КОНТРОЛЬ СОСТОЯНИЯ КОМПОНЕНТОВ ЛОКАЛЬНОЙ СЕТИ: ПРОБЛЕМЫ БЕЗОПАСНОСТИ

В.Д. Шантарович, В.А. Ганжа

Протокол SNMP был разработан с целью управления сетевыми устройствами и допускает возможность внесения изменений в функционирование этих устройств. В наше время вопросы сетевой безопасности приобретают особое значение, особенно когда речь идет о протоколах передачи данных, в корпоративных сетях. После знакомства с SNMP становится понятно, что разработчики протокола думали об этом в последнюю очередь. К сожалению, в SNMP реализована очень простая система паролей, которую не следует считать безопасной. SNMP-запрос содержит групповое имя (community name), которое является разновидностью пароля. Создается впечатление что протокол рассчитан на работу в среде так называемых «доверенных хостов».

Управление сетью подразумевает установку на управляемые устройства специальных программных компонентов, называемых агентами управления; они могут отчитываться или отвечать на опросы объектов управления в системе управления сетью (NMS).

Несмотря на то, что большинство процессов, связанных с управлением сети, осуществляются средствами этой самой сети (что называется внутриполосным управлением), почти все системы управления сетями предусматривают различные методы внеполосного управления, обеспечивающие возможность обращения к управляемым устройствам даже тогда, когда сама сеть не функционирует.

Система управления сетью устроена на двух основных видах деятельности: способности управляемых устройств выдавать предупреждения об определенных событиях и способности объектов управления регулярно опрашивать управляемые устройства с целью сбора и группировки данных об этих устройствах, а также о сетях, их соединяющих.

БРАНДМАУЭР КАК ЭЛЕМЕНТ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Е.О. Шевчук, С.Г. Шульдова

Брандмауэр (межсетевой экран или файрвол) – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

Основной задачей брандмауэра является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети.

Межсетевые экраны сейчас часто устанавливают не только на границе локальной сети и сети Интернет, но и между локальными сегментами сети для того, чтобы защитить и приходящий и локальный трафики. Программно-аппаратные элементы представлены в двух видах: в виде отдельного модуля в коммутаторе или маршрутизаторе и в виде специализированного устройства. Плюсы программно-аппаратных элементов защиты информации в том, что необходимо одно отдельное физическое устройство, как правило, с установленной ОС семейства *nix, которые настроены таким образом, чтобы выполнять только необходимые функции. Такие системы просто внедрять, управлять ими, они более производительны, так как из ОС исключены все неиспользуемые сервисы. Программно-аппаратные системы имеют высокую отказоустойчивость и доступность.

Основываясь на принципах работы аппаратных брандмауэров Cisco, в частности Cisco ASA 5500-X, в рамках магистерской диссертации планируется составить правила фильтрации, а также схему подключения брандмауэров в сети из нескольких серверов, что позволит обеспечить достаточный уровень безопасности любой сети.

Литература

1. Лебедь С.В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. МГТУ им. Н. Э. Баумана, 2002. 306 с.

2. Ingham K., Forrest S. A History and Survey of Network Firewalls. University of New Mexico, 2002. 42 p.

3. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: ИНФРА-М, 2011. 416 с.