УДК 004.(491+738.5.057.4):65.012.8

IP-СПУФИНГ. МЕТОДЫ ОПРЕДЕЛЕНИЯ И ОСЛАБЛЕНИЯ АТАКИ

Прокопчук А.Е, Мешков В.И.
Государственный ВУЗ «Национальный горный университет», nmu.org.ua, alex0392@gmail.com

В данной работе рассмотрена сетевая атака типа IP-спуфинг, а так же методы определения данной атаки и способы её ослабления.

Ключевые слова – IP-спуфинг; сетевая атака; RFC 2827.

ВВЕДЕНИЕ

Недавно наблюдавшиеся DoS-атаки с использованием подмены адреса отправителя показали наличие серьезной опасности для провайдеров Internet (ISP) и сообщества Internet в целом. В данной работе рассматривается простой и эффективный метод борьбы с такими атаками путем фильтрации входящего трафика с целью блокирования DoS-атаки, в которых используются IP-адреса, не относящиеся к точкам агрегирования ISP.

Сетевая атака – действие, целью которого является захват контроля над удалённой/локальной вычислительной системой, либо её дестабилизация, либо отказ в обслуживании, а также получение данных пользователей удалённой/локальной вычислительной системы. На данный момент выделяют следующие атаки: mailbombing, переполнение буфера, использование специализированных программ, сетевая разведка, IP-спуфинг, man-in-the-middle, отказ в обслуживании, phishing-атаки. В данной работе рассмотрим IP-спуфинг.

МЕТОДЫ ОПРЕДЕЛЕНИЯ АТАКИ

Проанализировав IP-пакет, а в частности адрес хоста можно определить IP-адрес источника данных. IP-спуфинг скрывает IP-адрес создавая пакеты, содержащие ложные адреса чтобы скрыть данные при соединении, а также при отправке информации. IP-спуфинг – это общепризнанный метод используемый спаммерами и хакерами для маскировки своего реального IP-адреса.

Если же злоумышленнику удается поменять таблицы маршрутизации и направить трафик на ложный IP-адрес, то он получит все пакеты и сможет отвечать на них так, как будто является санкционированным пользователем.

Определить IP-спуфинг можно следующим образом:

1. Проверить IP-адрес который был найден в данных и ответить на него. В результате ответ может не прийти, по причине не реального хоста или подделки IP-адреса.

2. Проверить значение TTL (Time to Live) оригинального пакета перед отправкой на сомнительный хост. Проверить TTL обеих пакетов, чтобы убедиться, что они совпадают. Если они не совпадают, то вполне вероятно, что источником является поддельный IP.

3. Проверить идентификационный номер пакета.

МЕТОДЫ ОСЛАБЛЕНИЯ АТАКИ

Угрозу IP-спуфинга можно немного ослабить (но не устранить) с помощью следующих мер:

- Контроль доступа. Самый простой способ предотвращения IP-спуфинга состоит в правильной настройке управления доступом. Чтобы снизить эффективность IP-спуфигна, необходимо настроить контроль доступа на отсечение любого трафика, поступающего из внешней сети с исходным адресом, который должен располагаться внутри сети. Это помогает бороться с IP-спуфингом, когда санкционированными являются только внутренние адреса. Если санкционированными являются и некоторые адреса внешней сети, данный метод становится неэффективным.
- Фильтрация RFC 2827. Можно пресечь попытки IP-спуфинга чужих сетей пользователями своей сети. Для такой реализации требуется фильтрация любого исходящего трафика, исходный адрес которого не является одним из IP-адресов организации. Этот тип фильтрации, известный под названием "RFC 2827", может выполнять и провайдер. В конечном итоге отфильровывается весь трафик, который не имеет исходного адреса, ожидаемого на определенном интерфейсе. К примеру, если провайдер предоставляет соединение с IP-адресом 192.1.1.0/24, он может настроить фильтр таким образом, чтобы с данного интерфейса на маршрутизатор провайдера допускался только трафик, поступающий с адреса 192.1.1.0/24. Кроме того, чем дальше от фильтруемых устройств, тем труднее проводить точную фильтрацию.

Наиболее подходящим методом является использование контроля доступа, после внедрения определенных мер – атака является бессмысленной.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы [Текст] / А. Е. Боршевников // Современные тенденции технических наук: материалы междунар. заоч. науч. конф. (г. Уфа, октябрь 2011 г.). — Уфа: Лето, 2011. — С. 8-13.

2. Кадер М. Сетевые атаки. (Электрон. ресурс) / Способ доступа: URL: http://www.cnews.ru/reviews/free/oldcom/security/cisco_attacks.shtml - Сетевые атаки

3. What Is IP Spoofing and How Does It Work? (Электрон. ресурс) . Способ доступа: URL: https://www.classle.net/content-page/what-ip-spoofing-and-how-does-it-work - What Is IP Spoofing and How Does It Work?