УДК 004.056 DOI:10.31673/2412-4338.2020.022930

Киричок Р. В., Шуклін Г. В. *Державний університет телекомунікацій, Київ*

МЕТОДИКА АНАЛІЗУ ЯКОСТІ РОБОТИ МЕХАНІЗМУ ВАЛІДАЦІЇ ВРАЗЛИВОСТЕЙ КОРПОРАТИВНИХ МЕРЕЖ

Анотація: *У статті розглядається проблема визначення та оцінки якості роботи механізму валідації вразливостей інформаційних систем та мереж. На основі практичного аналізу процесу валідації вразливостей та отриманих, за допомогою поліномів Бернштейна, аналітичних залежностей базових характеристик якості валідації вразливостей, було виділено та охарактеризовано додаткові ключові показники, які дозволяють з великою достовірністю стверджувати про позитивний хід або наслідки валідації вразливостей цільової корпоративної мережі. Експериментально визначено інтервали даних показників, при яких механізм валідації вразливостей має високу якість. Окрім цього, в ході проведення розрахунків, також було виведено єдиний інтегральний показник для кількісної оцінки якості роботи механізму валідації вразливостей корпоративних мереж та проведено експериментальне дослідження і оцінку якості роботи механізму автоматичної валідації вразливостей плагіна db_autopwn призначеного для автоматизації засобу експлуатації вразливостей Metasploit framework.*

В результаті, було запропоновано методику аналізу якості механізму валідації вразливостей корпоративних мереж, яка дозволяє кількісно оцінити якість роботи досліджуваного механізму валідації, що в свою чергу дозволить в режимі реального часу відслідковувати та контролювати хід валідації виявлених вразливостей. Також, в дослідженні було отримано залежності визначених ключових показників якості роботи механізму валідації вразливостей від часу раціонального циклу, що надає змогу будувати функції належностей для нечітких множин. Побудова даних множин, зокрема, дозволить приймати рішення з мінімальними ризиками щодо проведення активного аналізу захищеності корпоративних мереж.

Ключові слова: *активний аналіз захищеності, корпоративна мережа, цільова система, показники якості механізму, валідація вразливостей.*

Kyrychok R., Shuklin G. *State University of Telecommunications, Kyiv*

METHODOLOGY FOR ANALYSING THE QUALITY OF THE VULNERABILITY VALIDATION MECHANISM IN THE CORPORATE NETWORKS

Abstract: *The article considers the problem of determining and assessing the quality of the vulnerability validation mechanism of the information systems and networks. Based on the practical analysis of the vulnerability validation process and the analytical dependencies of the basic characteristics of the vulnerability validation quality obtained using the Bernstein polynomials, additional key indicators were identified and characterised, which make it possible to assert with high reliability about the positive progress or consequences of the vulnerability validation of the target corporate network. The intervals of these indicators were experimentally determined at which the vulnerability validation mechanism is of high quality. In addition, during the calculations, a single integral indicator was also derived to quantitatively assess the quality of the vulnerability validation mechanism of the corporate networks, and an experimental study was carried out, as well as the assessment of the quality of the automatic vulnerability validation mechanism of the db_autopwn plugin designed to automate the Metasploit framework vulnerability exploitation tool.*

As a result, it was proposed the methodology for analysing the quality of the vulnerability validation mechanism in the corporate networks, which allows one to quantify the quality of the validation mechanism under study, which in turn will allow real-time monitoring and control of the validation progress of the identified vulnerabilities. Also, in the study, the dependences of previously determined key performance indicators of the vulnerability validation mechanism on the rational cycle time were obtained, which makes

it possible to build the membership functions for the fuzzy sets. The construction of these sets, in particular, allows making decisions with minimal risks for an active analysis of the security of corporate networks.

Keywords: *active analysis of the security, corporate network, target system, vulnerability validation, mechanism quality.*

Киричок Р.В., Шуклин Г.В. *Государственный университет телекоммуникаций, Киев*

МЕТОДИКА АНАЛИЗА КАЧЕСТВА РАБОТЫ МЕХАНИЗМА ВАЛИДАЦИИ УЯЗВИМОСТЕЙ КОРПОРАТИВНЫХ СЕТЕЙ

Аннотация: *В статье рассматривается проблема определения и оценки качества работы механизма валидации уязвимостей информационных систем и сетей. На основе практического анализа процесса валидации уязвимостей и полученных с помощью полиномов Бернштейна, аналитических зависимостей базовых характеристик качества валидации уязвимостей, было выделено и охарактеризовано дополнительные ключевые показатели, которые позволяют с большой достоверностью утверждать о положительном ход или последствиях валидации уязвимостей целевой корпоративной сети. Экспериментально определены интервалы данных показателей, при которых механизм валидации уязвимостей имеет высокое качество. Кроме этого, в ходе проведения расчетов, также был выведен единый интегральный показатель для количественной оценки качества работы механизма валидации уязвимостей корпоративных сетей и проведено экспериментальное исследование, а также оценку качества работы механизма автоматической валидации уязвимостей плагина db_autopwn предназначенного для автоматизации средства эксплуатации уязвимостей Metasploit framework.*

В результате, было предложено методику анализа качества механизма валидации уязвимостей корпоративных сетей, которая позволяет количественно оценить качество работы исследуемого механизма валидации, что в свою очередь позволит в режиме реального времени отслеживать и контролировать ход валидации выявленных уязвимостей. Также, в исследовании было получено зависимости ранее определенных ключевых показателей качества работы механизма валидации уязвимостей от времени рационального цикла, что дает возможность строить функции принадлежностей для нечетких множеств. Построение данных множеств, в частности, позволят принимать решения с минимальными рисками по проведению активного анализа защищенности корпоративных сетей.

Ключевые слова: *активный анализ защищенности, корпоративная сеть, целевая система, качество механизма, валидация уязвимостей.*

Вступ

Сучасні системи активного аналізу захищеності інформаційних систем та мереж, ґрунтуючись на різних методах та методиках проведення тестування на проникнення, дозволяють змоделювати потенційну кібератаку на інформаційну інфраструктуру організації та встановити фактичний стан її захищеності. При цьому, узагальнений алгоритм проведення активного аналізу захищеності [1] складається з:

- планування активного аналізу захищеності, зокрема, визначаються цілі, терміни, методи та форма звіту;
- розвідки – збір та аналіз вхідних даних про цільовий об’єкт (організація в якій проводиться аналіз захищеності);
- сканування цільової мережі, що дозволяє визначити перелік доступних хостів, відкриті на них порти та запущені сервіси, а також виявити вразливості в програмному забезпеченні, помилки в налаштуванні обладнання та інші прогалини в периметрі захисту інформаційної інфраструктури;
- перевірки та підтвердження можливості реалізації (валідації) виявлених вразливостей шляхом спроби їх експлуатації за допомогою спеціалізованих програмних

засобів, зокрема, з використанням так званих експлойтів вразливостей (шкідливих скриптів, виконуваних модулів та ін);

- формування звіту, який обов'язково включає перелік валідованих вразливостей, рівень їх критичності (небезпеки) та рекомендації щодо усунення даних вразливостей.

Найбільш ключовими моментами є саме сканування мережі та валідація виявлених вразливостей, при чому, останній є досить трудомістким та часозатратним, оскільки слід перевірити велику кількість потенційних вразливостей всіх інформаційних систем (хостів) цільової мережі, що є особливо критичним при активному аналізі захищеності великих мереж, таких, як корпоративні. Окрім цього, валідація вразливостей, в певній мірі, є небезпечною процедурою, оскільки з'являється можливість виникнення критичної помилки в цільовій системі під час експлуатації виявлених вразливостей, наприклад, в результаті невірно підібраних експлойтів або допущенні помилки при їх налаштуванні.

З вищесказаного виникає актуальне питання – визначення якості роботи механізму валідації вразливостей інформаційних систем та мереж.

Аналіз досліджень і публікацій

З огляду останніх досліджень та публікацій стає зрозуміло, що питання якості процесу активного аналізу захищеності, зокрема і валідації виявлених вразливостей інформаційних систем та мереж, не розглядається зовсім. Більшість наукових робіт, в контексті питання аналізу захищеності, зосереджено лише на моделюванні та подальшому аналізі самих кібератак і вразливостей за рахунок яких реалізуються дані атаки.

При цьому, моделювання здійснюється ґрунтуючись на різних математичних апаратах, таких як, графи та дерева атак [2-5], марківский процес прийняття рішень [6], частково спостережуваний марківський процес прийняття рішень [7], а також мережі Петрі [12].

Так, використання графів та дерев атак дозволяє досить просто та зрозуміло описувати проведення ймовірної кібератаки на інформаційну систему чи мережу, хоча, більшість з них поєднує одна проблема – зі збільшенням розміру мережі, зростає і складність алгоритму генерації графа атак. В той же час, комплексна модель [7] заснована на частково спостережуваних марківських процесах прийняття рішень (POMDPs) дозволила враховувати невизначеності (неповноту знань на стороні зловмисника) в контрольованих сценаріях кібератак при проведенні тестування на проникнення комп'ютерної мережі, однак, при цьому, залишилася немасштабованою – ні з точки зору моделювання, ні з точки зору складності обчислень. З іншої сторони, використання класичного алгоритму планування [8] чудово підходить для великих мереж, однак спрощує припущення щодо повноти знань зловмисника та повністю детермінує результати, тим самим, призводячи до надмірно оптимістичної точки зору зловмисника. Марківські процеси прийняття рішень (MDPs) [6] є проміжною ланкою – серединою між класичним плануванням і POMDPs та надають дещо більш реалістичний опис проблеми, враховуючи можливості провалу атакуючих дій. Проте, як і при класичному плануванні, в даному випадку не враховується часткова інформація, яку може мати зловмисник, і дії, які можуть йому знадобитися.

Також слід відзначити роботи, що скеровані на оптимізацію алгоритмів планування кібератак та побудови графів атак [9-12]. В [12] автори використовують мережі Петрі для моделювання вразливостей та синтезу графа атак, при цьому зменшуючи часові затрати та складність його побудови, а в [9] представлено автоматичний алгоритм генерування графа атак, який дозволяє ефективно скоротити надлишкову інформацію необхідну для проведення аналізу захищеності, шляхом оптимізації топології мережі перед формуванням графа атак.

Мета і задачі дослідження

Метою даного дослідження є розробка методики аналізу якості механізму валідації вразливостей корпоративних мереж, що дозволить отримувати точну картину якості процесу валідації виявлених вразливостей під час проведення активного аналізу захищеності.

Для досягнення поставленої мети було виділено ключові показники, за допомогою яких можна з великою достовірністю стверджувати про позитивний хід або наслідки валідації вразливостей цільової корпоративної мережі в цілому.

Результати дослідження

На сьогоднішній день, сформувалася певна кількість провідних засобів експлуатації виявлених вразливостей, серед яких слід відзначити Metasploit Framework, Core Impact та SAINT Security Suite. Дані засоби дозволяють експертам або звичайним системним адміністраторам проводити валідацію виявлених вразливостей цільових хостів. При цьому, у більшості випадків валідація здійснюється вручну, що призводить до суб'єктивної результативності та якості самого процесу, оскільки в даному разі все залежить від кваліфікації спеціаліста, який проводить валідацію виявлених вразливостей. Також, ручна валідація вразливостей потребує значних часових затрат на перевірку та підтвердження можливості реалізації кожної з виявлених вразливостей.

Задля зменшення часу валідації вразливостей, особливо при проведенні аналізу захищеності великих мереж, використовують засоби автоматизації процесу валідації, які є переважно вже інтегрованими в засоби експлуатації додатковими модулями. Більшість алгоритмів роботи даних модулів базуються на послідовній реалізації, або всіх наявних в базі даних експлойтів (і в такому разі єдиним обмеженням є чисельність експлойтів в базі конкретного засобу експлуатації), або ж відібраних експлойтів з урахуванням простих критеріїв, таких як сімейство операційної системи (ОС), для якого призначений даний експлойт, запущений вразливий сервіс або ранг якості експлойта.

Для автоматизації засобу експлуатації вразливостей Metasploit framework може використовуватися плагін db-autopwn, який, за замовчуванням, після сканування цільової системи або мережі, послідовно запускає на виконання всі експлойти призначені для виявленого типу ОС цільового хоста. Подібні механізми автоматичної валідації вразливостей зменшують її якість та збільшують ризик виникнення критичної помилки в функціонуванні цільової системи і її повного виведення з ладу в процесі реалізації виявленої вразливості.

Тому, виходячи з вище окреслених проблем, стає більш очевидним доцільність формування характеристик, за допомогою яких визначається якість валідації вразливостей. В роботі [13], на основі практичного аналізу процесу валідації вразливостей було виділено три таких характеристики, а саме: *SV* (змінна q_s) – кількість успішно валідованих вразливостей цільової системи (*success validation*); *FV* (змінна q_f) – кількість невалідованих вразливостей (*failed validation*); *CV* (змінна q_c) – кількість випадків валідації вразливостей, які призвели до критичної помилки в цільовій системі та подальшої втрати з нею зв'язку (*crash validation*). Окрім цього, в роботі також, за допомогою поліномів Бернштейна

$$f(t_н) = \sum_{k=0}^{n} f\left(\frac{k}{n}\right) b_{k,n}(t_н), \text{ при } t_н \in [0;1], \tag{1}$$

були отримані аналітичні залежності для вищезазначених характеристик:

$$q_s(t_н) = \sum_{i=0}^{n} q_s(t_н^{(i)}) b_{k,n}(t_н), \quad q_f(t_н) = \sum_{i=0}^{n} q_f(t_н^{(i)}) b_{k,n}(t_н), \quad q_c(t_н) = \sum_{i=0}^{n} q_c(t_н^{(i)}) b_{k,n}(t_н). \tag{2}$$

Час $t_н$ – це час нормування, який визначається наступним відношенням:

$$t_н = \frac{t_i}{T}, \tag{3}$$

де T – час проведення валідації вразливостей цільового хоста в секундах (час раціонального циклу);

t_i – час, за який відповідні характеристики (2) приймали свої значення в межах раціонального циклу.

Залежності (2) дають можливість розраховувати показники, які більш точно визначають якість роботи механізму валідації вразливостей. Такими показниками є:

1) A – акуратність (*accuracy*) – доля вірно прийнятих рішень щодо реалізації конкретних експлойтів відносно всіх прийнятих рішень. Даний параметр характеризує здатність механізму валідації виявлених вразливостей вдало перевіряти та підтверджувати можливість їх реалізації за рахунок вірно прийнятих рішень щодо застосування відібраних експлойтів з відповідним корисним навантаженням для даних вразливостей;

2) E – похибка (*error*) – доля прийнятих рішень щодо реалізації конкретних експлойтів, які не підтвердили можливість реалізації відповідних вразливостей відносно всіх прийнятих рішень. Параметр похибки характеризує здатність механізму валідації виявлених вразливостей приймати рішення щодо застосування відібраних експлойтів, які з певних причин не спрацьовують. До таких причин відноситься, наприклад, невідповідність цільової системи умовам реалізації обраного експлойта, зміна портів на яких за замовчуванням працюють вразливі сервіси, реакція системи захисту – блокування можливості реалізації експлойта;

3) Ce – критична помилка (*critical error*) – доля випадків прийняття рішень щодо реалізації конкретних експлойтів, що призвели до критичних помилок в цільовій системі та подальшої втрати з нею зв'язку відносно всіх прийнятих рішень. Критична помилка характеризує здатність механізму валідації виявлених вразливостей приймати рішення щодо застосування відібраних експлойтів, які в процесі їх реалізації призводять до критичної помилки в функціонуванні цільової системи і подальшого виведення її з ладу.

Згідно (2) ці показники визначаються наступним чином:

$$A = \frac{\int_0^1 q_s(\theta)d\theta}{\int_0^1 (q_s(\theta) + q_f(\theta) + q_c(\theta))d\theta}, \tag{4}$$

$$E = \frac{\int_0^1 q_f(\theta)d\theta}{\int_0^1 (q_s(\theta) + q_f(\theta) + q_c(\theta))d\theta}, \tag{5}$$

$$Ce = \frac{\int_0^1 q_c(\theta)d\theta}{\int_0^1 (q_s(\theta) + q_f(\theta) + q_c(\theta))d\theta}. \tag{6}$$

Експериментально було встановлено, що якщо значення показника A, що обчислюється за формулою (4) належить інтервалу $(0,8;1]$, а при цьому показники E, що обчислюється за формулою (5) і Ce, що обчислюється за формулою (6) одночасно належать інтервалу $[0;0,1)$, то це означає, що механізм валідації вразливостей має високу якість.

Однак, якщо при умові, що $A \in (0,8;1]$, хоча б один з показників E або Ce більший за 0,1 то маємо невизначеність, при якій необхідно більш ретельно аналізувати виявлені вразливості хостів цільової корпоративної мережі та здійснювати підбір відповідних експлойтів для їх валідації.

В даному дослідженні, збір статистичних даних щодо процесу валідації виявлених вразливостей окремих хостів фрагменту потенційної цільової корпоративної мережі відбувався з використанням раніше згадуваного засобу експлуатації вразливостей Metasploit framework та спеціально створеного в роботі [13] тестового стенда. Однак, слід відзначити, що цього разу використовувався вже інший засіб автоматизації процесу валідації вразливостей – спеціальний плагін db_autopwn. Результати даної симуляції процесу валідації вразливостей наведено в таблиці 1.

