МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное
образовательное
учреждение высшего образования
«Московский авиационный институт
(национальный исследовательский университет)» (МАИ)

Кафедра «Моделирование систем и информационные технологии»

«НАСТРОЙКА И ИСПОЛЬЗОВАНИЕ СКАНЕРА УЯЗВИМОСТЕЙ OPENVAS»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ПРАКТИЧЕСКОЙ РАБОТЕ

ПО КУРСУ: «МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

Составитель: В. С. Соломыков

Москва 2018

Цели работы

1. Изучение оценки уязвимостей на основе CVSS (Common Vulnerabilities Scoring System) – общей системы оценки уязвимостей.
2. Получение практических навыков по работе с OpenVAS.
3. Получение практических навыков по работе с описанием уязвимостей

Описание работы

Уязвимость – Слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами. (ГОСТ Р ИСО/МЭК 27002-2012).

Управление уязвимостями - процесс, в котором определяются уязвимости в программном обеспечении, и оценивается риск этих уязвимостей.

Процесс управления уязвимостями представляет собой бесконечный цикл от обнаружения уязвимости до её исправления и последующего мониторинга состояния информационной системы.

Общая система оценки уязвимостей (**Common Vulnerability Scoring System – CVSS**) – это система, которая позволяет осуществлять сравнение уязвимостей программного обеспечения с точки зрения их опасности.

В настоящее время наибольшее распространение в практической деятельности по оценке опасности уязвимостей получила **версия 2.0** общей системы оценки уязвимостей.

Система оценки CVSS v2.0 состоит из **трех групп** метрик (критериев): базовых, временных и контекстных.

Группа базовых метрик (критериев) отражает аспекты опасности уязвимости, влияющие на доступность, целостность и конфиденциальность информации.

Группа временных метрик (критериев) отражает характеристики уязвимости, которые изменяются со временем (подтверждение технических параметров уязвимости, статус исправления уязвимости и доступность технологии эксплуатации), но не зависят от среды функционирования программного обеспечения.

Группа контекстных метрик (критериев) отражает характеристики уязвимости, зависящие от среды функционирования программного обеспечения.

Для осуществления комбинированной оценки уязвимостей по различным группам метрик (критериев) используются **базовый, временной** и **контекстный** векторы уязвимости.

Количественная оценка степени опасности уязвимости проводится по результатам анализа базового вектора уязвимости. Временные и контекстные векторы применяются только в тех случаях, когда возникает необходимость уточнения базового вектора.

Базовый вектор уязвимости CVSS v2.0 представляет собой комбинированную информацию о базовых метриках (критериях), представляемую в виде текстовой формализованной записи (строки) и численного значения (оценки) [1].

CVSS хорошо подходит в качестве стандартной системы измерения для предприятий, организаций и правительств, которые требуют точной и последовательной оценки влияния уязвимостей. CVSS представляет собой универсальный открытый и стандартизированный метод рейтинга IT-уязвимостей [2].

Численное значение базового вектора уязвимости (базовая оценка) изменяется **от 0 до 10**.

На основе численного значения базового вектора V уязвимости (базовой оценки) присваиваются один из **четырех уровней опасности**:

- низкий уровень опасности, если $0,0 \leq V \leq 3,9$;
- средний уровень опасности, если $4,0 \leq V \leq 6,9$;
- высокий уровень опасности, если $7,0 \leq V \leq 9,9$;
- критический уровень опасности, если $V = 10,0$

Более подробная информация о CVSS может быть получена в [2].

Сканер уязвимостей — программное или аппаратное средство, служащее для осуществления диагностики и мониторинга сетевых компьютеров, позволяющее сканировать сети, компьютеры и приложения на предмет обнаружения возможных проблем в системе безопасности, оценивать и устранять уязвимости.

