Анализатор протоколов Tcpdump

Tcpdump – это утилита Unix, которая была разработана еще в конце 80-х годов сотрудниками Lawrence Berkeley Laboratory и до сих пор находит свое применение. Tcpdump поддерживает интерфейс командной строки в классическом Unix-стиле; результаты также выдаются на экран в виде текстовых строк, а также могут записываться в файл. Существует и версия WinDump, которая работает под Windows. Разработчики tcpdump создали открытую библиотеку программ ***pcap (p***acket ***cap***ture***)***, с помощью которой приложение, занимающееся мониторингом трафика сети может получить доступ к сетевому алаптеру и выполнить захват кадров. Кроме того, определен формат файла с расширением '.pcap', в который помещаются захваченные кадры; этот формат сегодня поддерживают практически все программные и программно-аппаратные средства мониторинга трафика.

Tcpdump переводит сетевой адаптер компьютера в режим неразборчивого захвата пакетов ***(promiscuous mode)***. В обычном режиме адаптер Ethernet буферизует и передает для дальнейшей обработки сетевым модулям операционной системы только те кадры, у которых MAC- адрес назначения совпадает с MAC- адресом адаптера. В неразборчивом режиме адаптер захватывает все пакеты, биты которых появляются на его входе. В сетях Ethernet на разделяемой среде (которые практически уже не встречаются) это означает, что захватываются вообще все пакеты, циркулирующие в сети. В локальных коммутируемых сетях ситуация другая – здесь трафик сегментируется и на интерфейс компьютера в принципе не могут попасть кадры, которые ему не адресованы. Поэтому для захвата трафика, направляемого к серверу или группе серверов, применяется *зеркализация портов коммутатора*, иллюстрируемая примером сети на рис. 1.

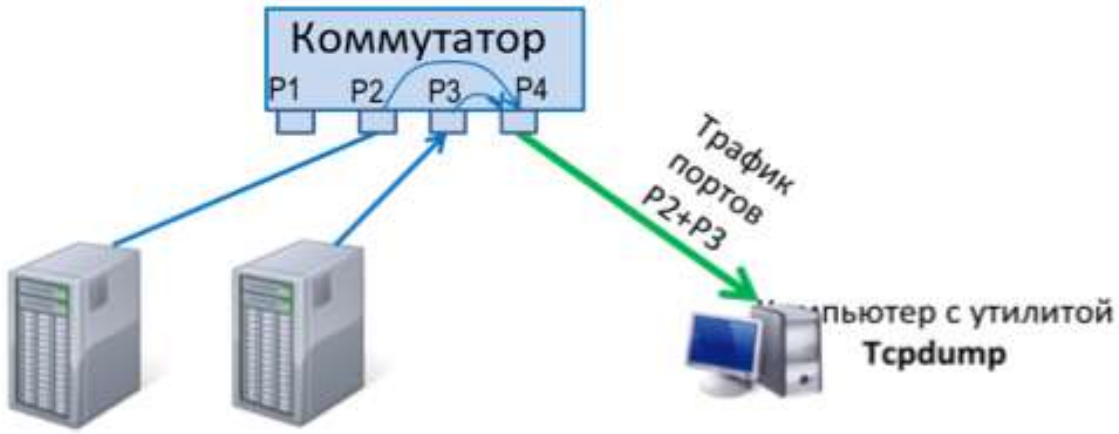

Рис. 1. Зеркализация трафика в коммутируемых локальных сетях

Здесь коммутатор сконфигурирован так, что весь трафик, поступающий и покидающий порты P2 и P3, направляется (зеркализуется) на порт P4, к которому подключен компьютер с утилитой Tcpdump. В результате анализатор протоколов Tcpdump получает возможность захватывать весь трафик серверов, подключенных к портам P2 и P3.