Формування рекомендацій для усунення наслідків мережевих атак

Суприган О.І., Гикава М.В.
Вінницький національний технічний університет
Вінниця, Україна
maria.gykava@gmail.com

Formating recommendations for solving the consequences of network attack

O. Supryhan , M.Hykava
Vinnytsia National Technical University
Vinnytsia, Ukraine
: maria.gykava@gmail.com

Анотація – у даній роботі розглядаються мережеві атаки та формування рекомендацій для усунення їх наслідків, а саме атаки переповнення буферу та DDoS-атаки. Виявлення атак та формування рекомендацій для усунення їх наслідків відбувається за допомогою використання принципів лінійної регресії та нелінійної динаміки.

Ключові слова – мережеві атаки, переповнення буферу, DDoS-атаки, нелінійна динаміка, лінійна регресія.

Abstract – In this paper network attacks are considered and recommendations are formulated to eliminate their effects, in particular attacks of buffer overflow and DDoS-attacks. Detection of attacks and the formulation of recommendations to eliminate their consequences is through the use of the principles of linear regression and nonlinear dynamics.

Keywords – network attacks, buffer overflows, DDoS-attacks, nonlinear dynamics, linear regression.

I. ВСТУП

Без належних заходів безпеки комп'ютерам в мережі загрожують самі різні фактори. Однією із самих серйозних являється загроза несанкціонованого доступу ззовні, в мережу, організації зломщиків (хакерів). Друга загроза – комп'ютерні віруси.

Мережева атака - дія, метою якого є захоплення контролю (підвищення прав) над віддаленою локальною обчислювальною системою [1].

Знання методів атак необхідне для появи необхідних методів захисту. Тому одним із найбільш актуальних питань безперебійного функціонування комп'ютерної системи, є питання забезпечення безпеки даних цієї системи.

Метою даної роботи є дослідження способів виявлення та формування рекомендацій усунення наслідків атаки на мережеві ресурси. Об'єктом дослідження являються атаки та їхній вплив на мережеві ресурси за їхньою активністю. Якщо немає безпосереднього впливу на роботу системи, але можливе порушення її політики безпеки, то на розподілену обчислювальну систему діє пасивний вплив атаки, в іншому випадку – якщо є безпосередній вплив на роботу системи (зміна конфігурації, порушення працездатності і т. д.) і порушується прийнята в ній політика безпеки, то діє активний вплив атаки. Практично всі типи віддалених атак мають активний вплив. Особливістю активного впливу в порівнянні з пасивним є принципова можливість його виявлення, так як в результаті його здійснення в системі відбуваються певні зміни.

Серед атак найбільш відомими являються атаки переповнення буферу та DDOS-атаки.

Переповнення стека/буфера (stack/buffer overflow) – результатом атаки є порушення умов цілісності, доступності та конфіденційності інформації. Методами захисту є використання спеціальних «безпечних» аналогів небезпечних функцій, заборона на використання коду в області стека, перевірка меж змінних при кожному доступі до них [2, 3].

DDOS-атаки - розподілені атаки, спрямовані на відмову в обслуговуванні, продовжують залишатися однією з найважливіших загроз в мережі. Атаки такого типу можуть швидко

виснажити мережеві ресурси або потужності сервера, що призведе до неможливості отримати доступ до ресурсу і викличе серію негативних наслідків [4]. Необхідно виявити DDOS-атаку на ранній стадії її дії для швидкого усунення наслідків атаки.

II. ФОРМУЛЮВАННЯ МОДЕЛІ

Для прогнозування впливу атаки на мережеві ресурси та дослідження її характеристик, для формування рекомендацій усунення наслідків атак, проведемо математичне дослідження.

Математичне моделювання є одним із основних сучасних методів дослідження. Для дослідження характеру поведінки системи під дією атаки, доцільно використовувати принципи регресії та нелінійної динаміки, які дозволять виявити динамічну зміну поведінки атаки.

