Дніпровський національний університет імені Олеся Гончара Факультет прикладної математики Кафедра обчислювальної математики та математичної кібернетики

Лабораторна робота №1

Захист інформації

студента групи ПА-19-2

Ільяшенко Єгора

Варіант №7

Дніпро, 2022

Изображение выглядит как текст

Автоматически созданное описание

Варіант 7: Система обміну повідомленнями

Споживачі ПЗ:

Викостовувати систему обміну повідомленнями можна використовувати як в особистих цілях (спілкування друзів на відстані), так і у комерційній діяльності (спілкування між компанією та покупцем), тощо.

Модель порушника:

Людина, яка зацікавлена в ваших особистих даних. Це може бути як і одна людина, так і ціла огранізація. Це може бути полювання за паролями, які деякі люди пишуть у месенджерах. Бютжету залежить напряму від «цікавості» цілі атаки. Простим людям не варто турбуватися про ціленаправлені атаки на них. Публічно відомим людям, або власникам бізнесів вже варто турбуватися про таки. Зазвичай ж достатньо дотримуватися інтернет гігієни.

Типи атак:

Спам – це небажані повідомлення, що надсилаються у великій кількості користувачам, які не давали на це своєї згоди. Існують програмні засоби, які зчитують, у яких сервісах користувач зареєструвався. Це може бути навіть доставка піци. Далі програми починають посилати на цей номер велику кількість повідомлень, починаюсь реєструватися в неймовірній кількості сервісів та створювати замовлення у сервісах, де користувач вже зареєструвався.

Фішинг – це метод атаки, при якому злочинці починають розповсюджувати повідомлення, які мають у собі сховане злочинне програмне забезпечення. Це можуть бути файли, зображення, посилання, замасковані під відомі сервіси, або стиснуті повідомлення, де кінцеву адресу не можна побачити.

Сніффінг – це метод прослуховування мережі, через яку проходять повідомлення користувача. Усі пакети зараз зашифровуються, але все ще є вірогідність, що зловмисник зможе підібрати ключі до пакетів.

Підбір паролів – атака, при якій зловмисник намагається напряму зламати акаунт користувача, перебираючи їх або по-символьно (brute force), або по спеціальним спискам найрозповсюдженіших паролів. Нещодавно атака brute force була майже неможливою, але з кожним роком це змінюється все сильніше. Наприклад, остання відеокарта від NWIDIA RTX4090Ti має кількість операцій 83TFLOPS. Це 83000000000000 операції у секунду.

Як захиститися від атак:

Спам

Мало чого може зробити сам користувач. Якщо користувач – звичайна людина, то навряд-чи хтось буде таким займатися. Відомим людям варто використовувати один телефон для комерційної діяльності та не розповсюджувати інформацію про нього. На другому телефоні блокувати усі повідомлення.

Сніффінг – не залежить від користувача. Використовуйте популярні месенджери. Дуже часто, популярність засобу – це гарантія якості. Але популярніші засоби частіше атакують.

Підбір паролів:

Використовуйте якомога складніший пароль, використовуйте різні паролі до різних застосунків. Налаштуйте двофакторну аутентифікацію, це чудовий засіб для захисту акаунтів. Без прямого доступу до вашого телефону, зламати ваш акаунт не вдасться.

Фішинг

Не відкривайте підозрілі повідомлення. Не відкривайте скомпресовані повідомлення з джерел, яким не довіряєте. Якщо у програмному засобі є захит від спаму, увімкніть його.