ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Рєзнік Р.В.
(прізвище та ініціали)
Керівник Марченко В.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2021 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Рєзніку Роману Вікторовичу
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія виявлення вразливостей в корпоративній інформаційній системі»

керівник магістерської роботи Марченко Віталій Вікторович, асистент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «11» жовтня 2021 року №170.

2. Строк подання студентом магістерської роботи 15.12.2021 р.

3. Вихідні дані до магістерської роботи
корпоративна інформаційна система;
програмні комплекси виявлення вразливостей;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми виявлення вразливостей в інформаційних системах.
2. Склад та умови функціонування корпоративної інформаційної системи.
3. Методи та засоби виявлення вразливостей.
4. Варіант технології по виявленню вразливостей в інформаційній системі.
5. Перелік графічного матеріалу
1. Тема магістерської роботи.
2. Об'єкт, предмет, мета та наукові завдання дослідження.

3.

4.

5.

6.

7.

8.

9. Рекомендації

10. Висновки за результатами роботи.

6. Дата видачі завдання 12.10.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми виявлення вразливостей корпоративних інформаційних систем.	12.10.2021 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	02.11.2021 р.	
3.	Аналіз методів та засобів виявлення вразливостей.	12.11.2021 р.	
4.	Розроблення варіанту технології виявлення вразливостей корпоративної інформаційної системи.	24.11.2021 р.	
5.	Розроблення рекомендацій щодо застосування технології виявлення вразливостей корпоративної інформаційної системи.	03.12.2021 р.	
6.	Оформлення результатів дослідження.	10.12.2021 р.	
7.	Підготовка доповіді до захисту.	15.12.2021 р.	

Студент Рєзнік Р.В.
(підпис) прізвище та ініціали

Керівник магістерської роботи Марченко В.В.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента Рєзніка Романа Вікторовича
на тему: «Технологія виявлення вразливостей в корпоративній інформаційній системі»

Актуальність: Використання корпоративних інформаційних систем, що не є перевіреними на відомі вразливості, у рази збільшує ризики несанкціонованого доступу до ресурсів підприємства та порушення працездатності сервісів, що веде до репутаційних, а також фінансових збитків організації. Тому важливо забезпечити надійний та ефективний моніторинг та перевірку систем на наявність вразливостей із застосуванням найсучасніших засобів.

На сьогоднішній день проведення сканування систем засобом Tenable Nessus вважається перспективним напрямком та забезпечує всебічний захист від актуальних вразливостей. Тому тема магістерської роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі було встановлено зміст проблеми виявлення вразливостей та визначено мету та завдання даного процесу, а також його складові частини.
2. Було досліджено методи та засоби виявлення вразливостей на базі Tenable Nessus Essentials.
3. Запропоновано порядок застосування технології виявлення вразливостей на базі Tenable Nessus Essentials.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У магістерській роботі бажано було б провести аналіз процесу виявлення вразливостей на прикладі конкретного підприємства та описати його цілі та умови функціонування.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку **відмінно**, а студентк **Рєзнік Р.В.** – присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ

ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ

ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Рєзнік Р.В. до захисту магістерської роботи
(прізвище та ініціали)

спеціальності 125 Кібербезпека

освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія виявлення вразливостей в корпоративній інформаційній системі».

Магістерська робота і рецензія додаються.

Директор інституту _____ _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Рєзнік Роман Вікторович за період навчання в інституті
(прізвище та ініціали студента)

ННІЗІ з 2020 року по 2022 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту _____ Журенкно О.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент ***Рєзнік Р.В.*** обрав тему роботи, метою якої було методи та засоби виявлення вразливостей в корпоративній інформаційній системі та розробити варіант технології виявлення вразливостей на підприємстві. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Рєзнік Р.В. показав відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.
Все це дозволяє оцінити виконану магістерську роботу студента Рєзніка Романа Вікторовича на оцінку **«відмінно»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека

Керівник магістерської роботи _____ Марченко В.В.
(підпис) (прізвище та ініціали)
“____” _____ 2021 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Рєзнік Р.В.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи: 54 сторінок, 26 рисунків, 17 джерел.

Об'єкт дослідження – процес виявлення вразливостей в корпоративній інформаційній системі.

Предмет дослідження – методи та засоби виявлення вразливостей в корпоративній інформаційній системі.

Мета роботи – виявити особливості та розробити рекомендації щодо процесу виявлення вразливостей в корпоративній інформаційній системі.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації.

В роботі проведено аналіз проблеми процесу виявлення вразливостей в корпоративній інформаційній системі та визначено мету та завдання цього процесу. Проаналізовано існуючі технології рішення виявлення вразливостей в корпоративній інформаційній системі.

Досліджено методи та засоби виявлення вразливостей на прикладі рішення Tenable Nessus Essential. Визначено призначення, основні функції та склад програмного комплексу Tenable Nessus Essential.

На основі досліджень проведених в роботі розроблено варіант технологій виявлення вразливостей корпоративної інформаційної системи та рекомендації щодо застосування її на підприємстві.

Галузь використання – кібербезпека корпоративної інформаційної системи.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ, МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ, СКАНЕРИ

ABSTRACT

Master’s thesis: 54 pages, 26 figures, 17 sources.

Object of research – the process of vulnerability identifying of the corporate information system.

Subject of research – the technology and methods of identifying vulnerabilities in the corporate information system.

The aim of research – to identify features and develop recommendations for the process of identifying vulnerabilities in the corporate information system.

Research methods – elaboration of literature on the topic, analysis of operational documentation.

The paper analyzes the process of vulnerability identifying of the corporate information system and defines the purpose and objectives of the process. The existing technologies of management of vulnerability identifying of the corporate information system are analyzed.

The paper studies methods and tools for vulnerability identifying on the example of Tenable Nessus Essential solution. The purpose, main functions and composition of the Tenable Nessus Essential software package are defined.

Based on the research conducted in the work, a variant of the technology of identifying vulnerabilities of the corporate information system and recommendations for using technology in companies.

Field of use – cybersecurity of corporate information system.

CORPORATE INFORMATION SYSTEM, CYBER SECURITY, VULNERABILITY IDENTIFYING, METHODS AND MEANS OF MANAGEMENT OF VULNERABILITY IDENTIFYING, SCANERS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КІС	–	корпоративна інформаційна система
IT	–	Information Technology
ІС	–	інформаційна система
IP	–	Internet Protocol
СУБД	–	система управління базами даних
ПЗ	–	програмне забезпечення
ОС	–	операційна система
SIEM	–	Security Information and Event Management
SQL	–	Structured Query Language
LDAP	–	Lightweight Directory Access Protocol
CVE	–	Common Vulnerabilities and Exposures
XSS	–	Cross Site Scripting
АРМ	–	автоматизоване робоче місце
CIRT	–	Computer Incident Response Team
OWASP	–	Open Web Application Security Project

ВСТУП

На сьогоднішній день, значна частина життя кожної людини проходить в комп'ютерах, смартфонах та інших девайсах з виходом в інтернет. Це полегшує життя в багатьох його аспектах. Саме це перейняв бізнес та компанії різної величини та бюджету. Вони використовують комп'ютерні мережі для комунікації, передачі інформації, спрощення та автоматизації певних процесів. Але кожна мережа та програма, яка в ній використовується створена людиною, а, отже, не є ідеально, та може мати певні недоліки, які в свою чергу є потенційною небезпекою для бізнесу.

Кожного дня ми зустрічаємо новини, що повідомляють нам про ті чи інші порушення кібербезпеки, такі як перехоплення конфіденційної інформації, шахрайство на інформаційному рівні тощо. І кожна людина відчуває цей вплив.

Саме для забезпечення високого рівня захищеності корпоративних мереж, та з метою підтримування конфіденційності і цілісності інформації повинна регулярно проводитися перевірка вразливості мережі.

На ринку існує багато постачальників, які пропонують рішення, що дозволяють проводити ідентифікацію на такі вразливості. Одним з таких вендорів є Tenable Network Security з продуктом Nessus.

Саме потреба в якісній та комплексній перевірці на вразливості в корпоративній інформаційній системі визначає актуальність даної теми.

Галузь використання: кібербезпека корпоративної інформаційної системи.

Об'єкт дослідження: процес виявлення вразливостей в корпоративній інформаційній системі.

Предмет дослідження: методи та засоби виявлення вразливостей в корпоративній інформаційній системі.

Методи дослідження: опрацювання літератури за даною темою, аналіз експлуатаційної документації.

Мета роботи: виявити особливості та розробити рекомендації щодо процесу виявлення вразливостей в корпоративній інформаційній системі.

Наукові завдання:

проаналізувати існуючі методи та засоби виявлення вразливостей в корпоративній інформаційній системі;

дослідити сучасні інструменти виявлення вразливостей в корпоративній інформаційній системі;

проаналізувати особливості та виявити основні труднощі процесу виявлення вразливостей в корпоративній інформаційній системі;

розробити рекомендації щодо процесу виявлення вразливостей в корпоративній інформаційній системі на базі Tenable Nessus Essential.

Практичне значення одержаних результатів полягає у розробці технології виявлення вразливостей для використання її в корпоративній інформаційній системі.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференція «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2021 року в Державному університеті телекомунікацій, м. Київ.

1 ДОСЛІДЖЕННЯ СУТНОСТІ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Задля забезпечення захищеності та цілісності корпоративної інформаційної системи необхідно постійно слідкувати за її станом, одним із дій є виявлення вразливостей – процес, який дає змогу визначити та зрозуміти слабкі місця у системі, базовій інфраструктурі та основних її додатках. Важливо не плутати поняття ідентифікації вразливостей з управлінням. Оскільки, процес виявлення є тільки однією складовою процесу управління вразливостями, разом з такими як оцінювання, виправлення та звітування.

1.1 Особливості побудови, класифікації, призначення та функції корпоративної інформаційної системи

Корпоративна інформаційна система (КІС) – це інформаційна система, що підтримує автоматизацію функцій управління на підприємстві (корпорації) та постачає інформацію для прийняття управлінських рішень. У ній реалізована управлінська ідеологія, яка об'єднує бізнес-стратегію підприємства і прогресивні інформаційні технології [1].

Корпоративна ІС є інформаційно-керуючою системою, що включає бізнес-архітектуру підприємства, його персонал, ІТ-архітектуру та є діючою частиною кіберкорпорації.

На власному досвіді багато розробників усвідомили, що ефективність автоматизації в першу чергу залежить від того, наскільки широко вона охоплює комплекси розрахунків, проведених в управлінні. Тому останнім часом, стала настільки популярною ідея побудови корпоративних інформаційних систем (КІС) стосовно не тільки великих, територіально розподілених інформаційних систем, але і будь-яких підприємств, незалежно від їх масштабу і форми власності. Організація, маючи сьогодні одну мережу з локальним сервером і десятком

комп'ютерів, завтра може розширитися і представляти із себе саморегулюючу систему, здатну досить гнучко та оперативно перебудовувати принципи і процеси свого функціонування, маючи в своєму активі інтеграцію великого числа програмних продуктів [2].

Основними особливостями корпоративних ІС є:

- комплексність охоплення функцій управління;
- підвищена впорядкованість ділових процесів;
- масовість операцій;
- ефективність використання комп’ютерно-телекомунікаційного устаткування і програмного забезпечення;
- можливість локальної установки та впровадження окремих частин системи;
- адаптивність функціональної та інструментальної структури системи до особливостей керованого об’єкта;
- можливість розвитку системи після її впровадження.

Корпоративні ІС призначені для автоматизації всіх функцій управління фірмою або корпорацією, що має територіальну роз’єднаність між підрозділами, філіями, відділеннями та офісами.

Корпоративна інформаційна система охоплює всі бізнес-функції та всі управлінські процеси корпорації. В умовах великих підприємств і корпорацій вона може бути більш ефективна, оскільки забезпечує взаємодію масових і добре організованих процесів швидкодіючими засобами сучасних інформаційних і телекомунікаційних технологій високого науково-технічного рівня.

Забезпечення розподіленої роботи та віддаленого доступу до документів – це обов’язкова вимога до інформаційних систем корпоративного рівня. Останнім часом невід’ємною складовою частиною цієї вимоги стала підтримка роботи в мережевій архітектурі, а, отже, сучасна корпоративна інформаційна система повинна мати такі основні характеристики як: масштабність, мульти-платформенні обчислювання, робота в неоднорідному обчислювальному середовищі та розподілені обчислення. Масштабна ІС – одна із важливих характеристик

інформаційних систем такого класу, повинна функціонувати на масштабній програмно-апаратній платформі що складається з різних операційних систем, серверів, СУБД і т.д., та потребує значного рівня спеціалістів з проектування й упровадження таких систем. Оскільки варіантів конфігурації базового устаткування і програмного забезпечення може бути багато. Але при цьому, обов'язково, мають бути забезпечені однакові інтерфейс, поведінка на різних платформах та узгоджена підтримка незалежно від платформи та логіка роботи на всіх платформах, інтегрованість з користувацьким операційним середовищем тощо.

Така характеристика, як робота в неоднорідному обчислювальному середовищі є важливою перевагою КІС що полягає в можливості роботи в мережах, до яких входять комп'ютери, що працюють під управлінням різних операційних систем або побудовані на різних обчислювальних платформах. При цьому має бути забезпечена взаємодія всіх робочих обчислювальних платформ і операційних систем, які використовуються.

Один із видів роботи в клієнт-серверній архітектурі – розподілені обчислення, це коли дані чи запити, що надходять з клієнтських машин, розподіляються поміж кількома серверами, що забезпечує кращу пропускну здатність для користувача, що в свою чергу зменшує навантаженість на сервер і дає можливість багатопоточної роботи.

Головними особливостями сучасного підходу до побудови корпоративної інформаційної системи підприємства є [3]:

- всебічний аналіз бізнес-процесів, на основі якого проводиться розробка проекту інформаційної системиі обґрунтування закладених в ньому рішень;
- використання широкої палітри сучасних методологій та інструментальних засобів моделювання та проектування систем;
- підтримка міжкорпоративного бізнесу;
- детальне опрацювання та узгодження з замовником всіх етапів розробки проекту, контрольних точок, необхідних ресурсів.

Такий підхід забезпечує розробку інтегрованих рішень, побудованих на об'єктивних даних про роботу підприємства, своєчасне узгодження всіх принципових питань між замовником, генеральним підрядником та іншими учасниками робіт і направлений на збереження зроблених в систему інвестицій.

Корпоративні інформаційні системи великих компаній регулярно зазнають змін – оновлюється конфігурація обладнання, змінюється топологія мереж, з'являються нові вузли і цілі системи. Для більшості корпорацій з розподіленою інфраструктурою процес безперервного забезпечення комплексного захисту інформаційних активів стає непростим завданням через високу складність архітектури і велику кількості взаємозв’язків всередині окремих підсистем [4].

КІС надає користувачеві можливість вирішення таких глобальних задач:

- зробити прозорим для керівництва корпорацією використання вкладених у бізнес капіталів;
- надати повну інформацію для економічної доцільності стратегічного планування;
- професійно керувати витратами, наочно і своєчасно показувати, за рахунок чого можна мінімізувати витрати;
- реалізувати оперативне управління підприємством згідно вибраних ключових показників (собівартість продукції, структура витрат, рівень прибутковості тощо);
- забезпечити гарантовану прибутковість підприємства за рахунок оптимізації і прискорення ряду процесів (строків виконання нових замовлень, перерозподілу ресурсів і т. д.) [5].

Сучасні підприємства є складними та динамічними системи. Кожна з яких розвивається та включає в себе велику кількість елементів, що реалізують безліч виробничих та управлінських функцій. Такі економічні об'єкти мають мультирівневу структуру, а також велику кількість інформаційних зв’язків на зовнішньому на внутрішньому рівнях. У наш час починають розуміти всю важливість і необхідність саме комплексного підходу до автоматизації інформаційних процесів на підприємствах та організаціях [6].

Розглянемо класифікацію корпоративних інформаційних систем:

1. Локальні ІС – успішно справляються з вирішенням окремих задач на підприємстві, але, як правило, не надають цілісної інформації для автоматизації управління. Перевагою цих систем є порівняно невисока ціна і відносна простота впровадження. Прикладами таких систем є: «1С Бухгалтерія», БОСС, «Інфобухгалтер».

2. Середні інтегровані ІС – призначені для комплексної автоматизації управління підприємствами складної структури, різних напрямків діяльності та форм власності. До цього класу належать системи «1С Підприємство», «AVACO SOFT», «ПАРУС».

3. Великі інтегровані системи – це функціонально найрозвинутіші, найскладніші і найдорожчі системи. В них реалізуються зазвичай стандарти управління рівня MRPII та ERP. Цей вид систем представлений на нашому ринку продуктами фірм SAP, ORACLE, BAAN, PeopleSoft.

Іншими словами, корпоративна інформаційна система – це цілісний апаратно-програмний комплекс, що дозволяє задовольнити як оперативні, так і стратегічні потреби підприємства в опрацюванні даних. Як висновок, вибір конкретної КІС для впровадження є складним завданням через їх високу вартість та різноманітність, тривалий час впровадження та складну підготовку спеціалістів для обслуговування таких систем.

1.2 Аналіз проблеми виявлення вразливостей в корпоративній інформаційній системі

Кожна країна з появою комп’ютера, який революційно змінив усі засоби і технології комунікації, досить важко і невпевнено почала контролювати функціонування інформаційного контенту на своєму інформаційно-комунікаційному полі. В різних формах всі почали запозичувати досвід один одного, особливо при створенні власних баз даних комп’ютерної інформації, різноманітних віртуальних інформаційних продуктів, витісняючи чужі на

периферію й захищаючи власні інтереси в інформаційно-комунікаційній сфері, такий досвід перекинувся і на корпоративні інформаційні системи.

Основним завданням фахівців у сфері захисту комп'ютерної інформації є убезпечення її від несанкціонованого доступу, модифікації або знищення даних що передаються та зберігаються. В інформаційних системах сьогодні сконцентрована величезна кількість відомостей про різні сфери діяльності. У зв'язку з цим одним з основних питань ефективного функціонування інформаційних систем є захист комп'ютерної інформації, що зберігається в них.