Сканеры уязвимостей выделяется среди остальных средств защиты следующими особенностями:

1. Они могут использоваться как средство обеспечения безопасности, так и как средство нападения на информационную систему. Данные об обнаруженных уязвимостях могут быть использованы администратором безопасности для повышения уровня защищённости узлов сети, а также злоумышленником, который может эксплуатировать найденную уязвимость для взлома системы с помощью эксплойта.
2. Неочевидная польза от применения сканеров безопасности. Например, польза от использования межсетевого экрана ясна – он не пропускает сетевые пакеты согласно настроенным правилам. Или система обнаружения сетевых атак. Ее роль тоже очевидна – непрерывный мониторинг трафика и обнаружение в нем признаков атак по определённым сигнатурам. В свою очередь, результат работы сканера уязвимостей – это получение перечня уязвимостей, которые можно использовать для проведения атаки. Однако, речь идет лишь о потенциальной возможности использования уязвимости и совершения атаки, а не о свершившимся факте.
3. Сканеры уязвимостей могут оказывать негативное воздействие на объекты защиты. Некоторые сканер имеют сценарии проверки на атаки типа отказ в обслуживании, которые реализуют при проверке.

В целом, сканер – это средство защиты информации, которое реализует механизм выявления уязвимостей, что позволяет предотвратить использование этих уязвимостей.

OpenVAS.

Open Source Vulnerability Scanner (OpenVAS) – сканер уязвимостей, представляет собой систему из нескольких сервисов и инструментов, с возможностью проведения мощного сканирования системы на наличие уязвимостей. Сканер постоянно выполняет обновление списка уязвимостей через сетевые службы.