При проведенні простої лінійної регресії основною задачею є визначення параметрів b і a. Після визначення цих параметрів, наприклад, можна спрогнозувати показник Y. Застосовуємо лінійну функцію виду:

$$K=f(x_1, x_2, m_1, m_2, a,b) \quad (1)$$

де x_1, x_2 – вхідні параметри системи;

m_1, m_2 – параметри атаки;

a, b – параметри, які визначають наслідки дії атаки;

При використанні лінійної регресії взаємозв'язок між даними моделюється за допомогою лінійних функцій, а невідомі параметри моделі оцінюються за вхідними даними. Подібно до інших методів регресійного аналізу лінійна регресія повертає розподіл умовної імовірності Y в залежності від X , що дає можливість зробити висновок про характер дії атаки на параметри системи та її регресування вцілому.

Для отримання оцінки параметрів лінійної функції регресії взята вибірка, яка складається з векторних змінних (X,Y):

$$Y=a+b\times X \quad (2)$$

де $X = f(m_1, m_2)$ – характеристика системи, що дозволяє визначити напрямок та інтенсивність процесу атаки.

Лінійна регресія оцінює коефіцієнти лінійного рівняння, яка показує залежність характеристик атак від формування рекомендацій щодо усунення дій атаки та містить одну або кілька незалежних змінних, що дозволяють найкращим чином передбачити значення залежної змінної.

Такий підхід лінійної регресії дозволяє визначити ступінь пошкоджень та спрогнозувати найбільш ймовірну атаку та необхідні дії для усунення її наслідків.

Для аналізу мережевих ресурсів з урахуванням виявлених властивостей дії атак визначимо $X = \{m_1, m_2, \dots m_n\}$, тоді

$$X = b_0 + b_1m_1 + b_2m_2 + \dots + b_nm_n \quad (3)$$

Для прогнозування необхідних дій, що гарантують коректну роботу системи після виявлення атаки розглянемо метод Лагранжа, що дозволяє виконати згладжування атаки (нейтралізацію). Розглянемо квадратичну форму:

$$A(x_i, m_k) = \sum_{i,k=1}^{n} a_{ik} \times x_i \times m_k \quad (4)$$

$$B(x_i, m_k) = \sum_{i,k=1}^{n} b_{ik} \times x_i \times m_k \quad (5)$$

Розглянемо функцію F, яка описує прогнозовані наслідки дії атаки

$$F = f(A, B) \quad (6)$$

$$A(x_i, m_k) = \frac{1}{4a_{ij}}\left(\frac{\partial A}{\partial x_i}\right)^2 + A_1(x_i, m_k) \quad (7)$$

$$B(x_i, m_k) = \frac{1}{4b_{ij}}\left(\frac{\partial B}{\partial x_i}\right)^2 + B_1(x_i, m_k) \quad (8)$$

$$F(A,B) = \frac{1}{4ab}\left[\left(\frac{\partial A}{\partial x_i} + \frac{\partial A}{\partial x_k}\right)^2 - \left(\frac{\partial B}{\partial x_i} + \frac{\partial B}{\partial x_k}\right)^2\right] + A + B \quad (9)$$

де A – показник реакції системи на атаку;

B – показник прогнозування дії системи для усунення наслідків атаки;

i – номер елементу атаки в певний проміжок часу;

k – показник кількості атак.

Многочлен Лагранжа застосовують при наближенні табличних записів даних у вигляді функції, яка є дуже хорошим наближенням, якщо для функцій зі швидкозмінною похідною обрана мала кількість вузлів інтерполяції.

Для діагностування мережевих ресурсів на наявність атак та в подальшому формуванні рекомендацій щодо їх усунення застосовується пасивне діагностування. Пасивний метод діагностики полягає у виявленні місць ураження атакою та розпізнавання атаки за її відомими характеристиками. Цей метод є оптимальним у разі дії невеликої кількості атак.

За допомогою нелінійної динаміки є можливим по початковим характеристикам атаки спрогнозувати, як саме ця атака зможе вплинути на мережеві ресурси і відповідно, це дає змогу сформувати рекомендації щодо усунення її наслідків [5]. Для цього використовуємо динамічну системи. Для опису стану динамічної системи використовується формула:

$$x = [x_1, x_2, \dots, x_n] \quad (10)$$

де $\mathbf{x}$ – характеристика акати, яка діє на мережеві ресурси.

Задаємо всі характеристики можливої атаки по яким буде проводитись діагностування мережевих ресурсів, щоб виявити найбільш ймовірну атаку.

Для встановлення часу виявлення та розпізнавання атаки по характеристикам використовуємо зміну системи, а саме:

$$\frac{dx_i}{dt} = F_i[x_1, x_2, \dots, x_n] \qquad (11)$$

де t – час дії атаки, протягом якої буде відбуватися діагностування і розпізнавання;

Отже, враховуючи діагностування мережевих ресурсів на наявність атаки, місце ураження атакою, час її виявлення, визначення характеристик атаки, можливо сформувати найбільш ймовірні рекомендації щодо усунення її наслідків.

Представимо структурну схему діагностування мережевих ресурсів на наявність атаки та формування рекомендацій щодо їх усунення.

На початковому етапі потік інформації аналізується на наявність атаки. Якщо пошкоджень не виявлено передається інформація, якщо виявлено атаку, визначається за характеристиками найбільш ймовірна атака. Після розпізнавання атаки формуємо рекомендації щодо усунення її наслідків.

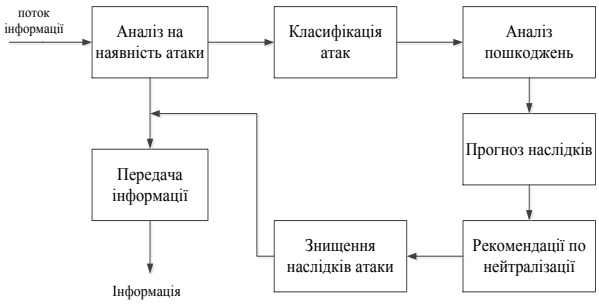

Рис. 1. Структурна схема діагностування мережевих ресурсів

Для діагностування мережевих ресурсів на наявність атак та формування рекомендацій усунення наслідків їх дії застосовується експертна система. Результат експертної системи формування рекомендацій для усунення наслідків мережевих атак повинний містити всі можливі способи ліквідації цих наслідків. Відбувається діагностування мережевих ресурсів на виявлення виду атаки, перевіряються всі характеристики цієї атаки і виходячи з результатів проводиться формування рекомендацій.

Інструментальні засоби експертної системи (ЕС) легко інтегруються з іншими інформаційними технологіями і засобами, зокрема з СКБД, контролерами, концентраторами даних. ЕС можуть розроблятися з дотриманнями стандартів, котрі забезпечують відкритість і переміщуваність [6, 7]. Тому використання ЕС для формування рекомендацій усунення наслідків атак є найбільш оптимальним.

III. МЕТОДИКА ФОРМУВАННЯ РЕКОМЕНДАЦІЙ

Початковим етапом являється авторизація користувача, після успішної автентифікації клієнтська частина відправляє запит на початок тестування мережі до серверної частини. В свою чергу сервер здійснює запити на отримання потрібної інформації із бази даних та отримує відповідь.

Основним процесом являється серверна частина, адже в даному процесі закладена головна логіка роботи програми.

Можливості мови програмування залежать від сфери застосування та наявності альтернативних реалізацій.

Робота програми базується на основі класичної трирівневої архітектури: клієнт-сервіси-зберігання. Кожен із рівнів має своє чітке призначення, розробляється окремо і може бути замінений на іншу реалізацію за умови збереження інтерфейсу (рис.2.).

