УДК 004.056

АНАЛИЗ РАСПРЕДЕЛЕННОЙ АТАКИ ТИПА «ОТКАЗ В ОБСЛУЖИВАНИЕ»

А.А. Милосердов
Научный руководитель – д.т.н., профессор Ю.А. Гатчин

В работе производится анализ распределенной атаки типа «отказ в обслуживание» (DDoS). Рассматриваются основные методы атаки и способы противодействия.

Одной из самых популярных и результативных атак на сегодняшний день является DoS-атака (Denial of Service, отказ в обслуживании). Это атака на вычислительную систему с целью довести ее до отказа, т.е. создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам), либо этот доступ затруднен. Отказ «вражеской» системы может быть как самоцелью (например, сделать недоступным популярный сайт), так и одним из шагов к овладению системой (если во внештатной ситуации ПО выдает какую-либо критическую информацию – например, версию, часть программного кода и т.д.) [1].

Цель работы – определить наиболее эффективные методы борьбы с DDoS-атакой. Задача – проанализировать методы DDoS-атаки и основные способы противодействия ей.

Существуют различные причины, по которым может возникнуть DoS-условие.

1. Ошибка в программном коде. Это может привести к обращению к неиспользуемому фрагменту адресного пространства, выполнению недопустимой инструкции или другой необрабатываемой исключительной ситуации, когда происходит аварийное завершение серверного приложения. Классическим примером является обращение по нулевому (null) указателю.
2. Атака второго рода – атака, которая стремится вызвать ложное срабатывание системы защиты и таким образом привести к недоступности ресурса. Т.е. в данном случае нарушители будут классифицироваться как авторизованные пользователи (ошибка второго рода).
3. Недостаточная проверка данных пользователя. Это приведет к бесконечному либо длительному циклу или повышенному длительному потреблению процессорных ресурсов (исчерпанию процессорных ресурсов) либо выделению большого объема оперативной памяти (исчерпанию памяти).
4. Флуд (англ. flood) – атака, связанная с большим количеством обычно бессмысленных или сформированных в неправильном формате запросов к компьютерной системе или сетевому оборудованию, имеющая своей целью или приведшая к отказу в работе системы из-за исчерпания ресурсов системы – процессора, памяти либо каналов связи. Наиболее распространенная причина отказа в обслуживание [2].

Для создания подобной атаки могут применяться как обычные сетевые утилиты наподобие ping, так и особые программы. Если на сайте с высокой посещаемостью будет обнаружена уязвимость типа «межсайтовый скриптинг» или возможность включения картинок с других ресурсов, этот сайт также можно применить для DDoS-атаки [3].

Методы обнаружения можно разделить на несколько больших групп:

- сигнатурные – основанные на качественном анализе трафика;
- статистические – основанные на количественном анализе трафика;
- гибридные – сочетающие в себе достоинства двух предыдущих методов [2].

DDoS нападение распознать просто – замедление работы сети и серверов, заметное как администратору системы, так и обычному пользователю. Первым шагом в защите это идентификация типа трафика, который загружает сеть. Большинство нападений DDoS посылает очень определенный тип трафика – ICMP, UDP, TCP, часто с поддельными IP адресами. Нападение обычно характеризует необычно большое количество пакетов

некоторого типа. Исключением к этому правилу являются DDoS нападения, направленные против определенных служб, типа HTTP, используя допустимый трафик и запросы [3].

Чтобы идентифицировать и изучить пакеты, необходимо анализировать сетевой трафик. Это можно сделать двумя различными методами в зависимости от того, где исследуется трафик. Первый метод может использоваться на машине, которая расположена в атакуемой сети. Tcpdump – популярный сниффер, который хорошо подойдет для этих целей. Анализ трафика в реальном масштабе времени невозможен на перегруженной сети, так что нужно использовать опцию «-w», чтобы записать данные в файл. Затем, используя инструмент типа tcpdstat или tcptrace, проанализировать результаты.

DDoS, в отличие от традиционного DoS, исходит из множественных источников. Поэтому необходить определить транзитный маршрутизатор, через который проходят большинство пакетов. Для этого потребуется сотрудничать с несколькими источниками. Каждый участник процесса (главным образом ISP провайдеры) будут использовать очень похожие методы. Идентифицировав злонамеренный тип трафика, используя вышеописанные методы, будет создан новый список ограничения доступа. Добавив его к правилам, которые применены к интерфейсу, который посылает трафик атакуемому адресату, снова используется команда «log-input». Регистрация подробно запишет информацию об исходном интерфейсе и MAC адресе источника атаки. Эти данные могут использоваться, чтобы определить IP адрес маршрутизатора, отправляющего злонамеренный трафик. Процесс будет повторен на следующем маршрутизаторе в цепочке. После нескольких итераций, источник (или один из них) будет обнаружен. Тогда можно создать соответствующий фильтр, который заблокирует атакующего. Недостаток в этом методе защиты от DDoS нападения – время и сложность. Получение таких данных требует работы с несколькими сторонами, и иногда использование правового принуждения [1].

Анализируя методы проведения атаки и способы противодействия можно прийти к выводу, что не существует универсальных способов борьбы с данным видом атаки. Это означает, что необходимо четко знать, как реагировать на нападение – идентифицируя трафик, разрабатывая и осуществляя фильтры. Подготовка и планирование, безусловно, лучшие методы для того, чтобы смягчить будущие DDoS нападения.

Литература

1. Крис Касперски. Компьютерные вирусы изнутри и снаружи. – Питер. – СПб: Питер, 2006. – С. 527.
2. Stephen Northcutt, Mark Cooper, Matt Fearnow, Karen Frederik Анализ типовых нарушений безопасности в сетях = Intrusion Signatures and Analysis. – New Riders Publishing (англ.) СПб: Издательский дом «Вильямс» (русск.), 2001. – С. 464.
3. www.securitylab.ru

УДК 81.09.03

ПРОИЗВОДСТВЕННЫЕ ФАКТОРЫ, ВЛИЯЮЩИЕ НА РАБОТУ ИНФОРМАЦИОННОЙ СИСТЕМЫ И ЕЕ ЗАЩИТУ

Е.Д. Светлова
Научный руководитель – к.т.н., доцент Д.А. Светлов

1. Эксплуатация ЭВМ. Выявление носителей опасности.

Предметом труда является программное обеспечение, установленное на используемой ЭВМ.

Нормальная работа современных вычислительных машин невозможна без создания и поддержки искусственного климата. На работу машины оказывает влияние, как температуры, так и относительной влажности воздуха. Это объясняется тем, что параметры полупроводниковых приборов зависят от их температуры.