КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (14), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.14.148157
УДК 004.82

Киричок Роман Васильович
доктор філософії
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0002-9919-9691
r.kyrychok@kubg.edu.ua

Бржевська Зореслава Михайлівна
доктор філософії
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0002-7029-9525
z.brzhevska@kubg.edu.ua

Гулак Геннадій Миколайович
доктор технічних наук, доцент
професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0001-9131-9233
h.hulak@kubg.edu.ua

Бессалов Анатолій Володимирович
д.т.н., професор,
професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-6967-5001
a.bessalov@kubg.edu.ua

Астапеня Володимир Михайлович
к.т.н., доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0003-0124-216X
v.astapenia@kubg.edu.ua

ПРАВИЛА РЕАЛІЗАЦІЇ ЕКСПЛОЙТІВ ПІД ЧАС АКТИВНОГО АНАЛІЗУ ЗАХИЩЕНОСТІ КОРПОРАТИВНИХ МЕРЕЖ НА ОСНОВІ НЕЧІТКОЇ ОЦІНКИ ЯКОСТІ МЕХАНІЗМУ ВАЛІДАЦІЇ ВРАЗЛИВОСТЕЙ

Анотація. Динаміка зростання кількості вразливостей програмних та апаратних платформ корпоративних мереж, загальнодоступність модулів експлойтів даних вразливостей в мережах Інтернет та Даркнет, наряду з відсутністю достатньої кількості висококваліфікованих фахівців з кібербезпеки, робить проблему ефективної автоматизації превентивних механізмів захисту інформації досить актуальною. Зокрема, базові алгоритми послідовної реалізації експлойтів закладені в засоби експлуатації вразливостей є досить примітивними, а запропоновані підходи щодо їх покращення, потребують постійної адаптації математичних моделей реалізації атакуючих дій. Цим і обґрунтовується напрям даного дослідження. В роботі розглядається проблематика формування правил прийняття рішень щодо реалізації експлойтів вразливостей під час проведення активного аналізу захищеності корпоративних мереж. На основі результатів аналізу кількісних показників якості роботи механізму валідації виявлених вразливостей та використанні методів нечіткої логіки було сформовано нечітку систему, визначено функції належності для кожної з лінгвістичних змінних та побудовано базу знань, що дозволяє визначити рівень якості роботи механізму валідації виявлених вразливостей на основі всієї наявної інформації. Водночас, задля

виключення «людського фактору» допущення помилки при валідації вразливостей, ґрунтуючись на сформованій нечіткій базі знань та визначених рівнях ефективності модулів експлойтів вразливостей, сформовано правила реалізації окремих модулів експлойтів під час проведення активного аналізу захищеності корпоративної мережі. Отримані результати надають можливість створювати експертні системи діагностування ефективності механізму валідації виявлених вразливостей цільових систем, а також допомагають вирішити питання відсутності кваліфікованих спеціалістів з аналізу та підтримки належного рівня інформаційної безпеки корпоративних мереж.

Ключові слова: активний аналіз захищеності; корпоративна мережа; експлойт; валідація вразливостей; нечітка логіка.

ВСТУП

Майже щоденно, з інформаційних медіа ресурсів ми дізнаємося про нові витоки інформації та зломи, від яких страждають одні із найбільших у своїх галузях компанії. Хоча, слід відзначити, що це лише незначна частина загальнодоступної інформації щодо успішно реалізованих кібератак. Більшою повнотою та структурованістю володіють щорічні звіти провідних організацій з розслідувань корпоративних кіберінцидентів та аналізу ризиків.

Так, до прикладу, одним із останніх звітів, на який слід звернути увагу є «State of Cybersecurity Resilience 2021» [1], випущений в листопаді 2021 року компанією Accenture. Дане дослідження відповідає на одне з головних питань сьогодення в сфері забезпечення інформаційної безпеки та мінімізації кіберризиків, а саме: наскільки ефективні заходи з захисту своїх корпоративних мереж вживають компанії. Командою Accenture Research було опитано 4744 керівників компаній з річним доходом не менше 1 млрд доларів з 23 галузей у 18 країнах світу. За опублікованою інформацією, 55% великих компаній недостатньо ефективно попереджають кібератаки, а також надто повільно виявляють та усувають уразливості.

