Міністерство освіти і науки України
Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

Дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

ґалузь знань *12 Інформаційні технології*
(шифр і назва ґалузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній рівень *магістр*
(назва освітнього рівня)

кваліфікація _____
(код і назва спеціальності)

на тему: *Розробка методики сканування на вразливості на базі Tenable*

Виконавець: студент шостого **курсу, групи** КБм-21

_____ **Гетман Владислав Євгенович**
(підпис) (прізвище ім'я по батькові)

	Прізвище, ініціали	Оцінка	Підпис
Науковий керівник	**Толюпа С.В.**		
Рецензент	**Степанов М.М.**		
Нормоконтроль	**Даков С.Ю.**		

Київ
2022

Міністерство освіти і науки України

Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту інформації

_____ Лукова-Чуйко Н.В.

«_____»_____2021року

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

студенту КБм-21 (група) Гетьману Владиславу Євгеновичу (прізвище ім'я по-батькові)

Тема дипломного роботи Розробка методики сканування на вразливості на базі Tenable

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 29.10.2021 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень процес сканування на вразливості інформаційної системи

Предмет досліджень методи та засоби сканування мережі на вразливість

Мета розробка методики сканування на вразливості на базі Tenable

Вихідні дані для проведення роботи результати сканування мереж на вразливість

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна полягає у реалізації запропонованої методики сканування на вразливості на базі Tenable

Практична цінність полягає у реалізації методики сканування на вразливості на базі Tenable. Результати здійснених у кваліфікаційній роботі досліджень можуть бути використані у сфері захисту банківської інформації, у вищих навчальних закладах з підготовки ІТ-фахівців, для підготовки сертифікованих співробітників у сфері управління вразливостями, а також у науково-популярних цілях.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Обґрунтування вибору теми роботи. Попереднє складання змісту магістерської роботи.	29.10.2021 – 01.01.2022
Первинний аналіз літературних джерел. Збір і обробка конкретних теоретичних положень.	02.01.20122 – 02.03.2022
Проведення необхідних практичних досліджень. Написання та оформлення бакалаврської роботи.	03.03.2022 – 01.05.2022
Перевірка роботи науковим керівником. Оформлення і друк пояснювальної записки.	02.05.2022 – 19.05.2022

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект зниження витрат на покриття збитків через вразливість

Соціальний ефект Покращення оцінки рівня захищеності інформаційної мережі

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ _____
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ЕК _____

РЕФЕРАТ

Пояснювальна записка: 51 с., 13 рис., 2 табл., 2 додатків, 20 джерел.

Об’єкт дослідження: процес сканування на вразливості інформаційної системи.

Мета роботи: розробка методики сканування на вразливості на базі Tenable.

Методи дослідження: аналіз, синтез та індукція існуючих поглядів на процес сканування на вразливості, системний підхід до сфери керування вразливостями.

У роботі досліджено принцип роботи сканерів вразливостей, проведено аналіз регулюючих та нормативних стандартів в області керування вразливостями, запропоновано, побудовано основні етапи процесу керування вразливостями, розроблено власну методику сканування на вразливості.

Практичне завдання роботи полягає у реалізації методики сканування на вразливості на базі Tenable. Результати здійснених у дипломній роботі досліджень можуть бути використані у сфері захисту банківської інформації, у вищих навчальних закладах з підготовки ІТ-фахівців, для підготовки сертифікованих співробітників у сфері управління вразливостями, а також у науково-популярних цілях.

Наукова новизна дослідження полягає у сформульованій державною мовою теоретичній та практичній нормативній базі, що регулює процедури сканування на вразливості. Напрямки подальших досліджень полягають у реалізації даної методики як іншими інструментами, так розширення місця її застосування (державні установи, в яких акумулює державна таємниця).

Ключові слова: сканування, вразливість, методика, процес, процедура, Tenable.

ЗМІСТ

ВСТУП

Інформаційна безпека підприємства починається зі співробітників, які до безпеки не мають жодного стосунку. Кожен пристрій, незалежно від того, чи працює з ним клієнт або менеджер (правильніше буде сказати навіть оператор) є ресурсом підприємства, а тому може зазнавати змін, видалення, псування, нейтралізації, компрометації, і саме в такому порядку, адже в першу чергу для співробітників безпеки важливий контроль над заявленою зоною контролю [1, 2]. У разі відсутності цього контролю ми ризикуємо зіткнутися з компрометацією як ресурсу (пристрою, про яку йдеться мова вище), так й самої системи, у якій даний ресурс функціонує.

Завдання спеціаліста інформаційної безпеки точно визначити, який ресурс може зазнавати несанкціонованих змін (грубо кажучи, компрометації в перспективі), після чого ухвалити рішення щодо усунення ризиків ресурсу до появи наслідків дії цього ризику (в терміновому порядку після появи) [3].

Одним з напрямків роботи в даній сфері є управління вразливістю. Сканування пристроїв, систем, ресурсів на уразливості є невід'ємною частиною зазначеного процесу. Вибір методики з управління вразливістю є одним із питань, з яким пов'язане сканування на вразливості.

У даній роботі з виконання індивідуального навчального завдання дисципліни «Науково-дослідної практики», а саме формалізації вимог щодо створення методики для проведення сканування на вразливості на основі інструменту Tenable, розглядається комплекс обов’язкових до виконання мір, для забезпечення вимог нормативної бази процесу сканування на вразливості, визначений перелік проблем, які виникають при спробі створити регламентований процес сканування в підприємстві.

Ця тема є конкурентоспроможною по відношенню до інших тем у сфері кібербезпеки і виділяється відсутністю єдиного вірного рішення за своїм визначенням, так як основа управління вразливістю скоріше лежить у

багатогранності та кількості рішень, ніж в універсальності одного окремо взятого, проте це не дозволяє робити висновок, що останній варіант побудови управління уразливістю неможливий.

Так чи інакше, дана робота служить рішенням для фахівців банківської сфери у питаннях підготовки до впровадження управління вразливістю, вибору методики проведення сканування на вразливості, уточнення найважливіших позначень у зазначених вище категоріях. Також цей матеріал пропонується до використання у ВНЗ з підготовки фахівців інформаційної безпеки, фахівців фінансової безпеки та мережевих інженерів, для підготовки сертифікованих співробітників у сфері управління вразливостями, а також у науково-популярних цілях.

РОЗДІЛ 1
ПЕРЕДУМОВИ ДЛЯ РОЗРОБКИ

1.1 Актуальність проблеми

Загалом, в інформаційній безпеці наявна проблема її абсолютності [4], що вказує на те, що захист системи так, щоб її цілісність, доступність та конфіденційність були витримані на рівні 100%, все ще не досліджений, проте це легко обґрунтувати фізикою процесу – будь-який пристрій працює завдяки електроенергії, що вже компрометує його на предмет сигналу.

Так, звужуючи об’єкт до інформаційної безпеки у підприємстві, ми отримуємо оцінно-імовірнісний підхід до забезпечення інформаційного захисту ресурсів організації [5]. Так, наприклад, наведення побічним електро-магнітним випромінюванням менш імовірне, аніж небезпека в програмному забезпеченні ресурсу, адже реалізувати наведення злодію складніше.

В такому підході першу роль відіграють вразливості, які існують у кожному ресурсі системи. Кожна вразливість має свої характеристики, такі як об’єкт, вірогідність, наслідки та інше. Так, вразливість є мірою опису тієї проблеми абсолютності інформаційної безпеки, про яку йдеться мова вище [6].

Банк як об’єкт критичної інфраструктури дуже критичний до втрат інформації, розголошення даних, що зберігаються на його ресурсах, втрат коштів і т. п. Робота над пошуком вразливостей для їх послідовного усунення є обов’язковою вимогою Національного Банку України [7]. Головним чином, для банків постає питання не «що потрібно зробити, щоб захистити себе?», а «як зробити так, щоб захистити себе?».

Так, кожне рішення з пошуку та власними варіантами усунення вразливості дуже дорого коштує на ринку. Особливо дорого коштують рішення з пошуку вразливостей програмного забезпечення, мережевих пристроїв та мережевої інфраструктури, адже саме дані технології забезпечують банку

сучасні можливості, про які знає кожен клієнт. Якісним варіантом слугують сканери на вразливості, які допомагають вирішити проблему з вразливостями в системі.

Тема сканування на вразливості має свої проблеми:

1) недостатня стурбованість темою проведення сканування на вразливості (відсутність якісних обґрунтувань для її актуалізації);

2) сканування на вимогу аудиту (окремий вид сканування, який за основну мету має сканування на відповідність);

3) відсутність нормативно-правової основи для формалізації процесу;

4) проблеми патч-менеджменту;

5) конфлікт з невідмовністю системи та комунікація підрозділів в управлінні вразливістю.

6) складність оптимізації процесу без зміни інструменту сканування;

7) вибір інструменту для сканування;

Проте особливе місце відведено саме методу сканування. Чому?

1. Тому що інструменти, які використовуються для впровадження даної поставленої мети, обмежені в кількості (і якості: свій інструмент, який буде сертифікований на рівні Tenable, створити в короткостроковій перспективі та на базі, яка є в Україні - складно, а якщо сказати простіше – неможливо).

2. Тому що в порівнянні з такими факторами, як суб'єкт проведення (безпосередньо співробітник інформаційної безпеки), об'єкт проведення (зріз мереж, сервер, робоча станція, мережеві вузли (комутатори, роутери, свитчі тощо), технологія (структура) шуканого (експлойту), інтеграція коїться з іншими сферами, економічний чинник, філософське наповнення (терміни, визначення) саме методологія сканування грає провідну роль впливу на об'єкт дослідження (сканування) як такий.

Тож метою, яка була поставлена в рамках першого розділу, є проведення пошуку тієї нормативної бази щодо створення методики для проведення сканування на вразливості та її аналіз для актуалізації задокументованих знань, які знаходяться у відкритому доступі.

1.2 Нормативна база або дослідження, що проведені на даний час

1.2.1 Українська державна регулююча документація.

На сьогодні проблема, що представляє собою відсутність відповідної методології щодо проведення сканування на вразливості в підприємстві за нормативно-правовою галуззю в Україні набирає досить великих масштабів. Спеціалісти, яким поставлена задача організувати в своїй компанії процес регулярного сканування, стикаються з проблемою формалізації та наповнення ще на етапі ознайомлення з проблемою. На жаль, головним чином, основний нормативний регулятор державних норм в сфері кібербезпеки – Держспецзв'язок – не отримував завдань щодо побудови власної державної методології сканування на вразливості чи хоча б рекомендацій щодо проведення її власним інструментарієм (для цього потрібен власний інструмент державного походження, який на даний момент, як сказано в пункті 1.1, відсутній). При цьому засади організації процесу сканування зовнішніми компаніями або створеним на підприємстві комісіями були зазначені в документі «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті» від 15.01.16 [8, 9].

Даний документ в цілому фокусує уваґу на державних інформаційних ресурсах розміщених в інтернеті. Терміни, що наведені в Порядку, вживаються у значеннях, що і в законах України «Про захист інформації в інформаційно-телекомунікаційних системах» [10], «Про телекомунікації» [11], «Про Державну службу спеціального зв'язку та захисту інформації України» [12], «Про основні засади забезпечення кібербезпеки України» [13]. Варто помітити, що термін «вразливість» зустрічається декілька разів лише в законі «Про основні засади забезпечення кібербезпеки України», в той момент як «сканування» загалом відсутнє (якщо не звертати уваги на словосполуку «виявлення вразливостей») [13].

Проте варто зазначити, що зґаданий Порядок містить формалізовану процедуру ініціації сканування в інформаційно-телекомунікаційній системі, в якій обробляються державні інформаційні ресурси. Окремий розділ, шо стосується процесу сканування, має такі вказівки [9]:

«… 2. ДЦКЗ Держспецзв'язку організовує заходи зі сканування на підставі письмового звернення розпорядника розміщеного в Інтернеті ДІР та за рішенням Голови Держспецзв'язку або його заступника відповідно до розподілу функціональних обов'язків.

3. ДЦКЗ Держспецзв'язку:

письмово інформує розпорядника розміщеного в Інтернеті ДІР та власника ІТС (якщо розпорядник розміщеного в Інтернеті ДІР не є власником ІТС, у якій обробляється відповідний ресурс) про строки, обсяг та зміст заходів, які будуть проведені у процесі сканування;

не пізніше ніж за три робочих дні інформує Службу безпеки України про об'єкт, строки та методи проведення сканування. Для термінового інформування також використовується електронна пошта.

