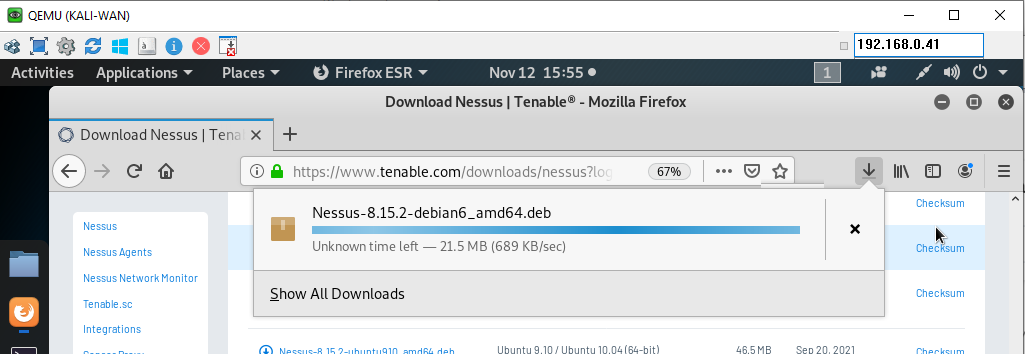


Рис. 11.

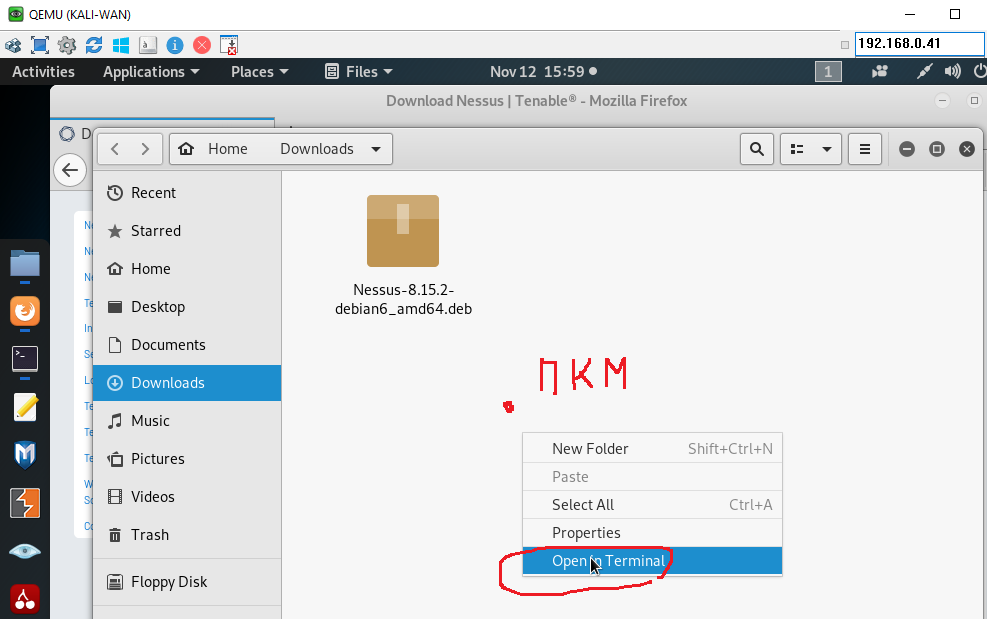


Рис. 12.

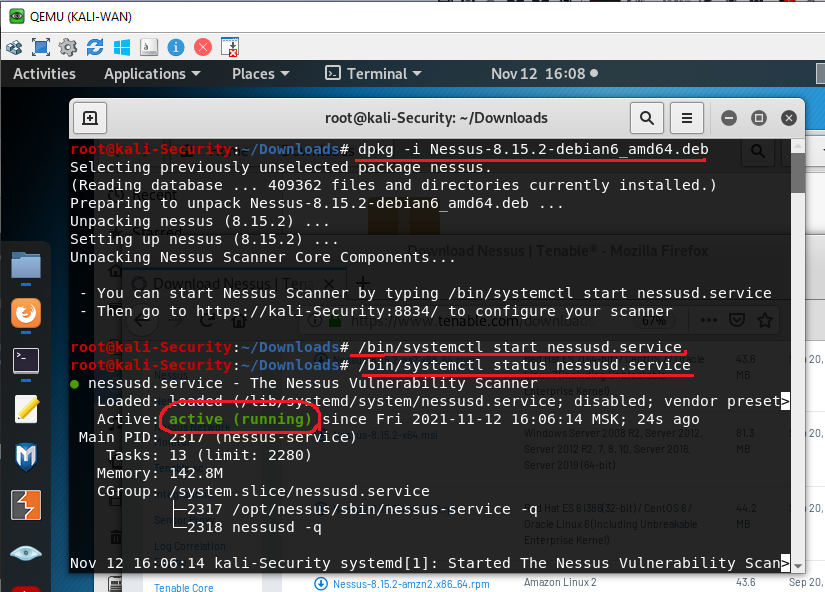


Рис. 13.

Пробуем перейти по адресу своей кали-линукс на порт 8834

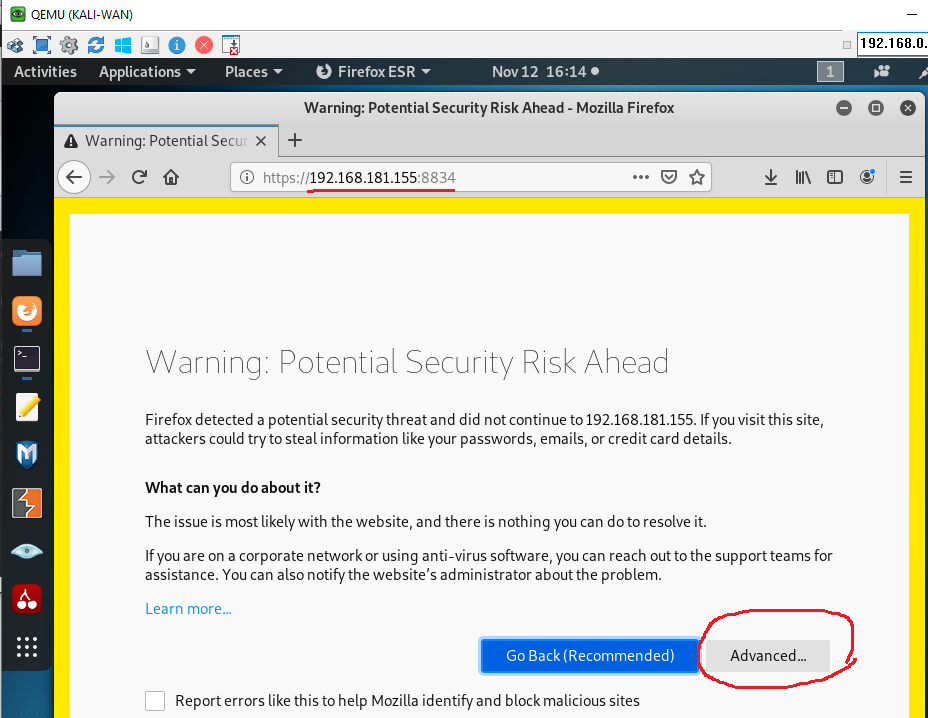


Рис. 14.

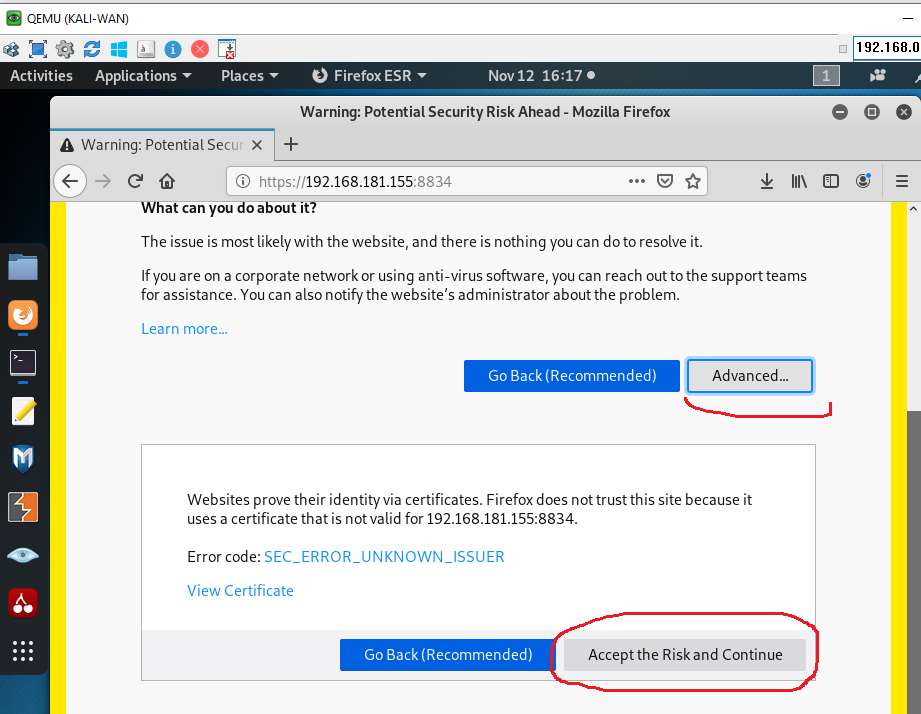


Рис. 15.

