МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования «Ижевский государственный технический  
университет имени М. Т. Калашникова»

Институт «Информатика и вычислительная техника»

Кафедра «Защита информации в компьютеризированных системах»

**ОТЧЕТ**

по лабораторной работе №4

по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем»

на тему «Анализ защищенности компьютера с помощью OpenVAS»

Выполнили:  
студент гр. С17-361-1 Буров К.А.

Проверил:  
ст. преп. Кудашев П. А.

Ижевск 2021

# **Цель работы**

Исследовать хост в локальной сети на наличие уязвимостей с помощью средства оценки OpenVAS.

# **Задачи**

1. Развернуть виртуальную машину для установки OpenVAS
2. Установить OpenVAS
3. Обновить базы данных уязвимостей
4. Просканировать локальную сеть (хостовую машину)

# **Ход работы**

В качестве виртуальной машины был взят готовый образ Kali Linux для Oracle VirtualBox.

Перед установкой непосредственно OpenVAS обновим все пакеты с помощью следующих команд.

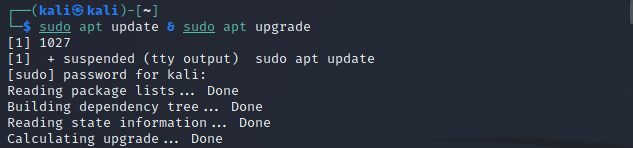


Рисунок 1 - Обновление пакетов

При обновлении не удалось подтянуть некоторые пакеты, однако они не требуются для работы OpenVAS.

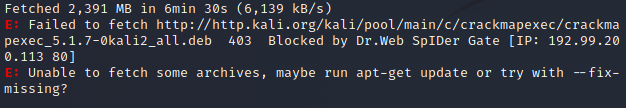


Рисунок 2 - Пакеты, которые не удалось обновить

Установка OpenVAS происходит с помощью следующей команды:

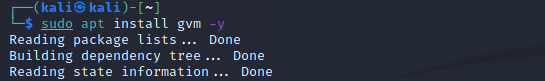


Рисунок 3 - Команда для установки OpenVAS

В процессе установки будут выведены несколько информационных сообщений.

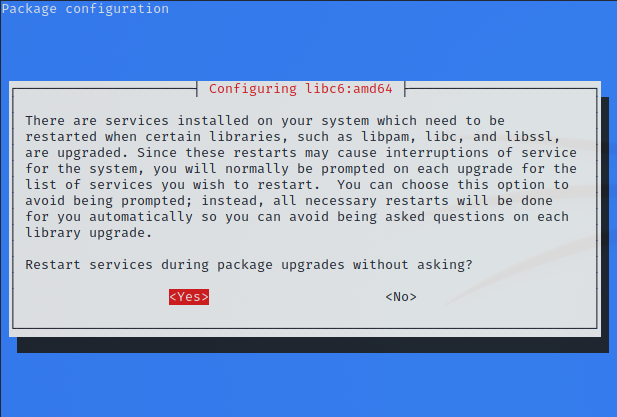


Рисунок 4 - Диалоговое окно для настройки запросов рестарта сервисов

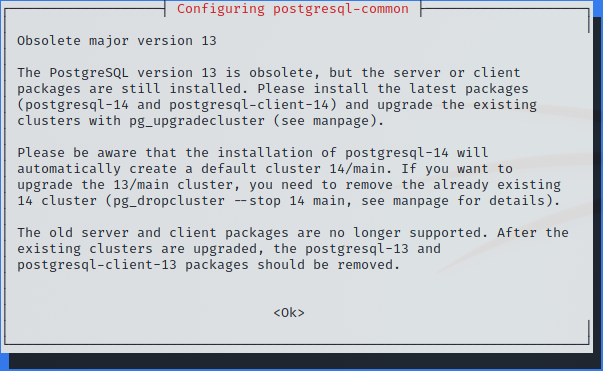


Рисунок 5 - Уведомление об устаревшей версии Postgresql

Для избежания проблем при настройке OpenVAS обновим Postgresql и удалим старую версию.