Таблиця 1

Результати проведення валідації вразливостей за допомогою Metasploit-autopwn

Платформа (ОС)	£	q_s	q_f	q_c	*t (секунди)*
Windows XP SP2	63	3	58	2	244
Windows XP SP3	58	3	53	2	286
Windows 7	63	3	60	2	369
Windows 8.1	65	0	64	1	281
Windows 10	1255	0	1255	0	1523
Windows Server 2008 R2	84	1	82	1	363
Windows Server 2016	32	0	32	0	43
Mac OS X 10.13	59	1	58	0	249
Mac OS X 10.14	41	1	40	0	58
Metasploitable 2	1445	3	1442	0	1462
Metasploitable 3	1911	3	1908	0	1933

де £ – загальна кількість спроб експлуатацій виявлених вразливостей окремого хоста цільової корпоративної мережі;

t – загальний час проведення валідації виявлених вразливостей окремого хоста цільової корпоративної мережі, виражений в секундах.

У відповідності до алгоритму побудови аналітичних залежностей показників якості валідації вразливостей [14], спершу, за даними таблиці 1, здійснюємо нормування відрізка часу $[0;1933]$, оскільки час раціонального циклу проведення валідації вразливостей, в даному випадку, складає саме 1933 секунди, та отримуємо нормований час на відрізку $[0;1]$, який представлено в таблиці 2.

Таблиця 2

Нормування часу раціонального циклу

t - реальний час	0	43	58	244	249	281	286	363	369	1462	1523	1933
$t_н$ - нормований час	0	0,022	0,03	0,126	0,129	0,145	0,148	0,188	0,191	0,756	0,788	1

Значення змінних $q_s(t_н)$, $q_f(t_н), q_c(t_н)$, як функції від часу нормування, представлені в таблиці 3.

Таблиця 3

Значення кількості успішно валідованих вразливостей $q_s(t_н)$, кількості невалідованих вразливостей $q_f(t_н)$ і кількості випадків валідації вразливостей, які призвели до критичних помилок $q_c(t_н)$

$t_н$ - нормований час	0	0,022	0,03	0,126	0,129	0,145	0,148	0,188	0,191	0,756	0,788	1
$q_s(t_н)$	0	0	1	3	1	0	3	1	3	3	0	3
$q_f(t_н)$	0	32	40	58	58	64	53	82	60	1442	1255	1908
$q_c(t_н)$	0	0	0	2	0	1	2	1	2	0	0	0

Використовуючи дані таблиці 3 і представлення (1) було отримано початкові аналітичні залежності для кількості успішно валідованих вразливостей $q_s = q_s(t)$:

$$q_s(t_н) = q_s(0)b_{0.11}(t_н) + q_s(0,022)b_{1.11}(t_н) + q_s(0,03)b_{2.11}(t_н) + q_s(0,126)b_{3.11}(t_н) +$$
$$+ q_s(0,129)b_{4.11}(t_н) + q_s(0,145)b_{5.11}(t_н) + q_s(0,148)b_{6.11}(t_н) + q_s(0,188)b_{7.11}(t_н) +$$
$$+ q_s(0,191)b_{8.11}(t_н) + q_s(0,756)b_{9.11}(t_н) + q_s(0,788)b_{10.11}(t_н) + q_s(1)b_{11.11}(t_н)$$

Після підстановки відповідних значень з таблиці 3, отримуємо

$$q_s(t_н) = b_{2.11}(t_н) + 3b_{3.11}(t_н) + b_{4.11}(t_н) + 3b_{6.11}(t_н) + b_{7.11}(t_н) + 3b_{8.11}(t_н) + 3b_{9.11}(t_н) + 3b_{11.11}(t_н) \quad (7)$$

Підставивши значення відповідних поліномів $b_{k,11}(t_н)$ з таблиці 4 та спростивши вираз маємо:

$$q_s(t_н) = -1273t^{11} + 5610t^{10} - 8250t^9 + 1485t^8 + 9570t^7 - 12474t^6 + 6930t^5 - 1650t^4 + 55t^2 \quad (8)$$

Таблиця 4

Значення поліномів $b_{k,11}(t_н)$ для $k = \overline{0...11}$.

k	$b_{k,11}(t_н)$
0	$(1-t)^{11}$
1	$11t(1-t)^{10}$
2	$55t^2(1-t)^9$
3	$165t^3(1-t)^8$
4	$330t^4(1-t)^7$
5	$462t^5(1-t)^6$
6	$462t^6(1-t)^5$
7	$330t^7(1-t)^4$
8	$165t^8(1-t)^3$
9	$55t^9(1-t)^2$
10	$11t^{10}(1-t)$
11	t^{11}

Аналогічно, використовуючи представлення (1) та дані з таблиці 3, отримуємо початкові аналітичні залежності для кількості невалідованих вразливостей $q_f = q_f(t)$:

$$q_f(t_н) = 32b_{1.11}(t_н) + 40b_{2.11}(t_н) + 58b_{3.11}(t_н) + 58b_{4.11}(t_н) + 64b_{5.11}(t_н) + 53b_{6.11}(t_н) + \\ + 82b_{7.11}(t_н) + 60b_{8.11}(t_н) + 1442b_{9.11}(t_н) + 1255b_{10.11}(t_н) + 1908b_{11.11}(t_н) \quad (9)$$

Підставивши значення відповідних поліномів $b_{k,11}(t_н)$ з таблиці 4 та спростивши вираз маємо:

$$q_f(t_н) = 78237t^{11} - 204633t^{10} + 213290t^9 - 168300t^8 + 144870t^7 - 98406t^6 + \\ + 52668t^5 - 20460t^4 + 5610t^3 - 1320t^2 + 352t \quad (10)$$

А також, отримуємо початкові аналітичні залежності для кількості випадків валідації вразливостей, які призвели до критичних помилок $q_c = q_c(t)$:

$$q_c(t_н) = 2b_{3.11}(t_н) + b_{5.11}(t_н) + 2b_{6.11}(t_н) + b_{7.11}(t_н) + 2b_{8.11}(t_н) \quad (11)$$

Підставивши значення відповідних поліномів $b_{k,11}(t_н)$ з таблиці 4 та спростивши вираз маємо:

$$q_c(t_н) = -132t^{11} - 1122t^{10} + 7920t^9 - 19470t^8 + 25740t^7 - 20328t^6 + 9702t^5 - 2640t^4 + 330t^3. \quad (12)$$

Згідно (4), (5), (6), при підстановці спрощених виразів початкових аналітичних залежностей (8), (10), (12), отримуємо наступні значення показників якості роботи механізму валідації вразливостей:

$$A = \frac{1,5}{423,16} = 0,0035;$$

$$E = \frac{421}{423,16} = 0,994;$$

$$Ce = \frac{0,66}{423,16} = 0,0015.$$

Після чого, зводимо в єдиний інтегральний показник якості роботи механізму валідації вразливостей корпоративних мереж:

$$J_{qv} = \frac{A}{E} - Ce \quad (13)$$

де J_{qv} – інтегральний індекс якості роботи механізму валідації вразливостей.

При цьому, якщо $J_{qv} > 1$, то механізм валідації вразливостей має високу якість.

$$J_{qv} = \frac{0,0035}{0,994} - 0,0015 = 0,00202$$

Отриманий результат свідчать про низьку якість роботи механізму автоматичної валідації вразливостей плагіна db_autopwn для засобу експлуатації вразливостей Metasploit framework. Якщо більш детально розглядати, то отримані значення показників якості роботи механізму валідації вразливостей A, E, Ce свідчать про те, що даний плагін дозволяє вірно валідувати вразливості лише в 0,35 % випадків, при цьому допускає надзвичайно велику похибку, яка складає 99,4 % та приймає рішення щодо застосування відібраних експлойтів, які в процесі їх реалізації призводять до критичної помилки в функціонуванні цільової системи в 0,15 % випадків (що загалом є допустимим).

Таким чином, можна виділити наступні кроки методики аналізу якості механізму валідації вразливостей корпоративних мереж:

1. Збір статистичних даних щодо процесу валідації виявлених вразливостей корпоративної мережі оцінюваного механізму валідації;

2. Нормування відрізка часу проведення валідації вразливостей хостів цільової корпоративної мережі;

3. Побудова поліномів Бернштейна задля отримання початкових аналітичних залежностей для базових характеристик (*SV, FV* та *CV*) якості валідації вразливостей;

4. Розрахунок більш точних показників якості роботи механізму валідації вразливостей: акуратності, похибки та критичної помилки;

5. Оцінка якості роботи механізму валідації вразливостей корпоративних мереж на основі обчислення єдиного інтегрального показника.

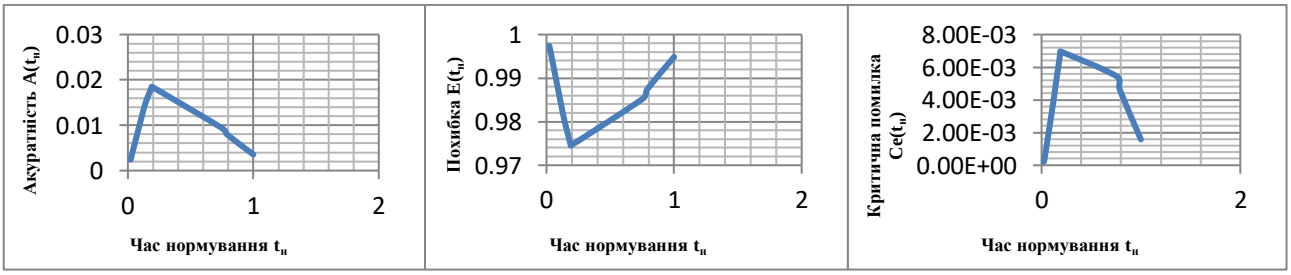
Також, слід зазначити, що залежності (4), (5), (6) в загальному вигляді є функціями від часу

