ISSN 2658 – 7505
Выпуск №1, 2019
Электронный научный журнал «Вестник молодёжной науки России»

УДК 004.056

СИСТЕМЫ АНАЛИЗА СЕТЕВЫХ ПАКЕТОВ

Джавад Х. А., *Hassanjawad1986@gmail.com,* ***Хорошко М. Б.*** *clevermaks@yandex.ru*
Южно-Российский государственный политехнический университет (НПИ)
имени М.И. Платова, г. Новочеркасск

В данной статье рассмотрим системы, которые могут анализировать пакеты сети. Ведь большинство систем захвата трафика, так называемые сниферы, по результатам работы выдают пакеты, которые приходится анализировать вручную. Задача данной стати, это поиск и описание систем которые могут не просто анализировать трафик, но и искать уязвимости. Уязвимости могут быть разного характера – незащищенные сайты которые передают в открытом доступе логин и пароль. Почтовые клиента, где в результате перехвата можно получить доступ ко всей переписке. По результатам найденных уязвимостей, администратор сети уже будет принимать решение. Самый простой вариант – это закрыть доступ к ресурсу. Но данное решение не всегда оправдано. Возможно будет достаточно перенастройки пользовательских настроек – например смена протокола ftp на sftp.

SNIFFER AND ANALYSIS OF THE SECURITY OF WI-FI NETWORKS IN PUBLIC PLACES IN ROSTOV-ON-DON

Dhavad H. A., Horohko M.B.
Platov South-Russian State Polytechnic University (NPI), Novocherkassk

In this article, we'll look at systems that can analyze network packets. After all, most traffic capture systems, the so-called sniffers, on the basis of the work results in packages that have to be analyzed manually. The goal of this article is to find and describe systems that can not simply analyze traffic, but also look for vulnerabilities. Vulnerabilities can be of a different nature - unprotected sites that give public access to the login and password. Mail client, where as a result of the interception you can access all correspondence. Based on the results of the vulnerabilities found, the network administrator will already make a decision. The simplest option is to close the access to the resource. But this decision is not always justified. It may be enough to reconfigure user settings - for example, changing the ftp protocol to sftp.

С постоянно расширяющейся сферой Интернета и его приложений, масштабы сетей, передачи данных и безопасности данных также значительно возросли. Это привело к появлению сложных инструментов, которые хотя и полезны, но также широко используются киберпреступниками для прослушивания или получения незаконного доступа. Это относится к инструментам мониторинга сети и Packet Sniffing. Хотя они были разработаны, чтобы помочь сетевым администраторам лучше оценивать серверы, трафик и диагностировать проблемы, но они стали любимым инструментом хакеров для сканирования конкретной сети и обнаружения незащищенных данных. Хакеры White Hat используют эти инструменты для предотвращения таких атак со стороны преступников, поскольку они выявляют и отфильтровывают вредоносные пакеты и их источники. В этой статье мы тщательно сравнили наиболее широко используемые инструменты отслеживания пакетов и мониторинга сети.

Процесс захвата состоит из получения, прослушивания в сети для каждого транзитного кадра, независимо от его источника или назначения. Компьютер, отправляющий данные, называется источником, а компьютер, принимающий данные, является местом назначения. Для отправки данных через Интернет исходный компьютер должен сначала разбить данные на более мелкие части, известные как пакеты.

Обнаружение пакетов - это процесс сбора информации, передаваемой по сети [1]. Packet Sniffing в основном используется для управления сетью, мониторинга и этического взлома. Для выполнения сниффинга мы используем инструмент под названием пакетный сниффер. Анализатор пакетов, иногда называемый анализатором сети, который может использоваться сетевым администратором для мониторинга и устранения неполадок сетевого трафика.