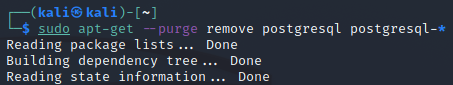


Рисунок 6 - Команда для удаления Postgresql

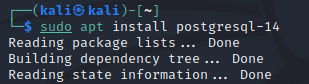


Рисунок 7 - Команда для установки Postgresql 14

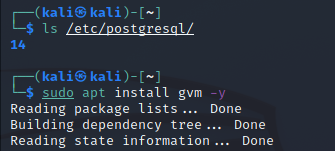


Рисунок 8 - Проверка версии Postgresql и повторная установка OpenVAS

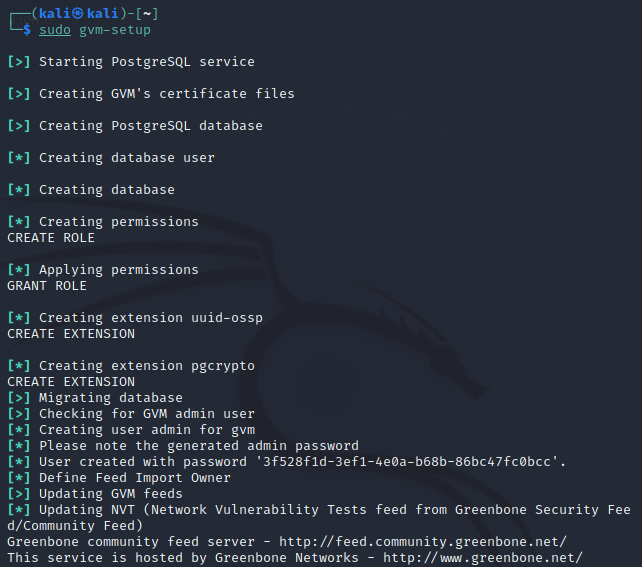


Рисунок 9 - Команда для автоматической настройки OpenVAS

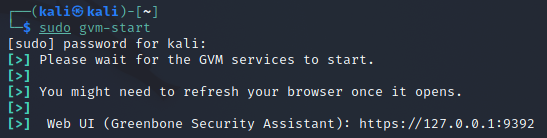


Рисунок 10 - Запуск OpenVAS

