Технічні науки

УДК 004.9

Авксентьєва Іванна Олегівна

студентка

Інституту прикладного системного аналізу

Національного технічного університету України

«Київський політехнічний інститут імені Ігоря Сікорського»

Авксентьева Иванна Олеговна

студентка

Института прикладного системного анализа

Национального технического университета Украины

«Киевский политехнический институт имени Игоря Сикорского»

Avksentieva Ivanna

Student of the

Institute of applied systems analysis of the

National technical university of Ukraine

"Ihor Sikorskiy Kyiv Politechnical Institute"

Науковий керівник:

Кухарев Сергій Олександрович

асистент

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

ПАКЕТНІ СНІФЕРИ
ПАКЕТНЫЕ СНИФФЕРЫ
PACKET SNIFFERS

Анотація. *Висвітлено застосування та можливості сніферних пакетів, наведено приклади деяких з них та їх використання.*

Ключові слова: *сніфери, трафік,мережа, аналізатори.*

Аннотация. *Показано применение и возможности снифферных пакетов, приведены примеры некоторых из них и их использования.*

Ключевые слова: *снифферы, трафик, сеть, анализаторы.*

Summary. *The application and modalities of sniffer packages are covered, examples of some of them and possibilities of their use are given.*

Keywords: *sniffers, traffic, network, analyzers.*

Сніферний пакет - це або програмний, або апаратний інструмент для перехоплення, реєстрації та аналізу мережевого трафіку та даних. Ці інструменти допомагають визначити, класифікувати та усунути неполадки мережевого трафіку за типом програми, джерелом та пунктом призначення. На ринку є різноманітні інструменти, більшість з яких покладаються на інтерфейси прикладних програм (API), відомі як pcap (для Unix-подібних систем) або libcap (для систем Windows) для захоплення мережевого трафіку. Тоді найкращі сніфери пакетів аналізують ці дані, що дозволяє вам точно визначити джерело проблеми та не допустити її в майбутньому [1].

Щоб по-справжньому зрозуміти важливість сніфферів , важливо розуміти як відбувається маршрутизація в Інтернеті. Почнемо з початку. Кожен електронний лист, який ви надсилаєте, відкрита веб-сторінку та файл, яким ви ділитесь, поширюється в Інтернеті як тисячі маленьких керованих фрагментів, відомих як пакети даних. Ці пакети передаються через стек протоколів, відомий як протокол управління передачею / протокол Інтернету (TCP / IP). TCP / IP розбивається на чотири шари: рівень протоколу додатків, рівень протоколу управління передачею (TCP), рівень інтернет-протоколу (IP) та апаратний рівень [2].

Кожен пакет переміщується через рівень програми вашої мережі до рівня TCP, де йому присвоєний номер порту. Далі, пакет переходить на IP-

рівень і отримує свою цільову IP-адресу. Як тільки пакет має номер порту та IP-адресу, він може бути відправлений через Інтернет. Надсилання здійснюється через апаратний рівень, який перетворює пакетні дані в мережеві сигнали. Коли пакет прибуває до місця призначення, дані, які використовуються для маршрутизації пакету (номер порту, IP-адреса тощо), видаляються, і пакет рухається далі через стек протоколів нової мережі. Після досягнення вершини він збирається в первісну форму .

Як працюють пакетні сніфери ?

Пакетні сніфери працюють, перехоплюючи дані про трафік під час проходження по дротовій або бездротовій мережі та копіюючи їх у файл. Це відомо як захоплення пакетів. Хоча комп'ютери, як правило, розроблені для того, щоб ігнорувати ступінь трафікової активності від інших комп'ютерів, пакетні сніфери це перетворюють. При встановленні програмного забезпечення, мережева карта інтерфейсу (NIC) - інтерфейс між вашим комп'ютером та мережею - повинна бути встановлена в розрядний режим. Це дає змогу комп'ютеру зафіксувати та обробити через sniffer пакет все, що потрапляє в мережу.

