Лабораторная работа № 4

Тема: Сканер уязвимостей OpenVas

Уязвимость - это слабое место или недостаток в системе, программном обеспечении, сети или процессе, которое может быть использовано злоумышленниками для несанкционированного доступа, атаки, нарушения конфиденциальности, целостности или доступности данных, или какого-либо другого негативного воздействия на систему или среду.

Виды уязвимостей:

Уязвимость веб-приложений: К таким уязвимостям относятся SQL-инъекции, межсайтовые сценарии (XSS), уязвимости кросс-сайтового запроса (CSRF), уязвимости аутентификации и авторизации, уязвимости в обработке файлов и другие. Уязвимости веб-приложений могут позволить злоумышленникам выполнить вредоносный код на сервере или украсть конфиденциальные данные пользователей.

Уязвимость операционных систем: Операционные системы, такие как Windows, macOS и Linux, также могут иметь уязвимости, которые могут быть использованы для несанкционированного доступа к системе или повышения привилегий. Это может быть вызвано незапланированными ошибками в программном обеспечении, неправильной конфигурацией, уязвимостями ядра и другими факторами.

Уязвимость сетевой инфраструктуры: Здесь включаются уязвимости протоколов сетевого уровня, таких как IP, TCP, UDP, а также уязвимости маршрутизаторов, коммутаторов и брандмауэров. Эти уязвимости могут привести к перехвату трафика, отказу в обслуживании или несанкционированному доступу к сети.

Уязвимость приложений и сервисов: Многие приложения и сервисы имеют свои собственные уязвимости, которые могут быть эксплуатированы. Это может включать уязвимости в почтовых серверах, базах данных, протоколах обмена сообщениями и других программных решениях.

Физические уязвимости: К ним относятся уязвимости, связанные с физическим доступом к системе или активам. Например, это может быть уязвимость в системе контроля доступа, некорректно организованное хранение данных, слабые замки или отсутствие видеонаблюдения.

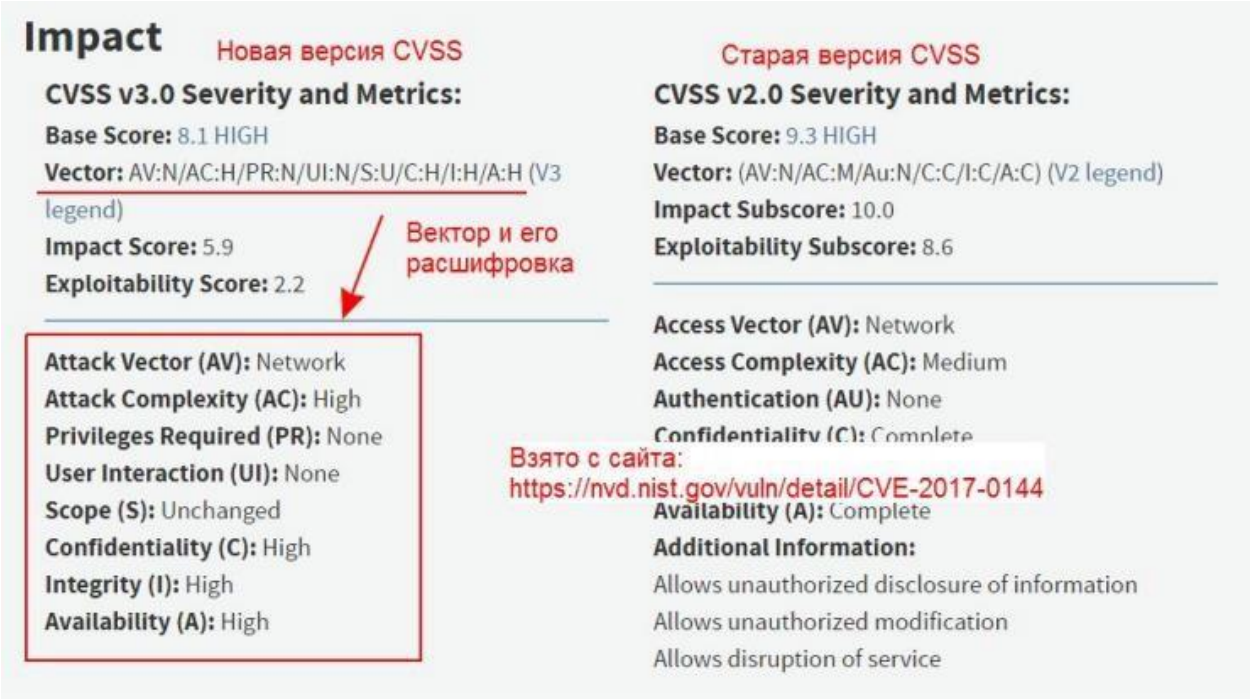
Социальная инженерия: Это уязвимость, связанная с манипуляцией и обманом людей для получения несанкционированного доступа или конфиденциальной информации. Например, фишинг, подделка личности, обман и другие тактики могут быть использованы для обхода технических мер безопасности.

