УДК 004.056.5
А.А. Микитишин, Т.А. Лечаченко, д-р. філософії, ст.викл.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

АНАЛІЗ МЕТОДИК ВИЯВЛЕННЯ ВТОРГНЕНЬ У СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

A. A. Mykytyshyn, T. A. Lechachenko, Ph.D., Senior Lecturer

ANALYSIS OF INTRUSION DETECTION METHODS IN INFORMATION SECURITY SYSTEMS

На сьогоднішній день захист інформації є дуже важливою складовою нашого життя. Інформаційні системи стрімко розвиваються і разом з цим зростає кількість загроз та вразливостей до яких ці системи чутливі. Тому механізми та комплекси виявлення та запобігання вторгнень є дуже важливим напрямком в сфері комп'ютерної безпеки. Не можна недооцінювати ризики пов'язані з порушенням конфіденційності, цілісності та доступності даних.

Вторгнення в мережу – це будь-яка несанкціонована діяльність в цифровій мережі. Вторгнення в мережу часто пов'язані з крадіжкою цінних мережевих ресурсів і майже завжди ставлять під загрозу безпеку мереж або їх даних [1].

Виявлення кібератак має важливе значення для забезпечення безпеки мереж і систем. Тому, щоб виявити зловмисну діяльність, багато компаній використовують платформи які забезпечують захист інформації та здійснюють керування подіями, щоб збирати, керувати та аналізувати дані з різних джерел журналів, таких як брандмауери та операційні системи.

Загалом, зловмисну активність можна виявити, реалізувавши правила виявлення в таких системах, які перевіряють шаблони активності або код, що відповідають атакам, тобто сигнатури зловмисної діяльності. Однак, незважаючи на те, що виявлення атак за допомогою сигнатур добре працює в багатьох ситуаціях, це також створює деякі проблеми та обмеження, такі як труднощі у виявленні варіантів атак або невідомих атак, оскільки для них немає спеціальних сигнатур [2].

Щоб подолати ці обмеження, все частіше застосовують інший підхід до виявлення: виявлення аномалій. Системи виявлення аномалій моделюють нормальну поведінку користувачів, мереж і систем, щоб встановити нормальні шаблони та виміряти відхилення від цих параметрів, оскільки значні відхилення представляють невідповідності з нормальною поведінкою і, отже, вказують на підозрілу активність.

В результаті дослідження, на основі архітектури ElasticSearch, розроблено та впроваджено алгоритм машинного навчання, спрямований на виявлення аномалій у системних та мережевих даних. Цей алгоритм базується на вивченні нормальних шаблонів та виявленні відхилень, що вказують на можливі загрози. Програмне забезпечення на Python буде використано для аналізу та інтеграції цих подій у систему виявлення аномалій на базі ElasticSearch. Цей комплексний підхід дозволить забезпечити ефективне виявлення та реагування на потенційні кіберзагрози, забезпечуючи надійний рівень безпеки інформаційних систем

Література

1. Network Intrusion. [Електронний ресурс]. URL:https://awakesecurity.com /glossary /network-intrusion/ Дата доступу: 07.10.21

2. Liao, Hung-Jen, et al. "Intrusion detection system: A comprehensive review." Journal of Network and Computer Applications 36.1 (2013): 16-24.