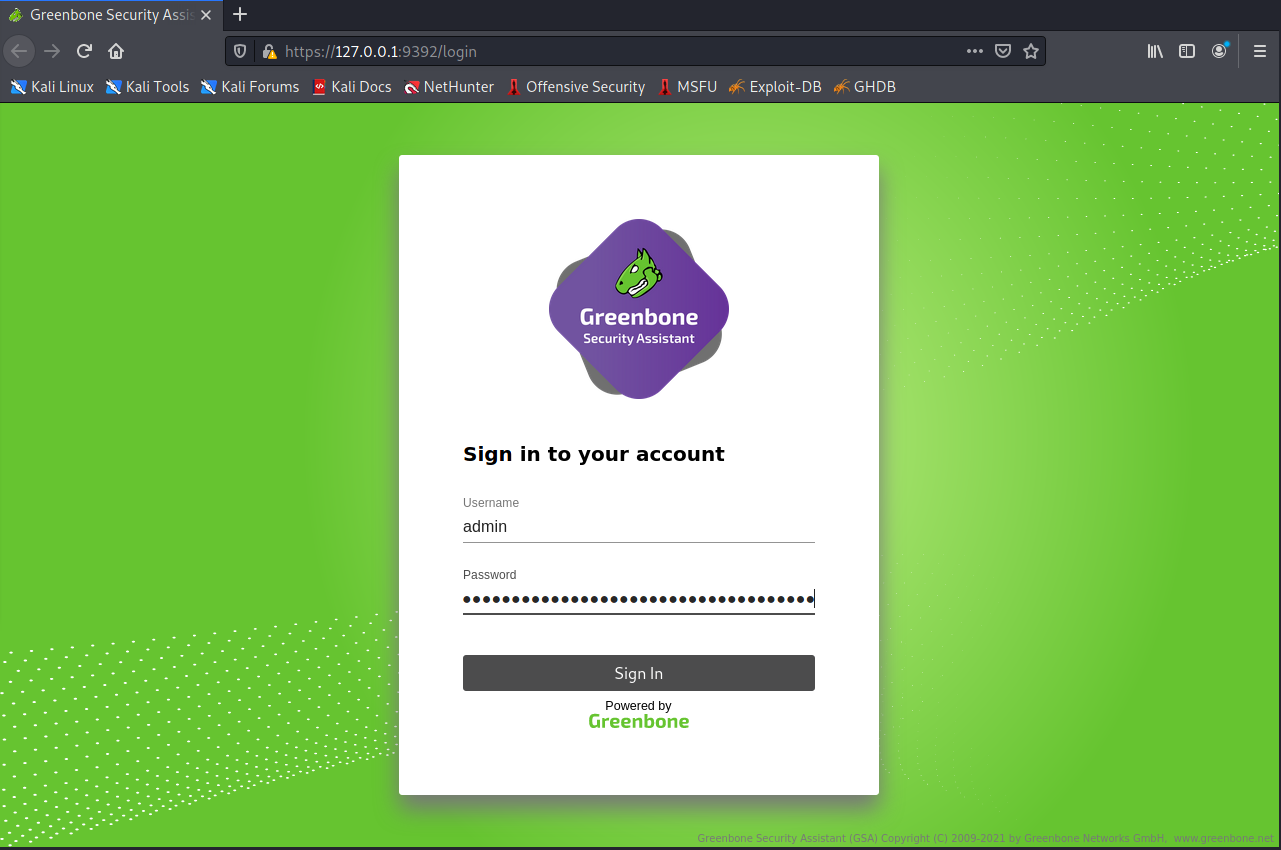


Рисунок 11 - Окно входа в веб-интерфейс

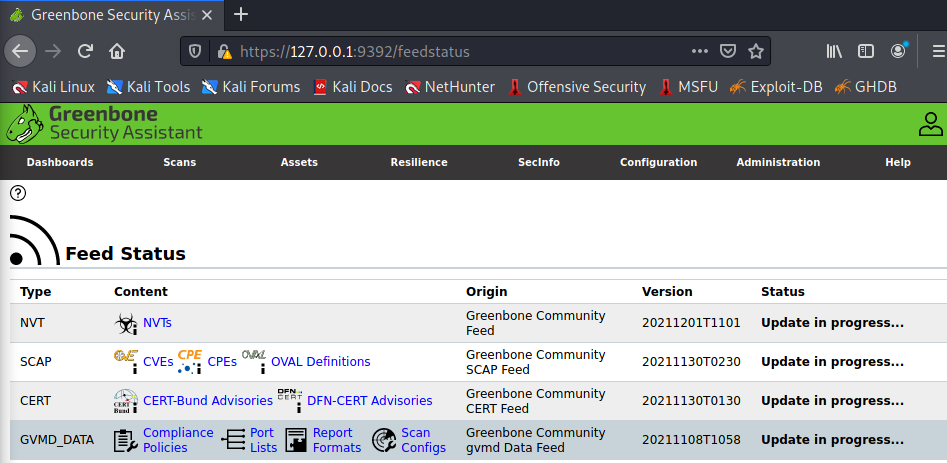


Рисунок 12 - Окно обновления базы данных OpenVAS

NVT – тесты уязвимости сети.

SCAP – Протокол автоматизации безопасности контента

CERT – группа реагирования на чрезвычайные компьютерные ситуации.

GVMD\_DATA – Настройки GVM

Процесс автоматического обновления долго находился в статусе Update n progress, поэтому было вызвано ручное обновление с помощью следующей команды:

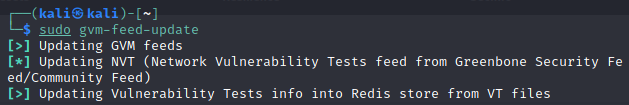


Рисунок 13 - Команда для обновления баз OpenVAS

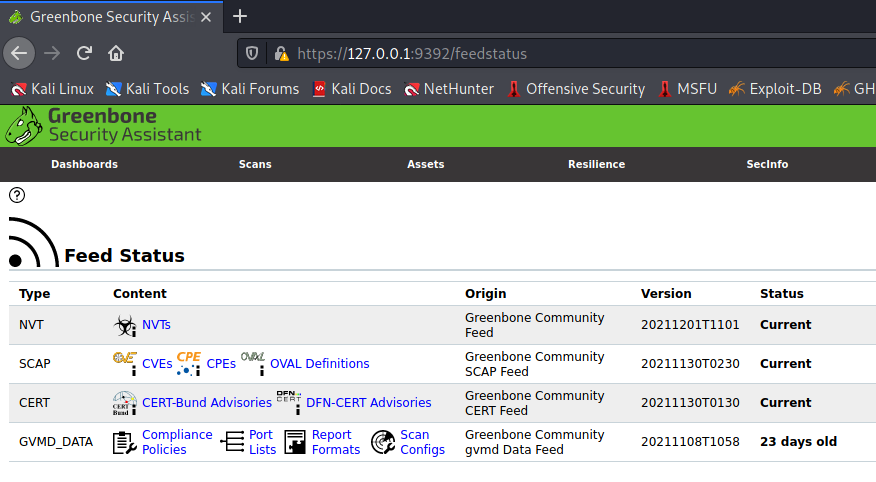


Рисунок 14 - Статусы баз после обновления

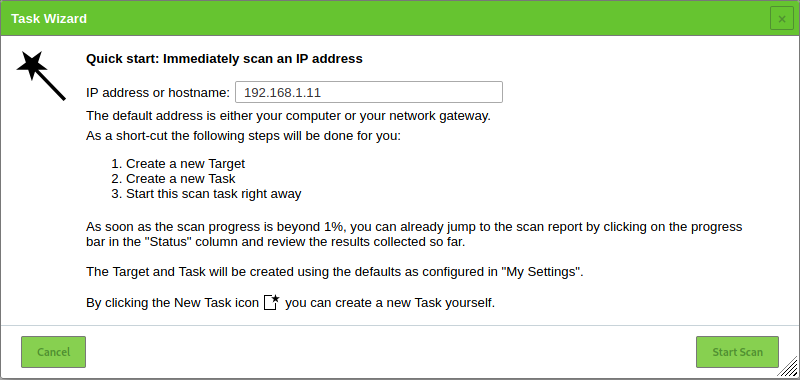


Рисунок 15 - Создание задачи для быстрого сканирования хоста

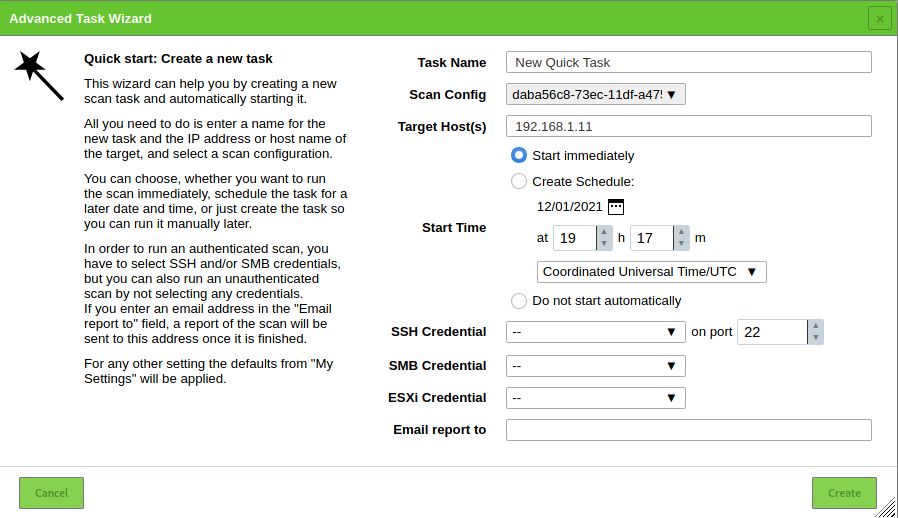


Рисунок 16 - Создание задачи для моментального сканирования хоста

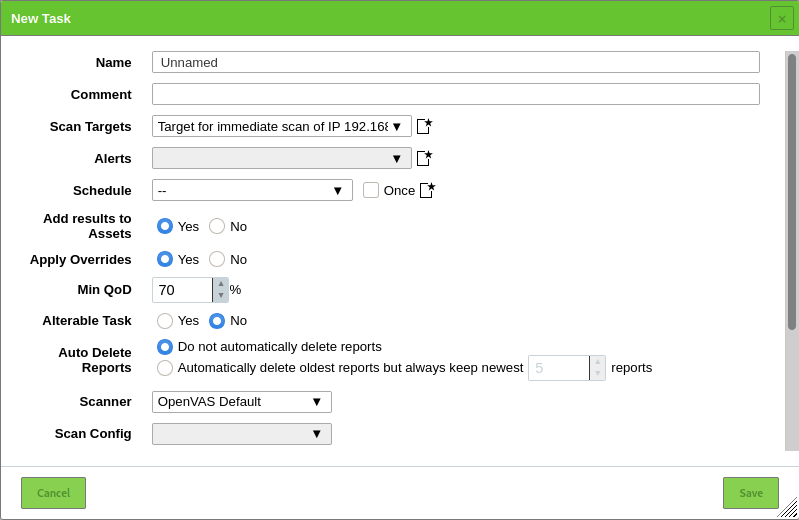


Рисунок 17 - Создание задачи для настраиваемого сканирования хоста

