Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

Дипломної роботи
магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*
(назва освітньої програми)

освітньо-наукова програма *кібербезпека*

на тему: «Віртуальна лабораторая для тестування співробітників організації щодо фішингових атак»

Виконавець: студентка ІІ курсу, групи КБм-21

(підпис) **Мовчан Дар'я Андріївна**
(прізвище ім'я по-батькові)

	Прізвище, ініціали	**Оцінка**	**Підпис**
Науковий керівник	Бучик С.С.		
Рецензент	Сайко В. Г.		
Нормоконтроль	Даков С.Ю.		

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«___» _____ 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студентці КБм-21 (група) Мовчан Дар'ї Андріївні (прізвище ім'я по-батькові)

Тема дипломної роботи Віртуальна лабораторія для тестування співробітників організації щодо фішингових атак

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

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

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес створення віртуальних лабораторій для проведення тестування співробітників організації щодо фішингових атак
Предмет досліджень	Інструменти створення фішингових атак.
Мета	Розробка віртуальної лабораторії для проведення тестування співробітників організації щодо фішингових атак
Вихідні дані для проведення роботи	Набір утиліт для створення фішингових атак, ОС KaliLinux, рекомендації ДСТУ ISO/IEC 27032:2016

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна удосконалення використання сукупності інструментів створення фішингових атак для проведення тестування співробітників організації за рахунок включення їх до віртуальної лабораторії, що дозволить швидко та ефективно здійснювати оцінку готовності співробітників до подібних атак з урахуваннях вимог ДСТУ ISO/IEC 27032:2016

Практична цінність можливість практичної реалізації запропонованої віртуальної лабораторії для проведення тестування співробітників організації щодо фішингових атак з урахуваннях вимог ДСТУ ISO/IEC 27032:2016

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	29.10.2021 – 22.01.2022
Аналіз літературних джерел	23.01.2022 – 11.02.2022
Обґрунтування вибору рішення	12.02.2022 – 15.02.2022
Вивчення сучасних технік фішингових атак	16.02.2022 – 28.02.2022
Вичення ринку рішень для тестування співробітників	01.03.2022 – 20.03.2022
Розробка структури віртуальної лабораторії	21.03.2022 – 05.04.2022
Дослідження роботи інструментів для створення вішингових атак	06.04.2022 – 16.04.2022
Порівняння ефективності роботи інструментів створення фішингових атак	17.04.2022 – 25.04.2022
Оформлення пояснювальної записки	26.04.2022 – 15.05.2022
Підготовка до захисту дипломної роботи	16.05.2022 – 19.05.2022

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Можливе зменшення збитків організації, які можуть наступити у результаті реалізації атак за допомогою фішингу

Соціальний ефект Навчання співробітників організації

7. ДОДАТКОВІ ВИМОГИ

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

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

Дата видачі завдання: _____
Термін подання дипломної роботи до ЕК _____

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Віртуальна лабораторія для тестування співробітників організації щодо фішингових атак»: 64 сторінок, 59 рисунків, 1 додаток та 2 таблиці. 27 літературних джерел.

Об’єкт дослідження – процес створення віртуальних лабораторій для проведення тестування співробітників організації щодо фішингових атак.

Предмет дослідження – інструменти створення фішингових атак.

Мета роботи – розробити віртуальну лабораторію для проведення тестування співробітників організації щодо фішингових атак.

У роботі досліджено сучасні вектори фішингових атак та таксономію фішингу. Проаналізовано ринок рішень з тестування співробітників на предмет фішингових атак. Досліджена та проаналізована ефективність інструментів для створення фішингових атак з ціллю використання їх під час тренування співробітників.

Запропоновано рішення проблеми неефективного тестування співробітників – віртуальна лабораторія на базі ОС Kali Linux.

Актуальність теми: фішингові атаки мають рекордний рівень і завдають мільярдів доларів збитків. Від фішингових атак потерпають як звичайні люди, так і підприємства, тому ефективне навчання співробітників є одним з ключових методів пом’якшення впливу фішингових атак. Набори інструментів створення фішингових атак для проведення тестування не є досконалими і завжди є актуальним пошук рішень в цій сфері.

Ключові слова: тестування співробітників, фішингові атаки.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

PIN — аналог до паролю

IM — система обміну миттєвими повідомленнями

VoIP — технологія передачі медіа-даних у реальному часі за допомогою сімейства протоколів TCP/IP.

TF-IDF — статистичний показник, що використовується для оцінки важливості слів у контексті документа

SQL — декларативна мова програмування для взаємодії користувача з базами даних

SET — Social-engineering toolkit

HTML — мова розмітки гіпертексту

ОС — операційна система

ISO — загальновживана назва комп'ютерного файла, що має розширення «.iso»

USB — стандарт роз'ємів і кабелів

VPN — віртуальна приватна мережа

WSL — Windows Subsystem for Linux

АРМ — автоматизоване робоче місце

CSV — comma-separated values, файловий формат

HTTP — протокол передачі даних

ПК — персональний комп’ютер

GPU — графічний процесор

IP — Internet Protocol

ВСТУП

Фішинг – це крадіжка особистих даних, яка обманює користувачів Інтернету, щоб розкрити їхні конфіденційні дані, наприклад, дані для входу, дані кредитної/дебетової картки тощо. За останні роки дослідники розробили різні методи боротьби з фішингом. Проте проблема все ще існує.

За даними досліджень, більш ніж 80% фішингових атак поширюються через масову розсилку електронних листів. Фішингові атаки мають рекордний рівень і завдають мільярдів доларів збитків. Від фішингових атак потерпають як звичайні люди, так і підприємства, тому ефективне навчання співробітників є одним з ключових методів пом’якшення впливу фішингових атак. Набори інструментів створення фішингових атак для проведення тестування не є досконалими і завжди є актуальним пошук рішень в цій сфері.

Метою дослідження є розроблення віртуальної лабораторії, яка дозволить тестувати співробітників організації на предмет фішингових атак.

Об’єктом даного дослідження є процес створення віртуальних лабораторій для проведення тестування співробітників організації щодо фішингових атак.

Предметом дослідження виступають інструменти створення фішингових атак.

Наукова новизна полягає у удосконаленні використання сукупності інструментів створення фішингових атак для проведення тестування співробітників організації за рахунок включення їх до віртуальної лабораторії, що дозволить швидко та ефективно здійснювати оцінку готовності співробітників до подібних атак з урахуванням вимог ДСТУ ISO/IEC 27032:2016.

РОЗДІЛ 1
ТАКСОНОМІЯ ФІШИНГОВИХ АТАК

1.1 Аналіз сучасного фішингу

Фішинг є автоматизованою формою соціальної інженерії, за допомогою якої злочинці використовують Інтернет для шахрайського вилучення конфіденційної інформації від компаній та окремих осіб, часто видаючи себе за законні веб-сайти. Високий потенціал винагород (наприклад, через доступ до банківських рахунків і номерів кредитних карток), легкість надсилання підроблених повідомлень електронної пошти, що видають себе за законні органи, і труднощі правоохоронних органів у переслідуванні винних злочинців призвели до сплеску фішингу.

Типова фішингова атака починається з електронного листа жертві, нібито від авторитетної установи, але насправді від зловмисника. Текст повідомлення зазвичай попереджає користувача про те, що проблему необхідно негайно виправити за допомогою облікового запису користувача. Потім жертву ведуть до підробленого веб-сайту (підроблений, створений так, щоб нагадувати офіційний веб-сайт установи). Під час цієї пасивної атаки веб-сторінка пропонує жертві ввести інформацію облікового запису (наприклад, ім’я користувача та пароль), а також може запитати інші особисті дані, такі як номер соціального страхування жертви, номери банківських рахунків, PIN коди банкоматів тощо. інформація передається зловмиснику, який потім може використовувати її для доступу до облікових записів користувача [1].

Фішинг є дорогим кіберзлочином для компаній і окремих осіб. Згідно інформації від американського інституту Понемон середні збитки компаній від фішингових атак в 2021 році становлять 14,8 мільйонів доларів, що більш ніж втричі більше, ніж у 2015 році. Це означає сотні мільярдів доларів загальних збитків від фішингових атак для глобальних компаній [2].

1.2 Процес реалізації фішингової атаки

Фішинг залишається популярним серед кіберзлочинців з багатьох причин. По-перше, фішери мають доступ до недорогих інструментів. Робоча група по боротьбі з фішингом повідомила, що 180 577 кіберзлочинців ініціювали атаки в четвертому кварталі 2017 року, націлені на понад 348 брендів і надіславши 233 613 відомих унікальних спроб фішингу. Такі атаки забезпечуються безкоштовними фішинговими наборами, доступними для кіберзлочинців у світлій і темній мережі, що надає звичайні можливості для проведення шкідливих фішингових кампаній. По-друге, оскільки виплати від продажу облікових даних і кредитних карток у темній мережі зменшилися через надмірну доступність, кіберзлочинці звернули більше уваги на цілеспрямовані та складні фішингові атаки з потенційно більшими виплатами. Нарешті, можливо, через слабку або невиконану організаційну політику, користувачі залишаються слабкою ланкою в безпеці, оскільки, за оцінками, 90% зломів даних є результатом соціально спроектованих кібератак [3].

Для виконання фішингової атаки зловмиснику необхідно пройти 3 основних етапи процесу реалізації.

Процес реалізації фішингової атаки розділяється на фази, які виконуються послідовно. Вони включають в себе такі кроки:

- Підготовка;
- Реалізація;
- Використання результатів атаки.

Під час виконання етапу підготовки зловмисник поширює «приманку», наприклад, оманливого електронного листа, яке може спровокувати жертву видати конфіденційну інформацію.

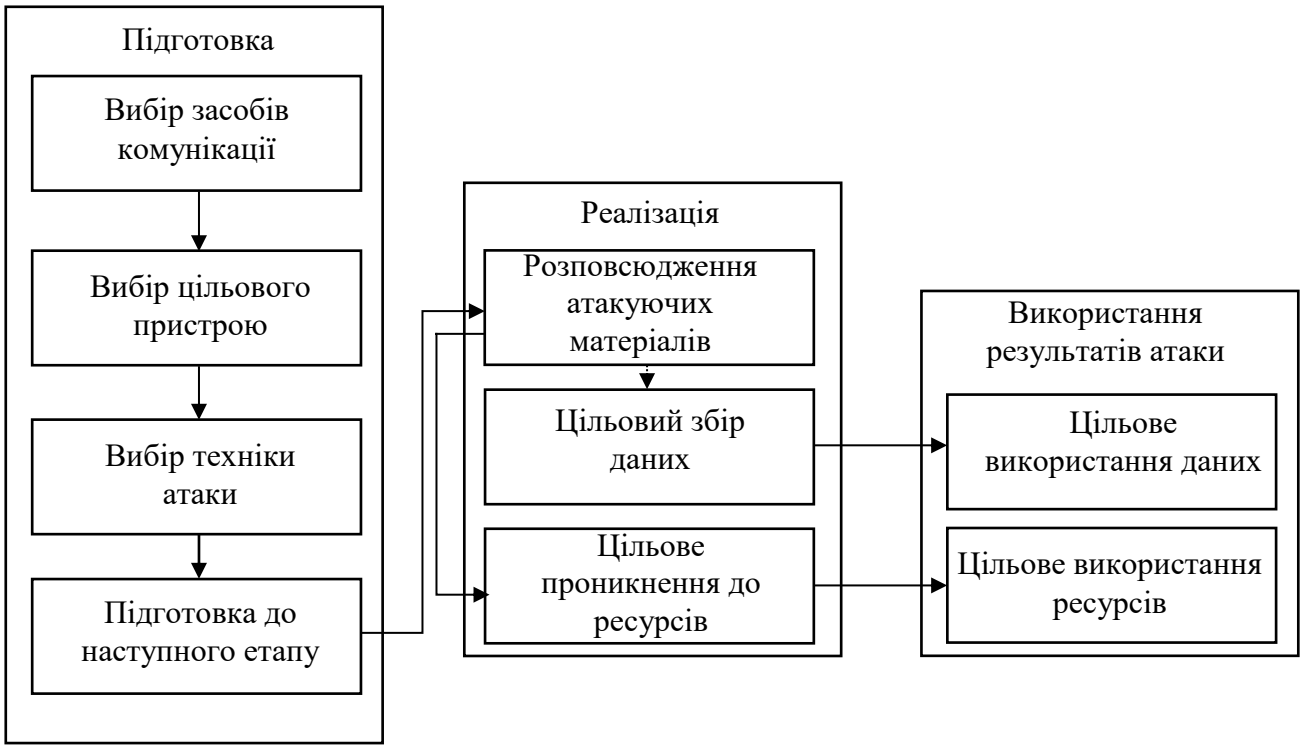

Рисунок 1.1 – Процес реалізації фішингової атаки

Підготовка до атаки – зловмисник спочатку обирає засоби зв'язку для здійснення атаки. Найчастішим цільовим засобом є електронна пошта, але є й інші, такі як миттєві повідомлення (ІМ), мобільні додатки, соціальні та голосові медіа.

Крім того, зловмисник також обирає цільові пристрої (наприклад, смартфони). Середовище, в якому ініціалізуються фішингові атаки, є носіями зв'язку та цільовими пристроями. Далі зловмиснику необхідно обрати методи атаки, такі як підробка веб-сайтів, і, нарешті, приступають до підготовки матеріалу для атаки та майбутнього розповсюдження. Підготовку до атак виконують вручну або за допомогою деяких автоматизованих інструментів, таких як фішингові набори . Набори для фішингу можуть включати попередньо розроблені веб-сторінки для популярних компаній, підозрілі сценарії для збору облікових даних користувачів і механізми розміщення фішингових сайтів. Підготовка атакуючого матеріалу залежить від цільового середовища. Наприклад, у випадку електронної пошти матеріалом атаки буде текст електронної пошти або будь-який інший підозрілий код, вбудований в електронний лист.

Реалізація атаки: цей етап складається з трьох підпроцесів – розподіл матеріалу атаки, збір цільових даних і проникнення цільових ресурсів. Матеріал атаки може бути розповсюджений серед однієї або кількох жертв залежно від передбачуваного масштабу атаки. Стратегія розподілу матеріалу також залежить від матеріалу атаки та типу цільового пристрою. Наприклад, якщо матеріал атаки міститься в тексті, а метою є мобільний пристрій, бездротові мережі будуть кращим вибором. Збір даних об’єкта не почнеться, доки жертва не відповість на надісланий матеріал, як очікують фішери. Нарешті, зловмисники можуть скомпрометувати системні ресурси, щоб полегшити процес збору інформації про користувача за допомогою таких засобів, як введення клієнтського сценарію на веб-сторінки.

Використання результатів атаки: це остання фаза атаки, коли дані, зібрані від цільової жертви, такі як його/її облікові дані, використовуються, як правило, для того, щоб видавати себе за жертву. На основі поглибленого аналізу процесу фішингу визначається чотири виміри фішингу – засоби комунікації, цільове середовище, методи атак і заходи протидії.

Спираючись на існуючі таксономії та моделі процесу фішингових атак, виділяється наступна система [4]:

Засоби комунікації:

- Електронна пошта;
- Веб-сторінки;
- Мессенджери;
- Соціальні мережі;
- Блоги та форуми;
- Мобільні додатки;
- VoIP.

Цільові пристрої:

- Персональний комп’ютер;
- Смартфон;
- Голосові пристрої (VoIP пристрої, телефони);
- Wi-fi пристрої.

Техніки атаки:

- Ініціалізація атаки:
  - Підробка електронної пошти:
    - Вкладення;
    - Використання соціального контексту;
    - Підробка електронної адреси.
  - Підробка веб-сторінки;
  - Інтерактивна голосова відповідь;
  - Реверсна соціальна інженерія;
  - «Людина по-середині»;
  - Цільовий фішинг;
  - Підробка мольних веб-браузерів;
  - Вбудований веб-контент.
- Збір даних:
  - Підроблені форми;
  - Кейлоггери;
  - Запис повідомлень;
  - Обман людини;
  - Соціальні мережі.
- Проникнення в систему:
  - Міжсайтовий скриптинг;
  - Підробка міжсайтових запитів;
  - Fast flux.

Контрзаходи:

- Машинне навчання:
  - Класифікація;
  - Кластеризація;
  - Виявлення аномалій.
- Пошук інформації:

- TF-IDF;
- Відповідність чорного/білого списку;
- Візуальна та структурна відповідність.

- Інше:
  - Пошукові системи;
  - Онтологія;
  - Клієнт-серверна аутентифікація.

1.3 Цільовий фішинг. Техніки.

Зловмисники можуть надсилати фішингові повідомлення через сторонні служби, щоб отримати конфіденційну інформацію, яку можна використовувати під час атаки. Цільовий фішинг для отримання інформації – це спроба обдурити ціль, щоб розкрити інформацію, часто облікові дані чи іншу інформацію. Цільовий фішинг для збору інформації часто включає прийоми соціальної інженерії, такі як фальсифікація джерела для збору інформації (наприклад, створення облікових записів або компрометація облікових записів) та/або надсилання кількох, здавалося б, термінових повідомлень.

Усі форми цільового фішингу — це соціальна інженерія, яка надається електронними послугами, націлена на окремих осіб, компанії чи галузі. У цьому випадку зловмисники надсилають повідомлення через різні сервіси соціальних мереж, особисту веб-пошту та інші некорпоративні сервіси [5]. Політика безпеки для цих служб може бути не настільки суворою, як політика підприємства. Як і у більшості видів цільового фішингу, мета полягає в тому, щоб зв’язатися з жертвою або зацікавити її якимось чином. Зловмисники можуть створювати фейкові акаунти в соціальних мережах і повідомляти співробітників про потенційні перспективи в роботі. Це дає слушну причину для запитань про послуги, політику та інформацію про їхнє середовище. Зловмисники також можуть використовувати інформацію з попередніх розвідувальних заходів (наприклад, соціальні мережі або пошукові веб-

сайти, що належать жертвам), щоб створити переконливі та правдоподібні приманки [6].

