Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Система контроля и анализа сетевого взаимодействия для предотвращения сетевых атак

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Павлова Андрея Игоревича

Научный руководитель

доцент, к.п.н. _____ А.С. Гераськин

31.12.2016 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

31.12.2016 г.

Саратов 2017

ВВЕДЕНИЕ

Сложность современных компьютерных сетей связана с большим количеством их типов, вариативностью используемых технологий и предоставляемых услуг, а также с возросшим числом пользователей этих сетей. Вслед за увеличивающимся числом пользователей, растет и количество передаваемой по сети информации. Как следствие, число угроз сетевой безопасности возрастает, а задача их обнаружения и предотвращения значительно осложняется. Сетевым администраторам требуются автоматизированные средства, которые будут предоставлять информацию об элементах сети и помогать управлять сетевой инфраструктурой.

Для эффективной обработки высокоскоростного трафика должен быть найден компромисс между вычислительными возможностями и детальностью предоставляемой информации. Чем подробней собираемая информация, тем эффективней основанный на ней анализ, но тем выше вычислительные затраты на ее обработку.

При написании работы, ставились следующие задачи:

1) Произвести анализ существующих подходов к сбору информации о сетевом взаимодействии и построить, на основе наиболее эффективных из них, системы, осуществляющие сбор и хранение информации. При этом информация, перед помещением в базу, должна быть преобразована к единому формату, удобному для дальнейшей обработки.

2) Разработать систему, осуществляющую визуализацию собранных данных. Информация должна быть представлена наглядно и давать четкое понимание того, что происходит в сети.

3) Разработать систему, осуществляющую анализ собранных данных, как в режиме реального времени, так и на основе долговременно хранящейся информации, с целью обнаружения аномальной активности в сети. При обнаружении такого рода активности, система должна иметь возможность

как оповещать об этом администратора сети, так и предотвращать ее дальнейшее воздействие.

4) Обеспечить возможность автоматизированного внедрения разработанного системного комплекса в функционирующую компьютерную сеть.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 6 приложений. Общий объем работы – 68 страниц, из них 40 страниц – основное содержание, включая 10 рисунков и 2 таблицы, список использованных источников из 21 наименования.

КРАТКОЕ СОДЕРЖАНИЕ

1. Система обнаружения и предотвращения сетевых вторжений

В данном разделе описываются системы обнаружения и предотвращения сетевых вторжений, выделяются и рассматриваются их основные логические элементы, которыми являются:

- подсистема сбора информации;
- подсистема анализа;
- подсистема представления;
- подсистема предотвращения.

В подразделе 1.1 «Методы обнаружения вторжений» приводится классификация методов обнаружения вторжений, а в подразделе 1.2 «Анализ аномального поведения в сети» более подробно рассматриваются методы, применяемые в рамках обнаружения аномалий сетевого трафика.

Выделяются две группы методов: с контролируемым обучением (обучение с учителем), и с неконтролируемым обучением (обучение без учителя).

2. Выбор технологии для сбора информации

В данном разделе описывается, какая информация о сетевом взаимодействии может быть получена и использована для анализа. Возможна обработка:

- полного содержимого пакетов;
- статистики потока;
- количественной статистики;
- системных журналов.

Для каждого из подходов описываются преимущества и недостатки, на основе которых принимается решение о сборе статистики сетевого потока и анализа системных журналов. Такая комбинация в совокупности дает неплохое представление о сетевом взаимодействии.

При выборе потоковой технологии рассматриваются такие протоколы как NetFlow, SFlow, JFlow, Netstream, IPFIX. Технологии различных производителей не совместимы друг с другом, но работы в этом направлении уже ведутся. Документ RFC 3917 [9] стандартизирует версию технологии NetFlow под названием IPFIX, что должно способствовать ее распространению. Кроме того, протокол IPFIX является продолжением протокола NetFlow v9, поэтому принимается решение использовать именно его.

