МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Государственное образовательное учреждение высшего профессионального образования   
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ

Кафедра компьютерных технологий и программной инженерии (№43)

ОТЧЕТ

ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

|  |  |  |
| --- | --- | --- |
| канд. техн. наук, доцент | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Фаткиева Р. Р. |
|  | подпись, дата |  |

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №1

Оценка нарушения информационной безопасности с использованием Марковской цепи

По дисциплине: ЗАЩИТА ИНФОРМАЦИИ

РАБОТУ ВЫПОЛНИЛ

|  |  |  |  |
| --- | --- | --- | --- |
| СТУДЕНТ ГР. № |  |  |  |
|  |  | подпись, дата | фамилия, инициалы |

**Санкт-Петербург, 2023**

**Лабораторная работа №1**

**«Оценка нарушения информационной безопасности   
с использованием Марковской цепи»**

**I. Постановка задачи**

Порядок выполнения лабораторной работы:

1. Определение процессы , происходящие в системе в штатном режиме функционирования;
2. Формирование перечня атак и построение модели угроз;
3. Определение интенсивностей перехода процесса из состояния в состояние и нахождение начальных состояний на момент ;
4. Решение системы дифференциальных уравнений относительно полученных интенсивностей перехода и начальных состояний;
5. Получение значений вероятностей перехода из состояния в состояние на основе рассмотренной ранее системы дифференциальных уравнений для различных наборов значений интенсивностей, характерных альтернативным мероприятиям защиты;
6. Влияние на процесс функционирования системы. Определение наилучшего варианта мероприятий по обеспечению информационной безопасности защиты согласно ;

**II. Ход работы**

Определим процессы , происходящие в системе в штатном режиме функционирования. Пусть система – *корпоративная сеть, доступ к ресурсам которой пользователь получает после успешной авторизации*. Обобщенно на графе штатный режим функционирования системы выглядит так:

|  |  |
| --- | --- |
|  | 1 – Клиент заполняет форму логина;  2 – Производится попытка локальной аутентификации (проверка кэша компьютера);  3 – Запрос на аутентификацию к серверу с БД учетных записей;  4 – Получение доступа к сетевым ресурсам; |

Сформируем перечень атак – и отобразим на графе:

|  |  |
| --- | --- |
|  | 1 – Клиент заполняет форму логина;  2 – Производится попытка локальной аутентификации (проверка кэша компьютера);  3 – Запрос на аутентификацию к серверу с БД учетных записей;  4 – Получение доступа к сетевым ресурсам;  5 – *Атака* «подбор пароля»;  6 – *Атака* «подделка кэша данных об аутентификации»;  7 – *Атака* «man-in-the-middle (посредник)»; |

Составим систему дифференциальных уравнений:

Определим интенсивности перехода процесса из состояния в состояние:

, , , , , , , ,

, , , , , , , ,

Вектор инициализации – .

Получаем графики:

|  |  |
| --- | --- |
| 1 – Клиент заполняет форму логина; | 2 – Производится попытка локальной аутентификации (проверка кэша компьютера); |
|  |  |
| 3 – Запрос на аутентификацию к серверу с БД учетных записей; | 4 – Получение доступа к сетевым ресурсам; |
|  |  |
| 5 – *Атака* «подбор пароля»; | 6 – *Атака* «подделка кэша данных об аутентификации»; |
|  |  |
| 7 – *Атака* «man-in-the-middle (посредник)»; |  |
|  |  |

Оценим графики и составим таблицу вероятностей процессов за 120 секунд:

|  |  |
| --- | --- |
| **Процесс** | **Вероятность без мероприятий по обеспечению безопасности** |
| Клиент заполняет форму логина; | 0.05 |
| Производится попытка локальной аутентификации (проверка кэша компьютера); | 0.42 |
| Запрос на аутентификацию к серверу с БД учетных записей; | 0.3 |
| Получение доступа к сетевым ресурсам; | 0.4 |
| *Атака* «подбор пароля»; | 0.1 |
| *Атака* «подделка кэша данных об аутентификации»; | 0.06 |
| *Атака* «man-in-the-middle (посредник)»; | 0.37 |

Сформируем перечень мероприятий по защите от трех представленных атак:

* Для защиты от атаки «*подбор пароля*» будем использовать генераторы паролей с аппаратным датчиком случайных чисел;
* Для защиты от атаки «*подделка кэша данных об аутентификации*» будем использовать антивирус на клиентском компьютере;
* Для защиты от атаки «*man-in-the-middle (посредник)*» будем использовать процесс оценки подозрительных действий узлов сети (и анализ их трафика).

Тогда интенсивности изменятся:

, , , , , , , ,

, , , , , , , ,

Построим графики с учетом изменений:

|  |  |
| --- | --- |
| 1 – Клиент заполняет форму логина; | 2 – Производится попытка локальной аутентификации (проверка кэша компьютера); |
|  |  |
| 3 – Запрос на аутентификацию к серверу с БД учетных записей; | 4 – Получение доступа к сетевым ресурсам; |
|  |  |
| 5 – *Атака* «подбор пароля»; | 6 – *Атака* «подделка кэша данных об аутентификации»; |
|  |  |
| 7 – *Атака* «man-in-the-middle (посредник)»; |  |
|  |  |

Оценим графики и дополним ранее составленную таблицу:

|  |  |  |
| --- | --- | --- |
| **Процесс** | **Вероятность без мероприятий по обеспечению безопасности** | **Вероятность при мероприятиях по обеспечению безопасности** |
| Клиент заполняет форму логина; | 0.05 | 0.05 |
| Производится попытка локальной аутентификации (проверка кэша компьютера); | 0.42 | 0.5 |
| Запрос на аутентификацию к серверу с БД учетных записей; | 0.3 | 0.37 |
| Получение доступа к сетевым ресурсам; | 0.4 | 0.53 |
| *Атака* «подбор пароля»; | 0.1 | 0.01 |
| *Атака* «подделка кэша данных об аутентификации»; | 0.06 | 0.05 |
| *Атака* «man-in-the-middle (посредник)»; | 0.37 | 0.19 |

Как можно заметить, вероятности атак снизились, а вероятности штатных для системы процессов либо не изменились, либо увеличились.

**Приложение: Код программы**

Файл main2.m:

**global** l12 l15 l21 l23 l24 l26 l27 l32 l34 l37 l42 l43 l47 l51 l62 l72 l73 l74;

l12 = 0.4;

l15 = 0.3;

l21 = 0.1;

l23 = 0.2;

l24 = 0.7;

l26 = 0.1;

l27 = 0.4;

l32 = 0.4;

l34 = 0.8;

l37 = 0.1;

l42 = 0.7;

l43 = 0.5;

l47 = 0.4;

l51 = 0.4;

l62 = 0.9;

l72 = 0.9;

l73 = 0.6;

l74 = 0.9;

initial = [1; 0; 0; 0.7; 0; 0; 0];

time = [0, 25];

[T, Y] = ode45('LotVol', time, initial);

**for** i = 1:7

pl = plot(Y(:,i), [";" num2str(i) ";"]);

refresh()

waitfor(pl)

**end**

Файл LotVol.m:

**function** **result** = **LotVol**(t, y) % первая функция

coef = LotVolCoefSource();

[r, c] = size(coef);

result = zeros(r, 1);

**for** i = 1:r

**for** j = 1:c

result(i) = result(i) + coef(i, j) \* y(j);

**end**

**end**

**end**

Файл LotVolCoef.m:

**function** **result** = **LotVolCoef**( lambda )

s = size(lambda);

**if** (s(1) ~= s(2))

result = 0;

**return**;

**end**

s = s(1);

d = zeros(s);

**for** k = 1:s

**for** i = 1:s

d(k, i) = lambda(i, k);

**end**

**end**

**for** k = 1:s

**for** i = 1:s

d(k, k) = d(k, k) - lambda(k, i);

**end**

**end**

result = d;

**end**

Файл LotVolCoef.m:

**function** **result** = **LotVolCoefSource**()

*%LOTVOLCOEFSOURCE Summary of this function goes here*

*% Detailed explanation goes here*

**global** l12 l15 l21 l23 l24 l26 l27 l32 l34 l37 l42 l43 l47 l51 l62 l72 l73 l74;

lambda = [

*% --1 --2 --3 --4 --5 --6 --7*

0 l12 0 0 l15 0 0 *% 1*

0 0 l23 l24 0 l26 l27 *% 2*

0 l32 0 l34 0 0 l37 *% 3*

0 l42 l43 0 0 0 l47 *% 4*

l51 0 0 0 0 0 0 *% 5*

0 l62 0 0 0 0 0 *% 6*

0 l72 l73 l74 0 0 0 *% 7*

*% --1 --2 --3 --4 --5 --6 --7*

];

result = LotVolCoef(lambda);

**end**