

ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ АНАЛОГІВ АВТОМАТИЗОВАНОЇ СИСТЕМИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ МЕРЕЖЕВИМ АТАКАМ НА СУБД

Вікторія Войтко, к.т.н., доцент кафедри програмного забезпечення,
Вінницький національний технічний університет, Україна,

Алла Денисюк, асистент кафедри програмного забезпечення, Вінницький
національний технічний університет, Україна,

Ася Костельна, студентка групи ІПІ-11б, факультет інформаційних технологій
і комп'ютерної інженерії, Вінницький національний технічний університет,
Україна

З розвитком мережових технологій роль інформаційних ресурсів зростає. Разом з тим актуалізується проблема захисту інформації від несанкціонованого доступу і мережових атак [1-3].

Метою роботи є підвищення надійності систем управління базами даних (СУБД) шляхом розробки та використання програмних засобів захисту інформації.

Об'єктом дослідження є мережеві технології. Предметом дослідження постає програмний продукт для захисту бази даних, який аналізує звіти мережевого обладнання та мережевого екрану та приймає рішення про те, чи були спроби несанкціонованого доступу до бази даних (далі інноваційний програмний продукт).

Проаналізуємо можливості розробленого програмного продукту у порівнянні з сучасними аналогами.

Програмами аналогами, присутніми на ринку, є продукти іноземного виробництва: FireMon Firewall Log Analysis та Firegen 3.0 Log Analyzer [4-5]. Розглянемо ключові переваги та недоліки цих продуктів.

Основні переваги Firewall Log Analysis:

- швидкий доступ до журналу подій;
- простий і водночас гнучкий спосіб налаштування правил у мережевому екрані;
- автоматичне вивчення та видалення правил та об'єктів, що не використовуються;
- автоматичний пошук найбільш оптимізованих правил для підвищення продуктивності.

Основні характеристики Firewall Log Analysis:

- дані зберігаються протягом тривалого періоду часу для точної звітності та можуть бути досліджені з графічною гістограми;
- правила, які використовуються, приведені поряд з об'єктами, для яких спрацювало дане правило;
- відображення останньої дати використання правил, що дозволяє видаляти застарілі правила.

Основним базовими недоліком розглянутого програмного забезпечення є те, що воно розповсюджується у складі пакету програмних продуктів FireMon Security Manager. Ціна усього пакету становить 8000 грн.

Основні переваги Firegen 3.0 Log Analyzer:

- підтримка необмеженої кількості міжмережевих екранів;
- підтримка декількох типів брандмауерів: Cisco Pix, Cisco ASA, Cisco FWSM, Sonicwall, Netscreen, SGS, Fortigate і Adtran;
- звіти у форматі HTML (можна їх переглядати прямо в браузері або ж вони опублікована на внутрішньому сайті);

Основні характеристики Firegen 3.0 Log Analyzer:

- дані зберігаються протягом тривалого періоду часу для точної звітності;
- автоматичний пошук та визначення мережеских екранів;
- погодинний графік успішних подій і відмов;
- автоматичне визначення кращих джерел трафіку, напрямків, протоколів, попередження відмов і URL-адрес.

Програмне забезпечення Firegen 3.0 Log Analyzer постачається як окремий продукт. Кожен з перерахованих програмних продуктів має свої особливості в використанні, налаштуванні, параметрах мережі, для якої застосовуються. Найбільш популярною серед користувачів є система Firegen 3.0 Log Analyzer через більш доступну ціну та свою чітку спеціалізацію. Згідно зі статистичними даними цей програмний продукт використовують більш як 30% користувачів систем захисту такого типу.

У порівнянні з аналогами розроблена система захисту СУБД орієнтована на роботу в автоматизованому режимі. Крім того, програмно забезпечена можливість ручного керування адміністратором процесу блокування IP-адрес та створення власних правил захисту системи.

Розроблена система захисту СУБД від мережеских атак орієнтована на протидію атакам, спрямованим на підбір паролів доступу до інформаційних ресурсів та облікових записів. Запропонована система захисту має графічний інтерфейс, що забезпечує автоматизований і ручний режими визначення правил захисту даних.

Література

1. Бойко В.В. Проектирование базы данных информационных систем. / В.В. Бойко, В.П. Савинков - М.: Финансы и статистика, 1989. - 215 с.
2. Тарасов Д.О. Специфічні для СУБД загрози захисту інформації // Защита информации: Сб. науч. тр. – К.: НАУ, 2001. – С. 53-60.
3. Bonatti P.A, Foundations of Secure Deductive Databases / P.A. Bonatti, S.Kraus, V.S. Subrahmanian, // IEEE Transactions on Knowledge and Data Engineering. – 2011. – Vol. 7, No. 3. – P. 406–422.
4. FireMon Firewall Log Analysis [Електронний ресурс] – Режим доступу: <http://www.firemon.com/tag/log-analysis/>
5. Firegen 3.0 Log Analyzer [Електронний ресурс] - Режим доступу: <http://www.firegen.com/>