УДК 004.056

Олійник А.О., студент 2-го курсу
спеціальності 122 «Комп'ютерні науки»
Антонов Ю.С. к. фіз.-мат. наук, доцент
доцент кафедри інформаційних технологій

ПРОГРАМНИЙ АНАЛІЗ ЖУРНАЛІВ ВЕБ СЕРВЕРІВ АРАСНЕ З МЕТОЮ ЗАПОБІГАННЯ МЕРЕЖЕВИМ АТАКАМ

Донецький національний університет ім. Василя Стуса, (Вінниця, Україна)

У сучасному діджиталізованому світі використання вебсайтів або сервісів є невід'ємною частиною життя людини та бізнесу. Від будь-якого інтернет ресурсу користувачі очікують безперебійної роботи сервісу 24/7, забезпечення цілісності інформації, захищеності персональних даних, тощо. Саме тому, з точки зору вдалого ведення бізнесу, довіри користувачів вебресурсів та питань інформаційної безпеки необхідно здійснювати постійний моніторинг та аналіз журналів доступу.

Серед існуючих аналогів систем аналізу логів веб-серверів можна виділити Web Log Explorer [1] та GoAccess [2], що дозволяють відображати результати аналізу за допомогою графічного інтерфейсу. До недоліку цих програм можна віднести те, що аналіз інформації у звітах та прийняття певних рішень щодо захисту системи здійснюється виключно людиною. Але дуже часто можуть виникати ситуації, які потребують прийняття певних рішень в автоматичному режимі [3].

Запропонований у цій роботі комплекс програмного забезпечення був реалізований з використанням багатошарової (Multilayer) архітектури [4] та містить як десктопний додаток з графічним інтерфейсом, так і консольний додаток (рис. 1).

Десктопний додаток дозволяє імпортувати дані з журналів та на їх основі генерувати наступні звіти:

- загальна статистика;
- коди статусів HTTP;
- методи HTTP запитів;
- URL аргументи запитів;
- хости;
- домени;
- операційні системи;
- браузери.

Дані з цих звітів можуть бути експортовані до файлів у форматах xls, xlsx, csv.

Консольний додаток дозволяє: аналізувати лог-файли у фоновому режимі (режимі реального часу); генерувати звіти; відправляти звіти та інформаційні повідомлення засобами комунікації (електронна пошта, месенджер Telegram);

блокувати доступ до серверу шляхом взаємодії з файєрволом.

У якості прикладу було розглянуто журнали веб серверу, на якому розміщувалась автоматизована система контролю знань «A.S.T.S.» («Antonov Students Test System») [3, 5 ,6] (рис. 2).

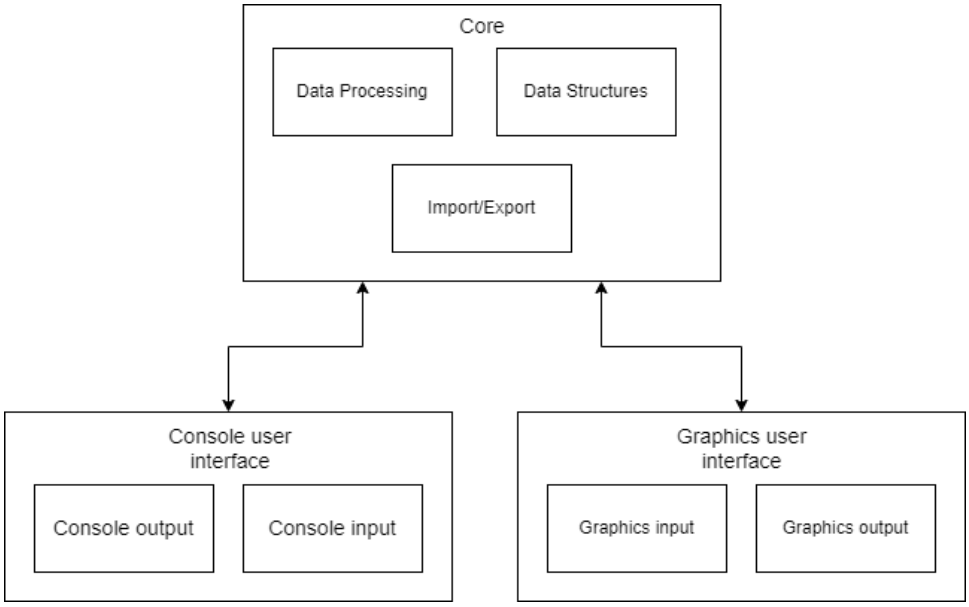

Рисунок 1. Компонентна схема додатку

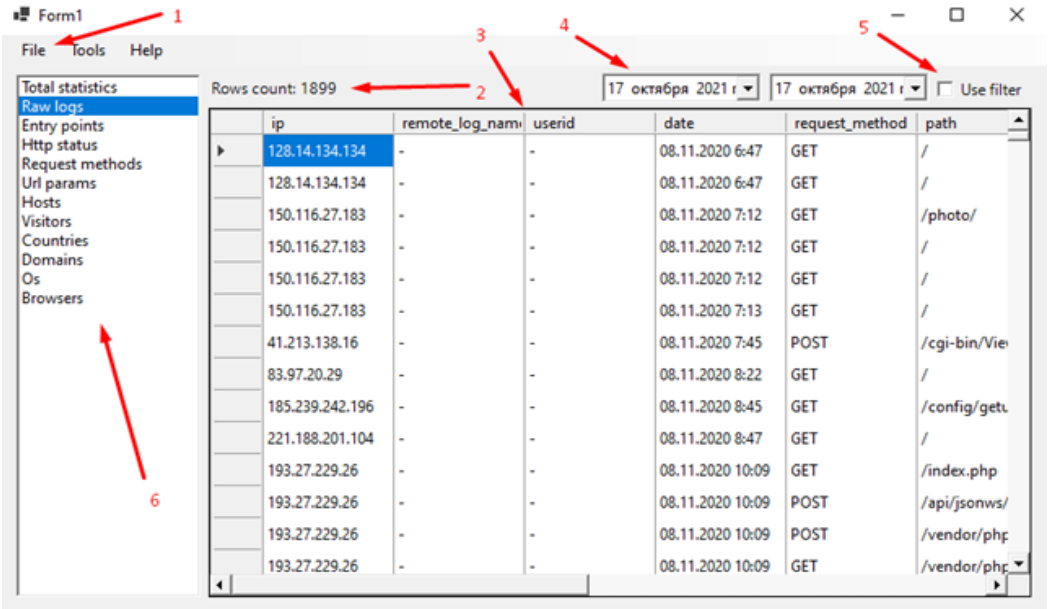

Рисунок 2. Інтерфейс програми

Список літератури:

1. Exacttrend Software - 2021. [Електронний ресурс] - URL: https://www.exacttrend.com/ Дата звернення: 06.11.2021

2. GoAccess [Електронний ресурс] - URL: https://goaccess.io/ Дата звернення: 28.09.2021

3. Антонов Ю.С., Римар П.В., Антонова О.Г. Проблема DoS/DDoS атак навчальних ресурсів студентами. Сучасний захист інформації. 2019. № 4(40). С. 52-62

4. Software Architecture Patterns by Mark Richards. [Електронний ресурс] - URL: https://www.oreilly.com/library/view/software-architecture-patterns/9781491971437/ch01.html Дата звернення: 21.09.2021
5. Антонов Ю.С. Комп'ютерні системи тестування на основі технології трирівневих баз даних. Інформаційні технології і засоби навчання. 2008. Т.6, №2. URL: https://journal.iitta.gov.ua/index.php/itlt/article/view/133 (дата звертання: 21.04.2021) https://doi.org/10.33407/itlt.v6i2.133
6. Антонов Ю.С., Космінська О.М. Методика аналізу тестових завдань на основі отриманих результатів. Інформаційні технології і засоби навчання. 2009. Т.12, №4. URL: https://journal.iitta.gov.ua/index.php/itlt/article/view/81/. (дата звертання: 21.09.2021) https://doi.org/10.33407/itlt.v12i4.81

УДК 004.8

Сніжинський М.В., студент 4 курсу спеціальності 122 «Комп'ютерні науки»
Потапова Н. А., к.е.н, доцент, доцент кафедри інформаційних технологій

ЗАСОБИ ЗАХИСТУ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖІ INTERNET

Донецький Національний університет імені В. Стуса, м. Вінниця

Сучасне розповсюдження з'єднань з мережею Internet, забезпечує інформаційними та комунікаційними ресурсами, але попри всі переваги приховує загрозу несанкціонованого доступу до конфіденційної інформації. Кожна установа, яка веде обмін даними у всесвітній мережі, повинна зіставляти можливі втрати з перевагами, що надає можливість виходу в Internet, та забезпечувати відповідний захист власних ресурсів.

Серед варіантів захисту web-серверів найпопулярнішим на сьогоднішній день є використання протоколу SSH — засіб організації безпечного доступу до комп 'ютерів під час роботи небезпечними каналами зв'язку. [1, 2]

SSH (Secure Shell) є мережевим протоколом, який використовується для віддаленого керування комп'ютером і передавання інформаційних пакетів. За функціональністю SSH схожий на протоколи Telnet і rlogin, але шифрує увесь трафік разом із паролями, що передаються.

Для організації безпечного доступу застосовується процедура аутентифікації з використанням асиметричного шифрування з відкритим ключем, що забезпечує вищий рівень безпеки, ніж при симетричному шифруванні, яке дозволяє заощаджувати процесорний час і використовується під час подальшого обміну даними.[4]

Протокол надає можливість підтвердження оригінальності хосту, з яким відбувається з 'єднання. SSH підтримує два основних протоколи: SSHv1 і SSHv2.