УДК 004.49

Розробка автоматизованої системи для проведення аудиту інформаційної безпеки комп'ютерних систем та мереж «Vine»

Мелешко Є.В., канд. техн. наук, доцент, elismeleshko@gmail.com
Хох В.Д., лаборант, ch2oa516@gmail.com
Кіровоградський національний технічний університет, м. Кіровоград

Аудит інформаційної безпеки (АІБ) – це системний процес одержання об'єктивних якісних і кількісних оцінок поточного стану безпеки інформаційної системи або інформаційно-телекомунікаційної системи, комплексна оцінка рівня інформаційної безпеки системи, що проходить аудит з урахуванням трьох факторів: персоналу, процесів та технологій. Порівняльний аналіз поточного стану інформаційної системи, що визначається за підсумками анкетування, з тестовою моделлю вимог стандарту ISO 27001. Аудит ІС та ІТС проводиться на відповідність вимогам [1]:

– Нормативних документів у галузі технічного захисту інформації України (НД ТЗІ).
– ISO/IEC 27001:2005 (поточна редакція 2013).
– PCI DSS.

Ціллю розроблюваної системи є часткова або повна автоматизація АІБ комп'ютерних систем та мереж, шляхом моделювання ситуації атаки на систему, що проходить аудит.

До найближчих аналогів даної системи можна віднести комплекси програмного забезпечення на зразок Armitage, який, по-суті, є графічним інтерфейсом, що об'єднує Metasploit Framework, сканер nMap та має інтегровану систему пошуку по базі експлойтів Metasploit Framework, на основі результатів сканування. Armitage не має інтегрованої експертної системи, а відтак не може генерувати певні нові рішення.

Розроблювана система відрізняється від подібних, використанням у своєму ядрі експертної системи (ЕС). Розроблена ЕС використовує апарат нечіткої логіки та продукційну модель представлення знань. Однією з особливостей розробленої системи є реалізація механізму просторів імен, що дозволяє значно пришвидшити роботу системи, а також, у деяких випадках, відновити певні данні, які були не помічені або проігноровані користувачем-оператором. Механізм простору імен споріднений з механізмом простору імен в Сі-подібних мовах програмування у тому сенсі, що простір імен визначає область видимості фактів та продукцій. Один і той же факт може бути по-різному обчислений у різних просторах імен. До того ж під час роботи експертів по заповненню або редагуванню бази знань може виникати ситуація, коли продукція використовує декілька фактів з різних просторів імен – система спроможна відтворити такі зв'язки, увімкнувши додатково певні простори імен. Так користувачу надається більше простору для творчого пошуку вирішення проблеми, а на систему лягає задача забезпечити працездатність цих рішень. Схема побудови або відновлення подібних зв'язків наведена на рис. 1.

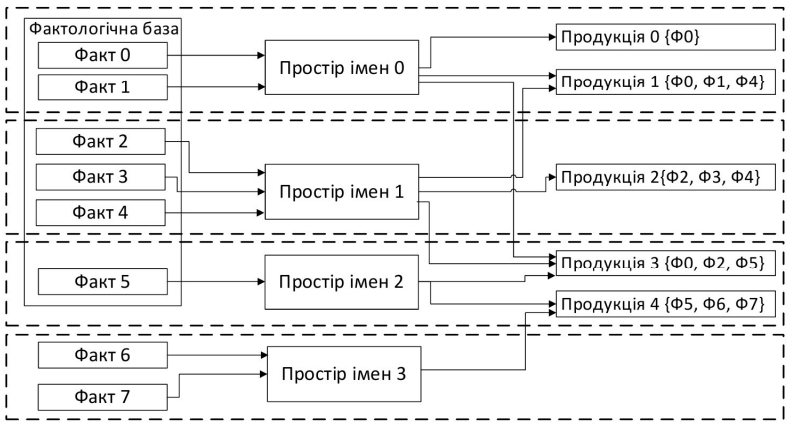

Рисунок 1 – Схема відновлення зв'язків за допомогою механізму простору імен

Один з механізмів, який дає змогу автоматизувати процес керування простором імен і зробити його більш точнішим – механізм фактів-трігерів. Факт-трігер – це такий факт, значення якого явно вказує на певний простір імен, наприклад, якщо системі доведеться проводити АІБ мережі, в якій усі пристрої використовують одну й ту ж саму операційну систему і її версію. Такий механізм значно зменшить кількість проходів по базі знань.