4. За результатами сканування посадові особи ДЦКЗ Держспецзв'язку, що безпосередньо здійснювали сканування, складають акт сканування на предмет вразливості розміщених в Інтернеті державних інформаційних ресурсів (далі - Акт) за формою, що наведена у додатку до цього Порядку, в якому викладають результати сканування, висновки та відповідні рекомендації.

5. Акт складається у двох примірниках, його затверджує Голова Держспецзв'язку або його заступник відповідно до розподілу обов'язків.

6. Примірники Акта не пізніше ніж за десять днів після його затвердження надсилаються розпоряднику розміщених в Інтернеті ДІР для ознайомлення з ним керівника або уповноваженої особи державного органу, що звертався…».

Акт розташований за посиланням [9]. Важливо розуміти, що дана процедура регулює процес ініціації та формалізації результатів сканування,

проте методика за якою сканування буде проводитись в даному Порядку відсутня.

Вище окреслене підтверджує думку про відсутність власної нормативно-правової бази щодо методології сканування на вразливості в головних законах України, які стосуються безпеки на підприємствах. Проте варто розуміти, що організаційна модель процедури ініціації перевірки інформаційної системи на вразливості все ж створена, приймає формалізований вигляд та знаходиться у відкритому доступі.

Стосовно вимог, про які йдеться при створенні методики (або в результаті побудови методології) сканування на вразливості в фінансовій установі, йдеться в постанові від Національного Банку України від 28.09.2017 №95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі» [7], проте вимога лише одна і виглядає вона наступним чином: «Банк зобов'язаний на стадії експлуатації інформаційних систем задокументувати положення щодо: … 2) контролю вразливостей в обладнанні та програмному забезпеченні інформаційних систем банку». Як можна зрозуміти з наведеного пункту, методика сканування на вразливостей (та керування вразливостями загалом) має бути створена на підприємстві, проте які пункти вона має містити та які вимоги має виконувати (оцінка, якість, час, тощо) цілком і повністю має визначати в своєму положенні фінансова установа. Тож проблема, з якою стикається спеціаліст інформаційної безпеки і про яку зазначено вище (в пункті 1.1), про державні нормативно-правові засади для створення методики на сканування вразливостей, дійсно існує і не мають регламентованого вигляду.

1.2.2 Згадування в серії ISO/IEC

Якщо задача на підприємстві поставлена, її потрібно виконувати в строки. Спеціаліст, що не знайшов відповіді на питання в державних джерелах, звертається до джерел іноземних (державних та приватних).

Такі джерела існують – головним чином, інформація, яка стосується керування вразливостями, виражена в стандарті ISO/IEC 29147:2018 «Vulnerability Disclosure in Information Technology» («Розкриття уразливостей в інформаційних технологіях») [14].

Для цілей інформаційних технологій та кібербезпеки, відповідно до стандарту ISO/IEC 29147:2018 – Інформаційні технології – Методи безпеки – Розкриття вразливостей, уразливість – це поведінка або набір умов, присутніх у системі, продукті, компоненті чи службі, які «порушують неявні або чітку політику безпеки». ISO/IEC 29147:2018 описує розкриття вразливостей, яке він визначає як «методи та політики для постачальників, щоб отримувати звіти про вразливості та публікувати інформацію про усунення». ISO/IEC 29147:2018 надає вказівки та рекомендації щодо розкриття вразливостей для постачальників, що дає змогу користувачам виконувати технічне керування вразливими місцями, як зазначено в ISO/IEC 27002:2013 – Кодекс практики щодо методів безпеки інформаційних технологій для контролю інформаційної безпеки [15]. Зокрема, ISO/IEC 29147:2018 містить рекомендації щодо отримання звітів про потенційні вразливості, рекомендації щодо розкриття інформації про усунення вразливостей, терміни та визначення, специфічні для розкриття вразливостей, концепції розкриття вразливостей, методи та міркування політики, пов’язані з методами розкриття вразливостей, а також приклади політики та комунікації [14].

Врахування цих різних вразливих факторів і процесів має вирішальне значення, оскільки організації зараз можуть покладатися на системи з відомими вразливими місцями. У багатьох випадках персонал може навіть не знати про наявність вразливостей, не звертаючись до цих інструкцій. ISO/IEC 29147:2018 є другим виданням міжнародного стандарту для розкриття вразливостей. Він оновлює видання 2014 року з такими змінами: Додано декілька нормативних положень (вони узагальнено в Додатку D «Резюме нормативних елементів»). Для наочності внесено численні організаційні та редакційні зміни. Інші пов’язані дії, які відбуваються між отриманням та розкриттям звітів про

вразливості, описані в ISO/IEC 30111:2019 – Інформаційні технології – Методи безпеки – Процеси обробки вразливостей [16].

На жаль, стандарту ISO/IEC 29147:2018 немає у відкритому доступі, що також зводить нанівець старання з організації процесу проведення сканування на підприємстві, якщо стоїть завдання створити таку процедуру користуючись лише власними ресурсами. Це у жодному разі не говорить про відсутність даної нормативно-регулюючої бази, проте варто зауважити і те, що даний стандарт носить рекомендації зі створення та не є чільним та обов'язковим до виконання в такому ж вигляді, в якому означене рішення пропонується.

1.2.3. Серія NIST SP.

У серії стандартів NIST проблема опису процесу вирішена і викладена у вільному доступі, що є перевагою над окресленими вище прикладами формалізації процедури сканування. NIST надає всеосяжний огляд процедури сканування починаючи з вимог до процесу керування вразливостями і закінчуючи вендорами, які є сертифікованими NIST.

Таким стандартом є публікація NIST SP 800-40 v.2.0 «Creating a Patch and Vulnerability Management Program», видана підрозділом комп'ютерної безпеки лабораторії інформаційних технологій національного інституту стандартів та технології в листопаді 2005.

Як правильно зазначено у вступі до статті, «…The expected result is to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities…» - «…Очікуваний результат – скорочення часу і гроші, витрачені на усунення вразливостей та використання цих вразливостей…», адже це входить в бізнес-ціль будь-якого підприємства, яке впроваджує процес сканування та усунення вразливостей [17].

Також на початку надаються певні вимоги, які висуваються до процедури керування вразливостями [17]:

– організації повинні створити певну групу з виявлення та усунення вразливостей, щоб полегшити ідентифікацію та поширення патчів всередині організації;

– організації повинні використовувати автоматизовані інструменти керування виправленнями, щоб прискорити розповсюдження виправлень серед систем;

– організації повинні розгортати корпоративні інструменти управління виправленнями, використовуючи поетапний підхід;

– організації повинні оцінити та пом'якшити ризики, пов'язані з розгортанням корпоративних інструментів управління виправленнями;

– організації повинні розглянути можливість використання стандартизованих конфігурацій для IT-ресурсів;

– організації повинні постійно вимірювати ефективність своєї програми керування вразливостями та патч-менеджменту та застосовувати коригувальні дії, якщо необхідно.

NIST рекомендує організаціям створити групу осіб, яку називають групою виправлення та вразливості (PVG), яким спеціально доручено впроваджувати програму управління виправленнями та вразливістю [17].

PVG є центральним пунктом для зусиль щодо усунення вразливостей (наприклад, виправлення та зміни конфігурації). Оскільки PVG має активно співпрацювати з локальними адміністраторами, великим організаціям може знадобитися мають кілька PVG. Ці PVG можуть працювати разом у конфедерації або можуть бути структуровані ієрархічно з авторитетним PVG верхнього рівня. Решта цього документа базується на припущенні, що на одну організацію існує лише один PVG [17].

Першим на етапі роботи PVG NIST називає інвентаризацію системи. PVG має використовувати наявні інвентаризації IT організації ресурси, щоб визначити, яке апаратне обладнання, операційні системи та програмні додатки використовуються в організації.

Далі NIST наводить такі пункти [17]:

1. Відстеження вразливостей, усунення вразливостей та загроз. PVG відповідає за моніторинг джерел безпеки для повідомлень про вразливості і нові загрози, які відповідають програмному забезпеченню в системі PVG.

2. Пріоритет усуненню вразливостей. PVG має розставити пріоритети в порядку, в якому організація займається усуненням уразливостей.

3. Створення базу даних виправлення для конкретної організації. PVG має створити базу даних виправлення, які необхідно застосувати до організації.

4. Проведення загального тестування виправлень. PVG повинен мати можливість тестувати виправлення та виправлення без виправлень на IT-пристроях, які використовують стандартизовані конфігурації. Це дозволить уникнути необхідності для локальних адміністраторів для виконання надлишкового тестування. PVG також має тісно співпрацювати з локальні адміністратори, щоб перевірити виправлення та зміни конфігурації на важливих системах.

5. Розгорнення засоби усунення вразливостей. PVG має наглядати за усуненням уразливостей.

6. Надання місцевим адміністраторам інформацію про вразливості та усунення несправностей. PVG несе відповідальність за інформування місцевих адміністраторів про вразливі місця та їх усунення відповідають пакетам програмного забезпечення, що входять до сфери застосування PVG і які входять до організаційної інвентаризація програмного забезпечення.

7. Автоматичне розгортання патчів. PVG має автоматично розгортати виправлення IT-пристрої з використанням корпоративних засобів керування виправленнями. Крім того, PVG може тісно співпрацювати з групою, яка фактично запускає інструменти керування виправленнями. Автоматичні інструменти виправлення дозволяють адміністратору оновлення сотень і навіть тисяч систем з однієї консолі. Розгортання є досить простим, коли існують однорідні обчислювальні платформи, с стандартизовані настільні системи та сервери, налаштовані аналогічно. Багатоплатформні середовища, нестандартні

настільні системи, застарілі комп’ютери та комп’ютери з незвичайною конфігурацією можуть також бути інтегрованим.

8. Налаштування автоматичне оновлення програм, коли це можливо та доречно. Системи вразливостей забезпечують функцію, яка перевіряє веб-сайт постачальника на наявність оновлень. Ця особливість може бути дуже корисним для мінімізації рівня зусиль, необхідних для виявлення, поширення та встановлення патчів. Однак деякі організації можуть не захотіти впроваджувати цю функцію, оскільки вона може заважати їхньому процесу керування конфігурацією. Рекомендованим варіантом буде локально розподілений автоматизований процес оновлення, де виправлення стають доступними з мережа організації. Потім програми можна оновлювати з локальної мережі, а не з інтернет.

9. Перевірка усунення вразливості за допомогою сканування уразливостей мережі та хосту. PVG має переконатися, що вразливості були успішно усунені.

10. Навчання з усунення вразливостей. PVG має навчати адміністраторів тому, як подати заявку усунення вразливостей. В організаціях, які покладаються на кінцевих користувачів у виправленні комп’ютерів, PVG також необхідно навчати користувачів цій функції.

Так, сам NIST (точніше дане положення NIST) містить рекомендації для роботи системним адміністраторам, є корисним в зазначеній сфері.

Не менш важливим є і пункт «Групування та визначення пріоритетів ресурсів інформаційних технологій» про категоріювання ресурсів в даному положенні.

Ресурси в рамках інвентаризації повинні бути «згруповані» та призначені рівні пріоритету, щоб полегшити зусилля з відновлення. «Групування» ресурсів і визначення пріоритетів корисні для оцінки ризику для систем, і їх слід використовувати, щоб допомогти визначити, які системи можуть потребувати особливої уваги з боку програми управління виправленнями та вразливими місцями. Основне «групування» має проводитися за назвою системи та

позначенням впливу за Федеральним стандартом обробки інформації (FIPS) 199.9 [18]. Також може бути корисно «групувати» ресурси за розташуванням мережі. Це особливо важливо для тих ресурсів, які безпосередньо відкриті для Інтернету, і тих, які знаходяться за внутрішніми зонами високої безпеки. Якщо це «групування» та визначення пріоритетів не виконуються, організації можуть розпочати невиправдано дорогі стратегії відновлення. Наприклад, коли в організації виявлено нову вразливість, яка не визначає пріоритети усунення, системним адміністраторам може бути доручено негайно виправити всі вразливі комп'ютери. Це може призвести до серйозних збоїв, оскільки системні адміністратори припиняють всю іншу роботу, щоб вони могли виправити комп'ютери. Ще гірше те, що виправлення можна застосувати швидко без ретельного тестування, що призведе до фактичного пошкодження систем організації. З визначенням пріоритетів організація може зрозуміти, що більшість уразливих комп'ютерів можна виправити протягом певного періоду часу, використовуючи стандартний процес керування конфігурацією організації та процедури тестування виправлень. Тоді організація могла б зосередити свої негайні зусилля по виправленню виправлень на вразливих комп'ютерах, які найбільше піддаються ризику (наприклад, на тих, хто безпосередньо підключений до Інтернету) [17].

