Ульяніцький М. А., магістрант,
Фальковський І. Г., ст. викладач,
Державний університет «Житомирська політехніка»

ПРОЕКТ СИСТЕМИ ВИЯВЛЕННЯ АТАК НА ОСНОВІ SNORT В IT-ІНФРАСТРУКТУРІ

IDS/IPS відстежує весь трафік у мережі, щоб виявити будь-яку відому шкідливу поведінку. Одним із способів, якими зловмисник намагатиметься скомпрометувати мережу, є використання вразливості в пристрої або програмному забезпеченні. IDS/IPS ідентифікує ці спроби використання та блокує їх до того, як вони успішно скомпрометують будь-яку кінцеву точку в мережі.

Для виявлення інцидентів зазвичай використовуються три методології виявлення IDS:

- Виявлення на основі сигнатур порівнює сигнатури з спостережуваними подіями, щоб визначити можливі інциденти. Це найпростіший метод виявлення, оскільки він порівнює лише поточну одиницю активності (наприклад, пакет або запис у журналі зі списком підписів) за допомогою операцій порівняння рядків.
- Виявлення на основі аномалій порівнює визначення того, що вважається нормальною активністю, із спостережуваними подіями, щоб виявити значні відхилення. Цей метод виявлення може бути дуже ефективним для виявлення раніше невідомих загроз.
- Аналіз протоколу з урахуванням стану порівнює попередньо визначені профілі загальноприйнятих визначень доброякісної активності протоколу для кожного стану протоколу з спостережуваними подіями, щоб виявити відхилення.

Snort – це система виявлення вторгнень (IDS) та інтрузійно-профілактична система (IPS) в одному рішенні. Вона використовується для аналізу мережевого трафіку на предмет шкідливої або небажаної активності. У режимі IDS Snort виявляє потенційні загрози, а в режимі IPS може блокувати або відхиляти цей трафік в реальному часі.

Suricata – це конкурент системи Snort на ринку середнього бізнесу з відкритим вихідним кодом, що вперше була представлена у 2010 році. Однією з переваг Suricata є те, що вона є молодою системою, що дозволяє уникнути великої кількості застарілого коду. Крім того, вона використовує новіші технології, що сприяє її швидкій роботі порівняно з конкурентами. Розробники Suricata також піклуються про сумісність зі стандартними утилітами аналізу результатів, що дозволяє їй підтримувати ті ж модулі, що й Snort. Ця система може виявляти загрози за допомогою сигнатур і підходить для середніх і великих компаній.

McAfee Network Security Platform за стартову ціну близько $10 000. Ця система виявлення вторгнень (IDS) здатна ефективно блокувати широкий спектр загроз, включаючи доступ до шкідливих сайтів та запобігання DDoS-атакам. Проте через свою розмахність, вона може сповільнити роботу мережі. Тут важливо вирішити, що пріоритетнішим: інтеграція з іншими сервісами або максимальний рівень безпеки.

Zeek – це безкоштовна система виявлення вторгнень з відкритим вихідним кодом. Вона підтримує як стандартний режим виявлення вторжень, так і режим виявлення шкідливих сигнатур. Окрім цього, Zeek може виявляти події і дозволяє користувачам визначати власні скрипти політик. Однак недоліком Zeek є складність взаємодії з інструментом через відсутність графічного інтерфейсу, оскільки розробка спрямована на функціональність.

Системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS) постійно спостерігають за вашою мережею, виявляючи можливі інциденти та записуючи інформацію про них, зупиняючи інциденти та повідомляючи про них адміністраторам безпеки. Крім того, деякі мережі використовують IDS/IPS для виявлення проблем із політиками безпеки та запобігання порушенням політик безпеки.

У доповіді буде представлено детальний огляд систем виявлення вторгнень (IDS) і систем запобігання вторгненням (IPS), їх роль і значення в інфраструктурі безпеки мережі. Доповідь розгляне принципи роботи цих систем, їхні можливості виявлення та реагування на потенційні загрози, а також їхні переваги та недоліки. Також буде розглянуто важливість IDS/IPS у забезпеченні відповідності політикам безпеки та їхню роль у запобіганні порушенням цих політик. На доповіді буде розглянуто сучасні тенденції та рекомендації з використання IDS/IPS у контексті сучасних загроз та вимог до безпеки мережі.

Список використаних джерел

1. "IDS/IPS: Intrusion Detection and Prevention Systems" – R. Lippmann, D. P. Fried, K. W. Ingols URL: https://www.researchgate.net/publication/368928254

2. Augmenting zero trust architecture to end points using blockchain: A state-of-the-artreview URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.191