УДК 004.77

ПІДХІД ДО АНАЛІЗУ ВИХІДНОГО ТРАФІКУ

Наталія Петляк[1], Юлія Хохлачова[2], Юрій Кльоц[3]
[1]Національний авіаційний університет, npetlyak@khmnu.edu.ua,
[2]yuliiahohlachova@gmail.com
[3]Хмельницький національний університет, klots@khmnu.edu.ua

Все більше і більше люди стають залежними від комп'ютерів, Інтернету та інших цифрових технологій. Цифровізація проникає в усі сфери життя, включаючи критичну інфраструктуру, бізнес, громадські послуги та інше. Однак, залежність від цифрових технологій також призводить до зростання кіберзлочинності.

Аналіз IPS/IDS систем показав, що вони орієнтовані на захист від зловмисних дій у корпоративних мережах, а самі системи потребують спеціального обладнання та фахівців для налаштування й подальшої підтримки мережі. Тому такі системи, зазвичай, не використовують для загальнодоступних мереж. Для вирішення задач аналізу трафіку застосовують методи параметричного аналізу, нечіткої логіки або штучний нейронних мереж. Однак окреме використання таких підходів має значні недоліки. Відповідно, проблема аналізу вихідного трафіку задля забезпечення безпеки в мережі, захисту її від компрометації та зменшення навантаження на мережу залишається актуальною.

Метою даної роботи є розробка підходу до аналізу вихідного трафіка задля запобігання витоку зловмисного трафіка з мережі та виявлення порушника.

Дослідивши типову поведінку порушників у мережі під час атаки та проаналізувавши пакети можна сформувати набір параметрів, за якими можна виявити зловмисні дії. Задля швидшої роботи системи, яка розроблена на основі вказаного підходу, доцільно обрати параметри з найбільшою ефективністю. На основі оптимізованих параметрів слід сформувати сигнатуру пакета, що використовуватиметься для виявлення зловмисного трафіку:

$$s = \{IPs, IPd, Ps, Pd, Pr, Sd, T\}, \quad (1)$$

де IPs – IP-адреса джерела; IPd – IP-адреса призначення; Ps – порт джерела; Pd – порт призначення; Pr – протокол; Sd – швидкість передачі даних; T – час надходження пакету на перевірку.

Елементи сигнатури IPs, IPd, Ps, Pd, Pr можуть набувати один із трьох станів: заборона, дозвіл та невизначено. Елемент сигнатури Sd може приймати один із трьох станів: низька, середня та висока. Пряме порівняння сигнатур забезпечує максимальну швидкість аналізу, однак, для досягнення необхідної ефективності аналізу трафіку потрібно сформувати словники сигнатур. Однак виникає задача формування словника сигнатур та підтримання його в актуальному стані.

Для аналізу вихідного трафіку та формування словників сигнатур доцільно використати набір правил, що дозволяють провести класифікацію пакетів за критеріями. Задачі такого класу зазвичай вирішуються методами нечіткої логіки. Це дозволить вести аналіз трафіку та будувати словники в режимі реального часу. Перевагою такого підходу є висока достовірність отриманого результату, однак вона досягається за рахунок збільшення часу і ресурсів для аналізу пакету. В умовах

критичного завантаження каналів зв'язку або процесора пристрою, на якому проводиться аналіз доцільно зменшити навантаження на систему за рахунок використання для аналізу попередньо навченої ШНМ.

ШНМ довготривалої короткочасної пам'яті дозволяють знизити навантаження на систему при аналізі трафіку, що дозволяє їх використання в пікових режимах.

З огляду на вищевикладене, для ефективного виявлення порушників у мережі запропонований підхід (рис.1.) складається із трьох методів, що мають різні механізми виявлення.

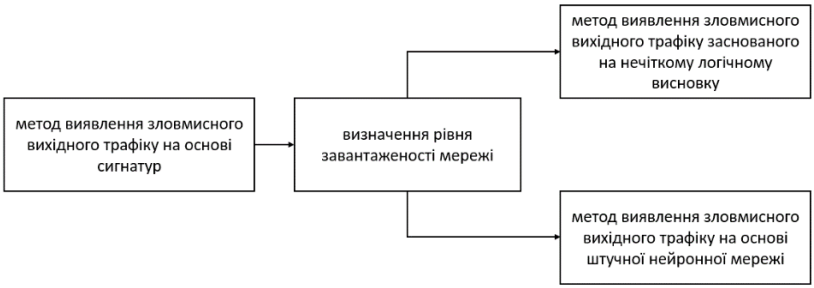

Рис.1. Підхід до аналізу вихідного трафіка

Першочергово має формуватися сигнатура та передаватись на метод виявлення зловмисного вихідного трафіку на основі сигнатур. Даний метод порівнює одержану сигнатуру із сформованими словниками (словник має початкові дані та наповнюється на методі з використанням нечіткого логічного висновку) дозволених та заборонених сигнатур. Якщо сигнатуру класифіковано, то з'єднання дозволяється чи блокується. Якщо сигнатуру не класифіковано, то відбувається перехід до наступного кроку: перевірка завантаженості мережі.

Якщо завантаження мережі та обладнання далеке від пікового, то буде виконуватися метод виявлення зловмисного вихідного трафіку, заснований на нечіткому логічному висновку. Під час виконання буде здійснюватися перевірка сигнатур відповідно до заданого набору правил. Якщо сформована сигнатура пакета відповідає одному з правил, які задовольняють вимогу дозволеного трафіку, то пакету дозволено з'єднання та сигнатура пакета записується в словник дозволених з'єднань. Інакше пакет відкидається та сигнатура пакета записується в словник заборонений з'єднань.

Якщо мережа функціонує в піковому навантаженні, то буде використовуватись метод виявлення зловмисного вихідного трафіку на основі штучної нейронної мережі. Перш ніж даний метод буде функціонувати, він проходить навчання та тестування на попередньо розроблених базах даних. Метод розроблено відповідно до двійкової класифікації довготривалої короткочасної пам'яті.

Запропонований підхід дозволяє класифікувати вихідний мережевий трафік з метою блокування зловмисних дій, що дає змогу запобігти перевантаженню мережевого обладнання та зменшити ймовірність компрометації поточної мережі та її власника.