УДК 004.725.7

Жуков И.А., д.т.н.,
Балакин С.В.

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ МЕТОДА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫЕ СЕТИ НА ОСНОВЕ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ

Национальный авиационный университет

zhuia@ukr.net
bpys@i.ua

Рассмотрено исследование эффективности метода обнаружения несанкционированных действий в компьютерной сети, получена информация для проведения эксперимента. Рассмотрены варианты распознавания неизвестных вторжений. Выявлены и описаны общие особенности поведения вторжений в компьютерных сетях. Приведены результаты реализации и эффективности предложенного метода

Ключевые слова: компьютерная сеть, метод обнаружения вторжений, искусственная иммунная система

Введение

Важной проблемой в сетевых технологиях является рост количества разнообразных вредоносных программ и атак на компьютерные сети [1-2]. Существующие антивирусные продукты не могут обеспечить абсолютно надежную защиту компьютерной сети. Применяемые в антивирусах принципы поиска не позволяют обнаруживать новые разновидности вредоносных программ до их изучения аналитиками и внесения дополнений и изменений в базы антивирусных программ. К недостаткам известных методов обнаружения вторжений в компьютерной сети можно отнести уязвимость к новым атакам, низкую точность и скорость работы [3-4].

Проведено исследование эффективности метода обнаружения несанкционированных действий (НД) в компьютерной сети на основе искусственных иммунных систем (ИИС) [5].

Постановка задачи

Решаемой проблемой выступает эффективность распознавания вредоносных программ в компьютерной сети средствами ИИС [6]. Исходя из особенностей исследуемого процесса, эффективность предложенного решения оценивается путем сравнения его с аналогами [7].

Цель исследования

Целью исследования является повышение эффективности обнаружения НД в компьютерной сети на основе ИСС.

Организация исследования

При выполнении поставленного задания использовался метод ИИС. Проводились исследования последовательностей вызова API функций и переданных им аргументов. Исследование и обучения проведено на базе процессора Intel Core 2 Duo T7300 на ОС Linux.

Негативные факторы, влияющие на результат работы, – разнообразие исследуемых служб и программ на базе экспериментальной системы.

При работе с вредоносными действиями использовался эмулятор iMUL, чтобы исключить возможность НД взаимодействовать напрямую с системой пользователя [8].

НД запускаются на эмуляторе для получения протоколов их работы. При построении эксперимента использованы НД, представленные на рис. 1.

Рис.1. Перечень использованных НД

Для данных НД и вторжений при помощи эмулятора получаем протоколы работы, из которых удаляется служебная информация о вызовах, не изменяющих поведение системы пользователя. Далее протоколы сравниваются друг с другом [5, 10].

В результате получаем выборку фрагментов характерных поведенческих признаков протоколов. Выявлено 15 признаков для Synflood и Slowloris атак:

1. Характеристика 1 содержится в 3-9; 14; 15. Рейтинг появления: 9/15 = 0.6.
2. Характеристика 2 содержится в 1-15. Рейтинг появления: 15/15 = 1.
3. Характеристика 3 содержится в 1-15. Рейтинг появления: 15/15 = 1.
4. Характеристика 4 содержится в 1-11; 14; 15. Рейтинг появления: 13/15 = 0.86.
5. Характеристика 5 содержится в 1-6; 10-12. Рейтинг появления: 9/15 = 0.6.
6. Характеристика 6 содержится в 1-5; 10, 11. Рейтинг появления: 7/15 = 0.46.
7. Характеристика 7 содержится в 1-15. Рейтинг появления: 15/15 = 1.
8. Характеристика 8 содержится в 1-8; 11-15. Рейтинг появления: 13/15 = 0.86.
9. Характеристика 9 содержится в 1-7; 10-15. Рейтинг появления: 13/15 = 0.86.
10. Характеристика 10 содержится в 1-7; 10-15. Рейтинг появления: 13/15 = 0.86.
11. Характеристика 11 содержится в 1-7; 10-15. Рейтинг появления: 13/15 = 0.86.
12. Характеристика 12 содержится в 1-7; 10-15. Рейтинг появления: 13/15 = 0.86.
13. Характеристика 13 содержится в 1-4; 9-11. Рейтинг появления: 7/15 = 0.46.
14. Характеристика 14 содержится в 1-5; 9-12. Рейтинг появления: 9/15 = 0.6.
15. Характеристика 15 содержится в 1-9; 12-15. Рейтинг появления: 13/15 = 0.86.

Выявлено 15 характерных признаков поведения для НД и вторжений Synflood и Slowloris атак. Определены рейтинги появления представленных вы-

ше НД. На основе обучающей выборки из вычисленных рейтингов появления признаков вторжений проводится моделирование ИИС. Обработка полученной информации и выявление новых НД реализуется утилитой DaigNet.

Для проверки корректности выявления НД используются Synflood и Slowloris атаки. Для обучения ИИС сформируем обучающую выборку из рейтингов появления признаков НД и вторжений и признаков системных вызовов. Данные рейтинги указаны в табл. 1.

Графическая интерпретация разработанной ИИС приведена на рис.2. Получено два кластера входных данных. Первый кластер состоит из антител: 1, 2, 5, 7, 13, 15; второй – антител: 3, 4, 6, 8, 9, 10, 11, 12, 14. Полученные данные для выявления новых антигенов обрабатываются утилитой DaigNet.

Результаты работы утилиты DaigNet приведены на рис. 3.

Таблица 1. Обучающая выборка для выявления НД семейств Synflood и Slowloris

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1		1	1	0.86	0.6	0.46	1	0.86	0.86	0.86	0.86	0.86	0.46	0.6	0.86
2		1	1	0.86	0.6	0.46	1	0.86	0.86	0.86	0.86	0.86	0.46	0.6	0.86
3	0.6	1	1	0.86	0.6	0.46	1	0.86	0.86	0.86	0.86	0.86	0.46	0.6	0.86
4	0.6	1	1	0.86	0.6	0.46	1	0.86	0.86	0.86	0.86	0.86	0.46	0.6	0.86
5	0.6	1	1	0.86	0.6	0.46	1	0.86	0.86	0.86	0.86	0.86		0.6	0.86
6	0.6	1	1	0.86	0.6		1	0.86	0.86	0.86	0.86	0.86			0.86
7	0.6	1	1	0.86			1	0.86	0.86	0.86	0.86	0.86			0.86
8	0.6	1	1	0.86			1	0.86							0.86
9	0.6	1	1	0.86			1						0.46	0.6	0.86
10		1	1	0.86	0.6	0.46	1		0.86	0.86	0.86	0.86	0.46	0.6	
11		1	1	0.86	0.6	0.46	1	0.86	0.86	0.86	0.86	0.86	0.46	0.6	
12		1	1		0.6		1	0.86	0.86	0.86	0.86	0.86		0.6	0.86
13		1	1				1	0.86	0.86	0.86	0.86	0.86			0.86
14	0.6	1	1	0.86			1	0.86	0.86	0.86	0.86	0.86			0.86
15	0.6	1	1	0.86			1	0.86	0.86	0.86	0.86	0.86			0.86

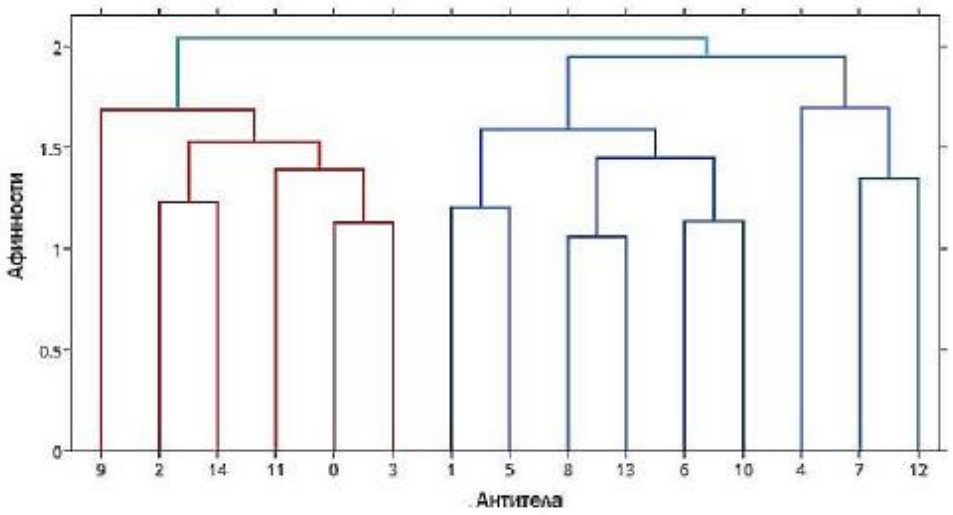

Рис. 2. Дендограмма обученной ИИС

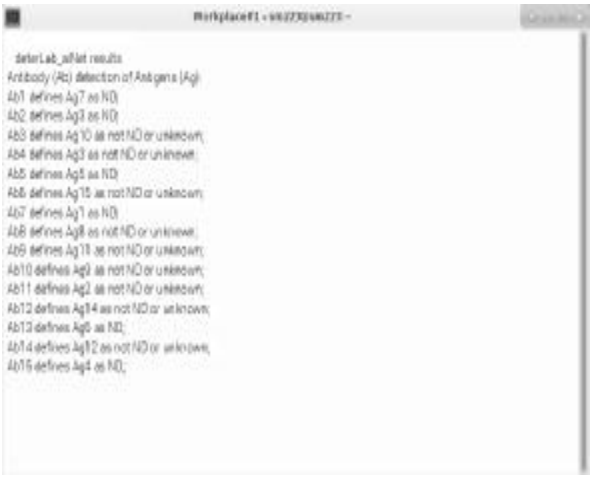

Рис. 3. Окно утилиты DaigNet

Антитела 1, 2, 5, 7, 13, 15 обнаруживают антигены НД (1-й кластер), а антитела под номерами 3, 4, 6, 8-12, 14 выявляют антигены действий пользователя или вторжения других типов (2-й кластер).

Для выявления новых антигенов НД и вторжений (тех, которые не включены в обучающую выборку) использовались одновременно запущенные Synflood и Slowloris атаки со средней интенсивностью:

1-й антиген - loggining;

2-й антиген - NETSTAT - TcpExt - Listen Drops.

Характеристики новых антигенов показаны в табл. 2.

Результаты выявления новых антигенов приведены на рис. 4.

Рис. 4. Результаты распознавания новых антигенов

Результаты показывают, что разработанная ИИС приняла верное решение и отнесла 1-й и 2-й антигены к НД и вторжениям. Таким образом ИИС корректно решила задачу по выявлению как представленных в обучающей выборке вторжений, так и новых (ранее неизвестных системе) атак (рис. 1) [10,11].

Таблица 2. Характеристики новых антигенов

Ag	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1		1	1	0.86	0.6	0.46	1	0.86	0.86	0.86	0.86	0.86	0.46	0.6	0.86
3		1	1	0.86	0.6	0.46	1	0.86	0.86	0.86	0.86	0.86	0.46	0.6	0.86

На основе анализа полученной информации сделан следующий вывод: при корректной обучающей выборке и верном выборе параметров обучения ИИС показывает высокую точность обнаружения новых НД. При длительном обучении выборки получаются более разнообразные варианты работы и антигенов и антител, что позволяет системе гибко и оперативно реагировать на новые вторжения. Обучение ИИС требует дополнительного времени, но при этом повышается точность.

Для анализа эффективности распознавания НД по сравнению с известными методами выбраны программные решения Kaspersky и AVIRA.

Результаты тестирования программ представлены в табл. 3.

Таблица 3. Результаты исследования эффективности методов обнаружения НД

НД	ИИС	AVIRA	Kaspersky
NETSTATACK Locked	+	+	+
NETSTAT-ACK Lost	+	+	-
Response Time 1	+	+	+
TCP Flag ACK 1	+	+	+
TCP Flag SYN 1	+	+	+
TCP ACK Num	+	-	+
LOADAVG Act Proc	+	+	+
Serve Time	+	+	+
Final HTTP Status	+	+	+
Closing Connection	+	-	-
Logging	+	+	+
Waiting For Connection	+	+	-
Wget Return Code	+	-	+
TCP Flag FIN	+	+	-
TCP Flag PSH	+	+	+

С помощью предложенных методов и моделей распознаны все НД, присутствовавшие в обучающей выборке (рис. 1).

Существующие же решения AVIRA и Kaspersky не смогли определить 3 и 4 НД соответственно, что свидетельствует о несовершенстве данных программных решений при работе с поведенческим анализом вторжений.

Результаты сравнительного анализа НД показывают, что предложенные методы превосходят известные антивирусные продукты, использованные в сравнительном тесте и способны обнаружить неизвестные НД.

Выводы

Представлена модель распознавания вредоносных программ и атак в компьютерной сети на основе ИИС. Основной проблемой при проведении исследования является корректное выявление вредных действий из-за того, что иногда они могут маскироваться как действия пользователя для сокрытия своей деятельности.

Предложено оценивать

достоверность распознавания вредоносных активностей с помощью анализа протоколов работы программ. Таким образом, блокируются вредные действия, но с другой стороны могут блокироваться некоторые программы и утилиты пользователя.

Приведены результаты исследования эффективности метода обнаружения НД в компьютерной сети на основе ИИС. Сформулированы пути повышения достоверности обнаружения вредоносных программ и атак в компьютерной сети.

В целом, проведенные исследования показали целесообразность используемых инструментов. Данный подход эффективен при выявлении и предотвращении НД к информации в компьютерной сети.

Эксперимент проведен с заранее известными действиями, но метод смог конструировать новые атаки. При необходимости данную систему можно дополнить новыми функциями для обработки всех возможных вторжений и угроз. Адаптивность предложенного метода позволяет модифицировать его на работу с новыми вторжениями.

Список литературы

1. Норткат С., Новак Д. Обнаружение нарушений безопасности в сетях. – [3-е издание]. – [пер. с англ.]. – М.: "Вильямс", 2003. – 448 с.

2. Милославская Н.Г., Толстой А.И. Интрасети: обнаружение вторжений: учеб/ пособие для вузов. – М.: Юнити-Дана, 2001. – 592 с.

3. Таненбаум Э. Компьютерные сети // СПб.: Питер, 2008. – 848 с.

4. Іванов В.Г., Карасюк В.В., Гвозденко М.В. Основи інформатики та обчислювальної техніки: навч. посібник // Юрінком Інтер, 2004. – 328 с.

5. Балакин С.В. Выявление компьютерных атак с помощью мониторинга сетевых объектов // Технологический аудит и резервы производства. – Т.5, №6 (25), 2015. – С. 36-38.

6. Jerne N.K. Idiotypic networks and other preconecived ideas // Immunological review, Vol. 79, 1984. – P. 5-24.

7. Watkins A.B., Phadke A. Parallelizing an Immune-Inspired Algorithm for Efficient Pattern Recognition // Intelligent Engineering Systems through Artificial Neural Networks: Smart Engineering System Design: Neural Networks, Fuzzy Logic, Evolutionary Programming, Complex Systems and Artificial Life, Vol. 13, 2003. – P. 225-230.

8. Bejtlich R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response // No Starch Press, 1 edition, 2013. – 376 p.

9. Пат. 110330 Україна, МПКG06F 12/14. Спосіб запобігання комп'ютерним атакам в мережі за допомогою фільтрації вхідних пакетів / І.А.Жуков, С.В.Балакін; власник Нац. авіаційний університет. – №201602196; заявл. 09.03.2016; Опубл. 10.10.2016, Бюл. № 19. – 6 с.

10. Balakin S.V., Zhukov I.A. Detection of computer attacks using outliner method // Young scientist, № 9 (36), 2016. – P. 91-93.

11. Балакин С.В. Организация пересечения вторжений в компьютерные сети алгоритмами выявления изменений // Вісник НТУ «ХПІ». Серія: Механіко-технологічні системи та комплекси. – Харків: НТУ «ХПІ». – 2017. – №20. – С. 3-7.

Статтю подано до редакції 04.09.2017