Основною причиною вищезазначеної ситуації можна вважати громіздку та складну архітектура корпоративних мереж – постійно зростаюча та видозмінювана екосистема, в якій досить тяжко виявити та закрити, або контролювати наявні вразливості. Особливо, за умови динамічного зростання кількості та критичності вразливостей як програмних, так і апаратних платформ, що зокрема відображають дані Національної бази вразливостей – NVD представлені на рис. 1 [2].

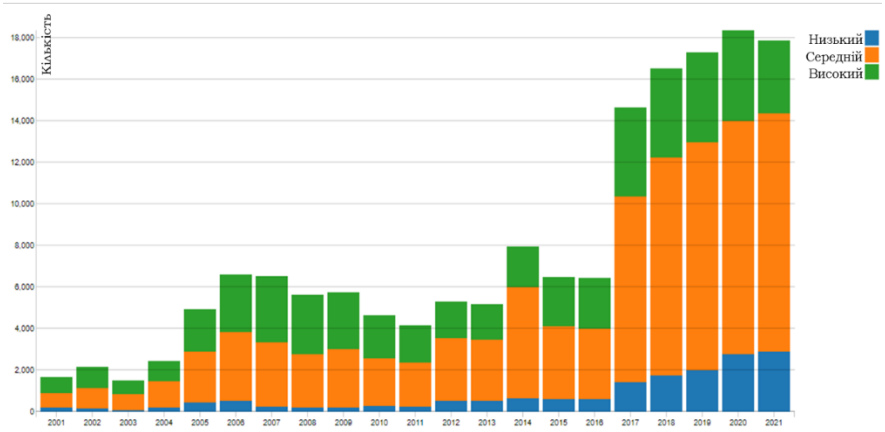

Рис. 1. Розподіл кількості вразливостей за роками в розрізі їх критичності

Одним із найбільш дієвих методів попередження кібератак є активний аналіз захищеності, який дозволяє своєчасно виявляти, підтверджувати, а також закривати слабкі місця та вразливості, як в самих інформаційно комунікаційних системах, так і в системах їх захисту.

Постановка проблеми. Проведення активного аналізу захищеності інформаційних систем та мереж, особливо таких масштабних, як корпоративні, вимагає значних часових затрат та високої кваліфікації спеціалістів з кібербезпеки, оскільки перевірка виявлених вразливостей здійснюється здебільшого вручну, хоча й існують засоби автоматизації даного процесу.

Аналіз останніх досліджень і публікацій. Провівши аналіз останніх досліджень і публікацій, слід відзначити, що наявні методи проведення активного аналізу захищеності корпоративних мереж в автоматичному режимі використовують різну математичну базу. При цьому, більшість ґрунтується на використанні класичних алгоритмів планування [3], частково спостережуваних та звичайних марківських процесів прийняття рішень [4-8].

Згідно проаналізованих підходів, основою прийняття рішень щодо реалізації тієї чи іншої атакуючої дії є виключно сформовані математичні моделі цих дій. Це є обмеженням в плані їх масштабованості, оскільки в міру розвитку інформаційних технологій, розробки нового програмного забезпечення, а також зростання кількості їх вразливостей та відповідних векторів атак, ускладняється створення та підтримка таких моделей в актуальному стані.

Кардинально інший підхід викладено в роботі [9], який на основі аналізу та оцінки якості роботи механізму валідації виявлених вразливостей дозволяє абстрагуватися від умов динамічної зміни середовища та враховувати лише параметри якості самого процесу валідації вразливостей під час проведення активного аналізу захищеності корпоративних мереж. При цьому, саме питання формування правил прийняття рішень щодо реалізації атакуючих дій під час проведення активного аналізу захищеності залишається не розкритим. Отже, дана проблема потребує подальшого розкриття та є актуальною.

Мета статті. Метою даного дослідження є розробка методу формування правил прийняття рішень щодо реалізації експлойтів вразливостей під час проведення активного аналізу захищеності на основі нечіткої оцінки якості роботи механізму валідації вразливостей та рівня ефективності самого експлойта.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Застосування превентивних механізмів кіберзахисту, зокрема активного аналізу захищеності, що є безпосередньо симуляцією атакуючих дій, дозволяють окрім своєчасного виявлення вразливостей цільової системи (тобто системи над якою здійснюється аналіз) ще й валідувати їх.

При цьому, під валідацією вразливостей розуміється процес підтвердження можливості реалізації конкретної вразливості шляхом використання експлойта даної вразливості з доставленням відповідного корисного навантаження на цільову систему та отриманням зворотного відклику (реакції) від неї.

Експлойти – це програмні модулі, які шляхом використання слабких місць компонентів інформаційно-комунікаційних систем та вразливостей програмного забезпечення, дозволяють здійснювати несанкціонований вплив на цільову систему.

Водночас слід зазначити, що кожен окремий модуль володіє певним рівнем ефективності (рангом) заснованим на потенційному впливі даного експлойта на цільову систему та складності його застосування.

Нижче, в таблиці 1, представлено опис окремих рівнів ефективності експлойтів вразливостей згідно з правилами ранжування встановленими в базі Vulnerability & Exploit Database [10] від компанії Rapid7 (США), яка є інтегрованою до засобу експлуатації використовуваного у межах даного дослідження Metasploit Framework.

Таблиця 1

Оцінка ефективності модулів експлойтів вразливостей згідно з Vulnerability & Exploit Database

Ранг	Опис
Excellent	Використання даного модуля експлойта ніколи не призводить до збою (порушення роботи) сервісу чи платформи в цілому.
Great	Експлойт має вказану ціль за замовчуванням, або автоматично визначає відповідну ціль, або використовує адресу повернення для конкретного додатку після перевірки версії.
Good	Експлойт має вказану ціль за замовчуванням та є «загальним випадком» для даного типу платформ (наприклад: англійська мова, операційна система Windows 7 для ПК або Windows Server 2012 для сервера і т.д.).
Normal	Експлойт є досить надійним, однак, залежить від конкретної версії платформи і не може надійно виконати автовизначення цілі.
Average	Здебільшого, модуль експлойта є ненадійним або складним у реалізації.
Low	Практично неможливе використання даного експлойта для розповсюджених платформ (оскільки відсоток успішних спрацювань складає менше 50).
Manual	Експлойт нестабільний або складний у використанні і може призвести до відмови в обслуговуванні, або вимагає від експерта спеціального ручного налаштування.

Оскільки, деякі з вразливостей є лише теоретичними, а інші – можуть бути реалізовані за допомогою експлойтів, саме валідація виявлених вразливостей є ключовим елементом активного аналізу захищеності.

Водночас, слід відзначити, що кожна система активного аналізу захищеності володіє власною базою експлойтів, що постійно оновлюється, та алгоритмами їх послідовного виконання, або ж з врахуванням досить простих критеріїв (до прикладу: сімейство операційної системи, функціонуючі сервіси та ін.), в автоматичному режимі. Однак, такий неконтрольований запуск експлойтів окрім часових затрат, значно підвищує ризик повного виведення з ладу цільової системи в результаті критичних помилок під час самого процесу експлуатації знайдених вразливостей.

Саме тому, процес автоматичного вибору та реалізації наступного експлойта, з послідуючим очікуванням відклику від цільової системи повинен бути в певній мірі самоконтрольованим.

Останнім часом для опису різних процесів інтелектуальної діяльності, а також підтримки процесу прийняття рішень в умовах невизначеності та неповної вхідної інформації досить широко застосовується теорія нечітких множин, формування якої розпочалося ще 1965 року на основі робіт професора Лотфі Заде.

Нечітка множина A задається за допомогою функції належності $\mu_A : X \to [0,1]$, яка є суб'єктивною мірою відповідності елемента x нечіткій множині A, де $x \in X$ – універсальна множина, яка описує предметну область. При цьому, рівність $\mu_A(x) = 1$ відображає, що x точно належить множині A, а рівність $\mu_A(x) = 0$ – що x точно не

належить множині A. Таким чином, для звичайної множини x функція належності приймає вигляд (1) [11].

$$\mu_A(x) = \begin{cases} 0, & x \in Y \\ 1, & x \notin Y \end{cases} \quad (1)$$

Водночас, нечіткі множини відрізняються від звичайних тим, що допускають проміжні степені приналежності, до прикладу, $\mu_A(x) = 0,5$. В результаті, дана теорія, на відміну від статистичної невизначеності, дозволяє працювати з так званою лінгвістичною невизначеністю надаючи експертам значно більшої гнучкості при оцінюванні чисельних показників.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Аналіз отриманих в [12] функцій розподілу кількісних показників якості роботи механізму валідації виявлених вразливостей, графіки яких було побудовано на основі експериментального практичного дослідження процесу валідації вразливостей інформаційних систем із застосуванням спеціального плагіна автоматизації даного процесу Autopwn в засобі експлуатації Metasploit Framework, надає можливість будувати функції належності для нечітких множин, елементами яких є безпосередньо акуратність, похибка та критична помилка.

Для побудови нечіткої системи та подальшого формування правил прийняття рішень щодо запуску на виконання експлойтів знайдених вразливостей було використано принцип формування структури залежності «вхід-вихід» у вигляді нечіткої бази знань [13, 14]. Така база являє собою певну сукупність правил логічного висновку наступного вигляду: *ЯКЩО* «вхідний параметр» *ТО* «вихідний параметр» та відображає, здебільшого, досвід групи експертів (рідше, одного експерта) і їхнє розуміння причинно-наслідкових зв'язків у контексті задачі прийняття рішень, що розглядається.

Так, нехай $Q_{mv} = f(A, E, Ce)$ – нечітка система оцінки якості роботи механізму валідації виявлених вразливостей, де вихідна змінна Q_{mv} – рівень якості роботи механізму валідації виявлених вразливостей, що розраховується на основі значень узагальнюючих показників (вхідні змінні): A – акуратності механізму, E – похибки, Ce – критичної помилки.

Перш за все, визначаємо терм-множини для вхідних і вихідних лінгвістичних змінних використавши універсальну множину $T = \{Min, Low, Med, High, Max\}$.

Наступним кроком будуємо функції належності для вхідних та вихідних змінних скориставшись методом статистичної обробки навчальної вибірки та експертної інформації. Значення параметрів функцій належності нечітких термів вхідних-вихідних лінгвістичних змінних представлені в таблиці 2.

Таблиця 2

Параметри функцій належності нечітких термів вхідних-вихідних змінних

Лінгвістичні змінні	Терми	Інтервали функцій належності	Лінгвістичні змінні	Терми	Інтервали функцій належності
A	*Min*	$[0; 0,1)$	Ce	*Min*	$(0,4; 1]$
	Low	$[0,1; 0,5)$		*Low*	$(0,2; 0,4]$
	Med	$[0,5; 0,7]$		*Med*	$[0,15; 0,2]$

	High	$(0,7;\ 0,8]$		*High*	$[0,1;\ 0,15)$
	Max	$(0,8;\ 1]$		*Max*	$[0;\ 0,1)$
E	*Min*	$(0,7;\ 1]$	Q_{mv}	*Min*	$[0;\ 0,1)$
	Low	$(0,3;\ 0,7]$		*Low*	$[0,1;\ 0,5)$
	Med	$[0,2;\ 0,3]$		*Med*	$[0,5;\ 0,7]$
	High	$[0,1;\ 0,2)$		*High*	$(0,7;\ 0,8]$
	Max	$[0;\ 0,1)$		*Max*	$(0,8;\ 1]$

В якості прикладу графічного відображення, на рис. 2. представлені функції належності, терми та інтервали різних станів вихідної лінгвістичної змінної Q_{mv}.

