УДК 004.056
О.А. Черник
Тернопільський національний технічний університет імені Івана Пулюя, Україна

СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

O.A.Chernyk

INTRUSION DETECTION SYSTEMS

Система виявлення вторгнень СВВ (IDS) відстежує мережевий трафік на предмет аномального впливу і повідомляє користувачів про виявлення аномального трафіку. З кінця 1980-х років адміністратори корпоративних мереж стали включати СВВ до інструментів, що забезпечують безпеку мережі, і застосовували їх у роботі. Однак при функціонуванні були виявлені недоліки використання систем, такі як неможливість виявити атаки нульового дня, оскільки трафік порівнювався тільки зі списком відомих сигнатур, та використання великої кількості ресурсів для постійного сканування. Вирішення проблеми виявлення нових атак прийшло з впровадженням нового методу – виявлення аномалій (ВА). Він був заснований на виявленні нетипових поведінок у мережі та забезпечував виявлення аномальних ситуацій [1].

В даний час найбільший інтерес становлять СВВ, що працюють на хмарних обчисленнях. На підставі даних компанії Thread Stack, IDS є одними з технологій, що найбільше продаються в галузі забезпечення безпеки.

СВВ відрізняються одна від одної, в основному, за місцем збору інформації, механізмом виявлення і за швидкістю реагування. На основі даних критеріїв наведемо класифікацію СВВ [1].

За місцем збору інформації IDS поділяються на хостові (HIDS) - представник OSEEC, та мережеві (NIDS) - Cisco Secure IDS, Dragon Enterasys. Перші контролюють безпеку комп'ютера чи системи від внутрішніх та зовнішніх атак. Внутрішні – аномальні види поведінки програм, спроба доступу до заборонених ресурсів. Зовнішні – аномальна активність або вміст пакетів, виявлені під час аналізу мережевих взаємодій. До мінусів таких систем можна віднести збір даних на рівні вузла та пасивність системи. Другі відстежують мережевий трафік, і при ВА, які повідомляють про це адміністраторів.

За швидкістю реагування IDS: динамічні системи - ІКС UTM+, Рубікон (працюють у реальному часі) та статичні системи - Hummingbird (аналізують мережу, перевіряють зміни мережевих сервісів). Дані IDS як реального часу відстежують трафік на наявність аномальних ознак. Статичні здійснюють аналіз мережі, перевіряють зміни мережевих сервісів. Надають дані про атаку та допомагають усунути заподіяну шкоду.

За механізмом ВА IDS: сигнатурні – Suricat, та ВА - Snort, Bro-IDS. У першому типі систем кожен пакет мережного трафіку порівнюється з шаблонами атак, які у базі даних атак. До переваг даного методу відносяться простота використання та низький показник хибних спрацьовувань при хорошому підборі сигнатури атак. Основними недоліками є необхідність збирання якісної бази сигнатур атак та складність детектування раніше невідомих або не внесених до бази атак. Другий тип IDS, засновані на ВА, аналізує дії, що відбуваються в мережі. Стандартна поведінка в мережі визначається адміністратором або за допомогою навчального набору даних при розробці системи. Дії, які не вписуються у рамки стандартної поведінки, вважаються аномальними. Аналіз трафіку щодо аномалії дає можливість виявляти атаки, невідомі системі раніше. До недоліків такого типу систем належать завдання правил визначення аномалій та сильна залежність ефективності роботи від них.

Література

1. Коробейнікова Т., Цар О. Аналіз сучасних відкритих систем виявлення та запобігання вторгнень. – Grail of Science, (27), 2023. с. 317–325.