Работа с программой WinDump/tcpdump

Описание

Tcpdump – программа для перехвата и анализа сетевого траффика.

Tcpdump не является стандартной утилитой Windows. Изначально представляло UNIX-приложение, но со временем было портировано и под Windows. Проект, в рамках которого осуществляется портирование, известен как WinDump.

Для использовния Tcpdump следует сначала загрузить и установить библиотеку WinPcap (http://www.winpcap.org). После этого с того же сайта нужно загрузить исполняемый файл Tcpdump, который называется WinDump.exe (http://www.winpcap.org/windump/).

ВАЖНО! Для работы windump в ОС Windows XP необходима библиотека winpcap версии 3.1, для более поздних ОС (windows 7, 8) необходимо скачать библиотеку winpcap версии 4 и выше.

Использование

Tcpdump используется посредством командной строки. Формат командной строки следующий:

tcpdump [**-ABdDeflLnNOpqRStuUvxX**] [**-c** *count*]

[**-C** *file_size*] [**-F** *file*]

[**-i** *interface*] [**-m** *module*] [**-M** *secret*]

[**-r** *file*] [**-s** *snaplen*] [**-T** *type*] [**-w** *file*]

[**-W** *filecount*]

[**-E** spi@ipaddr *algo:secret,...*]

[**-y** *datalinktype*] [**-Z** *user*]

[*expression*]

Набор параметров командной строки tcpdump очень разнообразен. Здесь не рассматриваются все возможности и ключи программы, а только необходимые для выполнения лабораторной работы. Полное описание всех ключей программы tcpdump с примерами можно получить по адресу http://www.winpcap.org/windump/docs/manual.htm.

Как видно из синтаксиса команды ни одна из команд не является обязательной.
Программа может работать в трех режимах:

1. Вывод перехваченного сетевого траффика на экран (в текстовую консоль);
2. Вывод перехваченного траффика в файл дампа для его последующего анализа (на это указывает опция **-w**). В этом режиме информация на экран не выводится;
3. Вывод перехваченного ранее сетевого траффика из файла дампа на экран (на это указывает опция **-r**).

Tcpdump позволяет выбрать сетевой интерфейс для просмотра траффика. Для указания используемого сетевого интерфейса нужно использовать параметр **–i** с явным указанием имени интерфеса. Чтобы получить список имеющихся в системе сетевых интерфейсов, нужно воспользоваться параметром командной строки **–D.**

Пример:

> windump -D

1.\Device\NPF_GenericDialupAdapter (Generic dialup adapter)

2.\Device\NPF_{9002F569-498C-46E5-8BBC-3359ADC56DA1} (Marvell Gigabit Ethernet Controller (Microsoft's Packet Scheduler))

По умолчанию tcpdump прослушивает первый адаптер (на примере .\Device\NPF_GenericDialupAdapter). Для прослушивания второго интерфейса необходимо запустить windump с параметром **–i2.**

Пример:

> windump -i2

После чего windump выводит на экран название прослушиваемого адаптера:

windump: listening on \Device\NPF_{9002F569-498C-46E5-8BBC-3359ADC56DA1}

Для прекращения работы windump следует нажать комбинацию клавиш Ctrl+C – на экран выводится краткая статистика работы программы:

22 packets captured
22 packets received by filter
0 packets dropped by kernel

По умолчанию программа tcpdump захватывает максимум 68 первых байт каждого перехваченного пакета. Для изменения этого числа предусмотрена опция **–s**, задающая максимальный размер части захваченного пакета. В следующем примере захватываемая длина пакетов устанавливается равной 1024 байта.

> windump -i2 –s 1024

Примечание: как и любая консольная программа, windump позволяет перенаправить вывод информация в файл, что чаще удобнее для последующегог просмотра и анализа. Для этого после параметров командной строки следует указать знак ‘>’ и имя файла, например:

> windump -i2 –s 1024 > c:\output.log

Windump позволяет настроить формат вывода информации. Можно, к примеру, выводить информацию о перехваченных пакетах в hex-виде, можно в символьном виде, либо совместить разную информацию. Для этого используются ключи командной строки **-x, -xx, -X, -XX.**

-x – Выводит содержимое перехваченного пакета в hex-виде (заголовок протокола канального уровня не включается в вывод)

-xx – Выводит содержимое перехваченного пакета в hex-виде (заголовок протокола канального уровня также выводится)

-X – Выводит содержимое перехваченного пакета в hex- и ASCII-виде (заголовок протокола канального уровня не включается в вывод)

-XX – Выводит содержимое перехваченного пакета в hex- и ASCII-виде (заголовок протокола канального уровня также выводится)

-A – Выводит содержимое пакета в символьном(ASCII)-виде.

-e – Для каждого пакета выводит заголовок канального уровня в удобочитаемом виде.

-v – Выводит информацию по каждому полю IP-пакета в удобочитаемом виде

Последним необязательным параметром является выражение-фильтр, посредством которого можно перехватывать или выводить на экран или в файл только нужную информацию. В качестве параметра expression можно указывать любое выражение, которое удовлетворяет правилам его составления. Набор правил очень широк и позволяет гибко настраивать фильтр перехватываемых пакетов. Далее представлено правило формирования выражения и некоторые его элементы.

Выражение фильтра состоит из примитивов. Примитивы объединяются логическими операциями по правилам языка Си. Допуститмыми являются три типа примитивов:

type – квалификатор типа. В качестве квалификатора может быть использован **host**, **net , port** и **portrange.** Например: **host foo**, **net 128.3**, **port 20**, **portrange 6000-6008**.

direction – квалификатор направления. В качестве квалификатора может быть использован **src**, **dst**, **src or dst** и **src and dst**. Например, **src foo**, **dst net 128.3**, **src or dst port ftp-data**.

protocol – квалификатор протокола. В качестве квалификатора может быть использован **ether**, **fddi**, **tr**, **wlan**, **ip**, **ip6**, **arp**, **rarp**, **decnet**, **tcp** и **udp**. Например, **ether src foo, arp net 128.3, tcp port 21, udp portrange 7000-7009**.

Примитивы могут объединятся посредством следующих логических операций:

Отрицание ('**!**' или `**not**')

Объединение (`**&&**' или `**and**')

Альтернативы (`||' или `**or**')

Примеры использования выражений:

Вывод на экран всех пакетов, отправленных хосту CADNET:

> windump -i2 –s 1024 dst host CADNET

Вывод на экран всех пакетов, отправленных на TCP-порт 9110:

> windump -i2 –s 1024 dst port 9110

Вывод на экран в символьном виде всех пакетов, отправленных на хост CADNET на TCP-порт 8080.

windump –i2 -A dst port 8080 && dst host CADNET

Как уже было сказано, Windump имеет богатый набор примитивов для составления фильтра перехватываемых запросов. Например, можно выводить пакета только с определенным набором TCP-флагов, либо пакеты с размером определенного диапазона. Internet-ссылка на полное описание параметров дана выше.