КЛАСИФІКАЦІЯ СИСТЕМ ВИЯВЛЕННЯ АТАК IDS

Концеба В.Д., Колесніков К.В.
Черкаський державний технологічний університет, Черкаси, Україна

Кількість атак на інформаційні системи невпинно збільшується, та динамічно змінюються технології вторгнень, отже є нагальна необхідність у розробці нових моделей та методів протидії цим небажаним впливам.Метою роботи єрозробка сучасної класифікації механізмів атак в системах виявлення атак IDS**(**IntrusionDetectionSystem**)**. Механізми, якізастосовані у сучасних системах виявлення атак IDS, основані на декількох загальних методах.

В багатьох системах використовують їх комбінації:

а) **за способом реагування** розрізняють *пасивні* так *активні*IDS. Пасивні фіксують факт атаки, записують дані у файл журналу і видають попередження. Активні намагаються протидіяти атаці [1] ;

б) **за способом виявлення атаки** системи IDS прийнято поділяти на такі категорії:виявлення аномальної поведінки; виявлення зловживань.

Технологія *виявлення аномальної поведінки*заснована на наступному. Аномальна поведінка користувача часто проявляється як відхилення від нормальної поведінки.

Технологія виявлення аномалійорієнтована на нові типи атак. Однак головний недолік її – необхідність постійного навчання.

Технологія *виявлення зловживань*полягає в описі атаки у вигляді сигнатури і пошуку даної сигнатури в контрольованому просторі. Дана технологія виявлення атак дуже схожа на технологію виявлення вірусів, при цьому система може виявити всі відомі атаки. Однак системи даного типу не можуть виявити нові, ще не відомі види атак [1, 2];

в) найбільш популярна класифікація **за способом збору інформації про атаку:** виявлення атак на рівні мережі (network-based); виявлення атак на рівні хоста (host-based); виявлення атак на рівні додатка (application-based) [3].

Подальші роботи в даному напрямку дозволять застосувати новітні ефективні технології виявлення несанкціонованих вторгнень в інформаційні системи, що є перспективним напрямком прикладних наукових досліджень.

Список літератури

1. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. — М.: ИД «ФОРУМ»: ИНФРА-М, 2017. — 416 с. — (Профессиональное образование).

2. Mozhaev O. Multiservise network security metric / O. Mozhaev, H. Kuchuk, N. Kuchuk, M. Mozhaev, M. Lohvynenco // IEEE Advanced information and communication technologies-2017. Proc. of the 2th Int. Conf. – Lviv, 2017. – P. 133-136.

3. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах В. І. Мєшков, В. О. Віролайнен [Електронний ресурс] Режим доступу: http://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf