МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ВИПУСКНА РОБОТА

на тему:

«Методика проведення аудиту компанії на схильність до атак методами соціальної інженерії»

Завідувач випускаючої кафедри — **Довбиш А.С.**

Керівник роботи — **Лаврик Т.В.**

Студента групи КБ – 71 — **Цубін О.Ю.**

СУМИ 2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерних наук

Затверджую_____

Зав. кафедрою Довбиш А.С.

"_____" _____2021 р.

ЗАВДАННЯ

до випускної роботи

Студента четвертого курсу, групи КБ-71 спеціальності "Кібербезпека" денної форми навчання Цубіна Олега Юрійовича.

Тема: "Методика проведення аудиту компанії на схильність до атак методами соціальної інженерії"

Затверджена наказом СумДУ

№_____ від _____2021 р.

Зміст пояснювальної записки: 1) аналітичний огляд методик аудиту безпеки; 2) постановка завдання й формування завдань дослідження; 3) характеристика векторів атак соціальної інженерії; 4) розробка методики; 5) аналіз отриманого результату.

Дата видачі завдання "_____"_____2021 р.

Керівник випускної роботи _____ Лаврик Т. В.

Завдання прийняв до виконання _____ Цубін О.Ю.

РЕФЕРАТ

Записка: 64 стор., 29 рис., 15 джерел.

Об’єкт дослідження — атаки засобами соціальної інженерії і методи їх виявлення.

Мета роботи — розроблення методики аудиту компанії на схильність до атак методами соціальної інженерії.

Методи дослідження — метод аналітичного огляду, метод порівняння, метод моделювання.

Результати — розроблено методику аудиту компанії на схильність до атак соціальної інженерії. Створений опис до кожного кроку тестування та керівництво до впровадження.

МЕТОДИКА АУДИТУ, СОЦІАЛЬНА ІНЖЕНЕРІЯ, ЗБІР ІНФОРМАЦІЇ, АНАЛІЗ ВРАЗЛИВОСТЕЙ, ПРОНИКНЕННЯ

ЗМІСТ

ВСТУП

Сучасні системи захисту можуть захистити дані практично від усього, крім людського фактору. Можна спорудити неприступну програмну стіну перед потенційним хакером, але всі праці виявляться марними, якщо наївний користувач сам повідомить зловмисникові паролі. «Зламати людину набагато простіше, ніж комп'ютер, оскільки комп'ютери дотримуються інструкцій, а люди – піддаються емоціям[1]», – стверджує Кевін Митник, один з найвідоміших хакерів світу. Соціальна інженерія – це набір технік, які широко використовуються в кібератаках для організації деяких із найбільш успішних атак.

Соціальна інженерія спрямована виключно на слабкий компонент в ланцюжку кібербезпеки – користувача. На відміну від систем і мереж, користувачі не можуть бути захищені від соціальної інженерії за допомогою дорогих інструментів, таких як брандмауери і антивірусні програми. Вони завжди відкриті і видають інформацію, яка може бути використана зловмисниками для нанесення по ним удару, коли цього найменше очікують. Протягом години експерт в області соціальної інженерії може зібрати стільки інформації, скільки йому вдалося б за 100 годин, безпосередньо атакуючи систему. Зловмисники знають про сучасну складність елементів безпеки, що захищають системи. Більшість організацій використовують кілька рівнів безпеки. Навіть якщо один з них зламаний, хакер не може легко обійти інші. Тому стає все складніше намагатися атакувати самі системи. У той же час, хакери виявляють, що зламати сьогоднішніх користувачів дуже просто, і це підтверджується зростаючим числом опосередкованих атак соціальної інженерії.

Зростає кількість хакерських атак, що використовують технології соціальної інженерії, щоб використати людський фактор комп’ютерних систем. Ці прийоми нападів використовуються як у приватному, так і в діловому контексті. В останніх вони утворюють головний інструмент промислового шпигунства. Незважаючи на те, що існують стандарти оцінки програмного та апаратного забезпечення, що мають важливе значення для безпеки, а також їх робочого середовища, не існує стандарту для оцінки вразливості організацій щодо соціальної інженерії. У цій роботі буде

представлено структуру для оцінки такого роду вразливості. Структура дозволяє організаціям розробити рівень опору, а також виявити конкретні вразливі місця. Вони можуть бути використані для здійснення конкретних заходів щодо поліпшення ситуації, тобто рівня опору.

1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Актуальність аудиту компанії

1.1.1. Статистика атак з використанням соціальної інженерії

У IV кварталі 2019 року соціальна інженерія в поєднанні зі зловмисним програмним забезпеченням (далі – ПЗ) використовувалася в 54% атак. Користувачам варто бути особливо уважними до електронної кореспонденції в період свят. До знаменних дат зловмисники приурочують фішингові розсилки. Наприклад, до Дня подяки в США кіберзлочинці розіслали листи нібито з вітальними листівками. Насправді ж вкладення до листів були шкідливими - доставляли на комп'ютери жертв Emotet і інше шкідливе ПЗ. Масові розсилки листів нібито із запрошеннями на вечірку, що доставляють у вкладеннях Emotet, були приурочені також до Хеллоуїну і Різдва [2].

Якщо ви не переходите за підозрілими посиланнями і не завантажуєте сумнівні вкладення, це ще не означає, що ви не можете потрапити на вудку інтернет-шахраїв. Так, в IV кварталі зловмисники використовували для фішингових атак особливості Microsoft OAuth API. Протокол OAuth дозволяє видавати сторонніх додатків токен на доступ без знання облікових даних. Суть атаки в наступному. Фішинговий лист містить посилання на файл нібито в OneDrive або SharePoint. Однак після переходу за посиланням і введення облікових даних користувач бачить форму із запитом на надання доступу до аккаунту Office 365. Якщо жертва неуважна, вона може надати запитувані права одним кліком. В результаті зловмисники отримують список контактів, файли і особисту переписку.

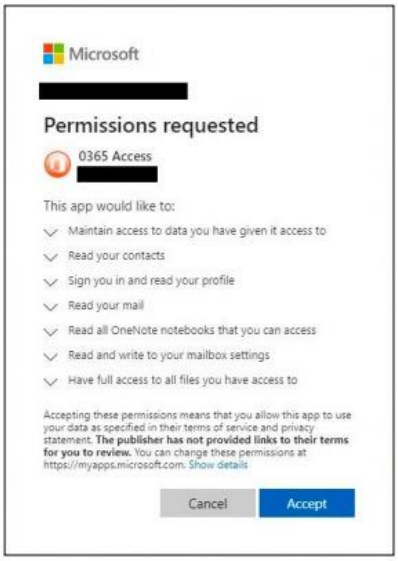

Рисунок 1.1 – Запит від фішингового додатку O365 Access

Листи, в яких зловмисники шантажують жертв розголошенням нібито наявного у них компромату, – далеко не новий спосіб незаконного заробітку, проте він як і раніше приносить кіберзлочинцям чималий дохід. Наприклад, за оцінкою фахівців Check Point за п'ять місяців оператори ботнету Phorpiex, що розсилає подібні листи, заробили близько 115 тисяч дол. США. Зловмисники включають в текст листа паролі жертв як доказ компрометації. Шахраї беруть їх із баз даних, що вже є скомпрометованими і розміщеними в Інтернет [2].

1.1.2. Втрати бізнесу від атак за допомогою соціальної інженерії

1) Фінансові втрати в результаті атак соціальної інженерії.

Це, мабуть, єдиний наслідок хакерських атак, про який всі знають – кількість грошей, яку компанія втрачає безпосередньо в результаті атаки соціальної інженерії. Залежно від розміру вашої компанії та жадібності зловмисника ця цифра може коливатися від 20 000 до мільйонів доларів.

2) Втрата продуктивності в результаті кібератаки соціальної інженерії.

Будь-яка успішна кібератака спричиняє величезні порушення нормальної ділової діяльності. IT-команді та декільком працівникам на рівні керівництва потрібно відкласти свої інші завдання, щоб впоратися з порушенням, всім працівникам потрібно повідомити про хакерство та навчити їх запобігати одній і тій

же атаці в майбутньому тощо. Все це забирає час від обов'язків працівника і значно знижує продуктивність праці.

3) Вартість відновлення після нападу соціальної інженерії.

Ще однією загальною вартістю, пов’язаною з атаками на підводний фішинг, є вартість відновлення, яка представляє суму грошей, необхідну для найму команди реагування на інциденти, придбання програмного забезпечення, яке може запобігти виникненню такої самої атаки в майбутньому та вирішенню проблеми із клієнтами, якщо їх дані були вкрадені під час нападу.

4) Кібератаки спричиняють зрив бізнесу.

Цей наслідок соціальної інженерії схожий на втрату продуктивності, але він вимірює вплив хакерства на рівень задоволеності споживачів та ваш ланцюг поставок. Оскільки успішна хакерська атака порушує ваші звичайні ділові операції, ваш бізнес може зазнати простою у виробництві продуктів, доставці та інших операціях. Це може призвести до втрати клієнтів або навіть постачальників. Крім того, ваша страхова компанія та ваш банк можуть захотіти перевірити практику кібербезпеки вашої компанії після порушення.

5) Хакери соціальної інженерії завдають величезної шкоди вашій репутації.

Якби ви були замовником або постачальником компанії, яка зазнала значного порушення кібербезпеки, наскільки ймовірно, ви могли б знову довіряти цій компанії? Ви б продовжували вести бізнес з цією компанією? На жаль, для багатьох підприємств переважатиме відповідь "ні": люди не хочуть піддавати себе та свою інформацію небезпеці. Тому багато підприємств втрачають значну кількість клієнтів та постачальників після порушення безпеки.

1.2. Огляд існуючих рішень

У цьому розділі розглянемо існуючі методики у сфері тестування на проникнення. Було обрано 4 найпопулярніші методики на даний момент: OWASP, OSSTMM, ISSAF та PTES.

1.2.1. Методика OWASP

Методика Open Web Application Security Project (OWASP) створена співтовариством OWASP в 2004 р і розвивається по теперішній час міжнародною групою незалежних експертів-ентузіастів. Методика орієнтована на тестування веб-додатків. Організація OWASP зареєстрована в США і Бельгії (OWASP Europe VZW). Методика докладно описує тестування веб-додатків і фактично є єдиною подібною методикою, вузько орієнтованої саме на веб-додатки.

Цей фреймворк забезпечує методологію тестування на проникнення додатків, яка може не тільки виявити вразливості, які часто зустрічаються в Інтернеті та мобільних додатках, але також ускладнити логічні недоліки, що виникають внаслідок небезпечної практики розробки. Оновлений посібник містить вичерпні вказівки щодо кожного методу тестування на проникнення, із загальною кількістю 66 контрольних елементів, що дозволяє тестувальникам виявляти вразливі місця в широкому діапазоні функціональних можливостей, які сьогодні є в сучасних додатках.

За допомогою цієї методології організації мають більше можливостей захищати свої програми – як веб, так і мобільні від типових помилок, які можуть мати потенційно критичний вплив на їх бізнес. Організаціям, які прагнуть розробляти нові веб-програми та програми для мобільних пристроїв, слід також розглянути можливість включення цих стандартів на етапі їх розробки, щоб уникнути загальних недоліків безпеки.

Під час оцінки безпеки програми слід очікувати, що буде застосовано стандарт OWASP, щоб переконатись, що жодні вразливості не залишились позаду і що ваша організація отримує реалістичні рекомендації, адаптовані до конкретних функцій та технологій, що використовуються у ваших додатках.

Методика OWASP містить наступні розділи:

1. Вступ.
2. Керівництво по тестуванню OWASP.
3. Тестування на проникнення веб-додатків.
4. Керівництво зі складання звітів.

У розділі 3 «Тестування на проникнення веб-додатків» описано набір тестів, орієнтованих на перевірку наступних аспектів інформаційної безпеки (ІБ):

- збір інформації;
- тестування управління конфігурацією і розгортанням;
- тестування управління ідентифікацією;
- тестування аутентифікації;
- тестування авторизації;
- тестування управління сесіями;
- тестування перевірки введення;
- тестування обробки помилок;
- тестування на криптографічний стійкість;
- тестування бізнес-процесів;
- тестування клієнтської сторони.

Методику OWASP можна використовувати як на етапі попередньої оцінки захищеності веб-додатків в інтересах перевірки можливості їх використання в складі будь-якої інформаційної системи, так і на етапі розробки веб-додатків для перевірки окремих можливостей і функцій ІБ.

1.2.2. Методика OSSTMM

Методика The Open Source Security Testing Methodology Manual (OSSTMM) розроблена інститутом ISECOM (Institute for Security and open Methodologies), який є відкритим співтовариством вчених і практиків в області ІБ.

Методика OSSTMM є високо формалізованою і добре структурованим документом який регламентує практично всі аспекти тестування на проникнення, орієнтована на тестування переважно комп'ютерних мереж. Методика періодично оновлюється. З недоліків варто відзначити малу кількість інформації з практичних дій та інструментарію тестування.

Методика визначає, так звану «карту безпеки» - візуальне відображення основних категорій ІБ, які оцінюються в процесі тестування:

- інформаційна безпека;
- безпеку соціальних процесів;

- безпеку інформаційних процесів;
- безпеку Інтернет-технологій;
- безпеку каналів зв'язку;
- безпеку бездротових технологій;
- безпеку фізичної інфраструктури.

Як такої, класифікації вразливостей в цій методиці немає. Поняття «вразливість» в методиці вводиться як обмеження безпеки - це дефект або помилка, яка забороняє доступ авторизованим користувачам або процесам до інформаційних ресурсів або дозволяє несанкціонований доступ неавторизованих користувачів або процесів до ресурсів.

Цю методику можна використовувати як на етапі попередньої оцінки захищеності об'єктів в інтересах перевірки можливості їх використання в складі будь-якої інформаційної системи, так і на етапі розробки об'єктів для перевірки окремих можливостей і функцій ІБ [4].

1.2.3. Методика ISSAF

Методика Information System Security Assessment Framework (ISSAF) розроблена консорціумом OISSG (Open Information Systems Security Group) в якості стандарту внутрішнього аудиту організацій цього консорціуму. При цьому аудиті виконується оцінка наступних аспектів ІБ:

- оцінка політик і процедур ІБ організації, а також ступінь їх відповідності IT-стандартам та вимогам нормативних документів в
- області ІБ;
- виявлення і оцінка «залежності» бізнес процесів організацій від IT-інфраструктури;
- проведення оцінки вразливостей і тестів на проникнення для виділення вразливостей в системі, які можуть привести до потенційних ризиків інформаційних ресурсів;
- вказівка моделей оцінки по доменах безпеки;
- знаходження і усунення неправильних конфігурацій аппаратно-программних засобів;

- ідентифікація та зниження ризиків, пов'язаних з IT;
- ідентифікація та зниження ризиків, пов'язаних з персоналом або бізнес-процесами;
- посилення безпеки існуючих процесів і технологій;
- впровадження кращого досвіду забезпечення ІБ в практику і процедури бізнес-процесів.

Методика ISSAF включає в себе велику кількість питань, пов'язаних з тестуванням ІБ, а матеріал методики організований у вигляді двох частин:

- рекомендації для менеджменту;
- рекомендації з тестування.

У методиці ISSAF представлені 3 етапи, які необхідно реалізувати для коректного проведення тестів на проникнення.

1. Планування і підготовка. Отримання початкової вихідної інформації про об'єкт тестування, планування і підготовка до тестів. Перед тестуванням сторонам необхідно буде підписати формальної угоди, яке забезпечить основу для проведення тестування і взаємну правову захист. У ньому також буде вказаний порядок взаємодії, точні дати, тривалість тестування, способи проведення тестування тощо.

2. Оцінка. На цьому етапі проводиться виконання тестування.

Передбачені наступні підетапи проведення тестування:

- збір інформації;
- мережеве картографування;
- ідентифікація вразливостей.

Відзначимо, що в методиці ISSAF для вразливостей визначається два типи ризиків: технічний ризик і бізнес-ризик. У свою чергу кожен з них ділиться на 3 рівні: низький, середній, високий.

3. Безпосередньо тестування на проникнення.

4. Отримання доступу або розширення привілеїв.

5. Додаткові тести, наприклад, отримання зашифрованих паролів для їх подальшого злому в режимі off-line, перехоплення трафіку і його аналіз тощо.

6. Компрометація віддалених користувачів, інформаційних ресурсів, об'єктів мережі.

7. Підтримка несанкціонованого доступу до мережі.

8. Приховування слідів роботи.

ISSAF є найбільш докладною, з розглянутих, методикою тестування на проникнення як в теоретичному, так і в практичному плані. Цю методику можна використовувати як на етапі попередньої оцінки захищеності об'єктів мережі в інтересах перевірки можливості їх використання в складі будь-якої інформаційної системи, так і на етапі розробки об'єктів для перевірки окремих можливостей і функцій ІБ [5].

1.2.4. Методика PTES

Стандарт проведення тестування на проникнення PTES - Penetration Testing Execution Standard розроблена в 2009 р міжнародною групою незалежних експертів-ентузіастів в області ІБ. PTES як стандарт офіційно зареєстрована тільки в США. З моменту появи стандарт отримав розвиток у вигляді версії 1.1 в 2017 р Стандарт PTES передбачає 7 основних етапів проведення тестування на проникнення, описаних у відповідних розділах:

- етап початкового спілкування;
- збір інформації;
- моделювання загроз;
- аналіз вразливостей;
- експлуатація;
- постексплуатація;
- звітність.