1.4 Основні техніки

Зловмисники можуть створювати та розвивати облікові записи у мережах, які можна використовувати під час націлювання. Шахраї можуть створювати акаунти, які можна використовувати для створення особистості для подальших операцій. Розвиток особистості складається з розвитку публічної інформації, присутності, історії та відповідних зв'язків. Ця тактика може бути застосована до соціальних медіа, веб-сайту чи іншої загальнодоступної інформації, на яку можна посилатися та перевірити її на легітимність під час операції з використанням цієї особи або особи.

Для операцій, що включають соціальну інженерію, використання онлайн-персонажу може бути важливим. Ці особи можуть бути вигаданими або видавати себе за реальних людей. Особа може існувати на одному сайті або на кількох сайтах (наприклад: Facebook, LinkedIn, Twitter, Google, GitHub, Docker Hub тощо). Для встановлення особи може знадобитися розробка додаткових документів, щоб вони виглядали реальними. Це може включати заповнення інформації профілю, створення соціальних мереж або додавання фотографій [7][8].

Створення облікових записів також може включати створення облікових записів у постачальників послуг електронної пошти, які можна безпосередньо використовувати для фішингу [9] [10].

Зловмисники можуть зламати облікові записи за допомогою різноманітних сервісів призначених для цього. Для операцій, що включають соціальну інженерію, використання онлайн-особи може бути важливим. Замість того, щоб створювати та розвивати облікові записи, зловмисники можуть скомпрометувати наявні облікові записи. Використання існуючої особи може викликати певний рівень довіри до потенційної жертви, якщо у неї є стосунки або знання про скомпрометовану персону.

Існують різноманітні методи для компрометації облікових записів, як-от збір облікових даних за допомогою фішингу для отримання інформації, придбання облікових даних на сторонніх сайтах або підбір облікових даних (наприклад, повторне використання паролів із дампів облікових даних про порушення) [11]. Перш ніж скомпрометувати облікові записи, зловмисники можуть провести розвідку, щоб прийняти рішення про те, які облікові записи скомпрометувати для подальшої роботи.

Фальшиві особистості можуть існувати на одному сайті або на кількох сайтах (наприклад, Facebook, LinkedIn, Twitter, Google тощо). Зламані облікові записи можуть вимагати додаткової розробки, це може включати заповнення або зміну інформації профілю, подальший розвиток соціальних мереж або додання фотографій.

Зловмисники можуть безпосередньо використовувати зламані облікові записи електронної пошти для фішингу [12].

1.5 Навчання співробітників на предмет фішингових атак

Багато досліджень і дослідницьких проектів намагалися вивчити варіанти виявлення фішингових листів та пом’якшення їх наслідків. Деякі підходи використовують розширену семантичну обробку та сканування ключових слів для блокування небажаних листів, інші методи використовують візуальні підказки в поштовому клієнті, щоб попередити користувачів про підозрілі листи. У більшості досліджень, незалежно від застосованих технологій, якщо електронна пошта досить якісно імітує оригінал, користувач стане жертвою [13, 14]. Автори провели багато досліджень щодо ефективності навчання та освіти для подолання сприйнятливості людини до фішингу. У перших дослідженнях у центрі уваги досліджень була проста ефективність фішингових вправ [15]. У цих ранніх результатах автори побудували інфраструктуру для виконання фішингу і досягли результатів, які вказують на середню 40% схильність до фішингу. Ці результати були підтверджені в подальшому дослідженні [16] і далі показали, що вправи, повторювані протягом

короткої тривалості, підвищували обізнаність і сприйнятливість знижувалися до 5%. Останні дослідження аналізували вплив соціальних мереж на сприйнятливість [17]. У цих результатах було виявлено групування жертв за організаціями; якщо керівництво організації було вразливим – імовірно, що так буде і з персоналом цієї організації. На рис.1.2 більші кола вказують на керівників, а червоні – на те, що стали жертвою фішингу.

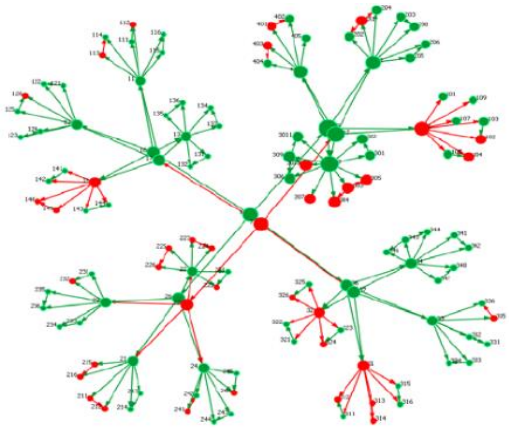

Рисунок 1.2 – Розмір жертв фішингових атак за централізованістю

Багатьом великим організаціям потрібна підготовка, щоб переконатися, що співробітники знають про ризики, які утворюються для організації через користувачів, які стають жертвами фішингових електронних листів. Ця підготовка, як правило, оплачується організацією фінансово та персоналом. За останні кілька років фішингові тренування стали ефективним механізмом для забезпечення можливості навчання, що забезпечує менші інвестиції з боку організації [18].

Висновки до розділу 1

Через фішингові атаки підприємства зазначають катастрофічних фінансових втрат. Однією з найслабкіших ланок, що забезпечують безпеку інформації на

підприємствах є саме люди. 90% зламів є результатом соціально спроектованих кібератак.

Цільовий фішинг є одним з найпопулярніших серед зловмисників типом фішингових атак, а саме фішинг з використанням електронної пошти. Цей вид кібератак є одним з найдешевших, бо злочинці мають доступ до недорогих або безкоштовних інструментів, які можна отримати як темній частині інтернету, так і на світлій. Зловмисники задля досягнення своєї цілі використовують підробку облікових записів, створюють онлайн-особистості.

Для мінімізації наслідків фішингових атак необхідно проводити навчання співробітників. Близько 40% людей схильні до фішингових атак, як показують дослідження, після проведення тренування сприйнятливість знижується на 5%. Навчання та тренування робітників є невід’ємним процесом задля досягнення достатнього рівня безпеки інформації на підприємстві.

РОЗДІЛ 2
ІНСТРУМЕНТИ ДЛЯ ТЕСТУВАННЯ СПІВРОБІТНИКІВ НА ПРЕДМЕТ ФІШИНГОВИХ АТАК

2.1 Законодавчі нормативи

Згідно з ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT), обізнаність та навчання в галузі безпеки, охоплюючи регулярне оновлення відповідних знань, є важливим елементом протидії атакам соціальної інженерії. Як частина програми кібербезпеки організації, співробітники та сторонні підрядники повинні бути зобов'язані проводити мінімальну кількість годин навчань для того, щоб забезпечити, що вони проінформовані про свої ролі та обов'язки в кіберпросторі й технічні засоби управління, які вони повинні впровадити як приватні особи, використовуючи кіберпростір. Додатково як частина програми протидії атакам соціальної інженерії, такі навчання мають містити таке:

- Останні загрози та форми afaK соціальної інженерії, наприклад, як фішинг еволюціонував від одних підроблених веб-сайтів до комбінації спаму, Cross-Site Scripting-атак та SQL-lnjection-атак;
- Як персональна та корпоративна інформація може бути викрадена та використана за допомогою атак соціальної інженерії, що надає розуміння того, як зловмисники можуть скористатися людською природою, такою як тенденція виконувати запити, які йдуть від авторитета (навіть якщо це може бути нереальним), доброзичлива манера поведінки, видання себе жертвою та взаємність за допомогою надання чогось цінного або допомоги;
- Яку інформацію необхідно захищати та як її захищати відповідно до політики інформаційної безпеки;
- Коли повідомляти або виконувати ескалацію підозрілих подій або шкідливого програмного забезпечення відповідним органам чи агентствам

реагування, та інформація про їхні доступні контакти Організації, Що надають прикладні онлайн-програми та послуги в кіберпросторі, повинні надавати інформаційні матеріали абонентам або споживачам, охоплюючи наведене вище в контексті їхніх прикладних програм або послуг.

Також у стандарті ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT) зазначені рекомендації щодо тестування співробітників, а саме те, що співробітники повинні підписати підтвердження, що вони приймають та розуміють зміст політики безпеки організації. Як частина процесу покращення обізнаності та приділення належної уваги такому ризику, організація повинна розглянути проведення періодичних тестів для визначення рівня обізнаності та дотримання відповідних політик, і практик. Працівники можуть зробити письмовий тест для визначення того, чи розуміють вони зміст політики безпеки організації. Такі тести можуть містити, але не обмежуватися, створенням цільових, але контрольованих, фітингових сайтів, спаму та шахрайськими електронними повідомленнями, використовуючи соціальну інженерію та правдоподібний зміст. Під час проведення таких тестів важливо переконатися в тому, що:

- усі тестові сервери та їхній вміст перебувають під контролем та управлінням команди тестування;
- по можливості залучають професіоналів, які мають попередній досвід проведення таких тестів;
- користувачів підготовлено до таких тестів за допомогою програм підвищення обізнаності та навчання;
- усі результати тесту представлено в агрегованому вигляді з метою захисту конфіденційності приватних осіб, оскільки вміст, поданий у таких тестах, може занепокоювати приватних осіб та спричиняти проблеми конфіденційності, якщо його виконують неналежно.

У той час як приватні особи є головними цілями атак соціальної інженерії, організація також може бути навмисною жертвою. Проте люди залишаються головною точкою входу для атак соціальної інженерії. Тому людей повинно бути

поінформовано щодо пов'язаних ризиків у кіберпросторі, та організації повинні встановити відповідні політики та здійснити застережні кроки для фінансової підтримки таких програм, які спрямовані на забезпечення обізнаності та компетентності людей. Як загальна рекомендація, усі організації (зокрема підприємства, постачальників послуг та державні органи) повинні заохочувати споживачів вивчати та розуміти ризики соціальної інженерії в кіберпросторі й кроки, які вони мають здійснити для їхнього захисту від потенційних атак [19].

2.2 Дослідження ринку

Однією з найпопулярніших платформ для тестування співробітників на сьогоднішній день є KnowBe4.

Рисунок 2.1 – Офіційна сторінка платформи KnowBe4

Платформа дозволяє [20]:

- Тестування одночасно до 100 користувачів;
- Локалізація шаблонів понад 20 мовами та налаштування його відповідно до середовища;
- Вибір цільової сторінки;
- Звіт у форматі PDF з відсотком схильності до фішингу.

2.3 Можливості Kali Linux у сфері імітації фішингових атак.

Соціальна інженерія має різні фази, перш ніж буде досягнутий кінцевий результат.

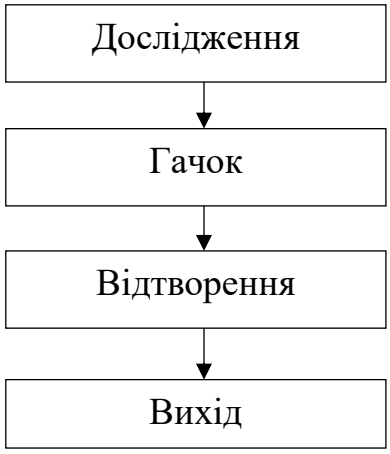

Рисунок 2.2 – Фази соціальної інженерії

Фаза дослідження. На етапі дослідження збирається інформація про ціль. Ця початкова фаза не залежить від того, чи є ціль компанія чи окрема організація. Існують різні способи, які зловмисники використовують для отримання інформації про своїх цілей. Серед них — отримання документів із загальнодоступного доступу, відвідування веб-сайту відповідної установи, а в деяких випадках взаємодія один на один є конструктивною. Крім того, на цій стадії атаки важливо занурюватися в смітник.

Фаза гачка. Це другий етап атаки, при якому нападник починає розмову зі своєю метою.

Фаза відтворення. Після гачка фаза є фазою гри, яка зміцнює відносини між нападником і метою. Зловмисник користується цією можливістю, щоб дізнатися, як отримати потрібну інформацію.

Фаза виходу. Це остання фаза, і зловмисник чутливий, щоб не створювати сцену, яка будь-яким чином зробить ціль підозрілою. Ідея полягає в тому, щоб вийти, не маючи жодного натяку на розгляд справи [21].

Нижче наведено опис кількох інструментів соціальної інженерії, доступних у Kali Linux.

Набір інструментів соціальної інженерії, який зазвичай називають SET, є інструментом тестування на проникнення з відкритим кодом для соціальної інженерії та інших атак. SET має кілька користувацьких векторів атаки, які дозволяють атакувати ціль в найкоротші терміни.

Ці інструменти використовують поведінку людей, щоб обманути їх у векторі атаки. У SET є два основних типи атак: тестування на проникнення та соціальна інженерія.

Команда setoolkit використовується для запуску SET.

Набір має три основні варіанти запуску атаки:

1. Виберіть варіант 1, щоб запустити атаки соціальної інженерії;
2. Виберіть варіант 2, щоб почати атаки тестування на проникнення на ціль;
3. Виберіть варіант 3, щоб використовувати сторонні модулі, інструменти та програми, за допомогою яких можна вставляти шкідливий код у веб-сторінку, електронну пошту або мережеву систему цілі.

Рисунок 2.3 – settoolkit

Приклад атаки називається фішинговою атакою. Під час цієї атаки модуль створює електронний лист, що містить шкідливий код, який надсилається на групу користувачів.

SET містить в собі інструменти для ряду атак зі сфери соціальної інженерії.

В розділі Spear-Phishing Attack Vectors містяться інструменти для масового розсилання електронних листів, що містять файли зі шкідливим вмістом.

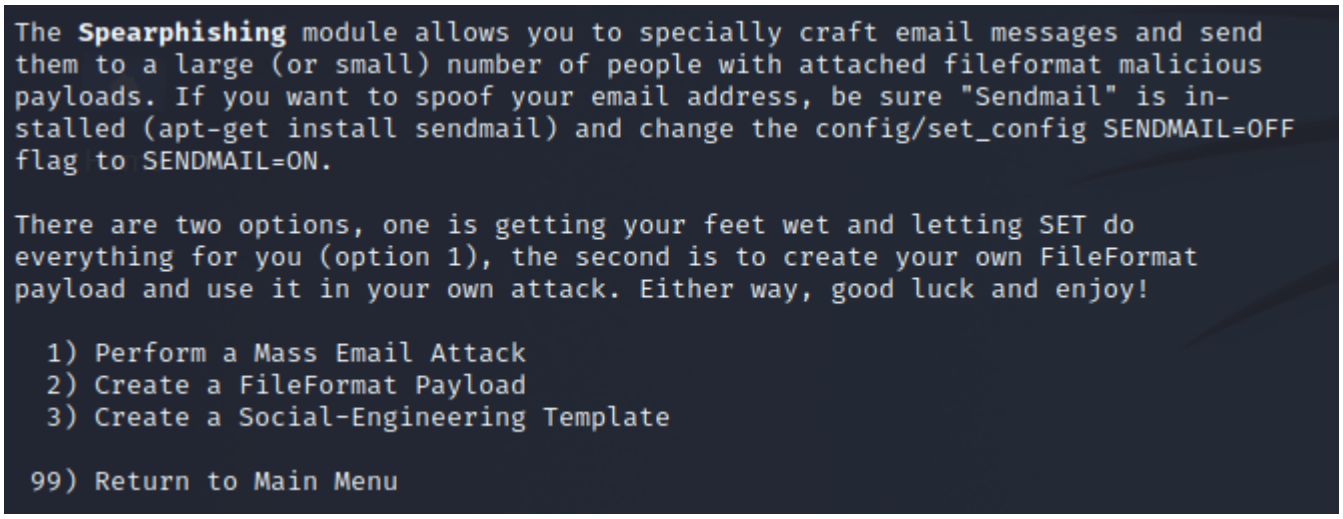

Рисунок 2.4 – Опції SET

Генератор листів має вигляд звичайного текстового редактору без застосування HTML.

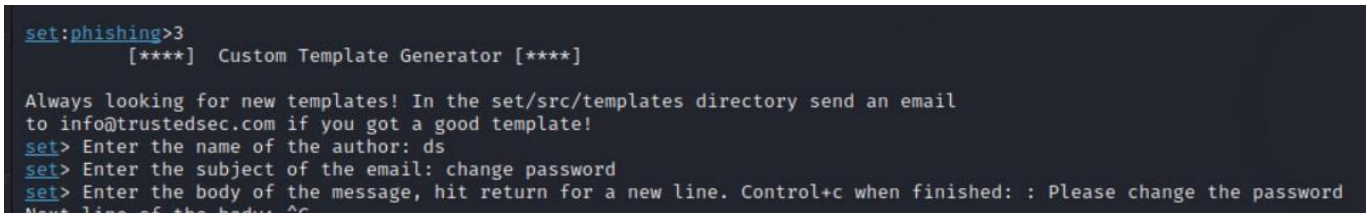

Рисунок 2.5 – Редактор шаблонів електронних листів в SET

Функціонал SET обмежений та застарілий, тому що відсутня можливість зробити повноцінний шаблон електронного листа з редактором HTML структури, зображеннями та посиланнями, без яких сучасні фішингові листи не мають успіху, тобто тестування не є ефективним.

2.4. Віртуальна лабораторія для тестування співробітників щодо фішингових атак

Виходячи з того, що наявні інструменти Kali Linux, які було описано у попередньому підрозділі недостатні, як і тренувальні платформи, необхідне рішення, яке буде зручним та ефективним для тестування співробітників компаній на предмет фішингових атак.

Під час дослідження цієї проблеми було знайдено її можливе вирішення – віртуальна лабораторія для тестування співробітників на предмет фішингових атак.

Тестування у такій лабораторії відбувається тільки згідно чинного законодавства та при узгодженості всіх сторін, які приймають участь у процедурі.

