МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Разработка системы обнаружения вторжений

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Епифанова Александра Романовича

Научный руководитель
доцент, к.п.н. _____ А. С. Гераськин
21.01.2023 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
21.01.2023 г.

Саратов 2023

ВВЕДЕНИЕ

В наши дни электронный документооборот, онлайн сервисы и приложения достигли огромного количества. Всемирная сеть все больше влияет на нашу жизнь, все большее количество конфиденциальных данных хранится в сети. Как пример, Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг», на котором хранится такая информация как паспортные данные, ИНН, СНИЛС и другие. Число утечек информации в первом полугодии 2022 года выросло почти в два раза в мире и в полтора раза – в России (по сравнению с 1 полугодием 2021 года). Во всем мире в первой половине 2022 года «утекло» около 3 млрд записей персональных данных и платежной информации[1]. В связи с этим, это порождает повышенную опасность утечки конфиденциальной информации и, соответственно, требуется повышенное внимание к безопасности таких сетей и систем. В небольших компаниях мало обращают внимание на эту проблему и считают, что достаточно установки простейших антивирусных пакетов и разграничения прав доступа к ресурсам. Но на практике этих мер зачастую недостаточно. Большое влияние имеет человеческий фактор и зачастую проблемы в безопасности связаны с невнимательностью или с халатностью администраторов безопасности. По статистике большинство взломов и утечек конфиденциальных данных из серверов, обслуживающих сервисы, связанные с электронной коммерцией, происходит по причине игнорирования администраторами безопасности ошибок, которые на первый взгляд кажутся малозначительными. Но в результате оказывается, что именно из-за таких ошибок конфиденциальные данные становятся доступными злоумышленникам.

Важным аспектом в обеспечении безопасности является обнаружение попыток несанкционированного доступа к системе в реальном времени и их

[1] Аносонов, Д. Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года [Электронный ресурс] / Д. Аносонов // Экспертно-аналитический центр InfoWatch [Электронный ресурс]. – URL: https:// www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-annykh-za-1-polugodie-2022-goda_1.pdf (дата обращения 25.11.2022). – Загл. с экрана. – Яз. рус.

пресечение. Невозможно создать комплексно защищенную сеть без средств, обеспечивающих защиту от несанкционированного доступа.

Один из первостепенных элементов комплексной системы обеспечения безопасности – это средства обнаружения вторжений. Обнаружение вторжений является процессом оценки аномальных действий, которые происходят в контролируемой информационной среде.

Целью данной работы является рассмотрение и реализация методов статистического анализа для обнаружения сетевых вторжений.

В процессе работы необходимо решить следующие задачи:

1. Рассмотреть анатомию сетевых атак.
2. Подробно проанализировать атаки типа «отказ в обслуживании».
3. Рассмотреть и изучить статистические методы обнаружения вторжений.
4. Рассмотреть архитектуру систем обнаружения вторжений.
5. Исследовать готовые решения на рынке СОВ.
6. Реализовать программный продукт, позволяющий обнаруживать вторжения в систему в реальном времени на основе статистических методов.

Дипломная работа состоит из введения, 6 разделов, заключения, списка использованных источников и 5 приложений. Общий объем работы – 85 страниц, из них 58 страниц – основное содержание, включая 36 рисунков, список использованных источников из 21 наименования.

КРАТКОЕ СОДЕРЖАНИЕ

В дипломной работе в разделе 1 «Анатомия атаки» приводятся необходимые определения, которые используются в данной работе, а также классификация сетевых атак.

Информационная безопасность (сокр. «ИБ») – это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств.

Угроза – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Угроза ИБ – возможность реализации воздействия на информацию, приводящего к искажению, уничтожению, копированию, блокирования доступа к информации, а также возможность воздействия на компоненты информационной системы (сокр. «ИС»), приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.

Сетевой атакой называют намеренные действия третьих лиц, направленные на установление контроля над локальным или удаленным компьютером, или вычислительной системой. В результате атак злоумышленники могут нарушать работу сети, изменять права аккаунта, получать персональные данные пользователей и реализовывать другие цели.

Система обнаружения вторжений (сокр. «СОВ») – программное или аппаратное средство, предназначенное для выявления фактов несанкционированного доступа в ИС или компьютерную сеть, либо несанкционированного управления ими.

