Туржанська І.Д.

ЗАСТОСУВАННЯ ТЕОРІЇ ГРАФІВ ДЛЯ ОПИСУ КІБЕРАТАК

Вінницький національний технічний університет

Анотація

У статті наведено основні підходи щодо застосування теорії графів у сфері кібербезпеки, окрім цього, було розглянуто найпопулярніші види кібератак.

Ключові слова: теорія графів, кібербезпека, інформаційні технології.

Abstract

The article presents the main approaches to the application of graph theory in the field of cyber security, in addition, the most popular types of cyber attacks were considered.

Keywords: graph theory, cybersecurity, information technology.

Вступ

Кібератаки є серйозною загрозою для інформаційних систем та мереж. Вони можуть призвести до крадіжки даних, порушення роботи систем, а в деяких випадках навіть до фізичних збитків. Фахівці з кібербезпеки намагаються вдосконалювати засоби виявлення недоліків в комп'ютерних системах. Моделювання кібератак використовуючи засоби теорії графів має ряд переваг. По-перше, це дозволяє візуалізувати кібератаки, що робить їх легше зрозуміти та проаналізувати. По-друге, цей підхід дозволяє враховувати складність кібератак, яка може включати кілька етапів та взаємозв'язки між різними компонентами інформаційної системи. Саме тому було вирішено проаналізувати етапи моделювання кібератак засобами теорії графів.

Результати досліджень

На початку дослідження варто уточнити визначення понять, які безпосередньо стосуються теми. Отже, теорія графів – це розділ математики, що вивчає властивості графів[1]. Граф – це модель, що складається з вершин та ребер, що безпосередньо з'єднують ці вершини. Оскільки поняття графа є настільки загальним, то вони використовуються у багатьох сферах життя, зокрема у схемотехніці, економіці, логістиці тощо.

У цьому контексті, експлойт – це програма, код або алгоритм, що використовує вразливості в програмному забезпеченні для проведення кібератак. Кібератаки спрямовані на отримання несанкціонованого доступу до комп'ютерних мереж з метою завдання шкоди важливим файлам. Оскільки технології постійно розвиваються, появляються нові методи здійснення таких атак[2]. Таким чином, розвиток галузі кібербезпеки стає необхідністю для запобігання витоку чи пошкодження конфіденційних документів. Серед найпоширеніших видів кібератак можна виділити:

- SQL-ін'єкції;
- фішинг
- DDoS-атака та інші.

Метою фішингових атак є викрадення або пошкодження інформації, шляхом отримання доступу до персональних даних користувача[3]. Існує декілька найпоширеніших видів фішингових атак, зокрема: електронні листи, смс, цільовий фішинг, спеціальні програми тощо. Принцип отримання даних дещо подібний – жертві приходить лист, що дещо схожий на звичайне повідомлення від популярних сервісів. У випадку якщо людина, що отримала таке повідомлення, перейде за гіперпосиланням, її дані будуть передані зловмисникам.

SQL-ін'єкція – це метод отримання доступу до бази даних, шляхом введення шкідливого коду під час маніпуляцій із таблицями баз даних. Такий метод зазвичай використовують ті, хто має безпосередній доступ до бекенду сервісів. Наприклад, існує запит на пошук певного значення в таблиці (SELECT * FROM users WHERE user_id = 22), в даному випадку користувач отримає дані про поле в таблиці, де значення user_id дорівнює 22. Проте якщо користувач введе запит (SELECT * FROM users WHERE user_id = 20; DROP TABLE users;), то разом із отриманням даних про поле, таблицю users буде

видалено[4]. Таким самим чином можливий і витік конфіденційної інформації, якщо використовувати завжди істинну умову.

DDoS-атака в свою чергу направлена на порушення функціонування роботи інтернет-сервісів шляхом їх перевантаження. Зазвичай жертвами таких атак стають ігрові сервери та телекомунікації. Зловмисники наповнюють сервіси фальшивим трафіком, що в свою чергу вичерпує ресурс сервісу, це призводить до погіршення роботи або навіть повного відключення[5].

Використання теорії графів у кібербезпеці відкриває нові можливості у проектуванні можливих сценаріїв кібератак. Наприклад, за допомогою графів можна провести аналіз топології мережі. Такий підхід дозволяє змоделювати усі можливі шляхи атаки на різних рівнях, що в свою чергу надає краще розуміння про те, як окремі або загальні компоненти системи впливають на безпеку системи[6].

Також графи можна використовувати для моделювання атак. Для цього створюється граф атаки, в якому враховуються множини запитів, реакцій системи, експлойтів, вразливостей тощо. На основі чого, будуються графи залежності вразливостей для оцінки впливу атак, в яких відносини між атаками та вразливостями описуються кон'юкціями та диз'юнкціями. Після цього, розраховуються ймовірнісний граф атаки, у якому в свою чергу враховується часовий розподіл для кожного етапу кібератаки.

Після проведення моделювання атак та вразилостей, будується граф залежності. Так як інформаційні системи складаються з великої кількості програмного та апаратного забезпечення, що взаємопов'язані між собою, вводять моделі залежностей окремих компонентів[6]:

- надмірності (залежність від надмірних компонентів);
- деградації (при виході з ладу одного компоненту, система частково втрачає роботоспроможність);
- повної залежності (при виході з ладу одного компоненту, всі залежні компоненти перестають функціонувати).

Такий підхід дозволяє скласти систему рівнянь, яка буде відображати стан різних компонентів інформаційної системи та ступінь їх залежності задля прогнозування розвитку багатоступеневих складних атак та знайти можливі варіанти захисту.

Висновок

В процесі дослідження можна відзначити, що проблема кібербезпеки є досить актуальною, адже зловмисники вдосконалюють та створюють нові методи здійснення кібератак. Наразі існує механізм моделювання таких атак використовуючи засоби теорії графів. Це дозволяє спеціалістам з кібербезпеки краще виявляти вразливості в комп'ютерних системах, вираховувати та прогнозувати вразливості та знаходити варіанти захисту від майбутніх атак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Bender Edward A. Lists, Decisions and Graphs. With an Introduction to Probability. / Bender Edward A., Williamson S. Gill., 2010.
2. Що таке кібератака? | Захисний комплекс Microsoft [Електронний ресурс] Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack
3. Що таке фішинг? | Захисний комплекс Microsoft [Електронний ресурс] Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing
4. SQL-ін'єкції | aCode [Електронний ресурс] Режим доступу: https://acode.com.ua/sql-injection/
5. Що таке DDoS-атака? | Захисний комплекс Microsoft [Електронний ресурс] Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-ddos-attack
6. The Cyberattack Simulation by Graph Theory [Електронний ресурс] Режим доступу: https://doi.org/10.31673/2409-7292.2019.040611

Туржанська Ірина Дмитрівна – студентка групи 2БС-22Б, факультет інформаційних технологій і комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: turzhanskayaryna@gmail.com

Науковий керівник – Кондратенко Наталія Романівна

Turzhanska Iryna Dmitrievna – student of group 2BS-22B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: turzhanskayaryna@gmail.com

Supervisor – Nataliya Romanivna Kondratenko