Практическая работа № 7

Тема: Определение и устранение уязвимостей программного обеспечения, работающего под управлением операционных систем Windows.

Цель работы: Формирование навыков работы с приложением для автоматизированной проверки наличия уязвимостей программного обеспечения, работающего под управлением операционных систем Windows.

Теоретическая часть.

Одной из важнейших проблем при анализе защищенности информационной системы является проблема поиска уязвимостей в системе защиты. Под понятием уязвимость понимают слабость в системе защиты, которая дает возможность реализовать ту или иную угрозу. Под угрозой понимают совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности и конфиденциальности информации, хранящейся, обрабатывающейся и проходящей через компьютерную систему. Уязвимости могут являться как следствием ошибочного администрирования компьютерной системы, так и следствием ошибок, допущенных при реализации механизмов безопасности разработчиком ПО.

Для облегчения работы специалистов информационной безопасности существуют программы, позволяющие сократить суммарно потраченное время на поиск уязвимостей, за счет автоматизации операций по оценке защищенности систем. Такие программы называют сканерами безопасности. Сканеры выявляют слабые места в безопасности на удаленном либо локальном ПК. Некоторые из них способны выдавать рекомендации по устранению обнаруженных уязвимостей.

Информацию об уязвимостях можно получить из общедоступных источников – специализированных баз данных уязвимостей (БДУ), которые, как правило, предоставляют информацию об уязвимостях программного обеспечения в XML формате:

- Open Source Vulnerability Database (www.osvdb.org) – предоставляет информацию как в XML-формате, так и в виде SQL дампов;

- Common Vulnerabilities and Exposures (www.cve.mitre.org) – является поставщиком единого общего словаря уязвимостей CVE, информация поставляется в виде XML-файлов;

- National Vulnerability Database (www.nvd.nist.gov) – является наиболее подробной БДУ; включает метрики для оценки степени критичности уязвимостей, а также предоставляет XML словарь для идентификации программного обеспечения и системной конфигурации, содержащих уязвимость;

- Банк данных угроз безопасности информации ФСТЭК России (https://bdu.fstec.ru/vul) – является российской базой данных уязвимостей, содержащей описание уязвимости на русском языке, включая оценку степени опасности уязвимости, способы эксплуатации и устранения.

Одной из программ для оперативного автоматизированного обнаружения уязвимостей программного обеспечения на рабочих станциях и серверах, функционирующих под управлением операционных систем семейства Microsoft Windows, является программа ScanOVAL.

Выявление уязвимостей производится на основании сравнения состояния системных параметров сканируемого программного обеспечения (или его компонентов) с базой уязвимостей, представленной в виде OVAL-описаний, разработанных в соответствии со спецификацией OVAL не ниже версии 5.10.1.

Программа позволяет выявлять одиночные и множественные уязвимости, в зависимости от количества представленных OVAL-описаний.

Программа предназначена специалистам в области информационной безопасности для проведения оценки защищенности информационных систем на наличие уязвимостей, сведения о которых содержатся в БДУ, а также других известных уязвимостей, описанных в формате OVAL.

ScanOVAL функционирует под управлением клиентских операционных систем Microsoft Windows 7/8/8.1/10 или серверных операционных систем Microsoft Windows Server 2008/2008R2/2012/2012R2/2016.

Задание на практическую работу

1. Скачать и установить бесплатную программу ScanOVAL для автоматизированной проверки наличия уязвимостей программного обеспечения. Загрузку программы целесообразно производить с сайта Федеральной службы по техническому и экспортному контролю (ФСТЭК России): https://bdu.fstec.ru/files/scanoval.msi

2. Загрузить с сайта ФСТЭК России XML-файл с OVAL-описаниями уязвимостей: https://bdu.fstec.ru/files/scanoval.xml

3. Произвести проверку на наличие уязвимостей локального компьютера.

4. Провести анализ найденных уязвимостей: идентифицировать уязвимость, определить уровень опасности, программный продукт содержащий уязвимость.

5. С помощью открытых источников (базы данных ФСТЭК, банк данных Mitre) определить метод устранения одной из наиболее критичных уязвимостей (на Ваш выбор) и провести ее устранение.