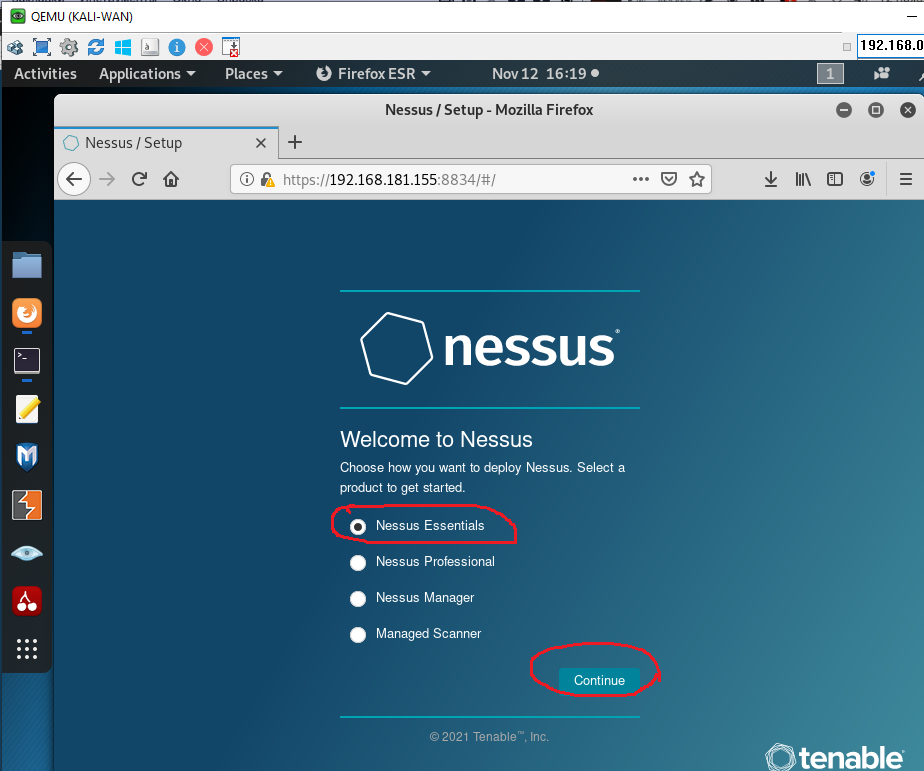


Рис. 16.

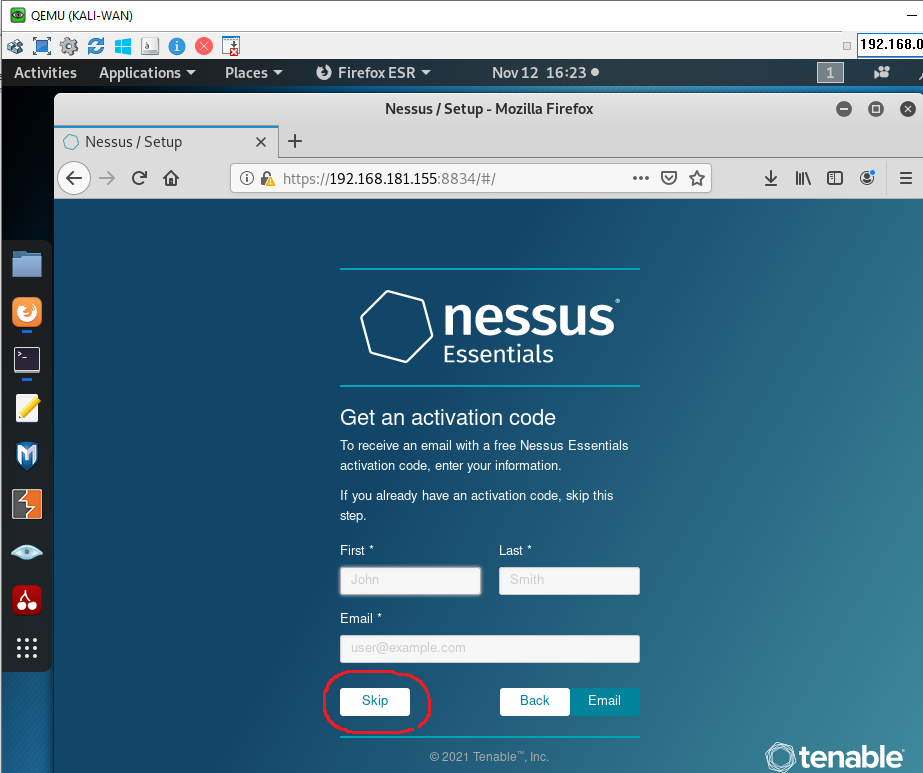


Рис. 17.

