Запис в журнал безпеки проводиться лише системними компонентами, коди подій однозначно ідентифікують події. Журнал подій Безпека є важливим джерелом інформації при розслідуванні інцидентів порушення безпеки і його аналіз актуальний для адміністраторів безпеки, фахівців з інформаційної безпеки і фахівців по цифровій криміналістичної експертизи.

ЛІТЕРАТУРА

1. Оливер Ибе, Компьютерные сети и службы удаленного доступа/Ибе Оливер -М: ДМК Пресс, 2019- 336 с.
2. Журнал роботи WindowsEventLog і системи оповіщення. URL: https://habr.com/ru/post/65652/.
3. Тейлор Дейв, Сценарії командної оболочки/ Дейв Тейлор-М: СПБ: Питер ,2017- 448 с.
4. Системний журнал повідомлень. URL: https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.html.

Краснобокий Р. С.,
Криворізький національний університет
Музика І. О.,
к.т.н., доцент, Криворізький національний університет

ЛОКАЛЬНА КОМП'ЮТЕРНА МЕРЕЖА ІНТЕРНЕТ-СЕРВІС ПРОВАЙДЕРУ З ПОКРАЩЕНОЮ НАДІЙНІСТЮ ПЕРЕДАЧІ ДАНИХ

Проведено аналіз проблеми колізії хеш-сум MAC-адрес у мережі. Наведено вірогідність виникнення колізії. Розглянуто проблему переповнення буферу комутатора. Запропоновано рішення щодо вирішення порушених питань та покращення послуг інтернет-сервіс провайдера.

На сьогоднішній день, інтернет є невід'ємною частиною людства, оскільки він не тільки спрощує життя, але й впливає на нього. Інтернет не має чіткої структури, однак умовним центром можна назвати 13 [1] кореневих DNS серверів, а інтернет-сервіс провайдери в свою чергу надають доступ до інтернету звичайним користувачам.

Мета – досягти максимально можливої надійності передачі даних та високої якості інтернет з'єднання для кінцевого користувача.

Проблема – Погіршення надійності передачі даних і як наслідок – деградація сервісу для кінцевого користувача.

Причина – Наявність хеш-колізій в мережі. Оскільки для економії пам'яті комутатор зберігає відомі MAC-адреси у вигляді хеш-суми адреси і номера vlan, при великих кількостях адрес існує ймовірність однакової хеш-суми для двох різних пар адреси і номера vlan, що в свою чергу викликає потрапляння «чужого» трафіку на інтерфейс кінцевого користувача, тим самим викликає погіршення якості обслуговування.

Переповнення буфера комутатора. Так само проблемою є те, що на рівні доступу використовуються комутатори з пропускною спроможностю до 1Гбіт / с, в свою чергу на рівні розподілу використовуються комутатори, із пропускною здатністю до 10Гбіт / с. У зв'язку з цим, комутатор рівня розподілу може відправляти дані зі швидкістю, що перевищує робочу швидкість комутатора рівня доступу, тому останньому доведеться поглинати додатковий трафік, заповнюючи буфер і в разі переповнення, відкидати пакети, які він не встигає обробити, що тягне за собою втрату пакетів і як наслідок погіршення якості обслуговування.

Проблематика хеш-колізій в комутаторі побічно розглядалася в статті «Practical Hash-Based Anonymity for MAC Addresses» [2], де говорилося про те, що ймовірність колізії може залежати від алгоритму шифрування і кількості біт вихідний комбінації. Згідно з їхніми дослідженнями, довжина вихідної комбінації хеш-функції з урахуванням використання алгоритму шифрування Argon2d, для одного мільйона MAC-адрес повинна бути мінімум 21 біт, для збереження ймовірності колізій менше 1%. На рисунку 1 зображена гістаграма кількості біт вихідний комбінації хеш-функції для m MAC адрес для досягнення вероятнсоті колізії p, і графік ймовірності виникнення колізії p при вхідному кількості MAC-адрес m і кількості біт вихідний комбінації n.

