Lucrarea de laborator nr. 2

Inginerie socială și factorul uman

Scop

Scopul lucrării este studierea principalelor tehnici de inginerie socială și evaluarea vulnerabilității factorului uman în contextul securității informaționale, prin analiza și simularea unui scenariu de atac.

Cerință generală

Studiați principalele tehnici de **inginerie socială** și analizați modul în care acestea exploatează comportamentul uman. Pe baza cunoștințelor acumulate, elaborați un **scenariu de atac simulat** și evaluați riscurile asociate.

Cerințe obligatorii

1. Clasificarea tehnicilor de inginerie socială

Descrieți următoarele tehnici:

- phishing;
- pretexting;
- baiting;
- tailgating.

Pentru fiecare tehnică indicați:

- descrierea generală;
- scopul atacatorului;
- tipul de victimă vizat.

2. Alegerea unui scenariu de atac (simulat)

Alegeți **o singură tehnică** dintre cele analizate și construiți un **scenariu ipotetic de atac**, specificând:

- contextul (organizație, domeniu, utilizator);
- rolul atacatorului;
- rolul victimei;
- obiectivul atacului (obținerea de date, acces, informații sensibile).

3. Analiza vulnerabilității factorului uman

Analizați ce factori umani sunt exploatați în scenariul ales, de exemplu:

- lipsa de atenție;
- încrederea excesivă;
- presiunea timpului;
- necunoașterea regulilor de securitate;
- autoritatea aparentă.

4. Evaluarea riscurilor

Evaluați riscurile asociate scenariului propus, indicând:

- ce tipuri de date pot fi compromise;
- impactul potențial asupra organizației;
- componentele triadei CID afectate (Confidențialitate, Integritate, Disponibilitate).

5. Măsuri de conștientizare și prevenire

Propuneți **minimum 5 măsuri** de prevenire și conștientizare care ar reduce riscul unui astfel de atac, de exemplu:

- instruiri de securitate;
- politici interne;
- simulări de phishing;
- reguli de acces fizic;
- proceduri de verificare a identității.

Лабораторная работа №2

Социальная инженерия и человеческий фактор

Цель работы

Целью данной лабораторной работы является изучение основных техник социальной инженерии и оценка уязвимости человеческого фактора в контексте информационной безопасности посредством анализа и моделирования сценария атаки.

Общее требование

Изучите основные техники социальной инженерии и проанализируйте, каким образом они используют особенности человеческого поведения. На основе полученных знаний разработайте **смоделированный сценарий атаки** и оцените связанные с ним риски.

Обязательные требования

1. Классификация техник социальной инженерии

Опишите следующие техники:

- phishing;
- pretexting;
- baiting;
- tailgating.

Для каждой техники укажите:

- общее описание;
- цель атакующего;
- тип предполагаемой жертвы.

2. Выбор сценария атаки (смоделированного)

Выберите **одну** из проанализированных техник и разработайте **гипотетический сценарий атаки**, указав:

- контекст (организация, сфера деятельности, пользователь);
- роль атакующего;
- роль жертвы;
- цель атаки (получение данных, доступа, конфиденциальной информации).

3. Анализ уязвимости человеческого фактора

Проанализируйте, какие человеческие факторы используются в выбранном сценарии, например:

- невнимательность;
- чрезмерное доверие;
- давление времени;
- незнание правил информационной безопасности;
- мнимая или формальная авторитетность.

4. Оценка рисков

Оцените риски, связанные с предложенным сценарием, указав:

- какие типы данных могут быть скомпрометированы;
- потенциальное влияние на организацию;
- какие компоненты триады CID затронуты (Конфиденциальность, Целостность, Доступность).

5. Меры по повышению осведомлённости и предотвращению

Предложите **не менее 5 мер** по предотвращению и повышению осведомлённости, которые могли бы снизить риск подобной атаки, например:

- обучение по вопросам информационной безопасности;
- внутренние политики безопасности;
- симуляции фишинговых атак;
- правила физического доступа;
- процедуры проверки личности.