На почту пришел код активации

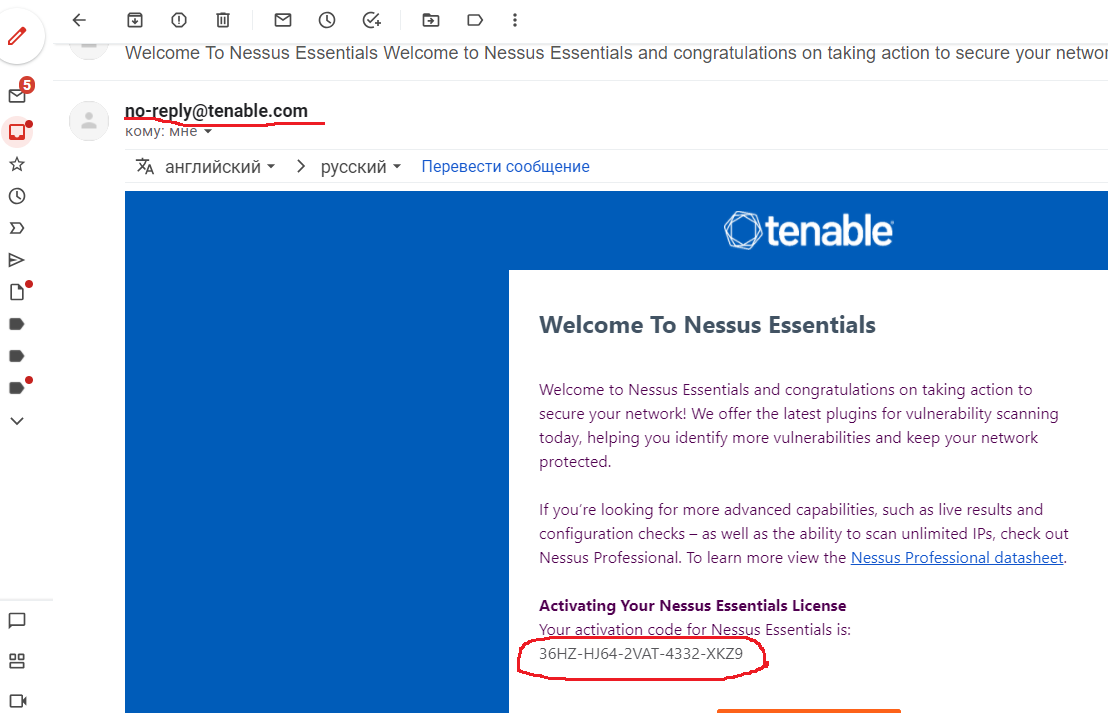


Рис. 18.

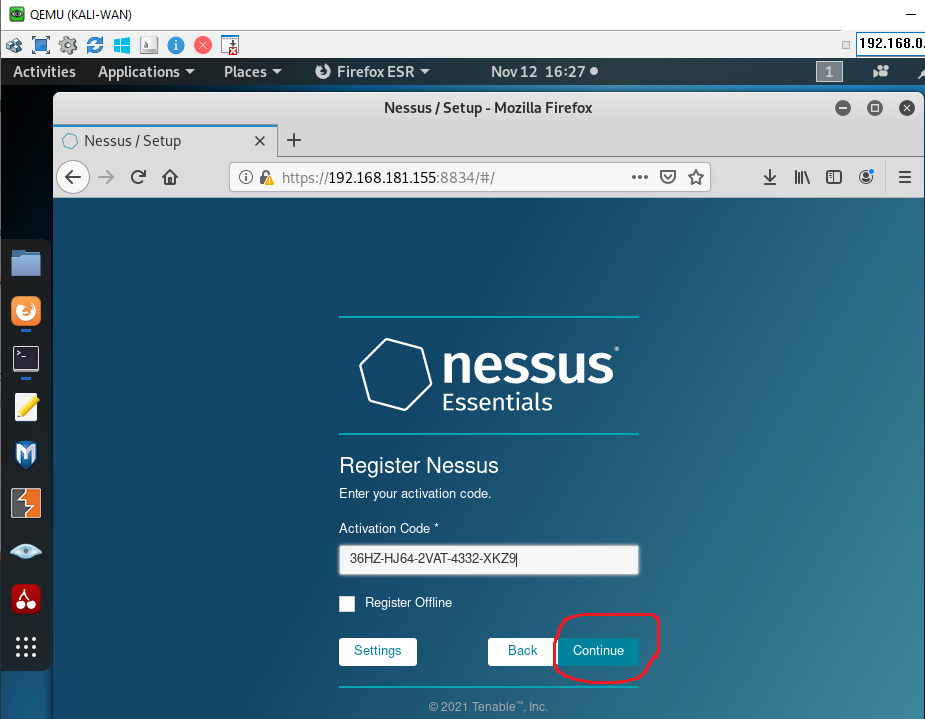


Рис. 19.