Выполнение программы

3.1. Установка и запуск программы

Установка программы осуществляется с помощью инсталляционного пакета ScanOVAL.msi.

Запустите исполняемый файл ScanOVAL.msi. Дождитесь появления окна приветствия и нажмите кнопку «Далее». В случае, если на компьютере уже установлена программа ScanOVAL, инсталлятор предложит осуществить следующие операции выполнения: «Изменить», «Восстановить», «Удалить».

Далее в появившемся окне будет предложено ознакомиться с лицензионным соглашением. После ознакомления с содержимым выберете пункт «Я принимаю условия данного лицензионного соглашения» и нажмите кнопку «Далее». Укажите каталог, в который будут установлены файлы программы.

В результате нажатия кнопки «Далее» появится окно «Все готово к установке ScanOVAL». В следующем окне необходимо нажать кнопку

«Установить», в результате чего появится статусная строка установочного процесса. О завершении процесса установки будет свидетельствовать сообщение «Установка ScanOVAL завершена», при этом на рабочем столе появится ярлык программы.

ВАЖНО! Установка и запуск программы должны проводиться от имени учетной записи, имеющей административные привилегии на компьютере.

3.2. Интерфейс программы

Графический интерфейс программы ScanOVAL представляет собой окно, разделенное на четыре логических зоны (Главное окно):

- строка меню, расположена в верхней части окна, предназначена для доступа к сервисным функциям программы, настройке программы и справке;

- панель быстрого доступа, расположена ниже строки меню, содержит функциональные кнопки для работы с Программой;

- панель «Результаты», расположена в центральной части Главного окна, отображает список результатов проверок;

- панель «Подробности», расположена в нижней части программы, отображает детализированную информацию об уязвимости.

3.3. Работа с программой

3.3.1. Загрузка описаний уязвимостей

Для автоматического обнаружения уязвимостей необходимо в программу ScanOVAL загрузить соответствующие XML-файлы, содержащие OVAL-описания уязвимостей.

Программа работает с описаниями уязвимостей, разработанным в соответствии со спецификацией OVAL версии не ниже 5.10.1. OVAL-описания могут быть загружены с сайта банка данных угроз безопасности информации ФСТЭК России (БДУ ФСТЭК России).

Загружаемый XML-файл с OVAL-описаниями может содержать как описания одиночных уязвимостей, так и множественные (пакетные) описания, собранные в один файл.

Для загрузки описаний уязвимостей в «Главном окне программы» (Рисунок 1 – Главное окно программы) необходимо нажать на кнопку

(«Открыть файл»). Открываемый XML-файл может быть загружен с локального диска компьютера, сетевого диска или иного места, доступного пользователю на данном компьютере.