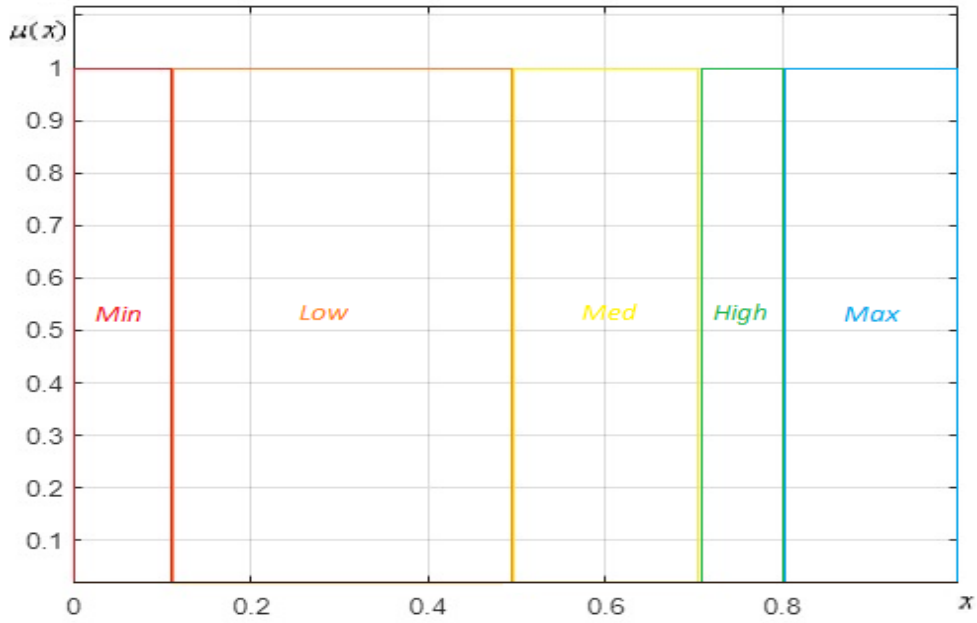

Рис. 2. Функції належності лінгвістичної змінної «рівень якості роботи механізму валідації виявлених вразливостей»

Наступним етапом є розробка нечіткої бази знань, тобто формування набору правил логічного висновку вигляду:

$$R(i): ЯКЩО\left(A_i \in T \,\&\, E_i \in T \,\&\, Ce_i \in T\right) TO\left(Q_{mv_i} \in T\right),\ i = \overline{1,k}, \qquad (2)$$

які дозволяють визначити відповідний рівень якості роботи механізму валідації виявлених вразливостей на основі всієї наявної інформації, зокрема:

- *Min* – мінімальний рівень якості, за якого використання поточного механізму валідації вразливостей є нерекомендованим, оскільки призводить до великої кількості збоїв у функціонуванні цільових систем;
- *Low* – низький рівень якості, за якого механізм валідації вразливостей, здебільшого є неефективним через неприйнятну кількість хибних рішень щодо використання експлойтів;
- *Med* – середній рівень якості роботи механізму валідації вразливостей сигналізує про його стабільність, однак, такий механізм дозволяє вірно валідувати вразливості не більше ніж у 70% випадків;

– *High* – високий рівень якості відображає здатність механізму валідації вдало перевіряти та підтверджувати можливість реалізації вразливостей за рахунок великої кількості вірно прийнятих рішень щодо застосування відібраних експлойтів при наявності незначної кількості хибних рішень;
– *Max* – максимальний рівень відображає надійність поточного механізму валідації вразливостей, який практично не призводить до порушення роботи цільових систем, а також допускає мінімальну кількість хибних рішень щодо використання експлойтів.