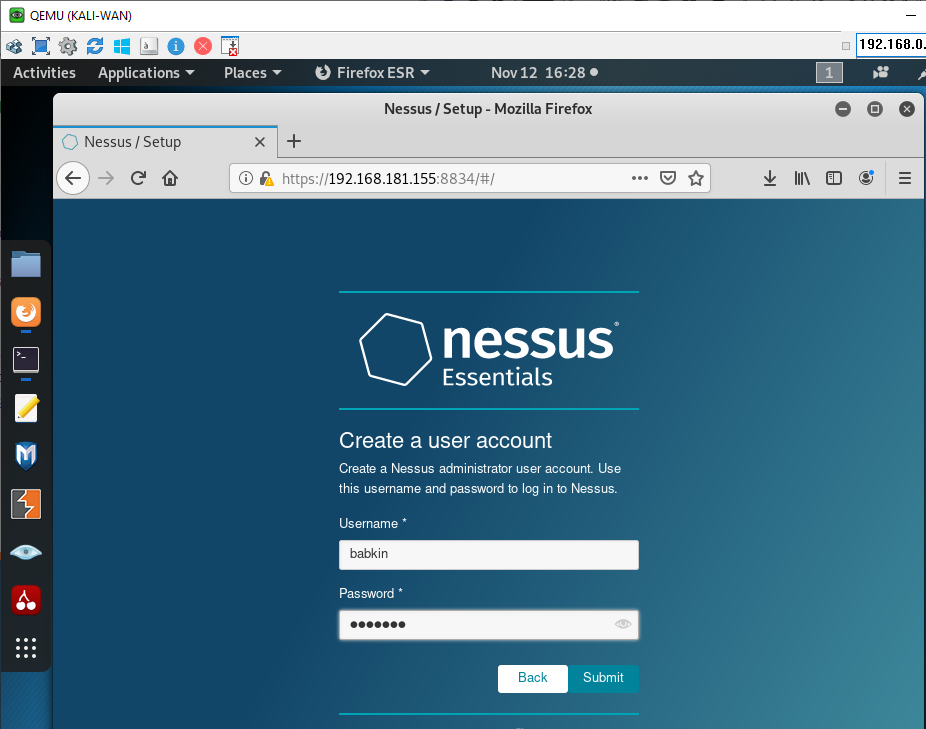


Рис. 20.

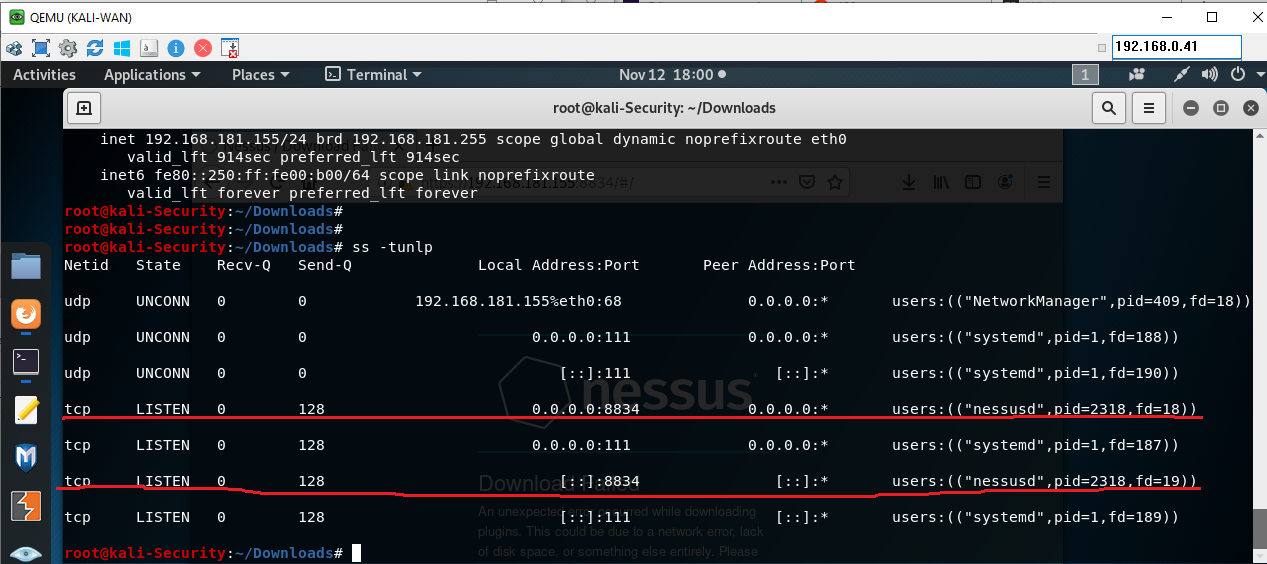


Рис. 21.

Видим, что есть сервисы nessusd, которые слушают на порту 8834. Задаем команду для того, чтобы сервис мог стартовать при перезагрузке системы.

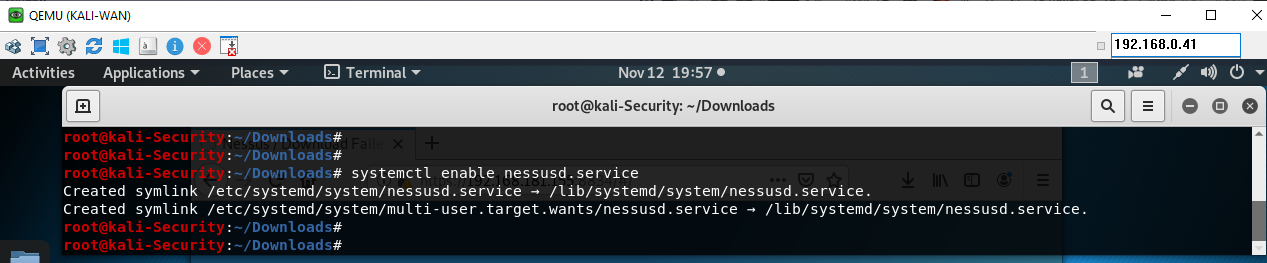


Рис. 22.