Роботу системи можна поділити на 2 етапи. На І етапі користувач щільно співпрацює з ЕС, намагаючись якомога точніше охарактеризувати область своїх інтересів, на цьому етапі формуються дві перші версії фактологічної бази (ФБ):

– 1 версія – формується повністю на основі вказівок користувача, йому доступна можливість додавання або виключення фактів з ФБ, вільно змінювати властивості фактів.

– 2 версія – формується із використанням механізму відновлення зв'язків за допомогою просторів імен. Система дає змогу користувачу надати додаткові данні, які їй невідомі. Користувач не може виключати факти, але може додавати або змінювати властивість факту на факт-трігер або звичайний.

На ІІ етапі система розробляє своє рішення та надає набір інструкцій, які будуть надіслані провайдеру інструментів за допомогою протоколу SSH. Вхідними даними на цьому етапі є ФБ з визначеними фактами. Вихідні дані – черга з блоками інструкцій. Черга надається як результат роботи ЕС на розсуд користувача, який сам приймає рішення, який з блоків застосувати, або модифікувати і потім застосувати. Схему роботи системи зображено на рис. 2.

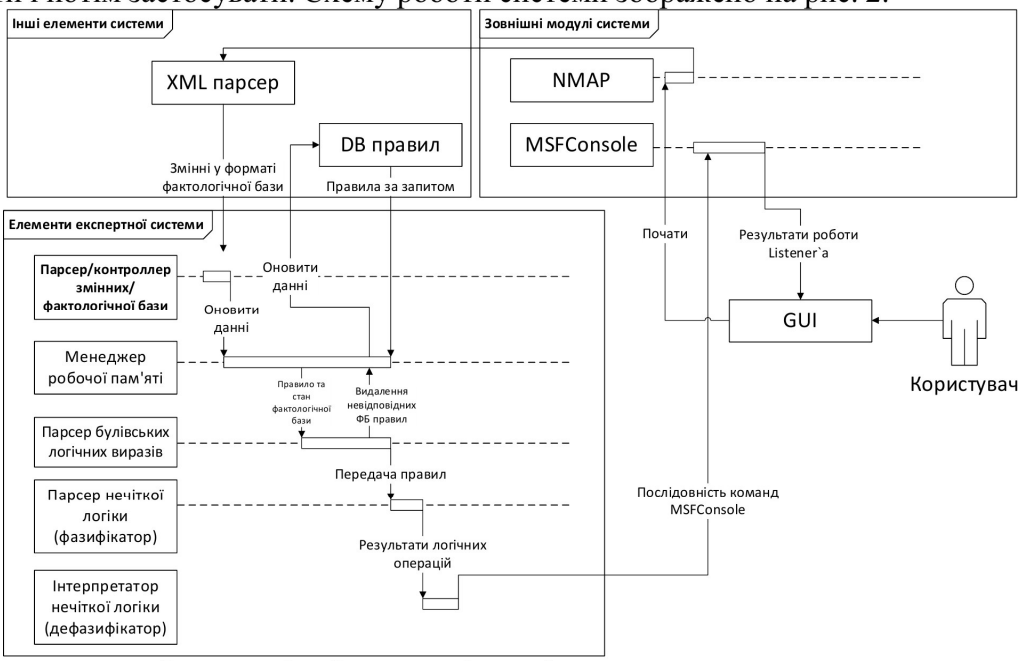

Рисунок 2 – Загальна функціональна схема системи

Розроблювана система досить гнучка, що дозволяє застосовувати її з OSSTMM (Open Source Security Methodology Manual) [3] та методологією NIST (National Institute of Standards and Technology) [4]. В наступних версіях розробленої системи планується реалізувати:

– Використання розподілених сканувань систем, що підлягають АІБ.
– Автоматизація процесів розподілених сканувань та атак за допомогою ЕС.
– Розробка протоколів ефективного розподілу навантаження серед вузлів системи.

Ефективний розподіл завдань серед вузлів планується розробляти на основі протоколів рівнорангових мереж, на кшталт протоколу Kademlia.

Список літератури

4. Аудит інформаційної безпеки інформаційних систем та інформаційно-телекомунікаційних систем [Електронний ресурс]. – Режим доступу: http://www.uss.gov.ua/audit-of-information-security

5. iWar: A new threat, its convenience and our increasing vulnerability [Електронний ресурс]. – Режим доступу: http://www.nato.int/docu/review/2007/issue4/english/analysis2.html

6. Open Source Security Testing Methodology Manual (OSSTMM) [Електронний ресурс]. – Режим доступу: http://www.isecom.org/research/osstmm.html

7. Technical Guide to Information Security Testing and Assessment [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf