УДК 004.056.53

студентка И.С. Корецкая
ГВУЗ «Национальный Горный Университет»

ПРОБЛЕМА ПОДСЛУШИВАНИЯ СЕТЕВОГО ТРАФИКА

В наше время очень актуальна проблема атак IP-сетей. В данной статьи изложено: назначение, виды, способы, одной из самых актуальных атак - атаки подслушивания, а также программы для реализации, меры предотвращения подслушивания.

На практике IP-сети уязвимы для ряда способов несанкционированного вторжения в процесс обмена данными. По мере развития компьютерных и сетевых технологий (например, с появлением мобильных Java-приложений и элементов ActiveX) список возможных типов сетевых атак на IP-сети постоянно расширяется. Одной из наиболее распространенной атакой в наше время является подслушивание.

Подслушивание (sniffing) – по большей части данные по компьютерным сетям передаются в незащищенном формате (открытым текстом), что позволяет злоумышленнику, получившему доступ к линиям передачи данных в вашей сети подслушивать или считывать трафик. Для подслушивания в компьютерных сетях используют сниффер. *Сниффер пакетов* представляет собой прикладную программу, которая перехватывает все сетевые пакеты, передаваемые через определенный домен.

Снифферы используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые протоколы передают данные в текстовом формате (Telnet, FTP, SMTP, POP3 и т.д.). С помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

Перехват пароля, передаваемого по сети в незашифрованной форме, путем подслушивания канала является разновидностью атаки подслушивания, которую называют *password sniffing*. Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Если приложение работает в режиме клиент-сервер, а аутентификационные данные передаются по сети в читаемом

текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам[1].

Выделяют два вида снифферов по категориям в сети: win снифферы (linux снифферы), предназначенные для перехвата сетевого трафика по локальным проводным и беспроводным сетям Wi-Fi и глобальным с использованием конфигураций Windows (Linux) и http-снифферы (они же online онлайн снифферы), предназначенные также для перехвата информации, преимущественно в глобальной сети Internet, но с использованием ресурсов программ на PHP Web-серверов Internet.

Анализ прошедшего через сниффер трафика позволяет:

– Обнаружить паразитный вирус;

– Выявить в сети вредоносное и несанкционированное ПО, например, сетевые сканеры, троянские программы, клиенты пиринговых сетей;

– Локализовать неисправность сети или ошибку конфигурации сетевых агентов (для этой цели снифферы часто применяются системными администраторами).

Перехват трафика может осуществляться:

– через анализ побочных электромагнитных излучений и восстановление таким образом прослушиваемого трафика;

– через атаку на канальном (MAC-spoofing) или сетевом уровне (IP-spoofing), приводящую к перенаправлению трафика жертвы или всего трафика сегмента на сниффер с последующим возвращением трафика в надлежащий адрес[2].

Существует два способа прослушивания сетей: пассивное и активное. При пассивном прослушивании сниффер просто переводит сетевую плату в неразборчивый режим и принимает весь проходящий через компьютер трафик, активное прослушивание подразумевает принятие специальных мер для того что бы принудительно переводить трафик на себя, даже из другого сегмента сети.

Другое дело активный сниффинг, существует большое количество способов активного прослушивания, рассмотрим некоторые:

– MAC flooding этот способ срабатывает на многих дешевых и устаревших моделях Switch. Switch имеет память для хранения адресной таблицы (соответствие MAC адреса и порта на который будут посылаться данные), если переполнить эту память фальшивыми адресами то свитч перестанет контролировать передачу. Этот способ действует и на мосты.

– MAC duplicating эта атака представляет собой простую подделку MAC адреса жертвы. Проблема тут в том что перехваченные данные не попадают на целевой компьютер и вас могут вычислить, кроме того таким способом можно перехватить только данные идущие к жертве но не наоборот[3].

Предотвратить угрозу сниффинга пакетов можно с помощью следующих мер и средств: применение для аутентификации однократных паролей; установка аппаратных или программных средств, распознающих снифферы; применение криптографической защиты каналов связи[1].

Перечень литературы:

1. http://www.opennet.ru/base/sec/arp_snif.txt.html
2. http://kunegin.com/ref5/ut/page8.htm
3. http://ru.neospy.net/articles/sniffer_menu.php?id=12&name=sniffer_i_proslushivanie_seti