На данный момент выделяют следующие виды сетевых атак:

1) Mailbombing.
2) Переполнение буфера.

3) Использование специализированных программ (вирусов, снифферов, троянских коней и т.д.).

4) Сетевая разведка.

5) IP-спуфинг.

6) Человек посередине.

7) Инъекция (SQL-инъекция, PHP-инъекция, межсайтовый скриптинг или XSS-атака, XPath-инъекция).

8) DoS-атаки («отказ в обслуживании», от англ. Denial of Service).

9) Phishing-атаки.

Остановимся на атаке типа «отказ в обслуживании». Количество проводимых DoS-атак неуклонно возрастает. Мировые лидеры по информационной безопасности ставят необходимость обнаружения DoS-атак и противостояния им как первостепенную задачу в своих исследованиях и разработках. Это свидетельствует о том, что разработка и внедрение методов защиты от DoS-атак – актуальная задача[2].

В разделе 2 «Атаки типа «отказ в обслуживании»» дается определение атаке типа «отказ в обслуживании», а также рассматриваются самые распространенные виды DDoS-атак. В подразделе «Защита от DDoS-атак» рассматриваются меры противодействия DDoS-атакам, а также методы их обнаружения. В подразделе «Этапы реализации атак» рассматриваются этапы, который злоумышленник проходит во время реализации DDoS-атак.

Атака типа «отказ в обслуживании» – атака на компоненты ИС, основанная на посыле стандартных либо нестандартных запросов, обработка которых требует ощутимых затрат вычислительных мощностей, тем самым создаются условия, при которых легальные пользователи не могут получить ответ на свои запросы. DoS-атака является наиболее известной сетевой атакой. Отказ также

---

[2] Бекенева, Я. А. Анализ актуальных типов DDoS-атак и методов защиты от них [Электронный ресурс] / Я. А. Бекенева // Известия СПбГЭТУ ЛЭТИ. – 2016. – № 1. – С. 7–14. – URL: https://izv.etu.ru/assets/files/izv-etu-1-20161-7-14.pdf (дата обращения 25.11.2022). – Загл. с экрана. – Яз. рус.

может быть полезен для последующего проникновения в систему (если в нештатной ситуации ПО выдает какую-либо критическую информацию – например, версию, часть программного кода и т.д.). Если DoS-атака ведется с нескольких хостов, то она называется распределенной (DDoS, Distributed Denial of Service).

Самые распространенные виды DDoS-атак:

1. ICMP Flood.
2. Sync Flood.
3. DDoS-атака на сервер доменных имен.
4. HTTP Flood.
5. Фрагментация данных.

Для осуществления DoS-атаки злоумышленник проходит три этапа реализации атак:

1) Сбор информации.
2) Реализация атаки.
3) Завершение атаки[3].

Таким образом, были рассмотрены особенности DDoS-атак, а также была подтверждена важность их обнаружения. Для обнаружения данных атак используются системы обнаружения вторжений, которые будут рассмотрены в следующем разделе.

В разделе 3 «Разработка СОВ» в подразделе «Задачи СОВ» представлены требования, которые предъявляются к СОВ в гос. системах. В подразделе «Признаки атак» рассмотрены параметры сетевого пакета, которые могут указывать на атаку. В подразделе «Анализ атаки» рассмотрены методы, с помощью которых можно обнаружить сетевые атаки. В подразделе «Архитектура СОВ» рассмотрены модули, из которых состоит СОВ, а также отличия сетевых СОВ от хостовых СОВ.

СОВ должна решать следующие задачи:

---

[3] Лукацкий, А.В. Обнаружение атак [Текст] / А.В. Лукацкий // 3-е изд., перераб. и доп. – СПБ. – 2003. – 608 с.

1) Обнаружение атаки.

2) Анализ атаки.

3) Реагирование на атаку[4].

Некоторые из признаков сетевой атаки:

1) IP-адрес отправителя.

2) Порт отправителя.

3) Протокол передачи сетевого пакета.

После обнаружения атаки необходимо её проанализировать и предпринять необходимые меры по обеспечению безопасности ИС. В этом помогают экспертные системы и нейронные сети.

Экспертная система – это система, которая в процессе обнаружения атаки, основываясь на сигнатурах, принимает решение о возможных последующих процессах в атаке.

СОВ должна включать в себя семь модулей:

1) Модуль работы с источником информации.

2) Модуль управления компонентами.

3) Хранилище данных.

4) База знаний.

5) Модуль обнаружения атак.

6) Модуль реагирования.

7) Графический интерфейс.

СОВ можно разделить на 2 вида:

1) СОВ на уровне узла.

2) СОВ на уровне сети.

Проанализировав плюсы и минусы, а также сферу применения хостовых и сетевых СОВ, выбор был сделан в пользу хостовой реализации.

---

[4] Ананьин, Е. В. Методы обнаружения аномалий и вторжений [Электронный ресурс] / Е. В. Ананьин, И. С. Кожевникова, А. В. Лысенко, А. В. Никишова // Научная электронная библиотека Elibrary [Электронный ресурс]. – Волгоград, 2016. – С. 48–50. – URL: https://www.elibrary.ru/item.asp?id=27336919 (дата обращения: 25.11.2022). – Загл. с экрана. – Яз. рус.

В разделе 4 «Обзор существующих СОВ» исследованы существующие решения на рынке СОВ, а именно:

1) Dallas Lock.
2) Suricata.
3) Snort.
4) OSSEC.

В ходе исследования существующих предложений на рынке СОВ, следующие удачные решения были имплементированы в собственный продукт, а именно:

- графический интерфейс с визуализацией текущего состояния системы;
- кроссплатформенность, то есть работа приложения на передовых ОС, включая Windows, Linux, MacOS и другие.

В разделе 5 «Методы обнаружения атак» были описаны статистические методы, которые использовались для обнаружения вторжений.

Для реализации статистических методов обнаружения вторжений были выбраны следующие два метода:

1. Пороговый анализ.

Для наблюдаемых параметров, число полученных пакетов в секунду и общее число пакетов за сессию, задается допустимый диапазон изменения их значений. Нахождение вне рамок этого диапазона соответствует аномальному поведению. Простейшей модификацией, позволяющей снизить количество ложных срабатываний, является добавление счетчика, который накапливает события «выпадения» наблюдаемых параметров из диапазона. При превышении счетчиком определенного значения фиксируется факт наличия аномалии.

2. Анализ распределений интенсивности отправки/приема пакетов.

Для данной сети строится модель, описывающая распределение интенсивности передачи пакетов (логнормальное, гамма и прочие). Для трафика без аномалий находятся параметры этого распределения. В тестовом режиме параметры новой построенной модели сравниваются с параметрами эталонной

модели. Сетевая аномалия регистрируется в случае значительных расхождений вычисленных параметров.

На основе вышеописанных методов, можно запрограммировать логику разрабатываемой СОВ для обнаружения DDoS-атак.

В разделе 6 «Программная реализация» была написана СОВ на основе статистических методов, описанных в разделе 5.

Для запуска программы необходимы права администратора. Главное окно программы включает в себя следующую информацию:

- кнопки для управления СОВ («Настройки», «Фильтр», «Старт», «Стоп», «Очистка», «Сброс»);
- таблица с описанием приходящих пакетов;
- график приходящих пакетов;
- фильтры пакетов;
- информация о полученном числе пакетов и общий размер логов с пакетами.

После нажатия кнопки «Настройки», пользователь может настроить следующие параметры системы:

1. Путь до папки с логами сетевых пакетов.
2. Путь до папки с логами атак и вторжений.
3. Путь до файла с правилами.
4. Лимит пакетов за сессию работы программы.
5. Адрес почты, на которую отправляется уведомление об обнаруженной атаке.

Также, при нажатии кнопки «Тренировка», система начинает пересчет статистик, путем анализа тренировочного файла.

После нажатия кнопки «Старт» появляется уведомление о начале работы системы. Постепенно таблица с сетевыми пакетами начинает заполняться. Логи с пакетами записываются в файл «logs.txt».

Программа позволяет фильтровать пакеты по IP-адресам и сетевым протоколам (UDP, TCP, ICMP и так далее).

При фиксировании числа пакетов больше установленного лимита, система предупреждает пользователя о превышении квоты. Работа графика в этот момент времени представлена на рисунке 19.

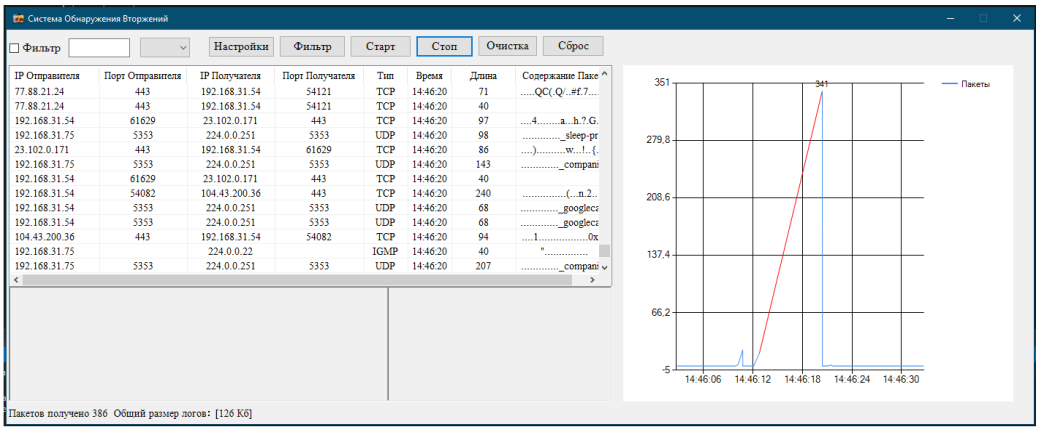

Рисунок 19 – Работа графика во время превышения лимита пакетов в секунду

Система записывает информацию о вторжении в файле «logs.txt», а также отсылает пользователю письмо на почту с уведомлением об обнаруженном вторжении.

Для симуляции атаки «Sync Flood» использовался интерфейс «msfconsole».

Для симуляции «ICMP Flood» атак использовалась следующая команда:

hping3 -l --fast 10.0.2.15

Эта команда позволяет отправлять эхо-пакеты на «жертву», без ожидания ответа от нее, со скоростью 10 пакетов в секунду.

Для симуляции атаки фрагментацией пакетов, выполнялась следующая команда:

ping 10.0.2.15 -l 65500 -w 1 -n 1

Она позволяет отправлять эхо-пакеты на «жертву» длиной 65500 байт.

Реализованный в данной работе программный продукт показал себя эффективным и достаточным для решения поставленной в работе цели. Всего было проведено 20 DDoS-атак, из них 18 были успешно обнаружены программой:

- 3 из 3-х атак фрагментацией пакетов.
- 7 из 7 атак «ICMP Flood».
- 8 из 10 атак «Sync Flood».

Также во время тестов было зафиксировано несколько ложных срабатываний во время высокой сетевой активности пользователя.

По итогам тестирования, программа показала достойное быстродействие и быструю реакцию на обнаруженное вторжение. Обнаружение вторжения и отправка письма происходит в течении нескольких секунд после запуска атаки.

Средний процент обнаружения системой составляет 90%. Таким образом, можно сделать вывод о высокой эффективности работы системы против DDoS-атак.

ЗАКЛЮЧЕНИЕ

Распознавание вторжения является не легкой задачей. Каждый год атаки становятся более продуманными и разнообразными, и в соответствии с ними должны изменяться и алгоритмы их распознавания.

В данной работе была изучена анатомия атак и их классификации.

Рассмотрены основные виды атак типа «отказ в обслуживании», а также методы их противодействия.

Рассмотрены три этапа реализации атак:

1. Сбор информации.
2. Реализация атаки.
3. Завершение атаки.

Были описаны методы обнаружения вторжений с использованием статистических методов.

На основе существующих решений была разработана собственная система обнаружения вторжений на языке C# с использованием сигнатурного метода, а также методов порогового анализа и метода распределений интенсивности отправки/приема пакетов. В результате тестирования программы, система показала себя эффективной как по точности, так и по быстродействию.

Результаты работы могут использоваться разработчиками СОВ, которые хотели бы улучшить распознавание рассмотренных DDoS-атак, путем возможного добавления реализованных статистических методов.

Таким образом, все поставленные задачи решены, цель работы достигнута.