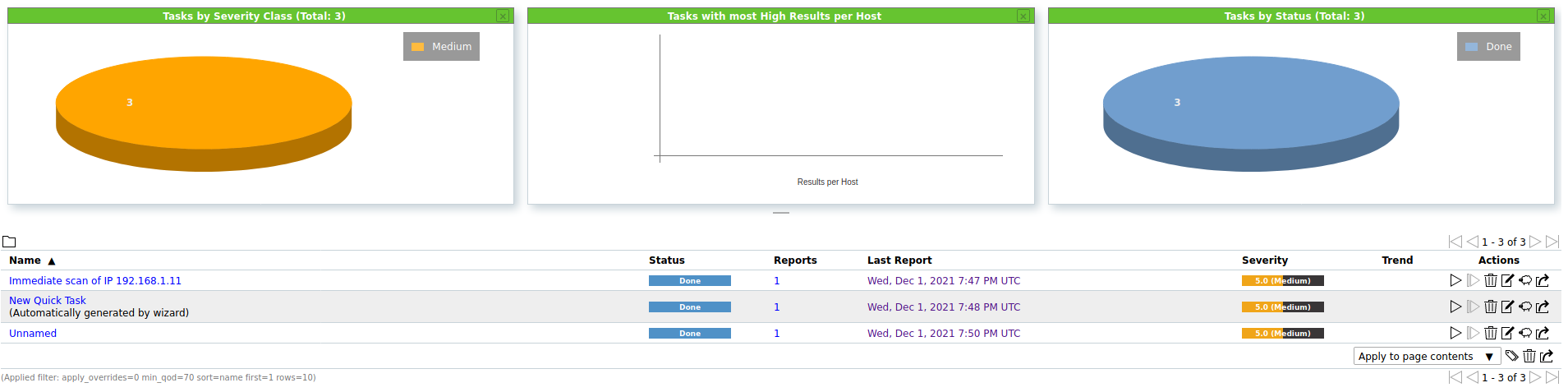


Рисунок 18 -Окно, отображающее статусы запущенных задач

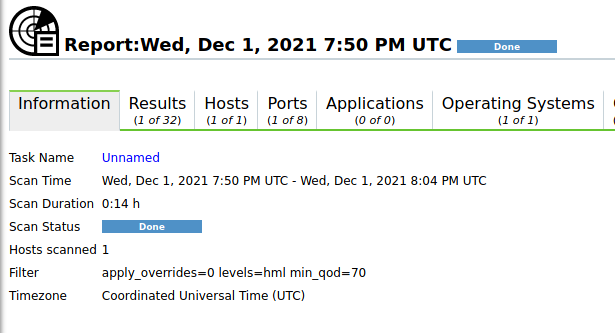


Рисунок 19 - Отчет после настраиваемого сканирования

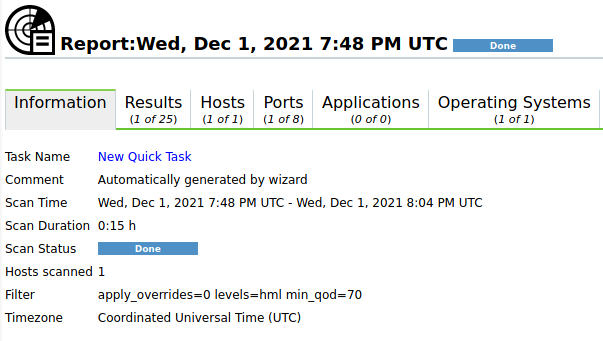


Рисунок 20 - Отчет после быстрого сканирования

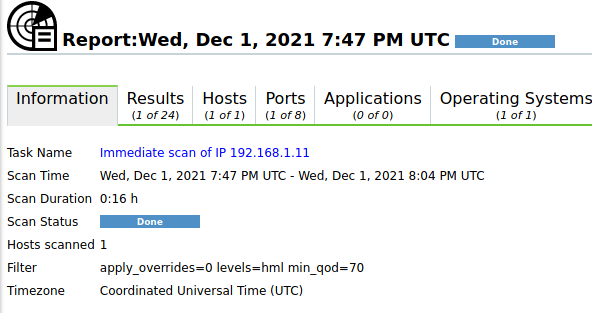


Рисунок 21 - Отчет после моментального сканирования

Отчеты всех трех сканирований содержали идентичные данные, поэтому каждый отчет отдельно рассматриваться не будет.

