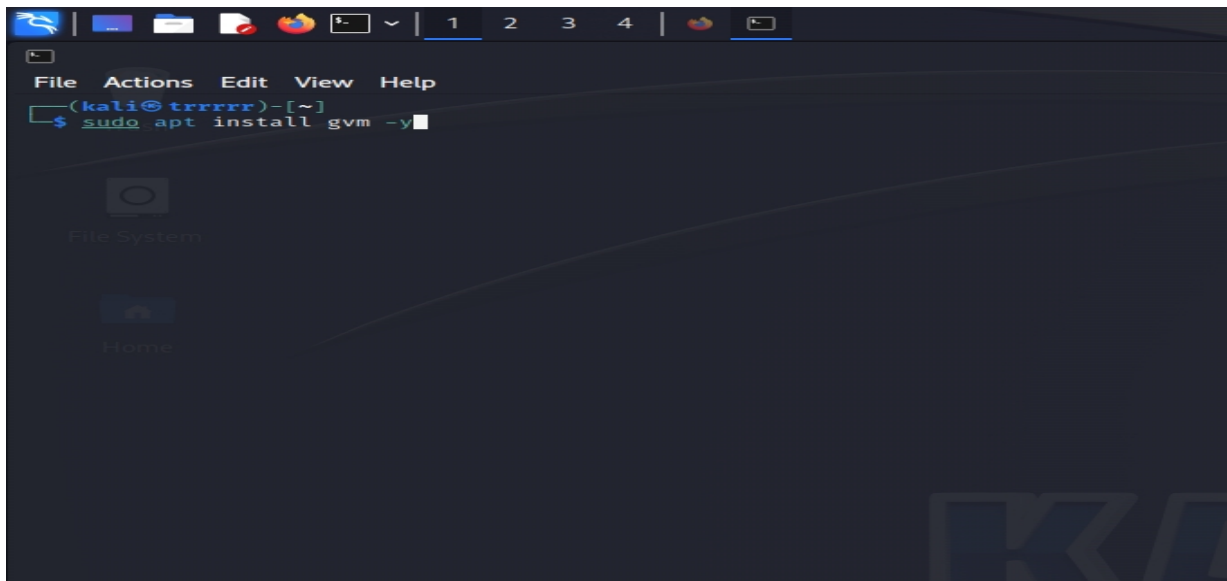


Work with OpenVas (Greenbone Security Assistant)

Step 1: Установить OpenVas.



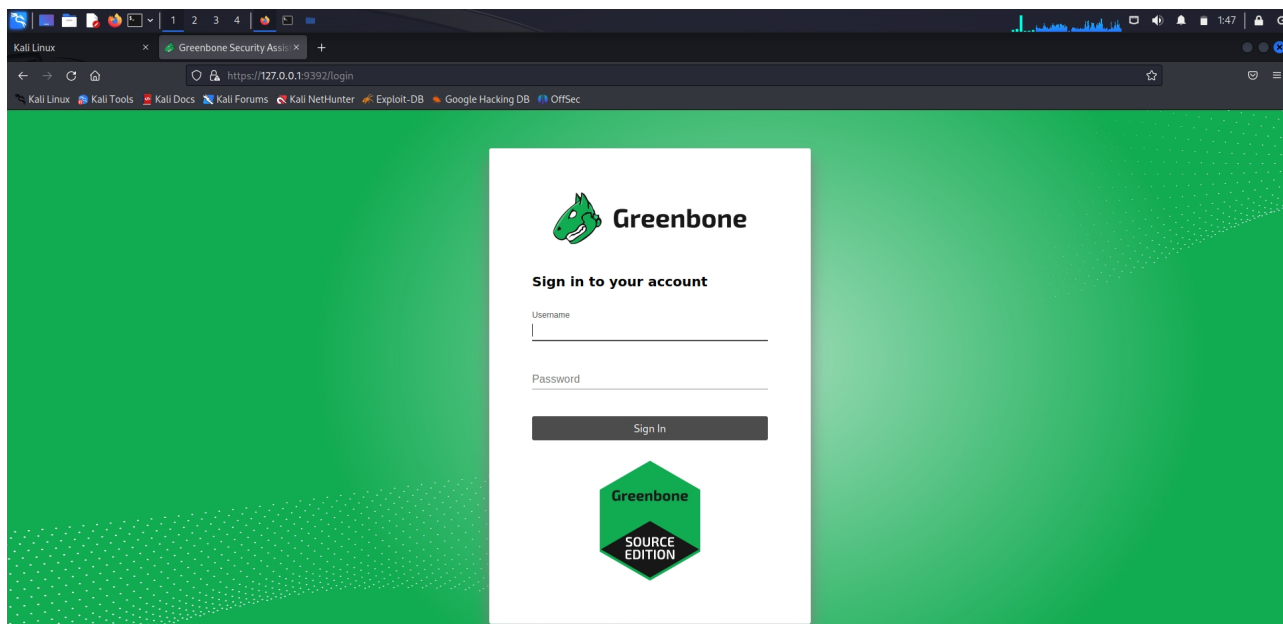
Перед этим я использовал `sudo apt update/sudo apt upgrade -y` (на всякий случай ещё `sudo apt dist-upgrade -y`). Использовал `sudo apt install gvm -y`.