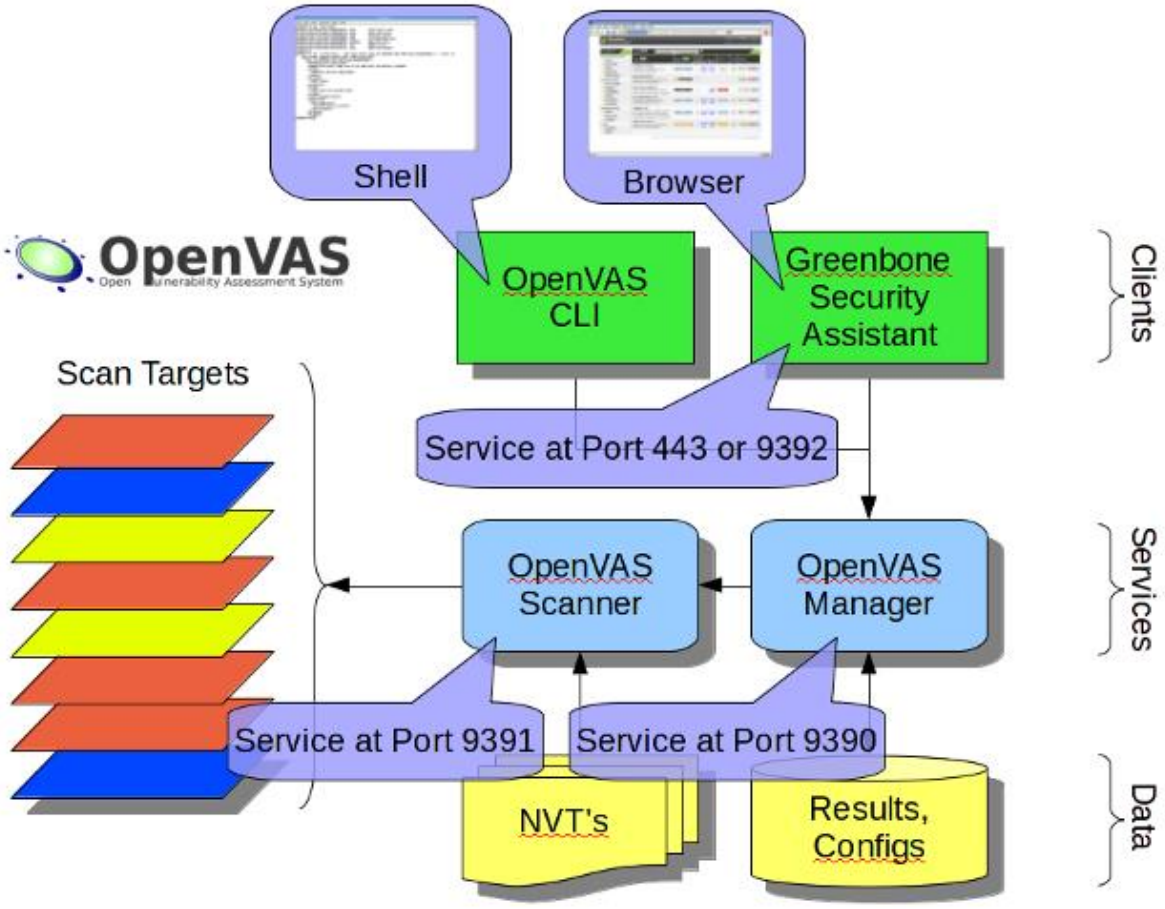

Рис. 1. Общая архитектура сканера OpenVAS.

Сканер уязвимостей состоит из следующих компонент (рис. 1) [4]:

OpenVAS Manager – центральная служба, которая объединяет обычный поиск уязвимостей и полноценное решение по управлению уязвимостями. Manager управляет сканером через OTP (OpenVAS Transfer Protocol) используя OpenVAS Management Protocol (OMP). Также OpenVAS Manager контролирует SQL базу данных (на основе sqlite), в которой хранятся все настройки и данные результатов сканирования.

Greenbone Security Assistant (GSA) – веб-интерфейс, представляющий пользовательский интерфейс для web-браузеров. GSA использует преобразование eXtensible Stylesheet Language (XSL) стилей, что преобразуют OMP ответы в HTML.

OpenVAS CLI – утилита командной строки «omp», которая позволяет создавать пакетные процессы выполнения OpenVAS Manager.

OpenVAS Scanner осуществлять контроль над сканированием с использованием протокола OTP. При этом данный протокол можно изменить.

Выполнение работы

1. Включите ПК. Запустите ПО VirtualBox, найдите в списке виртуальных машин образ с Kali Linux и запустите его. Для сохранения отчета сканирования, подключите USB-носитель к ПК. По умолчанию в Kali Linux логин – **root**, пароль – **toor**. Если возникают затруднения, обратитесь к преподавателю.
2. В случае, если OpenVAS не установлен в операционной системе, выполните шаги 3-5:

3. Проверьте актуальность операционной системы KaliLinux и репозитория с помощью команд:
   `apt-get update`
   `apt-get dist-upgrade`
4. Выполните команду установки пакета OpenVAS
   `apt-get install openvas`
5. Выполните команду настройки сканера OpenVAS
   `openvas-setup`
   в результате которой будет произведена настройка ПО, скачаны последние списки уязвимостей (процесс обновления длится достаточно долго), запущены необходимые служебные сервисы, при первом запуске данной команды также будет создан пользователь admin и сгенерирован пароль для данного пользователя.
6. Для запуска сервиса OpenVAS необходимо набрать команду
   `openvas-start`
   после которой OpenVAS будет готов для подключения через веб-интерфейс и запуска сканирования
7. Запустите браузер Firefox ESR и введите в адресную строку
   `https://127.0.0.1:9392`
8. В появившемся окне введите логин admin и пароль для данной учётной записи.
9. Перейдите в пункт меню `Scans -> Tasks`
10. Нажмите New Task на иконке в левом верхнем углу (Рис. 2)

