DOI 10.62731/mcnd-31.05.2024.007

СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ МЕРЕЖНИХ ОПЕРАЦІЙНИХ СИСТЕМ

Добуш Андрій Романович
аспірант кафедри електронних обчислювальних машин
Національний університет «Львівська Політехніка», Україна

Науковий керівник: Гаваньо Богдан Іванович
доктор філософії, асистент кафедри електронних обчислювальних машин
Національний університет «Львівська Політехніка», Україна

Системи виявлення вторгнень HIDS використовується в хостах Linux загального призначення, таких як сервери підключених до мережі хостів користувачів [1]. Host Intrusion Detection Systems (HIDS) за своєю природою діють в межах одного хоста, ретельно перевіряючи його внутрішню діяльність, щоб виявити та запобігти потенційним загрозам. З безліччю доступних варіантів HIDS, кожен з яких адаптований до певного середовища та випадків використання, розуміння їх нюансів і функцій стає першорядним.

Існуючі HIDS охоплюють широкий спектр можливостей, починаючи від систем виявлення на основі сигнатур до більш складних механізмів виявлення аномалій. У той час як деякі HIDS покладаються на заздалегідь визначені правила та шаблони для позначення підозрілої поведінки, інші використовують алгоритми машинного навчання, щоб розпізнавати аномальну діяльність у режимі реального часу.

Як зазначено в [2], є деякі заходи, які може використовувати виявлення вторгнень:

- Активність входу та сесії (частота входу, час, витрачений на кожен сеанс)
- Використання ресурсів (реалізація команд і процедур, • повторюваність використання ресурсів)
- Робота з файлами (частота читання, запису, створення та видалення файлів, кількість записів і читань файлів, читання, запис, створення та видалення файлу

В свою чергу мережні операційні системи мають специфічні вимоги та особливості, які відрізняються від традиційних серверних або настільних ОС. Вони оптимізовані для управління мережею та мають спеціалізовані компоненти, які потрібно контролювати.

Мережні операційні системи такі як SONiC використовується в мережних комутаторах та маршрутизаторах, які є критичними компонентами мережевої інфраструктури. Злом або неправильне функціонування цих пристроїв може призвести до серйозних проблем з безпекою всієї мережі.

Мережні ОС генерують специфічні журнали та події, які можуть вказувати на аномалії чи загрози. HIDS повинна бути адаптована для правильного аналізу цих даних, щоб ефективно виявляти вторгнення.

Серед найбільш використовуваних мережних операційних систем з відкритим кодом є мережна операційна система SONiC (Software for Open Networking in the Cloud).

Архітектура системи SONiC складається з різних модулів, які взаємодіють через централізовану масштабовану інфраструктуру. Ця інфраструктура спирається на механізм бази даних redis, який є базою даних ключ-значення, яка використовується

для забезпечення незалежного від мови інтерфейсу, забезпечення збереження даних, увімкнення реплікації та сприяння багатопроцесному зв'язку між усіма підсистемами SONiC.

SONiC приймає стратегію розміщення кожного модуля в незалежних докер-контейнерах, щоб підтримувати високу зв'язаність між семантично пов'язаними компонентами, одночасно зменшуючи зв'язок між різними. Кожен із цих компонентів розроблено таким чином, щоб бути повністю незалежним від специфічних для платформи деталей, необхідних для взаємодії з абстракціями нижчого рівня.

SONiC поділяє свої основні функціональні компоненти на такі докер-контейнери: Dhcp-relay, Pmon, Snmp, Lldp, Bgp, Teamd, Database, Swss, Syncd.

Для того щоб адаптувати системи виявлення вторгнень до мережної операційної системи SONiC потрібно також враховувати наступні параметри:

- Телеметрія мережних з'єднань
- Апаратні метрики маршрутизатора
- Логування докер контейнерів
- Зміни в конфігураціях
- Комунікація між докер контейнерами

Висновки. На прикладі мережної операційної системи SONiC розглянуто важливість вдосконалення і адаптації систем виявлення вторгнень до середовища роботи мережної операційної системи. Запропоновані параметри для покращення точності виявлення вторгнень при роботі мережної операційної системи SONiC

Список використаних джерел:

1. Niva Das, Tanmoy Sarkar. "Survey on Host and Network Based Intrusion Detection System" Int. J. Advanced Networking and Application. Volume: 6 Issue: 2 Pages: 2266-2269 (2014) ISSN: 0975-0290.
2. L. Ying, Z Yan OU Yang_jia "The Design and Implementation of Host-based Intrusion Detection System". DOI: 10.1109/IITSI.2010.127.