Розробка автоматизованої системи виявлення, оцінки та розробки заходів по усуненню загроз в інформаційних системах

УДК 004.056.53

Віталій Хох[1], ЄлизаветаМелешко[2],
Валентина Сидоренко[3]

Центральноукраїнський національний технічний університет,
[1]vd.khokh@gmail.com, [2]elismeleshko@gmail.com,
[3]Valentina.18.02.1976@gmail.com

Метою даної роботи єрозробка автоматизованої системи для виявлення, оцінки та розробки заходів по усуненню загроз в інформаційних системах. В основі розроблюваної системи лежить експертна система на основі нечіткої логіки.

Система розробляється з розрахунку можливості її використання користувачем у 3 режимах, перший – режим, при якому система не має профілю системи, з якою взаємодіє(blackbox), другий – при якому система має набір правил, які побудовані виходячи зі специфіки системи, в залежності від кількості наданої інформації це режими whitета greybox.

Зупинимося на варіанті, коли система отримала інформацію про певну кількість сервісів, їх назви та версії. Отримана інформація буде поміщена у фактологічну базу. Фактологічна база системи є вираженням контексту(зовнішнього(C_{ext}) та внутрішнього(C_{int})), в якому функціонує досліджувана система:

$$C_{ext} = \{c_{ext_i} | c_{ext} \in [0,1]\} \text{ та } C_{int} = \{c_{int_i} | \in [0,\ 1]\}, \quad (1)$$

$$C = C_{ext} \cup C_{int}, \quad (2)$$

виходячи з цього ми робимо висновок, що стан певних факторів у контексті може призвести до певної події чи низки подій–множина *E*:

$$C = \{c | c_i > sensibility\} \rightarrow E = \{e | e_i > sensibility\} \rightarrow I \vee \overline{R}, \quad (3)$$

де *C*(контекст) –множина фактів фактологічної бази, а *sensibility* –прийняте значення «чутливості» системи.*I* – інцидент, а$\overline{R}$ – прийнятий ризик тобто:

$$\overline{R} = f(I), \quad (4)$$

який в свою чергу є вектором:

$$\overline{R} = \ < D,\ Fr,\ Co,\ Ch >, \quad (5)$$

де *D* – оцінка небезпеки ризику(експертна оцінка),*Fr* – ймовірність виникнення ризику,*Co*–оцінка вартості(експертна оцінка),*Ch* – характеристика ризику(експертні данні).

Після проходження всіх запланованих тестів і заповнення фактологічної бази починається формування списку правил-кандидатів, що будуть застосовані до поточної фактологічної бази. Кожен факт, що використовується у правилі подано у вигляді нечіткої змінної а саме:

$$< x, \mu f(x), min, max >, \quad (6)$$

де *x*–поточне значення змінної,*min*та *max*– значення що визначають границі змінної а $\mu f(x)$ – характеристична функція:

$$\mu A(x) = \frac{1}{1 + \left(\frac{x - x_c^{fi}}{range}\right)^{sensibility}}, \quad (7)$$

де *range* – це коефіцієнт, що визначає діапазон граничного значення змінної, при якому змінна буде набувати значення істини, а *fi*– може набувати значень 1, 2 або 3, тоді:

$$x_c^{fi} \in \left[min, \ \frac{min+max}{2}\right] \text{якщо} fi = 1, \quad (8)$$

$$x_c^{fi} = \frac{min+max}{2} \text{якщо} fi = 2, \quad (9)$$

$$x_c^{fi} \in \left[\frac{min + max}{2}, \ max\right] \text{якщо} fi = 3. \quad (10)$$

Таким чином, після отримання даних про систему та сформувавши фактологічну базу з отриманих даних про сервіси, система починає формувати множину*C*зважаючи на те, що значення$sensibility$– визначається в залежності від рівня можливих втрат у разі реалізації відомих загроз для сервісу, значення *range* – визначається рівнем складності реалізації даної загрози. В множині *C*залишаються лише ті факти, поточне значення яких досягло граничного значення, що розраховано за формулою (7) - виконується пошук релевантних правил.Пошук виконується за відповідним блоком у записі бази знань – «правило використання», яке оперує чіткими значеннями:

$$F_1 \wedge F_2 \wedge F_3 \ldots F_n \quad (11)$$

де F_n – відповідний факт з множини *C*, у разі, якщо вираз набуває значення істини – виконується правило з відповідного запису бази знань.

Правило бази знань використовує змінні нечіткі, їх діапазони та характеристичні функції задано експертами зважаючи на контекст, до якого буде застосовуватись дане правило. Наприклад, у разі виявлення системою уразливого сервісуApacheCouchDBверсії 2.0.0, однозначно можливо сказати, що досліджувана система має критичну уразливість(CVE-2016-8742), але у правилі експерт зробить необхідні уточнення, що вразливість стосується лише Windowsверсій, якщо інформація про ОС не була зібрана у блоці даних, він може вказати системі на необхідність додаткового тесту у тому числі знизити рівень точності визначення ОС, адже достатньо буде знати що це ОС сімейства Windows, а також вказати в інформаційному блоку необхідні зміни у конфігурації сервісу, які згодом можливо буде використати у звіті. У випадках, коли система працює у режимі blackboxсаме експерт може надати у блоці даних необхідний набір інструкцій(у вигляді скрипту) для того, щоб перевірити можливість реалізації вразливості, у разі якщо вектор її реалізації віддалений.

Розроблювана система здатна автоматизовано виконувати регулярні перевірки досліджуваних систем, не потребує встановлення додаткового програмного забезпечення на стороні досліджуваних систем, здатна працювати у трьох режимах:black, greytawhitebox. Система здатна використовувати інструментарій, той самий, що використовують зловмисники.