ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕЛЕКТРОННА ІНЖЕНЕРІЯ
INFORMATION AND COMMUNICATION TECHNOLOGIES, ELECTRONIC ENGINEERING

№ 2 (1), 2022

https://doi.org/10.23939/ictee2022.01.044

ІНСТРУМЕНТИ ВІРТУАЛЬНОЇ ЛАБОРАТОРІЇ ТЕСТУВАННЯ СПІВРОБІТНИКІВ ДЛЯ ВИЗНАЧЕННЯ ГОТОВНОСТІ ПРОТИДІЇ ФІШИНГОВИМ АТАКАМ

С. Бучик, С. Толюпа, О. Бучик, Д. Мовчан

Київський національний університет імені Тараса Шевченка, вул. Володимирська, 60, Київ, 01033, Україна

Відповідальний за рукопис: Олександр Бучик (e-mail: alex8sbu@knu.ua).

(Подано 30 липня 2022)

Стаття стосується важливого та визначального напряму в кібербезпеці – навчання співробітників з метою виявлення та протидії фішинговим атакам. Від фішингових атак страждають як звичайні люди, так і підприємства, тому ефективне навчання працівників є одним із ключових способів пом'якшити наслідки фішингових атак. Сучасний ринок платформ та інструментів для перевірки співробітників щодо готовності виявляти та знешкоджувати фішингові атаки недостатній з погляду функціональності, швидкості та ефективності. Запропоновано вирішення цієї проблеми у вигляді запровадження віртуальної лабораторії для тестування співробітників, що дасть змогу швидко та якісно виявити недоліки у підготовці та провести навчання в цьому напрямі.

Ключові слова: *віртуальна лабораторія; фішинг; тестування співробітників; Kali Linux; фішингові атаки.*
УДК: 004.77

1. Вступ

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 вебсайти. Високий потенціал грошових винагород (наприклад, через доступ до банківських рахунків і номерів кредитних карток), легкість надсилання підроблених повідомлень електронної пошти, що видають себе за законні, і труднощі правоохоронних органів у переслідуванні винних злочинців призвели до сплеску фішингу.

Типова фішингова атака починається із 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 вебсайта (підроблений, створений так, щоб нагадувати офіційний вебсайт установи). Під час цієї пасивної атаки вебсторінка пропонує жертві ввести інформацію облікового запису (наприклад, ім'я користувача та пароль), а також може запитати інші особисті дані, такі як номер соціального страхування, номери банківських рахунків, PIN коди банкоматів тощо. Інформація передається зловмиснику, який потім може використовувати її для доступу до облікових записів користувача [1].

Фішинг за наслідками є дороговартісним та витратним кіберзлочином для компаній і окремих осіб. Згідно із інформацією американського інституту Понемон, середні збитки компаній від фішингових атак в 2021 р. становили 14,8 млн дол., що більш ніж втричі перевищує збитки у 2015 р. Це означає сотні мільярдів доларів загальних збитків від фішингових атак для глобальних компаній [2].

Від фішингових атак потерпають як пересічні громадяни, так і підприємства, тому ефективне навчання працівників є одним із ключових методів пом'якшення впливу фішингових атак. Набори інструментів створення фішингових атак для проведення тестування не є досконалими і завжди актуальний пошук оптимальних рішень в цій сфері.

Згідно з ДСТУ ISO/IEC 27032:2016 "Інформаційні технології. Методи захисту. Настанова щодо кібербезпеки" (ISO/IEC 27032:2012, IDT), обізнаність та навчання у галузі безпеки, охоплюючи регулярне оновлення відповідних знань, є важливим елементом протидії атакам соціальної інженерії. Як частина програми кібербезпеки організації, працівники та сторонні підрядники повинні бути зобов'язані пройти мінімальну кількість годин навчань для того, щоб забезпечити власну поінформованість про свої ролі та обов'язки в кіберпросторі й технічні засоби управління, які вони повинні впровадити як приватні особи, використовуючи кіберпростір [3].

2. Аналіз та постановка завдання

Багато досліджень і дослідницьких проєктів намагалися вивчити варіанти виявлення фішингових листів та пом'якшення дії їх негативних наслідків. Деякі підходи використовують розширену семантичну обробку та сканування ключових слів для блокування небажаних листів, інші методи – візуальні підказки в поштовому клієнті, щоб попередити користувачів про підозрілі листи.