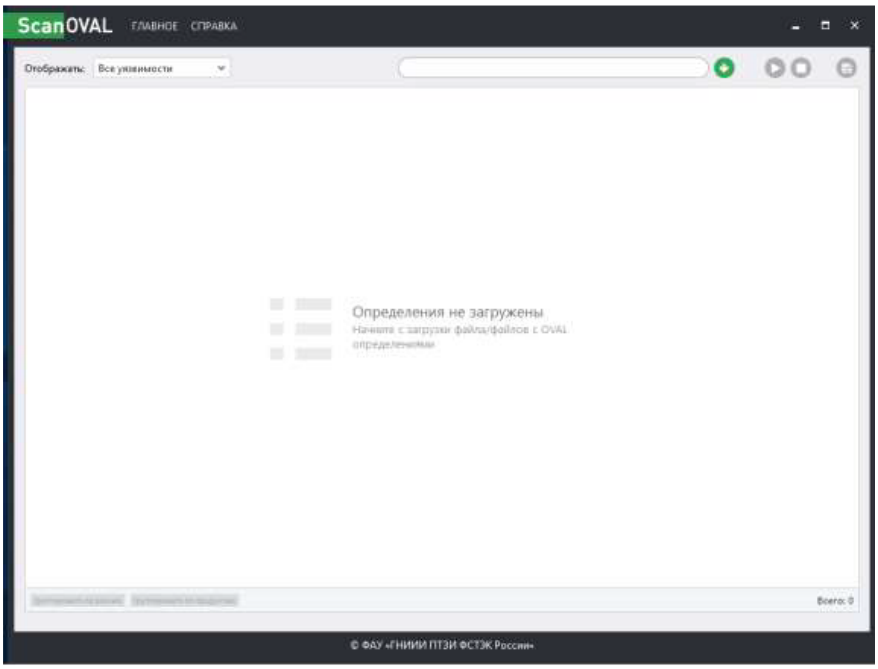

Рисунок 1 – Главное окно программы

В появившемся окне «Проводника». Выбрать необходимый файл и нажать кнопку «Открыть». В главном окне программы появится список выбранных описаний уязвимостей (Рисунок 2 – Список выбранных описаний уязвимостей).

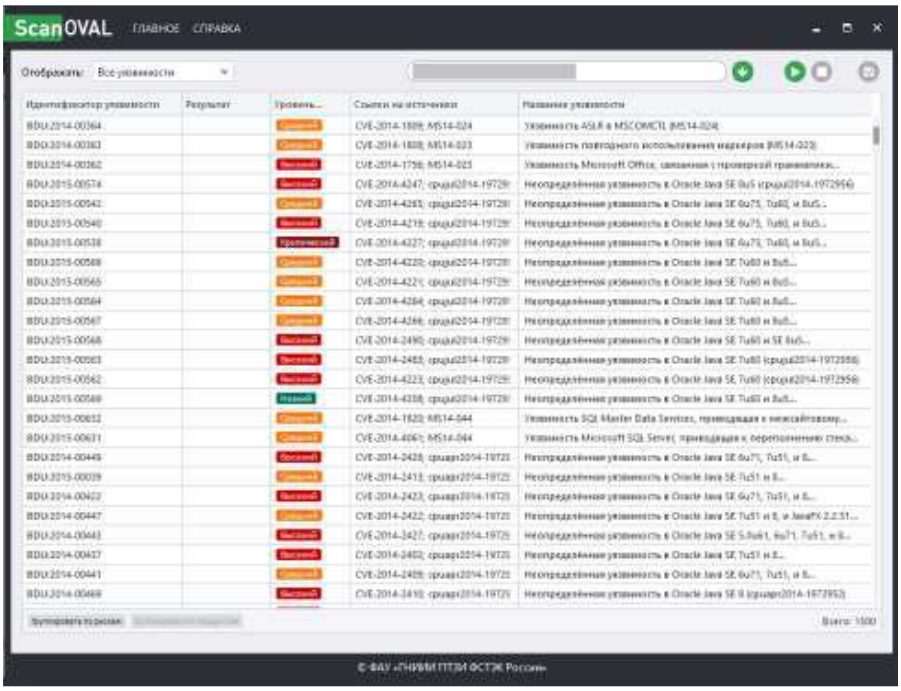

Рисунок 2 – Список выбранных описаний уязвимостей

В программе присутствует возможность добавления новых файлов и выгрузки уже используемых. Для этого необходимо воспользоваться диалогом выбора OVAL файлов (Рисунок 3).

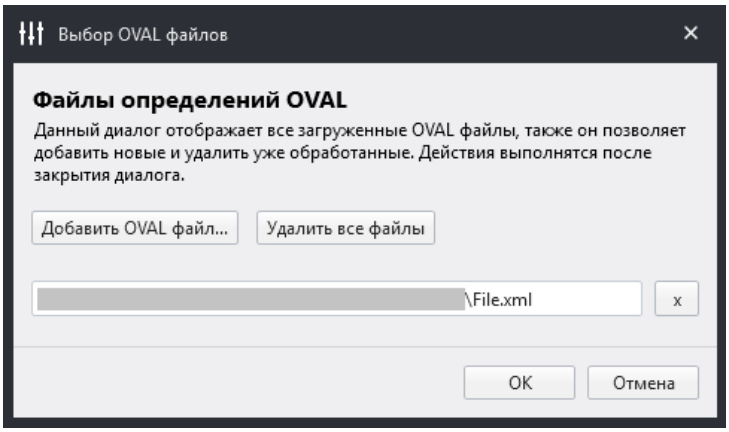

Рисунок 3 – Окно «Выбор OVAL файлов»

Данное окно вызывается автоматически по нажатию кнопки («Открыть файл») повторно, при уже загруженном файле описании уязвимостей, то есть при первой загрузке пользователю отображается стандартное диалоговое окно Windows для выбора файла, все последующие нажатия открывают окно «Выбор OVAL файлов».

