УДК 004.056.53

Жуков И.А., д.т.н.,
Балакин С.В.

ИДЕНТИФИКАЦИЯ АТАК В КОМПЬЮТЕРНОЙ СЕТИ МЕТОДОМ УСРЕДНЕННОГО ВРЕМЕНИ ОБРАЩЕНИЙ

Национальный авиационный университет

yabal@mail.ru

Проанализированы этапы реализации атак в компьютерных сетях. Рассмотрены варианты идентификации атак на уровне обнаружения и предотвращения. Рассмотрен вариант повышения достоверности идентификации атак в компьютерной сети. Приведено уравнение идентификации вторжений по времени обращений. Предложена классификация обращений к портам по времени активности

Ключевые слова: компьютерная сеть, атака, идентификация, достоверность, трафик, исследование, усредненное время обращений, активность

Введение

Известна тенденция роста количества атак на компьютерные сети. С большинством видов вторжений могут справиться антивирусы и фаерволы, но некоторые атаки могут обойти и такую защиту, принося вред пользователю.

Защита, которую предоставляет большинство антивирусных компаний, зачастую не своевременная: сначала идет распространение вируса, а после этого антивирусы занимаются его «лечением».

Рассмотрен один из вариантов повышения достоверности идентификации атак в компьютерной сети.

Постановка проблемы

Решаемой проблемой выступает достоверность идентификации атак в компьютерной сети и выбор методов защиты. Главной задачей является определение потоков данных и отказ в доступе вторжениям. Исходя из особенностей изучаемого процесса, предложено оценивать достоверность идентификации вторжений, используя анализ потоков данных в сети. Основным видом атак, с которыми предложено бороться – это *DoS* атаки.

Исследования в данной области

При выполнении поставленной задачи использовались методы наблюдения за пакетами и потоками передаваемой информации. В качестве программных средств использована программа *WireShark* и *WinDump* (в дальнейшем планируется использовать программу *NetFlow* для изучения потоков). Исследование проводилось на базе процессора *Intel Core* 2 *Duo T*7300 на ОС *Windows* 8.

Негативные факторы, влияющие на результат работы – службы и программы, которые были установлены в ОС на момент выполнения исследования.

Цель исследований

Применение повышения достоверности идентификации атак в локальных и глобальных компьютерных сетях. Определение актуальности использования данных программных методов и их эффективности. Определить вторжения, которые монополизируют определенные каналы путем длительных обращений по одному адресу. Идентифицировать потенциальные источники вторжений и ограничить к ним доступ.

Результат исследования

На основании фильтрации трафика и потоков получим карту обращений элемента сети к разным источникам извне и наоборот, что предоставляет

возможность отслеживать время взаимодействия портов. Определение структуры и выбор методов защиты представим в виде следующих задач:

1) отбор начальных данных (структура, качества, ПО и т.д;
2) определение путей для атак;
3) разработка схемы повышения достоверности идентификации атак в компьютерной сети;
4) выбор средств защиты;
5) оценка средств защиты информации относительно всех путей утечки данных;
6) определение и запись путей злоумышленного доступа (повышение безопасности);
7) общее сравнение степени защищенности, доработка (минимизация путей для атак).

Такие задачи состоят из заданий, которые можно решить с помощью элементов теории вероятности или математическим моделированием систем и процессов. Структура трафика в основном зависит от вида деятельности пользователя.

Известны программы, которые мониторят сетевой трафик. При этом некоторые системы могут быть не совместимы. Среди программных средств оптимальными проявили себя *WireShark* и *WinDump*. Более мощным инструментом является программа *NetFlow*.

Одной из задач при идентификации атак является выбор инструментов выявления каналов утечки информации с высоким уровнем обнаружения.

Основным требованием является не допущение снижения производительности тестируемой системы. Используемые инструменты влияют на скорость работы системы, поэтому важно чтобы используемые методы при работе не были заметны пользователю. Важная роль отведена мониторингу инструментов защиты, которые должны учитывать технические характеристики системы.

