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. № | 4931 |  | Кинько А. А. |
|  |  | 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 (домен), поделенная на две подсети: клиентскую с контроллером домена, выполняющим функции DNS и DHCP и серверную с маршрутизатором и терминальными устройствами, ресурсы которого могут использовать авторизованные в домене пользователи, а также получать информацию через сайт, размещенный на веб-сервере одного из терминалов.* Обобщенно на графе штатный режим функционирования системы выглядит так:

|  |  |
| --- | --- |
|  | 1 – Клиент заполняет форму авторизации;  2 – Попытка локальной аутентификации;  3 – Запрос на аутентификацию к контроллеру домена (Active Directory)  4 – Получение доступа к сетевым ресурсам первой сети  5 – Получение доступа к второй сети через маршрутизатор  6 – Получение доступа к ресурсам терминальных компьютеров  7 – Получение доступа к сайту веб-сервера второй сети |

Сформируем перечень атак и отобразим на графе:

|  |  |
| --- | --- |
|  | 1 – Клиент заполняет форму авторизации;  2 – Попытка локальной аутентификации;  3 – Запрос на аутентификацию к контроллеру домена (Active Directory)  4 – Получение доступа к сетевым ресурсам первой сети  5 – Получение доступа к второй сети через маршрутизатор  6 – Получение доступа к ресурсам терминальных компьютеров  7 – Получение доступа к сайту веб-сервера второй сети  8 – Атака «подбор пароля»  9 – Навязывание ложного маршрутизатора  10 – Атака «подмена содержимого» |

Составим систему дифференциальных уравнений:

Определим интенсивности перехода процесса из состояния в состояние:

Вектор инициализации =

Получаем графики:

|  |  |
| --- | --- |
| 1. Клиент заполняет форму авторизации | 2. Попытка локальной аутентификации |
| 3. Запрос на аутентификацию | 4. Получение доступа к сетевым ресурсам первой сети |
| 5. Получение доступа к второй сети через маршрутизатор | 6. Получение доступа к ресурсам терминальных компьютеров |
| 7. Получение доступа к сайту веб-сервера второй сети | 8. Атака «подбор пароля» |
| 9. Навязывание ложного маршрутизатора | 10. Атака «подмена содержимого» |

Оценим графики и составим таблицу вероятностей процессов за 120 секунд

|  |  |
| --- | --- |
| **Процесс** | **Вероятность без мероприятий по обеспечению безопасности** |
| Клиент заполняет форму авторизации | 0.29 |
| Попытка локальной аутентификации | 0.16 |
| Запрос на аутентификацию | 0.41 |
| Получение доступа к сетевым ресурсам первой сети | 0.09 |
| Получение доступа к второй сети через маршрутизатор | 0.01 |
| Получение доступа к ресурсам терминальных компьютеров | 0.01 |
| Получение доступа к сайту веб-сервера второй сети | 0.01 |
| Атака «подбор пароля» | 0.06 |
| Навязывание ложного маршрутизатора | 0.01 |
| Атака «подмена содержимого» | 0.01 |

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 навязывания ложного маршрутизатора будем фильтровать сообщения, используя Firewall, а также выберем сетевую ОС, которая будет игнорировать ложное ICMP Redirect сообщение.
* Для защиты от атаки «подмены содержимого», спуфинга, проведем мероприятия по доведению до персонала принципов безопасной работы в Интернете, а также установим антивирусное ПО.

Тогда интенсивности изменятся:

Построим графики с учетом изменений:

|  |  |
| --- | --- |
| 1. Клиент заполняет форму авторизации | 2. Попытка локальной аутентификации |
| 3. Запрос на аутентификацию | 4. Получение доступа к сетевым ресурсам первой сети |
| 5. Получение доступа к второй сети через маршрутизатор | 6. Получение доступа к ресурсам терминальных компьютеров |
| 7. Получение доступа к сайту веб-сервера второй сети | 8. Атака «подбор пароля» |
| 9. Навязывание ложного маршрутизатора | 10. Атака «подмена содержимого» |

Оценим графики и дополним ранее составленную таблицу:

|  |  |  |
| --- | --- | --- |
| **Процесс** | Вероятность без мероприятий по обеспечению безопасности | Вероятность при мероприятиях по обеспечению безопасности |
| Клиент заполняет форму авторизации | 0.29 | 0.29 |
| Попытка локальной аутентификации | 0.16 | 0.16 |
| Запрос на аутентификацию | 0.41 | 0.41 |
| Получение доступа к сетевым ресурсам первой сети | 0.09 | 0.09 |
| Получение доступа к второй сети через маршрутизатор | 0.01 | 0.01 |
| Получение доступа к ресурсам терминальных компьютеров | 0.01 | 0.01 |
| Получение доступа к сайту веб-сервера второй сети | 0.01 | 0.01 |
| Атака «подбор пароля» | 0.06 | 0.03 |
| Навязывание ложного маршрутизатора | 0.01 | 0.01 |
| Атака «подмена содержимого» | 0.01 | 0.01 |

Как можно видеть, вероятности атак снизились, а вероятности штатных для системы процессов либо не изменились, либо увеличились. В большинстве, изменения почти не наблюдаются из-за и без того малой интенсивности в случае без проведения мероприятий по обеспечению безопасности.

**III. Выводы**

В ходе выполнения данной лабораторной работы были получены навыки моделирования процессов, происходящих в системе в штатном режиме функционирования на примере корпоративной сети, а также атак на эту систему. Также были освоены методы защиты от данных атак и проведен анализ их пригодности на модели.

**Приложение А. Листинг программы**

Файл «main2.m»:

global l12 l18 l21 l23 l24 l32 l34 l42 l43 l54 l56 l57 l59 l65 l60 l75 l81 l95 l06;

l12 = 0.3;

l18 = 0.01;

l21 = 0.5;

l23 = 0.3;

l24 = 0.6;

l32 = 0.2;

l34 = 0.1;

l42 = 0.7;

l43 = 0.8;

l54 = 0.2;

l56 = 0.6;

l57 = 0.8;

l59 = 0.05;

l65 = 0.3;

l60 = 0.1;

l75 = 0.4;

l81 = 0.1;

l95 = 0.2;

l06 = 0.05;

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

time = [0, 25];

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

for i = 10:10

  plot(Y(:,i)); hold on

end

Файл «LotVolCoefSource.m»:

function result = LotVolCoefSource()

%LOTVOLCOEFSOURCE Summary of this function goes here

% Detailed explanation goes here

 global l12 l18 l21 l23 l24 l32 l34 l42 l43 l54 l56 l57 l59 l65 l60 l75 l81 l95 l06;

 lambda = [

% --1 --2 --3 --4 --5 --6 --7 --8 --9 -10

    0 l12 0 0 0 0 0 l18 0 0;

  l21 0 l23 l24 0 0 0 0 0 0;

    0 l32 0 l34 0 0 0 0 0 0;

    0 l42 l43 0 0 0 0 0 0 0;

    0 0 0 l54 0 l56 l57 0 l59 0;

    0 0 0 0 l65 0 0 0 0 l60;

    0 0 0 0 l75 0 0 0 0 0;

  l81 0 0 0 0 0 0 0 0 0;

    0 0 0 0 l95 0 0 0 0 0;

    0 0 0 0 0 l06 0 0 0 0

% --1 --2 --3 --4 --5 --6 --7 --8 --9 -10

 ];

 result = LotVolCoef(lambda);

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 «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