Причины уязвимостей:

Ошибки при написании программ — например, buffer overflow.
Слабые настройки — пароль «admin»
Ошибки логики работы приложения, компонента или иной сущности — Sql injection.
Архитектурная особенность — Meltdown и Spectre.
Прочие факторы, позволяющие провести атаку с использованием особенности системы.

Как оценивается уязвимость

Количественно — каждой уязвимости присваивается числовой показатель. Чем он выше — тем опаснее уязвимость. Пример: индекс CVSS, показывает impact-уязвимости и представляет собой набор показателей («вектор»).
Качественно — экспертная (примерная) оценка, насколько вероятна эксплуатация уязвимости. Пример — «низкая», «средняя», «высокая» опасность.



Информация об уязвимостях

https://cve.mitre.org — сайт-аггрегатор информации об уязвимостях. У каждой уязвимости есть индекс CVE. https://nvd.nist.gov — БД уязвимостей США. https://bdu.fstec.ru/vul — база данных уязвимостей ФСТЭК. https://www.exploit-db.com — база данных эксплоитов для уязвимостей.

Уязвимости нулевого дня

0 day — уязвимость, для которой не опубликован патч, но она уже встречается «в природе» (inthe-wild). У разработчиков не было времени на устранение уязвимости.
Как правило, их находят и эксплуатируют раньше, чем выпущено обновление, закрывающее уязвимость.
Пример 0-day уязвимости: CVE-2017-11882 в MS Office - оставалась неисправленной 17 лет.

Как работает сканер уязвимостей

У каждой уязвимости есть признаки, которые можно обнаружить при сканировании.
Признаки уязвимости оформляются в виде объектов, которые используются при сканировании.
Примерный аналог — сигнатура вируса.
Открытый язык описания и оценки уязвимостей Open Vulnerability and Assessment Language (OVAL).

Отличие сканеров

Платный или бесплатный?
Состав функций.
Полноценный сканер уязвимостей или просто плагин?
Работает ли поиск по CVE?
Работает ли с OVAL сущностями?
Может ли искать уязвимости не только в ОС?

Сканеры уязвимостей могут работать по одному из двух алгоритмов: WhiteBox и BlackBox. В первом случае мониторинг потенциальных угроз происходит изнутри сети, что дает больше возможностей для проверки всех составляющих ИБ-системы. Во-втором случае сканер находится вне периметра сети, то есть его работа максимально приближена к действиям реального киберзлоумышленника, которому нужно проникнуть в систему.

Некоторые из бесплатных сканеров уязвимостей:

Qualys Community Edition: Qualys предлагает бесплатную Community Edition своего коммерческого продукта. Он позволяет сканировать уязвимости в сети и веб-приложениях, а также предоставляет некоторые дополнительные функции, такие как сканирование SSL-сертификатов.

OWASP ZAP: ZAP (Zed Attack Proxy) - это инструмент сканирования уязвимостей для вебприложений, разработанный OWASP (Open Web Application Security Project). Он предоставляет возможности сканирования на основе шаблонов, анализа безопасности, перехвата и изменения трафика и других функций.

OpenVAS: OpenVAS (Open Vulnerability Assessment System) — это мощный и широко известный сканер уязвимостей, который входит в состав Kali Linux. Он обладает обширными возможностями для обнаружения и анализа уязвимостей в сети.

Nikto: Nikto также доступен в Kali Linux. Это популярный сканер веб-серверов, который ищет известные уязвимости и проблемы веб-приложений. Он может быть полезен для обнаружения уязвимостей, связанных с конфигурацией веб-серверов и популярными CMS.

Nessus: Kali Linux предлагает доступ к Nessus, одному из наиболее популярных коммерческих сканеров уязвимостей. Nessus имеет обширную базу данных уязвимостей и предоставляет широкий набор функций для обнаружения и анализа уязвимостей.

Burp Suite: Burp Suite — это комплекс инструментов для тестирования безопасности вебприложений. Он включает в себя сканер уязвимостей, прокси-сервер для перехвата и изменения трафика, а также другие инструменты для анализа безопасности.

Arachni: Arachni — это сканер уязвимостей веб-приложений с открытым исходным кодом. Он предоставляет возможность обнаружения и анализа уязвимостей, связанных с вебприложениями, включая XSS, CSRF, SQL-инъекции и другие.

