ЗАЩИТА ИНФОРМАЦИИ КОРПОРАТИВНЫХ СЕТЕЙ СВЯЗИ С ПОМОЩЬЮ ONLINE ПЕНТЕСТОВ

О.А. Хацкевич, А.Д. Михейчик

Защита информации на корпоративных сетях Республики Беларусь всегда являлась актуальной задачей. В настоящее время наблюдается непрерывное совершенствование механизмов реализации сетевых атак. В связи с этим системные администраторы должны периодически проверять на эффективность применяемые в их сети средства обеспечения сетевой безопасности. На рынке сетевых услуг существует большое количество программных и программно-аппаратных средств, предназначенных для мониторинга безопасности сетей. К недостаткам таких средств можно отнести высокую стоимость и сложность в реализации самостоятельной настройки. По этой причине в некоторых ситуациях имеет смысл прибегнуть к бесплатным online-инструментам, которые дают возможность оценить защищенность сети от актуальных сетевых атак владельцам даже небольших сетей. К таким online инструментам относятся пентесты. Под пентестом понимается мониторинг безопасности сети с помощью проведения испытаний на проникновения. Испытания основаны на сетевых атаках, реализуемых с целью обнаружения уязвимостей и недосатков. В работе исследовалась эффективности работы online-пентестов, направленных на межсетевые экраны, антивирусные программы и веб-сайты. Для проверки защищенности межсетевого экрана применялся сервис Check Point CheckMe . Представленный сервис включает в себя несколько тестов, с помощью которых выполняется анализ компьютера пользователя и сети на предмет наличия уязвимостей, связанных с вредоносными программами, удаленным доступом, утечкой данных, кражей конфиденциальной информации, эксплойтами и использованием анонимайзеров. Для мониторинга безопасности межсетевых экранов, антивирусных программных средств, веб-сайтов был использован дистрибутив Linux – Kali Linux, который непосредственно используется для осуществления пентестинга, благодаря большому количеству встроенных в данный дистрибутив инструментов. В качестве объекта исследования использовалась сеть БГУИР. Результат показал эффективность метода и достаточно высокую степень защищенности сети.