УДК 004.056

Р.С.Липянчик, Б.М. Липа, О.В.Мардинавка
(Тернопільський національний технічний університет імені Івана Пулюя)

ШЛЯХИ УДОСКОНАЛЕННЯ ВИЯВЛЕННЯ ВТОРГНЕНЬ В МЕРЕЖЕВИХ IDS СИСТЕМАХ

UDC 004.056

R. Lypianchyk, B. Lypa, O. Mardynavka

WAYS TO IMPROVE INTRUSION DETECTION IN NETWORK IDS SYSTEMS

Використання комп'ютерних систем та Інтернету останнім часом призвело до серйозних проблем безпеки, приватності та конфіденційності. Кількість кібератак постійно зростає, і з кожним роком вони стають більш складними та витонченими. Злочинці використовують новітні методи, такі як атаки нульових днів, фішинг, складні типи DoS-атак і шкідливі програми.

Комерційні компанії широко використовують IDS (системи виявлення вторгнень) та IPS (системи запобігання вторгненням) для забезпечення безпеки своїх інформаційних систем і захисту від руйнівних кібератак. Ці технології працюють разом, але мають різні функції та завдання [1]. Системи виявлення вторгнень (Intrusion Detection System IDS) допомагають аналізувати мережевий трафік і генерувати сповіщення в разі виявлення зловмисної активності. Система запобігання вторгненням (Intrusion Prevention System IPS) активно реагує на потенційні загрози, не лише виявляючи їх, але й блокуючи або припиняючи атакуючі дії в реальному часі.

Деякі організації використовують брандмауери, а також маршрутизатори разом з IPS/IDS. Основна різниця між ними полягає в тому, що брандмауер перевіряє лише IP-адресу та номер порту. Використовуючи номер порту та IP-адресу, він блокує трафік. Брандмауер - це перша лінія, яка може захистити мережу від зловмисників. Він може виявити лише обмежену кількість атак. Тому рекомендують додатково використовувати IDS/IPS, щоб забезпечити додатковий рівень захисту трафіку від атак з боку веб-серверів, доступних з Інтернету [2].

Відповідно до [3], IDS є одним з широко розповсюджених інструментів, що дозволяє здійснювати моніторинг цілого ряду мережевих систем, хмарних обчислень, а також інформаційної системи. За місцем встановлення систем виявлення вторгнень (IDS), їх поділяють на:

- Мережеві IDS (NIDS - Network IDS). Ці системи розташовані на рівні мережі і аналізують весь трафік, що проходить через мережу. Вони допомагають виявити атаки, спрямовані на мережу або що використовують мережеві вразливості.
- Хостові IDS (HIDS - Host IDS). Ці системи встановлюються на окремих пристроях (наприклад, серверах, комп'ютерах) і контролюють їх активність, включаючи доступ до файлів, журнали подій, використання процесора тощо.

NIDS сканує мережевий трафік з сегмента локальної мережі. Він також може відстежувати більше мережевих цілей, намагаючись виявити загрози, які можуть бути пропущені HIDS, оскільки HIDS не може читати заголовки пакетів і не може виявити певні

типи атак. Проте мережеві дані генеруються з великою швидкістю та у значній кількості. Тому є дуже важливою задача правильної репрезентації характеристик мережевого трафіку, виділяють пакетний, потоковий та аналіз на рівні прикладного шару. Пакетний аналіз розглядає характеристики мережевих пакетів. Потоковий аналіз оперує групами пакетів із однієї сесії та їх агрегованими характеристиками. Аналіз на рівні прикладного шару використовує мережеві дані додатків.

За способом виявлення атак IDS поділяють на:

- Сигнатурні IDS (Signature-Based IDS). Ці системи працюють за принципом порівняння з відомими шаблонами атак (сигнатурами). Якщо виявлено дії, які відповідають відомим атакам, система сигналізує про загрозу.
- Аномалійні IDS (Anomaly-Based IDS). Ці системи вивчають нормальну поведінку системи або мережі і сигналізують, коли відбувається відхилення від цієї норми. Це може бути ознакою нової атаки
- Гібридні IDS (Hybrid IDS). Поєднують методи сигнатурного та аномалійного виявлення, щоб забезпечити більш точне та ефективне виявлення атак.

До переваг аномалійних IDS відносять здатність виявляти нові або невідомі атаки [3].

Аномалійні IDS можуть використовувати різні методи для виявлення відхилень:

- Статистичний аналіз: порівнює поточну активність з відомими статистичними моделями нормального використання.
- Методи машинного навчання (ML): деякі аномалійні IDS використовують алгоритми машинного навчання для розпізнавання шаблонів і виявлення аномальних поведінкових патернів. Це дозволяє системі адаптуватися до нових умов і загроз.
- Нейронні мережі: складніші моделі, які допомагають покращити точність виявлення, оскільки вони можуть аналізувати більше параметрів і взаємозв'язків у даних.

Автори [4] обґрунтували цінність методів машинного навчання для виявлення мережевих атак. Проте, використання методів машинного навчання вимагає грунтоної попередньої обробки даних, вибору моделей та налаштування їх гіперпараметрів.

Отже, основними шляхами дослідження щодо вдосконалення IDS систем визначено наступні:

- вибір та обґрунтування інструментів для формування простору ознак,
- підвищення якості вхідних даних методами їх попередньої обробки,
- вибір та налаштування гіперпараметрів моделі.

Література.

1. Safana Hyder Abbas, Wedad Abdul Khuder Naser, Amal Abbas Kadhim, 2023. Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Global Journal of Engineering and Technology Advances, No 14(02), P.155–158
2. Kanika, 2013 Intrusion Detection System and Intrusion Prevention System – a Review Study. International Journal of Scientific & Engineering Research, Volume 4, Issue 8, P.594-596
3. Aljanabi Mohammad, Ismail Mohd Arfian, Ali Ahmed, 2021. Intrusion Detection Systems, Issues, Challenges, and Needs. International Journal of Computational Intelligence Systems. No 14. P.1-11. DOI:10.2991/ijcis.d.210105.001.
4. J. Jabez, B.Muthukumar, 2015 Intrusion detection system (IDS): anomaly detection using outlier detection approach. Procedia Computer Science No 8, P.338 – 346, https://doi.org/10.1016/j.procs.2015.04.191
5. N Zagorodna, M Stadnyk, B Lypa, M Gavrylov, R Kozak. 2022. Network Attack Detection Using Machine Learning Methods. Challenges to national defence in contemporary geopolitical situation, No 1, P. 55-61