Практическая значимость и новизна подсистемы мониторинга и аудита в ОС Linux заключается в том, что предложенная система является адаптивной подсистемой активного аудита построенной на базе искусственной иммунной сети с использованием многоагентного подхода и может применяться как инструмент контроля над состоянием операционной среды и действиями пользователей в системе с целью выявления потенциальных злоумышленников как внутренних так и внешних, так и как элемент более сложных адаптивных самоорганизующихся систем защиты информации в ОС.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Оладько А.Ю.* Модель адаптивной многоагентной системы защиты в ОС Solaris 10 // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 210-217.
2. *Oladko A. Yu.* Application immune network to create the protection system of OS Solaris 10 // European Science and Technology: international scientific conference.// Bildungszentrum Rdk e.V. Wiesbaden, Germany 2012. – P. 261-266.
3. *Кашаев Т.Р.* Алгоритмы активного аудита информационной системы на основе технологий искусственных иммунных систем: Автореф. дис. … канд. техн. наук. – Уфа, 2008. – 20 с.
4. *Hoffmann G.W.* (2008) Immune Network Theory. Monograph. URL: www.physics.ubc.ca/~hoffmann/ni.html, 2008 г.
5. *Гвозденко А.* Искусственные иммунные системы как средство сетевой самозащиты // ITC Publishing. URL: http://itc.ua/articles/iskusstvennye_immunnye_sistemy_kak_sredstvo_setevoj_samozashhity_4270.
6. *Котов В.Д., Васильев В.И.* Система обнаружения сетевых вторжений на основе механизмов иммунной модели // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 180-190.
7. *Yoann Vandoorselaere, Laurent Oudot*. Prelude, an Hybrid Open Source Intrusion Detection System // URL: http://www.prelude-ids.org/, 2010.
8. Выбор системы обнаружения атак. URL: http://www.itsecurity.ru, 2007.
9. *Нестерук Ф. Г., Осовецкий Л. Г., Нестерук Г. Ф., Воскресенский С.И.* К моделированию адаптивной системы информационной безопасности // Перспективные информационные технологии и интеллектуальные системы. – 2004. – № 4. – С. 25-31.
10. *Ивахненко А.Г., Савченко Е.А., Ивахненко Г.А., Гергей Т., Надирадзе А.Б., Тоценко В.Г.* Нейрокомпьютеры в информационных и экспертных системах // Нейрокомпьютеры: разработка и применение. – 2003. – № 2.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Оладько Алексей Юрьевич – Волгоградский государственный университет; e-mail: bop-x@yandex.ru; 400062, г. Волгоград, пр-т Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; ассистент.

Oladko Alexey Yuryevich – Volgograd State University; e-mail: bop-x@yandex.ru; 100, University ave, Volgograd , 400062, Russia; phone: +78442460368; the department of Information security; assistant.

УДК 004.056.5, 004.89

А.В. Никишова

ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ МНОГОАГЕНТНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК

Была обоснована актуальность задачи обнаружения атак. Были рассмотрены особенности процесса проведения атаки. Были проанализированы действия злоумышленников различных типов на различных этапах атаки. Было показано, какие методы обнаружения атак необходимо применять на различных шагах реализации атак злоумышленником. Была

предложена модель многоагентной системы обнаружения атак. Была предложена интерпретация результатов анализа событий информационной системы (ИС) методом обнаружения атак. А также представлен алгоритм принятия общего решения агентами на основании нескольких источников сведений о состоянии ИС.

Атака; система обнаружения атак; нейронная сеть; интеллектуальный агент; многоагентная система; принятие совместного решения.

A.V. Nikishova

PRINCIPLES OF MULTI-AGENT INTRUSION DETECTION SYSTEM'S FUNCTIONING

Actualite of the intrusion detection problem has been substantiated. Characteristics of the process of attack implementation have been considered. Different types of intruders' actions during different attack stages have been analyzed. Has been shown what intrusion detection methods should be used on different steps in implementing of intruder's attack. Model of multi-agent intrusion detection system has been suggested. Interpretation of results of information system's (IS) events' analysis by intrusion detection method has been suggested. Also algorithm of making a joint decision based on several sources of information about IS's state has been presented.

Attack; intrusion detection system; neural network; intelligent agent; multi-agent system; make a joint decision.

Современный этап развития ИС основан на достижениях телекоммуникационных технологий, применяемых для распределенной обработки информации [1]. Это обусловило то, что большинство атак имеют распределенный характер. Это подтверждается данным лаборатории Касперского. За 2011 год постоянно увеличивалась сложность атакующих воздействий. Их технологический уровень значительно вырос даже по сравнению с прошлым годом. Зачастую атаки имели многошаговый алгоритм действий и распределенный характер. По данным за первый квартал 2012 года было осуществлено на 28% больше атак, чем за предыдущий квартал. Показатели распространения атакующих воздействий также увеличились на 61 %. [2] Все это подтверждает актуальность исследований в области обнаружения атак.

Как правило, атаки включают в себя следующие шаги [3]:

- сбор данных об объекте атаки;
- осуществление несанкционированного доступа (НСД) к требуемому узлу ИС;
- атакующее воздействие;
- распространение атаки на другие узлы ИС.

Ранее была предложена архитектура типовой информационной системы для задачи обнаружения атак [4]. Обозначим множество событий маршрутизатора как R, множество сетевых пакетов – N, множество событий хоста (как обычной рабочей станции, так и сервера) – W.

На первом шаге злоумышленник собирает информацию об ИС. Например, внешний злоумышленник может выполнять сканирование портов из внешней, по отношению к ИС, сети. Так как ИС отделена от внешней сети маршрутизатором, то на первом шаге внешний злоумышленник порождает подмножество событий $R_1 \subset R$.

Внутренний злоумышленник, находящийся в другом сегменте ИС относительно хоста-цели атаки, на данном этапе выполняет сбор сведений о конфигурации ИС. Для этого он может, например, сформировать запрос к DNS-серверу. Подобными действиями внутренний злоумышленник порождает подмножества событий $R_2 \subset R$ на внутренних маршрутизаторах ИС и пакетов $N_1 \subset N$ сегментов, не содержащих хост-цель атаки.

Внутренний злоумышленник, находящийся в том же сегменте ИС, что и хост-цель атаки, выполняет сбор сведений о самом хосте-цели атаки. Его действия порождают подмножества пакетов $N_2 \subset N$ сегмента, содержащего хост-цель атаки, и событий $W_1 \subset W$ хоста-цели атаки.

Для анализа сведений о порожденных злоумышленником на этом этапе событиях эффективно использовать методы, выявляющие определенные признаки вредоносного поведения, т.е. методы обнаружения злоупотреблений. Это связано с тем, что все операции нарушителя, при помощи которых он получает необходимую ему информацию, в большинстве случаев не вызывают никакого отклонения от нормального поведения ИС.

На втором этапе внешний злоумышленник должен получить НСД к внутренней сети ИС. При этом он порождает подмножество событий $R_3 \subset R$ на маршрутизаторе, отделяющем ИС от внешней сети. После удачного преодоления этого шага, поведение внешнего злоумышленника становится похожим на действия внутреннего злоумышленника, находящегося в другом сегменте ИС относительно хоста-цели атаки, и он выполняет первый и второй шаги аналогичные данному типу злоумышленника.

На втором шаге внутреннему злоумышленнику, находящемуся в другом сегменте ИС относительно хоста-цели атаки, необходимо осуществить НСД к сегменту сети, содержащему хост-цель атаки. Его действия порождают подмножества событий $R_4 \subset R$ на внутренних маршрутизаторах ИС и пакетов $N_3 \subset N$ сегментов, не содержащих хост-цель атаки. После удачного выполнения данного шага, поведение внутреннего злоумышленника, находящегося в другом сегменте ИС относительно хоста-цели атаки, становится похожим на действия внутреннего злоумышленника, находящегося в том же сегменте ИС, что и хост-цель атаки, и он выполняет первый и второй шаги аналогичные данному типу злоумышленника.

На данном шаге внутренний злоумышленник, находящийся в одном сегменте с хостом-целью атаки, пытается получить НСД к хосту-цели атаки. Подобные его действия порождают подмножества пакетов $N_4 \subset N$ сегмента, содержащего хост-цель атаки, и событий $W_2 \subset W$ хоста-цели атаки.

Обнаружение атаки на стадии получения НСД возможно как при помощи методов обнаружения злоупотреблений, так и при помощи методов, реагирующих на отклонения от нормального поведения, т.е. методов обнаружения аномалий. Это объясняется тем, что с одной стороны любое вторжение характеризуется определёнными характерными признаками атаки, а с другой стороны это же вторжение может также быть описано как некоторое отклонение от нормального поведения ИС. Поэтому наиболее эффективным является комбинированное использование данных методов обнаружения атак.

На третьем этапе все типы злоумышленников имеют похожее поведение, их задача повысить привилегии на хосте, чтобы получить доступ к цели атаки. Эти действия порождают подмножество событий $W_3 \subset W$ хоста-цели атаки.

На четвертом этапе злоумышленник осуществляет действия на хосте, которые позволят ему, в случае необходимости, продолжить атаку на ресурсы других узлов ИС. Эти действия порождают подмножество событий $W_4 \subset W$ хоста-цели атаки.

Эффективное выявление атак на стадиях атакующего воздействия и развития атаки возможно при помощи методов обнаружения аномалий, поскольку действия нарушителей на этих этапах могут сильно варьироваться в зависимости от целей проводимой атаки и поэтому не могут быть однозначно определены фиксированным множеством признаков атак.

Так как необходимо использовать и метод обнаружения злоупотреблений, и метод обнаружения аномалий, то был выбран метод обнаружения атак – нейронные сети, которые в зависимости от обучения могут обнаруживать и злоупотребления, и аномалии. Для этого обучающая выборка для нейронной сети формируется так, чтобы она содержала образцы и нормального поведения ИС, и вредоносных действий злоумышленников.

Предложена модель многоагентной системы обнаружения атак (СОА) [5, 6], проводящая распределенный сбор и анализ перечисленных сведений о состоянии ИС (рис. 1).

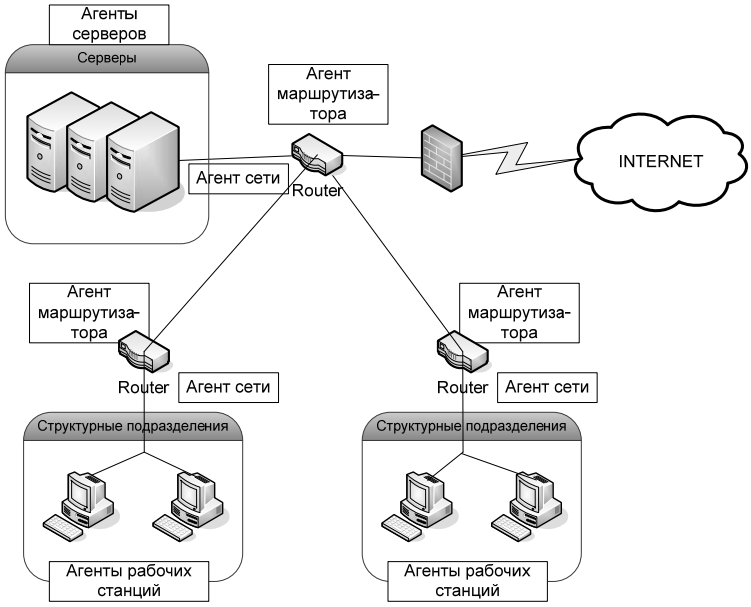

Рис. 1. Многоагентная СОА

Модель включает в себя:

- агентов маршрутизаторов A_R, анализирующих сведения о событиях маршрутизаторов, отражающихся в журнале маршрутизатора, R;
- агентов сети A_N, анализирующих сведения о пакетах, передаваемых по сети, N;
- агентов серверов A_S, анализирующих сведения о событиях, происходящих на серверах ИС, W;
- агентов рабочих станций A_W, анализирующих сведения о событиях, происходящих на рабочих станциях ИС, W.

Многоагентную СОА можно представить в виде графа $G = (A, B)$, где A – множество агентов, B – множество ребер графа; ребро существует тогда и только тогда, когда пара агентов может связаться друг с другом, минуя других агентов. Например, агент маршрутизатора и агент сети, или агент сети и агент рабочей станции связаны между собой ребрами.

База знаний всех агентов представляет собой нейронную сеть. При этом нейронные сети всех агентов обучены на обучающих выборках, содержащих как образцы нормального поведения, так и образцы атакующих воздействий злоумыш-

ленника на ИС, что позволяет агентам классифицировать анализируемое событие как нормальное событие или как атакующее воздействие. Практически выход нейронной сети представляет собой непрерывный сигнал на заданном интервале [a, b], где a – нижняя граница интервала, при получении которой на выходе, событие интерпретируется как атака; b – верхняя граница интервала, при получении которой на выходе, событие интерпретируется как нормальное.

При получении значения c на выходе нейронной сети, величину $p = \frac{c-a}{b-a}$ можно интерпретировать как вероятность, с которой нейронная сеть классифицирует анализируемое событие как нормальное. Чем меньше значение p, тем ближе c к нижней границе интервала a, и тем с большей вероятностью событие может быть классифицировано как атака.

Так как выход нейронной сети интерпретируется как вероятность, то исходный интервал [a, b] для удобства разбивается на 5 подинтервалов $[a_1,b_1]$, $(a_2,b_2]$, $(a_3,b_3]$, $(a_4,b_4]$, $(a_5,b_5]$, где $a_1 = a$, $a_i = b_{i-1}$ для i=2..5, $b_5 = b$. В зависимости от того, в какой интервал попал очередной выход нейронной сети, т.е. с какой вероятность событие было отнесено к нормальному, оно относится к одному из классов опасности, и агенты СОА могут выполнять различные действия в соответствии с настройками многоагентной СОА:

- запись события в журнал СОА;
- информирование администратора о произошедшем событии;
- блокирование процесса;
- разрыв соединения;
- прерывание процесса.

Кроме этого, если выход нейронной сети не попал ни в крайний левый интервал, т.е. не был отнесен к высшему классу опасности, ни в крайний правый интервал, т.е. не был отнесен к низшему классу опасности, то агенты СОА принимают совместное решение о том, как классифицировать данное событие, чтобы уменьшить вероятность ошибки при принятии решения одним агентом, путем сопоставления данных из нескольких источников.

Для принятия совместного решения, каждый агент формирует свои предпочтения, т.е. указывает, с каким приоритетом он относит событие к каждому из 5 классов. При этом формируются предпочтения вида $O_i \succ O_j \succ O_k \succ O_l \succ O_m$, где i определяет интервал, в который попал выход нейронной сети. Следующий класс в предпочтениях агента определяется как следующий ближайший подинтервал к значению выхода нейронной сети c, используя следующий алгоритм:

Если $\left(c > a_i + \frac{b_i - a_i}{2} \right)$ *то*

$j=i+1;\ a_j = a_i;\ b_j = b_{i+1}$

иначе

$j=i-1;\ a_j = a_{i-1};\ b_j = b_i$

Когда к предпочтению присоединяется один из крайних подинтервалов, то остальные подинтервалы добавляются к предпочтению в порядке удаления от текущего предпочтения.

После формирования предпочтений каждого агента, агенты объединяются в группы для принятия совместного решения. Согласно действиям злоумышленников, рассмотренных ранее, группа агентов A, например, для внешнего злоумышленника, выглядит следующим образом $A = \left\{A_R^1, A_N^1, A_R^2, A_N^2, A_W^1\right\}$. Причем в графе G, должен существовать путь, включающий всех агентов группы, т.е. $\exists G_1 = \left(A_R^1, A_N^1, A_R^2, A_N^2, A_W^1\right)$.

Общее решение находится голосованием. Победителем голосования, т.е. совместно принятым классом, к которому будет отнесено событие, будет уровень-победитель по Кондорсе, соответственно удовлетворяющий условию $\forall o' \in O, \#(o \succ o') \geq \#(o' \succ o)$. В связи с особенностью формирования предпочтений агентов, исключен так называемый парадокс Кондорсе, при котором нельзя выявить победителя. [7]

Предложенная многоагентная СОА позволяет повысить точность классификации событий ИС, т.е. уменьшить ошибки первого и второго рода.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Прокопьева М.В.* Информационные системы // URL: http://mimika87.narod2.ru/osnovnie_etapi_razvitiya_informatsionnih_sistem (дата обращения: 29.09.2012)
2. *Наместников Ю.* Развитие информационных угроз в первом квартале 2012 года // SecureList/ URL: http://www.securelist.com/ru/analysis/208050757/ Razvitie_informatsionnykh_ugroz_v_pervom_kvartale_2012_goda (дата обращения: 08.09.2012).
3. *Сердюк В.* Вы атакованы – защищайтесь! // BYTE. – 2003. – № 9 (61). URL: http://www.bytemag.ru/articles/detail.php?ID=9036 (дата обращения: 06.10.2011).
4. *Никишова А.В.* Архитектура типовой информационной системы для задачи обнаружения атак // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 104-109.
5. *Никишова А.В.* Архитектура многоагентной системы обнаружения атак. Актуальные вопросы информационной безопасности региона в условиях модернизации общества и внедрения инновационных технологий: материалы Региональной научю-практ. Конф., г. Волгоград, 9-10 июня 2011 г. – В.: Изд-во ВолГУ, 2011. – С. 101-103.
6. *Никишова А.В.* Интеллектуальная система обнаружения атак на основе многоагентного подхода // Вестник Волгоградского государственного университета. Серия 10. Инновационная деятельность. – 2011. – Вып. 5. – С. 35-37.
7. *Shoham Y., Leyton-Brown K.* Multiagent systems. Algorithmic, game-theoretic, and logic foundations. Cambridge University. –2008. – P. 256-260.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Никишова Арина Валерьевна – Волгоградский государственный университет; e-mail: arinanv@mail.ru; 400062, г. Волгоград, пр. Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; старший преподаватель.

Nikishova Arina Valerievna – Volgograd State University; e-mail: arinanv@mail.ru; 100, Universitetsky pr. Volgograd, 400062, Russia; phone: +78442460368; the department of informational security; senior lecturer.