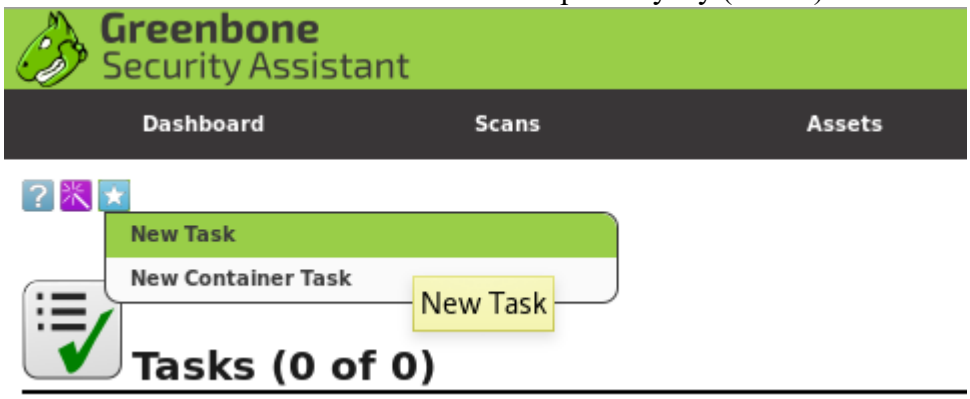

Рис. 2 Пиктограмма создания новой задачи

11. Задайте имя задачи (name), конфигурация сканирования (scan config) и цели сканирования (scan targets) (рис. 3). Остальные параметры оставьте по умолчанию