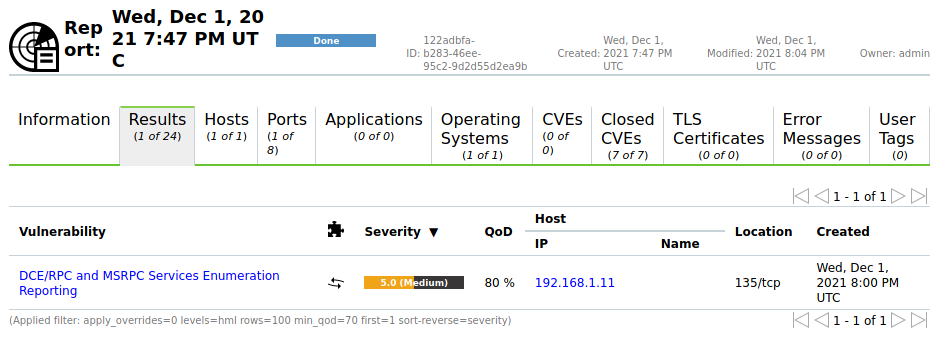
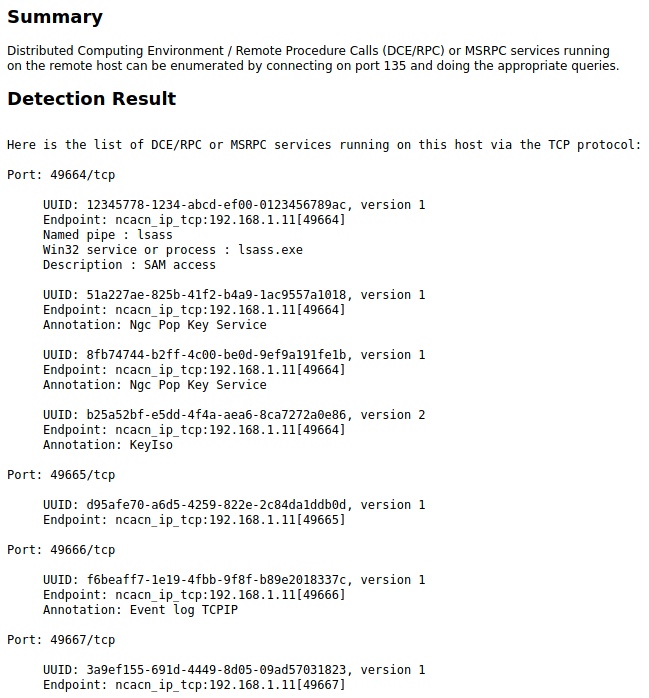
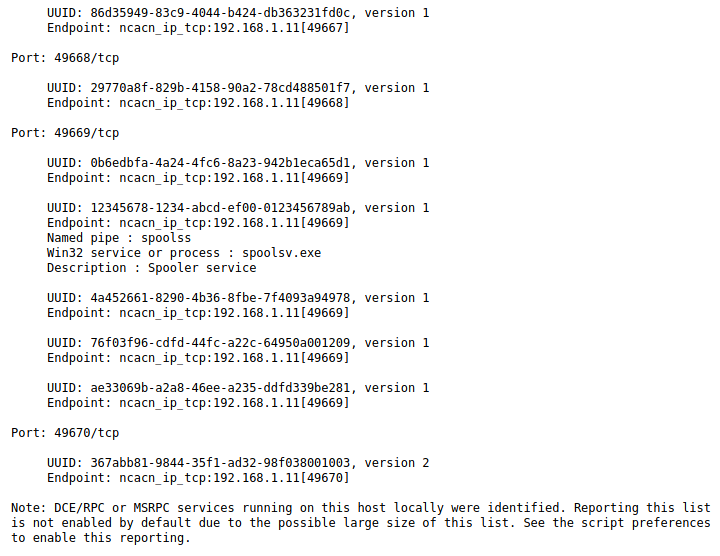


