Е. Б. Челдышкин, Е. А. Левчук
(*БГУ, Минск*)

АНАЛИЗ ЗАЩИЩЕННОСТИ СЕТЕВЫХ УЗЛОВ С ИСПОЛЬЗОВАНИЕМ СКАНЕРА УЯЗВИМОСТЕЙ OPENVAS

Сетевая безопасность привлекает широкое общественное внимание при реализации различных атак на серверы предприятий и учреждений. Рассмотрим сценарий анализа сетевой безопасности с помощью сканера OpenVAS, предназначенного для поиска уязвимостей. Для этого рекомендуется создать вычислительную сеть из ряда компьютеров и эмулировать виртуально сеть компьютеров.

В результате была создана виртуальная машина, использующая определенный объем компьютерных ресурсов. Пользователь имеет возможность определить необходимые ресурсы, в частности, выбрать максимальный объем требуемой оперативной памяти, видеопамяти и жесткого диска, установить количество процессоров, которые принимают участие в работе с приложением. Далее, на разработанную виртуальную машину установлена соответствующая операционная система, инсталированы распространенные программные комплексы и приложения. Таким образом, у пользователя имеется привычный функционал для работы с ними из своей операционной системы. Для создания и настройки виртуальных машин был использован продукт Oracle VM VirtualBox.

В тестовом стенде развернуты виртуальные машины: Windows 2000, Windows XP, Kali Linux, Debian 6, Debian 8, Dawn Vulnerable Linux Infectious Disease (DVL). После обзора отчетов сканирования была составлена общая гистограмма с найденными уязвимостями по различным операционным системам (рис. 1).

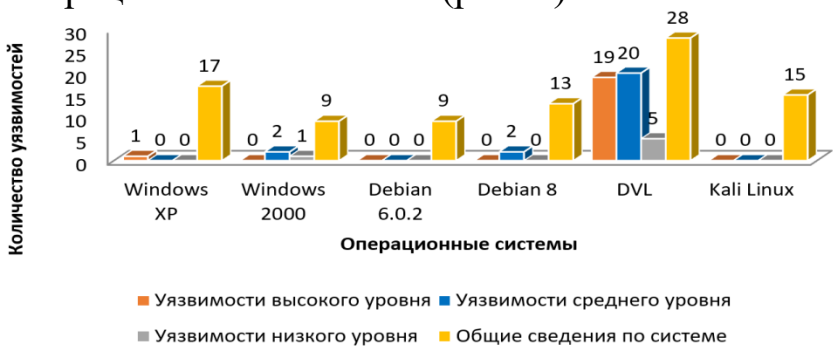

Рисунок 1 – Гистограмма с полученными результатами сканирования