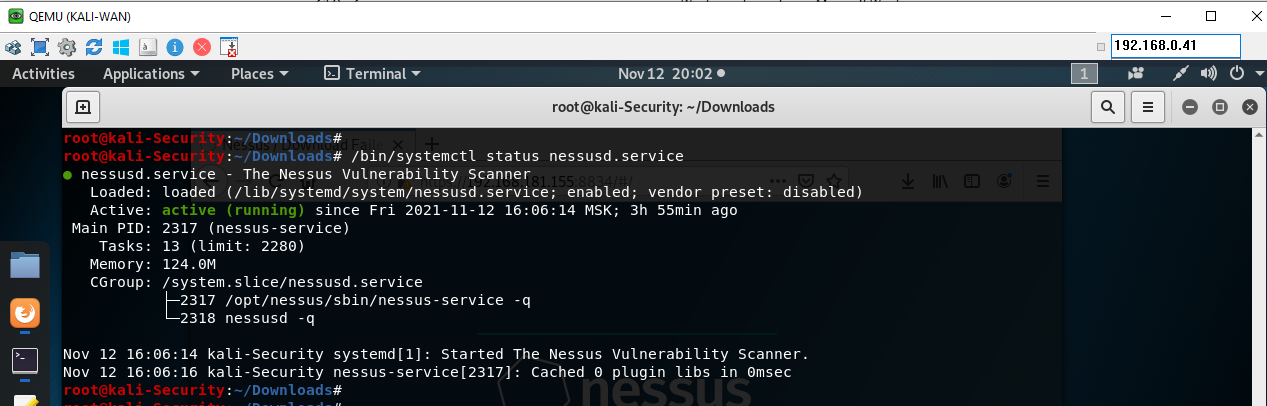


Рис. 23.

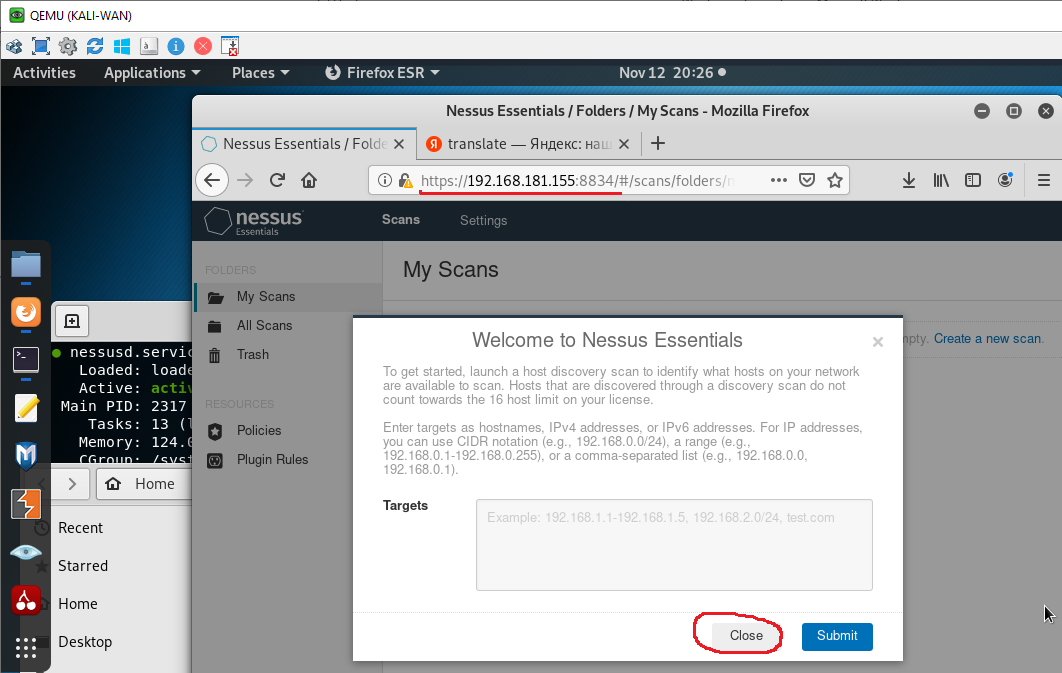


Рис. 24.

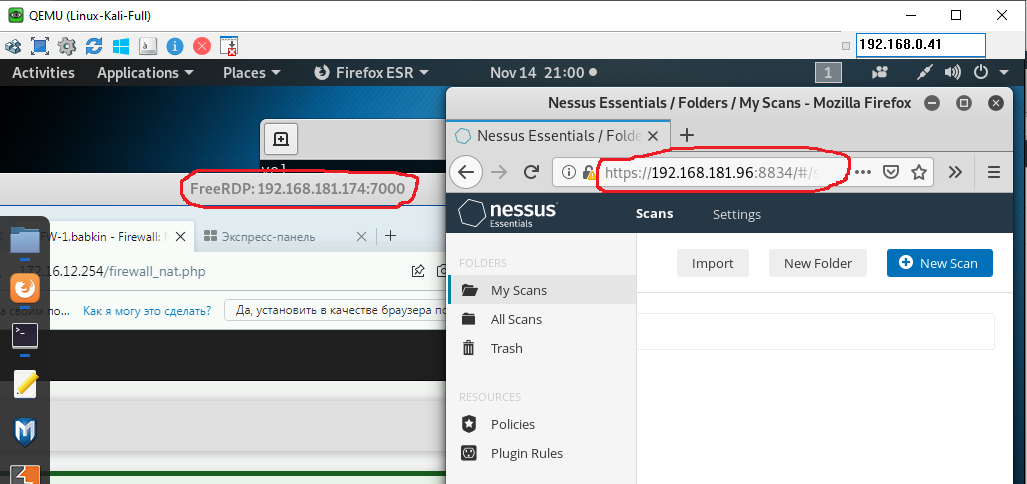


Рис. 25.

Теперь просканируем используя расширенное сканирование

Рис. 26.

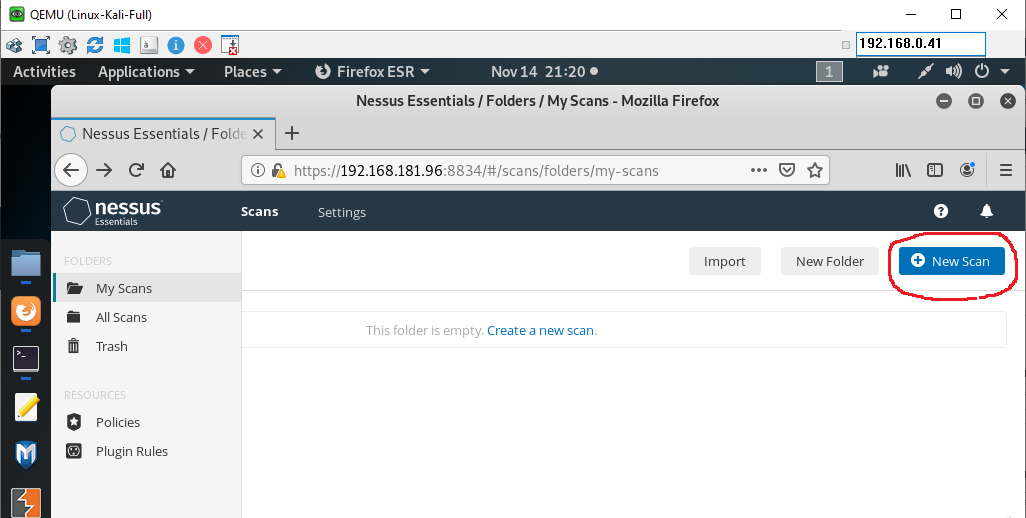


Рис. 27.

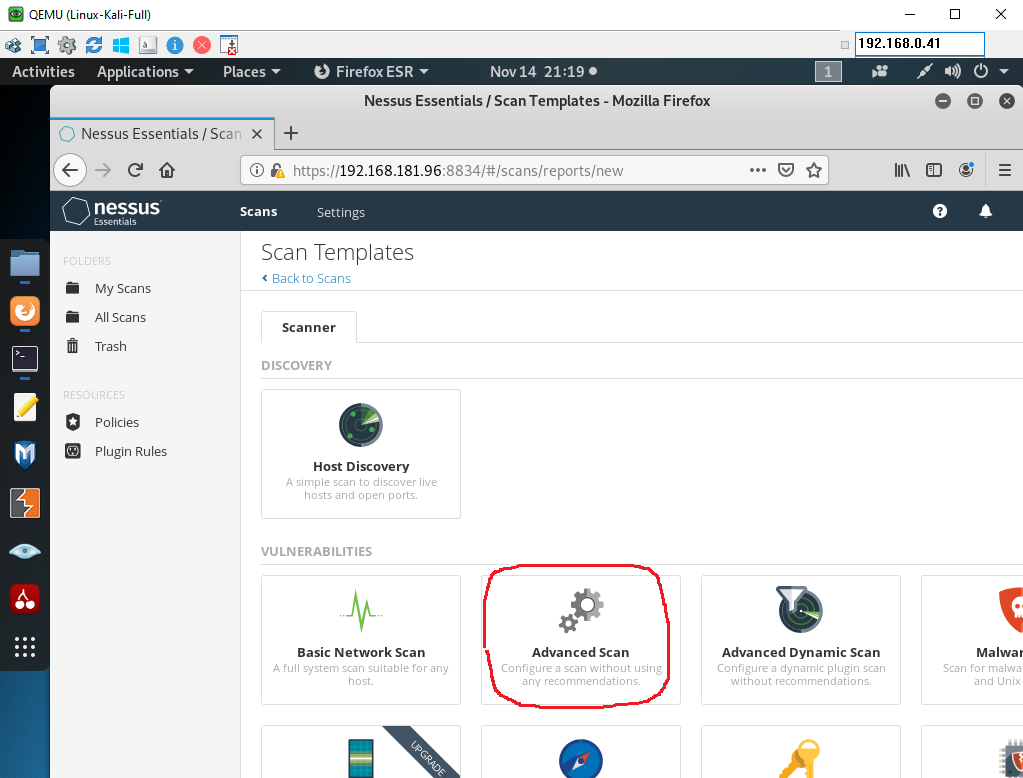


Рис. 28.



