**Національний технічний університет України**

**«Київський політехнчний інститут імені Ігоря Сікорського»**

**Навчально-науковий інститут атомної та теплової енергетики**

**Кафедра цифрових технологій в енергетиці**

**Звіт**

**з лабораторної роботи №1**

**з дисципліни «Безпека інформаційних систем»**

Виконав:

студент групи ТР-23

Ровний Г.О.

КИЇВ - 2024

**Частина 1.**

Тема 1. «Дослідження та виявлення атак соціальної інженерії»

**Мета роботи:**

лабораторна робота спрямована на набуття навичок дослідження особливостей атак типу соціальної інженерії та визначення способів розпізнавання та запобігання подібного типу атак.

**Поставлене завдання:**

За допомогою веб-браузера зверніться до офіційного веб-сайту SANS Institute (https://www.sans.org/) та скористайтеся їхньою пошуковою функцією для знаходження статей з теми соціальної інженерії.

Спеціалізовані розділи або блоги з інформаційної безпеки також можуть містити цікаві матеріали.

Інститут SANS — це спільна науково-освітня організація, яка пропонує навчання з інформаційної безпеки та сертифікацію з безпеки. Офіційний веб-сайт SANS містить багато статей, які стосуються практики аналізу кібербезпеки. Ви можете приєднатися до спільноти SANS, створивши безкоштовний обліковий запис користувача для доступу до останніх статей, або ви можете отримати доступ до старіших статей без облікового запису користувача.

Оберіть одну або декілька статей для дослідження теми соціальної інженерії. Зверніть увагу на дату публікації, автора статті, а також на основні методи та стратегії, які вони рекомендують для розуміння та зменшення атак соціальної інженерії. Перевірте, чи є підтвердження з наукового погляду та чи є стаття відомим джерелом в галузі інформаційної безпеки.

Якщо ви не знайдете конкретну статтю на веб-сайті SANS Institute, розгляньте аналогічні статті на інших визнаних ресурсах, таких як CERT, OWASP, або інші відомі інституції, які спеціалізуються в інформаційній безпеці. Після чого, підготуйте змістовні відповіді на наступні запитання

**Використані джерела:**

1. https://sansorg.egnyte.com/dl/ICNsgzn5Hp
2. <https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attack>
3. <https://www.sans.org/blog/why-strong-security-culture/>
4. <https://sansorg.egnyte.com/dl/a3SWCBUAOz>
5. <https://www.thinkhdi.com/library/supportworld/2021/what-to-know-about-social-engineering-for-cyberhackin>
6. <https://www.tessian.com/blog/examples-of-social-engineering-attacks/>
7. <https://www.namecheap.com/blog/social-engineering-social-media/>

**Результат виконання роботи**

1. Які основні характеристики визначають соціальну інженерію як метод кібератак?

Соціальна інженерія – це метод атаки, який сильно спирається на людську взаємодію і часто включає обман людей, щоб порушити нормальні процедури безпеки. Основним елементом будь-якої атаки соціальної інженерії є обман. Атакуючий повинен обманути, представляючи себе кимось (довіреною особою), або, у випадку фішингу, обманути користувача, змусивши його думати, що повідомлення містить правдиву інформацію, коли насправді воно призначене для отримання доступу до конфіденційної інформації.

1. Як визначається «інженерія соціальних інтеракцій» та як вона використовується у сфері кібербезпеки?

Інженерія соціальних інтеракцій - метод, який використовується для впливу на поведінку людей з метою отримання необхідної інформації, доступу до ресурсів або виконання певних дій. У сфері кібербезпеки використовують психологічну маніпуляцію, людські помилки або слабкості, а не технічні або цифрові системні вразливості. Зловмисники часто використовують тактику соціальної інженерії для отримання особистих даних - логінів, номерів кредитних карт, номерів банківських рахунків і т.д., які вони можуть використовувати для крадіжки особистості Але варто враховувати, що така атака також може бути першим етапом більш масштабної кібератаки.

