ИМИТАЦИЯ УДАЛЕННЫХ АТАК, НАПРАВЛЕННЫХ НА ОТКАЗ В ОБСЛУЖИВАНИИ СЕТЕВЫХ ОПЕРАЦИОННЫХ СИСТЕМ

Д.С. ПРИЩЕПА, В.Ф. ГОЛИКОВ

Атакой на информационную систему называется действие или последовательность связанных между собой действий нарушителя, которые приводят к реализации угрозы путем использования уязвимостей этой информационной системы. Все атаки можно разделить на локальные, которые производятся в пределах самой информационной системе, и удаленные, которые проводятся через сеть общего пользования. Первый тип атак является легко обнаружимым и нейтрализуемым с помощью административных мер. Второй класс является самым распространенным и наиболее тяжело поддается обнаружению и нейтрализации.

Удаленная активная атака – это упорядоченный набор сетевых операций, выполняемых на каждой фазе проведения атаки, организованный по последовательной или параллельной схемам воздействия на атакуемые узлы и направленный на обход средств защиты атакованного уз-

ла. Каждая сетевая операция, входящая в состав удаленной активной атаки, называется элементарной атакой.

Элементарная атака — это действия и правила, описывающие цикл сетевой операции в составе атаки, результат которого не обязательно направлен на обход защиты атакованного узла.

Одним из самых распространенных видов удаленных атак, который часто применяется как составная часть других более сложных атак, является класс атак, направленных на отказ в обслуживании (DoS — Denial of Service). Основной принцип таких атак — генерация большого числа запросов к атакуемой системе, приводящего к ухудшению работоспособности системы и, возможно, к отказу в обслуживании запросов от легальных клиентов. Примерами таких атак являются:

– затопление SYN-пакетами, которое приводит к блокированию атакуемого узла из-за переполнения его очереди запросов на установление TCP-соединений;

– передача широковещательного запроса от имени жертвы, что приводит к получению жертвой большого количества ответов от других узлов сети;

– рассинхронизация TCP-соединения, приводящая к разрыву установленного атакуемым узлом TCP-соединения;

– затопление UDP-пакетами, приводящее к блокированию атакуемого узла, всей сети или участка сети, вызванному чрезмерной загрузкой сети UDP-пакетами;

– зацикливание IP-пакетов, приводящее к блокированию атакуемого узла из-за переполнения его очереди TCP-соединений вследствие некорректной реализации стека протоколов TCP/IP.

Идеальная система обнаружения вторжений (СОВ) должна иметь средства определения аномального трафика и развитую систему принятия решений, способную блокировать трафик, сгенерированный нарушителем, оставляя таким образом систему доступной для легальных пользователей. В современных СОВ развиваются два типа методов обнаружения вторжений: методы обнаружения злоумышленного поведения и методы выявления аномальной активности. Первый метод основан на сравнении текущего поведения субъектов с сигнатурами (известными сценариями атак) злоумышленного поведения. Примером СОВ, использующей такие методы, является экспертная система P-BEST, входящая в состав продукта EMERALD [1]. Недостаток такого подхода в том, что нарушитель может прибегнуть к атаке, в ходе которой он генерирует безупречные с точки зрения политики безопасности запросы. Подобную атаку сигнатурными методами обнаружить невозможно. Способ проведения такой атаки известен: если генерировать поток обычных пакетов очень высокой интенсивности, можно добиться переполнения буфера ресурса и вызвать, таким образом, отказ в обслуживании.

Наибольший интерес представляют методы второго типа, так как они позволяют обнаруживать неизвестные атаки, для которых еще не составлены сигнатуры. Они основаны на сравнении текущих значений параметров субъекта или объекта, собранных за несколько часов со значением этих параметров, собранных за несколько недель или месяцев. Первые параметры составляют краткосрочный профиль активности, а вторые составляют долгосрочный профиль, значение которого является нормой.

Например, в системе NIDES [2] краткосрочный профиль представляет набор значений параметров активности, полученных из нескольких сотен последних записей аудита; долгосрочный профиль формируется из записей аудита, собранных в течение нескольких недель с учетом коэффициента старения данных.

Для исследования вопросов борьбы с перечисленными атаками необходимо научиться моделировать атакующие воздействия. В работе [3] была построена система имитации фонового трафика и потока запросов, созданного атакующим. При этом было сделано допущение, что время между поступлением запросов от легальных пользователей является случайной величиной и имеет нормальное распределение.

Для генерации атакующего трафика создавался поток запросов, не находящих подтверждения установления соединения, которые находятся в буфере в течении некоторого максимального срока, устанавливаемого администратором. При этом запросы генерировались через некоторый заданный интервал времени.

Данная система генерирует трафик по протоколу TCP (затопление SYN-пакетами).

В работе [4] была проведена доработка данной системы, в результате которой были добавлены некоторые протоколы прикладного уровня (SMTP, FTP и HTTP). Так же была добавлена возможность несколько увеличить максимальную интенсивность генерируемого трафика путем создания нескольких независимых процессов генерации.

Основными недостатками разработанной системы являются:

1) ограничение на интервал между генерацией двух запросов (10000 мксек), накладываемое ядром операционной системы Linux 2.4.22 на процессы, выполняемые на прикладном уровне;

2) нераспределенность атакующего трафика, что позволяет атакуемой системе блокировать трафик на основе отслеживания IP-адреса источника запросов;

3) ограниченность протоколами TCP, SMTP, FTP и HTTP.

В дальнейшем предполагается существенная доработка системы имитации трафика путем:

1) встраивание системы генерации в ядро операционной системы с использованием и доработкой существующего в ядре Linux 2.6.9 модуля pktgen;

2) создания системы шаблонов запросов для протоколов прикладного уровня, что приведет к возможности добавлять в систему новые протоколы без необходимости модификации самого модуля;

3) построение модели распределенной атаки путем использования нескольких узлов сети, синхронизированных по некоторому управляющему протоколу;

4) рассмотрение возможности расширения реализуемых моделей атакующего трафика.

Литература

1. Neumann Peter G., Porras Phillip A. Experience with EMERALD to DATE// Computer Science Laboratory SRI International. 1st USENIX Workshop on Intrusion Detection and Network Monitoring. Santa Clara, California, 11–12 April 1999. http://www.csl.sri.com/neumann/det99x.html#IDESFinal92.
2. 29 Javitz H. S., Valdes A., The NIDES Statistical Component: Description and Justification. March 1993 SRI International Menlo Park, California. http://www.sdl.sri.com/nides/reports/statreport.ps.gz.
3. Прищепа Д.С. Дисс. ... магистр техн. н. БГУИР. М. 2004г.
4. Отчет о научно-исследовательской работе "Разработать систему для проведения анализа устойчивости операционных систем (ОС) к воздействию удаленных активных атак и разработать рекомендации

по обеспечению устойчивости ОС, используемых в государственных структурах Республики Беларусь (заключительный)", номер госрегистрации 20013187, Минск, 2004 г.