Рассматривались атаки двух видов: распределенные атаки (РА) [1] и атаки на отказ в обслуживании (*DoS*) [2]. РА основаны на атаках типа *DoS*, но с их подтипами *Flood и Storm* атак. Данные атаки используют посылку большого количества пакетов на атакуемый узел. Такой узел не сможет функционировать, так как он "утонет" во входящих пакетах и будет недоступен для выполнения своих функций.

Исследованы атаки отказа обслуживания [2]. Основной принцип работы этих атак – получение доступа к ресурсам пользователя. Работа с такого типами атак позволяет перехватывать данные, необходимые для проведения исследования.

Время взаимодействия на атакуемый порт выше выполнения обычных задач, так как злоумышленник пытается захватить весь доступ к порту. Необходимо обратить внимание на те потоки, которые монополизируют доступ к определенным портам [3]. С помощью такого метода можно проводить фильтрацию и анализ потоков.

Выделяем следующие этапы реализации атаки: сбор информации, реализация атаки и завершение атаки.

Создание эффективного средства обнаружения вторжений – сложная задача: сложные и разнообразные компоненты изучаемых систем; широкая география элементов сетей, большое их количество; малоизученность проблемы в связи с относительно возникновением последней.

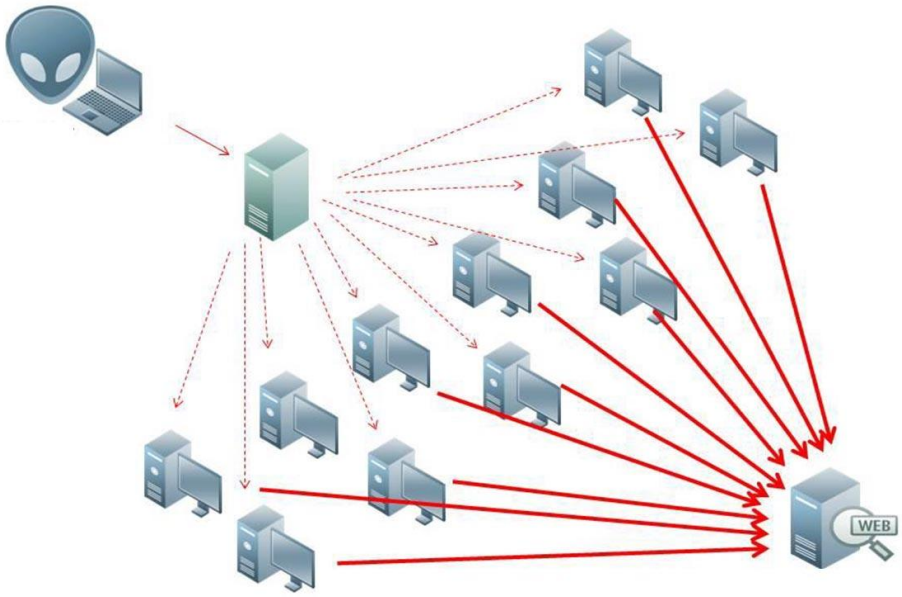

Рис. 1. Схема атаки на отказ в обслуживании

Атаки осуществляются через протоколы TCP/IP:

элемент сети имеет IP адрес;

соединение между элементами производится посредством порта;

обмен данными между элементами сети происходит пакетами, в заголовке каждого из которых указан адрес, порт отправителя и получателя.

Схему, по которой происходят DoS атаки, иллюстрирует рис.1. При вторжении длительность получения пакета в несколько раз превышает обычную длительность коммуникации портов, что может приводить к зависанию портов [4]. Для выявления вторжения использовалась формула, позволяющая системе самостоятельно выбирать процессы, идентифицируемые как вторжение.

Формула выбора усредненного времени отклика портов:

$$\bar{x} = \frac{x_1 + x_2 + x_3 + x_4 + \ldots + x_n}{n} = \frac{\sum_{i=1}^{n} x_i}{n}.$$

Период наблюдений разбиваем на интервалы обращений (Xn), где

Xn(Xi) – время отклика порта номер n;

$\overline{X}$ – усредненное время обращения пакета к источнику.

При наличии значения усредненного времени обращения по адресу, можно фильтровать источники, которые требуют много времени для сессии приема/передачи информации и пакетов.

Потенциально опасными и подверженными вторжениям пакеты будут считаться, если время отклика превышает усредненное. Если порты заняты программными элементами пользователя или самой системы (загрузка файла, обращение оперативной памяти к жесткому диску и т.д.), то это не считается вторжением [5].

Пакеты и потоки, которые при обращении к портам превышают усредненное время в системе, должны быть проверены, так как высока возможность быть подверженным *DoS* атаке, именно через данные узлы.

$\overline{X} \geq Xn(Xi)$ – пакет использует время порта в условно безопасном интервале.

$\overline{X} < Xn(Xi)$ – высокая вероятность *DoS* атаки, пакет и поток информации от источника должен быть проверен.

Элементы метода:

эмулятор: имитирует активность, подобную работе атак.

конвертор приводит полученные данные к виду, который можно легко считывать.

Подготовка данных: отбирает из всех пакетов только те, длительность сессии которых выше усредненного значения.

Реализация метода на основе метода усредненных обращений.

Реализация метода наблюдения за адресами источников

Рис. 2. Схема взаимодействия элементов программного комплекса

Схему определения элементов, которые попадают под категорию возможных вторжений, иллюстрирует рис. 2. Проблемой при проведении расчетов являлось то, что имея таблицу активности, невозможно отделить состояние пиковой активности от вторжений. Решением стало усреднение временного значения обычной деятельности портов по отношению к вторжениям.

Разработан комплекс, с помощью которого можно производить вычисления вторжений и повысить достоверность идентификации несанкционированных воздействий в системе. Исследованные методы эффективно распознают возможность угрозы *DoS* атаки через данные порты. Методы распознавания угроз показали положительные результаты в условиях слабой активности портов.

Несмотря на высокую точность полученных результатов, условия при проведении исследования не являются идеальными. Это связано с перенасыщенностью рынка программ и широкого доступа пользователей к

интернету, что приводит к агрессивному использованию системных ресурсов даже при выполнении обычных задач.

Поставленная задача мониторинга активности вторжений выполнена. Однако существует ряд факторов, которые необходимо использовать в проведенных расчетах для получения более точных данных.

Выводы

Представлены отчеты влияния разных типов атак на компьютерную сеть. Основной проблемой при проведении исследования было правильно идентифицировать вторжения от просто длительных обращений по указанному адресу. Предложено классифицировать обращения, длина которых больше усредненных, потенциальными угрозами проникновений. Таким образом не упускаются проникновения, но с другой стороны – блокируются некоторые пользовательские приложения.

Приведено уравнение идентификации вторжений по времени обращений, которое позволяет вычислить среднее время активности порта.

Сформулированы пути повышения достоверности идентификации несанкционированных воздействий и атак в компьютерной сети.

Проведенные исследования показали возможности и целесообразность используемых инструментов. Данный поход применим для обнаружения и предотвращения вторжений в компьютерной сети с одинаковой эффективностью.

Список литературы

1. Стивен Норткат, Джуди Новак. Обнаружение нарушений безопасности в сетях, 3-е издание: Пер. с англ. – М.: Изд. дом "Вильямс", 2003. – 448 с.

2. Щерба М.В. Система анализа устойчивости распределенных компьютерных сетей к атакам на «отказ в обслуживании» // Омский научный вестник, 2012. – 286 с.

3. Милославская Н.Г. Интрасети: обнаружение вторжений: учеб/ пособие для вузов / Н.Г. Милославская, А.И. Толстой. – М.: Юнити-Дана, 2001. – 592 с.

4. D.Denning, An Intrusion Detection Model // IEEE Transactions on Software Engineering, v. SE-13, № I, 2008. – 197 p.

5. Zargar, G.R., Kabiri, P. Identification of effective network features for probing attack detection, Networked Digital Technologies, 2009. NDT '09. First International Conference on Networked Digital Technologies (NDT 2009), Technical University of Ostrava, 2009. – P. 405-410.

Статью представлено в редакцию 18.05.2015