$$A(t_н) = \frac{\int_0^{t_н} q_s(\theta)d\theta}{\int_0^{t_н} (q_s(\theta) + q_f(\theta) + q_c(\theta))d\theta}, \quad (14)$$

$$E(t_н) = \frac{\int_0^{t_н} q_f(\theta)d\theta}{\int_0^{t_н} (q_s(\theta) + q_f(\theta) + q_c(\theta))d\theta}, \quad (15)$$

$$Ce(t_н) = \frac{\int_0^{t_н} q_c(\theta)d\theta}{\int_0^{t_н} (q_s(\theta) + q_f(\theta) + q_c(\theta))d\theta}, \quad (16)$$

графіки яких відображено на рис. 1.



(а) Акуратність $A(t_н)$ (б) Похибка $E(t_н)$ (в) Критична помилка $Ce(t_н)$

Рис. 1. Залежність кількісних показників якості роботи механізму валідації вразливостей від часу раціонального циклу

З рисунку 1 видно, що при проведених дослідженнях валідації вразливостей, максимальне значення акуратності A приймає значення 0,02 (а). При цьому мінімальна похибка E знаходиться в межах від 0,97 до 0,98 (б), а максимальна критична помилка Ce знаходиться в межах від $6 \cdot 10^{-3}$ до $8 \cdot 10^{-3}$ (в). Отриманні залежності виділених показників дають можливість будувати функції належностей для нечітких множин, елементами яких є акуратність, похибка та критична помилка. Побудова даних множин дає можливість

експертам з безпеки приймати відповідні рішення з мінімальними ризиками щодо проведення активного аналізу захищеності корпоративних мереж.

Висновки

В ході даного дослідження було виділено ключові показники якості роботи механізму валідації виявлених вразливостей, які дозволяють отримувати більш точну картину якості самого процесу валідації під час проведення активного аналізу захищеності корпоративних мереж. Також, в роботі було запропоновано методику аналізу якості механізму валідації вразливостей корпоративних мереж, яка дозволяє кількісно оцінити якість роботи даного механізму, що в свою чергу дозволить в режимі реального часу відслідковувати та контролювати хід валідації виявлених вразливостей.

Список використаної літератури

1. Киричок Р.В. Тест на проникнення як імітаційний підхід до аналізу захищеності корпоративних інформаційних систем. Сучасний захист інформації. 2018. №2(34). С. 53-58.

2. Chen F., Su J., and Zhang Y. A scalable approach to full attack graphs generation. Engineering Secure Software and Systems, Springer. 2009. P. 150-163.

3. Абрамов Е.С., Андреев А.В., Мордвин Д.В. Применение графов атак для моделирования вредоносных сетевых воздействий. Известия Южного федерального университета. Технические науки. 2012.Том 26. Вып.1. С.165-173.

4. Barik M., Sengupta A., Mazumdar C. Attack graph generation and analysis techniques. Defence Science Journal. 2016. №66(6). P. 559-567.

5. Шипилева А.В. Автоматическая генерация графов атак на основе ветвящихся процессов в случайной среде. Международная научно-практическая конференция «Новая наука: стратегии и векторы развития». Часть 2. г. Стерлитамак, 8 марта 2017 г. Стерлитамак. С. 143-144.

6. Durkota K. and Lisy V. Computing optimal policies for attack graphs with action failures and costs. In 7th European Starting AI Researchers` Symposium «STAIRS'14». January 2014.

7. Sarraute C., Buffet O., Hoffmann J. POMDPs make better hackers: Accounting for uncertainty in penetration testing. In Proceedings of the 26th AAAI Conference on Artificial Intelligence «AAAI'12». Toronto, ON, Canada, July 2012. AAAI Press. P. 1816-1824

8. Obes, J., Richarte G., Sarraute C. Attack planning in the real world. In Proceedings of the 2nd Workshop on Intelligent Security «SecArt'10». Atlanta, USA. July 12, 2010.

9. Qiu X., Wang S., Jia Q., Xia C. and Lv L. Automatic generation algorithm of penetration graph in penetration testing. Proceedings of the 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, IEEE. Guangdong, China. Nov 8-10, 2014. P. 531-537.