Рис. 29.

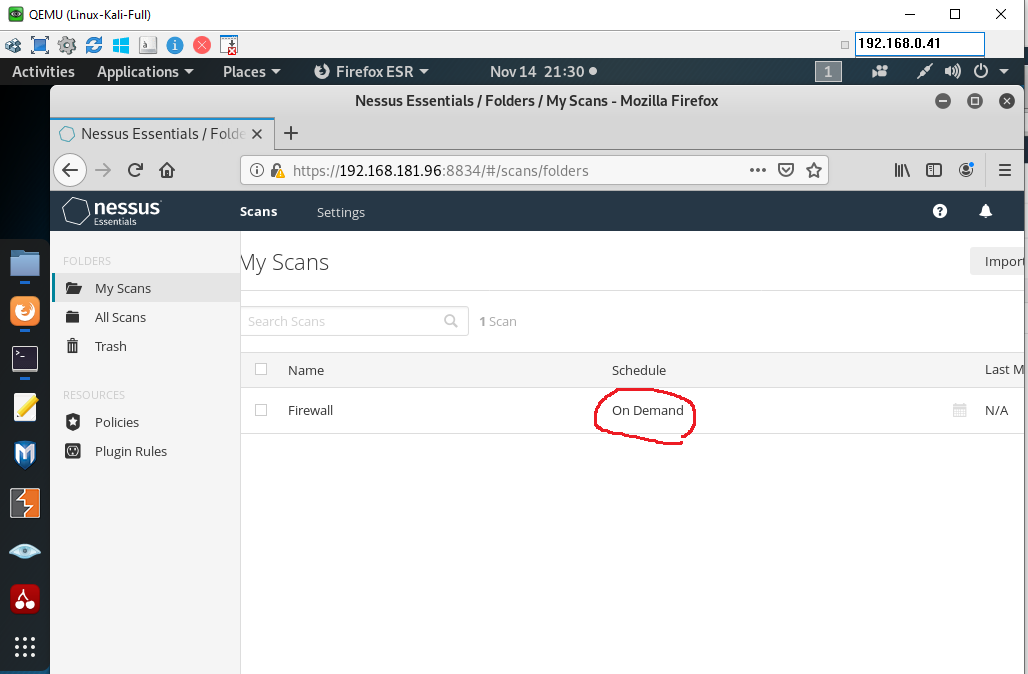


Рис. 30.

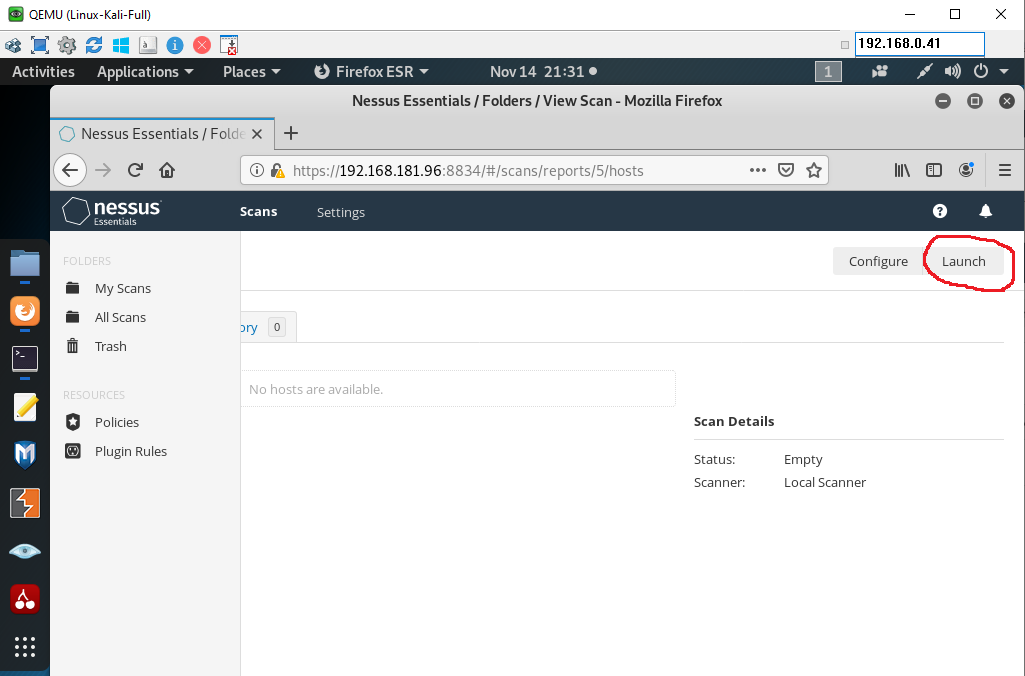


Рис. 31.



Рис. 32.