УДК 004.725.5(045)

Гніденко І.А.,
Воробйов І.Є.

АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ ЛОКАЛЬНОЇ МЕРЕЖІ ЗА ДОПОМОГОЮ ПРОГРАМНИХ СНІФЕРІВ

Національний авіаційний університет

irusya.gnidenko@gmail.com
ilya.vorobyev93@gmail.com

Проведено огляд програмних сніферів мережевого трафіку. Визначено їх характеристики та специфічні особливості. Здійснено аналіз мережевого трафіку локальної мережі за допомогою програми Wireshark, *яка має найбільше функціональних можливостей*

Ключові слова: сніфер, мережевий трафік, локальна мережа

Вступ

На сьогоднішній день аналіз мережевого трафіку в мережі досить актуальний за рахунок швидкого вдосконалення мережевої галузі, а саме створення нових мережних протоколів прикладного рівня [1, 2]. Поява великої кількості комп'ютерів привело до створення інформаційних спільнот, а також до проектування та використання різних інформаційних мереж (локальних, регіональних, глобальних) з багатьма користувачами. Для забезпечення безпеки даним виникла необхідність застосувати програмне забезпечення, за допомогою якого можна здійснити: аналіз мережевого трафіку для виявлення проблем та аналіз статистики мережевих даних. Для успішної роботи та виявлення всіх проблем аналіз трафіку повинен бути виявлений повністю, щоб забезпечити всі методи аналізу для ефективного результату. Для того, щоб захопити трафік необхідно використати сніфери - програми або програмно-апаратні пристрої, призначені для перехоплення мережевого трафіку в мережі.

Постановка задачі

Метою даної статті є порівняльний огляд існуючих програмних сніферів та аналіз мережевого трафіку локальної мережі за допомогою програми, яка має найбільше функціональних можливостей.

Основна частина

Сніфер – це програма або програмно-апаратний пристрій, який застосовується для захоплення і докладного аналізу перехопленого трафіку або окремого сегменту мережі. В процесі захоплення всіх потоків, аналізатор захоплює і записує всі пакети, отримані з інтернет-трафіку. У разі докладного і інформативного аналізу відбувається декодування пакетів з зашифрованої форми подання в ту, яку можна прочитати.

Існує два основних види роботи сніферів в комп'ютерних мережах: за місцем розташування (в певній мережі сніфер захоплює трафік і відправляє в іншу мережу або в зворотну сторону; якщо ж він встановлений на маршрутизаторі конкретного провайдера вашого інтернету, то є можливість відстеження трафіку користувачів цієї мережі) та на крайовому вузлі.

Аналізатор трафіку, або сніфер - мережевий аналізатор трафіку, програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіку, призначеного для інших вузлів.

Аналіз трафіку, який пройшов через сніфер дозволяє:

- виявити паразитний, вірусний і закільцьований трафік, наявність якого збільшує завантаження мережевого обладнання та каналів зв'язку (сніфери тут малоефективні; як правило, для цих цілей використовують збір різноманітної стати-

стики серверами і активним мережевим обладнанням і її подальший аналіз);

- перехопити будь-який незашифрований (а часом і зашифрований) призначений для користувача трафік з метою отримання паролів і іншої інформації;

- локалізувати несправність мережі або помилку конфігурації мережевих агентів (для цієї мети сніфери часто застосовуються системними адміністраторами).

Наразі існує значна кількість програмних продуктів, які призначені для аналізу мережевого трафіку. Розглянемо найбільш поширені з них, та визначимо програмний продукт з найбільшим функціоналом.

Wireshark - програма-аналізатор трафіку для комп'ютерних мереж Ethernet і деяких інших. Має графічний користувальницький інтерфейс. Wireshark - це програма, яка «знає» структуру самих різних мережевих протоколів, і тому дозволяє розібрати мережевий пакет, відображаючи значення кожного поля протоколу будь-якого рівня [3, 4]. Оскільки для захоплення пакетів використовується pcap, існує можливість захоплення даних тільки з тих мереж, які підтримуються цією бібліотекою. Проте, Wireshark уміє працювати з безліччю форматів вхідних даних, відповідно, можна відкривати файли даних, захоплених іншими програмами, що розширює можливості захоплення.

Iris Network Traffic Analyzer крім стандартних функцій збору, фільтрації та пошуку пакетів, а також побудови звітів, пропонує унікальні можливості для реконструювання даних. Iris The Network Traffic Analyzer допомагає детально відтворити сеанси роботи користувачів з різними web-ресурсами і навіть дозволяє імітувати відправку паролів для доступу до захищених web-серверів за допомогою cookies. Унікальна технологія реконструювання даних, реалізована в модулі дешифрування (decode module), перетворює сотні зібраних двійкових мережевих пакетів у звичні для ока електронні листи, web-сторінки і ін. EEye Iris дозволяє проглядати незашифровані повідомлення web-пошти та програм миттєвого обміну повідомленнями, розширюючи можливості наявних засобів моніторингу та аудита. Аналізатор пакетів eEye Iris дозволяє зафіксувати різні деталі атаки, такі як дата і час, IP-адреси і DNS-імена комп'ютерів хакера і «жертви», а також використані порти.

Ethernet Internet traffic Statistic відображає кількість отриманих та прийнятих даних (в байтах - всього і за останню сесію), а також швидкість підключення. Для наочності зібрані дані відображаються в режимі реального часу на графіку. Працює без інсталяції, інтерфейс - російська та англійська мови. Утиліта для контролю за ступенем мережевої активності - показує кількість отриманих та відправлених даних, ведучи статистику за сесію, день, тиждень і місяць.

CommTraffic – мережева утиліта для збору, обробки і відображення статистики інтернет-трафіку через модемне (dial-up) або виділене з'єднання. При моніторингу сегмента локальної мережі, CommTraffic показує інтернет-трафік для кожного комп'ютера в сегменті. CommTraffic включає в себе зрозумілий користувачеві інтерфейс, який легко настроїти та показує статистику роботи мережі у вигляді графіків і цифр.

З числа розглянутих програм-аналізаторів мережевого трафіку хотілося б виділити Wireshark, яка має більшу кількість функціональних можливостей. Дана програма надає можливість аналізу мережевих пакетів і розбір мережевих протоколів будь-якого рівня, а також інформативний розбір всього трафіку, що проходить в мережі, використовуючи мережеву карту в режимі promiscuous mode. Здатний аналізувати структуру всіх доступних мережевих протоколів і здійснювати їх фільтрацію за конкретними параметрами.

Для здійснення повноцінного аналіз мережевого трафіку локальної мережі з використанням wireshark, необхідно виконати наступні дії: запуск і настроювання програми аналізатора Wireshark; захоплення трафіку; перегляд захопленого трафіку; аналіз

захоплених пакетів; аналіз присутніх протоколів; знаходження пакетів з помилками; геопозіція ір джерел; перехоплення файлів, що скачали з захопленого трафіку; відновлення введених логінів і паролів.

Після запуску та налаштування програми аналізатора Wireshark активуємо захоплення мережевого трафіку локальної мережі. Програма аналізатор Wireshark безперервно відображає одержувані пакети з мережевого інтерфейсу. Для здійснення ефективного аналізу, необхідно працювати з захопленим трафіком в пасивному режимі. Необхідна інформація для виконання наступних кроків аналізу представлена в головній панелі інтерфейсу програми Wireshark, в якій знаходяться основні дані про захоплених пакетах. Основні дані мережевих пакетів в головній панелі (рис. 1): No - порядковий номер захопленого пакета; Time - час захоплення пакета в секундах; Source - мережеву адресу відправника; Destination - мережеву адресу одержувача; Protocol - протокол, що використовується; Length - довжина пакетаInfo - інформація про захопленому пакеті.

Рис. 1. Інформація про захоплені пакети

Для аналізу необхідно відобразити статистичні дані по захопленому мережевому трафіку в табл. 1, щоб оперувати цими значеннями в наступних етапах виконання аналізу.

Таблиця 1. Статистичні дані захопленого трафіку

Характеристика	Значення
First packet/Початок захоплення	2017-09-13 23:23:24
Last packet/ Останній захоплений пакет	2017-09-13 23:59:51
Elapsed/Час захоплення, хв.	00:36:28
Packets/Захопленні пакети	75133
Packets size/Розмір всіх пакетів, Мбайт	68 Mb
Average kbytes/s / Середня швидкість пакетів	67 kbytes/s
Average kbits/s / Середня швидкість	538 kbit/s

Використання Wireshark дає можливість отримання інформації про розподіл трафіку, необхідного для інтерпретації протоколів. Для цього необхідно впорядкувати весь захоплений трафік за наявністю різних протоколів та представити це у табл.2.

Таблиця 2. Протоколи, які використані в захоплених пакетах

Protocol /Протокол	Packets/ Пакети, kbit	Packets Size byte/ Розмір всіх пакетів	Average kbits/s/ Середня швидкість
Ipv6	796	72940	591
Ipv4	60635,7	6600731	534
UDP	678	107824	873
DNS	504	99700	808
TCP	16426,3	63665319	534
HTP	820	548548	444
ARP	5273	315822	456
Всього	75133 пакетів	71303168 Byte	

Для візуального представлення захоплених пакетів необхідно використовувати такий інструмент як Wireshark IO Graphs, в якому можна відобразити появу захоплених пакетів в залежності від усього часу захоплення (рис. 2). На даному графіку представлена поява пакетів, які відносяться до чотирьох основних протоколів мережі. На графіку видно, що більшість

пакетів належать протоколу IP [7]. Не важко побачити, що захоплення пакетів на конкретному проміжку часу нерівномірне, а стрибкоподібне, пояснюється це тим, що швидкість з'єднання з мережею інтернет не постійна.

У процесі аналізу мережевого трафіку локальної мережі за допомогою системного інструменту можна визначити наявність пакетів з помилками або попередженнями [5-6]. Для цього існує спеціальний інструмент, передбачений Wireshark. Expert Information - журнал в якому відображені помилки, попередження, примітки, викликані мережевими «аномаліями». (рис. 3).

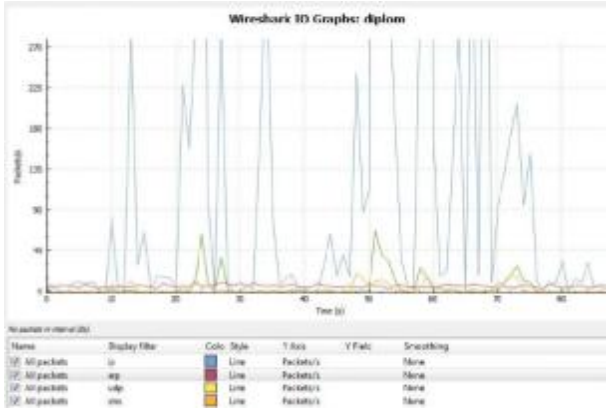

Рис. 2. Графічне представлення захоплення пакетів

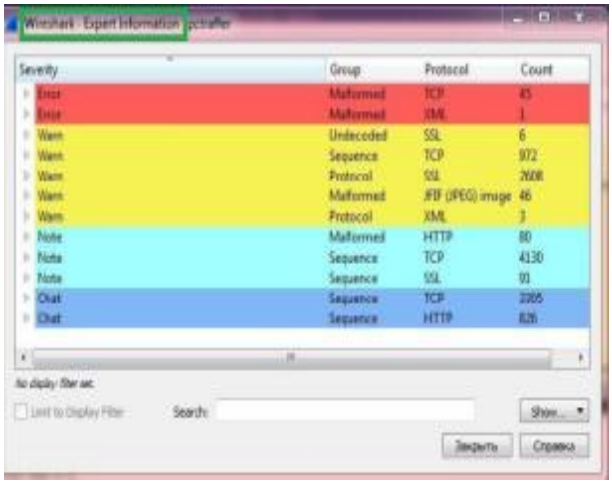

Рис. 3. Expert information

Одним з корисних інструментів в Wireshark є GeoIp Database. Даний інструмент дозволяє додати додаткову інформацію по захопленим пакетам. Додатковою інформацією буде прикріплення до кожного захопленого пакету інформації про ip адресу, а саме його місце розташування на карті. Це дає можливість дізнатися звідки був отриманий пакет, з якої країни, адреса, власник ip адреси і його місце розташування на карті.

Висновки

В результаті дослідження було проведено огляд програмних сніферів мережевого трафіку. Було визначено їх характеристики та притаманні їм особливості. Був зроблений аналіз мережевого трафіку локальної мережі за допомогою програми Wireshark, яка в ході аналізу була визначена як та, що має найбільше функціональних можливостей. А саме: можливість фіксації пакетів в мережевому сегменті; розшифровка пакетів; захоплення трафіку в реальному часі; підтримка багатьох протоколів; збереження дампов трафіку; фільтрація пакетів; надавати статистику про трафік.

Список літератури

1. А.Н. Андрончик, В.В. Богданов, Н.А. Домуховский, А.С. Защита информации в компьютерных сетях. 2008. – 248 с.

2. Таненбаум Э., Уэзеролл Д. Т18 Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. – 32 с.

3. Orebaugh Angela, Wireshark network protocol analyzer, 2006. – 450 с.

4. Стивен Норткат, Джуди Новак, Обнаружение нарушений безопасности в сетях (3-е издание), 2003. – 356 с.

5. Досталек Л., Кабелова А. TCP/IP и DNS в теории и на практике. Полное руководство. - Наука и техника, 2006. – 608 с.

6. Мамаев М. Телекоммуникационные технологии (Сети TCP/IP). Учебное пособие. Владивосток. 2001, v3.

7. Семенов Ю.А. Протоколы Internet. Энциклопедия. — М.: Горячая линия – Телеком, 2001. – 1100 с.

Статтю подано до редакції 19.09.2017