Відповідно до більшості досліджень, незалежно від застосованих технологій, якщо електронна пошта доволі якісно імітує оригінал, користувач стане жертвою [4, 5]. Автори здійснили 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 [6], згідно із ранніми даними автори побудували інфраструктуру для виконання фішингу і досягли результатів, які вказують на середню 40 % схильність до фішингу. Ці результати були підтверджені в подальшому дослідженні [7], а далі показали, що вправи, повторювані у короткотривалий період, підвищували обізнаність і сприйнятливість знижувалася до 5 %. Останні дослідження аналізували вплив соціальних мереж на сприйнятливість [8]. У цих результатах було виявлено групування жертв за організаціями; якщо керівництво організації вразливе – імовірно, таким буде і її персонал.

Багатьом великим організаціям потрібна підготовка, щоб переконатися, що співробітники знають про ризики, що виникають для організації через користувачів, які стають жертвами фішингових електронних листів. Цю підготовку, як правило, організація оплачує фінансово та забезпечує навчання персоналу. За останні кілька років фішингові тренування стали ефективним механізмом, який забезпечує можливості навчання, і, як наслідок, потрібні менші інвестиції в безпеку з боку організації [3].

Метою дослідження в статті є розроблення віртуальної лабораторії, яка дасть змогу тестувати працівників організації на предмет обізнаності та готовності до протидії фішинговим атакам.

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

Предмет дослідження – інструменти створення фішингових атак. Використання сукупності інструментів створення фішингових атак для тестування працівників організації за рахунок включення їх до віртуальної лабораторії повинно допомогти швидко та ефективно здійснювати оцінку готовності співробітників до подібних атак з урахуванням вимог ДСТУ ISO/IEC 27032:2016.

3. Виклад основного матеріалу

Розглянемо певні платформи для тестування співробітників та спробуємо визначити їх переваги та недоліки, а також інструменти, які доцільно використати у віртуальній лабораторії для подальшого використання під час тестування співробітників.

Окремо нагадаємо, що тестування співробітників має відбуватись відповідно до вимог, які викладені в стандарті ДСТУ ISO/IEC 27032:2016 “Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки” (ISO/IEC 27032:2012, IDT) [3], в якому визначено, що:

1) усі тестові сервери та їхній вміст перебувають під контролем та управлінням команди тестування;

2) за можливості залучають професіоналів, які мають попередній досвід проведення таких тестів;

3) користувачів підготовано до тестів за допомогою програм підвищення обізнаності та навчання;

4) усі результати тесту подано в агрегованому вигляді з метою захисту конфіденційності приватних осіб, оскільки вміст таких тестів може занепокоювати приватних осіб та спричиняти проблеми конфіденційності, якщо їх виконують неналежно.

Хоч 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 необхідно поінформовути щодо пов’язаних ризиків у кіберпросторі, а організації повинні встановити відповідні політики та здійснити застережні кроки для фінансової підтримки таких програм, які спрямовані на забезпечення обізнаності та компетентності людей. Загальна рекомендація: усі організації (зокрема підприємства, постачальники послуг та державні органи) повинні заохочувати споживачів вивчати та розуміти ризики соціальної інженерії в кіберпросторі й кроки, які вони повинні зробити для захисту від потенційних атак [3].

Щоб краще розуміти природу соціальної інженерії, розглянемо її складові у вигляді фаз, які потрібно реалізувати перед тим, як досягти кінцевого результату. Це дає змогу зрозуміти, які вимоги необхідно ставити до інструментів здійснення фішингових атак. Від їх якості залежатиме ефективність тестування співробітників.

Фази соціальної інженерії можна подати так, як на рис. 1 [9].

