УДК 004.056.53

А. М. Шуваева[*]

МОДЕЛЬ СИСТЕМЫ ОБНАРУЖЕНИЯ УДАЛЕННЫХ СЕТЕВЫХ АТАК НА ОСНОВЕ СЕТИ ПЕТРИ

Удаленная сетевая атака – информационное разрушающее воздействие на распределенную вычислительную систему, осуществляемое программно по каналам связи.

Для организации коммуникаций в неоднородной сетевой среде применяется набор протоколов *TCP*/*IP*, обеспечивая совместимость между компьютерами разных типов. Данный набор протоколов благодаря совместимости и предоставлению доступа к ресурсам глобальной сети Интернет стал стандартом для межсетевого взаимодействия, но повсеместное распространение обнажило и его слабые стороны. В особенности из-за этого удаленным атакам подвержены распределенные системы, поскольку их компоненты обычно используют открытые каналы передачи данных.

Сетевые атаки на удаленные серверы реализуются с помощью специальных программ – хакерских утилит. Вербальное описание удаленных сетевых атак строится с помощью сигнатур, таких как Land, WinNuke, UDP Flood, Smurf, ARP Spoofing, SYN Flood, SSPing, Ping of Death. Для представления сигнатур атак будем использовать семантические сети, так как они легче всего позволяют перейти от вербального описания к формальному.

Семантическая сеть – это ориентированный граф, вершины которого – понятия, а дуги – отношения между ними [1]. Узлы в семантической сети обычно соответствуют объектам, концепциям, событиям или понятиям. Логический вывод (поиск решения) на семантической сети заключается в том, чтобы найти или сконструировать подсеть, удовлетворяющую некоторым условиям.

Детектирование угрозы в такой сети будет выполняться следующим образом. В результате последовательного прохождения по вершинам такой сети определяются компоненты сигнатуры, совокупность которых характеризует конкретную атаку. Структура разработанной семантической сети позволяет значительно сократить время формирования цепочки соответствующих компонентов сигнатур, на основе группировки характеризующих определенный класс атак компонент и выделения наиболее показательных из них на верхний уровень сети.

---

[*] Работа выполнена под руководством канд. техн. наук, доцента ФГБОУ ВПО «ТГТУ» А. В. Яковлева.

Организация системы защиты сети является сложной задачей, в которой приходится учитывать большое количество параметров. Влияние этих параметров нередко взаимно противоположно, а часто неопределенно и плохо предсказуемо. В такой ситуации полезна система, способная моделировать процесс обнаружения атакующих воздействий в зависимости от наличия различных факторов.

Представим систему обнаружения вторжений в виде сети Петри с последующим ее анализом для получения важной информации о структуре и динамическом поведении моделируемой системы. Эта информация может использоваться для оценки моделируемой системы и выработки предложений по ее усовершенствованию.

Сети Петри – это аппарат для моделирования динамических дискретных систем и определяется как пятерка <P, T, I, O, μ>, где P и T – конечные множества позиций и переходов (табл. 1, 2); I и O – множества входных и выходных функций, μ – маркировка [2].

Известно [2], что сеть Петри выполняется посредством запусков переходов. Формально работа сети Петри описывается множеством последовательностей запусков и множеством реализуемых маркировок.

1. Описание позиций сетевой модели

Позиция	Описание	Позиция	Описание
*P*0	Начало анализа	*P*9	Действия применены
*P*1	Выбраны *ICMP* пакеты	*P*10	Факт атаки зарегистрирован
*P*2	Выбраны *UDP* пакеты	*P*11	Обнаружен разрыв или наложение фрагмента
*P*3	Выбраны *ARP* пакеты	*P*12	Тип *ICMP* пакета равен 0
*P*4	Выбраны *TCP* пакеты	*P*13	Угроза отсутствует
*P*5	Обнаружено изменение *ARP* таблицы	*P*14	Флаг *OOB* обнаружен
*P*6	Обнаружена сетевая атака	*P*15	Обнаружен флаг *SYN*, без *ASK*
*P*7	Угроза идентифицирована	*P*16	Угроза возможна
*P*8	Угроза блокирована	*P*17	Вероятность угрозы рассчитана

Каждому виду атак соответствует конкретная сеть Петри, которая моделирует процесс ее обнаружения. В данном случае цель состоит в том, чтобы показать совокупность условий, необходимых для успешного детектирования атаки. Если эти условия существуют, то можно говорить о том, что атака точно обнаружена. Но если их нет, или они присутствуют частично, то можно говорить о том, что атака отсутствует, либо присутствует с некоторой долей вероятности соответственно.

