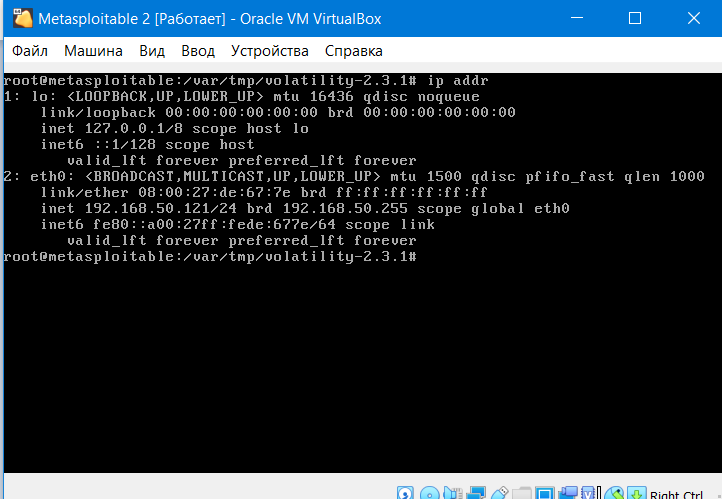
**Лабораторная работа №5. Сканер уязвимостей NESSUS**

**Кондратьев Артём 11-901**

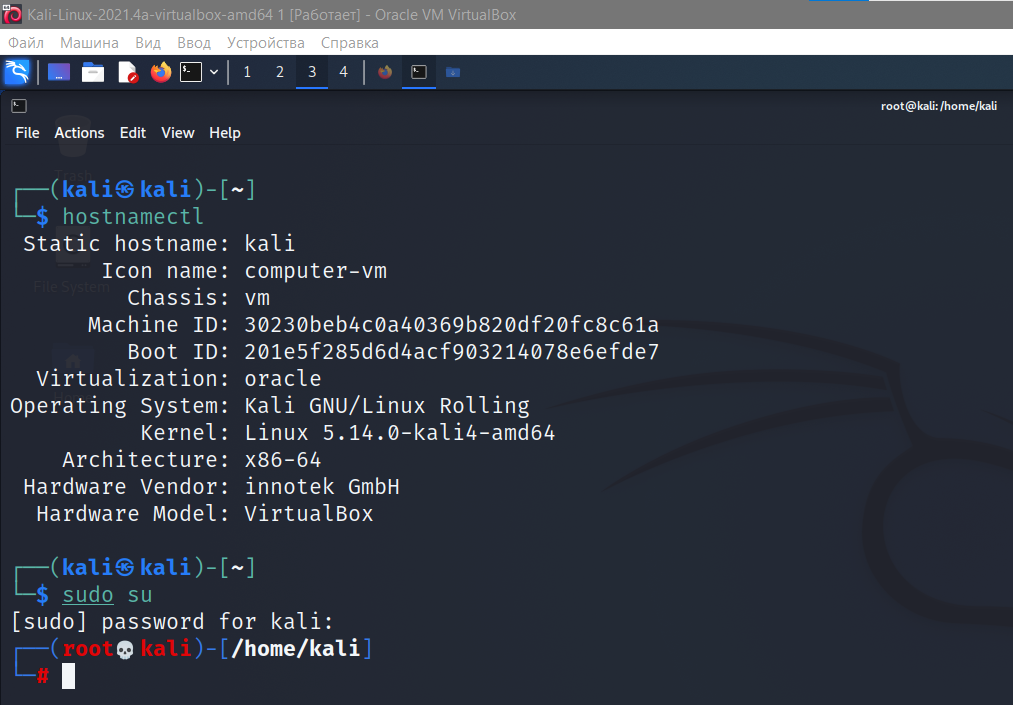
**1) Загрузка виртуальной машины Metasploitable**

1. Metasploitable 2



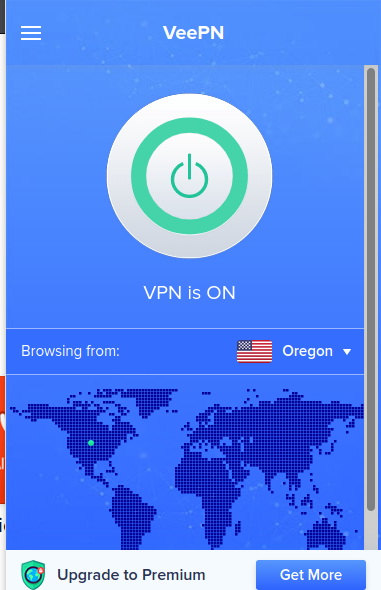
**2) Загрузка виртуальной машины Kali Linux**

1. Kali Linux 2021:

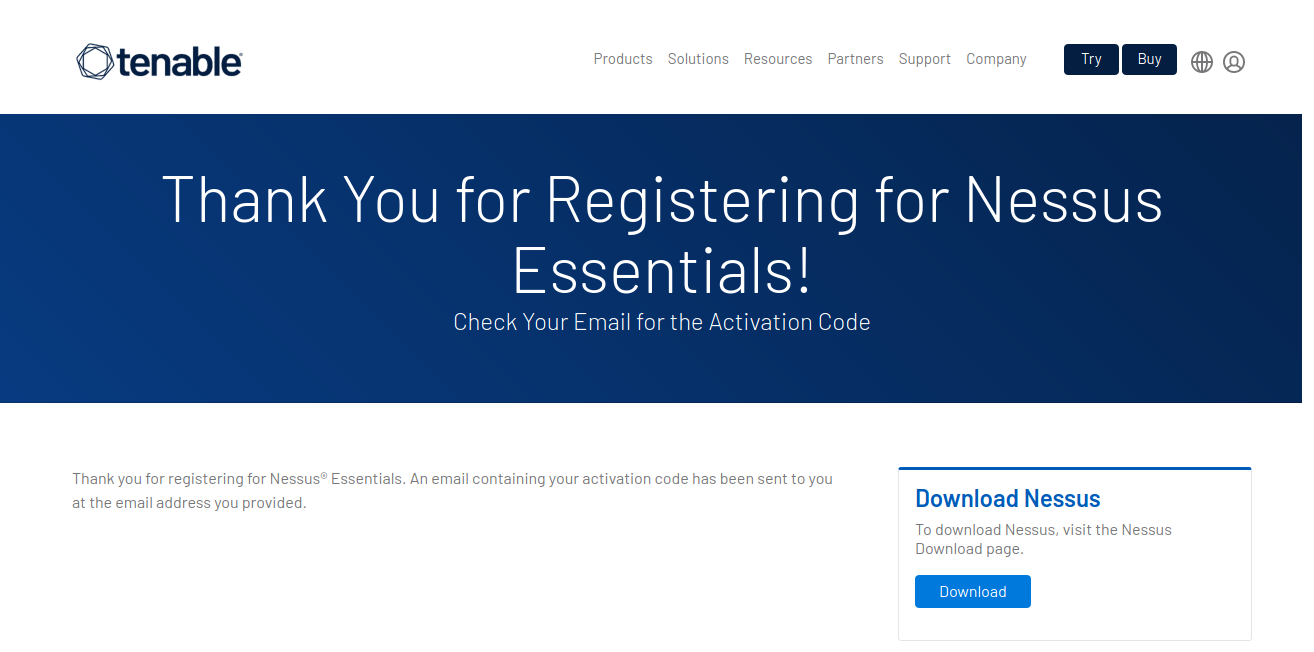


**3) Скачивание Nessus**

1. Для начала поставим любой VPN:

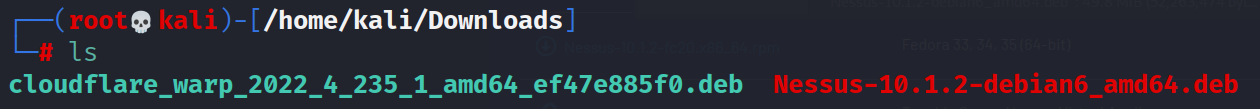
****

1. На виртуальной машине Kali Linux открыть любой браузер
2. В адресной строке указать адрес: <http://www.tenable.com/products/nessus/select-your-operating-system>

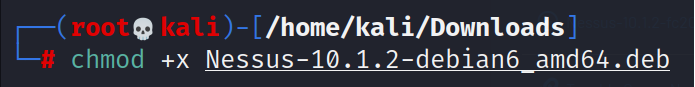


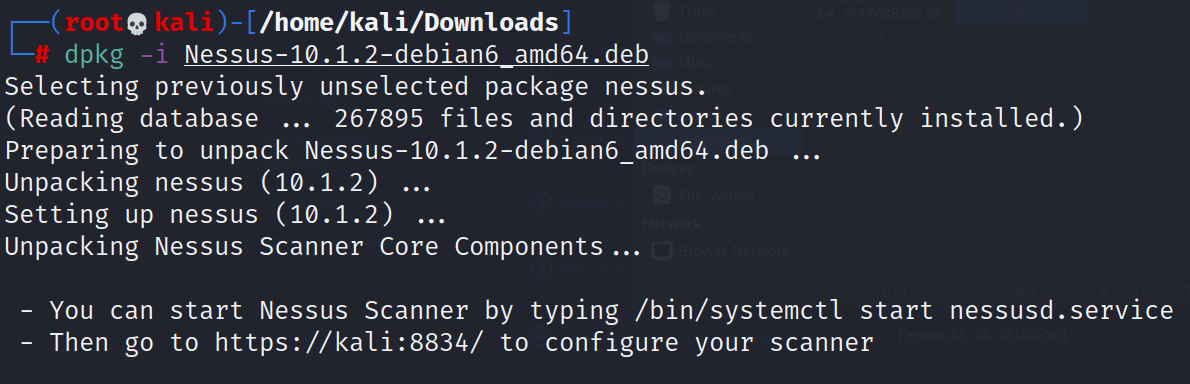
1. В появившемся окне нажать на кнопку «Download» в столбце «Nessus Home»

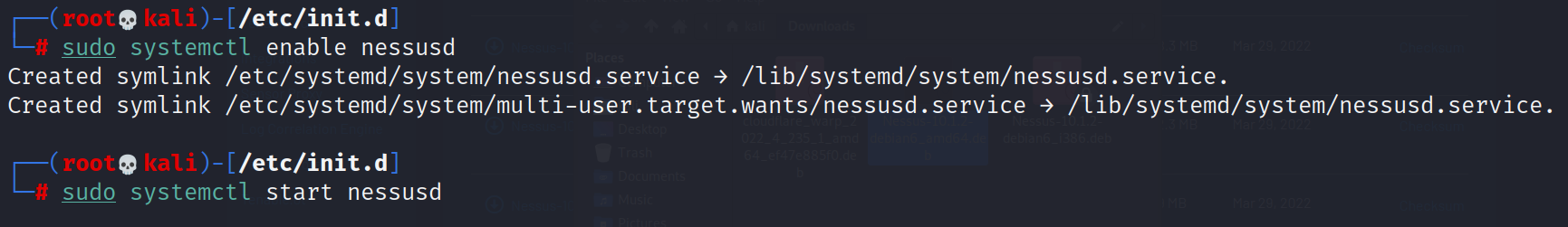
’

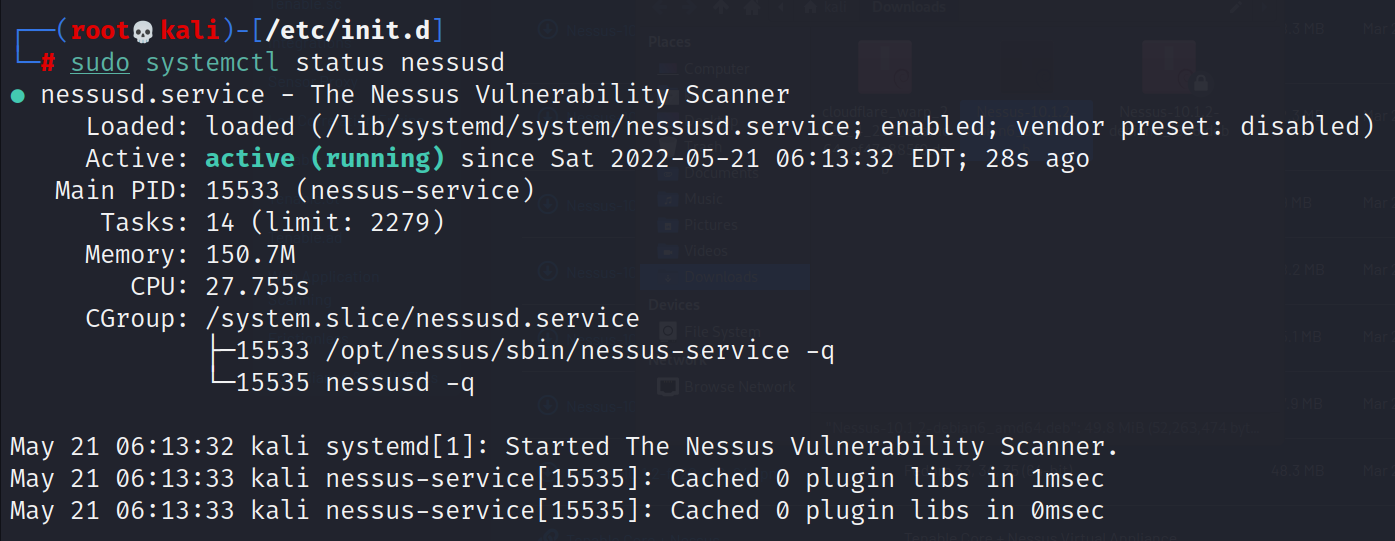
1. Убедиться в успешности выполненной загрузки, последовательно выполнив следующие команды: *cd ~/Загрузки* и *ls –la*

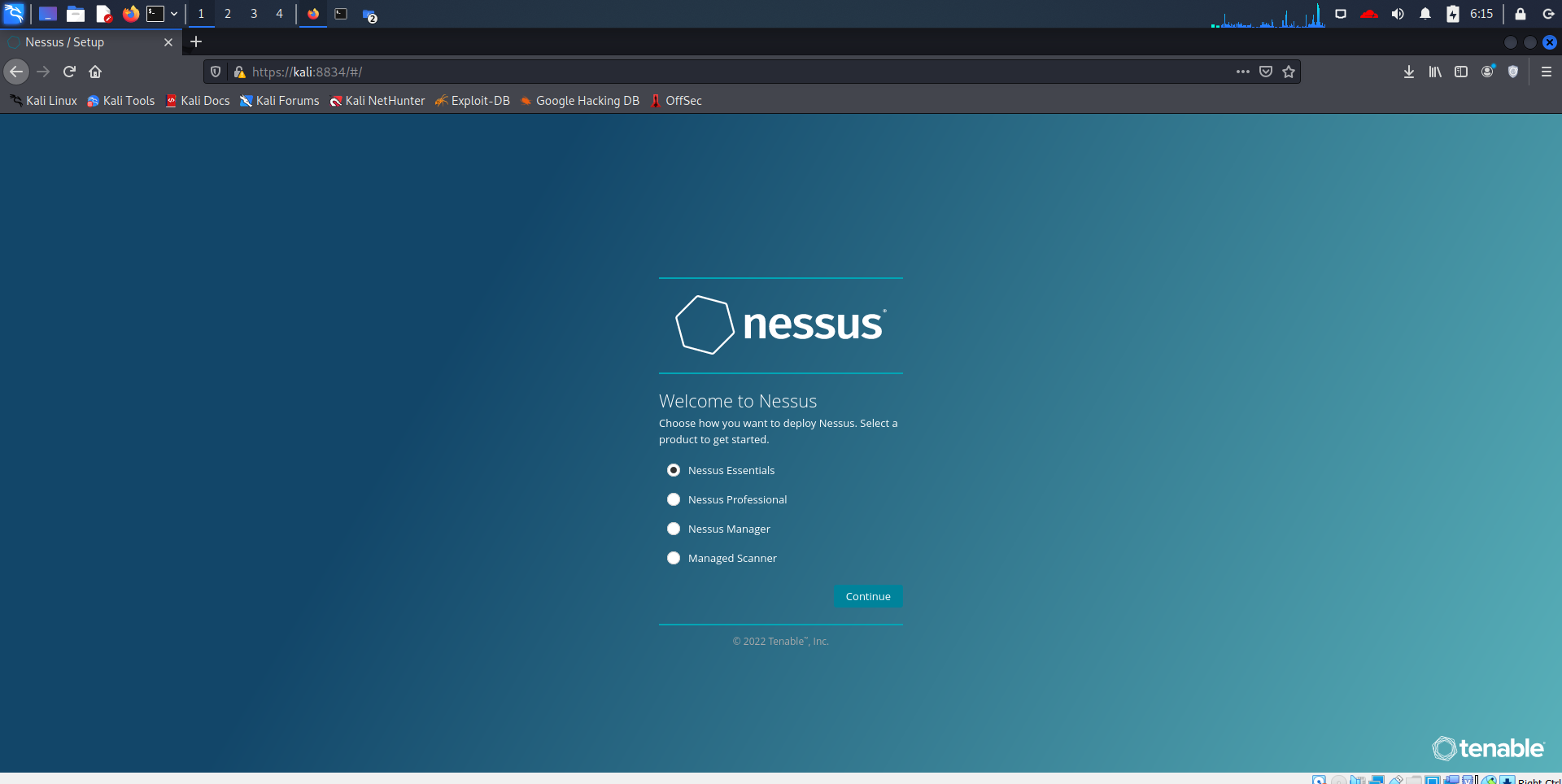
**4) Установка и запуск Nessus**

1. Выполнить установку сканера с помощью команды: *chmod* и *dpkg –i Nessus-10.1.2-debian6 \_amd64>.deb*