3. IPFIX протокол

Данные раздел полностью посвящен описанию IPFIX протокола. В подразделе 3.1 «Основные понятия» вводится базовая терминология, и описываются основные элементы, присущие методам потокового сбора. В подразделе 3.2 «Информационные элементы IPFIX протокола» описываются метрики, которые могут быть собраны с помощью IPFIX. В подразделе 3.2 «Способы применения IPFIX протокола» рассматриваются возможности использования данных, собранных с помощью IPFIX, для учета использования сетевых ресурсов, анализа, администрирования трафика и обнаружения сетевых атак и вторжений.

4. Разработка системы обнаружения и предотвращения вторжений

В данном разделе описывается разработанная в рамках данной работы система обнаружения и предотвращения сетевых вторжений. В подразделе 4.1 «Используемые технологии» перечисляются применяемые в процессе функционирования системы технологии, и дается объяснение, почему используются именно они.

Для хранения информации используется InfluxDB. Любой график сетевой активности представляет собой изменения определенных параметров в течение некоторого периода времени (час, сутки и т.д.) Для построения графика нужно обработать статистические данные, представленные в виде пар «время - значение» за заданный промежуток времени. Данные такого

формата называются временным рядом. InfluxDB – это база данных, разработанная как раз для хранения таких временных рядов.

Для представления данных используется Grafana. Она позволяет создавать панели, графики и таблицы и имеет широкий набор возможностей по сортировке и выборке необходимых данных.

Чтобы не сильно задумываться об операционной системе на хостах и иметь возможность быстро и просто внедрять новые модули разработанной системы, все ее компоненты запускаются в виде Docker-контейнеров.

Разработанная система написана на языке Python и для установки своих модулей на удаленные хосты использует библиотеку Fabric, работающую по SSH.

В подразделе 4.2 «Архитектура» описывается общая структура реализованной системы и каждая из ее частей по отдельности.

Система состоит из 7 основных компонент:

1) Сборщик информации из IPFIX потоков;
2) Сборщики информации из системных журналов;
3) База данных InfluxDB, в которой хранятся собранные данные;
4) Панель визуализации собранных метрик Grafana;
5) Анализаторы собранных метрик;
6) Модуль оповещения об обнаруженных угрозах;
7) Модуль предотвращения воздействия обнаруженных угроз.

Для сбора данных из системных журналов и для анализа собранных метрик реализована система расширений, позволяющая описывать новые способы сбора информации и ее анализа с помощью конфигурационных файлов.

Более подробно о способах настройки говорится в подразделе 4.3 «Конфигурация». В нем описано, как указать расположение компонент на хостах, как включить оповещения посредством электронной почты и SMS и

как включить режим активного реагирования на зафиксированные анализаторами угрозы.

В подразделе 4.4 «Установщик» описывается процесс автоматизированного внедрения разработанной системы с помощью написанного модуля установки. В этом же разделе даются советы по расположению компонент относительно друг друга и перечисляются требования к системе, необходимые для успешной установки. К этим требованиям относятся наличие Docker процесса на всех задействованных хостах и наличие SSH соединения до всех хостов с хоста, с которого происходит установка.

В подразделе 4.5 «Аналоги разработанной системы» производится сравнение реализованной системы с существующими аналогами, основные выводы которого содержатся в заключении данного документа.

Работа завершается приложениями.

В приложении А «Листинг модуля работы с InfluxDB» содержится исходный код модуля взаимодействия с базой данных InfluxDB.

В приложении Б «Листинг сборщика IPFIX» содержится исходный код IPFIX коллектора. Он включает в себя главный модуль, осуществляющий сбор IPFIX потоков в формате, непригодном для анализа, а также файлы, необходимые для приведения полученных IPFIX структур в типы данных, пригодные для обработки.

В приложении В «Листинг сборщика на основе журналов» содержится исходный код коллектора на основе системных журналов, поддерживающего систему расширений.

В приложении Г «Листинг модуля анализа» приводится исходный код модуля анализа, модуля оповещений и модуля предотвращений. В этом приложении также представлен механизм расширений, позволяющий добавлять в систему новые анализаторы.

В приложении Д «Файлы конфигурации» содержатся примеры конфигурационных файлов для системы в целом и для сборщиков и анализаторов в частности.

В приложении Ж «Листинг установщика» представлен исходный код, отвечающий за процесс установки и обновления всех модулей системы.

ЗАКЛЮЧЕНИЕ

На основе исследования существующих методов сбора информации о сетевом взаимодействии, было решено, в качестве основного способа, использовать анализ сетевых потоков (в частности протокол IPFIX), а в качестве дополнительного – анализ системных файлов.

В рамках практической части был реализован комплекс программных средств, осуществляющий сбор, преобразование, хранение, представление и анализ данных о сетевом взаимодействии. Данные, собираемые с IPFIX-экспортеров и системных журналов, отправляются на хранение в базу данных InfluxDB. Затем они используются для отображения в виде графиков и таблиц в Grafana и подвергаются анализу с помощью отдельного модуля. При обнаружении признака аномальной активности, имеется возможность оповестить администратора (посредством email и SMS), а также автоматически выполнить действие по предотвращению ее дальнейшего воздействия.

Разработанные системы предоставляют унифицированный интерфейс для работы с собранными метриками и гибкую модель расширений, позволяющую как добавлять сбор новых метрик, так и использовать новые алгоритмы для анализа уже существующих. Благодаря этому они могут быть использованы для реализации и разработки статистических алгоритмов анализа сетевого взаимодействия.

Также был реализован модуль, обеспечивающий автоматизированную установку данного комплекса в изолированных Docker-контейнерах. Благодаря контейнерной архитектуре достигается независимость от операционных систем и простота добавления и удаления компонент с сетевых узлов. А благодаря использованию специализированной на хранении временных рядов базе данных, обеспечивается лучшая производительность и надежность по сравнению с SQL базами данных.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Слюсаренко, И. М. Системы и методы обнаружения вторжений: современное состояние и направления совершенствования [Электронный ресурс] / И. М. Слюсаренко // CIT Forum [Электронный ресурс] : [сайт]. URL: http://citforum.ru/security/internet/ids_overview (дата обращения: 14.15.2016). Загл. с экрана. Яз. рус.

2 Bhuyan, M. H. Network Anomaly Detection: Methods, Systems and Tools [Электронный ресурс] / M. H. Bhuyan // IEEE COMMUNICATIONS SURVEYS & TUTORIALS [Электронный ресурс] : [сайт]. URL: http://www.nr2.ufpr.br/~jefferson/pdf/Network_Anomaly_Detection-Methods,_Systems_and_Tools.pdf (дата обращения: 14.15.2016). Загл. с экрана. Яз. англ.

3 Soule, A. Combining Filtering and Statistical Methods for Anomaly Detection [Электронный ресурс] / A. Soule // USENIX [Электронный ресурс] : [сайт]. URL: http://projects.laas.fr/METROSEC/soule.pdf (дата обращения: 14.15.2016). Загл. с экрана. Яз. англ.

4 Celeda, P. Network Security Monitoring and Behavior Analysis [Электронный ресурс] / P. Celeda // GEANT [Электронный ресурс] : [сайт]. URL: http://services.geant.net/cbp/Knowledge_Base/Network_Monitoring/Documents/gn3-na3-t4-cbpd133.pdf (дата обращения: 24.09.2016). Загл. с экрана. Яз. англ.

5 Ivanovic, I. Recommendations for Network Traffic Analysis Using the NetFlow Protocol [Электронный ресурс] / I. Ivanovic // GEANT Association [Электронный ресурс] : [сайт]. URL: http://services.geant.net/cbp/Knowledge_Base/Network_Monitoring/Documents/gn4_na3-t2_abpd104_v2_recommendations_for_network_traffic_analysis_using_the_netFlow_protocol.pdf (дата обращения: 24.09.2016). Загл. с экрана. Яз. англ.

6 Ahonen, P. Constructing network security monitoring systems [Электронный ресурс] / P. Ahonen // VTT Technical Research Centre of Finland [Электронный ресурс] : [сайт]. URL: http://www.vtt.fi/inf/pdf/tiedotteet/2011/T2589.pdf (дата обращения: 18.09.2016). Загл. с экрана. Яз. англ.

7 Bejtlich, R. The Practice of Network Security Monitoring [Электронный ресурс] / R. Bejtlich // No starch press [Электронный ресурс] : [сайт]. URL: http://pdf.th7.cn/down/files/1502/The%20Practice%20of%20Network%20Security%20Monitoring.pdf (дата обращения: 18.09.2016). Загл. с экрана. Яз. англ.

8 Питутин, В. В. Что такое IPFIX? [Электронный ресурс] / В. В. Питутин // SoftPi [Электронный ресурс] : [сайт]. URL: http://softpi.com.ua/files/IPFIX.pdf (дата обращения: 20.09.2016). Загл. с экрана. Яз. рус.

9 RFC 3917: Requirements for IP Flow Information Export (IPFIX) [Электронный ресурс] // Internet Engineering Task Force [Электронный ресурс] : [сайт]. URL: https://tools.ietf.org/html/rfc3917 (дата обращения: 23.09.2016). Загл. с экрана. Яз. англ.

10 RFC 7012: Information Model for IP Flow Information Export (IPFIX) [Электронный ресурс] // Internet Engineering Task Force [Электронный ресурс] : [сайт]. URL: https://tools.ietf.org/html/rfc7012 (дата обращения: 24.09.2016). Загл. с экрана. Яз. англ.

11 RFC 5472: IP Flow Information Export (IPFIX) Applicability [Электронный ресурс] // Internet Engineering Task Force [Электронный ресурс] : [сайт]. URL: https://tools.ietf.org/html/rfc5472 (дата обращения: 22.09.2016). Загл. с экрана. Яз. англ.

12 Документация InfluxDB [Электронный ресурс] // InfluxData [Электронный ресурс] : [сайт]. URL: https://docs.influxdata.com/influxdb/v1.0 (дата обращения: 14.09.2016). Загл. с экрана. Яз. англ.

13 Документация Grafana [Электронный ресурс] // Grafana [Электронный ресурс] : [сайт]. URL: http://docs.grafana.org (дата обращения: 14.09.2016). Загл. с экрана. Яз. англ.

14 Документация Docker [Электронный ресурс] // Docker [Электронный ресурс] : [сайт]. URL: https://docs.docker.com (дата обращения: 14.09.2016). Загл. с экрана. Яз. англ.

15 SoftPI Flow Collector [Электронный ресурс] // SoftPI [Электронный ресурс] : [сайт]. URL: http://softpiua.com/ru/продукты/softpi-flow-collector.html (дата обращения: 26.09.2016). Загл. с экрана. Яз. рус.

16 nProbe User's Guide [Электронный ресурс] // nTop [Электронный ресурс] : [сайт]. URL: https://github.com/ntop/nProbe/raw/master/doc/nProbe-UsersGuide.pdf (дата обращения: 14.09.2016). Загл. с экрана. Яз. англ.

17 Fabric's documentation [Электронный ресурс] // Fabric [Электронный ресурс] : [сайт]. URL: http://docs.fabfile.org (дата обращения: 15.12.2016). Загл. с экрана. Яз. англ.

18 Принимаем и отправляем СМС при помощи GSM-модема [Электронный ресурс] // журнал Хакер [Электронный ресурс] : [сайт]. URL: https://xakep.ru/2015/04/07/195-sms (дата обращения: 15.12.2016). Загл. с экрана. Яз. рус.

19 Документация sms.ru [Электронный ресурс] // sms.ru [Электронный ресурс] : [сайт]. URL: http://sms.ru/?panel=api (дата обращения: 15.12.2016). Загл. с экрана. Яз. рус.

20 Документация smsc.ru [Электронный ресурс] // smsc.ru [Электронный ресурс] : [сайт]. URL: http://smsc.ru/api (дата обращения: 15.12.2016). Загл. с экрана. Яз. рус.

21 Документация smspilot.ru [Электронный ресурс] // smspilot.ru [Электронный ресурс] : [сайт]. URL: http://www.smspilot.ru/apikey.php (дата обращения: 15.12.2016). Загл. с экрана. Яз. рус.