Step 2: Настроить OpenVas.

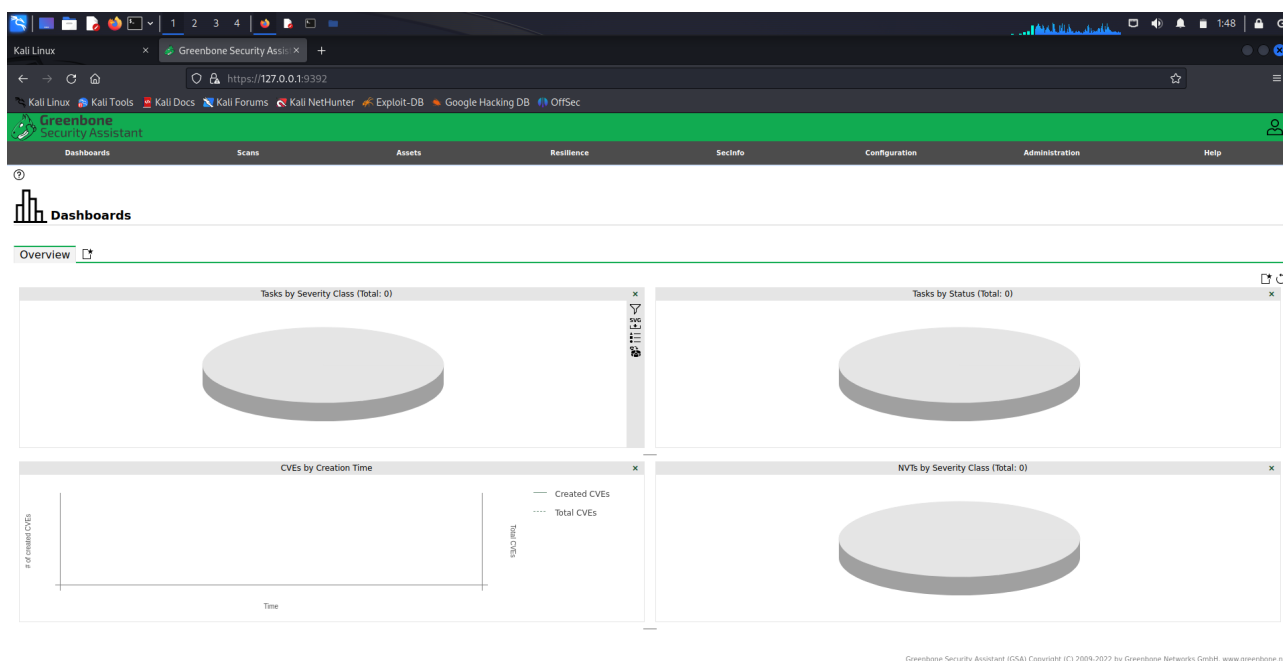


Для начала после установки набрать `sudo gvm-setup`, чтобы скрипт всё сделал (занимает это некоторое время — примерно чуть больше 80000 файлов, в целом для системы это мало). После данной команды — в конце появится имя пользователя (обычно это `admin`) и случайно сгенерированный пароль, похожий на IPV6. Затем набираю `sudo gvm-check-setup`, чтобы проверить — что конфигурация прошла успешно.

Если конфигурация нормальная, то набираем в браузере <https://localhost:9392>

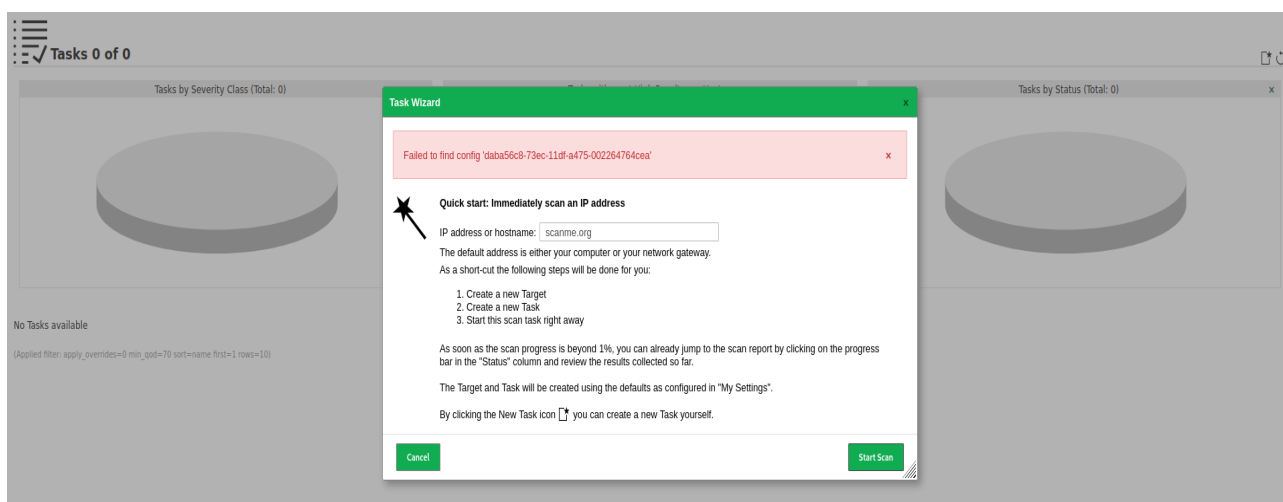


Должно появиться данное окно в браузере — набираем имя пользователя и пароль, сгенерированные после установки (можно и добавить другого пользователя с помощью команды, для него будет сгенерирован другой пароль).

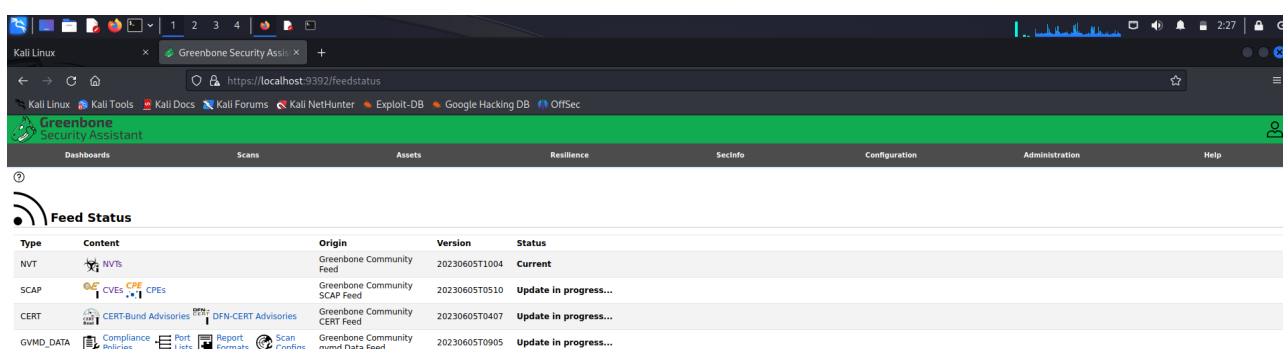


Меню выглядит примерно так.

