Инженерный вестник Дона, №9 (2019)
ivdon.ru/ru/magazine/archive/n9y2019/6182

Сетевой трафик в операционных системах WINDOWS: сравнение и анализ его генерирования

К.А. Василенко, Е.А. Верещагина, Н.В. Абрамов, Д.О. Новинский

Дальневосточный федеральный университет, Владивосток

Аннотация: В статье анализируется сетевой трафик в операционных системах WINDOWS, а также дается описание его инструментов, позволяющих выявить определенную избыточность сетевой активности. Кроме того, авторами сделан сравнительный анализ наиболее распространённых программных продуктов, выполняющих функции мониторинга сетевого трафика.
Ключевые слова: операционная система, системы обнаружения, сетевой протокол, анализ сетевого трафика, сети, сниффер, трафик, сетевая активность.

На сегодняшний день процесс анализа сетевого трафика имеет немаловажное значение для любого IT-специалиста, что обусловлено постоянным ростом необходимой информации, передающейся по вычислительной сети.

Операционная система WINDOWS с каждым пакетом обновления увеличивает количество генерирования служебной информации, которая в свою очередь осуществляет дополнительную нагрузку на каналы связи [1].

В проведенном исследовании объектом является сетевой трафик, сгенерированный операционной системой, предметом исследования является анализ инструментов сетевого трафика для выявления избыточной сетевой активности.

Целью статьи стала реализация сравнительного анализа наиболее популярных программ по мониторингу сетевого трафика.

Для достижения цели необходимо решить следующие задачи:

- исследования рынка IT на предмет поиска программ для отслеживания сетевой активности;
- анализ характеристик снифферов;
- сравнительный анализ программ по выявленным характеристикам.

При ведении мониторинга, учета сетевого трафика и анализа за определенный период времени информации сетевых пакетов, были получены данные о текущих отклонениях и не исправностей компьютерной сети. Различные виды компьютерных угроз, вредоносных программ и атак бывает находят свое подтверждение при использовании статистики о сетевом трафике [2]. Анализ сетевого трафика также ведется различными системами обнаружения, предупреждения и предотвращения вторжения и взломов в целях безопасности локальной вычислительной сети [3].

В настоящее время наиболее актуальными анализаторами трафика являются: Wireshark и tcpdump [4].

Wireshark использует для захвата библиотеку libpcap, реализующую API pcap (packet capture). Эту библиотеку использует также стандартная утилита tcpdump. Файлы, которые были созданные в tcpdump, можно передавать Wireshark для последующего анализа. В Wireshark каждый класс пакетов, включая поврежденные пакеты, имеет свой оттенок цвета. Это помогает отслеживать в каком именно месте произошло повреждение или изменение [5].

Определение взаимодействующих логических сущностей ведут к установлению самих характеристик потока сетевого трафика [6]. Установим под логической сущностью потока IP-адреса и порты отправителя и получателя пакетов. Таким образом, определенный интервал времени станет фактором применения метода статистического анализа для перемещаемых сетевых пакетов, несущих в себе идентичные друг другу логические сущности, позволяющие вести более углубленный и детальный анализ статистики сетевых взаимодействий [7].

Преимуществом tcpdump является то, что он использует минимум системных ресурсов, какой только вообще возможен, так как в некоторых средах или на слабых ПК минимализм может оказаться единственным

приемлемым вариантом. К тому же, в отличие от Wireshark, у tcpdump куда меньшее количество проблем с безопасностью и уязвимостей [8].

Также преимуществом tcpdump является то, что при использовании инструмента, отображающего сетевой трафик более естественным (простым) способом, сложность анализа ложится непосредственно на человека, а не на приложение. Этот подход развивает понимание набора TCP/IP [9].

Таким образом, мониторинг сети позволяет улучшить работу сетевых устройств, снизить на них нагрузку. Сравнительные характеристики снифферов Wireshark и tcpdump отображена на рис.1 Кроме улучшения работы сетевых устройств, клиент получает рекомендации и советы по выбору программного обеспечения и технических параметров компьютеров для еще более эффективного управления сетью [10].

Характеристика	Tcpdump	WireShark
поддерживаются такие интерфейсы захвата: Ethernet, IEEE 802.11, PPP, и локальные виртуальные интерфейсы	+	+
пакеты можно отсевать по множеству параметров с помощью фильтров	+	+
все известные протоколы подсвечиваются в списке разными цветами	-	+
поддержка захвата трафика VoIP звонков	-	+
поддерживается расшифровка HTTPS трафика	-	+
расшифровка WEP, WPA трафика беспроводных сетей	-	+
отображение статистики нагрузки на сеть	-	+
просмотр содержимого пакетов для всех сетевых уровней	-	+
отображение времени отправки и получения пакетов	+	+
Графический интерфейс	-	+

Рис. 1. - Сравнительные характеристики снифферов Wireshark и tcpdump

Существенными преимуществами Wireshark, в сравнении с tcpdump, являются более удобная, интуитивно понятная форма вывода данных, а так же то, что Wireshark поддерживает более трехсот сетевых протоколов, что охватывает практически все когда-либо изобретенные виды сетей. Исходя из полученного анализа характеристик двух представленных программ по анализу трафика, можно сделать вывод о том, что наиболее актуальным программным приложением будет то, которое оптимизирует работу пользователя и увеличивает его производительность. По этой причине, подходящим под данные критерии является Wireshark.