Рисунок 22 - Обнаруженные уязвимости





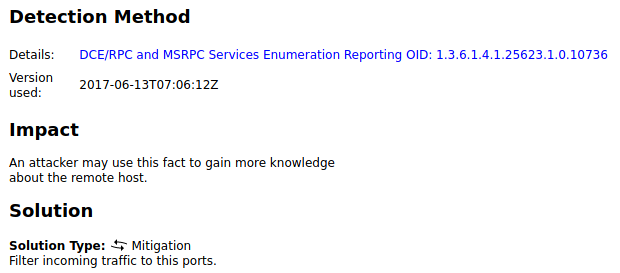


Рисунок 23 - Подробное описание найденной уязвимости

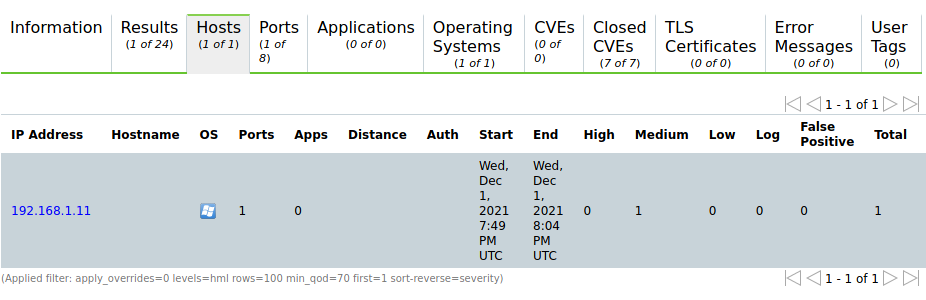


Рисунок 24 - Список просканированных хостов

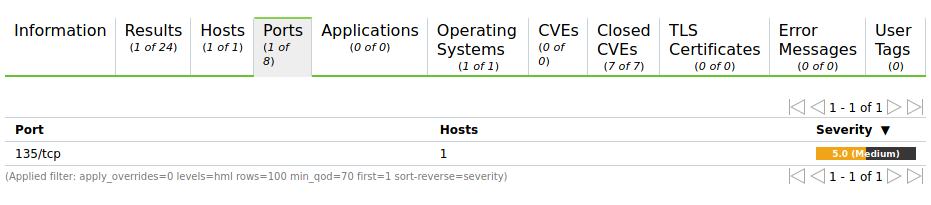


Рисунок 25 - Просканированные порты

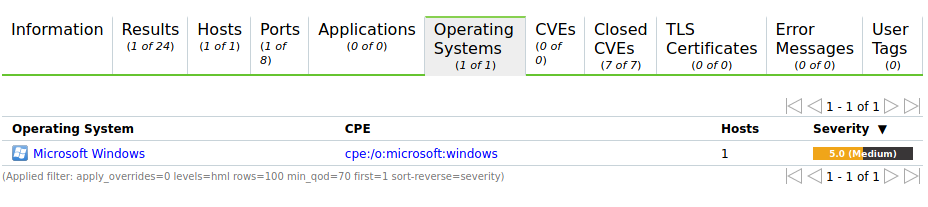


Рисунок 26 - Операционные системы хостов

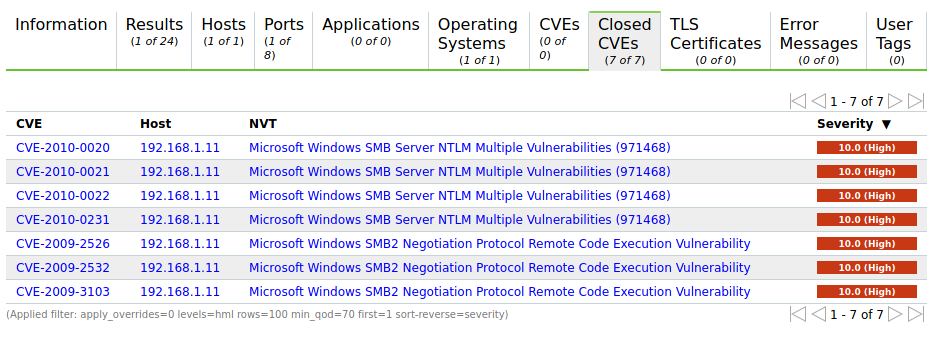


Рисунок 27 - Закрытые уязвимости хостов

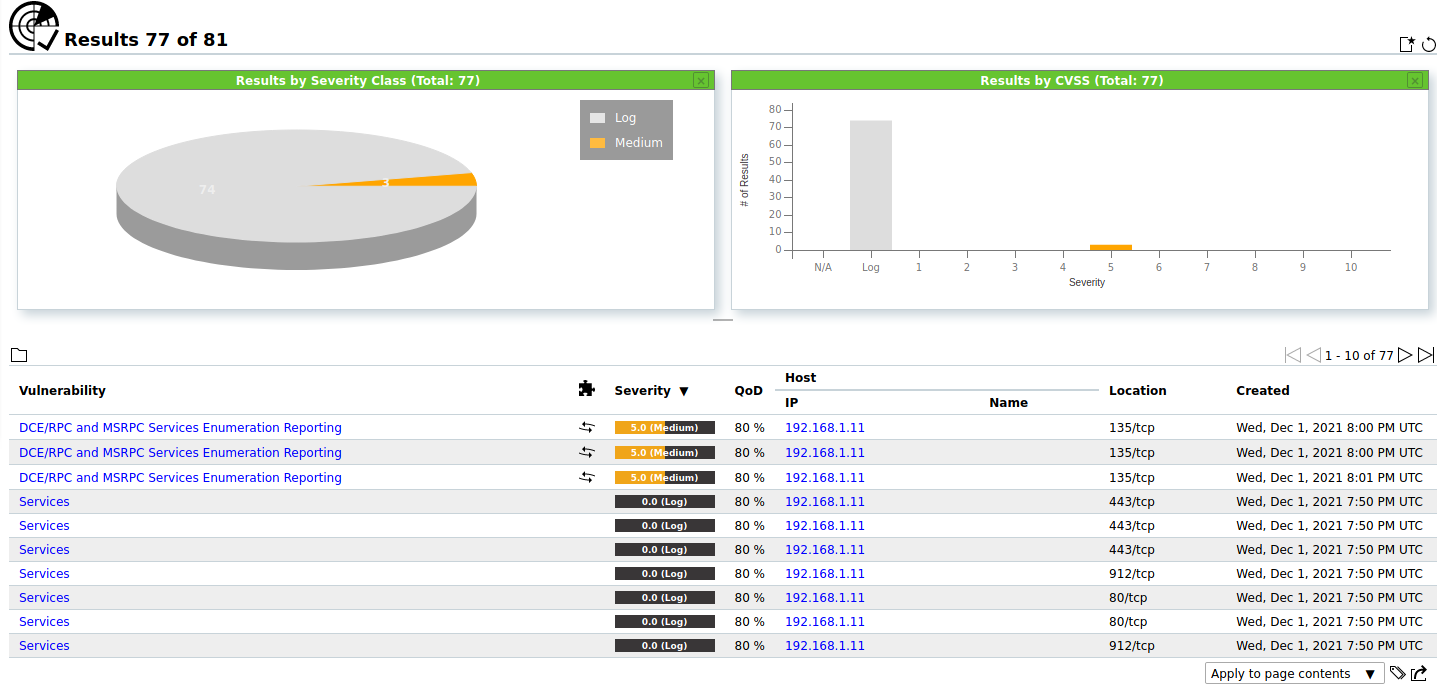


Рисунок 28 - Результаты сканирований

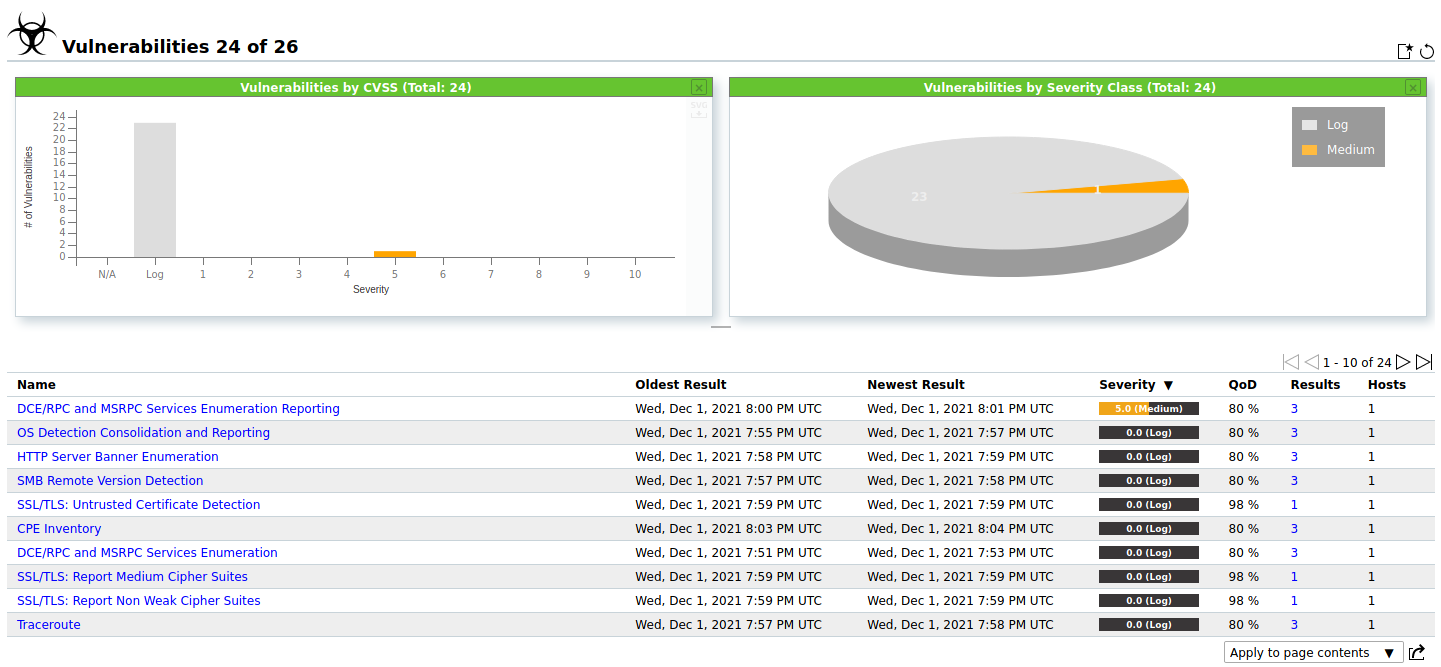


Рисунок 29 – Список уязвимостей с уровнем опасности

**Вывод:** В ходе выполнения лабораторной работы были обнаружены некоторые трудности при установке OpenVAS, для решения которых потребовалось вручную удалить неактуальные пакеты для PostgreSQL и установить последнюю их версию. Также обновление баз данных сканера уязвимостей потребовало ручного вмешательства. После настройки OpenVAS было выполнено 3 различных сканирования посредством создания соответствующих задач. В ходе сканирования всеми тремя способами была обнаружена единственная имеющая значение уязвимость DCE/RPC and MSRPC Services Enumeration Reporting, которая может позволить злоумышленнику получить некоторую информацию о системе жертвы посредством открытого порта 135. Результаты сканирования можно интерпретировать как относительно положительные, поскольку была найдена только одна уязвимость.