1. Запустить демон nessusd с помощью команды: */etc/init.d/nessusd start*

**

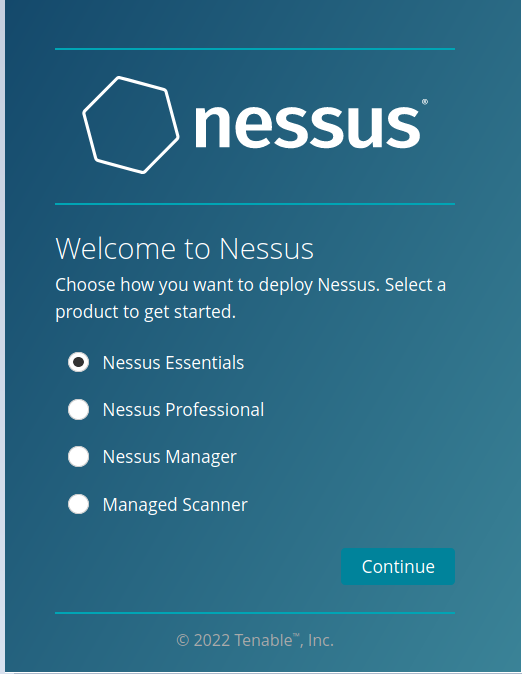
1. В адресной строке новой вкладки браузера iceweasel выполнить переход по адресу: https://kali:8834/;

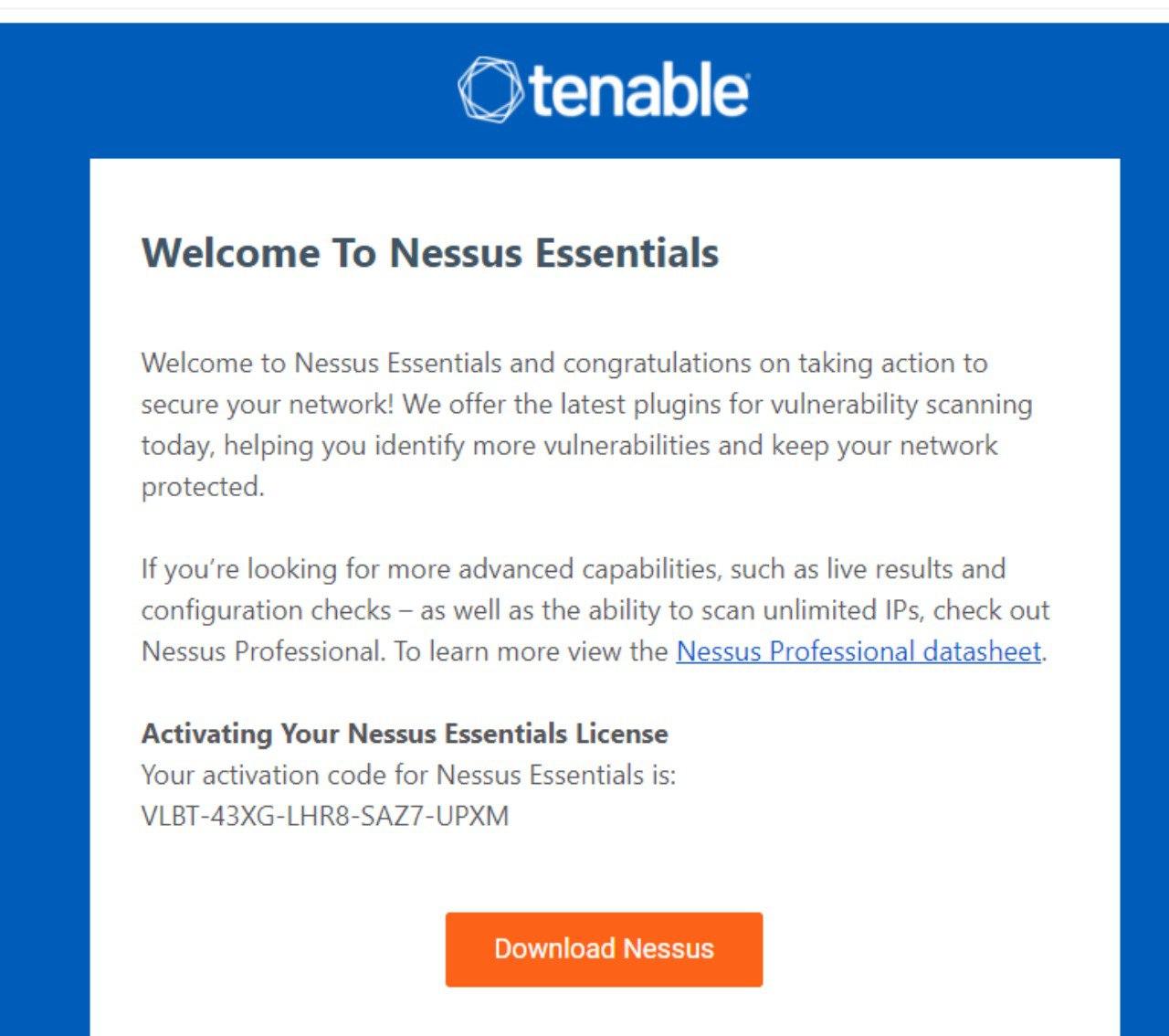
.

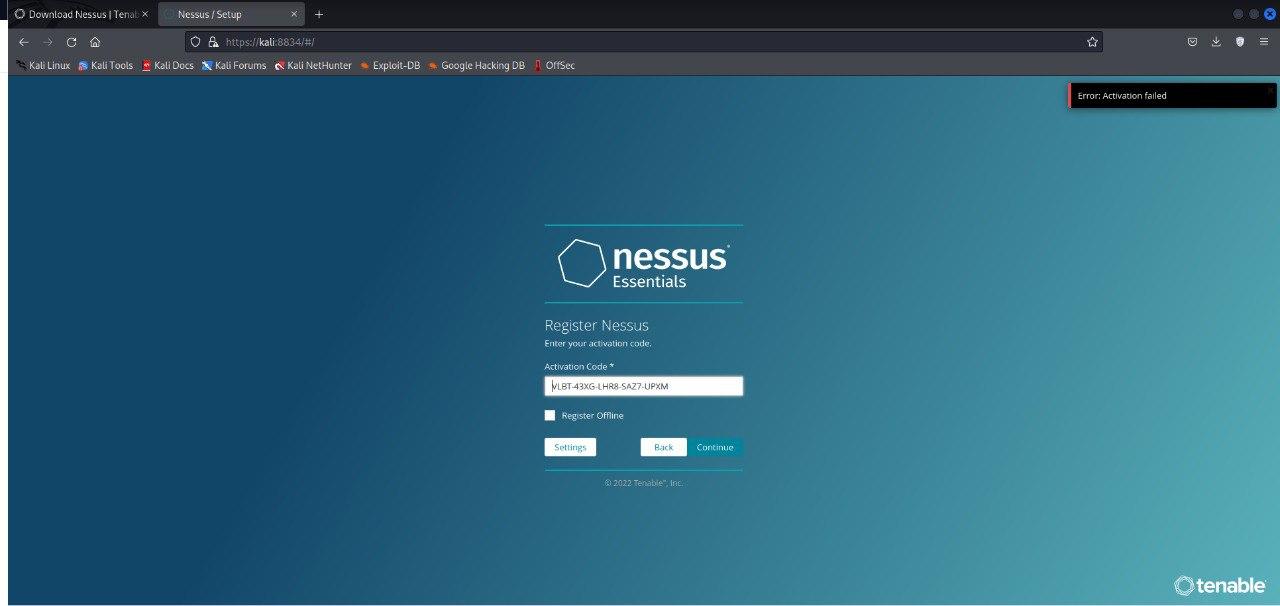
**5) Регистрация сканера**

**Дальнейшее выполнение работы невозможно ввиду наложенных санкций и т.д. Нельзя ввести лицензионный ключ!**

1. В адресной строке новой вкладки браузера iceweasel выполнить переход по адресу: http://www.tenable.com/products/nessus/nessus-professional/evaluate;
2. В появившемся окне заполнить ВСЕ поля с символом «\*» колонки «Register»
3. В окне браузера iceweasel с адресом https://kali:8834/ завершить регистрацию с помощью полученного ключа активации, при этом указать пользователя и пароль для дальнейшей работы со сканером.



****

****