**ФИО:** Степанищева Анастасия Андреевна

**Группа:** 11–902

**Тема:** ЛАБОРАТОРНАЯ РАБОТА №5. Сканер уязвимостей NESSUS.

**Содержание:**

1. Подготовка

2. Установка Nessus

3. Регистрация сканера (вынужденное завершение лабораторной работы №5)

**Отчет**

1. Подготовка

Разворачиваем виртуальные машины (Metasploitable (сетевой мост) и Kali Linux (NAT)), подготовленные в результате выполнения предыдущих лабораторных работ.

2. Установка Nessus

Откроем браузер iceweasel на виртуальной машине Kali Linux

В адресной строке укажем адрес <http://www.tenable.com/products/nessus/select-your-operating-system>. Доступ запрещен. Попробуем использовать vpn(в моем случае OpenVPN), для того чтобы обойти это ограничение.

Выполняем загрузку. Для проверки выполним ls -la из директории Загрузки.

Выполняем установку и запускаем демон (dpkg –i Nessus-6.5.2-debian6\_<архитектура>.deb) (/etc/init.d/nessusd start)

Перейдем по адресу <https://kali:8834>, открылось окно регистрации.(1)

3. Регистрация сканера

В новой вкладке откроем <http://www.tenable.com/products/nessus/nessus-professional/evaluate>. Открывается форма регистрации. Заполняем все обязательные поля и регистрируемся.

Во вкладке (1) завершим регистрацию, указав пользователь-пароль. При этом используем код активации с почты. Получаем ошибку. Сервис не доступен. Ограничение обойти не удалось. Лабораторная работа не может быть закончена в связи с недоступностью сервиса.