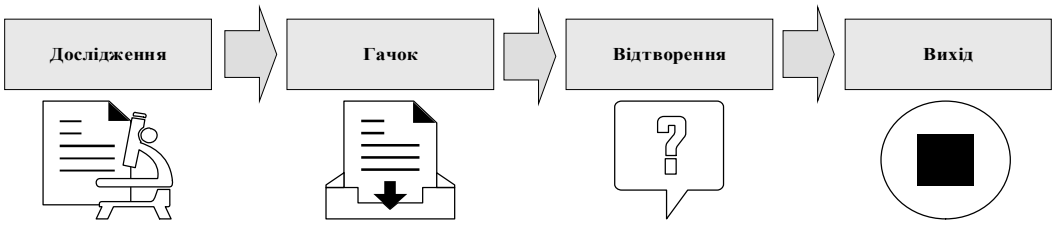

Рис. 1. Фази соціальної інженерії

Фаза дослідження. На етапі дослідження збирають інформацію про ціль. Ця початкова фаза не залежить від того, чи є метою атаки велика компанія, чи окрема організація. Існують різні способи, які зловмисники використовують для отримання інформації про свої цілі. Серед них – отримання документів загального доступу, відвідування вебсайта відповідної установи, а в деяких випадках конструктивна взаємодія у тісному контакті. Крім того, на цій стадії атаки важливо занурюватися в смітник.

Фаза гачка. Це другий етап атаки, на якому нападник встановлює контакт із майбутньою жертвою своєї фішингової атаки.

Фаза відтворення. Після фази гачка починається фаза відтворення, яка зміцнює відносини між нападником і ціллю. Зловмисник користується цією можливістю, щоб дізнатися, як отримати потрібну інформацію.

Фаза виходу. Це остання фаза, зловмисник обережний та чутливий, щоб не створювати ситуацію, яка у будь-який спосіб зробить ціль підозрілою. Ідея полягає у тому, щоб вийти на результат, не маючи жодного натяку на певні підозри щодо цілі.

Всі ці фази повинен виконати той, хто проводить тестування, причому, незважаючи на попередження співробітників щодо фішингових атак, він має діяти як звичайний зловмисник, щоб жертва (співробітник) майже нічого не підозрювала.

Одна із найпопулярніших платформ для тестування співробітників сьогодні – KnowBe4 (https://www.knowbe4.com). Платформа уможливлює [10]: тестування одночасно до ста користувачів; локалізацію шаблонів понад 20 мовами та налаштування їх відповідно до середовища; вибір цільової сторінки; звіт у форматі PDF із відсотком схильності до фішингу.

Також інтерес становлять певні інструменти соціальної інженерії, доступні в Kali Linux. Набір інструментів соціальної інженерії, який зазвичай називають SET, є інструментом тестування на проникнення із відкритим кодом для соціальної інженерії та інших атак. SET має кілька користувацьких векторів атаки, які дають змогу атакувати ціль у найкоротші терміни.

Ці інструменти використовують поведінку людей, щоб ввести їх в оману щодо вектора атаки. У SET є два основні типи атак: тестування на проникнення та соціальна інженерія.

Команду setoolkit використовують для запуску SET (рис. 2).

```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                        Version: 8.0.3
                     Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your
tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

Рис. 2. Результат виконання команди setoolkit у терміналі Kali Linux

Набір має три основні варіанти запуску атаки:

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

Якщо ввести 1, то потрапляємо в нове меню з різними типами атак соціальної інженерії (рис. 3, *а*). Надалі, вибравши, наприклад, знову 1, потрапляємо в розділ Spear-Phishing Attack Vectors, де наявні інструменти для масового розсилання електронних листів, що містять файли зі шкідливим вмістом (рис. 3, *б*).

Якщо далі ввести 3 (Create a Social-Engineering Template), то потрапляємо в генератор шаблона листів (Template Generator), який має вигляд звичайного текстового редактора без застосування HTML (рис. 4).

З наведеного прикладу зрозуміло, що 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 досягають успіху, тобто тестування не є ефективним.

```
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set>
```

Рис. 3а. Типи атак соціальної інженерії

```
set> 1

The Spearphishing module allows you to specially craft email messages and send
them to a large (or small) number of people with attached fileformat malicious
payloads. If you want to spoof your email address, be sure "Sendmail" is in-
stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do
everything for you (option 1), the second is to create your own FileFormat
payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>
```

Рис. 3б. розділ Spear-Phishing Attack Vectors

```
set:phishing>3
         [****]  Custom Template Generator [****]