Водночас, генерація множини правил проводилася виходячи з можливих поєднань нечітких висловлювань в передумовах і висновках правил, у відповідності до цього максимальна кількість правил в базі була визначена за наступним відношенням:

$$l_{\max} = l_1 \cdot l_2 \cdot ... \cdot l_n \cdot l_y \quad (3)$$

де $l_1 \cdot l_2 \cdot ... \cdot l_n \cdot l_y$ – число функцій належності для задання вхідних/вихідних змінних $(x_1, ..., x_n, y)$.

Оскільки сформована таким чином база знань є досить надмірною ($l_{\max} = 625$), набір правил логічного висновку було дещо оптимізовано на основі експертної інформації, в результаті чого, сформовано базу знань з 125 правил, фрагмент якої представлено в таблиці 3.

Таблиця 3

Фрагмент бази правил для нечіткої системи $\mathbf{Q_{mv} = f(A, E, Ce)}$

№ правила	*A*	*E*	*Ce*	Q_{mv}	№ правила	*A*	*E*	*Ce*	Q_{mv}
1.	*Max*	*Max*	*Max*	*Max*	7.	*Max*	*High*	*High*	*High*
2.	*Max*	*Max*	*High*	*Max*	8.	*Max*	*High*	*Med*	*High*
3.	*Max*	*Max*	*Med*	*Max*	9.	*Max*	*High*	*Low*	*Med*
4.	*Max*	*Max*	*Low*	*High*	10.	*Max*	*High*	*Min*	*Med*
5.	*Max*	*Max*	*Min*	*Med*	…	...	...	...	...
6.	*Max*	*High*	*Max*	*Max*	125.	*Min*	*Min*	*Min*	*Min*

Далі, на основі побудованої бази знань, а також раніше згадуваних рівнів ефективності експлойтів (див. табл. 1), формуємо правила прийняття рішень щодо реалізації окремих модулів експлойтів вразливостей під час проведення активного аналізу захищеності корпоративних мереж (таблиця 4).

Таблиця 4.

Правила прийняття рішень щодо реалізації модулів експлойтів вразливостей

Rank / Q_{mv}	*Max*	*High*	*Med*	*Low*	*Min*
Excellent	a_1	a_1	a_1	a_1	a_1
Great	a_1	a_1	a_1	a_1	a_1
Good	a_1	a_1	a_1	a_1	a_1
Normal	a_1	a_1	a_1	a_2	a_2
Average	a_1	a_1	a_2	a_2	a_2
Low	a_1	a_2	a_2	a_2	a_2
Manual	a_2	a_2	a_2	a_2	a_2

де *Rank* – рівень ефективності модуля експлойта вразливості; a_1 – реалізувати обраний експлойт вразливості; a_2 – пропустити обраний експлойт вразливості.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Ґрунтуючись на експертній інформації та статистичних даних щодо ефективності застосування засобів експлуатації вразливостей, у роботі було сформовано нечітку систему оцінки якості роботи механізму валідації виявлених вразливостей, для якої було визначено функції належності кожної з лінгвістичних змінних та побудовано базу знань. Водночас, побудована нечітка база знань, а також наведене в роботі ранжування ефективності модулів експлойтів вразливостей, дозволили сформувати правила, що дозволяють в режимі реального часу з мінімальним ризиком виведення з ладу цільової системи приймати рішення щодо реалізації окремих модулів експлойтів вразливостей задля їх валідації.