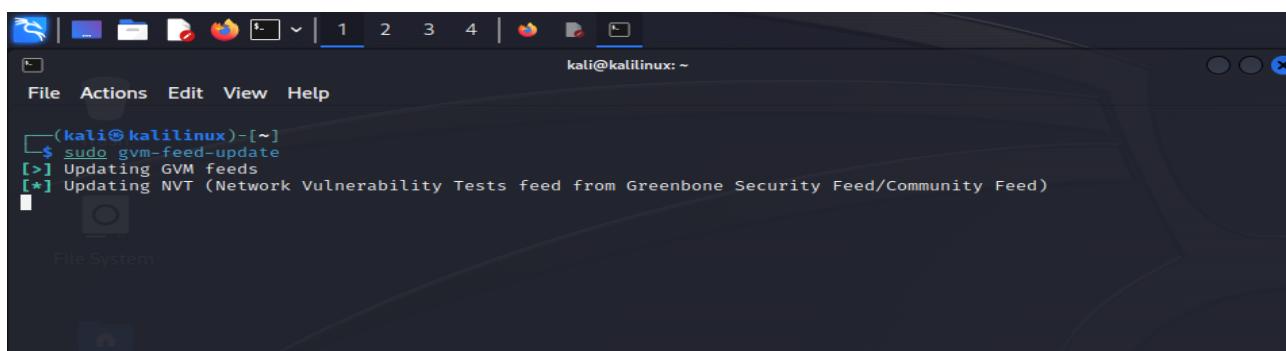
P.S. (без -у, я ввозился с файлами — были ошибки, при `sudo gvm-check-setup` застрял на шаге 1 — из-за сокетов, ошибка что не подключён сервер, потом `io timeout` ошибка при запуске скрипта `sudo runuser -u __gvm -- greenbone-nvt-sync`; это используя инструкцию из статьи под заданием — установка gvm не полностью завершена).



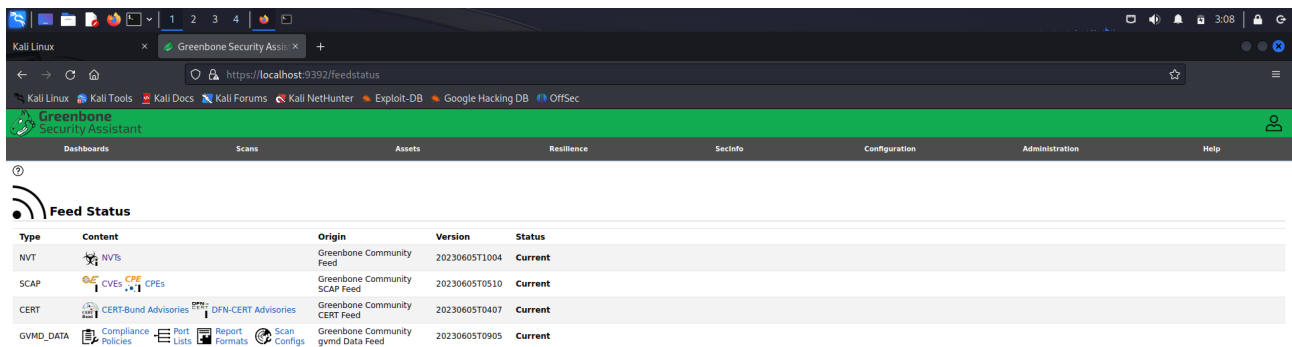
Прежде чем начать сканирование, нужно убедиться — чтобы не было такой ошибки.



А проблема такой ошибки из-за этого; для кого-то такой экран мог не меняться часами.



