Алгоритм резервирования системы обнаружения атак в сети специального назначения

Т. В. Лебедкина, email: alina010570@mail.ru
В. А. Львов

Краснодарское высшее военное училище
имени генерала армии С.М. Штеменко

Аннотация. *В статье рассматривается алгоритм реализации процесса резервирования системы обнаружения атак в сетях специального назначения. Описывается последовательность действий, поясняющая сущность разработанного алгоритма. Делается вывод о том, что разработанный алгоритм устраняет некоторые из недостатков аналогов и обеспечивает повышение живучести системы обнаружения атак.*

Ключевые слова: *вычислительная сеть, компьютерная атака, система обнаружения атак, несанкционированный доступ, сетевая разведка.*

Введение

Защита систем обнаружения атак (СОА) в сетях специального назначения, одна из задач для служб информационной безопасности, работающих на критически важных объектах России. На важность данной темы влияет рост числа компьютерных атак, направленных на нарушение доступности, целостности или конфиденциальности критических инфраструктур. Поэтому, в условиях всё большей зависимости граждан России от внедряемых во все сферы нашей жизни информационных технологий, небезопасное внедрение или управление которыми может повлечь за собой тяжелые последствия, больше внимания должно уделяться защите информации с использованием СОА.

Система обнаружения атак– это система, собирающая информацию из различных точек компьютерных сетей и анализирующая эту информацию для выявления признаков несанкционированной деятельности и попыток нарушений защиты.

СОА обеспечивают контроль функционирования компонентов системы защиты информации (межсетевых экранов, средств идентификации и аутентификации, управления доступом, шифрования, вирусных сканеров и т.п.), являющихся основными объектами

© Лебедкина Т. В., Львов В. А., 2023

нападения. Нарушение работоспособности отмеченных компонентов защиты может повлечь за собой серьезные нарушения безопасности информации. Контролируя файлы регистрации событий, сгенерированные этими системами, и проводя мониторинг выполняемых в системе действий на наличие несанкционированного доступа, СОА обеспечивают дополнительную защиту компонентов самой системы защиты.

Для классификации систем обнаружения сетевых атак используются следующие первичные классификационные признаки:

метод обнаружения;

этап сетевой атаки, на котором происходит ее обнаружение;

уровень централизации решений в системе о наличии атаки;

уровень информационной системы, на котором размещаются сенсоры системы обнаружения атак.

Совокупность этих признаком позволяет систематизировать представления практически обо всех известных сегодня системах обнаружения сетевых атак. Классификационная схема, построенная по указанным признакам, приведена на рисунке 1 [2].

1. Исследование процесса резервирования СОА

Компьютерная атака может быть направлена как на информацию, хранящуюся и обрабатываемую в автоматизированной системе, так и на саму систему обнаружения атак.

Для того чтобы выход системы обнаружения атак из строя не оказал критического воздействия на автоматизированную систему необходимо обеспечить беспрерывную работу СОА. Для этого необходимо разработать алгоритмы процессов резервирования и аварийного восстановления системы обнаружения атак в сетях специального назначения.

В целях обеспечения выполнения требований, предъявляемых к автоматизированным системам специального назначения, корректная работа алгоритмов процесса резервирования и аварийного восстановления системы обнаружения атак должна быть обусловлена следующими условиями:

– наличие непрерывно работающего сервера;

– способность алгоритма определять причину выхода системы обнаружения атак из строя;

– высокая частота обработки данных;

– автоматизированное сообщение администратору автоматизированной системы о выходе системы обнаружения атак из строя.

Рис. 1. Классификация систем обнаружения атак

Для того чтобы обнаружить в контролируемом пространстве (сетевом трафике или журнале регистрации) нарушения политики безопасности, необходимо уметь их идентифицировать и отличать от обычных событий безопасности. В качестве таких признаков атак могут выступать:

– повтор определенных событий;

– неправильные или несоответствующие текущей ситуации команды;

– использование уязвимостей;

– несоответствующие параметры сетевого трафика;

– непредвиденные атрибуты;

– дополнительные знания о нарушениях [2].

Любые средства защиты (межсетевые экраны, серверы аутентификации, системы разграничения доступа и т. п.) используют в своей работе одно или два из указанных условий, в то время как системы обнаружения атак (в зависимости от их реализации) задействуют практически все указанные признаки [3-6].

2. Описание алгоритма реализации процесса резервирования и аварийного восстановления СОА

В любой момент времени в СОА ведется журнал опережающей записи. В журнале описываются все изменения, применяемые к файлам данных системы обнаружения атак. Он необходим в первую очередь для защиты от сбоев. При возникновении сбоя системы, система обнаружения атак будет восстановлена с помощью «проигрывания» всех записей журнала, сделанных с момента последней контрольной точки. При необходимости восстановления СОА, восстанавливается резервная копия, а затем проигрываются записи из сохраненных файлов журнала, для доведения восстановленной системы обнаружения атак до актуального состояния. Применение этого подхода сложное, но у него есть несколько значительных преимуществ:

На начальный момент времени не требуется идеально целостная резервная копия. Все внутренние несоответствия в резервной копии будут исправлены при проигрывании журнала. Таким образом, не требуется наличия возможностей по созданию снимка файловой системы, достаточно инструмента для архивирования.

Так как нет ограничения на длину последовательности файлов журнала опережающей записи для последующего проигрывания, непрерывное резервное копирование может быть достигнуто просто непрерывным архивированием файлов журнала. Это особенно важно для больших СОА, когда отсутствует возможность часто делать полное резервное копирование.

Не является необходимым обязательное проигрывание содержимого журнала до самого конца.

В случае постоянной передачи порции файлов журнала опережающей записи на другую систему, на которой была загружена та же резервная копия СОА, возможно получение системы горячего резерва: в любой момент может быть подключена вторая система, при этом на ней будет ближайшая к текущей версия СОА [2].

Как и в случае резервного копирования на уровне файловой системы, этим методом можно восстановить только весь кластер системы обнаружения атак, но не его подразделы. Таким образом, требуется настроить и проверить процедуру архивирования файлов журнала перед тем, как сделать первую резервную копию СОА. В соответствии с этим, в первую очередь рассматривается архивирование файлов журнала опережающей записи.

В общем случае, работающая система резервирования производит неограниченную по длине последовательность записей в журнал

опережающей записи. Система физически делит эту последовательность на сегментные файлы журнала, которые имеют размер 16 МБ.

При архивировании данных журнала необходимо брать содержимое каждого сегментного файла по мере их заполнения и где-то сохранять эти данные перед тем, как очистить сегментный файл для повторного использования. В зависимости от приложения и доступного оборудования, сохранять эти данные можно несколькими способами:

- ✓ Копированием сегментных файлов на подсоединенный через NFS каталог на другой системе.
- ✓ Записью их на магнитную ленту (при условии, что существует способ идентификации первоначального имени каждого файла).
- ✓ Сбором их вместе и записью на лазерный диск, или куда-либо еще полностью.

Для того, чтобы предоставить администратору максимальную свободу выбора, алгоритм резервирования не делает никаких предположений о том, как именно производится архивирование. Напротив, алгоритм позволяет администратору определить, какую консольную команду следует использовать для копирования заполненного сегмента туда, куда он должен быть скопирован. Команда может быть простой или может вызывать в консоли сложный скрипт.

Для обеспечения этого основной и резервный серверы работают совместно, хотя связь между ними при этом достаточно слабая. Основной сервер работает в режиме непрерывного архивирования, а каждый резервный в режиме непрерывного восстановления, читая файлы с основного. Такая реализация не требует никаких изменений в системе обнаружения атак или таблицах, и потому предполагает меньшие затраты на администрирование по сравнению с некоторыми другими способами репликации.

Непосредственное перемещение записей с одного сервера системы обнаружения атак на другой обычно описывается как передача журнала транзакций. Реализуется передача журнала транзакций на уровне файлов, что означает передачу записей одним файлом (сегментом) за раз. Файлы могут быть легко переданы на любое расстояние будь то соседняя система, система, расположенная в том же месте, или расположенная на большом расстоянии. Требуемая пропускная способность при таком способе зависит от количества исполняемых транзакций в единицу времени на основном сервере. Передача журнала транзакций на уровне записей более детализирована и обеспечивает потоковую передачу изменений по сети.

Передача журнала транзакций носит асинхронный характер, то есть записи передаются только после подтверждения транзакции. Таким

образом, существует временное окно для потери данных в случае сбоя основного сервера, еще не переданные транзакции будут потеряны. Размер такого окна потери данных может быть ограничен и быть уменьшен вплоть до нескольких секунд, если это требуется.

Скорость восстановления достаточно хорошая тогда, когда резервный сервер от полной доступности отделяет небольшое время с момента активации. Резервный сервер может также быть использован для исполнения запросов «только чтения», в этом случае он называется сервером «горячего» резерва.

Обычно разумно создавать основной и резервные серверы максимально возможно похожими, как минимум с точки зрения сервера системы обнаружения атак. Аппаратное обеспечение не обязательно должно быть одинаковым, но опыт показывает, что поддержка двух идентичных систем на протяжении их жизни и функционирования гораздо легче чем различных. В общем случае, передача журнала между отличающимися основной версией серверами невозможна [2].

В режиме резервирования сервер непрерывно применяет журнал транзакций, полученный с основного сервера. Резервный сервер может получать данные из архива или непосредственно с основного сервера через TCP соединение (потоковая репликация). Резервный сервер также может пытаться восстановиться с журнала, расположенного в подкаталоге кластера резервного сервера [5]. Это обычно происходит после перезапуска сервера, когда резервный сервер снова выполняет копирование журнала регистрации, полученного с основного перед перезапуском, но существует возможность помещать вручную файлы в любое время для их применения. В процессе запуска резервный сервер начинает восстанавливать весь журнал, доступный в архиве. По достижению конца журнала в архиве он пытается восстановить журнал из каталога. Если это не удалось, и настроена потоковая репликация, резервный сервер пытается установить соединения с основным сервером и запустить потоковую репликацию с последней корректной записи, найденной в архиве. Если это не удалось, или не настроена потоковая репликация, или соединение было завершено, резервный сервер возвращается к первому шагу и снова пытается восстановить файл из архива. Этот цикл по опросу архива и потоковой репликации продолжается до остановки сервера или обнаружения необходимости процедуры восстановления после сбоя с помощью триггерного файла. Режим резервирования завершается, и сервер переключается в нормальный режим функционирования в случае обнаружения триггерного файла. Алгоритм реализации процессов резервирования выглядит в соответствии с рисунком 2.

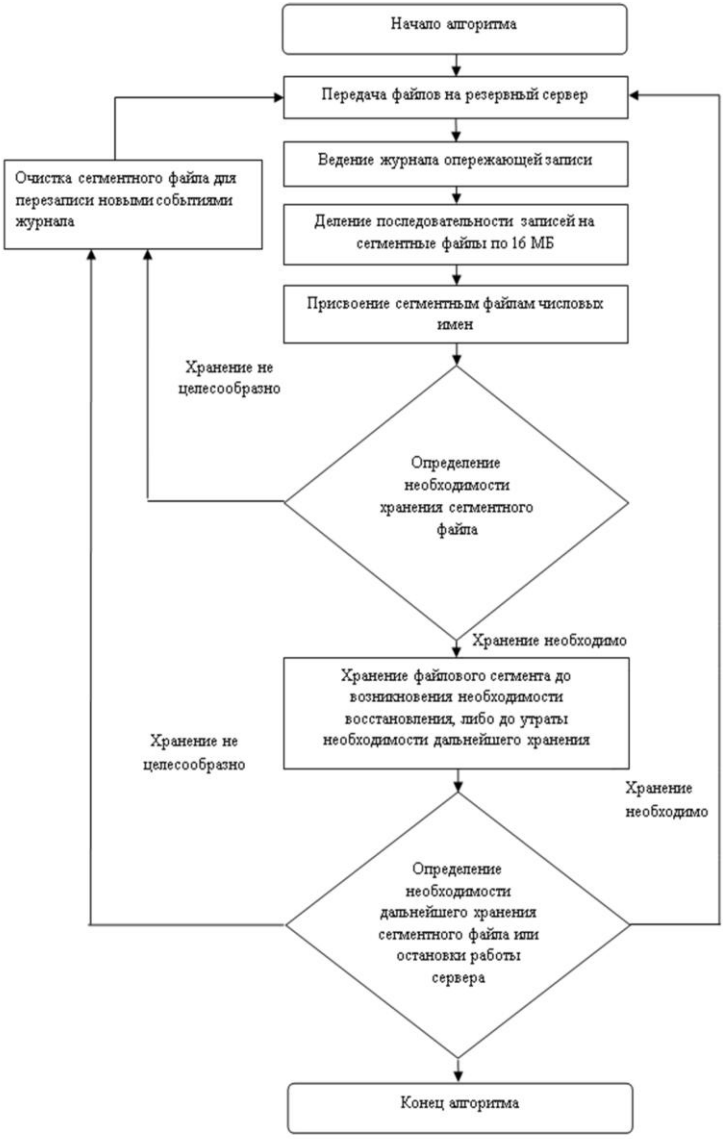

Рис. 2. Алгоритм реализации процесса резервирования СОА

Заключение

С целью повышения живучести системы обнаружения атак в сетях специального назначения исследована реализация процесса резервирования СОА. В ходе работы разработан эффективный алгоритм, который способен успешно восстановить систему обнаружения атак, случае выхода системы из строя.

Список литературы

1. Шерстобитов, Р. С. Маскирование интегрированных сетей связи ведомственного назначения / Р. С. Шерстобитов, С. Р. Шарифуллин, Р. В. Максимов // Системы управления, связи и безопасности. – 2018. – № 4. – С. 136–175.
2. Лукацкий, А. В. Обнаружение атак / А. В. Лукацкий. – 2-е изд. – Санкт-Петербург : БХВ-Петербург, 2003. – 596 с.
3. Соколовский, С. П. Концептуализация проблемы проактивной защиты интегрированных информационных систем / С. П. Соколовский, Д. Н. Орехов // Научные чтения имени профессора Н. Е. Жуковского: сб. научн. стат. VIII Междунар. науч. метод. конф. (Краснодар, 20–21 декабря 2017 г.). – Краснодар, 2018. – С. 47–52.
4. Соколовский, С. П. Способы снижения информативности демаскирующих признаков средств проактивной защиты вычислительных сетей / С. П. Соколовский, А. Л. Гаврилов, Д. Н. Орехов // Научные труды Кубанского государственного технологического университета. – 2018. – № 3. – С. 211-220.
5. Соколовский, С. П. Обоснование задач динамического конфигурирования информационных систем для обеспечения их безопасности / С. П. Соколовский, И. С. Ворончихин // Радиоэлектронная борьба в современном мире: сб. тр. участников I Всерос. научно-методич. конф. "Радиоэлектронная борьба в современном мире" (Воронеж, 1-2 октября 2019 г.). – Воронеж, 2019. – С. 300-304.
6. Соколовский, С. П. Поиск новых технических решений по маскированию структуры вычислительных сетей на основе динамического конфигурирования их параметров / С. П. Соколовский, И. С. Ворончихин, А. Д. Гритчин // Решетневские чтения: сб. тр. участников XXIII Междунар. науч.-практич. конф., посвященной памяти генерального конструктора ракетно-космических систем академика М. Ф. Решетнева "Решетневские чтения" (Красноярск, 11-15 ноября 2019 г.). – Красноярск, 2019. – Ч. 2. – С. 447-448.