Що можна захопити, залежить від типу мережі. Для дротових мереж конфігурація мережевих комутаторів, які відповідають за централізацію зв'язку з декількох підключених пристроїв, визначає, чи може мережевий сніфер бачити трафік у всій мережі або лише на її частині. У бездротових мережах інструменти збору пакетів зазвичай можуть захоплювати лише один канал одночасно, якщо хост-комп'ютер не має безлічі бездротових інтерфейсів.

Отже, у чому сенс аналізаторів пакетів? Сніффер може допомогти вам орієнтуватися на нові ресурси при розширенні пропускної спроможності мережі, керуванні пропускною здатністю, підвищенням ефективності, забезпеченням ділових послуг, підвищенням безпеки та покращенням роботи кінцевих користувачів. Що стосується великих та малих компаній,

щоденні завдання можуть бути негайно зірвані проблемами ефективності, пов'язаними з мережею, додатком чи обома. Щоб відновити роботу їхньої компанії, систематики повинні мати можливість швидко визначити першопричину. Оскільки sniffers пакетів переглядають та збирають інформацію для всього трафіку по всій мережі, вони можуть оцінювати критичні шляхи мережі, щоб допомогти адміністраторам визначити, що програма чи мережа є причиною поганого досвіду користувачів. З цією інформацією, адміністратори краще оснащені для визначення та вирішення походження проблеми.

Коли користувачі повідомляють про повільність, адміністратори можуть використовувати аналіз PCAP для вимірювання часу реакції в мережі - також відомий як затримка мережевого шляху - та визначати кількість часу, необхідний для переходу пакета через мережевий шлях від відправника до одержувача. Це дозволяє адміністраторам швидко визначити причину уповільнення та виявити постраждалі програми, тому вони можуть вжити заходів.

Проаналізуйте трафік за типом. Оцінюючи проблеми з мережею та додатками, першочергове значення має трафік у вашій мережі. За допомогою правильного аналізатора IP-sniffer та пакетів трафік класифікується на типи на основі IP-адрес сервера призначення, використовуваних портів та вимірювання загального та відносного обсягу трафіку для кожного типу. Це дає вам змогу виявити надмірний рівень некомерційного трафіку (наприклад, соціальних медіа та зовнішнього веб-серфінгу), який може знадобитися відфільтрувати чи іншим чином усунути. Ви також можете визначити трафік, що протікає через мережеве посилання, а також трафік на конкретні сервери або програми для цілей управління ємністю.

Поліпшення пропускної здатності. Коли користувачі скаржаться на те, що «мережа повільна» або «Інтернет знижується», продуктивність

припиняється, знижуючи рентабельність інвестицій . Щоб виправити цю помилку , вам потрібно зрозуміти, як та ким використовується пропускна здатність мережі. Сніфер пакету Wi-Fi може отримати показники продуктивності для автономних точок доступу, бездротових контролерів та клієнтів. Багато з них також пропонують моніторинг несправностей, продуктивності та доступності мережі, кореляцію даних між стековим стеком, аналіз мережевого шляху скакання та багато іншого, щоб допомогти вам виявити потенційні проблеми та мінімізувати час простою мережі.

Поліпшення безпеки. Великий обсяг вихідного трафіку може означати, що хакер використовує ваші програми, або для спілкування зовні, або для передачі великої кількості даних.

Пакети сніферів ManageEngine NetFlow Analyzer

ManageEngine пропонує sniffer пакетів у своєму інструменті NetFlow Analyzer, який можна встановити в Windows та Linux. NetFlow Analyzer - це повне програмне забезпечення для аналізу трафіку, що використовує технології потоку, щоб надати вашій команді поглиблене уявлення про продуктивність мережі та схему руху трафіку. Програмне забезпечення використовує надбудову DPI, щоб визначити, чи лежить в корені проблеми мережа чи додаток, що дозволяє вам покласти край проблемам продуктивності, перш ніж вони кардинально впливають на кінцевого користувача. Якщо проблема стосується групи кінцевих користувачів, NetFlow Analyzer дозволяє витягнути список постраждалих користувачів, щоб ви могли повідомити їх, що рішення в пошуці [3].

