УДК 004.492.2

С.А. Жаданов, Н.А. Маслова
Донецкий национальный технический университет
кафедра программного обеспечения интеллектуальных систем
E-mail: zhadyaka@i.ua

РАЗРАБОТКА АДАПТИВНОГО АЛГОРИТМА АВТОМАТИЧЕСКОГО ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

Аннотация

Жаданов С.А. Маслова Н.А. ***Разработка адаптивного алгоритма автоматического обнаружения сетевых атак.*** Выполнен анализ методов обнаружения сетевых атак, проведена их классификация. Изучен адаптивный поход к построению алгоритмов обнаружения сетевых атак. На его основе выбрано перспективное решение и изложена последовательность основных шагов процедуры автоматического обнаружения сетевых атак.

Ключевые слова: методы, сетевые атаки, адаптивный алгоритм, автоматическое обнаружение.

Общая постановка проблемы. В настоящее время любая деятельность, связанная с обменом информацией не обходится без использования компьютерных сетей. Вместе с тем повсеместное внедрение сетей увеличило количество потенциальных злоумышленников, имеющих доступ к открытым системам. Одной из самых сложных задач в сфере защиты компьютерных систем является предотвращение DDoS-атак. В настоящее время способов гарантирующих полную защиту от DDoS-атак не существует. Основная причина этого – дальнейшее развитие компьютерных систем, увеличение количества пользователей сети интернет, постоянное совершенствование методов, которыми пользуются киберпреступники. Поэтому возникает необходимость разработки методик и алгоритмов обнаружения и ликвидации DDoS-атак, для чего необходимо рассмотреть следующие вопросы:

- классифицировать DDoS- атаки;
- проанализировать существующие методы обнаружения сетевых атак;
- выбрать перспективное решение и сформулировать его основные принципы с целью дальнейшей программной реализации.

Анализ литературных источников. DDoS – атака (от англ. Distributed Denial of Service, распределенная атака типа «отказ в обслуживании») – атака на вычислительную систему, выполняемая с большого количества компьютеров, с целью довести ее до отказа. То есть создать такие условия, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам), либо этот доступ затруднен [1].

DDoS – атаки используются в самых различных целях: замедление работы пользователей; блокировка ключевых узлов сети Интернет; нарушение работоспособности интернет–сервисов компаний, бизнес которых основан на web-технологиях; в конкурентной борьбе; для оказания политического давления и т.д. Последствия DDoS – атак могут привести к утрате ключевых ресурсов сети, приложений и систем ведения бизнеса, потере репутации, финансовым затратам и т.п. Так же DDoS – атаки могут использоваться для отвлечения внимания при запуске других вредоносных программ, например, для похищения конфиденциальных данных.

Методы и технологии проведения DDoS - атак весьма разнообразны. Выделяют разрушающие и блокирующие виды атак.

Разрушающие атаки производятся таким образом, что узел сети становится полностью недоступным. Зависает, уничтожается операционная система, конфигурация устройства и т.п., такие атаки производятся посредством уязвимостей, находящихся в программном обеспечении.

При блокирующей атаке на ресурсы системы формируется большое количество бессмысленных или сформированных в неправильном формате запросов к узлам сети или приложениям, что приводит к значительному снижению производительности компьютерной системы или сетевого оборудования.

Выделяют HTTP GET, UDP - flood, TCP SYN, ICMP-атаки. При этом:

– HTTP GET – целенаправленная, скоординированная отправка на web-сервер жертвы большого количества запросов с «зомби» - сети;

– UDP – flood – этот тип атаки направлен на канал связи; на адрес атакуемой системы посылаются UDP запросы большого размера, при этом происходит быстрое исчерпание полосы пропускания канала связи, ведущего к атакуемой системе, и устройство, работающее по протоколу TCP, перестает отвечать;

– TCP SYN – flood – при этом типе атаки на атакуемый узел сети посылается большое количество запросов на открытие соединения, при этом атакуемому объекту приходится расходовать все свои ресурсы на отслеживание всех этих частично открытых соединений, что приводит к исчерпанию количества сокетов и устройство перестает отвечать;

– ICMP – flood (англ. flood – наводнение, затопление) – целенаправленная, специализированная отправка большого количества DNS запросов на DNS – сервер, при этом DNS – сервер становится не доступен для большого круга пользователей, т.к. его ресурсы заняты обработкой этих запросов.

Чаще всего, при проведении DDoS – атаки используется несколько типов атак, что, в значительной степени осложняет противодействие им. Они могут использовать предварительно зараженные компьютеры пользователей сети, сервера, недоработки программного обеспечения, хеш-таблицы [2-3].