WPScan: WPScan представляет собой специализированный сканер уязвимостей для популярной платформы управления контентом WordPress. Он может обнаруживать уязвимости, связанные с конфигурацией WordPress, плагинами и темами.

Nmap: является мощным инструментом для сканирования сети, который также может использоваться для обнаружения и оценки уязвимостей хоста.

Пример использования Openvas в Kali Linux:

Состав тестового стенда: Kali Linux 2018, Metasploitable 3 (Ubuntu 14)

В Kali Linux Openvas установлен по умолчанию. Проверка корректности установки:

```
root@kali:~# openvas-check-setup
openvas-check-setup 2.3.7
  Test completeness and readiness of OpenVAS-9
  (add '--v6' or '--v7' or '--v8'
   if you want to check for another OpenVAS version)

  Please report us any non-detected problems and
  help us to improve this check routine:
  http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss

  Send us the log-file (/tmp/openvas-check-setup.log) to help analyze the proble
m.

  Use the parameter --server to skip checks for client tools
  like GSD and OpenVAS-CLI.

Step 1: Checking OpenVAS Scanner ...
        OK: OpenVAS Scanner is present in version 5.1.3.
        OK: redis-server is present in version v=4.0.11.
        OK: scanner (kb_location setting) is configured properly using the redis
-server socket: /var/run/redis-openvas/redis-server.sock
        OK: redis-server is running and listening on socket: /var/run/redis-open
vas/redis-server.sock.
        OK: redis-server configuration is OK and redis-server is running.
```

Если нет критических ошибок, можно двигаться дальше.

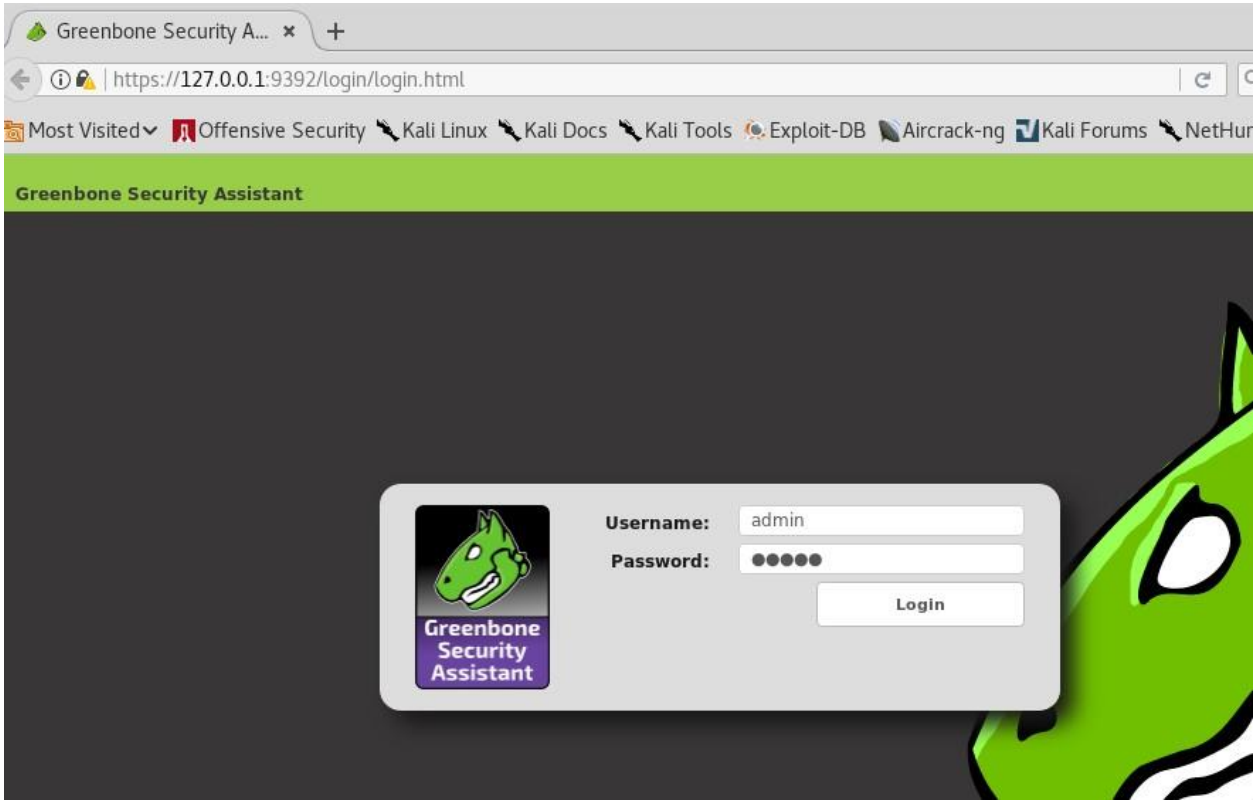
По умолчанию в openvas нет пользователей. Создание нового пользователя admin с паролем admin:

```
root@kali:~# openvasmd --create-user=admin
User created with password 'f47a319b-05e9-46cd-83a3-84a7a07e45e9'.
root@kali:~# openvasmd --user=admin --new-password=admin
root@kali:~# openvasmd --get-users
adminvas
QWerty
student
stud7
admin
root@kali:~#
```

