СТАТИСТИЧЕСКИЙ АНАЛИЗ СЕТЕВОГО ТРАФИКА

Н. М. Карпук

ВВЕДЕНИЕ

Сообщалось, что 24 января 2003 года в свет был выпущен W32.SQLExp.Worm (позднее названный Slammer/Sapphire), удваивающий количество зараженных систем каждые 8.5 секунд. Этот червь использовал уязвимость переполнения буфера в Microsoft SQL Server 2000 (включая MSDE 2000). Несмотря на то, что продукты Microsoft являются достаточно уязвимыми, скорость распространения этого червя была воистину пугающей. В течение 10 минут он поразил 90% всех аналогичных WEB-систем. Черви такого типа прежде существовали только в теории и представляли чисто академический интерес.

Для повышения эффективности обнаружения несанкционированного вторжения и различных аномалий (вирусов, хакерских атак и др.) могут быть использованы методы анализа трафика в компьютерной сети [1, 2]. Наиболее широко с этой целью используются методы и так называемые RBID-системы, основанные на правилах (от Rule-Based Intrusion Detection). Обычно RBID системы для выявления потенциальной атаки используют «сигнатуру» атаки с последующий анализом входящего трафика. Сигнатуры весьма разнообразны и могут определять конкретные параметры от номера порта в пакете до последовательности байт в серии пакетов. После того, как сигнатура разработана, её использование обычно довольно эффективно предотвращает нежелательную сетевую активность.

Главный недостаток такого подхода – то, что сигнатуры сначала надо разработать и обновить ими систему защиты. Так как обнаружение аномального трафика в RBID системах основано на сигнатурах, без их точного описания эффективность системы значительно понижается, но разработка правил даже для атаки средней сложности не тривиальна и требует времени. Сначала атака должна быть обнаружена, записана и проанализирована. Далее, необходимо создать новое правило для данной системы, что достаточно трудоемко. Самым оперативным поставщикам требуются часы или даже дни для выпуска сигнатуры. И даже если все эти шаги выполнены очень быстро, фундаментальная проблема остается: RBID система может не заметить аномальную активность без сигнатуры новой атаки. Поэтому такие черви, как W32.SQLExp, поражающие сеть в течение нескольких секунд, администратору не оставляют никаких шансов, несмотря на регулярно обновляемые RBID системы.

Решением этой проблемы может быть использование менее известного метода обнаружения вторжений и аномалий поведении, называемого статистическим [3].

СТАТИСТИЧЕСКИЙ ПУТЬ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Статистические системы (SBID) имеют другой подход к обнаружению вторжений. Концепция SBID систем проста: система определяет «нормальную» сетевую активность и затем весь трафик, не подпадающий под определение «нормального» помечается как аномальный. SBID системы пытаются изучить сетевой трафик каждой конкретной сети. Анализируя сетевой трафик, SBID системы ищут аномалии в установившейся картине нормального сетевого трафика. Всем пакетам дается оценка «аномальности» (включающая в себя степень ненормальности специфического события) и если эта оценка выше определенного предела, IDS генерирует сигнал тревоги. Ключевой особенностью любой SBID системы является её возможность изучать сетевую активность и отличать нормальную сетевую активность от аномальной.

ОСНОВА SBID СИСТЕМ

Работа SBID систем построена так: система изучает, что именно является “нормальным” для вашего трафика, наблюдая за активностью в течение некоторого периода времени. Когда происходит неизвестное или редкое (аномальное) событие, SBID обнаруживает его и генерирует сигнал тревоги. Разница между нормальным и аномальным событием определяется пороговой величиной. Если пороговая величина высока, то незначительные аномалии не принимаются во внимание. Если порог низок, то большинство аномалий являются причиной для дальнейшего анализа.

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ

Поскольку нас интересует не сигнатурный, а статистический метод анализа сетевого трафика, рассмотрим два возможных подхода:

- Подход, основанный на потоковом анализе трафика;
- Подход, анализирующий данные за фиксированные интервалы времени.

Первый подход не может отражать текущее изменение поведения трафика, поэтому для практической реализации был выбран второй подход. Кроме того, так как модели, достаточно полно описывающей все процессы, происходящие в сети, на сегодняшний день не существует, был выбран путь определения некоторых статистических параметров трафика (например, максимальное количество сетевых пакетов, пришедших на один локальный порт).

АРХИТЕКТУРА ПРОГРАММНОГО РЕШЕНИЯ

Разработанное приложение включает в себя:

- Сетевой монитор – модуль перехвата пакетов, проходящих через установленное на компьютере сетевое соединение;

- Анализатор – модуль, определяющий некоторые статистические величины, отражающие состояние трафика за определенный промежуток времени;
- Компаратор – модуль, сравнивающий статистические величины за последний и предпоследний промежутки времени;
- Клиент, обеспечивающий отображение данных и настройку модулей.

СЕТЕВОЙ МОНИТОР (СНИФЕР)

Данный модуль обеспечивает перехват всего сетевого трафика, проходящего через выбранное сетевое соединение. Перехват осуществляется открытием сетевого сокета, который принимает все проходящие пакеты. Перехватываются только заголовки пакетов, поскольку именно они несут всю статистическую информацию, содержимое пакетов нас не интересует.

АНАЛИЗАТОР

Данный модуль обеспечивает расчет параметров, по которым оценивается состояние сетевого трафика. Данные собираются за 30-ти секундный промежуток времени. На момент подготовки этого материала, в модуль было включено определение параметров сетевого трафика, среди которых:

- Общее количество пакетов за промежуток времени;
- Максимальное количество пакетов, пришедших на один IP адрес;
- Максимальное количество пакетов, пришедших с одного порта отправителя;
- Максимальное количество пакетов, пришедших на один порт;
- Наиболее используемый порт отправителя;
- Наиболее используемый порт получателя;
- Наиболее используемый IP адрес отправителя;

КОМПАРАТОР

Компаратор-модуль, который сравнивает состояние сетевого трафика за два промежутка времени (в настоящий момент за два последних промежутка времени) и определяет суммарный уровень отличия.

Данный модуль требует наибольшей по времени настройки, поскольку от того, как именно сравниваются величины и какой вклад вносит каждая в суммарный уровень различий, зависит реакция приложения на различные изменения состояния трафика. Кроме подробной информации по каждому параметру и суммарного коэффициента отличий в приложении существует индикатор, расположенный на верхней панели окна программы.

ОСОБЕННОСТИ ПРЕДЛОЖЕННОГО ПОДХОДА

К недостаткам решения, предложенного в данной работе, следует отнести недостатки, присущие статистическим методам вообще. Некоторые незначительные изменения в состоянии сетевого трафика, например сканирование портов с очень малой скоростью, может быть незамеченным.

ЗАКЛЮЧЕНИЕ

В данной работе исследован статистический метод анализа сетевого трафика, определены его преимущества и недостатки в сравнении с сигнатурным методом анализа, создан программный комплекс, способный анализировать и обнаруживать нехарактерную для сети активность, тем самым, пресекая атаки, неизвестные для сигнатурных средств защиты. Дальнейшим развитием статистического метода может быть его способность самообучаться и сохранять результаты своих анализов.

Литература

1. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2003.
2. *Хогдал Дж. Скотт.* Анализ и диагностика компьютерных сетей. Addison Wesley Longman, Inc., 2000.
3. *Юдицкий С. С., Швецов В .И.* Увидеть слона целиком // Сети и системы связи. 2001. № 10.
4. *Айвазян С. А., Енюков И. С., Мешалкин Л. Д.* Прикладная статистика: Исследование зависимостей. М.: Финансы и статистика, 1985. 488 с.

ЗАЩИТА ИНФОРМАЦИИ ОТ КОПИРОВАНИЯ ПРИ ИСПОЛЬЗОВАНИИ СМЕННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

А. С. Кудин

Эффективная борьба с пиратством в области IT-технологий в настоящее время является актуальной задачей. Существует несколько методов борьбы с пиратством, например: легитимный (взлом и незаконное распространение программного обеспечения описаны в законах и строго преследуются по ним), экономический (цена товара делается сравнимой с ценой подделки). Часто наиболее эффективной является техническая защита программных продуктов от копирования.

Защиту программного обеспечения, распространяемого на сменном носителе информации, надежнее всего построить на проверке уникальности этого носителя. В настоящее время подавляющее большинство ПО распространяется на CD и DVD дисках, поэтому о них и пойдет речь далее.