НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2022 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: Побудова ефективного процесу управління вразливостями_____

_____

_____

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи __ФБ-82__
(шифр групи)

_____Кузнєцов Ілля Сергійович_____ _____
(прізвище, ім'я, по батькові) (підпис)

Керівник Ткач Володимир Миколайович, к.т.н., доцент___ _____
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2022 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
«___»_____2022 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

_____Кузнєцову Іллі Сергійовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи «Побудова ефективного процесу управління вразливостями»,

керівник роботи доцент кафедри інформаційної безпеки Ткач В.М., _____
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від « » _____ 2022 р. №

2. Термін подання здобувачем вищої освіти роботи 14 червня 2022 р.

3. Вихідні дані до роботи: підхід до побудови ефективного процесу управління вразливостями

4. Зміст роботи: огляд основних відомостей про базовий процес управління вразливостями, аналіз зв'язку процесу управління вразливостями з процесом управління ризиками, огляд принципів роботи сканерів вразливостей, інтеграція оцінки ризиків в процес управління вразливостями, огляд методів боротьби з вразливостями, введення та аналіз метрик ефективності, розробка підходу до

побудови ефективного процесу управління вразливостями, оцінка ефективності розробленого підходу до побудови процесу управління вразливостями, демонстрація побудови ефективного процесу управління вразливостями

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) Побудова ефективного процесу управління вразливостями – презентація

6. Дата видачі завдання 1 січня 2022 року

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Отримання завдання	01.01.2022	виконано
2	Огляд та опрацювання інформаційних джерел	07.01.2022 – 21.01.2022	виконано
3	Аналіз базового процесу управління вразливостями та risk-based підходу	22.01.2022 – 05.02.2022	виконано
4	Аналіз зв'язку процесу управління вразливостями з процесом управління ризиками	05.02.2022 – 19.02.2022	виконано
5	Інтеграція оцінки ризиків в процес управління вразливостями	19.02.2022 – 05.03.2022	виконано
6	Введення метрик ефективності	05.03.2022 – 15.03.2022	виконано
7	Розробка підходу до побудови ефективного процесу управління вразливостями	15.03.2022 – 05.04.2022	виконано
8	Оцінка ефективності процесу управління вразливостями	05.04.2022 – 15.04.2022	виконано
9	Практична побудова ефективного процесу управління вразливостями на основі розробленого підходу	15.04.2022 – 05.05.2022	виконано

Здобувач вищої освіти _____ Ілля КУЗНЄЦОВ

(підпис) (**Власне ім'я, ПРІЗВИЩЕ**)

Керівник роботи _____ Володимир ТКАЧ

(підпис) (**Власне ім'я, ПРІЗВИЩЕ**)

РЕФЕРАТ

Обсяг роботи 68 сторінки, 25 ілюстрацій, 5 таблиць, 2 графіка, 2 додатка, 19 джерел літератури. В роботі досліджено ефективну побудову процесу управління вразливостями. В роботі оглянуто основні відомості про базовий процес управління вразливостями, risk-based підхід до процесу управління вразливостями, сканери вразливостей, принципи роботи сканерів вразливостей, проведено аналіз методів оцінки ризиків та методів боротьби з вразливостями, впроваджено метрики ефективності та розроблено підхід до побудови ефективного процесу управління вразливостями.

Метою дипломної роботи є побудова ефективного процесу управління вразливостями.

Об’єктом дослідження дипломної роботи є процес управління вразливостями.

Предметом дослідження дипломної роботи є розробка підходу до побудови ефективного та повноцінного процесу управління вразливостями з урахуванням введених метрик ефективності.

Ключові слова: вразливість, ризик, процес управління вразливостями, оцінка ризику, метрики, сканування, інвентаризація.

ABSTRACT

The volume of work is 68 pages, 25 illustrations, 5 tables, 2 graphics, 2 appendices, 19 sources of literature. The paper investigates the effective construction of the vulnerability management process. The paper reviews basic information about the basic process of vulnerability management, risk-based approach to vulnerability management, vulnerability scanners, principles of vulnerability scanners, analysis of risk assessment methods and vulnerability management methods, efficiency metrics and approach for building an effective vulnerability management process.

The aim of the thesis is to build an effective process of vulnerability management.

The object of research of the thesis is the process of vulnerability management.

The subject of the thesis is the development of a approach for building an effective and comprehensive process of vulnerability management, taking into account the introduced efficiency metrics.

Key words: vulnerability, risk, vulnerability management process, risk assessment, metrics, scanning, inventory.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Вразливість — нездатність системи протистояти реалізації певної загрози або сукупності загроз. Тобто, це певні недоліки в комп'ютерній системі, завдяки яким можна навмисно порушити її цілісність і викликати неправильну роботу.

Атака — спроба реалізації загрози. Тобто, це дії кібер-зловмисників (хакерів) або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу.

Загроза — будь-які обставини або події, що виникають у зовнішньому середовищі, які можуть бути причиною порушення політики безпеки інформації і (або) нанесення збитків автоматизованій системі.

Ризик — це операційний ризик, який полягає в отриманні прямих чи побічних збитків економічними суб'єктами внаслідок їх функціонування у кіберпросторі.

CVSS — це безкоштовний і відкритий галузевий стандарт для оцінки серйозності вразливостей безпеки комп’ютерної системи.

Актив — ресурси, контрольовані підприємством у результаті минулих подій, використання яких, як очікується, приведе до отримання економічних вигод у майбутньому.

SSH — мережевий протокол рівня застосунків, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань (наприклад, для передачі файлів).

RDP — протокол прикладного рівня, що використовується для забезпечення віддаленої роботи користувача із сервером, на котрому запущений сервіс термінальних з'єднань.

IDS — програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет.

IPS — система запобігання вторгнень в комп'ютерну систему або мережу, різновид системи виявлення вторгнень.

Qualys Cloud Platform – хмарна платформа, що надає безперервну, постійну оцінку цільової глобальної системи IT, безпеки та відповідності, видимістю всіх IT-активів, де б вони не знаходилися. Складається з більше ніж 20 модулів, кожний модуль виконує свої функції. Усі модулі поширюються за моделю SaaS.

Qualys Vulnerability Management (VM) – це один з модулів Qualys Cloud Platform, який дає миттєву глобальну видимість того, де ваші IT-системи можуть бути вразливими до останніх інтернет-загроз і як захиститися від них. Допомагає постійно захищати свою IT-інфраструктуру та відповідати внутрішнім політикам і зовнішнім правилам.

Гіпервізор VMware ESXi – найпопулярніший, функціональний і унікальний у своєму сегменті програмний продукт для серверної віртуалізації. Основна функціональна можливість, яку реалізує гіпервізор ESXi, це створення віртуальних машин на фізичному сервері. У якості гостьових операційних систем підтримуються всі основні версії, які використовуються в корпоративному секторі.

Metasploitable VM – це навмисно вразлива віртуальна машина Linux. Цю віртуальну машину можна використовувати для проведення навчання з кібербезпеки, тестування інструментів безпеки та застосування поширених методів тестування на проникнення.

Qualys Scanner Appliance – це віртуальна машина, яка виконує функцію сканера вразливостей. З допомогою Qualys Scanner Appliance можна просканувати на вразливості внутрішню мережу компанії.

ВСТУП

У світі не існує повністю безпечних інформаційних систем. Усі інформаційні системи за замовчування вразливі і стають все більш вразливішими з кожнем днем. Ідеально написаного та налаштованого програмного забезпечення не існує. Вразливості є невід'ємною частиною програмного забезпечення, і багато вразливостей мають жахливі наслідки для безпеки інформаційної системи. Боротьба з вищезазначеними вразливостями є постійною проблемою інформаційної безпеки.

Впровадження процеса управління вразливостями є першим кроком для забезпечення необхідного, базового рівня безпеки інформаційної системи, який може служити надійною основою для подальшого розширення та вдосконалення інформаційної системи.

Вразливості інформаційних систем впливають на всю IT-інфраструктуру компанії на всіх рівнях, тому процес керування вразливостями повинен повністю покривати всі аспекти IT-безпеки.

Наприклад, безпека кінцевих точок покладається на те, що робочі станції та сервери мають найновіші версії програмного забезпечення, щоб мінімізувати поверхню атаки. Проте завжди будуть існувати вразливості "нульового дня", які дозволяють зловмисникам успішно атакувати і обходити механізми захисту і скомроментовувати інформаційну систему навіть якщо на ній встановлено програмне забезбечення найновіших версій.

Механізми безпеки мережі роблять усе можливе, щоб забезпечити проходження лише легітимного трафіку між внутрішніми сегментами мережі компанії в мережу Інтернет та навпаки. Але, якщо операційні системи кінцевих точок містять відомі вразливості, або в мережі встановлені мережеві пристрої з вразливим програмним забезпеченням, то тоді вірогідність того, що компанію

успішно атакують зловмисники, значно зростає. Навіть на перший погляд, легітимний трафік може таким і не бути.

Отож можна остаточно зробити висновок, що повністю безпечних інформаційних систем не існує, а потенціальних векторів зловмисних атак - нескінченна кількість. Саме для цього необхідно впровадити та правильно налаштувати процес управління вразливостями. Якщо правильно налаштувати процес управління вразливостями, то зловмисник не зможе легко скомпроментувати систему безпеки компанії, а вірогідність успішної атаки буде прагнути до нуля. Але все частіше і частіше відсутність регулярної інвентаризації мережі, відсутність регулярних сканувань на враливості, відсутність метрик ефективності та відсутність розуміння концепції ризиків та їх оцінки опиняються на чолі головних проблем відділу з інформаційної безпеки. Проблеми описані вище призводять до впровадження неефективного процесу управління вразливостями, а це несе за собою великі ризики.

Метою дипломної роботи є побудова ефективного процесу управління вразливостями.

Об’єктом дослідження дипломної роботи є процес управління вразливостями.

Предметом дослідження дипломної роботи є розробка підходу до побудови ефективного та повноцінного процесу управління вразливостями з урахуванням введених метрик ефективності.

1 ОСНОВНІ ВІДОМОСТІ ПРО БАЗОВИЙ ПРОЦЕС УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ

Згідно з дослідженням Positive Technologies у 2020 році [1], 84% компаній мають уразливість високого ризику на зовнішніх мережевих ресурсах. А згідно з дослідженням уразливості Ponemon Institute [2], 60% жертв витоку даних заявили, що вони були зламані через не виправлену відому вразливість, до якої не застосовували патч, ще більший відсоток, 62%, заявили, що вони не знали, що їхні організації були вразливі до витоку даних. Саме тому організаціям по всьому світу необхідно правильно будувати процес управління вразливостями.

Процес управління вразливостями – це циклічна практика класифікації, визначення пріоритетів, усунення та пом'якшення вразливостей систем [3]. Якщо узагальнити, то процес управління вразливостями поділяється на 4 етапи:

1. Збір інформації про цільові активи і вразливості.
2. Аналіз зібраної інформації.
3. Розробка плану дій згідно проаналізованої інформації.
4. Активні дії.

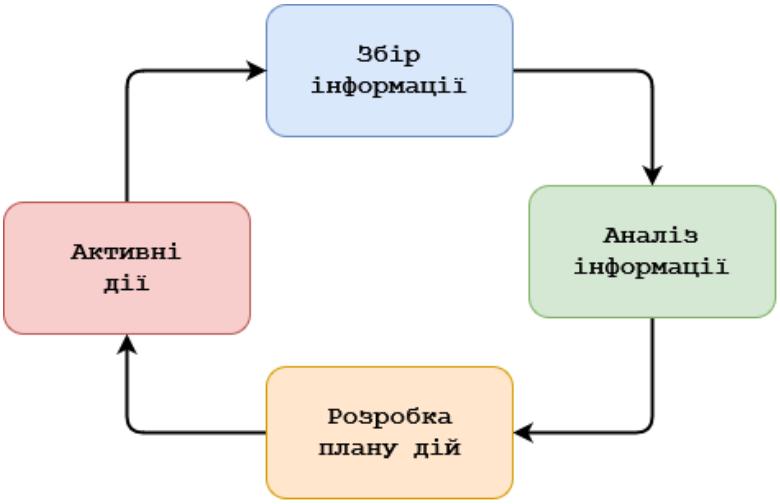


Рисунок 1.1 – Етапи базового процесу управлінння вразливостями

Збір інформації про цільові активи і вразливості робиться для розуміння поточного стану інфраструктури. Під час першого етапу процесу управління вразливостями збирається інформація щодо операційних систем, відкритих портів, встановленого програмного забезпечення цільових активів. Все це робиться для точного знаходження вразливостей і їх подальшої оцінки. Під час першого етапу збирається інформація про активність цільових активів в системі, мережева інформація, версія операційної системи і т.д. Після цього всі дані додаються до спеціальної бази даних, де йде зпівставлення активів і вразливостей на основі знайденої і проаналізованої інформації.

Аналіз зібраної інформації потрібен для правильної оцінки вразливості інформаційної системи, її масштабу та відповідності вимогам безпеки. На основі аналізу зібраної інформації розробляється план дій щодо ефективного покращення рівня захищенності інформаційної системи. Важливу частину на другому етапі займає CVSS, він оцінює загальну серйозність вразливості. Також потрібно не забувати й інформацію про вектори атаки та конкретні наслідки експлуатації вразливості.

Розроблений план дій, згідно проаналізованої інформації, повинен включати в себе ефективні рекомендації щодо покращення рівня захищенності інформаційної системи. Такими рекомендаціями можуть бути: встановлення виправлень(автоматично, або вручну), застосування засобів пом’якшення, або навіть прийняття ризиків.

Активні дії виконуються згідно з розробленим планом дій. На цьому етапі інженери відділу інформаційної безпеки повинні чітко доримуватись виконнаня всіх, описаних на попередньому етапі, рекомендацій.

Всі вищезазначені етапи проводяться ітеративно та циклічно.

Такий вигляд процесу управління вразливостями є досить поверхневим і застарілим. Експоненційне зростання кінцевих точок, а також збільшення складності IT-середовища з кожним днем стають все більшою проблемою для спеціалістів з інформаційної безпеки. Ці проблеми в поєднанні з іншими

пріоритетами бізнесу, такими як перехід до хмарних технологій та іншими зусиллями з трансформації інформаційних систем змусило визначити пріоритети діяльності та оптимізувати обмежені ресурси. В контексті вирішення цих проблем був запровадженний risk-based підхід до процесу управління вразливостями.

Risk-based підхід до процесу управління вразливостями спрямований на виявлення та усунення вразливостей, які становлять найбільший ризик для організації. І інструменти процесу управління вразливістями, що ґрунтуються на оцінці ризиків, і застарілі інструменти процесу управління вразливістями здатні ідентифікувати ризики в середовищі. Однак risk-based підхід демонструє набагато ефективніше визначення пріоритетів найбільш безпосередніх і критичних ризиків для організації [4].

1.1 Зв'язок процесу управління вразливостями з процесом управління ризиками

Для розуміння risk-based підходу до процесу управління вразливостями необхіжно розуміти зв’язок процесу управління вразливостями з процесом управління ризиками.

Процес управління ризиками – це процес виявлення, аналізу, оцінки та усунення загроз кібербезпеки на основі оцінки ризиків [5].

Дуже важливо розуміти, де аспекти процеса управління вразливостями переплітаються з аспектами процеса управління ризиками. Загальна структура процесу управління ризиками подібна до струтури процесу управління вразливостями. Етапи процесу управління ризиками полягають у визначенні критичних активів, ідентифікації та ранжуванні ризиків, ідентифікації засобів контролю, реалізації засобів контролю, а потім моніторингу ефективності засобів

контролю. Управління ризиками також є безперервним процесом, а не одноразовою подією з визначеною кінцевою точкою.

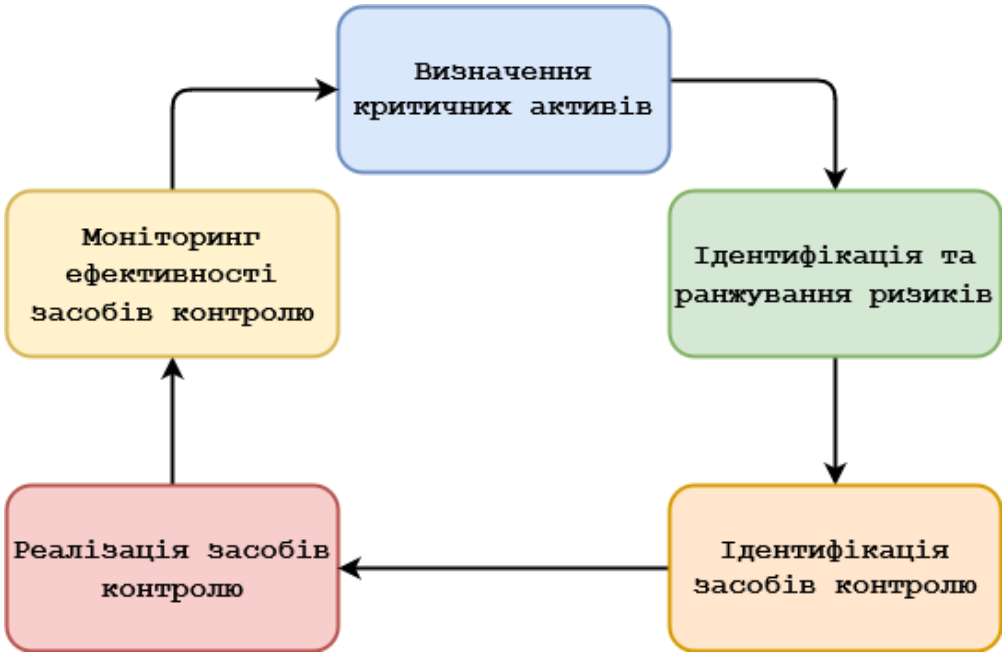


Рисунок 1.2 – Етапи процесу управлінння ризиками

Різні етапи управління вразливостями співвідносяться з різними фазами процесу управління ризиками. Наприклад, моніторинг ефективності засобів контролю та визначення критичних активів у структурі управління ризиками безпосередньо пов’язане зі збором інформації про активи та вразливості. Якщо проводити повне співвідношення зазначених вище процесів, то маємо наступний вигляд.

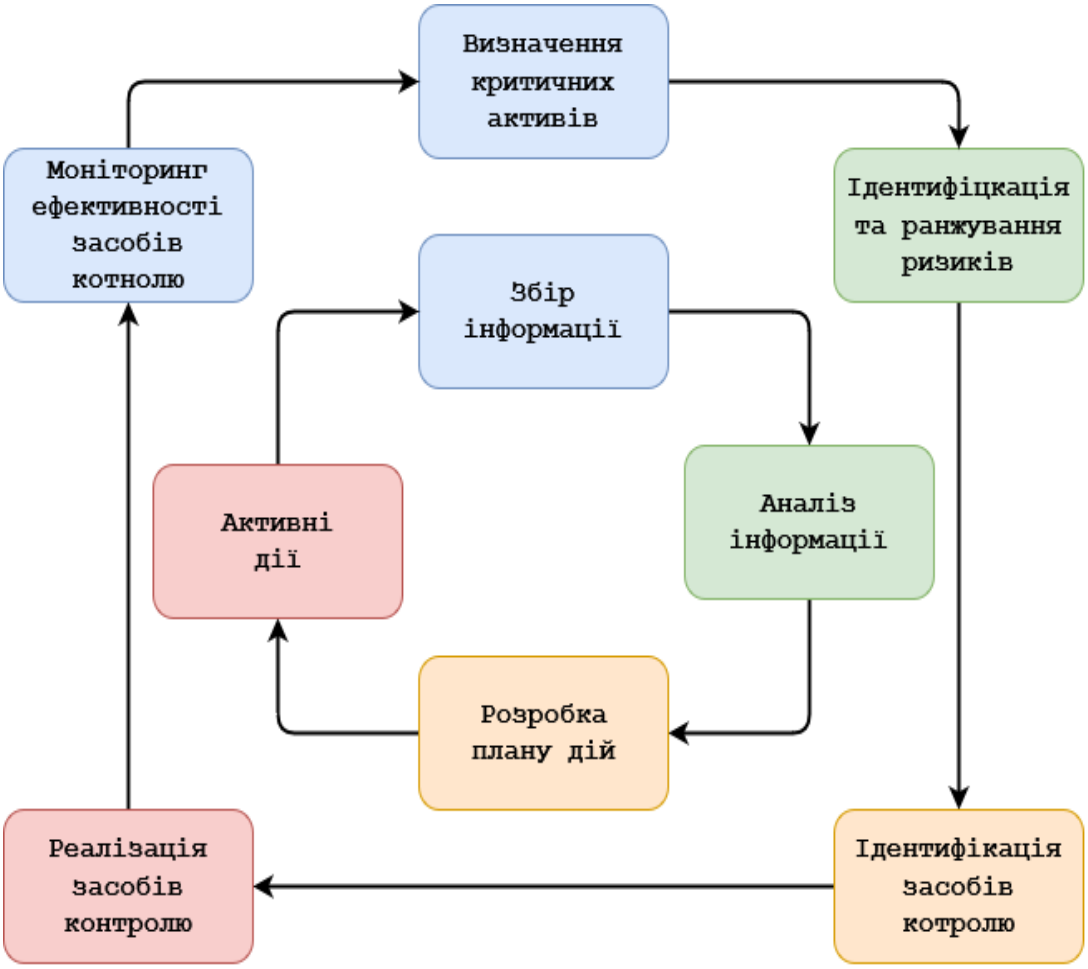


Рисунок 1.3 – Співвідношення етапів процесу управління вразливостями з етапами процесу управління ризиками

Ризики, пов’язані з вразливостями, виявленими в інформаційній системі, можуть спонукати до розглядання засобів контролю, які не усувають вразливості безпосередньо. Такий засоби контролю можуть бути не тільки ефективними проти деяких експлойтів, а й також можуть пом’якшити різні види ризику.

1.2 Сканери вразливостей, принципи роботи сканерів вразливостей

Неможливо уявити процес управління вразливостями без сканерів вразливостей.

Сканер вразливостей - це програмне забезпечення, призначене для оцінки комп’ютерів, мереж або програм на наявність відомих слабких місць. Вони використовуються для ідентифікації та виявлення вразливостей, що виникають внаслідок неправильної конфігурації або неякісного програмування в мережевих ресурсах, таких як брандмауер, маршрутизатор, веб-сервер, сервер додатків тощо [6].

Зазвичай інженери з інформаційної безпеки налаштовують сканери вразливостей для сканування певних мережевих діапазонів, окремих систем або цілей. Сканер вразливостей надсилає ping-пакети на всі IP-адреси в заданому інженером інформаційної безпеки діапазоні, звертаючись до хостів, щоб визначити, які з хостів є активними. Як тільки сканер дізнається, які IP-адреси належать активним пристроям, він надсилає додаткові ping-пакети, спеціальні запити на підключення до відкритих портів.

Після того, як сканер розпізнає, який саме пристрій він сканує і які сервіси працюють на ньому, він посилає спеціальні пакети-запити для визначення додаткової інформації.

Наприклад, якщо сканер вразливостей виявить, що у хоста відкритий порт 22 (типовий порт сервісу SSH), він спробує підключитися до хоста по SSH, щоб визначити, яка версія OpenSSH-серверу використовується на хості. Сканер вразливостей зпівставляє інформацію про знайдену версію OpenSSH-серверу з інформацією з власної внутрішньої базои даних вразливостей. Якщо, наприклад, на пристрої встановлено версію 2.82 OpenSSH-серверу, а вразливості версії 2.82 у цьому програмному забезпеченні були виправлені у версії 2.84, то сканер повідомляє про знайдені вразливості. Крім того, деякі сканери мають спеціальні тести на певні вразливості.

Сучасні сканери вразливостей дозволяють виконувати як автентифіковані, так і неавтентифіковані сканування. Сучасні сканери зазвичай доступні як SaaS (програмне забезпечення як послуга); надається через Інтернет і поставляється як веб-додаток. Сучасний сканер вразливостей часто має можливість налаштовувати звіти про вразливості, а також встановлене програмне забезпечення, відкриті порти, сертифікати та іншу інформацію про хост, яка може бути запитана як частина його робочого процесу.

Автентифіковані сканування - дозволяють сканеру отримувати прямий доступ до мережевих ресурсів за допомогою протоколів віддаленого адміністрування, таких як захищена оболонка (SSH) або протокол віддаленого робочого столу (RDP), а також автентифікуватися за допомогою наданих системних облікових даних. Це дозволяє сканеру вразливостей отримати доступ до низькорівневих даних, таких як конкретні служби та деталі конфігурації операційної системи хоста. Потім він може надати детальну та точну інформацію про операційну систему та встановлене програмне забезпечення, включаючи проблеми конфігурації та відсутні виправлення безпеки.

Неавтентифіковані сканування – це тип сканувань, який може призвести до великої кількості помилкових спрацьовувань і не може надати детальну інформацію про операційну систему активів та встановлене програмне забезпечення. Цей метод зазвичай використовується суб’єктами загроз або аналітиками з безпеки, які намагаються визначити стан безпеки доступних ззовні активів.

Висновки до розділу 1

В першому розділі був зроблений огляд основних відомостей про базовий процес управління вразливостями, аналіз зв’язку процесу управління

вразливостями з процесом управління ризиками, огляд принципів роботи сканерів вразливостей.

Після огляду базового процесу упраління вразливостями можна зробити висновок, що в базовий підхід до процесу управління вразливостями не є ефективним, бо деяким важливим аспектам інформаційної безпеки не приділяється достатньо уваги, а саме: оцінці ризиків, пріорітизації, автоматизації, групуванні активів за характеристиками, генерації звітів і т.д. Натомість, для покращення ефективності процесу управління вразливостями, було вирішино використати risk-based підхід до процесу управління вразливостями, а також ввести метрики ефективності для моніторингу і оцінки роботи процесу управління вразливостями.

В наступному розділі буде описана інтеграція оцінки ризиків в процес управління вразливостями та введені метрики ефективності. Також в другому розділі буде описана розробка підходу до побудови ефективного процесу управління вразливостями і оцінка ефективності такого процесу.

2 ТЕОРЕТИЧНА ПОБУДОВА ЕФЕКТИВНОГО ПРОЦЕСУ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ НА ОСНОВІ ПРОАНАЛІЗОВАНИХ ДАНИХ

Отже, для побудови ефективного процесу управління вразливостями на основі risk-based підходу необхідно додати в сам процес оцінку ризиків.

Щоб оцінити загальний ризик небажаної події зв'язаної, наприклад з експлуатацією вразливості на цільовому активі, потрібно розглянути дві метрики [7]:

1. **Likelihood** настання небажаної події. Наскільки ймовірно, що така подія станеться?
2. **Cost**. Якщо небажана подія станеться, то наскільки ця подія буде коштувати?

В результаті маємо наступну формулу розрахунку ризику:

$$Risk = Likelihood \times Cost \quad (2.1)$$

Використання формули розрахунку ризику розглянемо на прикладі. Представимо, що в абстрактній організації на вразливому сервері, доступному з будь-якої IP-адреси мережі Інтернет, встановлена база даних на якій зберігаються дуже ціні для організації дані. Проаналізуючи інформацію вище можна зробити висновок, що cost і likelihood успішного злому цієї бази даних є надзвичайно високою для організації. Враховуючи наведені вище показники cost і likelihood можна вирахувати, що загальний ризик є надзвичайно високим. Для того, щоб зменшити загальний ризик, потрібно або усунути вразливість на сервері тим самим зменшуючи likelihood успішного зламу, або перенести базу даних з цінними даними на більш захищений сервер тим самим зменшуючи cost успішного зламу.

Якщо було прийнято рішення усунути вразливість, потрібно звернути увагу на likelihood поганого результату усунення вразливості (збій, несумісність програми тощо) і cost такого роду подій (час очищення, час співробітника на вирішення проблеми, cost потенційно втраченого доходу), щоб оцінити ризик вирішення проблеми. Маючи дві оцінки відносного ризику виправлення та відносного ризику не виправлення можна вирішити, що буде кращим для покращення рівня захищеності та окремого сервера з базою даних.

Простим способом обчислення ризику без використання конкретних чисел є використання матриці ризиків [8].

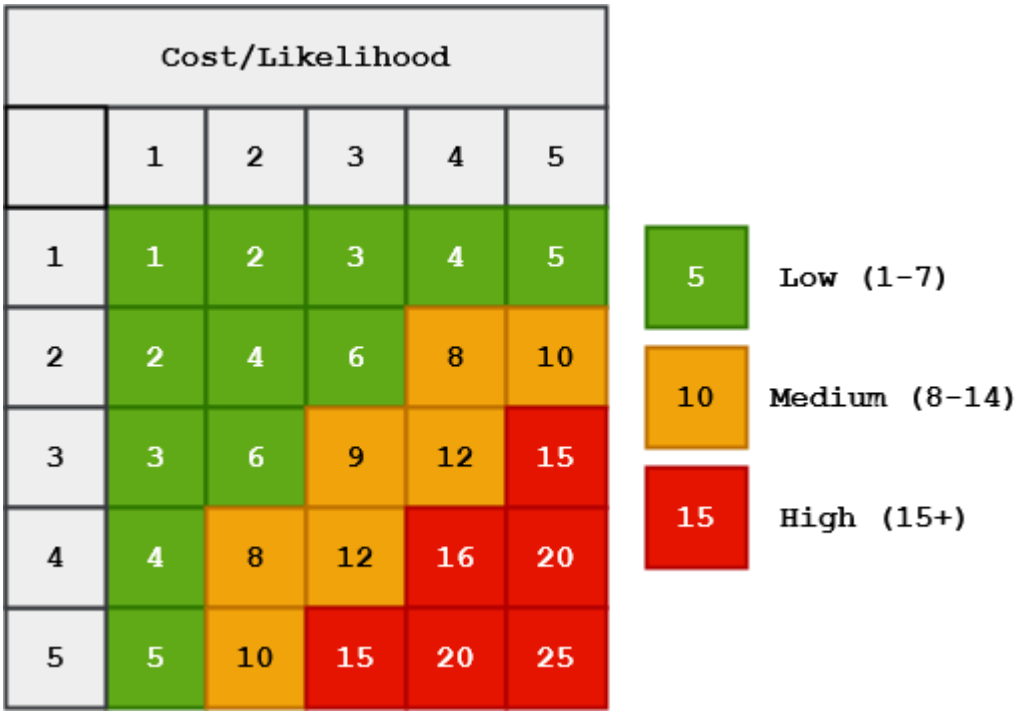


Рисунок 2.1 – Матриця ризиків

Матриця ризиків — це проста таблиця, яка ранжує ризики, призначаючи їм відносні ймовірності та витрати, що полегшує розуміння відносних значень двох різнорідних ризиків. Замість того, щоб намагатися визначити точні відсотки ймовірності та точні витрати, likelihood та cost оцінюється за шкалою від

1(незначний ризик) до 5(катастрофічний ризик). Потім об’єднується обидві осі, щоб визначити загальний рівень ризику — від низького до високого.

Повертаючись до прикладу з базою даних, можна присвоїти 4 бали ймовірності, що сервер з базою даних буде успішно зламаний, cost успішного зламу можна оцінити в 5 балів. Тож за допомогою формули розрахунку ризику можна порахувати, що загальний ризик для вразливого сервера становить 20 балів (високий ризик).

Розглянемо випадок, коли було прийнято рішення усунути вразливість, наприклад, оновленням ПЗ сервера до найновішої версії. В цьому випадку likelihood поганого результату усунення вразливості (збій, несумісність програми тощо) є трохи більше, ніж незначна – 2 бали, а cost поганого результату усунення можна оцінити в 5 балів, бо в базі даних зберігаються дуже важливі дані для компанії. Рахуємо загальний ризик за допомогою формули розрахунку ризику і отримуємо 10 балів (середній ризик).

В результаті маємо:

1. Відносна оцінка ризику виправлення вразливості – 10 балів.
2. Відносна оцінка ризику неивиправлення вразливості – 20 балів.
3. 10 < 20, а отже ризик не вжити заходів набагато вищий, ніж ризик застосування виправлення, тому вжити заходів – це правильно.

Подібні розрахунки ризику в тій, чи іншій ситуації допомагають відповісти на питання: “Діяти? Чи не діяти?”.

Оцінка загальних ризиків допомагає не тільки в момент випралвення вразливостей, а й в момент пріоритизації активів. На активи з найбільшою оцінкою ризику потрібну звертати увагу в першу чергу.

2.1 Боротьба з вразливостями

Для побудування ефективного процесу управління вразливостями необхідно розуміти способи боротьби з вразливостями.

Весь збір та аналіз даних можуть бути марними, якщо не буде чіткої мети щодо використання отриманої інформації. Основними заходами щодо боротьби з вразливостями є виправлення вразливості та пом'якшення вразливості. Виправлення та пом'якшення вразливостей використовується частіше всього і можуть здатись найочевиднішим рішенням. Найнеочевиднішим варіантом вирішення проблеми наявності вразливості являється прийняття ризиків.

Пом'якшення – це широка категорія дій, які або ускладнюють експлуатацію вразливості, або зменшують наслідки експлуатації вразливості [9].

Засоби пом'якшення поділяються на декілька категорій:

1. На основі програм

Цей тип пом'якшення змінюють вразливу програму, щоб усунути або обмежити небезпеку успішної експлуатації. Як приклад можна взяти недавно знайдену вразливість Log4Shell в java-біліотеку Log4j [10]. Виправити вразливість швидко не було змоги, тож для уникнення успішної експлуатації вразливості Log4Shell, java-бібліотеку Log4j можна відключити в конфігураціях веб-сервера. Крім того, можна спробувати відфільтрувати запити до зазначеної бібліотеки за допомогою певних сигнатур.

2. На основі хостів

Цей тип пом'якшення виконується на рівні ОС, а не в самій програмі. Зазвичай використовується внутрішні брандмауер хоста або деякий системний інструмент, такий як SELinux [11], який обмежує ефективність успішної експлуатації вразливості, ускладнюючи модифікацію базової системи та можливої ескалації присутності зловмисника в мережі.

3. На основі мережі

Цей тип пом’якшення виконується на рівні мережі для перехоплення або моніторингу внтурішнього та зовнішнього трафіку уразливого хоста. Прикладом є брандмауер або IDS, який спостерігає за трафіком, що вказує на атаку або успішний компроміс. Прикладом мережевого IDS є Snort [12].

4. Тимчасове

Цей тип не залишається в системі на довгий час і застосовується лише до моменту, коли вразливість буде усунена. Прикладом є блокування мережевого доступу до вразливого хосту.

5. Постійне

Цей тип пом’якшення використовується в тому випадку, якщо пом’якшення не впливає на нормальну роботу вразливого продукту, інколи можна залишити його на місці, навіть після того, як буде усунено основну вразливість. Це буде забезпечувати додатковий захист від майбутніх вразливостей і покращувати загальну безпеку системи.

6. Фізичне

Цей тип пом’якшення використовуть використовують, коли на вразливу систему потрібно вплинути фізично. Наприклад закриття USB портів спеціальними заглушками.

7. Логічне

Цей тип пом’якшення, на відміну від фізичного типу пом’якшення, застосовується на рівні програмного забезпечення або мережі. Наприклад вимкнення USB портів за допомогою інструментів операційної системи.

Виправлення – процес застосування оновленнь для усунення помилок і вразливостей [13].

Після того як вразливість знайдена, інженери інформаційної безпеки дивляться наявність виправлленя для знайденної вразливості. Потрібно якнайшвидше закрити діру в безпеці системи, перш ніж зловмисник скристається нею. Процес виправлення може бути як простим, так і комлпексним/складним. Наприклад натиснути кнопку “Оновити”, коли программа оновлювач зробить всі

необхідні дії автоматично – дуже просто. А от зібрати новий код з неофіційного ресурсу, застосувати його та схрестити пальці у надії, що все встановиться й запрацює, буває дуже складно.

Можуть існувати й інші причини, через які застосування виправлення неможливе. Наприклад вразливість є надто новою для розробника програмного забезпечення(виправлення просто не встигли розробити). В цьому випадку інженери інформаційної безпеки повинні розглядати варіанти пом'якшення або прийняти ризик.

Прийняття ризику — варіант, коли прийнято рішення взагалі нічого не робити [14]. Таке рішення приймається, коли аналіз зібранної інформації показує, що ризик є настільки незначним, або настільки рідкісним, що його не варто розглядати. Наприклад, ризик того що є на ваш сервер впаде метіорит є дуже незначним і рідкісним. Коли ризик приймається, потрібно задокументувати цю це рішення і переконатись, що всі зацікавлені сторони погоджуються з рішенням. В разі проведення аудиту стану інформаційної безпеки системи, потрібно продемонструвати аудиторам, що ризик був врахований, прийнятий і таке рішення задукоментовано. Незадукоментований ризик несе таку ж безпеку, як і неопрацьований, або непомічений ризик.

2.2 Метрики ефективності

Процес управління вразливостями є центральною частиною в будь-якій цілісній стратегії безпеки. Саме тому те, як оцінюється ефективність процесу управління вразливостями є дуже важливим. Ключові метрики ефективності процесу управління вразливостями допомагають кількісно оцінити ризики, пов'язані з вразливими місцями, і ефективно виміряти працездатність процесу управління вразливостями. Якщо будуть вибрані неправильні, або надлишкові

метрики ефективності, то організація не отримає правильної картини в контексті вразливостей , і це відобразиться на інших частинах інформаційної безпеки.

В результаті опитування експертів з інформаційної безпеки під час переддипломної практики, було визначено такі ключові метрики ефективності процесу управління вразливостями:

1. Усвідомлення наявності активів в цільовій мережі.

Чи про всі активи в цільовій мережі ви знаєте? Чи відстежується факт додавання нових активів в цільову підмережу? Позитивна відповідь на ці питання є дуже важливою, бо неможливо захищати те, про що ти не знаєш.

2. Повнонта охоплення скануваннь.

Які види сканування проводяться? Чи охоплений весь обсяг цільових активів? Чи включені в сканування всі критично важливі для бізнесу активи та програми?

3. Спроміжність оцінювати ризики на активах.

Ця метрика ефективності дає змогу зрозуміти наявні в цільовій мережі ризики і, таким чином, перефокусувати свої пріоритети по усуненню вразливостей.

4. Час на усунення критичних вразливостей.

Ця метрика ефективності вимірює середній час, витрачений спеціалістами з інформаційної безпеки, на усунення критичної вразливості. Чим швидше критичні вразливості усуваються, тим краще.

5. Частота сканувань.

Ця метрика ефективності вимірює як часто проводяться сканування на вралзливості в цільовій мережі. В ідеалі спеціалісти з інформаційної безпеки повинні знайти баланс між частотою сканувань та навантаженням, яке спричиняють сканування на цільову мережу.

6. Повнота та актуальність інформації про вразливості.

Ця метрика ефективності вимірює спроможність зберегти повноту та актуальність інформації про вразливості протягом часу. Чим більш повна і акутальніша інформація про вразливості в цільовій мережі, тим краще.

Дані метрики будемо вважати вирішальними в оцінці ефективності процесу управління вразливостями.

2.3 Ефективний процес управління вразливостями

Беручи за основу введені метрики ефективності та risk-based підхід можна побудувати дійсно ефективний процес управління вразливостями.

Регулярна інвентаризація активів в інформаційній системі та їх логічне розділення за характеристика значно покращує керованість цільових активів, повноту охоплення сканувань, зменшує час виявлення критичних вразливостей, а також дає максимально повне усвідомлення наявності цільових активів в мережі.

Введення процесу регулярної генерації звітів забезпечить максимальну повноту та актуальність інформації про вразливості в цільові мережі протягом часу.

Автоматизація та планування, регулярні запуски сканувань активів на вразливості допоможе знайти баланс між частотою сканувань та навантаженням на цільову мережу.

Автоматизація та планування сканувань інвентаризації, автентифікованих сканувань активів на вразливості, генерації звітів значно зберігає час співробітникам відділу інформаційної безпеки, зменьшує час виявлення та усунення критичних вразливостей. Рекомендується здійснювати заплановані сканування в неробочий час, коли будь-яке додаткове навантаження на мережу, чи операційну систему актива не спричинить проблем із продуктивністю. Після запланованого сканування створюватимуться оновлені звіти, які можуть надсилатися електронною поштою в зручний час.

Поєднання процесу управління вразливостями з елементами процесу управління ризиками дозволить оцінювати ризики на цільових активах, тим самим

оцінювати критичність цільових активів та вразливостей на них. Це в свою чергу дозволить оцінювати кількість відкритих критичних вразливостей та час на усунення критичних вразливостей.

Регулярні тести на проникнення, наприклад раз на рік, та регулярні пересканування мережі дозволять підтверджувати, що вразливості на цільових активах були дійсно усунені.

Проаналізувавши метрики ефективності та інтегрувавши оцінку ризиків, автоматизацію, групування активів за характеристиками, генерацію звітів в процес управління вразливостями, маємо наступний вигляд процесу управління вразливостями:

1. Регулярна інвентаризація активів в цільовій мережі.
2. Логічне розділення активів на групи.
3. Регулярний збір інформації про активи та вразливості в цільовій мережі.
4. Регулярна генерація звітів на основі зібраної інформації.
5. Аналіз зібраної інформації про знайдені на активах вразливості. Подальша оцінка і ранжуванння ризиків за допомогою формули розрахунку загального ризику та матриці ризиків. Визначення критичності активів.
6. Розробка плану дій згідно проаналізованої інформації та з урахуванням критичності цільових активів і виявлених вразливостей. Прийняття рішення щодо виправлення, пом’якшення, або прийняття ризику вразливостей.
7. Виконання активних дій згідно з розробленим планом дій.
8. Підтвердження, що вразливості на цільових активах усунені.

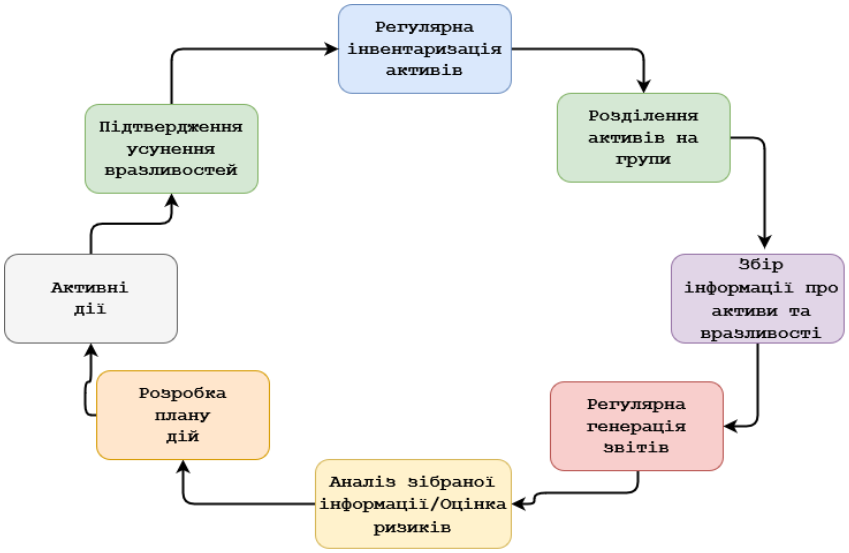


Рисунок 2.2 – Етапи ефективного процесу управлінння вразливостями

2.4 Оцінка ефективності розробленого процесу управління вразливостями

Ефективність розробленоного підходу до процесу управління вразливостями будемо оцінювати за допомогою введених раніше метрик ефективності. Кожній з метрик ефективності буде присвоєний свій ваговий коефіцієнт. Вагові коефіцієнти будуть визначені за допомогою матриці попарних порівнянь, взятої з методу аналізу ієрархій(методу Сааті) [15]. Матриця попарних порінянь є квадратною, тобто кількість рядків і стовпчиків повинно співпадати. На діагоналі матриці порівнянь завжи стоять одиниці, бо один і той же елемент порівнюється між собою. Загальний вигляд такої матриці:

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \quad (2.1)$$

де $a_{ji} = 1/a_{ij}$, $a_{ii} = 1$.

Тепер треба зрозуміти, як саме попарно порівнювати метрики між собою. Для цього введемо якісну шкалу попарного порівння метрик в якій будемо перетворювати якісні показники на бали (рис 2.7).

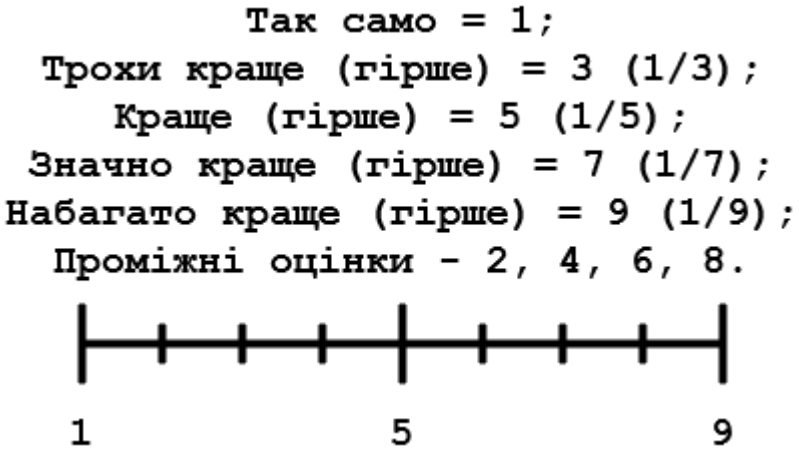


Рисунок 2.3 – Шкала попарного порівняння метрик

Наприклад, якщо вважати, що метрика “Повнота та актуальність інформації про вразливості” значно важливіша, ніж метрика “Усвідомлення наявності активів в цільовій мережі”, то метрика “Повнота та актуальність інформації про вразливості” буде оцінюватись в 5 разів більше, ніж метрика “Усвідомлення наявності активів в цільовій мережі”.

Використовуючи якісну шкалу попарного порівння метрик побудуємо наступну матрицю:

$$A = \begin{matrix} M_1 \\ M_2 \\ M_3 \\ M_4 \\ M_5 \\ M_6 \end{matrix} \begin{bmatrix} 1{,}00 & 1{,}00 & 0{,}14 & 0{,}14 & 5{,}00 & 0{,}20 \\ 1{,}00 & 1{,}00 & 0{,}33 & 0{,}33 & 7{,}00 & 1{,}00 \\ 7{,}00 & 3{,}00 & 1{,}00 & 1{,}00 & 8{,}00 & 2{,}00 \\ 7{,}00 & 3{,}00 & 1{,}00 & 1{,}00 & 8{,}00 & 5{,}00 \\ 0{,}20 & 0{,}14 & 0{,}13 & 0{,}13 & 1{,}00 & 0{,}14 \\ 5{,}00 & 1{,}00 & 0{,}50 & 0{,}20 & 7{,}00 & 1{,}00 \end{bmatrix}, \quad (2.2)$$

де M_1 - Усвідомлення наявності активів в цільовій мережі;

M_2 - Повнота охоплення сканувань;

M_3 - Спроможність оцінювати ризики на активах;

M_4 - Час на усунення критичних вразливостей;

M_5 - Частота сканувань;

M_6 - Повнота та актуальність інформації про вразливості.

Далі побудовану матрицю потрібно знормувати. Знаходиму суму значень по стовпцях і ділимо кожний елемент стовпця на його суму. Підрахуємо сумму елеметнів стовпців:

- Сума I стовпця = 21,20;
- Сума II стовпця = 9,14;
- Сума III стовпця = 3,10;
- Сума IV стовпця = 2,80;
- Сума V стовпця = 36,00;
- Сума VI стовпця = 9,34.

Поділимо кожний елемент стовпця на його суму і отримаємо нормовану матрицю.

$$N = \begin{matrix} M_1 \\ M_2 \\ M_3 \\ M_4 \\ M_5 \\ M_6 \end{matrix} \begin{bmatrix} 0{,}05 & 0{,}109 & 0{,}04607 & 0{,}05 & 0{,}1389 & 0{,}021407 \\ 0{,}05 & 0{,}109 & 0{,}10749 & 0{,}12 & 0{,}1944 & 0{,}107034 \\ 0{,}33 & 0{,}328 & 0{,}32246 & 0{,}36 & 0{,}2222 & 0{,}214067 \\ 0{,}33 & 0{,}328 & 0{,}32246 & 0{,}36 & 0{,}2222 & 0{,}535168 \\ 0{,}01 & 0{,}016 & 0{,}04031 & 0{,}04 & 0{,}0278 & 0{,}015291 \\ 0{,}24 & 0{,}109 & 0{,}16123 & 0{,}07 & 0{,}1944 & 0{,}107034 \end{bmatrix}$$

Наступним кроком є знаходження середнього значення кожного з рядків, це значення і буде значенням вагового коефіцієнту кожної з метрик:

$$W_1 = \frac{0{,}05+0{,}05+0{,}33+0{,}33+0{,}01+0{,}24}{6} = 0{,}0689840686978911 \approx 0{,}068;$$

$$W_2 = \frac{0{,}109+0{,}109+0{,}328+0{,}328+0{,}016+0{,}109}{6} = 0{,}114084254098305 \approx 0{,}114;$$

$$W_3 = \frac{0,109+0,109+0,328+0,328+0,016+0,109}{6} = 0,295675178132944 \approx 0,30;$$

$$W_4 = \frac{0,109+0,109+0,328+0,328+0,016+0,109}{6} = 0,34919199770481 \approx 0,349;$$

$$W_5 = \frac{0,109+0,109+0,328+0,328+0,016+0,109}{6} = 0,0255097076749903 \approx 0,026;$$

$$W_6 = \frac{0,109+0,109+0,328+0,328+0,016+0,109}{6} = 0,14655479369106 \approx 0,147.$$

Також слід зазначити, що вагові коефіцієнти є нормованими:

$$\sum_{i=1}^{6} W_i = 1$$

Вагові коефіцієнти для заданих метрик ефективності розраховано.

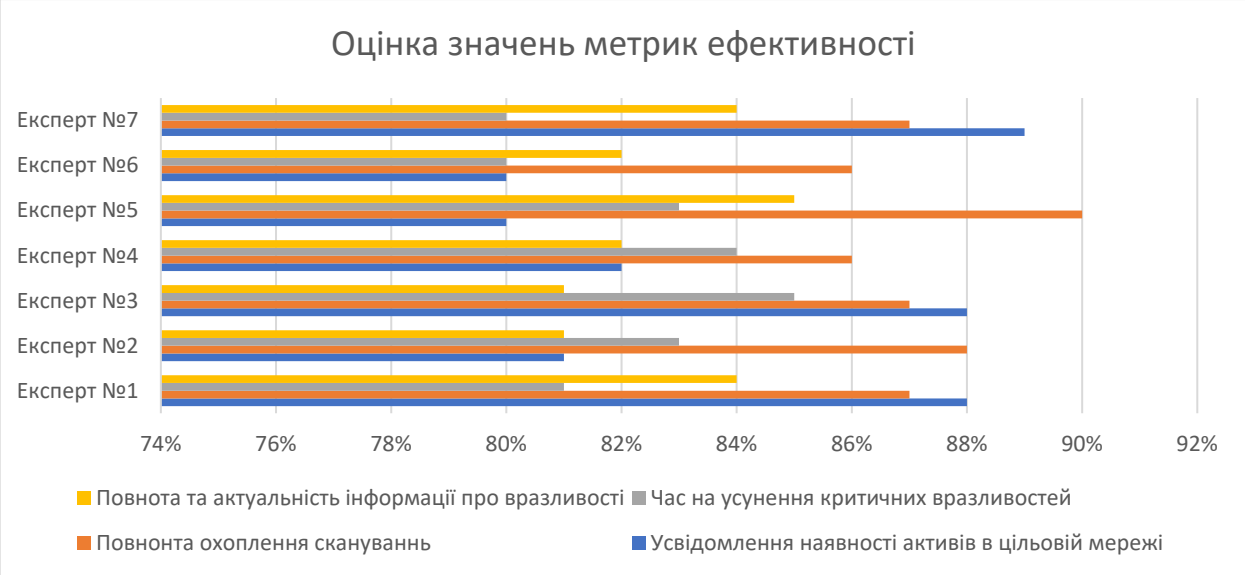
Таблиця 2.1 – Вагові коефіцієнти метрик ефективності

Метрика ефективності	Вага метрики
Усвідомлення наявності активів в цільовій мережі	0,069
Повнонта охоплення скануваннь	0,114
Спроможність оцінювати ризики на активах	0,30
Час на усунення критичних вразливостей	0,349
Частота сканувань	0,026
Повнота та актуальність інформації про вразливості	0,147

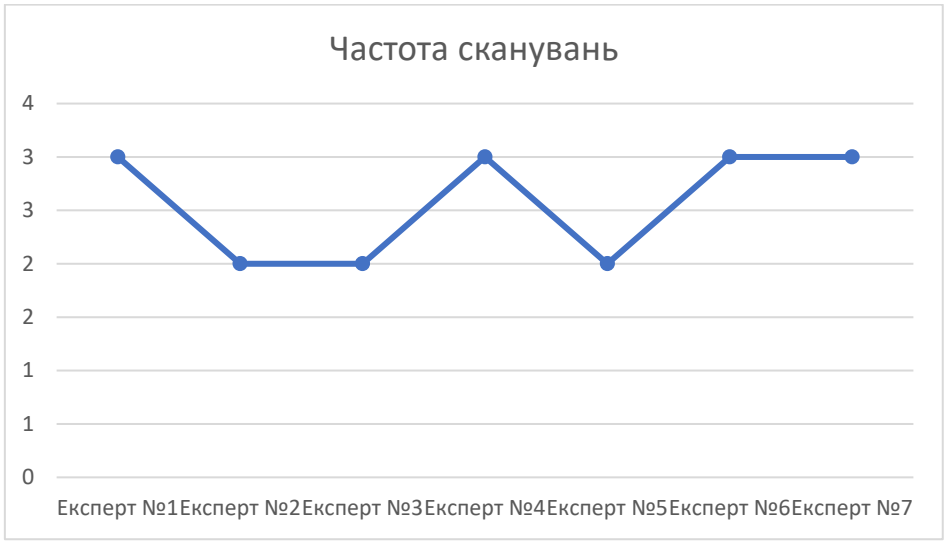
Тепер, після визначення вагових коефіцієнтів для метрик ефективності, можна оцінити виконання метрик ефективності для загального процесу управління вразливостями і розробленого процесу управління вразливостями.

Оцінка значення метрик ефективності загального процесу управління вразливостями проводилась шляхом опитування експертів з інформаційної безпеки. Значення метрик “Усвідомлення наявності активів в цільовій мережі”, “Повнонта охоплення скануваннь”, “Час на усунення критичних вразливостей”,

“Повнота та актуальність інформації про вразливості” оцінювались від 0%(дуже погано) до 100%(дуже добре) (граф 1) Значення метрики “Частота сканувань” оцінювалась кількістю днів на тиждень (граф 2). Слід зазначити, що в загальному процесі управління вразливостями немає елементу оцінки ризиків, тож метрика “Спроможність оцінювати ризики на активах” буде дорівнювати нулю за замовчуванням.



Графік 2.1 - Оцінка значень метрик ефективності



Графік 2.2 – Частота сканувань

Після оцінки значень метрик можна перейти до оцінки ефективності всього загального процесу управління вразливостями. Оцінювати ефективність загального процесу управління вразливостями будемо за наступною формулою:

$$I' = \sum_{i=1}^{7} W_i X_i' \tag{2.3}$$

Де W_i – ваговий коефіцієнт метрики, X_i' - середнє значення відповідних метрик ефективності загального процесу управління вразливостями.

Знайдемо всі X_i'. Для цього знайдемо середнє значення відповідних метрик ефективності і знормуємо їх так, щоб вони були в діапазоні від 0 до 1. Маємо наступну таблицю:

Таблиця 2.2 - Середнє значення відповідних метрик ефективності загального процесу управління вразливостями

Метрика ефективності	Сер. значення відповідних метрик ефективності загального процесу управління вразливостями(X_i')
Усвідомлення наявності активів в цільовій мережі	0,872
Повнонта охоплення скануваннь	0,840
Спроміжність оцінювати ризики на активах	0,000
Час на усунення критичних вразливостей	0,822
Частота сканувань	0,367
Повнота та актуальність інформації про вразливості	0,827

Тепер можна приступити саме до обчислення ефективності загального процесу управління вразливостями користуючись формулою (2.3):

$$I' = \sum_{i=1}^{7} W_i X_i' = 0{,}069 \times 0{,}872 + 0{,}114 \times 0{,}84 + 0{,}3 \times 0 + 0{,}349 \times 0{,}822 + 0{,}026 \times 0{,}367 + 0{,}147 \times 0{,}827 = 0{,}573587224803673 \approx 0{,}573$$

Отже, $I' = 0{,}573$ – ефективність загального процесу управління вразливостями.

Ефективність розробеного процесу управління вразливостями розраховується за тим самим принципом, проте оцінка значень метрик ефективності проводилась емпірично і для більш точних результатів повинно бути зроблено більше дослідів. Після всіх обчислень таблиця з середнім значенням відповідних метрик ефективності для розробленого процесу управління вразливостями виглядає наступним чином:

Таблиця 2.3 - Сер. значення відповідних метрик ефективності розробленого процесу управління вразливостями

Метрика ефективності	Сер. значення відповідних метрик ефективності розробленого процесу управління вразливостями (X_i'')
Усвідомлення наявності активів в цільовій мережі	0,891
Повнонта охоплення скануваннь	0,891
Спроміжність оцінювати ризики на активах	1,000
Час на усунення критичних вразливостей	0,822
Частота сканувань	0,571

Продовження таблиці 2.3

Повнота та актуальність інформації про вразливості	0,936

Використовуючи формулу (2.3) розрахуємо ефективність розробленого процесу управління вразливостями:

$$I'' = \sum_{i=1}^{7} W_i X_i'' = 0{,}069 \times 0{,}891 + 0{,}114 \times 0{,}891 + 0{,}3 \times 1 + 0{,}349 \times 0{,}822 + 0{,}026 \times 0{,}571 + 0{,}147 \times 0{,}936 = 0{,}897577138566821 \approx 0{,}897$$

$I'' = 0{,}897$ – ефективність розробленого процесу управління вразливостями.

Порівнюючи I' і I'', бачимо, що значення I'' є більшим, ніж значення I' на 56,5%. А отже, можна зробити висновок що розроблений процес управління вразливостями є на 56,5% ефективнішим за загальний процес управління вразливостями.

Висновки до розділу 2

В другому розділі було проаналізовано та проведено інтеграцію оцінки ризиків в процес управління вразливостями, праоаналізовано методи боротьби з вразливостями, введенно метрики ефективності, розроблено підхід до побудови ефективного процесу управління вразливостями. З допомогою введених метрик ефективності була проведена оцінка розробленого підходу до побудови процесу управління вразливостями.

Процес управління вразливостями, побудований з допомогою розробленого підходу, є на 56.5% ефективнішим за загальний процес управління вразливостями.

В наступному розділі буде продемонстрована практична побудова ефективного процесу управління вразливостями з допомогою хмарної платформи Qualys Cloud Platform.

3 ПРАКТИЧНА ПОБУДОВА ЕФЕКТИВНОГО ПРОЦЕСУ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ

Лабораторне середовище для виконання дипломної роботи складається з потужностей Qualys Cloud Platform та трьох віртуальних машин, які встановлені на сервері віртуалізації VMware ESXi: сканер вразливостей Qualys Scanner Appliance, віртуальна машин на якій встановлено операційну систему Ubuntu 14.04, віртуальна машина зі встановленою Metasploitable OS. Дане лабораторне середовище імітує мережу довільної, абстрактної організації.

Верхньорівнева архітектура лабораторного середовища:

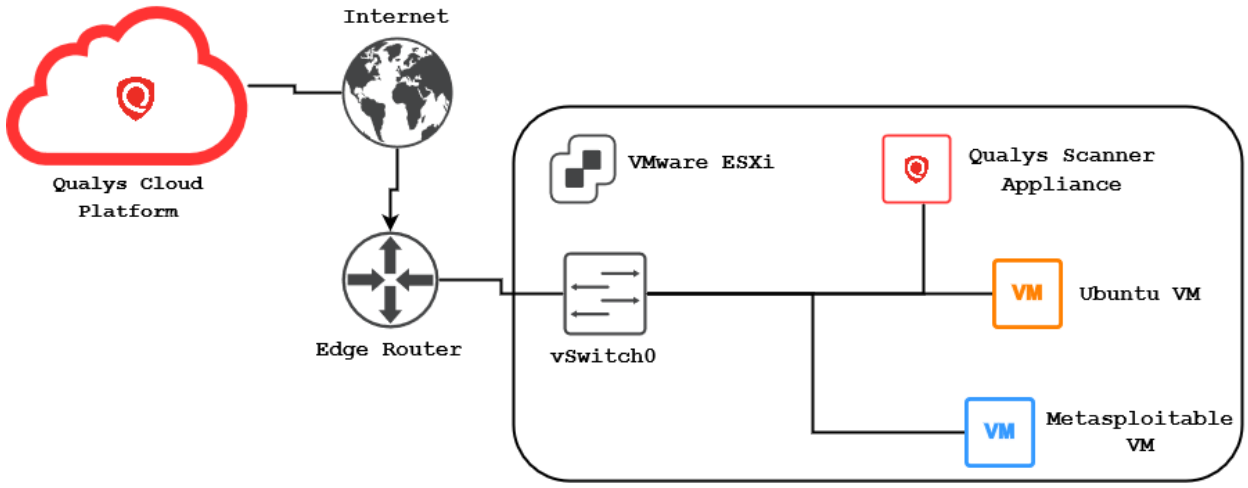


Рисунок 3.1 – Верхньорівнева архітектура лабораторного середовища

Активу Metasploitable VM відведена роль тестового серверу, де адміністратори мережі можуть тестувати роботу деякого програмного забезпечення. Cost успішного зламу цього тестового серверу умовно будемо оцінюватив 50 тисяч доларів США.

Ubuntu VM буде виконувати роль робочої станції адміністратора мережі організації. Cost успішного зламу цього хосту оцінюємо в 200 тисяч доларів США, бо хост адміністратора має доступ до усіх хостів в цільовій підмережі.

Таблиця 3.1 – Назва цільових активі, їх роль та Cost успішного зламу

Актив	Роль	Cost (USD)
Metasploitable VM	Test Server	90 тис. доларів
Ubuntu VM	Admin Workstation	250 тис. доларів

3.1 Процес інсталяції сканеру вразливостей Qualys Scanner Appliance

Інформацію щодо процесу інталяції сканеру вразливостей Qualys Scanner Appliance було взято з офіційної документації Qualys, а саме з Virtual Scanner Appliance User Guide [16].

Для того, щоб встановити Qualys Scanner Appliance на гіпервізор VMware ESXi, треба отримати образ .ova віртуальної машини Qualys Scanner Appliance. Це можна зробити з допомогою веб-консолі Qualys Cloud Platform.

Після успішної авторизації у системі, перейдемо до модулю Vulnerability Management. У модулі Vulnerability Management перейдемо у вкладку Scans. У вкладці Scans перейдемо у вкладку Appliances, де й відображаються усі Qualys Scanner Appliances. Для того щоб, додати новий Qualys Virtual Scanner Appliance натиснемо на кнопку New та виберемо пункт Virtual Scanner Appliance.

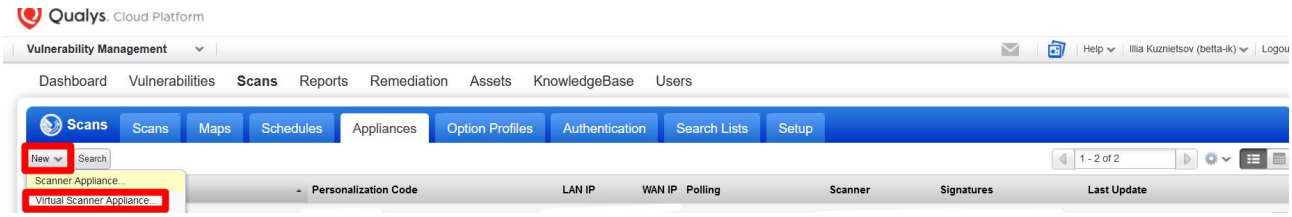


Рисунок 3.2 – Створення нового Qualys Cloud Appliance

Одразу ж відкриється віконце Майстра інсталяції. Обираємо Start Wizard та вводимо назву Qualys Virtual Scanner Appliance. Також потрібно вибрати

платформу віртуалізації, на яку буде встановлено Qualys Virtual Scanner Appliance, в нашому випадку це VMware ESXi. Натискаємо кнопку Next. Починається скачування .ova образу на локальний комьютер.

На наступному етапі потрібно імпортувати скачаний .ova образ у віртуальне середовище VMware ESXi і встановити віртуальну машину. Після успішного встановлення віртуальної машини, потрібно буде активувати Qualys Virtual Scanner Appliance. Робиться це з допомогою Personalization Code, який генерується випадково і відображається в веб-інтерфейсі Qualys Cloud Platform.

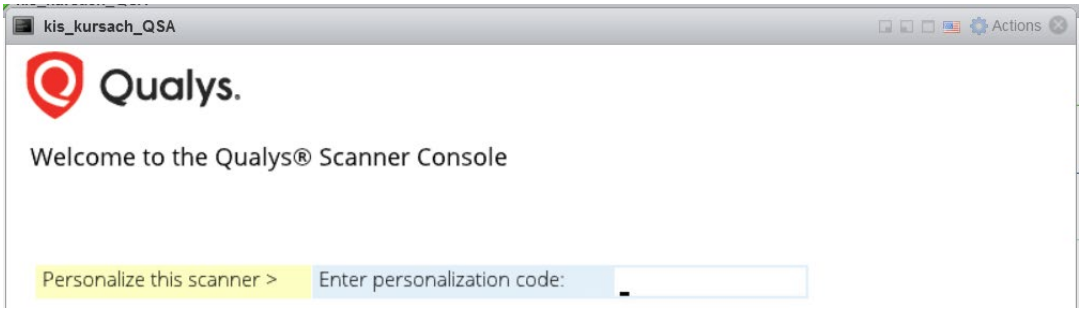


Рисунок 3.3 – Введення Personalization Code для активації Qualys Virtual Scanner Appliance

Після вводу Personalization Code, система почне оновлюватись та скачувати необхідні файли. Після успішного оновлення процес базової інсталяції Qualys Virtual Scanner Appliance буде завершено.

Рисунок 3.4 – Інтерфейс Qualys Virtual Scanner Appliance

Для того, щоб переконатися, що Qualys Virtual Scanner Appliance був успішно встановлений та має зв’язок з хмарною платформою Qualys Cloud

Platform, необхідно перейти в Vulnerability Management->Scans->Appliances. Можна побачити, що Qualys Virtual Scanner Appliance успішно з’єднався з хмарною платформою Qualys Cloud Platform та готовий працювати.

3.2 Налаштування регулярної інвентаризації цільових активів, додавання цільових активів в підписку Qualys Vulnerability Management та логічне групування цільових активів

Регулярна інвентаризація цільових активів дуже важлива, адже ми не можемо захищати те, про що не знаємо.

Для регулярної інвентаризації цільових активів з допомогою Qualys Cloud Platform застосовують так звані Map-сканування. Під час Map-сканувань внутрішньої мережі використовується Qualys Scanner Appliance сканер для створення карти видимих пристроїв у внутрішній мережі. Під час Map-сканувань спочатку визначається, які хости є живими. Кожен хост у мережевому блоку цільового домену тестується за допомогою з ICMP, TCP та UDP запитів. Запити TCP і UDP надсилаються на порти за замовчуванням для загальних служб, таких як DNS, TELNET, SMTP, HTTP і SNMP. Якщо ці запити викликають хоча б одну відповідь від хоста, хост вважається. Для кожного виявленого хоста створюється список відкритих портів та сервісів, запущених на хості. Для кожного сервісу можна переглянути метод виявлення, який використовується для ідентифікації сервісу, а також порт, на якому сервіс запущений.

Регулярні Map-сканування дозволяють мати повну інформацію про наявність активів в цільовій підмережі.

Для того щоб, проводити будь-які сканування потрібно створити та налаштувати профілі конфігурації сканувань. Для цього потрібно перейти у вкладку VM->Scans->Option Profiles, натиснути на кнопку New та Option Profile.

Відкриється нове вікно в якому треба дати назву профілю конфігурації та призначити власника цього профілю кофнігурацій. Також робимо новий профіль конфігурацій доступним для усіх користувачів в рамках усієї підписки.

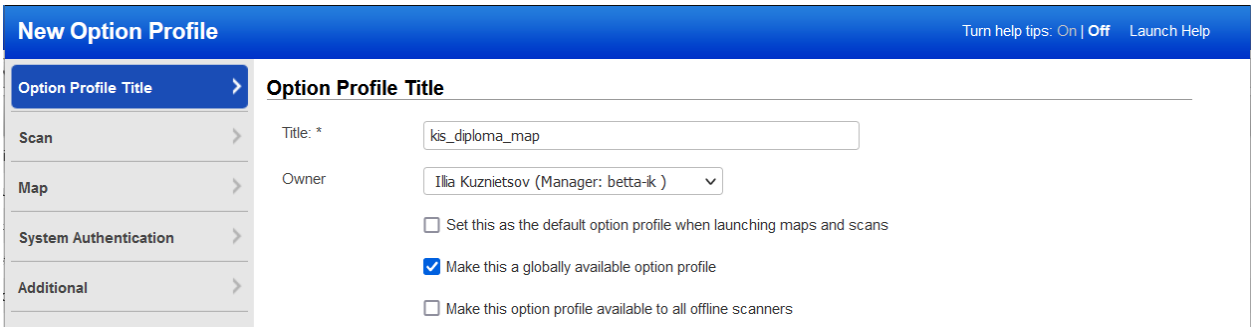


Рисунок 3.5 – Новий Option Profile

У вкладці Map знаходятся налаштування з якими буде запущене Map-сканування цільової підмережі.

Існують наступні налаштування для проведення Map-сканувань:

- **Perform Basic Information Gathering on** – використовується для запуску додаткових тестових сканування, які можуть призвести до виявлення додаткових пристроїв, наприклад маршрутизаторів. Під час таких сканувань Qualys намагається визначити операційну систему, встановлену на кожному хості, і сканує порти, щоб визначити, які порти відкриті.
- **TCP Ports** - використовується для вибору TCP портів, які потрібно просканувати.
- **UDP Ports** - використовується для вибору UDP портів, які потрібно просканувати.
- **Options** – якщо вимкнути опцію Live Host Sweep, то виявлення пристроїв буде здійснюватись лише за допомогою методів виявлення DNS (DNS, Reverse DNS і DNS Zone Transfer). Опція Disable DNS traffic дозволяє не генерувати DNS трафік під час Map-сканування.
- **Performance** - використовується для налаштування параметрів продуктивності для сканування мережі. Для звичайних мереж рекомендується використовувати

Normal, проте якщо мережа знаходиться під навантаженням, то Performance краще змінити на Low.

- **Authentication** - автентифікація дозволяє сканеру входити в систему під час сканування, щоб розширити можливості виявлення.

Налаштування Map-сканувань було вирішено залишити за замовчуванням, а саме: проводити додаткові тестові сканування на всій підмережі, обрав стандартний набір TCP/UDP портів, Live Host Sweep увімкнено, Performance поставлений на Normal, автентифікацію не проводити.

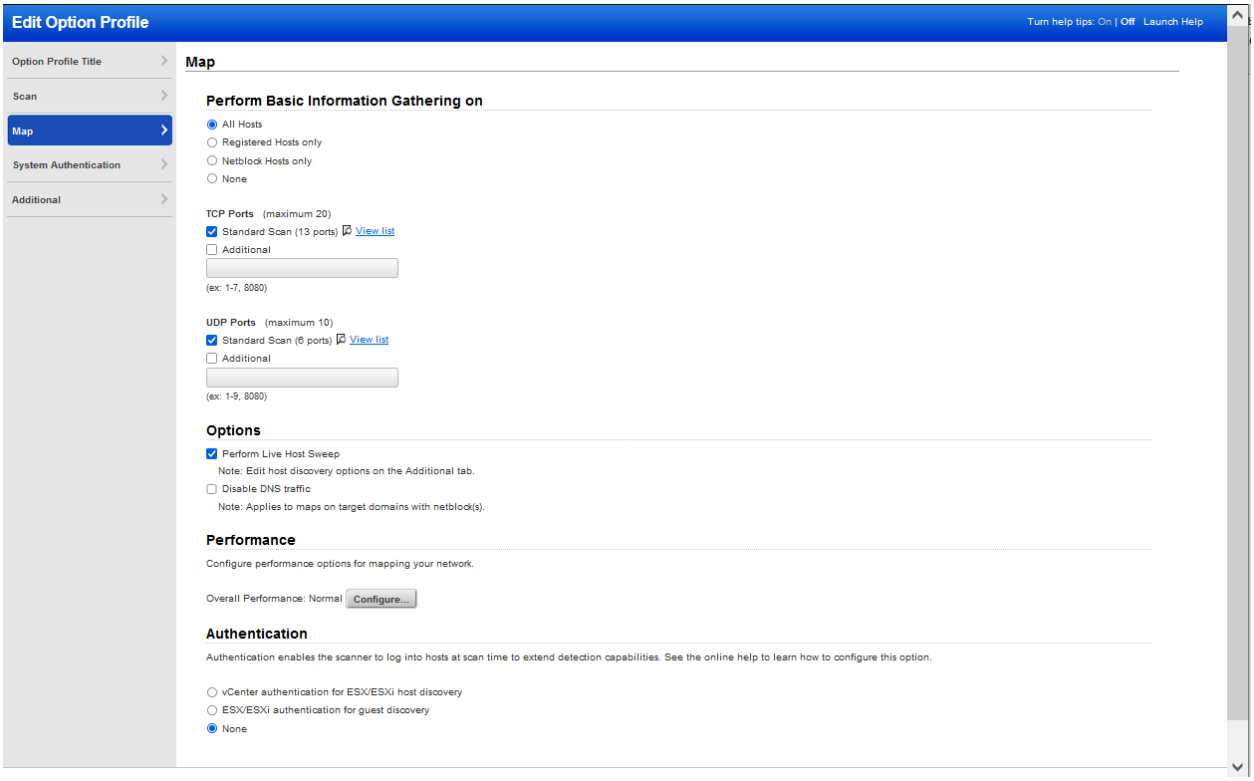


Рисунок 3.6 – Основні налаштування Map-сканувань

На цьому налаштування Option Profile для проведення Map-сканувань закінчено. Зберігаємо профіль конфігурації натиснувши на кнопку Save. Профіль конфігурацій успішно створено.

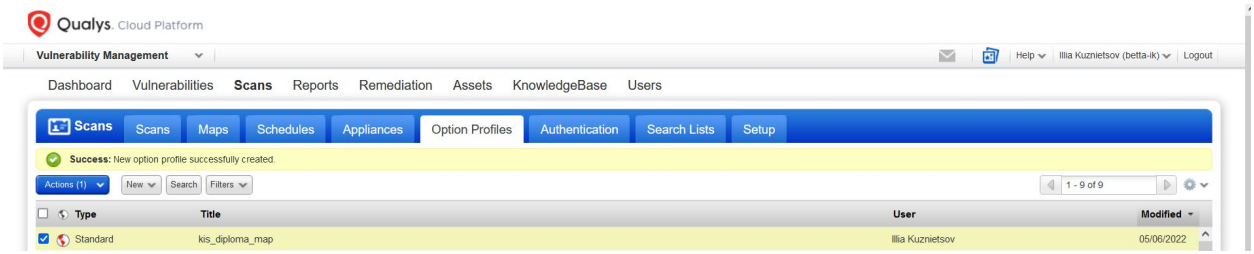


Рисунок 3.7 – Створений Option Profile для проведення Map-сканувань

Для запуску регулярних, запланованих Map-скануваннь необхідно перейти у вкладку VM-> Scans->Schedules натиснути кнопку New та обрати Schedule Map. У відкрившомуся вікні необхідно задати ім’я та власника Map-сканування, а також обрати профіль конфігурацій і Scanner Appliance, який буде виконувати Map-сканування.

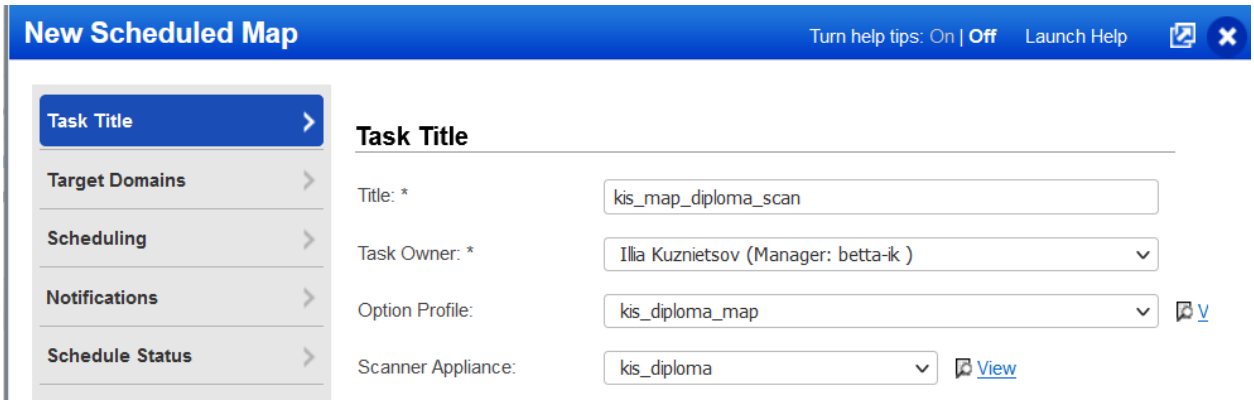


Рисунок 3.8 – Створення запланованого Map-сканування

Після задання основних параметрів необхідно вибрати цільові домени в рамках яких буде виконуватись Map-сканування. Обираємо домен створений раніше – kis.diploma:[192.168.0.0-192.168.255.255].

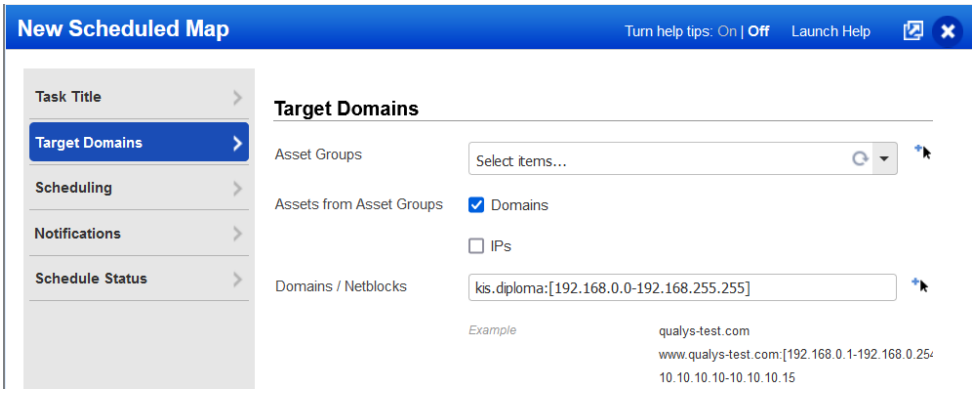


Рисунок 3.9 – Обрання цільової підмережі

Для того, щоб сканування були запланованими та регулярними у пункті Scheduling необхідно налаштувати параметри дати та часу старту Map-сканування та інтервал з яким воно буде виконуватись. Тривалість сканування можна задати додатково. Сканування краще проводити в неробочий час, щоб не сильно навантажувати цільову підмережу.

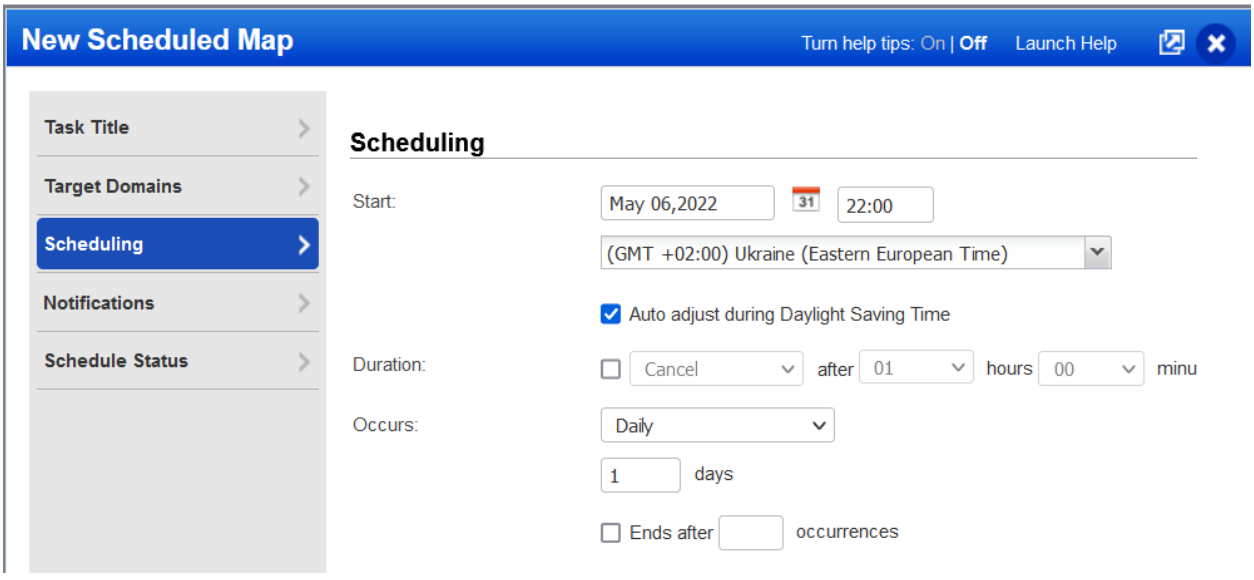


Рисунок 3.10 – Налаштування часу запуску Map-сканувань

Всі необхідні налаштування завершені, можна запускати Map-сканування.

В результаті сканування інвентаризації були виявлені цільові активи, які належать до лабораторного середовища:

Таблиця 3.2 – IP-адреси виявлених цільових активів

Актив	IP-адреса
Metasploitable VM	192.168.100.164
Ubuntu VM	192.168.100.168

Тепер можна додати знайдені цільові активи в підписку Qualys Vulnerability Management. Це робиться того щоб, мати змогу запускати сканування на вразливості та генерувати звіти для цільових активів Для цього треба перейти у вкладку VM-Assets-Asset Management, натиснути на кнопку New та обрати метод відстежування активів. Обираємо IP Tracked Hosts (метод відстежування за IP-адресою).З’явиться нове вікно з основною інформацією про підписку та необхідними налаштуваннями в контексті додавання нових активів. Переходимо на вкладку Host IPs та вписуємо IP-адреси машин Metasploitable VM(192.168.100.164) та Ubuntu VM (192.168.100.168).

Цільові активи успішно додані у підписку Qualys Vulnerability Management.

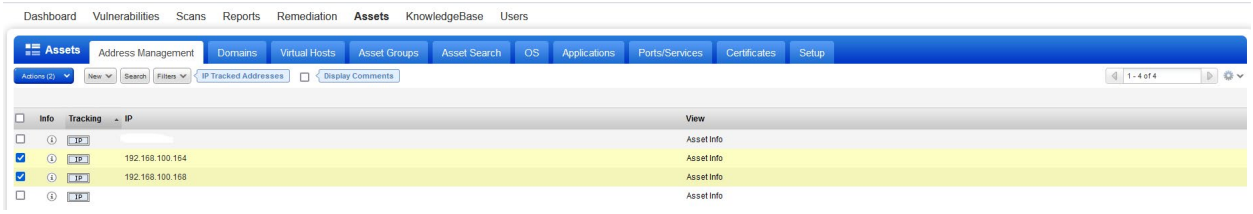


Рисунок 3.11 – Знайдені цільові активи додані в підписку

Для того щоб, було зручніше працювати з цільовими активами треба згупувати їх. Для цього потрібно перейти у вкладку VM-Asset Groups, натиснути на кнопку New та обрати Asset Group. З’явиться нове вікно в якому треба дати назву групі активів, призначити власника цієї групи та вписати IP-адреси активів, які будуть входити в нову групу активів. Варто зазначити, що в Asset Group можна додавати лише ті IP-адреси, які вже знаходяться у підписці Qualys Vulnerability

Management. Тож додаємо цільові активи Metasploitable VM і Ubuntu VM в Asset Group з назвою kis_diploma_lab.

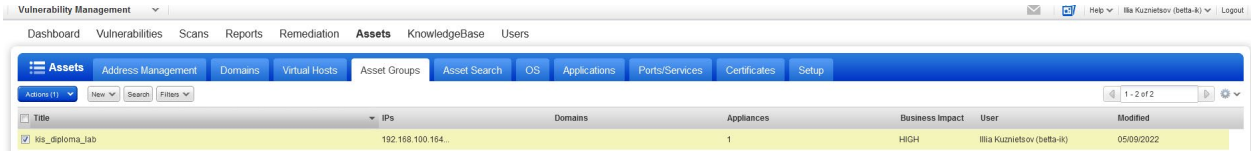


Рисунок 3.12 – Створена Asset Group

Таким чином були налаштовані регулярні сканування інвентаризації підмережі 192.168.0.0/16. Виявлені цільові активи були додані в підписку та логічно згруповані.

3.3 Налаштування регулярного збору інформації про активи та вразливості в цільовій підмережі

Тепер потрібно налаштувати регулярні, автентифіковані сканування цільових активів на вразливості. Для початку потрібно налаштуванти облікові записи, які Qualys Scanner Appliance буде використовувати для автентифікації в системі, та профіль конфігурацій з яким буде виконуватись сканування цільових активів.

Почнемо з налаштування обілкових записів. Для налаштування облікових записів потрібно перейти у вкладку VM-Scans-Authentication, натиснути на кнопку New та обрати для якої операційної системи буде створений обліковий запис. Обираємо Unix, так як автентифіковані сканування будут проводить для Metasploitable VM та Ubuntu VM.

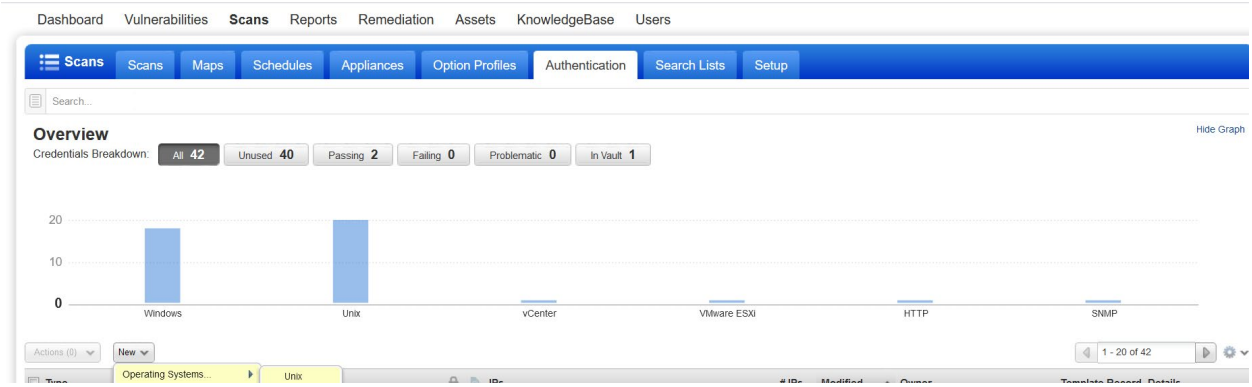


Рисунок 3.13 – Створення нового облікового запису

Обліковий запис Metasploitable VM. У вікні яке з'явилось вводимо ім'я нового облікового запису та переходимо на наступну вкладку.

У вкладці Login Credentials потрібно вписати облікові дані та перейти на владку Root Delegation.

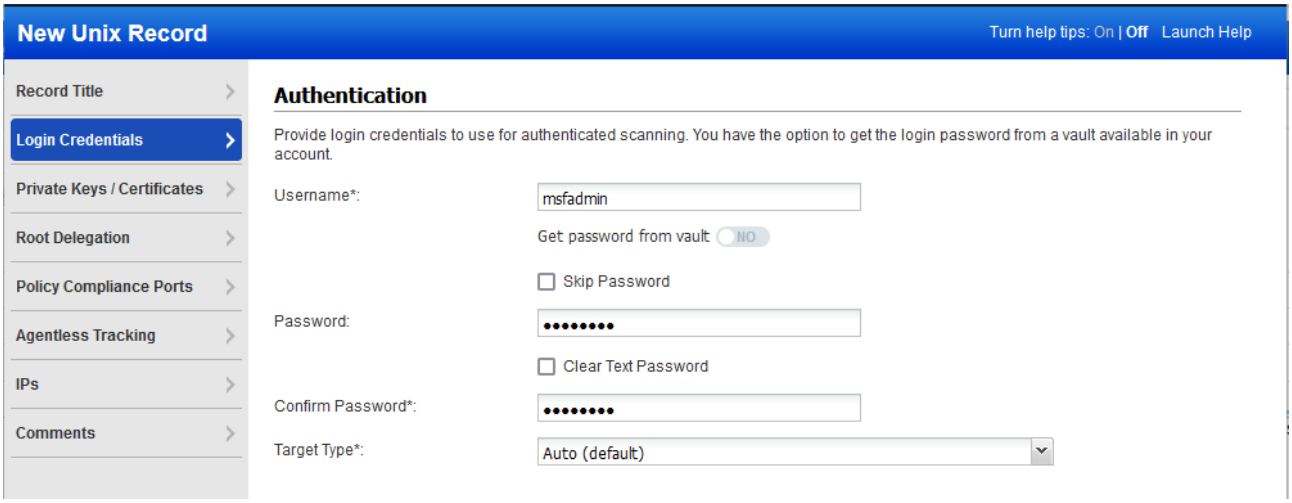


Рисунок 3.14 – Налаштування обілкових даних

У вкладці Root Delegation необхідно вказати механізм підвищення привілей та пароль суперкористувача. Root Delegation відповідає за те, щоб під час сканування деякі тести виконувалися с підвищеними привілеями.

З вкладки Root Delegation потрібно перейти у вкладку IPs та вказати IP-адресу цільового активу для якого буде застосовувати цей обілковий запис. Зберігаємо обліковий запис.

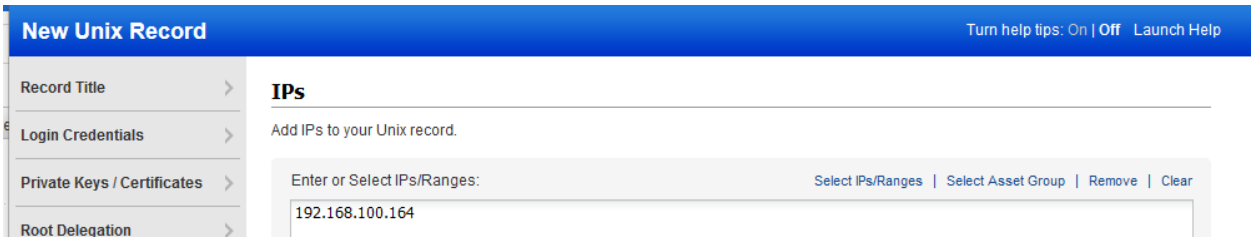


Рисунок 3.15 – Вказування IP-адреси цільового активу

Аналогінчі дії потрібно зробити для Ubuntu VM. Облікові записи успішно створились.

Рисунок 3.16 – Створені нові облікові записи

Перейдемо до налаштування конфігураційного профілю сканувань на вразливості. Для цього потрібно перейти у вкладку VM-Scans-Option Profiles, натиснути на кнопку New та Option Profile.

З’являється нове вікно в якому треба дати назву профілю конфігурації та призначити хазяїна цієї групи. Після того як заповнили необхідну інформацію та зробили цей профіль конфігурацій доступним для усіх користувачів в рамках усієї підписки, переходимо до вкладки Scan.

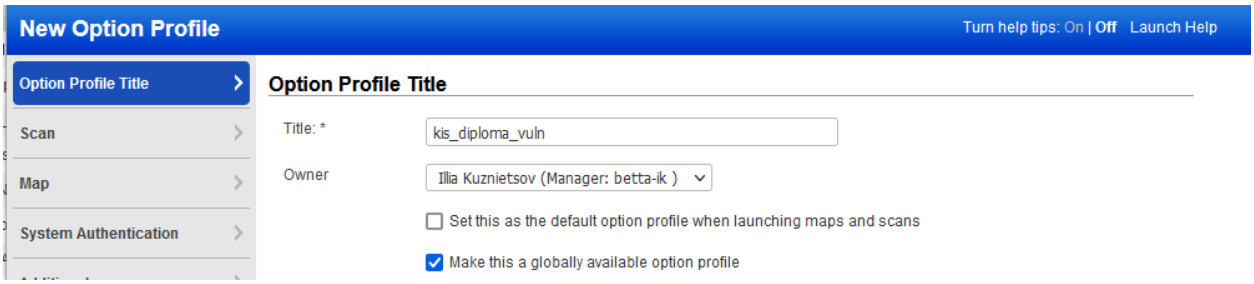


Рисунок 3.17 – Створення нового Option Profile для сканувань на вразливості

У вкладці Scan знаходяться налаштування з якими буде запущене сканування цільових активів на вразливості.

Існують наступні налаштування:

- **TCP Ports** - використовується для вибору TCP портів, які потрібно просканувати.
- **UDP Ports** - використовується для вибору UDP портів, які потрібно просканувати.
- **Authoritative Option for light scans** - Ця опція змінює обробку даних сканування, щоб статус вразливості (New, Active, Reopened, Fixed) оновлювався для всіх вразливостей на цільових хостах, а не лише для перевірених портів. Ви можете вибрати цю опцію лише для Light port scans, або тих, де налаштовано «None + additional ports».
- **Scan Dead Hosts** – Сканувати мертві хости. За замовчуванням мертві хости ігноруються. Включення цієї опції може збільшити час сканування і не рекомендується для мереж класу C або більших.
- **Close Vulnerabilities on Dead Hosts** - Якщо після певної кількості сканувань хост виявиться неживим, то статус вразливостей на цьому хості буде оновлено на Виправлено.
- **Purge old host data when OS is changed** - Якщо сканування виявляє значну зміну в ОС хосту порівняно з попереднім скануванням, то старі дані хоста будуть остаточно видалені, а нові дані хосту, пов’язані лише з новою ОС, будуть збережені.
- **Performance** - використовується для налаштування параметрів продуктивності для сканування мережі. Для звичайних мереж рекомендуюється використовувати Normal, проте якщо мережа знаходиться під навантаженням, то Performance краще змінити на Low.
- **Load Balancer Detection** - Якщо цей параметр увімкнено, сканер намагатиметься визначити балансувальники навантаження та кількість веб-серверів за ними.
- **Password Brute Forcing** - Виберіть рівень підбору пароля, який виконується скануванням. Параметр «Вичерпний» збільшить час сканування.

- **Vulnerability Detection** – Якщо вибрано Complete, то Qualys буде сканувати хост на всі вразливості які існують у базі даних хмарної платформи. Опцію Custom потрібно вибирати, якщо треба просканувати хост на конкретні вразливості визначені користувачем. Select at runtime дозволяє вибирати між Complete та Custom під час запуску сканування.
- **Authentication** - Автентифікація дозволяє сканеру входити в систему під час сканування, щоб розширити можливості виявлення.
- **Test Authentication** - Якщо ввімкнено, сканер перевірить автентифікацію цільових хостів. Інших тестів сканування не буде. Ви повинні вибрати принаймні один тип автентифікації
- **Additional Certificate Detection** - Qualys знайде сертифікати для портів/сервісів із повним скануванням портів за замовчуванням. Увімкніть цей параметр, щоб знайти сертифікати в інших місцях за допомогою автентифікації, наприклад, в Apache, Tomcat, Jboss, Java KeyStore і Windows IIS. Потрібна автентифікація.
- **Dissolvable Agent** – Qualys шле на сканований хост (функція доступна тільки для Windows) подобу хмарного агента, який збирає необхідну інформацію, відправляє її на платформу і самознищується.
- **Lite OS Scan** - Якщо вибрано цей параметр і QID 45017 включено в перевірку, завдання сканування зменшує тестування цілей на виявлення ОС під час фази виявлення хоста перед тестуванням уразливості. Кілька повільних методів виявлення ОС виключені (наприклад, telnet, msrpc, ntp тощо).
- **Add a Custom HTTP Header value** - Встановіть користувацьке значення, щоб відключити захист (наприклад, журналювання, IP-адреси тощо) під час виконання авторизованого сканування.
- **Host-Alive Testing** - Якщо ввімкнено, тестування сканування повідомлятиме про хости, знайдені живими під час процесу виявлення або сканування портів. Інших тестів не буде.

- **Do not overwrite OS** - Якщо ввімкнено, Qualys не буде оновлювати ОС цільових хостів під час обробки сканування.

Скріншоти з налаштуваннями профілю конфігурацій сканувань на вразивості знаходяться в Додатках.

Усі необхідні налаштування були зроблені, зберігаємо профіль конфігурації натиснувши на кнопку Save. Профіль конфігурацій успішно створено.

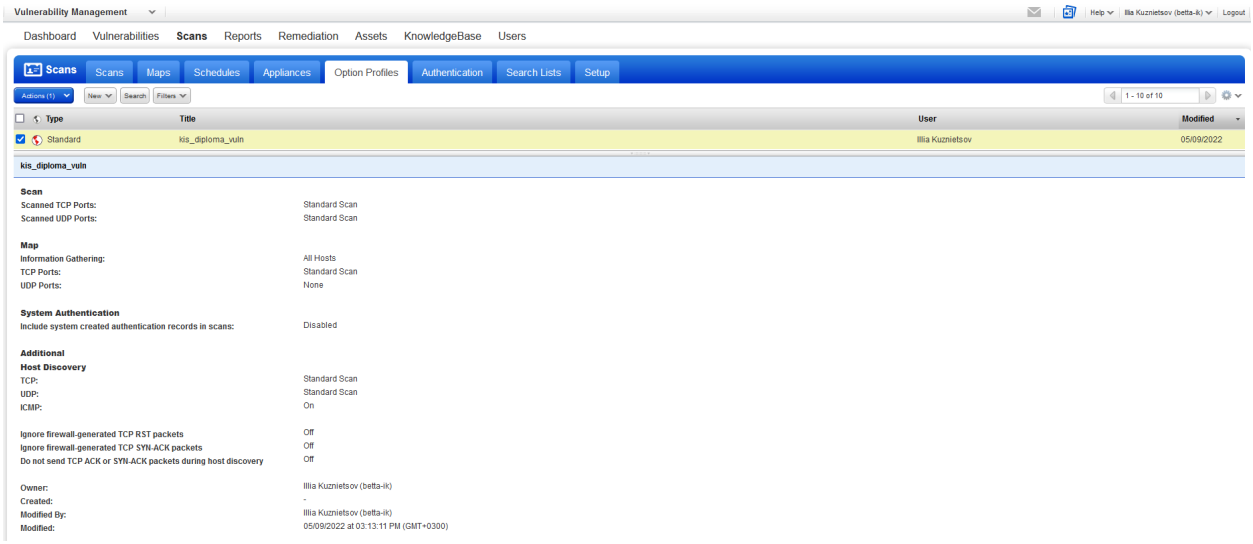


Рисунок 3.18 – Створений Option Profile для сканувань на вразливості

Накінець можна перейти до налаштування запланованих, регулярних сканувань цільових активів на вразливості. Для того щоб, налаштувати та запустити сканування потрібно перейти у вкладку VM->Scans->Schedules, натиснути на кнопку New та обрати Schedule Scan.

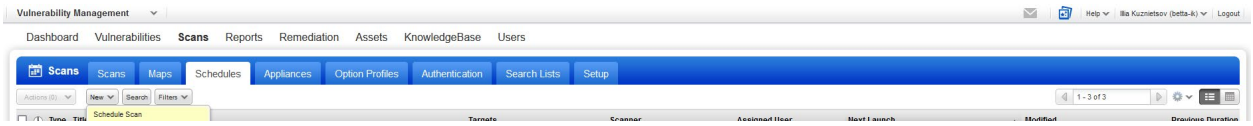


Рисунок 3.19 – Створення запланованого сканування на вразливості

У відкрившомуся вікні необхідно задати ім’я та власника сканування на вразливості. Також потрібно обрати профіль конфігурацій і Scanner Appliance, який буде виконувати сканування.

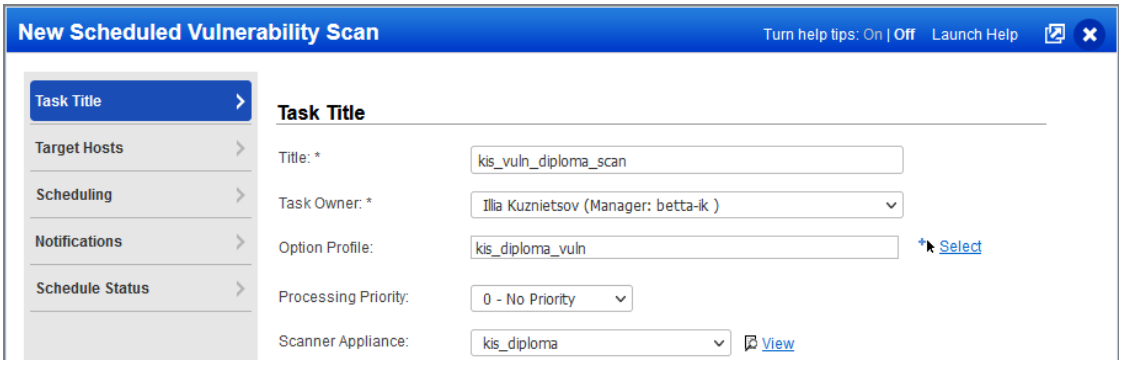


Рисунок 3.20 – Налаштування нового запланованого сканування

Після задання основних параметрів необхідно вибрати цільові групи активів в рамках яких буде виконуватись сканування. Обираємо групу актиіві створену раніше раніше – kis_diploma_lab

Для того, щоб сканування були запланованими та регулярними у пункті Scheduling необхідно налаштувати параметри дати та часу старту сканування та інтервал з яким воно буде виконуватись. Тривалість сканування можна задати додатково. Мною було вирішено проводити сканування на вразливості кожного дня у 20:00 (неробочий час), щоб не створювати додаткове навантаження на цільову підмережу.

Всі необхідні налаштування завершені, можна запускати сканування. Бачимо, що сканування успішно створилось.

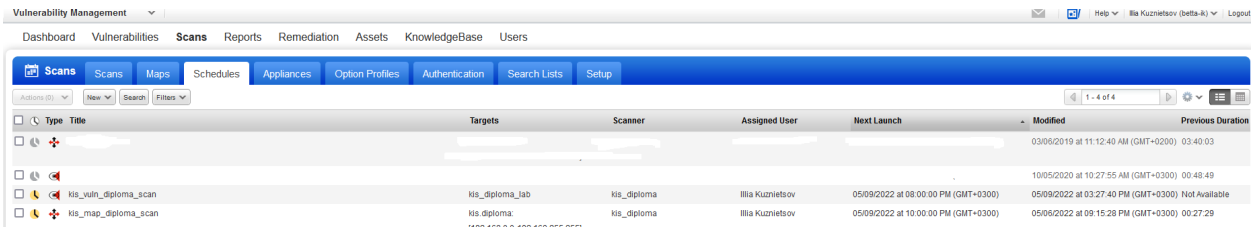


Рисунок 3.21 – Створене заплановане сканування на вразливості

Таким чином були налаштовані регулярні, автентифіковані сканування цільових активів на вразливості.

3.4 Налаштування регулярної генерації звітів на основі зібраної інформації

У Qualys Cloud Platform звіти генеруються на основі певних шаблонів. Шаблони відповідають за те, як і яка інформація у звіті буде відображатись. Шаблони можуть бути створені вручну, або взяті з бази даних Qualys Cloud Platform.

У даному випадку щаблон буде взятий з бази даних Qualys Cloud Platform, його назва – Technical Template і в ньому містяться усі необхідні налаштування для відображення повної картини по знайденим вразливостям.

Для налаштування запланованої, регулярної генерації технічних звітів потрібно перейти у вкладку VM-> Reports -> Schedules, натиснути на кнопку New та обрати Scan Report-Template Based.

Рисунок 3.22 – Створення нового процесу регулярної генерації звітів

З’явиться нове вікно в якому треба дати назву звіту, призначити шаблон, формат в якому буде створено звіт, а також вибрати цільові активи, інформацію яких буде внесено у звіт. Також у пункті Scheduling було вирішено створювати звіти кожен день в 6:00 до початку робого дня, для того щоб інженер відділу

інформаційної безпеки прийшовши зранку на роботу вже мав перед собою готовий технічний звіт.

Заповнюємо необхідну інформацію та запускаємо створення звіту натиснувши на кнопку Schedule.

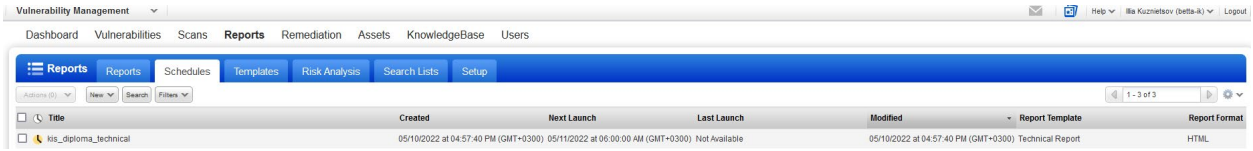


Рисунок 3.23– Створений процес регулярної генерації звітів

Таким чином була налаштована запланована, регулярна геренація технічних звітів.

3.5 Аналіз зібраної інформації про знайдені на активах вразливості. Ідентифікація і ранжуваннння ризиків за допомогою формули розрахунку загального ризику та матриці ризиків. Визначення критичності активів

Аналіз зібраної інформації проводиться після того як технічний звіт згенерувався і можна в зручному вигляді отримати інформацію про знайдені вразливості на цільових активах. Отже, під час автентифікованого сканування на вразливості в цільовій підмережі було виявлено в сумі 176 унікальних, активних вразливостей на цільових активах (Додаток Б).

Таблиця 3.3– Кількість знайдених вразливостей на цільових активах (автентифіковане сканування)

Актив	IP-адреса	Активні вразливості
Metasploitable VM	192.168.100.164	156
Ubuntu VM	192.168.100.168	20

Проте, якщо б було проведене неавтентифіковане сканування на вразливості, то кількість знайдених вразливостей, наприклад на Ubuntu VM, зменшилась на 90% (Додаток Б). Таким чином можна зробити висновок, що проведення саме автентифікованих сканувань на вразливості значно збільшує ефективність процесу управління вразливостями, збільшуючи кількість знайдених критичних вразливостей та зменьшуючи час на знайдення вразливостей.

Для загальної оцінки ризику потрібно перевести відносну cost успішного зламу в оціночний вигляд.

Таблиця 3.4– Оціночний вигляд вартості успішного зламу

Тис. доларів США	Оцінка вартості успішного зламу
0-50	1
50-100	2
100-150	3
150-200	4
>200	5

1) Більшість вразливостей на активі Metasploitable VM мають досить високий рейтинг CVSS. Також усі вразливості зв’язані з різними векторами атаки: помилки в конфігурації, застаріле ПО, словарні паролі, RCE, DoS і т.д. Відносно велика кількість активних вразливостей, загальний високий рейтинг CVSS разом з великою кількістю векторів атак дають надзвичайно високу likelihood успішного зламу цього цільового активу. Проаналізуючи likelihood успішного зламу та cost успішного зламу можна оцінити загальний ризик цільового активу за допомогою формули розрахунку загального ризику та матриці ризиків.

$$\text{Загальний ризик}(Metasploitable\ VM) = 5\ (Likelihood) \times 2\ (Cost)$$
$$= 10\ (\text{Середній ризик})$$

Отже, загальний ризик для активу Metasploitable VM є середнім.

2) Більшість вразливостей на активі Ubuntu VM мають низький, або середній рейтинг CVSS. 95% вразливостей активу зв'язані з застарілою EOL версією ОС. Відносно середня кількість активних вразливостей, загальний середній рейтинг CVSS разом з малою кількістю векторів атак дають середню likelihood успішного зламу цього цільового активу. Проаналізуючи likelihood успішного зламу та cost успішного зламу можна оцінити загальний ризик цільового активу за допомогою формули розрахунку загального ризику та матриці ризиків.

$$\text{Загальний ризик}(Ubuntu\ VM) = 3\ (Likelihood) \times 5\ (Cost) = 15\ (\text{Високий ризик})$$

Отже, загальний ризик для активу Ubuntu VM є високим. У підсумку маємо наступну таблицю:

Таблиця 3.5 – Оцінка загального ризику цільових активів

Актив	IP-адреса	Активні вразливості	Ризик
Metasploitable VM	192.168.100.164	156	Medium
Ubuntu VM	192.168.100.168	20	High

Таким чином оцінка загального ризику допомагає визначитись, що на актив Ubuntu VM потрібно звернути увагу в першу чергу і у нього є найвищий пріорітет в контексті усунення вразливостей, бо у нього найвищий рівень загального ризику. Додатково можна зробити висновок, що загальна кількість вразливостей не впливає на пріорітетність цільового активу.

3.6 Розробка плану дій згідно проаналізованої інформації та з урахуванням критичності цільових активів і виявлених вразливостей

Після аналізу зібраної інформації про знайдені на активах вразливості, розрахунку загального ризику активу, а також визначення критичності активів можна переходити до розробки плану дій.

Так як актив Ubuntu VM є більш критичним, ніж актив Metasploitable VM було прийнято рішення почати розробку плану дій саме з активу Ubuntu VM. Згідно проаналізованої інформації більшість вразливостей на даному активі можна усунути шляхом оновлення операційної системи. Вразливості ж OpenSSH можна усунити шляхом переконфігурації сервісу.

Тепер потрібно вирішити питання: “Діяти? Чи не діяти?”. Для цього потрібно розрахувати відносну оцінки виправлення/невиправлення вразливості та порівняти ці дві оцінки. Розглянемо випадок, коли було прийнято рішення усунути вразливості шляхом оновлення ОС до найновішої версії. В цьому випадку likelihood поганого результату усунення вразливості (збій, несумісність програми тощо) є не дуже значною – 2 бали, а cost поганого результату усунення все ще можна оцінити в 5 балів. Рахуємо відносну оцінку ризику виправлення вразливості за допомогою формули розрахунку ризику і отримуємо 10 балів (середній ризик). З пункту 3.5 знаємо, що відносна оцінка ризику невиправлення вразливості дорівнює 15 балів (високий ризик).

В результаті маємо:

1. Відносна оцінка ризику виправлення вразливості – 10 балів.
2. Відносна оцінка ризику неивиправлення вразливості – 15 балів.
3. $10 < 15$, а отже ризик не вжити заходів є більшим, ніж ризик застосування виправлення, тому вжити заходів буде правильним рішення.

Розрахувавши відносні оцінки виправлення/невиправлення вразливості та порівнявши ці дві оцінки було прийнято рішення оновлювати операційну систему

на активі Ubuntu VM для усунення вразливостей зв’язаних з застарілою версією ОС. Проробивши такі ж самі дії та розрахувавши відносні оцінки виправлення/невиправлення вразливостей зв’язаними з сервісом OpenSSH приймаємо рішення змінити конфігурацію цільового сервісу на більше безпечну, тим самим усуваючи вразливості.

Отже, для того, щоб оновити ОС до останньої версії на активі Ubuntu VM потрібно в командному рядку Terminal виконати команду *sudo apt-get upgrade*. Ця команда використовується для встановлення найновіших версій усіх пакетів, які зараз встановлені в системі. Пакети, встановлені на даний момент з доступними новими версіями, витягуються та оновлюються; за жодних обставин не видаляються в даний момент встановлені пакети або не витягуються та інсталюються ще не встановлені. Нові версії поточних інстальованих пакетів, які не можна оновити без зміни статусу встановлення іншого пакета, залишаться у поточній версії. Після оновлення ОС необхідно потрібно змінити конфігурацію сервісу OpenSSH на більш безпечну, а саме: вимкнути застарілі криптографічні шифри [17] та збільшити розмір публічного ключа SSH серверу [18].

Таким чином був розроблений план дій для усунення вразливостей на активі Ubuntu VM. Даний план дій був розроблений з урахуванням оцінки загальних та відносних ризиків. Оцінка загальних та відносних ризиків в контектсі розробки плану дій допоможе значно збільшити ефективність боротьби з дійсно критичними вразливостями. Для активу Metasploitable VM необхідно провести аналогічні дії.

Висновки до розділу 3

У даному розділі було продемонстровано побудову ефективного процесу управління вразливостями, а саме: налаштування регулярної інвентаризації

цільових активів, логічне групування цільових активів, налаштуваннння регулярного збору інформації про цільові активи, налаштування регулярної генерації звітів, аналіз зібраної інформації та оцінка загального та відносного ризиків, розробка плану дій в контексті боротьби з вразливостями на цільових активах.

ВИСНОВКИ

Метою дипломної роботи було побудувати ефективний процес управління вразливостями.

Проведений аналіз інформаційних джерел показав, що основними проблемами у вже існуючих процесах управління вразливостями
є: відсутність регулярної інвентаризації мережі, відсутність регулярних сканувань на враливості, відсутність метрик ефективності та відсутність розуміння концепції ризиків та їх оцінки. Зазначеним проблемам вище просто не уділяють достатньо уваги, тим самим процес управління вразливостями не є ефективним.

Проаналізовано та визначено зв’язок процесу управління вразливостями з процесом управління ризиками. Також було розглянуто та проаналізовано способи оцінки загального та відносного ризиків. Оцінка ризиків була інтегрована в процес управління вразливостямми для визначення критичності активів та вразливостей. Разом з цим було проаналізовано вплив оцінки ризиків на етапі розробки плану дій. Були розглянуті та проаналізовані методи боротьби з вразливостями. Для оцінки ефективності процесу управління вразливостями були введені метрики ефективності.

Розроблений підхід до побудови процесу управління вразливостями є послідовним, зрілим та насамперед ефективним та легким в оцінці ефективності. Розроблений підхід до побудови ефективного процесу управління вразливостями базується на risk-based підході до процесу управління вразливостями. Розроблений підхід враховує кращі сторони risk-based підходу управління вразливостями, є легкою легкою у побудові та спирається на введені метрики ефективності, також у розробленого підходу немає недоліків застарілого підходу до побудови процесу управління вразливостями.

Процес управління вразливостями, побудований з допомогою розробленого підходу, є на 56.5% ефективнішим за загальний процес управління вразливостями.

На практиці було продемонстровано приклад побудови ефективного процесу управління вразливостями на основі розробленого підходу. Ефективність побудованого процеса управління вразливостями оцінювалась за допомогою введених метрик ефективності.

Розглянута тема потребує подальшого дослідження. Зокрема, можливо більш поглиблено дослідити питання пріорітизації цільових активів та знайдених вразливостей. Також можна проаналізувати можливості автоматизації оцінки ризиків на основі штучного інтелекту.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Positive Technologies: 84 percent of companies have high-risk vulnerabilities on the network perimeter [Електронний ресурс] – 28.10.2020 – Режим доступу до ресурсу: https://www.ptsecurity.com/ww-en/about/news/positive-technologies-84-percent-of-companies-have-high-risk-vulnerabilities-on-the-network-perimeter/

2. 67 Percent of Healthcare Organizations Hit By Ransomware [Електронний ресурс] – 29.09.2021 – Режим доступу до ресурсу: https://www.hcinnovationgroup.com/cybersecurity/data-breaches/news/21240292/survey-22-percent-report-an-increase-in-mortality-rate-due-to-ransomware

3. Vulnerability management [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Vulnerability_management

4. What is Risk Based Vulnerability Management? [Електронний ресурс] – 20.12.2021 – Режим доступу до ресурсу: https://www.crowdstrike.com/cybersecurity-101/risk-based-vulnerability-management/

5. Cyber Risk Management Service [Електронний ресурс] – Режим доступу до ресурсу: https://www.itgovernance.co.uk/cyber-security-risk-management

6. Vulnerability scanner [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Vulnerability_scanner

7. Formula for Calculating Cyber Risk [Електронний ресурс] – 22.01.2021 – Режим доступу до ресурсу: https://stateofsecurity.com/formula-for-calculating-cyber-risk/

8. Risk matrix [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Risk_matrix

9. Vulnerability Remediation | A Step-by-Step Guide [Електронний ресурс] – 30.09.2021 – Режим доступу до ресурсу: https://www.hackerone.com/vulnerability-remediation-step-step-guide

10. Log4Shell: RCE 0-day exploit found in log4j 2, a popular Java logging package [Електронний ресурс] – 19.12.2021 – Режим доступу до ресурсу: https://www.lunasec.io/docs/blog/log4j-zero-day/

11. What is SELinux? [Електронний ресурс] – Режим доступу до ресурсу: https://www.redhat.com/en/topics/linux/what-is-selinux

12. Qualys Cloud Platform [Електронний ресурс] – 30.08.2019 – Режим доступу до ресурсу: https://www.qualys.com/cloud-platform/

13. Fix your vulnerabilities [Електронний ресурс] – Режим доступу до ресурсу: https://docs.snyk.io/features/fixing-and-prioritizing-issues/issue-management/remediate-your-vulnerabilities/

14. Accepting Risk [Електронний ресурс] – 03.10.2021 – Режим доступу до ресурсу: https://www.investopedia.com/terms/a/accepting-risk.asp

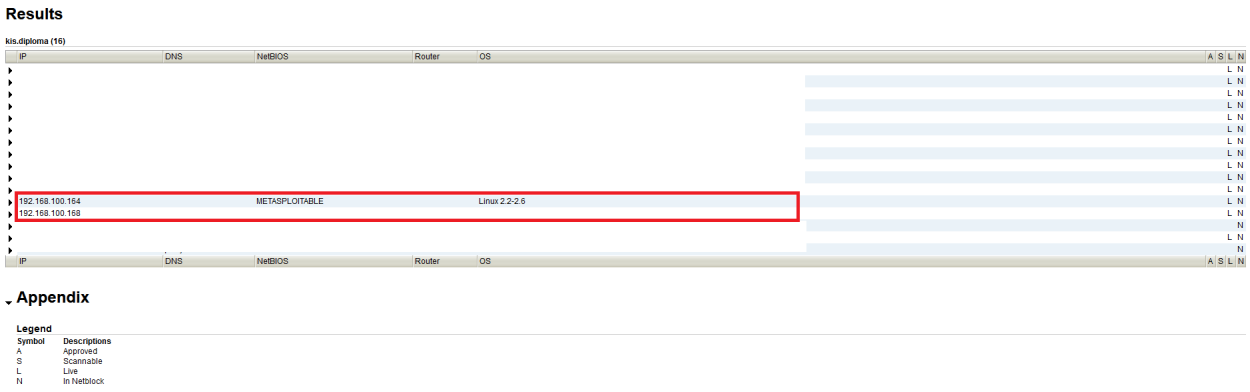
15. Метод аналізу ієрархій як інструмент для прийняття рішень при стратегічному плануванні [Електронний ресурс] – Режим доступу до ресурсу: https://pidru4niki.com/15660721/menedzhment/metod_analizu_iyerarhiy_instrument_dlya_priynyattya_rishen_pri_strategichnomu_planuvanni

16. Virtual Scanner Appliance User Guide [Електронний ресурс] – Режим доступу до ресурсу: https://www.qualys.com/docs/qualys-virtual-scanner-appliance-user-guide.pdf

17. Security of Interactive and Automated Access Management Using Secure Shell (SSH) [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/publications/detail/nistir/7966/final

18. SSH Server Public Key Too Small [Електронний ресурс] – 23.07.2019 – Режим доступу до ресурсу: https://www.linuxminion.com/ssh-server-public-key-too-small/

ДОДАТОК А РЕЗУЛЬТАТИ СКАНУВАННЯ ІНВЕНТАРИЗАЦІЇ



Results

kis.diploma (16)

IP	DNS	NetBIOS	Router	OS	A	S	L	N
							L	N
							L	N
							L	N
							L	N
							L	N
							L	N
							L	N
							L	N
							L	N
							L	N
192.168.100.164		METASPLOITABLE		Linux 2.2-2.6			L	N
192.168.100.168							L	N
								N
							L	N
								N
IP	DNS	NetBIOS	Router	OS	A	S	L	N

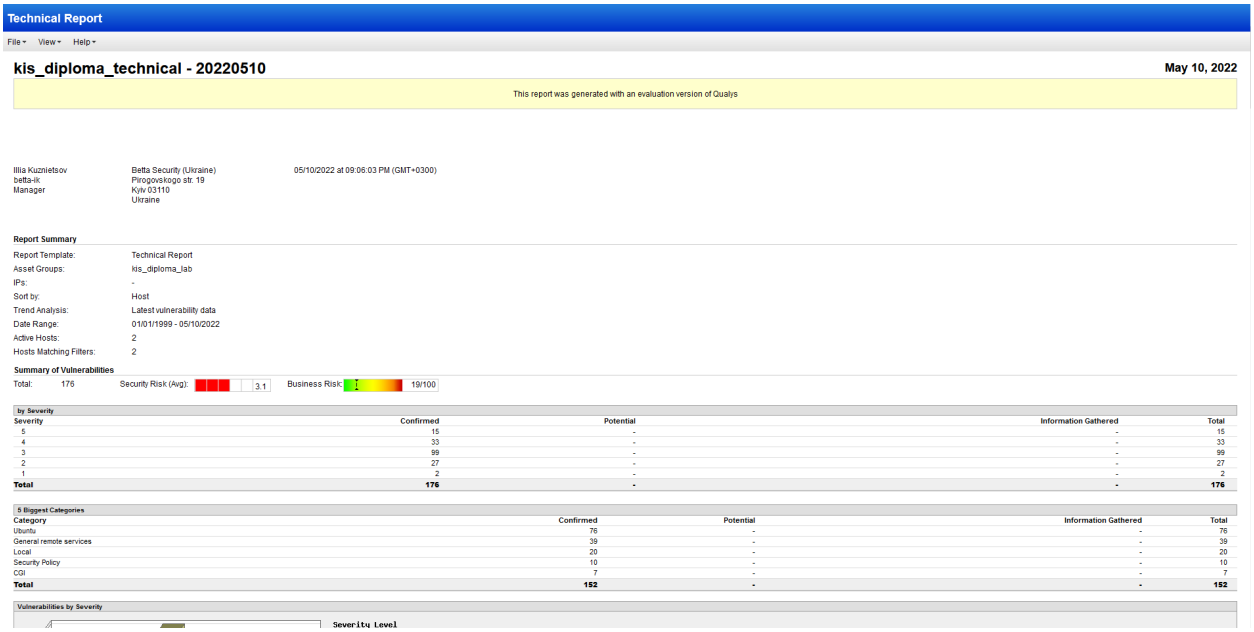
Appendix

Legend

Symbol	Descriptions
A	Approved
S	Scannable
L	Live
N	In Netblock

Рисунок А.1 – Знайдені цільові активи Ubuntu VM та Metasploitable VM

ДОДАТОК Б РЕЗУЛЬТАТИ СКАНУВАННЯ НА ВРАЗЛИВОСТІ



Technical Report

File ▾ View ▾ Help ▾

kis_diploma_technical - 20220510 May 10, 2022

This report was generated with an evaluation version of Qualys

Illia Kuznietsov
betta-ik
Manager

Betta Security (Ukraine)
Pirogovskogo str. 19
Kyiv 03110
Ukraine

05/10/2022 at 09:06:03 PM (GMT+0300)

Report Summary

Report Template:	Technical Report
Asset Groups:	kis_diploma_lab
IPs:	-
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	01/01/1999 - 05/10/2022
Active Hosts:	2
Hosts Matching Filters:	2

Summary of Vulnerabilities

Total: 176 Security Risk (Avg): 3.1 Business Risk: 19/100

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	15	-	-	15
4	33	-	-	33
3	99	-	-	99
2	27	-	-	27
1	2	-	-	2
Total	**176**	**-**	**-**	**176**

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
Ubuntu	76	-	-	76
General remote services	39	-	-	39
Local	20	-	-	20
Security Policy	10	-	-	10
CGI	7	-	-	7
Total	**152**	**-**	**-**	**152**

Vulnerabilities by Severity

Severity Level

Рисунок Б.1 – Загальна інформація

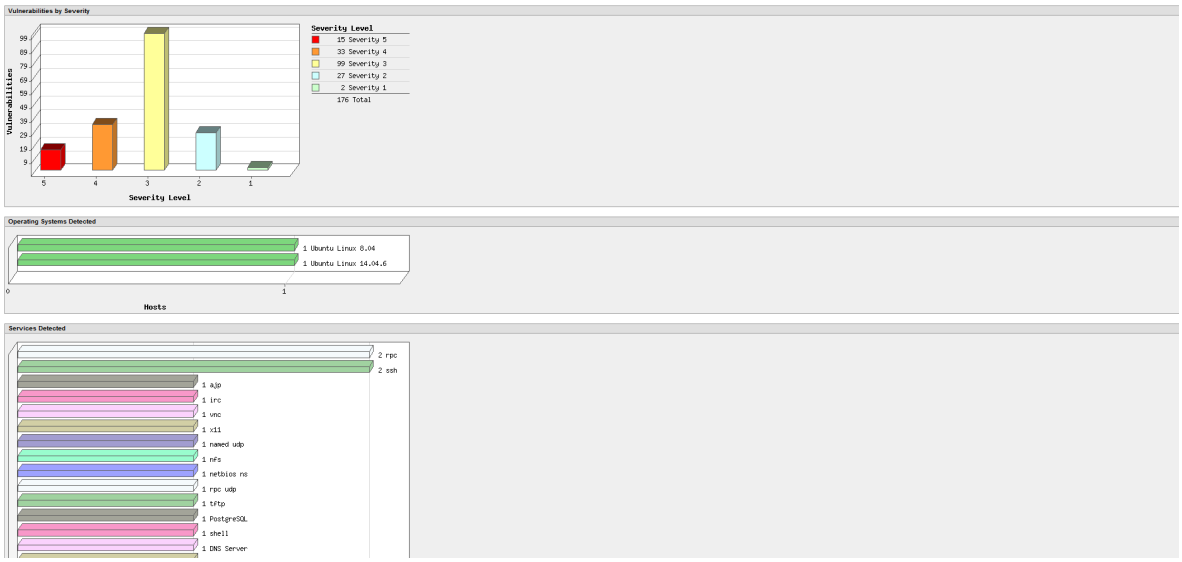


Рисунок Б.2 – Графіки

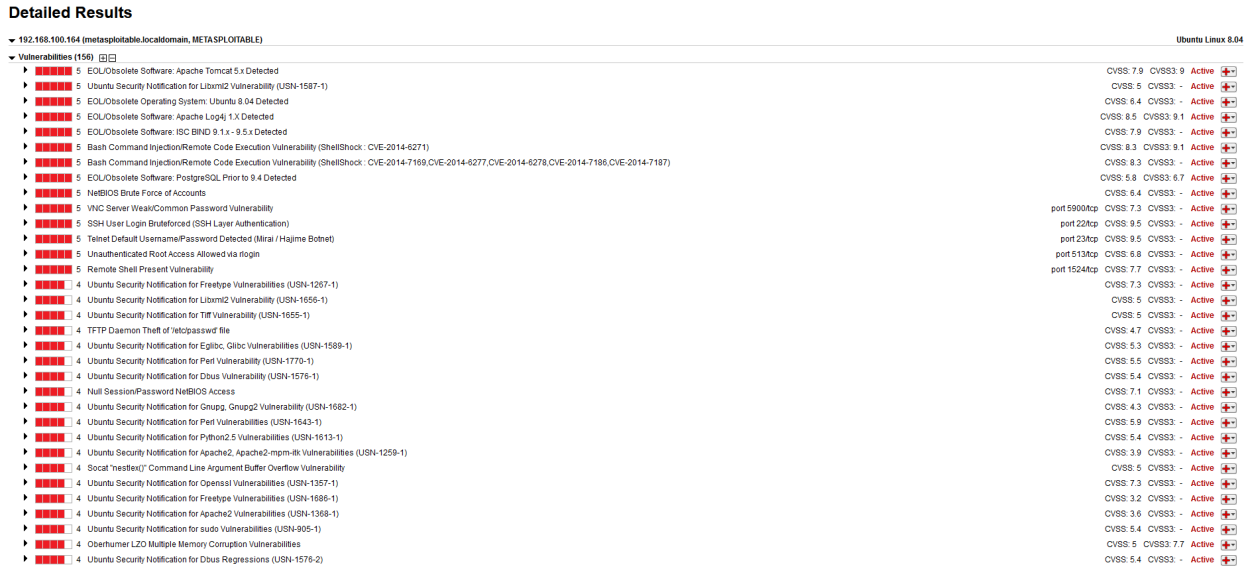


Рисунок Б.3 – Знайдені вразливості на Metasploitable VM

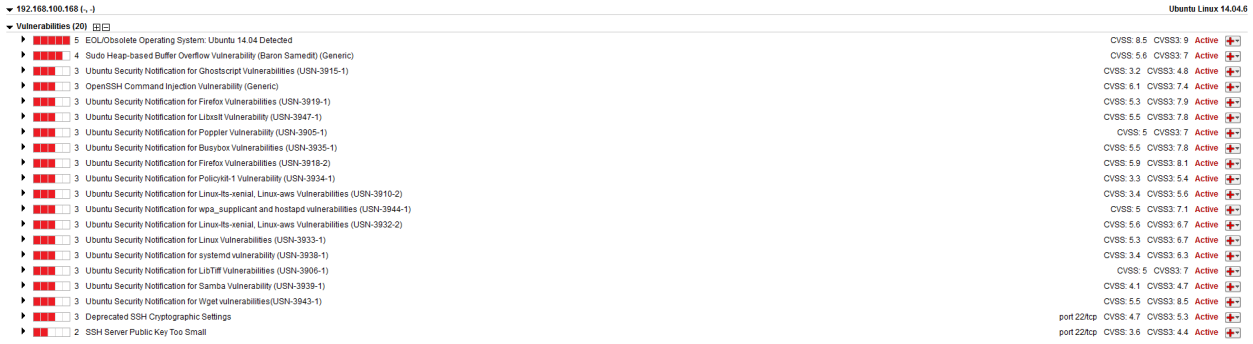


Рисунок Б.4 – Знайдені вразливості на Ubuntu VM (автентифіковане сканування)

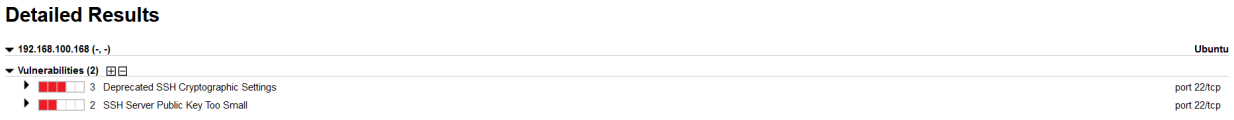


Рисунок Б.5 – Знайдені вразливості на Ubuntu VM (неавтентифіковане сканування)