Обзор программ. *SolarWinds* - это комплексный инструмент для мониторинга производительности, управления сбоями и доступности сети, помогающий гарантировать, что ваша сеть всегда работает с максимальной производительностью. Благодаря ультрасовременному настраиваемому веб-интерфейсу SolarWinds дает вам единое представление о производительности тысяч узлов и интерфейсов в вашей сети. На одной веб-странице вы можете перейти к любому элементу вашей сети, чтобы точно увидеть, что происходит в режиме реального времени.

Эти данные мониторинга производительности предупреждают вас о плохих сетевых условиях, таких как медленный трафик, потеря пакетов или поврежденные устройства.

С помощью SolarWinds вы также можете автоматически отслеживать и устанавливать оповещения о дисковом пространстве, загрузке ЦП и использовании памяти для сетевых устройств. Благодаря встроенной поддержке многих поставщиков и операционных систем SolarWinds гарантирует, что вы можете легко собирать и оповещать о состояниях, которые могут вызвать сбой сети или снижение производительности [2]. Работает только на окнах.

Tcpdump - это обычный анализатор пакетов, который запускается из командной строки. Это позволяет пользователю перехватывать и отображать TCP / IP и другие пакеты, передаваемые или принимаемые по сети, к которой подключен компьютер. Tcpdump работает в большинстве Unix-подобных операционных систем: Linux, Solaris, BSD и Mac OS.

Его также можно использовать для анализа самой сетевой инфраструктуры, определяя, происходит ли вся необходимая маршрутизация должным образом, что позволяет пользователю дополнительно изолировать источник проблемы. Также возможно использовать tcpdump для конкретной цели перехвата и отображения сообщений другого пользователя или компьютера [3]. Tcpdump также имеет некоторые ограничения, такие как Tcpdump также может сообщать только о том, что он находит в пакете. Если в пакете подделан IP-адрес, tcpdump не имеет возможности сообщать что-либо еще, а TcpDump очень экономичен с точки зрения памяти, поскольку его размер установочного файла составляет всего 484 КБ. TcpDump не имеет удобного графического интерфейса пользователя (GUI). Таким образом, пользователь должен изучить эти команды и ознакомиться с командной строкой, например, с экраном. Это ограничение может сыграть ключевую роль в том, чтобы не выбирать его.

Cain and Abel. Это программное обеспечение имеет странное название и противоречит замечательной широте задач, которые может выполнять программа. Cain & Abel - это инструмент для восстановления пароля для операционных систем Microsoft. Он позволяет легко восстанавливать пароли различного типа, прослушивая сеть, взламывая зашифрованные пароли с помощью атак по словарю,

перебором и криптоанализом. Программа не использует никаких программных уязвимостей или ошибок, которые не могли быть исправлены без особых усилий. Он охватывает некоторые аспекты / недостатки безопасности, присутствующие в стандартах протокола, методах аутентификации и механизмах кэширования; его основное назначение - упрощенное восстановление паролей и учетных данных из различных источников [4]. Доступно только для Windows.

Colasoft Capsa - еще один усовершенствованный сетевой анализатор. Тем не менее, его сильные функции доступны только после оплаты определенной цены. Он также может выполнять захват пакетов в реальном времени, мониторинг сети, анализ протоколов и решение проблем приложений. Он имеет довольно сильные встроенные функции, хорошо продуманный графический интерфейс, а также может захватывать как проводной, так и беспроводной трафик. Другими особенностями Colasoft Capsa являются анализ VOIP, оповещение о тревоге по электронной почте и аудио для проблем в сети, а также обеспечивает автоматический захват пакетов в течение заранее определенного времени. Аналогичным образом, еще одна особенность Capsa - это визуальные графики и матричные функции для точного сетевого взаимодействия и анализа протоколов [5].

Он не показывает общую веб-страницу, показывает как отдельные ссылки для отдельных файлов. Capsa Free - это отличное сочетание мощного мониторинга, глубокого декодирования пакетов, надежной диагностики сети, оповещения в режиме реального времени и тщательной отчетности, а также инновационные решения для многочисленных сетевых проблем [6]. И доступно только для окон.