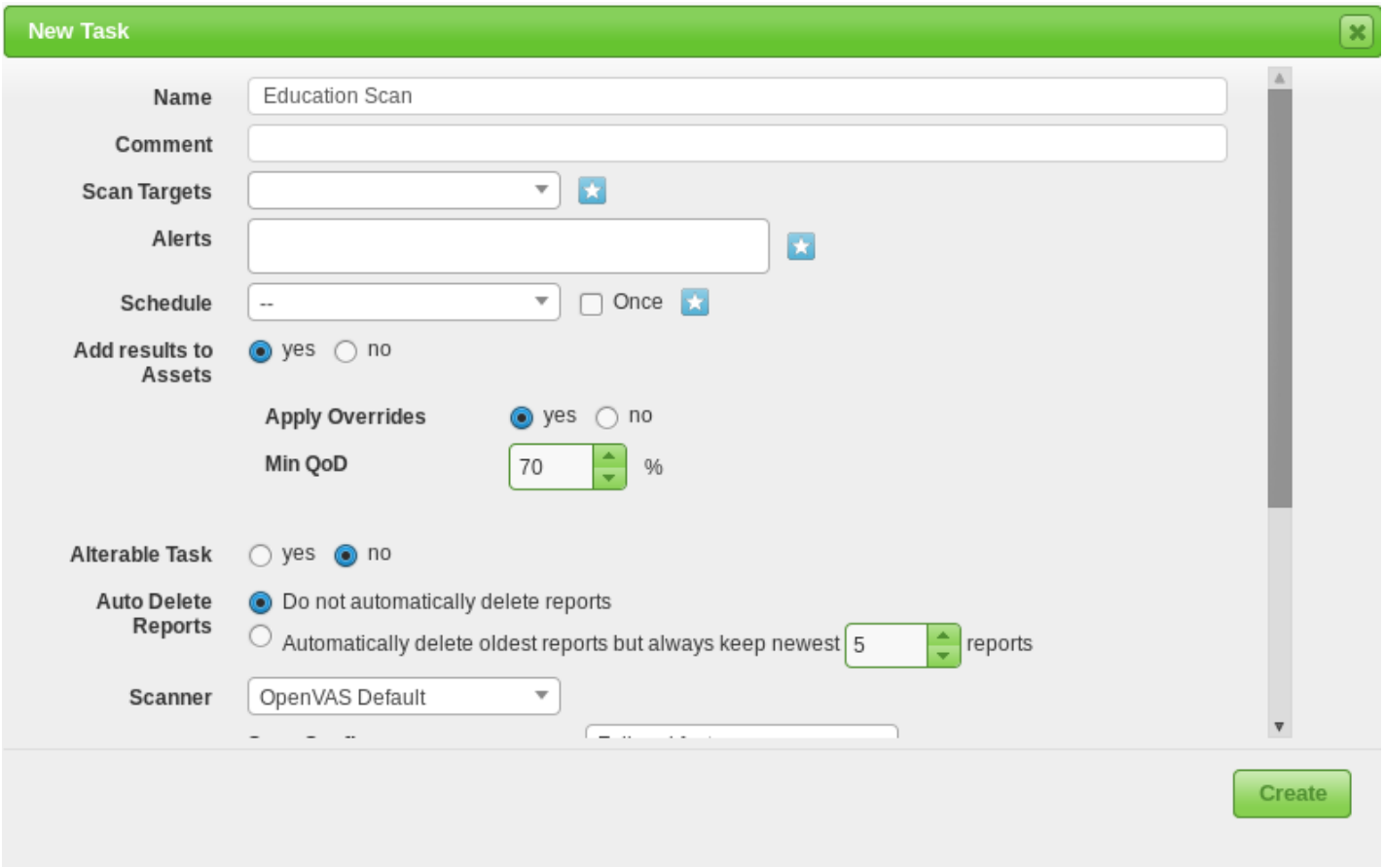

Рис. 3 Создание новой задачи сканирования

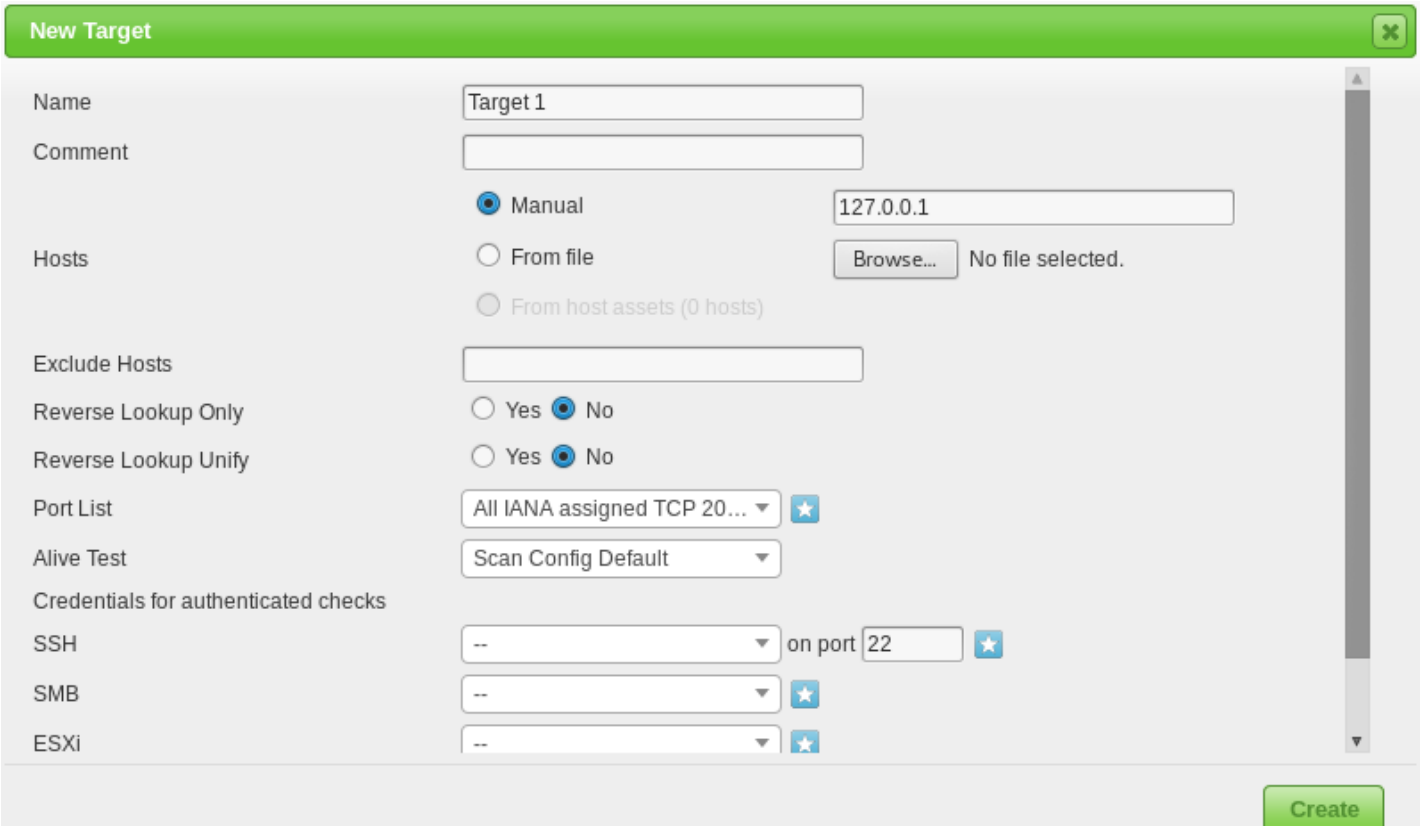

Рис. 4 Задание параметров сканирования цели

12. В параметрах отчета рекомендуется выставить отражение всех уровней уязвимостей, т.к. несколько некритических уязвимостей или неправильных настроек могут привести к тем же

результатам, что и одна критическая уязвимость. По результатам сканирования выберите самые опасные уязвимости (ориентируйтесь на числовую оценку CVSS)

13. После настройки всех необходимых параметров, ваша задача появится в списке задач в нижней части экрана раздела Tasks. Для запуска сканирования и формирования отчёта нажмите кнопку Start в разделе Actions.

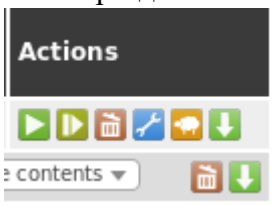

Рис. 5 Раздел Actions

14. По ссылкам после описания уязвимости, если они есть, определите коды уязвимостей в других базах уязвимостей. Например, многие уязвимости продуктов Microsoft, кроме кода CVE-0000-0000, могут иметь перекрестное описание в базах Microsoft с номерами MS00-000.
15. В отчёте приведите оригинал описания уязвимостей и переводы этих описаний. Сформулируйте рекомендации по их закрытию. Опишите этапы работы со сканером OpenVAS.

Содержимое отчёта

В отчете необходимо привести:

- ✓ формулировку цели и задания на выполнение работы;
- ✓ список ПО и оборудования;
- ✓ информацию по пунктам 14-15;