Перспективними векторами подальших досліджень є розробка експертної системи діагностування ефективності механізму валідації виявлених вразливостей цільових систем, а також підвищення рівня автоматизації активного аналізу захищеності корпоративних мереж за рахунок розробки методу самоадаптації правил прийняття рішень щодо реалізації окремих модулів експлойтів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 *State of Cybersecurity Resilience 2021 (4th Annual Report): How aligning security and the business creates cyber resilience*. Accenture. https://www.accenture.com/_acnmedia/ PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf
2 *CVSS Severity Distribution Over Time.* National vulnerability database. https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time#CVSSSeverityOverTime.
3 Durkota, K. & Lisy, V. (2014). Computing optimal policies for attack graphs with action failures and costs. *In 7th European Starting AI Researchers` Symposium (STAIRS)*. https://doi.org/10.3233/978-1-61499-421-3-101
4 Obes, J., Richarte, G., Sarraute, C. (2010). Attack planning in the real world. *In 2nd Workshop on Intelligent Security (SecArt)*. https://arxiv.org/abs/1306.4044
5 Sarraute, C., Buffet, O., Hoffmann J. (2011). Penetration testing == POMDP solving? *In 3rd Workshop on Intelligent Security (SecArt'11).* https://arxiv.org/abs/1306.4714
6 Sarraute, C., Buffet, O., Hoffmann, J. (2012). POMDPs make better hackers: Accounting for uncertainty in penetration testing. *In 26th AAAI Conference on Artificial Intelligence (AAAI'12)*. https://arxiv.org/abs/1307.8182
7 Shmaryahu, D., Shani, G., Hoffmann, J. (2017). Partially observable contingent planning for penetration testing. *In 1st Int Workshop on Artificial Intelligence in Security. Melbourne*. https://cyber.bgu.ac.il/wp-content/uploads/2017/10/IWAISe-17_paper_8-ds.pdf
8 Zhou, T., Zang, Y., Zhu, J. & Wang, Q. (2019). NIG-AP: a new method for automated penetration testing. *Frontiers of Information Technology & Electronic Engineering*. https://doi.org/10.1631/FITEE.1800532
9 Киричок, Р., Зінченко, О., Срібна, І., Марченко, В., Кітура, О. (2021). Удосконалений метод автоматичного активного аналізу захищеності корпоративної мережі. *Захист інформації*, 23(2), 83-89. https://doi.org/10.18372/2410-7840.23.15725
10 *Vulnerability & Exploit Database*. Rapid7. https://www.rapid7.com/db/
11 Зак, Ю. (2013). *Принятие решений в условиях нечетких и размытых данных: Fuzzy-технологии.* Либроком.
12 Киричок, Р., Шуклін, Г. (2020). Методика аналізу якості роботи механізму валідації вразливостей корпоративних мереж. *Телекомунікаційні та інформаційні технології*. 2(67). 29-40. https://doi.org/10.31673/2412-4338.2020.022930
13 Орловский, С. (1981). *Проблемы принятия решений при нечеткой исходной информации.* Наука.
14 Поспелов, Д. (1986). *Нечеткие множества в моделях управления и искусственного интеллекта*. Наука.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (14), 2021
ISSN 2663 - 4023

Roman V. Kyrychok
PhD
Associate Professor of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0002-9919-9691
r.kyrychok@kubg.edu.ua

Zoreslava M. Brzhevska
PhD
Associate Professor of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0002-7029-9525
z.brzhevska@kubg.edu.ua

Hennadii M. Hulak
Doctor of Technical Sciences, Associate Professor
Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0001-9131-9233
h.hulak@kubg.edu.ua

Anatoly V. Bessalov
DSc, Professor
Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0002-6967-5001
a.bessalov@kubg.edu.ua

Volodymyr M. Astapenya
PhD, Associate Professor
Associate Professor of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0003-0124-216X
v.astapenia@kubg.edu.ua

RULES FOR THE IMPLEMENTATION OF EXPLOITS DURING AN ACTIVE ANALYSIS OF THE CORPORATE NETWORKS` SECURITY BASED ON A FUZZY ASSESSMENT OF THE QUALITY OF THE VULNERABILITY VALIDATION MECHANISM