До даного стандарту додається технічне керівництво (PTES

Technical Guidelines) докладно викладає основні технічні аспекти тестування:

1. інструментарій тестування;
2. збір інформації про об'єкт тестування;
3. аналіз вразливостей;
4. експлуатація вразливостей;
5. постексплуатація;
6. звітність.

Дані етапи охоплюють практично всі дії, пов'язані з тестом на проникнення - від початкового спілкування і обґрунтування завдання на тестування до етапу формування звіту, в якому весь процес фіксується найбільш ергономічним для замовника чином, а також формуються рекомендації щодо підвищення захищеності тестованої системи.

Цей стандарт можна використовувати як на етапі попередньої оцінки захищеності об'єктів в інтересах перевірки можливості їх використання в складі будь-якої інформаційної системи, так і на етапі розробки об'єктів для перевірки окремих їх можливостей і функцій ІБ [6].

З розглянутих методологій тільки ISSAF та PTES у повній мірі виконують тести, що направлені на перевірку людського фактору, але й вони не позбавлені недоліків. У цій роботі буде розроблятись методологія, що візьме корисні напрацювання з усіх методологій.

1.3. Постановка задачі

Проаналізувавши існуючі методології у сфері тестування на проникнення, розглянувши статистику уражень та втрат для підприємств у попередньому пункті завданням для дипломної роботи було обрано розробку методики для аудиту компанії на схильність до атак методами соціальної інженерії.

2. ХАРАКТЕРИСТИКА МЕТОДІВ ПРОВЕДЕННЯ АТАК З ВИКОРИСТАННЯМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

2.1. Методи та техніки проведення атак

2.1.1. Процес атаки

Опишемо основні кроки, необхідні для початку психологічної атаки на ваш цільовий об’єкт. Показаний у цьому розділі метод далеко не єдиний і не найуспішніший. Але, дізнавшись про нього, ви отримаєте уявлення про атаки за допомогою соціальної інженерії. Збір розвідданих, виявлення вразливих точок, планування і виконання атаки – це основні кроки, що вживаються соціальними інженерами для успішного отримання потрібної інформації або доступу в заборонену зону.

Збір розвідданих. Існує безліч методів, за допомогою яких визначається найбільш привабливий для випробувача на проникнення об'єкт. Це можна зробити, зібравши корпоративні адреси електронної пошти (використавши інструмент розширеного пошуку). Гарні результати можна отримати, зібравши персональну інформацію про людей, які працюють в самій цільової організації (в тому числі через соціальні мережі). Додаткову інформацію вам дасть виявлення сторонніх програмних пакетів, які використовуються в цільової організації. Не завадить і участь в корпоративних заходах і вечірках, а також в конференціях. Це дозволить виявити найбільш зручне і корисне джерело інформації.

Виявлення уразливих точок. Після того як ключове джерело інформації визначено, слід рухатися далі, а саме встановити довірчі відносини. Це потрібно, щоб в цільової організації не дізналися про ваших спробах отримання корпоративної інформації. Протягом всього процесу дуже важливо підтримувати високий рівень скритності. При пошуку інформації бажано отримати відомості про застосовуваний застарілому програмному забезпеченні, яке може бути використане для доставки шкідливого контенту по електронній пошті або через Інтернет, що, в свою чергу, дозволить заразити комп'ютер довіреної сторони.

Планування атаки. Як організувати атаку на позицію об'єкта – вибирати вам. Ви можете піти на особисте спілкування з цільовим об'єктом, а можете обрати пасивний

метод, із застосуванням електронних засобів. Ґрунтуючись на виявлених вразливих точках входу, можна легко визначити шлях і метод атаки. Скажімо, знайти дружнього представника служби підтримки клієнтів, наприклад Боба, який, не усвідомлюючи того, що може принести шкоду організації, без узгодження з вищим керівництвом буде запускати отримані електронною поштою шкідливі файли.

Виконання. Для заключного етапу вам знадобляться рішучість і терпіння, які дозволять вам контролювати хід атаки і оцінити отримані результати. На цьому етапі соціальним інженерам потрібні достатня кількість інформації і доступ до власності об'єкта, що, в свою чергу, дасть їм можливість в подальшому проникнути в корпоративні активи. При успішному виконанні цього завдання процес експлуатації та придбання буде завершено.

2.1.2. Методологія нападів

Соціальна інженерія фокусується на різних аспектах нападу, які використовують довіру та вроджену корисність людини для обману та маніпуляцій з метою компрометації мережі та її ресурсів. На наступній схемі зображено різні типи методів атаки, якими зловмисники можуть брати участь у збиранні інформації:

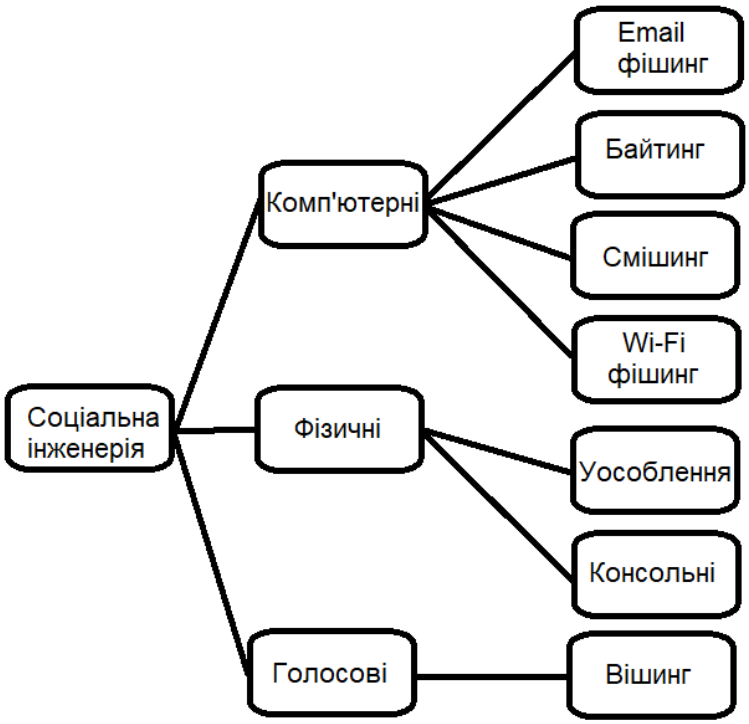

Рисунок 2.1 – Види атак соціальної інженерії

Соціальна інженерія включає три основні категорії: комп'ютерна, голосова та фізична атаки. Розглянемо кожен з цих типів: комп'ютерні атаки, фізичні атаки та фішинг електронної пошти, зокрема за допомогою Kali Linux.

1. Комп'ютерні атаки

Атаки, що використовують комп'ютери для соціальної інженерії, поділяються на такі типи. Всі ці різні типи найкраще використовувати лише тоді, коли вся пасивна та активна розвідувальна інформація використовується в повній мірі:

Фішинг електронної пошти: Зловмисники, які використовують електронну пошту для збору інформації або для використання відомої вразливості програмного забезпечення в системі жертв, називають фішингом електронної пошти.

Наживка: Ця техніка використовує приманку, щоб переконати вас зробити щось, що дозволить хакеру заразити ваш комп'ютер шкідливим ПЗ і, отже, отримати ваші особисті дані. Багато соціальні інженери використовують USB-пристрої в якості приманки, залишаючи їх в офісах або на парковках з такими ярликами, як «Зарплата керівників» в четвертому кварталі 2019 року. Люди, які знаходять їх, спокушаються цікавістю і вставляють їх у комп'ютер. Вірус, захований всередині, швидко поширюється на їх пристрій.

SMSishing: вид фішингу через SMS. Шахраї відправляють жертві SMS-повідомлення, що містить посилання на фішинговий веб-сайт і мотивуюче повідомлення увійти на цей сайт.

Фішинг Wi-Fi: Тестери проникнення можуть використовувати цю техніку для збору імен користувачів та паролів, створивши фальшиву мережу Wi-Fi, схожу на мережу цільової компанії. Наприклад, якщо зловмисники націлені на компанію, встановивши SSID у фальшивій мережі Wi-Fi точно такий же SSID цієї компанії, користувачі зможуть підключитися до підробленого бездротового маршрутизатора без пароля [7].

2. Голосові атаки

Будь-яка атака, що включає голосове повідомлення та обманює користувача виконати дію на комп'ютері або призводить до витоку конфіденційної інформації, називається голосовою соціальною інженерією.

ViShing – один з методів шахрайства з використанням соціальної інженерії, який полягає в тому, що зловмисники, використовуючи телефонну комунікацію і граючи певну роль (співробітника банку, покупця і т. д.), під різними приводами виманюють у власника платіжної картки конфіденційну інформацію або стимулюють до здійснення певних дій зі своїм картковим рахунком / платіжною карткою.

«Привіт, мені телефонує XX із компанії Y, яка, як було оголошено, приєднається до вас у новому спільному підприємстві. Оскільки ми зараз працюємо в одній команді, чи можете ви повідомити мене, де знаходяться ваші центри обробки даних, і надати мені список критично важливих серверів? Якщо ти не та людина, ти можеш вказати мені потрібну людину? На здоров'я! ZZ "[7].

3. Фізичні атаки

Фізичні атаки – це ті, які передбачають фізичну присутність зловмисника, який здійснює соціальну інженерну атаку на місці. Нижче наведено два типи фізичних атак, які можна виконати під час вправи червоної команди або під час тестування на проникнення

Уособлення: Соціальний інженер «видає себе за людину» або грає роль людини, якій ви, ймовірно, будете довіряти або якому ви будете досить переконливо підкорятися, щоб обманом змусити вас дозволити доступ до вашого офісу, інформації або вашим інформаційним системам.

Консольна атака: це атаки, що передбачають фізичний доступ до системи, наприклад, зміна пароля користувача адміністратора, встановлення кейлоггера, вилучення збережених паролів браузера або встановлення бекдору.

Фізичні консольні атаки

У цьому розділі ми розглянемо різні атаки, які зловмисники зазвичай виконують на систему, коли вони мають фізичний доступ до неї[8].

«Клейкі» ключі

У цьому розділі ми розглянемо, як використовувати фізичний доступ до консолі комп'ютера Windows, який розблокований або без пароля. Зловмисники можуть скористатися функцією Windows Sticky Keys, щоб за лічені секунди встановити бекдор; однак застереження полягає в тому, що вам потрібно мати права

адміністратора, щоб замінити виконуваний файл. Але коли система завантажується через Kali Linux, зловмисники можуть замінювати файли без будь-яких обмежень.

Далі наведено перелік утиліт Windows, які зловмисники можуть замінити cmd.exe або powershell.exe:

sethc.exe

utilman.exe

osk.exe

narrator.exe

magnify.exe

displaywitch.exe

Створення неправдивого фізичного пристрою

Kali також сприяє атакам, коли зловмисник має прямий фізичний доступ до систем та мережі. Це може бути ризикованою атакою, оскільки зловмисник може бути помічений. Однак винагорода може бути значною, оскільки зловмисник може скомпрометувати конкретні системи, що мають цінні дані.

Фізичний доступ зазвичай досягається як прямий результат соціальної інженерії, особливо коли використовується імітація. Поширені уособлення включають наступне:

Людина, яка заявляє, що вона з IT-служби, і їй просто потрібно швидко перервати жертву, встановивши оновлення системи.

Продавець, який заїжджає, щоб поговорити з клієнтом, а потім виправдовується, щоб поговорити з кимось іншим або відвідати туалет.

Доставщик. Зловмисники можуть придбати форму кур’єра через Інтернет; однак, оскільки більшість людей припускають, що той, хто одягнений у все жовте і має рюкзак, є працівником Glovo, уніформа рідко є необхідністю для соціальної інженерії.

Торговцю, одягненому в робочий одяг, з робочим замовленням, яке вони роздрукували, зазвичай дозволяється доступ до електропроводки та інших приміщень, особливо коли вони заявляють, що присутні на прохання керівника будівлі.

Одягайтесь у дорогий костюм, носіть з собою буфер обміну та швидко гуляйте – працівники вважатимуть вас невідомим менеджером. Проводячи такий тип проникнення, ми зазвичай повідомляємо людям, що ми є аудиторами; інспекторів рідко допитують.

Мета ворожого фізичного доступу - швидко компрометувати обрані системи; це зазвичай досягається шляхом встановлення на цілі прихованого або подібного пристрою [7].

Однією з класичних атак є розміщення CD-ROM, DVD або USB-ключа в системі та надання системі можливості встановити його за допомогою опції автовідтворення; однак багато організацій вимикають автовідтворення в мережі.

Зловмисники можуть також створювати приманки, наприклад, мобільні пристрої, що містять файли з іменами, що запрошують людину клацнути на файл та вивчити його вміст. Деякі приклади включають наступне:

USB-ключі з ярликами, такими як "Зарплата працівника" або "Оновлення медичного страхування".

Metasploit дозволяє зловмисникові прив’язати корисне навантаження до виконуваного файлу, такого як заставка. Зловмисник може створити заставку, використовуючи загальнодоступні корпоративні зображення, і видавати компакт-диски працівникам за допомогою нової "схваленої заставки". Коли користувач встановлює програму, також встановлюється бекдор, що підключає зловмисника до системи.

Якщо зловмисник знав, що співробітники брали участь у нещодавній конференції, вони можуть видати себе за постачальника, який був присутній, і надіслати цілі лист із натяком на те, що це є продовженням презентації. Типовим повідомленням буде: "Якщо ви пропустили демонстрацію нашого продукту та річну безкоштовну пробну версію, перегляньте слайд-шоу на вкладеному USB-ключі, натиснувши start.exe".

Мікрокомп'ютерні атакуючі агенти

Raspberry Pi є мікрокомп'ютер - він має розмір приблизно 8,5 см x 5,5 см, але має 8 Гб оперативної пам'яті, два порти USB і порт Ethernet, підтримуваний чіпом

Broadcom з використанням процесора ARM з тактовою частотою 1,5 ГГц. Він не має жорсткого диску, але використовує SD-карту для зберігання даних.

Як показано на наступній фотографії, Raspberry Pi становить приблизно дві третини довжини стандартної ручки; легко сховатися в мережі (за робочими станціями або серверами, усередині серверних шаф або приховано під панелями підлоги в центрі обробки даних).

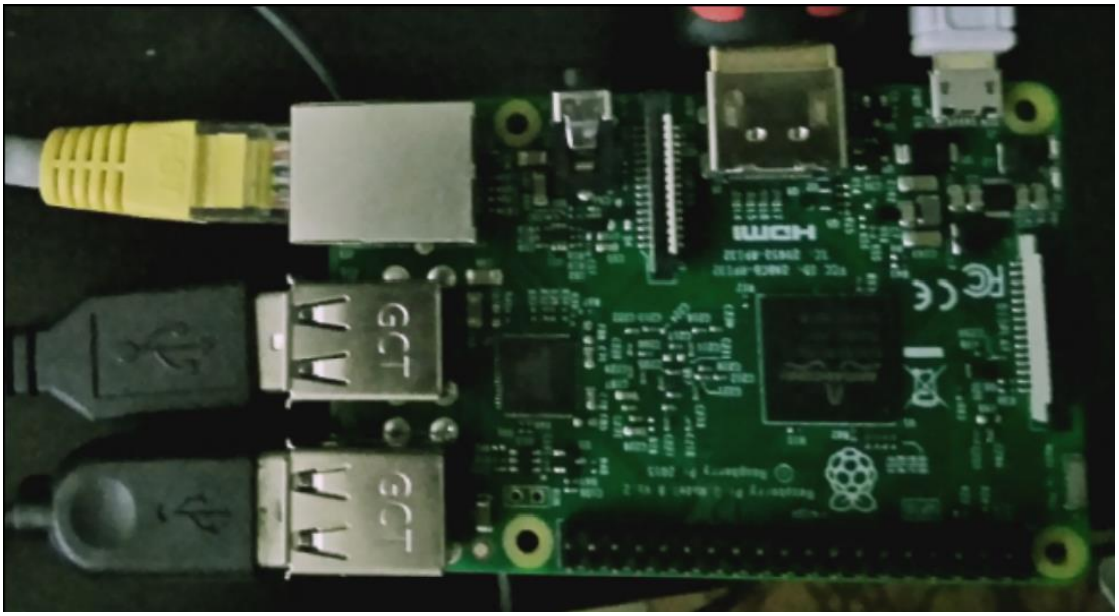

Рисунок 2.2 – Raspberry Pi

Щоб налаштувати Raspberry Pi як вектор атаки, потрібні такі елементи:

- Raspberry Pi Model B, або новіші версії.
- Кабель HDMI.
- Кабель micro USB та блок зарядки.
- Кабель Ethernet або міні-бездротовий адаптер.
- Картка SD, клас 10, щонайменше 8 ГБ [7].

2.2. Огляд інструментарію впровадження атак

Social Engineering Toolkit

Одним з основних та найпотужніших засобів проведення комп’ютерної атаки є SET(Social Engineering Toolkit), він включає всі необхідні інструменти для проведення атак.

SET був створений і написаний Девідом Кеннеді і підтримується активною групою співавторів. Це фреймворк, керований Python, з відкритим кодом, спеціально розроблений для полегшення атак соціальної інженерії.

SET був розроблений з метою досягнення безпеки шляхом навчання. Суттєвою перевагою SET є взаємозв'язок з Metasploit Framework, який забезпечує корисне навантаження, необхідне для експлуатації, шифрування в обхід антивірусного програмного забезпечення та модуль прослуховування для підключення до зламаної системи, коли він відправляє оболонку назад зловмиснику.

Щоб відкрити SET у дистрибутиві Kali, перейдіть до Додатки в Kali Linux / Інструменти експлуатації / Набір інструментів соціальної інженерії setoolkit або введіть setoolkit у підказці оболонки. Вам буде представлено головне меню, як показано на наступному скріншоті:

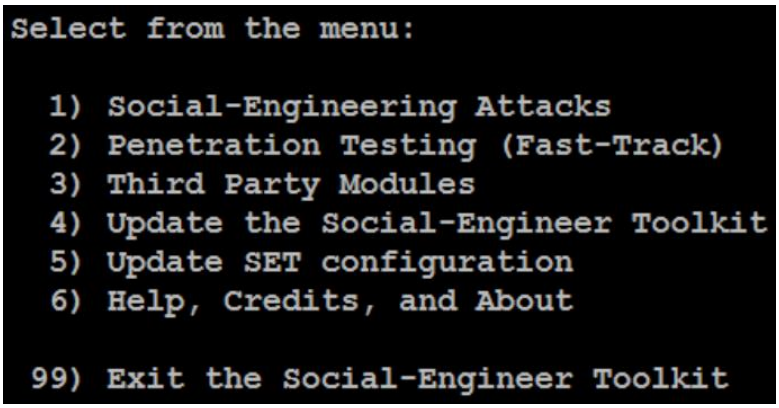

Рисунок 2.3 – Головне меню SET

Якщо вибрати 1) Соціально-інженерні атаки, перед вами з'явиться таке підменю:

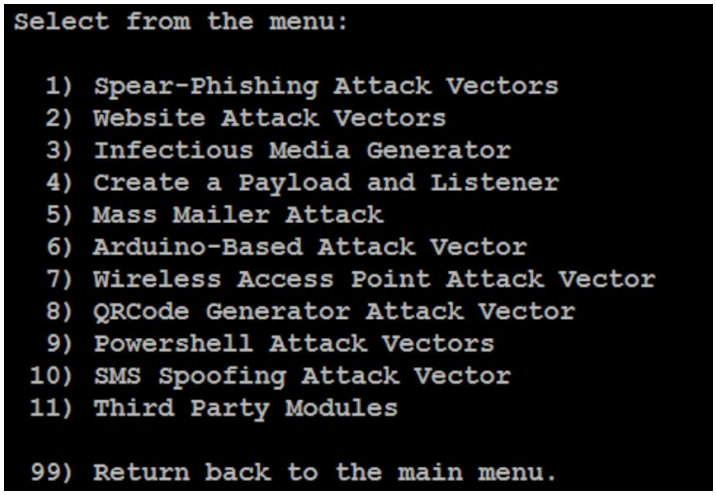

Рисунок 2.4 – Види атак у підменю

Розділ включає в себе список векторів для атак:

- Вектори атаки веб-сайтів.
- Інфекційний медіагенератор.
- Створення корисного навантаження і слухача.
- Масова атака.
- Вектор атаки на основі Arduino.
- Вектор атаки бездротової точки доступу.
- Вектор атаки генератора QRCode.
- Вектори атаки Powershell.
- Сторонні модулі.

Сам розділ може працювати в декількох напрямках, починаючи від створення і впровадження шкідливих навантажень, масових атак, атак на різні точки Wi-Fi, генерації QR-коду та інше.

Розділ вектори веб-сайтів підрозділяється на методи:

метод впровадження Java;

метод використання браузера Metasploit;

метод атаки на харвестер;

метод атаки таббата;

метод атаки веб-гейдінга;

метод атаки HTA.

Методи атак поділяються на розділи, починаючи від впровадження та створення всередині java, використання вже готових метасплойтів для фішингу, збору даних, розрахованих на багато користувачів методів атак на вибір; є можливість використовувати і все разом - все залежить від фантазії зловмисника [8].

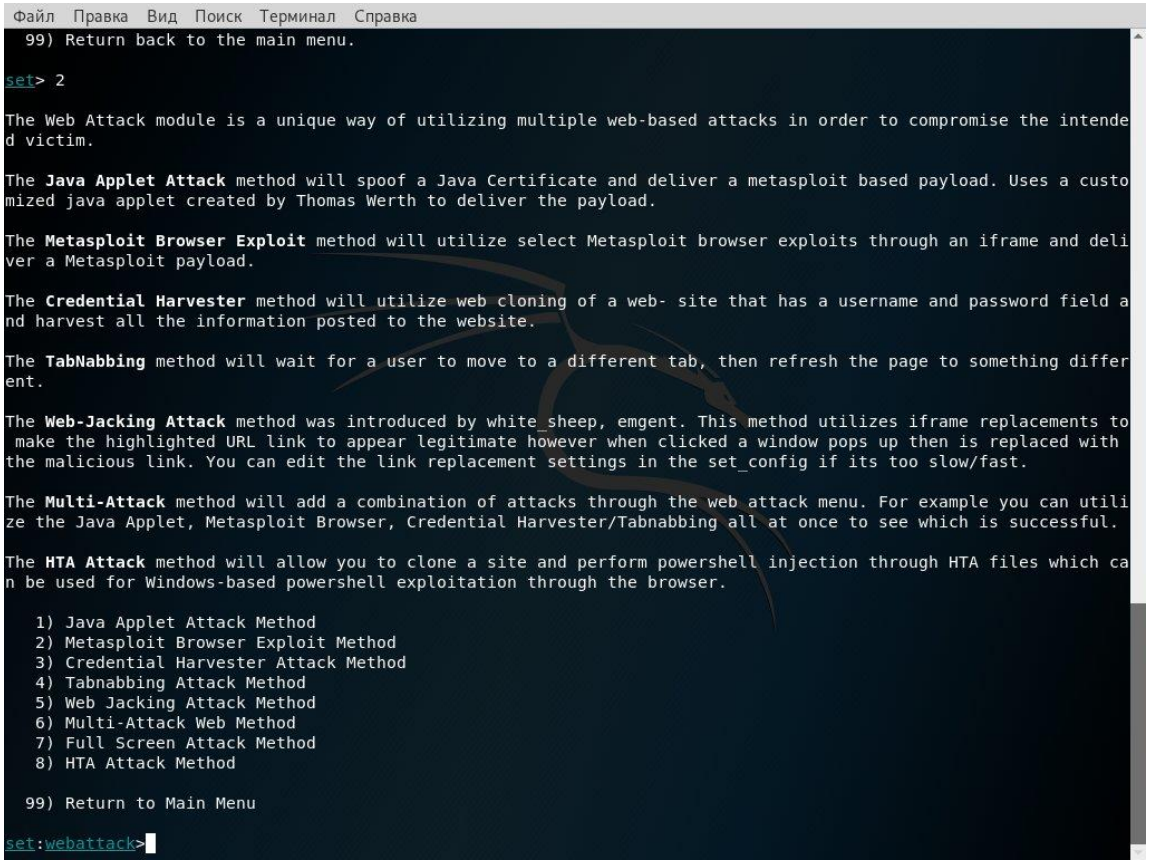

Рисунок 2.5 – Методи атак соціально-технічного розділу

Wifiphisher

Wifiphisher - це унікальний інструмент соціальної інженерії, який автоматизує фішинг-атаки на мережі Wi-Fi для отримання паролів WPA / WPA2 цільової бази користувачів. Інструмент може вибрати будь-яку точку доступу Wi-Fi поблизу, заблокувати її (скасувати автентифікацію всіх користувачів) і створити точку доступу-клону, для приєднання якої не потрібен пароль.

Будь-якій людині, яка підключається до злої близнюкової відкритої мережі, представляється на перший погляд законна фішинг-сторінка з проханням ввести пароль Wi-Fi для завантаження оновлення мікропрограми, яка називається причиною непрацювання Wi-Fi.

Як тільки цілі вводять пароль, Wifiphisher надсилає попередження, затримуючись на час. Після передачі захопленого пароля він відображатиме як підроблений таймер перезавантаження, так і підроблений екран оновлення, щоб придбати час для тестування захопленого пароля. Це зручний інструмент для оцінки рівня захисту від соціальної інженерії на основі Wi-Fi [9].

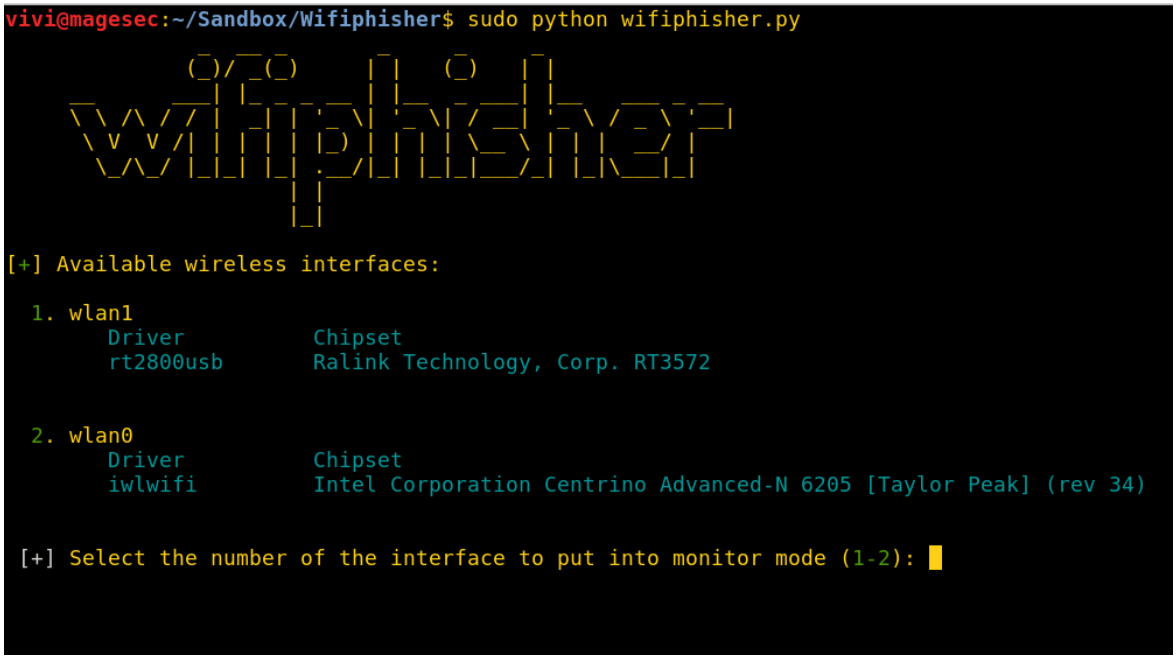

Рисунок 2.6 – Інтерфейс Wifiphisher

MSFvenom Payload Creator (MSFPC)

MSFPC – це зручний інструмент, який спрощує створення основних корисних навантажень. Це допомагає користувачам уникнути необхідності писати довгі команди msfvenom для формування корисного навантаження. За допомогою цього генератора ви можете створювати корисні навантаження з мінімум одним аргументом.

MSFPC можна використовувати для створення корисних навантажень Windows, Linux і навіть Android. Його сценарій - це реальна економія часу, коли ви хочете швидко створити прості корисні навантаження. Хоча це не передбачає кодування для обходу антивірусного вірусу, все одно може бути корисним для вивчення.

Іноді ви просто хочете швидко зробити корисний товар, доставити його кудись і продовжувати виконувати свої рутинні справи. У таких сценаріях msfpc.sh може стати в нагоді.

Щоб використовувати MSFPC, ви повинні визначити потрібну корисну навантаження лише за допомогою розширення файлу, яке ви хочете мати, або платформи, на якій ви збираєтесь його опустити. Набравши msfpc у терміналі, ви зможете запустити інструмент [9].

3. МЕТОДИКА ПРОВЕДЕННЯ АУДИТУ КОМПАНІЇ НА СХИЛЬНІСТЬ ДО АТАК МЕТОДАМИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

3.1. Опис методики проведення аудиту

Існує безліч стандартів, що стосуються теми організаційних тестів безпеки, хоча ця література рідко стосується вимірювання соціальної інженерії. Серія стандартів ISO27000 спеціально зарезервована Міжнародною організацією зі стандартизації (ISO) з питань захисту інформації. Тому визначено багато модулів, які намагаються перерахувати деякі рекомендації щодо найкращих практик. Незважаючи на те, що це величезні документи з величезним обсягом, ця серія стосується соціальної інженерії лише незначно. Просто ISO27005 пропонує більше деталей щодо оцінки ризиків. Тим не менше, він не пропонує конкретних методів аналізу ризиків. На відміну від тестування безпеки ISO27000, запропонована система тестування соціальної інженерії не спрямована на випуск сертифікатів, а на вимірювання конкретної вразливості соціальної інженерії. Отже, тестована організація отримає оцінку щодо соціальної інженерії [10].

Щоб отримати реалістичний огляд безпеки компанії, ми пропонуємо провести кілька різних експериментів та додаткове внутрішнє спостереження.

В якості вхідних даних для розробки нашого аудиту соціальної інженерії ми також вивчили найпоширеніші методики проведення тестування на проникнення. В ході аналізу було визначено п’ять основних фаз аудиту: ознайомлення, розвідка, планування, проникнення та документація.

Дана методика складається з трьох етапів:

етап 1 – попереднє знайомство та планування;

етап 2 – оцінка;

етап 3 – звітність.

3.1.1. Етап попереднього знайомства та планування

Цей етап включає в себе кроки з обміну початковою інформацією, планування та підготовки до тестування. Перед початком тестування з обох сторін буде підписано офіційну Угоду про аудит. Вона забезпечить основу для даного завдання і взаємну юридичний захист. У ньому також будуть вказані конкретна команда, точні дати і час

проведення тестування, шляхом ескалації та інші домовленості. Даний етап містить наступні кроки:

Визначення об’єму

На даному кроці ми визначаємо рамки проведення нашого тесту.

Визначення меж взаємодії тих середовищах, де інфраструктура може бути не повністю належить клієнту. Ці компоненти інфраструктури слід зазначити та забезпечити їх виключення з активних методів тестування на проникнення.

Цілі

Кожен тест на проникнення повинен бути цілеспрямованим. Це означає, що метою тесту є виявлення конкретних вразливих місць, які призводять до компромісу з бізнес-цілями або завданнями клієнта. Йдеться не про пошук невідпрацьованих систем. Йдеться про визначення ризику, який негативно вплине на організацію.

Оцінка часу

Оцінка часу безпосередньо пов’язана з досвідом випробувача в певній області тестування. Якщо тестувальник має значний досвід проведення певного тесту, він, швидше за все, відразу зможе визначити, скільки часу триватиме тестування. Якщо тестувальник має менше досвіду в цій області, повторне читання звітів сканування з попередніх подібних тестів, які проводила фірма, є чудовим способом оцінити час, необхідний для поточної участі. Як тільки визначено час тестування, розумною практикою є додати 20% до цього часу. Вони забезпечують страхування на випадок перебоїв у тестуванні.

Ще однією складовою метрики часу та тестування є те, що кожен проект повинен мати остаточну дату знищення. Усі хороші проекти мають чітко визначений початок і кінець. Вам потрібно мати підписаний робочий документ із зазначенням роботи та необхідних годин, якщо ви досягли певної дати закінчення тестування або якщо після цієї дати вам потрібно буде просити додаткове тестування або роботу. Деяким тестерам важко це робити, оскільки вони відчувають, що їм надто боляче, якщо мова йде про вартість і години. Однак, як зазнав досвід автора, якщо ви надасте виняткову цінність для основного тесту, замовник не буде змушений платити вам за додаткову роботу.

Правила взаємодії

Правила взаємодії передбачають узгоджений підхід до тесту на проникнення. Сюди входять такі пункти, як час і спосіб проведення випробування на проникнення, які системи та людей дозволено випробовувати та наскільки далеко може пройти тестер проникнення з обраною мішенню. Це також включатиме затверджений час доби для проведення тестування.

Встановіть зв'язку

Наявність задокументованого плану спілкування є надзвичайно важливим фактором, і це може заощадити час, якщо виникає проблема при тестуванні поза робочим часом. Не виключено, що під час тестування система може вийти з ладу, і тестер проникнення або команда повинна мати контакт з клієнтом для спілкування під час тесту.

Зберіть наступну інформацію про кожен екстрений контакт:

1. Повне ім'я
2. Посада
3. Форма цілодобового негайного контакту, наприклад, дзвінок, месенджер чи пошта

Захист себе

Важливою частиною Угоди про аудит має бути захист інтересів. Цей пункт, дає тестеру дозвіл на проведення тесту на проникнення. Він захищає аудитора від відповідальності, якщо є негативні наслідки внаслідок випробування на проникнення.

3.1.2. Етап оцінки

На цьому етапі проводиться оцінка компанії, відбувається збір інформації, її аналіз та проникнення у систему.

Збір інформації

Цей етап передбачатиме збір розвідданих із відкритим кодом, що включає огляд загальнодоступної інформації та ресурсів. за допомогою технічних (DNS / WHOIS) і нетехнічних (пошукові системи, групи новин, списки розсилки тощо) методів. Метою цього етапу є виявлення будь-якої інформації, яка може допомогти під час наступних етапів тестування, яка може включати адреси електронної пошти, імена користувачів, номери телефонів, інформацію про компанію, яка може бути використана для того,

щоб зробити нас схожими на внутрішніх працівників або працівників інших компаній, що взаємодіють з нашою, тим кому можуть довіряти робітники компанії. Крім того, цей крок включатиме пошук конфіденційної інформації, яка не повинна бути загальнодоступною, наприклад, внутрішні комунікації, інформація про заробітну плату чи інша потенційно шкідлива інформація.

Цей розділ надзвичайно важливий для оцінювача. Оцінки, як правило, обмежені у часі та ресурсах. Тому надзвичайно важливо визначити точки, які, найімовірніше, будуть вразливими, і зосередитись на них. Навіть найкращі інструменти марні , якщо не використовується належним чином і в потрібному місці і часі. Ось чому досвідчені оцінювачі витрачають багато часу на інформаційний збір.

Так як соціальна інженерія має на увазі взаємодію лише з людським фактором, тому і при зборі інформації ми будемо користуватися тільки відкритими джерелами, щоб знайти те, що людина сама залишила.

Ми проводимо збір інформації з відкритим кодом, щоб визначити різні точки входу в організацію. Ці точки входу можуть бути фізичними, електронними та / або людськими. Багато компаній не беруть до уваги, яку інформацію про себе вони публічно розміщують і як ця інформація може бути використана рішучим зловмисником. Крім того, багато співробітників не враховують, яку інформацію вони розміщують про себе публічно та як ця інформація може бути використана для нападу на них або їх роботодавця.

Інформація, яку ми зможемо знайти з відкритих джерел:

Цілі бізнесу

Розуміння того, чим займається компанія, які її ідеали і як вона працює, завжди є ключовою інформацією. Якщо обраний підхід полягає в тому, щоб видати себе за співробітника, необхідно провести ретельне дослідження, щоб впоратися із завданням. Розуміння основ організації, а також деяких жаргонних слів, які використовуються в даній сфері діяльності, може принести багато користі. Знання про бізнес також можуть допомогти при складанні обґрунтованих припущень про тип систем, які можуть використовуватися.

Невелике копання може також дати підказки про те, з яким опором доведеться зіткнутися під час дзвінка або виїзду на місце. Якщо компанія звикла мати справу з урядовими та військовими установами, соціальний інженер, швидше за все, зіткнеться з добре підготовленими людьми у сфері інформаційної безпеки. Іншими показниками потенційного рівня безпеки організації можуть бути логотипи стандартів забезпечення інформаційної безпеки, таких як ISO або PCI. Знову ж таки, це індикатори того, що принаймні деякі люди в компанії пройшли навчання, що може зробити їх більш складними для використання.

Партнери, клієнти, постачальники

Багато організацій публікують на своєму сайті списки клієнтів, партнерів і постачальників. Що може бути кращим приводом для дзвінка з метою збору інформації? Зателефонувавши в службу підтримки і видавши себе за клієнта, ви, швидше за все, отримаєте корисну інформацію. Якщо у цільової організації є клієнтський портал, ви можете отримати до нього доступ, спробувавши скинути пароль клієнта. У багатьох випадках, щоб завоювати чиєсь довіру, досить знати трохи інформації, яка буде вважатися конфіденційною. Це може бути URL-адреса клієнтського порталу та використання імені клієнта.

Адреси електронної пошти

Адреси електронної пошти виключно корисні в атаках соціальної інженерії, і вони будуть більш детально розглянуті далі в цій главі, включаючи способи їх збору із загальнодоступних ресурсів. Існує кілька способів їх використання, наприклад, вибір шляху цільових або широкомасштабних фішингових атак або використання їх для атак на VPN і поштові портали. Хоча останнє може здатися більш схожим на тестування на проникнення, багато завдань по соціальної інженерії складаються з такого змішаного підходу.

Адреса електронної пошти також може вказувати на внутрішню угоду про ім'я користувача, що означає, що якщо вдасться ідентифікувати більше співробітників, можна скласти ще більший список адрес електронної пошти і користувачів.

Імена співробітників

Швидше за все, кількість імен співробітників на корпоративному сайті буде обмежено керівництвом. Пошук людей, що знаходяться нижче по ієрархії, все ще можливий, особливо якщо у організацій є блоги або новинні статті, написані співробітниками. Імена співробітників корисні з точки зору уособлення або для згадки імені при дзвінку.

Ієрархія персоналу

Розуміння ієрархії персоналу завжди корисно для соціального інженера. Це дає нам інформацію про те як люди взаємодіють всередині компанії.

Фотографії співробітників і місцезнаходження бізнесу

Фотографії можуть містити метадані. Вони можуть розповісти про тип пристрою, яким була зроблена фотографія, географічне розташування і багато іншого.

Крім того, існує більш очевидна цінність інформації на фотографіях. Це можуть бути фотографії фізичних об'єктів, внутрішнє планування офісів і навіть ідентифікаційні бейджі. Наприклад, часто ідентифікаційні бейджи виявляються на рекламних фотографіях і потім використовуються для створення дублікатів.

Соціальні мережі

Імена співробітників та фотографії з корпоративного сайту відкривають ще більший простір для індивідуального пошуку. Ми можемо знайти профіль у соціальних мережах, що може розповісти нам ще більше інформації, такої як: особисті інтереси, улюблені місця, особіста пошта чи номер телефону тощо [11].

Аналіз вразливостей

У цьому пункті відбувається сортування зібраної інформації, визначення важливості тих чи інших даних для тестування. Визначення слабких місць нашої системи.

Далі повинен бути розроблений чіткий план для виконання тестування. Потрібно визначити вектори атак на кожну людину та прописати сценарій проникнення у систему для отримання фізичного доступу до інформації.

Ідентифікація цілі

Ідентифікація цілі - це структурований процес сортування, що призводить до цілей, які вважаються найбільш придатними. На рисунку 3.1 показано базовий загальний трикутник ідентифікації цілі, який можна використовувати у багатьох різних ситуаціях. Під час атаки на бізнес, кожен працівник є потенційною ціллю, а також усі, хто безпосередньо чи опосередковано пов'язаний з цим бізнесом. Тому вихідним пунктом у цьому процесі є побудова трикутника з цими цілями. Кількість цілей зменшиться, оскільки їх «підвищують» на вищий рівень на основі певних критеріїв. Окремі рівні критеріїв на рисунку 3.1 є досить загальними, тому їх можна застосовувати до різних цілей.

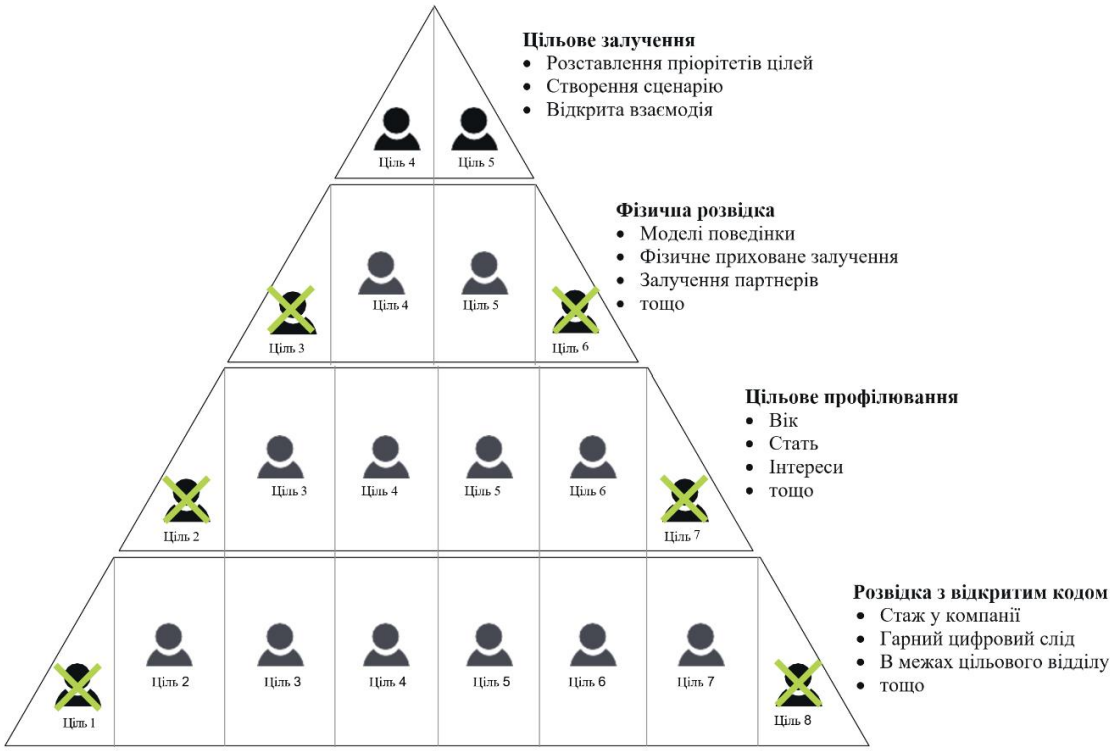

Рисунок 3.1 – Загальний трикутник ідентифікації цілі

Розробка сценарію

Після того, як аудитор відібрав найбільш придатні цілі потрібно розробити сценарій атаки на них. При розробці сценарію требя пам’ятати про рамки, що були встановлені на першому етапі.

Кожен сценарій складається з двох ключових частин: персонажа та ситуації, коли ваш персонаж може намагатися отримати доступ до інформації, яку ви шукаєте [11].

Проникнення

На даному етапі відбувається саме процес проникнення у систему аудитором шляхами, що були визначені у минулому етапі. Сам процес впровадження також має три кроки.

Встановлення відносин і взаєморозуміння.

На цьому кроці встановлюються робочі відносини з ціллю. Це критичний момент, оскільки якість відносин визначає рівень співпраці і ступінь, в якій ціль піде, щоб допомогти зловмисникові в досягненні мети. Це може бути так само швидко, як поспіх до дверей з широкою посмішкою і зоровим контактом, щоб мета тримала двері відкритими, щоб зловмисник міг пройти. Або це може бути з'єднання на особистому рівні по телефону або таке приватне, як показ сімейних фотографій і обмін історіями з адміністратором у вестибюлі. Він також може бути настільки ж великим, як побудова онлайн-відносин з ціллю через видавання себе за співробітника компанії партнера.

Експлуатація

Це коли зловмисник використовує як інформацію, так і відносини, щоб активно проникнути в ціль. На цьому етапі зловмисник зосереджується на підтримці імпульсу відповідності, встановленого на етапі 2, не викликаючи підозр. Експлуатація може відбуватися шляхом розголошення, здавалося б, несуттєвою інформації або доступу, наданого зловмиснику. Приклади успішної експлуатації:

- Акт утримання дверей відкритими чи іншого дозволу зловмисникові проникнути всередину приміщення.
- Розкриття пароля та імені користувача по телефону.
- Пропонуючи соціальне доказ шляху введення SE інший персонал компанії.
- Вставка USB-накопичувача з шкідливою корисним навантаженням на комп'ютер компанії.
- Відкриття зараженого вкладення електронної пошти.
- Розголошення комерційної таємниці в розмові з передбачуваним «колегою».

Виконання

На цьому кроці аудитор досягає своєї кінцевої мети або з різних причин завершує атаку таким чином, щоб не викликати підозр. Зазвичай атака закінчується до того, як ціль починає сумніватися щось підозрювати. Крім того, аудитор стирає цифрові сліди і гарантує, що ніякі елементи або інформація не залишаться позаду. В результаті досягаються дві важливі цілі. По-перше, ціль не знає, що відбувся напад. По-друге, аудитор приховує свою особистість. Добре спланована і плавна стратегія виходу - це мета атакуючого і заключний акт атаки.

3.1.3. Етап підготовки звітних документів

Після завершення всіх тестових випадків, визначених у обсязі робіт, необхідно підготувати письмовий звіт, що описує детальні результати тестів і оглядів, з рекомендаціями щодо поліпшення. Звіт повинен слідувати добре документованої структурі. У звіті обов'язково повинні бути наступні розділи:

- Резюме.
- Масштаб проекту.
- Використані інструменти.
- Дати і час проведення фактичних випробувань систем.
- Всі результати проведених тестів.

3.2. Практичне керівництво до етапу оцінки

Детальніше розглянемо послідовність дій, які потрібно виконати, щоб реалізувати усі кроки тестування на етапі оцінки.

3.2.1. Збір інформації

В описі методики було розібрано основні види інформації, які можна знайти:

- Цілі бізнесу.
- Партнери, клієнти, постачальники.
- Адреси електронної пошти.
- Імена співробітників.
- Ієрархія персоналу.
- Фотографії співробітників і місцезнаходження бізнесу.

Збір інформації з корпоративного сайту

Основним ресурсом для її пошуку є веб-сайт компанії. Далі ознайомимося з інструментами, що допоможуть нам їх знайти.

Метадані документа

Метадані документа - це, по суті, атрибутивна інформація, що зберігається в офісних документах. Коли створюється документ Microsoft Word або PDF , він автоматично позначається деякими метаданими, причому автор навіть не підозрює про це. Ця інформація може бути отримана будь-якою людиною, у якого є документ.

Зазвичай метадані являють собою ім'я користувача і ім'я підприємства, обрані при установці офісного продукту. Принаймні, деякі метадані документа можна переглянути , перевіривши властивості документа з офісного додатку

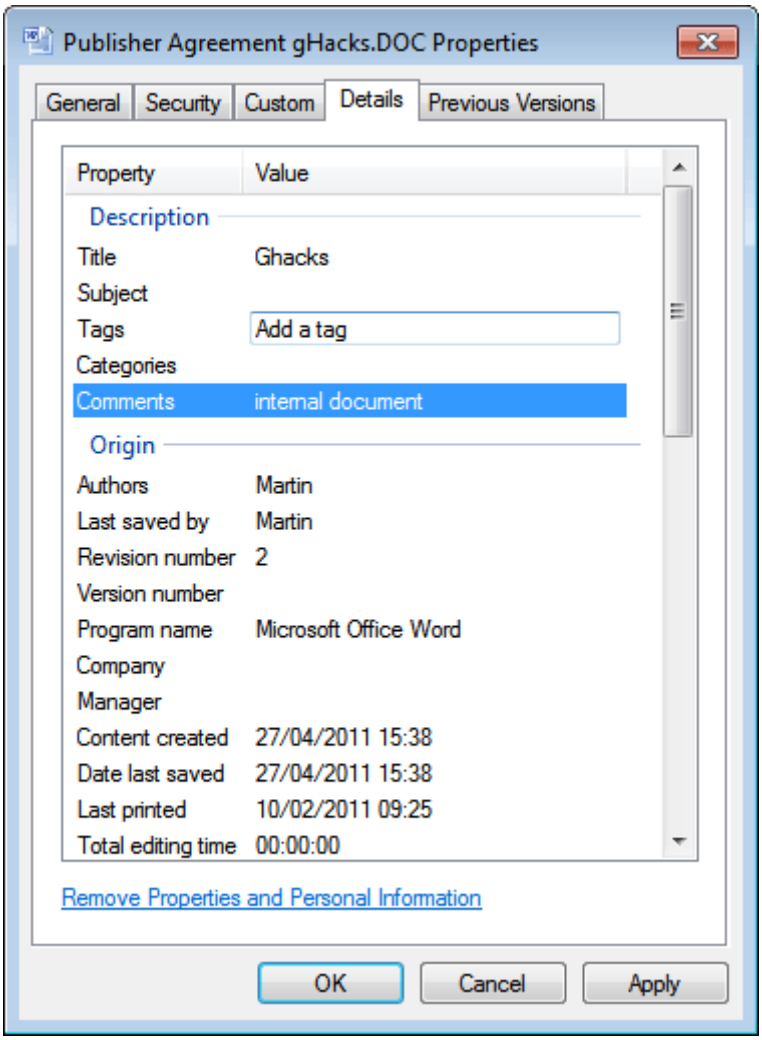

Рисунок 3.2 – Властивості документу

Це ясно показує, що документ може містити ім'я людини, який його створив. Потім його можна додати в списки імен користувачів або, можливо, назвати під час дзвінка в організацію.

Існує безліч інших тегів метаданих, які можуть бути додані окремою людиною, і досить багато тегів, які додаток додає самостійно.

Зазвичай в цих прихованих метаданих можна знайти версії операційних систем, структури каталогів і користувачів. Крім того, можна знайти точну версію програмного забезпечення, використаного для створення файлу. Ось деякі інструменти, які можна використовувати для вилучення цих відомостей:

Визначити метадані можливо за допомогою спеціалізованої пошукової системи. Мета полягає у визначенні даних, що мають відношення до цільової корпорації. Можливо, можна буде визначити місцезнаходження, обладнання,

програмне забезпечення та інші відповідні дані з публікацій у соціальних мережах. Деякі пошукові системи, які надають можливість пошуку метаданих, є такими:

- ixquick – http://ixquick.com
- MetaCrawler – http://metacrawler.com
- Dogpile – http://www.dogpile.com
- Search.com – http://www.search.com
- Переглядач Exif Джеффрі – http://regex.info/exif.cgi

Окрім пошукових систем, існує кілька інструментів для збору файлів та збору інформації з різних документів.

FOCA

FOCA – це інструмент, який зчитує метадані з широкого кола форматів документів та носіїв інформації. FOCA отримує відповідні імена користувачів, шляхи, версії програмного забезпечення, деталі принтера та адреси електронної пошти. Це все можна виконати без необхідності індивідуального завантаження файлів.

Процес вилучення метаданих практично повністю автоматизований. FOCA задається домен, і вона від спрямовується на пошуки всіх документів, які існують в ньому. Потім FOCA повідомляється, що потрібно завантажити документи і витягти мета-дані. Він класифікує кожен знайдений тип і відображає їх у вигляді дерева з зручною навігацією. Потім метадані можуть бути експортовані в файли, щоб можна було ними маніпулювати.

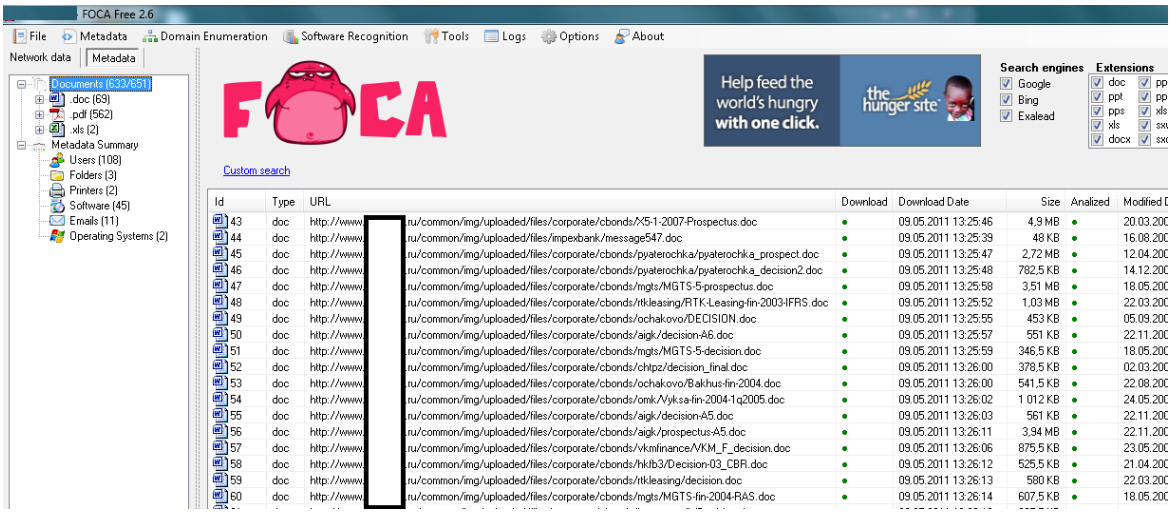

Рисунок 3.3 – Результат пошуку файлів за допомогою FOCA

Metagoofil

Metagoofil – це засіб збору інформації на основі Linux, призначений для вилучення метаданих публічних документів (.pdf, .doc, .xls, .ppt, .odp, .ods), доступних на веб-сайтах клієнта.

Metagoofil працює аналогічно FOCA . Він починає з пошуку в Google , а потім завантажує документи з цільового веб-сайту. Потім Metagoofil може приступити до вилучення метаданих з документів і представити результати у вигляді звіту. Як і у випадку з FOCA, Metagoofil здатний витягувати імена користувачів, версії програмного забезпечення, адреси електронної пошти та шляхи до документів.

Команда для запуску метагофілу така:

metagoofil.py -d <client domain> -l 100 -f all -o <client domain>.html -t micro-files

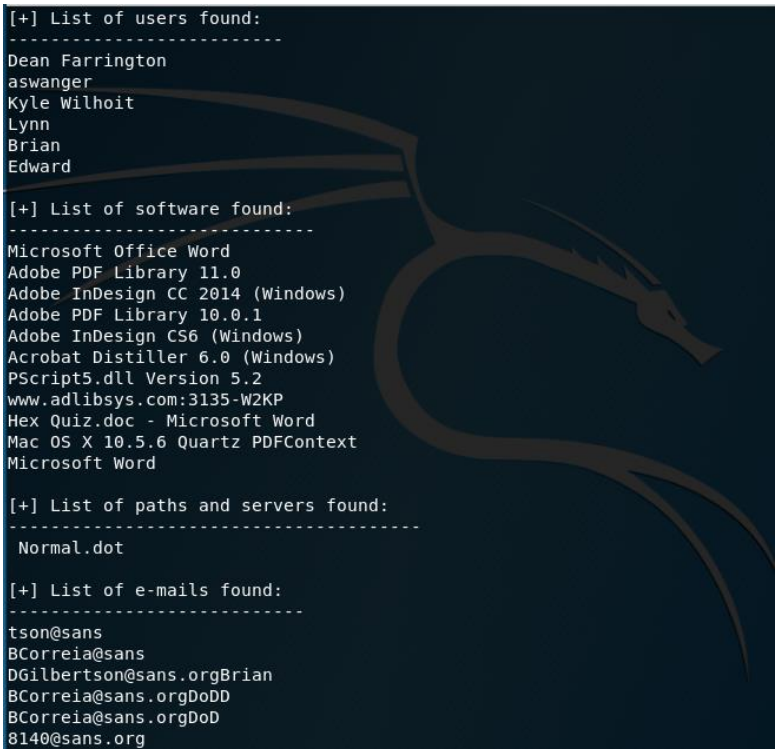

Рисунок 3.4 – Вилучені дані за допомогою Metagoofil

ExifTool

Exiftool - це безкоштовна програма для читання Exif як для Windows , так і для OSX. Exiftool можна використовувати як для редагування метаданих, так і для їх отримання, що означає, що його можна використовувати для знезараження корпоративних фотографій перед їх публікацією.

ExifTool можна завантажити з https://exiftool.org/.

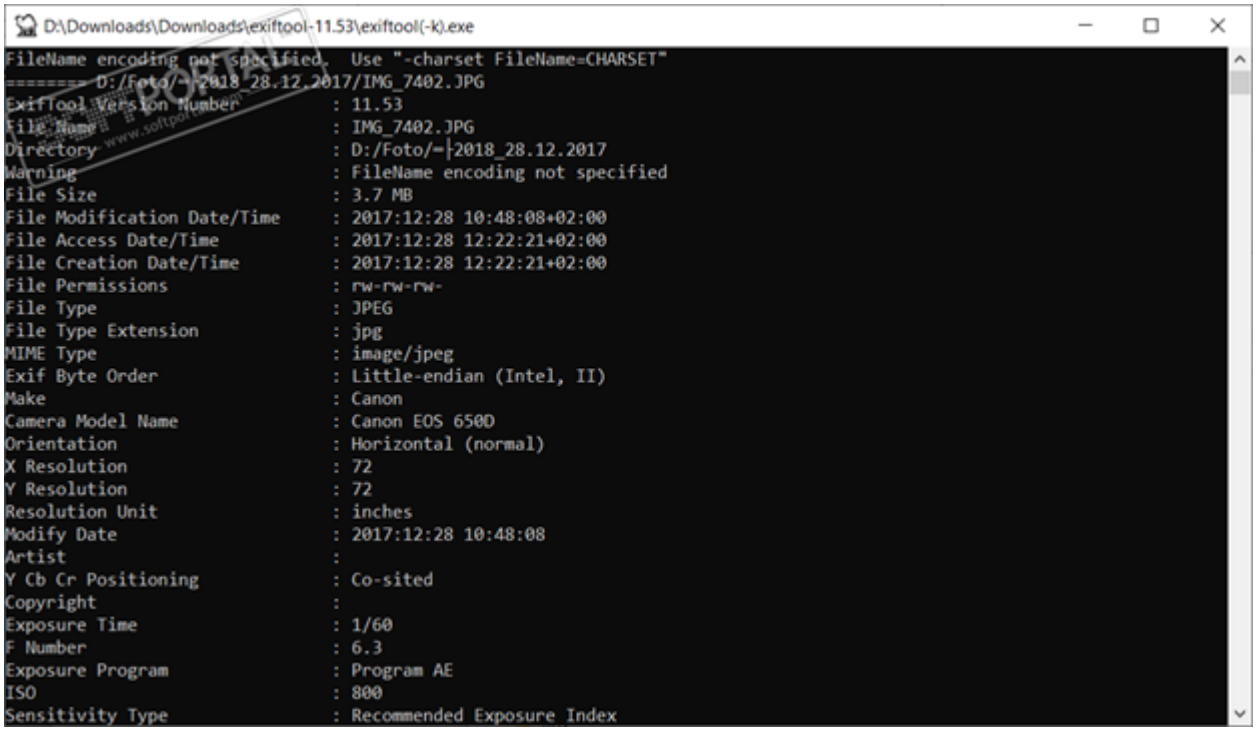

Рисунок 3.5 – Дані отримані за допомогою ExifTool

Wget для завантаження зображень з сайту

Wget - це інструмент командного рядка, який може створювати HTTP , HTTPS і FTP з'єднання з сайтом, в основному для автоматичного вилучення файлів. Це інструмент командного рядка, який доступний для Linux, OSX і Windows . Wget можна доручити переглянути посилання на сторінці і завантажити всі знайдені зображення на певну глибину.

GeoSetter

GeoSetter - це додаток для Windows , яке знімає геодані з зображень і потім робить з них карту. Додаток надзвичайно простий у використанні і швидко виділяє потенційні фізичні місця, які можуть бути використані у ваших оцінках. Програма підтримує експорт даних в Google Earth і редагування геоінформації, якщо ви хочете знезаразити зображення.

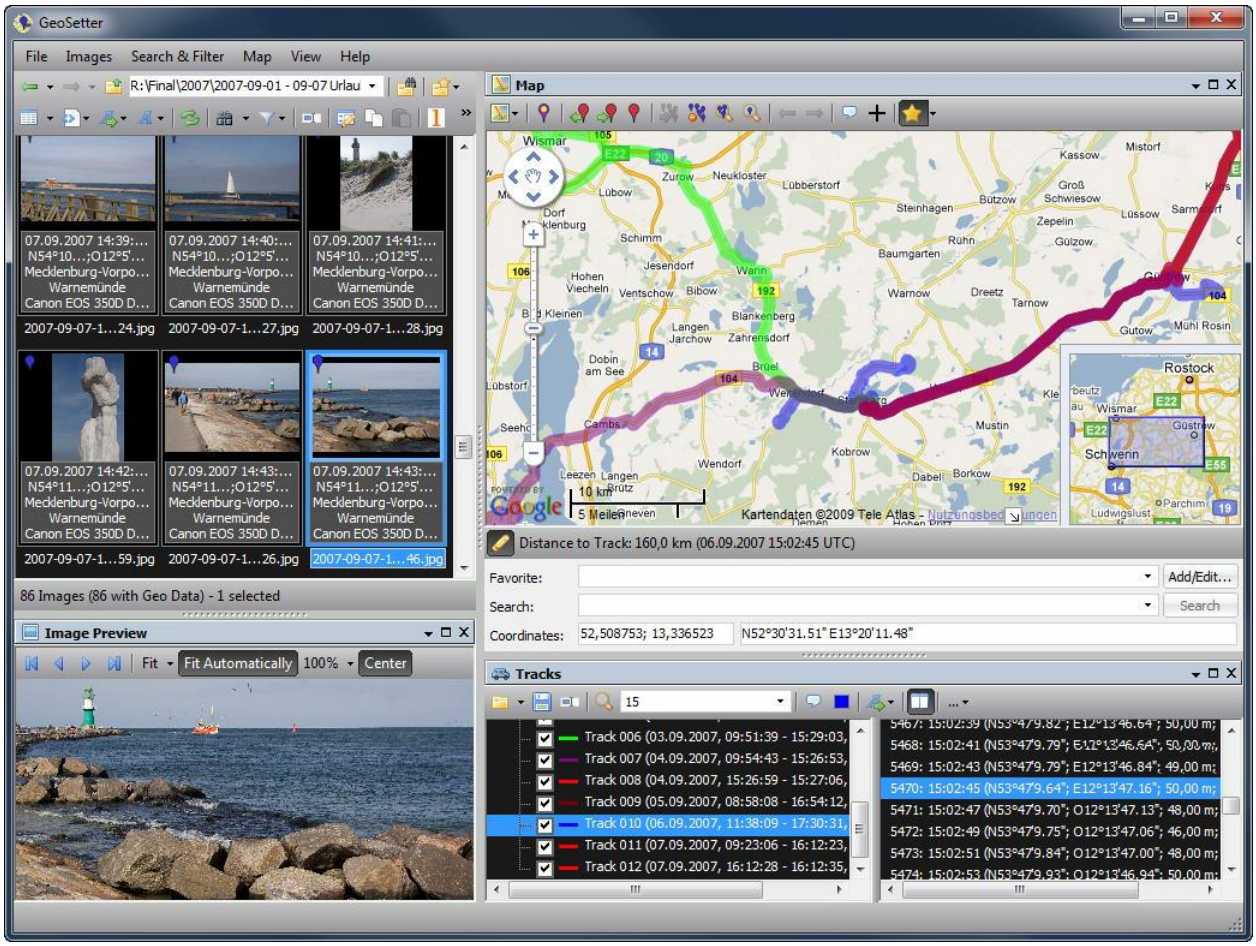

Рисунок 3.6 – Дані отримані за допомогою Geosetter

Наведемо декілька прикладів того, які корисні відомості може надати соціальному інженеру робота з набором інструментів, зазначених вище:

- Корпоративне розташування і офіси.
- Розміщення центру обробки даних.
- Потенційні місця, куди співробітники організації ходять спілкуватися.
- Клієнти і постачальники, пов'язані з організацією.
- Типи корпоративних пристроїв (iPhone , Android).
- Імена пристроїв. (Ім'я пристрою iPhone дуже часто є ім'ям користувача).

Деякі організації ретельно охороняють місцезнаходження своїх об'єктів, тому можливість показати їм збитки, завдані в результаті ненавчених співробітників роботі з даними Exif , може бути цінною вправою сама по собі.

Визначення потенційних місць, де співробітники можуть проводити час, відкриває перед соціальним інженером багато можливостей. Це може бути проста дія

- пронести RFID -бейдж, або складне - вивудити інформацію зі співробітників, коли вони не напоготові.

Зворотній пошук зображень

Ці служби пропонують можливість завантажити зображення і спостерігати, як пошукова система простежує його в інших місцях. Деякі з них також намагаються зіставити атрибути зображення з іншими фотографіями, що зберігаються в Інтернеті, наприклад, колір та форма.

Їх багато, але найпопулярнішими, мабуть, є пошук зображень Google і TinEye.

Цей вид послуг корисний для соціальних інженерів, оскільки він допомагає зіставити одне зображення з акаунтами в соціальних мережах, блогами, корпоративними та особистими сайтами. Наприклад, фотографія колеги з LinkedIn потрапила в зворотний пошук зображень Google. У результатах пошуку він відразу ж визначив їх аккаунт в Twitter , тому якщо фотографія співробітника виявлена на корпоративному сайті, але немає представлення про те, хто це, це може виявитися надзвичайно корисною функцією. Чим більше онлайн-присутності можна пов'язати з людиною, тим більше шансів створити правдоподібний привід і отримати додаткові відомості.

The Way Back Machine

The Way Back Machine – це архів старих версій веб-сайтів. У деяких випадках він охоплює роки і містить регулярні знімки багатьох веб-сайтів. Часто це може бути корисно для перевірки домену цілі на наявність конфіденційної інформації, такої як контактні дані і фізичне місце розташування. Незважаючи на те, що сьогодні інформаційної безпеки приділяється велика увага, не потрібно заглядати далеко в минуле, щоб зрозуміти, що так було не завжди.

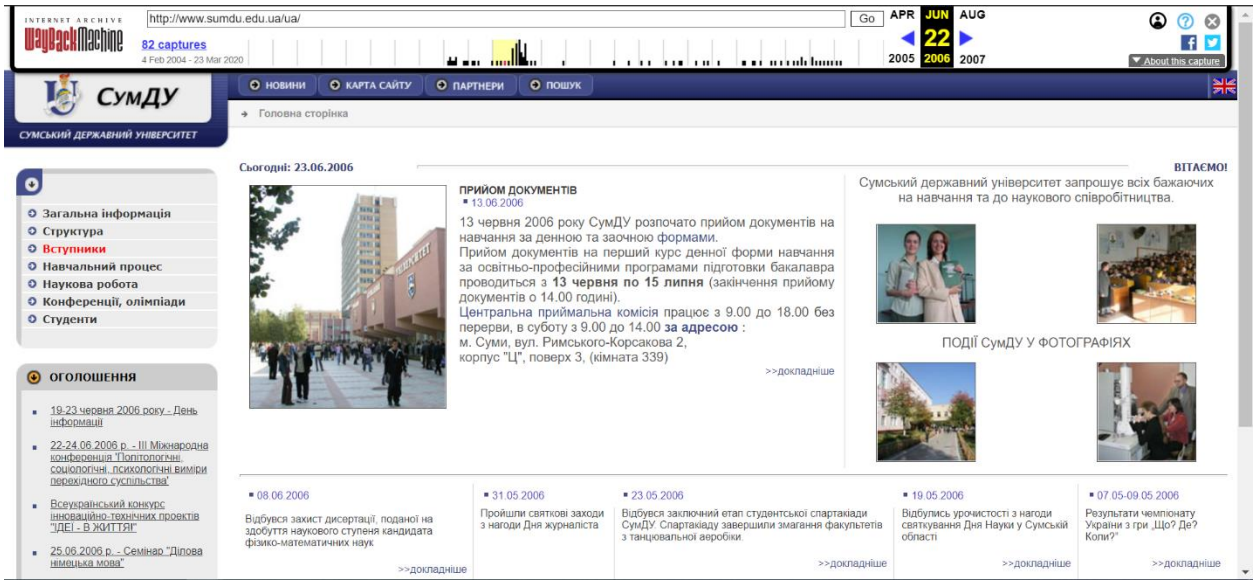

Рисунок 3.7 – Сайт СумДУ у 2006 році

Як очевидно, корпоративний веб-сайт є відмінним джерелом інформації для соціального інженера. Деякі з доступних речей більш очевидні, наприклад, контактні дані, ієрархія персоналу і мета бізнесу. Ці дані, а також інформація про клієнтів, постачальників і партнерів можуть бути використані для формування ефективних стратегій. Давайте відразу ж перейдемо до розгляду адрес електронної пошти, способів їх пошуку і їх значення для подібних взаємодій.

Адреси електронної пошти

Важливість отримання адрес електронної пошти мети в ході оцінки неможливо переоцінити, проте їх роздають без роздумів. Співробітники використовують їх для реєстрації на форумах, в інтернет-магазинах, соціальних мережах і навіть в особистих блогах. Чи є адреса електронної пошти частиною інформації, до якої слід ставитися більш серйозно?

Загальний досвід показує, що багато компаній не стежать за тим, що їх користувачі роблять з корпоративними адресами електронної пошти. Іноді краще призначати поштову скриньку тільки тим, кому він дійсно потрібний.

Чому ж соціальні інженери та до зацікавлені в такій, здавалося б, неважливою інформації?

Фішингові атаки

Фішингові атаки стали дуже популярними в сучасному ландшафті загроз. Причина цього може бути двоякою. По-перше, вони неймовірно прості у виконанні,

принаймні, за базовими стандартам. По-друге, люди потрапляють на подібні атаки майже кожен день. Схоже, це виграшна комбінація для будь-якого шахрая.

Інсайдерські знання

Збір адреси електронної пошти і подальше з'ясування того, де вона використовується в Інтернеті, може привести до отримання додаткової корисної інформації. Це може привести до створення власного приводу. Дзвінок в організацію під виглядом користувача, який не може увійти в свою поштову скриньку, може здатися банальністю, але цей спосіб має довгу історію успіху.

Умовні позначення адреси електронної пошти

Хоча про атаки на паролі згадується мимохіть, однак корпоративна адреса електронної пошти може стати справжньою «ногою» в двері.

Більшість організацій намагаються публікувати загальні поштові скриньки, такі як info@sumdu.edu.ua. Це ускладнює соціальному інженеру проведення будь-якого роду фішингових афер. Якщо вдається отримати доступ до адресою одного користувача, все змінюється. Тепер за допомогою LinkedIn можна отримати список всіх співробітників цільової компанії. Ці відомості можна використовувати для створення набагато більшого списку потенційних цільових адрес електронної пошти з достатнім ступенем впевненості в їх існуванні.

Тепер, коли ми розглянули кілька вагомих причин, за якими необхідно збирати корпоративні адреси електронної пошти, наведемо огляд того, як цього можна досягти.

Утиліта TheHarvester

Theharvester насправді виконує набагато більше, ніж просто знаходити потрібні адреси електронної пошти, він також знаходить піддомени, імена співробітників, х ости і відкриті порти. Мета створення цього інструменту полягала в тому, щоб забезпечити платформу для збору розвідданих у час тестування на проникнення. Інформація, яку він видає, як і раніше корисна для соціальних інженерів, можливо, навіть більше, ніж для тестерів проникнення.

Приклад запиту: theharvester -d pixar.com -b all

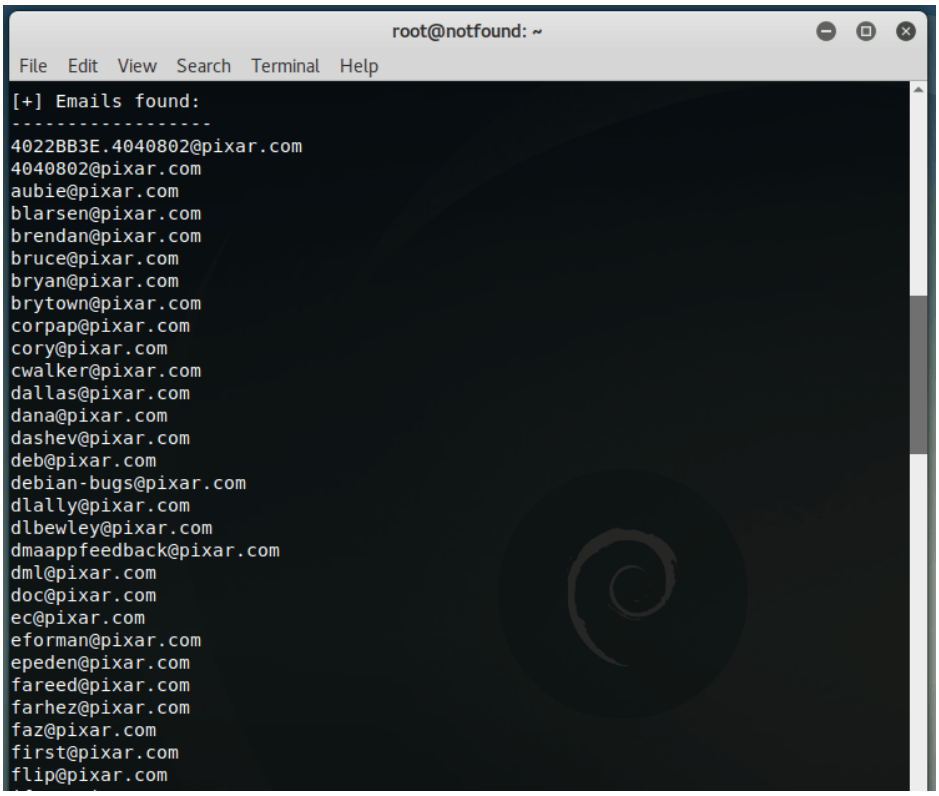

Рисунок 3.8 – Дані отримані за допомогою theHarvester

Утиліта Whois

До записів Whois часто можуть додаватися контакти адміністратора, технічного фахівця і реєстратора. Кожна з цих записів може містити адреси електронної пошти, які можуть бути додані в наш список. Команди Whois можна легко запускати з командного рядка linux :

```
susel:~ # whois -H linux-bible.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: LINUX-BIBLE.COM
   Registrar: LAUNCHPAD.COM, INC.
   Whois Server: whois.launchpad.com
   Referral URL: http://www.launchpad.com
   Name Server: NS6175.HOSTGATOR.COM
   Name Server: NS6176.HOSTGATOR.COM
   Status: clientTransferProhibited
   Updated Date: 16-may-2014
   Creation Date: 16-may-2014
   Expiration Date: 16-may-2015
   Registrant Name: Antun Peicevic
   Registrant Organization: 1
   Registrant Street: Nova cesta 1
   Registrant City: Zagreb
   Registrant State/Province: Zagreb
   Registrant Postal Code: 10000
   Registrant Country: HR
   Registrant Phone: +385.921021346
   Registrant Phone Ext:
   Registrant Fax:
   Registrant Fax Ext:
   Registrant Email: antunpeicevic@gmail.com
```

Рисунок 3.9 – Дані отримані за допомогою whois

Збір інформації за допомогою соціальних мереж

Кількість активних веб-сайтів соціальних мереж, а також кількість користувачів роблять це найкращим місцем для виявлення дружніх стосунків, спорідненостей, спільних інтересів, фінансових обмінів, симпатій / антипатій, сексуальних стосунків чи переконань. Можна навіть визначити корпоративні знання або престиж працівника.

- Facebook - https://www.facebook.com/
- LinkedIn - https://www.linkedin.com/
- Twitter - https://twitter.com/
- Вконтакте - https://vk.com/
- Instagram - https://www.instagram.com/
- Pinterest - https://www.pinterest.com/

Якщо ми знайшли профіль у одній соціальній мережі, ми зможемо знайти його у іншій, якщо нікнейми співпадають за допомогою сервісу https://checkusernames.com/

Враховуючи, що сайти соціальних мереж посилили свою гру, чи можуть соціальні інженери по-ін ежнему використовувати їх у своїх цілях? Щоб відповісти на це питання, ми розглянемо деякі з найбільш популярних сайтів соціальних мереж і виявимо корисні відомості.

Intelligence X

Інструмент для пошуку у Facebook, Twitter та LinkedIn, має ті ж функції, що і вбудований пошук у цих мережах але подає у більш зручному вигляді.

Ви можете шукати публікації від певної дати або місяця, публікації від конкретного користувача, можна також шукати публікації невідомих користувачів.

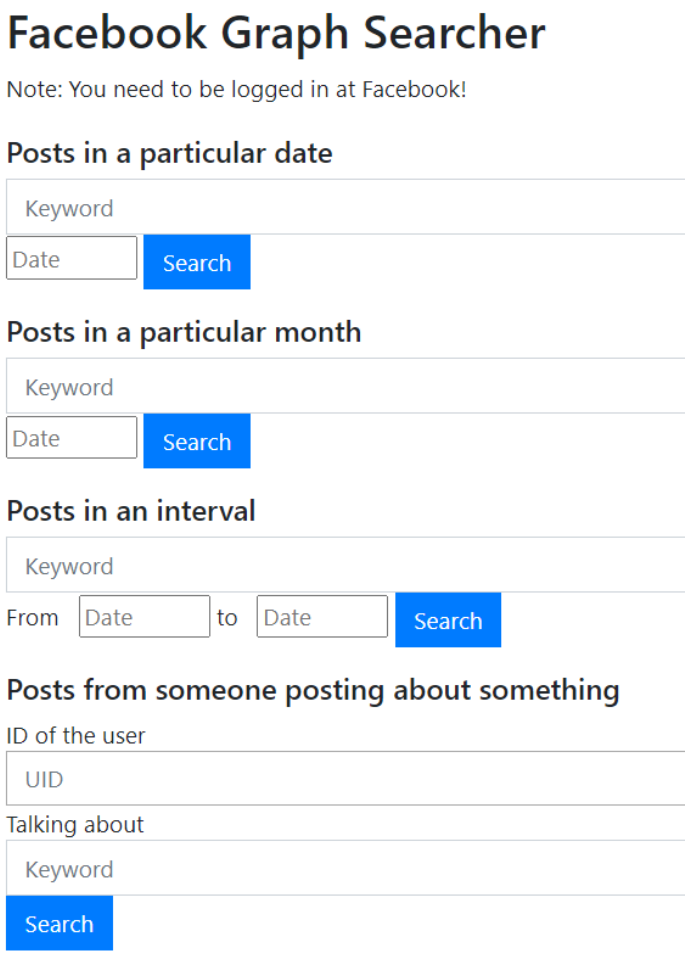

Рисунок 3.10 – Пошук у Facebook за допомогою Intelligence X

Cree.py

Cree.py - це інструмент, який використовується для автоматизації збору інформації з Twitter, а також FourSquare. Крім того, Cree.py може збирати будь-які геолокаційні дані з flickr, twitpic.com, yfrog.com, img.ly, plixi.com, twitrpix.com, foleext.com, shozu.com, pickhur.com, moby.to, twitsnaps.com та twitgoo.com. Cree.py - це програма для збору розвідданих з відкритим кодом. Щоб встановити Cree.py, вам потрібно буде додати сховище до вашого /etc/apt/sources.list.

echo "deb http://people.dsv.su.se/~kakavas/creepy/ binary /" >> /etc/apt/sources.list

Оновити список пакетів

apt-get update

Встановіть Cree.py

apt-get install Cree.py

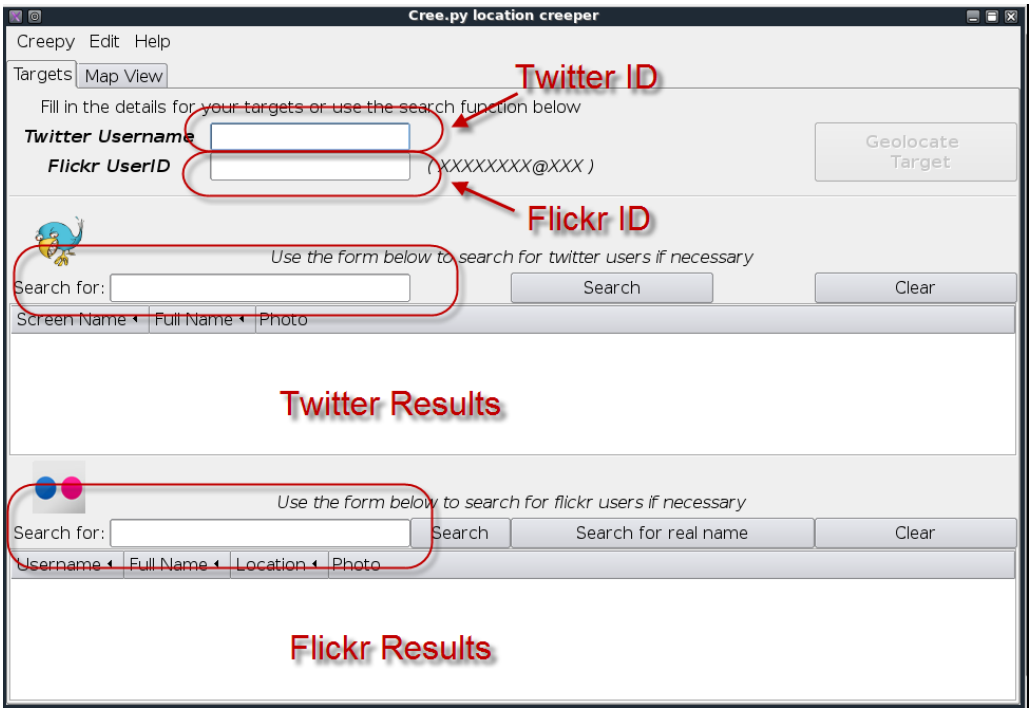

Рисунок 3.11 – Інтерфейс Cree.py

Cree.py в першу чергу орієнтована на інформацію про геолокацію про користувачів із платформ соціальних мереж та служб хостингу зображень. Інформація представлена на карті всередині програми, де відображаються всі отримані дані, а також відповідна інформація.

Збір з інших ресурсів

Інформація про конкретну ціль повинна включати інформацію щодо юридичної особи. Ця інформація може містити інформацію про акціонерів, членів, службових осіб чи інших осіб, які беруть участь у цільовій організації.

- https://usr.minjust.gov.ua/content/free-search
- https://youcontrol.com.ua

Місцезнаходження

Часто першим кроком у OSINT є визначення фізичного розташування цільової корпорації. Ця інформація може бути легко доступною для публічно відомих або опублікованих місць, але не настільки проста для більш секретних сайтів. Загальнодоступні сайти часто можуть знаходитись за допомогою пошукових систем, таких як:

- Google - http://www.google.com
- Yahoo - http://yahoo.com
- Bing - http://www.bing.com

Вакансії

Пошук поточних вакансій або розміщення оголошень через корпоративний веб-сайт або через систему пошуку роботи може надати цінне розуміння внутрішньої роботи цілі. Часто поширеною практикою є включення інформації про поточні або майбутні впровадження технологій. Існує декілька пошукових систем для пошуку роботи, щодо яких можна отримати інформацію щодо цілі [12].

- https://www.work.ua/
- https://rabota.ua/
- https://jobs.ua/
- https://ua.jooble.org/

Збір за допомогою фізичної розвідки

Якщо ваш тест на соціальну інженерію передбачає спробу отримати фізичний доступ до певного місця, вам доведеться зробити додаткову розвідку. Ви можете здійснити фізичну розвідку віддалено. Наприклад, використовуйте Карти Google і

Перегляд вулиць, щоб побачити, як виглядає місце розташування. Визначте входи та виходи та зазначте, що знаходиться навколо будівлі [13].

На якомусь етапі вам потрібно буде відвідати місце, куди ви намагаєтесь отримати доступ. У цьому випадку проведіть трохи часу біля будівлі, зібравши якомога більше інформації про неї. Шукайте таку інформацію:

- Де розташовані охоронці?
- Чи збираються курці у певній місцевості за межами?
- Де знаходяться камери відеоспостереження?
- Чи носить персонал та / або демонструє посвідчення особи? Чи можете ви їх скопіювати?
- Які інші види контролю існують для запобігання несанкціонованому доступу до будівлі (турнікети, картки доступу, введення пін-коду, навіть захисний дизайн ландшафту)?
- Слідкуйте за рухами персоналу. О котрій годині працівники прибувають або залишають офіс? О котрій годині вони обідають? Чи є вподобане кафе чи ресторан неподалік?
- Чи є в будівлю нестандартні шляхи, наприклад, пожежні сходи чи парковка

3.2.2. Аналіз вразливостей

Ідентифікація цілей

У описі методологій вже було розглянуто трикутник, за допомогою якого ми зможемо відсортувати цілі придатні для тестування. У цьому ж пункті ми розберемо окремо кожен його етап.

Розвідка з відкритим кодом

Для того, щоб ціль була перенесена на наступний рівень, вона повинна пройти ряд основних критеріїв. На першому рівні критерії ґрунтуються на розвідці відкритого джерела. Усунути велику кількість потенційних цілей можна виключно на основі інформації, яку ви зібрали віддалено, та на основі загальної мети атаки.

- Стаж у компанії

Вибір цілі з вищими привілеями, ніж інші, часто може бути вигідним. Однак, якщо ціль аудиту вимагає орієнтації на нових уразливих початківців, тоді все навпаки.

- Гарний цифровий слід

Якщо інформація про ціль обмежена, то і підґрунтя для акаки бути не може. Однак може бути прийнято рішення про розробку атак, які отримують цю інформацію, але для цього повинна бути вагома причина, оскільки це може зайняти час. Однак, якщо ціллю є генеральний директор, а дослідження виявило дуже мало інформації про нього, то атаки, призначені для отримання цієї інформації, можуть бути виправданими.

- У межах цільового відділу

Хоча теоретично будь-який працівник може надати дійсний пропуск, зазвичай це приймальна служба, тому має сенс просувати цілі в потрібному відділі.

Тут наведені лише основні критерії відбору, під час ідентифікації повинні бути додані критерії, що відповідають цілям аудиту. Також під час сортування не буває однозначного розділення, можна знайти багато інформації про людину, яка не допоможе нам досягти цілі перевірки, аудитор повинен індивідуально вирішувати про фільтрування окремих цілей.

Цільове профілювання

Наступний шар трикутника зосереджений на цільовому профілюванні. Попередні критерії включали хороший цифровий слід; про кожну ціль має бути достатньо інформації для прийняття рішень. На даний момент рішення приймаються, виходячи з індивідуальних особливостей цілі. Очевидно, ці характеристики не гарантують успіху; ідея просто збільшити шанси на успіх на основі узагальнень. Наприклад, фішингова електронна пошта, мабуть, мала б більше успіху для людей похилого віку, ніж для молодого покоління. Ключовим терміном тут є "мабуть".

- Вік

Певні атаки можуть бути більш успішними залежно від віку цілі. Однак, хоча тенденція полягає в придирці до людей похилого віку, оскільки вони рідше володіють комп’ютерною грамотністю, будьте дуже обережні, щоб не витрачати дорогоцінний час. Якщо метою було маніпулювати ціллю для розкриття інформації, то, можливо, буде кращим рішенням вибрати молодшого нового сажиста, а не загартованого

колишнього військового. Важливо ретельно продумати мету і те, як критерії повинні впливати на будь-яке рішення щодо просування або усунення цілі.

- Стать

Сценарій може бути гендерно орієнтовним, в залежності від мети аудиту. Тому потрібно користуватися схильністю людей мислити стереотипно.

- Інтереси

Якщо дослідження виявило, що ціль має багато інтересів, то ця інформація може бути використана проти них.

Фізична розвідка

Третій шар трикутника віддаляється від дистанційної розвідки і фокусується на цілях і на тому, як вони співвідносяться з метою аудиту.

- Моделі поведінки

Ці критерії можуть означати дуже різні речі залежно від мети. Тут описуються повсякденні дії працівника на робочому місці, наприклад, куди та з ким йде на перерву.

- Фізична прихована взаємодія

Фізичне прихована взаємодія може означати фотографування або запис цілі для збору інформації. Цей рівень залучення, як правило, не є необхідним для більшості оцінок соціальної інженерії, він включений сюди просто для детальної демонстрації процесу.

- Залучення партнерів

У ході вивчення цілей має стати зрозумілим, хто з ким взаємодіє. Це важливо знати для побудови сценарію, щоб не під час тестування не виявити, що ціль та той кого ми вдаємо близькі друзі.

Цільове залучення

Останній шар розкриває найкращі цілі для атаки на основі всієї зібраної інформації.

- Розставити пріоритети на цілі

Існуватимуть відмінності між кінцевими цілями в загальному плані. Наприклад, один, можливо, відповідав більшій кількості критеріїв, ніж інший, отже, є гарною

ідеєю визначити пріоритети цілей і сконцентруватися спочатку на найбільш перспективних.

- Створення сценарію

Тепер, коли ціль або цілі були визначені, настав час розробити відповідний сценарій соціальної інженерії.

- Відверта участь

Це заключний етап взаємодії з ціллю: фактичне виконання сценарію соціальної інженерії.

Пам’ятайте, що є вірогідність досягти цього етапу, а потім зрозуміти, що кінцева ціль насправді непридатна. Або після виконання сценаріїв ви можете атакувати інші цілі. У цих випадках основна увага приділяється наступному шару вниз у трикутнику, переглядаючи попередньо усунені цілі. Слідуючи цьому процесу, на правильних людей націлюються у правильній послідовності, використовуючи відведений час якомога ефективніше [11].

Створення сценарію впровадження атаки

Хоча створення сценарію є цілком творчим етапом, який не можна буде зробити за єдиним алгоритмом, у цьому розділі ми розглянемо методи, що допоможуть аудитору їх створити.

Сценарій - це історія, яка пояснює, хто ви і навіщо вам потрібна інформація, яку ви вимагаєте; це навіть впливає на ваше ставлення під час виконання тесту. Ви будете використовувати свій придуманий сценарій, щоб переконати свою цільову особу виконати певну дію.

Для створення персонажу потрібно намагатися бути такою людиною, якій хочуть допомогти. Враховуйте тип особи, якій міг би допомогти ваш об’єкт. Можливо, ціль допоможе людині, подібній до неї самої.

Для комп’ютерних атак є можливість не прописувати персонажа детально, адже при листуванні є час, щоб підлаштуватися під умови, але якщо обрано атаку з фізичним доступом до системи, персонажа потрібно створювати з подробицями, тому було підготовлено список питань, що можуть допомогти під час створення [13]:

1. Як звати вашого персонажа?

2. Напишіть фізичний опис. Яку поставу має ваш персонаж? Як він ходить?
3. Опишіть зовнішній вигляд вашого персонажа. Який одяг носить ваш персонаж? Дорогий чи недорогий?
4. Опишіть мовлення свого персонажа: швидкість розмови, діалект, часто вживані слова
5. Опишіть манери вашого персонажа (круто/впевнено/нервово/сором'язливо/інше).
6. Дрібні звички персонажа (кусає нігті, барабанить пальцями, грає волоссям)?
7. Звідки ваш персонаж?
8. Які заняття у вашого персонажа і де він працює?
9. Чим цей персонаж відрізняється від вас?
10. Чим цей персонаж схожий на вас?
11. Чому людям подобається / не подобається цей персонаж?
12. Який рівень задоволеності персонажем від роботи?

3.2.3. Проникнення

В цьому розділі розглянемо процес впровадження різних видів атак на практиці.

Фішинг

Фішинг атака починається з надсилання електронного листа. Ми розглянемо інструменти, які допоможуть замаскувати відправника, та створити шкідливий вміст фішинг-листа.

Спочатку ми отримуємо MX DNS запис сервера нашого одержувача. Беремо те, що йде після @, і пишемо в консолі «nslookup -type = mx target.com».

```
$ nslookup -type=mx yandex.ru
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
yandex.ru       mail exchanger = 10 mx.yandex.ru.

Authoritative answers can be found from:
```

Рисунок 3.12 – Отримання MX DNS записів

Потім підключаємося до 25-го порту отриманого сервера. Для цього можна використовувати ncat. Після привітання від сервера ми пишемо:

HELO any_text – Це наше вітання.

MAIL FROM: any_name@any_host.com – Тут ми повинні вказати, від кого лист.

RCPT TO: victim@target.com – Адресат листа.

DATA – Переходимо до тіла повідомлення.

To: victim@target.com – Поле «Кому» в поштовому клієнті.

From: any_name@any_host.com – Поле «Від кого». Ці дані будуть відображатись у адресата.

Subject: blah-blah – Поле «Тема».

Далі через рядок ми пишемо текст нашого повідомлення, а в кінці ставимо крапку і перенесення для закінчення команди DATA [14].

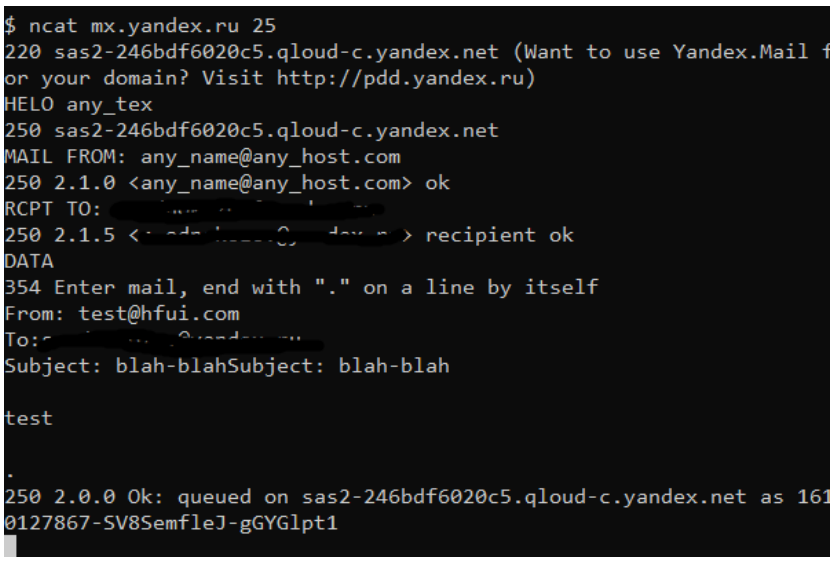

Рисунок 3.13 – Створення листа

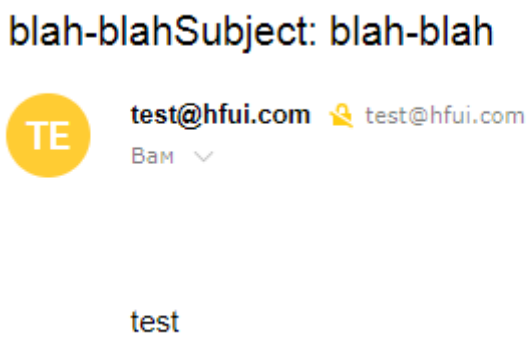

Рисунок 3.14 – Отриманий лист

Розглянемо створення фішингового сайту за допомогою інструменту Social Engineering Toolkit.

Аудитор робить наступним чином: вибирає пункт Social-Engineering Attacks (Соціально-технічні атаки), потім – Website Attack Vectors (Вектори веб-сайтів), після цього - Credential Harvester Attack Method (Спосіб атаки на харвестер). З'явиться три пункти меню: 1) Шаблони веб сайтів; 2) Клонування сайтів; 3) для користувача імпорт.

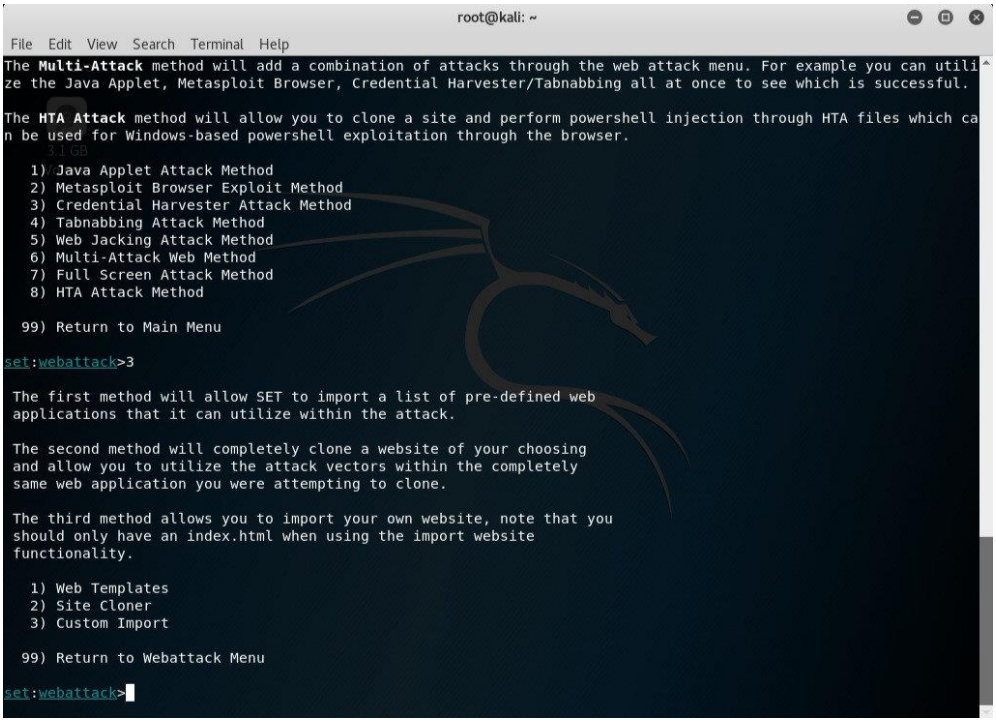

Рисунок 3.15 – Харвестерний тип вектору атаки

Далі аудитор дізнається тип свого мережевого адреси, так Social-Engineer Toolkit знатиме, куди перенаправляти всю зібрану інформацію. Для цього вводиться команда ifconfig. В даному випадку це адреса 192.168.0.20 (IP-адреса, що присвоюється вашому інтерфейсу). Приклад з соціальною мережею ВКонтакті показаний нижче на малюнку.

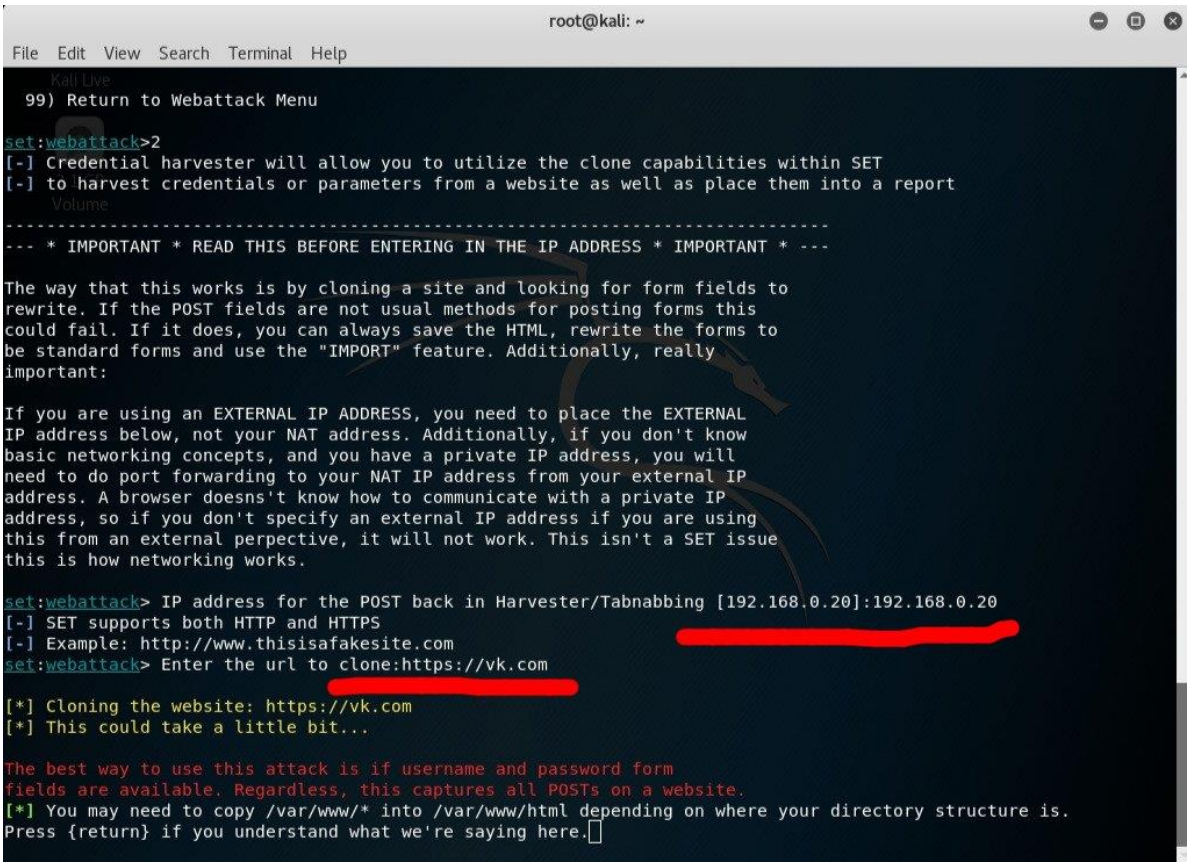

Рисунок 3.16 – Введення мережевої адреси та клонування сайту

Після завершення конфігурації зловмисник використовує стандартний сервіс для конвертації посилання і відправляє її жертві. Після переходу за посиланням користувач бачить знайомий інтерфейс. Однак подивившись в адресний рядок, можна звернути увагу, що замість звичного адреси там зазначено той самий 192.168.0.20. Через неуважність багато хто просто не звертають на це увагу і вводять свої логін і пароль.

