УДК 004.056

ИССЛЕДОВАНИЕ МЕТОДОВ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

Гаврилова Е.А.,
студентка, Финансовый университет, Москва, Россия
gava95@bk.ru

Аннотация. *На сегодняшний момент одна из самых серьезных угроз национальной безопасности — кибератаки на важные информационные инфраструктуры. Именно по этой причине сфера их выявления и противодействия компьютерным атакам является приоритетной. Цель данной статьи — изучение видов кибератак и методов их обнаружения. Также приводятся варианты решения проблемы выявления атак такого типа.*

Ключевые слова: *сетевые атаки; обнаружение атак; информационная безопасность.*

RESEARCH METHODS FOR DETECTING NETWORK ATTACKS

Gavrilova E.A.,
student, Financial University, Moscow, Russia
gava95@bk.ru

Abstract. *To date, one of the most serious threats to national security is cyberattacks on important information infrastructures. It is for this reason that the scope of their detection and counteraction to computer attacks is a priority. The purpose of this article is to study the types of cyber attacks and methods of their detection. Also, options for solving the problem of detecting attacks of this type are given.*

Keywords: *network attacks; detection of attacks; Information Security.*

1. Введение

Государство обеспечивает национальную безопасность во многих областях, но одной из самых важных в последнее время стала защита от кибератак. После появления Интернета жизнь общества разделилась на два мира: реальный и виртуальный. Большое количество людей проводит свое время в виртуальном мире. Немалая часть из них используют интернет-сообщество для незаконных целей. Вследствие этого киберпреступность и количество кибератак растут с каждым днем. Кибератаками называют действия по незаконному проникновению в компьютерную систему путем обхода защитных механизмов. Обнаружение кибератак можно охарактеризовать как «проблему выявления фактов неавторизованного доступа в компьютерную систему или сеть». Статья имеет следующую структуру: во 2 разделе представлены наиболее распространенные виды компьютерных атак, 3 раздел посвящен методам обнаружения атак, в 4 разделе приведены возможные варианты решения проблемы обнаружения кибератак.

2. Категории сетевых атак

В 1998 г. в программе оценки обнаружения кибератак DARPA была смоделирована локальная сеть американских ВВС, чтобы получить необработанные данные дампа TCP/IP. Локальная сеть управлялась как настоящая, но была подвержена множественным атакам. У каждого соединения TCP/IP были обнаружена 41 различная количе-

Научный руководитель: ***Крылов Г.О.,*** *доктор физико-математических наук, профессор кафедры информационной безопасности, Финансовый университет.*

ственная (тип текущих данных) и качественная (тип дискретных данных) функции. Среди них 34 функции были числовые и 7 функций символьные. Данные содержали 24 типа атак, которые могли быть классифицированы в четыре основных категории:

a) DDoS атаки (отказ в обслуживании.

Атаки класса DDoS производятся на систему с целью довести ее до отказа путем перегрузки запросами, вследствие чего пользователь не может получить доступ к ее ресурсам. Такая атака может быть первым шагом к овладению системой, но чаще всего служит просто для приведения в неработоспособное состояние. Есть много вариантов DDoS-атак, одни используют совершенно легальные методы (например, смурфинг), другие же могут создавать поврежденные пакеты, путая TCP/IP стек машины, пытающей восстановить эти пакеты (например, apache2);

b) R2L атаки.

Характеризуются получением доступа неавторизованного пользователя к компьютеру со стороны удаленной машины. Атакующий посылает пакеты машине по сети, а затем использует уязвимости системы, чтобы незаконно получить локальный доступ. Существует несколько способов реализации, например Xlock, когда атакующий использует приемы социальной инженерии — имитирует окно ввода пароля пользователя в заставке, которая на самом деле является троянским конем;

c) U2R атаки.

Тип атак, когда злоумышленник, имея учетную запись пользователя, использует уязвимости системы для получения прав администратора. Самый популярный способ — переполнение буфера. Переполнение буфера происходит, когда программа копирует слишком много данных в статический буфер, не проверяя данные на соответствие;

d) атаки зондированием.

Для реализации таких атак злоумышленник сканирует сеть, чтобы получить информацию об известных уязвимостях системы или найти новую. Цель сканирования портов состоит в том, чтобы определить, какие порты открыты, и, следовательно, какие службы, которые могут работать в системе, доступны атакующему. Результаты сканирования используются не только системными администраторами для проведения аудита сетевой безопасности, но и злоумышленниками, которые используют информацию об открытых портах для своих целей [3].

3. Методы обнаружения компьютерных атак

Все современные системы обнаружения кибератак проводят мониторинг или главных компьютеров, или сетевых соединений, чтобы собрать данные о вторжении.

