УДК 681.3:004.056

МЕТОД ВЫЯВЛЕНИЯ МЕДЛЕННОЙ АТАКИ ТИПА ОТКАЗ В ОБСЛУЖИВАНИИ

Рубан И.В.[1)], Прибыльнов Д.В.[2)], Лошаков Е.С.[3)]
Харьковский университет Воздушных Сил имени Ивана Кожедуба
[1)]адъюнкт; [3)]д.т.н, профессор; [3)]адъюнкт

На современном этапе развития информационных технологий вопросы непрерывности предоставления сервисов выходят на передний план. Кроме этого, существует ряд задач непрерывность выполнение которых является критичной. Среди таковых необходимо особенно выделить задачи прикладной военной направленности: обработка информации о воздушной остановке, выдача целеуказаний, выдача сигналов управления и оповещения и другие. Среди наиболее распространённых на сегодняшний день кибернетических угроз следует выделить атаки типа «Отказ в обслуживании». Простота и доступность инструментов для реализации делают их наиболее опасными. Одним из подклассов являются медленные атаки типа «Отказ в обслуживании». Особенностью данного подкласса является использование недостатка механизма рестарта протокола TCP. Соответственно, все информационно телекоммуникационные сети в основе которых на транспортном уровне функционирует протокол TCP, являются уязвимыми к данного рода атакам. Методы противодействия указанной кибернетической угрозе на данный момент времени только разрабатываются.

Анализ литературы показал, что на текучий момент времени известных методов обнаружения медленных DOS – атак не существует. Метод противодействия путём задания случайного значения таймеру повторной передачи приводит к уменьшению пропускной способности канала связи блокируя возможность проведения данного типа атак, но не даёт возможность выявления хоста с которого производится атака. По данной причине предлагается метод выявления медленных DOS – атак путем распознавания шаблонов трафика, то есть в информационно-телекоммуникационной сети происходит непрерывный мониторинг загруженности канала связи. В случае достижения определённого уровня загрузки более 90% включается система документирования операций сетевого и транспортного уровня, которая в базе данных фиксирует суммарный трафик по потокам и специальное программное обеспечение производит далее анализ и сравнение полученной загрузки. Если выявлено совпадение с шаблоном трафика по интенсивности от некоторой совокупности потоков, то принимается решение о наличии атаки, в противном случае принимается решение об отсутствии атаки, то есть о наличии временного пика трафика. Вся полученная информация и отчёты передаются на анализ системному администратору как эксперту данной системы, который по совокупности полученных данных делает выводы о состоянии системы в целом.

Один из предлагаемых методов противодействия медленным атакам типа отказ в обслуживании - метод поиска и отбрасывания наиболее интенсивного потока. Суть метода заключается в выявлении и использовании недостатка метода реализации атаки. Если принять ограничение, что атака проводится с одного хоста, то отбрасывая наиболее интенсивный поток, обрабатываемый сервером, через некоторое количество итераций, в зависимости от загрузки, будет достигнуто состояние, когда будет заблокирован именно атакующий поток и станет возможным выявить IP адрес атакующего. Предлагаемый метод не является абсолютной защитой от данного рода вредоносных воздействий, но позволяет выявить и заблокировать атакующий хост без внесения ограничений пропускной способности канала связи с одной стороны и без необходимости наращивания пропускной способности канала связи с другой. Вероятность выявления вредоносного воздействия предложенным методом колеблется от 0.9 до 0.95, вероятность правильного блокирования и противодействия в зависимости от загрузки сети происходит в пределах от 0.6 до 0.85. Полученные результаты свидетельствуют о работоспособности предлагаемых методов.

Список использованных источников

1. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атаки через Internet. — СПб.: НПО "Мир и семья 95", Серия учебной литературы "Магистр", 1997.
2. Ховард М., Лебланк Д. Защищенный код. Пер. с англ. – 2-е изд., испр. М.: Издательско-торговый дом «русская редакция», 2004. – 704 стр.: ил.