Always looking for new templates! In the set/src/templates directory send an email
to info@trustedsec.com if you got a good template!
set> Enter the name of the author: Serhii
set> Enter the subject of the email: Надати іфдповідь по справі
set> Enter the body of the message, hit return for a new line. Control+c when finished: :
```

Рис. 4. Вигляд генератора шаблона листів

Зважаючи на вказані недоліки, пропонуємо інший підхід до організації тестування співробітників на предмет фішингових атак. Для цього створено власну лабораторію на основі наявних інструментів та операційних систем (ОС). Для прикладу, як жертву вибирали ОС Windows та Android. Звичайно, для цього випадку можна розглядати й інші ОС.

Під час побудови віртуальної лабораторії було вирішено використовувати VirtualBox – програму віртуалізації для ОС. Для імітації машини зловмисника, який атакує, вибрали операційну систему Kali Linux, на роль жертви – машини з операційними системами Windows та Android

Логічну структуру віртуальної лабораторії подано на рис. 5.

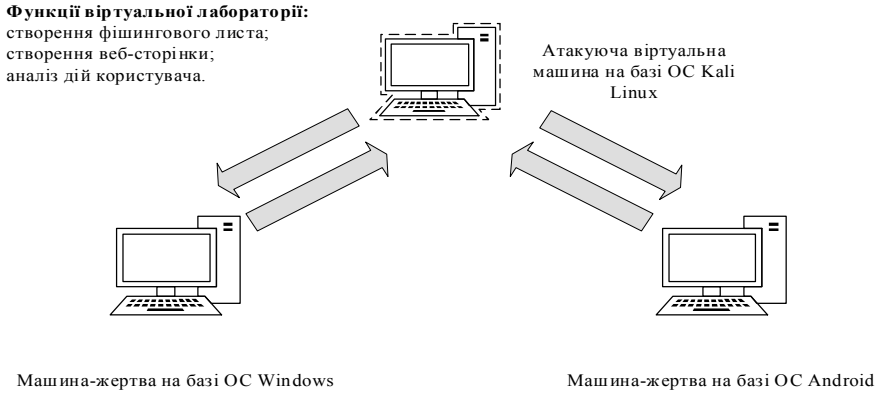

Рис. 5. Логічна структура віртуальної лабораторії

Створення імітації фішингового листа – один із ключових етапів фішингової кампанії. За основу шаблонів можна взяти приклади, які пропонує платформа KnowBe4. KnowBe4 дає змогу подивитись, які саме елементи в листі повинні викликати підозри у користувача. Це корисна функція, яку необхідно впровадити у віртуальну лабораторію на етапі створення імітації фішингового листа.

Наступним етапом імітації фішингової кампанії є розсилання листів електронною поштою. Задля реалізації цього кроку запропоновано використовувати фреймворк Gophish, який надає всі необхідні функції. Переваги фреймворка Gophish [11]:

- Gophish дає змогу легко створювати або імпортувати pixel perfect шаблони листів фішингу. Вебінтерфейс містить повноцінний редактор HTML, що полегшує налаштування шаблонів прямо у браузері;
- функція надсилання листів у фоновому режимі, а також можливість відкладеного надсилання;
- відстеження результатів. Детальні результати надаються практично в режимі реального часу, їх можна експортувати для використання у звітах.

Під час побудови віртуальної лабораторії запропоновано використовувати VirtualBox – програму віртуалізації для ОС. 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, що є хостовою, усередину цієї програми встановлюється інша ОС, яка є гостьовою [12].

Тестування співробітників на предмет фішингу відбувається відповідно до схеми типової фішингової атаки (рис. 6).

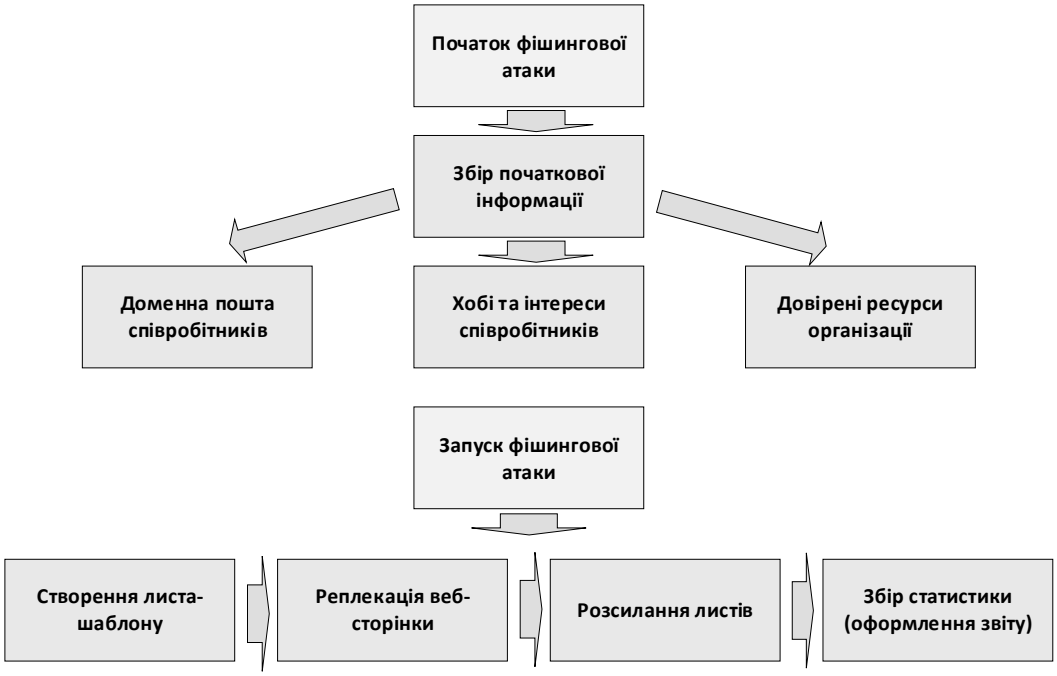

Рис. 6. Схема типової фішингової атаки

Задля імітації фішингової атаки запроновано використовувати такий набір інструментів:

1. Ngrok (https://dl.equinox.io/ngrok/ngrok/stable) – ця програма робить доступними в Глобальній мережі локальні сервіси, навіть якщо комп'ютер не має білої IP-адреси і його знаходять за NAT і фаєрволами.

2. Seeker (https://github.com/thewhiteh4t/seeker) – знаходить точне розташування пристрою (смартфона, планшета, ноутбука, стаціонарного комп'ютера) за допомогою соціальної інженерії. Концепція Seeker проста – вона полягає у розміщенні підробленої сторінки, яка запитує місцезнаходження. Вебсайт запитує дозвіл на місцезнаходження і, якщо ціль дозволяє, зловмисник може дізнатись довготу, широту тощо. Поряд із інформацією про місцезнаходження, інструмент отримує інформацію про пристрій без будь-яких дозволів.