3.3.2. Обнаружение уязвимостей

Функция «Обнаружение уязвимостей» становится доступной при наличии загруженных в программу описаний уязвимостей.

Для обнаружения уязвимостей необходимо нажать на кнопку «Выполнить аудит». При этом в главном окне появится сообщение «Выполнение…» и на затемненном фоне окна будет наблюдаться динамика выполнения проверок.

Свидетельством окончания проверок является исчезновение сообщения «Выполнение…» и в главном окне появятся результаты проверок с подсвеченными маркерами сообщениями – «не обнаружено» / «обнаружено» (Рисунок 4). Время сканирования проверок зависит от количества загруженных OVAL описаний, а также от аппаратных ресурсов компьютера. Сканирование может занимать от нескольких секунд для одного или нескольких описаний до нескольких минут и более для сотен и тысяч загруженных описаний.

При работе со списком уязвимостей доступны группировки по рискам и по продуктам (Рисунок 4). Группировка по рискам доступна после загрузки файлов OVAL-описаний. Группировка происходит после нажатия на кнопку «Группировать по рискам» в левой нижней части окна, в результате осуществляется группировка по столбцу «Уровень опасности уязвимости»;

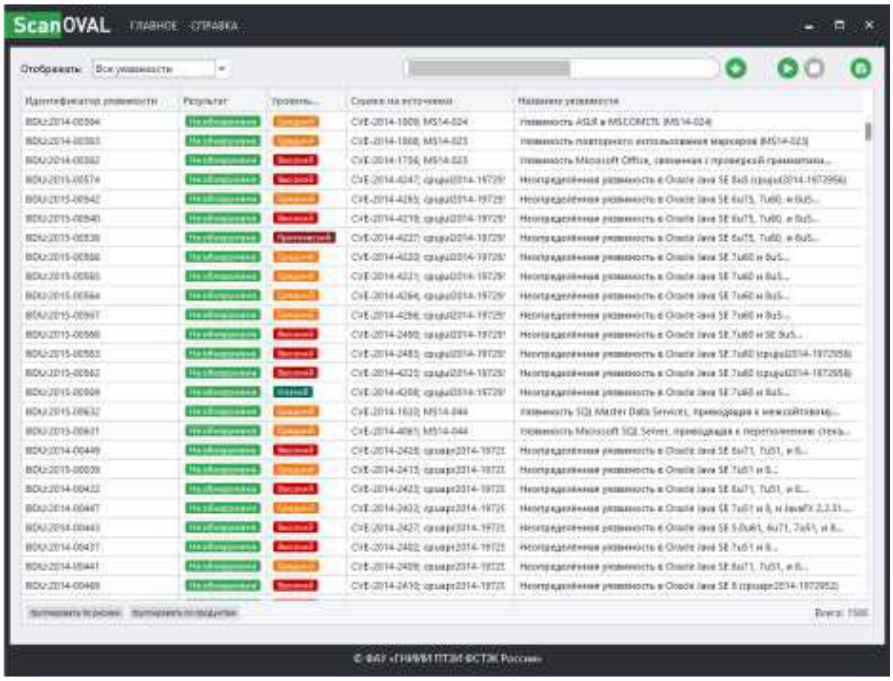

Рисунок 4 – Результат выполненной проверки

Группировка по продуктам доступна только после проведения проверки обнаружения уязвимостей и происходит после нажатия на кнопку «Группировать по продуктам» в левой нижней части окна, в результате осуществляется группировка по классификатору CPE (Common Platform Enumeration).

3.3.3. Просмотр результатов проверок

Результаты проверок отображаются в Главном окне программы на панелях «Результаты» и «Подробности».