Литература

1. Усманова И.М. Анализ сетевого трафика на сервере с помощью tshark URL: habrahabr.ru/company/selectel/blog/233837/ (Дата обращения: 25.11.2019).
2. Уилсон Эд. Мониторинг и анализ сетей. Методы выявления неисправностей. – М.: Лори, 2016. – 480 с.
3. Шепелев А.Н., Букатов А.А., Пыхалов А.В., Березовский А.Н. Анализ подходов и средств обработки сервисных журналов // Инженерный вестник Дона, 2013, №4, URL: ivdon.ru/magazine/archive/n4y2013/1966 (Дата обращения: 25.11.2019).
4. Бабенко Г.В., Белов С.В. Анализ трафика TCP/IP на основе методики допустимого порога и отклонения // Инженерный вестник Дона, 2011, №2. URL: ivdon.ru/magazine/archive/n2y2011/446 (Дата обращения: 25.11.2019).
5. Петров А.Г. Как пользоваться WireShark для анализа трафика URL: losst.ru/kak-polzovatsya-wireshark-dlya-analiza-trafika (Дата обращения: 25.11.2019).
6. Смирнов А.В. Руководство по захвату сетевого трафика. URL: blog.packet-foo.com/2016/11/the-network-capture-playbook-part-3-network-cards/(Дата обращения: 25.11.2019).

7. Гетман А.В. Фильтрация трафика. URL: asv0825.ru/sisadmin/18.html (Дата обращения: 25.11.2019).
8. Жуков Ф.М. Захват и анализ сетевого трафика в Windows Server 2008 R2 /2012. URL: blog.it-kb.ru/2013/10/15/capture-and-analyze-network-traffic-trace-on-windows-7-server-2008-r2-2012-via-netsh-and-network-monitor/ (Дата обращения: 25.11.2019).
9. Perlman R. Interconnections: Bridges & Routers. Addison-Wesley, USA, 1992. 245 p.
10. Oggerino C. High Availability Network Fundamentals. Cisco Press, USA, 2001. 327 p.

References

1. Usmanova I.M. Analiz setevogo trafika na servere s pomoshch'yu tshark. [Analysis of network traffic on the server using tshark]. URL: habrahabr.ru/company/selectel/blog/233837/ (Data accessed: 25.11.2019).
2. Uilson Ed. Monitoring i analiz setej. Metody` vy`yavleniya neispravnostej [Network monitoring and analysis. Methods of fault detection]. M.: Lori, 2016. 480 p.
3. Shepelev A.N., Bukatov A.A., Py`xalov A.V., Berezovskij A.N. Inzenernyj vestnik Dona, 2013, №4. URL: ivdon.ru/magazine/archive/n4y2013/1966 (Data accessed: 25.11.2019).
4. Babenko G.V., Belov S.V. Inzenernyj vestnik Dona, 2011, №2. URL: ivdon.ru/magazine/archive/n2y2011/446 (Data accessed 25.11.2019).
5. Petrov A.G. Kak pol'zovat'sya WireShark dlya analiza trafika [How to use WireShark to analyze traffic]. URL: losst.ru/kak-polzovatsya-wireshark-dlya-analiza-trafika (Data accessed: 25.11.2019).
6. Smirnov A.V. Rukovodstvo po zahvatu setevogo trafika. [Guide to capturing network traffic]. URL:blog.packet-foo.com/2016/11/the-network-capture-playbook-part-3-network-cards/ (Data accessed: 25.11.2019).

7. Getman A.V. Fil'traciya trafika. [Traffic filtering]. URL: asv0825.ru/sisadmin/18.html (Data accessed: 25.11.2019).
8. Zhukov F.M. Zahvat i analiz setevogo trafika v Windows Server 2008 R2 /2012. [Capturing and analyzing network traffic in Windows Server 2008 R2. 2012].URL:blog.it-kb.ru/2013/10/15/capture-and-analyze-network-traffic-trace-on windows-7-server-2008-r2-2012-via-netsh-and-network-monitor/ (Data accessed: 25.11.2019).
9. Perlman R. Interconnections: Bridges & Routers. Addison-Wesley, USA, 1992. 245 p.
10. Oggerino C. High Availability Network Fundamentals. Cisco Press, USA, 2001. 327 p.