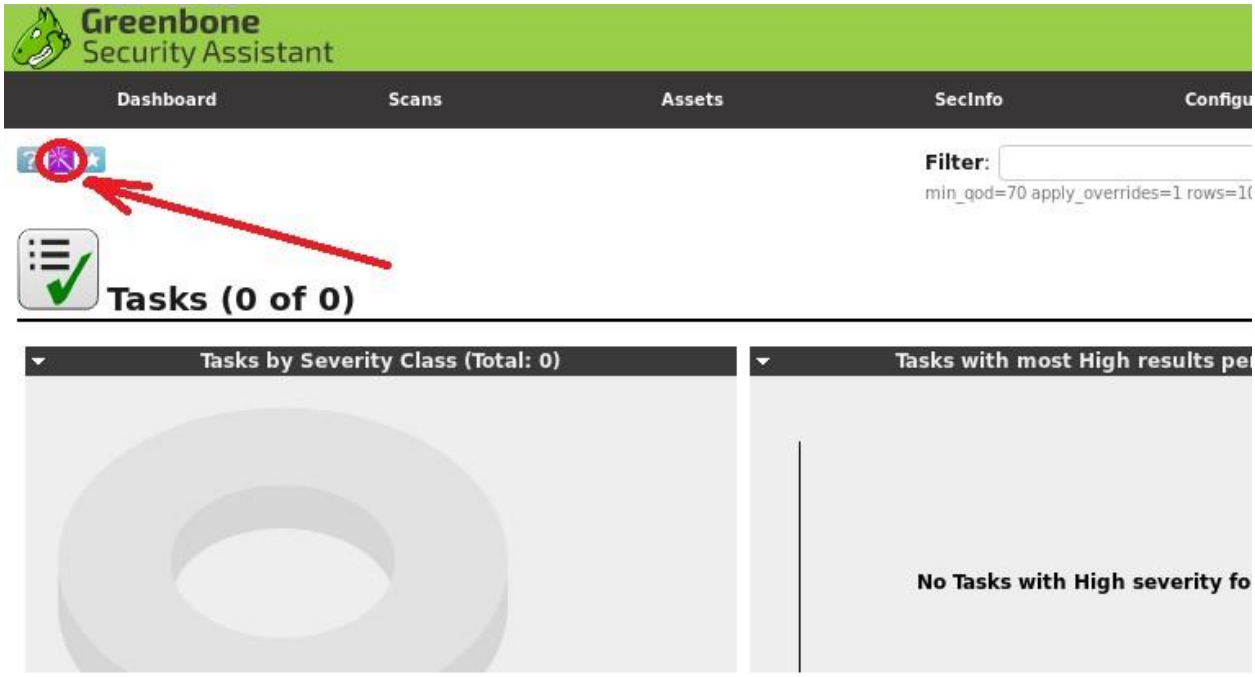
Запуск openvas:

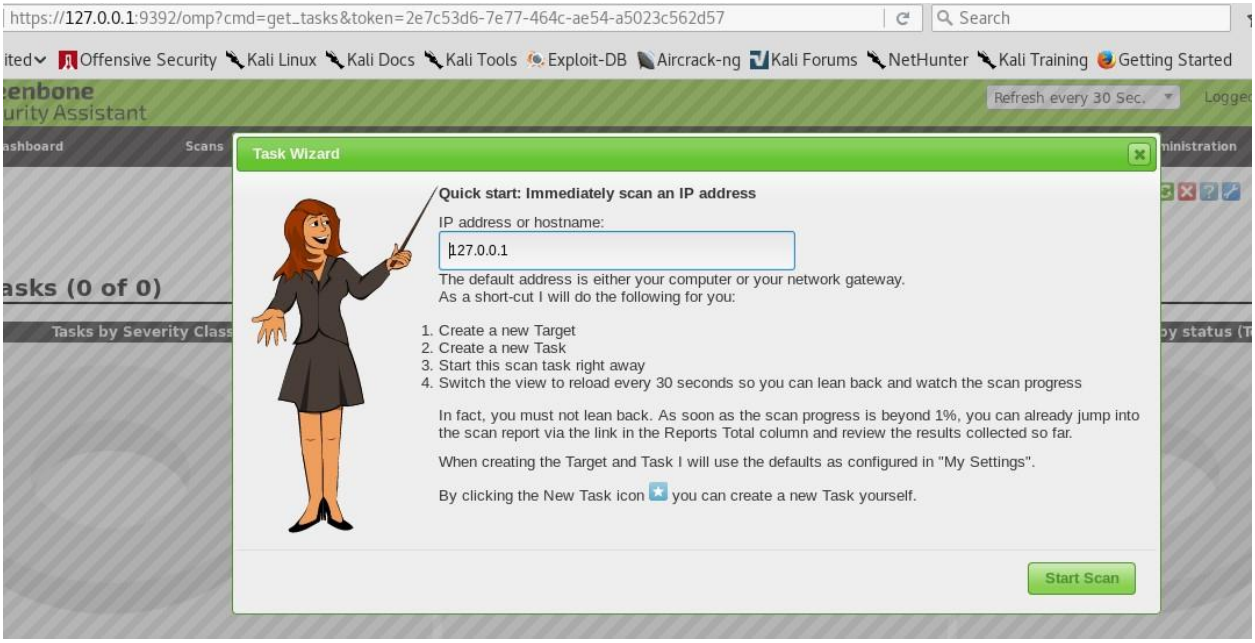
```
root@kali:~# openvas-start
[i] Something is already using port: 9392/tcp
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
gsad    1795 root    5u  IPv4  26586      0t0  TCP localhost:9392 (LISTEN)

UID        PID  PPID  C STIME TTY      STAT   TIME CMD
root      1795     1  0 21:57 ?        SLsl   0:02 /usr/sbin/gsad --foreground -

[*] Please wait for the OpenVAS services to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
```

В окне браузера открывается веб-интерфейс программы, вводим свои учетные данные:

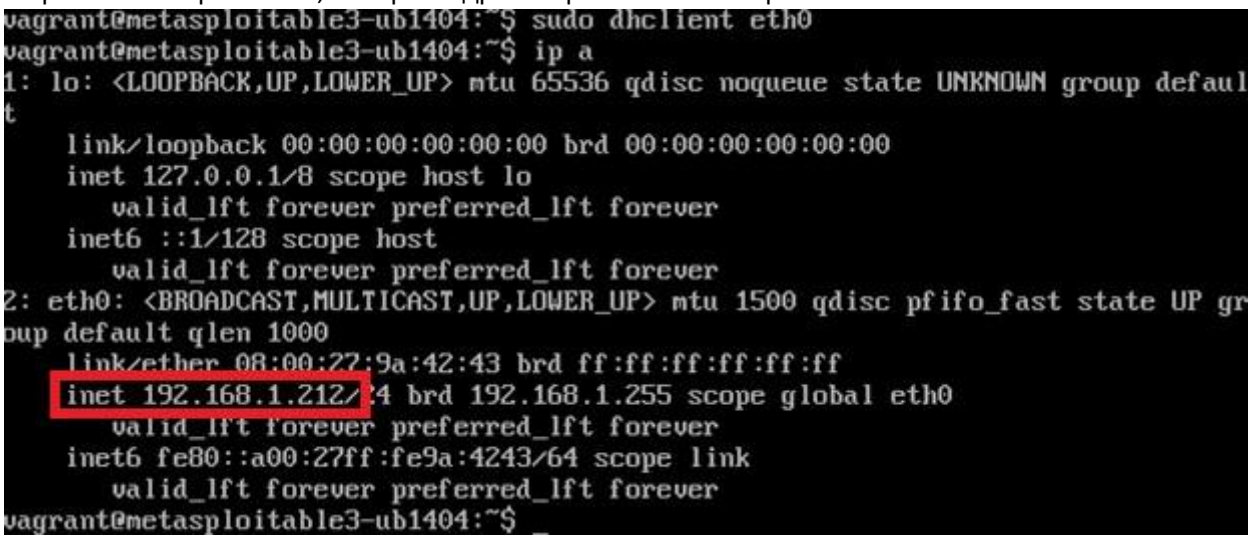


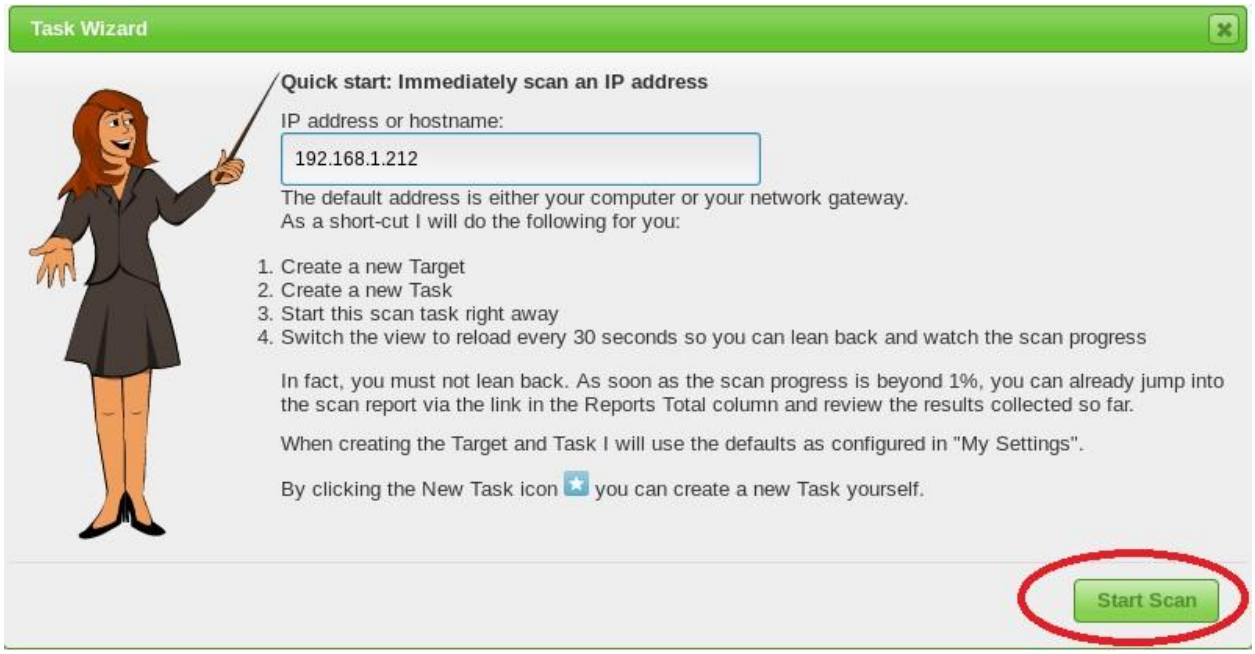
Создание новой задачи. scans – tasks – Task Wizard