1. Які психологічні та соціальні аспекти використовуються в атаках соціальної інженерії?

Соціальна інженерія ґрунтується на обмані та маніпуляції людськими емоціями, мотивами або слабкостями. Для цього люди використовують різні психологічні техніки, такі як створення умов терміновості, викликання довіри, використання авторитету, або також можуть бути застосовані соціальні фактори, такі як норми поведінки, груповий тиск, соціальні мережі та особисті інтереси.

4. Які основні етапи використовуються при проведенні атак соціальної інженерії?

Зазвичай відокремлюють чотири етами: дослідження цілі, розробку плану атаки, встановлення довіри, експлуатацію довіри та виконання атаки.

5. Як соціальна інженерія може бути використана для обходу технічних заходів безпеки?

Використовуючи людський фактор: наприклад зловмисник може переконати співробітника якоїсь компанії перейти за шкідливим посиланням, або відкрити шкідливий файл/ресурс та отримати доступ до конфіденційної інформації.

6. Як оцінити ризики в сфері соціальної інженерії для конкретної організації?

Для оцінок ризиків в сфері соціальної інженерії можна проаналізувати наступні фактори:

Аналіз людського фактору – для визначення рівня свідомості та поведінки співробітників щодо соціальної інженерії.

Виявлення слабких місць в технічних, фізичних та організаційних заходах безпеки, які можуть бути використані соціальними інженерами.

Тестування на вразливість ПЗ або проведення аудитів безпеки дадуть можливість проведення симульованих атак на різних каналах комунікації для перевірки ефективності заходів безпеки.

7. Чому важливо навчання персоналу для запобігання атакам соціальної інженерії?

Навчання персоналу може допомогти зменшити ймовірність такого виду атак. Надаючи співробітникам інформацію про різні види, методи та підходи соціальної інженерії, а також про способи їх виявлення, запобігання та реагування сприяє формуванню культури безпеки в організації, залучаючи співробітників до спільної відповідальності за захист інформації та ресурсів.

8. Які типи інформації є особливо цінними для зловмисників, які використовують соціальну інженерію?

Загалом зловмисники намагаються в першу чергу отримати інформацію про облікові дані, куди входять юзернейми, пін-коди, ключі/токени доступу. Такого роду дані можуть бути використані для враження безпеки інформаційних систем. Також дані про особисту інформацію можуть бути використаними для шантажу, шпигунстві саботажу тощо.

9. Які заходи безпеки можуть запобігти фішинговим атакам, що базуються на соціальній інженерії?

Для запобігання фішинговим атакам можна використовувати антивірусне програмне забеспечення, використання фільтру повідомлень на електронній пошті для запобігання фішингового спаму, а також перевірка надійності джерела та відстеження інформації в інтернеті про останні атаки таких типів.

10. Як організації можуть створити культуру безпеки, яка враховує аспекти соціальної інженерії?

Культуру безпеки можна створити створивши середовище, в якому люди будуть відчувати себе безпечно, повідомляючи про інциденти, навіть якщо вони їх спричинили; де співробітники включать охорону як частину своєї посадової інструкції, і допомагають своїм колегам бути більш захищеними; де співробітникам проводять інструктажі безпеки, а також залучають служби безпеки до створення своїх проектів.

11. Які нові тренди чи методи в атаках соціальної інженерії можуть з'явитися в майбутньому?

З розвитком ШІ та нейромереж, цілком ймовіно що в майбутньому його будуть використовувати як мінімум для вироблення максимально правдивих фейків, або підробки інформації.

12. Як збільшити обізнаність персоналу щодо загроз соціальної інженерії та вдосконалити їхні навички виявлення?

Проведення тренінгів та аудитів із запобігання атак соціальної інженерії, а також проходження спеціалізованих курсів з приводу таких атак або постійне підіймання цього питання може збільшити обізнаність персоналу щодо цих загроз.

13. Які три способи використовуються у соціальній інженерії для отримання доступу до інформації?

Фішинг (виманювання конфіденційної інформації шляхом маскування під надійний суб’єкт), претекстинг (створення ситуації пов’язаної з терміновістю, що змушує надавати важливу інформацію) а також шантажування/цькування або все інше, що може викликати емоції (іншими словами маніпуляція емоціями).

14. Які три конкретні приклади атак соціальної інженерії відповідають першим двом методам, про які було сказано у попередньому запитанні?

**Атака на Google та Facebook:** Литовський громадянин Evaldas Rimasauskas створив фальшиву компанію, яка нібито працювала з Google та Facebook. Він також відкрив банківські рахунки на ім’я цієї компанії. Зловмисники відправляли фішингові листи конкретним співробітникам Google та Facebook, виставляючи рахунки за товари та послуги, які виробник дійсно надав, але направляючи їх на внесення грошей на свої шахрайські рахунки. Між 2013 та 2015 роками Rimasauskas та його співробітники обманули дві технологічні гіганти на суму понад 100 мільйонів доларів.

**Телефонний дзвінок з банку**: Зловмисник телефонує жертві, видаючи себе за представника банку. Він створює правдоподібний привід, наприклад, підозрілу активність на рахунку, і просить жертву підтвердити особисті дані, такі як PIN-код або номер картки тощо.

**Працівник техпідтримки**:

Зловмисник телефонує жертві, видаючи себе за службовця техпідтримки відомої компанії. Він повідомляє про проблему з комп'ютером або програмним забезпеченням жертви і пропонує допомогу. Для "виправлення" проблеми зловмисник просить жертву надати доступ до комп'ютера або встановити шкідливе програмне забезпечення.

15. Які загрози в сфері соціальної інженерії представляють соціальні мережі?

Зловмисники можуть скопіювати профіль користувача в соціальній мережі та розміщувати повідомлення, від імені цього користувача, або відправляти приватні повідомлення всім його контактам. Часто шахраю навіть не потрібен доступу до акаунту, вони можуть створити дуже переконливу копію акаунту, використавши фото профілю жертви або іншу публічну інформацію.

Також це може бути цільове шахрайство, коли ваша інформація розміщена в публічному доступі може бути використана проти вас

16. Як організація або компанія може забезпечити свій захист від атак соціальної інженерії?

Використання багатофакторної авторизації а також токенів доступу, підвищення фільтрації спаму через шлюзи електронної пошти, періодичне проведення тестових атак на власні сервіси з використанням методів соціальної інженерії, навчання з кібербезпеки – це одне з небатьох що може забезпечити додатковий захост від такого роду атак.

**Висновок:**

Завдяки дослідженням, виявленню та активній протидії можна значно зменшити ризики, пов'язані з атаками соціальної інженерії.

**Частина 2.**

Тема 2. «Дослідження мережевих атак та особливостей аудиту безпеки»

**Мета роботи:**

лабораторна робота спрямована на набуття навичок дослідження різних мережевих атак, векторів атак та особливостей їх реалізації, також спрямована на дослідження інструментів аудиту безпеки мережі.

**Поставлене завдання:**

1) Дослідження мережевих атак. У цій частині студенту необхідно дослідити особливості атак на мережі, які вже сталися. Необхідно обрати три відомі мережеві атаки та ретельно описати, як вони були виконані, які були наслідки та якими методами можна запобігти розповсюдженню подібних атак у майбутньому (заповнити Таблицю 1 та Таблицю 2 відповідно)

2) Дослідження інструментів аудиту безпеки. У цій частині студенту необхідно дослідити інструменти для аудиту безпеки мережі та інструменти, що використовуються при проведенні атак. Необхідно розглянути можливість використання одного з таких інструментів для ідентифікації слабких місць в хостах чи мережевих пристроях. Підготувати змістовний огляд (резюме) обраного інструменту (заповнити Таблицю 3) та підготувати презентацію для захисту Лабораторної роботи №1.

**Результат виконання роботи –** <https://docs.google.com/presentation/d/1TRE0VPOn4nnrJG4qo6EF43oRaok7cuLIrZy8F8XNgts/edit?usp=sharing>