NIST регулює і донесення інформації про вразливості та усунення адміністраторам. Основним способом, яким PVG повинен доносити звіт про вразливості спеціальним програмним забезпечення (vulnerability system), яке керує корпортивними виправленнями згідно NIST SP 800-40 v.2.0. Однак іноді PVG має повідомити про виправлення безпосередньо локальними комунікаційними каналами. Наприклад, електронна пошта може слугувати ефективним методом поширення інформації щодо пріоритету вразливостей, відомості про відповідні патчі, модифікації конфігурації та інше деталі. Однак, щоб зменшити ймовірність підробленого електронного листа, що містить експлойт троянського коня, актуальні патчі повинні передаватися группою PVG адміністраторам із внутрішнього захищеного веб-сайту (в ідеалі патчі

розповсюджуються за допомогою автоматизованих інструментів відправки). До речі, така опція присутня в Tenable, практична реалізація якого наведена далі в роботі. Додаткові елементи керування можуть використовуватися для підтримки цілісності патчів і електронної пошти, наприклад, використання цифрових підписів. Кілька електронних листів списки можуть підтримуватися для адміністраторів, які відповідають за різні типи систем (наприклад, UNIX адміністратори, адміністратори Windows). Альтернативні методи розповсюдження патч і інформації, наприклад, на диску, слід враховувати, якщо мережа або захищений веб-сайт нестабільні або непридатні для використання [17].

Загалом, до моменту з фальш-позитивами та після, NIST наводить інформацію про інструменти, процедуру, деталі сканування, що є досить важливим моментом, коли мова заходить про методику сканування. NIST досить розгорнуто фокусує уваґу і на інших етапах керування вразливостями – патч-менеджменту, повторного сканування, вибору інструмента, оцінки отриманих вразливостей, тощо.

Якісною різницею з наведеними раніше стандартами та положеннями є згадка про фальш-позитиви та фальш-негативи, про які далі каже NIST. «Усі програми метрики патчінгу та вразливості мають певною мірою працювати з фальш-позитивами та фальш-негативами. Помилково-позитивний – це коли щось (наприклад, вразливість) насправді не існує, але враховується при вимірюванні. Помилково-негативний – це коли щось існує, але не враховується у вимірювання. Історично склалося так, що інструменти патч-менеджменту підприємства мали не так багато проблем у цій області, як сканери вразливостей на базі хостів, і тим паче, ніж мережеві сканери вразливостей. Проте корпоративні інструменти патч-менеджменту можуть навіть стикатися з фальш-позитивами, коли вони працюють ідеально. Наприклад, якщо виправлення неможливо застосувати до певного сервера, то відсутність виправлення не враховується в метриках (хоча сервер має бути захищений через альтернативні механізми). PVG повинен буде відстежувати відомі фальш-

позитивні та фальш-негативні результати та видаляти такі «вразливості» з процесу вимірювання. Сканери вразливостей часто містять підписи, призначені для інформаційних цілей. "Alert" на одному з цих підписів не вказує на реальну вразливість. Ці інформаційні підписи можуть бути великим джерелом фальшпозитивних результатів у програмі сканування вразливостей.

Висновки за розділом 1

Тепер, коли були всеосяжно розглянуті головні серії стандартів та положень, якими має користуватись спеціаліст з інформаційної безпеки, вивчаючи питання створення методики сканування на вразливості, або хоча б проведення такого сканування, можна зробити декілька головних висновків:

- дійсно, нормативне регулювання ситуації з керуванням вразливостями на підприємствах, що стосуються фінансової сфери, в Україні проводить НБУ, а термінологію та певну базу для такого регулювання готує Держспецзв'язок, і можливо, саме недостатнє охоплення приватного бізнеса (мається на увазі, сфери, що не регулюються ані Держспецзв'язком, ані НБУ) в сфері керування вразливостями є перешкодою до створення власної державної методології з даного питання. Іншою проблему може бути достатня «насиченість» українського бізнес-ринку закордонними стандартами, тобто велика кількість компаній, що дотримуються стандарту серій ISO/IEC або NIST, і саме тому немає потреби в створенні власної методології.
- виходячи з розгорнутості окремих положень стандартів серій ISO/IEC та NIST, варто сказати, що NIST має більш сфокусований порядок правил та більш орієнтовану на реалізацію процедуру проведення сканування, аніж європейська серія. Так, звичайно, стосовно якості стандартів говорити не доводиться, проте акцент на NIST все одно буде вважатися більш наближеним до деталізованого процесу, аніж у зворотньому випадку.

Головним чином, актуальність проблеми не тільки не втратила своєї сили, а і набула її, адже при створенні власної методики варто звертати на сильні сторони усіх формалізованих регулятивних документів.

В наступних розділах на результатах вже виконаної роботи буде проведена розробка методики на сканування вразливостей на вже розібраному в роботі інструментарії Tenable [19, 20].

РОЗДІЛ 2
МЕТОДИКА СКАНУВАННЯ НА ВРАЗЛИВОСТІ

2.1 Визначення сфери дії

Визначення сфери дії методики є головним чинником тих змін, які будуть відбуватися в результаті виконання зазначеної методики.

Методика, що розроблятиметься, (сканування на вразливості в інформаційних системах) регламентує організаційну діяльність структурних підрозділів підприємства (фінансової установи) щодо виявлення вразливостей в інформаційних системах (далі – ІТ) та їх категоріювання в залежності від рівня їх критичності та відповідно до норм і стандартів безпеки цієї фінансової установи.

Сфера дії поширюється на всі етапи процедури сканування, тобто виявлення вразливостей в інформаційних системах Банку, як на одну з основних складових частин забезпечення їх життєвого циклу та в межах визначеного ним основного порядку виконання робіт, відповідно до норм та стандартів безпеки. Це визначення включає всі активи обробки інформації. Сюди входять усі системи, підключені до мережі, а також хмарні активи, мобільні пристрої чи контейнерні активи.

Усі роботи, які проводяться відповідно до цієї методики, повинні виконуватись виключно в рамках процесів керування конфігураціями, змінами та роботами з обов’язковою реєстрацією у системі змін.

Управління вразливостями — разом із розвідкою загроз — відповідає за моніторинг джерел інформації щодо повідомлень про вразливості, усунення виправлення та усунення несправностей, а також загроз, які відповідають активам в рамках інвентаризації активів організації.

2.2 Процес керування вразливостями та його основні етапи

Процес керування вразливостями має визначати процедури взаємодії відповідального спеціаліста з інформаційної безпеки та адміністраторів серверів і систем головним чином по виявленню та усуненню вразливостей, а також їх повторній перевірці, відповідно до норм та стандартів безпеки підприємства з забезпечення надійної роботи інформаційної системи організації. Процедура керування вразливостями в інформаційних системах організації схематично може мати вигляд як показано на рисунку 2.1.

Основні етапи процесу керування вразливостями, які було означено [20]:

1. планування та погодження сканування;
2. проведення первинного та повторного сканування;
3. аналіз результатів та визначення відповідальних;
4. визначення фальш-позитивності вразливостей;
5. визначення систем які підлягають тестуванню на вразливості;
6. усунення вразливостей;
7. пост-перевірка усунення вразливостей.

2.3 Планування та погодження сканування

Графік планового сканування інформаційної системи створює відповідальний працівник управління інформаційної безпеки на основі інформації карти мереж організації та інформації отриманої в результаті сканування мереж (дискаверінг) на наявність мережевих пристроїв.

Графік має містити наступну інформацію про інформаційні системи:

- ідентифікатор мережі серверів;
- тип мережі;
- дата та час сканування.

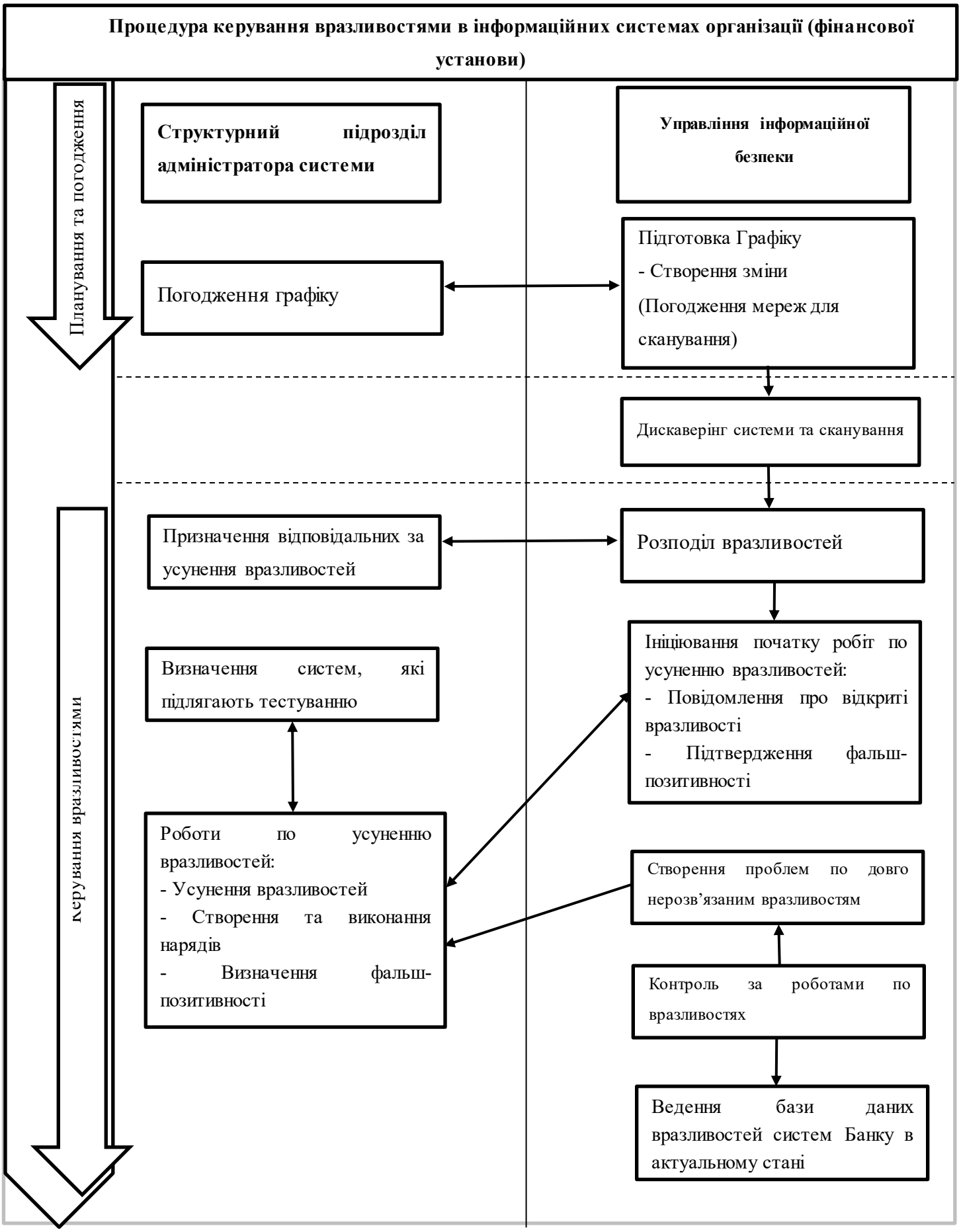

Рисунок 2.1 – Процедура керування вразливостями

Графік планового сканування має бути завчасно створеним. При створенні графіку враховується, що:

- планове сканування повинно проводиться з періодичністю один раз на місяць [20];
- сканування відбувається в розрізі мереж;
- у графіку повинна бути вказана дата початку сканування;
- графік погоджується з директорами структурних підрозділів (відділів телекомунікаційних технологій та бізнес-власників мережевих ресурсів) та начальником управління інформаційної безпеки.

Погодження графіку виконується в системі змін шляхом створення відповідної зміни з обов'язковим винесенням на голосування.

2.4 Проведення первинного та повторного сканування

Сканування виконується згідно з погодженим графіком.

Перед кожним щомісячним скануванням відповідальний спеціаліст з інформаційної безпеки створює в системі змін інцидент з інформацією про сканування (дату та час його початку і завершення). Перед кожним плановим скануванням за два дні відправляється засобами електронної пошти підприємства лист-попередження про початок сканування на IT-власників системи/серверу.

Забороняється проводити позапланові сканування без додаткового погодження з IT-власником системи/серверу. Додаткове погодження виконується в системі змін шляхом створення відповідної зміни на погодження.

Сканування на вразливості в розрізі мереж та серверів відбувається виключно через авторизацію користувачем (опція в Tenable, яка допомагає забезпечити аутентифікацію), тобто через спеціальний обліковий запис. Цей обліковий запис має відповідати стандарту управління ідентифікацією та доступом за всією компанією.

Сканування тестових мереж та серверів розташованих в тестових мережах може проводитися без попереднього погодження.

Сканування мереж робочих станцій та самих робочих станцій проводиться без попереднього погодження.

Результатом проведення сканування серверів є звіти, які включають в себе інформацію про виявлені вразливості, їх опис та список серверів на яких вони були знайдені та рекомендації щодо усунення вразливостей.

2.5 Аналіз результатів та визначення відповідальних за вразливості

Коли сканування вже проведене, необхідно забезпечити процес усунення вразливостей перед повторним скануванням. В рамках цієї процедури відповідальний працівник управління інформаційної безпеки проводить аналіз отриманої інформації та створює необхідну звітну документацію, яка містить:

- список усіх відкритих вразливостей;
- список усіх закритих вразливостей;
- середня кількість вразливостей на хості (critical, high, medium);
- інформацію про вразливість;
- інформацію про IP-адресу та мережевий порт, на яких виявлено вразливість.

Розподілення нарядів в системі змін на усунення вразливостей відбувається на основі визначених IT-власників систем/серверів та адміністраторів серверів і систем, на яких було знайдено вразливості.

Відповідальність за створення та контроль за виконанням змін щодо усунення вразливостей несе відповідальний працівник управління інформаційної безпеки. Відповідальність за усунення вразливостей системи/серверів та створення нарядів несе відповідний IT-власник системи/ серверу.

В ході визначення відповідальних за вразливості та за умови неможливості визначення IT-власника системи, такі вразливості відносяться до вразливостей

сервера та назначаються відповідному адміністратору сервера. Якщо програмне забезпечення знаходиться за межами зони відповідальності структурного підрозділу адміністратора серверу – такі вразливості направляються до відповідального працівника ІТ для уточнення ІТ-власника програмного забезпечення. Ця операція виконується шляхом зміни виконавця по наряду чи створення нового наряду на відповідального працівника ІТ з відповідним коментарем в протоколі. Якщо адміністратору серверу відомий ІТ-власник системи/серверу чи ІТ-власник програмного забезпечення – цю інформацію також необхідно вказати в протоколі до наряду.

Після виявлення ІТ-власника програмного забезпечення відповідальний працівник управління інформаційної безпеки повідомляє ІТ-власника та адміністратора програмного забезпечення про встановлену інформацію, в свою чергу ІТ-власник та адміністратор програмного забезпечення зобов'язані зробити відповідні зміни в системі змін по відображенню зв'язку програмного забезпечення до відповідного сервера з заповненням в наряді у системі змін переліку мережевих портів (поле IP-порт), які відносяться до зазначеного ресурсу.

У випадку неможливості визначення ІТ-власника програмного забезпечення відповідальний працівник ІТ ініціює процес по виведенню з експлуатації цього програмного забезпечення з обов'язковим погодженням з керівниками всіх самостійних структурних підрозділів вертикалі інформаційних технологій.

Після завершення планового сканування відповідальний працівник управління інформаційної безпеки створює та відправляє звіт по вразливостям на всі задіяні структурні підрозділи вертикалі ІТ. В свою чергу працівник структурного підрозділу вертикалі ІТ після отримання звіту по вразливостям повинен перевірити наявність нових вразливостей на серверах/системах та проаналізувати їх:

1) у випадку, якщо вразливість відноситься до програмного забезпечення, то зміна створюється на усунення вразливості по програмному забезпеченню, а

наряди створюються в розрізі серверів, на яких була знайдена ця вразливість (на адміністратора програмного забезпечення);

2) у випадку, якщо вразливість відноситься до серверу (операційної системи), то зміна створюється на усунення вразливості по серверу, а наряди створюються в розрізі виявлених вразливостей або груп вразливостей (на адміністратора серверу);

3) до зміни по усуненню вразливостей останнім в ланцюгу після нарядів по усуненню вразливостей додається наряд на повторну перевірку наявності вразливостей відповідальним працівником ІТ.

Адміністратор системи погоджує зміни з ІТ-власником системи і на його вимогу – з іншими ІТ-власниками систем, які знаходяться у безпосередній залежності, та при необхідності виносить наряд за усуненням вразливостей в системі змін.

В рамках погодження зміни адміністратор сервера/системи також погоджує дату та час проведення робіт. Якщо сервер/система має «технологічне вікно», то бажаний час проведення робіт має бути в його рамках.

2.6 Визначення фальш-позитивності вразливостей

Адміністратор сервера або системи після підтвердження відповідальним працівником УІБ, може визначити вразливість як фальш-позитивну або таку, що не може бути усунена та змінює статус цієї вразливості в Tenable.

У випадку фальш-позитивної вразливості та вразливість яку неможливо усунути створюється правило в «Accept Risk» та змінюється її статус з вказанням причини, по який цю вразливість не можливо усунути.

Вразливості, які занесенні до «Accept Risk» періодично переглядаються відповідальним працівником управління інформаційної безпеки на можливість їх усунення. Відповідальний працівник управління інформаційної безпеки має право змінити статус вразливості.

В рамках процесу визначення фальш-позитивних вразливостей відбувається наступна процедура:

– адміністратор сервера/системи, відповідальний за усунення вразливостей, в робочому порядку звертається до відповідального працівника управління інформаційної безпеки та надає інформацію, що підтверджує статус конкретної фальш-позитивної вразливості;

– відповідальний працівник управління інформаційної безпеки, у випадку обґрунтованості та достатності отриманої інформації, інформує адміністратора сервера чи системи про підтвердження статусу вказаної вразливості як фальш-позитивної або ж здійснює запит додаткової інформації;

– в разі підтвердження статусу визначеної вразливості, відповідальний працівник управління інформаційної безпеки створює відповідне правило в «Accept Risk» та переводить вразливість в системі Tenable у відповідний стан.

2.7 Визначення систем які підлягають тестуванню на вразливості

Цей пункт описує умови проведення тестування серверів та систем на працездатність та усунення вразливостей після встановлення патчів та оновлення для усунення вразливостей. Під ці вимоги підпадають виключно системи, які знаходяться в продуктовому середовищі (в т.ч. в демілітаризованій зоні, або мають доступ до продуктивного середовища).

Процес усунення вразливості має бути протестований перед його безпосереднім застосуванням на продуктивній (робочій) системі у випадках:

– якщо в результаті усунення вразливостей системи змінюється версія програмного комплексу;

– якщо в результаті усунення вразливостей системи змінюється версія операційної системи;

– якщо усунення вразливості безпосередньо або опосередковано впливає на працездатність системи, або пов’язаних з нею систем;

– якщо ІТ-власник системи/серверу вважає, що така зміна потребує тестування;

– якщо підтримку системи здійснює зовнішня організація;

– якщо для усунення вразливості потрібна доробка програмного забезпечення.

В рамках проведення тестування та після отримання результатів про виявленні вразливості, адміністратор/ ІТ-власник системи/серверу, звертається до розробника (внутрішнього/зовнішнього) програмного забезпечення з метою отримати доопрацювання інформаційної системи та планує в разі необхідності бюджет.

Основні задачі проведення тестування усунення вразливостей:

– визначення впливу на працездатність системи та пов’язаних з нею систем;

– визначення етапів та необхідного часу для усунення вразливості.

Процес тестування усунення вразливостей оформляється в системі змін у вигляді нарядів до зміни по усунення вразливості. Результати проведеного тестування заповнюються в відповідні поля до зміни відповідальним за:

– прийняття рішення про необхідність тестування;

– ініціацію тестування.

Відповідальний по зміні ІТ-власник системи/серверу в разі прийняття рішення про необхідність тестування, є ініціатором тестування.

Наряди оформляються на проведення тестування працездатності системи або пов’язаних з нею систем в розрізі кожної системи на відповідного адміністратора системи.

Після проведеного тестування, та за умови його успішності така зміна, за необхідністю, виноситься в системі змін.

IT-власник системи/серверу (він же відповідальний по зміні) є відповідальним за:

− прийняття рішення про необхідність тестування;

− за ініціацію тестування;

− за проведення тестування та оформлення результатів.

2.8 Усунення вразливостей

Патчі та оновлення повинні бути перевірені перед розгортанням їх у продуктивному середовищі.

Виправлення та оновлення повинні надходити з внутрішнього корпоративного сервера служби оновлень, якщо це технічно можливо.

Якщо неможливо встановити оновлення або виправлення протягом визначеного періоду часу, виняток необхідно задокументувати.

Має бути введене поняття екстренного виправлення. Екстренне виправлення має відбутися, коли постачальник надає негайне (позачергове) виправлення/обхід, щоб пом’якшити критичні вразливості.

Максимальний період для пом’якшення вразливостей залежить від ступеня тяжкості уразливості:

− один місяць (30 днів) для critical-класифікованих вразливостей (після ідентифікації)

− два місяці (60 днів) для high-класифікованих вразливостей (після ідентифікації)

− шість місяців (180 днів) для medium-класифікованих вразливостей (після ідентифікації)

− дванадцять місяців (365 днів) для low-класифікованих вразливостей (після ідентифікації)

Якщо вразливість відноситься до сервера/системи, який/яку виведено з експлуатації, тоді адміністратор системи змінює статус вразливості в Tenable на «Resolved» та вписує в полі «Description», що сервер виведено з експлуатації.

Відповідальний працівник управління інформаційної безпеки вносить необхідні зміни в перелік серверів в Tenable.

Адміністратор сервера/системи в процесі усунення вразливості може долучати працівників інших структурних підрозділів в межах зон їх відповідальності шляхом створення наряду у зміні по усуненню вразливості в системі змін з обов'язковим зазначенням переліку робіт, які необхідно виконати.

Якщо вразливість систематично не усувається (більше 6 місяців) та її статус не був змінений на фальш-позитивну, відповідальний працівник управління інформаційної безпеки ініціює процес по створенню проблеми в системі змін на усунення вразливості та назначає відповідальним за закриття проблеми IT-власника системи/серверу.

2.9 Пост-перевірка усунення вразливостей

Пост-перевірка усунення вразливостей являє собою пересканування на вразливості після завершення усунення вразливостей відповідальними працівниками IT.

Після усунення вразливостей, відповідальний працівник IT робить наряд на перевірку вразливостей по хосту, за який він відповідальний. У разі, якщо вразливості відсутні, Ticket закривається відповідальним працівником IT.

2.10 Розподіл відповідальності між учасниками процесу

Схема розподілу відповідальності між задіяними структурними підрозділами в процесі керування вразливостями на системах організації зазначена на таблиці 2.2.

Таблиця 2.1 – Схема розподілу відповідальності між задіяними структурними підрозділами в процесу керування вразливостями

	Етап процесу керування вразливостями	**IT-власник системи/ серверу**	**Управління інформаційної безпеки**
	Планування та погодження сканування		
	Складання графіку сканування		x
	Погодження графіку сканування	x	x
	Проведення первинного та повторного сканування		
	Проведення сканування		x
	Формування звіту за результатами сканування		x
	Аналіз результатів та визначення відповідальних.		
	Визначення відповідальних на основі інформації з системи змін		x
	Визначення IT-власника систем в рамках процесу описаного цим Положенням	x	x
	Актуалізація інформації в системі змін по взаємозв’язках систем та їх адміністраторах	x	
	Створення змін/нарядів на усунення вразливостей	x	
	Визначення фальш-позитивності вразливостей	x	x
	Визначення необхідності проведення тестування	x	
	Усунення вразливостей	x	
	Встановлення зміни в продуктивному середовищі	x	
	Закриття нарядів в системі змін щодо усунення вразливостей	x	
	Створення проблем в системі змін для усунення вразливостей які систематично не усуваються		x
	Підготовка звітів встановленої форми для обробки та аналізу в рамках процедур, що зазначені вище		x
	Інформування керівництва організації про проведення сканування на вразливості та його результатах		x

До основних функцій по усуненню вразливостей адміністратора серверу/системи відносяться наступні:

− визначення складових компонентів програмного комплексу та занесення інформації в системі змін;

− визначення систем, які підлягають тестуванню;

− здійснення комунікацій з управлінням інформаційної безпеки щодо переведення виявлених вразливостей в статус фальш-позитив.

До основних функцій по усуненню вразливостей відповідального працівника управління інформаційної безпеки відносяться наступні:

− планування та погодження сканування інформаційної системи;

− проведення планових та позапланових сканувань інформаційної системи;

− підготовка звітів встановленої форми для обробки та аналізу в рамках процедур, описаних вище;

− актуалізація списку серверів організації в Tenable шляхом видалення серверів, що виведені з експлуатації або не існують;

− інформування керівництва про поточний стан інформаційної системи організації відносно наявності вразливостей;

− комунікація з адміністраторами серверів/систем стосовно призначення вразливості статусу фальш-позитив;

− періодичний перегляд списку вразливостей, які не можуть бути усунені без впливу на діючі бізнес-процеси організації;

− періодичне інформування керівництва організації стосовно результатів процесу керування вразливостями в організації.

2.11 Оцінка рівня критичності для виявлених вразливостей

Для організації процедур сканування на вразливості та керування вразливостями в організації загалом використовується спеціалізований

ліцензійний інструмент призначений для керування повним циклом управління вразливостями – Tenable [3].

В ході проведення сканування Tenable проводить ранжування ризиків, пов'язаних з виявленою вразливістю за наступною класифікацією (таблиця 2.2):

В рамках процесу усунення вразливостей, обов'язковому та першочерговому усуненню підлягають вразливості з рівнем критичний (critical), високий (high) та середній (medium) згідно з класифікацією Tenable [3], та сервера або системи що знаходяться в демілітаризованій зоні організації. Вразливості з рівнем низький (low) також потрібно усунути до наступного планового сканування.

Таблиця 2.2 – Класифікація ризиків, пов'язаних з виявленою вразливістю

Рівень критичності	**Опис дій**	**Можливі загрози**
Критичний (critical)	Зловмисник може взяти під повний контроль веб-додатки та веб-сервера, систему або компоненти системи, а також впровадити відомі вразливості операційної системи.	Експлуатація вразливості, яка призводить до компрометації кореневого рівня серверів або інфраструктурних пристроїв.
Високий (high)	Зловмисник може легко отримати контроль над хостом, що може призвести до компрометації безпеки всієї мережі.	Вразливості ІС, які дають можливість: – контролювати операційну систему; – виконати довільний програмний код, в результаті якого можлива крадіжка, видалення чи внесення змін до інформації, яка оброблюється

Продовження таблиці 2.2

		цим сервером; − вивід з ладу системи.
Середній (medium)	Зловмисник може мати можливість отримати доступ до специфічної інформації, яка зберігається на хості та включає налаштування безпеки	Вразливості, які можуть включати в себе: часткове розкриття змісту, доступ до визначених файлів на хості, перегляд директорій, часткове розкриття механізмів захисту, атаки відмови у обробці (DOS), неавторизоване використання сервісів.
Низький (low)	Зловмисник може зібрати інформацію про: − операційну платформу; − версію сервісів; − відкриті мережеві порти; − іншу технічну інформацію, яка може бути використана для несанкціонованого доступу до системи.	Прямих загроз ці вразливості не несуть однак вони можуть бути використані для пошуку інших більш критичних вразливостей.

Після виявлення вразливостей програмного забезпечення, що використовує в роботі вразливі сервери або системи, відповідальний працівник управління інформаційної безпеки повинен проінформувати IT-власника системи/серверу IT-власника програмного забезпечення про можливі наслідки експлуатації вразливого бізнес-процесу.

Висновки за розділом 2

Знання, які були отримані внаслідок ознайомлення з регулюючими (та) літературними джерелами, а також власні судження, яких було набуто в результаті проведених робіт з формалізації вимог до розробки методики сканування на вразливості, допомогли синтезувати багаточисельні поняття та тези в одне регламентоване положення, яке формулює процедуру та порядок сканування на вразливості в мережі підприємства.

У другому розділі були окреслені, головним чином, питання сфери дії, етапів процесу керування вразливостями, їх опису, порядку, відповідальності за проведення та результати сканування, особливості патч-менеджменту, та оцінці результатів проведеної процедури.

Створення такого ґрунту у вигляді повної методики сканування на вразливості дає можливість для практичної реалізації виявлення та усунення вразливостей у складних інформаційних системах, таких як підприємства, фінансові установи, тощо, що і стане головною метою в третьому розділі роботи «Розробка методики сканування на вразливості» на базі Tenable.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ

За ініціативою правління організації (фінансової установи) було прийнято рішення про впровадження методики сканування на вразливості. Завдання було отримано заздалегідь, в результаті чого було ініційоване питання актуалізації існуючих в підприємстві мережевих ресурсів та підмереж. На запит спеціаліста інформаційної безпеки підрозділом телекомунікаційних технологій був наданий перелік необхідних та наявних для сканування мереж, який наведено на рисунку 3.1 разом із узгодженими днями тижня, коли підготовка до сканування не є затратною, ресурсна система є міцною, а адміністратори серверів готови до ситуацій відмовою в обслуговуванні або з надмірним навантаженням.

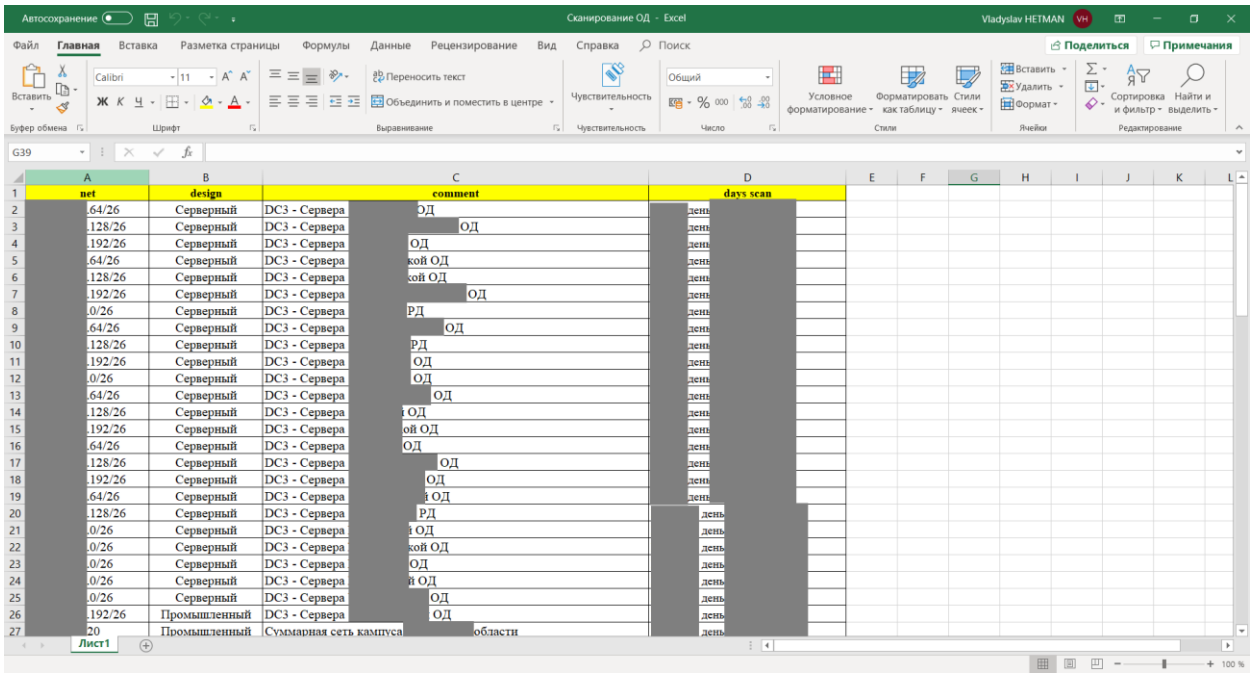

Рисунок 3.1 – Перелік необхідних та наявних для сканування мереж

Даний перелік був погоджений директорами структурних підрозділів рівня В-1 та начальником управління інформаційної безпеки засобами Atlassian Jira (зареєстрований системою змін), що вказано на рисунку 3.2.

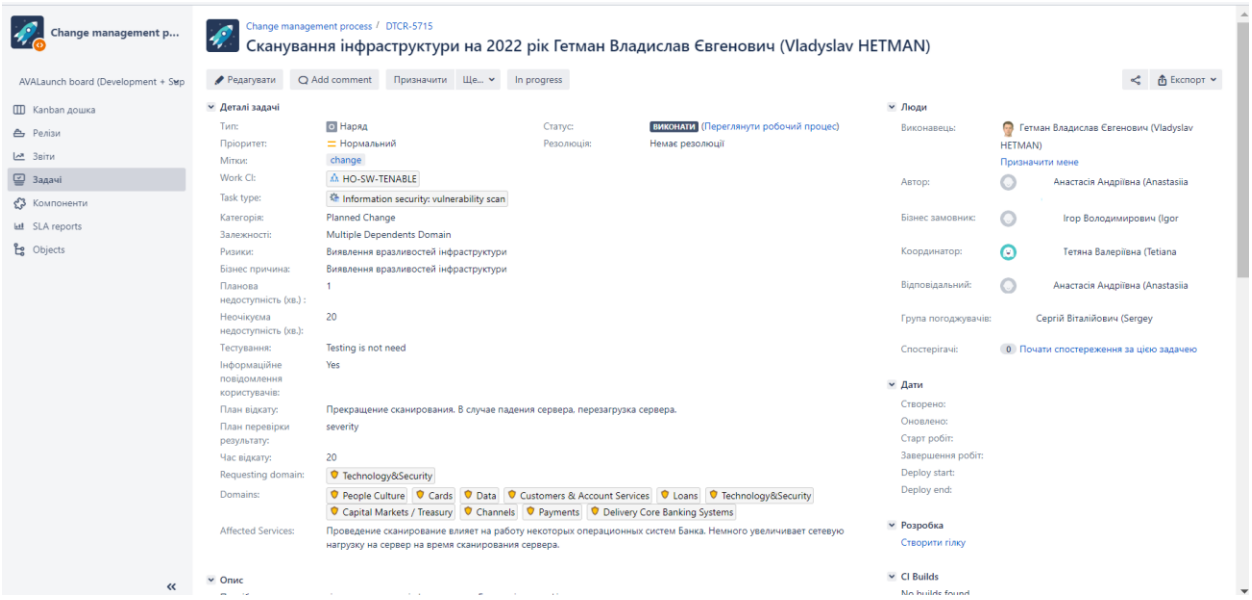

Рисунок 3.2 – Реєстрація погодження сканування інфраструктури системою змін

Окреслене узгодження було надано виходячи з розпорядження організації про сканування інфраструктури підприємства. На основі погоджених даних було створено графік сканування, інформацію з якого за травень наведено на рисунку 3.3.

Даний графік носить обов'язковий характер і є неодмінним до виконання (відхилення від даного графіку має бути врегульоване політикою безпеки підприємства – головними причинами можуть стати події, за яких належне використання emergency-плану підприємства).

Варто акцентувати увагу, що підприємство, інфраструктуру якого сканують на вразливості, є досить великим, що створює деякі проблеми з одночасним скануванням усіх підмереж. Для цього графік сканування було роздрібнено за сегментами та часом (днями, годинами).

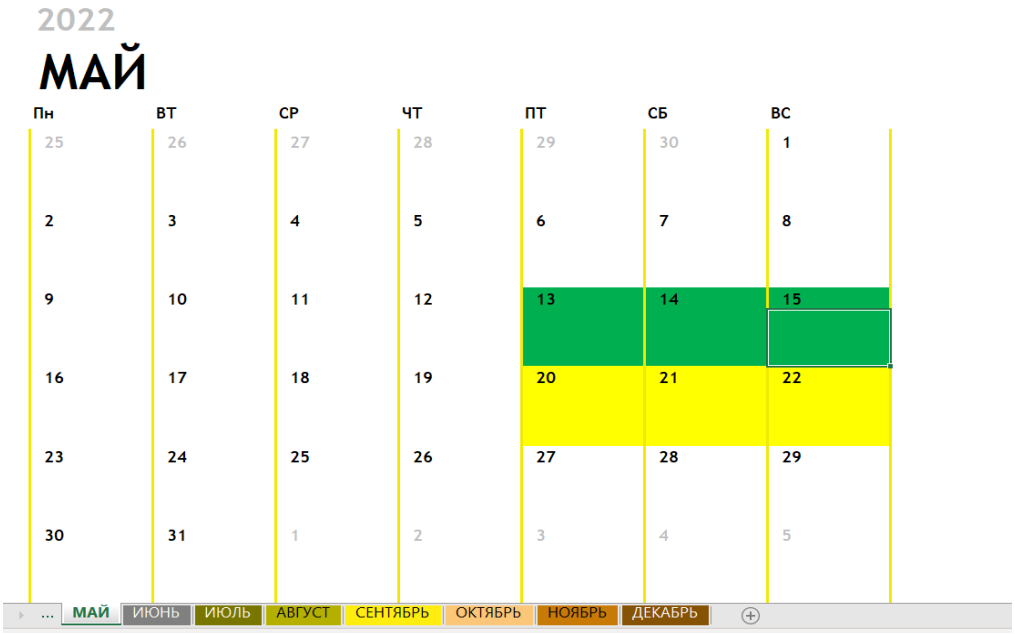

Рисунок 3.3 – Графік сканування за травень

Для занесення відповідних мереж до інструментарію Tenable.sc було створена відповідна політика для проведення сканування на діскаверінґ, внаслідок якої перелічені сервери були додані до системи вразливостей (vulnerability system). Як вказано у попередньо проведеній роботі «Вимоги щодо створення власної методики сканування на вразливості», дане сканування використовується саме перед проведенням сканування на вразливості для визначення активних та пасивних серверів в означеному діапазоні мережі [20].

Окрім того, на серверах створюється обліковий запис check для аутентифікації сканера, що також позначено в вимогах методики (див. рисунок 3.4).

Варто загострити увагу, що в разі відсутності облікового запису check на сервері, що підлягає скануванню, в результаті інформація з хоста не буде отримана, що ставить під сумнів всеосяжність методики. Тому варто заздалегідь зв’язатись комунікаційними каналами із бізнес-власниками ресурсів та проконтролювати створення та правильність супроводу облікового запису check.

Рисунок 3.4 – Створення облікового запису користувача check

Ознаки даного сканування наведені на наступному рисунку 3.5. Виходячи з налаштувань даного сканування, можна визначити, що даний вид сканування не виявляє та не ідентифікує вразливості на хостах. Discovering scan визначає операційні системи, які працюють у мережі, зіставляє ці системи з IP-адресами та перераховує відкриті порти та служби в цих системах. Сканування виявлення — це внутрішній сканер Metasploit.

Це сканування має такі властивості:

− постійна перевірка локальним хостом Nessus (включає локальний хост Nessus до сканування, це використовується, коли хост Nessus потрапляє в діапазон цільової мережі для сканування)

− використання швидкого виявлення мережі (якщо хост відповідає на запит ping, Nessus не намагається уникнути помилкових спрацьовувань, виконуючи додаткові тести, щоб переконатися, що відповідь не надходить від проксі-сервера або балансувальника навантаження. Ці перевірки можуть зайняти деякий час, особливо якщо віддалений хост має брандмауер).

− пінг хостів за допомогою:

✓ TCP

✓ ARP

✓ ICMP (2 повтори)

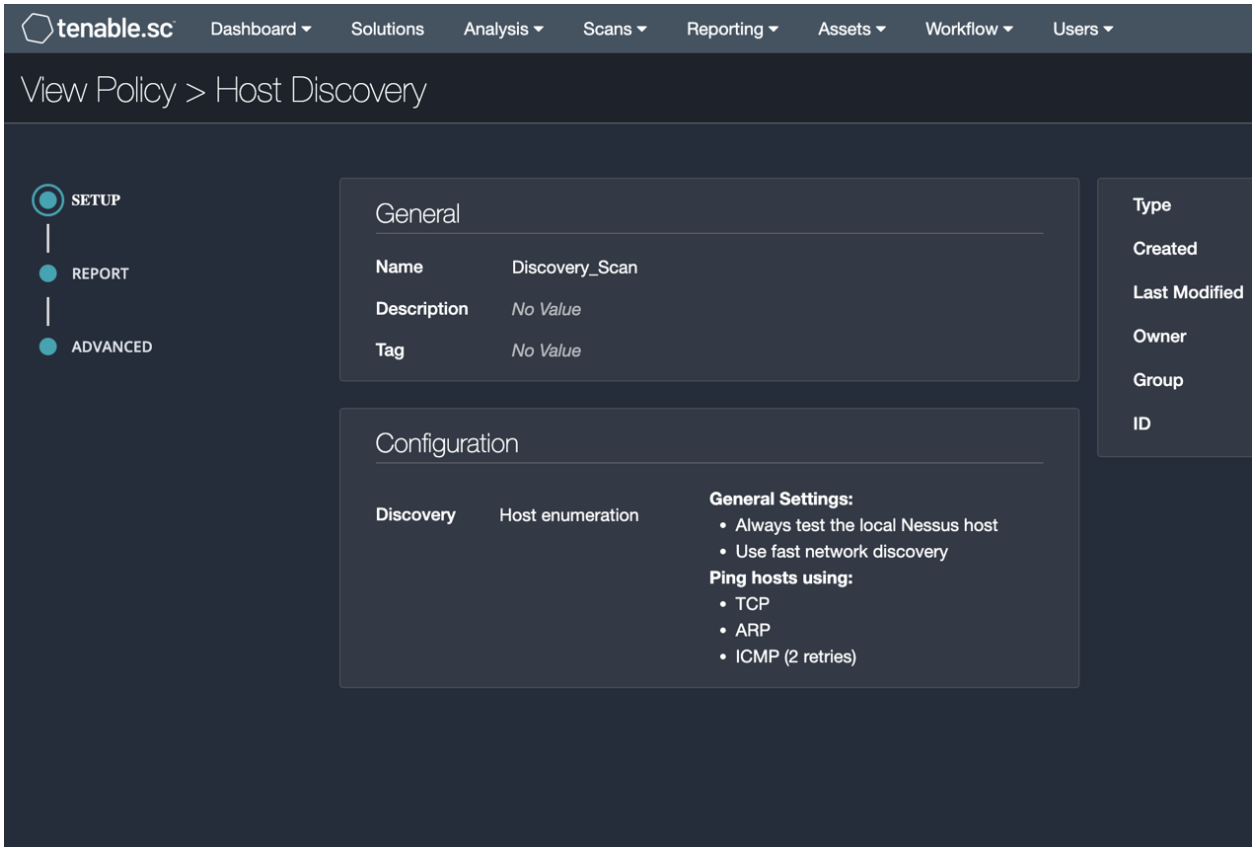

Рисунок 3.5 – Діскаверінґ наданого переліку підмереж.

Для проведення первинного сканування на вразливості була створена відповідна політика в інструментарії Tenable, інформація за якої наведена на рисунку 3.6. Головні ознаки даної політики були такими ж як і у discovering scan policy з єдиною відмінністю - ця політика застосовується для сканування безпосередньо на вразливості і видає іншу за характером інформацію, аніж минуле сканування.

Варто зазначити, що Tenable дозволяє залишати налаштування однаковими при різних типах політики, при цьому змінюючи об'єкти-результати сканування.

Так, це дозволяє бути впевненим, що усі хости, що пройшли сканування на «активність», пройшли й сканування на вразливості, проте варто зауважити, що це частковий випадок і створений навмисно для спрощення процедури сканування.

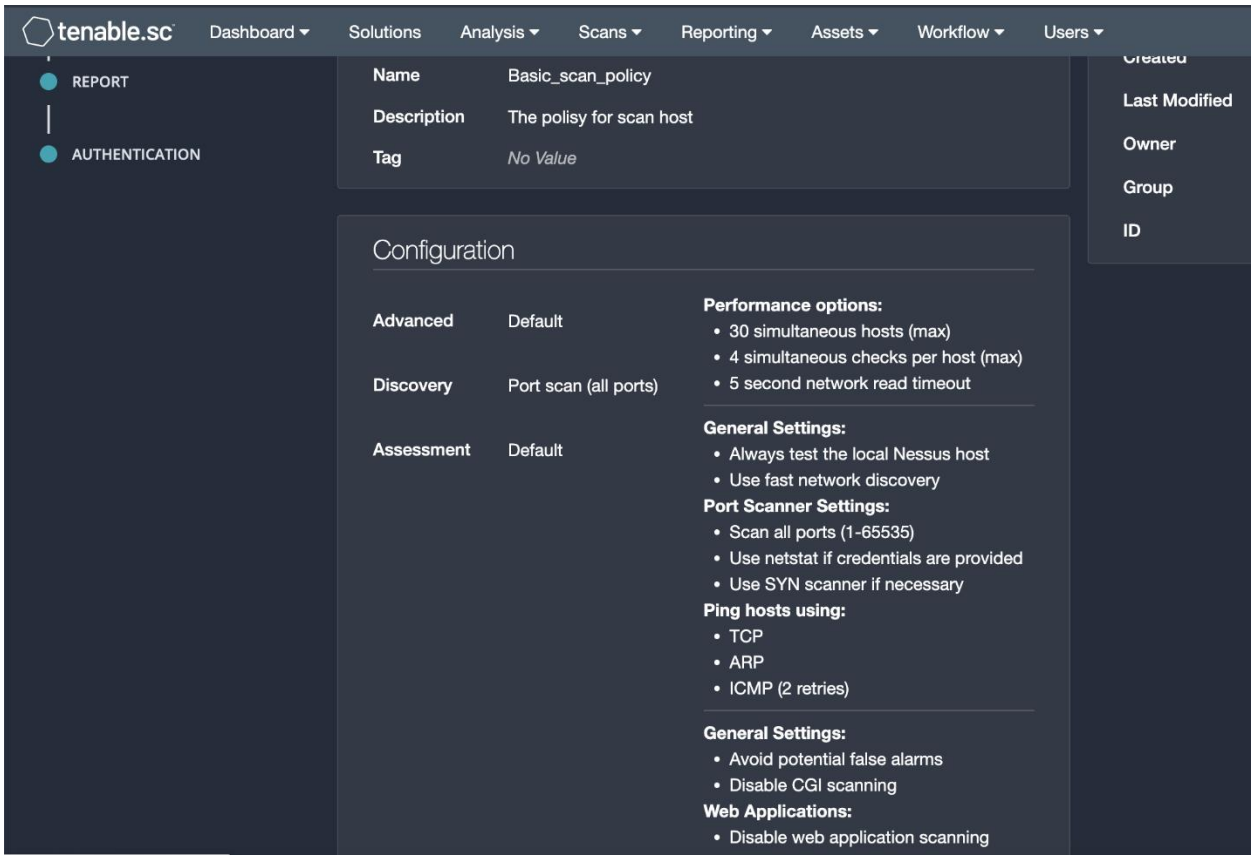

Рисунок 3.6 – Політика сканування на вразливості інструментом Tenable.sc

Згідно узгодженого графіку на заявлені дати були створені та налаштовані сканування пристроїв, що знаходяться у визначених зонах сегментованої мережі підприємства. Відповідно до кожного з сегментів було обрано час та добу, за якої мало проводитися сканування (дана процедура була узґоджена раніше, див. рисунки 3.2 – 3.3)

Ім’я та політика, про яку йшла мова вище і яка використовується, наглядно продемонстровані на рисунку 3.7.

Налаштуваннями для скану, головним чином, слугували ж звичайно перелік підмереж та час їх сканування. Окрім того, в самому скані було налаштовано автентифікацію на хостах, що дало можливість інформувати адміністратора системи про більший перелік вразливостей.

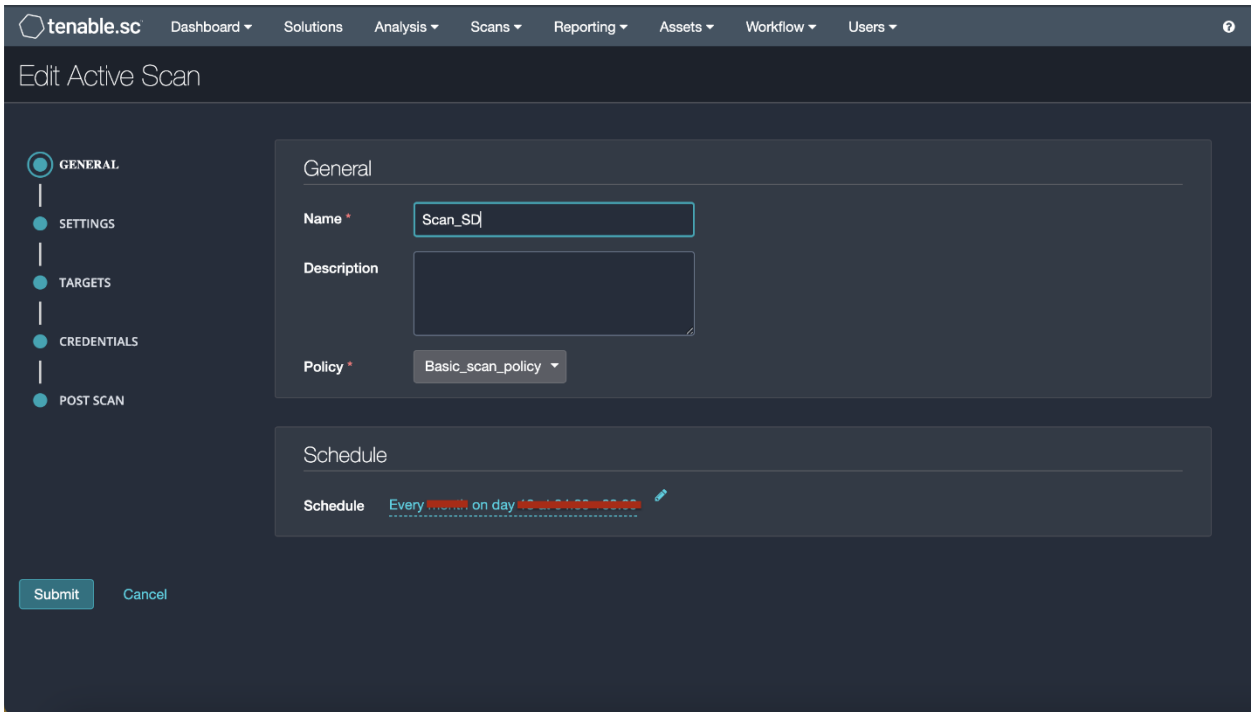

Рисунок 3.7 – Створене сканування відповідно до графіку

Згідно графіку, за два дні до проведення сканування був відправлений засобами електронної пошти підприємства лист-попередження про початок сканування на IT-власників системи/серверу. Скріншот такого попередження наведений на рисунку 3.8.

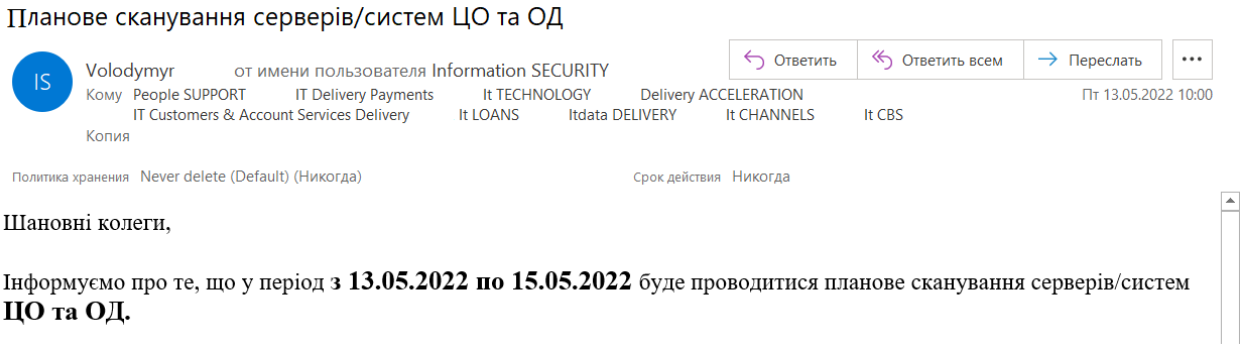

Рисунок 3.8 – Лист-попередження про початок сканування

В результаті проведеного сканування було виявлено вразливості на серверах, оцінка, опис та рішення для усунення яких визначені системою керування вразливостями Tenable.sc. Опцією для формалізації значень, отриманих в ході сканування, створений відповідний звіт про вразливості, який містить інформацію про:

- список усіх відкритих вразливостей;
- список усіх закритих вразливостей;
- середня кількість вразливостей на хості (critical, high, medium);
- інформацію про вразливість;
- інформацію про IP-адресу та мережевий порт, на яких виявлено вразливість.

Оформлення даного звіту можна побачити в додатку Б.

Списки усіх відкритих вразливостей та список усіх закритих вразливостей подаються у вигляді окремих таблиць до кожного з серверів, які мають наступний вигляд (рисунок 3.9 та рисунок 3.10):

Plugin	Plugin Name	Severity	Protocol	Port
142457	RHEL 7 : freetype (RHSA-2020:4907)	Medium	TCP	0
Plugin Output: **Plugin Output**: Remote package installed : freetype-2.8-14.el7 Should be : freetype-2.8-14.el7_9.1 NOTE: The vulnerability information above was derived by checking the package versions of the affected packages from this advisory. This scan would normally rely on checking for the presence of specific installed Red Hat repositories, but either no repositories were found in the repository list, the file was empty or missing, or the scan account lacked permissions to access it. Please ensure that the repository file is populated and the scanning account has permissions to examine the /etc/yum.repos.d/redhat.repo file.				
Synopsis: The remote Red Hat host is missing a security update.				
Description: The remote Redhat Enterprise Linux 7 host has packages installed that are affected by a vulnerability as referenced in the RHSA-2020:4907 advisory. - freetype: Heap-based buffer overflow due to integer truncation in Load_SBit_Png (CVE-2020-15999) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.				
Solution: Update the affected freetype, freetype-demos and / or freetype-devel packages.				
See Also: https://cwe.mitre.org/data/definitions/122.html https://cwe.mitre.org/data/definitions/190.html https://access.redhat.com/security/cve/CVE-2020-15999 https://access.redhat.com/errata/RHSA-2020:4907 https://bugzilla.redhat.com/1890210				
CPE: cpe:/o:redhat:enterprise_linux:7 p-cpe:/a:redhat:enterprise_linux:freetype p-cpe:/a:redhat:enterprise_linux:freetype-demos p-cpe:/a:redhat:enterprise_linux:freetype-devel				
First Discovered: Feb 14, 2021 09:53:17 UTC				
Last Observed: Nov 21, 2021 11:23:15 UTC				
Version: 1.10				

Рисунок 3.9 – Список відкритої вразливості на окремому сервері.

Внаслідок патч-менеджменту, який проводиться адміністраторами серверів після отримання результатів сканування, проводиться або усунення вразливостей або віднесення їх до переліку допустимих.

На рисунку 3.10 наведена вразливість, яка була помилково визначена внаслідок неправильної інсталяції Windows Server, і яку слід віднести до переліку допустимих.

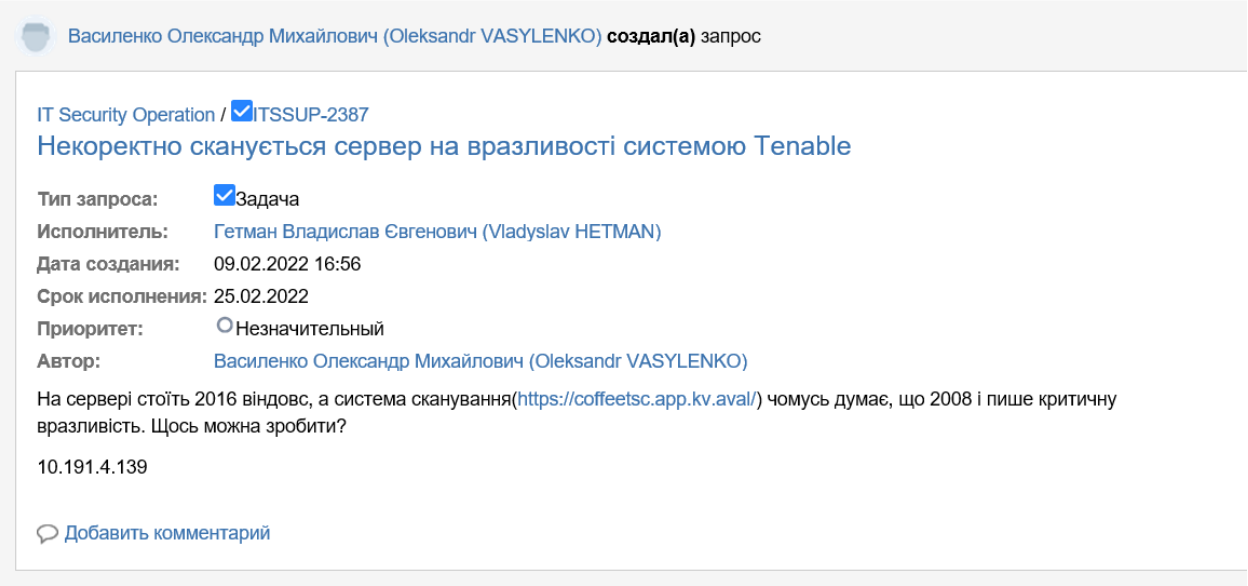

Рисунок 3.10 – Визначена вразливість, занесена в Accept Risk

Для перевірки на усунення тієї чи іншої вразливості кожен користувач / адміністратор серверу/IT-системи має увійти у свій обліковий запис до Tenable.sc та просканувати той чи інший сервер на певну вразливість. У разі, якщо вразливість усунена в опції Analysis – Vulnerabilities на головній панелі в Tenable при уточненні за фільтром IP та Plugin ID вразливість виводитися не буде.

Висновки за розділом 3

Дослідження створеної методики в підприємстві було успішно завершено.

Практична реалізація сканування на вразливості в широкому сегменті мереж надала можливість усій ІТ-команді підприємства виконати завдання щодо підвищення рівня захищеності власних ресурсів та ІТ-систем.

Протягом роботи було проведено:

− формалізацію переліку необхідних та наявних для сканування мереж на підприємстві;

− регламентація процедури погодження сканування інфраструктури в системі змін Jira;

− врегулювання процесу аутентифікації обліковим записом на хостах, що скануються;

− діскаверинг мереж, що знаходяться на супроводі підприємства (фінансової установи);

− створення власних політик безпеки, що персоніфікують та індивідуалізують (головним чином, за рахунок спрощеності) процес сканування;

− сканування на вразливості згідно власної методики;

− патч-менеджмент, занесення певних вразливостей до «Accept Risk»;

− створення звіту про отримані результати на керівництво підприємства.

Таким чином, головне завдання третього розділу, а саме реалізація власної створеної методики та перевірка її обсягу та повноти на практиці виконано.

ВИСНОВКИ

Загалом, хід роботи з розробки методики був сприятливим для отримання якісного результату.

Важливо зазначити, що без актуалізації знань наукової, технологічної (корпоративної) та державно-нормативної літератури з обраної тематики досягнути поставленої мети було б неможливо, хоча й означені в роботі проблеми дійсно мають місце. Можливість синтезувати отримані знання в критерії для вимог створення власної методики з проведення сканування на вразливості, а після і в саму методику, стала рушійною силою для отримання практичних результатів, як перевірки роботи цієї самої методики.

Аналіз функціоналу обраного інструменту для перевірки на відповідність заданим критеріям (можливість проведення сканування за заданими критеріями, аналіз функціоналу) був проведений раніше [3], хоча варто акцентувати, що на виході практичної реалізації ми отримуємо досить індивідуалізовану методику, яка підходить для сканування майже будь-якого підприємства, що є позитивним фактором для оцінки роботи – в такому випадку, дана методика дійсно стала в нагоді під випробувану на вразливості систему, адже має свої об’єктивні переваги в своєму використанні, засновані на її адекватності та відповідності тим факторам, яких вона покликана підтримувати.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. В. Н. Ясєнєв. Конспект лекцій з інформаційної безпеки 254 с. / В. Н. Ясєнев – Нижній Новгород, 2017 - [Електронний ресурс]. Режим доступу: http://www.iee.unn.ru/wp-content/uploads/sites/9/2017/02/konspekt-lektsij-po-IB.pdf . Дата звернення: 19.05.2022

2. Цикл лекцій з дисципліни "Автоматизація процесів управління інформаційною безпекою" / Рахметов Р. - для ТОВ «Інтелектуальна безпека» (Security Vision), 2020 – [Електронний ресурс]. Режим доступу : https://www.securityvision.ru/blog/protsessy-upravleniya-ib-konspekt-lektsii/ Дата звернення: 19.05.2022

3. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник /А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с. Режим доступу: https://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1I%D0%91%D0%9D%D0%98%D0%9A%20%D0%9E%D0%A3I%D0%91%20.pdf . Дата звернення: 19.05.2022

4. Поняття, сутність, значення захисту інформації. Режим доступу: www.infobezpeka.com/publications/?id=102 . Дата звернення: 19.05.2022

5. Гончар С. Ф. Аналіз ймовірності реалізації загроз захисту інформації вавтоматизованих системах управління технологічним процесом / С. Ф. Гончар // Захистінформації. – 2014. – № 1 (16). – С. 40–46.

6. Загальна система оцінки вразливостей. Режим доступу: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BE%D1%86%D1%96%D0%BD%D0%BA%D0%B8_%D0%B2%D1%80%D0%B0%D0%B7%D0%BB%D0%B8%D0%B2%D0%BE%D1%81%D1%82%D0%B5%D0%B9 . Дата звернення: 19.05.2022.

7. Про затвердження Положення про організацію кіберзахисту в банківській системі України: постанова Правління Національного банку України від 04.11.2021 №447/2021

8. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Наказ Адміністрації Держспецзв'язку від 02.12.14 р. № 660. Офіційний вісник України. 2015. № 12. Ст. 323

9. Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті: Наказ Адміністрації Держспецзв'язку від 15.01.16 р. № 20. Офіційний вісник України. 2016. № 17. Ст. 695.

10. Про захист інформації в інформаційно-телекомунікаційних системах від 05.07.1994 № 80/94-ВР

11. Закон України Про телекомунікації від 18.11.2003 № 1280-IV

12. Закон України Про Державну службу спеціального зв'язку та захисту інформації України від 23.02.2006 № 3475-IV

13. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. Відомості Верховної Ради України. 2017. № 45. Ст. 403. 6

14. ISO/IEC 29147:2018 – Vulnerability Disclosure in information technology – ANSI BLOG. Режим доступу: https://blog.ansi.org/2018/11/iso-iec-29147-2018-vulnerability-disclosure/#gref. Дата звернення: 19.05.2022.

15. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT)

16. ISO/IEC 30111:2019. Information technology — Security techniques — Vulnerability handling processes

17. NIST SP 800-40 v.2.0 «Creating a Patch and Vulnerability Management Program», November 2005. Режим доступу: https://csrc.nist.rip/library/alt-SP800-40v2.pdf . Дата звернення: 19.05.2022.

18. Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems

19. Порівняльний аналіз сканерів для вразливостей / Гетман В. Є. – наукова теза, 2021 3

20. «Вимоги щодо створення власної методики сканування на вразливості», переддипломна практика – Гетман В. Є., 15 с., 2022 р.

ДОДАТОК А

Comparative analysis of well-known security scanners (with Nessus)

Vladyslav Hetman[a], Serhii Toliupa[b]

[ab]*Faculty of Information Technology, Taras Shevchenko National University of Kyiv, 60 Volodymyrska St., Kyiv, 01601, Ukraine*

Abstract

For checking the security of information resources, specialists increasingly resort to tools such as a security scanner or even a full-fledged vulnerability management platform, which includes a security scanner, and integration with infrastructure, and integration with other systems. This article includes a list of such tools and their institutional comparison with each other (according to the main factors on vulnerability).

Keywords

Security, scanners, vulnerability, Nessus.

1. Introduction

The presence of vulnerabilities in information systems, infrastructure nodes or components of the complex is not disputed as a big problem for information security systems. Of course, you can manually search for gaps, but it will be an extremely labor-intensive process that will take a lot of time with a high probability of missing something.

The global vulnerability market itself is already quite scanned. These are system systems tools for managing vulnerabilities. Vulnerability tracing projects contain, in which representatives of various structures participate. Also, scanners perform integration with risk management systems or patch management, platforms for manufacturers of incidents, secure, without using the already mentioned SIEM.

An urgent task of choosing a solution for managing vulnerabilities. This work contains statistics of testing various solutions and a conclusion why one or another scanner is suitable for its purposes.

2. Base for statistics

The results of the comparison of network security scanners were obtained through penetration tests with nodes at the network perimeter. At the same time, the following were evaluated [1]:

- number of vulnerabilities found;
- false positives;
- false negatives;
- reasons for missing;
- completeness of the database of checks (in the context of this task);
- quality of inventory mechanisms and software version detection;
- the accuracy of the scanner (in the context of this task).

The listed criteria together characterize the "suitability" of the scanner for solving the task assigned to it, in this case it is the automation of routine actions in the process of monitoring the security of the network perimeter.

The scanners presented in Table 1 were selected to participate in the tests [2].

Table 1
Selected scanners

Name	Version	Link
Nessus	3.2.1	http://www.nessus.org/download
Max Patrol	8.0	http://www.ptsecurity.ru/maxpatrol.asp
Internet Scanner	7.2.58	http://www-935.ibm.com/services/us/index.wss/offering/iss/a1027208
Retina Network Security Scanner	5.10.2.1389	http://www.eeye.com/html/products/retina/index.html
Shadow Security Scanner	7.141	http://www.safety-lab.com/en/products/securityscanner.htm
NetClarity Auditor	6.1	http://netclarity.com/branch-nacwall.html

Three PCs were selected as a network node within the same network and similar parameters.

2.1 Second level heading

The first place according to all the criteria of this comparison (table 2) goes to the MaxPatrol scanner, the second place is taken by the Nessus scanner, the results of the other scanners are significantly lower.

Table 2
The results of the tests

Index	MaxPatrol	InternetScanner	Nessus Tenable	Shadow	NetClarity Auditor	Retina
Vulnerabilities found, total	163	51	81	69	57	38
False positives	8	3	7	36	14	4
Found correctly (out of 225 possible)	155	48	74	33	43	34
False negatives	70	177	151	192	182	191
Of these, due to the absence in the database	63	170	59	150	179	170
Of these, caused by the need for authentication	0	6	36	0	0	16

In fact, there is nothing unexpected or surprising in the result obtained. It is no secret that the MaxPatrol and Nessus scanners are popular among security professionals [2].

Let's try to analyze the reasons for the clear leadership of MaxPatrol and Nessus Scanners, as well as the reasons for the "loss" of other scanners.

First of all, it is a high-quality identification of services and applications. Inference-based checks are highly dependent on the accuracy of the information collection [3].

The second reason for their success is the completeness of the base and its adequacy to the task at hand and in general to "today". According to the results, it is noticeable that the base of checks in MaxPatrol and Nessus has been significantly expanded and detailed, it is "put in order", while the obvious "bias" towards web applications is compensated by the expansion of checks in other areas.

The third reason is a qualitative analysis of application versions, taking into account operating systems, distributions and various "branches". You can also add and use different sources (vulnerability databases, notifications and "vendor" bulletins).

Finally, we can add that MaxPatrol and Nessus have a very convenient and logical interface that reflects the main stages of the work of network security scanners.

3. Disadvantages of Nessus

The main reason for the lag in Nessus is missing vulnerabilities, but not because of the lack of checks in the database, as in most other scanners, but because of the implementation specifics. Firstly (and this is the reason for a significant part of the omissions), there is a tendency in the Nessus scanner towards "local" or system checks, which involve connecting with an account [4]. Secondly, the Nessus scanner took into account fewer (in comparison with MaxPatrol) sources of information about vulnerabilities [5].

4. Conclusions

The work doesn't show that Tenable is necessarily much better than the rest of the products. It's just that in this context, this solution coped better than the rest.

Tenable's products offer a wide range of capabilities to identify and effectively address many security threats in real time. Companies that are considering using vulnerability scanners in their infrastructure should decide on the required capabilities of the product (whether flexible configuration of the reporting subsystem is required or basic enough, whether continuous monitoring of the network or determination of behavior anomalies is needed, etc.), as well as the types and amount of information assets in the organization. Despite the large number of possibilities for security analysis, all the solutions presented lack built-in support for domestic standards, because the company recently entered the domestic market, which is partially offset by the ability to create its own reports. For the same reasons, the products have not yet been certified by the State Communications Service of Ukraine. Nevertheless, the solutions allow you to fully protect the organization from vulnerabilities, erroneous settings and malware, which positively affects the overall security of the infrastructure and allows you to assess and mitigate information security risks [6].

5. References

Vulnerability scanning and secure development. URL: https://habr.com/ru/post/444534/

Vulnerability scanners - an overview of the global and Russian markets. URL: https://www.anti-malware.ru/analytics/Market_Analysis/Vulnerability-scanners-global-and-Russian-markets

Vulnerability scanners. Comparison of network security scanners Programs for scanning networks for vulnerabilities. URL: https://beasthackerz.ru/wi-fi-ethernet/skanery-uyazvimostei-sravnenie-setevyh-skanerov-bezopasnosti-programmy-dlya.html

Programs for scanning the network for vulnerabilities. Best Pen Tester Tools: Security Scanners. How a LAN Network Scanner Keeps It Secure. URL: https://bookfix.ru/programmy-dlya-skanirovaniya-seti-na-uyazvimosti-luchshie/

Overview of Tenable products for analyzing the security of corporate infrastructure, 23.11.17. URL: https://www.anti-malware.ru/reviews/tenable-analysis-security-corporate-infrastructure.

Overview and comparison of vulnerability scanners. Best Vulnerability Scanners for Linux Check Local Network for Vulnerabilities. URL: https://olacom.ru/security/obzor-i-sravnenie-skanerov-uyazvimostei-luchshie-skanery-uyazvimostei-dlya-linux/

ДОДАТОК Б

Департаменту ІТ розвитку технологій
підприємства (фінансової установи) N
п. Іванову І. І.

Вих.66-0-0-00/
Від --.--.2022.

Службова записка

Департаментом інформаційної безпеки в рамках процесу управління вразливостями підприємства N в період з 13.05.2022 по 15.05.2022 було проведено сканування серверів Центрального офісу підприємства з метою виявлення вразливостей.

В ході сканування було перевірено 202 мережі серверного та промислового сегменту, з них, було просканована 7654 IP адрес, що на 1585 стало більше від попереднього сканування. В результаті перевірки встановлено, що загальний стан інформаційних ресурсів ЦО Банку за кількістю вразливостей **покращився** у порівнянні за квітень місяць 2022 року, відповідно до наведеної таблиці:

Критичність	**Вразливості**		**Динаміка**
	Травень 2022	**Квітень 2022**	
Critical	6687	7913	**-1226**
High	19640	19338	**+302**
Medium	12099	12099	**+0**

Проведено аналіз отриманих результатів сканування за травень 2022 року. За результатами аналізу створено рейтинги найбільш вразливих ІТ-систем та серверів підприємства, які наведені в таблицях нижче.

Рейтинг найбільш вразливих ІТ- систем підприємства:

№	Система	ІТ власник системи	Критичність		
			С	Н	М
1	Поштовий сервер post.server.ua	СИДОРОВ В. В.	25	39	81
2	Поштовий сервер server.post.ua	СИДОРОВ В. В.	25	39	81
3	Тестова база даних з реальними даними	ПЕТРОВ П. П.	23	27	73
4	Мережа серверів Citrix	КУЛАКОВ К. К.	18	40	20
5	Менеджер транзакций Tuxedo	НОГОТКОВ Н.Н.	15	3	35

Рейтинг найбільш вразливих серверів підприємства:

	Сервер (DNS – ім’я)	Критичність			Адміністратор	Призначення
		С	Н	М		
	. . .122 post.server.ua	25	39	81	СИДОРОВ В. В.	Поштовий сервер
	. . .121 server.post.ua	25	39	81	СИДОРОВ В. В.	Поштовий сервер
	. . .136 base.test.ua	23	27	73	ПЕТРОВ П.П.	Тестування додатків
	. . .1 citrix1.prod.seg	13	27	13	ШЕВЧЕНКО Т. Т.	Підключення до віртуальних станцій
	. . .13 tuxedo.mgm.ua	15	3	35	НОГОТКОВ Н. Н.	менеджер транзакций Tuxedo

Звертаю Вашу увагу, що під час аналізу отриманих даних було виявлено, що переважна більшість вразливостей пов’язана з відсутністю встановлених оновлень на UNIX-системах, Oracle та протоколу SSL/TLS. Крім того, частина виявлених вразливостей свідчить про порушення вимог інформаційної безпеки підприємства та стандартів щодо налаштування програмного забезпечення.

В зв’язку з цим, прошу Вас організувати заходи щодо:

– налагодження процесу своєчасного встановлення оновлень на операційні системи та програмне забезпечення;

– перевірки та проведення налаштувань програмного забезпечення до вимог стандартів безпеки та нормативних документів з інформаційної безпеки підприємства.

Прошу Вас повідомити Департамент інформаційної безпеки про заплановані заходи щодо усунення виявлених вразливостей до 29.05.2022р.

Директор з інформаційної безпеки КОНЮХОВ О. О.

«__» _____ 2022 року