Список використаних джерел

1.Шеннон К. Работы по теории информации и кибернетике. – М: Изд. иностр. лит., 2002.
2. Гиббс Дж. Термодинамика. Статистическая механика. Серия: Классики науки. М.: Наука, 1982. 584 с.
3. Thimas H. Cormen; Charles E. Leiserson; Ronald L. Rivest; Clifford Stein. Introduction to Algorithms (2nd ed.) The MIT Press. ISBN 0-07-013151-1
4. Пресс И. А. Основы общей химии для самостоятельного изучения. – 2-е изд., перераб. – СПб.: Лань, 2012. – 496 с. – ISBN 978-5-8114-1203-7.

УДК 004.056.53

Юкальчук А.І., здобувач 3 курсу
спеціальність 125 «Кібербезпека»
Наукові керівники:
Загоруйко Л.В., к.т.н., доцент, доцент кафедри інформаційних технологій
Мартьянова Т.А. к.т.н., ст. викладач кафедри інформаційних технологій

МОДЕЛЮВАННЯ АРТ-АТАК, ЩО ЕКСПЛУАТУЮТЬ ВРАЗЛИВІСТЬ ZEROLOGON

Донецький національний університет ім. Василя Стуса, м. Вінниця

В роботі наводиться приклад дослідження реалізації комп'ютерної атаки у типовій інформаційній інфраструктурі, яка вміщує корпоративну мережу з доменною архітектурою та автоматизовану систему управління технологічним процесом. Для розглянутого прикладу визначено оптимальні значення часових параметрів безпеки.

Практична значимість: результати дослідження можна використовувати при проектуванні та тестуванні систем безпеки об'єктів критичної інформаційної інфраструктури з урахуванням параметрів системи безпеки і порушника які задаються.

Ключові слова: значущий об’єкт, комп’ютерна атака, критична інформаційна інфраструктура, марківський процес, система безпеки.

Вступ

Наразі питання безпеки інформаційних систем, інформаційно-телекомунікаційних мереж та автоматизованих систем управління суб'єктів критичної інформаційної інфраструктури (КІІ) набувають важливого значення. Форсування створення систем безпеки значущих об'єктів КІІ визначається не лише вимогами нормативно-правових та керівних документів у галузі інформаційної безпеки, а й різким зростанням кількості повідомлень про комп'ютерні інциденти на об'єктах КІІ України, а також на об'єктах інформаційної інфраструктури зарубіжних країн.

У цих умовах особливо важливими є питання оцінки ефективності систем безпеки значущих об'єктів КІІ. Тому в ході проектування системи безпеки значущого об'єкта з метою тестування рекомендовано її макетування або створення тестового середовища з використанням засобів та методів моделювання.

Необхідність оцінки ефективності систем безпеки, що створюються, значущих об'єктів КІІ визначає потребу у розробці простих та адекватних математичних моделей реалізації комп'ютерних атак. Використання методів математичного моделювання в ході проектування системи безпеки значущого об'єкта дозволяє без значних витрат та впливу на функціонування об'єкта обґрунтувати вимоги до системи в цілому або її окремих частин.

Проведений аналіз методичного забезпечення [1-5], що застосовується при дослідженні в галузі забезпечення комп'ютерної безпеки, показав, що у разі складних систем, до яких належать значущі об'єкти КІІ, найбільш підходящими методами та підходами до моделювання комп'ютерних атак є використання теорії марківських випадкових процесів.

Одним із найбільш небезпечних сценаріїв цілеспрямованих програмних впливів на об'єкти КІІ та мережі електрозв'язку в даний час вважається комп'ютерна атака, що реалізується шляхом експлуатації вразливості Zerologon. Ця вразливість заснована на дефекті в реалізації процедур аутентифікації на контролері домену і дозволяє порушнику отримати привілеї адміністратора домену *Active Directory* і потім реалізувати використання корисного навантаження (скрипту). Зазначений дефект є у реалізації криптографічного перетворення, що використовується при аутентифікації в протоколі *Microsoft Windows Netlogon Remote Protocol*, що використовується для зв'язку робочих станцій та серверів з контролерами домену захищеним каналом.

