# МЕТОДИКА ПОИСКА И АНАЛИЗА УЯЗВИМОСТЕЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

*Нгуен К.А., ст. гр. 961402*

*Белорусский государственный университет информатики и радиоэлектроники*

*г. Минск, Республика Беларусь*

*Бойправ О.В. – канд. техн. наук*

**Аннотация.** В докладе представлены результаты обоснования и разработки методики и анализа уязвимостей в информационных системах. Эта методики основана на использовании сканера уязвимостей OpenVAS.

Уязвимость – это недостаток программно-технического средства или информационной системы в целом, который может быть использован для реализации угроз безопасности информации. Иными словами, уязвимость – это слабое место актива или средства контроля и управления, которое может быть использовано злоумышленниками. Сведения об известных уязвимостях систематизированы в базе CVE (Common Vulnerabilities and Exposures). Для оценки уязвимостей используется система CVSS (от англ. Common Vulnerability Scoring System).

Сканеры уязвимостей – это, как правило, программные средства, предназначенные для выявления проблем безопасности на узлах вычислительной сети. Позволяют исследовать систему с целью обнаружения уязвимостей.

Известными коммерческими сканерами являются Nessus, GFI LANguard, XSpider (MAxPatrol). Nessus. Они предназначены для автоматического поиска известных уязвимостей и организации защиты информационных систем. В отлчиие от перечисленных сканеров OpenVAS является сканером уязвимостей и средство управления ими с открытым исходным кодом. Проект OpenVAS поддерживается организацией Software in the Public Interest. База уязвимостей OpenVAS включает в себя около 35000 проверок, так называемых Network Vulnerability Tests (NVTs), а также подключение к базе CVE, описывающей известные уязвимости. В отличии от прочих, OpenVAS бесплатен, работает без каких-либо ограничений и может пригодится как сетевым администраторам, так и специалистам ИБ для выявления актуальных проблем своей инфраструктуры. В связи с указанными преимуществами OpenVAS по сравнению с другими сканерами уязвимостей, это программное средство было выбрано в качестве инструмента для разработки методики.

Сканер уязвимостей OpenVAS может быть установлен с помощью VirtualBox в виде виртуальной машины. Для этого енобходимо выполнить следующие шаги.

1. Задать в VirtualBox следующие параметры устанавливаемой виртуальной машины: операционная система – Other Linux, оперативная память – 5120 Мб, процессоры – 2, видеопамять – 9 Мб, носители – загружаемый файл OVA, сеть – сетевой мост.

2. Выполнить процесс установки виртуальной машины.

3. Получить доступ к ресурсам установленной виртуальной машины при использовании следующих учетных данных: логин – admin, пароль – admin.

4. Создать новую учетную запись веб-администратора.

Сканер уязвимостей OpenVAS также может быть установлен в дистрибутив операционной системы Kali Linux. Для этого необходимо выполнить следующие шаги.

1. Полностью обновить систему Kali Linux путем применения команды apt update && apt upgrade -y.

2. Выполнить следующую команду, чтобы загрузить OpenVAS: apt install openvas.

3. Запустить программу установки OpenVAS путем применения следующей команды: gvm-setup.

4. Сгенерировать пароль для первого входа в систему.

5. Проверить настройки OpenVAS путем использования следующей команды: gvm-check-setup.

6. Сгенерировать новый пароль администратора.

Управление OpenVAS выполняется через веб-интерфейс. Доступ к веб-интерфейсу OpenVAS, установленного в виде виртуальной машины, необходимо получать следующим образом.

1. Ввести IP-адрес веб-интерфейса устройства.

2. Войти в систему под учетной записью веб-администратора, созданной во время установки виртуальной машины.

Доступ к веб-интерфейсу OpenVAS, установленного в дистрибутив операционной системы Kali Linux, необходимо получать следующим образом.

1. Открыть веб-интерфейс: http://localhost:9293.

2. Войти в систему при использовании следующих учетных данных: имя пользователя – admin, пароль – новый пароль администратора, сгенерированный при установке.

В ходе апробации разработанной методики были обнаружены 4 уязвимости: 2 уязвимости высокого уровня риска: SMB логины (имя и пароль совпадают), SMB сервер (ms17–010) с портом 445/TCP; 1 уязвимость среднего уровня риска (причина – DCE/RPC сервис с портом 135/TCP); 1 уязвимость низкого уровня риска (причина – временные метки пакетов, передаваемых по протоколу TCP). Следует отметить, что в OpenVAS предусмотрена возможность генерирования отчетов по результатам выполненного сканирования.

Разработанная методика может быть использована для поиска и анализа уязвимостей информационных систем различного масштаба.