DOI: 10.17117/na.2016.09.01.443

<http://ucom.ru/doc/na.2016.09.01.443.pdf>

Поступила (Received): 28.09.2016

Мирошина И.Е. Экспериментальное моделирование процесса преодоления средств защиты информации в вычислительных сетях

Miroshina I.E.
Experimental modeling of the process of
overcoming of information security in
computer networks

Представлены результаты экспериментального исследования преодоления средств защиты информации в вычислительных сетях Internet (Intranet) средствами неправомерного доступа в различных ситуациях. Результаты представлены в виде гистограмм зависимости количества вскрытых средств защиты от времени

Ключевые слова: моделирование, защита информации

Results of the pilot study of overcoming means of information protection in Internet (Intranet) computer networks by means of illegal access in different situations are provided. Results are presented in the form of histograms of dependence of quantity of the opened security features from time

Key words: modeling, information security

Мирошина Ирина Евгеньевна

Ассистент

Воронежский государственный педагогический университет

г. Воронеж, ул. Ленина, 86

Miroshina Irina Evgenievna

Assistant

Voronezh state pedagogical university

Voronezh, Lenina st., 86

Теоретические основы взаимовлияния средств защиты информации (СЗИ) и средств неправомерного доступа (СНД) в вычислительных сетях организационного управления предприятием [1] даны в [2].

Паролевая или ключевая защита широко используется для обеспечения безопасности информации в сети Internet [3]. Сеть Internet работает по определенным протоколам, локальные вычислительные сети (Intranet) работают по таким же протоколам. Поэтому экспериментальное моделирование можно проводить с вычислительной сетью Intranet. Кроме того, такой подход позволяет в короткое время изменять свойства как средств защиты, так и средств воздействия на них. В связи с этим экспериментальное моделирование проводилось на трех ЛВС, которые были объединены в одну сеть Intranet одного из институтов военного профиля со следующими характеристиками:

- протокол работы сети идентичен протоколу сети Internet;
- нет выхода в сеть Internet;

– 45 рабочих станций объединены двумя серверами;
– каждый сервер имеет паролевую защиту с обязательным разграничением прав доступа для пользователей сети;
– все рабочие станции имеют паролевую защиту;
– пользователи сети имеют паролевую защиту для своих рабочих папок и файлов.

При экспериментальном моделировании были использованы следующие приемы вскрытия паролевых защит:

– последовательный перебор символов;
– произвольный перебор символов;
– подбор пароля комбинированным методом с различными программно-техническими средствами его вскрытия или обхода, а также с возможностью объединения для доступа к защищаемой информации через коммуникационные линии вычислительной сети.

В эксперименте было задействовано 100 курсантов, которые выполняли роль злоумышленников. Курсанты имели разный уровень подготовки: новички – 94%, имеющие опыт взлома паролей – 6%. Во время эксперимента из курсантов организовали три группы по 32, 33 и 35 человек. При этом курсанты, имеющие опыт вскрытия паролевых средств защиты, были распределены следующим образом: в первой группе – один курсант, во второй – два курсанта, в третьей группе – три курсанта. Эксперимент состоял из трех частей. В каждой части применялся свой способ преодоления паролевых средств защиты. Для первых двух частей использовался последовательный и случайный перебор символов паролевых средств защиты соответственно, а курсанты были лишены возможности действовать согласованно. Индикатор частоты вскрытия средств защиты определялся на всю группу в целом. В третьей части курсанты осуществляли согласованные действия по преодолению средств защиты.

Для каждой группы участников эксперимента было создано по 100 паролевых средств защиты с длиной паролей из трех символов прописных букв английского алфавита (26 символов). Эта информация доводилась до сведения курсантов. Каждый курсант может набрать 3 символа за 1-1.5 сек, а общее количество переборов независимых символов определяется из формулы размещения с повторениями. В нашем случае максимальное количество комбинаций перебора ключа до момента вскрытия пароля равно 17575, курсант за 60 сек способен выполнить 60 комбинаций. Следовательно, 17575 комбинаций можно перебрать примерно за 292 мин.

В третьей части генерировалось по 100 паролевых средств защиты длиной от трех до десяти символов. Курсанты на данном этапе могли преодолевать паролевые средства защиты, объединяясь в группы с максимум пятью других участников, выбранных случайным образом, а обмен информацией между ними разрешался только через один из серверов сети Intranet после вскрытия его пароля длиной в 10 символов. Как и ранее, индикатор частоты вскрытия средств защиты любой длины определялся в результате действий всех курсантов в целом. Результаты экспериментального моделирования в зависимости от способа

вскрытия паролевых средств защиты приведены на рис.1 – 3. На рис. 1 представлены результаты первой части эксперимента, анализ которых (гистограмма рис.1а частот вскрытия СЗИ с паролем) позволил сделать заключение о нормальном законе распределения количества вскрытых средств защиты с характеристиками: математическое ожидание $\mu=8.9$, среднеквадратическое отклонение $\sigma=2.78$. На рис.1б приведен график нормального распределения с указанными параметрами.

а)

б)

Рис. 1. а) –гистограмма зависимости количества вскрытых паролей СЗИ от времени первой части эксперимента; б) – нормальный закон распределения плотности вероятности количества вскрытых паролей

Анализ результатов второй части эксперимента (рис.2.а) позволил предположить, что индикатором частоты является количество вскрытых средств защиты, распределенное по экспоненциальному закону и получить характеристику этого закона $\lambda=0.096$. На рис.2б приведен график экспоненциального распределения с указанным параметром.

Полученные экспериментальные данные для первых двух способов преодоления паролевых средств защиты в ЛВС идентичны результатам, которые

были получены например в работе [4] для вскрытия отдельных средств защиты отдельным взломщиком.

Рис. 2. а) – гистограмма зависимости количества вскрытых паролей СЗИ от времени второй части эксперимента; б) – экспоненциальный закон распределения плотности вероятности количества вскрытых паролей

В третьей части эксперимента в отличие от первых двух частей для «взлома» паролевых средств защиты в ЛВС использовались различные программно-технические средства, а также объединения действий курсантов. В результате получена следующая зависимость количества вскрытых средств защиты от времени (рис.3).

Рис. 3. Гистограмма зависимости количества вскрытых паролей СЗИ от времени третьей части эксперимента

В соответствии с результатами, полученными в работах [37, 95, 97, 120], вид зависимости на рис.3 соответствует так называемому негауссовому закону распределения плотности вероятности.

Список используемых источников:

1. Греченко Д.А., Чулюков В.А. Ситуационное моделирование в задачах организационного управления вузом // Научные труды SWorld. 2009. Т. 3. № 1. С. 13-15.

2. Мирошина И.Е., Чулюков В.А. Распределенная информация, средства защиты и средства воздействия в модели вычислительной сети // Научные труды SWorld. 2013. Т. 5. № 3. С. 36-39.
3. Хоффман Л. Современные методы защиты информации. М: Сов. Радио, 1980. 264 с.
4. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. М.: Энергоатомиздат, 1994. 400 с.
5. Яблонский А.И. Математические модели в исследовании науки. М.: Наука, 1986. 352 с.

© 2016, Мирошина И.Е.

*Экспериментальное моделирование процесса
преодоления средств защиты информации в
вычислительных сетях*

© 2016, Miroshina I.E.

*Experimental modeling of the process of overcoming
of information security in computer networks*