Abstract. The dynamics of the increase in the number of vulnerabilities of software and hardware platforms of corporate networks, the accessibility of exploit modules for these vulnerabilities in the Internet and the Darknet, along with the lack of a sufficient number of highly qualified cybersecurity specialists make the problem of effective automation of preventive information protection mechanisms quite urgent. In particular, the basic algorithms for the sequential implementation of exploits embedded in the vulnerability exploitation tools are quite primitive, and the proposed approaches to their improvement require constant adaptation of mathematical models of the implementation of attacking actions. This justifies the direction of this research. This paper considers the issue of forming decision-making rules for the implementation of vulnerabilities' exploits during an active analysis of the corporate networks' security. Based on the results of the analysis of quantitative indicators of the quality of the validation mechanism of the identified vulnerabilities and the use of fuzzy logic methods, a fuzzy system was formed, membership functions for each of the linguistic variables were determined and a knowledge base was built, which makes it possible to determine the quality level of the validation mechanism of the identified vulnerabilities based on all available information. At the same time, in order to eliminate the "human factor" of making mistakes

when validating vulnerabilities, based on the built fuzzy knowledge base and the established levels of exploit modules' efficiency, the rules for the implementation of individual exploit modules during an active analysis of the corporate network's security were formed. Results of research make it possible to create expert systems for diagnosing the effectiveness of the validation mechanism of the identified vulnerabilities of target systems, and also help to solve the problem of the lack of qualified specialists in the analysis and maintenance of an appropriate level of information security of corporate networks.

Keywords: active analysis of the security; corporate network; exploit; vulnerability validation; fuzzy logic.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 *State of Cybersecurity Resilience 2021 (4th Annual Report): How aligning security and the business creates cyber resilience*. Accenture. https://www.accenture.com/_acnmedia/ PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf
2 *CVSS Severity Distribution Over Time.* National vulnerability database. https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time#CVSSSeverityOverTime.
3 Durkota, K. & Lisy, V. (2014). Computing optimal policies for attack graphs with action failures and costs. *In 7th European Starting AI Researchers` Symposium (STAIRS)*. https://doi.org/10.3233/978-1-61499-421-3-101
4 Obes, J., Richarte, G., Sarraute, C. (2010). Attack planning in the real world. *In 2nd Workshop on Intelligent Security (SecArt)*. https://arxiv.org/abs/1306.4044
5 Sarraute, C., Buffet, O., Hoffmann J. (2011). Penetration testing == POMDP solving? *In 3rd Workshop on Intelligent Security (SecArt'11).* https://arxiv.org/abs/1306.4714
6 Sarraute, C., Buffet, O., Hoffmann, J. (2012). POMDPs make better hackers: Accounting for uncertainty in penetration testing. *In 26th AAAI Conference on Artificial Intelligence (AAAI'12)*. https://arxiv.org/abs/1307.8182
7 Shmaryahu, D., Shani, G., Hoffmann, J. (2017). Partially observable contingent planning for penetration testing. *In 1st Int Workshop on Artificial Intelligence in Security. Melbourne*. https://cyber.bgu.ac.il/wp-content/uploads/2017/10/IWAISe-17_paper_8-ds.pdf
8 Zhou, T., Zang, Y., Zhu, J. & Wang, Q. (2019). NIG-AP: a new method for automated penetration testing. *Frontiers of Information Technology & Electronic Engineering*. https://doi.org/10.1631/FITEE.1800532
9 Kyrychok, R., Zinchenko, O., Sribna, I., Marchenko, V., Kitura, O. (2021). Improved method of automatic active analysis of corporate network security. *Ukrainian Information Security Research Journal*, 23(2), 83-89. https://doi.org/10.18372/2410-7840.23.15725
10 *Vulnerability & Exploit Database*. Rapid7. https://www.rapid7.com/db/
11 Zak, Yu. (2013). *Decision making in conditions of fuzzy and blurry data: Fuzzy technologies*. Book House "LIBROKOM".
12 Kyrychok, R., Shuklin, G. (2020). Methodology for analysing the quality of the vulnerability validation mechanism in the corporate networks. *Telecommunication and information technologies*. 2(67). 29-40. https://doi.org/10.31673/2412-4338.2020.022930
13 Orlovsky, S. (1981). *Decision-making problems with fuzzy initial information.* The science.
14 Pospelov, D. (1986). *Fuzzy Sets in Management and Artificial Intelligence Models*. The science.