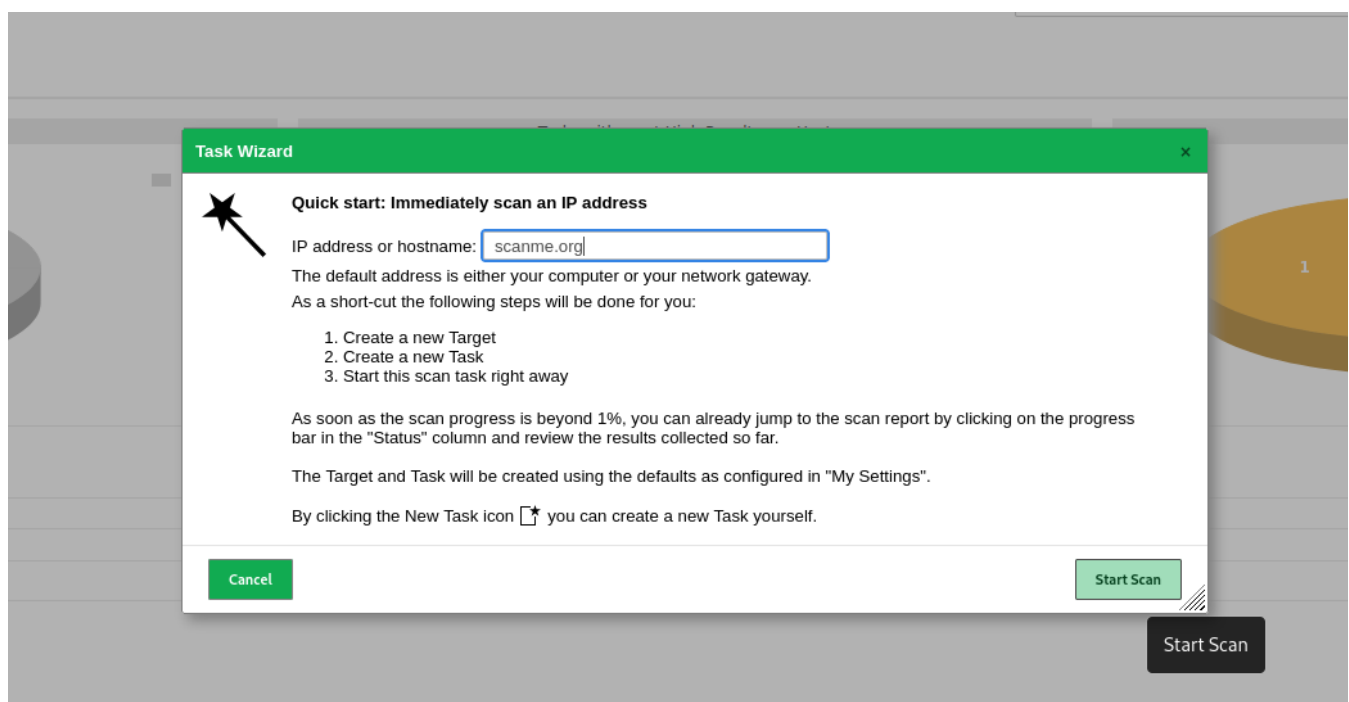
Я её решил используя данную команду. Но для кого-то нужно будет обновить те базы данных вручную, для кого-то перезапустить службы данного сервиса. После этого нужно будет подождать примерно от 15 до 60 минут (у каждого по-разному).



Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20230605T1004	Current
SCAP	CVEs CPE CPEs	Greenbone Community SCAP Feed	20230605T0510	Current
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone Community CERT Feed	20230605T0407	Current
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Community gvmd Data Feed	20230605T0905	Current

Спустя примерно 20 минут, статусы изменились.

Step 3: Просканировать ресурс scanme.org с помощью OpenVas.