Атака *Zerologon* реалізується шляхом скидання пароля облікового запису *Active Directory* контролера домену в домені в порожній рядок. Це дозволяє порушникові з мережним доступом до контролера домену, що не пройшов перевірку автентичності, аутентифікуватися і отримати доступ до командної консолі на іншому або цьому ж контролері домену і повністю контролювати весь об'єкт КІІ. Тому як тестовий програмний вплив на об'єкти КІІ при моделюванні розглядатимемо саме комп'ютерну атаку, що експлуатує вразливість *Zerologon*.

У ході реалізації подібної атаки з різними варіантами векторів атак порушник має успішно пройти такі етапи:

- отримання доступу (фізичного чи віддаленого) до мережі КІІ;
- сканування ресурсів корпоративної локальної обчислювальної мережі (ЛОМ) з метою одержання відомостей про *IP*-адреси контролерів домену, їх *NetBIOS*-іменах, назвах домену;
- вилучення з дампа пам'яті машинного облікового запису контролера домену та підвищення прав доступу в атакованому домені;
- ескалація привілеїв адміністратора домену та використання корисного навантаження (скрипту);

- віддалене підключення до автоматизованого робочого місця (АРМ) оператора технологічної установки;
- Пошук файлів, що містять проекти управління, на АРМ оператора технологічної установки;
- блокування доменного облікового запису оператора технологічної установки;
- віддалене вимкнення АРМ оператора об'єкта КІІ.

Оскільки розгалужень та відповідних ним логічних умов реалізації комп'ютерної атаки, що експлуатує вразливість Zerologon, немає, то для її моделювання може бути використаний апарат марківських випадкових процесів.

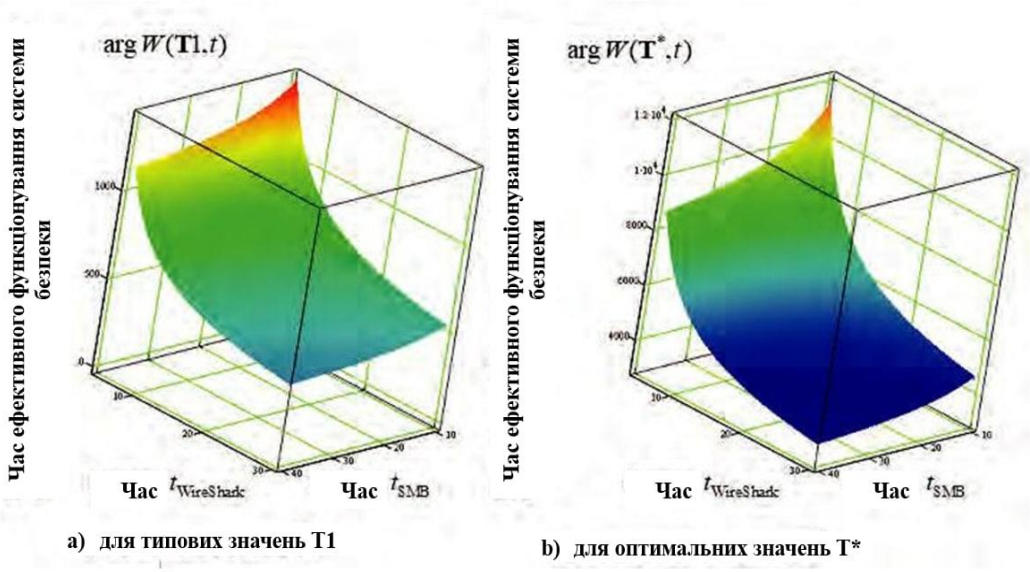

Рис. 1. Поверхня залежності часу ефективного функціонування системи безпеки $t_{захисту}$ для типових та оптимальних значень параметрів захисту.