- ✓ выводы по результатам сканирования.

Контрольные вопросы

1. Что такое сканер уязвимостей?
2. Опишите структуру OpenVAS.
3. Перечислите, какие модули сканера вы использовали при сканировании? Для чего нужны эти модули?
4. Что такое уязвимость и как она влияет на безопасность системы?
5. Откуда сканер берет описания уязвимостей? Что такое NVT?
6. Для чего нужна общая система оценки уязвимостей?
7. В каком случае использование сканера уязвимости может представлять опасность для информационной безопасности?
8. Какие метрики входят в CVSS? Что они характеризуют?
9. Почему важно искать уязвимости с точки зрения защиты информации?
10. Из каких частей обычно состоит бюллетень уязвимости?

Список литературы.

1. Калькулятор CVSS V2 // Банк данных угроз информационной безопасности ФСТЭК [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/cvss2 (Дата обращения 12.04.2018).
2. Mell P., Scarfone K., Romanosky S., A Complete Guide to the Common Vulnerability Scoring System Version 2.0 Forum for Incident Response and Security Teams, 2007.
3. Официальный сайт компании Greenbone Networks [Электронный ресурс]. – Режим доступа: https://www.greenbone.net/en/ (Дата обращения 10.04.2018).

4. Описание и архитектура сканера уязвимостей OpenVAS // Официальный сайт OpenVAS [Электронный ресурс]. – Режим доступа: http://www.openvas.org/software.html (Дата обращения 11.04.2018).