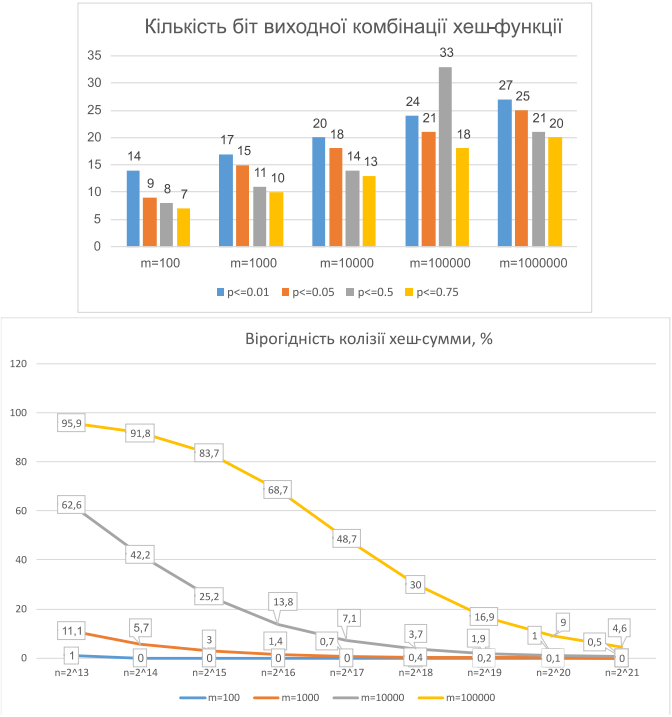

Рис.1 Кількість біт виходної комбінації хеш-функції та вірогідність колізії

Оскільки MAC-адреса хешується в парі з номером vlan, мережеві адміністратори можуть виділяти кожному користувачеві унікальний номер vlan, тим самим вносячи більше даних для хешування, тим самим зменшуючи ймовірність збігу хеш-суми для двох різних пар значень. Додатково пропоную застосувати технологію qinq, що дозволяє створювати ще 4096 vlan всередені одного vlan, що позитивно вплияє на вірогідність колізії

Рішення другої проблеми зазвичай здійснюють шляхом обмеження смуги пропускання до оптимальних значень. Для цього існують два способи: полісінг і шейпінг, де перший, в свою чергу зрізає весь трафік, понад обмеження на смузі пропускання, другий же зберігає надлишок до буферу, зберігаючи всі дані. Для даного випадку пропоную використовувати полісер і налаштувати алгоритм Token Bucket Single Rate - Three Color Marking (sr-TCM) [3], що дозволить

обмежити пропускну здатність до потрібного значення, при цьому дозволяючи сплески трафіку.

ВИСНОВКИ

Таким чином було проведено аналіз проблеми покращення надійності передачі даних у мереж інтернет-сервіс провайдеру. Для зведення до мінімуму хеш-колізій у мережі за технології qinq кожному користувачу надається vlan in vlan. Додатково на смугу пропускання що з'єднує рівень доступу та розподілу встановлюється полісер із алгоритмом sr-TCM.

ЛІТЕРАТУРА

1. Conrad D. Краткий обзор системы корневых серверов [Електронний ресурс] / David Conrad. – 2020. – Режим доступу до ресурсу: https://www.icann.org/ru/system/files/files/octo-010-06may20-ru.pdf.
2. Ali J. Practical Hash-based Anonymity for MAC Addresses [Електронний ресурс] / J. Ali, V. Dyo // University of Bedfordshire. – 2020. – Режим доступу до ресурсу: https://www.researchgate.net/publication/341396003_Practical_Hash-based_Anonymity_for_MAC_Addresses.
3. Васильев М. Базовые принципы полисеров и шейперов [Електронний ресурс] / Михаил Васильев. – 2020. – Режим доступу до ресурсу: https://habr.com/ru/post/507494/.