2. Описание переходов сетевой модели

Переход	Описание	Переход	Описание
*T*0 – *T*3	Для анализа выбираются *ICMP* (*UDP*, *ARP*, *TCP*) пакеты	*T*21	Обнаружение значительного превышения нормы уровня пакетов для *ICMP*
*T*4	Проверка наличия изменения *ARP* таблицы	*T*22	Не удается обнаружить отклонение от нормального уровня *ICMP* пакетов
*T*5	Не удается обнаружить изменение *ARP* таблицы	*T*23	Проверка совпадения портов получателя и отправителя
*T*6	Обнаружение значительного превышения нормы уровня пакетов для *ARP*	*T*24	Проверка совпадения *IP* получателя и отправителя
*T*7	Не удается обнаружить отклонение от нормы уровня *ARP* пакетов	*T*25	Проверка наличия флага *SYN* и отсутствия флага *ASK*
*T*8	Блокирование угрозы	*T*26	Не удается найти характерный признак атаки
*T*9	Выдача сообщения по ликвидации угрозы	*T*27	Проверка наличия флага *OOB*

Продолжение табл. 2

Переход	Описание	Переход	Описание
*T*10	Идентификация угрозы	*T*28	Не удается обнаружить соответствие портов
*T*11	Регистрация факта атаки	*T*29–*T*30	Проверка соответствующих портов получателя и отправителя значению *, 135 (*, 139)
*T*12 – *T*14	Проверка соответсвующих портов получателя и отправителя значению 7, 19 (13, 37, 19)	*T*31	Обнаружение превышения нормального уровня пакетов для *TCP*
*T*15	Не удается обнаружить соответствие портов	*T*32	Не удается обнаружить отклонение от нормального уровня *TCP* пакетов
*T*16	Обнаружение разрыва или наложения фрагмента	*T*33–*T*34	Подготовка системы к новому сканированию
*T*17	Проверка соответствия типа *ICMP* пакета 0	*T*35 – *T*37	Обнаружение превышения нормы уровня пакетов для *TCP* (*ICMP*, *ARP*)
*T*18	Не удается найти характерный признак атаки	*T*38	Расчет вероятности угрозы
*T*19	Поиск пакетов с разрывом или наложением фрагмента	*T*39	Принятие решения о наличии угрозы
*T*20	Не удается найти подобные пакеты	*T*40	Принятие решения об отсутствии угрозы

К статическим свойствам сети относятся: конечное множество позиций, конечное множество состояний, множество входных позиций переходов, множество выходных позиций переходов, начальная мар-

кировка, дерево достижимости [2]. Дерево достижимости представляет все достижимые маркировки сети Петри, а также все возможные последовательности запусков ее переходов.

Полный анализ сети Петри можно провести с помощью изучения и анализа ее динамических свойств: достижимость, ограниченность, активность, обратимость и достижимость тупиковой разметки [2]:

1) достижимость: маркировка μ_n достижима из маркировки μ_0, если существует последовательность запусков, приводящих от μ_0 к μ_n;

2) ограниченность: сеть Петри называется *K*-ограниченной, или просто ограниченной, если для любой маркировки, достижимой от маркировки μ_0, количество фишек в любой позиции не превышает некоторого числа *K*, т.е. $\mu(p) \le K$ для любого *p* и любой маркировки μ, принадлежащей $R(\mu_0)$;

3) активность: сеть Петри активна, если независимо от достигнутой μ_0 маркировки, для любого перехода существует последовательность дальнейших запусков, приводящая к его запуску;

4) обратимость и базовое состояние: сеть Петри обратима, если для любой маркировки μ из $R(\mu_0)$ маркировка μ_0 достижима от μ;

5) достижимость тупиковой разметки делает дальнейшее срабатывание любого перехода в данной сети невозможным [2].

Детектирование угрозы невозможно, пока она себя никак не проявит, следовательно, необходимо некоторое время, в течение которого она выполнит свои деструктивные функции. После этого атаку необходимо блокировать, чтобы она не достигла своего логического завершения.

Таким образом, без использования СОВ время реакции на атакующее воздействия зависит от должностной инструкции администратора по безопасности и чаще всего составляет не менее 24 часов. Такой подход не позволяет оперативно реагировать на атаку и тем более предотвратить ее. Использование разработанной системы обнаружения вторжений позволит значительно снизить время реакции на атакующие воздействия и в значительной мере позволит сократить нанесенный системе ущерб.

Список литературы

1. *Представление* и использование знаний / Х. Уэно и др. ; пер. с япон. – Москва : Мир, 1989. – 220 с.

2. *Питерсон*, *Дж*. Теория сетей Петри и моделирование систем / Дж. Питерсон. – Москва : Мир, 1984. – 264 с.

Кафедра «Информационные системы и защита информации»
ФГБОУ ВПО «ТГТУ»