3. Bigbro (https://github.com/Bafomet666/Bigbro) – має аналогічну до seeker концепцію.

Порівняння Seeker та Bigbro.

Переваги Seeker:

- інформація про жертву є розширенішою. В Seeker можна отримати не лише геодані, як в Bigbro, але й технічні характеристики девайса, IP-адресу тощо;
- всі скрипти в ngrok працюють коректно. Під час дослідження Bigbro на деяких пристроях Android не вдалось отримати інформацію про місцезнаходження умовної жертви через 404 або 408 помилки у js-скриптах. У Seeker всі чотири сайти виконувалися справно, без помилок у скриптах;
- логічне завершення сценарію сайта після отримання даних. У Seeker, одержавши доступ 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. У разі відкриття посилань з версії Android сайт коректно відображався, а 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 вебсторінки, що є незаперечною перевагою під час реалізації фішингової атаки із метою тестування.

Переваги Bigbro:

- більший вибір сайтів. Seeker пропонує лише чотири шаблони для вебсторінок, тоді як Bigbro – на вибір 40 сторінок у премія-версії, що додає гнучкості в імітації фішингової кампанії. Проте близько половини сторінок, запропонованих в Bigbro, не є актуальними для України та можуть викликати підозру в користувача. Наприклад, сторінки із сайтами знайомств вважаються апріорі підозрілими, тому користувач, швидше 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 сайта, 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 небезпечний. Поряд з цим у Bigbro браузер не “бачить” сторінку як потенційно небезпечну.

Переваги обох утиліт:

- простота у використанні. За допомогою Seeker і Bigbro доволі легко створити фішинг-сайт буквально за декілька дій. Не потрібні редактори або інші інструменти редагування сайтів, що істотно пришвидшує тестування працівників на готовність протидіяти фішинговим атакам;
- правдоподібність. Вебсторінки, які пропонують досліджувані утиліти, доволі точно копіюють оригінальні ресурси.

Недоліки обох утиліт:

- повідомлення про можливу небезпеку. На деяких етапах експерименту браузер сповіщав користувача про потенційну небезпеку вебсайта, а це може викликати підозру щодо фальшивості ресурсу;
- нелогічність у сценарії сайтів. Деякі вебсторінки запитують доступ до місцезнаходження, тоді як контент сторінки не повинен цього передбачати. Наприклад, запит на надання місцезнаходження на сторінці із запрошенням до конференції Zoom виглядає доволі дивно і це може спонукати умовну жертву покинути такий вебсайт.

Висновки

За результатами досліджень і тестувань (детальніше висвітлених у [13]) виявлено, що цей інструментарій достатній для імітації фішингової атаки із метою навчання співробітників та підвищення їх обізнаності.

Тестування потрібно здійснювати тільки за узгодженості та поінформованості обох сторін-учасниць процесу тестування.

Seeker та Bigbro – легкі та зручні у використанні утиліти, які надають можливість створити якісні фішингові вебсторінки та отримати доволі багато інформації як про пристрій умовної