Для того, щоб зробити аналіз DPI на крок далі, NetFlow Analyzer надає інформаційну панель часу відгуку, що містить графіки для обсягів трафіку на основі верхніх додатків, надаючи необхідні деталі для усунення проблем з пропускною здатністю з першого погляду. Після того, як ви ідентифікуєте додаток та / або користувача, напружуючи свою пропускну здатність, NetFlow Analyzer надає можливості регулювання у формі формування

трафіку (також відомого як формування пакету). Формування трафіку - це технологія управління пропускною здатністю для затримки потоку певних типів мережевих пакетів для забезпечення продуктивності мережі для додатків з більш високим пріоритетом.

NetFlow Analyzer також пропонує деякі функції звітування. Завдяки функції звіту про розмови, sysadmins може детальніше зрозуміти розмову між основними користувачами та додатками, тим самим допомагаючи запобігти майбутнім проблемам. У цьому випадку звіт допомагає виявити тенденції та повторювані проблеми, тож ви можете вжити заходів, щоб не допустити їх повторення.

Існує дві версії NetFlow Analyzer: видання Essential та видання Enterprise. Однак DPI вважається доповненням для обох.

Wireshark

Wireshark існує вже декілька десятиліть і допомагає встановити стандарт для аналізу мережевих протоколів. Wireshark - це абсолютно безкоштовний інструмент з відкритим кодом, який переноситься майже на всі мережеві операційні системи, включаючи Windows, Linux, macOS, Solaris, FreeBSD та NetBSD. На сьогоднішній день Wireshark залишається організацією, яка керується волонтерами, підкріпленою кількома значними спонсорськими організаціями.Програма-аналізатор трафіку для комп'ютерних мереж Ethernet і деяких інших. Має графічний 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 [4].

Інструмент Wireshark відомий як захопленням даних, так і можливостями їх аналізу. Ви можете застосувати фільтри, щоб обмежити обсяг даних, які збирає Wireshark, або просто дозволити їм збирати весь трафік, що проходить через обрану мережу. Що важливо, він може збирати дані лише на сервері з встановленим робочим столом. Оскільки настільні

ПК на серверах нечасті, багато системних адміністраторів обирають використовувати tcpdump або WinDump для збору трафіку у файл, який вони завантажують у Wireshark для глибокого аналізу.

Незалежно від того, використовуєте ви Wireshark чи ні для збору даних, ви все одно можете використовувати його динамічний набір фільтрів для домашнього введення точного набору інформації, яка вас цікавить. Однією з особливостей фільтра, яка відрізняє Wireshark від пакета, є його здатність слідкувати за потоком даних. Наприклад, якщо ви хочете переглянути лише IP-адресу Google, ви можете натиснути правою кнопкою миші та вибрати "Слідувати", а потім "Потік TCP", щоб переглянути всю історію. Окрім своїх можливостей фільтрації, Wireshark широко відомий за його багатий аналіз VoIP, декомпресію gzip, зчитування даних в Ethernet та підтримку дешифрування для багатьох протоколів, включаючи IPsec, WPA та WPA2 та SNMPv3.

Література

1. Що таке сніфер? URL: https://www.avg.com/en/signal/what-is-sniffer (дата звернення: 13.05.2020) [англійською]
2. Стівен Норткат, Джуді Новак, Знаходження порушень безпеки в мережі (3-є видання), 2003. 356 с.
3. Кращі 10 сніферних пакетів та їх інструментів у 2020 URL: https://www.dnsstuff.com/packet-sniffers (дата звернення: 13.05.2020) [англійською]
4. Оребо Анджела, Аналізатор мережевих протоколів Wireshark, 2006. 450 с.

References

1. What is a sniffer? URL: https://www.avg.com/en/signal/what-is-sniffer (data zvernennia: 13.05.2020)

2. Stephen Northcat, Judy Nowak, Network Security Discovery (3rd Edition), 2003. 356 p.
3. Best 10 Packet Sniffer and Capture Tools in 2020 URL: https://www.dnsstuff.com/packet-sniffers (data zvernennia: 13.05.2020)
4. Orebaugh Angela ,Wireshark network protocol analyzer, 2006. 450 p.