Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Факультет комп’ютерних наук
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

«Допущено до захисту»
В. о. завідувача кафедрою БІСТ
Мелкозьорова О. М.
_____
« » 2024 р.

Пояснювальна записка
до кваліфікаційної роботи бакалавра
на тему: «Розробка методики пошуку вразливостей та обґрунтування її властивостей»

оцінка « »
Голова ЕК
Лемешко О. В. _____

Керівник проф. Олійников Р. В.
Рецензент доцент Родінко М. Ю.
Виконавець: студентка групи КБ-41

_____ Дегнера. Д. О.

Харків – 2024

РЕФЕРАТ

В пояснювальній записці до дипломної роботи є : 43 сторінки, 24 рисунка, 1 таблиця, 1 додаток та 33 посилання на джерела.

Метою дипломного проекту є розробка методики пошуку вразливостей для регулярного сканування. Проведений аналіз сучасних методів сканування та вибір найкращих варіантів для використання у власній методиці. Проведений аналіз найпопулярніших методик сканування, виявлення їх недоліків для регулярного сканування та внесення переваг до своєї методики. Проведений аналіз вразливих місць сучасних мереж для розуміння на які проблеми при тестуванні на безпеку корпоративних мереж потрібно звертати увагу при підготовці індивідуальної методики тестування. Огляд сучасних інструментів для сканування та вибір тих, що найкраще підходять для методики.

Методика є гнучкою для її зміни менеджером інформаційної безпеки для потреб компанії. Важливим аспектом розробленої залишається людський фактор, тому розроблено окремий пункт для перевірки обізнаності працівників компанії в сфері інформаційної безпеки. Таким чином, компанія може робити висновки щодо подальшого проведення тренінгів з інформаційної безпеки та стає більш стійкою до атак соціальної інженерії.

Ключові слова: СКАНУВАННЯ ВРАЗЛИВОСТЕЙ, СКАНЕРИ БЕЗПЕКИ, ПЕНТЕСТ, КІБЕРБЕЗПЕКА, ВРАЗЛИВІСТЬ, PTES, ISSAF, РОЗРОБКА МЕТОДИКИ

ABSTRACT

The explanatory note to the thesis contains: 43 pages, 24 figures, 1 table, 1 appendix, and 33 references.

The purpose of the thesis project is to develop a methodology for finding vulnerabilities for regular scanning. The analysis of modern scanning methods and the selection of the best options for use in their own methodology. Analyzing the most popular scanning methods, identifying their disadvantages for regular scanning and adding advantages to your own methodology. An analysis of vulnerabilities in modern networks to understand what problems in corporate network security testing should be taken into account when preparing an individual testing methodology. Review of modern scanning tools and selection of those that are best suited for the methodology.

The methodology is flexible enough to be modified by the information security manager to meet the needs of the company. The human factor remains an important aspect of the developed methodology, so a separate item has been developed to test the awareness of the company's employees in the field of information security. In this way, the company can draw conclusions about further information security trainings and becomes more resistant to social engineering attacks.

Keywords: VULNERABILITY SCANNING, SECURITY SCANNERS, PENTEST, CYBERSECURITY, VULNERABILITY, PTES, ISSAF, METHODOLOGY DEVELOPMENT

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІШІ – Штучний інтелект

CWE - Common Weakness Enumeration

DDOS – Distributed Denial of Service

IP - Internet Protocol

IPSec - IP Security

IoT - Internet of Things

ISSAF - Information System Security Assessment Framework

L2F - Layer 2 Forwarding Protocol

L2TP - Layer 2 Tunnelling Protocol

Nmap - Network Mapper

OpenVAS - Open Vulnerability Assessment System

OSSTMM – Open Source Security Testing Methodology Manual

PPTP - Point-to-Point Tunneling Protocol

PTES - Penetration Testing Execution Standard

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

VPN - Virtual Private Network

ВСТУП

День сучасної людини починається набагато легше ніж для людей минулого. Сьогодні багато речей є автоматизованими. Інтернет речей (IoT – Internet of Things) – це мережа фізичних об'єктів, які підключені до Інтернету та обмінюються даними без необхідності людської інтеграції. Завдяки швидкому розвитку технологій, IoT стає все більш поширеним і затребуваним у різних галузях, але зростає й кількість кібератак на пристрої IoT, що зумовлює важливість кібербезпеки цих технологій. [1]

Розумні кондиціонери регулюють температуру в приміщенні, базуючись на даних про температуру, сонячне світло, час доби, вологість, погоду. Аналізуючи всі показники він визначає як зробити кімнату максимально комфортною для людей. І також багато інших пристроїв, які роблять життя людини більш комфортним.

Сучасний світ також дає можливість скористатися безпілотними машинами, де «водій» точно не буде перевищувати швидкість та іншим чином порушувати правила дорожнього руху. Натомість, сама машина прорахує найзручніший та найшвидший маршрут.

Також за допомогою дронів в агрокультурі можна перевіряти склад ґрунту, прогнозувати кліматичні зміни чи перевіряти стан здоров’я тварин. В ритейлі розумні пристрої допомагають найточніше налаштовувати рекламу, аналізуючи досвід покупця та показучи саме те, що потрібно конкретному клієнту.

Найголовнішим буде згадати інтернет речей у сфері охорони здоров’я. Він допомагає краще проаналізувати стан здоров’я пацієнта - можна спостерігати за серцебиттям, рівнем глюкози, пульсом та рівнем кисню у крові, знайти індивідуальний підхід до кожного, щоб підібрати потрібне лікування.

Тепер можна дистанційно слідкувати за станом здоров’я людей, не тримаючи їх під постійним наглядом в лікарнях - це все пристрої, які в реальному часі надсилають дані до медичних працівників та за потреби повідомляють, коли потрібно піти до лікаря.

За допомогою такого моніторингу значно поліпшилися достовірність експериментів та клінічних досліджень. Адже тепер можна не покладатись на те, чи зможе досліджуваний точно контролювати та описувати своє самопочуття, все і так буде зрозуміло з показників, а людина може продовжувати своє звичне життя.[2]

Спираючись на звіт Unit 42 IoT Threat Report [3] – 30% від усіх пристроїв підключених до мережі в середньому підприємстві - це IoT. Також дослідження розповідає про те, що більшість пристроїв IoT мають вразливості до атак високого та середнього рівнів. А база даних Gartner Machina IoT Forecast прогнозує, що вже до 2030 року кількість пристроїв, що буде мати доступ до мережі буде в чотири рази більша ніж кількість працівників на підприємствах. Тобто бачимо тенденцію, що кількість пристроїв Інтернет Речей стрімко зростає, а безпека залишає бажати кращого. [3]

А що як доступ до наших пристроїв можуть мати злочинці? Описане вище дає зрозуміти наскільки важливою частиною нашого життя стали інформаційні технології і наскільки ці технології є вразливими до хакерських атак. Для того, щоб зрозуміти якими можуть бути наслідки хакерської діяльності розглянемо приклад.

Спираючись на базу знань *cloudflare* нам відомо, що програма-вимагач WannaCry станом на 12 травня 2017 року пошкодив понад 200 000 комп’ютерів у понад 150 країнах світу. Програма-вимагач – це зловмисне програмне забезпечення, що блокує доступ до файлів, щоб отримати викуп у користувача. Після оплати злодії обіцяють повернути доступ до файлів, проте в багатьох випадках користувач не отримує свої дані навіть після оплати. Хакери не люблять залишати зайвих «слідів», адже так їх легше виявити, тому розшифрування даних є невигідними для них. [4]

Типовий принцип роботи програми вимагача:

1. Спочатку програмі-вимагачу потрібно закріпитися на пристрої або в мережі.

2. Потім він шифрує файли користувача.

3. Останнім етапом показує повідомлення з інформацією про можливість викупити дані.[5]

Відомими жертвами атаки були: Національна служба охорони здоров'я Великобританії (відома як NHS), Honda, FedEx та Nissan. Цей приклад показує, що навіть великі компанії з розвиненою інформаційною безпекою і кваліфікованими спеціалістами є вразливими до хакерських атак, що вже й говорити про звичайних користувачів. Адже в кожного з нас є важливі документи, фотографії з рідними, які легко можуть стати причиною шантажу заради викупу. [4]

Отримавши доступ до мережі, хакери можуть в подальшому отримати доступ до банківських реквізитів, видалити важливі дані, мати доступ до камери, слідкувати за користувачем, використовувати ресурси системи, тим самим суттєво уповільнюючи роботу комп'ютера.

Тепер ми бачимо як саме нам можуть нашкодити дії хакерів, отже важливо задуматись про інформаційну безпеку.

1 АКТУАЛЬНИЙ СТАН І ПЕРСПЕКТИВИ РОЗВИТКУ МЕТОДІВ ВІДДАЛЕНОГО СКАНУВАННЯ ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ

1.1 Сучасний стан віддаленого сканування

В зв’язку з COVID-19 все більше компаній з 2019 року почало переходити на віддалену роботу, що стало серйозним викликом для спеціалістів з кібербезпеки. Компанії були більше зосереджені на утриманні бізнес-процесів, аніж на безпеці. Спеціалісти, які раніше займалися обслуговуванням локальних комп’ютерів зіштовхнулися з загрозами використання віддаленого доступу. Все більше компаній почало використовувати RDP, VPN, хмарні ресурси. Але важливо зазначити, що перехід не залишився в 2019 році, так як забезпечення безпеки – це постійний процес, контроль користувачів, перехід на хмарні інфраструктури, синхронізація з ними, проблеми конфігурацій та віддаленого доступу все ще залишаються актуальними і будуть актуальними в найближчі роки. [13]

Зміни в мережевій структурі та безпеці призвели до нових вразливостей, що в свою чергу вплинуло і на сканування мережі.

Інформаційна безпека - це система заходів, що дає змогу виявляти вразливі місця інформаційно-комунікативної системи підприємства, небезпеки, які загрожують їй, і методи нейтралізації виявлених загроз. [6]

Комп’ютерна мережа – це сукупність комп’ютерів та інших пристроїв, зв’язаних каналами передавання даних. За допомогою комп’ютерної мережі стає можливим спільне користування периферійними пристроями : принтерами, сканерами, модемами тощо. [7]

Мережевий порт - це унікальний ідентифікатор мережевого сервісу на окремому комп'ютері. [15]

Вище було написано про проникнення хакерів в мережі IoT, тому зазначимо поняття мережевої безпеки.

Мережева безпека – це процес захисту цифрових інформаційних активів, цілями безпеки є захист конфіденційності, підтримка цілісності та забезпечення доступності. [8]

Сканери безпеки - це програмні та апаратні засоби, призначені для діагностики і моніторингу різних елементів мережі, що дозволяють шляхом сканування мережі, персональних комп'ютерів і додатків, оцінювати і усувати вразливість. [20]

Пасивна розвідка - пошук інформації у відкритих джерелах, коли жертва ніяк не може дізнатися про розвідувальні дії. [24]

Активна розвідка - розвідка за допомогою спеціального програмного забезпечення, яке може бути виявлено захисними системами жертви. [24]

Деякі з можливих загроз мережі: [9]

- Шкідливі програми
- Програми-вимагачі
- Атаки «людина посередині»
- Фішинг
- DDoS
- Інсайдерські загрози

Безпеку мережі можна досягти за допомогою надійного багаторівневого захисту: захист роутера та захист окремих пристроїв.

Способи забезпечення безпеки мережі: [10]

- проксі-сервери;
- системи виявлення та запобігання загрозам злому;
- засоби захисту від цільових атак;
- міжмережеві екрани;
- системи мережевого моніторингу;
- VPN;
- Та інші.

Але варто зазначити, що в засобах забезпечення безпеки також бувають вразливості, тому важливою є перевірка та перегляд безпеки самих засобів.

Задля захисту потрібно знайти слабкі місця в системі до того як це зроблять зловмисники, тому потрібно періодично перевіряти системи на вразливості.

Вразливість - це слабке місце або недолік, який дозволяє зловмиснику порушити цілісність системи. [11]

Експлойт - техніка, яка використовує вразливість для здійснення атаки. [11]

Для деяких вразливостей вже може існувати експлойт, а для деяких ні.

В яких місцях можуть зустрічатися вразливості: [12]

- Обладнання, пристрої
- Бізнес-процеси
- Програмне забезпечення
- Персонал
- Політики безпеки

Для перевірки безпеки організації з правами людини, що має доступ до мережі – проводиться внутрішнє сканування вразливостей.

Для перевірки безпеки організації з точки зору людини, що не має доступу до мережі – проводиться зовнішнє сканування вразливостей.

1.2 Проблемні моменти при скануванні [14]

На які проблеми при тестуванні на безпеку корпоративних мереж потрібно звертати увагу:

1) Облікові записи користувачів

Системи RDP часто мають проблему з слабкими користувацькими паролями. Багато компаній не приділяють достатньо уваги політикам управління паролями, що полегшує роботу зловмисникам. Так реальними стають атаки грубої сили, наприклад, password spraying, коли зловмисник використовує найбільш популярні паролі на всі відомі облікові записи.

2) Порти

Необмежений доступ до портів є проблемою. Особливо зараз це стосується 3389 порту, який використовується для віддаленого підключення за протоколом RDP. Він має бути закритим від підключення через відкритий інтернет без строгої політики паролей та відсутності безпечного тунелю VPN.

3) Протидія атакам методом перебору паролей

Такі атаки дають можливість зловмиснику підібрати пароль до моменту, коли він їх все ж підбере. Отже спроби входу мають бути обмеженими за кількістю та компанія повинна вести детальне логування дій в мережі для запобігання доступу хакерів до серверів.

4) Встановлення останніх оновлень та патчів

Багато вразливостей вже виправлені в оновлених версіях. Але багато людей не ставляться до оновлень з серйозністю, так як не повністю розуміють ризики вразливостей. Задачею спеціалістів з кібербезпеки в компанії є своєчасне встановлення оновлень, патчів та проведення лекцій з інформаційної безпеки для співробітників стосовно цього.

5) Управління привілеями користувачів

Важливе правильне розподілення прав між користувачами і видача тільки тих прав, які потрібні для роботи конкретній людині. Ситуація де звичайний користувач має права адміністратора мережі є критично небезпечною та потребує негайного реагування. Тому це має контролюватися та чітко зазначатися права кожного користувача в документації.

6) Кінцеві точки доступу

Важливим і складним аспектом є контроль кінцевих точок доступу. В період віддаленої роботи, контроль програмного забезпечення, що встановлено на особистий пристрій користувача є складним завдання для команди інформаційної безпеки. Складно контролювати, які носії вставляються в пристрій та чи систематично людина встановлює останні оновлення(поширена ситуація, коли системні адміністратори помічають, що оновлень давно не було, коли користувач

сам звертається через неправильну роботу системи/програм). Користувачі часто нехтують політиками безпеки. Тому можливі підключенням до сервісів компанії через особистий обліковий запис,(де можуть бути встановлені заражені вірусами програми) а не окремий робочий, на який розповсюджуються політики безпеки. Людський фактор так і залишається одним з найвразливіших моментів в кібербезпеці.

7) VPN

Більшість компаній підвищують рівень своєї безпеки за рахунок використання VPN, тому хакери постійно шукають і експлуатують нові вразливості в даній технології.

1.3 Перспективи розвитку віддаленого сканування

Все більше сфер починають працювати зі штучним інтелектом, кібербезпека не є виключенням. Майбутнє інформаційної безпеки буде впливати і на проведення віддаленого сканування. Штучний інтелект зможе покращувати виявлення загроз за допомогою алгоритмів машинного навчання, будуть можливим неймовірно швидкий аналіз великих обсягів даних. Нові алгоритми зможуть ідентифікувати шаблони та аномалії, що можуть свідчити про потенційні загрози. За допомогою нових технологій компанії зможуть раніше детектувати злочинні дії та реагувати на них.

На відміну від сучасних алгоритмів, штучний інтелект зможе швидко адаптуватися до нових загроз, нової поведінки шкідливих програм.

Штучний інтелект зможе сканувати системи, оцінювати вразливості та керувати ними, цей процес буде проходити набагато швидше ніж зараз і за менші кошти, що покращить захист компаній. ШІ зможе виявити слабкі місці в конфігураціях, системах, програмах, надаючи звіт організаціям із запропонованими рішеннями усунення з урахуванням ризиків.

Моделюючи дії зловмисників, ШІ зможе допомогти зрозуміти вразливі місця в інфраструктурі компаній. Тоді ця процедура буде доступнішою для

бізнесів, адже зараз за проведення пентесту компанії потрібно виділити багато коштів.

1.4 Постановка задачі досліджень

Метою даного дипломного проекту є дослідження відомих методів та методик пошуку вразливостей, розробка невеликої методики для регулярної перевірки компанії та її тестування. Так молодші фахівці з кібербезпеки чи системні адміністратори (в залежності від розмірів та ресурсів компанії) зможуть ретельно перевіряти свою мережу та вчасно реагувати на кіберінциденти.

Висновок: метою дипломного проекту є розробка методики. Проаналізувавши вразливі місця сучасних мереж, тепер розуміємо на які проблеми при тестуванні на безпеку корпоративних мереж потрібно звертати увагу при підготовці індивідуальної методики тестування:

1) Облікові записи користувачів
2) Порти
3) Протидія атакам методом перебору паролей
4) Встановлення останніх оновлень та патчів
5) Управління привілеями користувачів
6) Кінцеві точки доступу
7) VPN

2 ВІДДАЛЕНЕ СКАНУВАННЯ НА БАЗІ ПРОТОКОЛІВ ТРАНСПОРТНОГО РІВНЯ

2.1 Порти

В більшості засобів сканування порти поділяються на закриті, відкриті та фільтровані. Проте варто відмітити, що в залежності від сканеру статуси можуть відрізнятися. За допомогою відкритих портів можна виявити активні хости в мережі. Це дозволяє виявити точки входу для потенційних атак і вжити заходів щодо усунення вразливостей.

Відкритий.[16]

Основною ціллю сканування є визначення портів саме з таким статусом. Це означає, що на ньому активно запущена служба, порт приймає запити, можливе з'єднання за допомогою протоколів TCP та UDP. За допомогою відкритих портів можна виявити доступні в мережі служби.

Фільтрується.[16]

Такий статус може означати, що порт може бути прихований за міжмережевим екраном і його статус невідомий.

Закритий.[16]

Такий статус означає, що порт закритий.

Для початку, потрібно виявити всі хости в мережі. Для цього існують різні методи виявлення активних хостів:

2.2 Огляд методів сканування [16, 17, 18, 19]

Ping сканування. [16, 17, 18, 19]

Таке сканування допомагає визначити активні хости в мережі. Базується на широкомовній розсилці на активні хости. Засіб безпеки надсилає запити echo request кожному пристрою за вказаним діапазоном та чекає у відповідь echo reply. Якщо відповідь надійшла – пристрій є активним в мережі. Ця опція корисна системним адміністраторам для моніторингу доступу до серверів, діагностики. Важливе правильне налаштування засобів захисту периметру, щоб не надати

зайву інформацію зловмисникам. Зовнішнє сканування в корпоративних мережах може не спрацювати, тому що засоби захисту в більшості блокують ICMP відповіді або і весь протокол. Тобто можливо, що echo reply дійде до хоста, а echo request – ні. Але це стосується зовнішнього сканування, в локальній мережі Ping сканування може добре працювати.

TCP SYN пінгування. [16, 17, 18, 19]

Такий метод є дуже популярний, використовується в більшості випадків. За допомогою нього можна дізнатися про активність хоста в мережі та чи відкриті потрібні нам порти. При такому скануванні з'єднання не встановлюється до кінці, на потрібний нам порт відправляється повідомлення SYN(тобто пакет з встановленими SYN прапором, що означає, що ми хочемо встановити TCP-з'єднання з цілевим хостом) і чекаємо відповіді. Якщо відповідь буде SYN/ACK(тобто пакет з встановленим SYN/ACK прапором, що означає, що хост готовий встановити з нами з'єднання по вказаному порту) – порт відкритий, хост активний. Якщо ж у відповідь отримали RST – порт закритий. Але ці дві відповіді означають одне – хост активний.

TCP ACK пінгування. [16, 17, 18, 19]

ACK пінгування близьке до SYN пінгування - також використовується протокол TCP. Проте замість відправлення пакету зі встановленим прапором SYN, відправляється пакет з прапором ACK. Цей прапор відповідає за підтвердження отриманих даних в TCP. Але так як попереднього з'єднання не було і дані хост не відправляв – він відправить пакет з описаним вище прапором RST. Так ми дізнаємось про активність хоста.

Деякі системні адміністратори при налаштування міжмережевого екрану можуть заблокувати вхідне TCP з'єднання, тобто користувач зможе користуватися Інтернетом та ініціювати TCP з'єднання, але хтось ззовні мережі цього зробити не зможе. Саме тому TCP SYN пінгування та Ping сканування можуть не дати правильного результату на відміну від ACK пінгування. Але інші

налаштування можуть не пропустити і ACK пінгування через розпізнавання непередбачених пакетів як фіктивних.

TCP сканування за допомогою системного виклику connect. [16, 17, 18, 19]

У випадку, якщо SYN сканування не може використовуватись (користувач не має достатніх прав для формування сирих пакетів, або якщо сканується мережа з використанням IPv6) використовується TCP сканування за допомогою системного виклику connect. Сканер через операційну систему встановлює з'єднання з іншим хостом через системний виклик connect. Для того, щоб отримати інформацію про з'єднання сканер використовує Berkeley Sockets API .

Такий тип сканування вимагає більше часу від стандартного SYN сканування. SYN сканування працює з напіввідкритими портами, на відміну від роботи з системним викликом – де з'єднання встановлюється повністю. З мінусів не тільки час, описуваний спосіб також є більше помітним для системних адміністраторів та систем виявлень вторгнень – так як встановлені з'єднання будуть записуватись з лог файли.

UDP пінгування. [16, 17, 18, 19]

Такий метод використовує протокол UDP для пінгування хостів. Використання UDP робить сканування більш повільним ніж за допомогою TCP через те, що ми не встановлюємо зв'язок перед відправкою даних. Отже не маємо повідомлення про отримання як в TCP. Також складності та повільності сприяє те, що більшість служб будуть ігнорувати порожній пакет і ми не отримуємо жодного повідомлення, проте деякі все ж відповідають. Засіб сканування надсилає порожній пакет на цільовий хост. Відповідь з помилкою «порт недосяжний» повідомляє про закритий порт та працездатність системи. Якщо ж повідомлення буде містити інформацію про недоступність цільової машини, мережі чи перевищення TTL – машина вимкнена або недоступна. Протоколи, які найчастіше використовують UDP: DNS (53), NTP (123), SNMP (161), VPN (500, 1194, 4500), RDG (3391).

Сканування нестандартними ICMP запитами. [16, 17, 18, 19]

Протокол ICMP має не тільки echo запити, а ще й запити для отримання інформації. Це можуть бути як запит адресної маски чи поточного часу. Відповідь хоста на такий запит буде означати, що хост активний. Такі запити використовуються рідко. Якщо системний адміністратор відключив можливість стандартного Ping сканування echo запитами , але забув про інші види запитів протоколу ICMP – то можна спробувати.

TCP NULL, FIN, Xmas. [16, 17, 18, 19]

Методи TCP NULL, FIN, Xmas використовуються набагато рідше, вони базуються на RFC 793, згідно з яким при закритому порті, на вхідний пакет відмінний від RST, потрібно відповідати пакетом з RST. Саме через те, що метод базується на особливості специфікації, він працює не завжди. У методі NULL-сканування не встановлюється жоден біт в TCP-заголовку. На закритий порт, система відправляє відповідь пакет з бітом RST. Якщо порт відкритий - відсутній відгук. У методі FIN-сканування встановлюється біт TCP FIN у TCP-заголовку. Якщо порт закритий - генерується RST у відповідь. Якщо порт відкритий – буде відсутній відгук. У Xmas-скануванні встановлюються прапори FIN, PSH та URG в TCP-заголовку. Коли порт закритий, очікується відправка RST у відповідь. Якщо порт відкритий - відсутній відгук.

TCP-сканування Меймона. [16, 17, 18, 19]

Методика TCP-сканування Меймона дуже схожа на NULL, FIN і Xmas-сканування, але використовує запити FIN/ACK. Згідно з RFC 793 при використанні TCP на такий запит має генеруватися RST-пакет, якщо порт відкритий чи закритий. Меймона помітив вразливість, пов’язану з тим, що багато BSD систем, якщо порт відкритий не генерують новий RST пакет, а просто відкидають вхідний пакет.

Сканування TCP-портів прапорами SYN|FIN з використанням IP-фрагментації. [16, 17, 18, 19]

Метод сканування TCP-портів прапорами SYN|FIN з використанням IP-фрагментації схожий то описаних вище методів TCP SYN і TCP FIN пінгування.

Проте має деякі додаткові деталі. Невеликий пакет TCP поділяється на два IP-фрагменти та надсилається на цільову машину. На стороні цільової машини ці два пакети з'єднуються в один та обробляється як один звичайний пакет TCP з прапором SYN або TCP з прапором FIN. Таким чином можна обійти міжмережевий екран.

Висновки по розділу: Проаналізувавши найвідоміші методи сканування, вибираємо для використання в своїй методиці TCP SYN та UDP сканування. Протоколи, які найчастіше використовують UDP: DNS (53), NTP (123), SNMP (161), VPN (500, 1194, 4500), RDG (3391). При недоступності TCP SYN та TCP ACK пінгування використовуємо TCP сканування за допомогою системного виклику connect. TCP SYN знаходиться вище за пріоритетом, тому що TCP сканування за допомогою системного виклику connect займає більше часу і є більше помітним для системних адміністраторів та систем виявлень вторгнень – так як встановлені з'єднання будуть записуватись з лог файли.

3 ВІДДАЛЕНЕ СКАНУВАННЯ НА ПРИКЛАДНОМУ РІВНІ

3.1 Засоби віддаленого пошуку вразливостей

Є багато різних сканерів, кожен з яких має унікальні можливості, що робить їх корисними для різних завдань. Для досягнення максимально точних і повних результатів рекомендується використовувати кілька сканерів. [33]

Nmap (Network Mapper)

Nmap є одним з найбільш відомих мережевих сканерів. Він підтримує всі методи сканування, описані в розділі 2, і пропонує широкий спектр функцій для аналізу мереж.

Wireshark

Wireshark є популярним інструментом для аналізу мережевих пакетів. Його можна використовувати як для аналізу трафіку в мережі, так і для сканування мереж.

Zenmap

Zenmap - це графічний інтерфейс для Nmap, що робить його більш зручним для звичайних користувачів.

Angry IP Scanner

Angry IP Scanner - простий і швидкий інструмент для сканування IP-адрес, що надає базову інформацію про пристрої в мережі та їхні порти.

OpenVAS (Open Vulnerability Assessment System)

OpenVAS є системою інструментів для виявлення вразливостей. Вона пропонує широкий спектр тестів на проникнення і є відкритим програмним забезпеченням, яке часто використовується як альтернатива Nessus.

Netcat

Netcat - це мережевий інструмент, який дозволяє встановлювати TCP і UDP з'єднання для читання та запису даних у мережі. Він корисний для дослідження мереж, сканування портів та тестування з'єднань.

Masscan

Masscan є високошвидкісним сканером портів, який створений для швидкого сканування великих мереж.

Aircrack-ng

Aircrack-ng - це набір програм для аудиту та тестування бездротових мереж, що включає інструменти для сканування та аналізу.

Частіше його використовують для виявлення вразливостей у веб-додатках, але він також має можливості для сканування мережі на вразливості.

3.2 Nessus [22]

Nessus є найпопулярнішим інструментом для виявлення вразливостей та проведення тестів на проникнення в корпоративних мережах. Він дає можливість просканувати периметр різними методами та різними вже готовими шаблонами сканів, після сканування показує вразливості та методи їх усунення. В результатах сканування виводить загальні рекомендації, що зручно для оцінки вразливостей та подальшого покращення безпеки системи.

Інтерфейс Nessus:

Nessus має дві основні сторінки: Scans (рис. 3.1) та Settings (рис.3.2).

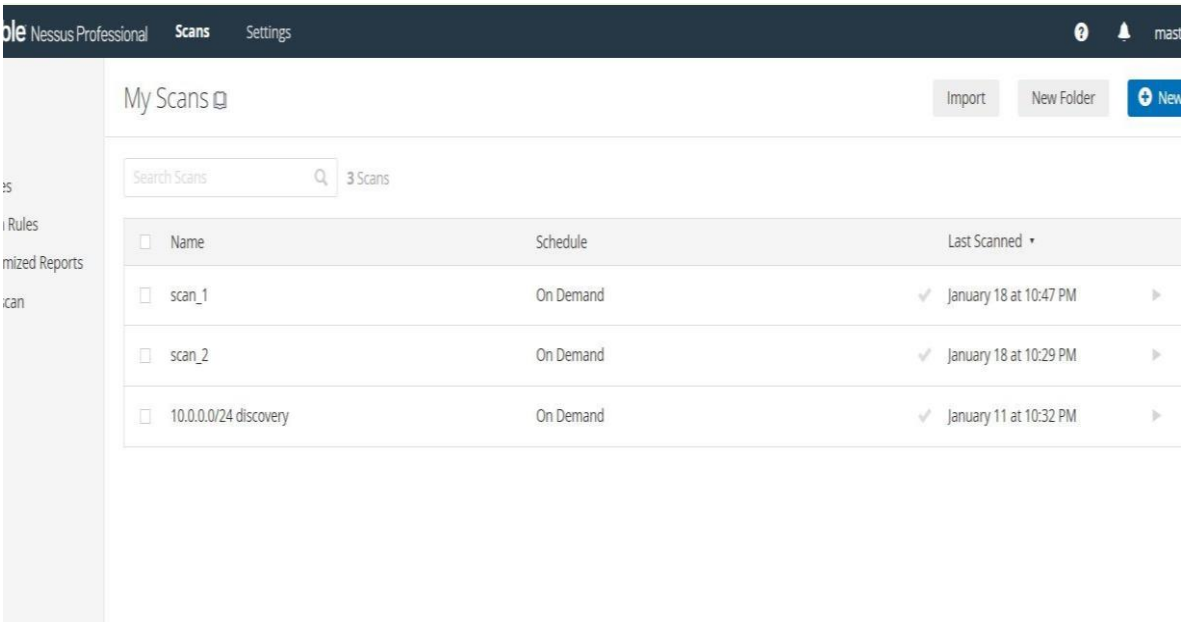

Рисунок 3.1 – Інтерфейс сторінки Scans

На сторінці Scans ми можемо побачити вже проведені сканування, що не були розподілені по папкам і створити нове сканування.

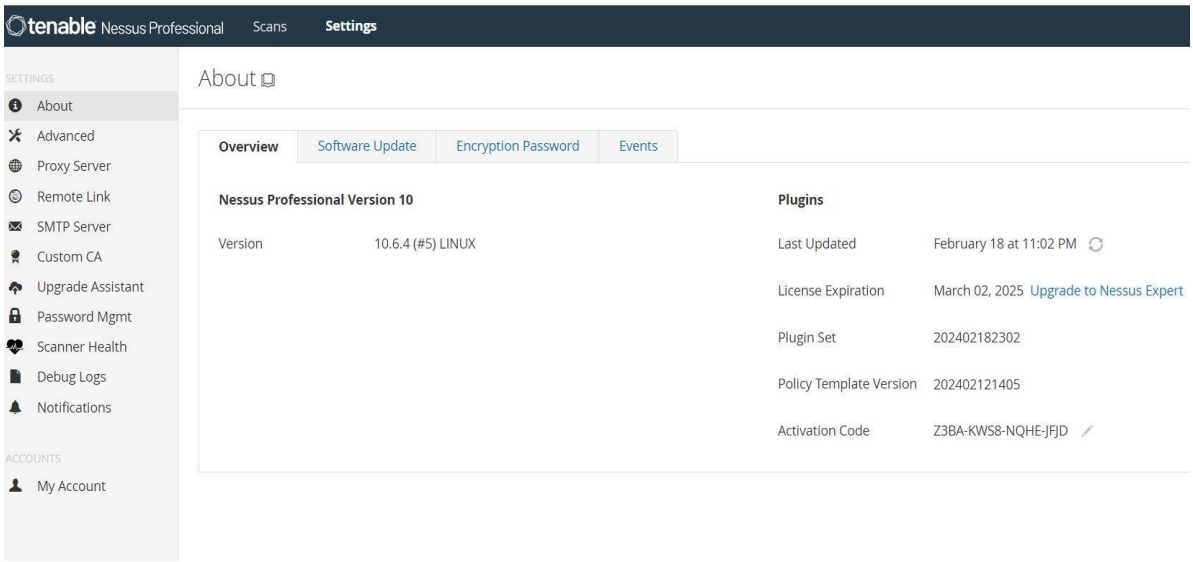

Рисунок 3.2 – Інтерфейс сторінки Settings

Також наведені вже готові шаблони сканування (рис. 3.3-3.5).

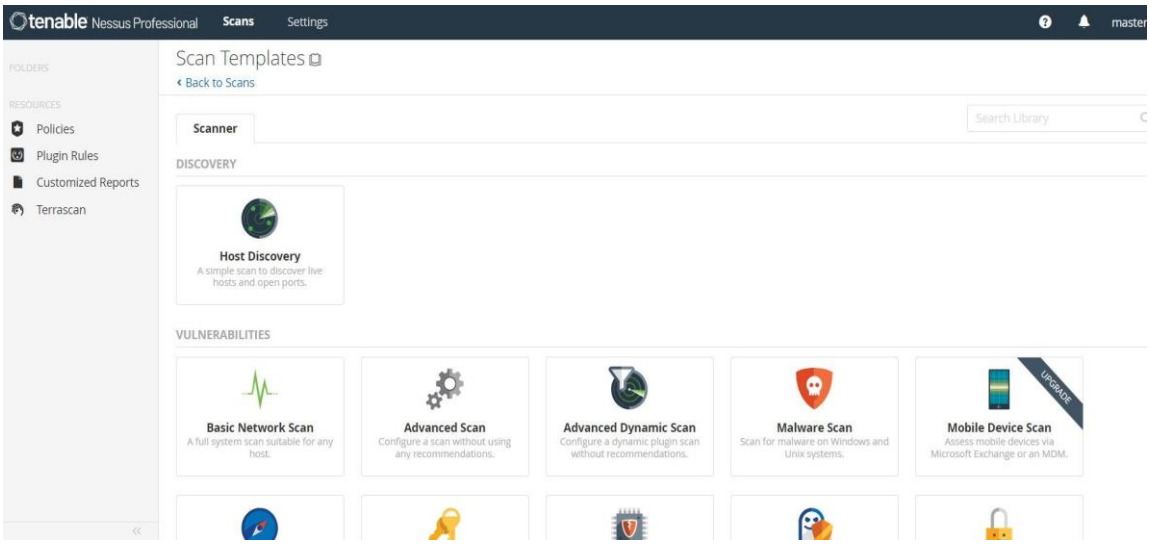

Рисунок 3.3 – Шаблони сканування

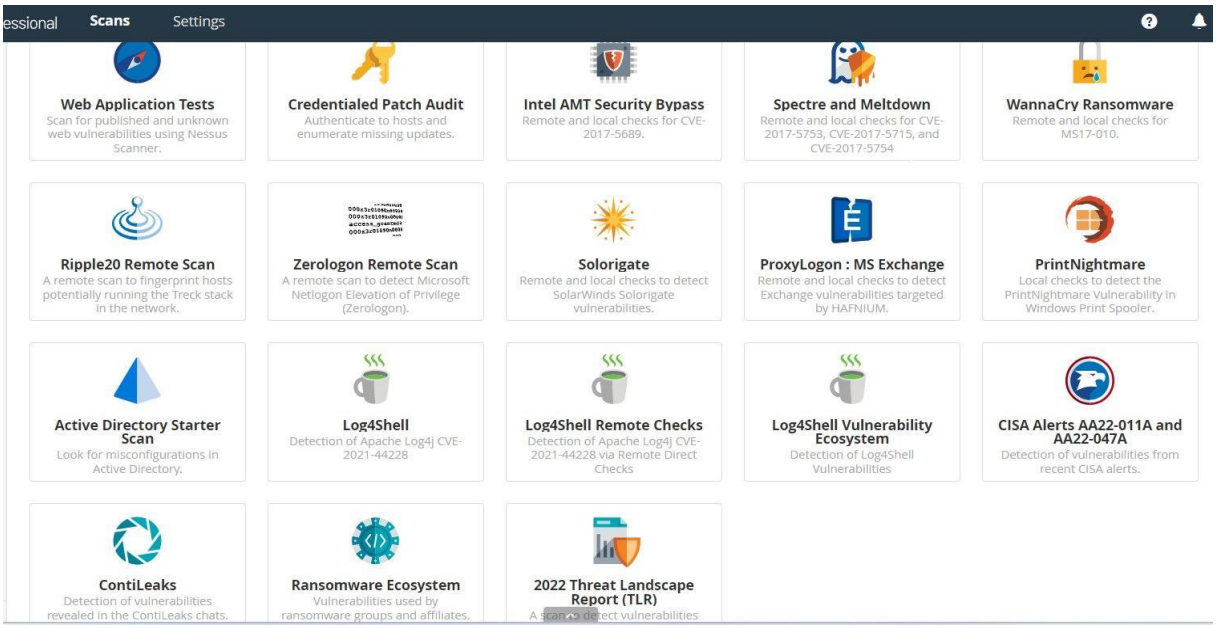

Рисунок 3.4 – Шаблони сканування для найпопулярніших вразливостей

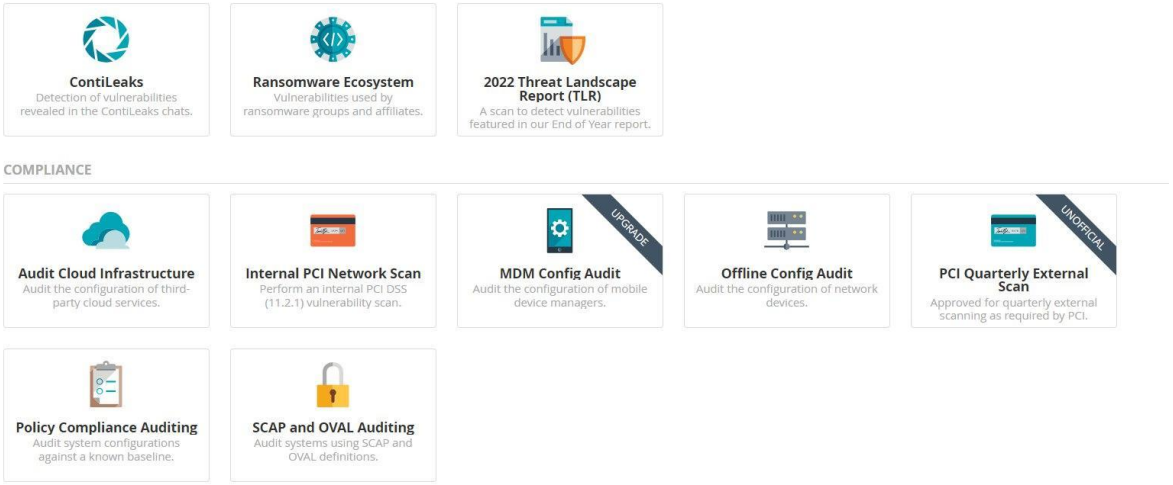

Рисунок 3.5 – Шаблони сканування для проведення аудиту на відповідності до політик

Приклад сканування наведений на рис. 3.6.

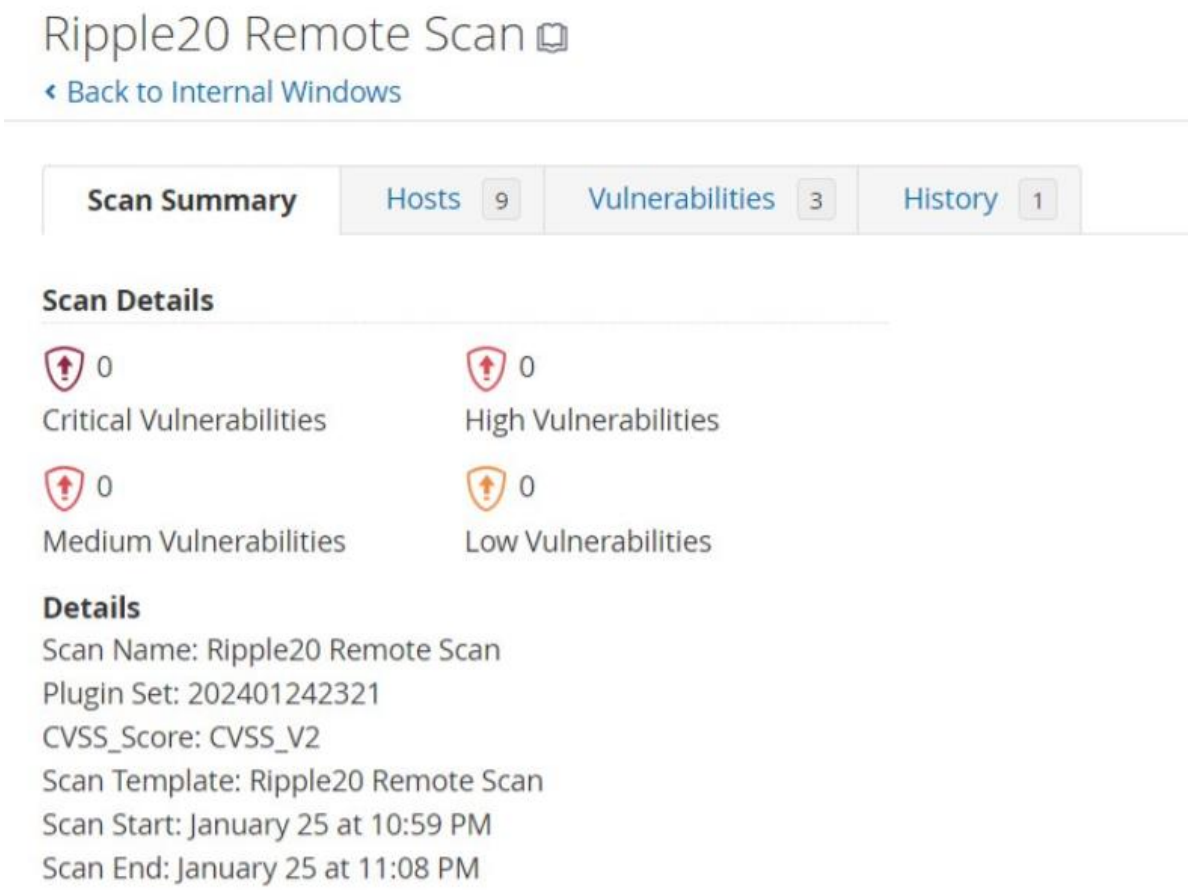

Рисунок 3.6 – Приклад результатів сканування

На останньому рисунку бачимо, що сканер надає нам загальний опис та оцінку виявлених вразливостей по рівнях критичності. На сусідній вкладці hosts приведений список просканованих хостів. На вкладці History можна переключатися між цим самим скануванням проведеними в різний час.

3.3 Огляд використання OpenVAS [23] (рис. 3.7-3.18)

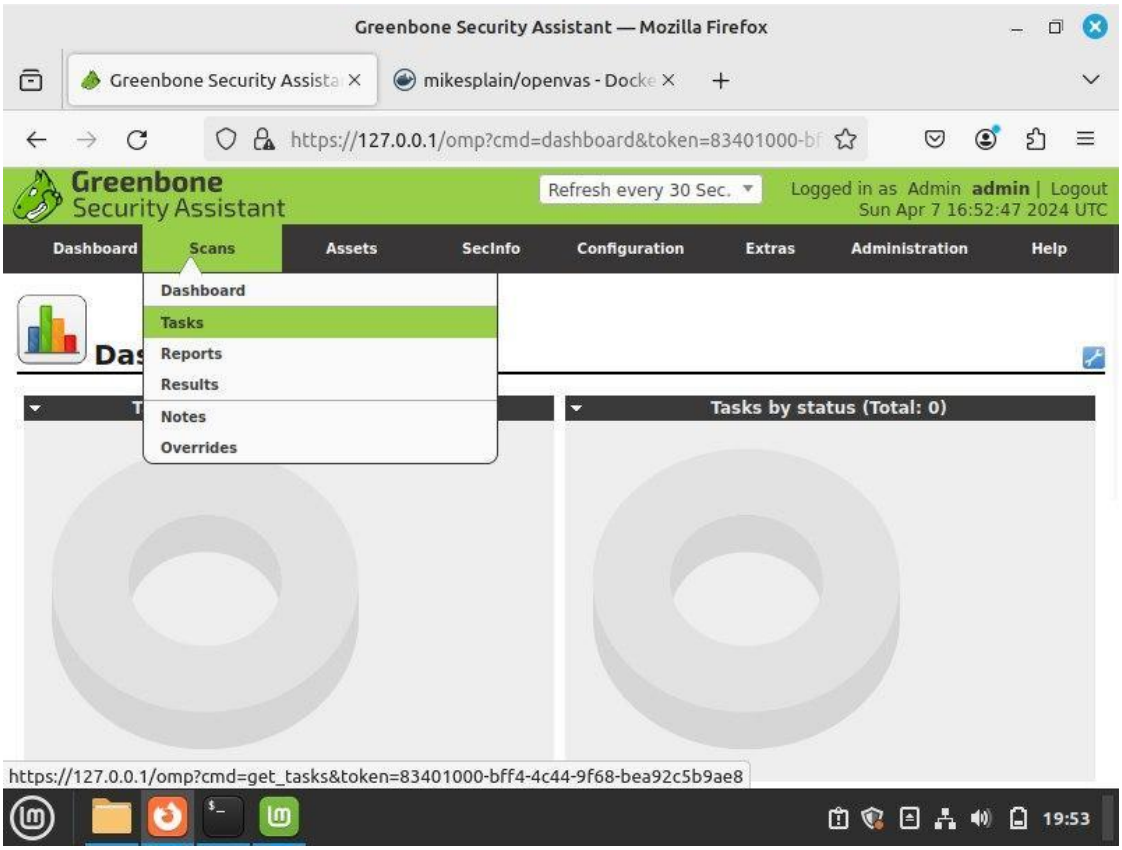

Рисунок 3.7 – Створення сканування

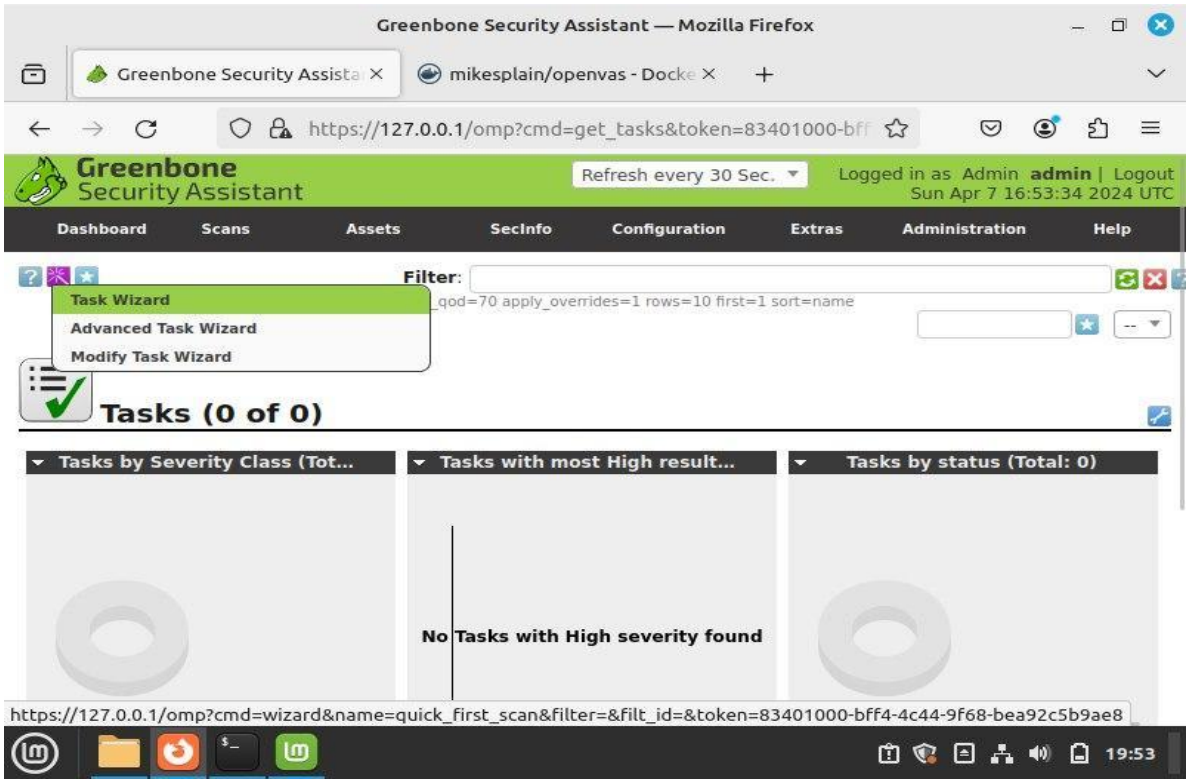

Рисунок 3.8 – Створення простого сканування

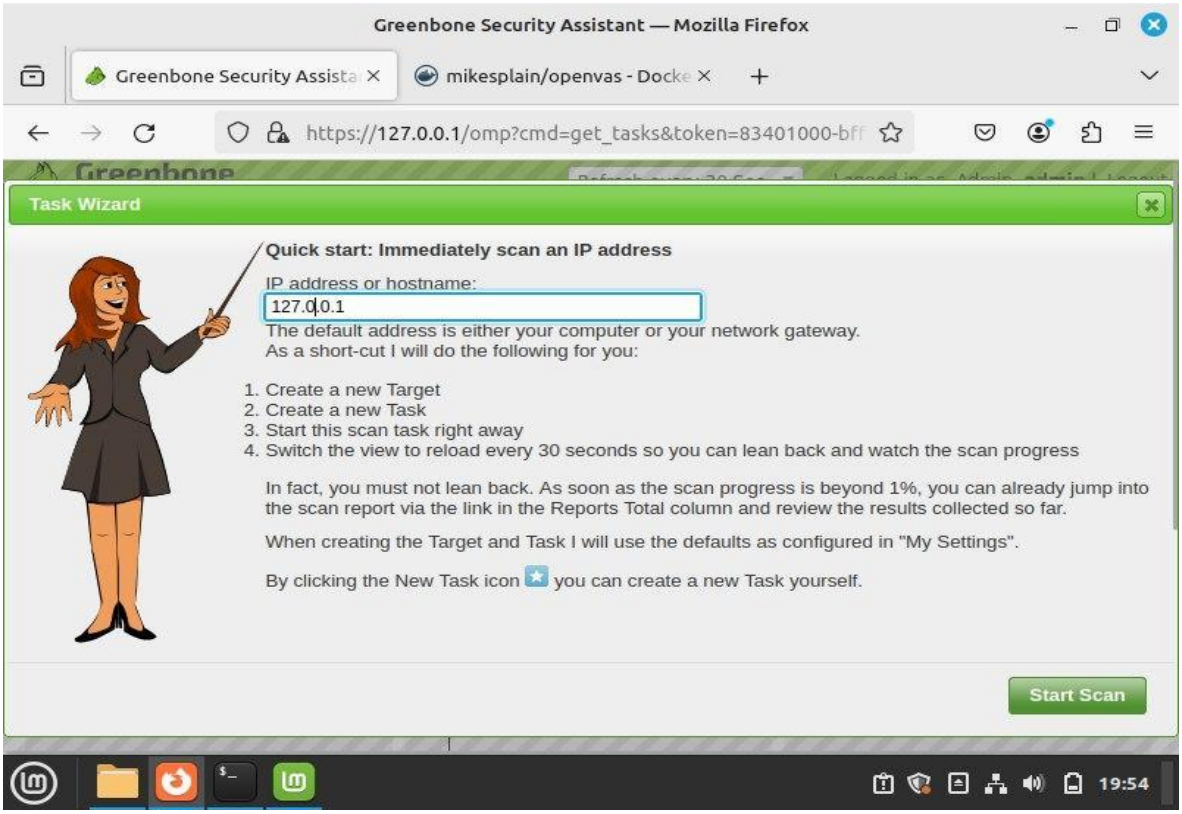

Рисунок 3.9 – Створення простого сканування

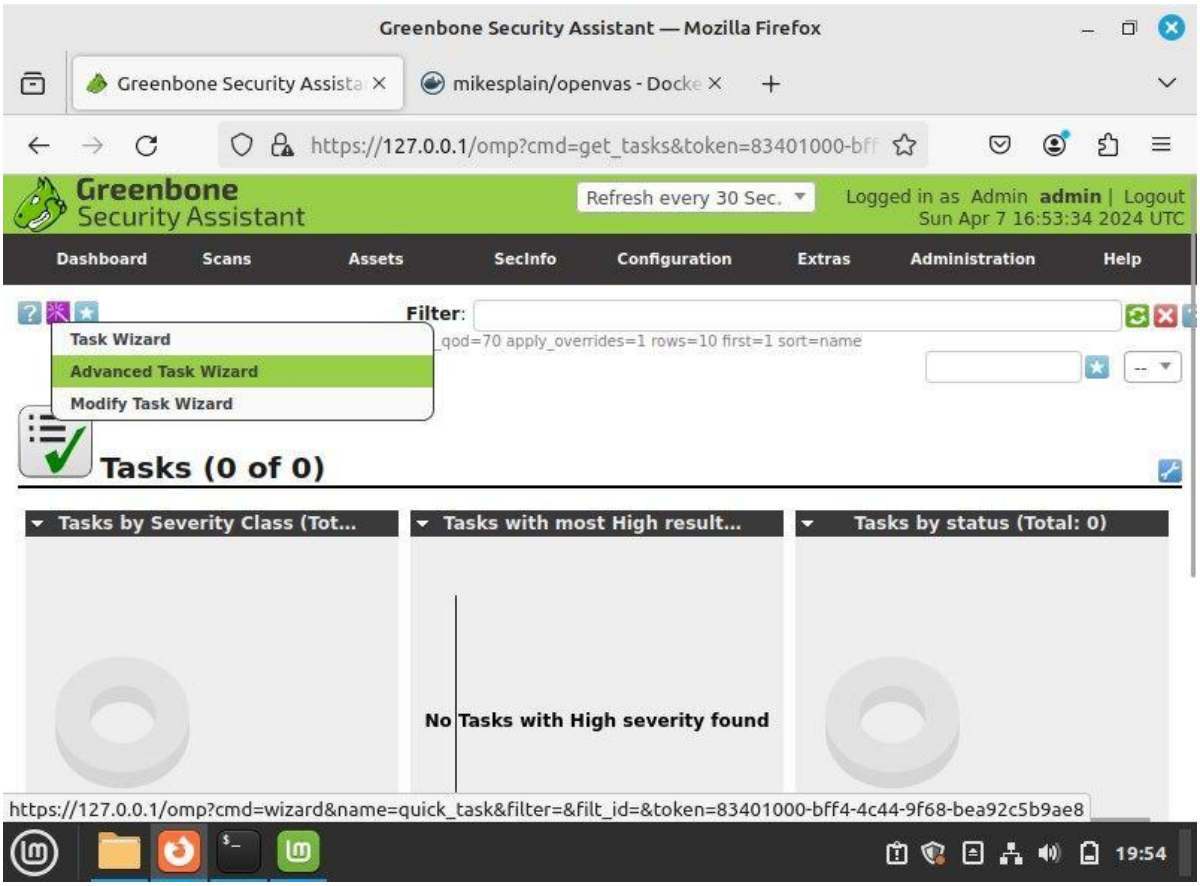

Рисунок 3.10 – Створення розширеного сканування

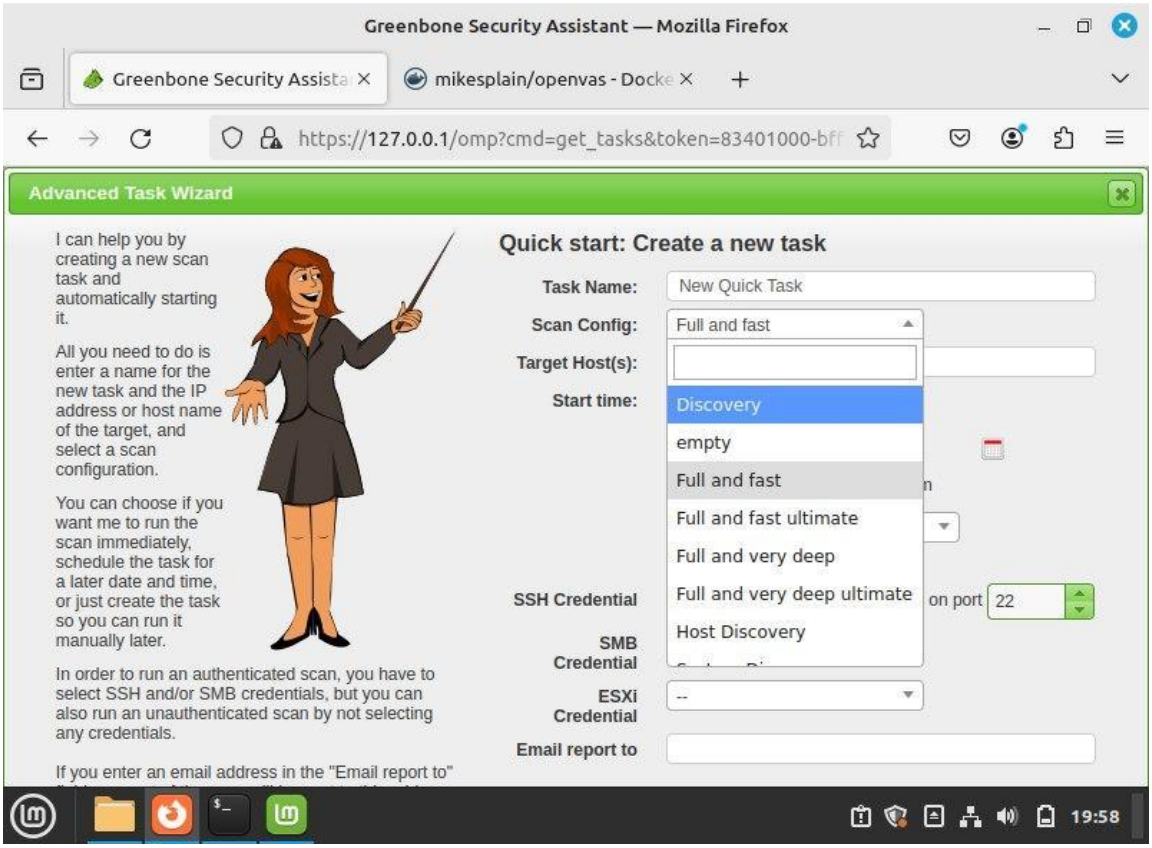

Рисунок 3.11 – Створення розширеного сканування

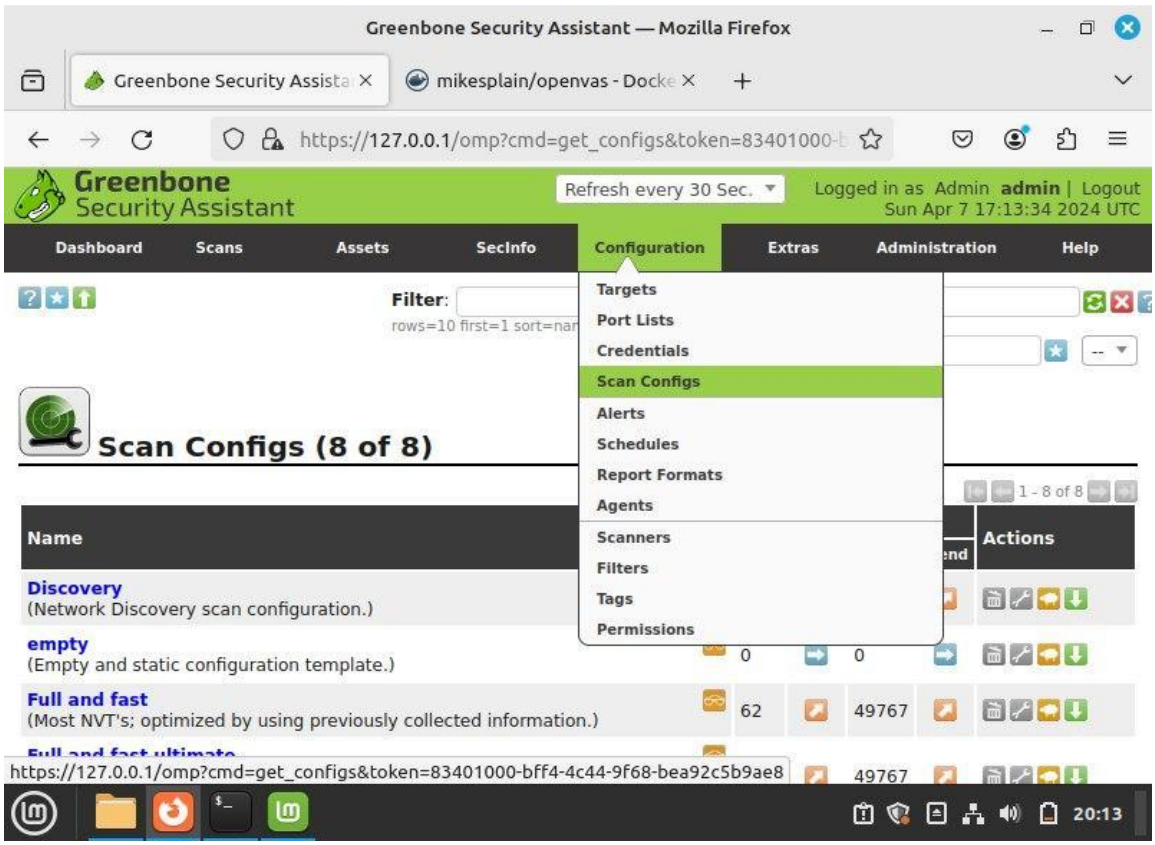

Рисунок 3.12 – Конфігурація сканувань

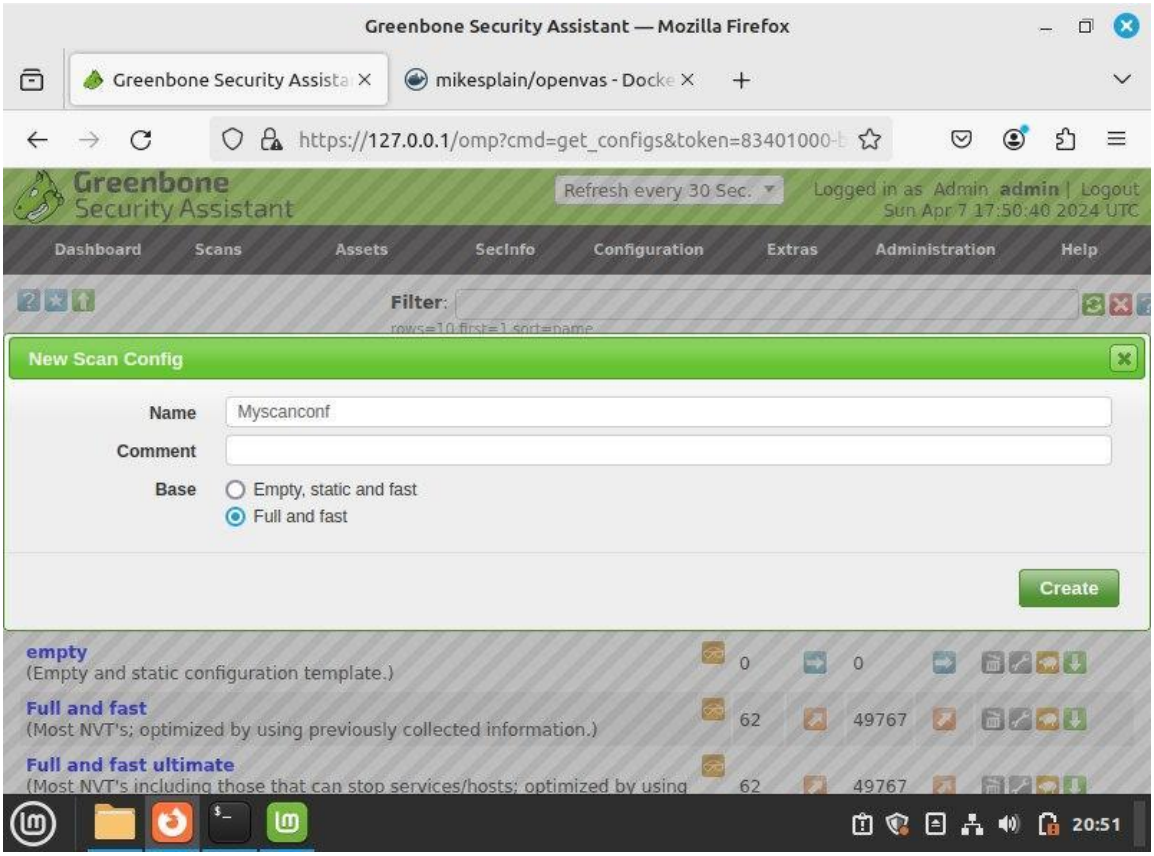

Рисунок 3.13 – Створення нового сканування

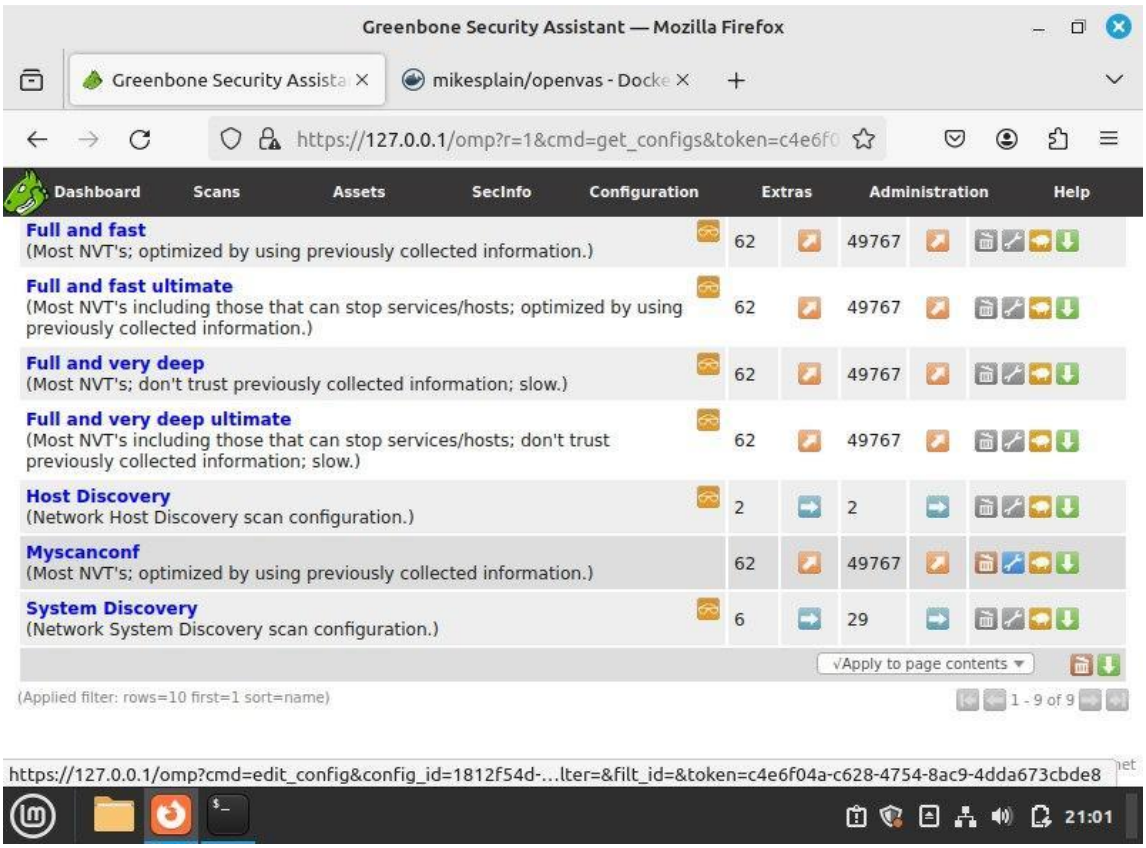

Рисунок 3.14 – Редагування нового сканування

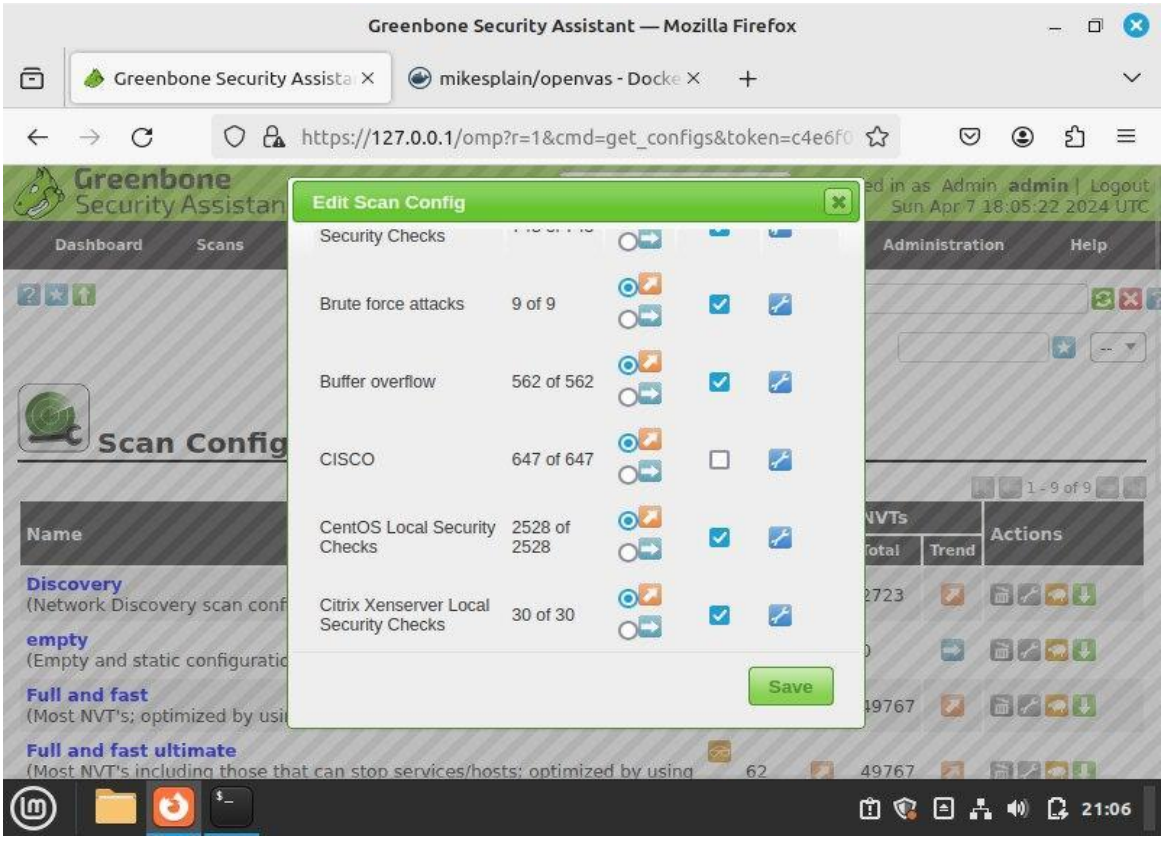

Рисунок 3.15 – Редагування конфігурації сканування

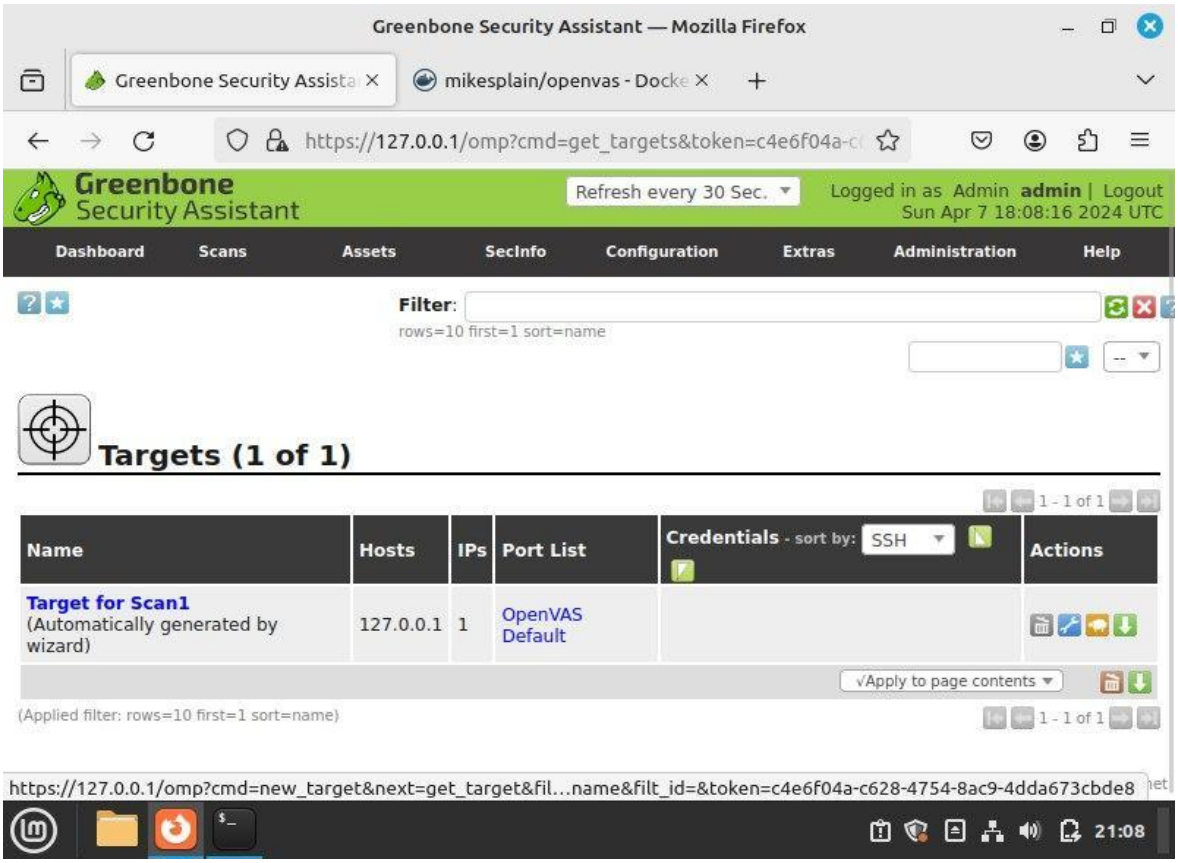

Рисунок 3.16 – Налаштування цілей сканування

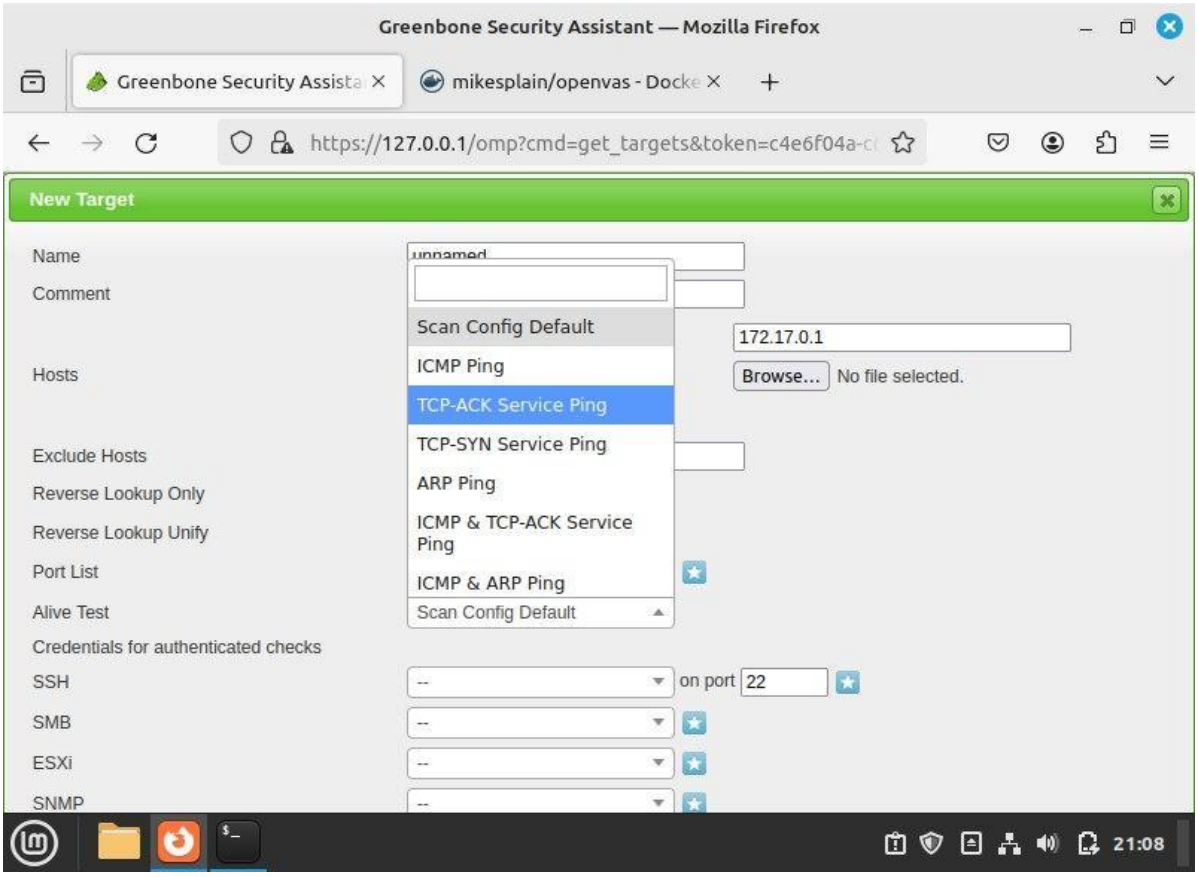

Рисунок 3.17 – Налаштування цілей сканування

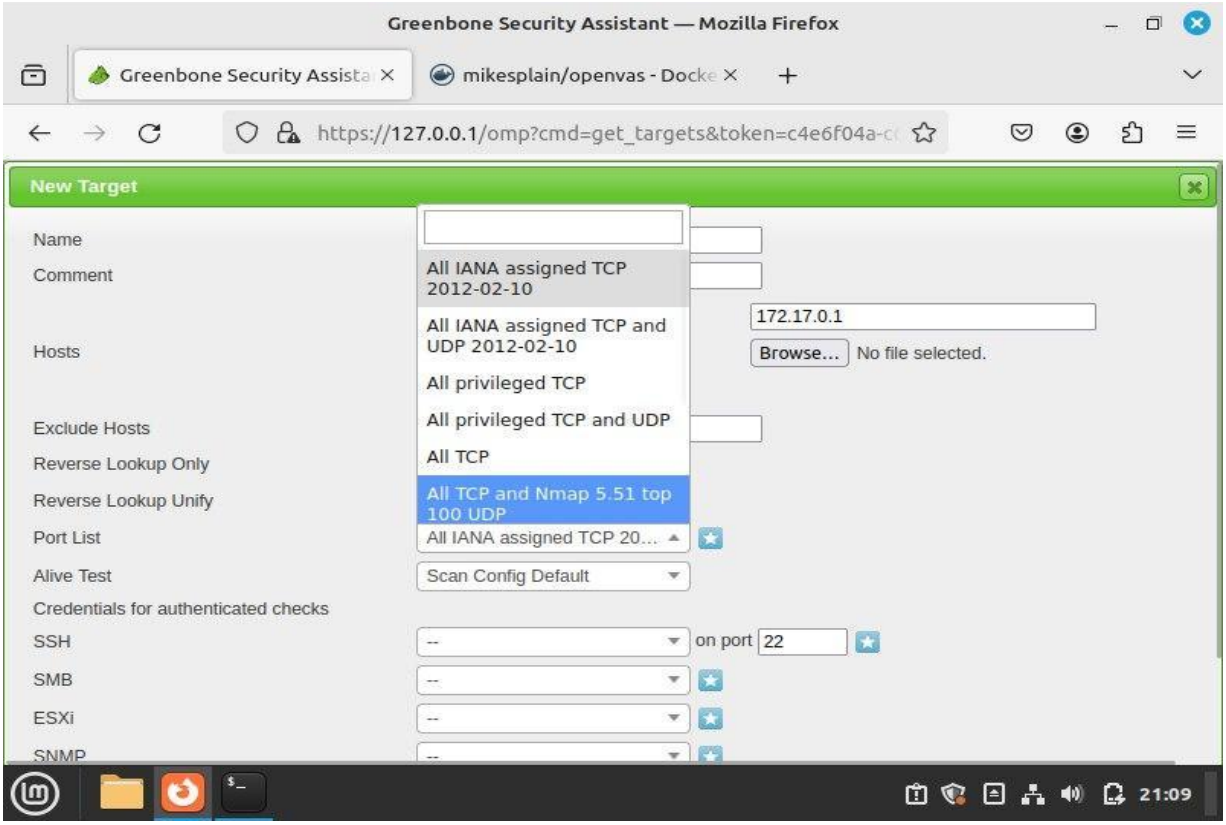

Рисунок 3.18 – Налаштування цілей сканування

Якщо ми не маємо інформацію про мережу, яку будемо сканувати – доречно використовувати вже готові сканування. Якщо ми маємо інформацію про мережу, розуміємо на яких портах, на яких ір є служби, які б ми хотіли перевірити на вразливості – буде логічніше сформувати своє сканування в OpenVAS. Таке сканування пройде набагато швидше та побачимо тільки корисну інформацію.

Ми можемо налаштувати сканування під наші потреби, просканувавши потрібні нам порти, хости, протоколи, видаливши непотрібне з базових сканувань.

Наприклад, якщо ми знаємо, що нам не потрібне сканування CISCO, то можемо його видалити. Бачимо, що відразу ж видаляється 647 скриптів в нашому скануванні. Якщо знаємо, що не будемо сканувати CentOS – в нашій конфігурації стає менше на 2528 скриптів. Таким чином можна налаштувати сканер під наші потреби.

Висновки по розділу: Для розширення діапазону компаній, які зможуть користуватись розробленою методикою – залишаю вибір між Nessus та OpenVAS в залежності від бюджету компанії на кібербезпеку. Функціонали цих сканерів найбільше підходять для проведення повноцінного сканування компанії з чіткими висновками.

4 РОЗРОБКА ВЛАСНОЇ МЕТОДИКИ ПОШУКУ ВРАЗЛИВОСТЕЙ

4.1 Аналіз існуючих стандартів та методик тестування на проникнення:[30]

OSSTMM [25]

The Open Source Security Testing Methodology Manual - це відомий стандарт тестування на проникнення. Базуючись на ньому можна зробити чіткий структурований план, сформулювати власну шкалу оцінювання рівня безпеки компанії. Тобто в кінці ми отримаємо детальні результати проведення пентесту. Ця методологія має декілька напрямків: безпека мережі, безпека людини, безпека телекомунікації та мережі передачі даних. Також методика описує деякі реакції на кібератаки та інциденти. [31] Важливо зазначити, що дана методика оновлюється з певною періодичністю, тобто залишається актуальною.

Недоліки:

Мало інформації по практиці проведення тестування та набору інструментів для цього. Відсутність класифікації вразливостей.

ISSAF

OISSG є розробником Information System Security Assessment Framework. Методика є дуже детальною та має план виконання пентесту з прописаними командами для кожного з етапів атак. Методика реалізована в двох частинах, це рекомендації: для управління та з самого тестування. [32]

Реалізація тестування включає в себе етапи:

1) Планування та підготовка (тобто підготовка плану тестування та налагодження всіх правових аспектів, договорів, термінів).

2) Оцінка (дізнаємось більше інформацію про систему, мережу організації, вразливості)

Потім саме проведення тестування, пробуємо отримати привілеї адміністратора, розширити свої привілеї, скомпрометувати більше користувачів та залишити для себе можливість подальшого підключення для мережі. Важливим є також приховування слідів після проведення тестування.

Недоліки: методика буде займати багато часу для регулярної перевірки.

PTES [29]

Penetration Testing Execution Standard

Даний стандарт включає в себе технічні рекомендації щодо проведення пентесту: операційні системи та програмне забезпечення, апаратні засоби та радіотехнічні. Він дає змогу чітко описати цілі тестування та отримати детальний чіткий результат базуючись на вихідних даних аналізу захищеності. Також методика має рекомендації для перевірки закриття вразливостей після першого проведення тестування.

За PTES потрібно спочатку узгодити всі моменти проведення пошуку вразливостей із замовником. Потім зібрати всю можливу інформацію про компанію та інформаційну систему компанії, змоделювати загрози. Проводиться аналіз вразливостей з подальшою експлуатацією та постексплуатацією. Кінцевим етапом виступає підготовка звіту про проведену роботу з детальним описом проведення кожного з етапів.

Недоліки: методика буде займати багато часу для регулярної перевірки.

4.2 Розробка власної методики та обґрунтування її властивостей

1) Планування.
   - Узгодження плану проведення тестування з керівництвом
   - Отримання потрібної інформації від керівництва щодо проведення тестування
   - Планування часу виконання
   - Визначення дедлайну
   - Формату подачі звіту
2) Пасивна розвідка

- Спроба знайти інформацію про підключені пристрої компанії до мережі інтернет (Інструменти, що використовується: Shodan або ZoomEye).
- Спроба знайти відкриту інформацію про домени, які використовує

компанія (Інструмент, що використовується: Google).

- Спроба знайти пошти працівників, їх посади, всю інформацію, яку вони залишають в соцмережах про роботу на компанію (Інструменти, що використовується: Google, Social Media).
- Об`єднання та аналіз зібраних даних для виявлення потенційних загроз, які можуть являти собою працівники компанії (Інструмент, що використовується: Maltego).

3) Активна розвідка

Використовуємо TCP SYN та UDP сканування. При недоступності TCP SYN використовуємо TCP Connect (причини даного вибору вказані в розділі 2) . Обов`язкові UDP порти для сканування: DNS (53), NTP (123), SNMP (161), VPN (500, 1194, 4500), RDG (3391).

В даній методиці надано рекомендації щодо використання Nmap та інших інструментів. Як було вказано в розділі 3 OpenVAS це гнучкий інструмент, тому його конфігурація проводиться менеджером інформаційної безпеки базуючись на програмному забезпеченні, що використовує компанія та потребах в скануванні.

- Сканування мережі жертви для виявлення активних хостів. (Інструменти, що використовується: nmap, Nessus або OpenVAS)
- Сканування мережі жертви для виявлення відкритих портів і служб. (Інструменти, що використовується: nmap, Nessus або OpenVAS).

Nmap TCP SYN сканування: [27]

nmap -sS 192.168.0.52

Nmap UDP сканування:

Nmap -sU 192.168.0.52

Nmap TCP Connect сканування:

nmap -sT 192.168.0.52

- Сканування мережі жертви для виявлення версій програмного забезпечення (Інструменти, що використовується: nmap, Nessus або OpenVAS). Дана методика не включає проведення етапу експлуатації,

тому висновок щодо захищеності системи буде ґрунтуватися на основі поточних версій програмного забезпечення. Так працює та аналізує систему на вразливості Nessus. В звіті мають бути вказані CWE вразливостей, до яких вразлива поточна версія програмного забезпечення.

- Виявлення програмного забезпечення, що використовується та його версій за допомогою Nmap:

nmap -sV 192.168.1.1

- Сканування мережі жертви для виявлення конфігураційних даних (Інструменти, що використовується: nmap, Nessus або OpenVAS).
- Сканування мережі жертви для виявлення нових способів вторгнення (Інструменти, що використовується: nmap, Nessus або OpenVAS).

4) Перевірка відомих загроз [26]

Особливу увагу, як було зазначено в розділі 1 потрібно звернути на VPN.

VPN забезпечує:

- Аутентифікацію користувача
- Управління адресами
- Шифрування даних
- Керування ключами
- Підтримка кількох протоколів

Тому потрібно протестувати, проаналізувати та оцінити реалізацію цих пунктів та включити до кінцевого звіту.

Знайти VPN сервер можна по відкритих портах, які використовуються при роботі VPN та наведено в таблиці 4.1.

Таблиця 4.1 – Протоколи та порти

	PPTP	IPSEC	L2TP	L2F
TCP/IP Protocol – Port/Option	IP– 47(GRE)	UDP – 500(IKE)	UDP - 1701	UDP - 1701
TCP/IP Protocol - Port/Option	TCP - 1723	IP – 50(ESP)		
TCP/IP Protocol - Port/Option		IP – 51(AH)		

Приклад використання за допомогою nmap:

nmap –P0 -sU –p 1701 192.168.0.3

Інструмент IpSecScan використовується для пошуку систем, які підтримують IPSec. Приклад використання:

IpSecScan 192.168.0.1 192.168.0.19

Існує багато вразливостей пов’язаних з реалізацією PPTP, тому сніфер dsniff може розпізнати протоколи автентифікації при встановленні сеансу PPTP.

- Для перевірки стійкості системи до методу brute forde використовується потужний інструмент THC-Hydra. В багатьох джерелах цей інструмент зазначається як швидкий завдяки функції одночасних запитів, тому вибираємо саме його. Приклад застосування:

hydra -L logins.txt -P passwords.txt 192.168.0.32 ssh

- Вище також було зазначено про вразливість систем до атак типу password spraying, тому наведемо приклад реалізації перевірки:

hydra -L users.txt -p password 192.168.0.32 ssh

5) Перевірка обізнаності персоналу:

Людський фактор є одним з найнебезпечніших загроз в інформаційній безпеці. Тому важливим етапом є перевірка обізнаності персоналу стосовно інформаційної безпеки:

a) Розсилання фішингових повідомлень з детектуванням відкриття без шкідливого програмного забезпечення. Проводиться з ціллю зрозуміти наскільки персонал вразливий до даного виду атак.

b) Проведення короткого тесту для працівників стосовно обізнаності в області інформаційної безпеки. Тест складається менеджером інформаційної безпеки компанії індивідуально, враховуючи життєвий цикл інформації в компанії.

6) Звітування

В звіті мають бути зазначені результати всіх етапів проведення тестування. З описом виявлених вразливостей, порад щодо їх усунення або зниження ризику.

Методика є рекомендаційною та може змінюватися в залежності від потреб компанії.

4.3Тестування розробленої методики

1) Планування

Пошук вразливостей проводиться менеджером з інформаційної безпеки.

Початок виконання: 06.05.2024

Кінець виконання: 17.05.2024

Формату подачі звіту: файл .docx.

Додаткова інформація, що стосується використання методики: VPN в даній компанії не використовується, тому перевірка його вразливостей не потрібна.

2) Пасивна розвідка

Спроба знайти інформацію про підключені пристрої компанії до мережі інтернет(рис.4.1): [28]

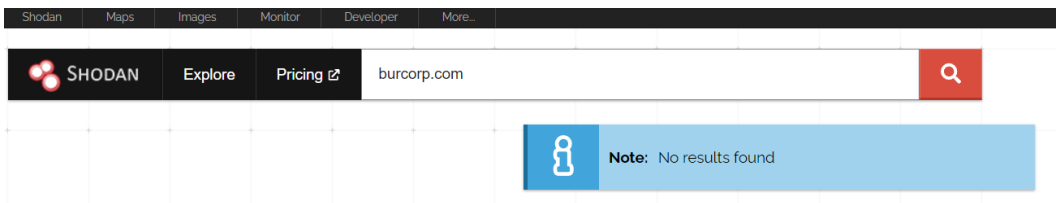

Рисунок 4.1 – Результат пошуку в Shodan

Спроба знайти відкриту інформацію про домени, які використовує компанія:

На сайті компанії можна знайти домен, який використовується для спілкування з потенційними клієнтами. Дана інформація не несе загрози.

Спроба знайти пошти працівників, їх посади, всю інформацію, яку вони залишають в соціальних мережах про роботу на компанію:

Проаналізувавши соціальні мережі співробітників, згадки про компанію та потенційних загроз виявлено не було.

Висновок: інформації, яка може бути виявлена про компанію в інтернеті та використана зловмисником – немає.

3) Проведення сканування:

Nmap TCP SYN сканування (рис.4.3):

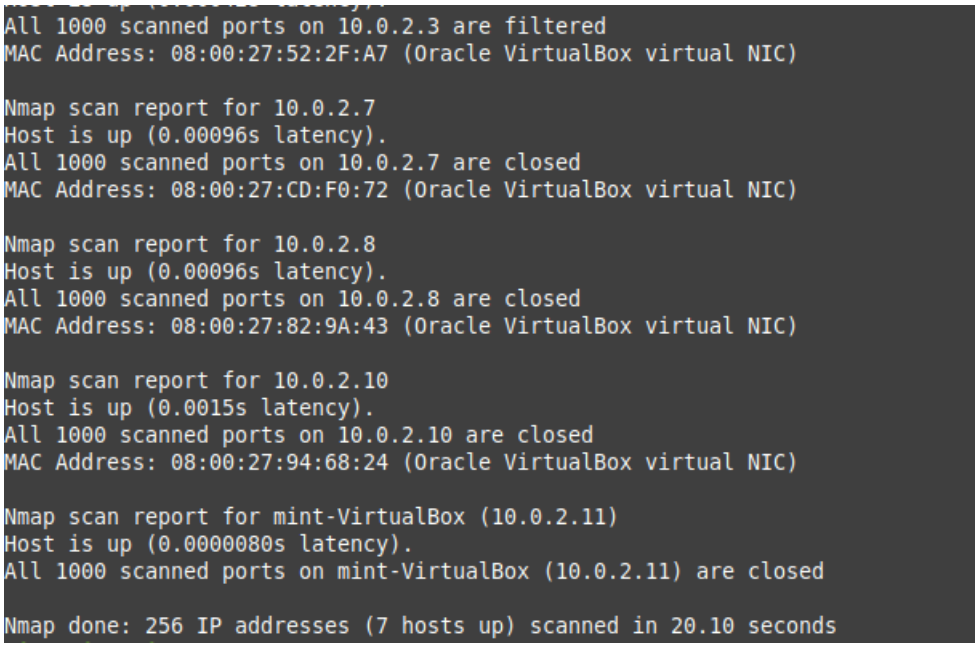

Рисунок 4.3 – Результат TCP SYN сканування

Nmap UDP сканування (рис. 4.4):

```
MAC Address: 08:00:27:CD:F0:72 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.8
Host is up (0.0012s latency).

PORT     STATE  SERVICE
53/udp   closed domain
123/udp  closed ntp
161/udp  closed snmp
3391/udp closed savant
MAC Address: 08:00:27:82:9A:43 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.10
Host is up (0.0011s latency).

PORT     STATE  SERVICE
53/udp   closed domain
123/udp  closed ntp
161/udp  closed snmp
3391/udp closed savant
MAC Address: 08:00:27:94:68:24 (Oracle VirtualBox virtual NIC)

Nmap scan report for mint-VirtualBox (10.0.2.11)
Host is up (0.00016s latency).
```

Рисунок 4.4 - Результат UDP сканування

Nmap TCP Connect сканування (рис. 4.5):

```
Nmap scan report for _gateway (10.0.2.1)
Host is up (0.0092s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.0.2.7
Host is up (0.010s latency).
All 1000 scanned ports on 10.0.2.7 are closed

Nmap scan report for 10.0.2.8
Host is up (0.0097s latency).
All 1000 scanned ports on 10.0.2.8 are closed

Nmap scan report for 10.0.2.10
Host is up (0.0079s latency).
All 1000 scanned ports on 10.0.2.10 are closed

Nmap scan report for mint-VirtualBox (10.0.2.11)
Host is up (0.0081s latency).
All 1000 scanned ports on mint-VirtualBox (10.0.2.11) are closed

Nmap done: 256 IP addresses (5 hosts up) scanned in 5.99 seconds
```

Рисунок 4.5 – Результат TCP Connect сканування

Виявлення програмного забезпечення, що використовується та його версій за допомогою Nmap (рис. 4.6):

```
Nmap scan report for 10.0.2.7
Host is up (0.0096s latency).
All 1000 scanned ports on 10.0.2.7 are closed

Nmap scan report for 10.0.2.8
Host is up (0.010s latency).
All 1000 scanned ports on 10.0.2.8 are closed

Nmap scan report for 10.0.2.10
Host is up (0.0093s latency).
All 1000 scanned ports on 10.0.2.10 are closed

Nmap scan report for mint-VirtualBox (10.0.2.11)
Host is up (0.010s latency).
All 1000 scanned ports on mint-VirtualBox (10.0.2.11) are closed

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 27.90 seconds
```

Рисунок 4.6 – Результат сканування на виявлення програмного забезпечення

Висновки: вразливості не знайдено. Система є захищеною.

4) Перевірка обізнаності персоналу

Проведення короткого тесту для працівників стосовно обізнаності в області інформаційної безпеки (рис. 4.2):

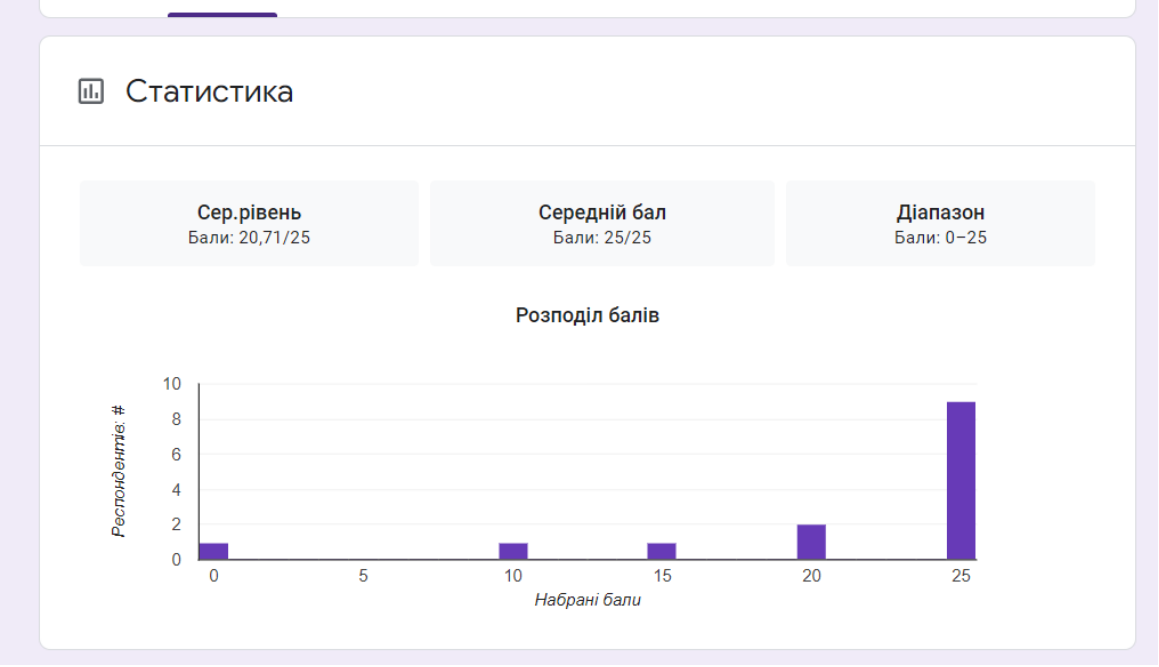

Рисунок 4.2 – Статистика опитування

Статистичні дані показують, що більшість працівників компанії обізнані в області інформаційної безпеки. Але не всі.

Висновок: Загроза використання зловмисником методів соціальної інженерії є високою. Проведення тренінгу з інформаційної безпеки є обов'язковим для зниження ризику.

Висновки: розроблена методика охоплює проблеми, описані в попередніх розділах. На відміну від оглянутих вище методик, її можна проводити регулярно. Це дозволить вчасно та якісно виявляти вразливості та усувати їх.

ВИСНОВКИ

В зв’язку з COVID-19 все більше компаній з 2019 року почало переходити на віддалену роботу, що стало серйозним викликом для спеціалістів з кібербезпеки. Компанії були більше зосереджені на утриманні бізнес-процесів, аніж на безпеці. Спеціалісти, які раніше займалися обслуговуванням локальних комп’ютерів зіштовхнулися з загрозами використання віддаленого доступу. Все більше компаній почало використовувати RDP, VPN, хмарні ресурси.

Метою дипломного проекту була розробка методики. Проаналізувавши вразливі місця сучасних мереж, стало зрозуміло на які проблеми при тестуванні на безпеку корпоративних мереж потрібно звертати увагу при підготовці індивідуальної методики тестування:

- Облікові записи користувачів
- Порти
- Протидія атакам методом перебору паролей
- Встановлення останніх оновлень та патчів
- Управління привілеями користувачів
- Кінцеві точки доступу
- VPN

Було проаналізовано найвідоміші методики пошуку вразливостей, проте були виявлені недоліки:

- Мало інформації по практиці проведення тестування та набору інструментів для цього.
- Відсутність класифікації вразливостей.
- Методика буде займати багато часу для регулярної перевірки.

Розроблена методика охоплює проблеми, описані в попередніх розділах. На відміну від оглянутих вище методик, її можна проводити регулярно. Це дозволить вчасно та якісно виявляти вразливості та усувати їх.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналіз сучасних наукових публікацій за напрямком тематики кібербезпеки IoT технологій. [Електронний ресурс]. – Режим доступу: https://archive.journal-grail.science/index.php/2710-3056/article/view/1021

2. 10 найпопулярніших сфер використання інтернету речей. [Електронний ресурс]. – Режим доступу: https://www.imena.ua/blog/top-10-scope-iot/

3. Securing IoT without Added Burden. [Електронний ресурс]. – Режим доступу: https://www.paloaltonetworks.com/cybersecurity-perspectives/expanding-iot-visibility

4. What was the WannaCry ransomware attack? [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

5. What is ransomware? Ransomware meaning. [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/learning/security/ransomware/what-is-ransomware/

6. Інформаційна безпека як складова економічної безпеки підприємств. [Електронний ресурс]. – Режим доступу: http://eztuir.ztu.edu.ua/bitstream/handle/123456789/7088/234.pdf?sequence=1&isAllowed=y

7. Інформатизація та комп'ютеризація суспільства. Цифрові технології. [Електронний ресурс]. – Режим доступу: https://repository.mu.edu.ua/jspui/bitstream/123456789/1077/1/KS_Informatyz_ta_komp_2018.pdf#page=55

8. Збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів [Електронний ресурс]. – Режим доступу: https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/9607/1/%D0%97%D0%B0%D1%

85%D0%B8%D1%81%D1%82%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97%20%28%D0%B7%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA%29%20-%202021%202.0.pdf#page=86

9. Що таке кібербезпека? [Електронний ресурс]. – Режим доступу: https://aws.amazon.com/ru/what-is/cybersecurity/

10. Мережева безпека/Безпека мережі. [Електронний ресурс]. – Режим доступу: https://itglobal.com/ru-ru/company/glossary/setevaya-bezopasnost-bezopasnost-seti/

11. Управління інформаційною безпекою. [Електронний ресурс]. – Режим доступу: http://dspace.wunu.edu.ua/bitstream/316497/49115/1/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%8E%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%BE%D1%8E.pdf

12. Системи класифікації та оцінки вразливостей та загроз інформаційних систем: які вони бувають і навіщо потрібні. [Електронний ресурс]. – Режим доступу: https://habr.com/ru/companies/bastion/articles/706884/

13. Top 5 Remote Work Security Threats. [Електронний ресурс]. – Режим доступу: https://www.varonis.com/blog/top-5-remote-work-security-threats

14. Захист Протоколу RDP: ключові рекомендації щодо безпеки корпоративних мереж. [Електронний ресурс]. – Режим доступу: https://habr.com/ru/articles/792016/

15. Сканери портів. Відомі реалізації. [Електронний ресурс]. – Режим доступу: https://elibrary.ru/item.asp?id=27186934

16. Nmap: сканування портів. [Електронний ресурс]. – Режим доступу: https://habr.com/ru/articles/767590/

17. Виявлення хостів. [Електронний ресурс]. – Режим доступу: https://nmap.org/man/ru/man-host-discovery.html

18. Основи сканування портів. [Електронний ресурс]. – Режим доступу: https://nmap.org/man/ru/man-port-scanning-basics.html

19. Різні прийоми сканування портів. [Електронний ресурс]. – Режим доступу: https://nmap.org/man/ru/man-port-scanning-techniques.html

20. Сканери безпеки і вразливостей. [Електронний ресурс]. – Режим доступу: https://yug.com.ua/uk/software/vulnerability-scanners/

21. Топ-15 платних і безплатних інструментів для сканування вразливостей. [Електронний ресурс]. – Режим доступу: https://itest.com.ua/instrumenty/top-15-platnyh-i-bezplatnyh-instrumentiv-dlya-skanuvannya-vrazlyvostey/

22. Встановлення та використання сканеру вразливостей Nessus до Kali Linux. [Електронний ресурс]. – Режим доступу: https://etc.hneu.edu.ua/docs/nessus/

23. Встановлення та використання OpenVAS (GVM) на Kali Linux. [Електронний ресурс]. – Режим доступу: https://spy-soft.net/openvas-gvm-kali-linux/

24. Тестування на проникнення: як перевірити безпеку та вразливість вашого продукту шляхом імітації атаки. [Електронний ресурс]. – Режим доступу: https://fastercapital.com/ru/content/Тестирование-на-проникновение--как-проверить-безопасность-и-уязвимость-вашего-продукта-путем-имитации-атаки.html

25. Аналіз стандартів та методик тестування на проникнення. [Електронний ресурс]. – Режим доступу: https://cyberleninka.ru/article/n/analiz-standartov-i-metodik-testirovaniya-na-proniknovenie

26. Information System Security Assessment Framework (ISSAF). [Електронний ресурс]. – Режим доступу: https://untrustednetwork.net/files/issaf0.2.1.pdf

27. Nmap — посібник для початківців [Електронний ресурс]. – Режим доступу: https://habr.com/ru/articles/131433/

28. Shodan. [Електронний ресурс]. – Режим доступу: https://www.shodan.io/search?query=mindy-teams.com

29. Penetration Testing Execution Standard (PTES). [Електронний ресурс]. – Режим доступу: http://www.pentest-standard.org/index.php/Main_Page

30. Інфраструктурний пентест за кроками: інструменти, методології та розвідка. [Електронний ресурс]. – Режим доступу: https://habr.com/ru/companies/bastion/articles/767704/

31. Міжнародні стандарти та методики тестування при аналізі захищеност. [Електронний ресурс]. – Режим доступу: https://ddos-guard.net/ru/blog/mezhdunarodnie-standarti-analiza-zashchishchennosti

32. Сучасні методики пентесту.[Електронний ресурс]. – Режим доступу: https://roundsec.io/sovremennye-metodiki-pentesta/

33. Топ-15 платних і безплатних інструментів для сканування вразливостей. [Електронний ресурс]. – Режим доступу: https://itest.com.ua/instrumenty/top-15-platnyh-i-bezplatnyh-instrumentiv-dlya-skanuvannya-vrazlyvostey/

ДОДАТОК А

Протокол сканування цільової системи:

```
mint@mint-VirtualBox:~$ sudo nmap -sS 10.0.2.0/24
[sudo] password for mint:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-21 00:35 EEST
Nmap scan report for _gateway (10.0.2.1)
Host is up (0.00041s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0013s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.00042s latency).
All 1000 scanned ports on 10.0.2.3 are filtered
MAC Address: 08:00:27:52:2F:A7 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.7
Host is up (0.00096s latency).
All 1000 scanned ports on 10.0.2.7 are closed
MAC Address: 08:00:27:CD:F0:72 (Oracle VirtualBox virtual NIC)
```

Nmap scan report for 10.0.2.8
Host is up (0.00096s latency).
All 1000 scanned ports on 10.0.2.8 are closed
MAC Address: 08:00:27:82:9A:43 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.10
Host is up (0.0015s latency).
All 1000 scanned ports on 10.0.2.10 are closed
MAC Address: 08:00:27:94:68:24 (Oracle VirtualBox virtual NIC)

Nmap scan report for mint-VirtualBox (10.0.2.11)
Host is up (0.0000080s latency).
All 1000 scanned ports on mint-VirtualBox (10.0.2.11) are closed

Nmap done: 256 IP addresses (7 hosts up) scanned in 20.10 seconds
sudo nmap -sU -p 53,123,161,3391 10.0.2.0/24
Starting Nmap 7.80 (https://nmap.org) at 2024-05-21 00:37 EEST
Nmap scan report for _gateway (10.0.2.1)
Host is up (0.00098s latency).

PORT STATE SERVICE
53/udp open domain
123/udp closed ntp
161/udp closed snmp
3391/udp closed savant
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.00045s latency).

PORT STATE SERVICE
53/udp open|filtered domain
123/udp open|filtered ntp
161/udp open|filtered snmp
3391/udp open|filtered savant
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.0013s latency).

PORT STATE SERVICE
53/udp closed domain
123/udp closed ntp
161/udp closed snmp
3391/udp closed savant
MAC Address: 08:00:27:52:2F:A7 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.7
Host is up (0.0029s latency).

PORT STATE SERVICE
53/udp closed domain
123/udp closed ntp
161/udp closed snmp
3391/udp closed savant
MAC Address: 08:00:27:CD:F0:72 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.8
Host is up (0.0012s latency).

PORT STATE SERVICE
53/udp closed domain
123/udp closed ntp
161/udp closed snmp
3391/udp closed savant
MAC Address: 08:00:27:82:9A:43 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.10
Host is up (0.0011s latency).

PORT STATE SERVICE
53/udp closed domain
123/udp closed ntp
161/udp closed snmp
3391/udp closed savant
MAC Address: 08:00:27:94:68:24 (Oracle VirtualBox virtual NIC)

Nmap scan report for mint-VirtualBox (10.0.2.11)
Host is up (0.00016s latency).

PORT STATE SERVICE
53/udp closed domain
123/udp closed ntp
161/udp closed snmp
3391/udp closed savant

Nmap done: 256 IP addresses (7 hosts up) scanned in 3.23 seconds
mint@mint-VirtualBox:~$ nmap -sT 10.0.2.0/24
Starting Nmap 7.80 (https://nmap.org) at 2024-05-21 00:37 EEST

Nmap scan report for _gateway (10.0.2.1)
Host is up (0.0092s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open domain

Nmap scan report for 10.0.2.7
Host is up (0.010s latency).
All 1000 scanned ports on 10.0.2.7 are closed

Nmap scan report for 10.0.2.8
Host is up (0.0097s latency).
All 1000 scanned ports on 10.0.2.8 are closed

Nmap scan report for 10.0.2.10
Host is up (0.0079s latency).
All 1000 scanned ports on 10.0.2.10 are closed

Nmap scan report for mint-VirtualBox (10.0.2.11)
Host is up (0.0081s latency).
All 1000 scanned ports on mint-VirtualBox (10.0.2.11) are closed

Nmap done: 256 IP addresses (5 hosts up) scanned in 5.99 seconds
mint@mint-VirtualBox:~$ nmap -sV 10.0.2.0/24
Starting Nmap 7.80 (https://nmap.org) at 2024-05-21 00:37 EEST
Nmap scan report for _gateway (10.0.2.1)
Host is up (0.011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
53/tcp open domain (generic dns response: NOTIMP)

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port53-TCP:V=7.80%I=7%D=5/21%Time=664BC2C5%P=x86_64-pc-linux-gnu%r(DNSV

SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x83\0\x01\0\0\0\0\0\0\x07version\

SF:x04bind\0\0\x10\0\x03")%r(DNSStatusRequestTCP,E,"\0\x0c\0\0\x90\x04\0\

0

SF:\0\0\0\0\0\0");

Nmap scan report for 10.0.2.7

Host is up (0.0096s latency).

All 1000 scanned ports on 10.0.2.7 are closed

Nmap scan report for 10.0.2.8

Host is up (0.010s latency).

All 1000 scanned ports on 10.0.2.8 are closed

Nmap scan report for 10.0.2.10

Host is up (0.0093s latency).

All 1000 scanned ports on 10.0.2.10 are closed

Nmap scan report for mint-VirtualBox (10.0.2.11)

Host is up (0.010s latency).

All 1000 scanned ports on mint-VirtualBox (10.0.2.11) are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 256 IP addresses (5 hosts up) scanned in 27.90 seconds