жертви, так і про її місцезнаходження. Проте Seeker показав кращі результати щодо сценаріїв сайтів та меншу похибку під час надання інформації про місцезнаходження.

Отже, для створення віртуальної лабораторії з метою тестування співробітників необхідно мати можливість (якщо у вас відсутня біла IP-адреса (чи хостинг)) створювати посилання на ваш сайт, завдяки чому сайт на вашому локальному комп'ютері можна відкрити в інтернеті (за допомогою утиліти Ngrok) та скористатись, залежно від вимог, необхідною утилітою (у цьому випадку автори пропонують прості та зручні інструменти Seeker та Bigbro).

Список використаних джерел

[1] *Adam Kavon Ghazi-Tehrani & Henry N. Pontell (2021). Phishing Evolves: Analyzing the Enduring Cybercrime, Victims & Offenders, pp. 316–342. DOI: 10.1080/15564886.2020.1829224.*

[2] *Ankit Kumar Jane, B. B. Gupta (2021). A survey of phishing attack techniques, defence mechanisms and open research challenges. Enterprise Information Systems, pp. 527–565. DOI: 10.1080/17517575.2021.1896786.*

[3] *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.*

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

[5] *Hong J. Why have there been so mane security breaches recently? [Електронний ресурс]// 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.*

[6] *Dodge R. (2006). Using Phishing for User Email Security Awareness. Proceedings of the 21st IFIP International Information Security Conference.*

[7] *Dodge R. Rovira E, Radwick Z, and Shevchik J. (2011). Phishing Awareness Exercises. Proceedings of the 15th Colloquium for Information Systems Security Education.*

[8] *K. Coronges, R. Dodge, C. Mukina, Z. Radwick (2012). The Influences of Social Networks on Phishing Vulnerability. System Science (HICSS), 2012 45th Hawaii International Conference on At: Maui, Hawaii. pp. 2366–2373. DOI:10.1109/HICSS.2012.657.*

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

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

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

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

[13] *Мовчан Д. А. (2022), Віртуальна лабораторія для тестування співробітників організації щодо фішингових атак: пояснюв. зап. диплом. роботи магістра: 125 Кібербезпека / Мовчан Дар'я Андріївна. Київ, 64 с.*

VIRTUAL LAB TOOLS FOR TESTING EMPLOYEES TO DETERMINE READINESS AGAINST PHISHING ATTACKS

S. Buchyk, S. Tolyupa, O. Buchyk, D. Movchan

Taras Shevchenko National University of Kyiv, 60, Volodymyrska str., Kyiv, 01033, Ukraine

The article is devoted to an important and most important direction in cyber security – training employees about possible phishing attacks. Phishing attacks affect both individuals and businesses, so effective employee training is one of the key ways to mitigate the effects of phishing attacks. The current market of platforms and tools for checking employees for phishing attacks is insufficient in terms of functionality, speed and efficiency. The solution to this problem is offered in the form of a virtual laboratory for testing employees for phishing attacks, which will allow for quick and high-quality training in this area.

Key words: *virtual lab; phishing; employee testing; Kali Linux; phishing attacks.*