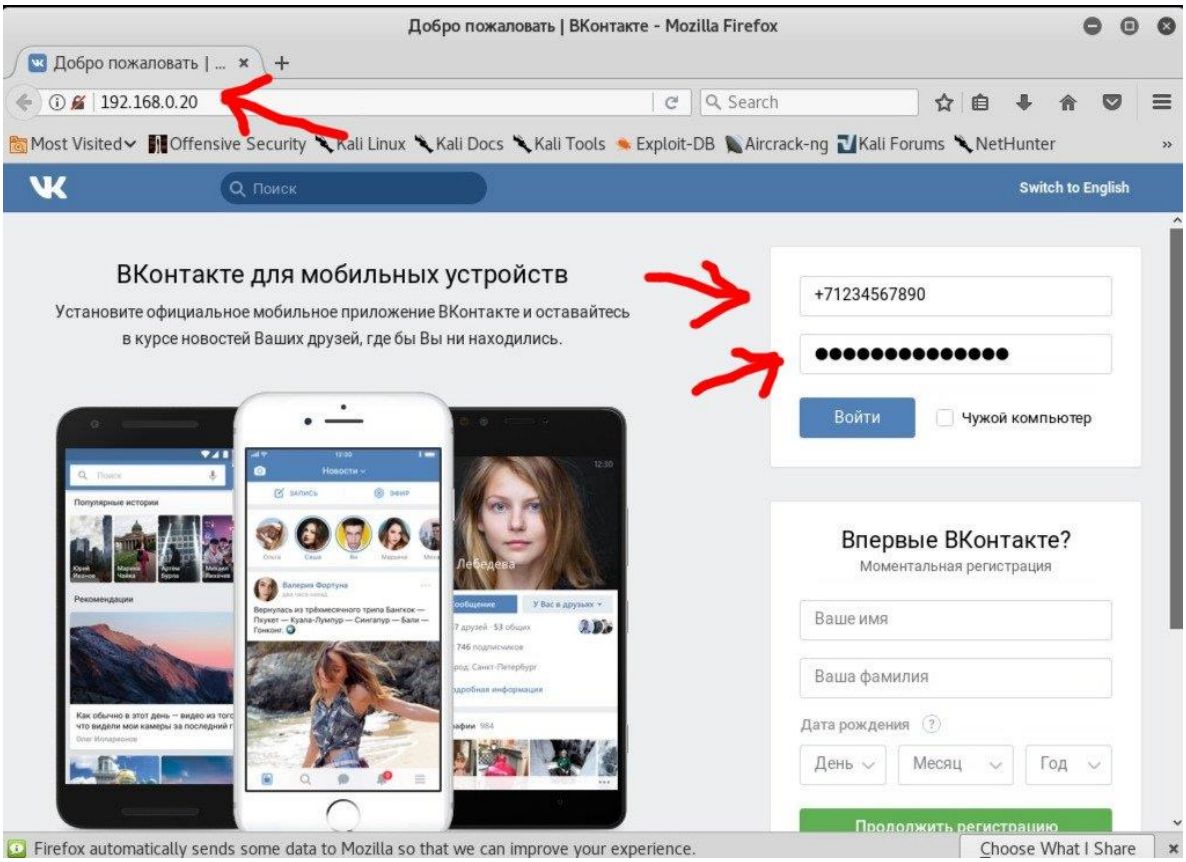

Рисунок 3.17 – Вид підробної сторінки

Після введення своїх конфіденційних даних, система пропонує жертві зайти пізніше, нібито стався якийсь збій або пара логін-пароль не знайдена [15].

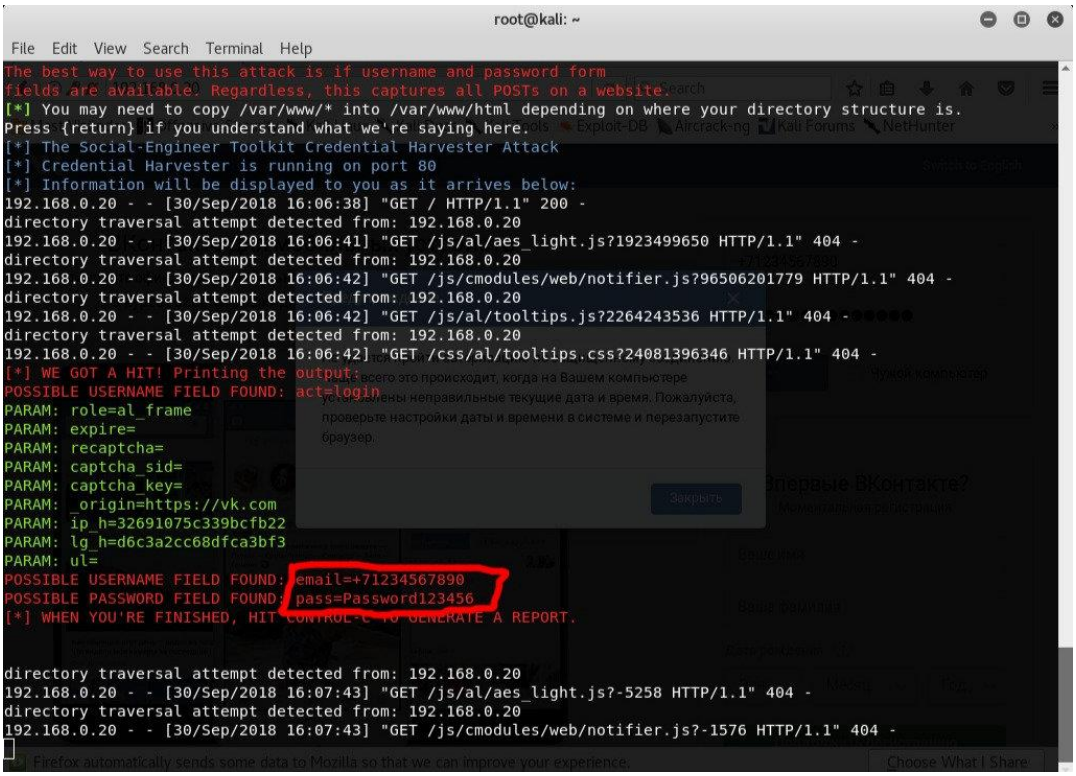

Рисунок 3.18 – Кінцевий результат – злодій отримує логін та пароль

Фішінг Wifi

Для фішингу Wifi використовується утиліта для Kali Linux – Wifiphisher. Утиліта виконує наступні дії:

- Відключає користувача від справжньої точки доступу.
- Дозволяє підключитися до підробленої точки доступу.
- Демонструє користувачеві веб-сторінку, яка надіслала повідомлення про необхідність повторного введення облікових даних.
- Передає хакеру пароль від Wi-Fi, в той час як нічого не підозрюючи користувач продовжує спокійно користуватися інтернетом.

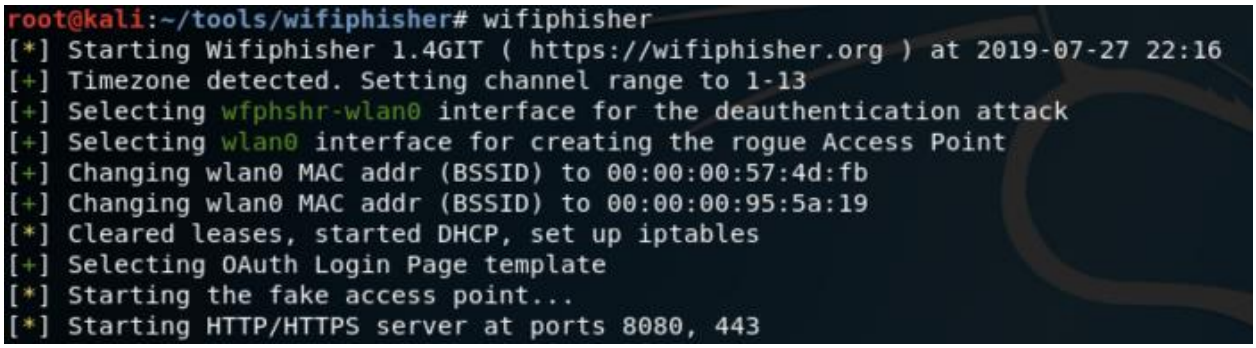

Рисунок 3.19 – Початок роботи з Wifiphisher

Далі відкриється вікно, в якому видно, які мережі Wi-Fi є поблизу:

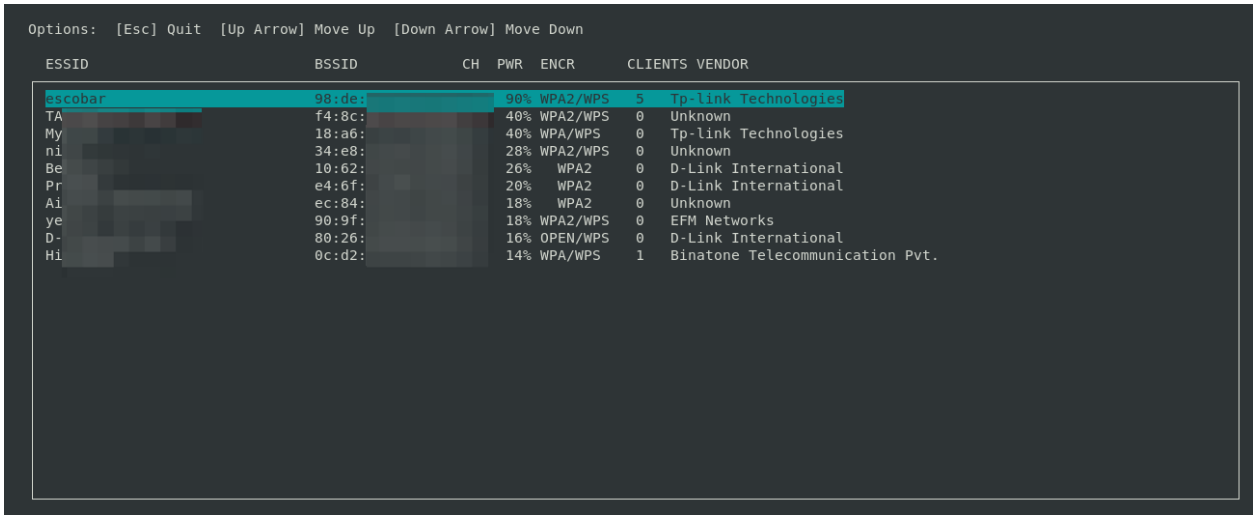

Рисунок 3.20 – Список доступних точок доступу

Вибираємо потрібну точку доступу, натиснувши клавішу ENTER. Як тільки це буде зроблено, відбудеться перенаправлення на сторінку, де почнеться атака, яка буде виглядати приблизно так:

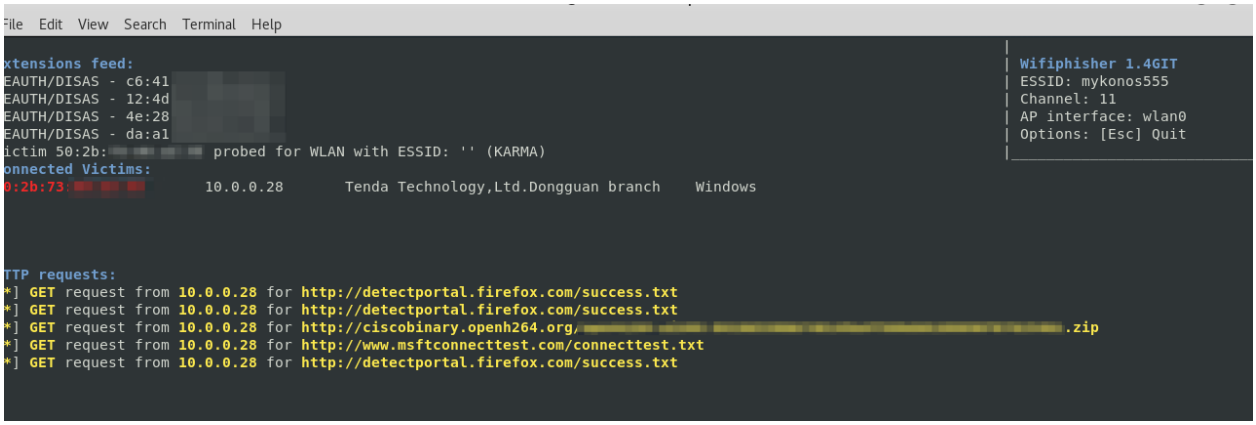

Рисунок 3.21 – Виконання атаки Wifiphisher

Після натискання клавіші Enter, буде відбуватися безпосередньо клонування SSID і атака обраної точки доступу.

У цей момент всі користувачі, будуть відключені від оригінальної точки, а під час спроби повторного підключення перенаправлені на нашу підроблену.

Після цього спеціальний проксі на веб-сервері перехопить запит і підсуне користувачу підроблену сторінку входу, інформуючи про встановлення нової версії прошивки маршрутизатора і необхідності повторної аутентифікації .

Коли користувач введе свій пароль, він буде переданий вам через відкритий термінал Wifiphisher. Потім утиліта пропустить користувача в інтернет через вашу систему, щоб він нічого не запідозрив.

Фізичний доступ

Розглянемо пристрої, що використовуються під час атаки з отриманням фізичного доступу до системи клієнта.

Keylogger

Апаратні кейлоггери використовуються для реєстрації натискань клавіш , методу фіксації та запису натискань клавіш користувачів комп'ютера, включаючи конфіденційні паролі. Вони можуть бути реалізовані за допомогою мікропрограмного забезпечення рівня BIOS , або, за допомогою пристрою, підключеного вбудовано між клавіатурою комп'ютера та комп'ютером. Вони реєструють усі дії клавіатури у свою внутрішню пам’ять.

Однією з найбільш поширених атак є Badusb, логер під видом накопичувача з автозапуском можна просто залишити на видному місці та чекати, коли хтось його перевірить на своєму комп’ютері [8].

Рисунок 3.22 – Логер замаскований під накопичувач

Пристрої запису

Існує низка фізичних інструментів, які ви можете розглянути, використовуючи як частину тесту соціальної інженерії. Більшість із них належать до категорії записуючих пристроїв.

ВИСНОВКИ

Соціальна інженерія – це методологія злому людини, а саме, використання довіри та корисності людини для нападу на мережу та її пристрої.

У ході даної роботи було розглянуто, як соціальна інженерія застосовується для атак, призначених для збирання облікових даних мережі, активації шкідливого програмного забезпечення або допомоги у запуску подальших атак. Більшість атак залежать від Social Engineering Toolkit. Однак у Kali є ще кілька додатків, які можна вдосконалити за допомогою методології соціальної інженерії. Ми також дослідили, як фізичний доступ, як правило, спільно з соціальною інженерією, може бути використаний для розміщення ворожих пристроїв у цільовій мережі.

Також було розглянуто актуальність проведення аудиту компанії на схильність до атак соціальної інженерії, шляхом розгляду актуальної статистики з ураження даним видом атаки.

Були досліджені актуальні на даний момент методики проведення аудиту, для того щоб у подальшій розробці скористатися їх сильними сторонами та уникнути слабких.

Створена методика проведення аудиту на схильність до атак методами соціальної інженері, що складається з трьох основних етапів. На першому відбувається планування аудиту с клієнтом. На другом проводиться комплексна оцінка, проводиться збір інформації з відкритих джерел, аналіз виявлених вразливостей та їх експлуатація.

Також було створено практичне керівництво етапу оцінки. Покроково розглянуто використання інструментарію, що допоможе впроваджувати розроблену методику на практиці. Її можуть використовувати або всередині компанії, або компанії, що займаються тестуванням на проникнення.

СПИСОК ЛІТЕРАТУРИ

1. Мітник К. Мистецтво обману / К. Мітник. – John Wiley & Sons, 2002. – 304 с.
2. ptsecurity.com: [Electronic resource]. – Access mode: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q4/
3. owasp.org: [Electronic resource]. – Access mode : https://owasp.org/project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf
4. isecom.org: [Electronic resource]. – Access mode: https://www.isecom.org/OSSTMM.3.pdf
5. cuchillac.net: [Electronic resource]. – Access mode: http://cuchillac.net/archivos/pre_seguridad_pymes/2_hakeo_etico/lects/metodologia_oissg.pdf
6. pentest-standard.org: [Electronic resource]. – Access mode: http://www.pentest-standard.org/index.php/Main_Page
7. Парасрам Ш. Kali Linux. Тестування на проникнення і безпеку / Ш. Парасрам // Санкт-Петербург: Пітер, 2020. – 448 с.
8. Віджай К. Освоєння Kali Linux для розширеного тестування на проникнення / К. Віджай. – Бермінгем: Packt Publishing Ltd, 2017. – 485 с.
9. linuxhint.com: [Electronic resource]. – Access mode: https://linuxhint.com/social_engineering_tools_kali_linux_2020-1/
10. intercert.com.ua: [Electronic resource]. – Access mode: https://intercert.com.ua/articles/regulatory-documents/210-iso-27000
11. Ватсон Дж., Мейсон Е. Тестування на проникнення в соціальну інженерію: виконання тестів, оцінок та захисту соціальної інженерії / Дж. Ватсон, Е. Мейсон. – Syngress, 2014. – 386 с.
12. osintframework.com: [Electronic resource]. – Access mode: https://osintframework.com/
13. Конхіді Ш. Соціальна інженерія в галузі IT-безпеки: інструменти, тактика та методи / Конхіді Ш. – McGraw-Hill Education, 2014. – 272 с.

14. xakep.ru: [Electronic resource]. – Access mode: https://xakep.ru/2014/03/05/easy-hack-182/
15. Діогенес Ю., Озкая Е. Кібербезпека - атака і оборонні стратегії / Ю. Діогенес, Е. Озкая. – Бірмінгем: Packt Publishing Ltd, 2018. – 354 с.