Wireshark - это анализатор пакетов. Используется для устранения неполадок в сети, анализа. Первоначально названный Ethereal, в мае 2006 года проект был переименован в Wireshark из-за проблем с товарными знаками. Wireshark позволяет пользователю переводить сетевые интерфейсы, поддерживающие случайный режим, в этот режим, чтобы видеть весь трафик, видимый на этом интерфейсе, а не только трафик, адресованный одному из настроенных адресов интерфейса, и широковещательный / многоадресный трафик [7].

Когда вы что-то делаете в Интернете, например просматриваете веб-сайты, используете VoIP и т. Д., И данные всегда преобразуются в пакеты, когда они проходят через сетевой интерфейс или сетевую карту. Wireshark будет охотиться за этими пакетами на вашем уровне TCP / IP во время передачи, и он будет хранить и представлять эти данные в графическом интерфейсе. Возможно, Wireshark - один из лучших анализаторов пакетов с открытым исходным кодом, доступных на сегодняшний день для UNIX и Windows.

	Operating System	**User Interface**	**Software license**	**Disk usage**
WireShark	*Windows, MacOS, Unix*	*GUI*	*Free*	*81m*
TcpDump	Linux, MacOS, Unix and Windows	*CLI*	*Free*	*448kb*
Solarwinds Npm	*Windows*	*GUI*	*Not Free*	*To 20gb*
Cain and Abel	*Windows*	*GUI*	*Free*	*10mb*
Colasoft Capsa	*Windows*	*GUI*	*Not Free*	*32mb*

Заключение

Wireshark, Solarwinds, Colasoft Capsa, Cain и Abel имеют удобный интерфейс, отображающий информацию внутри пакетов значимым образом. С другой стороны, TCPdump не имеет графического интерфейса. Графический интерфейс помогает лучше понять инструменты. Чем лучше интерфейс, тем больше его используют. Труднее изучить TCPdump и его правила фильтрации, чем другие, потому что правила TCPdump сначала кажутся сложными. Colasoft Capsa имеет лучший интерфейс, включая поток пакетов в сети, отображаемый графически через матрицу, но это очень дорого, тогда как в Wireshark можно анализировать захват пакетов и создавать сравнительные графики с ограничениями протоколов, IP-адреса назначения и т. Д. С другой стороны Solarwinds использует большую емкость диска и не бесплатно. У Cain and Abel есть ограничения на дешифрование пакетов, но в TCPdump невозможно нарисовать один граф без использования стороннего инструмента. Пользователь получает информацию только в виде текстовых слов. Кроме того, чем больше инструмент является графическим, тем больше будут его системные требования.

Список цитируемой литературы

1. Qadeer M.A., Zahid M., Iqbal A., Siddiqui M.R “Network Analysis and Intrusion Detection Using Packet Sniffer ICCSN ' Second International Conference, 2010, Page(s): 313 – 317.
2. http://content.solarwinds.com/creative/pdf/datasheets/sw_npm_datasheet_0512.pdf.
3. Dulal C. Kar Felix Fuentes. Ethereal vs. tcpdump: A comparative study on packet sniffing tools for educational purpose. Journal of Computing Sciences in Colleges archive, Volume 20(4), pp 169-176, (2005).
4. 1Prof. Dept. Computer Science & Application, Chaudhary Devi Lal " Efficient Method for Preventing Password Sniffing Using MD5Algorithm" International Journal of Advanced Engineering Research and Science (IJAERS) Vol-3, Issue-3 , March- 2016] ISSN: 2349-6495.
5. Colasoft.com, (2001). Colasoft Capsa’s Official Website. [Online] Available at: http://www.colasoft.com/capsa/ [Accessed: 2nd March, 2016].
6. All about capsa [Online] Available www.colasoft.com.
7. A. Dabir, A. Matrawy, "Bottleneck Analysis of Traffic Monitoring Using Wireshark", 4th International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov. (2007), Page(s): 158- 162(2007).