Логічна структура віртуальної лабораторії для тестування співробітників на предмет фішингових атак має таку логічну структуру:

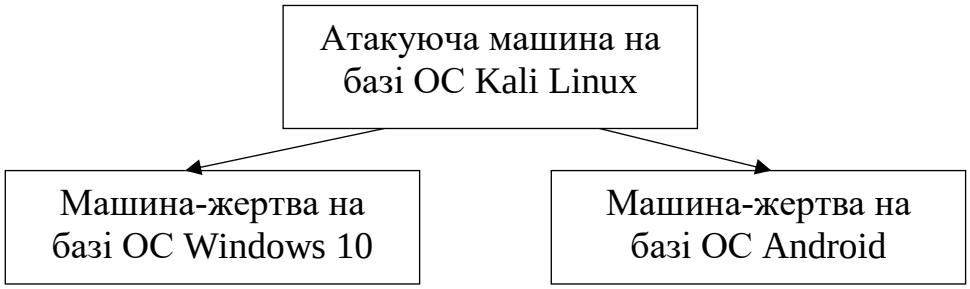

Рисунок 2.6 – Логічна структура віртуальної лабораторії

Структура лабораторії має такий такі функції:

- Створення фішингового листа;
- Створення веб-сторінки;
- Аналіз дій користувача.

Створення імітації фішингового листа один з ключових етапів фішингової кампанії. За основу шаблонів можна взяти приклади, які пропонує платформа KnowBe4, що була описана в попередньому підрозділі.

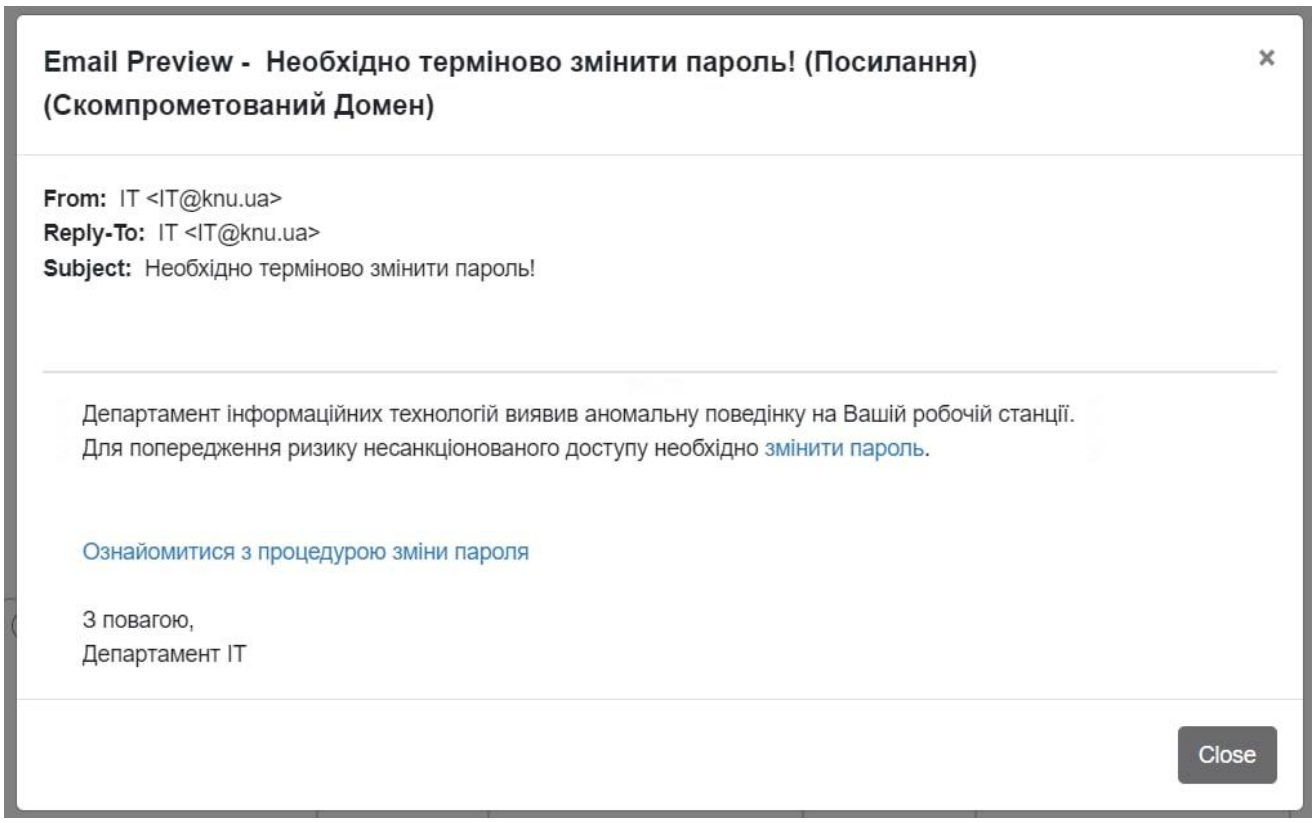

Рисунок 2.7 – Приклад фішингового листа

KnowBe4 дає змогу подивитись які саме елементи в листі повинні викликати підозри у користувача. Це є корисною функцією, яку необхідно впровадити в віртуальну лабораторію на етап створення імітації фішингового листа.

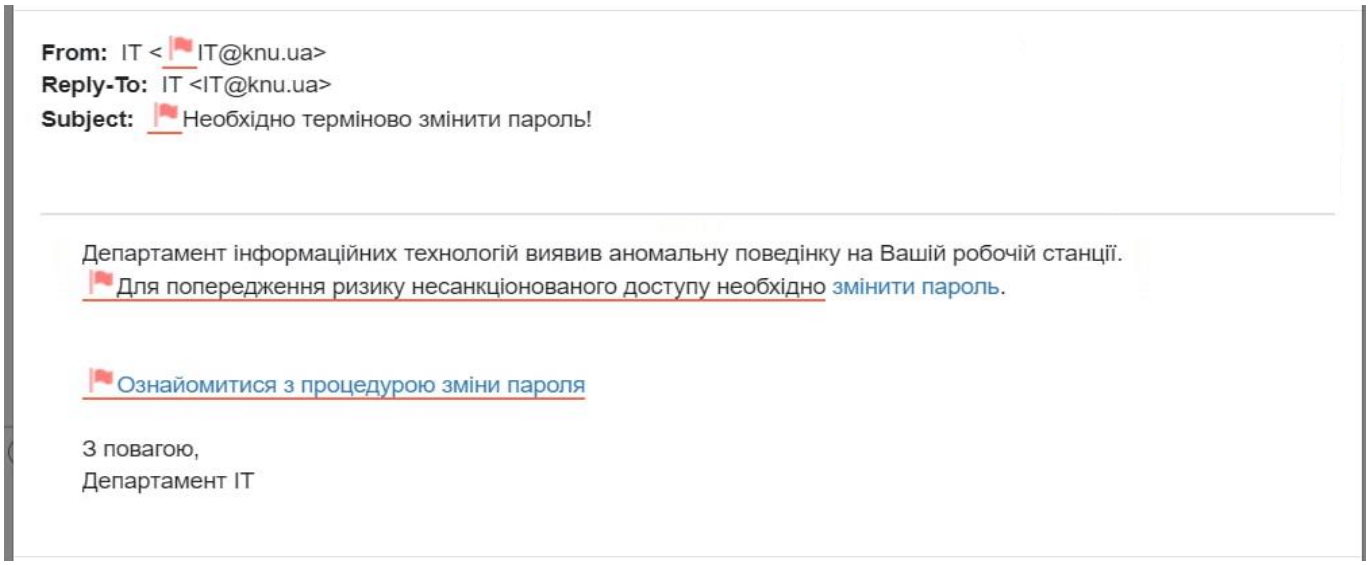

Рисунок 2.7 – Позначення ознак фішингового листу

Наступним етапом імітації фішингової кампанії розсилка листів електронною поштою. Задля реалізації цього кроку пропоную використовувати фреймворк Gophish, який має в собі всі необхідні функції.

Після надсилання листів необхідно реалізувати спостереження за діями користувача після його отримання та його реакцію на імітацію веб-сторінки, на яку він має перейти по маскованому посиланню в листі. Щоб здійснити цей етап пропоную використовувати інструменти ngrok, seeker, bigbro. В своєму функціоналі вони містять створення веб-сторінки та реагування на дії користувача на ній та під час переходу на неї.

Фінальним етапом тестування є отримання звіту про схильність співробітників до фішингових атак. Звіт має містити в собі оцінки дій користувача на всіх етапах імітаційної фішингової кампанії та відсоток користувачів, які перейшли за межу недопустимого реагування на фішингову атаку. Межею пропоную вважати перехід за посиланням в імітації листа. Будь-яке посилання в листі від справжнього зловмисника може мати шкідливі файли або направляти жертву на сторінку, за допомогою якої атакуючий може отримати інформацію з обмеженим доступом. Після пересічення даної межі пропоную вважати тест нескладеним, користувачу терміново необхідно пройти навчання.

Висновки до розділу 2

Згідно стандарту ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT) організації зобов’язані проводити навчання серед свої співробітників на предмет фішингових атак.

Для тестування робітників із застосуванням імітації фішингових атак існують такі платформи як, наприклад, KnowBe4. Але функціонал таких сервісів не є достатнім, тому необхідне більше повнофункціональне рішення у цій сфері. Також було досліджено ОС Kali Linux, яку зазвичай використовують для пентестування тощо. Ця операційна система містить в собі інструменти, які дозволяють проводити

імітацію фішингової атаки, проте, цей інструментарій не є зручним та не є достатнім для імітації фішингової атаки. Тому в цьому розділі було запропоноване рішення – віртуальна лабораторія для тестування співробітників щодо фішингових атак. Ця лабораторія має досить просту структуру та достатній функціонал для повноцінної імітації фішингової кампанії, а також функціонал, який дозволяє спостерігати за схильністю працівників до фішингових атак.

РОЗДІЛ 3
ПОБУДОВА ВІРТУАЛЬНОЇ ЛАБОРАТОРІЇ

3.1 Складові віртуальної лабораторії.

Під час побудови віртуальної лабораторії було вирішено використовувати VirtualBox – програму віртуалізації для оперційних систем. Підтримується такими системами як Linux, FreeBSD, Mac OS X, OS/2 Warp, Microsoft Windows, які підтримують роботу гостьових операційних систем FreeBSD, Linux, OpenBSD, OS/2 Warp, Windows і Solaris. Програма встановлюється на наявну ОС, яка є хостовою, усередину цієї програми встановлюється інші ОС, яка є гостьовою [22].

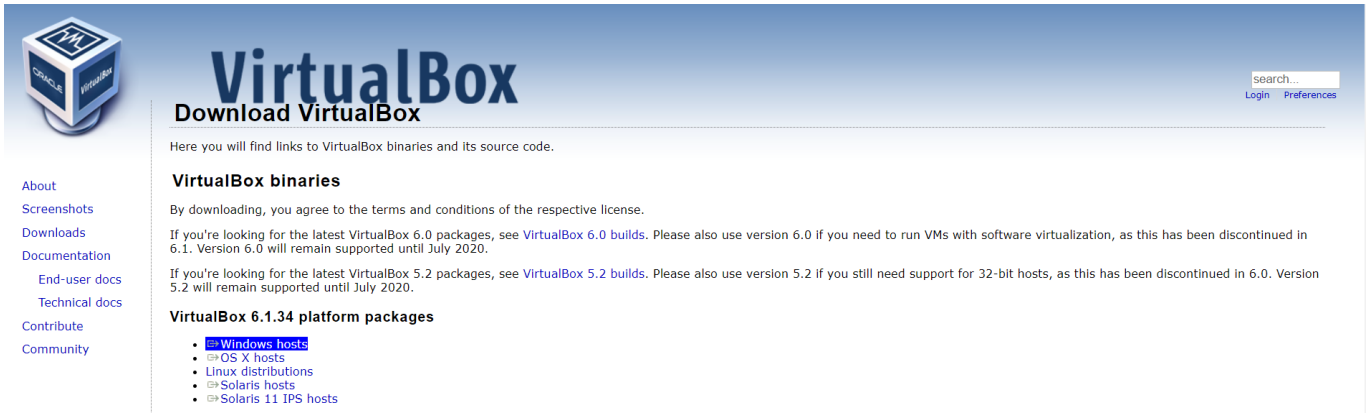

Рисунок 3.1 -- Офіційна сторінка VirtualBox

Для імітації машини атакуючого було обрано операційну систему Kali Linux.

Системні вимоги Kali Linux:

- Kali Linux потребує не менше 20 ГБ простору на жорсткому диску для установки;
- Мінімум 1 ГБ оперативної пам'яті для архітектур i386 та amd64;
- Завантажувальний CD-DVD диск або USB флешку.

Kali Linux має спеціалізований проект, відведений для утворення сумісності та перенесення для конкретних пристроїв Android, що називається Kali Linux NetHunter.

BackTrack (попередник Kali) мав у собі режим, відомий як forensic mode, який був пізніше перенесений у Kali Linux з live boot. Цей режим дуже популярний, особливо через те, що користувачі містять в собі носій із завантажувальною Kali, і цей режим дозволяє легко виконувати криміналістичну роботу. При завантаженні в forensic mode, система не зачіпає внутрішній жорсткий диск і автоматичне встановлення відключене. Проте, розробники рекомендують користувачам перевірити функції перед широким використанням Kali для реальної цифрової криміналістики [23].

Особливості даної ОС [24]:

- Повне налаштування ISO Kali . Завдяки використанню метапакетів , оптимізованих для конкретних потреб спеціаліста з безпеки, і дуже доступного процесу налаштування ISO завжди легко створити оптимізовану версію Kali для конкретних потреб. Kali Linux інтегровано з live-build , що забезпечує нескінченну гнучкість у налаштуванні та адаптації кожного аспекту образів ISO Kali Linux. Це можна продемонструвати за допомогою базового прикладу пресетів збірки, наприклад, Kali ISO пресету doom, який показує типи та складність можливих налаштувань - створення образу Kali, що самовстановлюється, автоматичного підключення до VPN, мережевого моста - для ідеального апаратного бэкдора.
- Live USB Boot. Це дозволяє розмістити Kali на USB-пристрій і завантажуватися, не торкаючись операційної системи хоста (ідеально підходить для будь-якої криміналістичної роботи). З додатковими постійними томами можна обирати, яку файлову систему використовувати під час запуску Kali, дозволяючи зберігати файли між сеансами, створюючи кілька профілів. Кожен постійний том може бути зашифрованою важливою ознакою, необхідною в галузі. Якщо цього недостатньо, також є опція LUKS nuke , що дозволяє швидко контролювати знищення даних.
- Калі під прикриттям. Kali Undercover ідеально підходить для того, щоб не виділятися, поєднуючись зі звичною операційною системою, яку більшість людей знає.

- Win-KeX. Використання Kali на WSL забезпечує підсистему Kali Desktop Experience для Windows для Linux із безперебійними вікнами, спільним доступом до буфера обміну, підтримкою аудіо тощо.
- Kali APM . Підтримка понад 12 різних пристроїв ARM та поширеного обладнання, такого як Raspberry Pi, Odroid, Beaglebone тощо. Пропонуються попередньо згенеровані зображення, готові до використання, а також скрипти для створення інших.
- Галузевий стандарт. Kali Linux є безперечним галузевим стандартом платформи тестування на проникнення з відкритим кодом.

Для імітації машин-жертв було обрано ОС Windows 10 та Android. Згідно статистики Windows є найпопулярнішою ОС серед користувачів [25].

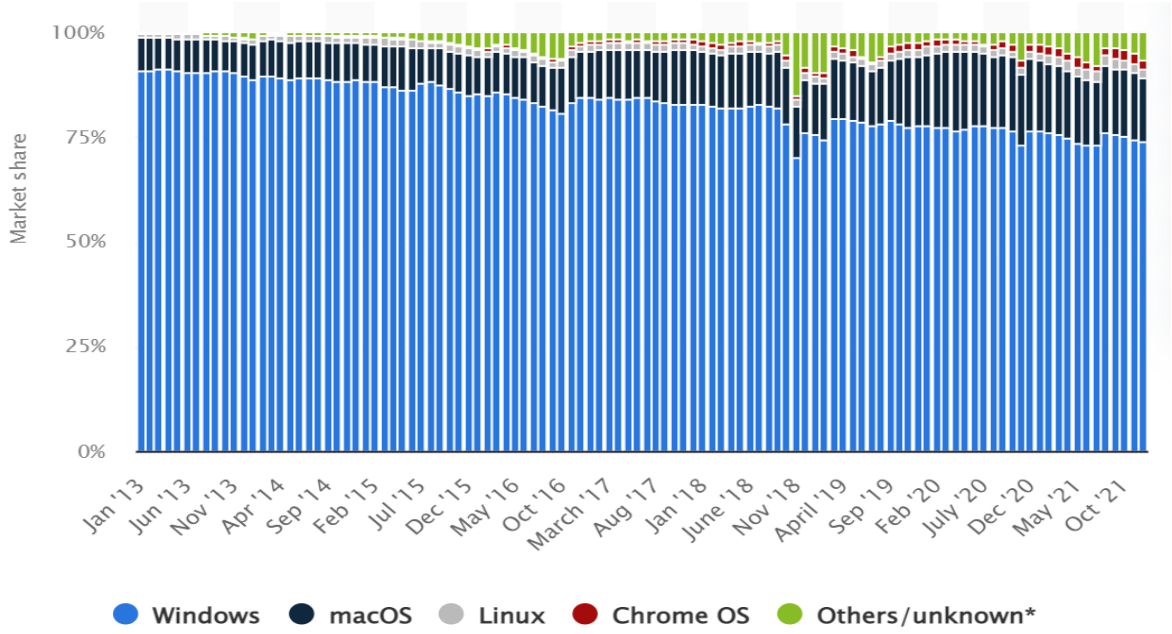

Рисунок 3.2 – Статистика популярності ОС серед користувачів

Згідно статистики Android є найпопулярнішою операційною системою для мобільних девайсів [26].

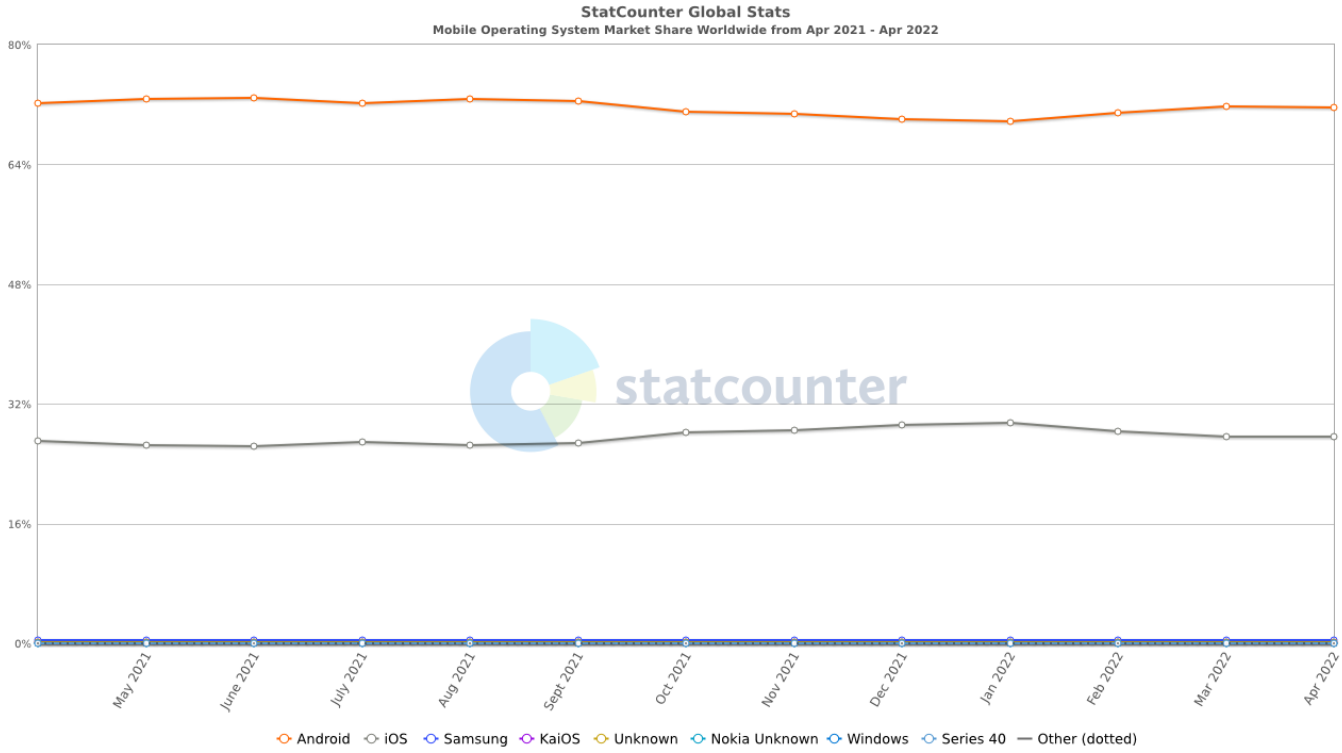

Рисунок 3.3 – Статистика популярності ОС для смартфонів

Після встановлення гостьових ОС їх можна запустити у менеджері віртуальних машин VM VirtualBox.

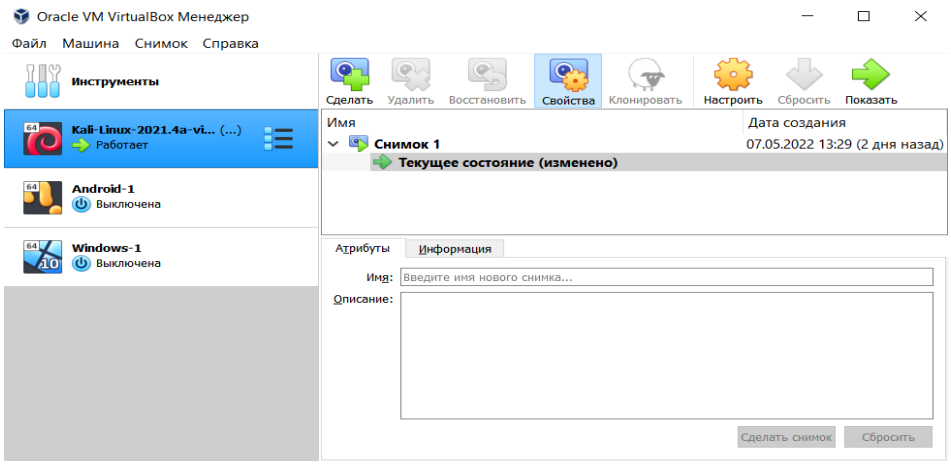

Рисунок 3.4 – Менеджер VM VirtualBox

3.2 Створення листа.

Електронна пошта у сучасному світі є зручним і потужним інструментом зв’язку. Небажана комерційна електронна пошта, або «спам», є відправною точкою

для багатьох шахрайств електронною поштою. До появи електронної пошти зловмисники повинні були зв’язатися з кожною потенційною жертвою окремо поштою, факсом, телефоном або через прямий особистий контакт. Ці методи часто вимагають значних вкладень часу та грошей. Щоб підвищити шанси на зв’язок із вразливими жертвами, шахраю, можливо, довелося провести попереднє дослідження «особливостей», на які він або вона націлився. Електронна пошта змінила гру для шахраїв. Зручність та анонімність електронної пошти, а також можливість легкого зв’язку з тисячами людей одночасно дають змогу шахраям активно працювати. Шахраям потрібно лише обдурити невеликий відсоток з десятків тисяч людей, яким вони надсилають електронні листи, щоб це окупилося.

Тестування співробітників на предмет фішингу відбувається згідно схеми типової фішингової атаки, яка представлена на наступному рисунку.

Рисунок 3.5 – Схема фішингової атаки

Згідно рис.3.5 першим кроком фішингової кампанії є створення листа-шаблону для поштової розсилки жертвам. Задля забезпечення цієї функції у віртуальний лабораторії пропоную використовувати фреймворк Gophish.

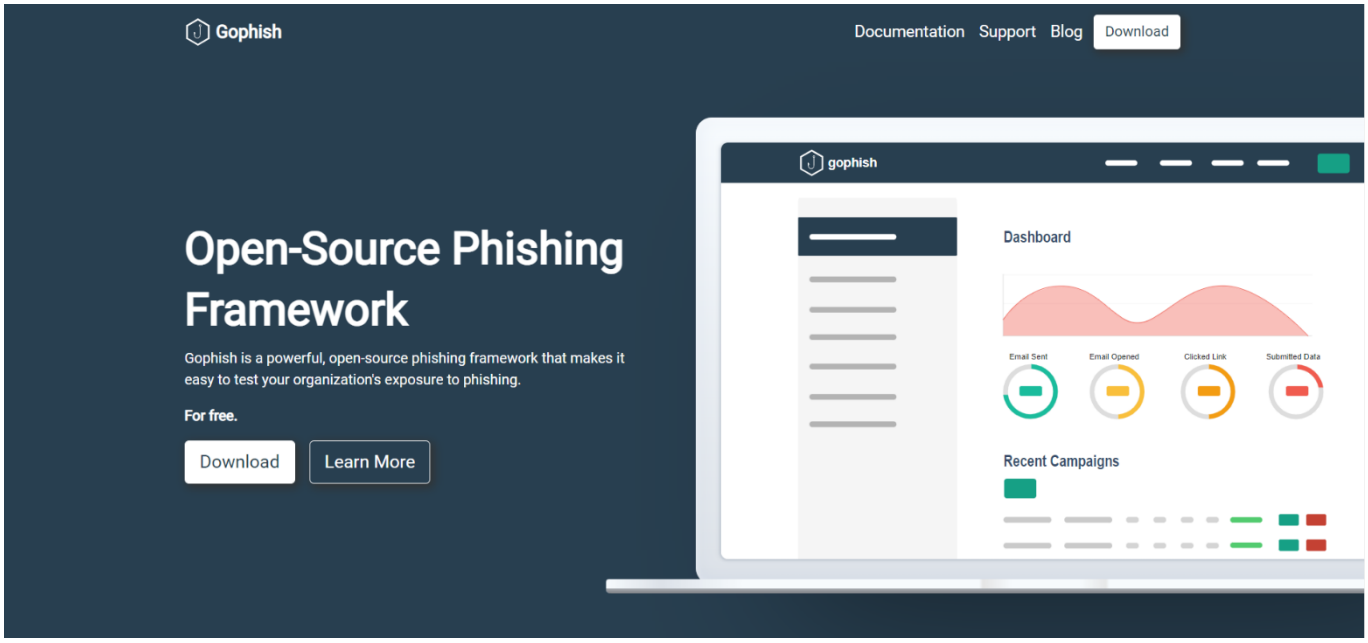

Рисунок 3.6 – Офіційна сторінка Gophish

Переваги фреймворку Gophish [27]:

- Gophish дозволяє легко створювати або імпортувати pixel perfect шаблони листів фішингу. Веб-інтерфейс містить повноцінний редактор HTML, що дозволяє легко налаштовувати шаблони прямо у браузері;
- Функція надсилання листів у фоновому режимі, а також можливість відкладеного надсилання;
- Відстеження результатів. Детальні результати надаються майже в режимі реального часу. Результати можна експортувати для використання у звітах.

Запропонована програма має зручний інтерфейс для створення груп розсилки, який зображено на рис.3.7.

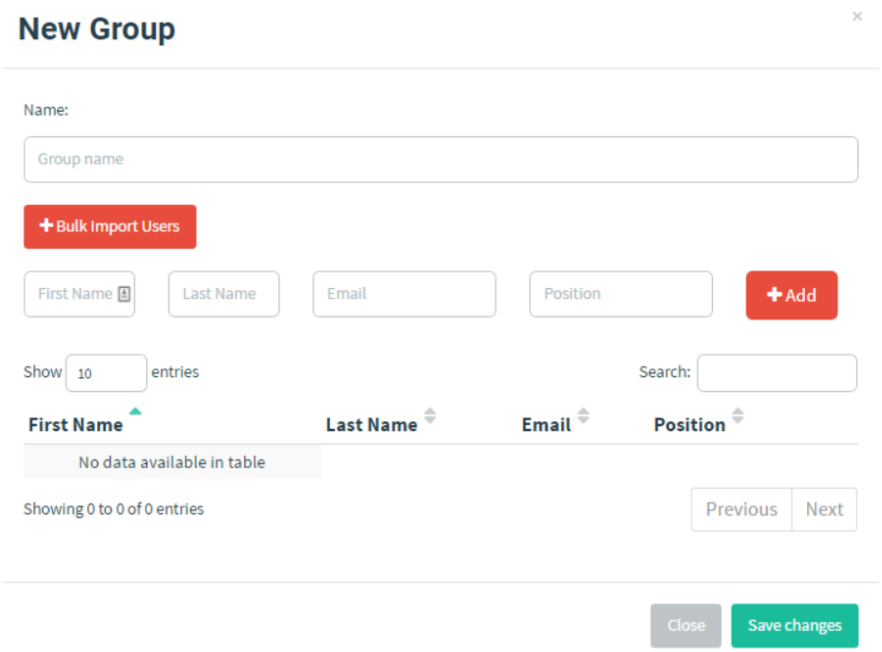

Рисунок 3.7 – Створення групи в Gophish

Додавання користувачів вручну може бути проблемою. Щоб виправити це, Gophish дозволяє масово завантажувати користувачів із файлу CSV.

Формат CSV, який Gophish очікує, має такі значення заголовків:

- Ім'я;
- Прізвище;
- Електронна пошта;
- Позиція.

Задля початку розсилки листів необхідно обрати потрібний шаблон. Популярними шаблонами для фішингових листів є листи, які імітують такі популярні сервіси як Outlook, Microsoft365, Facebook, Linkedin, Google Drive тощо. Слід зазначити, що gophish має зручний інтерфейс для створення шаблонів фішингових листів.

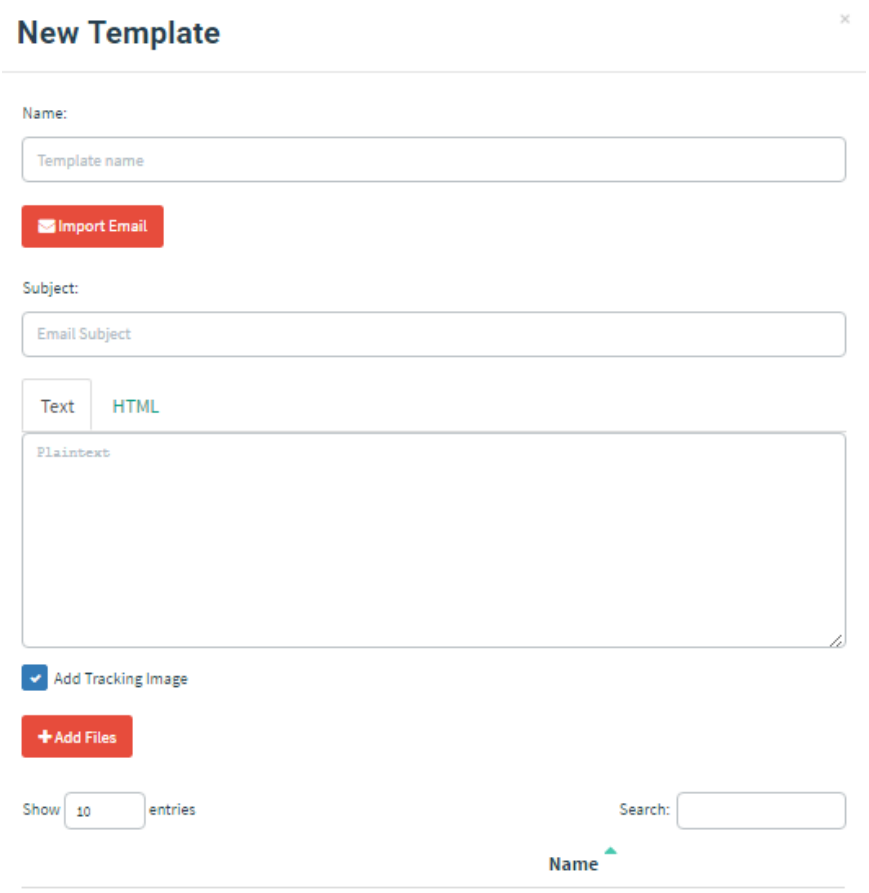

Рисунок 3.8 – Інтерфейс створення шаблону фішингової сторінки

Потужною особливістю Gophish є редактор HTML.

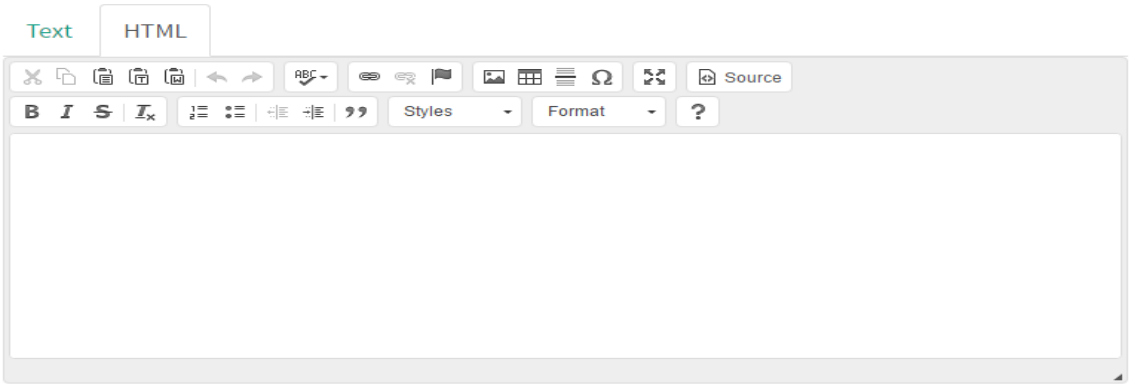

Рисунок 3.9 – HTML редактор вбудований в Gophish

Gophish підтримує можливість імпортування електронних листів.

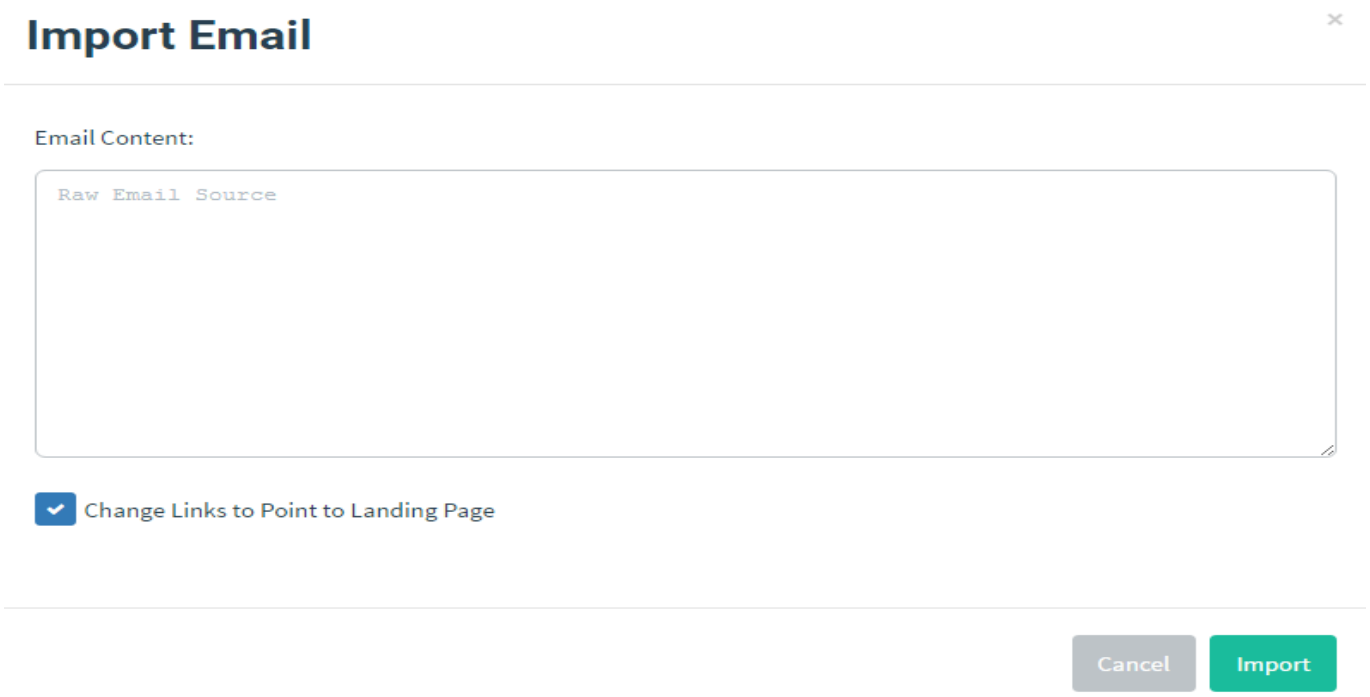

Рисунок 3.10 – Інтерфейс імпортування електронних листів в Gophish

3.3 Інструменти створення фішингових атак

Перед тим як встановлювати необхідні інструменти в машину атакуючого, необхідно підготувати систему.

По-перше, потрібно оновити систему. Для оновлення системи (її пакетів) використаємо команди apt-get update та apt-get upgrade.

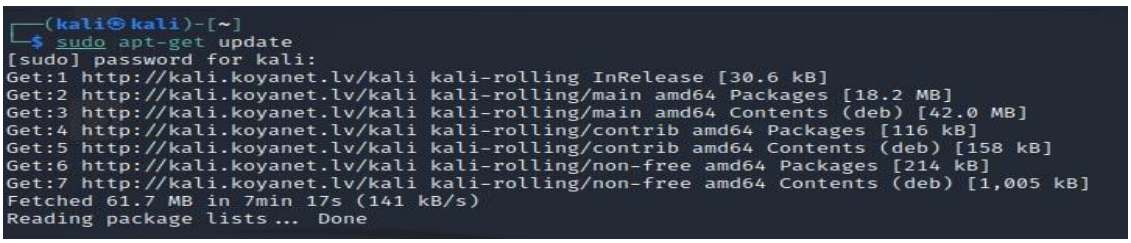

Рисунок 3.11 – apt-get update

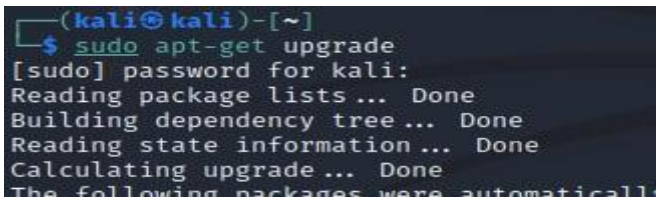

Рисунок 3.12 – apt-get upgrade

Необхідно здійснити очищення системи Kali Linux. Для початку було видалено проміжні пакети (пакети, які були потрібні для встановлення інших пакетів) за допомогою команди apt-get autoremove.

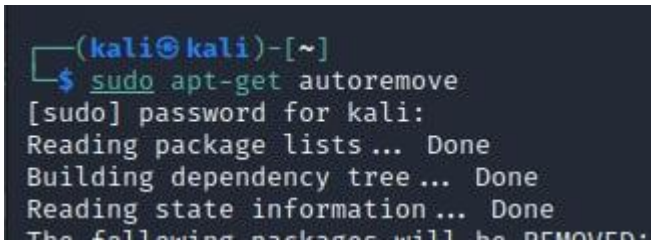

Рисунок 3.13 – apt-get autoremove

Далі видалимо deb-файли із директорії apt cache командою apt-get autoclean.

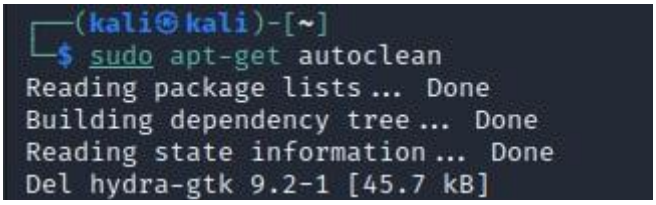

Рисунок 3.14 – apt-get autoclean

Необхідно перевірити які пакети встановлені командою dpkg --list | grep linux-image.

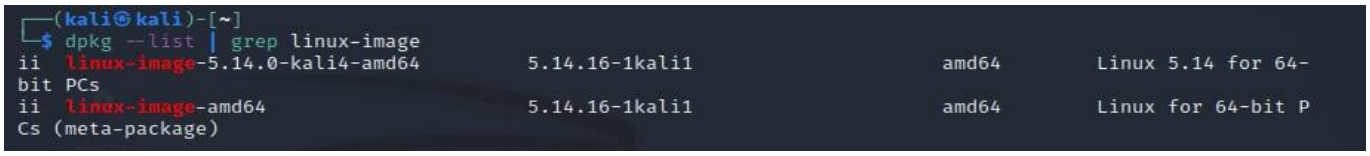

Рисунок 3.15 – dpkg --list | grep linux-image

За допомогою команди uname -r можна перевірити чи присутні зайві пакети.

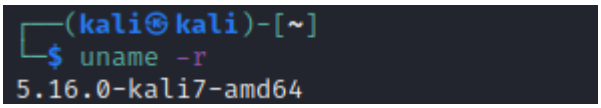

Рисунок 3.16 – uname -r

На скріншоті можна побачити, що зайві пакети відсутні, тому переходимо до наступного кроку. Так як python3 не встановлено в системі, переходимо до встановлення за допомогою команди apt install python3 python3-pip php ssh git.

Рисунок 3.17 – apt install python3 python3-pip php ssh git

Для роботи з HTTP необхідно інсталювати модуль requests за допомогою команди pip install requests.

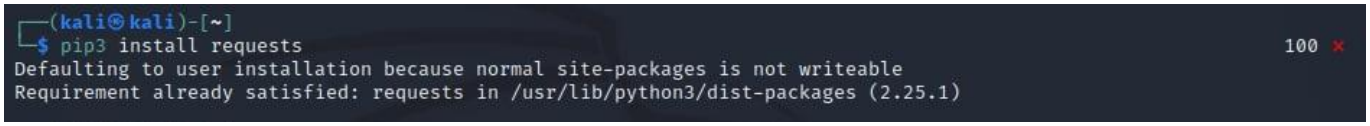

Рисунок 3.18 – pip install requests

Далі необхідно завантажити seeker за допомогою команди git clone.

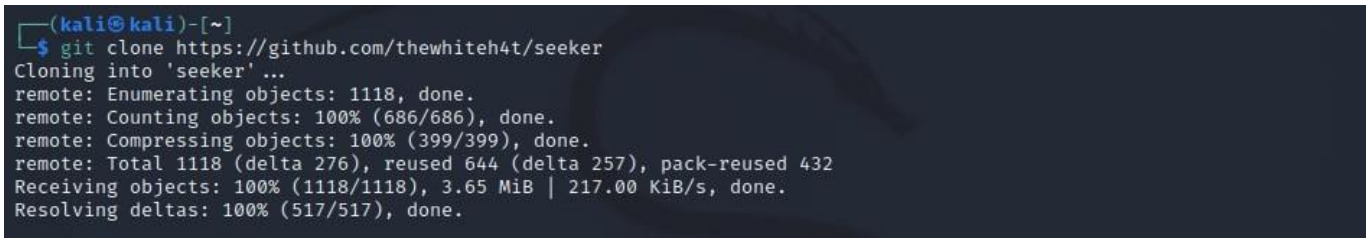

Рисунок 3.19 – git clone https://github.com/thewhiteh4t/seeker

Бачимо, що seeker вже присутній в нашій системі. Наступним кроком буде перевірка наявності файлу seeker.py в системі.

Рисунок 3.20 – Перевірка наявності seeker в системі

На скріншоті можна побачити перехід у директорію /seeker, що свідчить про те, що вона існує у системі та всі необхідні файли присутні. Надати право на виконання файлу seeker.py можна за допомогою команди chmod +x seeker.py

Рисунок 3.21 – chmod +x seeker.py

Прапорці seeker наведені в таблиці 3.1.

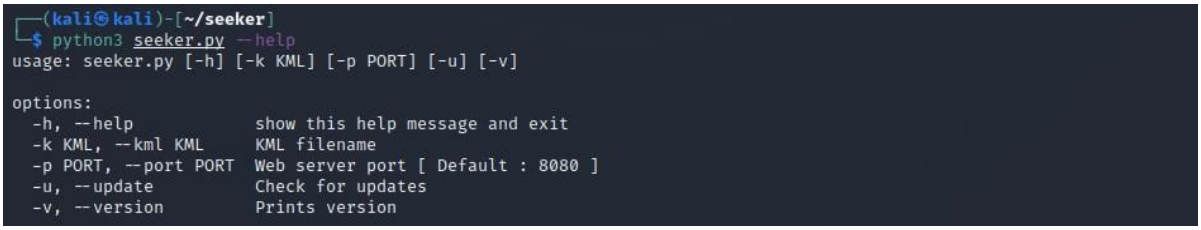

Рисунок 3.22 – python3 seeker.py --help

Таблиця 3.1

Прапорці seeker

Прапорець	**Опис**
-h, --help	Показати інструкцію
-s, --subdomain	Субдомен для Serveo URL
-k KML, --kml KML	Ім'я файлу KML
-t, --tunnel	Вказати режим тунелю
-p, --port	Порт для Веб Сервера

Для початку процесу інсталювання необхідно завантажити архів з офіційної сторінки ngrok.com

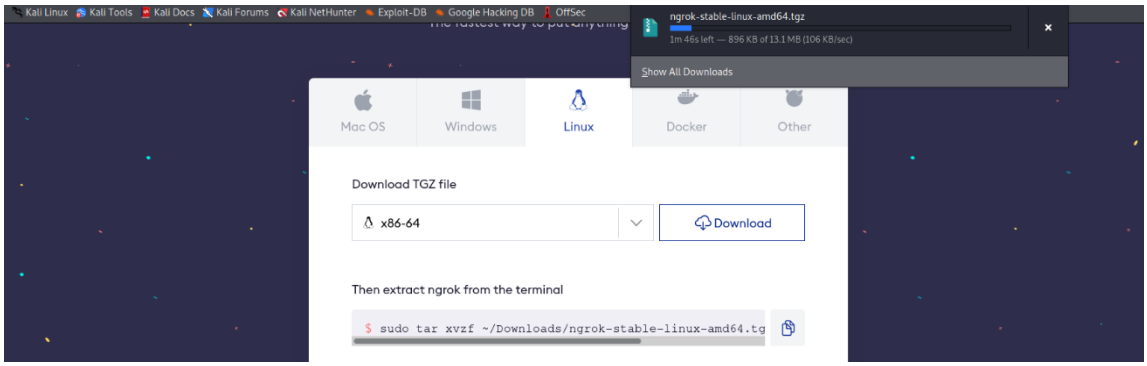

Рисунок 3.23 – Офіційна сторіка ngrok

Розпакування архіву tgz виконується за допомогою команди sudo tar xvzf ~/Downloads/ngrok-stable-linux-amd64.tgz -C /usr/local/bin

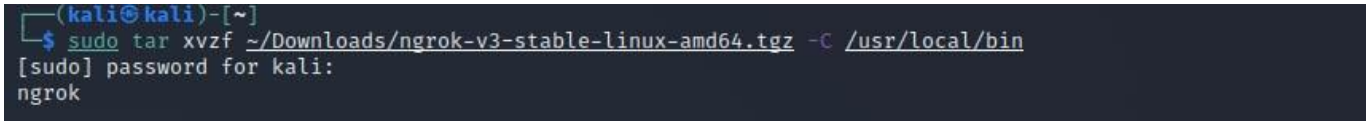

Рисунок 3.24 – Розпакування архіву ngrok

Щоб переглянути інструкцію до ngrok необхідно виконати команду ngrok --help (рис.3.25). Команди ngrok наведені в таблиці 3.2.

Таблиця 3.2

Команди ngrok

Команда	**Опис**
authtoken	Зберегти токен аутентифікації в конфігураційний файл
credits	Надрукувати інформацію про автора та ліцензію
http	Запустити HTTP тунель
start	Запустити тунелі по ім'ям з конфігураційного файлу
tcp	Запустити TCP тунель
tls	Запустити TLS тунель
update	Оновити ngrok до останньої версії
version	Надрукувати версію ngrok
help	Вивести інструкцію

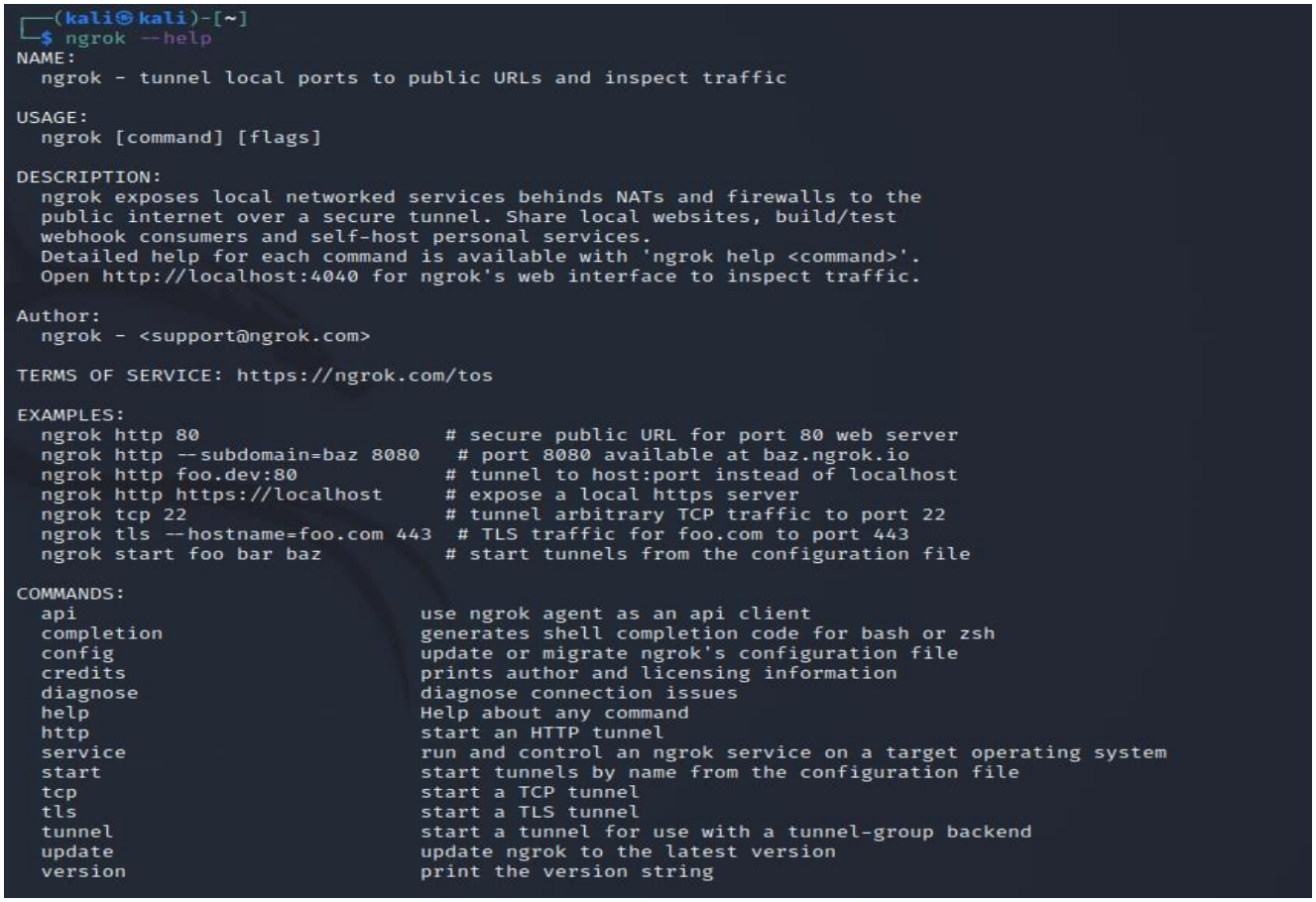

Рисунок 3.25 – Доступні команди ngrok

Далі перейдемо до використання seeker та ngrok. Вимоги для проведення тестування фішингової атаки: усі тестові сервери (ПК, смартфони і т.ін) та їхній вміст перебувають під контролем та управлінням керуючого тестуванням. Тестування відбувається тільки після проінформованості та узгодженості організації. Тестування фішингової атаки було з віртуальної системи Kali Linux, а цільовою була віртуальна система Windows.

Запуск seeker.py. Пропонується на вибір 4 шаблони веб-сторінок за допомогою яких буде створена фішингова сторінка. Також розробник seeker надає можливість створювати свій шаблон фішингової сторінки.

Запускаємо seeker.py за допомогою команди python3 ./seeker.py

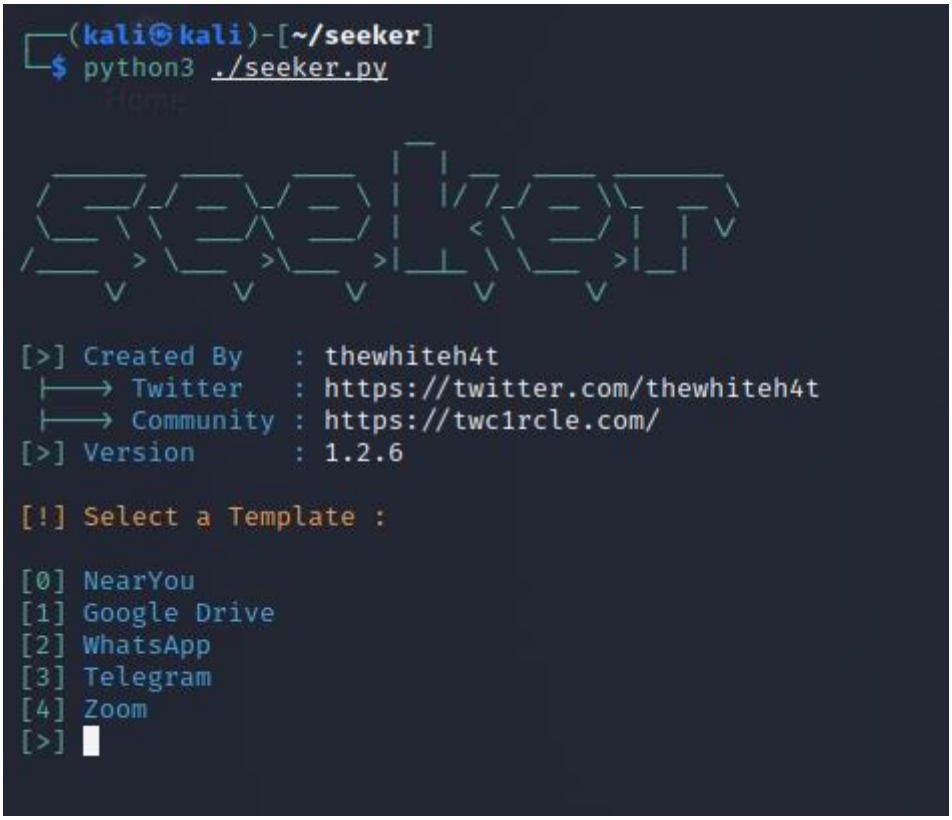

Рисунок 3.26 – Seeker

Далі seeker пропонує 5 шаблонів веб-сторінок, які імітують такі сервіси як NearYou, Google Drive, WhatsApp, Telegram, Zoom. Обираємо один з шаблонів та ініціюємо тунель за допомогою ngrok на потрібному порті.

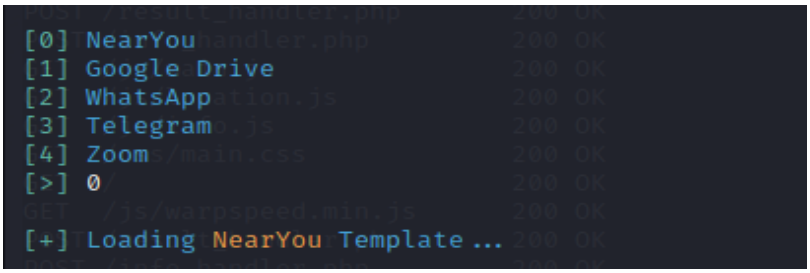

Рисунок 3.27 – Обрано перший шаблон NearYou

Рисунок 3.28 – Ініціювання тунелю в ngrok

Далі необхідно скопіювати посилання з ngrok на фішингову веб-сторінку.

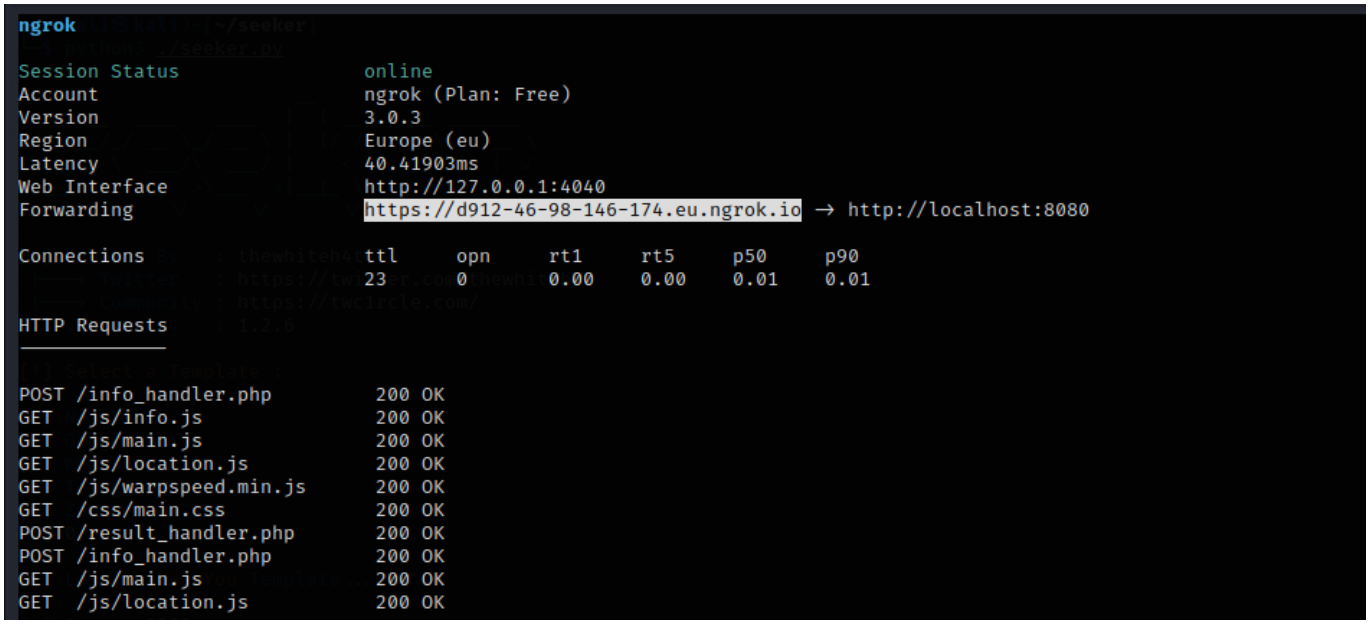

Рисунок 3.29 – Створений тунель ngrok

Це посилання необхідно вбудувати у лист, який буде надіслано жертві.

При переході по посиланню жертва бачить таку сторінку (рис.3.30).

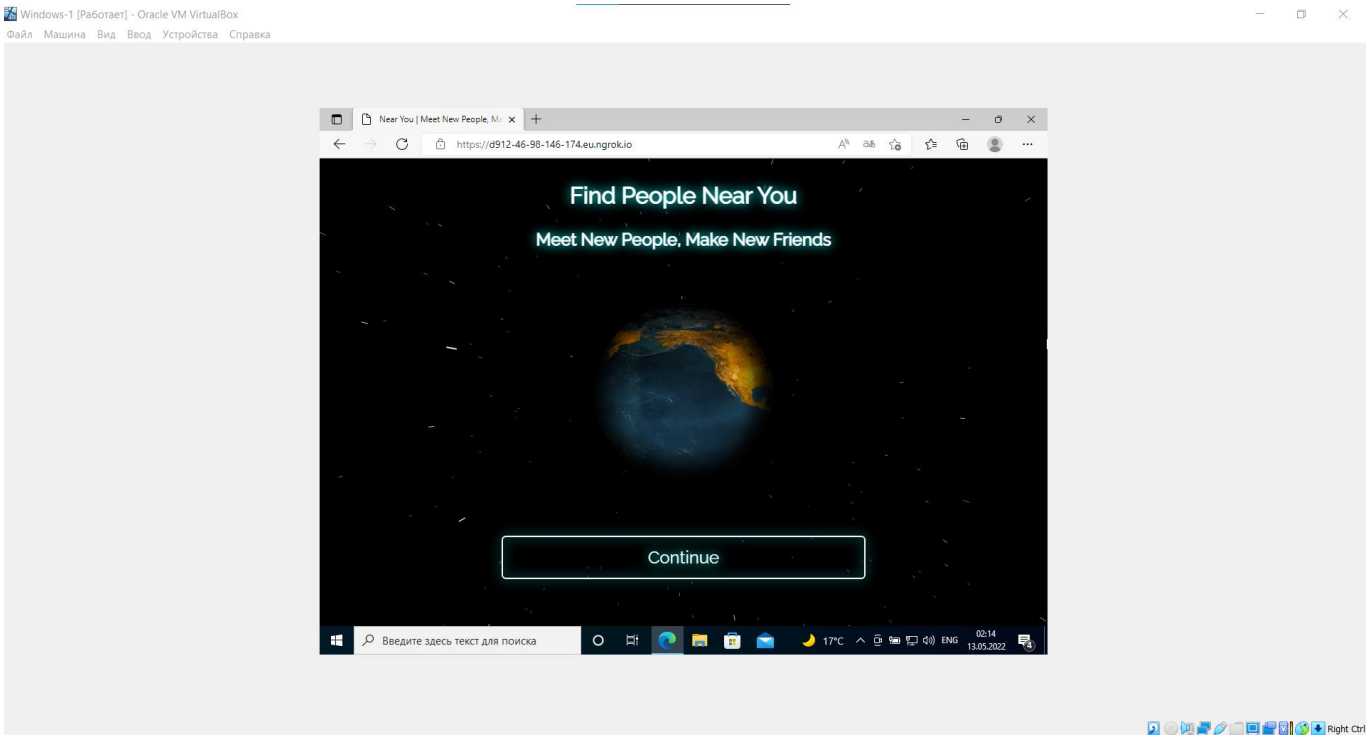

Рисунок 3.30 – Фішингова сторінка від seeker

Після натискання на кнопку “Continue” в браузері з’являється запит на поширення місцезнаходження. Для успішного фішингу користувач повинен дати згоду на поширення цієї інформації.

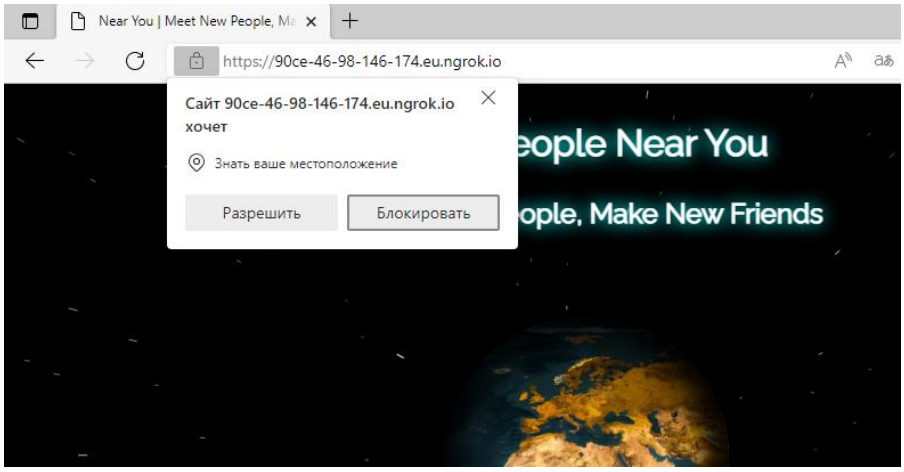

Рисунок 3.31 – Запит на поширення місцезнаходження

Коли користувач погоджується на поширення свого місцезнаходження він бачить на екрані модальне вікно від ngrok, а машина атакуючого отримує дані про його місцезнаходження, характеристики девайсу тощо (докладніше про данні, які може отримати атакуючий наведено в таблиці 3.3).

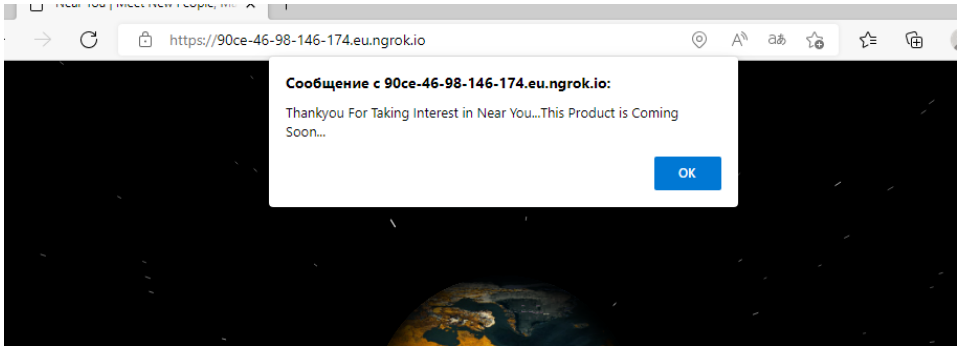

Рисунок 3.32 – Модальне вікно від seeker

```
[!] Select a Template :

[0] NearYou
[1] Google Drive
[2] WhatsApp
[3] Telegram
[4] Zoom
[>] 1

[+] Loading Google Drive Template ...
[+] Enter GDrive File URL : https://drive.google.com/drive/folders/1DhvOOrzp_e9JRCw1iiz_FyPj2hvAeTsH

[+] Port : 8080

[+] Starting PHP Server ... [ ✔ ]

[+] Waiting for Client ... [ctrl+c to exit]
```

Рисунок 3.33 – Вибір другого шаблону Google Drive

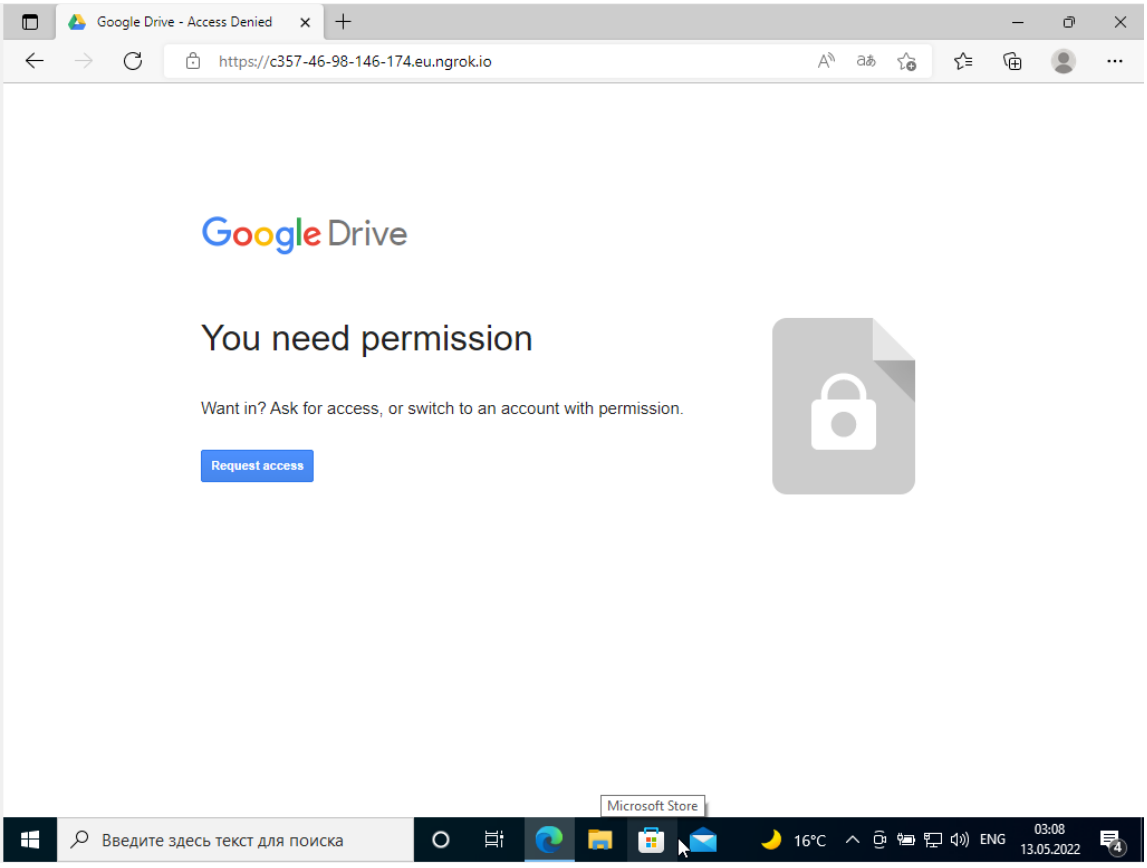

Рисунок 3.34 – Фішингова сторінка Google Drive

Після того, як користувач дає згоду на поширення свого місцезнаходження, він переходить за посиланням, яке вказував зловмисник на рис.3.33.

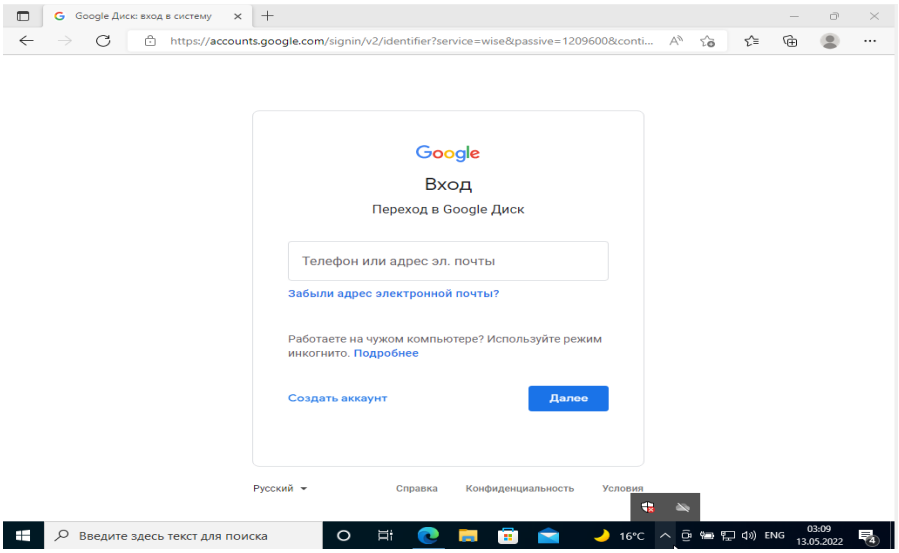

Рисунок 3.35 – Сторінка яка відкривається після поширення місцезнаходження.

При виборі шаблону WhatsApp є можливість обрати свій заголовок групи та її аватарку.

Рисунок 3.36 – Формування веб-сторінки переходу в чат WhatsApp

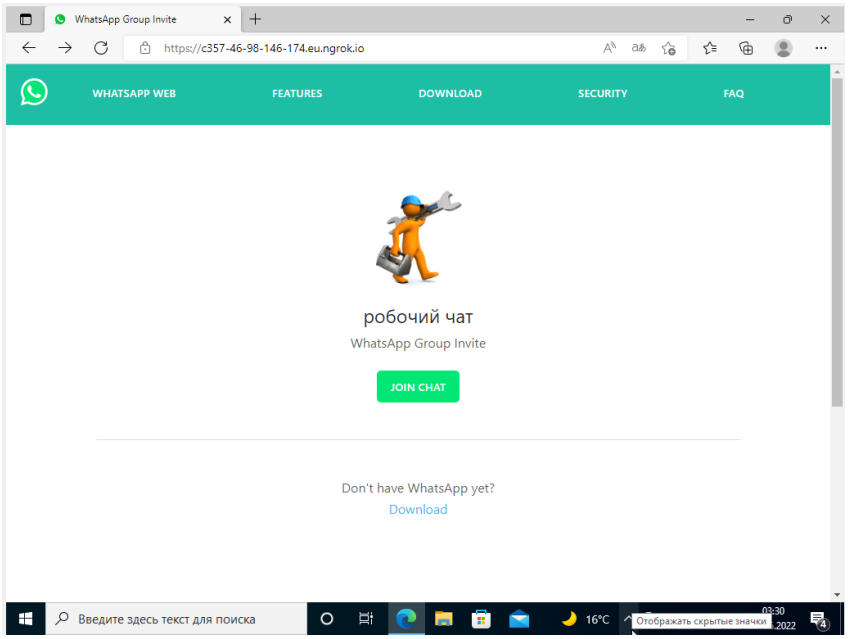

Рисунок 3.37 – Вигляд фальсифікованої сторінки WhatsApp

Останнім з запропонованих вбудованих в seeker шаблонів є сторінка, яка імітує запрошення на приєднання до онлайн-конференції в додатку Zoom.

```
[>] Created By    : thewhiteh4t
 ├──> Twitter     : https://twitter.com/thewhiteh4t
 ├──> Community   : https://twc1rcle.com/
[>] Version       : 1.2.6

[!] Select a Template :

[0] NearYou
[1] Google Drive
[2] WhatsApp
[3] Telegram
[4] Zoom
[>] 3

[+] Loading Telegram Template ...
[+] Group Title : робочий чат
[+] Group Description : Чат для працівників відділу охорони праці.
[+] Image Path (Best Size : 300×300) : /home/kali/Downloads/worker.jpg
[+] Number of Members : 34
[+] Number of Members Online : 10
```

Рисунок 3.38 – Введення даних для заповнення шаблону Telegram

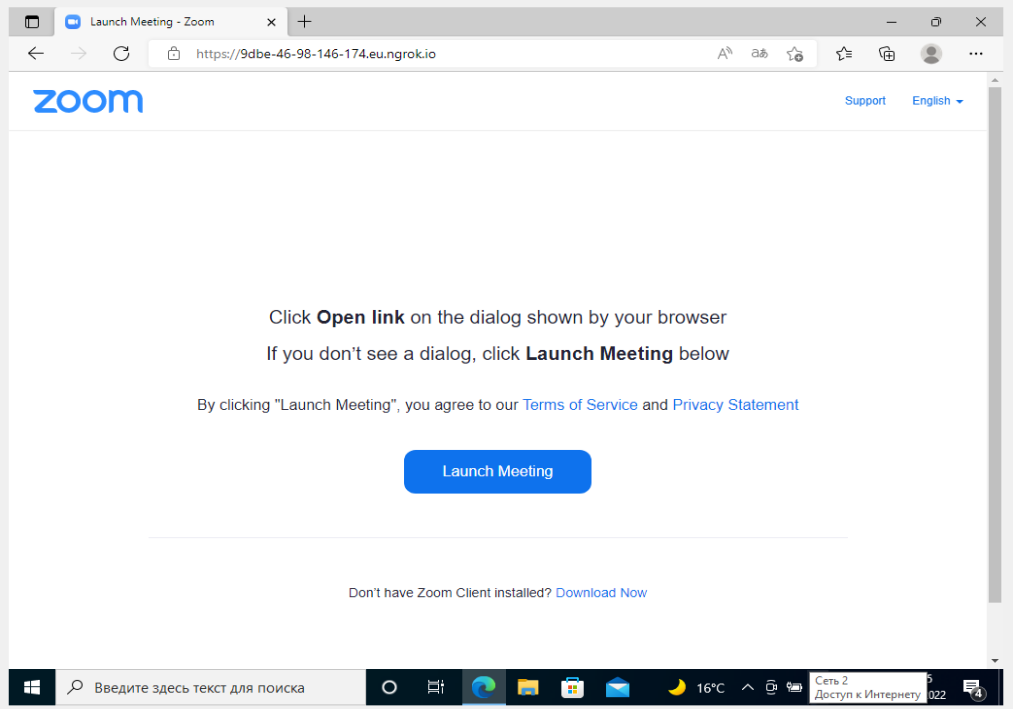

Рисунок 3.39 – Фішингова сторінка Zoom

Якщо користувач дає дозвіл на поширення місцезнаходження зловмисник отримує такі дані за допомогою seeker:

- Довготу;
- Широту;
- Точність;
- Висоту над рівнем моря — не завжди доступно;
- Напрямок руху — доступно тільки якщо користувач рухається;
- Швидкість руху — доступно тільки якщо користувач рухається;
- Посилання на google maps.

Поряд з інформацією про місцезнаходження атакуючий також отримує інформацію про пристрій без будь-яких дозволів:

- Операційна система;
- Платформа;
- Кількість ядер процесора;
- Обсяг оперативної пам'яті – приблизні результати;
- Розширення екрану;

- Інформація про GPU;
- Ім'я та версія браузера;
- Публічна IP-адреса;
- Розкриття IP-адрес.

Рисунок 3.40 – Дані, які отримав зловмисник за допомогою seeker

На рис.3.41 можна спостерігати, що різниця між даними від seeker та фактичним місцезнаходженням жертви складає 57 метрів.

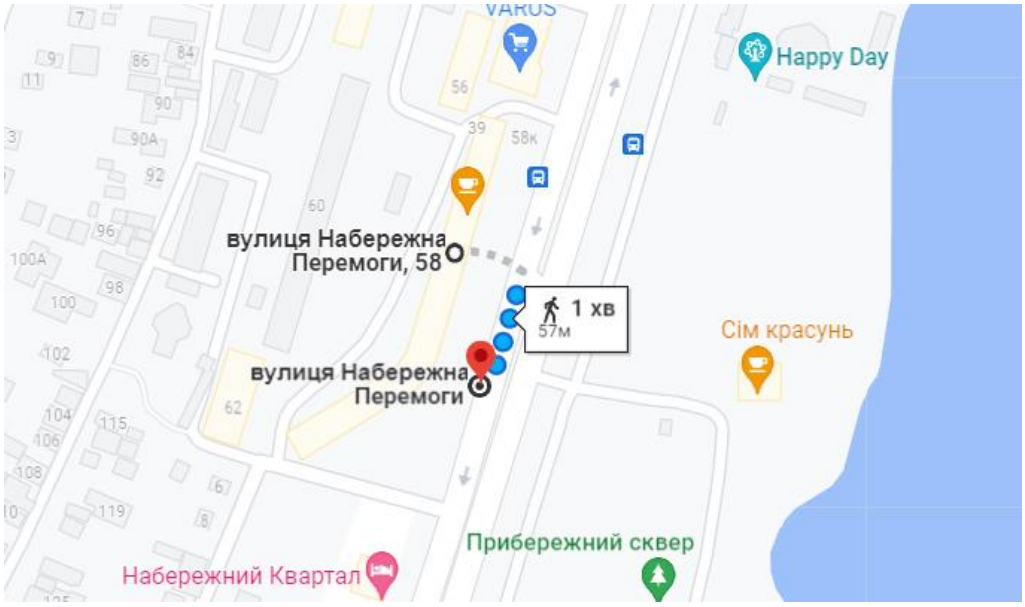

Рисунок 3.41 – Погрішність в інформації від seeker

Поряд з цим, seeker автоматично формує звіт до процесу тестування у вигляді текстового файлу.

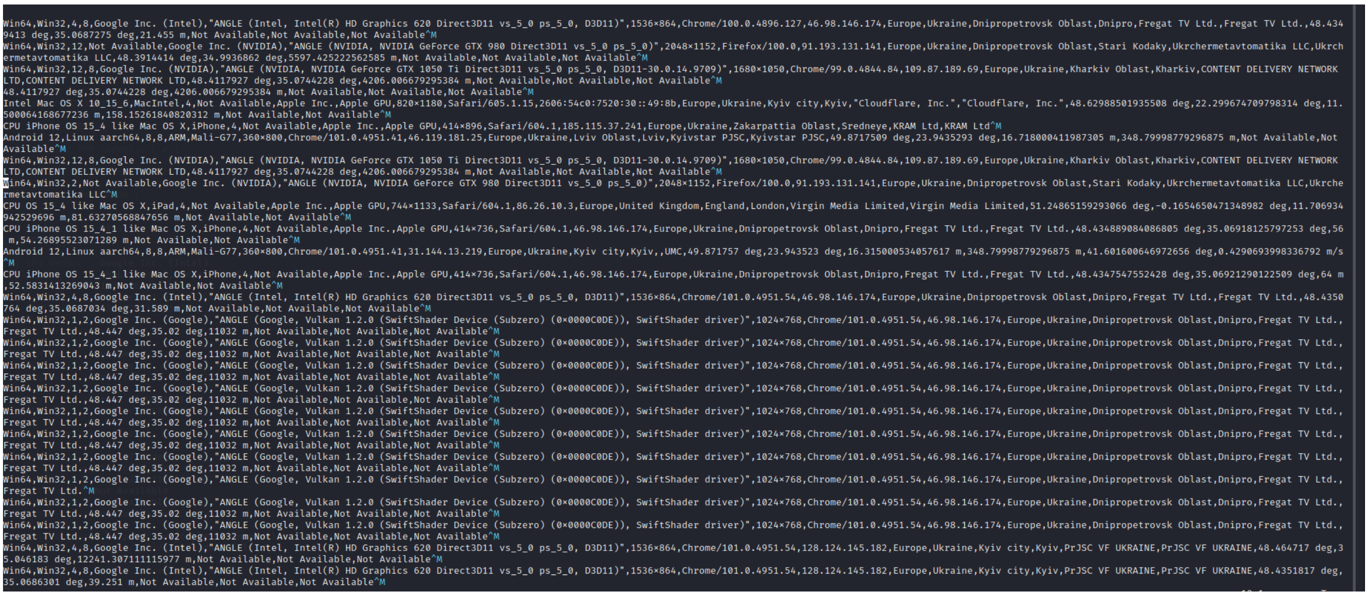

Рисунок 3.42 – Звіт до тестування

Досліджування порядку тестування можливої фішингової атаки за допомогою Big Bro.

Для інсталяції bigbro необхідно завантажити всі файли зі сторінки розробника за допомогою команди git clone.

Рисунок 3.43 – git clone bigbro

Після інсталяції запуск можна здійснити за допомогою команди python3 brother.py. Так як і seeker bigbro пропонує ряд вбудованих фішингових сторінок.

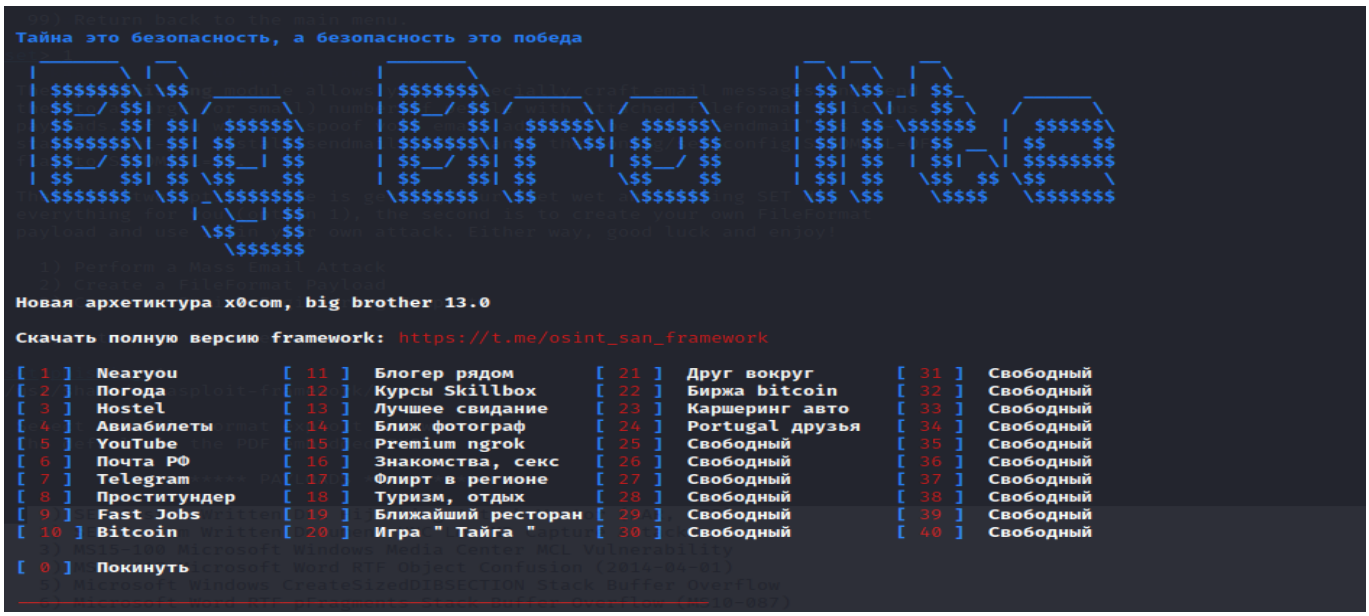

Рисунок 3.44 – Список шаблонів в bigbro

Для прикладу було обрано веб-сторінку, яка представляє собою сервіс каршерінгу автомобілів, та відкриваємо її на машині-жертві з ОС android.

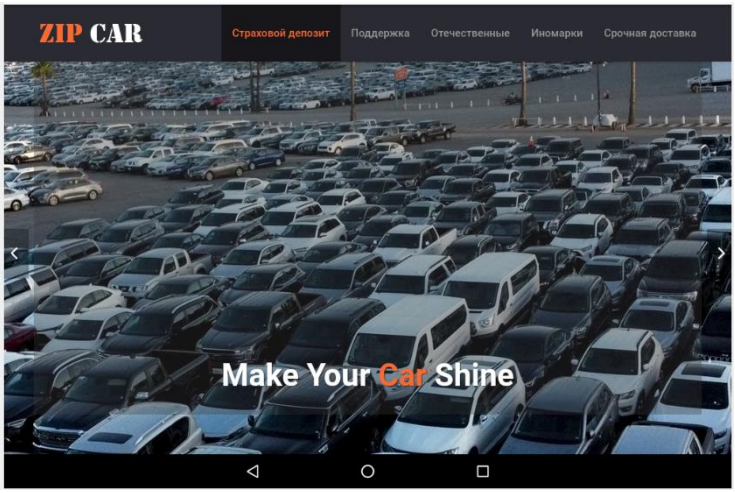

Рисунок 3.45 – Фішингова сторінка каршерінгу від bigbro

На відміну від seeker інформація про девайс за допомогою bigbro надходить одразу ж, коли користувач переходить на фішингову сторінку.

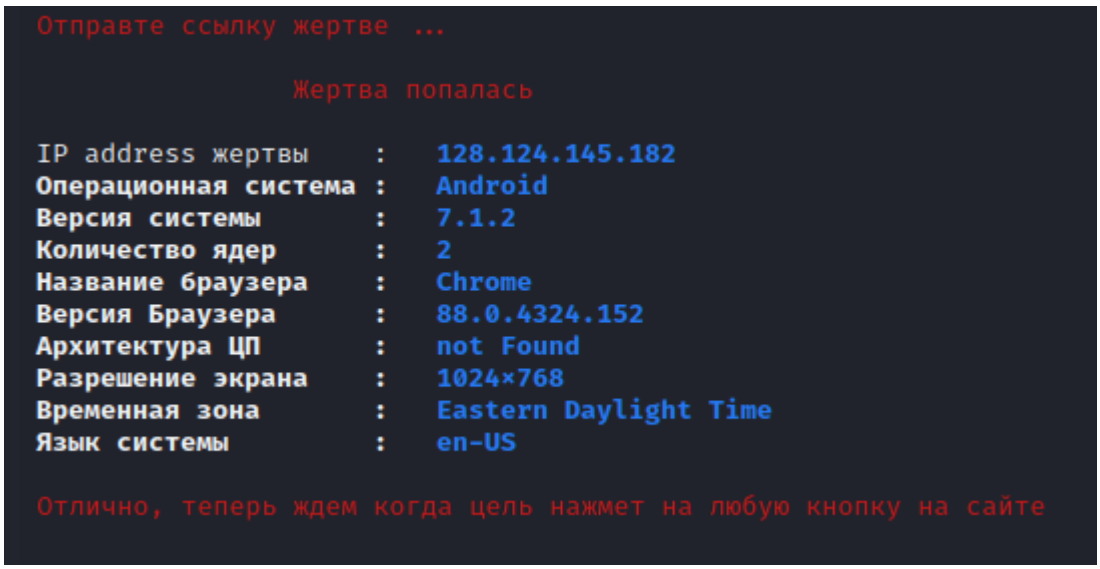

Рисунок 3.46 – Інформація про пристрій отримана в bigbro

Для отримання інформації про місцезнаходження, жертва повинна натиснути будь-яку кнопку на сторінці та дати згоду на поширення своєї геолокації.

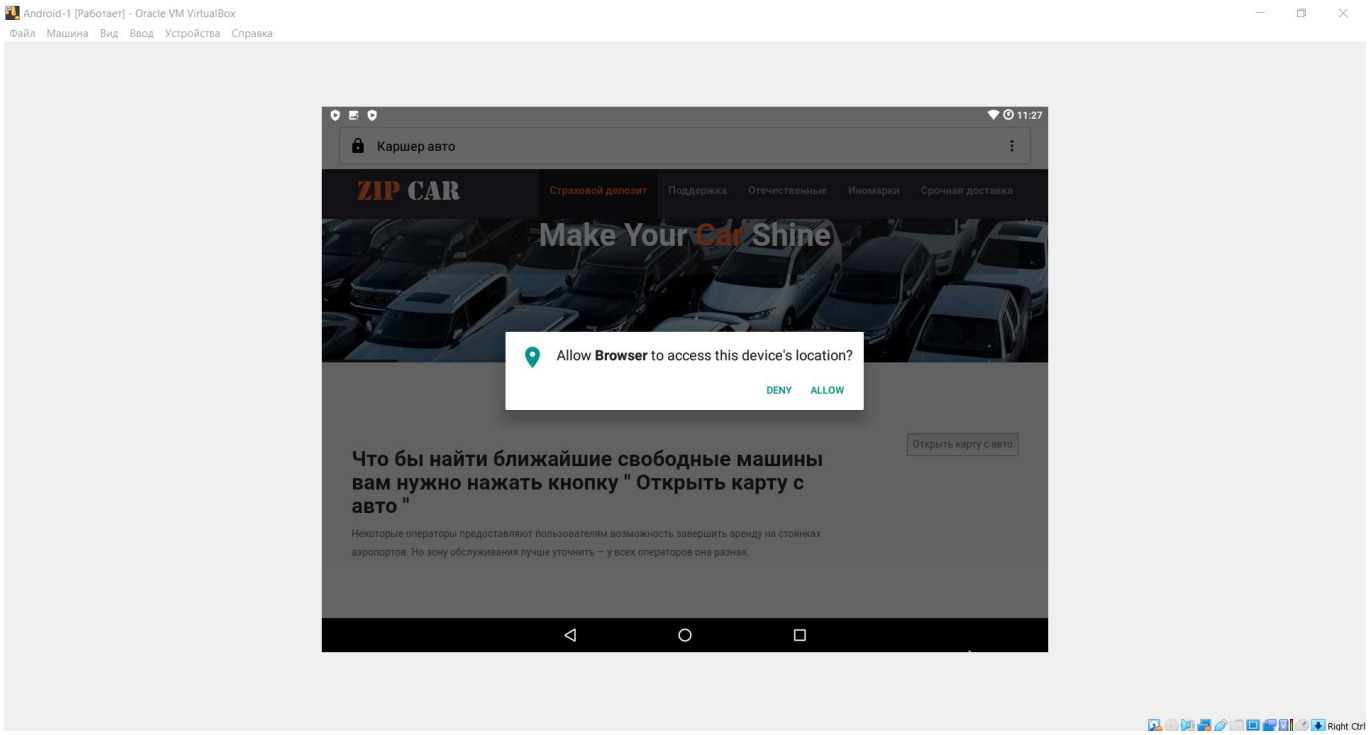

Рисунок 3.47 – Запит на поширення геолокації на веб-сторінці bigbro

За допомогою bigbro зловмисник може отримати координати жертви та посилання на google maps з місцезнаходженням жертви.

```
Координаты цели: Широта - 48.43482722333386 Долгота - 35.06906188141455
https://www.google.com/maps/place/48.43482722333386+35.06906188141455
Сайты с геолокацией открыты
```

Рисунок 3.48 – Координати жертви

Після перевірки на точність результатів було виявлено погрішність в 120 метрів.

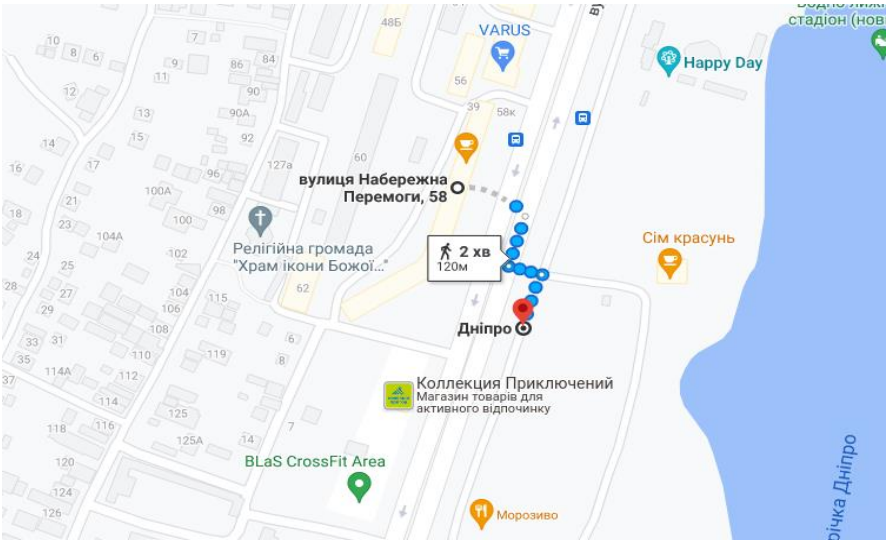

Рисунок 3.49 – Різниця між отриманими даними від bigbro та фактичним місцезнаходженням

Переваги seeker:

- Інформація про жертву є більш розширеною. В seeker можна отримати не лише геодані, як це можливо в bigbro, але й технічні характеристики девайсу, ip-адресу тощо.
- Всі скрипти в ngrok працюють коректно. Під час дослідження bigbro на деяких пристроях android неможливо було отримати інформацію про місцезнаходження умовної жертви через 404 або 408 помилки у js-скриптах. В seeker всі 4 сайти виконувалися справно, без помилок в скриптах.

- Логічне завершення сценарію сайту після отримання даних. В seeker після отримання доступу до геоданих утиліта генерує продовження сценарію, тобто або надає доступ до ресурсу (як це було в Google Drive), або ж видає повідомлення про помилку. В bigbro після надання доступу (в деяких сайтах) нічого не відбувається, що може викликати підозру.
- Кращий вигляд на смартфоні. При відкритті посилань з версії Android сайт коректно відображався, при цьому на деяких сторінках від bigbro хибна локалізація, тому текст чи різні графічні елементи можуть некоректно відображатись на екрані пристрою.
- Зручність збереження. Всі результати атак зберігаються у відповідному файлі, тому доступ до них можна отримати в будь-який час.
- Розробник seeker інформує про те, що є можливість створення свого шаблону веб-сторінки, що є незаперечною перевагою під час реалізації фішингової атаки у цілях тестування.

Переваги bigbro:

- Більший вибір сайтів. Одночасно з тим, як seeker пропонує всього 4 шаблони для веб-сторінок, bigbro пропонує на вибір 40 сторінок у преміум версії, що додає гнучкості в імітації фішінгової кампанії. Проте, близько половини сторінок, запропонованих в bigbro не є актуальними для України та можуть викликати підозру у користувача. Наприклад, сторінки з сайтами знайомств вважаються апріорі підозрілими, тому користувач скоріш за все не дасть згоду на поширення свого місцезнаходження.
- Можливість локалізації на різних мовах. Seeker надає лише стандартні можливості для сайтів (на базовій мові), а в bigbro можна вибрати мову сайту (найчастіше – англійську або російську), тому це також дає перевагу умовному зловмиснику.
- Деякі сайти не відображаються, як шкідливі в google chrome. В seeker перед відкриттям всіх сайтів користувач отримує сповіщення про те, що цей сайт є небезпечним. Поряд з цим в bigbro браузер не «бачить» сторінку як потенційно небезпечну.

Переваги обох утиліт:

- Простота у використанні. За допомогою seeker і bigbro досить легко створити фішинг-сайт буквально в декілька дій. Не потребуються редактори або інші інструменти редагування сайтів, що значно пришвидшує процес тестування співробітників організації на предмет фішингових атак.
- Правдоподібність. Веб-сторінки, які пропонують досліджувані утиліти досить точно копіюють оригінальні ресурси.

Недоліки обох утиліт:

- Повідомлення про можливу небезпеку. На деяких етапах експерименту браузер сповіщав користувача про потенційну небезпеку веб-сайту, що може викликати підозру про фальшивість ресурсу.
- Нелогічність в сценарії сайтів. Деякі веб-сторінки запитують доступ до місцезнаходження в той час, як контент сторінки не повинен цього передбачати. Наприклад, запит на надання місцезнаходження на сторінці з запрошенням до конференції Zoom виглядає досить дивно і це може спровокувати умовну жертву покинути даний веб-сайт.

Seeker та Bigbro легкі та зручні у використанні утиліти, які надають можливість створити якісні фішингові веб-сторінки, та отримати досить багато інформації як про пристрій умовної жертви так і про її місцезнаходження. Проте, seeker показав кращі результати щодо сценаріїв сайтів та має меншу погрішність при наданні інформації про місцезнаходження.

Висновки до розділу 3

За основу віртуальної лабораторії було взято три віртуальні лабораторії на базі VM VirtualBox. Лабораторія складається з трьох машин: ОС Kali Linux (атакуюча), ОС Windows 10 та Android. Ціль цієї віртуальної лабораторії полягає в прискоренні та підвищенні ефективності процесу тестування співробітників щодо фішингових атак.

Функціонал лабораторії має містити в собі такі пункти як створення шаблону електронного листа, створення розсилки цих листів, створення імітації фішингової сторінки та відстеження дій та реакцій користувача під час тестування.

У цьому розділі було досліджено роботу фреймворку Gophish, інструментів ngrok, seeker та bigbro в межах віртуальної лабораторії. За результатами було виявлено, що цей інструментарій достатній для імітації фішингової атаки в цілях навчання співробітників та підвищення їх обізнаності.

ВИСНОВКИ

Для мінімізації наслідків фішингових атак необхідно проводити навчання співробітників. Близько 40% людей схильні до фішингових атак, як показують дослідження, після проведення тренування сприйнятливість знижується на 5%. Було досліджено таксономію фішингу.

Згідно стандарту ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT) організації зобов'язані проводити навчання серед свої співробітників на предмет фішингових атак. Для тестування робітників із застосуванням імітації фішингових атак існують такі платформи як, наприклад, KnowBe4. Також можна використовувати вбудовані в Kali Linux інструменти для імітації фішингової кампанії. Але функціонал таких сервісів не є достатнім, тому необхідне більше повнофункціональне рішення у цій сфері.

Було запропоноване рішення – віртуальна лабораторія для тестування співробітників щодо фішингових атак. Ця лабораторія має досить просту структуру та достатній функціонал для повноцінної імітації фішингової кампанії, а також функціонал, який дозволяє спостерігати за схильністю працівників до фішингових атак.

За основу віртуальної лабораторії було взято три віртуальні лабораторії на базі VM VirtualBox. Лабораторія складається з трьох машин: ОС Kali Linux (атакуюча), ОС Windows 10 та Android. Ціль цієї віртуальної лабораторії полягає в прискоренні та підвищенні ефективності процесу тестування співробітників щодо фішингових атак.

Функціонал лабораторії має містити в собі такі пункти як створення шаблону електронного листа, створення розсилки цих листів, створення імітації фішингової сторінки та відстеження дій та реакцій користувача під час тестування.

Було досліджено роботу та ефективність інструментів ngrok, seeker та bigbro в межах віртуальної лабораторії. За результатами було виявлено, що цей

інструментарій достатній для імітації фішингової атаки в цілях навчання співробітників та підвищення їх обізнаності.

Мета роботи полягала в розробці віртуальної лабораторії для проведення тестування співробітників організації щодо фішингових атак, всі поставлені задачі було виконано, мета роботи досягнута.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Газі-Терані А. К. Phishing Evolves: Analyzing the Enduring Cybercrime / Адам Кавон Газі-Терані, Генрі Н. Понтелл // Victims & Offenders. – 2021.

2. Kumar Jane A. A survey of phishing attack techniques, defence mechanisms and open research challenges [Електронний ресурс] / Ankit Kumar Jane, B. B. Gupta // Enterprise Information Systems. – 2021. – С. 527–565. – Режим доступу: https://www.tandfonline.com/doi/abs/10.1080/17517575.2021.1896786.

3. Pienta D. A Taxonomy of Phishing: Attack Types Spanning Economic, Temporal, Breadth, and Target Boundaries / Daniel Pienta, Jason Bennett Thatcher, Allen C. Johnston // WISP. – 2018.

4. Alerout A. Phishing Environments, Techniques, and Countermeasures: A Survey / Ahmed Alerout, Lina Zhou // Computers & Security. – 2017. 1-s2.0-S0167404817300810-am.pdf

5. Facebook: A Top Launching Pad For Phishing Attacks [Електронний ресурс] // Threatpost | The first stop for security news. – Режим доступу: https://threatpost.com/facebook-launching-pad-phishing-attacks/160351/

6. Phishing for Information: Spearphishing Service, Sub-technique T1598.001 - Enterprise | MITRE ATT&CK® [Електронний ресурс] // MITRE ATT&CK®. – Режим доступу: https://attack.mitre.org/techniques/T1598/001/

7. Iranian Hackers Targeted US Officials in Elaborate Social Media Attack Operation | SecurityWeek.Com [Електронний ресурс] // Cybersecurity News, Insights and Analysis | SecurityWeek. – Режим доступу: https://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

8. Black-Hat USA 2010 [Електронний ресурс]. – Режим доступу: http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf

9. McWhorter D. APT1: Exposing One of China's Cyber Espionage Units | Mandiant [Електронний ресурс] / Dan McWhorter // Cyber Threat Defense Solutions |

Threat Intelligence Services. – Режим доступу: https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

10. Establish Accounts, Technique T1585 - Enterprise | MITRE ATT&CK® [Електронний ресурс] // MITRE ATT&CK®. – Режим доступу: https://attack.mitre.org/techniques/T1585/

11. Anonymous speaks: the inside story of the HBGary hack [Електронний ресурс] // Ars Technica. – Режим доступу: https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/

12. Compromise Accounts, Technique T1586 - Enterprise | MITRE ATT&CK® [Електронний ресурс] // MITRE ATT&CK®. – Режим доступу: https://attack.mitre.org/techniques/T1586/

13. Markoff J. Larger Prey Are Targets of Phishing [Електронний ресурс] / John Markoff // The New York Times. – 2008. – Режим доступу: https://www.nytimes.com/2008/04/16/technology/16whale.html

14. Hong J. Why have there been so mane security breaches recently? [Електронний ресурс]/ Hong J// CACM. – 2011. – Режим доступу: https://www.researchgate.net/deref/http%3A%2F%2Fcacm.acm.org%2Fblogs%2Fblog-cacm%2F107800-why-have-there-been-so-many-security-breachesrecently%2Ffulltext.

15. Dodge R. Using Phishing for User Email Security Awareness / R. Dodge, A. Ferguson // Pro-ceedings of the 21st IFIP International Information Security Conference. – 2006.

16. Dodge R. Rovira E, Radwick Z, and Shevchik J., Phishing Awareness Exercises / Dodge R. Rovira E, Radwick Z, and Shevchik J.// Pro-ceedings of the 15th Colloquium for Information Systems Security Education. – 2011.

17. The Influ-ences of Social Networks on Phishing Vulnerability / K. Coronges [та ін.] // 2012 45th Hawaii International Con-ference on System Sciences. – 2012.

18. Dodge R. C. Empirical Benefits of Training to Phishing Susceptibility / Ronald C. Dodge, Kathryn Coronges, Ericka Rovira // 27th IFIP TC 11 Information Security and Privacy. – 2012.

19. ДСТУ ISO/IEC 27032:2016. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT). – На заміну ДСТУ ISO/IEC 27032:2015 ; чинний від 2018-01-01. – Вид. офіц. – [Б. м. : б. в.], 2016.

20. Security Awareness Training | KnowBe4 [Електронний ресурс] // Security Awareness Training | KnowBe4. – Режим доступу: https://www.knowbe4.com/

21. Social Engineering in Kali Linux - javatpoint [Electronic resource] // www.javatpoint.com. – Mode of access: https://www.javatpoint.com/social-engineering-in-kali-linux

22. Oracle VM VirtualBox [Електронний ресурс] // Oracle VM VirtualBox. – Режим доступу: https://www.virtualbox.org/

23. Contributors to Wikimedia projects. Kali Linux – Википедия [Електронний ресурс] / Contributors to Wikimedia projects // Википедия – свободная энциклопедия. – Режим доступу: https://ru.wikipedia.org/wiki/Kali_Linux

24. Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution [Електронний ресурс] // Kali Linux. – Режим доступу: https://www.kali.org/

25. Computer operating systems market share 2012-2021 | Statista [Електронний ресурс] // Statista. – Режим доступу: https://www.statista.com/statistics/268237/global-market-share-held-by-operating-systems-since-2009/

26. Mobile Operating System Market Share Worldwide 2012-2021 | Statcounter [Електронний ресурс] // Statcounter. – Режим доступу: https://gs.statcounter.com/os-market-share/mobile/worldwide

27. Gophish - Open Source Phishing Framework [Електронний ресурс] // Gophish - Open Source Phishing Framework. – Режим доступу: https://getgophish.com/

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Тези наукових доповідей:

1. Бучик С.С., Мовчан Д. А. Віртуальна лабораторія для тестування співробітників організації щодо фішингових атак. IV Міжнародної науково-практичної конференції PCSITS – 2022 – подано тези.