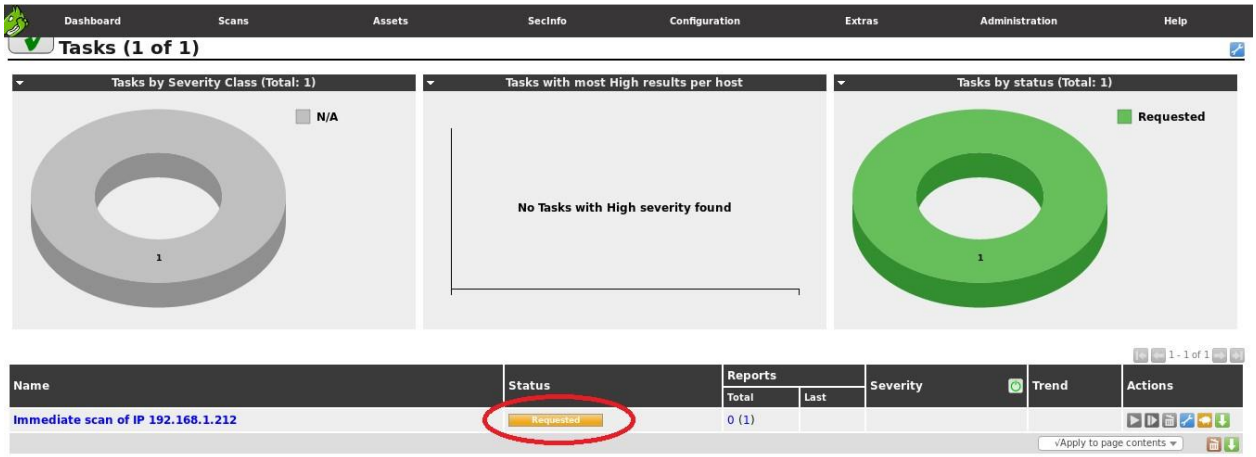




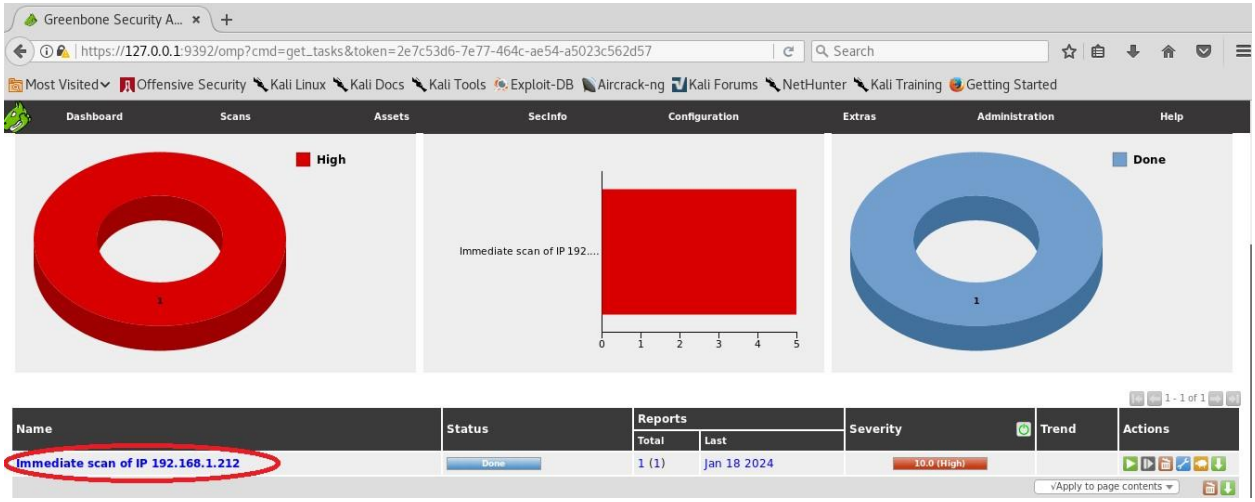
Жертва – metasploitable3, смотрим адрес и прописываем в openvas:

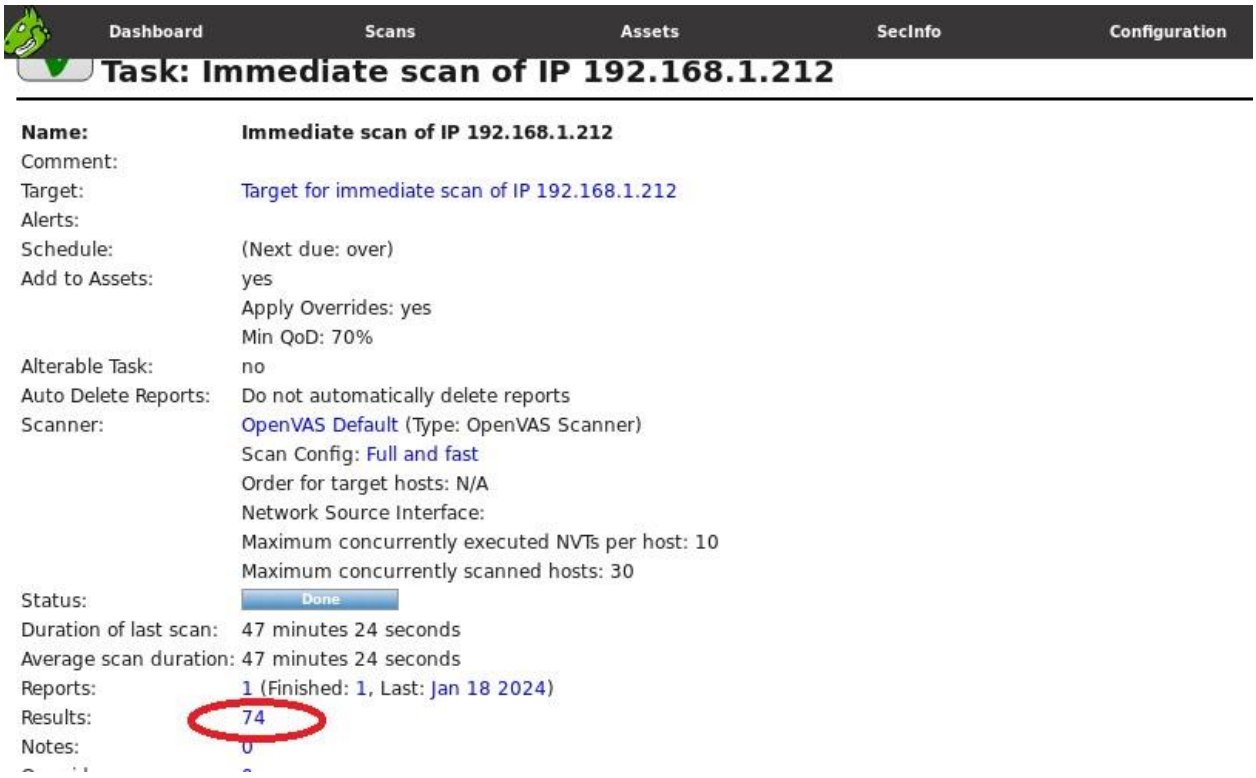




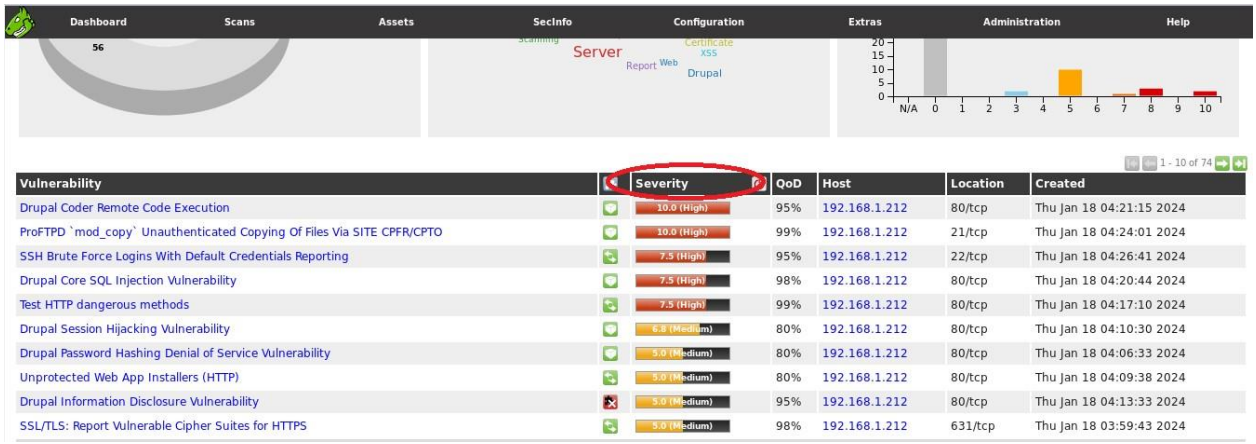


Результаты сканирования:



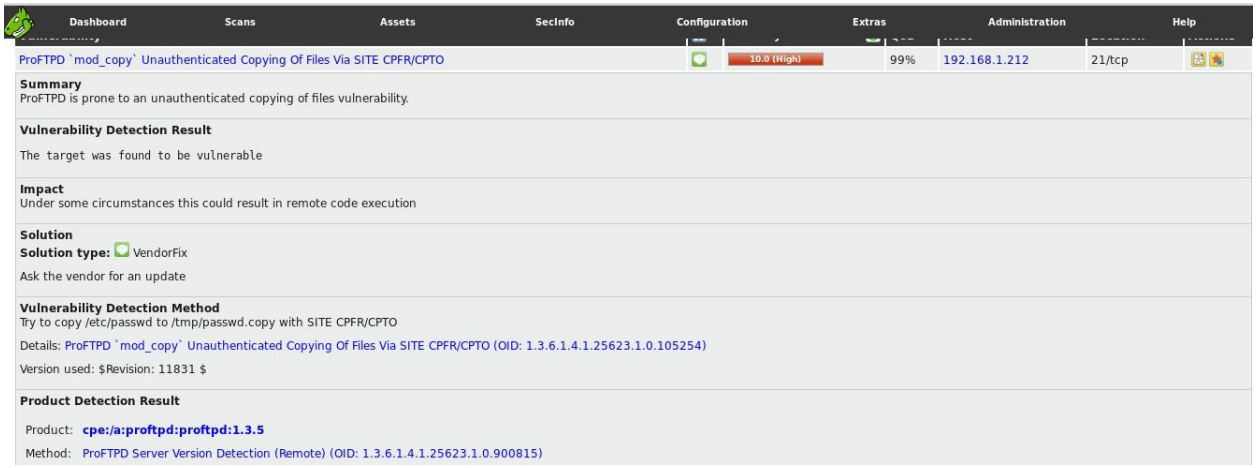


Отсортируем уязвимости по критичности:



Видим 5 критичных и 11 средних уязвимостей.

Если кликнуть на уязвимость, можно узнать подробности об уязвимости и способ устранения:



Задание:

1. Собрать испытательный стенд в VirtualBox из виртуальных машин Kali Linux и Windows (metasploitable 3).
2. Просканировать на наличие уязвимостей машину на базе Windows.
3. Сделать выводы.