10. Steinmetz M. Critical constrained planning and an application to network penetration testing. 26th Int Conf on Automated Planning and Scheduling. 2016. P.141-144.

11. Hoffman J. Simulated Penetration Testing: From "Dijkstra" to "Turing Test++". In Proceedings of the Twenty-Fifth International Conference on Automated Planning and Scheduling, «ICAPS'15». Jerusalem, Israel. June 7-11, 2015. P. 364–372.

12. Luan J., Wang J., Xue M. Automated Vulnerability Modeling and Verification for Penetration Testing Using Petri Nets. Springer, Lecture Notes in Computer Science. July 2016.

13. Киричок Р.В., Шуклін Г.В., Барабаш О.В., Гайдур Г.І. Моделювання механізму валідації вразливостей при активному аналізі захищеності корпоративних мереж за допомогою поліномів Бернштейна. // Сучасні інформаційні системи. Том 4, №3(2020) С.118-123.

14. Киричок Р.В., Шуклін Г.В. Алгоритм побудови аналітичних залежностей показників якості валідації вразливостей при активному аналізі захищеності корпоративних мереж. IX Міжнародна науково-практична конференція «SCIENCE, SOCIETY, EDUCATION: TOPICAL ISSUES AND DEVELOPMENT PROSPECTS». м. Харків, 2-4 серпня 2020 р. Харків. С. 113-115.

References

1. Kyrychok R. Penetration test as a simulation approach to the analysis of security of corporate information systems. Modern information protection. 2018. №2(34). P. 53-58.

2. Chen F., Su J., and Zhang Y. A scalable approach to full attack graphs generation. Engineering Secure Software and Systems, Springer. 2009. P. 150-163.

3. Abramov E., Andreev A., Mordvin D. Application of attack graphs for modeling malicious network attacks. Bulletin of the Southern Federal University. Technical science. 2012. Volume 26. Issue 1. P. 165-173.

4. Barik M., Sengupta A., Mazumdar C. Attack graph generation and analysis techniques. Defence Science Journal. 2016. №66(6). P. 559-567.

5. Shipileva A. Automatic generation of attack graphs based on branching processes in a random environment. International scientific and practical conference "New Science: Strategies and Development Vectors". Part 2. Sterlitamak, March 8, 2017. P. 143-144.

6. Durkota K. and Lisy V. Computing optimal policies for attack graphs with action failures and costs. In 7th European Starting AI Researchers` Symposium «STAIRS'14». January 2014.

7. Sarraute C., Buffet O., Hoffmann J. POMDPs make better hackers: Accounting for uncertainty in penetration testing. In Proceedings of the 26th AAAI Conference on Artificial Intelligence «AAAI'12». Toronto, ON, Canada, July 2012. AAAI Press. P. 1816-1824

8. Obes, J., Richarte G., Sarraute C. Attack planning in the real world. In Proceedings of the 2nd Workshop on Intelligent Security «SecArt'10». Atlanta, USA. July 12, 2010.

9. Qiu X., Wang S., Jia Q., Xia C. and Lv L. Automatic generation algorithm of penetration graph in penetration testing. Proceedings of the 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, IEEE. Guangdong, China. Nov 8-10, 2014. P. 531-537.

10. Steinmetz M. Critical constrained planning and an application to network penetration testing. 26th Int Conf on Automated Planning and Scheduling. 2016. P.141-144.

11. Hoffman J. Simulated Penetration Testing: From "Dijkstra" to "Turing Test++". In Proceedings of the Twenty-Fifth International Conference on Automated Planning and Scheduling, «ICAPS'15». Jerusalem, Israel. June 7-11, 2015. P. 364–372.

12. Luan J., Wang J., Xue M. Automated Vulnerability Modeling and Verification for Penetration Testing Using Petri Nets. Springer, Lecture Notes in Computer Science. July 2016.

13. Kyrychok R., Shuklin G., Barabash O., Gaidur G. Modeling the vulnerabilities validation mechanism in the active analysis of the security of corporate networks using Bernstein polynomials. // Morden informations systems Vol.4, №3(2020) P. 118-123.

14. Kyrychok R., Shuklin G. Algorithm for constructing analytical dependences of vulnerability validation quality indicators in active analysis of corporate network security. Abstracts of the 9th International scientific and practical conference «SCIENCE, SOCIETY, EDUCATION: TOPICAL ISSUES AND DEVELOPMENT PROSPECTS». Kharkiv, Ukraine. August 2-4, 2020. P. 113-115.