Панель «Результаты» содержит общую информацию о результатах проверок. В строке результата отображается следующая информация:

- Идентификатор уязвимости – идентификатор уязвимости в БДУ ФСТЭК России;

- Результат – результат проверки («Обнаружено» / «Не обнаружено»);

- Уровень опасности уязвимости;

- Ссылки на источники описания уязвимости;

- Название уязвимости.

Панель «Подробности» расположена ниже панели «Результаты» и раскрывается кликом мыши по строке результата проверки или нажатием на кнопку «Подробности» (Рисунок 5).

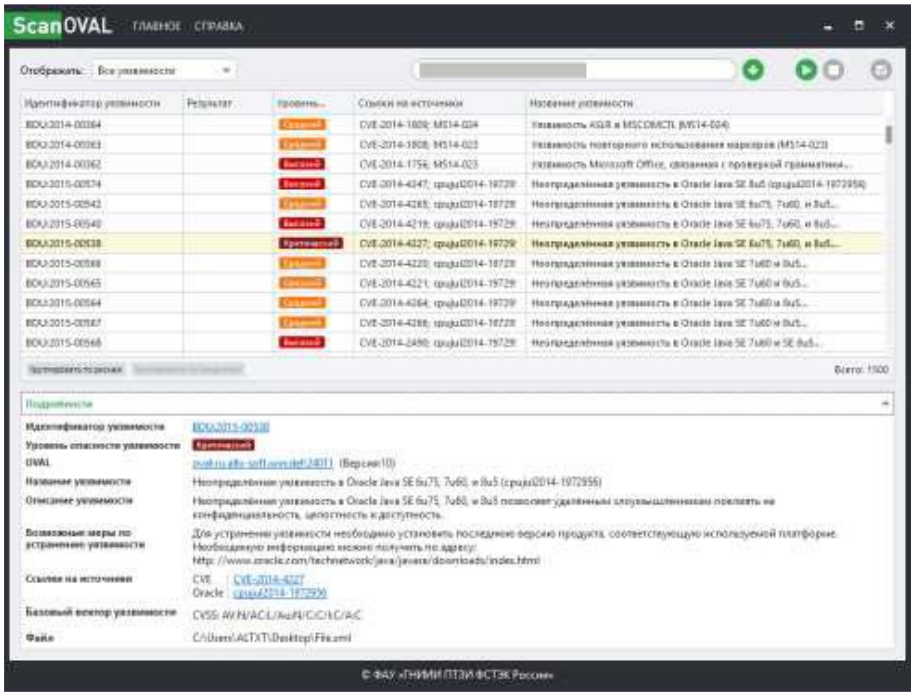

Рисунок 5 – Детализированная информация об уязвимости

В панели представлена детализированная информация об уязвимости:

- Идентификатор уязвимости в БДУ ФСТЭК России, содержащий гиперссылку на соответствующую страницу сайта БДУ ФСТЭК России;

- Результат – результат проверки: «Обнаружена» / «Не обнаружена»;

- Уровень опасности уязвимости;

- OVAL – путь к месту загрузки OVAL-описания;

- Название уязвимости;

- Описание уязвимости;

- Возможные меры по устранению уязвимости;

- Ссылки на источники;

- Базовый вектор уязвимости (CVSS);

- Программное обеспечение – обозначение уязвимого программного обеспечения в классификации CPE (Common Platform Enumeration);

- Детализация – объект для которого осуществлялась проверка;

- Файл – путь к расположению уязвимого ПО (файла). Данная строка появляется только при выявлении уязвимости.

3.3.4. Сохранение результатов проверок

Программа позволяет сохранять на локальном компьютере или любом доступном для компьютера месте результаты сканирования в формате HTML.

Для сохранения результатов проверок в Главном окне нажмите на кнопку «Создать отчет». В появившемся окне «Проводника» укажите место для сохранения отчета и нажмите кнопку «Сохранить». После сохранения появится сообщение «Отчет сохранен». Для просмотра сохраненных отчетов можно воспользоваться произвольным веб-браузером.

3.3.5. Завершение выполнения программы

Работа Программы завершается нажатием на кнопку в правом верхнем углу или через Меню: Главное -> Выйти из программы.