УДК 004.77

Д. С. Слободяник

ВИКОРИСТАННЯ ПРОГРАМ-SNIFFER-ІВ ПРИ ДОСЛІДЖУВАННІ МЕРЕЖІ

Вінницький національний технічний університет

Анотація

В даній роботі описуються засоби аналізу мережевого трафіку (сніфери). Розглядаються можливості роботи основних програм-sniffer-ів WireShark Packet Sniffer, Capsa Packet Sniffer Free, SniffPass Password Sniffer, iTraffic Monitor. Зроблено висновки щодо виявлення кращих програм-sniffer-ів, які можна використовувати користувачам.

Ключові слова: Програма-sniffer, мережевий трафік, мережевий пакет, мережевий протокол.

Abstract

This paper describes the network traffic analysis tools (sniffers). The possibilities of major sniffer programs WireShark Packet Sniffer, Capsa Packet Sniffer Free, SniffPass Password Sniffer, iTraffic Monitor. Conclusions to identify the best sniffer-programs that users can use.

Keywords: sniffer-programs, network traffic, network packet network protocol.

Сучасний розвиток інформаційних технологій та збільшення вимог до використання мережевих ресурсів передбачає постійне дослідження інформаційних потоків з метою покращення їх ефективності. Особливу роль в цьому процесі займають програми дослідження стану трафіку мережі, які мають назву сніферів (від англ. Sniff - нюхати).

Оскільки існує досить значна кількість програм, які мають потрібну функціональність, то актуальною постає задача порівняння програм-sniffer-ів з точки зору можливостей дослідження мережевого трафіку .

В сучасному світі існує багато засобів для аналізу мережі. Тому доволі важко обрати потрібний засіб для вирішення поставленої задачі. Кожен з засобів має свої особливості. Деякі з них вже давно застарілі, інші ж лише набирають популярності.

Аналізатор трафіку (мережевий аналізатор, sniffer) являє собою комп'ютерну програму або частину комп'ютерного обладнання, що може перехоплювати і в подальшому аналізувати мережевий трафік. Аналізатор пакетів також може іноді декодувати і аналізувати мережевий трафік для вилучення корисної інформації. Така інформація може бути паролі або інші облікові дані, що передаються по мережі

Сніфери застосовуються як в благих, так і в деструктивних цілях. Аналіз трафіку, що пройшов через сніфер, дозволяє:

1. Виявити паразитний, вірусний і закільцований трафік, наявність якого збільшує завантаження мережного устаткування і каналів зв'язку.
2. Виявити в мережі шкідливе і несанкціоноване ПЗ, наприклад, мережеві сканери, троянські програми.
3. Перехопити будь-який незашифрований (а деколи і зашифрований) призначений для користувача трафік з метою отримання паролів і іншої інформації.
4. Локалізувати несправність мережі або помилку конфігурації мережних агентів .

Оскільки в «класичному» сніфері аналіз трафіку відбувається вручну, із застосуванням лише простих засобів автоматизації (аналіз протоколів, відновлення TCP-потоку), то він підходить для аналізу лише невеликих його обсягів [1].

Розглядаються такі безкоштовні програми-sniffer-и як WireShark Packet Sniffer, Capsa Packet Sniffer Free, SniffPass Password Sniffer, iTraffic Monitor. Розглянуто як загальну інформацію, так і специфічні особливості кожного з засобів.

WireShark Packet Sniffer - це крос-платформний аналізатор трафіку, і працює як на Unix, а також Windows. Постачається з графічним інтерфейсом, що робить його надзвичайно простим у

використанні. Працює в режимі реального часу, розшифровує пакети на основі їх протоколу, здатний виявляти і захоплювати VOIP дзвінки, а в деяких випадках навіть може відтворювати медіа. Дана програма може захоплювати сотні протоколів та відображати докладні дані протоколу, включаючи байтову інформацію [2].

Capsa Packet Sniffer Free хороший як для домашнього використання, так і в малому бізнесі. Працює в режимі реального часу. Дозволяє відстежувати до 50 IP-адрес одночасно, що корисно для мережевих адміністраторів. Можна здійснювати моніторинг поведінки мережі, мережеву діагностику для виявлення проблем мережі [3].

SniffPass Password Sniffer – фокусується на захопленні паролів з мережевого трафіку. При перехоплені паролю він миттєво відображає знайдену інформацію на екрані. Це відмінний спосіб знайти забуті паролі веб-сайтів. Легкий у використанні, зручний графічний інтерфейс. Підтримує мережеві протоколи POP3, IMAP4, SMTP, FTP, HTTP. Працює на Windows 98, Windows Millenium, Windows NT, Windows 2000, Windows XP, Windows 2003 і Windows Vista. Зберігає власні налаштування у файл, а не робить запис в реєстр. Сумісний з драйверами Microsoft Network. Має можливість імпорту з tcpdump/libpcap файлу. [4].

iTraffic Monitor – надає в реальному часі інформацію про вашу мережеву активність. Відображає завантаження мережі та мережеву активність у вигляді графіків. Можна переглядати звіти про щоденну, щомісячну, щорічну мережеву активність Важливою особливістю є те, що дана програма є передовим інструментом фільтрації мережі. Він дозволяє фільтрувати ваш локальний мережевий трафік через конкретні IP адреси. Не багато додатків існує, щоб надавати таку можливість. Зазвичай, вони дорого вартісні. Даний продукт є безкоштовним. [5].

В результаті, було виявлено, що кожна з порівнюваних програм має свої особливості. І використання кожної з них залежить від цілей, які потрібно реалізувати. Проте, найбільш потужними та функціональними є WireShark Packet Sniffer та Capsa Packet Sniffer Free. Хоч інші програми теж можуть успішно використовуватись.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ / REFERENCES

1. Аналізатор трафіку [Електронний ресурс]. Режим доступу: URL: https://uk.wikipedia.org/wiki/Аналізатор_трафіку. - Назва з екрану.
2. WireShark [Електронний ресурс]. Режим доступу: URL: http://www.ilovefreesoftware.com/04/windows/security/download-wireshark-best-free-network-protocol-analyzer.html. - Назва з екрану.
3. Capsa Packet Sniffer Free [Електронний ресурс]. Режим доступу: URL: http://www.colasoft.com/capsa-free/. - Назва з екрану.
4. SniffPass Password Sniffer [Електронний ресурс]. Режим доступу:URL:http://www.ilovefreesoftware.com/06/windows/internet/network/sniffpass-password-sniffer-free-password-sniffer.html. - Назва з екрану.
5. iTraffic Monitor [Електронний ресурс]. Режим доступу: URL: http://www.ilovefreesoftware.com/17/windows/free-software-monitor-network-activity-itraffic-monitor.html. - Назва з екрану.

Слободяник Денис Сергійович – студент групи 1ПІ-13б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: d.slobodyanyk@gmail.com.

Науковий керівник: ***Катєльніков Денис Іванович*** – кандидат технічних наук, доцент, Вінницький національний технічний університет. E-mail: fuzzy2dik@gmail.com.

Slobodianyk Denys S. - Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: d.slobodyanyk@gmail.com.

Supervisor– ***Katielnikov Denys Ivanovych***, PhD, Associate Professor of Software Engineering Department, Vinnytsia National Technical University, Vinnytsia, E-mail: fuzzy2dik@gmail.com.