УДК 004.042

Байлюк Є. М., асистент кафедри
Житомирський державний технологічний університет

РОЛЬ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ В КІБЕРБЕЗПЕЦІ

Кібербезпека має надзвичайно важливе значення в сьогоднішньому мережевому світі. Оскільки Інтернет не має кордонів, кібер-атаки можуть надходити з будь-якого місця і в будь-який час. Ці атаки, які спрямовані на уряд і критичну інфраструктуру, можуть швидко стати проблемою національної безпеки.

Забезпечення обізнаності щодо безпеки у високошвидкісних мережах є ресурсоємним завданням. На сьогоднішній час потрібні висококваліфіковані команди мережевої безпеки, які мають глибоке розуміння поведінки мережі, а також знання мережі та підключених вузлів. Їх звичайні робочі процедури складаються з спостереження за графіками статистики трафіку, пошуку незвичайних обсягів переданих даних або пакетів, і, відповідно, вивчення окремих підозрілих подій за допомогою таких інструментів, як пакетні аналізатори, аналізатори потоку, системи виявлення вторгнення, брандмауери та система журналювання подій. Такий поглиблений аналіз трафіку окремих пакетів і потоків є трудомістким та вимагає відмінних знань про поведінку мережі. Дослідження вдосконаленого аналізу трафіку необхідно для того, щоб забезпечити методи, які потребуватимуть менше людського втручання і, водночас, поліпшуватимуть виявлення атак, загроз і зловживання системою.

Аналіз мережевого трафіку – це метод виявлення вірусів і шкідливих програм різного типу, заснований на перевірці даних, що проходять через вузли мережі (наприклад, сервери електронної пошти) або по каналах передачі даних. Для цього створені спеціальні пристрої або програми, які називаються аналізаторами трафіку.

Проблемами аналізу трафіку є обмеження методів вимірювання та виявлення, великий обсяг трафіку та подій, а також необхідність захисту персональних даних. Кожне мережеве середовище є унікальним, і просте співвідношення подій безпеки може працювати в невеликих і добре підтримуваних мережах. Такі середовища є рідкісними. Як правило, будь-яка мережа, що підключена до Інтернету, піддається щоденному мережевому скануванню, спаму, атак нульового дня, а також шкідливим користувачам мережі, які є прихованими у величезних обсягах трафіку в просторах Інтернету. Величезний обсяг трафіку може перешкоджати роботі засобів аналізу трафіку, змусити їх відмовитися від даних і погіршити їхні загальні можливості аналізу. На-

приклад, неправильно працююча система виявлення аномалій може створити таку велику кількість повідомлень, що команда безпеки перестане їх аналізувати. Не менш важливим є те, що чутливий характер даних, які передаються по мережі, вимагає, щоб аналіз трафіку ретельно враховував питання конфіденційності.

Детальна інформація про трафік необхідна для забезпечення постійної ситуаційної обізнаності про мережу. Така інформація може бути слідами пакетів, статистикою потоку або статистикою обсягу. Як правило, необхідно зробити компроміс між обчислювальною доцільністю та наданим рівнем інформації для ефективної обробки високошвидкісного трафіку у великих мережах.

Повні сліди пакетів, що традиційно використовуються аналізаторами трафіку, забезпечують найбільш детальну інформацію. Проте, масштабованість і можливість обробки постійного спостереження за трафіком і зберігання у високошвидкісних мережах є проблемою внаслідок необхідності збереження конфіденційності та високих експлуатаційних витрат. Статистика потоків надає інформацію з заголовків Інтернет-протоколу (IP). Вони не містять інформації про корисне навантаження; однак, ми все ще знаємо, з точки зору інформаційної системи, хто спілкується з ким, коли і як довго, який протокол використовувався, а також, скільки даних було передано. Такий підхід значно зменшує обсяг даних, які необхідно обробити та зберегти. Статистика потоків надає інформацію навіть про зашифрований трафік, оскільки заголовки пакетів не шифруються. Статистику обсягу надають більшість мережевих пристроїв для керування мережею (наприклад, статистичні дані інтерфейсу протоколу SNMP). Вони забезпечують менш деталізований перегляд мережі порівняно з статистикою потоків і повними слідами пакетів, та не дозволяють провести додатковий аналіз трафіка.

Апаратне прискорення інструментів моніторингу використовується для того, щоб впоратися з високошвидкісним мережевим трафіком, особливо в середовищах, де потрібно гарантувати функціональність моніторингу навіть у найгірших випадках, таких як атаки відмови в обслуговуванні. Проте, будь-який апаратний або програмний прискорювальний механізм часто повинен використовувати оптимізовані версії операційної системи і засоби моніторингу.

Таким чином, аналіз потоків забезпечує масштабований підхід до моніторингу великих мереж. Однак необхідно проаналізувати дані про потоки, а не тільки зберігати їх для отримання даних, обробки інцидентів та проведення експертизи.