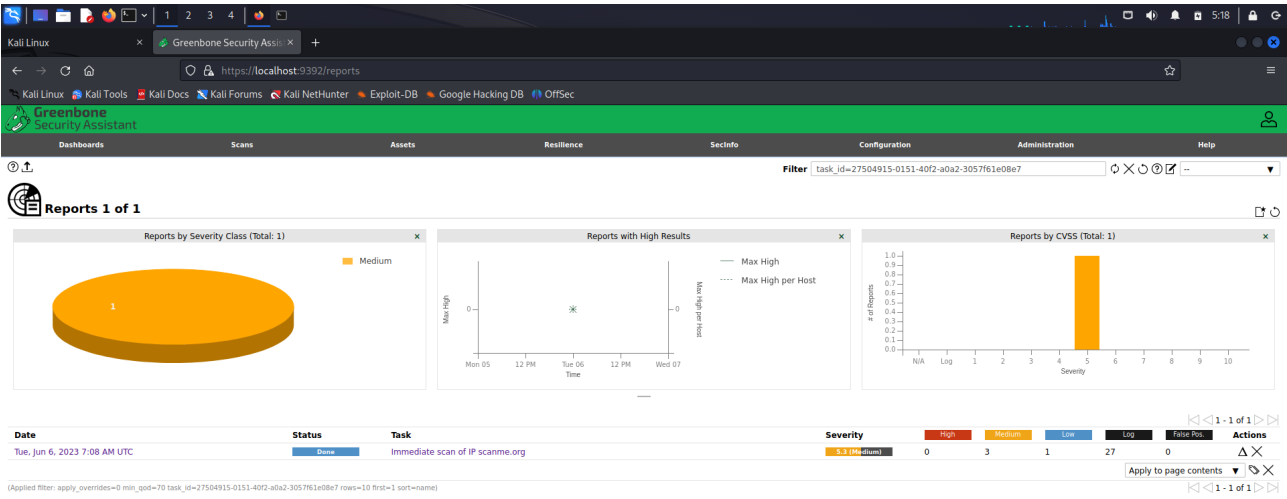


Нажать на «задачи» → «Колдун задач» → в «IP адрес или имя хозяина» просто набрать IP или имя домена и нажать «Начать сканирование»*. После этого ждать результата или же отчёта.

*Перед этим надо заранее исправить ошибку с отсутствием баз данных

Step 4: Получить отчёт по сканированию.

Спустя чуть больше 2 часов сканирования (это видимо было полным сканированием) вот такой отчёт у меня получился.**



Information User Tags Permissions

Name: Immediate scan of IP scanme.org

Comment:

Alterable: No

Status: Done

Target

Target for immediate scan of IP scanme.org - 2023-06-06 07:08:55

Scanner

Name: OpenVAS Default

Type: OpenVAS Scanner

Scan Config: Full and fast

Order for target hosts:

Maximum concurrently executed NVTs per host: 4

Maximum concurrently scanned hosts: 20

Assets

Add to Assets: Yes

Apply Overrides: Yes

Min QoD: 70 %

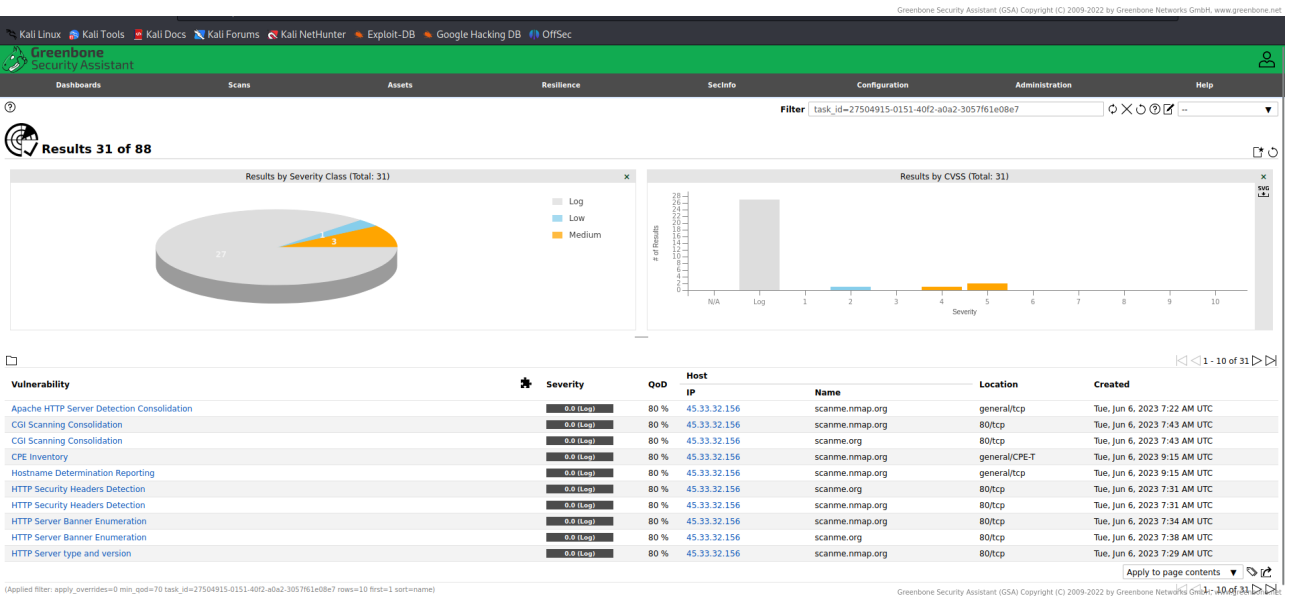
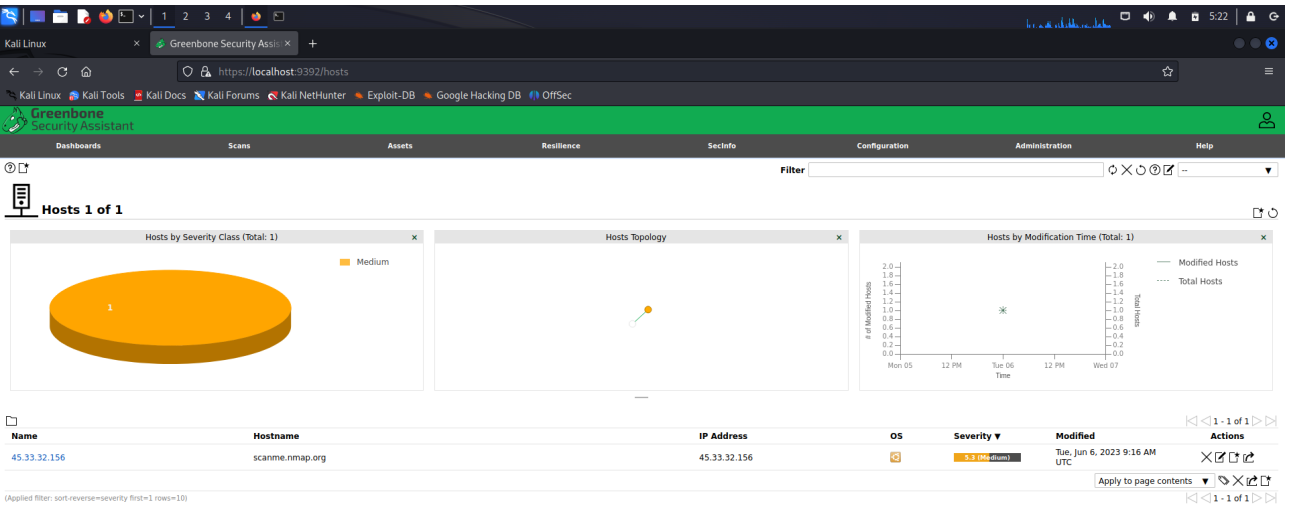
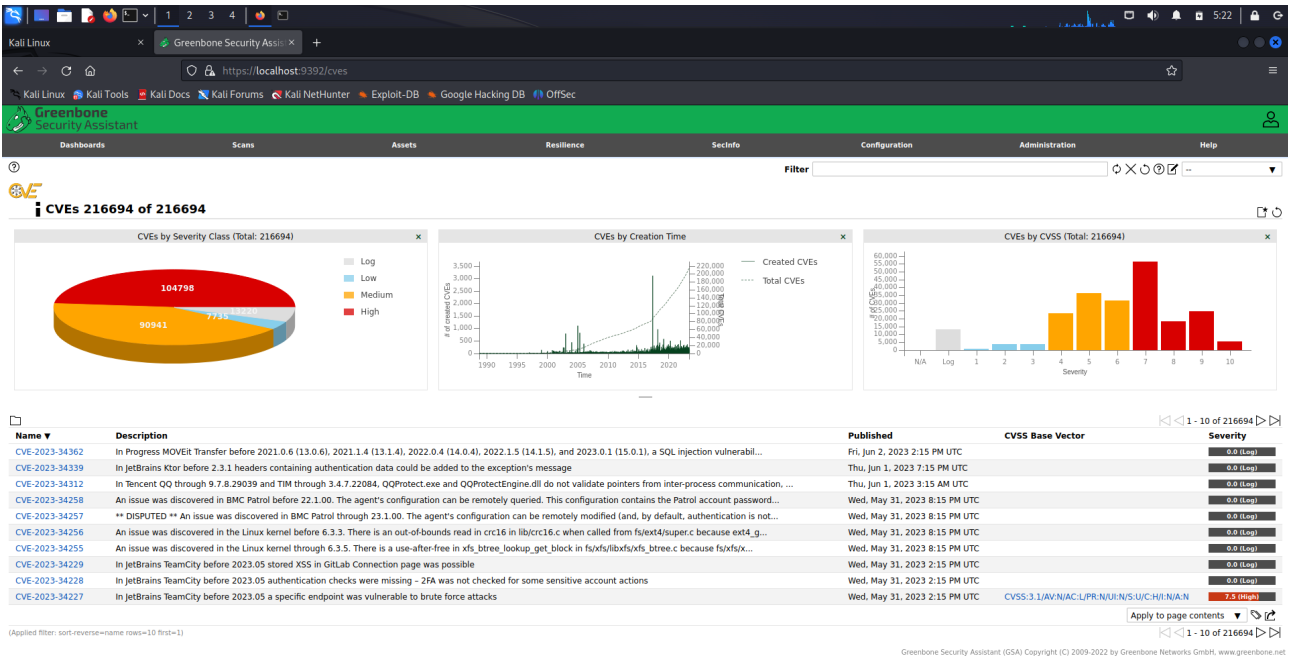
Scan

Duration of last Scan: 2 hours

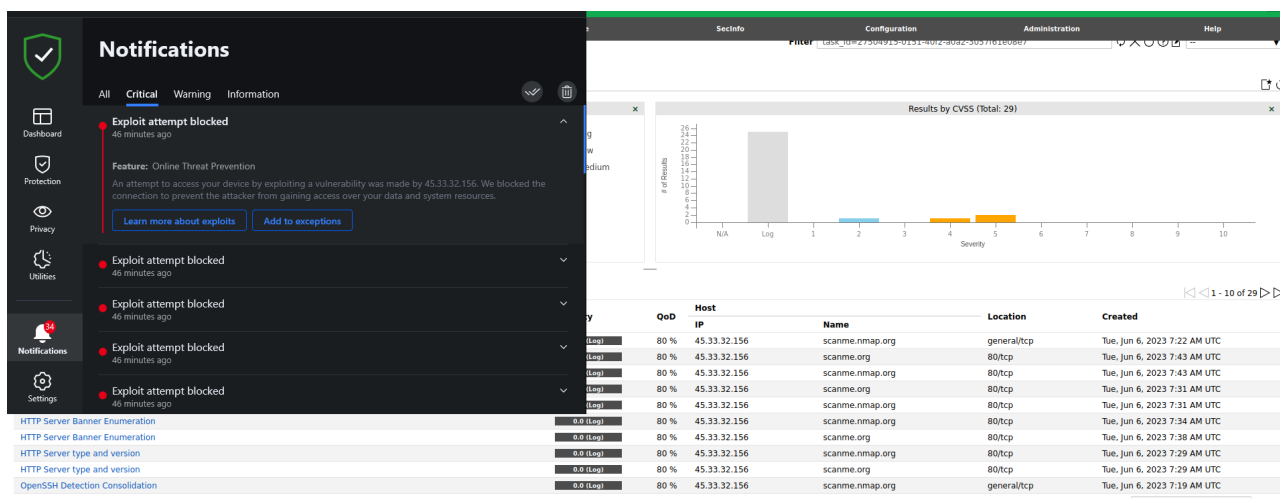
Average Scan duration: 2 hours

Auto delete Reports: Do not automatically delete reports

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net



**** Во время сканирования, антивирус блокировал запросы от данного домена (scanme.org) и его IP (примерно 160 запросов от домена и его IP были заблокированы как эксплоит или угроза). Может быть это стало причиной такого долгого сканирования.**



P.S. Я знаю что malware в виртуальных машинах обычно не касается настоящей машины, и вряд-ли перекинется на настоящую машину (такая возможность крайне мала, но есть) но всё же антивирус его блокировал.