Призначення рівнів:

- клієнт - генерує код, який буде відправлено браузеру користувача. Цей код у браузері буде перетворено у звичайну веб-сторінку. Задача клієнт опитати поточний стан програми і згенерувати такий код. Користувач звертається тільки до клієнта, а клієнт може звертатися тільки до сервісів;
- сервіси - код який вирішує основну логіку роботи нашої програми - тестування комп’ютерної мережі. Сервіси розуміють повідомлення із клієнта і повідомляють шар зберігання про необхідність пошуку даних, які необхідні для забезпечення логіки роботи програми;
- зберігання - код, який має розуміти запити від сервісів і вміти співпрацювати із базую даних та надсилати відповідь назад сервісам із корисною інформацією з БД.

При розгляді найбільш розповсюдженіших мережевих атаки та їх характеристик, показана можливість виявлення дії атаки на мережеві ресурси, яка базується на створені математичної моделі діагностування мережевих ресурсів, що виявляє дію атаки та визначає ступінь пошкодження і формує рекомендації стосовно усунення наслідків атак.

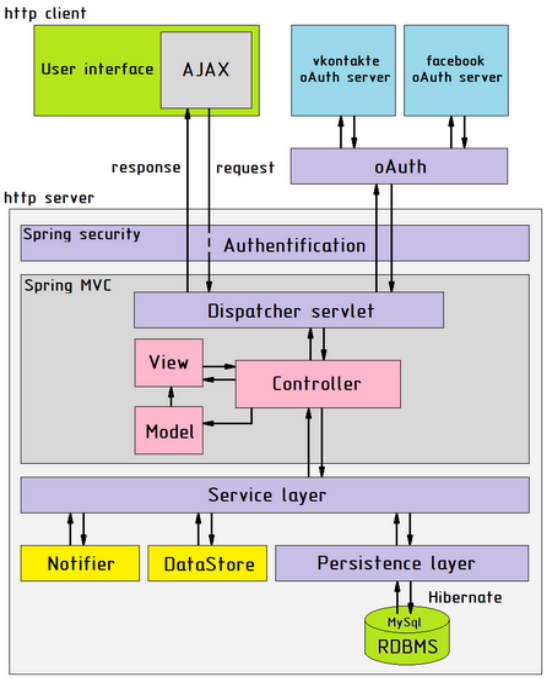

Рис. 2. Архітектура програмного забезпечення

Тестування показало результат, який підтверджує збільшення швидкості виявлення дії атаки, ймовірність розпізнавання самої атаки та методів усунення її наслідків.

ЛІТЕРАТУРА REFERENCES

[1] А. Е. Боршевников. Сетевые атаки. Виды. Способы борьбы [Текст] // Современные тенденции технических наук: материалы междунар. науч. конф. — Уфа, лето 2011. — С. 8-13.

[2] Современные тенденции технических наук: материалы междунар. заоч. науч. конф. Г.Д. Ахметовой. – Уфа, лето 2011. – С. 78.

[3] Peter Bright. How security flaws work: The buffer overflow [Електронний ресурс]. — Режим доступу: https://habrahabr.ru/post/266591

[4] Методы защиты от DDOS нападений [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/analytics/216251.php.

[5] В.С. Анищенко, Т.Е. Вадивасова. Лекции по нелинейной динамике. – Издательство Саратовского университета, 2010. – с. 350.

[6] Б.М. Герасимов. Системи штучного інтелекту: Навч. посібник / Б. М. Герасимов, В. М. Локазюк, О. Г. Оксіюк, О. В. Поморова. – К.: Вид-во Європ. ун-ту, 2007. – 335 с.

[7] В.М. Локазюк. Засади системи підтримки прийняття рішень на основі комп'ютерних систем та їх компонентів: Навч. Посібник для вузів. – Хмельницький, «ПП Гонта», 2011. - с. 337.