Таким чином, проблеми інформаційно-комунікаційної безпеки починають посідати одне з ключових місць у системі забезпечення реалізації всіх політико-правових проблем, стають життєво важливими при реалізації інтересів усіх без винятку осіб, країн та корпорацій. Вони стають ключовою організаційно-управлінською та регулятивно-контрольною функцією в діях всіх структур, оскільки порушення нормального функціонування інформаційних та телекомунікаційних систем становлять собою серйозну небезпеку, що обумовлює нагальну потребу створення нових, більш досконалих адміністративно-правових норм інформаційно-комунікаційної діяльності.

Аналіз ситуації, що склалася, дозволяє говорити про захист інформації в двох аспектах: в широкому сенсі – про захист інформації як відомостей (повідомлень, даних) незалежно від форми їх подання й у вузькому сенсі – про захист інформації, яка міститься в інформаційних системах – комп'ютерної інформації [7].

Локальна обчислювальна мережа є основою функціонування будь-якої КІС. До найбільш поширених загроз інформаційної безпеки даного типу мереж належать:

- недоліки захисту службових протоколів, що призводять до перенаправлення трафіку і перехоплення інформації про конфігурацію мережі;
- словникові паролі;
- недостатній рівень захисту привілейованих облікових записів;
- зберігання важливої інформації у відкритому вигляді;
- недоліки захисту протоколів NBNS і LLMNR;

- недостатньо ефективна реалізація антивірусного захисту;
- використання слабких алгоритмів шифрування при зберіганні паролів;
- вразливі версії програмного забезпечення;
- надлишкові привілеї додатків або СУБД;
- використання відкритих (незахищених) протоколів передачі даних.

Також не треба недооцінювати вразливості на мережевому рівні (Рис. 1.1.).

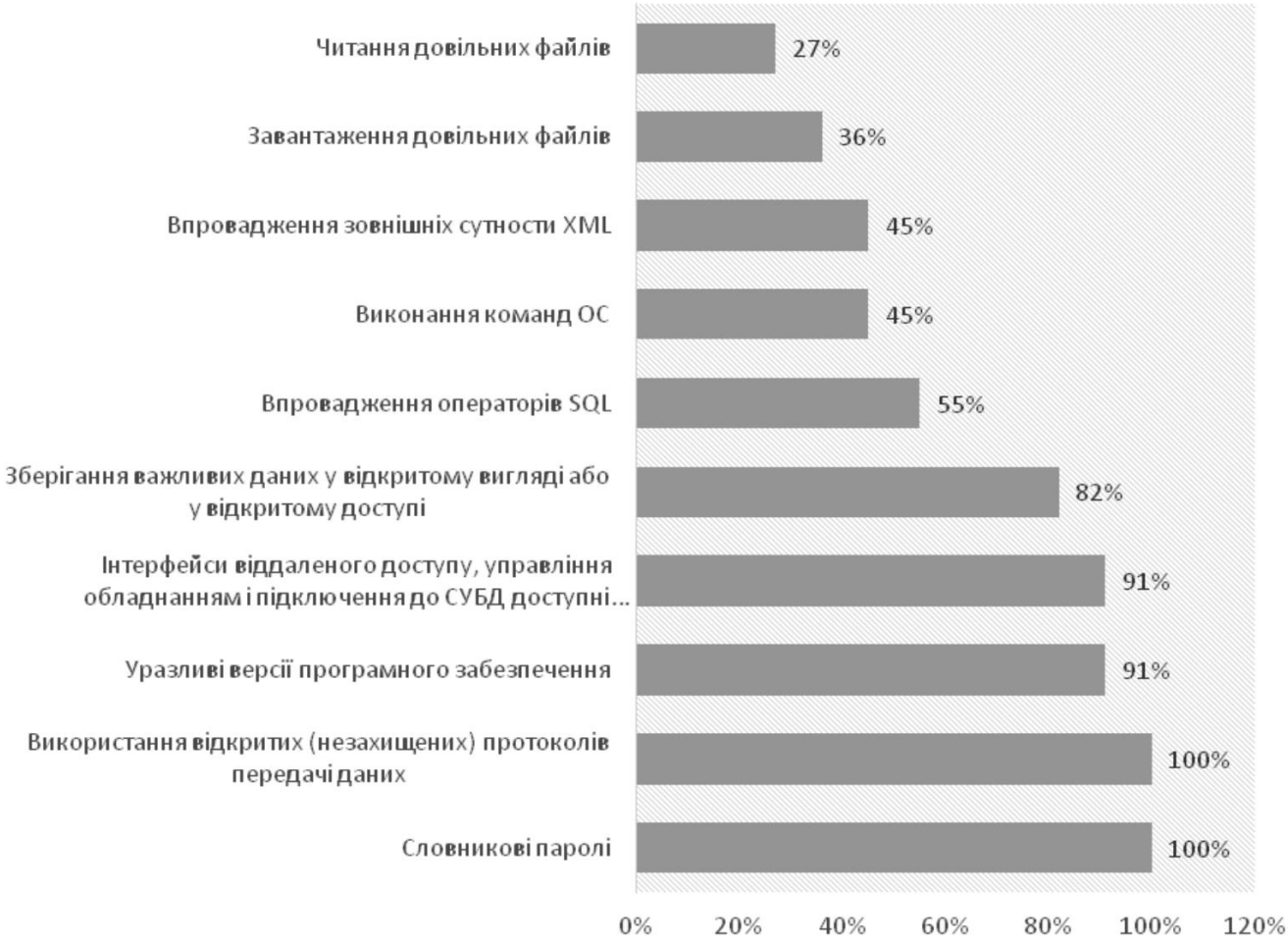

Рис. 1.1. Найбільш поширені вразливості на мережевому периметрі за даними аналітики компанії Positive Technologies 2017 рік [7]

За результатами звітів компаній [8], діяльністю яких є аналіз та захист інформаційної безпеки підприємств, перше місце в рейтингу найбільш поширених вразливостей захисту внутрішніх ресурсів належить недолікам захисту протоколів мережевого і канального рівнів, що призводить до перенаправлення трафіку і перехоплення інформації про конфігурацію мережі. Кожна досліджувана система

містила різні недоліки захисту службових протоколів, таких як ARP, STP, BOOTP, CDP. У кожному з проектів, де проводився аналіз мережевого трафіку локально обчислювальної мережі, було виявлено відсутність механізмів захисту від атак ARP Cache Poisoning. Даний недолік може бути використаний для прослуховування трафіку в мережі і проведення атак типу «людина посередині» [4].

В ході успішної реалізації атаки порушник може перехоплювати конфіденційну інформацію, змінювати дані в процесі передачі і блокувати мережеву взаємодію.

На другому місці серед вразливостей внутрішніх мереж знаходиться використання словникових паролів.

Третє місце – недостатній рівень захисту привілейованих облікових записів. Таким чином, можна зробити наступні висновки: сучасні корпоративні інформаційні системи мають велику кількість вразливостей з боку зовнішніх і внутрішніх зловмисників, а реалізація їх атак не вимагає серйозної кваліфікації. Досить низьким є рівень захищеності бездротових мереж і рівень обізнаності користувачів в питаннях інформаційної безпеки.

Необхідно також відзначити, що вектори атак на корпоративні інфраструктури ґрунтуються на експлуатації поширених вразливостей і недоліків, для усунення яких, як правило, досить застосувати базові принципи забезпечення інформаційної безпеки:

- використовувати сувору парольний політику;
- захищати привілейовані облікові записи;
- не зберігати конфіденційну інформацію у відкритому вигляді або у відкритому доступі;
- обмежити число доступних для підключення на мережевому периметрі інтерфейсів мережевих служб;
- захищати або відключати в локальної обчислювальної мережі протоколи канального або мережевого рівня, які не використовуються та розділяти мережу на сегменти;

- мінімізувати привілеї користувачів і служб;
- регулярно оновлювати ПЗ і встановлювати оновлення безпеки ОС;
- для своєчасного виявлення атак використовувати SIEM-системи;
- для захисту веб-додатків використовувати web application firewalls;
- проводити регулярні тренінги, спрямовані на підвищення обізнаності користувачів в питаннях інформаційної безпеки (при цьому важливо проводити і оцінку ефективності таких тренінгів);
- для захисту від поширення шкідливого ПЗ із застосуванням соціальної інженерії використовувати спеціалізовані антивірусні рішення;
- регулярно проводити тестування на проникнення для своєчасного виявлення нових векторів атак і перевірки вжитих заходів захисту на практиці.

При цьому важливо забезпечити всі ці заходи в комплексі, тільки тоді захист буде ефективним, а витрати на різні дорогі рішення виявляться виправданими.

Вплив порушення безпеки завжди є досить високим, та несе за собою фінансові та репутаційні збитки. Закон щодо захисту персональних даних змушує менеджерів діяти, щоб зменшити вплив або ймовірність цього ризику безпеки. І те, що IT-менеджери або вище керівництво знають, що інформаційні системи та програми мають вразливості, і не роблять нічого, щоб запобігти ризикам – розглядається як проступок в більшості законодавств.

Нижче наведено найбільш критичні виявлені та підтвердженні вразливості за версією Edgescan SaaS у 2020 році (Рис. 1.2.) [8]:

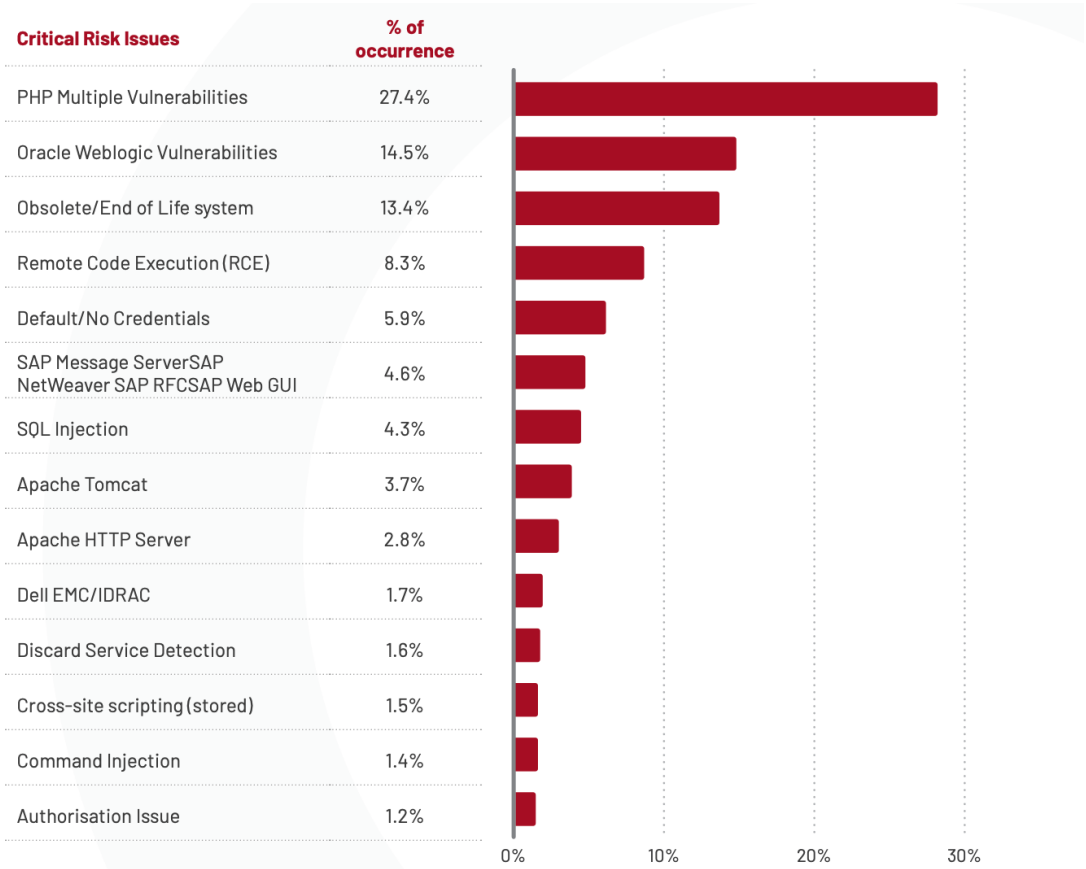

Рис. 1.2. Виявлені та підтвердженні вразливості за версією Edgescan SaaS 2020 рік [8]

Однією з головних концепцій забезпечення інформаційної безпеки є принцип комплексного захисту: тобто створення багатошарової системи захисту, яка може як виявляти атаку та можливі вразливості та і вичислити агентів загроз і переслідувати їх. Системи виявлення вразливостей є прикладом класу систем, що використовуються для попередження таких атак.

1.3 Мета і завдання виявлення вразливостей в корпоративній інформаційній системі

Вразливість – це недолік, який може призвести до порушення конфіденційності, цілісності або доступності інформаційної системи. Ідентифікація вразливостей включає процес виявлення вразливостей та документування їх у інвентаризації в цільовому середовищі.

Вразливість виникає через допущення помилок програмування, проектування систем, а також через слабкі паролі, необізнаність користувачів ІС тощо.

Процес виявлення вразливостей розглядається як превентивний захід для зниження ризиків, пов’язаних з інформаційною безпекою, за рахунок виявлення та аналізу проблем в мережевій та інших інфраструктурах корпоративної інформаційної системи.

Основні завдання процесу [9]:

- виявлення ризиків для безпеки;
- ідентифікація та звіт про налаштування безпеки мережі;
- виявлення некерованих пристроїв і додатків всередині корпоративної мережі;
- створення звітів на предмет відповідності стандартам ІБ.

Ризик безпеки зазвичай неправильно класифікується як вразливість. Використання вразливості з ідентичним значенням ризику може викликати плутанину. Проблема полягає в тому, що можливий серйозний вплив в результаті використання вразливості в той час, як є вразливості без ризику, наприклад, коли актив, який постраждав, не має цінності.

Вчасне виявлення вразливостей дозволяє співробітникам з інформаційної безпеки підприємства швидко застосовувати послідовний, комплексний та чіткий підхід до вирішення загроз та ризиків безпеці. Це дозволить організації захиститися від злому даних та несанкціонованого доступу, забезпечити відповідність вимогам кібербезпеки та нормативним вимогам.

Цінність для бізнесу:

- підвищення загального рівня безпеки корпоративної мережі;
- зниження ймовірності кібератак;
- відповідність стандартам ISO 27001, PCI-DSS.

Важливо розуміти, що виявлення вразливостей – це процес, який потрібно виконувати періодично, оскільки робиться зріз тільки на один момент часу, а корпоративна інформаційна система постійно зазнає оновлення та змін.

Основним способом виявлення вразливостей є сканування вразливостей, а ефективність сканера залежить від двох речей:

- здатність спеціального програмного забезпечення знаходити та ідентифікувати пристрої, програмне забезпечення та відкриті порти, а також збирати іншу системну інформацію;

- можливість співвідносити цю інформацію з відомою інформацією про вразливості з однієї або кількох баз даних про вразливості.

Коли вразливості залишаються невизначеними, зловмисники можуть використовувати їх, щоб пошкодити програми, виконувати заборонені дії в КІС або створити умови для подальших порушень. Зловмисники маніпулюють вразливими місцями, щоб вилучити конфіденційні та власні дані, які є життєво важливими для ділової діяльності та професійної репутації підприємства.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Комп'ютерні системи та мережі досягли більш високого рівня складності, ніж коли-небудь. На сьогоднішній день середньостатистичний сервер зазвичай може виконувати сотні процесів. Кожен з цих процесів є комп'ютерною програмою або скриптом, деякі з них є досить великими та складаються з тисяч рядків вихідного коду. І в межах цього коду, можливо, є всілякі несподівані речі. Наприклад, розробник може додати деяку функцію бекдора, щоб полегшити налагодження програми. І пізніше ця функція може потрапити в кінцеву версію та викликати деякі проблеми з безпекою додатку і всієї мережі підприємства. Також можуть бути деякі помилки у перевірці вхідних даних, які призведуть до несподіваних і небажаних результатів при певних обставинах.

Будь-яка з помилок, може бути використана, щоб спробувати отримати доступ до систем і даних. Існує величезна спільнота людей, які не мають нічого кращого, ніж знайти ці отвори в безпеці і використовувати їх для атаки на ваші системи у власних цілях. Вразливості – це те, що називається цими отворами. Якщо їх залишити без нагляду, зловмисники можуть використовувати вразливості для доступу до вашої мережі – або, можливо, гірше – до даних вашого клієнта, або іншим чином завдати шкоди, наприклад, зробити систему непридатною для використання.

2.1 Аналіз механізмів роботи засобів виявлення вразливостей в КІС

Засоби виявлення вразливостей сканують мережу або систему на наявність слабких місць та вразливостей безпеки, які можуть бути використані зловмисником. Процес сканування вразливості – має одну основну функцію – виявлення вразливостей у системах, пристроях, обладнанні та програмному

забезпеченні. Інструменти називаються сканерами, оскільки вони, як правило, сканують ваше обладнання для пошуку відомих вразливостей.

Засіб виявлення вразливостей комплексно перевіряє кожен аспект вашої системи. Після завершення сканування інструмент повідомляє про всі виявлені проблеми та пропонує подальші дії задля забезпечення безпеки. Більш повнофункціональні інструменти можуть дати уявлення про безпеку та оперативний вплив усунення ризику, а не просто його визначення. Дані сканування вразливостей також можуть бути інтегровані в SIEM разом з іншими даними для ще більш цілісної аналітики загроз на підприємстві.

Різні інструменти сканування вразливостей шукають різні вразливості. Наприклад, сканери вразливості мережі сканують корпоративні мережі, щоб знайти вразливі та невідомі системи – сервери, пристрої, кінцеві точки та порти на них, які потенційний зловмисник міг би використати. З іншого боку, сканери вразливості веб-додатків шукають вразливості та загальні недоліки веб-сайтів та веб-додатків. До них належать:

- міжсайтові сценарії (XSS);
- SQL-ін'єкція;
- командна ін`єкція;
- обхід шляху;
- атака «людина посередині» (MITM);
- шкідливий код (зловмисне програмне забезпечення).

Ці сканери в основному шукають вразливості програмного забезпечення, недоліки кодування та неправильні конфігурації у веб-додатках. Як правило, вони працюють на основі відомого списку поширених експлойтів, наприклад, OWASP Top 10.

Функціонувати такі засоби можуть на мережевому рівні (network-based), рівні операційної системи (host-based) і рівні додатку (application-based). Найбільшого поширення набули засоби аналізу захищеності мережевих сервісів і протоколів. Пов’язано це, в першу чергу, з універсальністю використовуваних протоколів. Крім виявлення вразливостей, за допомогою засобів аналізу

захищеності можна швидко визначити всі вузли корпоративної мережі, доступні в момент проведення тестування, виявити всі використовувані в ній сервіси та протоколи, їх налаштування і можливості для несанкціонованого впливу (як зсередини корпоративної мережі, так і зовні). Також ці засоби виробляють рекомендації і покрокові заходи, що дозволяють усунути виявлені недоліки. [10].

Загалом існує два основних механізми виявлення вразливостей:

- сканування (scan);
- зондування (probe).

Різниця полягає в тому, що сканування є методом пасивного аналізу системи на вразливості без фактичних їх підтверджень (за не прямим ознаками). Такий метод є простішим та швидшим у реалізації. В той час зондування – це метод активного аналізу, під час якого можна достовірно переконатися в наявності вразливості в системі, цей метод виконується шляхом імітації атаки.

Сканування включає в себе такі відомі методи як перевірка заголовків (banner check), активні зондуючі перевірки (active probing check). В свою чергу зондування має метод імітація атак (exploit check).

Після того, як інструменти перевірили можливі вразливості в доступних пристроях, сканер створює звіт. Результати звіту потім можна проаналізувати та інтерпретувати, щоб визначити можливості для покращення безпеки організації.

Існують різні автентичні джерела задокументованих вразливостей, зокрема такі як бази даних, повідомлення постачальників ПЗ, списки та бюлетені CIRT.

Бази даних – такі бази даних містять різну інформацію про вразливості. Наприклад, інформація може включати посилання на контрольний список безпеки, недоліки програмного забезпечення, пов’язані з безпекою, неправильні конфігурації, назви продуктів та показники впливу. Нижче наведено кілька прикладів:

- NVD від NIST – це сховище, яким керує уряд США;
- OWASP – керує списком вразливостей у проекті, відомому як OWASP Top 10. Тут вразливості класифікуються на основі їх частоти атак. Список

оновлюється лише тоді, коли OWASP вирішить, що це необхідно, причому між оновленнями часто проходить кілька років;

- база даних експлойтів – ця база даних керується Offensive Security.

Повідомлення постачальників ПЗ – постачальники програмного забезпечення можуть видавати рекомендації щодо того, як боротися з вразливими місцями безпеки, застосовуючи виправлення, які усувають ці проблеми безпеки. Microsoft, Adobe, VMware – типові постачальники ПЗ, які використовують такий підхід.

Різні засоби сканування виявляють вразливості на різних рівнях корпоративної інформаційної системи. Деякі, з різних типів інструментів виявлення вразливостей, включають наступне [11]:

1. Сканування на основі мережі – використовуються для виявлення можливих атак на безпеку мережі. Цей тип сканування також може виявити вразливі системи в дротових або бездротових мережах.

2. Сканування на основі хостів – використовуються для пошуку та ідентифікації вразливостей на серверах, робочих станціях або інших мережевих хостах. Цей тип сканування зазвичай перевіряє порти та служби, які також можуть бути видимі для мережевого сканування.

3. Сканування бездротових мереж Wi-Fi мереж організації зазвичай фокусуються на точках атаки в інфраструктурі бездротової мережі. Крім виявлення вразливостей на точці доступу, сканування бездротової мережі також може підтвердити, що мережа компанії безпечно налаштована.

4. Сканування бази даних може виявити слабкі місця в базі даних, щоб запобігти зловмисним атакам, наприклад, атаки ін'єкції SQL.

Щоб виявити вразливі місця, їх потрібно точно нанести на карту сканування. Існують списки вразливостей, які полегшують це. Список вразливостей – це документований перелік поширених вразливостей. Задокументованим вразливостям зазвичай присвоюється ідентифікаційний номер, опис і загальнодоступні посилання.

Списки та бюлетені CIRT – це групи, які обробляють події, які передбачають порушення безпеки:

- US-CERT – це національний радник США з питань ризику. Вони відповідають за надання знань та консультацій щодо кібербезпеки, щоб забезпечити краще управління ризиками для організацій;
- SANS CIS Critical Security Controls – надає засоби контролю безпеки, які допомагають запобігти найбільш поширеним кібератакам сьогодні;
- SANS Internet Storm Center – це бюлетень з безпеки, у якому часто обговорюються теми, пов’язані з безпекою, особливо ті, які зараз популярні.

Як досягається ідентифікація вразливості? Щоб правильно ідентифікувати та класифікувати вразливість, необхідно врахувати ряд міркувань. Перш за все, виконується сканування, потім, після завершення, вразливості видають ідентифікатори, такі як номери CVE, EDB-ID та рекомендації постачальника. Ці ідентифікатори в поєднанні з оцінкою CVSS вразливості можна використовувати для обчислення рейтингу ризику.

Інструменти ідентифікації зазвичай розглядають рейтинг ризику сканування, для того щоб зрозуміти положення безпеки середовища. Однак результати зазвичай є загальними та можуть відрізнятися, як показано нижче:

1. True positives: це підтверджує, що виявлено вразливість.
2. False positives: навіть якщо вразливість знайдено, проблема не є справжнім ризиком.
3. True negatives: у цьому випадку вразливість не знайдено, оскільки підпис не збігається.
4. False negatives: у цьому випадку підпис не збігається, однак вразливість існує.

Оскільки універсально визначеного рейтингу ризику не існує, більшість фахівців з інформаційної безпеки рекомендує використовувати спеціальну публікацію NIST 800-30 як основу для оцінки рейтингів ризику. NIST розглядає справжній ризик вразливості як комбінацію ймовірності її виникнення та потенційного впливу [12].

Незважаючи на те, що вразливості можуть бути ідентифіковані та класифіковані, як показано вище, організації та підприємства можуть прийняти такий ризик і дати згоду на роботу систем із ідентифікованими вразливими місцями. Це може бути нормально з багатьох причин, включаючи відсутність бюджету для оновлення систем, які потребують дорогого оновлення.

Без ідентифікації вразливостей неможливо було б визначити, які вразливості існують у мережі, та наскільки їх багато. Дуже важливо розуміти, що у вашій мережі може існувати вразливість, і ще важливіше – яка саме.

Сканування вразливостей – це лише частина виявлення вразливості, інші процеси, такі як тестування на проникнення, можуть виявити різні типи загроз для IT у вашій інформаційній системі. Тестування на проникнення доповнює сканування вразливостей і корисне для визначення того, чи можна вжити заходів щодо вразливості, а також чи спричинить ця дія пошкодження, втрату даних чи інші проблеми. Сканування вразливостей, як доповнення до тестування на проникнення використовується для оцінки, що допомагає виявити ці слабкі місця в корпоративній мережі.

2.2 Penetration testing як спосіб виявлення вразливостей

Тестування на вразливості є досить важливим і необхідним для того, щоб знати ризики, з якими постійно працює ваша корпоративна мережа. Щоб мати реальне уявлення про небезпеку, яким піддається ваша організація, існують певні інструменти, які необхідно розглянути і оцінити по їх можливостям. У протилежному випадку ми можемо недооцінити слабкі місця в безпеці, які можуть поставити під загрозу корпоративну інформаційну мережу.

Мета тестування на проникнення – визначити, наскільки мережа стійка до атаки. У ньому беруть участь авторизовані користувачі – іноді зовнішня сторона або організація – які досліджують мережу на наявність потенційних слабких місць і намагаються їх використати. Також доступне програмне забезпечення, яке дозволяє мережевим менеджерам самостійно тестувати стійкість мережі.

Окрім надання програмних систем тестування ручок, деякі фірми, які займаються тестуванням на проникнення, також перевіряють фізичну безпеку. Деякі постачальники навіть мають вантажівки та уніформу, що нагадують відомі служби доставки посилок. Всього через кілька хвилин тестувальники можуть адресувати, наприклад, посилки ключовому персоналу компанії. Коли кур'єр підходить до входу в заклад з повними руками, охоронці іноді залишають свої місця або відкривають двері для тестувальника. Запит на доступ до ванної кімнати майже завжди задовольняється. Тестувальник може знайти час, щоб встановити невеликий пристрій, щоб зламати Wi-Fi, або залишити USB-пристрій в надії, що хтось підключить його до ПК або ноутбука. Залишені пакети також можуть містити пристрої, які одержувачі можуть підключати, наприклад USB-ключі та рамки для фотографій із підтримкою Wi-Fi.

Виявлення вразливості та тестування на проникнення – в чому ж різниця? Ідентифікація вразливості часто включає компонент тестування на проникнення для виявлення вразливостей персоналу, процедур або процесів організації. Ці вразливості зазвичай не можна виявити під час сканування мережі або системи. Цей процес іноді називають оцінкою вразливості, тестуванням на проникнення або VAPT.

Однак тестування на проникнення недостатньо як повної оцінки вразливості і це існує, по суті, окремим процесом. Ідентифікація вразливості має на меті виявити вразливі місця в мережі та рекомендувати відповідні зміни чи виправлення задля зменшення або усунення знайдених ризиків.

Оцінка вразливості використовує автоматизовані інструменти сканування безпеки мережі. Результати наводяться у звіті про оцінку вразливостей, який зосереджується на наданні підприємствам переліку вразливостей, які необхідно виправити. Однак це робиться без оцінки конкретних цілей або сценаріїв атаки.

Залежно від цілей ручного тесту організація надає тестувальникам різний рівень інформації про цільову систему або доступ до неї. У деяких випадках команда тестування встановлює один підхід на початку і дотримується його. В інших випадках команда тестувальників розвиває свою стратегію, оскільки їхня

обізнаність про систему збільшується під час ручного тесту. У галузі інформаційної безпеки визначено три типи тестування на проникнення:

1. Чорна скринька. Команда нічого не знає про внутрішню структуру цільової системи. Вони діють так само, як хакери, вишукуючи будь-які зовнішні недоліки, які можна використовувати ззовні.

2. Сіра скринька. Команда має певні знання про один або кілька наборів облікових даних. Вони також знають про внутрішні структури даних, код і алгоритми цілі. Тестери можуть створювати тестові випадки на основі детальних проектних документів, таких як архітектурні схеми цільової системи.

3. Біла скринька. Для тестування білої скриньки тестувальники мають доступ до систем і системних артефактів: вихідного коду, двійкових файлів, контейнерів, а іноді навіть до серверів, на яких працює система. Підходи до білої скриньки забезпечують найвищий рівень гарантії за найнижчий проміжок часу.

Після цього необхідно вибрати один із різних методів пентестинга. Вибір буде обумовлений характеристиками системи, або, навіть діяти відповідно до зовнішніх вимог компанії. У будь-якому випадку доступні методи включають ISSAF, PCI, PTF, PTES, OWASP та OSSTMM. У кожного методу достатньо багато своїх нюансів, і їх глибоке знання необхідно при реалізації пентестів.

То ж який метод обрати? За оцінками ряду експертів, досить хорошими типами пентестів є PTES і OWASP, завдяки тому, як ці методи структуровані. За словами експертів з інформаційної безпеки, Penetration Testing Execution Standard (або PTES) прийнято багатьма авторитетними спеціалістами, та в той же час є моделлю, що використовується в навчальних посібниках для таких систем пентестинга, як, наприклад, Rapid7 Metasploit [13].

З іншого боку, Open Source Security Testing Methodology Manual (OSSTMM) став також стандартом. Хоча ці тести не є особливо новаторськими, вони є одними із передових підходів до універсальної структури концепції безпеки. Сьогодні він став орієнтиром не тільки для організацій, які хочуть розробляти якісний, організований та ефективний пентестинг, але й для цілого ряду компаній.

Як альтернатива, Information Systems Security Assessment Framework (ISSAF) організовує дані навколо таких званих «критеріїв оцінки», кожен з яких був складений та розглянутими експертами в кожній сфері застосування рішень безпеки.

В свою чергу, Payment Card Industry Data Security Standard (PCI DSS) був розроблений радою провідних компаній-емітентів кредитних і дебетових карт та служить у якості посібника для організацій, які обробляють, зберігають і передають дані про власників карт. Саме під цим стандартом був розроблений PCI-пентестинг.

Тестування на проникнення можна виконувати вручну або автоматизувати. Тестування за допомогою автоматизованих інструментів оптимізує ресурси, автоматизуючи елементи процесу тесту, тому ідентифікацію вразливостей можна виконувати безперервно та без втручання фахівця з інформаційної безпеки мережі. Завдяки великій кількості гнучких частин, автоматизовані інструменти тестування економлять час і зазвичай дають кращі результати тесту на проникнення, ніж ручні спроби.

Як описувалося раніше, тестери мають на меті імітувати атаки, що здійснюються вмотивованими супротивниками-шахраями. Для цього вони зазвичай дотримуються плану, який включає наступні кроки.

Розвідка – перший крок що має на меті збирання якомога більше інформації про ціль з публічних і приватних джерел, щоб побудувати стратегію атаки. Джерела включають пошуки в Інтернеті, пошук інформації про реєстрацію домену, соціальну інженерію, ненав’язливе сканування мережі. Ця інформація допомагає тестеру визначити поверхню цілі та можливі вразливі місця. Розвідка може змінюватися в залежності від масштабу та цілей тесту, і може бути такою ж простою, як телефонний дзвінок, щоб ознайомитися з функціональними можливостями системи.

Наступний крок – це сканування. Тестер використовує інструменти для перевірки цільової системи на наявність слабких місць, зокрема відкритих служб, проблем із безпекою програм і вразливостей із відкритим кодом. Тестери

використовують різноманітні інструменти на основі того, що вони знаходять під час розвідки та під час тесту.

Далі йде отримання доступу – мотивація зловмисників варіюється від крадіжки, зміни або видалення даних до переміщення коштів і просто завдавання шкоди репутації підприємству. Щоб виконати кожен тестовий приклад, тестувальники повинні вибрати найкращі інструменти та методи для отримання доступу до вашої системи, чи то через слабкість, наприклад, ін’єкцію SQL, чи за допомогою зловмисного програмного забезпечення, соціальної інженерії чи чогось іншого.

Підтримка доступу – після того, як тестувальники отримують доступ до цілі, їх змодельована атака повинна залишатися доступною достатньо довго, щоб досягти своїх цілей (вилучення даних, їх модифікація або зловживання функціональними можливостями).

Серед плюсів тестування на проникнення є:

- знаходження прогалин в попередніх методах забезпечення безпеки, таких як автоматизовані інструменти, стандарти конфігурації та кодування, аналіз архітектури та інші менші заходи щодо оцінки вразливостей;
- знаходження як відомих, так і невідомих недоліків програмного забезпечення та вразливостей безпеки, у тому числі невеликі, які самі по собі не викликають особливого занепокоєння, але можуть завдати матеріальної шкоди як частина складної моделі атаки;
- може атакувати будь-яку систему, імітуючи поведінку більшості зловмисних хакерів.

Щодо мінусів:

- є трудомістким і дорогим;
- не всебічно запобігає вразливостям та недолікам інформаційної системи.

На найпростішому рівні сканування вразливостей спрямоване на виявлення будь-яких систем, які піддаються відомим вразливостям, тоді як тест на проникнення спрямований на виявлення слабких місць у конкретних конфігураціях системи та організаційних процесах і методах, які можуть бути використані для

компрометації безпеки. Як ілюстрація різниці між скануванням вразливостей і тестом на проникнення, тест на проникнення може включати:

- використання методів соціальної інженерії, таких як видавати себе за менеджера та запитувати у співробітника пароль, щоб отримати доступ до бази даних або іншої системи;

- перехоплення та використання незашифрованих паролів, надісланих по мережі;

- надсилання фішингових листів користувачам для отримання доступу до облікових записів.

Організації повинні регулярно проводити тестування на вразливість, щоб забезпечити безпеку своїх мереж, особливо коли вносяться зміни. Наприклад, тестування слід проводити, коли додаються служби, встановлюється нове обладнання або відкриваються порти. Тестування на проникнення передбачає виявлення вразливостей у мережі, і воно намагається використати їх для атаки на систему. Незважаючи на те, що пентестинг іноді проводиться разом з оцінкою вразливості, основна мета тестування на проникнення полягає в тому, щоб перевірити, чи справді існує вразливість. Крім того, тестування на проникнення намагається довести, що використання вразливості може пошкодити програму або мережу.

У той час як процес виявлення вразливості зазвичай автоматизований для охоплення широкого спектру невиправлених вразливостей, тестування на проникнення зазвичай поєднує автоматизовані та ручні методи, щоб допомогти тестувальникам глибше заглиблюватися у вразливості та використовувати їх для отримання доступу до мережі в контрольованому середовищі.

2.3 Аналіз існуючих засобів з виявлення вразливостей

Слід враховувати дуже багато критеріїв вибираючи сканер вразливостей для інформаційної системи. Набір пристроїв(хостів), які можуть сканувати сканери вразливостей – один із найголовніших аспектів. Потрібен інструмент, який зможе відсканувати все обладнання, яким ми володіємо. Наприклад, якщо у вас багато серверів Linux, треба вибрати інструмент, який може їх сканувати, а не той, який лише обробляє Windows пристрої. Також важлива максимальна точність у середовищі системи, оскільки не хотілося б мати помилкові спрацювання.

Іншим важливим фактором, що розрізняє сканери, є база даних вразливості інструмента. Основні питання які треба розглядати для вибору засобів виявлення вразливостей відповідно до такої бази:

- чи зберігається вона у постачальника, чи від незалежної організації;
- чи регулярно оновлюється;
- чи зберігається локально, або в хмарі;
- чи потрібно сплачувати додаткові вартості для використання таких баз даних вразливостей або для одержання їх оновлень.

Деякі сканери вразливості будуть використовувати більш інтрузивний метод сканування, який потенційно може вплинути на продуктивність системи. Це не обов'язково є поганим фактором при виборі сканера, але якщо вони впливають на продуктивність системи, то треба обов’язково знати про це і планувати свої сканування відповідно. До речі, планування є ще одним важливим аспектом засобів сканування мережевих вразливостей. Оскільки такий тип сканувань досить сильно навантажує мережу. Деякі інструменти навіть не мають запланованих сканувань і їх потрібно запускати вручну.

Існують також дві інші важливі особливості інструментів сканування вразливостей: оповіщення та звітування. Що відбувається після виявлення вразливості? Чи є повідомлення корректним та легким для зрозуміння? Як це надано? Це екранне спливаюче вікно, електронна пошта, текстове повідомлення? І що ще важливіше, чи дає інструмент певне уявлення про те, як виправити вразливі

місця, які він ідентифікує? Деякі інструменти таке можуть зробити, а деякі – ні. Деякі сканери навіть мають автоматичне виправлення певних вразливостей. Інші інструменти можуть інтегруватися з програмним забезпеченням для керування вразливостей, або з корпоративними системами моніторингу.

Що стосується звітності, це часто є предметом особистих уподобань. Однак, ви повинні переконатися, що інформація, яку ви очікуєте та потребуєте знайти у звітах, насправді буде там. Деякі інструменти мають лише попередньо визначені звіти, інші дозволяють змінювати вбудовані звіти. А найкращі – принаймні з точки зору звітності – дозволяють створювати власні звіти з нуля [14].

Тож варто розглянути які інструменти можна використовувати для ідентифікації вразливостей. Протягом багатьох років дослідники інформаційної безпеки та постачальники намагалися зробити процес виявлення вразливостей якомога простим і швидким. Це стало можливим завдяки розробці та внеску в такі проекти, як проект Kali Linux, який передбачає інтеграцію багатьох інструментів безпеки в операційну систему безпеки. Ця ОС Linux містить інструменти для різних завдань безпеки, включаючи таку як ідентифікація вразливостей. Нижче наведено деякі інструменти ідентифікації вразливостей, наявні в операційній системі Kali Linux:

- сканер вразливостей Nessus – це один із найпоширеніших сканерів вразливостей, доступних сьогодні, здатний виявляти вразливості як у веб-додатках, так і в кількох системах;
- OpenVAS Vulnerability Scanner – це сканер вразливостей мережі, здатний ідентифікувати вразливості, наявні на пристроях у мережі;
- Nikto Vulnerability Scanner – це сканер вразливостей веб-сервера, здатний ідентифікувати вразливості, наявні на веб-серверах;
- Nmap Vulnerability Scanner – це, мабуть, найвідоміший сканер вразливостей для хакерів сьогодні, що здатний виявити безліч вразливостей у кількох цілях;
- Wapiti Vulnerability Scanner – це сканер вразливостей веб-додатків, здатний виявляти проблеми, пов'язані з веб-додатками, такі як SQL та XSS.

Ці інструменти дають змогу тестувальникам та фахівцям з інформаційної безпеки виявляти велику кількість інформації з системи підприємсва, а потім перевіряти цю інформацію на наявність вразливостей. Перевірена інформація може відрізнятися від версії операційної системи до рівня виправлення, версій програмного забезпечення тощо.

Важливо звернути увагу на кількість ресурсів, які будуть використані, перш ніж виконувати сканування за допомогою цих інструментів. Якщо, наприклад, цільова система споживає багато ресурсів, це слід розглянути заздалегідь.

Основними вимогами до програми-сканера, що забезпечує перевірку системи і її окремих вузлів на вразливості, є:

1. Кросплатформеність або підтримка декількох операційних систем. При наявності такої особливості можна виконувати перевірку мережі, що складається з комп'ютерів з різними платформами. Наприклад, з декількома версіями Windows або навіть з системами типу UNIX.

2. Можливість сканувати одночасно кілька портів – така функція помітно зменшує час на перевірку.

3. Сканування всіх видів ПЗ, які зазвичай схильні до атак з боку хакерів. Серед шкідливих програм відносять продукцію компанії Adobe і Microsoft (наприклад, пакет офісних додатків MS Office).

4. Перевірку мережі в цілому і окремих її елементів без необхідності запускати сканування для кожного вузла системи.

Більшість сучасних скануючих програм мають інтуїтивно зрозуміле меню і досить легко налаштовуються відповідно до виконуваних завдань.

Практично кожен такий сканер дозволяє скласти список вузлів і програм що потрібно перевірити, вказати додатки, для яких будуть автоматично встановлюватися оновлення при виявленні вразливостей, і задати періодичність сканування і створення звітів. Після отримання звітів деякі сканери дозволяють адміністратору запускати виправлення загроз.

Серед додаткових особливостей сканерів можна відзначити можливість економії трафіку, яка виходить при скачуванні тільки однієї копії

дистрибутива і її розподілі по всім комп'ютерам мережі. Ще одна важлива функція передбачає збереження історії минулих перевірок, що дозволяє оцінити роботу вузлів в певних тимчасових інтервалах і оцінити ризики появи нових проблем з безпекою.

Асортимент програм-сканерів на сучасному ринку ПО досить великий. Всі вони відрізняються один від одного функціональністю, ефективністю пошуку вразливостей і ціною. Для оцінки можливостей таких додатків варто розглянути характеристики і особливості популярних варіантів на ринку.

Nessus. Програму Nessus вперше випустили 20 років тому, але тільки з 2003-го року вона стала платною. Монетизація проекту не зробила його менш популярним – завдяки ефективності і швидкості роботи кожен шостий адміністратор в світі застосовує саме цей сканер (Рис. 2.1.).

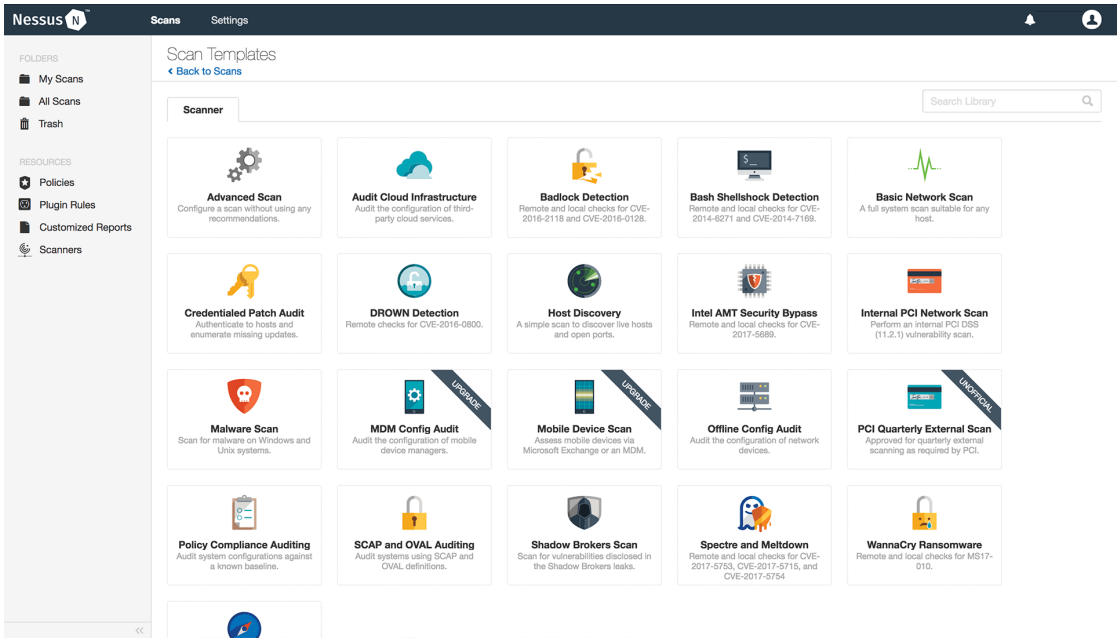

Рис. 2.1. Інтерфейс сканера Nessus

До переваг вибору Nessus відносять:

- постійно оновлювану базу вразливостей;
- просту установку і зручний інтерфейс;
- ефективне виявлення проблем з безпекою;
- використання плагінів, кожен з яких виконує своє завдання – наприклад, забезпечує сканування ОС Linux або запускає перевірку тільки заголовків.

Додаткова особливість сканера – можливість використання тестів, створених користувачами за допомогою спеціального програмного забезпечення. У той же час у програми є і два серйозних недоліки. Перший – можливість виходу з ладу деяких програм при скануванні за допомогою методу «імітації атак», другий – досить висока вартість [15].

Менеджер конфігурації мережі SolarWinds. Основна утиліта SolarWinds Network Configuration Manager як інструмент сканування вразливостей, полягає у перевірці конфігурацій мережевого обладнання на наявність помилок та упущень. Інструмент також може періодично перевіряти конфігурації пристрою на зміни. Це також корисно, оскільки деякі атаки починаються шляхом зміни конфігурації мережевих пристроїв, які часто не є настільки безпечними, як сервери, таким чином, щоб полегшити доступ до інших систем. Інструмент також може допомогти вам у дотриманні стандартів або відповідності нормативних вимог до його автоматизованих інструментів налаштування мережі, які можуть розгортати стандартизовані конфігурації, виявляти зміни поза процесом, конфігурації аудиту та навіть виправляти порушення(Рис. 2.2.).

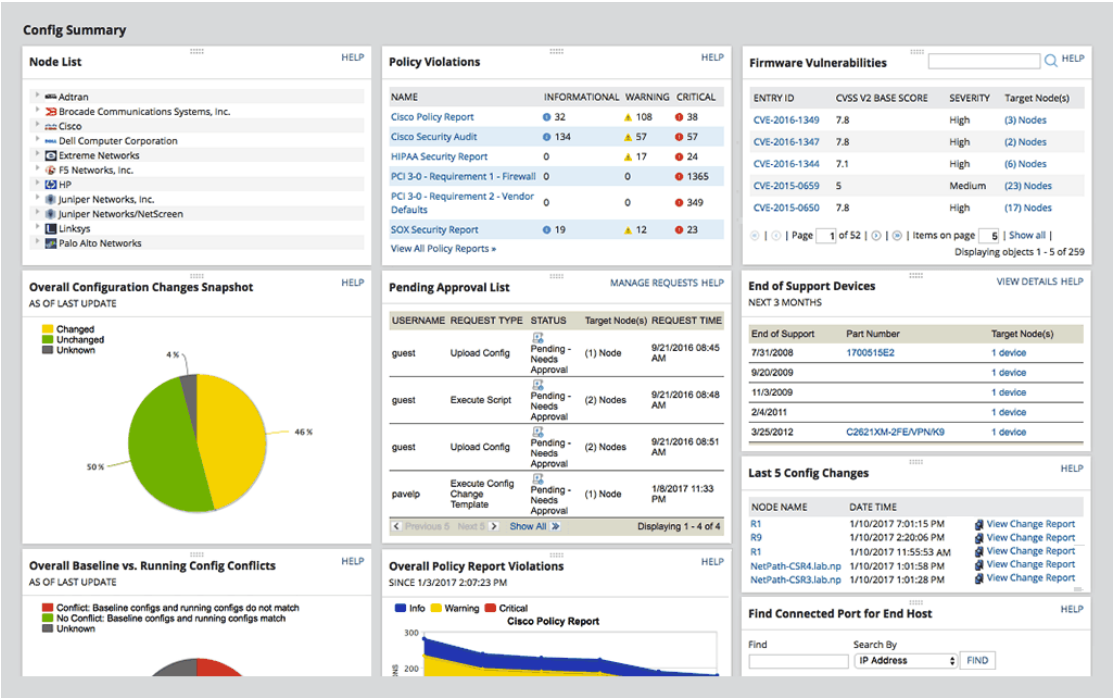

Рис 2.2. Інтерфейс сканера SolarWinds

Програмне забезпечення інтегрується з Національною базою даних вразливості. Інструмент має доступ до найновіших CVE для виявлення

вразливостей у пристроях Cisco. Він буде працювати з будь-яким пристроєм Cisco, що працює під керуванням ASA, IOS або Nexus. Насправді, у цей продукт вбудовано два інших корисних інструменти: мережева статистика для ASA та мережева статистика для Nexus.

Ціни на Менеджер конфігурації мережі SolarWinds починаються від трьох тисяч доларів для 50 керованих вузлів і змінюються залежно від кількості вузлів.

Наш наступний інструмент називається Open Vulnerability Assessment System або OpenVAS. Він являє собою базу декількох сервісів і інструментів. Всі вони об'єднуються, щоб зробити його всеосяжним і потужним інструментом сканування вразливостей. Рамки, що стоять за OpenVAS, є частиною рішення для управління вразливостями Greenbone Networks, з якого елементи були внесені до спільноти протягом десяти років. Система повністю вільна, і більшість її компонентів є відкритими, лише деякі з них – ні. Сканер OpenVAS поставляється з більш ніж п’ятдесятьма тисячами тестів мережі, які регулярно оновлюються (Рис. 2.3).

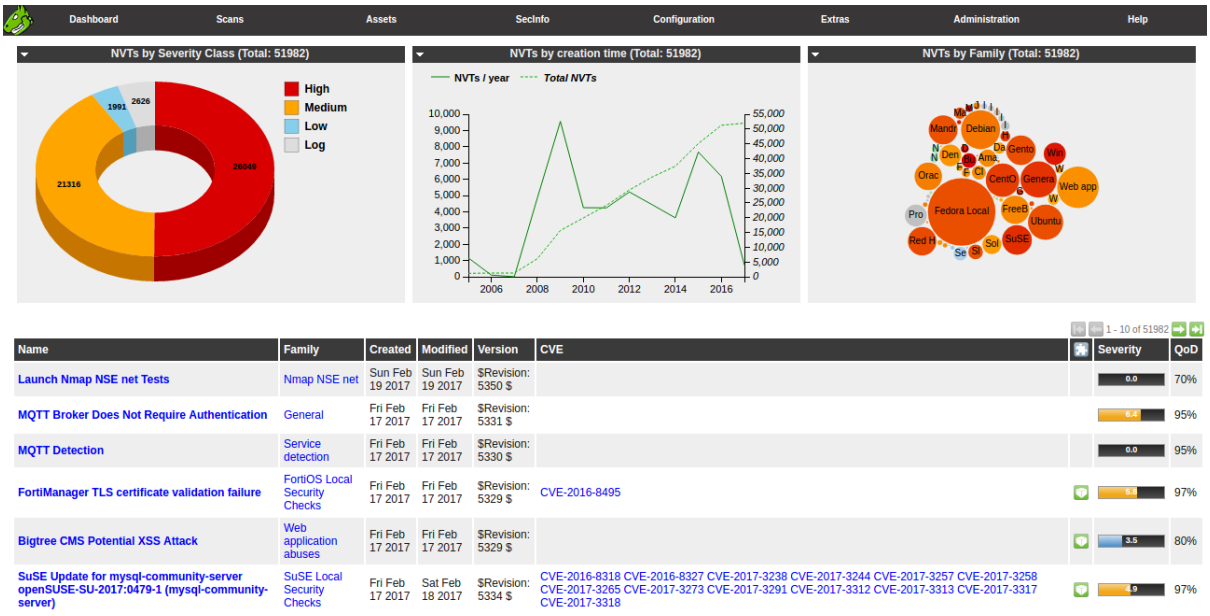

Рис. 2.3. Інтерфейс сканера OpenVAS

У OpenVAS є два основних компонента. Першим компонентом є сканер OpenVAS. Як випливає з назви, він відповідає за фактичне сканування цільових комп'ютерів. Другий компонент – менеджер OpenVAS, який обробляє все інше, наприклад, керує сканером, консолідує результати та зберігає їх у центральній базі

даних SQL. Система включає в себе як браузерні, так і командні рядки. Іншою складовою системи є база даних випробувань вразливості мережі. Ця база даних може отримати свої оновлення або від вільного каналу співтовариства Greenborne Community.

Наступний в списку – XSpider. Сканер XSpider випускається компанією Positive Technologies, представники якої стверджують, що програма не тільки виявляє вже відомі вразливості, але здатна знайти ще не створені загрози.

До особливостей застосування відносять:

- ефективне виявлення «дірок» в системі;
- можливість віддаленої роботи без установки додаткового програмного забезпечення;
- створення докладних звітів з порадами щодо усунення проблем;
- оновлення бази вразливостей і програмних модулів;
- одночасне сканування великої кількості вузлів і робочих станцій.

Також варто відзначити, що вартість використання сканера більш доступна в порівнянні з програмою Nessus (Рис. 2.4.) [14].

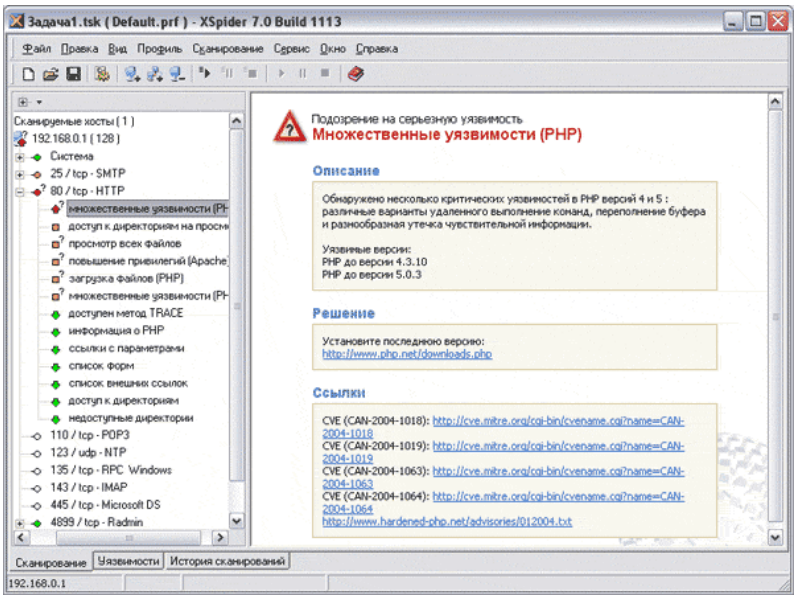

Рис. 2.4. Інтерфейс сканера Xspider

Далі – Rapid 7 Nexpose. Rapid7 Nexpose аналізує всі компоненти інфраструктури, включаючи мережі, операційні системи, бази даних та веб-програми. За підсумками перевірки програма здійснює пріоритезацію виявлених

загроз і генерує інструкції, як знизити кожну з них. Система Rapid7 Nexpose може інтегруватися з Metasploit – рішенням для тестування проникнення загроз для комплексного оцінювання ризиків безпеки в IT-інфраструктурі організації.

Rapid 7 Nexpose має багато варіантів поширення в залежності від потреб – від індивідуального рішення, до enterprise.

Система управління Nexpose динамічно виявляє об'єкти в мережі організації, на які можуть бути спрямовані атаки та визначає можливі ризики, пов'язані з вразливістю об'єктів у мережі. Додатково до безпеки, можна відстежувати в реальному часі, всі зміни, що відбуваються в мережі організації, і сканувати нові об'єкти в мережі, як тільки вони стануть доступні і видимі сканером. Для експлуатації вразливостей NeXpose інтегрується з системою експлуатації вразливостей Metasploit для проведення автоматизованого тестування на проникнення (Рис 2.5.).

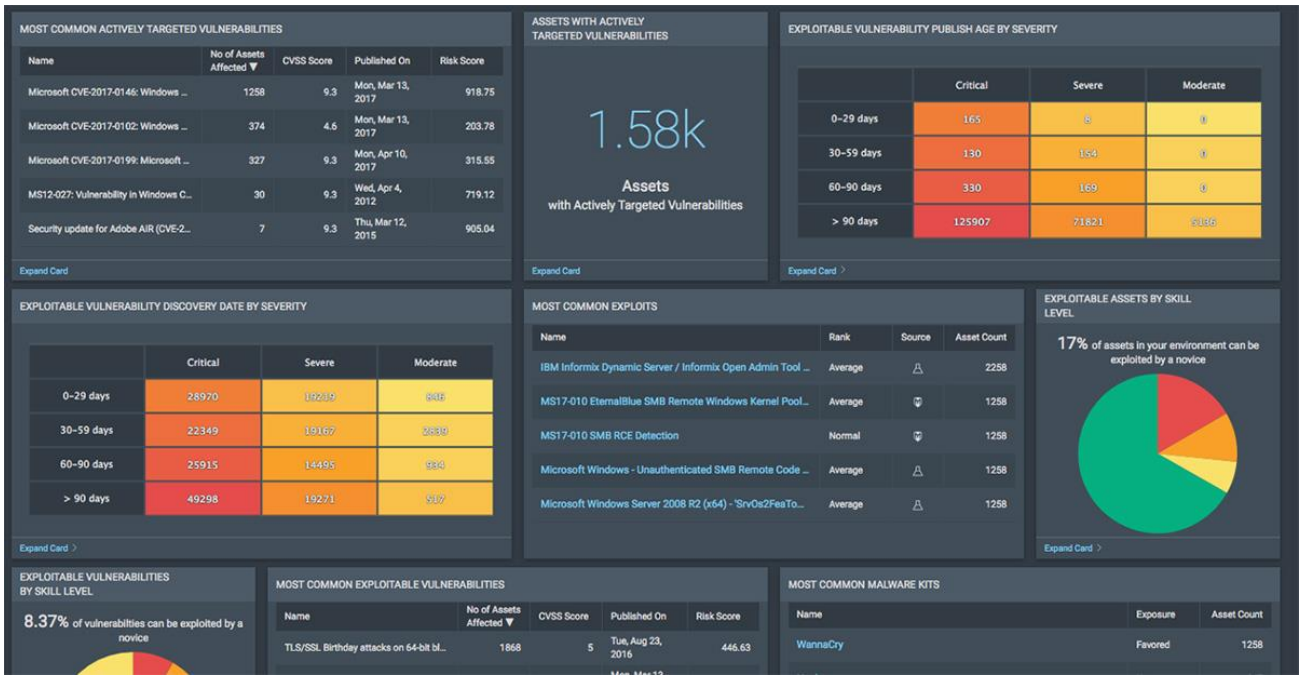

Рис. 2.5. Інтерфейс сканера Rapid 7 Nexpose

Отже, в даний час на ринку представлено достатню кількість варіантів інструментів з сканування вразливостей. Заключним фактором вибору є бюджет та потрібний функціонал відповідно до вимог політик та систем.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ НА БАЗІ TENABLE NESSUS ESSENTIALS

Одним з найпопулярніших сканерів вразливостей на ринку є Nessus Vulnerability Scanner. Він став свого роду стандартом для сканерів вразливостей. Спочатку він стартував як проект із відкритим кодом. Далі його придбала компанія Tenable, і тепер він є комерційним продуктом (версія Professional). Незважаючи на це, у Nessus Scanner, як і раніше, є «essential» версія, яка розповсюджується безкоштовно, але має обмеження в 16 IP адрес. Саме цю версію було розглянуто в даному варіанті технології із виявлення вразливостей.

3.1 Призначення та структура рішення Tenable Nessus Essentials

Nessus – один із найпопулярніших засобів зовнішньої оцінки вразливості, якому довіряють понад 30 000 організацій у всьому світі. Nessus сканує систему і видає попередження, якщо виявляє будь-які вразливості, які можуть використовувати зловмисники для отримання доступу. Nessus не запобігає атакам активно, він перевіряє «дирки» в інфраструктурі. Він надає докладні звіти про безпеку системи, які є великою підмогою усунення будь-яких вразливостей та підвищення безпеки мережі. Nessus доступний у багатьох різних версіях. У даній роботі було розглянуто та встановлено безкоштовну версію Nessus під назвою Nessus Essentials, яка може сканувати до 16 хостів.

Але не буде зайвим розглянути й інші версії Nessus. Nessus Professional – сканер вразливостей для невеликих організацій, що включають до 50 робочих машин, а також для аудиторів, що здійснюють аналіз безпеки своїх замовників. Продукт дозволяє оцінювати конфігурації, знаходити вразливості та, у разі виявлення проблем при налаштуванні інфраструктури, запобігати мережевим атакам.

До основних можливостей Nessus Professional можна віднести:

- широкий вибір режимів аналізу захищеності;
- гнучкі параметри аналізу вразливостей;
- управління оновленнями продукту та контенту;
- складання звітів за заданими критеріями;
- сумісність із плагінами Nessus;
- автоматичні щоденні поновлення системи.

Nessus Enterprise (або Tenable.io) – сканер, що включає в себе всі наявні можливості Nessus, включаючи функцію кількох сканерів, доступну як локально, так і з хмари з безлімітною кількістю хостів для сканування.

Нові функції Nessus Enterprise:

- спільний доступ – ресурси можуть бути розшарені між кількома користувачами та/або групами, за такими критеріями:
  - результати сканування – для надання докладних результатів по виявленню вразливостей експлуататорам систем у вашій організації;
  - розклад сканування – за для уникнення дублювання зусиль, надавши розклад сканування;
  - політики сканування – спеціальні політики сканування для відповідного середовища можна надати користувачам і командам в організації, уникаючи ще більшого дублювання зусиль.
- призначення користувачів до певного сканера, зменшення навантаження на основні сканери та передача області сканування своєї мережі відповідальним сторонам;
- контроль доступу – користувачам можуть бути надані ролі, які дають їм повний контроль над сканером, або ж до доступу лише для читання до результатів сканування;
- підтримка LDAP – інтеграція автентифікації з локальним сервером LDAP, щоб спростити обмін ресурсами та уникнути додаткових витрат на керування обліковими даними;

Чому саме цей продукт був вибраний для дослідження в даній роботі? На це питання краще за все відповість рейтинг оцінок від користувачів продуктів від G2 grid for Vulnerability Scanner Software (Рис. 3.1.).

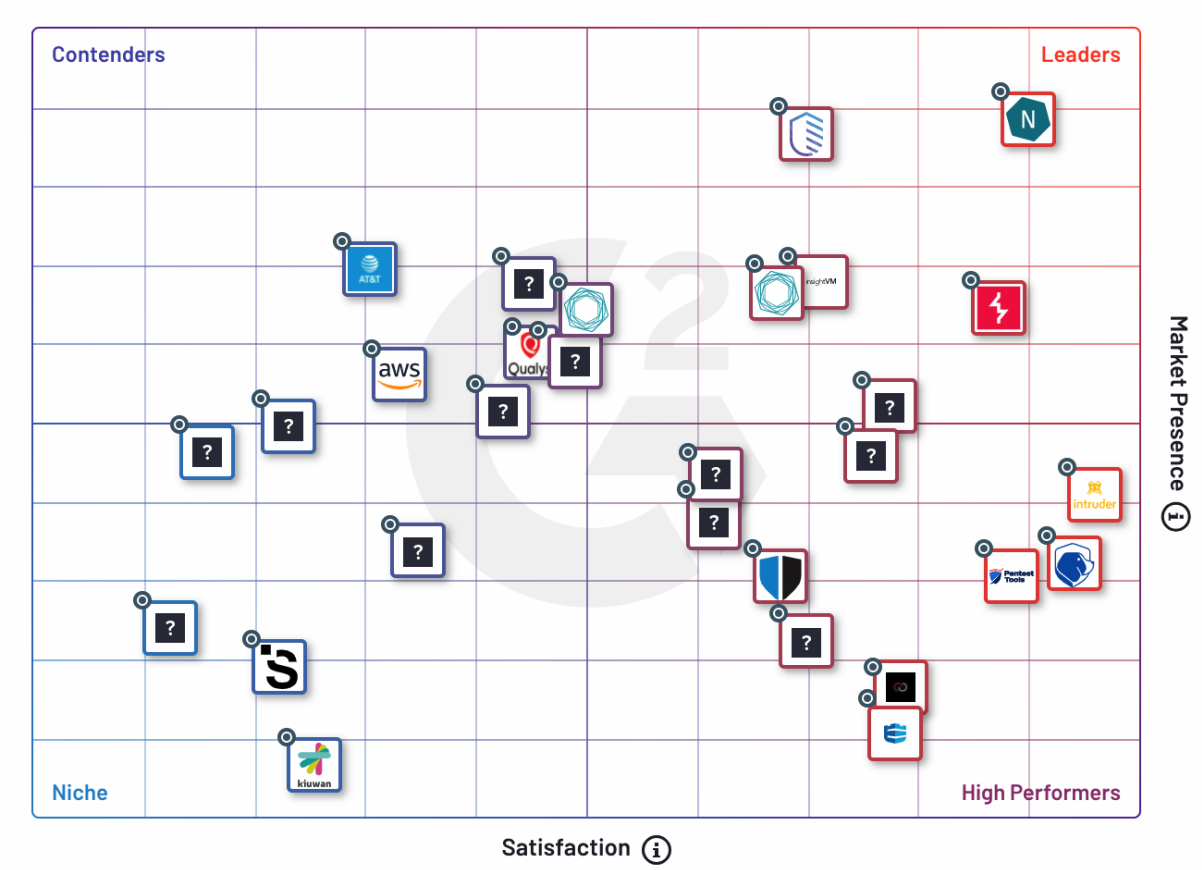

Рис. 3.1. G2 grid for Vulnerability Scanner Software [17]

Nessus – це сканер вразливостей, який використовує архітектуру Common Vulnerabilities та Exposures для легкого перехресного зв'язування між сумісними засобами безпеки. Nessus використовує Nessus Attack Scripting Language (NASL), просту мову, яка описує окремі загрози та потенційні атаки.

Nessus може сканувати:

- вразливості, які можуть дозволити несанкціонований контроль або доступ до конфіденційних даних у системі;
- неправильні конфігурації;
- паролі за замовчуванням, кілька поширених паролів і порожні/відсутні паролі в деяких системних облікових записах;

- Nessus також може викликати Hydra (зовнішній інструмент), щоб запустити словникову атаку (брут-форс);

- вразливі місця відмови в обслуговуванні.

Мабуть, найцікавіше в Nessus – це NASL (Nessus Attack Scripting Language). Він використовується для написання плагінів, які Nessus використовує для виконання різних сканувань. Плагіни легко писати, а будь-який із них можна читати та змінювати, що дозволяє краще інтерпретувати складні результати. Плагіни дуже безпечні з для інформаційної системи, оскільки Nessus запускає їх на віртуальній машині, тому, теоретично, плагін не може вплинути на вашу інфраструктуру. На даний момент доступно понад 165000 плагінів. Оновлення також доступне, і якщо не критично потрібні найновіші та найактуальніші плагіни, є можливість зареєструватися для безкоштовного облікового запису, який дозволить отримувати всі оновлення з тижневою затримкою. Якщо є потреба найновіших та без затримки – доведеться заплатити суму в 1200 доларів. Додатково варто знати, що також є RSS-канал з найновішими плагінами безпеки, доданими в базу даних.

Механізм сканування Nessus використовує плагіни для виявлення нових вразливостей. Tenable надсилає до систем клієнтів плагіни, які містять найновішу інформацію, протягом 24 годин після того, як вразливість стане загальнодоступною. Оскільки нові вразливості з’являються майже щодня, клієнти щодня отримують канали плагінів, щоб залишатися в курсі.

Інші цікаві функції Nessus – це «розумне розпізнавання служб», яке дозволяє Nessus виявляти служби, навіть якщо вони працюють на нестандартних портах, «повна підтримка SSL», яка використовується для тестування безпечних служб, і можливість виконувати ретельні тести, які викликають все на віддалених хостах, щоб побачити, як вони працюють. Додатково, трафік між сервером і клієнтом Nessus зашифрований. Ця функція є важливою для Nessus, оскільки за допомогою облікових даних, Nessus може ввійти на віддалені хости, щоб отримати вражаючу кількість даних про локальну конфігурацію. Шифрування захищає ці облікові дані та звіт, який доставляється клієнту. У локальній конфігурації є дані, які неможливо

виявити під час звичайного сканування, наприклад, яке програмне забезпечення встановлено та які номери версій [17].

Nessus Essential працює на Windows, Windows Server, Mac OS, Free BSD Unix, Debian, SUSE, Ubuntu, RHEL, Fedora та Amazon Linux.

В даній роботі далі проінстальовано версію Nessus 10.0.1 на системі Mac OS 11.2.1..

Коротко про інсталяцію засобу:

1. Завантаження потрібної версії продукту з офіційного сайту (Рис. 3.2.).

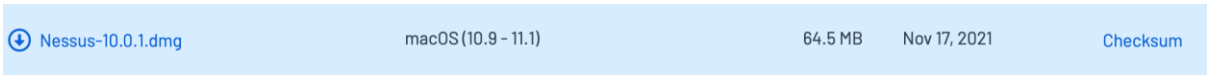

Рис. 3.2. Вибір продукту для завантаження [17]

2. Безпосередньо процес інсталяції продукту (включає погодження з політиками роботи інструменту), результатом якого буде запущено даний сервіс на порті 8834, клієнтом може виступати браузер.

3. Реєстрація та активація продукту (Рис.3.3-4.).

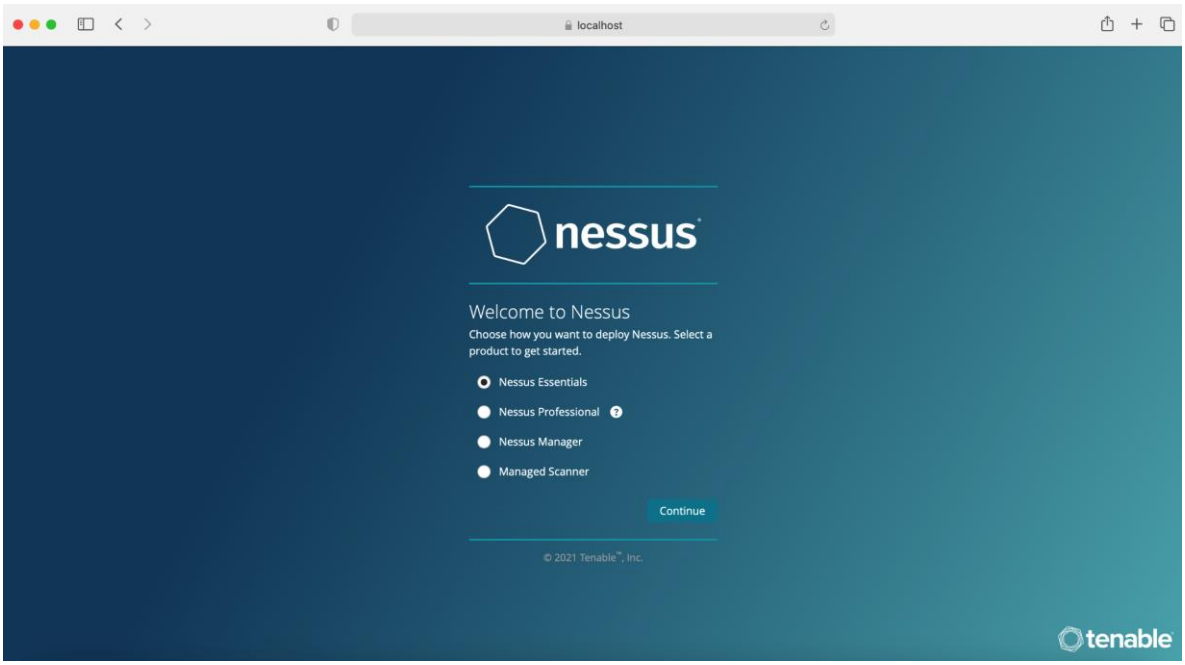

Рис.3.3. Вибір версії для встановлення

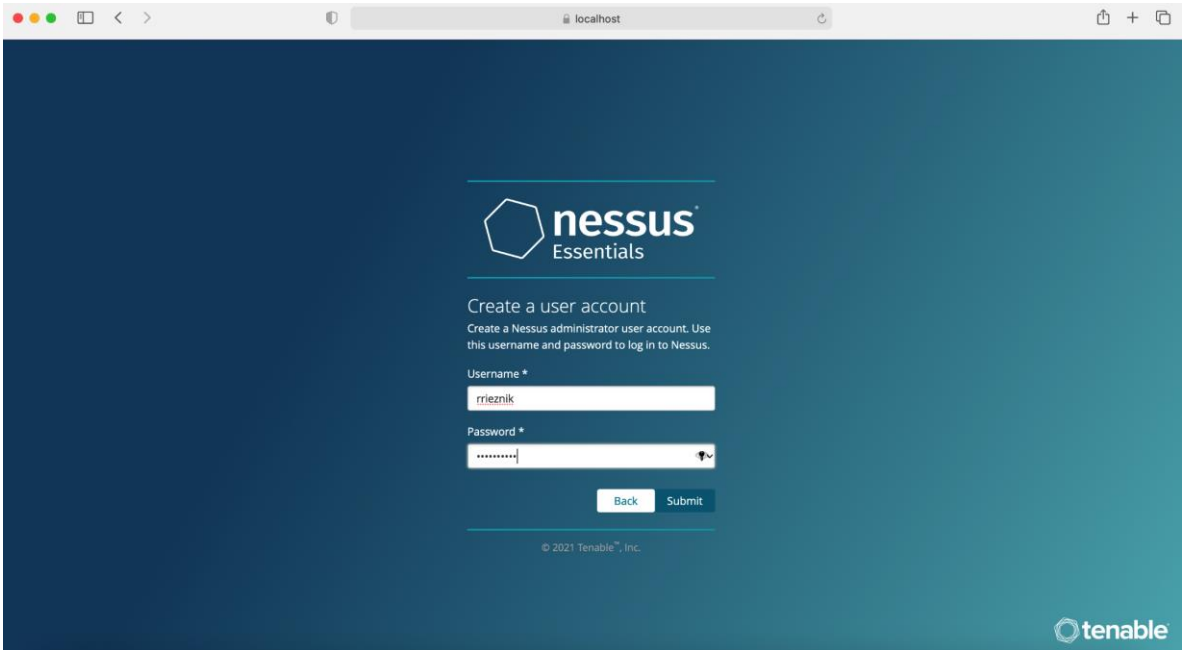

Рис.3.4. Реєстрація користувача в Nessus

4. Завантаження актуальних оновлень та плагінів, що відбувається автоматично після проходження попереднього пункту.

Після коректного встановлення програми з'являється головне меню програми. Варто розглянути скруктурну схему компонентів Nessus Tenable (Рис 3.5).

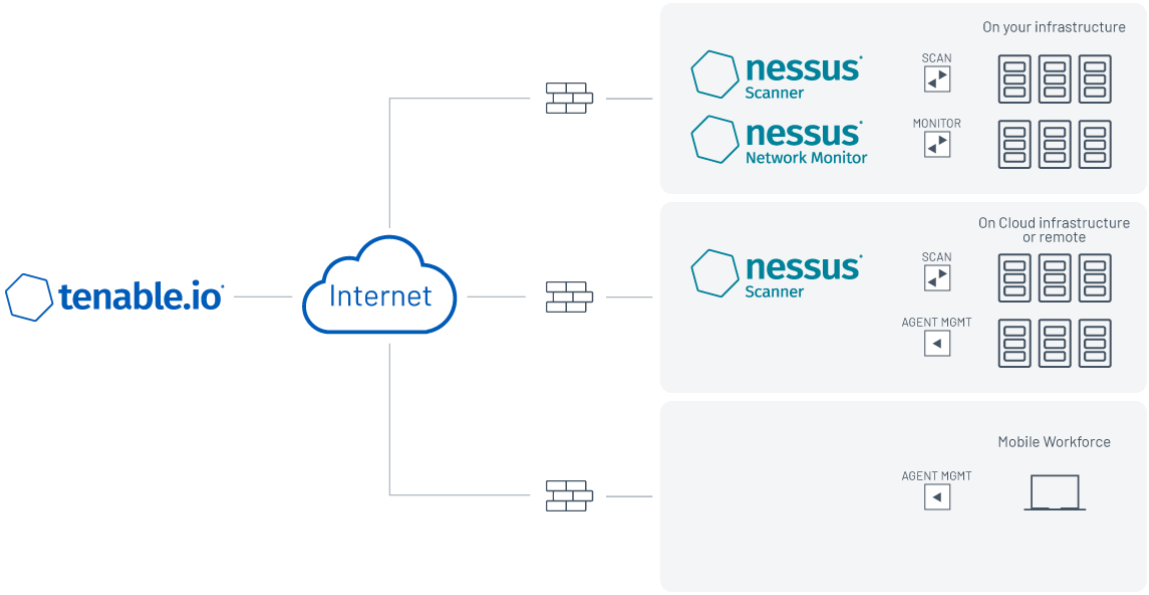

Рис. 3.5. Структура компонентів та продуктів Teneble [17]

Варто вказати мінімальні системні вимоги для проведення сканування (до 50000 хостів за одне сканування), дані взяті від розробника:

- процесор 4 ядра від 2GHz;
- оперативна пам’ять від 4GB;
- 30GB вільного місця на диску.

3.2 Технологія виявлення вразливостей за допомогою Tenable Nessus Essentials

Для розроблення технології виявлення вразливостей було розгорнуто локальну мережу з різними типами хостів, що схоже до реальної корпоративної мережі.

Тож першочергово було проведено інвентаризацію хостів, які підлягають скануванню. В розгорнутій локальній мережі наявні такі кінцеві точки:

- 192.168.0.1 – роутер;
- 192.168.0.108 – автоматизоване робоче місце (АРМ) з операційною системою Windows 10;
- 192.168.0.105 – автоматизоване робоче місце (АРМ) з операційною системою MacOS 11.2.1 (на якому встановлено Nessus);
- 192.168.0.112 – сервер баз даних з операційною системою Linux RedHat 6.1;
- 192.168.0.173 – сервер з центром сертифікації ключів з операційною системою Linux RedHat Enterprise 8.1.

Наступним кроком є проведення налаштування сканувань безпосередньо в Nessus. Для початку було виконано сканування портів на заданих хостах. Дане сканування знаходиться у вкладці «New Scan», далі – «Host Discovery» (Рис 3.6.).

Далі ми називаємо сканування, додаємо опис, вибираємо папку для зберігання, та задаємо потрібні таргети, в нашому випадку це – 192.168.0.1, 192.168.0.108, 192.168.0.105, 192.168.0.112 та 192.168.0.173 (Рис. 3.7.).

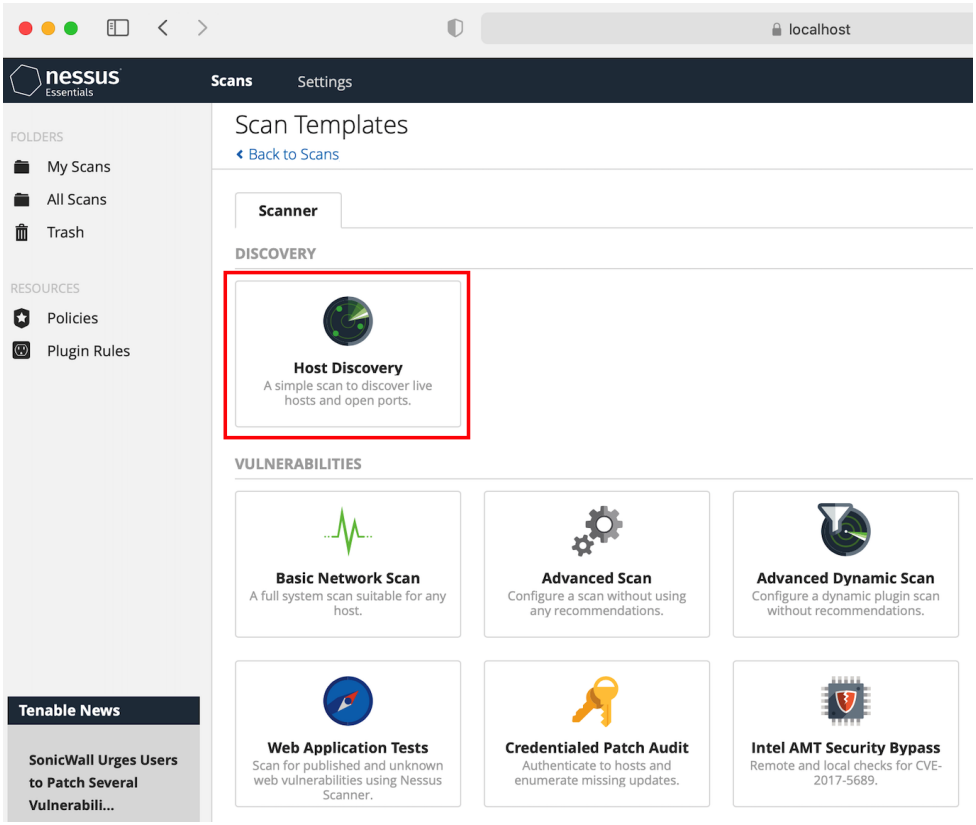

Рис. 3.6. Вибір варіанту сканування

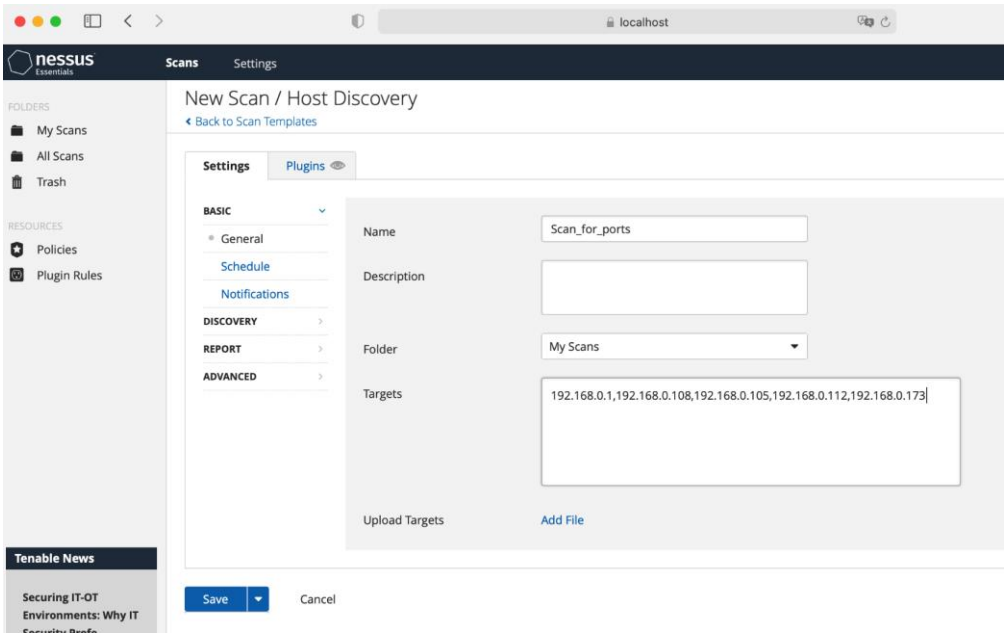

Рис. 3.7. Налаштування сканування

Також можливо налаштувати запланований запуск сканування та сповіщення про його відпрацювання в вкладках «Schedule» та «Notifications» відповідно. Але нам потрібно випрати розділ «Discovery» та змінити параметр «Scan Type» на «Port

scan (all ports)», для того щоб можливо було відсканувати весь діапазон портів від 1 до 65535 (Рис. 3.8.)

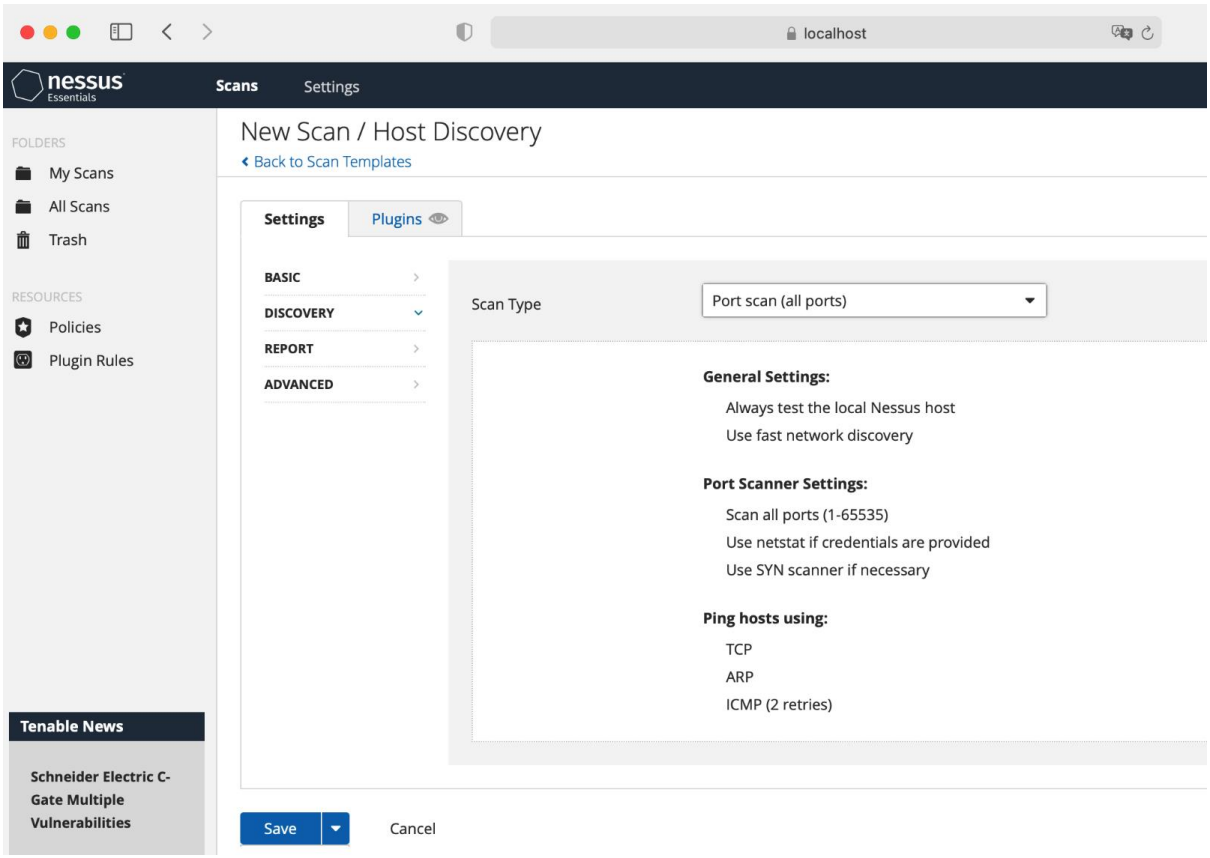

Рис. 3.8. Додаткові налаштування сканування

Також можливо налаштувати формування звіту на цьому кроці, але ми пропустимо цю опцію на даному етапі. Після збереження налаштувань, звіт зберігається в вибраній папці готовий до запуску, після чого ми його і запускаємо.

Після виконання заданого сканування переглядаємо його результати. У варіанті розгорнутої мережі вразливостей на відкритих портах не було знайдено. А ми отримали їх повний список для подальшого аналізу (Рис. 3.9.).

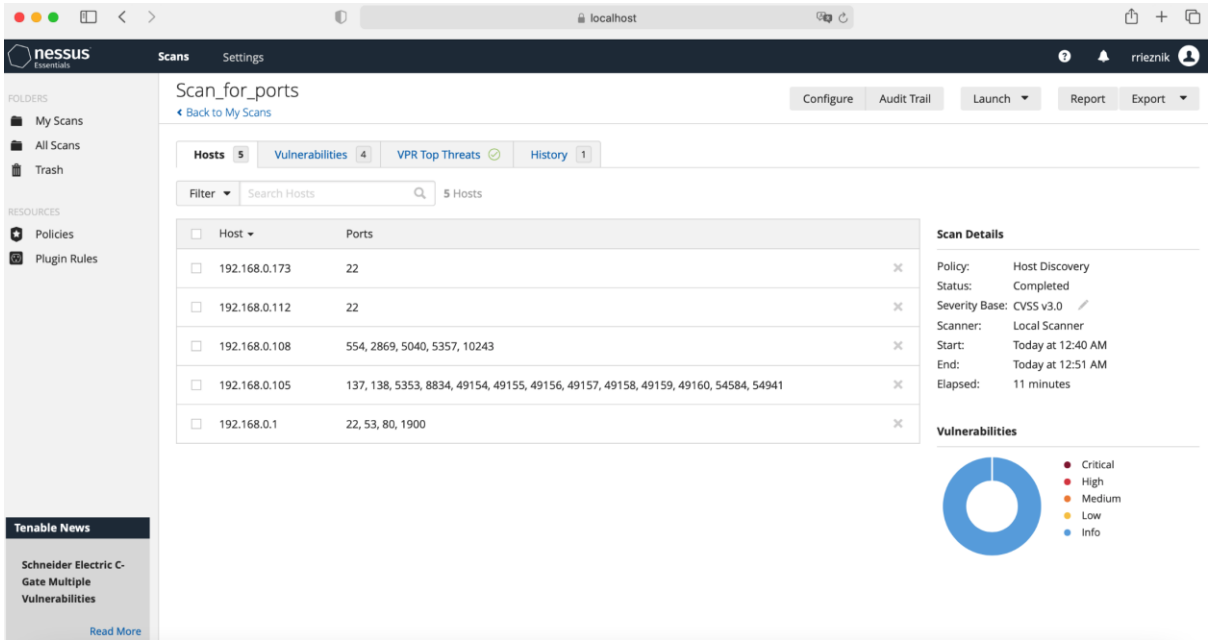

Рис. 3.9. Результати сканування

Для наглядності можливо створити звіт. Для цього потрібно вибрати опцію «Report», вибрати формат «HTML» чи «CSV» та шаблон (Рис. 3.10.).

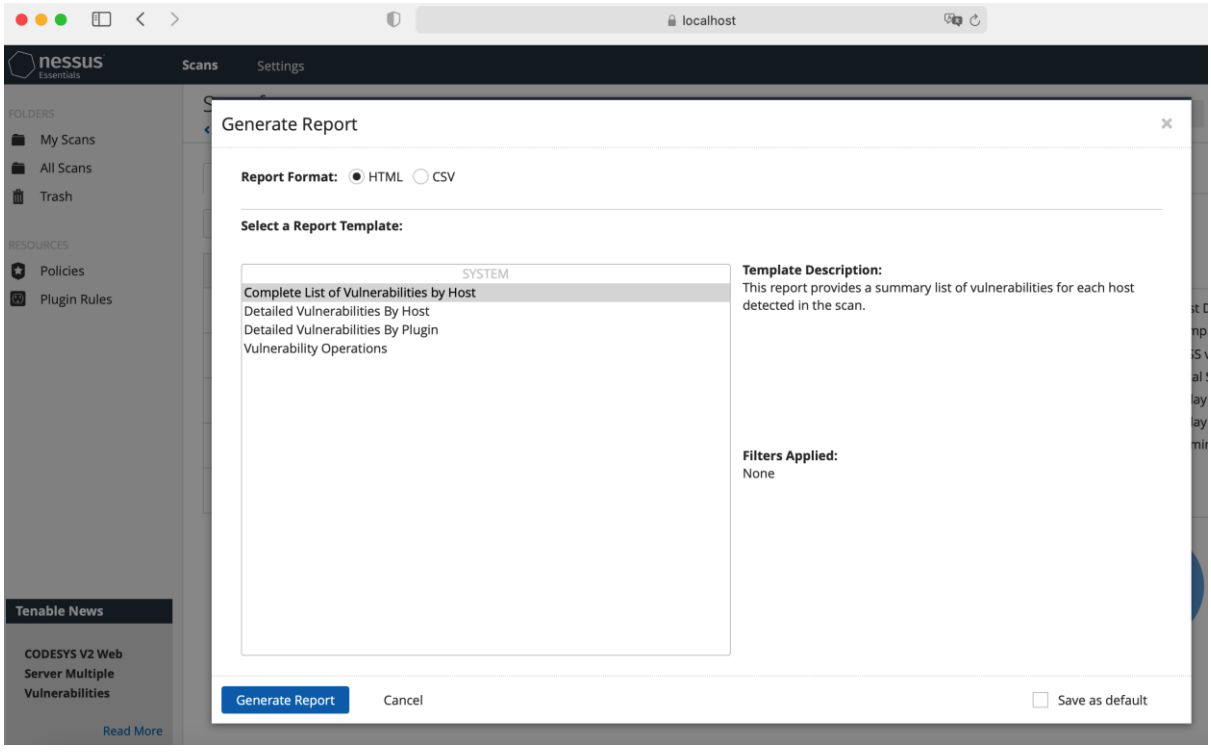

Рис. 3.10. Налаштування формування звіту по проведеному скануванню

Приклад варіанту звіту за попереднім скануванням (Рис. 3.11.).

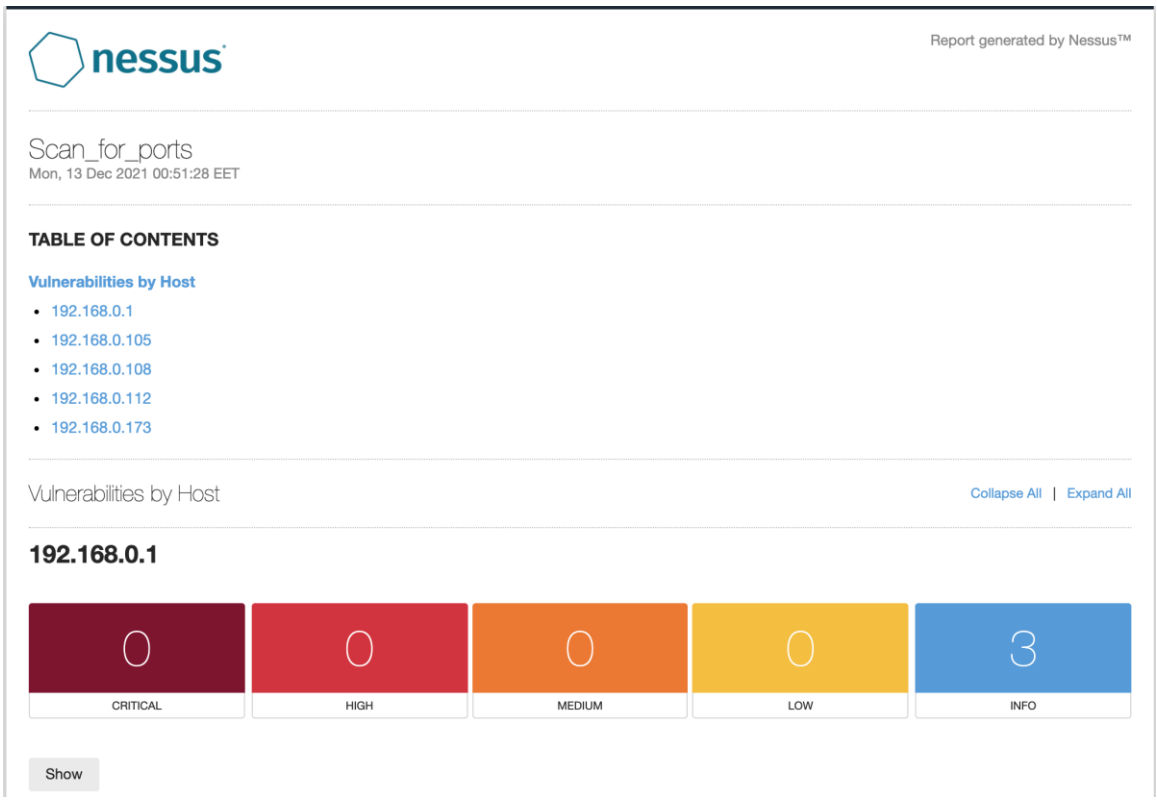

Рис. 3.11. Звіт

Після сканування портів наступним кроком технології є поглиблене дослідження заданих хостів в корпоративній мережі. Для цього потрібно вибрати відповідний тип сканування «Advanced Scan» (Рис. 3.12.).

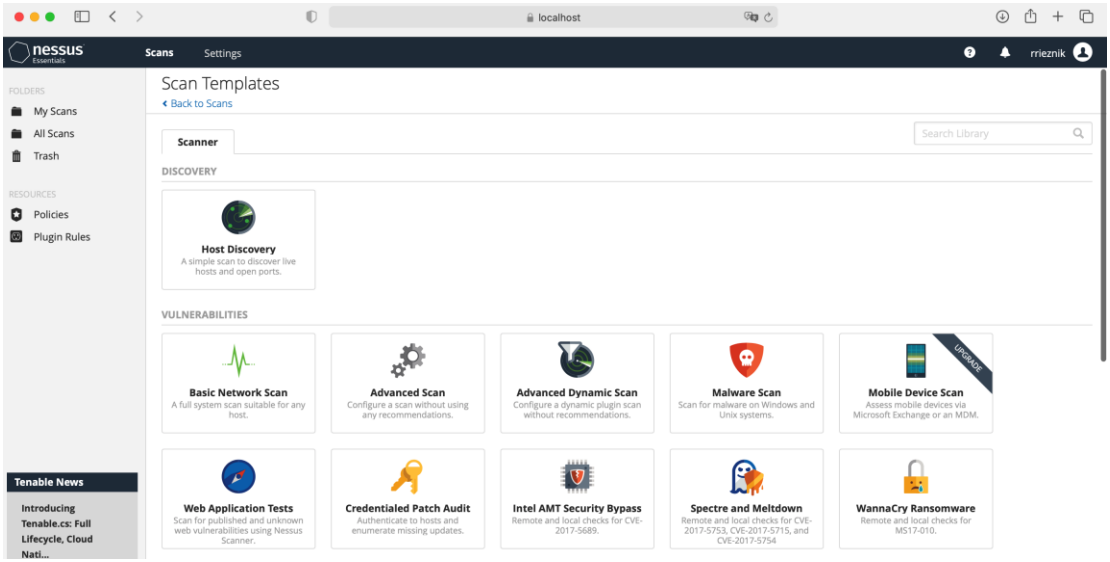

Рис. 3.12. Вибір варіанту сканування

Після чого по аналогії з минулим скануванням портів вказати потрібні ip-адреси назвати сканування, описати його та вибрати для нього папку. Тепер можем переглянути та налаштувати плагіни, які будуть використані під час цього сканування. Переходимо у вкладку «Plugins» та обираємо всі потрібні (Рис. 3.13).

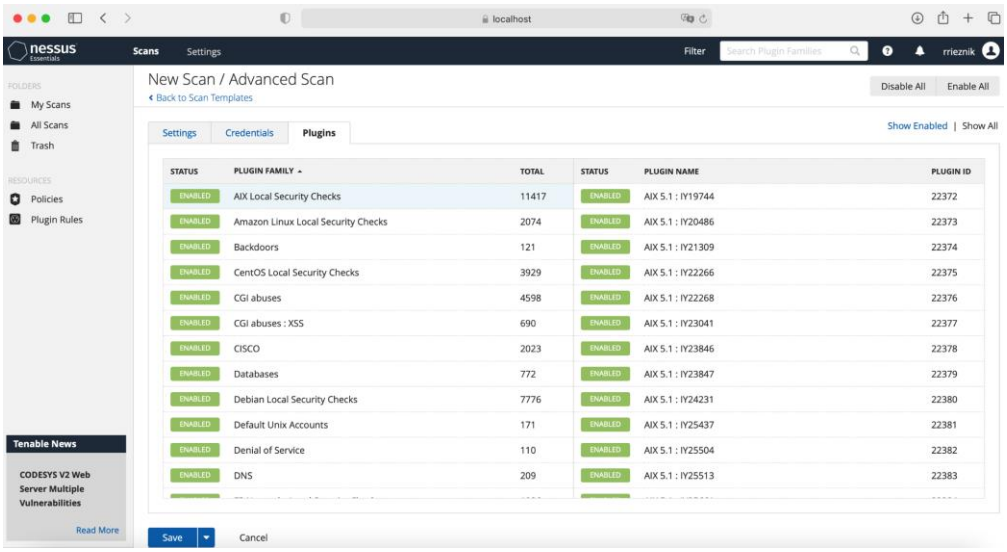

Рис. 3.13. Вибір плагінів для сканування.

Далі у вкладці «Host Discovery» обираємо сканування хоста, на якому встановлено Nessus, а також обираємо методи «ARP», «TCP» та «ICMP», все інше залишаємо за замовчуванням (Рис. 3.14.).

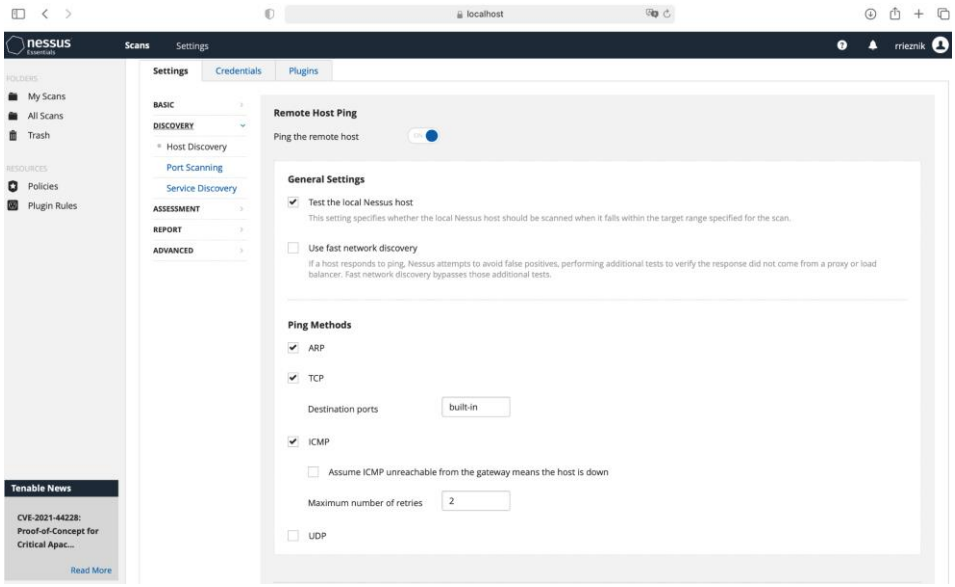

Рис. 3.14. Вибір методів сканування

Після чого можемо зберігати та запускати сканування. На змодельованій мережі з 5ма кінцевими точками даний варіант сканування був виконаний за 8 хвилин. Та отримані різноманітні результати, що включають в себе вразливості різних типів (Рис. 3.15.).

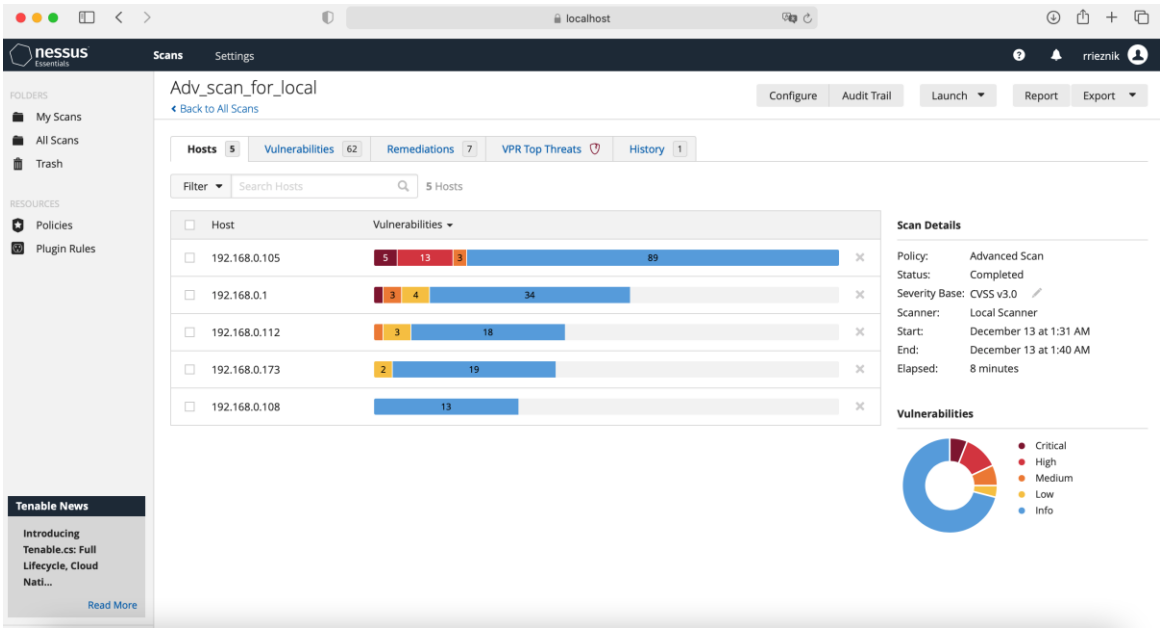

Рис. 3.15. Результати поглибленого сканування

Розглянемо перелік найбільш критичних за версією Nessus. Для цього перейдемо у вкладку «VPR Top Vulnerabilities» (Рис. 3.16).

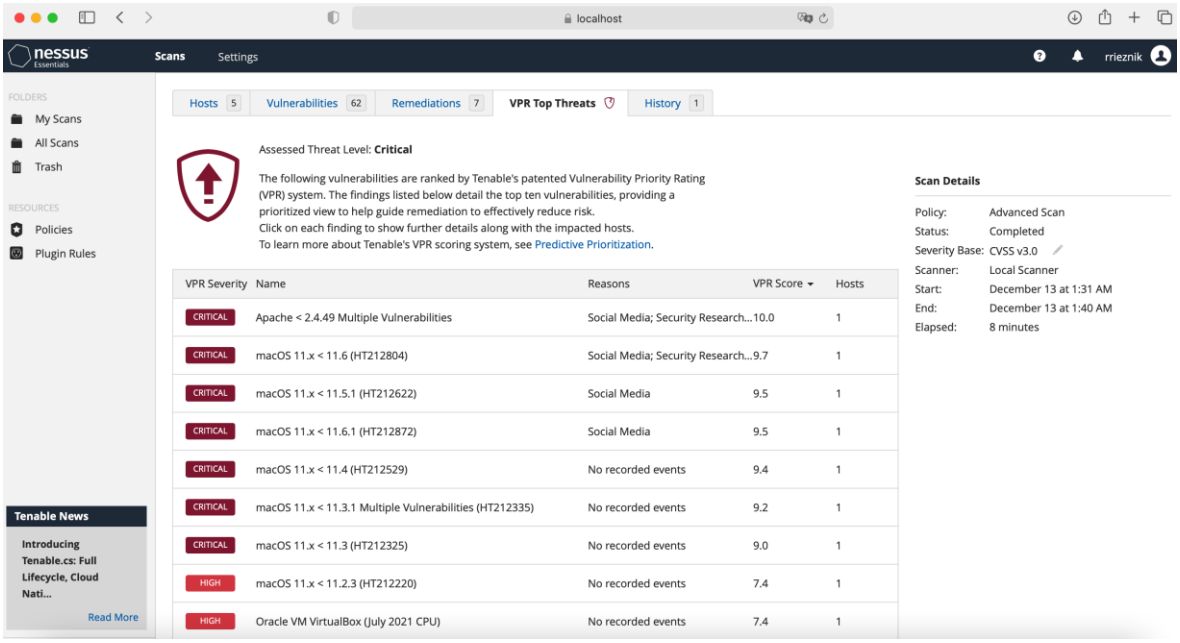

Рис. 3.16. VPR Top Vulnerabilities

Було розглянуто деякі з них більш детально. Наявна досить велика група вразливостей хоста 192.168.0.105 з встановленою ОС MacOS 11.2.1. і більшість вразливестей відносяться саме до версії ОС, яка не є актуальною та містить відомі «дирки». Наприклад критична вразливість «macOS 11.x < 11.3 (HT212325)». Дана вразливість містить опис – «На віддаленому хості працює версія macOS / Mac OS X 11.x до 11.3 Big Sur. Таким чином, на нього впливають численні вразливості, зокрема такі:

- проблема пошкодження пам’яті, яка може дозволити програмі обмежити доступ до читання пам’яті (CVE-2021-1808);
- проблема з пошкодженням пам'яті, яка може призвести до несподіваного завершення роботи програми або запису в пам'ять ядра (CVE-2021-1828);
- Проблема, яка може дозволити шкідливій програмі виконувати довільний код з привілеями ядра (CVE-2021-1834)».

Варто зауважити, що Nessus не тестував цю проблему, а натомість покладався лише на номер версії операційної системи, який сам повідомляє про наявність вразливості.

Додатково, Nessus повідомляє про шляхи вирішення деяких вразливостей, як, наприклад з вразливістю «IP Forwarding Enabled» середнього рівня, що була виявлена на хості 192.168.0.1 (роутер). Як видно з рисунка, надвіть надаються відповідні команди залежно від операційної системи (Рис. 3.17.).

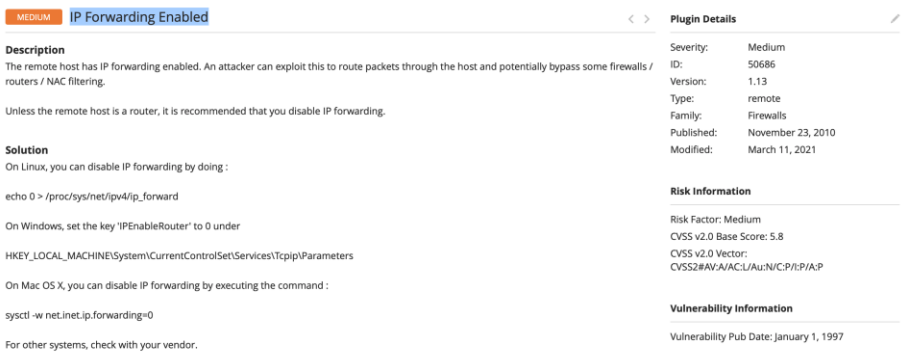

Рис. 3.17. Вразливість IP Forwarding Enabled

Щодо виявлення інших типів вразливостей – було ідентифіковано вразливість «APSB21-18 Adobe Creative Cloud Desktop < 5.4 Multiple

Vulnerabilities» високого рівня, яка стала можливою через застарілу версію ПЗ Adobe. Через це стало можливим запис довільного файлу, що призводить до виконання коду. (CVE-2021-21068), ін'єкції команд ОС, яка призводить до виконання довільного коду, неправильна перевірка введення що може дозволити зловмиснику підвищити свої привілеї.

Також на одному з серверів, а саме сервері баз даних було виявлено вразливість середнього рівня «SSH Weak Algorithms Supported». Nessus виявив, що віддалений SSH-сервер налаштований на використання потокового шифру Arcfour або взагалі без шифру. RFC 4253 не радить використовувати Arcfour через проблему зі слабкими ключами. І також надав рекомендації та шляхи вирішення цієї вразливості.

У вкладці «Remediations» можемо спостерігати загальні дії, які варто провести, щоб зменшити кількість вразливостей через не встановлені відповідні версії ПЗ або їх відповідні плагіни, що знаходяться на всіх відсканованих хостах (Рис. 3.18).

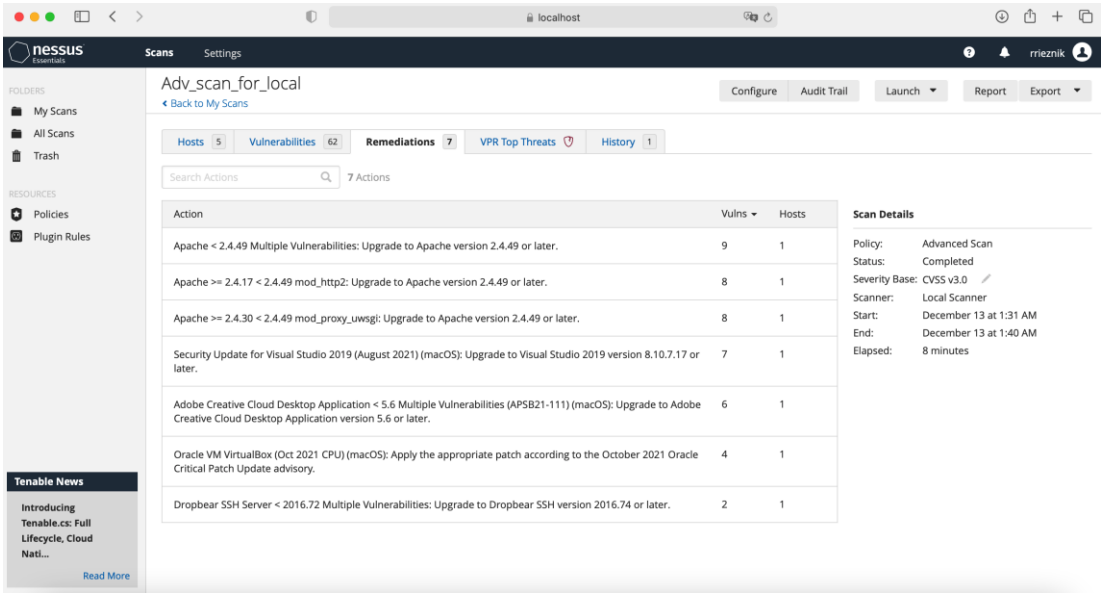

Рис. 3.18. Дії щодо усунення вразливестей через оновлення ПЗ

Також формуємо звіт щодо проведеного сканування, за таким же принципом, який розглядався раніше. Та отримуємо зручний до сприйняття мультимедійний звіт в форматі *.html в розрізі хостів, повністю готовий до використання, представлення та аналізу (Рис. 3.19.).

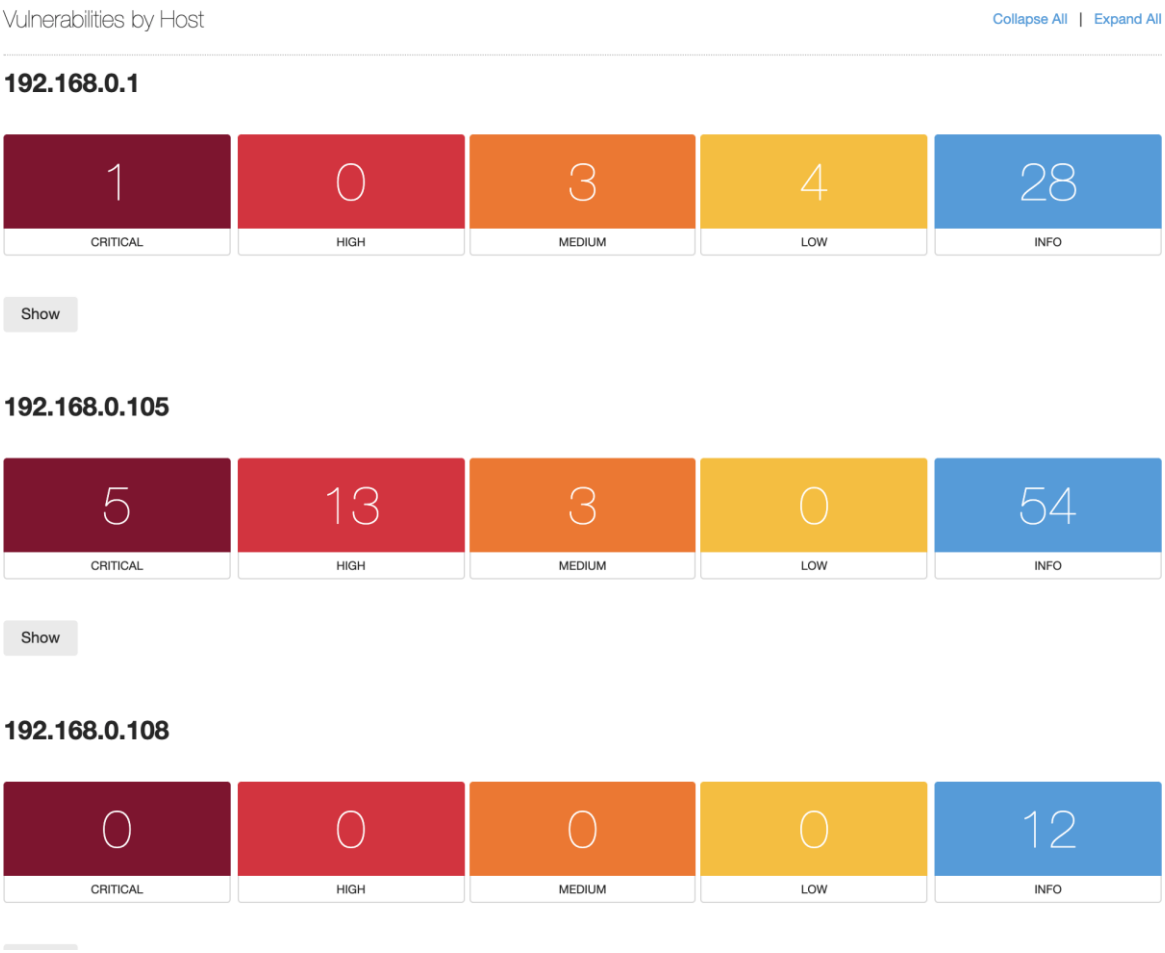

Рис. 3.19. Сформований звіт

Отже, на практиці пересвідчилися, що Nessus Vulnerability Scanner від компанії Tenable навіть у безкоштовній Essentials-версії є досить простим у використанні, але в той же час потужним сканером вразливостей. Головною його перевагою є те, що в ньому завжди можна знайти актуальні моделі загроз, на можливість експлуатації яких він швидко та якісно перевірить потрібну корпоративну мережу.

3.3 Розроблення рекомендацій щодо застосування технології виявлення вразливостей в корпоративній інформаційній системі

Провівши роботу з розгортання середовища та його сканування Nessus слід виділити певні моменти та рекомендації щодо оптимізації процесу виявлення вразливостей в КІС

Пробна версія надає всі можливості ефективної оцінки вразливостей та слабких місць у мережі. Після завершення сканування можливо створювати звіти за його результатами, які допоможуть продемонструвати якість сканера Nessus другим учасникам бізнесу. Звіти можуть бути повними або короткими, також їх можна експортувати у форматах HTML або PDF.

Варто не нехтувати можливістю проведення сканування з використанням облікових даних сервісів та хостів так як, переважна більшість вразливостей не буде виявлена, якщо сканування проводиться без використання цих даних . У такому режимі сканеру доступні всі повноваження адміністратора або root-а, або інший набір привілеїв, який вважається прийнятним, що дозволить повністю просканувати будь-яку частину мережі. Призначайте облікові дані на свій розсуд у початковій конфігурації сканування.

Необхідно використовувати динамічне та просунуте сканування, за допомогою якого можна налаштувати шаблон сканування, орієнтований на специфічні місця потенційного ризику, наприклад, конкретні CVE, які включені в останні бюлетені Microsoft, або вразливості в Java-додатках.

Створіть динамічні фільтри, вибравши атрибути, які потрібно відстежити, і відповідні плагіни будуть автоматично додаватися до вашої політики в міру їхнього випуску командою плагінів Tenable.

Використовуйте функцію «Live Results». При кожному оновленні плагінів ця функція виконує офлайн оцінку вразливостей за допомогою аналізу даних минулих сканувань, і цей процес не навантажує мережу або хости. Якщо ви проводите сканування нечасто або нерегулярно за допомогою функції Live Results, то зможете отримувати сповіщення про потенційні проблеми в режимі реального часу.

Не забувайте, що даний сканер має службу онлайн підтримку, представники якої доступні цілодобово. Клієнти можуть отримати підтримку по телефону, електронній пошті або онлайн-чату. Клієнти також можуть увійти на портал підтримки Tenable, щоб отримати доступ до бази знань і документації продукту, а також відкрити заявки на підтримку. Tenable пропонує безкоштовне навчання на вимогу 24/7, а також забезпечує віртуальне навчання в прямому ефірі, навчання в класі в навчальних центрах Tenable і індивідуальне навчання на місці в місцях для клієнтів за плату.

Сканер вразливостей Nessus є одним із найпоширеніших сканерів вразливостей в індустрії кібербезпеки сьогодні. Функціональність, яка отримується, особливо з комерційною версією, є повною гарантією співвідношення ціни та якості. Хоча також важливо підтвердити виявлення вразливостей, запустивши інші сканери вразливостей, щоб виключити можливість помилкових спрацьовувань, функції Nessus виправдовують його популярність.

Важливо сфокусуватися на виявленні вразливостей. Тому що кібербезпека починається з моніторингу, а оцінка вразливостей - це фундамент ефективного кіберзахисту. Пам'ятайте, що успіх якісної інформаційної безпеки – це регулярний аудит!

ВИСНОВКИ

Було досліджено процес виявлення вразливостей та визначено, що він є невід'ємною частиною в роботі корпоративної інформаційної мережі та в загальній роботі підприємства.

Встановлено, що вразливість – це недолік, який може призвести до порушення конфіденційності, цілісності або доступності інформаційної системи. А сканери вразливостей безпосередньо використовуються для їх ідентифікації, що дозволяє співробітникам з інформаційної безпеки підприємства швидко застосовувати послідовний, комплексний та чіткий підхід до вирішення загроз та ризиків безпеці.

Проведені в роботі аналізи та дослідження щодо особливостей роботи сканерів та процесу виявлення вразливостей в цілому, напрямлені на підвищення ефективності забезпечення інформаційної безпеки підприємтсва.

Також було досліджено програму Nessus версії Essentials, яка є лідером ринку серед засобів сканування та дозволяє оцінювати конфігурації, знаходити вразливості та вразливі місця кінцевих точок мережі.

Було визначено, що Nessus може сканувати: вразливості, які можуть дозволити несанкціонований контроль або доступ до конфіденційних даних у системі; неправильні конфігурації; паролі за замовчуванням, кілька поширених паролів і порожні/відсутні паролі в деяких системних облікових записах; вразливі місця відмови в обслуговуванні.

Було виготовлено технологію виявлення вразливостей, яка включає в себе інвентаризацію мережі, налаштування первинного сканування хостів, налаштування поглибленого сканування, розбір результатів та формування звітності за проведеними скануваннями.

Таким чином, на основі проведених досліджень, були розроблені рекомендації щодо застосування технології виявлення вразливостей.

ПЕРЕЛІК ПОСИЛАНЬ

1. Фролов Є. Современные концепции управления в производственной логистике, MES для дискретного производства — метод вычисляемых приоритетов / Є. Фролов., 2011. – 320 с.

2. Інформаційні системи і технології в управлінні організацією. // Вінниця: ПП Едельвейс і К. – 2015. – С. 496.

3. Інформаційні системи та технології в економіці // Укладач: Кельдер Т. Л., доцент кафедри економічної кібернетики ЗДУ. – К., 2008.

4. Базилевич В. Аналіз методів захисту від кіберзагроз в бездротових мережах стандарту IEEE 802.11 / В. Базилевич., 2017. – 222 с.

5. Корпоративна інформаційна система [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Корпоративна_інформаційна_система.

6. Інформаційні технології автоматизації управління в масштабах корпорації [Електронний ресурс] – Режим доступу до ресурсу: https://textbook.com.ua/informatika/1473447557/s-12.

7. Інформаційно-комунікаційна безпека в суспільстві: витоки проблем [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://lexinform.com.ua/dumka-eksperta/informatsijno-komunikatsijna-bezpeka-v-suspilstvi-vytoky-problem/.

8. VULNERABILITY STATISTICS REPORT [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://info.edgescan.com/hubfs/Edgescan2021StatsReport.pdf.

9. Сканування, виявлення та управління вразливостями [Електронний ресурс] – Режим доступу до ресурсу: https://www.sibis.com.ua/ua/services/sybersecurity/skanirovanie-vyyavleniya-i-upravleniya-uyazvimostyami/.

10. Рєзнік Роман Вікторович. Порівняння шляхів та засобів виявлення вразливостей в корпоративній інформаційній системі. ВСЕУКРАЇНСЬКА НАУКОВА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ». Державний Університет Телекомунікацій. 27 жовтня 2021. Тези доповідей. С. 95 – 96. http://www.dut.edu.ua/uploads/p_2099_79407917.pdf.

11. Vulnerability assessment [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis.

12. CIS Controls [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.sans.org/blog/cis-controls-v8/.

13. Pentesting [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.tadviser.ru/index.php/Статья:Pentesting_(пентестинг).

14. Найкращі інструменти та програмне забезпечення сканування вразливості [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://websetnet.net/uk/6-best-vulnerability-scanning-tools-and-software/.

15. Найкращі інструменти та програмне забезпечення сканування вразливості [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://websetnet.net/uk/6-best-vulnerability-scanning-tools-and-software/.

16. Rapid7 Overview [Електронний ресурс] – Режим доступу до ресурсу: https://softprom.com/ru/vendor/rapid7/product/rapid7-nexpose.

17. Nessus Teneble [Електронний ресурс] – Режим доступу до ресурсу: https://www.tenable.com/products/nessus.