Ромашкин Д.О., *Жилина Е.В.
студент факультета КТиИБ;
*к.э.н., доцент каф. ИТиЗИ
РГЭУ (РИНХ),
г. Ростов - на - Дону, Российская Федерация

АНАЛИЗ СЕТЕВОГО ТРАФИКА. СНИФФЕРЫ

Снифферы - это программы, перехватывающие сетевой трафик [1; 2]. Для администраторов сетей они необходимы для диагностики сети, а для злоумышленников для перехвата трафика и паролей. Обычно при упоминании снифферов многие проводят аналогию с прослушиванием разговоров по телефонной линии, т.е. происходит подключение к телефонной сети, с помощью чего можно перехватить беседу людей. Примерно также сложилась ситуация и в компьютерных сетях: на данный момент есть возможность перехватывать информацию, которой обмениваются несколько компьютеров.

Виды снифферов и сниффинга

Исходя из того, что теория сниффинга еще нигде и никем официально и в полном объеме не описывалась, все приведенные ниже классификации носят некий условный характер.

Итак, по среде обитания снифферы могут быть разделены так [3] (таблица 1).

Таблица 1 - Виды снифферов по среде обитания

Вид сниффера	Характеристика
снифферы на маршрутизаторе (шлюзе)	Создается возможность перехватывать трафик, проходящий через интерфейсы этого шлюза. Например, из локальной сети в глобальную и в обратную сторону. Соответственно, если установить сниффер на маршрутизаторе провайдера Интернет - сети, мы можем отслеживать трафик его пользователей.
на конечном узле сети	Применительно к сетям Ethernet. Классический, некоммутируемый Ethernet предполагает, что каждый сетевой интерфейс «видит» весть траффик своего сегмента. Однако в нормальном режиме работы сетевой карты, прочитав первые 48 бит заголовка фрейма, станция сравнивает свой MAC - адрес с адресом получателя, указанном во фрейме. Если адрес чужой, станция элементарно перестает читать чужой фрейм. Таким образом, в нормальном режиме можно перехватывать и анализировать только свой траффик.

Во втором виде снифферов для перехвата пакетов всех станций сегмента требуется перевести сетевую карту сниффера в режим «promiscuous mode», чтобы она читала непредназначенные ей пакеты до конца. Практически все реализации снифферов позволяют переход «promiscuous mode». Но при этом, в случае использования коммутируемого Ethernet - соединения, сетевая карта создает ситуацию, когда даже ее переход в режим «promiscuous mode» делает прослушивание непредназначенного трафика

для станции сниффера невозможным. Однако существует технология организации такого прослушивания путем так называемого «ARP - спуфинга». Суть заключается в следующем: коммутатор создает "broadcast domain", и хост с установленным сниффером с помощью подделки ARP - сообщений может притвориться, например, пограничным маршрутизатором. Таким образом, трафик соседей «насильственно отправится» в сторону злоумышленика.

Также снифферы могут отличаться по функциональными признакам:

– физические интерфейсы и протоколы канального уровня;
– качество декодирования и количество поддерживаемых протоколов;
– пользовательский интерфейс и удобство отображения;
– дополнительные особенности: статистика, генерирование или модификация пакетов, просмотр атаки в реальном времени и другое.

При выборе сниффера (как и любого другого программного обеспечения) злоумышленники (либо системные администраторы) руководствуются следующими правилами: из сущесвующего ПО под используемую операционную систему выбирают либо то, что максимально соответсвует поставленным целям, либо универсальное решение. Выбор сниффера, который максимально соответствует задачам, имеет смысл в том случае, если планируется либо какое - нибудь разовое мероприятие, либо постоянное выполнение одной и той же операции. Выбор сниффера с выполнением универсального круга задач лежит в идее, но заранее не извесно в какой ситуации он будет применен.

Реализации снифферов.

На данный момент общедступно предоставлено множество вариаций уже готовых сниффер - программ. Сначала рассмотрим снифферинг в операционной системе WINDOWS.

ПО под названием «CommView» (рис. 1). Чаще всего используют для административных задач.

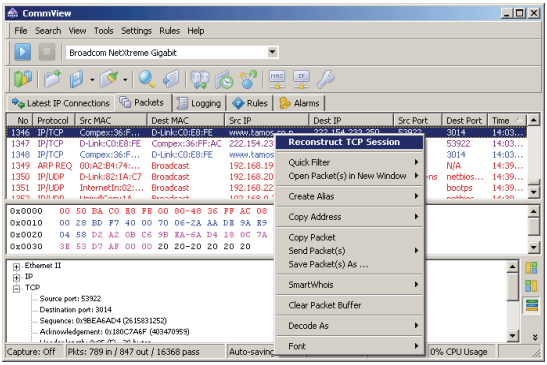

Рисунок 1 – Пример сниффера «CommView»

Описание с официального сайта программы: «CommView - это программа для перехвата и анализа трафика Интернета и локальной сети [4]. Она собирает информацию о данных, проходящих через модем (dial - up) или сетевую карту и декодирует анализируемые

данные». «CommView» является продвинутым сниффером производства компании TamoSoft. В нём можно установить свои правила на сниффинг (например, игнорировать ICMP - протоколы, а TCP в свою очередь снифферить, также имеется поддержка ethernet - протоколов ARP, SNMP, NOVELL и т.д.). Имеется подержка сниффинга только входящие пакеты при игнорировании других, можно указать файл для логов всех пакетов и лимитов их размера в мегабайтах.

ПО «IRIS» (рис. 2). Популярный сниффер для Windows.

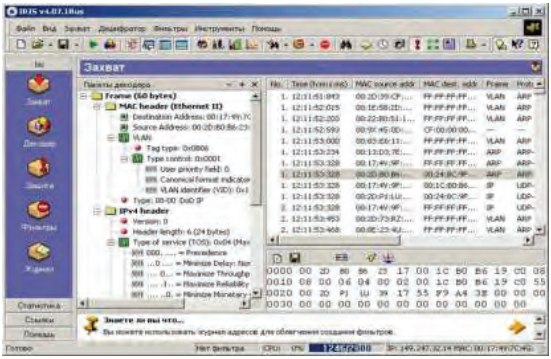

Рисунок 2 – Пример сниффера «IRIS»

Известный продукт фирмы eEye, скачать можно на официальном сайте [5]. Программа предоставляет обширные возможности по фильтрации перехватываемых пакетов. Также имеется декодер пакетов (Packet Decoder). Он поддерживает развитую систему логов, а доступные возможности фильтрации превосходят все приведенные в статье реализованные снифферы. Это фильтр, который может ловить либо все пакеты, либо с различными ограничениями (например, только multicast - пакеты, либо только MAC - фреймы). Можно фильтровать по определенным MAC / IP адресам, по портам, пакетам, по содержанию определенных символов.

Реализации снифферов в Unix - образных ОС.

ПО «Linsniffer» (рис. 3). Простой сниффер для перехвата логинов и паролей [1].

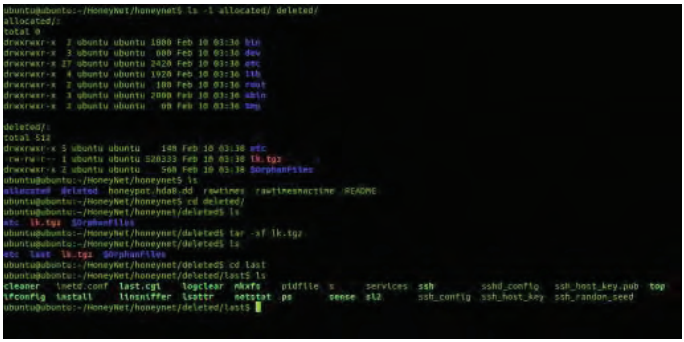

Рисунок 3 – Пример сниффера «Linsniffer»

У данного сниффера стандартная компиляция (gcc - o linsniffer linsniffer.c). В его функционал входит запись логов перехваченных данных.

ПО «Linux _ sniffer» (рис. 4). Популярный сниффер Интернет - сети.

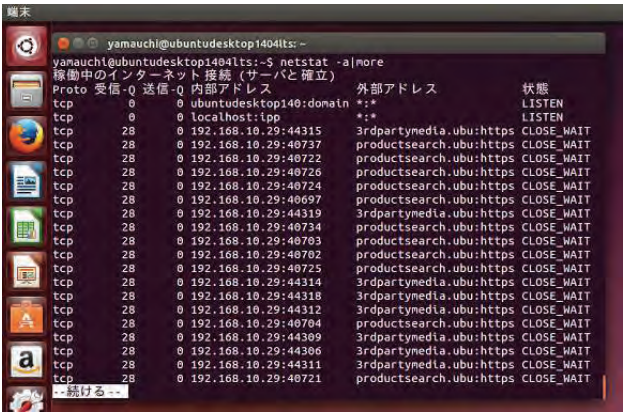

Рисунок 4 – Пример сниффера «Linux _ sniffer»

Требуется тогда, когда администратору или злоумышленнику необходимо детальное изучение сети. Стандартная компиляция. Также выдает дополнительную информацию, такую как isn, ack, syn, echo _ request (ping) и т.д.

ПО «Justniffer» (рис. 5). Анализатор пакетов протокола TCP [6].

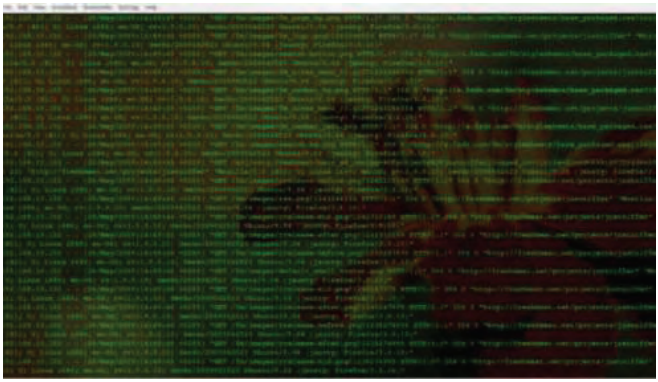

Рисунок 5 – Пример сниффера «Justniffer»

Justniffer может перехватывать сетевой трафик с использованием гибких настроек, может имитировать журналы веб - серверов в качестве access _ log Apache, включая в себя такую информацию, как время отклика (полезно для устранения проблем с производительностью). Justniffer был создан с целью отладки производительности в сети TCP услуг на основе анализа соединений HTTP, JDBC, RTSP, SIP, SMTP, IMAP, POP, LDAP и т.д.

Таким образом, при выборе снифер - программы, необходимо учитывать будущие цели и платформы использования для анализа трафика в сети.

Список использованной литературы:

1. Сниффер - что за зверь // Хакер. - Электронный ресурс: https: // xakep.ru / 2001 / 02 / 21 / 12020 / (дата обращения 13.02.2017, режим доступа: открытый).

2. Жилина Е.В., Ружицкий А.Г. Принципы сетевого сканирования в пентестинге // Fundamental and applied science today V. Vol. 1. Proceedings of the Conference (Материалы V международной научно - практической конференции "Фундаментальные и прикладные науки сегодня" 30 - 31 марта 2015 г.). – North Charleston, USA. – 2015. – Т. 1. - С. 140 - 143.

3. Почти все, что вы хотели знать о снифферах // Сетевые решения. – Электронный ресурс: http: // www.nestor.minsk.by / sr / 2000 / 12 / 01202.html (дата обращения 13.02.2017, режим доступа: открытый).

4. Официальный сайт CommView.org. – Электронный ресурс: http: // www.tamos.com / (дата обращения 14.02.2017, режим доступа: открытый).

5. Официальный сайт IRIS. – Электронный ресурс: www.eeye.com (дата обращения 14.02.2017, режим доступа: открытый).

6. Официальный сайт Justniffer. – Электронный ресурс: http: // justniffer.sourceforge.net / (дата обращения 14.02.2017, режим доступа: открытый).

Захаров И.С.,
магистрант
ФГБОУ ВО Кубанский государственный
аграрный университет имени И.Т.Трубилина
г. Краснодар, Российская Федерация

ПРЯМОЙ ВПРЫСК ТОПЛИВА – БУДУЩЕЕ ДВИГАТЕЛЕСТРОЕНИЯ

В чем же преимущество прямого впрыска топлива перед другими видами систем питания бензиновых ДВС? Первое большое преимущество такого впрыска заметили еще на моторах Mercedes 50 - х годов. Там впрыск благодаря более качественному по сравнению с карбюратором распылу и получению однородной горючей смеси сам по себе давал прирост мощности. Но если сейчас сравнивать идентичные агрегаты с распределенным и прямым впрыском, то никакой разницы в лошадиных силах не обнаружится. Так в чем смысл? В стремлении производителей следовать общим тенденциям – увеличивать КПД при снижении расхода топлива и вредных выбросов. Все это и ранее было достижимо с помощью оптимизации подачи смеси и процессов горения. Теперь же впрыск топлива вышел на новый виток эволюции.

Что же необходимо для внедрения direct injection в современные двигатели? На первый взгляд, немного: топливный насос высокого давления, форсунки, расположенные в камере сгорания и способные обеспечить более тонкий распыл и особая форма дна поршня,