УДК 004.7

Сарапин В.Є., магістрант
Київський національний університет будівництва і архітектури

ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ ЗАСОБАМИ АНАЛІЗУ ТРАФІКУ

Сучасні комп'ютерні мережі функціонують у високодинамічному середовищі, де зростання обсягів трафіку, ускладнення транспортних протоколів та інтенсивність мережевих викликів створюють підґрунтя для появи аномальних поведінкових патернів. Виявлення мережевих аномалій є одним із ключових завдань кібербезпеки, оскільки саме на ранніх етапах аномалії сигналізують про присутність загроз, експлуатацію уразливостей або функціональні збої систем. Аналіз трафіку як метод діагностики дозволяє досліджувати поведінку мережі у реальному часі, здійснювати її класифікацію та встановлювати відхилення від нормальних режимів роботи.

Мережеві аномалії можуть проявлятися у вигляді нетипових сплесків активності, надмірної фрагментації пакетів, перевищення порога затримок, порушення порядку доставки пакетів або зміни інтенсивності міжвузлової взаємодії. До поширених класифікаційних категорій аномалій належать поведінкові, структурні, протокольні та змішані. Поведінкові аномалії пов'язані зі змінами трафіку в часі, структурні – з порушенням узгодженості пакетів, а протокольні – з неправильним формуванням заголовків та нестандартними запитами. Виявлення таких аномалій вимагає наявності інструментів, здатних точно аналізувати характеристики потоків.

Для детального аналізу аномалій використовуються засоби пакетного аналізу, такі як Wireshark, які дозволяють вивчати структуру мережевих кадрів, визначати нестандартні поля та виявляти аномальні сигнатури. Засоби низькорівневого моніторингу tcpdump забезпечують збирання трафіку у середовищах з обмеженими ресурсами, що робить їх ефективними у випадках, коли потрібен мінімальний вплив на систему. Потокові протоколи NetFlow та IPFIX дозволяють аналізувати статистику потоків, що є надзвичайно корисним при пошуку аномалій, пов'язаних із тривалими атаками, скануванням портів або горизонтальним переміщенням загроз.

Виявлення аномалій також ґрунтується на побудові математичних моделей, що описують нормальну поведінку мережі. Значну роль відіграють статистичні підходи, зокрема дисперсійний аналіз, кореляційні методи та кластеризація поведінкових патернів. Методи машинного навчання, такі як алгоритми ізоляційних лісів, автоенкодери

та моделі часових рядів, дозволяють автоматично виявляти приховані закономірності у великих масивах трафіку. Використання таких методів забезпечує можливість раннього попередження про аномалії без необхідності попереднього визначення сигнатур або точних правил поведінки.

Не менш важливою складовою є оцінка якості обслуговування. Збільшення затримок, нерівномірність навантаження, коливання пропускної здатності, поява джитеру та збільшення втрат пакетів можуть бути маркерами некоректної роботи мережі або наслідком цілеспрямованої атаки. Моніторинг цих показників дозволяє визначити вузькі місця, встановити причини погіршення продуктивності та виявити неузгодженість у роботі механізмів маршрутизації.

У практичних мережах комплексна діагностика аномалій потребує використання як програмних, так і апаратних інструментів. Апаратні TAP-пристрої та SPAN-порти дозволяють отримувати копії трафіку у чистому вигляді, забезпечуючи безперервний моніторинг без впливу на роботу інфраструктури. Дані, отримані такими засобами, можуть бути інтегровані у системи SIEM, де здійснюється їх кореляція, нормалізація та детальний аналіз. Поєднання таких методів дозволяє створювати комплексні системи раннього виявлення інцидентів.

Отже, виявлення мережевих аномалій на основі аналізу трафіку є фундаментальним напрямом кібербезпеки, який забезпечує захист інформаційних систем від прихованих та активних загроз. Використання сучасних інструментів аналізу, статистичних методів та алгоритмів машинного навчання створює передумови для побудови стійких та адаптивних систем захисту, здатних забезпечити безперервне функціонування мережі.

Список використаних джерел:

1. Wireshark Foundation. Wireshark User Guide. URL: https://www.wireshark.org/docs/

2. Cisco Systems. NetFlow Services Export Version 9 : RFC 3954. IETF, 2004. URL: https://datatracker.ietf.org/doc/html/rfc3954

3. Lakhina A., Crovella M., Diot C. Characterization of Network-Wide Anomalies // ACM Internet Measurement Conference (IMC). 2004. URL: https://dl.acm.org/doi/10.1145/1028788.1028794 4. Barford P., Plonka D. Flow Analysis Techniques for Network Monitoring. IEEE Communications Magazine, 2001.

5. Tanenbaum A. Computer Networks. 5th ed. Upper Saddle River : Prentice Hall, 2010.