3.1. Хостовая система обнаружения вторжений

Это система обнаружения вторжений, которая ведет наблюдение и анализ событий, происходящих внутри системы. Есть много системных характеристик, изменения в которых отслеживает хостовая система обнаружения вторжений:

a) **файловая система** — изменения в файловой системе узла могут сигнализировать о действиях злоумышленника, происходящих в ней;

b) **сетевые события** — система обнаружения вторжения может прервать все сетевые соединения после того, как они были обработаны сетевым стеком, прежде чем они будут переданы процессам пользовательского уровня;

c) **системные вызовы** — с некоторой модификацией ядра узла система обнаружения вторжения может быть построена таким способом, чтобы наблюдать все системные вызовы, которые были сделаны. Это может предоставить системе обнаружения вторжения подробные данные, указывающие на поведение программы.

3.2. Сетевая система обнаружения вторжений

Это система обнаружения вторжений, которая отслеживает такие виды вредоносной деятельности, как DDoS атаки, сканирование портов или даже попытки проникновения в сеть. Сетевая СОВ просматривает все входящие пакеты на наличие в них подозрительных признаков. Если, например, обнаружено большое количество запросов на TCP соединение с широким диапазоном различных портов, то, вероятней всего, проводится сканирование портов. Также подобная система чаще всего отслеживает входящий код схожим образом с обычной СОВ.

Сетевая СОВ не ограничивается отслеживанием только входящего сетевого трафика. Часто

важную информацию о происходящем вторжении можно получить также из исходящего или локального трафика. Действие некоторых атак может разворачиваться внутри наблюдаемой сети или сегмента сети и никак не отражаться на входящем трафике.

4. Предлагаемые способы решения проблемы обнаружения атак

В данном разделе представлены альтернативные способы построения СОВ, которые могут улучшить эффективность обнаружения атак.

4.1. Агентный подход

В данном подходе серверы могут связываться друг с другом и подавать сигналы. Иногда, чтобы предотвратить атаку, достаточно разъединить подсеть. В такой системе для сдерживания угрозы распределенные СОВ могут упорядочить маршрутизаторы и сетевые коммутаторы, чтобы разъединить узлы. Одной из проблем таких систем является дополнительная рабочая нагрузка на сетевую инфраструктуру. Есть два способа реализации агентского подхода: в первом автономные распределенные агенты используются для контроля системы и связи с другими агентами, второй же является мультиагентным, и в таком случае система будет обладать большим количеством информации об инфраструктуре. В мультиагентном подходе используются четыре типа агентов: основной, координационный, агент глобальной координации и агент взаимодействия [9].

4.2. Разработка программного обеспечения

Специальный язык программирования может улучшить стандарт разработки для кода СОВ. Разработчики могут пользоваться преимуществами нового языка, созданного для систем обнаружения компьютерных атак. Такой язык улучшит и скорость программирования, и качество итогового кода. В статье Vigna и др. [13] основное внимание сосредоточено на аспекте разработки программного обеспечения СОВ. Новая платформа под названием State Transition Analysis Technique (STAT) представлена в этой газете. В их реализованной платформе предлагается тип системы конечного автомата под названием STAT, которая следит за изменением состояния образцов атаки. Такой подход может помочь выполнять обнаружение кибератаки более успешно.

4.3. Использование искусственного интеллекта

Исследователи предложили применить понятие нечеткой логики к проблеме обнаружения кибератак. Работы, о которых сообщает Ajit Abraham и др. [14], Bridges и др. [15] и T. S. Chou и др. [16], являются примерами тех исследователей, которые следуют за этим подходом. Некоторые даже использовали многодисциплинарный подход, например Gomez и др. [17] объединили нечеткую логику, генетический алгоритм и методы правила ассоциации в их работе. Cho [18] сообщает о работе, где нечеткая логика и Скрытая марковская модель (СММ) были использованы вместе, чтобы обнаружить кибератаки. Еще один вариант — использование искусственных нейронных сетей.

4.4. Иммунные методы

Иммунные методы предпринимают попытку распространить принципы обнаружения и противодействия иммунной системы живых существ чужеродным вирусам. Система включает в себя централизованную «библиотеку генов», формирующую ограниченный набор векторов, характеризующих потенциально чужеродные события, и распределенную систему датчиков, выполняющих собственно детектирование воздействий и обладающих обратной связью с «библиотекой генов». Методы характеризуются нетребовательностью к ресурсам, однако в некоторых условиях формируют высокий поток ложных событий.

5. Заключение

В данной работе рассмотрены различные методы компьютерных атак, а также способы их выявления, представлены возможные решения проблемы обнаружения вторжений.

К основным тенденциям развития современных методов обнаружения вторжений и аномалий киберсистем относятся: повышение достоверности и точности методов обнаружения вторжений и аномалий; увеличение доли корректирующих процессов, не требующих участия человека-эксперта, что снижает время принятия решения и позволяет перевести время реакции на злоумышленное воздействие на качественно новый уровень (например, при автоматической гене-

рации сигнатур для нового вредоносного кода через несколько минут после подтверждения факта его аномально быстрого распространения по сети).

Приведенная систематизация данных об атаках и этапах их реализации дает необходимый базис для понимания технологий обнаружения атак.

Список источников

1. SANS Institute Staff, Intrusion Detection and Vulnerability Testing Tools: What Works? 101Security Solutions E-Alert Newsletters. 2001. URL: https://www.giac.org/paper/gsec/2063/vulnerability-analysis-elimination-false-positives/103552 (дата обращения: 07.10.2016).
2. URL: http://paper.ijcsns.org/07_book/200905/20090501.pdf (дата обращения 09.08.2016).
3. *Marinova-Boncheva V.* Applying a Data Mining Method for Intrusion Detection. In: International Conference on Computer Systems and Technologies CompSysTech'07, 14–15 June 2007.
4. *Biswanath Mukherjee, Todd L. Heberlein, and Karl N. Levit*t. Network intrusion detection. IEEE Network, 8(3): 26–41, May/June, 1994.
5. *Heady R., Luger G., Maccabe A., Servilla M.* The Architecture of a Network Level Intrusion Detection System. Technical Report CS90–20, University of New Mexico, Department of Computer Science, August 1990.
6. *Ye N.* "A markov chain model of temporal behavior for anomaly detection," in Proceedings of the 2000 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, June, 2000.
7. *Sekar R., Gupta A., Frullo J., Shanbhag T., Tiwari A., Yang H., Zhou S.* "Specification-based anomaly detection: a new approach for detecting network intrusions," in Proceedings of the 9th ACM conference on Computer and communication security, pp. 265–274, Washington D.C., USA, no. 2002. ACM Press.
8. *Otey M., Parthasarathy S., Ghoting A., Li G., Narravula S., Panda D.* "Towards nic based intrusion detection," in Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 723–728. ACM, ACMPress, NY, USA, Aug. 2003. Poster Session: Industrial/government track.
9. *Zhang R., Qian D., Ba C., Wu W. and Guo X.*, "Multi-agent based intrusion detection architecture," in Proceedings of 2001 IEEE International Conference on Computer Networks and Mobile Computing, pp. 494–501, oct. 2001.
10. *Simon Y.* Foo and M. Arradondo, "Mobile agents for computer intrusion detection," in Proceedings of the Thirty-Sixth Southeastern Symposium on System Theory, pp. 517–521. IEEE, IEEE, 2004.
11. Mitsubushi Corporation. "Concordia mobile agent development kit,". Software, 1999.
12. *Luo G., Lu X.L., Li J., Zhang and J.* "Madids: A novel distributed ids based on mobile agent," ACM SIGOPS Operating Systems Review, vol. 37, pp. 46–53, Jan. 2003.
13. *Vigna G., Valeur F., Kemmerer. Richard A.* "Designing and implementing a family of intrusion detection systems," in Proceedings of the 9th European software engineering conference held jointly with 10th ACM SIGSOFT international symposium on Foundations of software engineering, pp. 88–97, Helsinki, Finland, 2003. Source: ACM Portal.
14. *Ajit Abraham, Ravi Jain, Johnson Thomas, Sang Yang Han* "D-SCIDS: Distributed softcomputing intrusion detection system" Journal of Network and Computer Applications, Elsevier, 2005.
15. *Susan M. Bridges and M. Vaughn Rayford*, "Fuzzy data mining and genetic algorithms applied to intrusion detection," in Proceedings of the Twenty-third National Information Systems Security Conference. National Institute of Standards and Technology, Oct. 2000.
16. *Chou T.S., Yen K.K. and Luo J.* " Network Intrusion Detection Design Using Feature Selection of Soft Computing Paradigms" International Journal of Computaional Intelligence Vol. 4, no. 3, 2007.
17. *Gomez and J., Dasgupta D.* "Evolving fuzzy classifiers for intrusion detection," in Proceedings of the 2002 IEEE Workshop on the Information Assurance, West Point, NY, USA, June, 2001.
18. *Cho S.B.* "Incorporating soft computing techniques into a probabilistic intrusion detection system," IEEE transactions on systems, man and cybernetics.