Як видно із рис. 1, максимальне значення часу ефективного функціонування системи безпеки в умовах проведення атак, що експлуатують уразливість *Zerologon*, визначається оперативністю (швидкістю) реагування на ті чи інші інциденти комп'ютерної безпеки. Наприклад, зниження часу реагування на виявлення, аналіз та вжиття заходів щодо запобігання повторному пасивному збору (прослуховування) інформації про підключені до мережі пристрої $t_{WireShark}$ або направного сканування за допомогою спеціалізованого програмного забезпечення підключених до мережі пристроїв з метою отримання конфігураційної інформації компонентів систем та мереж t_{SMB} з 30 до 10 хвилин дозволяє суттєво продовжити час ефективного функціонування системи безпеки.

Висновки

Таким чином, в умовах зростання загроз реалізації комп'ютерних атак проти значущих об'єктів КІІ актуальним завданням є розробка простих та адекватних математичних моделей, що дозволяють протестувати та оцінити ефективність системи безпеки під час її проектування. Застосування теорії марківських процесів дозволяє досить точно формалізувати процес комп'ютерної атаки.

Застосування чисельних методів розв'язання систем однорідних диференціальних рівнянь, реалізованих у середовищі проведення обчислювальних розрахунків *Matlab*, дозволило отримати графічні залежності ймовірностей знаходження в тому чи іншому стані системи, що моделюється. Рекомендовані тимчасові параметри раціональних засобів захисту на різних етапах комп'ютерної атаки, що експлуатує вразливість *Zerologon*, дозволяють забезпечити безпеку та підвищити час стійкого функціонування критичної інформаційної інфраструктури.

Список використаних джерел

1. Маслова Н.А. Методи оцінки ефективності систем захисту інформаційних систем//Штучний інтелект. 2008. № 4. С. 253-264.

2. Котенко Д.І., Котенко І.В., Саєнко І.Б. Методи та засоби моделювання атак у великих комп'ютерних мережах: стан проблеми // Праці СПІІРАН. 2012. № 3 (22). З. 5-30.

3. Котенко Д.І., Котенко І.В., Моделювання атак у великих комп'ютерних мережах // Технічні науки - від теорії до практики. 2013. № 17-1. З. 12-16.

4. Добришин М.М., Закалкін П.В. Модель комп'ютерної атаки типу «Phishing» на локальну комп'ютерну мережу // Питання кібербезпеки. 2021. № 2(42). З. 17-25. DOI: 10.21681/2311-3456-2021-2-17-25.

5. Вентцель Є.С., Овчаров Л.А. Теорія випадкових процесів та її інженерні програми. М: Вища школа, 2000. 383 с.

УДК 004.415.2+004.652.5

Юстименко Є. А. здобувач
Труханська В. О. здобувач
Горяшин А.С. асистент
кафедри інформаційних технологій

ПРОЕКТУВАННЯ ОБ'ЄКТНО-ОРІЄНТОВНИХ БАЗ ДАНИХ

Донецький національний університет імені Василя Стуса, м. Вінниця

Створення перших об'єктно-орієнтовних баз даних, надалі ООБД, почалося в кінці минулого століття. З стрімким розвитком програмного забезпечення потрібно було стрімко розвивати системи організації та зберігання даних. При цьому планувалось, що такі бази даних стануть основним напрямом використання, але цього не сталось. Нам зрозуміло, що зараз найпопулярніші реляційні моделі баз даних, з представленням даних у таблицях. Однак в наш час збільшується кількість спільнот, яка починає надавати перевагу саме ООБД.

Об'єктно-орієнтовані бази даних – це запрограмовані бази даних, які зберігають дані у вигляді об'єктів і їх зв'язки без стовпців і рядків, що робить їх більш придатними для програмного забезпечення, яке працює з великими об'ємами даних [2]. Графічно ООБД можна зобразити в вигляді дерева. База